Network quantum steering enables randomness certification without seed randomness

Shubhayan Sarkar

Laboratoire d'Information Quantique, Université libre de Bruxelles (ULB), Av. F. D. Roosevelt 50, 1050 Bruxelles, Belgium

Quantum networks with multiple sources allow the observation of quantum nonlocality without inputs. Consequently, the incompatibility of measurements is not a necessity for observing quantum nonlocality when one has access to multiple quantum sources. Here we investigate the minimal scenario without inputs where one can observe any form of quantum nonlocality. We show that even two parties with two sources that might be classically correlated can witness a form of quantum nonlocality, in particular quantum steering, in networks without inputs if one of the parties is trusted, that is, performs a fixed known measurement. We term this effect as swap-steering. The scenario presented in this work is minimal to observe such an effect. Consequently, a scenario exists where one can observe quantum steering but not Bell non-locality. We further construct a linear witness to observe swap-steering. Interestingly, this witness enables self-testing of the quantum states generated by the sources and the local measurement of the untrusted party. This in turn allows certifying two bits of randomness that can be obtained from the measurement outcomes of the untrusted device without the requirement of initially feeding the device with randomness.

1 Introduction

Quantum nonlocality is one of the most remarkable features of quantum mechanics that defy our classical intuitions about the world. It refers to the property of quantum particles to exhibit correlations that seem to occur instantaneously even when they are separated by large distances. This quantum property was first conceptualized in the celebrated work of Einstein, Podolsky and Rosen [EPR35]. Based on it, Bell in 1964 [Bel64; Bel66] proposed a theoretical test, known as Bell's inequality, that could distinguish between classical and quantum correlations. It was then experimentally verified [ADR82; AGR81; Giu+15; Sha+15] and is now recognized as a fundamental aspect of quantum mechanics. The implications of quantum nonlocality are far-reaching, with potential applications in fields such as cryptography, quantum teleportation, quantum communication, and quantum computing (refer to [Bru+14] for a review).

Another form of quantum nonlocality, known as quantum steering, allows for one observer to remotely influence the state of another observer's quantum system, even if the two observers are separated by large distances. Quantum steering was first conceptualized by Schrodinger [Sch35] and was then rigorously introduced in [WJD07]. The major difference between the scenarios to observe Bell nonlocality and quantum steering is that one of the parties is assumed to be trusted in the latter one, that is, known to perform fixed measurements.

To observe quantum nonlocality or quantum steering, any party involved in the experiment must have at least two inputs as incompatible measurements are necessary to witness any of these phenomena. Interestingly, quantum networks allow for witnessing such non-classical features without the requirement of incompatibility of measurements. The framework to witness quantum nonlocality in networks was introduced in [BGP10; Bra+12; Fri12]. However, it was first noted in [Bra+12] and then in [Fri12] that considering independent sources shared between non-communicating parties allows one to observe quantum nonlocality with a single fixed measurement for every party. Recently, the authors in [Ren+19; RB22; PGR23; Šup+22] explore this phenomenon to construct scenarios where one can observe genuine quantum network nonlocality.

One of the intriguing problems in this regard concerns the minimal scenario in which any form of quantum nonlocality can be observed without any inputs. It was shown in [Ren+19], that genuine network nonlocality can be observed without inputs if there are three parties with three independent sources. Inspired by entanglement swapping [Zuk+93], we show here that if one of the parties is assumed to be trusted then one can observe a form of quantum nonlocality, which we term as swap-steering, using only two parties and two sources. Unlike most of the considered quantum network scenarios where one assumes independence of the sources [see nevertheless Ref. [SBB20; Sar24a]], we relax this assumption and allow the sources to be classically correlated. Moreover, the swap-steering scenario is the minimal scenario where one can observe a form of quantum nonlocality without inputs. Further on, there is a lack of witnesses when observing quantum nonlocality without inputs in networks. This restricts the possibility of testing these phenomena at the operational level. Interestingly, we find a linear witness to observe swap-steering thus, making our notion of nonlocality experimentally testable. We further identify some states that are unsteerable in the standard quantum steering scenario are swap-steerable. In particular, any entangled two-qubit Werner state is swap-steerable, which can be interpreted as an entanglement-assisted activation of quantum steering.

As an application of our work, we utilize the above result for one-sided device-independent (DI) certification where one can completely characterize the states generated by the sources and the untrusted measurements up to some degrees of freedom. Using the outcomes of the certified measurement, one can then generate genuine randomness even when an intruder might have access to them. This is extremely important for any cryptographic scheme as the security of these schemes relies on access to random number generators. Moreover, any of the known schemes for DI certification of states, measurements or randomness requires access to seed randomness, that is, the measurement devices whose outcomes will be used to generate random numbers, have inputs that have to be chosen randomly in order for the protocol to be secure [for instance see Refs. [Pir+10; Ací+16; Góm+19; And+18; Cur+17; FGS13; NPS14; Tav+21; Šup+16; Sar+21; Bor+22]]. Furthermore, DI certification of quantum states and measurements in quantum networks was recently explored in Refs. [RKB18; ŠB23; Zho+22; Šup+23; Šup+22; SBB23; Sar+23b]. However, all of these certification schemes require at least two inputs for most of the measurement devices. A partial certification scheme was proposed in [SBB23] that utilizes the genuine network nonlocality without inputs in a triangle network [Ren+19]. However, using the proposed scheme [SBB23], one can only conclude that the sources need to prepare entangled states with at least 2.5 % of entanglement of formation and one can securely extract randomness of .04 bits. We utilize the maximal violation of the proposed swap-steering inequality for self-testing the singlet state along with the Bell basis which is then used for generating secured randomness of two bits without the requirement to initially feed the devices with random numbers. This is the first instance where the exact certification of quantum states, measurements, and randomness could be achieved without inputs.

2 The scenario

In this work, we consider the simplest scenario consisting of two parties namely, Alice and Bob in two different labs far away from each other. Both of them receive two subsystems from two different sources S_1, S_2 that might be classically correlated to each other. Now they perform a single four-outcome measurement on their respective subsystems where the outcomes are denoted as $a, b = 0, 1, 2, 3$ respectively for Alice and Bob. Alice is trusted here implying that the measurement performed by her on her subsystems is known (see Fig. 1). We consider here that she performs the measurement corresponding to the Bell basis given by $M_A = \{|\phi_+\rangle\langle\phi_+|, |\phi_-\rangle\langle\phi_-|, |\psi_+\rangle\langle\psi_+|, |\psi_-\rangle\langle\psi_-|\}_{A_1A_2}$ where

$$\begin{aligned} |\phi_\pm\rangle_{A_1A_2} &= \frac{1}{\sqrt{2}}\left(|0\rangle_{A_1}|0\rangle_{A_2} \pm |1\rangle_{A_1}|1\rangle_{A_2}\right) \\ |\psi_\pm\rangle_{A_1A_2} &= \frac{1}{\sqrt{2}}\left(|0\rangle_{A_1}|1\rangle_{A_2} \pm |1\rangle_{A_1}|0\rangle_{A_2}\right). \end{aligned} \tag{1}$$

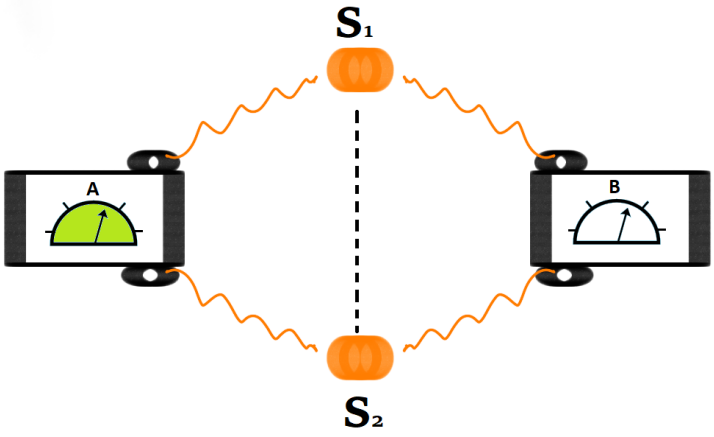

Figure 1: Swap-steering scenario. Alice and Bob are spatially separated and each of them receives two subsystems from the sources S_1, S_2. On the received subsystem they perform a single four-outcome measurement. Alice is trusted here, meaning that she is known to perform the Bell-basis measurement. They are not allowed to communicate during the experiment, however, the sources might classically communicate with each other. Once it is complete, they construct the joint probability distribution $\{p(a,b)\}$.

Here $A_1/A_2, B_1/B_2$ denote the two different subsystems of Alice and Bob respectively. Notice that in the particular case when the sources generate the singlet state, the above scenario is equivalent to entanglement swapping.

Now, Alice and Bob repeat the experiment enough times to construct the joint probability distribution (correlations) $\vec{p} = \{p(a,b)\}$ where $p(a,b)$ denotes the probability of obtaining outcome a, b with Alice and Bob respectively. These probabilities can be computed in quantum theory as

$$p(a,b) = \sum_j p_j \operatorname{Tr}\left[(M^a \otimes N^b)\rho^j_{A_1B_1} \otimes \rho^j_{A_2B_2}\right] \tag{2}$$

where M^a, N^b denote the measurement elements of Alice and Bob which are positive and $\sum_a M^a = \sum_b N^b = 1$ and $\sum_j p_j = 1$. It is important to recall here that Alice and Bob can not communicate with each other during the experiment.

3 Swap-steering

Suppose that there are some variables λ_i that are being sent by the sources S_i as depicted in Fig. 2. Further on, as Alice is known to perform quantum measurements, the variable she receives is some quantum state $\rho_{\lambda_1,\lambda_2}$, however, there is no such restriction on Bob. Let us now state the two assumptions, namely outcome-independence and separable quantum sources, that must be satisfied if Bob is classical, or equivalently if the correlations are not swap-steerable from Bob to Alice.

Assumption 1 (Outcome-independence)**.** *The outcomes of two parties are independent of each other if one has access to the hidden variables λ_i.*

In the scenario considered in this work, Bob's outcome b being independent of Alice's outcome a means that for any $a, b, \lambda_1, \lambda_2$,

$$p(b|\lambda_1, \lambda_2, a) = p(b|\lambda_1, \lambda_2). \tag{3}$$

This is a weaker definition of locality when compared to Bell's assumption of locality, or the notion of locality in the standard quantum steering scenario.

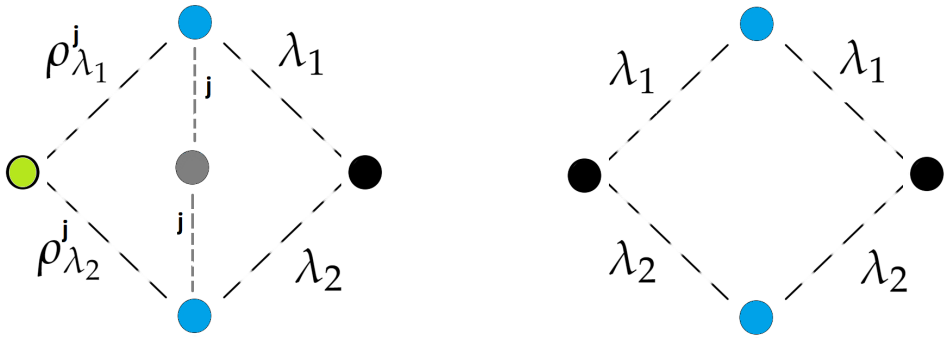

Figure 2: Difference between SOHS and NLHV model in the minimal scenario. (left) Alice and Bob can explain the observed correlations $p(a,b)$ using a SOHS model. Alice is trusted and thus receives quantum states from the sources but there is no restriction over Bob. The grey box denotes an unknown source of classical random variables that might correlate the sources S_1, S_2. (right) Alice and Bob can explain the observed correlations $p(a,b)$ using a NLHV model.

Assumption 2 (Separate quantum sources)**.** *Two sources S_i $(i = 1, 2)$ generating a joint quantum state $\rho_{\lambda_1,\lambda_2}$ are separate if the state $\rho_{\lambda_1,\lambda_2}$ is separable for any λ_1, λ_2.*

Notice that the in above assumption 2, we impose on the sources is weaker when compared to independent quantum sources. As a matter of fact, the above assumption allows the sources to communicate classically with each other or equivalently the sources might generate classically correlated states. Now, given two sources S_i for $i = 1, 2$ that generate some (for now hidden) states λ_i, we can always express the probability $p(a,b)$ as

$$p(a,b) = \sum_{\lambda_1,\lambda_2} p(\lambda_1,\lambda_2)p(a,b|\lambda_1,\lambda_2). \tag{4}$$

Using Bayes rule and the fact that Alice is known to be performing quantum measurements, we can express the above expression as

$$p(a,b) = \sum_{\lambda_1,\lambda_2} p(\lambda_1,\lambda_2)p(a|\rho_{\lambda_1,\lambda_2})p(b|\lambda_1,\lambda_2,a). \tag{5}$$

Assuming outcome-independence, we arrive at

$$p(a,b) = \sum_{\lambda_1,\lambda_2} p(\lambda_1,\lambda_2)p(a|\rho_{\lambda_1,\lambda_2})p(b|\lambda_1,\lambda_2). \tag{6}$$

Now, assuming separable quantum sources [assumption 2] we express $\rho_{\lambda_1,\lambda_2}$ using pure state decompositions to arrive at the following expression of $p(a,b)$

$$p(a,b) = \sum_{\lambda_1,\lambda_2} p(\lambda_1,\lambda_2) \sum_{p^j_{\lambda_1,\lambda_2}} p^j_{\lambda_1,\lambda_2} p(a| \left|\psi^j_{\lambda_1}\right\rangle \left|\psi^j_{\lambda_2}\right\rangle)p(b|\lambda_1,\lambda_2). \tag{7}$$

If correlations $\vec{p}$ admit the form (7), then they are describable using a separable outcome-independent hidden state (SOHS) model. A simple example of the SOHS model would be that sources S_1, S_2 locally toss a coin, that is, $\lambda_{1/2} = \{1(\text{head}),2(\text{tail})\}$ based on which they send a state ρ_λ to Alice and the outcome of the toss to Bob.

To witness swap-steering, a functional W can be constructed which depends on $\vec{p}$ as

$$W(\vec{p}) = \sum_{a,b} c_{a,b}p(a,b) \leq \beta_{SOHS} \tag{8}$$

where $c_{a,b}$ are real coefficients and β_{SOHS} denotes the maximum value attainable using assemblages admitting a SOHS model (7). For the purpose of this article, we consider only functionals that are linear over $\vec{p}$.

Now, consider the following functional

$$W = p(0,0) + p(1,1) + p(2,2) + p(3,3) \leq \beta_{SOHS} \tag{9}$$

Recall here that Alice is trusted and performs the measurements with elements given in (1). Let us now find the maximum value that can be achieved using correlations that admit a SOHS model (7).

Fact 1. *Consider the swap-steering functional W (9). The maximum value β_{SOHS} that can be achieved using correlations that admit a SOHS model (7) of W is $\beta_{SOHS} = \frac{1}{2}$.*

Proof. The proof follows the exact same lines as presented in [SSA22; Sar23; Sar+23a]. Let us consider the steering functional W in Eq. (9) and express it in terms of the SOHS model (7) as

$$\sum_{a=0}^{3} \sum_{\lambda_1,\lambda_2} p(\lambda_1,\lambda_2) p(a|\rho_{\lambda_1,\lambda_2}) p(a|\lambda_1,\lambda_2) \leq \sum_{\lambda_1,\lambda_2} p(\lambda_1,\lambda_2) \max_a \{p(a|\rho_{\lambda_1,\lambda_2})\} \tag{10}$$

where we used the fact that $\sum_a p(a|\lambda_1,\lambda_2) = 1$ for any λ_1, λ_2. Now, maximising over $\rho_{\lambda_1,\lambda_2}$ gives us

$$\sum_{\lambda_1,\lambda_2} p(\lambda_1,\lambda_2) \max_a \{p(a|\rho_{\lambda_1,\lambda_2})\} \leq \sum_{\lambda_1,\lambda_2} p(\lambda_1,\lambda_2) \max_{\rho_{\lambda_1,\lambda_2}} \max_a \{p(a|\rho_{\lambda_1,\lambda_2})\}. \tag{11}$$

Now, using the fact that $\sum_{\lambda_1,\lambda_2} p(\lambda_1,\lambda_2) = 1$ for $i = 1, 2$ allows us to conclude that

$$\beta_{SOHS} \leq \max_{|\psi\rangle_{A_1}, |\psi\rangle_{A_2}} \max_a \{p(a| \ |\psi\rangle_{A_1}, |\psi\rangle_{A_2})\}. \tag{12}$$

As the steering functional W is linear, without loss of generality we consider the maximization only over pure states. Now, putting in the measurement of the trusted Alice (1), which locally acts on qubit Hilbert spaces, and thus optimizing over pure states $|\psi\rangle_{A_1}, |\psi\rangle_{A_2} \in \mathbb{C}^2$ gives us $\beta_{SOHS} \leq \frac{1}{2}$. This bound can be saturated when the sources prepare the maximally mixed $\rho_i = \frac{1}{2}(|00\rangle\langle 00| + |11\rangle\langle 11|)_{A_i B_i}$ and the measurement with Bob is $\{|00\rangle\langle 00|, |01\rangle\langle 01|, |10\rangle\langle 10|, |11\rangle\langle 11|\}$. This state clearly has a SOHS model and thus we get the desired SOHS bound. □

Consider that the sources prepare the state $|\psi_i\rangle = |\phi_+\rangle_{A_i B_i}$ and Bob performs the same measurement as Alice, that is, $M_B = \{|\phi_+\rangle\langle\phi_+|, |\phi_-\rangle\langle\phi_-|, |\psi_+\rangle\langle\psi_+|, |\psi_-\rangle\langle\psi_-|\}_{B_0 B_1}$ where the corresponding states are given in (1). Using these states and Bob's measurement one can simply evaluate the steering functional W in (9) to get the value 1, which is the quantum bound of W. Notice that this is also the algebraic value of W.

Let us also show here that one can not observe Bell-type non-locality with only two parties without inputs. Without loss of generality, we consider here the scenario similar to one depicted in Fig. 1 such that Alice and Bob perform a measurement with arbitrary number of outcomes on subsystems sent by two independent or classically correlated sources. However, unlike the previous scenario, Alice is untrusted. If the correlations $\vec{p} = \{p(a,b)\}$ admit a network-local hidden variable (NLHV) model [Ren+19; Šup+22], then they can be represented as

$$p(a,b) = \sum_{\lambda_1,\lambda_2} p(\lambda_1) p(\lambda_2) p(a|\lambda_1,\lambda_2) p(b|\lambda_1,\lambda_2) \tag{13}$$

for any a, b. Let us state the following fact which is simple to prove.

Fact 2. *Consider the scenario depicted in Fig. 2. The correlations $\vec{p} = \{p(a,b)\}$ obtained by Alice and Bob can always be described by an NLHV model (13).*

Proof. It is well-known that if Alice and Bob do not have inputs in the standard Bell scenario, then any joint correlation can be represented using an LHV model of the form

$$p(a,b) = \sum_{\lambda} p(\lambda)p(a|\lambda)p(b|\lambda). \tag{14}$$

Now, let us consider the scenario depicted in Fig. 2 and consider that Alice and Bob's outcomes are independent of the source S_2 , that is, $p(a|\lambda_2) = p(a)$ and $p(b|\lambda_2) = p(b)$. Now, Eq. (14) can be rewritten using λ_2 and the fact that $\sum_{\lambda_2} p(\lambda_2) = 1$ as

$$p(a,b) = \sum_{\lambda,\lambda_2} p(\lambda)p(\lambda_2)p(a|\lambda,\lambda_2)p(b|\lambda,\lambda_2) \tag{15}$$

which is the form (13). □

The above fact can be straightforwardly generalized to the scenario with arbitrary number of sources between Alice and Bob. It is then well-known that one can not observe any non-locality without inputs when there is a single source distributing subsystems to Alice and Bob. Thus, to observe any form of quantum non-locality in the minimal possible scenario, in the sense that there are no inputs and only two parties, one has to trust either of the parties. Consequently, quantum steering can also be observed in scenarios where one can not observe Bell non-locality. Let us now show that a class of states that is unsteerable in the standard quantum steering scenario is swap-steerable.

3.1 Entanglement assisted activation of steerability

Let us now consider the Werner state given by

$$\rho^W(\alpha) = \alpha\,|\phi_+\rangle\langle\phi_+| + (1-\alpha)\frac{\mathbb{1}}{4}. \tag{16}$$

The above state is separable iff $\alpha \leq \frac{1}{3}$ [Wer89]. As proven in [WJD07; Bow+16], the above state is steerable in the standard quantum steering scenario iff $\alpha > \frac{1}{2}$. Thus, in the range of $\frac{1}{3} < \alpha \leq \frac{1}{2}$, the Werner state is unsteerable but entangled. We show here that the Werner state when coupled with the maximally entangled state is swap-steerable. Thus when assisted with entanglement, unsteerable states can be activated to display steerability without inputs.

Fact 3. *The Werner state $\rho^W(\alpha)$ (16) with the maximally entangled state is swap-steerable for any $\alpha > \frac{1}{3}$.*

Proof. Consider the scenario presented in Fig. 1. Now, suppose that the source S_i generates the state $\rho^W_{A_iB_i}(\alpha_i)$ for $i = 1, 2$. Bob again performs the Bell basis measurement M_B. Given these states and measurements, let us again evaluate the steering functional W in (9) to obtain

$$W = \frac{3\alpha_1\alpha_2 + 1}{4}. \tag{17}$$

As proven above in Fact 1, if $W > \frac{1}{2}$ then the state is swap-steerable from Bob to Alice. Thus, we have from (17) that the Werner state (16) is steerable if $\frac{3\alpha_1\alpha_2+1}{4} > \frac{1}{2}$. Consequently, for any value of $\alpha_1\alpha_2 > \frac{1}{3}$, the Werner states are swap-steerable. Let us now observe that if $\alpha_1 = 1$, that is, the source S_1 generates maximally entangled state, then for any $\alpha_2 > \frac{1}{3}$ the Werner state becomes swap-steerable. □

Thus, some states that are unsteerable in the standard quantum steering scenario can be activated using the maximally entangled state and shown to be swap-steerable. However, we also notice that to observe swap-steering, the states generated by both sources can not be unsteerable simultaneously. Let us now find some necessary conditions to observe swap-steering.

3.2 Necessary conditions for swap-steering

Consider again the scenario depicted in Fig. 1. Notice that one of the trivial necessary conditions to observe swap-steering is that the trusted party, here Alice, needs to perform an entangled measurement. Let us now restrict to the case when the number of outcomes on Bob's side is a composite number, that is, $b = b_0b_1$ where b_0, b_1 are positive integers. Now, Bob's measurement $\{N^b\}$ with $b = b_0b_1$ prepares a set of positive operators on the trusted Alice's side, known as assemblage, denoted as $\{\sigma_b\}$ where $\sigma_b = \sum_j p_j \operatorname{Tr}_B(\mathbb{1}_A \otimes N^b \rho^j_{A_1B_1} \otimes \rho^j_{A_2B_2})$. Now, we show that if the assemblage is of a particular form, one can never observe swap-steering.

Fact 4. *Consider the swap-steering scenario depicted in Fig. 1 where Alice and Bob share the states $\rho_{A_1B_1}, \rho_{A_2B_2}$. Let us assume that Bob performs a $n-$outcome measurement which prepares the assemblage $\{\sigma_{b_0b_1}\}$ on the trusted Alice's side. If $\sigma_{b_0b_1}$ is separable for $b_0 = 0, 1, \ldots, n_1-1$, $b_1 = 0, 1, \ldots, n_2-1$,then there exists a SOHS model for both the states $\rho_{A_1B_1}, \rho_{A_2B_2}$.*

Proof. Let us first notice that

$$\begin{aligned} \sum_{b_0,b_1} \sigma_{b_0b_1} &= \sum_{b_0,b_1,j} p_j \operatorname{Tr}_B(\mathbb{1}_A \otimes N^b \rho^j_{A_1B_1} \otimes \rho^j_{A_2B_2}) \\ &= \sum_j p_j \rho^j_{A_1} \otimes \rho^j_{A_2} \end{aligned} \tag{18}$$

which also allows us to conclude that $\sum_{b_0,b_1} \operatorname{Tr}(\sigma_{b_0b_1}) = 1$. Consider now the assemblage $\{\sigma_{b_0b_1}\}$ is separable, that is, the operators $\sigma_{b_0b_1} = \sum_j \sigma^j_{b_0} \otimes \sigma^j_{b_1}$. Notice that the following states

$$\tilde{\rho}^j_{A_iB_i} = \frac{1}{\mathcal{N}_{i,j}} \sum_{b_i=0}^{n_i-1} \sigma^j_{b_i,A_i} \otimes |b_i\rangle\langle b_i|_{B_i} \tag{19}$$

where $\mathcal{N}_{i,j} = \sum_{b_i} \operatorname{Tr}\left(\sigma^j_{b_i}\right)$ and Bob performing a measurement of the form

$$\tilde{M}_{b_0b_1} = |b_0\rangle\langle b_0|_{B_1} \otimes |b_1\rangle\langle b_1|_{B_2} \tag{20}$$

for $b_i = 0, 1 \ldots, n_i - 1$ give the same assemblage on Alice's side as the states $\sum_j p_j \rho^j_{A_1B_1} \rho^j_{A_2B_2}$ and the measurement $M_b = \{N^b\}$. It is straightforward to observe that the states $\tilde{\rho}_{A_iB_i}$ are separable and thus the $\rho_{A_iB_i}$ admit a SOHS model. □

Consequently, one can observe from Fact 4 that if Bob performs a product measurement, then the states are not swap-steerable from Bob to Alice. Further on, both states prepared from the sources are needed to be entangled to observe swap-steering. Thus, to observe swap-steering both the states and measurements must be entangled.

4 Self-testing and randomness certification

Let us now utilise the above swap-steering inequality (9) for self-testing the quantum realisations suggested after Fact 1. Self-testing in the 1SDI scenario was first defined in Ref. [ŠH16; GWK17]. Inspired by [SSA22; Sar+23a; Sar23], we present a general definition of self-testing in the 1SDI scenario in quantum networks without inputs with one trusted party. Interestingly, we do not require assuming a pure underlying state or projective measurements. For a note, we express the measurements of both parties in the observable picture and represent it as A_0, B_0. For a discussion on observables refer to Appendix A.

Let us revisit the previous experiment in which Alice and Bob conduct measurements on the states ρ_{AB} prepared by the sources S_i $(i = 1, 2)$ and observe the correlations $p(a, b)$. It is important to note that Alice's observables A_0 is fixed, whereas Bob's observables B_0 is arbitrary. Now, let us examine a reference experiment that reproduces the same statistics as the actual experiment but involves the states $\tilde{\rho}_{AB}$ and observables represented by $\tilde{B}_0$, which both parties wish to validate. The states ρ_{AB} and the observables B_0 are self-tested from $\{p(a, b)\}$ if there exists a unitary $U_B : \mathcal{H}_B \to \mathcal{H}_B$ such that

$$(\mathbb{1}_A \otimes U_B)\rho_{AB}(\mathbb{1}_A \otimes U_B^\dagger) = \tilde{\rho}_{AB'} \otimes \rho_{B''}, \tag{21}$$

$$U_B\, B_0\, U_B^\dagger = \tilde{B}_0 \otimes \mathbb{1}_{B''}, \tag{22}$$

where $\mathcal{H}_B$ decomposes as $\mathcal{H}_B = \mathcal{H}_{B'} \otimes \mathcal{H}_{B''}$ such that $\mathcal{H}_{B''}$ denotes the junk Hilbert space. The states $\rho_{B''}$ and $\mathbb{1}_{B''}$ denote the junk state and the identity acting on $\mathcal{H}_{B''}$.

Let us now state our self-testing statement but before proceeding, let us define Alice's observable corresponding to the Bell basis as

$$A_0 = \sum_{k=1}^{4} \mathbb{i}^k \left|\phi_k\right\rangle\!\!\left\langle\phi_k\right| . \tag{23}$$

where $|\phi_1\rangle = |\phi^+\rangle, |\phi_2\rangle = |\psi^+\rangle, |\phi_3\rangle = |\phi^-\rangle, |\phi_4\rangle = |\psi^-\rangle$.

Fact 5. *Assume that the steering inequality (9), with trusted Alice choosing the observable A_0 (33), is maximally violated by a separable state ρ_{AB} acting on $\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathcal{H}_B$ and Bob's observable B_0. Then, the following statements hold true:*

1. Bob's measurement is projective with his Hilbert space decomposing as $\mathcal{H}_B = (\mathbb{C}^2)_{B_1'} \otimes (\mathbb{C}^2)_{B_2'} \otimes \mathcal{H}_{B_{12}''}$ for some auxiliary Hilbert space $\mathcal{H}_{B_{12}''} = \mathcal{H}_{B_1''} \otimes \mathcal{H}_{B_2''}$.

2. There exist unitary transformations, $U_i : \mathcal{H}_B \to \mathcal{H}_B$, such that

$$(\mathbb{1}_A \otimes U_B)\rho_{AB}(\mathbb{1}_A \otimes U_B^\dagger) = \left|\phi^+\right\rangle\!\!\left\langle\phi^+\right|_{A_1B_1'} \otimes \left|\phi^+\right\rangle\!\!\left\langle\phi^+\right|_{A_2B_2'} \otimes \rho_{B_1''B_2''}, \tag{24}$$

where B_i'' denotes Bob's auxiliary system, and

$$U_B\, B_0\, U_B^\dagger = A_0 \otimes \mathbb{1}_{B_1''B_2''} \tag{25}$$

where $U_B = U_1 \otimes U_2$.

The proof of the above fact is given in Appendix A. An interesting application of the above self-testing statement is that the untrusted Bob's measurement device can generate true randomness that is secure against adversaries. For this purpose, we consider an eavesdropper, Eve, who cannot directly read Bob's outcomes but may have correlations with him that she can exploit to infer his results. Consequently, we consider a state ρ_{ABE} which is shared among Alice, Bob and Eve. As Eve's dimension is unrestricted, we can purify the state as $|\psi_{ABE}\rangle$ such that $\mathrm{Tr}_E\, \psi_{ABE} = \rho_{AB}$ where ρ_{AB} is separable.

Now, to certify whether the measurement outcomes as observed by Bob is truly random, we consider that Eve wants to guess the outcome of Bob's measurement. In order to do so, she performs a measurement $Z = \{E_e\}$ on her part of the shared states. Here the outcome e is Eve's best guess of Bob's outcome. However, any operation by Eve should not alter the statistics $\vec{p} = \{p(a,b)\}$ observed by Alice and Bob, that is,

$$p(a,b) = \langle\psi|\, M_a \otimes N_b \otimes \mathbb{1}_E\, |\psi\rangle . \tag{26}$$

This is extremely important as the adversary Eve would like to remain invisible to Alice and Bob.

The number of random bits that can be securely generated from Bob's measurement is quantified as $H_{\min} = -\log_2 G(y,\vec{p})$ [Pir+10], where $G(y,\vec{p})$ is known as the local guessing probability which can be computed as,

$$G(\vec{p}) = \sup_{S \in S_{\vec{p}}} \sum_b \langle\psi|\, \mathbb{1}_A \otimes N_b \otimes E_b\, |\psi\rangle , \tag{27}$$

where $S_{\vec{p}}$ is the set of all Eve's strategies comprising of the shared states and her measurement that reproduce the probability distribution $\vec{p}$ as expected by Alice and Bob.

Let us now suppose that the swap-steering inequality (9) is maximally violated by $\vec{p}$. As proven above in Fact 5, this implies that the state shared by Alice, Bob, and Eve up to local unitary operations is, $|\psi_{ABE}\rangle = \left|\phi^+_{A_1B_1'}\right\rangle \left|\phi^+_{A_2B_2'}\right\rangle \left|\mathrm{aux}_{\mathrm{B}_{12}''\mathrm{E}}\right\rangle$ as well as $N_b = |\phi_b\rangle\!\langle\phi_b| \otimes \mathbb{1}_{\mathrm{B}_{12}''}$ where $|\phi_b\rangle$ are given above Eq. (33). Putting these states and measurement in the formula (27) we obtain

$$G(\vec{p}) = \sum_b \left\langle\phi^+\right| \left\langle\phi^+\right| (\mathbb{1}_A \otimes |\phi_b\rangle\!\langle\phi_b|) \left|\phi^+\right\rangle \left|\phi^+\right\rangle \langle\mathrm{aux}|\, \mathbb{1}_{B_{12''}} \otimes E_b\, |\mathrm{aux}\rangle . \tag{28}$$

Now for all b, $\langle\phi^+|\langle\phi^+|(\mathbb{1}_A \otimes |\phi_b\rangle\langle\phi_b|)|\phi^+\rangle|\phi^+\rangle = 1/4$ which allows us to conclude from (28) that

$$G(\vec{p}) = \frac{1}{4}\sum_b \langle \text{aux}|\, \mathbb{1}_{B_{12}''} \otimes E_b\, |\text{aux}\rangle = \frac{1}{4}. \tag{29}$$

Consequently, $-\log_2 G(\vec{p}) = 2$ bits of randomness can be certified from Bob's measurement outcomes using our self-testing scheme.

It is important to note here that the generation of secure randomness is based on the assumption that the sources can only be correlated in a classical way. However, the adversary can always guess the outcomes of Bob if she manages to entangle the sources. For instance, (i) she can prepare both devices beforehand or (ii) she herself could perform an entangled measurement on the systems arriving on Bob's side and then send the outcome to Bob. This problem would persist in any security protocols involving two different constrained sources. However, the second type of attack (ii) can be avoided if Bob randomly chooses not to perform a measurement in some runs of the experiment. Since Eve is unaware of this fact, she would still entangle both sources and can be detected by Alice. It will be extremely interesting if Alice and Bob can perform some local operations on their subsystems to figure out whether the received subsystems are generated from separable sources or not.

5 Discussions

The idea of quantum steering in networks was introduced recently in [Jon+21]. However, the scenario considered in this work was not dealt with in Ref. [Jon+21]. Further on, the notion of quantum steering in networks [Jon+21] required the trusted party to perform a full tomography which implied that the trusted party has inputs. Contrary to this, in the swap-steering scenario described above even the trusted party performs a single fixed measurement. This also makes our scheme experimentally friendly as one has to consider less number of correlations in order to witness quantum steering in networks. However, the measurement elements of the trusted party are maximally entangled and thus it would be beneficial to explore the possibilities of observing swap-steering with less entangled measurements.

Constructing witnesses to observe quantum nonlocality in networks has been extremely difficult mainly due to the fact that the network-local polytope might not be convex as shown in [BGP10] [see nevertheless Ref. [Sar24a]]. In this work, we find that assuming one of the parties to be trusted allows constructing linear witnesses to observe a form of quantum nonlocality in networks. One of the interesting follow-up directions would be to explore the structure of the set of correlations admitting the SOHS model. We showed in this work that any entangled Werner state can be used to witness swap-steering. An interesting follow-up question is whether every entangled state violates the notion of swap-steering. This problem has now been resolved for every bipartite entangled state in [Sar24b]. Another direction to explore will be toward generalizing the notion of swap-steering to more parties and outcomes. It is known that quantum steering is asymmetric, that is, there are quantum states that are steerable from Alice to Bob but not the other way around. It will be interesting to find similar properties of quantum states when considering the notion of swap-steering. Furthermore, we used swap-steering for the certification of randomness without seed randomness. It will be highly desirable to generalize the above scheme to the DI regime where no party is trusted. Another direction would be to generalize the scheme presented in this work to certify an unbounded amount of randomness. Moreover, it would be interesting to investigate whether the randomness certification can be made robust to experimental imperfections.

Acknowledgments

We would like to thank Stefano Pironio for reviewing the manuscript and providing critical comments that considerably improved the manuscript. This project was funded within the QuantERA II Programme (VERIqTAS project) that has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No 101017733.

References

[Ací+16] Antonio Acín, Stefano Pironio, Tamás Vértesi, and Peter Wittek. "Optimal randomness certification from one entangled bit". **Phys. Rev. A** 93 (2016), p. 040102. DOI: 10.1103/PhysRevA.93.040102.

[ADR82] Alain Aspect, Jean Dalibard, and Gérard Roger. "Experimental Test of Bell's Inequalities Using Time-Varying Analyzers". **Phys. Rev. Lett.** 49 (1982), pp. 1804–1807. DOI: 10.1103/PhysRevLett.49.1804.

[AGR81] Alain Aspect, Philippe Grangier, and Gérard Roger. "Experimental Tests of Realistic Local Theories via Bell's Theorem". **Phys. Rev. Lett.** 47 (1981), pp. 460–463. DOI: 10.1103/PhysRevLett.47.460.

[And+18] 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 (2018), p. 012314. DOI: 10.1103/PhysRevA.97.012314.

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

[Bel66] John S. Bell. "On the Problem of Hidden Variables in Quantum Mechanics". **Rev. Mod. Phys.** 38 (1966), pp. 447–452. DOI: 10.1103/RevModPhys.38.447.

[BGP10] C. Branciard, N. Gisin, and S. Pironio. "Characterizing the Nonlocal Correlations Created via Entanglement Swapping". **Phys. Rev. Lett.** 104 (2010), p. 170401. DOI: 10.1103/PhysRevLett.104.170401.

[Bor+22] Jakub J. Borkała, Chellasamy Jebarathinam, Shubhayan Sarkar, and Remigiusz Augusiak. "Device-Independent Certification of Maximal Randomness from Pure Entangled Two-Qutrit States Using Non-Projective Measurements". **Entropy** 24.3 (2022). ISSN: 1099-4300. DOI: 10.3390/e24030350.

[Bow+16] 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 (2016), p. 022121. DOI: 10.1103/PhysRevA.93.022121.

[Bra+12] Cyril Branciard, Denis Rosset, Nicolas Gisin, and Stefano Pironio. "Bilocal versus nonbilocal correlations in entanglement-swapping experiments". **Phys. Rev. A** 85 (2012), p. 032119. DOI: 10.1103/PhysRevA.85.032119.

[Bru+14] Nicolas Brunner, Daniel Cavalcanti, Stefano Pironio, Valerio Scarani, and Stephanie Wehner. "Bell nonlocality". **Rev. Mod. Phys.** 86 (2014), pp. 419–478. DOI: 10.1103/RevModPhys.86.419.

[Cur+17] F. J. Curchod, M. Johansson, R. Augusiak, M. J. Hoban, P. Wittek, and A. Acín. "Unbounded randomness certification using sequences of measurements". **Phys. Rev. A** 95 (2017), p. 020102. DOI: 10.1103/PhysRevA.95.020102.

[EPR35] A. Einstein, B. Podolsky, and N. Rosen. "Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?" **Phys. Rev.** 47 (1935), pp. 777–780. DOI: 10.1103/PhysRev.47.777.

[FGS13] Serge Fehr, Ran Gelles, and Christian Schaffner. "Security and composability of randomness expansion from Bell inequalities". **Phys. Rev. A** 87 (2013), p. 012335. DOI: 10.1103/PhysRevA.87.012335.

[Fri12] Tobias Fritz. "Beyond Bell's theorem: correlation scenarios". **New Journal of Physics** 14.10 (2012), p. 103001. DOI: 10.1088/1367-2630/14/10/103001.

[Giu+15] Marissa Giustina et al. "Significant-Loophole-Free Test of Bell's Theorem with Entangled Photons". **Phys. Rev. Lett.** 115 (2015), p. 250401. DOI: 10.1103/PhysRevLett.115.250401.

[Góm+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 (2019), p. 032108. DOI: 10.1103/PhysRevA.99.032108.

[GWK17] Alexandru Gheorghiu, Petros Wallden, and Elham Kashefi. “Rigidity of quantum steering and one-sided device-independent verifiable quantum computation”. **New J. Phys.** 19.2 (2017), p. 023043. DOI: 10.1088/1367-2630/aa5cff.

[Jon+21] Benjamin D. M. Jones, Ivan Šupić, Roope Uola, Nicolas Brunner, and Paul Skrzypczyk. “Network Quantum Steering”. **Phys. Rev. Lett.** 127 (2021), p. 170405. DOI: 10.1103/PhysRevLett.127.170405.

[Kan+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 (2019), p. 198. ISSN: 2521-327X. DOI: 10.22331/q-2019-10-24-198.

[NPS14] O Nieto-Silleras, S Pironio, and J Silman. “Using complete measurement statistics for optimal device-independent randomness evaluation”. **New Journal of Physics** 16.1 (2014), p. 013035. DOI: 10.1088/1367-2630/16/1/013035.

[PGR23] Alejandro Pozas-Kerstjens, Nicolas Gisin, and Marc-Olivier Renou. “Proofs of Network Quantum Nonlocality in Continuous Families of Distributions”. **Phys. Rev. Lett.** 130 (2023), p. 090201. DOI: 10.1103/PhysRevLett.130.090201.

[Pir+10] S. Pironio et al. “Random numbers certified by Bell’s theorem”. **Nature** 464.7291 (2010), pp. 1021–1024. ISSN: 1476-4687. DOI: 10.1038/nature09008.

[RB22] Marc-Olivier Renou and Salman Beigi. “Nonlocality for Generic Networks”. **Phys. Rev. Lett.** 128 (2022), p. 060401. DOI: 10.1103/PhysRevLett.128.060401.

[Ren+19] Marc-Olivier Renou, Elisa Bäumer, Sadra Boreiri, Nicolas Brunner, Nicolas Gisin, and Salman Beigi. “Genuine Quantum Nonlocality in the Triangle Network”. **Phys. Rev. Lett.** 123 (2019), p. 140401. DOI: 10.1103/PhysRevLett.123.140401.

[RKB18] Marc-Olivier Renou, Jedrzej Kaniewski, and Nicolas Brunner. “Self-Testing Entangled Measurements in Quantum Networks”. **Phys. Rev. Lett.** 121 (2018), p. 250507. DOI: 10.1103/PhysRevLett.121.250507.

[Sar+21] Shubhayan Sarkar, Debashis Saha, Jędrzej Kaniewski, and Remigiusz Augusiak. **npj Quantum Information** 7 (2021), p. 151. DOI: 10.1038/s41534-021-00490-3.

[Sar+23a] Shubhayan Sarkar, Jakub J. Borkała, Chellasamy Jebarathinam, Owidiusz Makuta, Debashis Saha, and Remigiusz Augusiak. “Self-Testing of any Pure Entangled State with the Minimal Number of Measurements and Optimal Randomness Certification in a One-Sided Device-Independent Scenario”. **Phys. Rev. Appl.** 19 (2023), p. 034038. DOI: 10.1103/PhysRevApplied.19.034038.

[Sar+23b] Shubhayan Sarkar, Chandan Datta, Saronath Halder, and Remigiusz Augusiak. **Self-testing composite measurements and bound entangled state in a unified framework**. 2023. DOI: 10.48550/arXiv.2301.11409. arXiv: 2301.11409 [quant-ph].

[Sar23] Shubhayan Sarkar. “Certification of the maximally entangled state using nonprojective measurements”. **Phys. Rev. A** 107 (2023), p. 032408. DOI: 10.1103/PhysRevA.107.032408.

[Sar24a] Shubhayan Sarkar. “Causal links between operationally independent events in quantum theory”. **Physical Review A** 109.4 (2024). ISSN: 2469-9934. DOI: 10.1103/physreva.109.l040202.

[Sar24b] Shubhayan Sarkar. **Witnessing network steerability of every bipartite entangled state without inputs**. 2024. DOI: 10.48550/arXiv.2406.11994. arXiv: 2406.11994 [quant-ph].

[ŠB23] Ivan Šupić and Nicolas Brunner. “Self-testing nonlocality without entanglement”. **Physical Review A** 107.6 (2023). ISSN: 2469-9934. DOI: 10.1103/physreva.107.062220.

[SBB20] Ivan Šupi ć, Jean-Daniel Bancal, and Nicolas Brunner. “Quantum Nonlocality in Networks Can Be Demonstrated with an Arbitrarily Small Level of Independence between the Sources”. **Phys. Rev. Lett.** 125 (2020), p. 240403. DOI: 10.1103/PhysRevLett.125.240403.

[SBB23] Pavel Sekatski, Sadra Boreiri, and Nicolas Brunner. "Partial Self-Testing and Randomness Certification in the Triangle Network". **Phys. Rev. Lett.** 131 (2023), p. 100201. DOI: 10.1103/PhysRevLett.131.100201.

[Sch35] E. Schrödinger. "Discussion of Probability Relations between Separated Systems". **Mathematical Proceedings of the Cambridge Philosophical Society** 31.4 (1935), pp. 555–563. DOI: 10.1017/S0305004100013554.

[ŠH16] Ivan Šupić and Matty J Hoban. "Self-testing through EPR-steering". **New J. Phys.** 18.7 (2016), p. 075006. DOI: 10.1088/1367-2630/18/7/075006.

[Sha+15] Lynden K. Shalm et al. "Strong Loophole-Free Test of Local Realism". **Phys. Rev. Lett.** 115 (2015), p. 250402. DOI: 10.1103/PhysRevLett.115.250402.

[SSA22] Shubhayan Sarkar, Debashis Saha, and Remigiusz Augusiak. "Certification of incompatible measurements using quantum steering". **Phys. Rev. A** 106 (2022), p. L040402. DOI: 10.1103/PhysRevA.106.L040402.

[Šup+16] Ivan Šupić, Remiguisz Augusiak, Alexia Salavrakos, and Antonio Acín. "Self-testing protocols based on the chained Bell inequalities". **New J. Phys.** 18.3 (2016), p. 035013. DOI: 10.1088/1367-2630/18/3/035013.

[Šup+22] Ivan Šupić, Jean-Daniel Bancal, Yu Cai, and Nicolas Brunner. "Genuine network quantum nonlocality and self-testing". **Phys. Rev. A** 105 (2022), p. 022206. DOI: 10.1103/PhysRevA.105.022206.

[Šup+23] Ivan Šupić, Joseph Bowles, Marc-Olivier Renou, Antonio Acín, and Matty J. Hoban. "Quantum networks self-test all entangled states". **Nature Physics** 19.5 (2023), pp. 670–675. ISSN: 1745-2481. DOI: 10.1038/s41567-023-01945-4.

[Tav+21] Armin Tavakoli, Máté Farkas, Denis Rosset, Jean-Daniel Bancal, and Jedrzej Kaniewski. "Mutually unbiased bases and symmetric informationally complete measurements in Bell experiments". **Science Advances** 7.7 (2021). DOI: 10.1126/sciadv.abc3847.

[Wer89] Reinhard F. Werner. "Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model". **Phys. Rev. A** 40 (1989), pp. 4277–4281. 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 (2007), p. 140402. DOI: 10.1103/PhysRevLett.98.140402.

[Zho+22] Qing Zhou, Xin-Yu Xu, Shuai Zhao, Yi-Zheng Zhen, Li Li, Nai-Le Liu, and Kai Chen. "Robust self-testing of multipartite Greenberger-Horne-Zeilinger-state measurements in quantum networks". **Phys. Rev. A** 106 (2022), p. 042608. DOI: 10.1103/PhysRevA.106.042608.

[Zuk+93] M. Zukowski, A. Zeilinger, M. A. Horne, and A. K. Ekert. ""Event-ready-detectors" Bell experiment via entanglement swapping". **Phys. Rev. Lett.** 71 (1993), pp. 4287–4290. DOI: 10.1103/PhysRevLett.71.4287.

6 Appendix

A Self-testing

In quantum theory, it is advantageous to express the correlations $\{p(a,b)\}$in terms of expectation values rather than probability distributions. When dealing with d-outcome measurements, a useful technique is to utilize the two-dimensional Fourier transform of the conditional probabilities $p(a,b)$ as

$$\langle A_0^{(k)} B_0^{(l)} \rangle = \sum_{a,b=0}^{d-1} \omega^{ak+bl} p(a,b), \tag{30}$$

where ω is the d-th root of unity $\omega = \exp(2\pi \mathrm{i}/d)$ and $k, l = 0, \ldots, d-1$ and $A_0^{(k)}, B_0^{(l)}$ are known as observables. Using the inverse Fourier transform of (30), we obtain that

$$p(a,b) = \frac{1}{d^2} \sum_{k,l=0}^{d-1} \omega^{-(ak+bl)} \langle A_0^{(k)} B_0^{(l)} \rangle. \tag{31}$$

The expectation value appearing on the left-hand side of Eq. (30) can be simply represented as $\langle A_0^{(k)} B_0^{(l)} \rangle = \mathrm{Tr}\Big(A_0^{(k)} \otimes B_0^{(l)} \rho_{AB}\Big)$ for some state ρ_{AB} with $\{A_0^{(k)}\}$ and $\{B_0^{(l)}\}$ are operators defined as

$$A_0^{(k)} = \sum_{a=0}^{d-1} \omega^{ak} P^{(a)}, \qquad B_0^{(l)} = \sum_{b=0}^{d-1} \omega^{bl} Q^{(b)}. \tag{32}$$

where $P^{(a)}, Q^{(b)}$ represent the measurement elements of Alice, Bob respectively. As proven in [Kan+19], the observables $A_0^{(k)}$ have the following properties (same for $B_0^{(l)}$): $A_0^{(d-k)} = (A_0^{(k)})^\dagger$ and $A_0^{(k)}(A_0^{(k)})^\dagger \leq \mathbb{1}$. For the special case of projective measurements, the observables $A_0^{(k)}$ are unitary and $A_0^{(k)} = (A_0^{(1)})^k = A_0^k$. As Alice performs the Bell-basis measurement whose corresponding measurement elements for the rest of the manuscript will be denoted as $|\phi_1\rangle = |\phi^+\rangle, |\phi_2\rangle = |\psi^+\rangle, |\phi_3\rangle = |\phi^-\rangle, |\phi_4\rangle = |\psi^-\rangle$ and the corresponding observable using (32) is given as

$$A_0 = \sum_{k=1}^{4} \mathrm{i}^k \, |\phi_k\rangle\langle\phi_k| \, . \tag{33}$$

Let us first revisit the swap-steering inequality (9) and then using (31), the above steering inequality can be simply represented as

$$W = \frac{1}{4} \sum_{k=0}^{3} \langle A_0^k \otimes B_0^{(4-k)} \rangle \leq \beta_{LHS} \tag{34}$$

The quantum bound of the above steering inequality is 1 which is also the maximum algebraic value of W. Consequently, we observe from (34) that the maximum value can be attained iff each term is 1, that is, for $k = 0, 1, 2, 3$

$$\langle A_0^k \otimes B_0^{(4-k)} \rangle = 1. \tag{35}$$

Now, using Cauchy-Schwarz inequality we get that

$$A_0^k \otimes B_0^{(4-k)} \rho_{AB} = \rho_{AB}. \tag{36}$$

Recalling that ρ_{AB} is separable, we can express it as $\rho_{AB} = \sum_j p_j \; \rho^j_{A_1B_1} \otimes \rho^j_{A_2B_2}$ which using its eigendecomposition can be expressed as $\rho_{AB} = \sum_{s,s'} p_{s,s'} \, |\psi_{s,A_1B_1}\rangle\langle\psi_{s,A_1B_1}| \otimes |\psi_{s',A_2B_2}\rangle\langle\psi_{s',A_2B_2}|$. Consequently, we get from the above expression Eq. (38) that

$$\sum_{s,s'} p_{s,s'} A_0^k \otimes B_0^{(4-k)} \; \psi_s^1 \otimes \psi_{s'}^2 = \sum_{s,s'} p_{s,s'} \; \psi_s^1 \otimes \psi_{s'}^2 \tag{37}$$

where for simplicity, we represent the states $|\psi_{s,A_iB_i}\rangle\langle\psi_{s,A_iB_i}|$ as ψ_s^i. It is now straightforward to observe from the above relation that for all s, s'

$$A_0^k \otimes \overline{B}_{0,ss'}^{4-k} \;\; |\psi_s^1\rangle \, |\psi_{s'}^2\rangle = |\psi_s^1\rangle \, |\psi_{s'}^2\rangle \tag{38}$$

Here $\overline{B}_{0,ss'}$ is the projection of B_0 on the support of $\mathrm{Tr}_A \, \psi_s^1 \otimes \mathrm{Tr}_A \, \psi_{s'}^2$. The above relations are sufficient to self-test the state ρ_{AB} and Bob's measurement B_0. Before proceeding toward the self-testing result, it is important to recall the assumption that the local states are full-rank as the measurements can only be characterized on the local support of the states. For a note, we closely follow the techniques introduced in [SSA22].

Fact 5. *Assume that the steering inequality (34), with trusted Alice choosing the observable A_0 (33), is maximally violated by a separable state ρ_{AB} acting on $\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathcal{H}_B$ and Bob's observable B_0. Then, the following statements hold true:*

1. Bob's measurement is projective with his Hilbert space decomposing as $\mathcal{H}_B = (\mathbb{C}^2)_{B_1'} \otimes (\mathbb{C}^2)_{B_2'} \otimes \mathcal{H}_{B_{12}''}$ for some auxiliary Hilbert space $\mathcal{H}_{B_{12}''} = \mathcal{H}_{B_1''} \otimes \mathcal{H}_{B_2''}$.

2. There exist unitary transformations, $U_i : \mathcal{H}_B \to \mathcal{H}_B$, such that

$$\begin{aligned}&(\mathbb{1}_A \otimes U_B)\rho_{AB}(\mathbb{1}_A \otimes U_B^\dagger)\\ &= \left|\phi^+\right\rangle\!\left\langle\phi^+\right|_{A_1B_1'} \otimes \left|\phi^+\right\rangle\!\left\langle\phi^+\right|_{A_2B_2'} \otimes \rho_{B_1''B_2''},\end{aligned} \tag{39}$$

where B_i'' denotes Bob's auxiliary system, and

$$U_B\, B_0\, U_B^\dagger = A_0 \otimes \mathbb{1}_{B_1''B_2''} \tag{40}$$

where $U_B = U_1 \otimes U_2$.

Proof. Let us first show that Bob's measurement is projective. For this purpose, we consider the relations (36) for $k = 1$ and then multiply it with $A_0^3 \otimes B_0$ to obtain

$$\mathbb{1}_A \otimes B_0 B_0^{(3)}\ \rho_{AB} = A_0^3 \otimes B_0\ \rho_{AB} \tag{41}$$

where we used the fact that $A_0^4 = \mathbb{1}_A$. Notice that the right-hand side of the above expression (41) can be simplified using the relation (36) for $k = 3$ to obtain

$$\mathbb{1}_A \otimes B_0 B_0^{(3)}\ \rho_{AB} = \rho_{AB}. \tag{42}$$

Thus, taking a partial trace over Alice's subsystem and recalling that $B_0^{(3)} = B_0^\dagger$ gives us

$$B_0 B_0^\dagger\ \rho_B = \rho_B \tag{43}$$

where $\rho_B = \mathrm{Tr}_B\ \rho_{AB}$. As the local states are full-rank, they are invertible too and consequently one can arrive at

$$B_0 B_0^\dagger = \mathbb{1}_B. \tag{44}$$

Similarly, one can also find that $B_0^\dagger B_0 = \mathbb{1}_B$. Both these relations of Bob's observable suggest that the observable B_0 and unitary, and thus Bob's measurement is projective. In a similar manner, considering the relation (38) one can observe that $\overline{B}_{0,ss'}$ for all s, s' are unitary.

Let us now consider the relation Eq. (38) and characterize the states $\left|\psi_s^1\right\rangle, \left|\psi_{s'}^2\right\rangle$ that satisfy the relation (38). For simplicity, we drop the indices s, s' for now. As the local states on Alice's side belong to $\mathbb{C}^2$, using Schmidt decomposition we represent $\left|\psi^1\right\rangle, \left|\psi^2\right\rangle$ as

$$\left|\psi^i\right\rangle = \sum_{j=0,1} \lambda_{j,i} \left|e_{j,i}\right\rangle \left|f_{j,i}\right\rangle \tag{45}$$

where $\lambda_{j,i} \geq 0$ and $\{|e_{j,i}\rangle\}, \{|f_{j,i}\rangle\}$ form an orthonormal basis for each i. Now applying a unitary U_i on these states such that $U_i \left|f_{j,i}\right\rangle = \left|e_{j,i}^*\right\rangle$ gives us

$$\left|\tilde{\psi}^i\right\rangle = U_i \left|\psi^i\right\rangle = \sum_{j=0,1} \lambda_{j,i} \left|e_{j,i}\right\rangle \left|e_{j,i}^*\right\rangle. \tag{46}$$

Now, notice that the state on the right-hand side can be represented as

$$\left|\tilde{\psi}^i\right\rangle = P_i \otimes \mathbb{1}_{B_i} \left|\phi^+\right\rangle \tag{47}$$

where

$$P_i = \sqrt{2} \sum_{j=0,1} \lambda_{j,i} \left|e_{j,i}\right\rangle\!\left\langle e_{j,i}\right|. \tag{48}$$

Notice that P_i is full-rank as states that are separable between Alice and Bob can not violate the swap-steering inequality (9). Putting the state (47) in the relation (38) gives us

$$A_0(P_1 \otimes P_2) \otimes \tilde{B}_0^\dagger \left|\phi^+\right\rangle \left|\phi^+\right\rangle = P_1 \otimes P_2 \left|\phi^+\right\rangle \left|\phi^+\right\rangle \tag{49}$$

where $\tilde{B}_0 = U_1^\dagger \otimes U_2^\dagger \ \overline{B}_0 \ U_1 \otimes U_2$. Now, using the fact that

$$\left|\phi^+\right\rangle_{A_1B_1} \left|\phi^+\right\rangle_{A_2B_2} = \left|\phi_4^+\right\rangle_{A_1A_2|B_1B_2} \tag{50}$$

where $\left|\phi_4^+\right\rangle$ is the maximally entangled state of local dimension four. This allows us to conclude from (49) that

$$(P_1^{-1} \otimes P_2^{-1})A_0(P_1 \otimes P_2) \otimes \tilde{B}_0^\dagger \ \left|\phi_4^+\right\rangle = \left|\phi_4^+\right\rangle. \tag{51}$$

Now, using the fact that $R \otimes Q \left|\phi^+\right\rangle = RQ^T \otimes \mathbb{1} \left|\phi^+\right\rangle$, where T denotes the transpose in the computational basis, gives us

$$(P_1^{-1} \otimes P_2^{-1})A_0(P_1 \otimes P_2)\tilde{B}_0^* \otimes \mathbb{1}_B \left|\phi_4^+\right\rangle = \left|\phi_4^+\right\rangle. \tag{52}$$

Taking the partial trace over $B's$ subsystem allows us to conclude that

$$(P_1^{-1} \otimes P_2^{-1})A_0(P_1 \otimes P_2)\tilde{B}_0^* = \mathbb{1}_A \tag{53}$$

which eventually leads us to Bob's measurement being

$$\tilde{B}_0^T = (P_1^{-1} \otimes P_2^{-1})A_0(P_1 \otimes P_2). \tag{54}$$

As $\tilde{B}_0$ is unitary and P_1, P_2 are Hermitian, we get from the above condition that

$$(P_1^{-1} \otimes P_2^{-1})A_0(P_1 \otimes P_2)^2 A_0^\dagger (P_1^{-1} \otimes P_2^{-1}) = \mathbb{1}_A. \tag{55}$$

Rearranging the terms we obtain that

$$A_0(P_1 \otimes P_2)^2 = (P_1 \otimes P_2)^2 A_0 \tag{56}$$

which is equivalent to

$$[A_0, (P_1 \otimes P_2)^2] = 0. \tag{57}$$

Now, notice that if two matrices commute then they share the same basis. However, the matrix A_0 has an entangled basis and the matrix $P_1 \otimes P_2$ have a product basis. Thus, the only instance for these two matrices to commute is when $P_1 \otimes P_2 = \mathbb{1}$ which imposes that $P_1 = P_2 = \mathbb{1}$. Going back to Eq. (47) allows us to conclude that the states $\left|\psi^1\right\rangle, \left|\psi^2\right\rangle$ are the maximally entangled state, that is,

$$\mathbb{1}_A \otimes U_i \left|\psi^i\right\rangle = \left|\phi^+\right\rangle \quad i = 1, 2 \tag{58}$$

and Bob's measurement using (54) is

$$U_1^\dagger \otimes U_2^\dagger \ \overline{B}_0 \ U_1 \otimes U_2 = A_0^T = A_0. \tag{59}$$

Let us now bring back the indices s, s' and rewrite the states and measurements as

$$\left|\psi_s^i\right\rangle = \frac{1}{\sqrt{2}} \sum_{j=0,1} |j\rangle \left|f_{j,i,s}\right\rangle \tag{60}$$

where $U_{s,i}^\dagger |j\rangle = |f_{j,i,s}\rangle$ and

$$\overline{B}_{0,ss'} = U_{s,1} \otimes U_{s',2} \ A_0 \ U_{s,1}^\dagger \otimes U_{s',2}^\dagger \tag{61}$$

for all s, s'. From Theorem 1.1 of [SSA22], we can express B_0 as

$$B_0 = \overline{B}_{0,ss'} \oplus E_{ss'} \tag{62}$$

where $E_{ss'}$ are unitary matrices.

Let us now denote Bob's local support of the states $\left|\psi_s^i\right\rangle$ as $V_{i,s} = \text{span}\{|f_{0,i,s}\rangle\langle f_{0,i,s}|, |f_{1,i,s}\rangle\langle f_{1,i,s}|\}$ for all i, s. Further on, we will show that the supports $V_{i,l}, V_{i,l'}$ are orthogonal for any l, l'. For this purpose, we first express the product of the states $\left|\psi_s^1\right\rangle \left|\psi_{s'}^2\right\rangle$ as

$$\left|\psi_s^1\right\rangle \left|\psi_{s'}^2\right\rangle = \frac{1}{2} \sum_{i,j=0,1} |ij\rangle \, |f_{i,1,s}\rangle \, |f_{j,2,s'}\rangle \tag{63}$$

which can equivalently be expressed using the Bell basis as

$$\left|\psi_s^1\right\rangle \left|\psi_{s'}^2\right\rangle = \frac{1}{2} \sum_{i=1}^{4} |\phi_i\rangle \left|g_{ss'}^i\right\rangle \tag{64}$$

where $|\phi_i\rangle$ are given just above Eq. (33) and

$$\begin{aligned}
\left|g_{ss'}^1\right\rangle &= \frac{1}{\sqrt{2}} \left(|f_{0,1,s}\rangle \, |f_{0,2,s'}\rangle + |f_{1,1,s}\rangle \, |f_{1,2,s'}\rangle\right) \\
\left|g_{ss'}^2\right\rangle &= \frac{1}{\sqrt{2}} \left(|f_{0,1,s}\rangle \, |f_{1,2,s'}\rangle + |f_{1,1,s}\rangle \, |f_{0,2,s'}\rangle\right) \\
\left|g_{ss'}^3\right\rangle &= \frac{1}{\sqrt{2}} \left(|f_{0,1,s}\rangle \, |f_{0,2,s'}\rangle - |f_{1,1,s}\rangle \, |f_{1,2,s'}\rangle\right) \\
\left|g_{ss'}^4\right\rangle &= \frac{1}{\sqrt{2}} \left(|f_{0,1,s}\rangle \, |f_{1,2,s'}\rangle - |f_{1,1,s}\rangle \, |f_{0,2,s'}\rangle\right)
\end{aligned} \tag{65}$$

Let us again utilize the relation (38) and apply the state (64) to it to observe that

$$\sum_{i=1}^{4} \omega^i \, |\phi_i\rangle \, B_0^3 \left|g_{ss'}^i\right\rangle = \sum_{i=1}^{4} |\phi_i\rangle \left|g_{ss'}^i\right\rangle . \tag{66}$$

Multiplying with $\langle\phi_i|$ on both sides of the above expression gives us

$$\omega^i B_0^3 \left|g_{ss'}^i\right\rangle = \left|g_{ss'}^i\right\rangle \qquad \forall i. \tag{67}$$

As B_0 is unitary, we can conclude from the above formula (67) that

$$\langle g_{ll'}^j \left|g_{ss'}^i\right\rangle = 0 \qquad i \neq j \tag{68}$$

for any i, j, l, l', s, s'. Let us now consider Eq. (68) with $l = s, j = 1$ and expand it using (65) to obtain the following conditions for $i = 2, 3, 4$ as

$$\langle f_{0,2,l'} \left|f_{0,2,s'}\right\rangle - \langle f_{1,2,l'} \left|f_{1,2,s'}\right\rangle = 0 \tag{69a}$$

$$\langle f_{0,2,l'} \left|f_{1,2,s'}\right\rangle + \langle f_{1,2,l'} \left|f_{0,2,s'}\right\rangle = 0 \tag{69b}$$

$$\langle f_{0,2,l'} \left|f_{1,2,s'}\right\rangle - \langle f_{1,2,l'} \left|f_{0,2,s'}\right\rangle = 0. \tag{69c}$$

From Eqs. (69b) and (69c), it is straightforward to observe that $\langle f_{0,2,l'} \left|f_{1,2,s'}\right\rangle = \langle f_{1,2,l'} \left|f_{0,2,s'}\right\rangle = 0$. Let us now recall that $\left|\psi_{l'}^2\right\rangle$ and $\left|\psi_{s'}^2\right\rangle$ are orthogonal as they correspond to two different eigenvectors of ρ_{AB} which gives us an additional condition

$$\langle f_{0,2,l'} \left|f_{0,2,s'}\right\rangle + \langle f_{1,2,l'} \left|f_{1,2,s'}\right\rangle = 0. \tag{70}$$

It is again straightforward to observe from (69a) and (70) that $\langle f_{0,2,l'} \left|f_{0,2,s'}\right\rangle = \langle f_{1,2,l'} \left|f_{1,2,s'}\right\rangle = 0$. Thus, the local supports $V_{2,s'}$ and $V_{2,l'}$ are orthogonal for any s', l' such that $s' \neq l'$. Proceeding the same way as above, we can also conclude that the local supports $V_{1,s}$ and $V_{1,l}$ are orthogonal for any s, l such that $s \neq l$. Consequently, the local supports $V_{ss'} = V_{1,s} \otimes V_{2,s'}$ are mutually orthogonal for any s, s'.

The local supports $V_{ss'}$ being mutually orthogonal imply that Bob's Hilbert space admits the following decomposition

$$\mathcal{H}_B = \bigoplus_s \bigoplus_{s'} V_{ss'} = \bigoplus_s V_{1,s} \otimes \bigoplus_{s'} V_{2,s'}. \tag{71}$$

As $\dim V_{1,s} = \dim V_{2,s'} = 2$ for any s, s', we can straightforwardly conclude that $\mathcal{H}_B = (\mathbb{C}^2)_{B_1'} \otimes (\mathbb{C}^2)_{B_1'} \otimes \mathcal{H}_{B_{12}''}$ where $\mathcal{H}_{B_1''} \otimes \mathcal{H}_{B_2''}$ for some Hilbert spaces $\mathcal{H}_{B_i''}$.

The rest of the proof is exactly the same as step 3 in Theorem 1.2 of [SSA22], which allows us conclude that there exist unitary transformations, $U_i : \mathcal{H}_B \to \mathcal{H}_B$, such that

$$(\mathbb{1}_A \otimes U_1 \otimes U_2)\rho_{AB}(\mathbb{1}_A \otimes U_1^\dagger \otimes U_2^\dagger) = \left|\phi^+\right\rangle\!\left\langle\phi^+\right|_{A_1B_1'} \otimes \left|\phi^+\right\rangle\!\left\langle\phi^+\right|_{A_2B_2'} \otimes \rho_{B_1''B_2''}, \tag{72}$$

where $\rho_{B_1''B_2''}$ denotes Bob's auxiliary state which is separable with

$$U_i = \bigoplus_s U_{s,i} \qquad i = 1, 2 \tag{73}$$

and

$$U_1 \otimes U_2 \, B_0 \, U_1^\dagger \otimes U_2^\dagger = A_0 \otimes \mathbb{1}_{B_1''B_2''}. \tag{74}$$

This completes the proof. □