



PAPER • OPEN ACCESS

Sequential random access codes and self-testing of quantum measurement instruments

To cite this article: Karthik Mohan *et al* 2019 *New J. Phys.* **21** 083034

View the [article online](#) for updates and enhancements.

You may also like

- [Development of a quasi-ring airy vortex beam using an all-dielectric geometric phase metasurface](#)

Kaixiang Cheng, Zheng Da Hu, Jingjing Wu *et al.*

- [A quantum deep convolutional neural network for image recognition](#)

YaoChong Li, Ri-Gui Zhou, RuQing Xu *et al.*

- [Multiparty quantum random access codes](#)

Debashis Saha and Jakub J. Borkaa



PAPER

Sequential random access codes and self-testing of quantum measurement instruments

OPEN ACCESS

RECEIVED

21 May 2019

REVISED

12 July 2019

ACCEPTED FOR PUBLICATION

31 July 2019

PUBLISHED

20 August 2019

Karthik Mohan, Armin Tavakoli and Nicolas Brunner

Département de Physique Appliquée, Université de Genève, CH-1211 Genève, Switzerland

E-mail: armin.tavakoli@unige.ch**Keywords:** random access code, quantum correlations, self-testing

Original content from this work may be used under the terms of the [Creative Commons Attribution 3.0 licence](https://creativecommons.org/licenses/by/4.0/).

Any further distribution of this work must maintain attribution to the author(s) and the title of the work, journal citation and DOI.



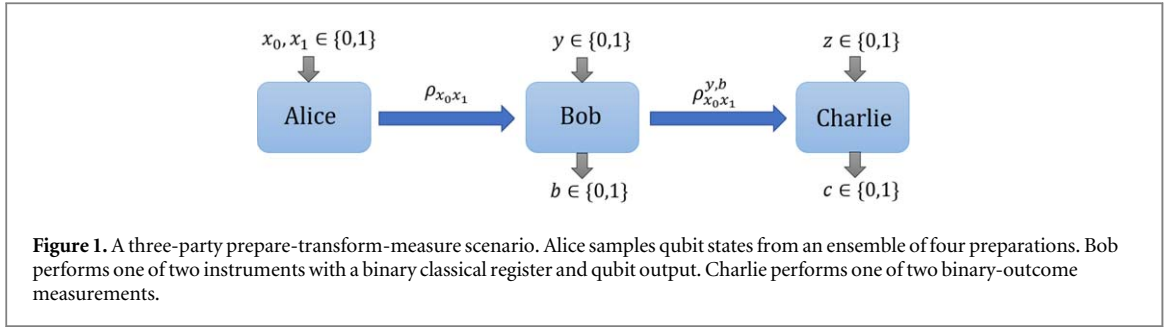
Abstract

Quantum random access codes (QRACs) are key tools for a variety of protocols in quantum information theory. These are commonly studied in prepare-and-measure scenarios in which a sender prepares states and a receiver measures them. Here, we consider a three-party prepare-transform-measure scenario in which the simplest QRAC is implemented twice in sequence based on the same physical system. We derive optimal trade-off relations between the two QRACs. We apply our results to construct semi-device independent self-tests of quantum instruments, i.e. measurement channels with both a classical and quantum output. Finally, we show how sequential QRACs enable inference of upper and lower bounds on the sharpness parameter of a quantum instrument.

1. Introduction

Random access codes (RACs) are an important class of communication tasks with a broad scope of applications. In a RAC, a party Alice holds a set of randomly sampled data and another party Bob attempts to recover some randomly chosen subset of Alice's data. This is made possible by Alice communicating with Bob. Therefore, this corresponds to a *prepare-and-measure scenario* in which Alice encodes her data into a message that she sends to Bob who aims to decode the relevant information. Naturally, this task would be trivial if Alice is allowed to send unlimited information. Therefore, a RAC requires that the message is restricted in its alphabet, so that it cannot encode all of Alice's data. Interestingly however, the probability of Bob to access the desired information can be increased if Alice substitutes her classical message with a quantum message of the same alphabet. Such quantum random access codes (QRACs) have been introduced and developed for qubit systems [1, 2] as well as higher-dimensional quantum systems [3]. They are primitives for network coding [4], random number generation [5] and quantum key distribution [6]. QRACs are also common in foundational aspects of quantum theory; examples include the comparison of different quantum resources [7, 8], dimension witnessing [9], self-testing [10–12] and attempts at characterising quantum correlations from information-theoretic principles [13].

Here, we present RACs beyond standard prepare-and-measure scenarios. Specifically, we consider a 'prepare-transform-measure' scenario involving three parties, Alice, Bob and Charlie, in a line configuration. In our scenario, both Bob and Charlie are interested in randomly accessing some information held by Alice, i.e. they individually implement a RAC with Alice. In a classical picture, such sequential RACs are trivial since any information made available to Bob via Alice's communication also can be relayed by Bob to Charlie. In this sense, there is no trade-off between how well Bob and Charlie can perform their RACs. In a quantum picture however, Alice communicates a qubit system that is first sent to Bob who applies a quantum instrument (a completely positive trace-preserving map with both a classical and quantum output) whose classical output is recorded and whose quantum output is relayed to Charlie who performs a measurement. Importantly, Bob's instrument disturbs the physical state of Alice's qubit, and therefore he cannot relay Alice's original quantum message to Charlie. In other words, Charlie's ability to access the desired information depends on Bob's preceding interaction. Consequently, one expects a trade-off in the ability of Bob and Charlie to perform their separate QRACs. Here, we consider Bob and Charlie the simplest RAC for qubits (sometimes referred to as a $2 \rightarrow 1$ RAC) in sequence, and derive the optimal trade-off relation between the two QRACs. In particular, we find that both QRACs can outperform the best possible classical RAC.



Subsequently, we apply our results to self-test a quantum instrument. Self-testing [14] is the task of inferring physical entities (states, channels, measurements) solely from correlations produced in experiments i.e. identifying the unique physical entities that are compatible with observed data. Self-testing is typically studied in Bell experiments where notably methods for self-testing quantum instruments have been developed [15, 16]. Recently however, self-testing was introduced in the broad scope of prepare-and-measure scenarios [10], and was further developed using QRACs to robustly self-test both preparations and measurements [10–12]. Notably however, prepare-and-measure scenarios do not enable self-tests of general quantum operations. In particular, it does not enable self-tests of quantum instruments since the quantum system after the measurement is irrelevant to the outcome statistics produced in the experiment. We show that our prepare-transform-measure scenario overcomes this conceptual limitation. We find that optimal pairs of sequential QRACs self-test quantum instruments. However, such optimal correlations require idealised (noiseless) scenarios which are never the case in a practical implementation. Therefore, we also show how sequential QRACs allow for inference of noise-robust bounds on the sharpness parameter in a quantum instrument. This makes our results applicable to experimental demonstrations. Finally, we discuss relevant generalisations of our results.

2. Sequential RACs

We focus on a prepare-transform-measure scenario that involves three parties. The first party (Alice) receives a uniformly random four-valued input $x = (x_0, x_1) \in \{0, 1\}^2$. For a given input, she prepares a quantum state ρ_x . This state is uncharacterised, up to the assumption of it being of Hilbert space dimension two, i.e. it is a qubit. The state is transmitted to the second party (Bob) who receives a random binary input $y \in \{0, 1\}$. Depending on his input, Bob applies an instrument characterised by Kraus operators $\{K_{b|y}\}$ to ρ_x which produces a classical binary outcome $b \in \{0, 1\}$ and a qubit post-measurement state

$$\rho_x^{y,b} = \frac{K_{b|y} \rho_x K_{b|y}^\dagger}{\text{tr}(\rho_x K_{b|y}^\dagger K_{b|y})}. \quad (1)$$

Notably, since the instrument realises a measurement, the Kraus operators of Bob must satisfy the completeness relation $\forall y : M_{0|y} + M_{1|y} = \mathbb{1}$, where $M_{b|y} = K_{b|y}^\dagger K_{b|y}$ are the corresponding elements of the positive operator-valued measures (POVMs). The post-measurement state $\rho_x^{y,b}$ is relayed to the third party (Charlie) who receives a random binary input $z \in \{0, 1\}$ to which he associates POVMs $\{C_{c|z}\}$ with a binary outcome $c \in \{0, 1\}$. The scenario is illustrated in figure 1.

In the limit of repeating the experiment many times, the results are described by the probability distribution

$$p(b, c|x, y, z) = \text{tr}[K_{b|y} \rho_x K_{b|y}^\dagger C_{c|z}]. \quad (2)$$

To enable a simple and qualitative treatment of the information stored in the distribution, one may employ a correlation witness, i.e. a map from $p(b, c|x, y, z)$ to a single real number. We are interested in two separate correlation witnesses, each corresponding to a RAC. The first RAC is considered between Alice and Bob. In this task, the partners are collectively awarded a point if and only if Bob can guess the y 'th bit of Alice input (x_0, x_1) . The correlation witness is the average success probability. It reads

$$W_{AB} = \frac{1}{8} \sum_{x,y} p(b = x_y|x, y) = \frac{1}{8} \sum_{x,y} \text{tr}[\rho_x M_{x_y|y}], \quad (3)$$

where in the second step we have assumed a quantum description. In a classical picture (in which all states are diagonal in the same basis), this witness obeys $W_{AB} \leq 3/4$ (which we further discuss later). The physical properties of $\{\rho_x\}$ and $\{M_{b|y}\}$ when the QRAC exceeds its classical bound were studied in [10]. It was shown that an optimal QRAC for qubits

$$W_{AB} = \frac{1}{2} \left(1 + \frac{1}{\sqrt{2}} \right) \approx 0.854 \quad (4)$$

self-tests that Alice's four preparations form a square in some disk of the Bloch sphere. Up to a choice of reference frame these are written

$$\begin{aligned} \rho_{00} &= \frac{1}{2} \left(\mathbb{1} + \frac{\sigma_x + \sigma_z}{\sqrt{2}} \right), & \rho_{11} &= \frac{1}{2} \left(\mathbb{1} - \frac{\sigma_x + \sigma_z}{\sqrt{2}} \right), \\ \rho_{01} &= \frac{1}{2} \left(\mathbb{1} + \frac{\sigma_x - \sigma_z}{\sqrt{2}} \right), & \rho_{10} &= \frac{1}{2} \left(\mathbb{1} - \frac{\sigma_x - \sigma_z}{\sqrt{2}} \right), \end{aligned} \quad (5)$$

where $\vec{\sigma} = (\sigma_x, \sigma_y, \sigma_z)$ denotes the Pauli matrices. Moreover, an optimal QRAC also self-tests Bob's observables (defined as $M_y = M_{0|y} - M_{1|y}$) to be anticommuting. In the stated frame, the observables are written

$$M_0 = \sigma_x \quad M_1 = \sigma_z. \quad (6)$$

Evidently however, the QRAC (3) is independent of both Charlie and of the choice of instrument for realising the POVMs $\{M_{b|y}\}$. To also take these into account, we consider an additional QRAC implemented between Alice and Charlie. Analogously, the partners are awarded a point if and only if Charlie can guess the z 'th bit of Alice's input (x_0, x_1) . The correlation witness corresponding to this QRAC reads

$$W_{AC} = \frac{1}{8} \sum_{x,z} p(c = x_z | x, z). \quad (7)$$

This QRAC is not independent of Bob since he applies an instrument to the preparation of Alice before they arrive to Charlie. In a quantum model, the effective state $\tilde{\rho}_x$ received by Charlie is the post-measurement state of Bob averaged over Bob's inputs and classical outputs, i.e.

$$\tilde{\rho}_x = \frac{1}{2} \sum_{y,b} p(b|y) \rho_x^{y,b} = \frac{1}{2} \sum_{y,b} K_{b|y} \rho_x K_{b|y}^\dagger. \quad (8)$$

Therefore, we have

$$W_{AC} = \frac{1}{8} \sum_{x,z} \text{tr}[\tilde{\rho}_x C_{x_z|z}] = \frac{1}{16} \sum_{x,y,b,z} \text{tr}[K_{b|y} \rho_x K_{b|y}^\dagger C_{x_z|z}]. \quad (9)$$

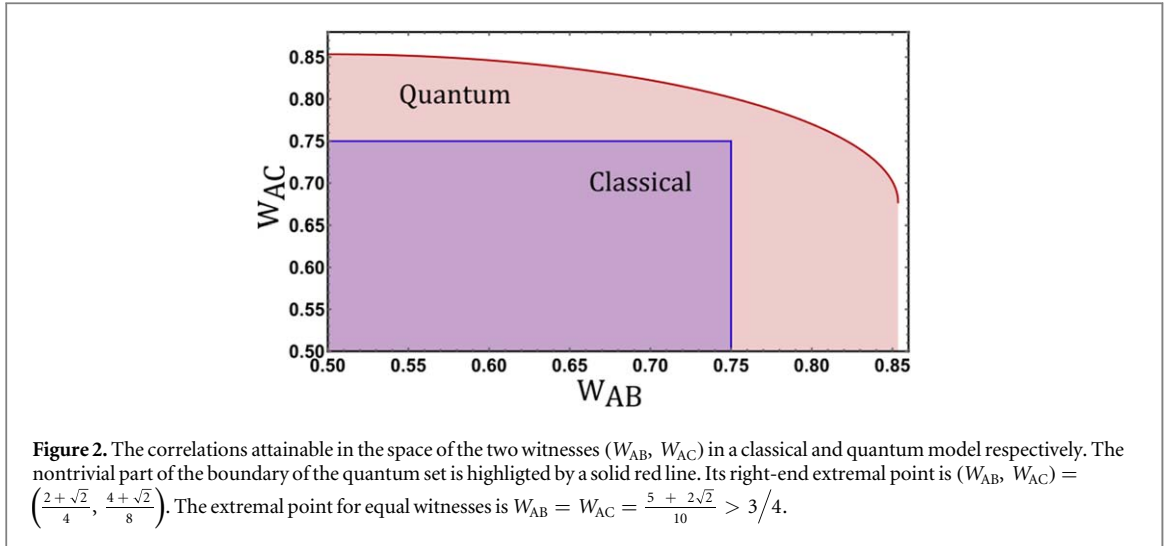
We are interested in the values attainable for the pair of QRACs (W_{AB}, W_{AC}) . We remark that the interesting range is when both W_{AB} and W_{AC} are confined to the interval $[1/2, (1 + 1/\sqrt{2})/2]$ since either witness being $1/2 - \epsilon$ for some $\epsilon > 0$ is equivalent to a witness value of $1/2 + \epsilon$ by classically bit-flipping the outcomes.

Typically, we expect there to be a trade-off between the two QRACs. The reason is as follows. In order for W_{AB} to be large, Alice must prepare states that are close to the ones in equation (5) and Bob must implement instruments that realise POVMs that are close to the ones in equation (6). This means that Bob's measurements must be reasonably sharp. This leads to a large disturbance in the state of the measured system which causes the effective ensemble of states $\{\tilde{\rho}_x\}$ arriving to Charlie to lesser reflect the ensemble $\{\rho_x\}$ originally prepared by Alice. Therefore, the value of W_{AC} is expected to be small. Conversely, if Bob makes a very unsharp measurement (almost noninteracting), he could almost completely avoid disturbing the state of Alice's system and thus we would find that $\{\tilde{\rho}_x\}$ closely approximates $\{\rho_x\}$ which allows Charlie to find a large value of W_{AC} . However, the weak interaction of Bob then would imply a correspondingly small value of W_{AB} .

In view of the above, characterising the set of pairs (W_{AB}, W_{AC}) that can be attained in quantum theory is a nontrivial matter. By finding such a characterisation and by understanding the trade-off between the two QRACs, we enable self-tests of Bob's instrument, along with self-tests of Alice's preparations and Charlie's measurements. Note that one may also consider alternative generalisations of QRACs to sequential scenarios [17].

3. Quantum correlations in sequential RACs

Which values of the pair of QRACs (W_{AB}, W_{AC}) can be realised in a quantum model based on qubit systems? Before addressing this matter, let us first examine the substantially simpler situation in which the physical devices are classical, i.e. the state at all times is diagonal in the same basis. In such situations, Bob can interact with the preparations of Alice without disturbing their state. Therefore, a large value of W_{AB} constitutes no obstacle for also finding a large value of W_{AC} . Classically, one can optimally achieve $W_{AB} = 3/4$. Clearly, as the interaction with Bob cannot contribute towards increasing the value of W_{AC} , it also holds that $W_{AC} \leq 3/4$. This value is saturated by Alice sending x_0 to Bob who outputs $b = x_0$ and relays x_0 to Charlie who outputs $c = x_0$.



Thus, the set of classically attainable correlations is $1/2 \leq (W_{AB}, W_{AC}) \leq 3/4$. This classically attainable set is illustrated in figure 2. Notice that there is no trade-off between W_{AB} and W_{AC} in a classical picture.

In a quantum model, the characterisation of the attainable set of witnesses is less straightforward. We phrase the problem as follows: for a given value (denoted α) of W_{AB} , what is the maximal value of W_{AC} possible in a quantum model? Answering this question for every $\alpha \in [1/2, (1 + 1/\sqrt{2})/2]$ provides the optimal trade-off between the two QRACs. Equivalently, it can be viewed as the nontrivial part of the boundary of the quantum set of correlations in the space of (W_{AB}, W_{AC}) . Formally, the optimisation problem reads

$$\begin{aligned}
 W_{AC}^\alpha &= \max_{\rho, U, M, C} W_{AC} \\
 \text{such that } \forall x : \rho_x &\in \mathbb{C}^2, \quad \rho_x \geq 0, \quad \text{tr} \rho_x = 1, \\
 \forall z, c : C_{c|z} &\geq 0, \quad C_{0|z} + C_{1|z} = \mathbb{1} \\
 \forall y, b : U_{yb} &\in \text{SU}(2), \quad M_{b|y} \geq 0, \quad M_{0|y} + M_{1|y} = \mathbb{1}, \\
 \text{and } W_{AB} &= \alpha,
 \end{aligned} \tag{10}$$

i.e. it is an optimisation of Charlie's witness over all preparations, instruments and measurements that can model the observation of $W_{AB} = \alpha$. In the above, we have used the polar decomposition to write the Kraus operators as $K_{b|y} = U_{yb} \sqrt{M_{b|y}}$ for some unitary operator U_{yb} and some POVM $\{M_{b|y}\}$. Kraus operators of this form correspond to extremal quantum instruments in the considered scenario [18].

We solve the problem (10) by first giving a lower bound on W_{AC}^α and then matching it with an upper bound. To this end, consider a quantum strategy in which Alice prepares the ensemble of states given in equation (5) and Charlie performs the measurements in equation (6). We let Bob perform an unsharp Lüders measurement (the Kraus operators have $U_{yb} = \mathbb{1}$) of the observables in equation (6), i.e. his observables correspond to $M_0 = \eta\sigma_x$ and $M_1 = \eta\sigma_z$ for some sharpness parameter $\eta \in [0, 1]$ (which we will later self-test). Evaluating the pair of witnesses with this quantum strategy gives

$$\begin{aligned}
 W_{AB} &= \frac{1}{4}(2 + \eta\sqrt{2}) \\
 W_{AC} &= \frac{1}{8}(4 + \sqrt{2} + \sqrt{2 - 2\eta^2}).
 \end{aligned} \tag{11}$$

Parameterising the latter in terms of the former returns a lower bound on W_{AC}^α . Importantly, this bound is optimal since it can be saturated with an upper bound on W_{AC}^α , thus solving the optimisation problem (10). This leads us to our first result.

Result 1. The optimal trade-off between the pair of QRACs (W_{AB}, W_{AC}) corresponds to

$$W_{AC}^\alpha = \frac{1}{8}(4 + \sqrt{2} + \sqrt{16\alpha - 16\alpha^2 - 2}), \tag{12}$$

where $\alpha \in [1/2, (1 + 1/\sqrt{2})/2]$. That is, the optimal witness pairs are of the form $(W_{AB}, W_{AC}) = (\alpha, W_{AC}^\alpha)$. This characterises the nontrivial boundary of the quantum set in the space of witness pairs.

The proof is analytical, of technical character and detailed in appendix B. It relies on (i) treating the maximisation in (10) over the unitaries $\{U_{yb}\}$ and measurements $\{C_{c|z}\}$ as an eigenvalue problem, (ii) using the

Bloch sphere parameterisation for the preparations and instruments, and (iii) noticing that the maximisation over the preparations can be relaxed to a maximisation over two pairs of antipodal pure states in some disk of the Bloch sphere.

In figure 2, we have illustrated the set of sequential QRACs attainable in a quantum model. Notice that a maximal value (4) of W_{AB} does not imply that W_{AC} is no better than what is obtained by random guessing. In contrast, one can achieve $(W_{AB}, W_{AC}) = \left(\frac{2+\sqrt{2}}{4}, \frac{4+\sqrt{2}}{8}\right)$. The reason is that the ensemble relayed to Charlie corresponds to that originally prepared by Alice but with Bloch vectors of half the original length. In addition, there exists a subset of the quantum set in which both W_{AB} and W_{AC} exceed the classical bound.

4. Self-testing

Finding the optimal trade-off between the two QRACs (Result 1) allows for self-testing. To obtain a self-test, one must additionally show that the optimal QRAC pairs only admit a realisation with unique preparations, instruments and measurements (up to collective unitary transformations). That is, we need to identify the unique physical entities $\{\rho_x\}$, $\{K_{b|y}\}$, and $\{C_{c|z}\}$ necessary for optimal correlations.

Such a self-testing argument can be established largely from the proof of Result 1 (see appendix B). The reason is that our approach to deriving Result 1 successively identifies the form of the physical entities required for optimality. To turn the statement into a self-test, we identify key inequalities used to upper bound W_{AC}^α and instead impose strict equality constraints. This allows us to pinpoint the states, measurements and instruments one by one. These additional arguments are discussed in appendix B. This leads us to the following self-test statement based on optimal sequential QRACs.

Result 2. An optimal pair of QRACs $(W_{AB}, W_{AC}) = (\alpha, W_{AC}^\alpha)$, as in equation (10), self-tests that

- Alice's states are pure and pairwise antipodal on the Bloch sphere, on which they form a square. These correspond to the states given in equation (5).
- Bob's instruments are Kraus operators $K_{b|y} = U_{yb} \sqrt{M_{b|y}}$ that correspond to unsharp measurements along the diagonals of Alice's square of preparations followed by a collective unitary. Specifically, $\forall y, b: U_{yb} = U$, $M_0 = \eta\sigma_x$ and $M_1 = \eta\sigma_z$ where $\eta = \sqrt{2}(2W_{AB} - 1)$.
- Charlie's measurements are rank-one projective along the diagonals of the square formed by Alice's preparations, up to the unitary of Bob. That is, $C_0 = U\sigma_x U^\dagger$ and $C_1 = U\sigma_z U^\dagger$.

The self-tests are valid up to a collective choice of reference frame.

This result applies to optimal pairs of QRACs (highlighted by a solid red line in figure 2). An interesting question is how to make this result noise-tolerant so that it applies to suboptimal pairs of QRACs that nevertheless lack a classical model. Naturally, when the QRACs are suboptimal, one can no longer pinpoint the physical entities as done in Result 2. However, it is possible to give qualitative statements about the quantum strategies that in principle could model the observed correlations. We consider this matter for the sharpness parameter in Bob's instruments. Since any binary-outcome qubit observable can be written on the form $M_y = c_{y0}\mathbb{1} + \vec{c}_y \cdot \vec{\sigma}$, we define the sharpness parameter of Bob's instrument as the length of the Bloch vector \vec{c}_y . For simplicity, we take both his instruments to have the same sharpness $\eta \equiv |\vec{c}_0| = |\vec{c}_1|$.

We can place a lower bound on η from the witness W_{AB} ; it corresponds to the smallest η for which there exists preparations and instruments that can model W_{AB} . In appendix C, we show that this lower bound reads

$$\eta \geq \sqrt{2}(2W_{AB} - 1). \quad (13)$$

This lower bound is nontrivial whenever $W_{AB} > 1/2$. Notice also that an optimal QRAC (4) necessitates a sharp measurement ($\eta = 1$). Similarly, we can place an upper bound on η from the witness W_{AC} , corresponding to the largest η for which there exists preparations, instruments and measurements that can model W_{AC} . In appendix C we show that such a bound reads

$$\eta \leq 2\sqrt{(2 + \sqrt{2} - 4W_{AC})(2W_{AC} - 1)}, \quad (14)$$

when $\frac{4+\sqrt{2}}{8} \leq W_{AC} \leq \frac{2+\sqrt{2}}{4}$ (otherwise the bound is trivial). The lower bound (13) and the upper bound (14) are tight, i.e. they can be saturated with an explicit quantum strategy. Notice that the upper bound (14) coincides with the lower bound (13) for optimal W_{AC} (i.e. when $W_{AC} = W_{AC}^\alpha$) as given in equation (12). In addition, the bound (14) reduces to the trivial $\eta \leq 1$ when $W_{AC} = (4 + \sqrt{2})/8 \approx 0.6767$.

As a simple example, consider an experiment that attempts to implement the quantum strategy (11) for the optimal witness pair (W_{AB}, W_{AC}) corresponding to $\eta = 1/\sqrt{2}$. However the experiment is subject to losses. For example, take a 95% visibility¹ in Alice's preparations, 90% visibility in Bob's instruments, and 95% visibility in Charlie's measurements. Instead of finding the optimal witness pair $(W_{AB}, W_{AC}) = (3/4, (5 + \sqrt{2})/8)$, one finds $(W_{AB}, W_{AC}) \approx (0.7138, 0.7826)$. Therefore, we find that η must be confined to the interval $0.6047 \leq \eta \leq 0.8010$. The interval is fairly wide, which emphasises the need for high-quality practical realisations in order to confine η to a reasonably small interval.

5. Generalisations

Above, we have thoroughly considered the scenario in which a sequence of three observers implement a pair of the simplest QRAC. This is arguably the simplest scenario in which to study sequential QRACs. It would be interesting to consider more general scenarios; both involving higher-dimensional [3] and many-input QRACs, as well as sequences of more than three observers.

Consider for example the above considered RAC played between Alice and a sequence of N parties. We denote the RAC between Alice and sequential party number k by W_k . Let Alice prepare the optimal states in equation (5). We know that if the first party performs optimal projective measurements (6) (with Kraus operators $K_{b|y} = M_{b|y}$), he will find the optimal QRAC given in equation (4). Moreover, if the second party performs the same Kraus operators we find $W_3 = (1 + 1/(2\sqrt{2}))/2$. The reason is that the effective state ensemble (8) relayed by the first party is identical to the preparations of Alice except that their Bloch vectors have shrunk to half the unit length. Similarly, the effective ensemble relayed by the second party will be identical to that relayed by the first party, except that the Bloch vectors will again be shrunk to a quarter of unit length. Continuing the sequence in this manner, the square formed in the Bloch sphere by the effective post-measurement ensemble will at each step have its half-diagonal reduced by a factor $1/2$, and we find

$$W_k = \frac{1}{2} \left(1 + \frac{\sqrt{2}}{2^k} \right). \quad (15)$$

Moreover, one can ask what is the longest sequence of QRACs such that all of them can exceed the classical bound. The number is at least two, since we found $W_{AB} = W_{AC} = \frac{5 + 2\sqrt{2}}{10} \approx 0.7828 > 3/4$. However, a third sequential violation is unlikely to be possible, i.e. to find $W_1 = W_2 = W_3 > 3/4$. The reason is based on the possibility of relating witnesses in dimension-bounded prepare-and-measure scenarios to Bell inequalities [19–21]. Via such methods, the considered RAC can be related to the CHSH inequality [19]. However, sequential violations of the CHSH inequality were studied in [22] and it was found that no more than two CHSH inequality violations are possible when inputs are uniformly distributed [23, 24].

6. Conclusions

We have studied sequential QRACs and characterised their optimal trade-off. This ties in with the recent interest in sequential quantum correlations obtained in various forms of tests of nonclassicality [22, 24–30]. We applied our results to show that quantum instruments can be semi device-independently self-tested. Notably, since all quantum instruments also realise some POVM, our results trivially implies a certification of unsharp measurements. Our results complement the many recent self-tests of preparations and measurements in standard prepare-and-measure scenarios with a method for self-testing quantum instruments. In addition, we showed how to robustly certify the sharpness parameter of quantum instruments based on noisy correlations. This makes our results readily applicable to experimental applications. Such tests are well within the state-of-the-art experiments [30–32]. Moreover, we notice that the class of quantum instruments self-tested in this work are precisely those implemented by the experimental realisations in [30–33].

We conclude with some open questions. Firstly, it would be interesting to generalise our results to cover higher-dimensional QRACs and longer sequences of observers. Secondly, a possible further development is to characterise the optimal trade-off between sequential QRACs encountered in tests of preparation contextuality [30]. Thirdly, in the spirit of [15], it would be interesting to develop noise-robust self-testing of quantum instruments. Typically, such a robust self-test address the closeness (based on observed witness values) between the unknown laboratory instrument and the ideal instrument that would have been self-tested in case correlations were optimal. Finally, one could consider the task of self-testing quantum instruments based on the sequential correlation experiments in the fully device-independent scenario (see [22]).

¹ Here, visibility corresponds to a parameter $v \in [0, 1]$ and means that the ideal physical entity is implemented with probability v and with probability $(1 - v)$ the implemented physical entity is maximally mixed.

Acknowledgments

We thank Denis Rosset and Jędrzej Kaniewski for discussions. This work was funded by the Swiss National Science Foundation (Starting grant DIAQ, NCCR-QSIT).

Note added

During the completion of this work, we became aware of the related work of [34].

Appendix A. Proof of results 1 and 2

We first prove Result 1 and then develop the argument further to also prove Result 2.

Consider the maximisation of the witness

$$W_{AC} = \frac{1}{16} \sum_{x,y,b,z} \text{tr}[K_{b|y} \rho_x K_{b|y}^\dagger C_{x_z|z}] \quad (\text{A1})$$

under the constraint that

$$\alpha \equiv W_{AB} = \frac{1}{8} \sum_{x,y} \text{tr}[\rho_x K_{x_y|y}^\dagger K_{x_y|y}]. \quad (\text{A2})$$

The optimisation is relevant for every $\alpha \in [1/2, (1 + 1/\sqrt{2})/2]$, ranging from the trivial witness value to the maximal witness value.

To contend with this, we first use the polar decomposition $K_{b|y} = U_{yb} \sqrt{M_{b|y}}$, where U_{yb} are arbitrary unitary operators. We can then use the cyclicity of the trace along with the substitution $C_{1|z} = \mathbb{1} - C_{0|z}$ to write equation (A1) as

$$W_{AC} = \frac{1}{2} + \frac{1}{16} \sum_{x,y,b,z} (-1)^{x_z} \text{tr}[\sqrt{M_{b|y}} \rho_x \sqrt{M_{b|y}} U_{yb}^\dagger C_{0|z} U_{yb}]. \quad (\text{A3})$$

The sum over x can be moved inside the trace; we define $\gamma_z = \sum_x (-1)^{x_z} \rho_x$. Moreover, we also define $A_{zyb} = U_{yb}^\dagger C_{0|z} U_{yb}$. We can now consider the optimisation over $\{U_{yb}\}$ and $\{C_{c|z}\}$ as a single optimisation over A_{zyb} . To this end, we note that the set of measurements $\{C_{c|z}\}$ is convex. Therefore, every nonextremal (interior point) measurement can be written as a convex combination of extremal measurements (on the boundary). Due to linearity, no nonextremal POVM can lead to a larger value of W_{AC} than some extremal POVM. The extremal binary-outcome qubit measurements are rank-one projectors. Therefore, we can consider the optimisation over A_{zyb} as an optimisation over general rank-one projectors. This gives

$$\begin{aligned} \max W_{AC} &= \frac{1}{2} + \max_{\rho, A, M} \frac{1}{16} \sum_{y,b,z} \text{tr}[\sqrt{M_{b|y}} \gamma_z \sqrt{M_{b|y}} A_{zyb}] \\ &= \frac{1}{2} + \max_{\rho, M} \frac{1}{16} \sum_{y,b,z} \lambda_{\max}[\sqrt{M_{b|y}} \gamma_z \sqrt{M_{b|y}}], \end{aligned} \quad (\text{A4})$$

where we have made the optimal choice of letting A_{zyb} project onto the eigenvector of $\sqrt{M_{b|y}} \gamma_z \sqrt{M_{b|y}}$ with the largest eigenvalue (denoted by λ_{\max}).

To proceed further, we make use of the fact that qubit operations can be parameterised on the Bloch sphere. We write the preparations as $\rho_x = (\mathbb{1} + \vec{n}_x \cdot \vec{\sigma})/2$ for some Bloch vectors $\vec{n}_x \in \mathbb{R}^3$ with $|\vec{n}_x| \leq 1$. This leads to

$$\gamma_z = [(\vec{n}_{00} - \vec{n}_{11}) + (-1)^z (\vec{n}_{01} - \vec{n}_{10})] \cdot \vec{\sigma}. \quad (\text{A5})$$

We define the effective (unnormalised) Bloch vectors $\vec{m}_z = (\vec{n}_{00} - \vec{n}_{11}) + (-1)^z (\vec{n}_{01} - \vec{n}_{10})$. Consequently, the dependence of W_{AC} on the preparations can be reduced to its dependence on (\vec{m}_0, \vec{m}_1) . However, given any set of preparations $\{\vec{n}_x\}$, we can consider other preparations $\{\vec{n}'_x\}$ chosen such that $\vec{n}'_{00} = -\vec{n}'_{11}$ and $\vec{n}'_{01} = -\vec{n}'_{10}$ with $2\vec{n}'_{00} = \vec{n}_{00} - \vec{n}_{11}$ and $2\vec{n}'_{01} = \vec{n}_{01} - \vec{n}_{10}$. The both ensembles $\{\vec{n}_x\}$ and $\{\vec{n}'_x\}$ imply the same vectors (\vec{m}_0, \vec{m}_1) . Moreover, it is evident that if not all preparations are pure, one cannot obtain optimal correlations (since impurity corresponds to decreasing the magnitude of (\vec{m}_0, \vec{m}_1)). This means that the Bloch vectors are of unit length and therefore that the optimal preparations *must* be of the type $\{\vec{n}'_x\}$ (i.e. two antipodal pairs). Notice that purity also implies that $\vec{m}_0 \cdot \vec{m}_1 = 0$.

W.l.g. we can choose a reference frame in which $\vec{m}_0 \propto (1, 0, 0)$ and $\vec{m}_1 \propto (0, 0, 1)$. We denote the relative angle between the two pairs of antipodal preparation pairs by $\theta \in [0, \pi/2]$. This gives

$$|\vec{m}_0| = \sqrt{2(1 + \cos\theta)} \quad \text{and} \quad |\vec{m}_1| = \sqrt{2(1 - \cos\theta)}.$$

We can further place an upper bound on equation (A4) by using the following relation

$$\forall M, \forall \vec{a} \in \mathbb{R}^3 : \sum_{b=0,1} \lambda_{\max} [\sqrt{M_b} (\vec{a} \cdot \vec{\sigma}) \sqrt{M_b}] \leq |\vec{a}|, \quad (\text{A6})$$

with equality if and only if \vec{a} is aligned with the Bloch vector of the POVM. Identifying \vec{a} with \vec{m}_z , we apply it twice to equation (A4) corresponding to the terms in which $z = y$. This gives

$$W_{\text{AC}} \leq \frac{1}{2} + \frac{1}{16} \left(|\vec{m}_0| + |\vec{m}_1| + \underbrace{\sum_{y,b} \lambda_{\max} [\sqrt{M_{b|y}} (\vec{m}_{\bar{y}} \cdot \vec{\sigma}) \sqrt{M_{b|y}}]}_{=S} \right), \quad (\text{A7})$$

where \bar{y} denotes a bit-flip. We turn our attention to the sum denoted by S in equation (A7). We define the observable $M_y = M_{0|y} - M_{1|y}$ and apply the Bloch sphere parameterisation. We may write $M_y = c_{y0} \mathbb{1} + \vec{c}_y \cdot \vec{\sigma}$ where $\vec{c}_y = (c_{y1}, c_{y2}, c_{y3})$ with $|\vec{c}_y| \leq 1$ and $|\vec{c}_y| - 1 \leq c_{y0} \leq 1 - |\vec{c}_y|$. These constraints ensure positivity. Hence

$$M_{b|y} = f_{yb} |\vec{c}_y\rangle \langle \vec{c}_y| + h_{yb} |\vec{c}_y\rangle \langle -\vec{c}_y|, \quad (\text{A8})$$

where $|\vec{c}_y\rangle$ is the pure state corresponding to the Bloch sphere direction of \vec{c}_y , and

$$\begin{aligned} f_{yb} &= \frac{1}{2} (1 + (-1)^b c_{y0} + (-1)^b |\vec{c}_y|) \\ h_{yb} &= \frac{1}{2} (1 + (-1)^b c_{y0} - (-1)^b |\vec{c}_y|). \end{aligned} \quad (\text{A9})$$

Firstly, this allows us to write the constraint (A2) as

$$\alpha = \frac{1}{8} (4 + |\vec{m}_0| c_{01} + |\vec{m}_1| c_{13}). \quad (\text{A10})$$

Secondly, we can now solve the characteristic equation $\det(\sqrt{M_{b|y}} (\vec{m}_{\bar{y}} \cdot \vec{\sigma}) \sqrt{M_{b|y}} - \mu \mathbb{1}) = 0$, and after some simplifications obtain

$$S = \sum_{y,b} \frac{|\vec{m}_{\bar{y}}|}{2} \sqrt{(1 + (-1)^b c_{y0})^2 - |\vec{c}_y|^2 (1 - \langle \vec{c}_y | \hat{m}_{\bar{y}} \cdot \vec{\sigma} | \vec{c}_y \rangle^2)}, \quad (\text{A11})$$

where $\hat{m} = \vec{m}/|\vec{m}|$. We can now consider the optimisation over c_{y0} by separately considering the two terms corresponding to $y = 0$ and $y = 1$ respectively. This amounts to maximising expressions of the form $\sqrt{(1+x)^2 - K} + \sqrt{(1-x)^2 - K}$, for some positive constant K . It is easily shown that such functions are uniquely maximised by setting $x = 0$. Thus, we require $c_{00} = c_{10} = 0$. Moreover, since (\vec{m}_0, \vec{m}_1) have no component along the y -axis, it is seen from (A10) and (A11) that one optimally chooses $c_{02} = c_{12} = 0$. This simplifies matters to

$$\max S = |\vec{m}_0| \sqrt{1 - (c_{11}^2 + c_{13}^2)(1 - c_{11}^2)} + |\vec{m}_1| \sqrt{1 - (c_{01}^2 + c_{03}^2)(1 - c_{03}^2)}. \quad (\text{A12})$$

Note that c_{03} and c_{11} do not appear in the constraint (A10), that they are associated to different settings of Bob and that they appear in different terms in equation (A12). Therefore, we can separately maximise search square-root expression above by standard differentiation. This returns that the unique maximum is attained for $c_{03} = c_{11} = 0$. Hence, we have

$$W_{\text{AC}} \leq \frac{1}{2} + \frac{1}{16} (|\vec{m}_0| + |\vec{m}_1| + |\vec{m}_0| \sqrt{1 - c_{13}^2} + |\vec{m}_1| \sqrt{1 - c_{01}^2}) \equiv W. \quad (\text{A13})$$

Denoting $c_{01} = \cos \phi_0$ and $c_{13} = \cos \phi_1$ for $\phi_1, \phi_2 \in [0, \pi/2]$, we can re-write the right hand side on the more convenient form

$$W = \frac{1}{2} + \frac{1}{8} \left(\cos \frac{\theta}{2} + \sin \frac{\theta}{2} + \cos \frac{\theta}{2} \sin \phi_1 + \sin \frac{\theta}{2} \sin \phi_0 \right) \quad (\text{A14})$$

and the constraint (A10) as

$$\alpha = \frac{1}{8} \left(4 + \cos \frac{\theta}{2} \cos \phi_0 + \sin \frac{\theta}{2} \cos \phi_1 \right). \quad (\text{A15})$$

To maximise W over (θ, ϕ_0, ϕ_1) , we use the following lemma.

Lemma 1. For every tuple (θ, ϕ_0, ϕ_1) corresponding to (α, W) , there exists another tuple $(\theta, \phi_0, \phi_1) = (\pi/2, \phi, \phi)$ that produces (α, W') with $W' \geq W$. Moreover, $\theta = \pi/2$ and $\phi_0 = \phi_1$ is necessary for an optimal W' .

To prove this statement, we must show that for all $\theta, \phi_0, \phi_1 \in [0, \pi/2]$ there exists a $\phi \in [0, \pi/2]$ such that

$$\begin{aligned} \cos \frac{\theta}{2} \cos \phi_0 + \sin \frac{\theta}{2} \cos \phi_1 &= \sqrt{2} \cos \phi \\ \cos \frac{\theta}{2} + \sin \frac{\theta}{2} + \cos \frac{\theta}{2} \sin \phi_1 + \sin \frac{\theta}{2} \sin \phi_0 &\leq \sqrt{2} + \sqrt{2} \sin \phi. \end{aligned} \quad (\text{A16})$$

Proof. It trivially holds that $\cos \frac{\theta}{2} + \sin \frac{\theta}{2} \leq \sqrt{2}$ with equality if and only if $\theta = \pi/2$. We eliminate this part from the second equation in (A16). Then, by squaring both equations, we can combine them into a single equation in which ϕ is eliminated. The statement reduces to the inequality

$$\cos \theta (\cos^2 \phi_0 - \cos^2 \phi_1) + \sin \theta \cos (\phi_0 - \phi_1) \leq 1. \quad (\text{A17})$$

Using differentiation w.r.t. ϕ_0 one finds that the optimum of the left hand side is attained for $\phi_1 = \phi_0$, which proves the relation (A17). ■

By virtue of lemma 1, we can reduce our consideration of (A14) and (A15) to $\theta = \pi/2$ and $c_{01} = c_{13} \equiv c$. Therefore equation (A10) reduces to

$$c = \sqrt{2}(2\alpha - 1) \quad (\text{A18})$$

and we also have $W = \frac{1}{2} + \frac{1}{4\sqrt{2}}(1 + \sqrt{1 - c^2})$. Thus, we have arrived to the upper bound

$$W_{AC}^\alpha \leq \frac{1}{8}(4 + \sqrt{2} + \sqrt{16\alpha - 16\alpha^2 - 2}). \quad (\text{A19})$$

As shown in the main text, this upper bound could be saturated with an explicit quantum strategy. This proves Result 1.

Let us now extend this to a proof of Result 2 by more closely examining the above steps needed to arrive at equation (A19). Firstly, we have already shown that the preparations must be pure, pairwise antipodal and by lemma 1 they must have a relative angle of $\pi/2$. Thus, this corresponds to a square in a disk of the Bloch sphere. The above arguments fully characterise Alice's preparations up to a reference frame.

For Bob's instrument, we have shown that the Bloch vectors (\vec{c}_0, \vec{c}_1) only can have non-zero components in the x - and z -directions respectively and that the length of the Bloch vector is given by equation (A18). This fully characterises the Bloch vectors. Moreover, in equation (A4) we required that A_{zyb} is aligned with the eigenvector of $\sqrt{M_{b|y}}\gamma_z\sqrt{M_{b|y}}$ corresponding to the largest eigenvalue. However, we now have that $\gamma_0 = \sigma_x$ and $\gamma_1 = \sigma_z$ whereas $M_0 \propto \sigma_x$ and $M_1 \propto \sigma_z$. Therefore, we have that $\forall y, b: A_{0yb} = |+\rangle\langle +|$ and $\forall y, b: A_{1yb} = |0\rangle\langle 0|$. Therefore, we have that

$$\forall yb: U_{yb}^\dagger C_{0|0} U_{yb} = |+\rangle\langle +|, \quad (\text{A20})$$

$$\forall yb: U_{yb}^\dagger C_{0|1} U_{yb} = |0\rangle\langle 0|. \quad (\text{A21})$$

This implies that all unitaries are equal; $U_{yb} = U$. Therefore, Charlie's observables $C_z = C_{0|z} - C_{1|z}$ satisfy $C_0 = U\sigma_x U^\dagger$ and $C_1 = U\sigma_z U^\dagger$.

Appendix B. Bounding the sharpness parameter from noisy correlations

In order to bound the sharpness of Bob's instrument, consider first the witness W_{AB} . Using the notations from the previous appendix, we have that

$$W_{AB} = \frac{1}{8}(4 + |\vec{c}_0||\vec{m}_0|\hat{m}_0 \cdot \hat{c}_0 + |\vec{c}_1||\vec{m}_1|\hat{m}_1 \cdot \hat{c}_1). \quad (\text{B1})$$

We focus on the simplified case in which the sharpness parameter is the same in Bob's two settings, i.e. $\eta \equiv |\vec{c}_0| = |\vec{c}_1|$. Re-arranging gives

$$\eta = \frac{8W_{AB} - 4}{|\vec{m}_0|\hat{m}_0 \cdot \hat{c}_0 + |\vec{m}_1|\hat{m}_1 \cdot \hat{c}_1}. \quad (\text{B2})$$

To find the smallest possible η , we maximise the denominator. That corresponds to setting $\hat{m}_0 \cdot \hat{c}_0 = \hat{m}_1 \cdot \hat{c}_1 = 1$ and $|\vec{m}_0| = |\vec{m}_1| = \sqrt{2}$. That gives the lower bound

$$\eta \geq \sqrt{2}(2W_{AB} - 1). \quad (\text{B3})$$

Consider now the witness W_{AC} . In the previous appendix, we have shown that its optimal value for a given choice of $\eta \equiv |\vec{c}_0| = |\vec{c}_1|$ is upper bounded as follows

$$W_{AC} \leq \frac{1}{2} + \frac{1}{4\sqrt{2}}(1 + \sqrt{1 - \eta^2}). \quad (\text{B4})$$

Solving this inequality for η gives

$$\eta \leq 2\sqrt{(2 + \sqrt{2} - 4W_{AC})(2W_{AC} - 1)}. \quad (\text{B5})$$

References

- [1] Ambainis A, Nayak A, Ta-Shma A and Vazirani U 1999 Dense quantum coding and a lower bound for 1-way quantum automata *Proc. 31st Annual ACM Symp. on Theory of Computing (STOC'99)* pp 376–83
- [2] Ambainis A, Leung D, Mancinska L and Ozols M 2008 *Quantum Random Access Codes with Shared Randomness* arXiv:0810.2937
- [3] Tavakoli A, Hameedi A, Marques B and Bourennane M 2015 Quantum random access codes using single d-Level systems *Phys. Rev. Lett.* **114** 170502
- [4] Hayashi M, Iwama K, Nishimura H, Raymond R and Yamashita S 2007 Quantum network coding *Proc. 24th Int. Symp. on Theoretical Aspects of Computer Science (STACS 2007), Lecture Notes in Computer Science 4393* pp 610–21
- [5] Li H-W, Yin Z-Q, Wu Y-C, Zou X-B, Wang S, Chen W, Guo G-C and Han Z-F 2011 Semi-device-independent random-number expansion without entanglement *Phys. Rev. A* **84** 034301
- [6] Pawłowski M and Brunner N 2011 Semi-device-independent security of one-way quantum key distribution *Phys. Rev. A* **84** 010302(R)
- [7] Tavakoli A, Marques B, Pawłowski M and Bourennane M 2016 Spatial versus sequential correlations for random access coding *Phys. Rev. A* **93** 032336
- [8] Hameedi A, Saha D, Mironowicz P, Pawłowski M and Bourennane M 2017 Complementarity between entanglement-assisted and quantum distributed random access code *Phys. Rev. A* **95** 052345
- [9] Wehner S, Christandl M and Doherty A C 2008 Lower bound on the dimension of a quantum system given measured data *Phys. Rev. A* **78** 062112
- [10] Tavakoli A, Kaniewski J, Vértesi T, Rosset D and Brunner N 2018 Self-testing quantum states and measurements in the prepare-and-measure scenario *Phys. Rev. A* **98** 062307
- [11] Farkas M and Kaniewski J 2019 Self-testing mutually unbiased bases in the prepare-and-measure scenario *Phys. Rev. A* **99** 032316
- [12] Tavakoli A, Smânia M, Vértesi T, Brunner N and Bourennane M 2018 *Self-Testing Non-Projective Quantum Measurements in Prepare-and-Measure Experiments* arXiv:1811.12712
- [13] Pawłowski M, Paterek T, Kaszlikowski D, Scarani V, Winter A and Żukowski M 2009 Information causality as a physical principle *Nature* **461** 1101
- [14] Mayers D and Yao A 2004 Quantum cryptography with imperfect apparatus *Quantum Inf. Comput.* **4** 273
- [15] Wagner S, Bancal J-D, Sangouard N and Sekatski P 2018 *Device-Independent Characterization of Generalized Measurements* arXiv:1812.02628
- [16] Sekatski P, Bancal J-D, Wagner S and Sangouard N 2018 Certifying the building blocks of quantum computers from Bell's theorem *Phys. Rev. Lett.* **121** 180505
- [17] Wang Y, Primaatmaja I W, Lavie E, Varvitsiotis A and Lim C C W 2019 Characterising the correlations of prepare-and-measure quantum networks *NPJ Quantum Inf.* **5** 17
- [18] Pellonpää J-P 2013 Quantum instruments: I. Extreme instruments *J. Phys. A: Math. Theor.* **46** 025302
- [19] Buhrman H, Cleve R and van Dam W 2001 Quantum entanglement and communication complexity *SIAM J. Comput.* **30** 1829
- [20] Brukner C, Żukowski M, Pan J-W and Zeilinger A 2004 Bell's inequalities and quantum communication complexity *Phys. Rev. Lett.* **92** 127901
- [21] Tavakoli A and Żukowski M 2017 Higher-dimensional communication complexity problems: classical protocols versus quantum ones based on Bell's theorem or prepare-transmit-measure schemes *Phys. Rev. A* **95** 042305
- [22] Silva R, Gisin N, Guryanova Y and Popescu S 2015 Multiple observers can share the nonlocality of half of an entangled pair by using optimal weak measurements *Phys. Rev. Lett.* **114** 250401
- [23] Mal S, Majumdar A S and Home D 2016 Sharing of nonlocality of a single member of an entangled pair of qubits is not possible by more than two unbiased observers on the other wing *Mathematics* **4** 48
- [24] Shenoy A H, Designolle S, Hirsch F, Silva R, Gisin N and Brunner N 2019 Unbounded sequence of observers exhibiting Einstein–Podolsky–Rosen steering *Phys. Rev. A* **99** 022317
- [25] Gallego R, Würflinger L E, Chaves R, Acín A and Navascués M 2014 Nonlocality in sequential correlation scenarios *New J. Phys.* **16** 033037
- [26] Curchod F J, Johansson M, Augusiak R, Hoban M J, Wittek P and Acín A 2017 Unbounded randomness certification using sequences of measurements *Phys. Rev. A* **95** 020102(R)
- [27] Tavakoli A and Cabello A 2018 Quantum predictions for an unmeasured system cannot be simulated with a finite-memory classical system *Phys. Rev. A* **97** 032131
- [28] Bera A, Mal S, Sen De A and Sen U 2018 Witnessing bipartite entanglement sequentially by multiple observers *Phys. Rev. A* **98** 062304
- [29] Sasmal S, Das D, Mal S and Majumdar A S 2018 Steering a single system sequentially by multiple observers *Phys. Rev. A* **98** 012305
- [30] Anwer H, Wilson N, Silva R, Muhammad S, Tavakoli A and Bourennane M 2019 *Noise-Robust Contextuality Shared Between Any Number of Observers* arXiv:1904.09766
- [31] Schiavon M, Calderaro L, Pittaluga M, Vallone G and Villoresi P 2017 Three-observer Bell inequality violation on a two-qubit entangled state *Quantum Sci. Technol.* **2** 015010
- [32] Hu M-J, Zhou Z-Y, Hu X-M, Li C-F, Guo G-C and Zhang Y-S 2018 Observation of non-locality sharing among three observers with one entangled pair via optimal weak measurement *NPJ Quantum Inf.* **4** 63
- [33] Foletto G, Calderaro L, Tavakoli A, Schiavon M, Picciariello F, Cabello A, Villoresi P and Vallone G 2019 arXiv:1906.07412 [quant-ph]
- [34] Miklin N, Borkala J J and Pawłowski M 2019 *Self-Testing of Unsharp Measurements* arXiv:1903.12533