

Semi-device-independent self-testing of unsharp measurements

Nikolai Miklin¹,* Jakub J. Borkała, and Marcin Pawłowski

Institute of Theoretical Physics and Astrophysics, National Quantum Information Center, Faculty of Mathematics, Physics and Informatics, University of Gdańsk, 80-952 Gdańsk, Poland



(Received 9 April 2019; revised 9 June 2020; accepted 12 June 2020; published 6 July 2020)

Unsharp quantum measurements provide a resource in scenarios where one faces the trade-off between information gain and disturbance. In this work we introduce a prepare-transform-measure scenario in which two-outcome unsharp measurements outperform their sharp counterparts, as well as any stochastic strategy involving dichotomic projective measurements. Based on that, we propose a scheme for semi-device-independent self-testing of unsharp measurements and show that all two-outcome qubit measurements can be characterized in a robust way. Along with the main result, in this work we introduce a method, based on semidefinite programming, for bounding quantum correlations in scenarios with sequential measurements of length 2. This method can also be applied to refine security analysis of the semi-device-independent one-way quantum key distribution. We also present an information gain–disturbance relation for pairs of dichotomic measurements.

DOI: [10.1103/PhysRevResearch.2.033014](https://doi.org/10.1103/PhysRevResearch.2.033014)

I. INTRODUCTION

Nonprojective, or generalized, measurements are known to provide an advantage in various quantum information processing tasks. Examples include quantum tomography [1,2], state discrimination [3,4], and randomness certification [5], to name a few. However, there is one important property of generalized measurements that is discussed less often than the others. It is the trade-off between information gain and disturbance that this type of measurement may allow for.

In quantum measurement, if some information is obtained about the state of the measured system, that state will necessarily be perturbed. This principle, which was formalized in Ref. [6], is central to quantum mechanics and it is also one of the pillars of quantum cryptography [7]. Quantitatively the interplay between information gain and disturbance has been formulated in numerous trade-off inequalities [8–11].

Sharp or “strong” measurement does not provide such a trade-off. The state of the system after sharp quantum measurement corresponds to one of the eigenstates of the measured observable. It means that the disturbance caused by sharp measurements is maximal and any subsequent measurement on the same system will not provide any additional information about its original state. On the other hand, maximally unsharp measurement, corresponding to an identity channel applied on the state, does not cause any disturbance, but at the same time it does not give any information about the state of the system. In the case of two-outcome qubit

measurements, which we discuss in this paper, the above two types of measurements are precisely the two variants of projective measurements. Hence, the aforementioned trade-off is possible only if one has access to a device performing nonprojective, or generalized, measurements.

At this point we should clarify some terminology that we use in this paper. Throughout the text we use the terms “two-outcome,” “binary,” and “dichotomic” interchangeably. For two-outcome qubit measurements, the terms “unsharp” and “nonprojective” mean the same thing except for the case of maximally unsharp measurements, which are trivial measurements and are not interesting to study. Keeping this in mind, we note that the term “nonprojective” is very often associated exclusively with three- or more-outcome measurements in the case of qubit systems. Hence, we chose to use the term “unsharp” to denote two-outcome nonprojective measurement throughout this work. Unsharp measurements that aim at bringing minimal disturbance to the system are often referred to as “weak measurements” [12].

Unsharp and, in particular, weak measurements have been the subject of numerous studies [8–11,13–17]. We would like to mention some of the recent results of Refs. [18–20] showing that nondestructive sequential unsharp measurements can be utilized to establish nonlocal correlations among multiple parties from one entangled pair and generate an unbounded amount of certified randomness. Naturally, given their importance, unsharp quantum measurements were reportedly implemented by various experimental groups [15,16]. However, all of these results require one’s trust in the measuring or preparation devices.

In this paper we ask the following questions: Is it possible to certify implementation of an unsharp measurement without making any assumptions, or with minimal assumptions made about the inner workings of the devices? If so, can one characterize the performed measurement based solely on the observed statistics? The answer comes from the rapidly

*nikolai.miklin@ug.edu.pl

growing field of *self-testing* [21,22]. It turns out that in quantum experiments it is possible to certify implementation of the target measurement or preparation of the desired state from the statistics alone and with minimal assumptions made about the inner workings of the devices. The most prominent example is self-testing of a two-qubit Bell state in the case of maximal violation of Clauser-Horne-Shimony-Holt (CHSH) inequality [23–25].

Self-testing was originally proposed in the framework of the Bell test [21], also known as device-independent (DI) characterization. However, it was soon generalized to a more experimentally appealing prepare-and-measure scenario [26], which followed the ideas of semi-device-independent (SDI) characterization of quantum systems [27]. In the SDI framework one assumes that the dimension of the degree of freedom of a physical system used for information processing is bounded from above. We would like to point out that the assumption on the dimension is not only natural for studying generalized measurements (due to the possibility of a dilation), but it is also necessary for obtaining nontrivial results in scenarios with sequential measurements, as widely discussed in the literature [28–30]. Additionally, more and more works on self-testing are now considering the SDI framework [26,31–33].

The majority of self-testing results, in both DI and SDI settings, consider target objects, e.g., an entangled state, that satisfy the property of extremality. In this case, one can hope to find a witness, e.g., a Bell inequality, that singles it out. In our case, the situation is somewhat more complicated. The reason is that statistics of an unsharp binary qubit measurement can be reproduced exactly by a statistical mixture of projective measurements on the same state space without any postprocessing [34]. As a consequence, if one considers a simple prepare-and-measure scenario, it will not be possible to distinguish whether the measuring device performs an actual unsharp measurement or its simulation.

In this work we overcome the above limitations by considering a tripartite prepare-transform-measure scenario. We introduce a game in which unsharp measurements outperform their sharp counterparts as well as any statistical mixture of projective measurements. This claim is formalized by two propositions in Sec. III. In Sec. IV we show that in the proposed scenario one can device-independently characterize all two-outcome unsharp qubit measurements, subject to an assumption that the physical system that parties use for information processing is a qubit. In the same section we show that this characterization is robust to noise. In our proofs regarding self-testing we use semidefinite-programming techniques that we describe in Sec. V. These techniques can be used to tackle many other problems involving sequential measurements outside of the current work. We demonstrate it by refining the security analysis of the SDI one-way quantum key distribution [27] in Sec. VI. Some proofs as well as minor technical details are left for the Appendix.

II. PREPARE-TRANSFORM-MEASURE SCENARIO

Let us now introduce our scenario which is a generalization of $2 \rightarrow 1$ quantum random access code (QRAC) [35]. Consider three parties, Alice, Bob, and Charlie, communicating in

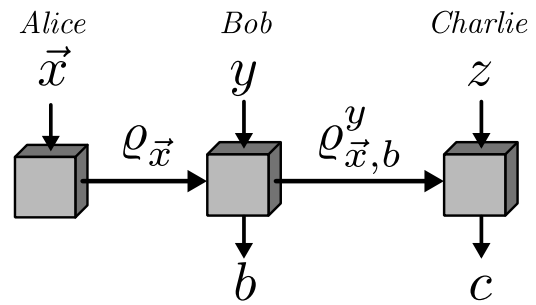


FIG. 1. Scenario: \vec{x} , input data of Alice; y and b , input and output of Bob; z and c , input and output of Charlie; $\rho_{\vec{x}}$, states that Alice sends to Bob; and $\rho_{\vec{x},b}^y$, states that Bob sends to Charlie.

a sequential way as shown in Fig. 1. Alice receives two random bits $\vec{x} = (x_0, x_1)$, $x_0, x_1 \in \{0, 1\}$. Bob and Charlie each receive a random bit, y and z , respectively, which indicates the bit of Alice this party needs to guess. All the random bits x_0, x_1, y , and z are independent and uniformly distributed. We assume that the parties do not share any entangled states; however, they may have access to any amount of shared classical randomness. Depending on \vec{x} , Alice prepares a qubit state $\rho_{\vec{x}}$ which she sends to Bob. Bob performs some quantum operation on $\rho_{\vec{x}}$, depending on his input y , and obtains a classical outcome b . Afterwards, Bob sends the postoperation state $\rho_{\vec{x},b}^y$ to Charlie, who performs a measurement depending on z .

A figure of merit that we consider is the following average success probability:

$$\bar{P}_{\text{succ}} = \frac{\alpha}{8} \sum_{\vec{x}, y} \Pr(b = x_y | \vec{x}, y) + \frac{1-\alpha}{8} \sum_{\vec{x}, z} \Pr(c = x_z | \vec{x}, z), \quad (1)$$

with $\alpha \in [0, 1]$ and where summation is taken over all values of \vec{x}, y and \vec{x}, z , respectively. The parameter α is announced prior to the game and remains unchanged throughout all the rounds. It dictates the parties whose guess contributes more to the overall success probability. As we show later in the text, the optimal operations that Bob performs in the case of $\alpha \in (0, 1)$ correspond to unsharp measurements.

Preliminary notions

Measurements in quantum mechanics are formalized by the notion of positive-operator-valued measure (POVM). For two-outcome measurements, which we consider in this paper, a POVM is an ordered pair of positive-semidefinite linear operators (B_0, B_1) , $B_i \in \mathcal{L}(\mathcal{H})$, $B_i \geq 0$, $i = 0, 1$, satisfying $B_0 + B_1 = \mathbb{1}$, where $\mathbb{1}$ is the identity operator. Projection-valued measure (PVM) is a special case that corresponds to $B_i^2 = B_i$, $i = 0, 1$. From here it is clear that the only two possibilities of two-outcome qubit PVMs are sharp measurements, with both B_i being normalized rank-1 operators, and the maximally unsharp, or trivial, measurement with one B_i equal to $\mathbb{1}$ and the other being zero. We call a POVM (B_0, B_1) unbiased if $\text{tr}(B_0) = \text{tr}(B_1) = 1$ and biased otherwise. In this work we concentrate on the former case as it encapsulates the resources that are interesting to us for the trade-off between information gain and disturbance. The biased case allows for

an additional flexibility with respect to probability distribution of the measurement outcomes.

In order to describe the operations of Bob we need to introduce the notion of a quantum instrument, which captures both measurement statistics and the state evolution (see, e.g., Ref. [36]). By *quantum instrument* for the case of two measurement outcomes $\{0, 1\}$ we mean an ordered pair of completely positive trace nonincreasing maps that sum to a channel, completely positive trace-preserving map. Let us denote the instruments of Bob by $(\mathcal{B}_0^y, \mathcal{B}_1^y)$ for each y , where each $\mathcal{B}_b^y: \mathcal{L}(\mathcal{H}) \mapsto \mathcal{L}(\mathcal{H})$ and $\dim(\mathcal{H}) = 2$, in agreement with our SDI assumption. If we apply these maps to the state $\rho_{\vec{x}}$ (for a given \vec{x}), which Alice sends to Bob, we obtain a pair of positive operators $\sigma_{\vec{x},b}^y = \mathcal{B}_b^y(\rho_{\vec{x}})$, $b = 0, 1$. Their traces form the probability distribution of Bob's measurement outcomes $p(b|\vec{x}, y) = \text{tr}(\sigma_{\vec{x},b}^y)$ and, if normalized, these operators correspond to the postmeasurement states that Bob sends to Charlie, $\rho_{\vec{x},b}^y = \sigma_{\vec{x},b}^y / p(b|\vec{x}, y)$. We say that instrument $(\mathcal{B}_0^y, \mathcal{B}_1^y)$ is compatible with a POVM (B_0^y, B_1^y) if for all states ρ , $\text{tr}(\rho B_b^y) = \text{tr}(\mathcal{B}_b^y(\rho))$, $b = 0, 1$.

Using the formalism of quantum instruments we can write the joint probability distribution of both parties' outcomes as follows:

$$p(b, c|\vec{x}, y, z) = \text{tr}(\mathcal{B}_b^y(\rho_{\vec{x}}) C_c^z), \quad (2)$$

where we denoted Charlie's POVMs by (C_0^z, C_1^z) , $z = 0, 1$. Naturally, using this formula we can calculate the probabilities in our figure of merit [Eq. (1) in the main text].

The action of an instrument on a state can be specified by its Kraus decomposition (see, e.g., Ref. [36]). However, it will be more convenient for us to work with instruments in their Choi-Jamiołkowski (CJ) representation (see, e.g., Ref. [36]). We obtain the CJ operators of Bob's instruments by the following map:

$$\mathfrak{B}_b^y = (\mathcal{I} \otimes \mathcal{B}_b^y(|\Omega\rangle\langle\Omega|)), \quad (3)$$

where \mathcal{I} is an identity map on elements of $\mathcal{L}(\mathcal{H})$ and $|\Omega\rangle$ is a non-normalized Bell state $|\Omega\rangle = \sum_{i=0,1} |ii\rangle$. The inverse map is given by the relation $\mathcal{B}_b^y(\rho) = \text{tr}_1(\rho^T \otimes \mathbb{1} \mathfrak{B}_b^y)$, where the partial trace is taken with respect to the first subsystem, and $(\cdot)^T$ stands for matrix transpose with respect to the basis $\{|i\rangle\}_{i=0,1}$ in which the CJ isomorphism is defined. From this relation it is clear that POVM (B_0^y, B_1^y) , associated with the CJ operator $(\mathfrak{B}_0^y, \mathfrak{B}_1^y)$, is simply a pair of reduced operators with the trace taken over the second (output) subsystem, i.e., $B_b^y = \text{tr}_2(\mathfrak{B}_b^y)^T$, $b = 0, 1$, for each $y = 0, 1$.

Using CJ representation of the instruments we can rewrite the conditional probabilities observed in our scenario as follows:

$$p(b, c|\vec{x}, y, z) = \text{tr}(\rho_{\vec{x}}^T \otimes C_c^z \mathfrak{B}_b^y). \quad (4)$$

One can immediately notice that the above formula is very similar to the one of tensor product measurements on an entangled state. This motivated us to try to apply the semidefinite-programming (SDP) techniques of Ref. [37] to bound correlations in Eq. (4). As discussed in Sec. V, these SDP techniques had to be modified for this purpose.

III. UNSHARPNESS AS A RESOURCE

We have already mentioned in the Introduction that unsharp measurements are needed to access the trade-off between information gain and disturbance. In this section we show that the figure of merit in Eq. (1) allows for witnessing unsharpness of the performed measurement in an SDI way, i.e., with no assumptions about the measuring or preparation devices apart from the upper bound on the dimension of the underlined Hilbert space. We are ready to present our first part of the results, which is given by the following two propositions.

Proposition 1. The average success probability \bar{P}_{succ} for strategies involving only projective measurements and their probabilistic mixtures is bounded by the following expression:

$$\bar{P}_{\text{succ}}^{\text{PVM}}(\alpha) = \begin{cases} \frac{1}{2} + \frac{1-\alpha}{2\sqrt{2}}, & 0 \leq \alpha \leq 1 - \frac{2}{\sqrt{7}} \\ \frac{1}{2} + \frac{1}{8}\sqrt{4 + (1-\alpha)^2}, & 1 - \frac{2}{\sqrt{7}} < \alpha \leq \frac{1}{3} \\ \frac{1}{2} + \frac{1}{4}\sqrt{1 + \alpha^2}, & \frac{1}{3} < \alpha \leq 1. \end{cases}$$

The reason that the function $\bar{P}_{\text{succ}}^{\text{PVM}}(\alpha)$ has three distinct segments is that Bob can choose to apply one of the three different optimal strategies depending on α . The first one, which we call ‘‘unitary,’’ corresponds to the maximally unsharp measurement $(\mathbb{1}, 0)$ for both $y = 0, 1$, which is compatible with Bob outputting $b = 0$ and applying a unitary channel on Alice's states. The third one is the ‘‘measure-and-prepare’’ strategy, in which Bob performs a sharp measurement for both $y = 0, 1$ and prepares some state that he sends to Charlie. The middle segment corresponds to Bob applying the unitary strategy for $y = 0$, and the prepare-and-measure strategy for $y = 1$ (or the other way around), which we refer to as a ‘‘mixed’’ strategy. The proof of Proposition 1 is too lengthy to be included in the main text and is given in Appendix C.

Proposition 2. The bound on the average success probability \bar{P}_{succ} for the general strategy involving unsharp measurements is the following:

$$\bar{P}_{\text{succ}}^{\text{POVM}}(\alpha) = \frac{1}{2} + \frac{1-\alpha}{4\sqrt{2}} + \frac{1}{4\sqrt{2}}\sqrt{(1-\alpha)^2 + 4\alpha^2}.$$

The results of both Propositions 1 and 2 are shown in Fig. 2. In this figure we also show the classical bound for this game, which evidently equals $\frac{3}{4}$ irrespective of α . We should point out that all the presented bounds are tight in the sense that there exist states and measurements reaching these average success probabilities.

The optimal quantum strategy that attains the bound in Proposition 2 is the following. The states of Alice have the same form as in the $2 \rightarrow 1$ QRAC, i.e., independent of α . Their explicit form is given below, where we denote $\rho_{\vec{x}}^T = |\psi_{\vec{x}}\rangle\langle\psi_{\vec{x}}|$:

$$\begin{aligned} |\psi_{00}\rangle &= \frac{|0\rangle + |+\rangle}{\sqrt{2 + \sqrt{2}}}, & |\psi_{01}\rangle &= \frac{|0\rangle + |-\rangle}{\sqrt{2 + \sqrt{2}}}, \\ |\psi_{10}\rangle &= \frac{|1\rangle + |+\rangle}{\sqrt{2 + \sqrt{2}}}, & |\psi_{11}\rangle &= \frac{|1\rangle - |-\rangle}{\sqrt{2 + \sqrt{2}}}. \end{aligned} \quad (5)$$

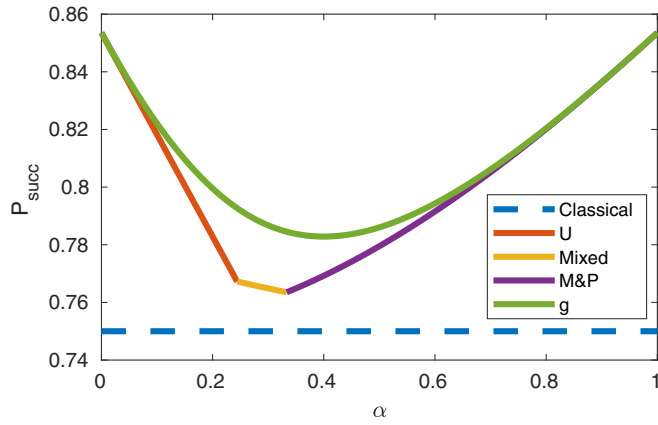


FIG. 2. Bounds on the average success probability. Blue (dashed) line corresponds to the classical strategy. The three-segment line corresponds (from left to right) to the unitary (orange), mixed (yellow), and measure-and-prepare (purple) projective strategies, respectively. The green (uppermost) line corresponds to the general strategy with unsharp measurements. All the bounds are tight.

The optimal POVMs of Charlie can be set to be the following:

$$\begin{aligned} (C_0^0, C_1^0) &= (|0\rangle\langle 0|, |1\rangle\langle 1|), \\ (C_0^1, C_1^1) &= (|+\rangle\langle +|, |-\rangle\langle -|), \end{aligned} \quad (6)$$

and the optimal instruments of Bob (their CJ operators) can be taken to be of the form $\mathfrak{B}_b^y = |\beta_b^y\rangle\langle\beta_b^y|$,

$$\begin{aligned} |\beta_0^0\rangle &= \sqrt{\lambda}|00\rangle + \sqrt{1-\lambda}|11\rangle, \\ |\beta_1^0\rangle &= \sqrt{1-\lambda}|00\rangle + \sqrt{\lambda}|11\rangle, \\ |\beta_0^1\rangle &= \sqrt{\lambda}|+\rangle + \sqrt{1-\lambda}|-\rangle, \\ |\beta_1^1\rangle &= \sqrt{1-\lambda}|+\rangle + \sqrt{\lambda}|-\rangle, \end{aligned} \quad (7)$$

where we left the real parameter λ unspecified. It is clear that λ determines the sharpness of the corresponding measurement of Bob. We find that the optimal λ is the following function of α :

$$\lambda = \frac{1}{2} + \frac{\alpha}{\sqrt{(1-\alpha)^2 + 4\alpha^2}}, \quad (8)$$

which leads to the expression of the optimal average success probability from Proposition 2.

The above analysis gives only a lower bound on the average success probability. In order to prove that this bound is also an upper bound we used the aforementioned SDP techniques, described in Sec. V. We compared the numerical results from the SDP for each value of α with a step of 0.001 with the lower bound values from Proposition 2 and the discrepancy was always less than or of the order of 10^{-9} , which leads us to conclude that the obtained bound is in fact the correct one.

Having a gap between success probabilities achieved by projective measurements and unsharp measurements is necessary for the self-testing claims. However, already from the results of Propositions 1 and 2 it follows that if one experimentally obtains a value of average success probability that is greater than $\bar{P}_{\text{succ}}^{\text{PVM}}(\alpha)$ for some α , one can conclude that Bob's measuring device performed an unsharp measurement. In

order to answer the question of exactly which measurements were performed by Bob we will need a stronger result, given in the next section.

IV. SDI CHARACTERIZATION OF UNSHARP MEASUREMENTS

The core idea that we use in our paper is to certify implementation of a quantum instrument that realizes the target unsharp measurement. The set of quantum instruments realizing a given unsharp POVM is strictly larger than the set of probabilistic mixtures of instruments corresponding to PVMs that reproduce the same measurement statistics for Bob. It is surprising that a simple and intuitive figure of merit [Eq. (1)] is sufficient to witness this fact. Although the target measurements that we would like to self-test are not extremal in the space of all POVMs, some instruments that realize these measurements are extremal and hence can potentially be witnessed by saturating the bound in Proposition 2.

In this paper we focus on certification of the unsharpness parameter of the performed measurement from the observed data. In this section we only consider two-outcome unbiased qubit POVMs. Hence, the unsharpness parameter, which can be taken to be the operator norm of one of the effects, completely characterizes these measurements up to an isometry. Hence, this SDI characterization is equivalent to the SDI self-testing of individual measurements.

Since the figure of merit in Eq. (1), when written in terms of probabilities in Eq. (4), is linear with respect to CJ operators of Bob's instruments, it is sufficient to consider only extremal instruments. In Appendix B we show that in our case the extremal instruments have the form as in Eq. (7) (with λ being dependent on y , in general). Hence, the sharpness of the corresponding POVM is exactly the parameter λ in Eq. (8).

Now, we come to our main question of what can be said about the unsharpness parameter λ for each y given the observed value of the average success probability in Eq. (1). We answer this question by setting the opposite problem: What are the maximal values of the average success probability attainable by POVMs (B_0^y, B_1^y) with a given norm? It turns out that the optimal (B_0^y, B_1^y) is always unbiased for the figure of merit in Eq. (1).

Our results on the robust SDI characterization of unsharp measurements are shown in Fig. 3. The black line represents the case of the ideal statistics, in which case the norm of the target measurements (B_0^y, B_1^y) is the same for both $y = 0, 1$ and is given by the expression in Eq. (8). As we can see, the above norm is a monotonically increasing function of α and its image is the interval $[\frac{1}{2}, 1]$. This fact suggests that we can self-test any unsharp unbiased two-outcome qubit measurement by picking the corresponding value of α .

In Fig. 3 each pair of lines of the same color represents upper and lower bounds on the norm of the POVM for each $y = 0, 1$, given that the average success probability is above some fixed value. We would like to stress that we do not assume that both norms for $y = 0$ and $y = 1$ are equal. In Fig. 3 we show four values $\{0\%, 0.25\%, 0.5\%, 1\%\}$ for $\frac{\epsilon}{\bar{P}_{\text{succ}}^{\text{PVM}}(\alpha)}$, where ϵ is the deviation of the observed value of \bar{P}_{succ}

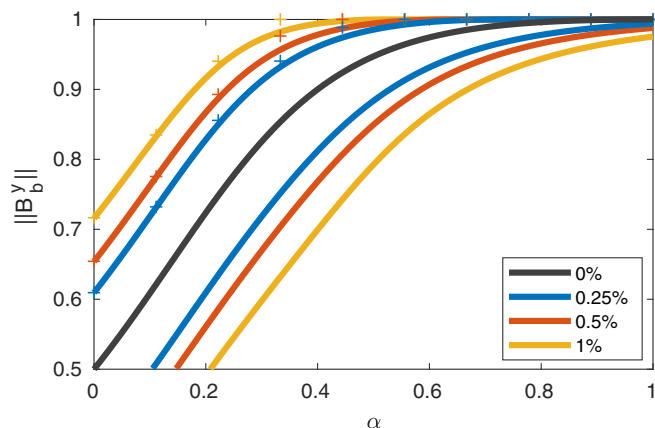


FIG. 3. Illustration of the results on robust SDI characterization of unsharp measurements. The optimal operator norm (black line) and bounds on the norm (color or grey lines) for different values of deviation from the optimal success probability. The crosses represent the discrepancy between the solution which we believe is optimal and the bound that we could prove with our SDP techniques. For more details please see Appendix D.

from the optimal value $\bar{P}_{\text{succ}}^{\text{POVM}(\alpha)}$. From the plot one can see that for ε going to zero, the region of the compatible norms shrinks monotonically to a point with λ given by Eq. (8) for both y . This fact suggests that our SDI characterization is indeed robust.

We would like to give an example of how to read the plots in Fig. 3. Let us say we wish to self-test a measurement with the norm equal to $\frac{1}{2} + \frac{1}{2\sqrt{5}}$. We would pick $\alpha = 0.2$, for which POVMs with this norm are the optimal ones. If now our observed average success probability is equal to 0.7975, which is 0.25% smaller than the optimal value $\bar{P}_{\text{succ}}^{\text{POVM}}(0.2) \approx 0.7995$, we can conclude that the norm of the implemented POVM for both $y = 0, 1$ must lay within the interval $[0.6095, 0.8281]$. A more detailed description of the robustness analysis is given in Appendix D. In Appendix E we also give a sufficient numerical evidence that our scheme can be adapted to SDI characterization of biased unsharp measurements.

V. METHODS

The proof of Proposition 1 is almost entirely analytical (see Appendix C). For the proof of Proposition 2 as well as for the results of the previous section we used SDP techniques that we describe in this section. These SDP techniques are based on the hierarchy of Navascués and Vértesi [37]. Below, we also provide an argument why the hierarchy of Ref. [37] cannot be directly applied to our problem. Moreover, our SDP techniques can be applied to a variety of problems involving two sequential measurements on a single system. For example, in Sec. VI we refine the analysis of the SDI one-way quantum key distribution proposed in Ref. [27]. There we show that a secure key can be distilled whenever the success probability of a QRAC exceeds the classical limit of $\frac{3}{4}$, which is a significant improvement compared to the original result [27].

The SDP hierarchy of Navascués and Vértesi [37] is very useful for bounding correlations in the Bell scenario with an additional restriction on the local dimension. One can

also use this hierarchy to approximate the sets of quantum correlations in the prepare-and-measure scenario, where the dimension constraint is crucial. In particular, using Ref. [37] one can directly obtain upper bounds on success probabilities of QRACs. We do not summarize the method of Ref. [37] here, so the interested reader should first make themselves familiar with it before reading the following description of the proposed modification.

In our modification of the hierarchy of Ref. [37], which we formulate here for what is known as the “1+AB” level, we consider the following set of operators

$$\mathcal{O} = \{\mathbb{1} \otimes \mathbb{1}\} \cup \{\varrho_{\vec{x}} \otimes \mathbb{1}\}_{\vec{x}} \cup \{\mathbb{1} \otimes C_0^z\}_z, \{\varrho_{\vec{x}} \otimes C_0^z\}_{\vec{x}, z}.$$

We then consider four moment matrices Γ_b^y for each y, b . For each Γ_b^y we assume the measure $\text{tr}(\cdot \mathfrak{B}_b^y)$; i.e., the entries $\Gamma_b^y(O_1, O_2)$ of the matrix correspond to $\text{tr}(O_1^\dagger O_2 \mathfrak{B}_b^y)$, $O_1, O_2 \in \mathcal{O}$. It is clear that each Γ_b^y must be positive semidefinite, i.e., $\Gamma_b^y \geq 0$, $y = 0, 1, b = 0, 1$. Also, we can use the main idea of the hierarchy of Ref. [37] and construct a basis for Γ_b^y from randomly sampled operators of fixed dimension. However, we need to apply more constraints on Γ_b^y in order to obtain nontrivial bounds on our figure of merit in Eq. (1).

In particular, we exploit the fact that $\text{tr}_2(\mathfrak{B}_0^y) + \text{tr}_2(\mathfrak{B}_1^y) = \mathbb{1}$, for each y . From this we can derive the following set of constraints that has to be satisfied by all quantum probabilities $p(b, c|\vec{x}, y, z)$:

$$\begin{aligned} \sum_{b=0,1} \Gamma_b^y(\mathbb{1} \otimes \mathbb{1}, \mathbb{1} \otimes \mathbb{1}) &= 2, \quad y = 0, 1, \\ \sum_{b=0,1} \Gamma_b^y(\varrho_{\vec{x}} \otimes \mathbb{1}, \mathbb{1} \otimes \mathbb{1}) &= 1, \quad \forall \vec{x}, y = 0, 1, \\ \sum_{b=0,1} \Gamma_b^0(\varrho_{\vec{x}} \otimes \mathbb{1}, \varrho_{\vec{x}'} \otimes \mathbb{1}) \\ &= \sum_{b=0,1} \Gamma_b^1(\varrho_{\vec{x}} \otimes \mathbb{1}, \varrho_{\vec{x}'} \otimes \mathbb{1}), \quad \forall \vec{x}, \vec{x}'. \end{aligned} \quad (9)$$

The above constraints should be interpreted as follows. The first type fixes the normalization of the instruments, and the second fixes the normalization of states $\{\varrho_{\vec{x}}\}_{\vec{x}}$. Finally, the third type of constraint ensures that all the inner products between the states $\{\varrho_{\vec{x}}\}_{\vec{x}}$ are the same for both choices of Bob’s operations. Although the above modification is formulated for our scenario with binary x_0, x_1, y, z, b , and c , it is straightforward to generalize it to other scenarios with arbitrary numbers of settings and outputs.

Now, we would like to argue why the original hierarchy of Ref. [37], as it stands, could not be applied to our problem. One could, in principle, try to explicitly include the CJ operators $\{\mathfrak{B}_b^y\}_{y,b}$ to the set of operators \mathcal{O} and consider a single moment matrix. However, this would require \mathfrak{B}_b^y to be projectors in some potentially larger Hilbert space, which is not in general the case, since we do not know the normalization of the CJ operator of each individual element of the instrument.

In this paper we have successfully used the proposed SDP method to confirm the bounds obtained with the inner approximation methods. It would be interesting to investigate the convergence of this modified hierarchy [38].

VI. APPLICATIONS

A. Trade-off relation

As an application of the results of Proposition 2, we can derive new trade-off relations in terms of QRAC success probabilities attainable in the described sequential scenario. Indeed, our figure of merit can be rewritten as $\bar{P}_{\text{succ}} = \alpha \bar{P}_{\text{Bob}} + (1 - \alpha) \bar{P}_{\text{Charlie}}$. From the condition $\bar{P}_{\text{succ}} \leq \bar{P}_{\text{succ}}^{\text{PVM}}(\alpha)$ we can derive the following trade-off relation:

$$\bar{P}_{\text{Charlie}} \leq \frac{1}{2} + \frac{1}{4\sqrt{2}} + \frac{\sqrt{16\bar{P}_{\text{Bob}}(1 - \bar{P}_{\text{Bob}}) - 2}}{8}.$$

This relation can be used to calculate the disturbance caused by the measurement of Bob by subtracting \bar{P}_{Charlie} from the maximally attainable value of $\frac{1}{2} + \frac{1}{2\sqrt{2}}$.

B. Security of the SDI one-way quantum key distribution

Here we demonstrate that the SDP techniques introduced in the previous section have applications outside of the current work. To do this we refine the analysis of the security in semi-device-independent one-way quantum key distribution (QKD), proposed in Ref. [27].

Let us briefly introduce this QKD scheme. In this scheme two communicating parties, Alice and Bob, are trying to establish a secret key without trusting their devices. As a measure of privacy of the generated key they use the figure of merit of the $2 \rightarrow 1$ QRAC, which reads

$$\bar{P}_{\text{succ}}^{\text{QRAC}} = \frac{1}{8} \sum_{\vec{x}, y} P(b = x_y | \vec{x}, y). \quad (10)$$

The eavesdropping party, Eve, is trying to guess the bit of Alice corresponding to Bob's input bit y , i.e., to maximize the probability $\bar{P}_{\text{succ}}^{\text{Eve}} = \frac{1}{8} \sum_{\vec{x}, y} P(e = x_y | \vec{x}, y)$, where e is Eve's output. We can then introduce a real parameter $\alpha \in [0, 1]$ just like we did in the main text and consider the following objective function,

$$\bar{P}_{\text{succ}} = \frac{\alpha}{8} \sum_{\vec{x}, y} P(b = x_y | \vec{x}, y) + \frac{1 - \alpha}{8} \sum_{\vec{x}, y} P(e = x_y | \vec{x}, y), \quad (11)$$

which resembles the figure of merit in Eq. (1). We then optimize the expression in Eq. (11) subject to the constraints of the SDP method described in Sec. V. Afterwards, by optimizing over α we obtain the monogamy relations between $\bar{P}_{\text{succ}}^{\text{Eve}}$ and $\bar{P}_{\text{succ}}^{\text{QRAC}}$ that we plot in Fig. 4.

As shown in Ref. [27], Alice and Bob are able to distill a secret key from their QRAC correlations whenever $P_{\text{QRAC}}^{\text{Charlie}} > P_{\text{Eve}}^{\text{Bob}}$. From this condition one can calculate the critical success probability of QRAC required for the task. In Ref. [27] the authors estimated this critical probability to be $\frac{5+\sqrt{3}}{8} \simeq 0.8415$, which is rather close to the maximal attainable success probability $\frac{1}{2} + \frac{1}{2\sqrt{2}} \simeq 0.8535$ of the $2 \rightarrow 1$ QRAC. From our plot in Fig. 4 one can see that it is enough for the average success probability $\bar{P}_{\text{succ}}^{\text{QRAC}}$ to be just above the classical limit of $\frac{3}{4}$. The latter value was also reported in Ref. [39], where the security of the SDI QKD scheme was analyzed from the point of view of the critical detection

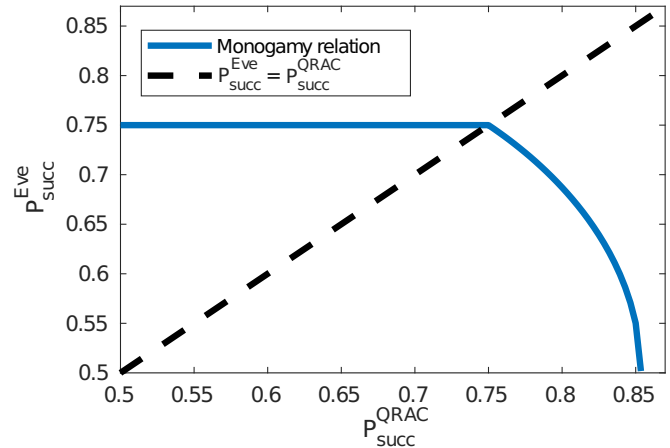


FIG. 4. Solid line: monogamy relation for the SDI QKD scheme. Dashed line: the critical regime in which the guessing probabilities of the receiver and the eavesdropper are the same.

efficiency of the receiver's detectors. However, to the best of our knowledge, the monogamy relation in Fig. 4 has not appeared in the literature prior to this work.

It is clear that our SDP techniques can be used for the analysis of the security of one-way quantum key distribution in scenarios beyond the one in Ref. [27]. Furthermore, there is a way to extend the SDP techniques to analyze correlations in scenarios with sequential measurements of length 3.

VII. CONCLUSIONS

In this paper we have discussed the advantages that unsharp measurements can provide if one faces the trade-off between information gain and state disturbance. We have proposed a scheme in which this advantage can be manifested within the semi-device-independent framework. Using this scheme we have shown that all unsharp binary measurements on a qubit can be semi-device-independently characterized in a robust manner, which also implies SDI self-testing of individual measurements for the case of unbiased POVMs. This was possible due to certification of the instruments implementing the respective unsharp measurement.

In this work we considered only SDI characterization of individual two-outcome qubit measurements since the latter can be achieved by certifying a single real parameter, the unsharpness. However, it is clear that our analysis can be extended to more complicated cases. One generalization, which is definitely worth considering, is certification of trinary qubit measurements. We believe that our scheme can be easily adapted to these purposes.

Semidefinite-programming techniques proposed in this paper can be readily applied to analyze the security of more complex SDI quantum key distribution schemes. These techniques can also be applied to explore the set of sequential quantum correlations for the case of time-dependent operations and sequences of length 3.

Note added. After completing this work, we have become aware of the related result in Ref. [40]. In Ref. [40] the authors discuss self-testing of binary unsharp qubit measurements in the framework of the Bell test. In Appendix F we give a quick

comparison of the obtained results and the used frameworks. We would also like to draw the reader's attention to work in Ref. [41].

ACKNOWLEDGMENTS

N.M. would like to thank Costantino Budroni, Nicolas Brunner, Mariami Gachechiladze, and Anubhav Chaturvedi for useful discussions. The work on this project was supported by First TEAM Grant No. 2016-1/5. The SDP optimization was performed with SDPT3 solver [42] and YALMIP toolbox [43] for MATLAB.

APPENDIX A: INTRODUCTION AND NOTATION

In this Appendix we provide technical details omitted in the main text. In Appendix B we discuss the optimality of Lüders instruments, a fact regarding extremal instruments that we use in the main text. In Appendix C we give a proof of Proposition 1. Appendix D is dedicated to a more detailed description of our results on the robustness of SDI characterization of unsharp measurements. Apart from that, in Appendix D we derive an upper bound on the average success probability of $2 \rightarrow 1$ QRAC for the case of a dephasing channel being applied on the states of Alice. These results are used for the robustness proofs. In Appendix E we present our observations regarding the possibility of SDI characterization of biased two-outcome qubit measurements. Finally, in Appendix F we provide a comparison of our results with Ref. [40].

We start by fixing the notations that we use in this Appendix. We denote the preparation states of Alice by $\varrho_{\bar{x}}$, where $\bar{x} \in \{(00), (01), (10), (11)\}$. The POVMs of Charlie we denote by (C_0^z, C_1^z) . We use the notation $|\cdot^\perp\rangle$ to denote the qubit state orthogonal to the given one, i.e., $\langle\psi|\psi^\perp\rangle = 0$, $\forall|\psi\rangle \in \mathcal{H}$, which is not ambiguous in the qubit case. We also use the common shorthand notation $|i\rangle \otimes |i\rangle = |ii\rangle$, as well as $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$.

APPENDIX B: OPTIMALITY OF LÜDERS INSTRUMENTS

In this Appendix we show that the optimal instruments of Bob are of Lüders type, which is essentially equivalent to saying that the optimal instruments have rank-1 CJ operators. Using the formula for conditional probability from Eq. (4) we can write explicitly the expression for the average success probability (1) in terms of operators $\sigma_{\bar{x},b}^y = \mathcal{B}_b^y(\varrho_{\bar{x}})$ as follows:

$$\bar{P}_{\text{succ}} = \frac{1}{16} \sum_{\bar{x},y,z,b,c} \text{tr}(\sigma_{\bar{x},b}^y C_c^z) (\alpha \delta_{b,x_y} + (1 - \alpha) \delta_{c,x_z}). \quad (\text{B1})$$

Let us introduce new operators $\varrho_{\bar{x},\oplus}^y = \sigma_{\bar{x},0}^y \oplus \sigma_{\bar{x},1}^y$, $\varrho_{\bar{x},\oplus}^y \in \mathcal{L}(\mathcal{H}')$, $\forall \bar{x}, y$, with $\dim(\mathcal{H}') = 4$. We can think of $\varrho_{\bar{x},\oplus}^y$ as a block-diagonal matrix for each y and \bar{x} , with two blocks being $\sigma_{\bar{x},0}^y$ and $\sigma_{\bar{x},1}^y$. In a similar fashion we can construct operators $C_{\bar{x},c}^z = C_c^z(\alpha \delta_{0,x_y} + (1 - \alpha) \delta_{c,x_z}) \oplus$

$C_c^z(\alpha \delta_{1,x_y} + (1 - \alpha) \delta_{c,x_z})$, $C_{\bar{x},c}^{y,z} \in \mathcal{L}(\mathcal{H}')$, $\forall \bar{x}, y, z, c$. The expression in Eq. (B1) can then be written simply as

$$\bar{P}_{\text{succ}} = \frac{1}{16} \sum_{\bar{x},y,z,c} \text{tr}(\varrho_{\bar{x},\oplus}^y C_{\bar{x},c}^{y,z}). \quad (\text{B2})$$

It is easy to see that each $\varrho_{\bar{x},\oplus}^y$ is a state, i.e., $\varrho_{\bar{x},\oplus}^y \geq 0$, $\text{tr}(\varrho_{\bar{x},\oplus}^y) = 1$. It is also clear that the set of $\varrho_{\bar{x},\oplus}^y$ is convex and closed. Moreover, for the given POVMs of Bob B_b^y we can always construct a “measure-and-prepare” instrument of the form $\mathcal{B}_b^y(\cdot) = \text{tr}(B_b^y \cdot) \tilde{\varrho}_b^y$, where $\tilde{\varrho}_b^y$ are states. The states $\varrho_{\bar{x},\oplus}^y$ can then be expressed as $\varrho_{\bar{x},\oplus}^y = \text{tr}(\varrho_{\bar{x}} B_0^y) \tilde{\varrho}_0^y \oplus \text{tr}(\varrho_{\bar{x}} B_1^y) \tilde{\varrho}_1^y$. Since $\tilde{\varrho}_b^y$ can be chosen arbitrarily, we can conclude that the extreme elements of the set of $\varrho_{\bar{x},\oplus}^y$ are direct sums of pairs of pure states, multiplied by $\text{tr}(\varrho_{\bar{x}} B_0^y)$ and $\text{tr}(\varrho_{\bar{x}} B_1^y)$. The proof can be obtained trivially by assuming the opposite and writing the spectral decomposition for each of $\tilde{\varrho}_b^y$, which is then nothing but a convex combination of rank-1 block-diagonal operators (which means that the corresponding states are pure). Of course, measure-and-prepare instruments will not be optimal, but it is sufficient to consider this type of instrument to prove the optimality of rank-1 operators $\sigma_{\bar{x},b}^y$.

Now we can show that from the optimality of pure states of Alice $\varrho_{\bar{x}}$ and rank-1 operators $\sigma_{\bar{x},b}^y$ it follows that CJ operators of optimal Bob instruments are necessarily rank 1. Let us write the spectral decomposition of \mathfrak{B}_b^y for each y, b ,

$$\mathfrak{B}_b^y = \sum_{k=0}^3 |\beta_k\rangle\langle\beta_k|, \quad (\text{B3})$$

where $|\beta_k\rangle$ are not normalized. We did not write the subscripts y, b for $|\beta_k\rangle$ to avoid unnecessary complication, but, of course, $|\beta_k\rangle$ will be different for different y, b . Each $|\beta_k\rangle$ can be written in its Schmidt decomposition [44] as $|\beta_k\rangle = |p_k\rangle \otimes |q_k\rangle + |p_k^\perp\rangle \otimes |q_k^\perp\rangle$, where we can require $|q_k\rangle, |q_k^\perp\rangle$ to be normalized, and leave $|p_k\rangle, |p_k^\perp\rangle$ not normalized. If we denote $\varrho_{\bar{x}} = |\psi_{\bar{x}}\rangle\langle\psi_{\bar{x}}|$, we can write the following:

$$\sigma_{\bar{x},b}^y = \sum_{k=0}^3 |q_{\bar{x},k}\rangle\langle q_{\bar{x},k}|, \quad \text{with} \\ |q_{\bar{x},k}\rangle = \langle\psi_{\bar{x}}|p_k\rangle|q_k\rangle + \langle\psi_{\bar{x}}|p_k^\perp\rangle|q_k^\perp\rangle. \quad (\text{B4})$$

However, we have already concluded that optimal $\sigma_{\bar{x},b}^y$ must be rank-1 operators, which means that all $|q_{\bar{x},k}\rangle$ must coincide up to a phase, i.e., $|q_{\bar{x},k}\rangle = e^{i\phi_{k,k'}} |q_{\bar{x},k'}\rangle$ for some phases $\phi_{k,k'}$. Now we can use the argument that the optimal $|\psi_{\bar{x}}\rangle$ must necessarily be linearly independent, i.e., $\langle\psi_{\bar{x}}|\psi_{\bar{x}'}\rangle \neq 1$ for at least two \bar{x}, \bar{x}' , $\bar{x} \neq \bar{x}'$. It is pretty clear that in the opposite case Alice is not sending any information to Bob. Since $\{|\psi_{\bar{x}}\rangle\}_{\bar{x}}$ span the entire Hilbert space, we come to the conclusion that $|p_k\rangle \otimes |q_k\rangle + |p_k^\perp\rangle \otimes |q_k^\perp\rangle = e^{i\phi_{k,k'}} (|p_{k'}\rangle \otimes |q_{k'}\rangle + |p_{k'}^\perp\rangle \otimes |q_{k'}^\perp\rangle)$, $\forall k \neq k'$, i.e., $|\beta_k\rangle = e^{i\phi_{k,k'}} |\beta_{k'}\rangle$, $\forall k \neq k'$. However, since Eq. (B3) is a spectral decomposition, it must be that $\langle\beta_k|\beta_{k'}\rangle = \delta_{k,k'}$, $\forall k \neq k'$, from which it follows that there is only one vector in the sum in Eq. (B3). This completes the proof. We should mention that the above proof can be directly extended to the higher-dimensional case.

APPENDIX C: PROOF OF PROPOSITION 1

In this Appendix we prove the bounds given in Proposition 1 on the average success probability in Eq. (1) for the case of projective strategies of Bob. There are two types of projective measurements that we need to consider, $(\mathbb{1}, 0)$ and $(|p\rangle\langle p|, |p^\perp\rangle\langle p^\perp|)$. The case $(0, \mathbb{1})$ is clearly equivalent to $(\mathbb{1}, 0)$. Since we need to consider only instruments of Bob corresponding to rank-1 CJ operators $\mathfrak{B}_b^y = |\beta_b^y\rangle\langle\beta_b^y|$, the latter can be taken of the form

$$|\beta_0^y\rangle = |0\rangle \otimes |q^y\rangle + |1\rangle \otimes |q^{y\perp}\rangle, \quad |\beta_1^y\rangle = 0, \quad (\text{C1})$$

for POVM $(\mathbb{1}, 0)$. In the main text of the paper we refer to this strategy as “unitary” because the Kraus operator for this instrument is a unitary. Another possibility for $\mathfrak{B}_b^y = |\beta_b^y\rangle\langle\beta_b^y|$ is the following:

$$|\beta_0^y\rangle = |p^y\rangle \otimes |q_0^y\rangle, \quad |\beta_1^y\rangle = |p^{y\perp}\rangle \otimes |q_1^y\rangle, \quad (\text{C2})$$

which corresponds to POVM $(|p^y\rangle\langle p^y|, |p^{y\perp}\rangle\langle p^{y\perp}|)$. We refer to this strategy as “measure and prepare.” In both cases all the vectors $|p^y\rangle, |q^y\rangle, |q_b^y\rangle, y = 0, 1, b = 0, 1$ are normalized. It is important to note that in Eq. (C1) the relative phase between $|q^y\rangle$ and $|q^{y\perp}\rangle$ should be taken into account.

Due to the same requirement on the rank of \mathfrak{B}_b^y we can directly see that the probabilistic strategies in which Bob applies, let us say, the operation from Eq. (C1) with some probability and the strategy from Eq. (C2) in all other cases will necessarily be less optimal than one of these strategies chosen with probability 1. It means that in order to analyze the bounds on the average success probability for strategies of Bob that correspond to projective measurements and their probabilistic mixtures it is sufficient to compute the bounds for the extreme projective strategies. Thus, we need to analyze the following three cases: (a) Bob applies a unitary strategy for $y = 0, 1$, (b) Bob applies a measure-and-prepare strategy for all $y = 0, 1$, and (c) Bob applies a unitary strategy for $y = 0$ and a measure-and-prepare strategy for $y = 1$. In the main part of the text we refer to the last case as a “mixed” strategy. It is also clear that strategies, equivalent to the ones listed, e.g., the unitary strategy with the outcome b flipped, or the mixed strategy with y flipped, will give the same bounds. In what follows we analyze in detail all three cases (a), (b), and (c). When combined, it gives the proof of Proposition 1.

1. Unitary strategy

As mentioned above, the instrument from Eq. (C1) has a single Kraus operator that is a unitary. Let us denote it as $U_y = |0\rangle\langle q^y| + |1\rangle\langle q^{y\perp}|$, $y = 0, 1$. Let us now write the expression for average success probability in terms of U_y :

$$\bar{P}_{\text{succ}} = \frac{\alpha}{8} \sum_{\bar{x}, y} \delta_{x_y, 0} + \frac{1-\alpha}{16} \sum_{\bar{x}, y, z} \text{tr}(U_y \varrho_{\bar{x}} U_y^\dagger C_{x_z}^z). \quad (\text{C3})$$

It is clear that the first sum is equal to 4. The second sum can be upper-bounded by $2 \max_y (\sum_{\bar{x}, z} \text{tr}(U_y \varrho_{\bar{x}} U_y^\dagger C_{x_z}^z))$ and for the maximal y we can introduce new $\tilde{C}_c^z = U_y^\dagger C_c^z U_y$. Maximization over \tilde{C}_c^z and $\varrho_{\bar{x}}$ is a standard optimization problem for $2 \rightarrow 1$ QRAC, and thus the upper bound on \bar{P}_{succ} in this case is $\frac{\alpha}{2} + (1-\alpha)(\frac{1}{2} + \frac{1}{2\sqrt{2}})$.

2. Measure-and-prepare strategy

In the proof we use two main facts regarding the optimality of certain relations between states and measurements. The first one concerns maximization of expectation values $\text{tr}(\varrho(a|\psi\rangle\langle\psi| + b|\phi\rangle\langle\phi|))$ over states $\varrho \in \mathcal{L}(\mathcal{H})$, for some $a, b \in \mathbb{R}$, and $|\psi\rangle, |\phi\rangle$ being normalized vectors in \mathcal{H} , $\dim(\mathcal{H}) = 2$. The maximum is obtained when $\varrho = |\xi\rangle\langle\xi|$ with $|\xi\rangle$ being a normalized eigenvector of $a|\psi\rangle\langle\psi| + b|\phi\rangle\langle\phi|$ corresponding to its maximal eigenvalue. When there are no further constraints on ϱ , the maximum can always be attained and the following formula gives its explicit form:

$$\begin{aligned} & \|a|\psi\rangle\langle\psi| + b|\phi\rangle\langle\phi|\| \\ &= \frac{a+b}{2} + \frac{1}{2} \sqrt{(a-b)^2 + 4ab|\langle\psi|\phi\rangle|^2}, \end{aligned} \quad (\text{C4})$$

where we used the notation $\|\cdot\|$ for the operator norm (operator’s maximal eigenvalue).

The second fact concerns optimization of expressions of type $\text{tr}(A(|\psi\rangle\langle\psi| - |\phi\rangle\langle\phi|))$ over $|\psi\rangle$ and $|\phi\rangle$, with both being normalized vectors in \mathcal{H} , with $\dim(\mathcal{H}) = 2$ and where $A \in \mathcal{L}(\mathcal{H})$ is some linear, not necessarily positive, operator. It can be seen that for optimal $|\psi\rangle$ and $|\phi\rangle$ necessarily $\langle\psi|\phi\rangle = 0$. To see that, let us write the spectral decomposition of the operator $|\psi\rangle\langle\psi| - |\phi\rangle\langle\phi| = \lambda|\xi\rangle\langle\xi| - \lambda|\xi^\perp\rangle\langle\xi^\perp|$, with $\langle\xi|\xi^\perp\rangle = 0$, and $\lambda \in [-1, 1]$. Then, $\max_{|\psi\rangle, |\phi\rangle} (\text{tr}(A(|\psi\rangle\langle\psi| - |\phi\rangle\langle\phi|))) = \max_{|\xi\rangle} (\max_{\lambda} (\lambda \text{tr}(A(|\xi\rangle\langle\xi| - |\xi^\perp\rangle\langle\xi^\perp|))))$. Clearly, the maximum over λ is attained at the boundary, i.e., for $\lambda \in \{1, -1\}$. It is also clear that for $\lambda = -1$, a simple relabeling $\xi^\perp \leftrightarrow \xi$ gives the same expression as for $\lambda = 1$. Without loss of generality we can take $|\psi\rangle = |\xi\rangle$ and $|\phi\rangle = |\xi^\perp\rangle$, which proves our claim.

Let us now proceed to the actual derivation of the bound. We remind ourselves that the CJ operators of the instruments of Bob have the following form [Eq. (C2)]:

$$|\beta_0^y\rangle = |p^y\rangle \otimes |q_0^y\rangle, \quad |\beta_1^y\rangle = |p^{y\perp}\rangle \otimes |q_1^y\rangle, \quad y = 0, 1. \quad (\text{C5})$$

After removing dependency due to POVM normalization, we can rewrite the average success probability as follows:

$$\begin{aligned} \bar{P}_{\text{succ}} &= \frac{1}{2} + \frac{\alpha}{8} (r_0^0 + r_1^0 + r_0^1 - r_1^1) \\ &+ \frac{1-\alpha}{16} ((r_0^0 + r_1^0) \text{tr}(|q_0^0\rangle\langle q_0^0| - |q_1^0\rangle\langle q_1^0|) C_0^0) \\ &+ (r_0^0 - r_1^0) \text{tr}(|q_0^0\rangle\langle q_0^0| - |q_1^0\rangle\langle q_1^0|) C_1^0) \\ &+ (r_0^1 + r_1^1) \text{tr}(|q_0^1\rangle\langle q_0^1| - |q_1^1\rangle\langle q_1^1|) C_0^0) \\ &+ (r_0^1 - r_1^1) \text{tr}(|q_0^1\rangle\langle q_0^1| - |q_1^1\rangle\langle q_1^1|) C_1^0), \end{aligned} \quad (\text{C6})$$

where $r_0^y = \langle p^y | \varrho_{00}^T - \varrho_{11}^T | p^y \rangle$ and $r_1^y = \langle p^y | \varrho_{01}^T - \varrho_{10}^T | p^y \rangle$. Now we can use the fact that the optimal states $\varrho_{\bar{x}}$ are pure. Here we take $\varrho_{\bar{x}}^T = |\psi_{\bar{x}}\rangle\langle\psi_{\bar{x}}|$ and, from what we have discussed in the beginning of this section, we can assume $\langle\psi_{00}|\psi_{11}\rangle = \langle\psi_{01}|\psi_{10}\rangle = \langle q_0^0|q_1^0\rangle = \langle q_0^1|q_1^1\rangle = 0$. This creates some redundancy in Eq. (C6), which can be removed. As a result one obtains the following expression for the optimal \bar{P}_{succ} :

$$\begin{aligned} \bar{P}_{\text{succ}} &= \frac{3}{4} - \frac{\alpha}{2} + \frac{2\alpha-1}{4} (|\langle p^0|\psi_{00}\rangle|^2 + |\langle p^1|\psi_{00}\rangle|^2) \\ &+ \frac{\alpha}{4} (|\langle p^0|\psi_{01}\rangle|^2 - |\langle p^1|\psi_{01}\rangle|^2) \end{aligned}$$

$$\begin{aligned}
& + \frac{1-\alpha}{4} \sum_{y=0}^1 \langle q_0^y | (|c_0^0\rangle\langle c_0^0| (|\langle p^y | \psi_{00} \rangle|^2 + |\langle p^y | \psi_{01} \rangle|^2 \\
& - 1) + |c_0^1\rangle\langle c_0^1| (|\langle p^y | \psi_{00} \rangle|^2 - |\langle p^y | \psi_{01} \rangle|^2)) | q_0^y \rangle, \quad (C7)
\end{aligned}$$

$$\begin{aligned}
\bar{P}_{\text{succ}} &= \frac{2-\alpha}{4} + \frac{\alpha}{4} \sum_{y=0}^1 (|\langle p^y | \psi_{00} \rangle|^2 + (-1)^y |\langle p^y | \psi_{01} \rangle|^2) \\
& + \frac{1-\alpha}{8} \sum_{y=0}^1 \sqrt{(1 - 2|\langle p^y | \psi_{01} \rangle|^2)^2 + 4(|\langle p^y | \psi_{00} \rangle|^2 - |\langle p^y | \psi_{01} \rangle|^2)(|\langle p^y | \psi_{00} \rangle|^2 + |\langle p^y | \psi_{01} \rangle|^2 - 1)} |c_0^0\rangle\langle c_0^1|^2}. \quad (C8)
\end{aligned}$$

Each of the square roots are monotonic functions of $|\langle c_0^0 | c_0^1 \rangle|^2$ and their domain is $[0,1]$, if all possible values of $|\langle p^y | \xi_i \rangle|$ are considered. Depending on the signs of $(|\langle p^y | \psi_{00} \rangle|^2 - |\langle p^y | \psi_{01} \rangle|^2)(|\langle p^y | \psi_{00} \rangle|^2 + |\langle p^y | \psi_{01} \rangle|^2 - 1)$ the bounds on each square root will be obtained for $|\langle c_0^0 | c_0^1 \rangle| = 0$ or $|\langle c_0^0 | c_0^1 \rangle| = 1$. One can expect that this is not the case for the sum of the square roots, i.e., the total \bar{P}_{succ} . However, one can upper-bound the maximum of sums of the square roots by the sum of the maxima. Thus, we need to consider two cases of $|\langle c_0^0 | c_0^1 \rangle| = 0, 1$ for each of the square roots, i.e., four cases in total. By doing so we obtain the following:

$$\begin{aligned}
\bar{P}_{\text{succ}} &\leq \frac{1}{4} \max(1 + |\langle p^0 | \psi_{00} \rangle|^2 + \alpha |\langle p^0 | \psi_{01} \rangle|^2 + |\langle p^1 | \psi_{00} \rangle|^2 \\
& - \alpha |\langle p^1 | \psi_{01} \rangle|^2, 2 - \alpha + |\langle p^0 | \psi_{00} \rangle|^2 + \alpha |\langle p^0 | \psi_{01} \rangle|^2 \\
& + \alpha |\langle p^1 | \psi_{00} \rangle|^2 - |\langle p^1 | \psi_{01} \rangle|^2), \quad (C9)
\end{aligned}$$

$$\begin{aligned}
& 1 + \alpha |\langle p^0 | \psi_{00} \rangle|^2 + |\langle p^0 | \psi_{01} \rangle|^2 + |\langle p^1 | \psi_{00} \rangle|^2 - \alpha |\langle p^1 | \psi_{01} \rangle|^2, \\
& 2 - \alpha + \alpha |\langle p^0 | \psi_{00} \rangle|^2 + |\langle p^0 | \psi_{01} \rangle|^2 + \alpha |\langle p^1 | \psi_{00} \rangle|^2 \\
& - |\langle p^1 | \psi_{01} \rangle|^2). \quad (C10)
\end{aligned}$$

For each of the four cases we can group the terms with respect to $|p^y\rangle$ and upper-bound each of these inner products by the norms of the respective operators that are expressions of $|\psi_{00}\rangle\langle\psi_{00}|$ and $|\psi_{01}\rangle\langle\psi_{01}|$ with coefficients depending on α . It is interesting that in each of these four cases the final upper bound is $1/2 + \sqrt{1 + \alpha^2}/4$, which completes the proof.

3. Mixed strategy

In this proof we use similar techniques as in the previous case of the measure-and-prepare strategy. In particular, we use the formula from Eq. (C4) and, whenever our success probability will be written as an affine function of operators of the form $|\psi\rangle\langle\psi| - |\phi\rangle\langle\phi|$, we assume $\langle\psi|\phi\rangle = 0$.

For the mixed strategy of Bob the formula for the average success probability takes the following form:

$$\begin{aligned}
\bar{P}_{\text{succ}} &= \frac{\alpha}{8} \sum_{\bar{x}} (\delta_{0,x_0}) + \frac{\alpha}{4} (\text{tr}((\varrho_{00}^T + \varrho_{10}^T) |p^1\rangle\langle p^1|) \\
& + \text{tr}((\varrho_{01}^T + \varrho_{11}^T) |p^{1\perp}\rangle\langle p^{1\perp}|))
\end{aligned}$$

where we have grouped the terms with respect to $|q_0^y\rangle$. We have also used the fact that extremal effects C_0^z in this case are necessarily rank 1 and introduced the notation $C_0^z = |c_0^z\rangle\langle c_0^z|$. Applying Eq. (C4) to Eq. (C7) for the expression enclosed in $|q_0^y\rangle$ we obtain the following:

$$\begin{aligned}
& + \frac{1-\alpha}{16} \sum_{\bar{x},z} \text{tr}(U_0 \varrho_{\bar{x}} U_0^\dagger C_{x_z}^z) \\
& + \frac{1-\alpha}{16} \sum_{\bar{x},z} (\text{tr}(\varrho_{\bar{x}}^T |p^1\rangle\langle p^1|) \text{tr}(|q_0^1\rangle\langle q_0^1| C_{x_z}^z) \\
& + \text{tr}(\varrho_{\bar{x}}^T |p^{1\perp}\rangle\langle p^{1\perp}|) \text{tr}(|q_1^1\rangle\langle q_1^1| C_{x_z}^z)), \quad (C11)
\end{aligned}$$

where we have introduced the notation $U_0 = |0\rangle\langle q^0| + |1\rangle\langle q^{0\perp}|$. Since we optimize the expression in Eq. (C13) over C_c^z and $|q_b^1\rangle\langle q_b^1|$ and we have no restrictions on the basis in which we consider these operators, we can apply U_0^\dagger to the basis of C_c^z and U_0 to the basis of $|q_b^1\rangle\langle q_b^1|$. Clearly, this will not change the optimal value for \bar{P}_{succ} , but it removes this unitary from the expression in Eq. (C13). We again use normalization of all POVMs in Eq. (C13) to simplify it, which gives the following expression:

$$\begin{aligned}
\bar{P}_{\text{succ}} &= \frac{1}{2} + \frac{\alpha}{8} \langle p^1 | (r_0 - r_1) | p^1 \rangle + \frac{1-\alpha}{16} (|c_0^0\rangle\langle r_0 + r_1 | c_0^0 \rangle \\
& + \langle c_0^1 | (r_0 - r_1) | c_0^1 \rangle + \langle p^1 | (r_0 + r_1) | p^1 \rangle \langle c_0^0 | (|q_0^1\rangle\langle q_0^1| \\
& - |q_1^1\rangle\langle q_1^1|) | c_0^0 \rangle + \langle p^1 | (r_0 - r_1) | p^1 \rangle \langle c_0^0 | (|q_0^1\rangle\langle q_0^1| \\
& - |q_1^1\rangle\langle q_1^1|) | c_0^1 \rangle), \quad (C12)
\end{aligned}$$

where we used the fact that the optimal $C_0^z = |c_0^z\rangle\langle c_0^z|$ is rank 1 and used a slightly different notation for r_0, r_1 , which are in this case $r_0 = |\psi_{00}\rangle\langle\psi_{00}| - |\psi_{11}\rangle\langle\psi_{11}|$, $r_1 = |\psi_{01}\rangle\langle\psi_{01}| - |\psi_{10}\rangle\langle\psi_{10}|$, with $\varrho_{\bar{x}}^T = |\psi_{\bar{x}}\rangle\langle\psi_{\bar{x}}|$ as before. Now we can make use of the orthogonality relations $\langle\psi_{00}|\psi_{11}\rangle = \langle\psi_{01}|\psi_{10}\rangle = \langle q_0^1|q_1^1\rangle = 0$ to obtain the following:

$$\begin{aligned}
\bar{P}_{\text{succ}} &= \frac{2-\alpha}{4} + \frac{2\alpha-1}{4} |\langle p^1 | \psi_{00} \rangle|^2 + \frac{\alpha}{4} |\langle p^1 | \psi_{10} \rangle|^2 \\
& + \frac{1-\alpha}{8} (|\langle c_0^0 | \psi_{00} \rangle|^2 - |\langle c_0^0 | \psi_{10} \rangle|^2 + |\langle c_0^1 | \psi_{00} \rangle|^2 \\
& + |\langle c_0^1 | \psi_{10} \rangle|^2) + \frac{1-\alpha}{4} (|\langle q_0^1 | c_0^0 \rangle|^2 (|\langle p^1 | \psi_{00} \rangle|^2 \\
& - |\langle p^1 | \psi_{10} \rangle|^2) + |\langle q_0^1 | c_0^1 \rangle|^2 (|\langle p^1 | \psi_{00} \rangle|^2 \\
& + |\langle p^1 | \psi_{10} \rangle|^2 - 1)). \quad (C13)
\end{aligned}$$

From this, it was not obvious how to proceed with the proof, so we tried to maximize the expression in Eq. (C16) nu-

merically. We used a simple parametrization of each vector with two real parameters and performed an unconstrained heuristic optimization over 12 real parameters with gradient method for each value of α . From this numerical optimization we could infer that the maximum of \bar{P}_{succ} is obtained when $|\langle q_0^1 | c_0^0 \rangle| = 1/2$ and $|\langle q_0^1 | c_0^1 \rangle| = 1$. We prove the validity of these observations later, but for now we assume them true and finish the calculations.

Taking $|\langle q_0^1 | c_0^0 \rangle| = 1/2$ and $|\langle q_0^1 | c_0^1 \rangle| = 1$ reduces Eq. (C16) to the following form:

$$\begin{aligned} \bar{P}_{\text{succ}} = & \frac{1}{4} + \frac{1+\alpha}{8} \langle p^1 | (|\psi_{00}\rangle\langle\psi_{00}| + |\psi_{10}\rangle\langle\psi_{10}|) | p^1 \rangle \\ & + \frac{1-\alpha}{8} \langle c_0^1 | (|\psi_{00}\rangle\langle\psi_{00}| + |\psi_{10}\rangle\langle\psi_{10}|) | c_0^1 \rangle \\ & + \frac{1-\alpha}{8} \langle c_0^0 | (|\psi_{00}\rangle\langle\psi_{00}| - |\psi_{10}\rangle\langle\psi_{10}|) | c_0^0 \rangle. \end{aligned} \quad (\text{C14})$$

Now we can put an upper bound on the expression in Eq. (C18) by substituting all expectation values of operators $|\psi_{00}\rangle\langle\psi_{00}| \pm |\psi_{10}\rangle\langle\psi_{10}|$ by their norms. Using Eq. (C4) we write \bar{P}_{succ} as a function of $|\langle\psi_{00}|\psi_{10}\rangle|$, which is $\bar{P}_{\text{succ}} = \frac{1}{2} + \frac{|\langle\psi_{00}|\psi_{10}\rangle|}{4} + \frac{1-\alpha}{8} \sqrt{1 - |\langle\psi_{00}|\psi_{10}\rangle|^2}$. Finally, optimization over $|\langle\psi_{00}|\psi_{10}\rangle|$ gives the result stated in the proposition, i.e., $\bar{P}_{\text{succ}} \leq \frac{1}{2} + \frac{\sqrt{4+(1-\alpha)^2}}{8}$.

Now, let us verify the assumptions $|\langle q_0^1 | c_0^0 \rangle| = 1/2$ and $|\langle q_0^1 | c_0^1 \rangle| = 1$. In order to do so, let us write all the states in Eq. (C16) in Bloch vector form. Since no basis is fixed, we can always assume $|\psi_{00}\rangle\langle\psi_{00}| = (\mathbb{1} + \sigma_z)/2$. We can also assume, without loss of generality, that $|\psi_{10}\rangle\langle\psi_{10}| = (\mathbb{1} + x_1\sigma_x + z_1\sigma_z)/2$, i.e., that $|\psi_{10}\rangle\langle\psi_{10}|$ lies in the x - z plane of the Bloch ball. The normalization condition for x_1, z_1 reads $x_1^2 + z_1^2 = 1$. For the rest of the states, in general, we will have all x, y, z components. Let us take $|p^1\rangle\langle p^1| = (\mathbb{1} + x_2\sigma_x + y_2\sigma_y + z_2\sigma_z)/2$, $|q_0^1\rangle\langle q_0^1| = (\mathbb{1} + x_3\sigma_x + y_3\sigma_y + z_3\sigma_z)/2$, $|c_0^0\rangle\langle c_0^0| = (\mathbb{1} + x_4\sigma_x + y_4\sigma_y + z_4\sigma_z)/2$, and $|c_0^1\rangle\langle c_0^1| = (\mathbb{1} + x_5\sigma_x + y_5\sigma_y + z_5\sigma_z)/2$. The normalization condition states that $x_i^2 + y_i^2 + z_i^2 = 1$, for all $i = 2, 3, 4, 5$. Inserting this form of states to Eq. (C16) gives the following expression:

$$\begin{aligned} \bar{P}_{\text{succ}} = & \frac{1}{2} + \frac{\alpha}{8} (z_2 + x_1x_2 + z_1z_2) + \frac{1-\alpha}{16} (z_4 + z_5 + x_1x_5 \\ & + z_1z_5 - x_1x_4 - z_1z_4) + \frac{1-\alpha}{16} z_2(x_3x_4 + y_3y_4 + z_3z_4 \\ & + x_3x_5 + y_3y_5 + z_3z_5) - \frac{1-\alpha}{16} (x_1x_2 + z_1z_2)(x_3x_4 \\ & + y_3y_4 + z_3z_4 - x_3x_5 - y_3y_5 - z_3z_5). \end{aligned} \quad (\text{C15})$$

We can show now that for solution maximizing the expression above we have necessarily $y_2 = y_3 = y_4 = y_5 = 0$. In order to

do so, let us consider the optimization problem

$$\begin{aligned} \max \quad & z_4 + z_5 + x_1x_5 + z_1z_5 - x_1x_4 - z_1z_4 \\ \text{such that} \quad & x_3^2 + y_3^2 + z_3^2 = 1, \\ & x_4^2 + y_4^2 + z_4^2 = 1, \\ & x_5^2 + y_5^2 + z_5^2 = 1, \\ & x_4x_3 + y_4y_3 + z_4z_3 = v_1, \\ & x_5x_3 + y_5y_3 + z_5z_3 = v_2, \end{aligned} \quad (\text{C16})$$

where maximization is carried over vectors (x_3, y_3, z_3) , (x_4, y_4, z_4) , and (x_5, y_5, z_5) . For the fixed vectors $(x_1, 0, z_1)$, (x_2, y_2, z_2) and the inner products $v_1, v_2 \in [-1, 1]$, this optimization problem is equivalent to the original maximization of the expression in Eq. (C20). Let us now construct a Lagrangian of the problem in Eq. (C16),

$$\begin{aligned} \mathcal{L} = & z_4 + z_5 + x_1x_5 + z_1z_5 - x_1x_4 - z_1z_4 \\ & + \sum_{i=1}^3 \lambda_i (x_i^2 + y_i^2 + z_i^2 - 1) \\ & + \lambda_4 (x_4x_3 + y_4y_3 + z_4z_3 - v_1) \\ & + \lambda_5 (x_5x_3 + y_5y_3 + z_5z_3 - v_2), \end{aligned} \quad (\text{C17})$$

where $\lambda_i, i \in \{1, \dots, 5\}$ are the Lagrange multipliers. The system of equations for stationary points of Eq. (C17) contains, among others, the following three systems of linear equations:

$$\begin{pmatrix} 2\lambda_1 & \lambda_4 & \lambda_5 \\ \lambda_4 & 2\lambda_2 & 0 \\ \lambda_5 & 0 & 2\lambda_3 \end{pmatrix} \begin{pmatrix} y_3 \\ y_4 \\ y_5 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}, \quad (\text{C18})$$

$$\begin{pmatrix} 2\lambda_1 & \lambda_4 & \lambda_5 \\ \lambda_4 & 2\lambda_2 & 0 \\ \lambda_5 & 0 & 2\lambda_3 \end{pmatrix} \begin{pmatrix} x_3 \\ x_4 \\ x_5 \end{pmatrix} = \begin{pmatrix} 0 \\ x_1 \\ -x_1 \end{pmatrix}, \quad (\text{C19})$$

$$\begin{pmatrix} 2\lambda_1 & \lambda_4 & \lambda_5 \\ \lambda_4 & 2\lambda_2 & 0 \\ \lambda_5 & 0 & 2\lambda_3 \end{pmatrix} \begin{pmatrix} z_3 \\ z_4 \\ z_5 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 + z_1 \\ 1 - z_1 \end{pmatrix}. \quad (\text{C20})$$

We can immediately notice that the first system in Eq. (C18) has nontrivial solutions if and only if the determinant of the system's matrix is zero. However, if this is the case, and $x_1 \neq 0, z_1 \neq \pm 1$, the second systems have no solutions. Since we know that the optimal solution to the problem in Eq. (C16) has to be among the stationary points, we can conclude that necessarily $y_3 = y_4 = y_5 = 0$. Now we just need to check the exceptions, which are the cases when $x_1 \neq 0, z_1 \neq \pm 1$. It is easy to see that in these cases the objective function becomes either $2z_4$ or $2z_5$, i.e., the maximum attained in the problem in Eq. (C16) is at most 2. However, we know from our numerical solution that the optimal value of the expression $z_4 + z_5 + x_1x_5 + z_1z_5 - x_1x_4 - z_1z_4$ is greater than 2 for all $\alpha < 1$.

Proving the optimality of $y_2 = 0$ is even easier. We can simply remove it from consideration by substituting the constraint $x_2^2 + y_2^2 + z_2^2 = 1$ with $x_2^2 + z_2^2 \leq 1$. Since the expression in Eq. (C20), which we need to maximize, is linear in x_2 and z_2 , it means that the maximum is attained at the boundary

of the subspace of x_2 and z_2 , i.e., when $x_2^2 + z_2^2 = 1$. This means in practice that $y_2 = 0$.

We can now apply the SDP relaxation of Lasserre to the polynomial optimization problems [45]. We considered the second level of the Lasserre hierarchy in which case the size of the moment matrix Γ is 66 and the number of variables in the dual SDP is exactly 1000. An important note, which might be of interest to those who would like to reproduce the result or solve a similar problem, is that in the optimization it was crucial to add the normalization constraints of the type $\Gamma(x_i, x_i x_j) + \Gamma(z_i, z_i x_j) = \Gamma(1, x_j)$ and $\Gamma(x_i, x_i z_j) + \Gamma(z_i, z_i z_j) = \Gamma(1, z_j)$, $i, j \in \{1, \dots, 5\}$ to the obvious constraints $\Gamma(x_i, x_i) + \Gamma(z_i, z_i) = 1$, $i \in \{1, \dots, 5\}$. If the former are not included in the SDP, the objective function in Eq. (C20) turns out to be unbounded.

By performing the above SDP optimization we were able to confirm the optimality of the conditions $|\langle q_0^1 | c_0^0 \rangle| = 1/2$ and $|\langle q_0^1 | c_0^1 \rangle| = 1$ up to numerical precision of 10^{-10} as well as reproduce the value of $1/2 + \sqrt{4 + (1 - \alpha)^2}/8$ of the bound up to the same precision. This completes our proof.

APPENDIX D: ROBUSTNESS OF SELF-TESTING

In this Appendix we give more details concerning the robustness of our SDI characterization of unsharp measurements. The question that we would need to answer is the following: Given the experimentally obtained value of the average success probability for some α , $\bar{P}_{\text{succ}}^{\text{exp}} \leq \bar{P}_{\text{succ}}^{\text{POVM}}(\alpha)$, what can we say about the unsharpness parameter of the implemented measurements? Here we again discuss the case of trace-1 POVMs of Bob. In order to answer the posed question we first try to answer the opposite question: Given the eigenvalues of the POVMs of Bob, what is the maximal average success probability that can be obtained?

We start by fixing the CJ operator of the first element of Bob's instrument to be

$$|\beta_0^0\rangle = \sqrt{\lambda_0}|00\rangle + \sqrt{1 - \lambda_0}|11\rangle, \quad (\text{D1})$$

where now λ_0 is the operator norm of the effects of the first POVM (its largest eigenvalue). We can then apply the seesaw method of Ref. [46] in order to establish the optimal form of other instruments of Bob and measurements of Charlie. From these numerical results we infer that we can make the following assumptions:

$$\begin{aligned} C_0^0 &= |0\rangle\langle 0|, & C_1^0 &= |1\rangle\langle 1|, & C_0^1 &= |+\rangle\langle +|, & C_1^1 &= |-\rangle\langle -|, \\ |\beta_1^0\rangle &= \sqrt{1 - \lambda_0}|00\rangle + \sqrt{\lambda_0}|11\rangle, \\ |\beta_0^1\rangle &= \sqrt{\lambda_1}|++\rangle + \sqrt{1 - \lambda_1}|--\rangle, \\ |\beta_1^1\rangle &= \sqrt{1 - \lambda_1}|++\rangle + \sqrt{\lambda_1}|--\rangle, \end{aligned} \quad (\text{D2})$$

where now λ_1 can be different from λ_0 . We confirm later that these choices of Charlie's measurements and Bob's instruments are indeed optimal, but for now we assume that it is true and continue with the derivations of the bound.

Using Eq. (D2) we can obtain the bound on the average success probability for given λ_0 and λ_1 . The states $\varrho_{\bar{x}}$ can be chosen to be the eigenstates of the respective operators corresponding to the operators' maximal eigenvalues, as it is often done in such proofs. We get the following:

$$\begin{aligned} \bar{P}_{\text{succ}}(\lambda_0, \lambda_1) &= \frac{1}{2} + \frac{1}{4} \sqrt{\frac{(1 - 3\alpha)^2}{2} + F(\lambda_0, \lambda_1)}, \quad \text{where} \\ F(\lambda_0, \lambda_1) &= (1 - \alpha)(1 - 3\alpha)(\sqrt{\lambda_1(1 - \lambda_1)} \\ &\quad + \sqrt{\lambda_0(1 - \lambda_0)}) - (1 + \alpha)(1 - 3\alpha)(\lambda_0^2 + \lambda_1^2) \\ &\quad + 4\alpha(1 - \alpha)(\sqrt{\lambda_0(1 - \lambda_0)}\lambda_1 \\ &\quad + \lambda_0\sqrt{\lambda_1(1 - \lambda_1)}) + (1 - 5\alpha^2)(\lambda_0 + \lambda_1). \end{aligned} \quad (\text{D3})$$

If we fix λ_0 to be some value between $\frac{1}{2}$ and 1, and optimize the expression in Eq. (D4) with respect to λ_1 , we find that the optimal λ_1 is in fact the one given by Eq. (8). The same goes for the optimal λ_0 , if λ_1 is fixed. It means that, if we want to find a rectangular area in the space of (λ_0, λ_1) for which \bar{P}_{succ} from Eq. (D4) is greater than or equal to some observed value $\bar{P}_{\text{succ}}^{\text{exp}}$, we should fix one of the norms, let us say λ_0 , to be one given by Eq. (8), and solve the inequality $\bar{P}_{\text{succ}}(\lambda_0, \lambda_1) \geq \bar{P}_{\text{succ}}^{\text{exp}}$ with respect to λ_1 . Unfortunately, solution to this inequality is too unwieldy to be written explicitly, even for this Appendix. However, since it is a single-variable problem it can be solved with numerical methods up to an arbitrary precision. It is instructive to give the solution in graphical form, which we do in the main text (see Fig. 3).

Let us now discuss the optimality of the solution in Eq. (D4). We further modified the SDP techniques, described in Sec. V in the main text, in order to account for the fixed values of λ_0 and λ_1 . We consider the vectors $|\beta_b^y\rangle$ to be of the following form:

$$\begin{aligned} |\beta_0^y\rangle &= \sqrt{\lambda_y}|p^y\rangle \otimes |q_0^y\rangle + \sqrt{1 - \lambda_y}|p^{y\perp}\rangle \otimes |q_0^{y\perp}\rangle, \\ |\beta_1^y\rangle &= \sqrt{1 - \lambda_y}|p^y\rangle \otimes |q_1^y\rangle + \sqrt{\lambda_y}|p^{y\perp}\rangle \otimes |q_1^{y\perp}\rangle, \end{aligned} \quad (\text{D4})$$

which is the general form of the vectors of CJ operators of instruments corresponding to two unbiased POVMs with effects' norms λ_0 and λ_1 .

As a first modification, we add two operators $\{|p^y\rangle\langle p^y| \otimes \mathbb{1}\}_{y=0,1}$ to the set of operators \mathcal{O} , where $|p^y\rangle$ are meant to be the vectors in the Schmidt decompositions from Eq. (D6). Considering these operators allows us to add the following constraints to Eq. (9):

$$\begin{aligned} \Gamma_0^y(|p^y\rangle\langle p^y| \otimes \mathbb{1}, \mathbb{1} \otimes \mathbb{1}) &= \lambda_y, & \Gamma_1^y(|p^y\rangle\langle p^y| \otimes \mathbb{1}, \mathbb{1} \otimes \mathbb{1}) &= 1 - \lambda_y, & y &= 0, 1, \\ \Gamma_0^y(\varrho_{\bar{x}} \otimes \mathbb{1}, \mathbb{1} \otimes \mathbb{1}) &= 1 - \lambda_y + \frac{2\lambda_y - 1}{\lambda_y} \Gamma_0^y(\varrho_{\bar{x}} \otimes \mathbb{1}, |p^y\rangle\langle p^y| \otimes \mathbb{1}), & y &= 0, 1, \\ (1 - \lambda_y)\Gamma_0^y(\varrho_{\bar{x}} \otimes \mathbb{1}, |p^y\rangle\langle p^y| \otimes \mathbb{1}) &= \lambda_y \Gamma_1^y(\varrho_{\bar{x}} \otimes \mathbb{1}, |p^y\rangle\langle p^y| \otimes \mathbb{1}), & y &= 0, 1. \end{aligned} \quad (\text{D5})$$

On top of that, we set the upper bound on the success probability of Charlie, if dephasing channels with parameters $\frac{1}{2} - \sqrt{\lambda_0(1-\lambda_0)}$, $\frac{1}{2} - \sqrt{\lambda_1(1-\lambda_1)}$ are applied to the states of Alice. In particular, we enforce the following:

$$\sum_{\bar{x}, z, c, b} \delta_{x_z, c} ((-1)^c \Gamma_b^y(\varrho_{\bar{x}} \otimes \mathbb{1}, \mathbb{1} \otimes C_0^z)) + \delta_{c, 1} \Gamma_b^y(\varrho_{\bar{x}} \otimes \mathbb{1}, \mathbb{1} \otimes \mathbb{1}) \leq 4 + 2\sqrt{1 + 4\lambda_y(1-\lambda_y)}. \quad (\text{D6})$$

After adding the constraints from Eqs. (D8) and (D10) to the SDP in Eq. (9) we can compare the bounds with the predictions given in Eq. (D4). Since we know that for deriving the bounds on the norms we need to take one of λ_y , let us say λ_0 , to be of the optimal form in Eq. (8), we just need to make a comparison for each pair (α, λ_1) . What we found is that the modified SDP gives the exact bound from Eq. (8) up to the numerical precision ($\sim 10^{-10}$), whenever

$$\sum_{b=0,1} |\beta_b^y\rangle\langle\beta_b^y| = |p^y\rangle\langle p^y| \otimes (\lambda_y |q_0^y\rangle\langle q_0^y| + (1-\lambda_y) |q_1^y\rangle\langle q_1^y|) + |p^{y\perp}\rangle\langle p^{y\perp}| \otimes ((1-\lambda_y) |q_0^{y\perp}\rangle\langle q_0^{y\perp}| + \lambda_y |q_1^{y\perp}\rangle\langle q_1^{y\perp}|) + \sqrt{\lambda_y(1-\lambda_y)} (|p^y\rangle\langle p^{y\perp}| \otimes (|q_0^y\rangle\langle q_0^{y\perp}| + |q_1^y\rangle\langle q_1^{y\perp}|) + |p^{y\perp}\rangle\langle p^y| \otimes (|q_0^{y\perp}\rangle\langle q_0^y| + |q_1^{y\perp}\rangle\langle q_1^y|)). \quad (\text{D7})$$

We can now rewrite this expression taking into account the normalization conditions, which yields the following:

$$\sum_{b=0,1} |\beta_b^y\rangle\langle\beta_b^y| = \mathbb{1} \otimes \mathbb{1} - \mathbb{1} \otimes ((1-\lambda_y) |q_0^y\rangle\langle q_0^y| + \lambda_y |q_1^y\rangle\langle q_1^y|) - |p^y\rangle\langle p^y| \otimes \mathbb{1} + |p^y\rangle\langle p^y| \otimes (|q_0^y\rangle\langle q_0^y| + |q_1^y\rangle\langle q_1^y|) + \sqrt{\lambda_y(1-\lambda_y)} (|p^y\rangle\langle p^{y\perp}| \otimes (|q_0^y\rangle\langle q_0^{y\perp}| + |q_1^y\rangle\langle q_1^{y\perp}|) + |p^{y\perp}\rangle\langle p^y| \otimes (|q_0^{y\perp}\rangle\langle q_0^y| + |q_1^{y\perp}\rangle\langle q_1^y|)). \quad (\text{D8})$$

We are interested in finding the maximum of the following average success probability of Charlie:

$$\bar{P}_{\text{succ}} = \frac{1}{8} \sum_{\bar{x}, z} \text{tr} \left(\varrho_{\bar{x}}^T \otimes C_{x_z}^z \sum_{b=0,1} |\beta_b^y\rangle\langle\beta_b^y| \right). \quad (\text{D9})$$

We can easily see that $\sum_{\bar{x}, z} \text{tr}(\varrho_{\bar{x}}^T \otimes C_{x_z}^z \mathbb{1} \otimes ((1-\lambda_y) |q_0^y\rangle\langle q_0^y| + \lambda_y |q_1^y\rangle\langle q_1^y|)) = 4$. From here it follows that the resulting expression is a linear function in $|q_0^y\rangle\langle q_0^y| + |q_1^y\rangle\langle q_1^y|$ and $|q_0^{y\perp}\rangle\langle q_0^{y\perp}| + |q_1^{y\perp}\rangle\langle q_1^{y\perp}|$. Suppose now the optimal $|q_0^y\rangle \neq |q_1^y\rangle$ and one of the vectors gives a larger contribution to the value of the expression in Eq. (D15). In this case taking both vectors equal to the optimal one will give a larger value of \bar{P}_{succ} , which contradicts our assumptions. It can also happen that $|q_0^y\rangle \neq |q_1^y\rangle$ and the values of the expressions corresponding to both $|q_0^y\rangle, |q_1^y\rangle$ are equal. In that case, however, there is no difference in taking them equal or not.

Let us now consider the channel

$$|p^y\rangle\langle p^y| \otimes |q_0^y\rangle\langle q_0^y| + |p^{y\perp}\rangle\langle p^{y\perp}| \otimes |q_0^{y\perp}\rangle\langle q_0^{y\perp}| + 2\sqrt{\lambda_y(1-\lambda_y)} (|p^y\rangle\langle p^{y\perp}| \otimes |q_0^y\rangle\langle q_0^{y\perp}| + |p^{y\perp}\rangle\langle p^y| \otimes |q_0^{y\perp}\rangle\langle q_0^y|), \quad (\text{D10})$$

which is the same channel as in Eq. (D12), but with $|q_1^y\rangle = |q_0^y\rangle$. We now derive the bound for each value of y independently. Since we have a freedom of fixing bases in this case, we can set $|p^y\rangle = |q_0^y\rangle = |0\rangle$. We can then see that the channel

$\lambda_1 \leq \lambda_0$, i.e., for all λ_1 less than or equal to the optimal norm. For $\lambda_1 > \lambda_0$ we obtained a slight discrepancy in the bounds.

We believe that the optimal solution is of the form in Eq. (D2) and the proposed bound is tight. However, for the results to be rigorous, we need to estimate the “error” in the estimation of the norms due to the fact that we could not reproduce exactly the bounds with the SDP method. In order to do so, we can use the simple error estimation formula $\Delta\lambda_1 = \frac{\partial\lambda_1}{\partial\bar{P}_{\text{succ}}(\lambda_0, \lambda_1)} \Delta\bar{P}_{\text{succ}}$. We have included the estimated “errors” in Fig. 3 as crosses of the respective colors corresponding to different relative discrepancies in the observed average success probability.

As a final remark we give a proof of the bound used in Eq. (D10). First of all, we can notice that for the channel corresponding to one of the settings of Bob we can take $|q_0^y\rangle = |q_1^y\rangle$. This can be easily seen if we write down the CJ operator of the channel:

we are considering is nothing but a dephasing channel of the form $\Lambda(\varrho) = (1-p)\varrho + p\sigma_z\varrho\sigma_z$ with parameter $p = \frac{1}{2} - \sqrt{\lambda_y(1-\lambda_y)}$. We derive the bound in the following section.

Success probability of 2 → 1 QRAC under a dephasing channel

Let us consider a 2 → 1 QRAC with two parties Alice and Charlie, Alice’s preparation states being $\{\varrho_{\bar{x}}\}$ and Charlie’s measurements $\{C_c^z\}_{c=0,1}$. Let us assume that the states of Alice undergo a transformation, corresponding to a dephasing channel $\Lambda(\varrho) = (1-p)\varrho + p\sigma_z\varrho\sigma_z$ with some parameter $p \in [0, \frac{1}{2}]$. The average success probability which we would like to maximize is the following expression:

$$\bar{P}_{\text{succ}} = \frac{1}{8} \sum_{\bar{x}, z} \text{tr}(\Lambda(\varrho_{\bar{x}}) C_{x_z}^z). \quad (\text{D11})$$

We now prove that $\bar{P}_{\text{succ}} \leq \frac{1}{2} + \frac{1}{4}\sqrt{1 + (1-2p)^2}$. First, let us expand the expression in Eq. (D17) and use the normalization condition for POVMs of Charlie. We obtain the following:

$$\bar{P}_{\text{succ}} = \frac{1}{8} \text{tr}(\Lambda(\varrho_{01} + \varrho_{10} + 2\varrho_{11}) + \Lambda(\varrho_{00} - \varrho_{11})(C_0^0 + C_0^1) + \Lambda(\varrho_{01} - \varrho_{10})(C_0^0 - C_0^1)). \quad (\text{D12})$$

Now we use the argument that we made already several times in this paper, that for optimal states of Alice we have $\varrho_{01} + \varrho_{10} = \mathbb{1}$ and $\varrho_{00} + \varrho_{11} = \mathbb{1}$. This leaves us with the

following function to maximize,

$$\bar{P}_{\text{succ}} = \frac{1}{4} + \frac{1}{4} \text{tr}(\Lambda(\varrho_{00})(C_0^0 + C_0^1) + \Lambda(\varrho_{01})(C_0^0 - C_0^1)), \quad (\text{D13})$$

where we used the fact that the dephasing channel is unital. Now let us write the states and POVM effects in Bloch form introducing the following notation:

$$\begin{aligned} \varrho_{00} &= \frac{1}{2}(\mathbb{1} + x_0\sigma_x + y_0\sigma_y + z_0\sigma_z), \\ \varrho_{01} &= \frac{1}{2}(\mathbb{1} + x_1\sigma_x + y_1\sigma_y + z_1\sigma_z), \\ C_0^0 &= \frac{1}{2}(\mathbb{1} + x_2\sigma_x + y_2\sigma_y + z_2\sigma_z), \\ C_0^1 &= \frac{1}{2}(\mathbb{1} + x_3\sigma_x + y_3\sigma_y + z_3\sigma_z). \end{aligned} \quad (\text{D14})$$

It is easy to see that the action of the dephasing channel is in multiplying the variables $x_0, x_1, y_0,$ and y_1 by the factor $(1 - 2p)$. The expression for \bar{P}_{succ} in terms of the Bloch coefficients reads

$$\begin{aligned} \bar{P}_{\text{succ}} &= \frac{1}{2} + \frac{1}{8}(z_0(z_2 + z_3) + z_1(z_2 - z_3) + (1 - 2p) \\ &\quad \times (x_0(x_2 + x_3) + y_0(y_2 + y_3) + x_1(x_2 - x_3) \\ &\quad + y_1(x_2 - x_3))). \end{aligned} \quad (\text{D15})$$

Without loss of generality we can take $x_0 = y_0 = 0, z_0 = 1$. We are then left with the following optimization problem:

$$\begin{aligned} \max \quad & \frac{1}{2} + \frac{1}{8}(z_2 + z_3 + z_1(z_2 - z_3) + (1 - 2p) \\ & \quad \times (x_1(x_2 - x_3) + y_1(y_2 - y_3))) \\ \text{such that} \quad & x_i^2 + y_i^2 + z_i^2 = 1, \quad i = 1, 2, 3. \end{aligned} \quad (\text{D16})$$

This problem can be easily solved using the Lagrange multipliers method, giving the bound of $\frac{1}{2} + \frac{1}{4}\sqrt{1 + (1 - 2p)^2}$.

APPENDIX E: BIASED CASE

Here we discuss the ‘‘biased’’ case, i.e., the case when $\text{tr}(B_b^y) \neq 1, b = 0, 1, y = 0, 1$. We use (λ_0, λ_1) to denote the spectrum of the first effects of Bob’s POVMs. The second effects then have the spectrum $(1 - \lambda_0, 1 - \lambda_1)$. These, in principle, can depend on y ; however, in our case they do not.

The figure of merit can be adjusted to account for the ‘‘bias’’ and here we consider the following expression for the average success probability:

$$\begin{aligned} \bar{P}_{\text{succ}} &= \frac{\alpha}{2} \sum_{\vec{x}, y} p(\vec{x}) \text{Pr}(b = x_y | \vec{x}, y) \\ &\quad + \frac{1 - \alpha}{8} \sum_{\vec{x}, z} \text{Pr}(c = x_z | \vec{x}, z), \end{aligned} \quad (\text{E1})$$

with $p(\vec{x})$ being the probability distribution $p(00) = \gamma^2, p(01) = p(10) = \gamma(1 - \gamma), p(11) = (1 - \gamma)^2$, with $\gamma \in [0, 1]$. Notice that we do not change the distribution of \vec{x} for Charlie. The case $\gamma = \frac{1}{2}$ corresponds to the original figure of merit in Eq. (1), with which we provided the SDI characterization of the ‘‘unbiased’’ case, i.e., $\lambda_0 + \lambda_1 = 1$. For $\gamma \neq \frac{1}{2}$, however, we noticed that the optimal eigenvalues of the first effect of Bob’s POVMs do not sum to 1. We summarized our findings in Fig. 5.

Let us first discuss the values of (λ_0, λ_1) that can occur. First of all, we know that $0 \leq \lambda_i \leq 1, i = 0, 1$, since the

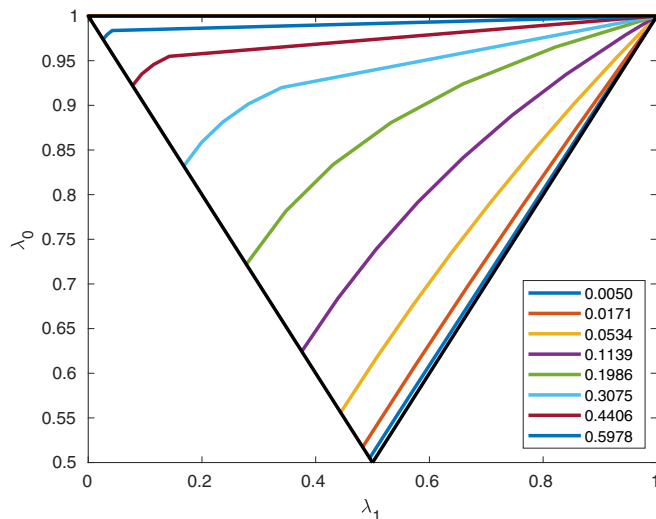


FIG. 5. Plot for various λ_0 and λ_1 . Different lines correspond to different values of α . The lines are ordered from top to bottom on the plot as α changes from 0.0050 to 0.5978.

second effects have to be positive. We can also consider the case when $\lambda_0 + \lambda_1 \geq 1$, since we have a freedom of denoting which effect is the first or the second. The corresponding region in space of (λ_0, λ_1) is a triangle, that is depicted with black lines in Fig. 5.

The edge of this triangle that connects the vertices $(0.5, 0.5)$ and $(0, 1)$ corresponds to the ‘‘unbiased’’ case of $\lambda_0 + \lambda_1 = 1$. If we wish to self-test POVMs corresponding to this line we take $\gamma = \frac{1}{2}$ and vary α between 0 and 1, as discussed in the main text. If we would like to ‘‘move’’ towards the vertex $(1, 1)$ of this triangle, we need to increase the parameter γ from $\frac{1}{2}$ to 1. In Fig. 5 we have depicted with color lines what happens with optimal values of (λ_0, λ_1) , for the given value of α , if we increase the parameter γ . These are the results of the optimization with the seesaw method of Ref. [46]. As we can see from these plots, we can cover all the area of the triangle by choosing appropriate (α, γ) . This supports our claims of the fact that all binary measurements on a qubit can be characterized in the proposed scenario. The robustness analysis of this characterization should be reported elsewhere.

APPENDIX F: COMPARISON BETWEEN SDI FRAMEWORK AND THE ONE USED IN REF. [40]

In Ref. [40] the authors discuss self-testing of unbiased binary qubit measurements in the Bell scenario. Normally, self-testing in the Bell scenario is a stronger result than the similar one in the SDI framework, because one does not assume the dimension of the underlined system. We would like to argue that, first of all, our scheme can also be adapted to the device-independent framework considered in Ref. [40]. Second, we consider the SDI framework to be much more natural for self-testing of unsharp measurements.

Below we propose a general, quite intuitive way to map SDI scenarios to the one considered in Ref. [40]. Let us say we are interested in optimizing a linear function of probabilities $p(b | \vec{x}, y) = \text{tr}(\varrho_{\vec{x}} B_b^y)$, where $\varrho_{\vec{x}} \in \mathcal{L}(\mathcal{H}), \forall \vec{x}$, are preparation states and $B_b^y \in \mathcal{L}(\mathcal{H}), \forall y, b$, are POVM effects of the

measuring party. In the SDI framework we assume that $\dim(\mathcal{H}) \leq d$, where $d \geq 2$. At this point we do not restrict the number of outcomes or the number of settings. Since we can always represent two sequential measurements as a single POVM, the following reasoning also applies to the scenario considered in the main text of this paper.

Let us now consider the same linear function as before, but now we substitute the probabilities with $p(0, b|\vec{x}, y) = \text{tr}(A_0^{\vec{x}} \otimes B_b^y \varrho_{AB})$, where $A_0^{\vec{x}}$ are the effects of POVMs of Alice corresponding to outcome zero and ϱ_{AB} is the state shared between the parties. If we can certify in a separate setup, as it is done in Ref. [40], that $\varrho_{AB} = |\Psi\rangle\langle\Psi|$ is a maximally entangled state $|\Psi\rangle = \frac{1}{\sqrt{d}} \sum_{i=1}^d |ii\rangle$ with local dimension d then $p(0, b|\vec{x}, y) = \frac{1}{d} \text{tr}((A_0^{\vec{x}})^T B_b^y)$. We can then relabel $(A_0^{\vec{x}})^T = \varrho_{\vec{x}}$ and return to the original optimization problem (up to a global factor $\frac{1}{d}$). This simple reasoning suggests that the case of maximal violation of the CHSH inequality in the scheme of Ref. [40] is equivalent to the assumption on the dimension in the SDI framework.

We would also like to argue that our scheme is the simplest and also more natural for self-testing of unsharp

measurements. Indeed, as clearly stated in the main text, unsharp measurements cannot be differentiated from their probabilistic realizations with PVMs in a simple two-party scenario, where the information about the postmeasurement states is discarded. This concerns both the prepare-and-measure scenario and the Bell-type scenario considered in Ref. [40]. We would like to argue that the SDI framework, corresponding to the prepare-and-measure scenario, is much more natural, because there is simply no way to avoid the assumption on the dimension of the Hilbert space of states that Bob sends to Charlie. If we lift this assumption, one can think about Bob and Charlie as a single party. In this case it is not possible to distinguish between two sequential binary measurements and the four-outcome POVM that one obtains by applying the Heisenberg dual of Bob's instruments to POVMs of Charlie. This assumption, although not explicitly stated, is also present in Ref. [40]. From our perspective, if one has to make the assumption on the dimension of the Hilbert space in which $\varrho_{\vec{x},b}^y$ are defined, there is no benefit in trying to relax this assumption for the states $\varrho_{\vec{x}}$ of Alice.

-
- [1] J. M. Renes, R. Blume-Kohout, A. J. Scott, and C. M. Caves, Symmetric informationally complete quantum measurements, *J. Math. Phys.* **45**, 2171 (2004).
- [2] A. Bisio, G. Chiribella, G. M. D'Ariano, S. Facchini, and P. Perinotti, Optimal Quantum Tomography of States, Measurements, and Transformations, *Phys. Rev. Lett.* **102**, 010404 (2009).
- [3] A. Chefles, Quantum state discrimination, *Contemp. Phys.* **41**, 401 (2000).
- [4] S. M. Barnett and S. Croke, Quantum state discrimination, *Adv. Opt. Photonics* **1**, 238 (2009).
- [5] A. Acín, S. Pironio, T. Vértesi, and P. Wittek, Optimal randomness certification from one entangled bit, *Phys. Rev. A* **93**, 040102(R) (2016).
- [6] P. Busch, No information without disturbance: Quantum limitations of measurement, in *Quantum Reality, Relativistic Causality, and Closing the Epistemic Circle* (Springer, Berlin, 2009), pp. 229–256.
- [7] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, *Theor. Comput. Sci.* **560**, 7 (2014).
- [8] C. A. Fuchs and A. Peres, Quantum-state disturbance versus information gain: Uncertainty relations for quantum information, *Phys. Rev. A* **53**, 2038 (1996).
- [9] C. A. Fuchs and C. A. Fuchs, Information gain vs. state disturbance in quantum theory, *Fortschr. Phys.* **46**, 535 (1998).
- [10] D. Kretschmann, D. Schlingemann, and R. F. Werner, The information-disturbance tradeoff and the continuity of Stinespring's representation, *IEEE Trans. Inf. Theory* **54**, 1708 (2008).
- [11] F. Buscemi, M. Hayashi, and M. Horodecki, Global Information Balance in Quantum Measurements, *Phys. Rev. Lett.* **100**, 210504 (2008).
- [12] Y. Aharonov, D. Z. Albert, and L. Vaidman, How the Result of a Measurement of a Component of the Spin of a Spin-1/2 Particle Can Turn Out to Be 100, *Phys. Rev. Lett.* **60**, 1351 (1988).
- [13] P. Busch, Unsharp reality and joint measurements for spin observables, *Phys. Rev. D* **33**, 2253 (1986).
- [14] P. Busch, Surprising features of unsharp quantum measurements, *Phys. Lett. A* **130**, 323 (1988).
- [15] N. W. M. Ritchie, J. G. Story, and R. G. Hulet, Realization of a Measurement of a Weak Value, *Phys. Rev. Lett.* **66**, 1107 (1991).
- [16] G. J. Pryde, J. L. O'Brien, A. G. White, T. C. Ralph, and H. M. Wiseman, Measurement of Quantum Weak Values of Photon Polarization, *Phys. Rev. Lett.* **94**, 220405 (2005).
- [17] Y. Aharonov, E. Cohen, and A. C. Elitzur, Foundations and applications of weak quantum measurements, *Phys. Rev. A* **89**, 052105 (2014).
- [18] R. Silva, N. Gisin, Y. Guryanova, and S. Popescu, Multiple Observers Can Share the Nonlocality of Half of an Entangled Pair by Using Optimal Weak Measurements, *Phys. Rev. Lett.* **114**, 250401 (2015).
- [19] 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**, 020102(R) (2017).
- [20] F. J. Curchod, M. Johansson, R. Augusiak, M. J. Hoban, P. Wittek, and A. Acín, Entangled systems are unbounded sources of nonlocal correlations and of certified random numbers, [arXiv:1802.07962](https://arxiv.org/abs/1802.07962).
- [21] D. Mayers and A. Yao, Self testing quantum apparatus, *Quantum Info. Comput.* **4**, 273 (2004).
- [22] I. Šupić and J. Bowles, Self-testing of quantum systems: A review, [arXiv:1904.10042](https://arxiv.org/abs/1904.10042).
- [23] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Proposed Experiment to Test Local Hidden-Variable Theories, *Phys. Rev. Lett.* **23**, 880 (1969).

- [24] S. L. Braunstein, A. Mann, and M. Revzen, Maximal Violation of Bell Inequalities for Mixed States, *Phys. Rev. Lett.* **68**, 3259 (1992).
- [25] S. Popescu and D. Rohrlich, Which states violate Bell's inequality maximally?, *Phys. Lett. A* **169**, 411 (1992).
- [26] A. Tavakoli, M. Smania, T. Vértesi, N. Brunner, and M. Bourennane, Self-testing non-projective quantum measurements, *Sci. Adv.* **6**, eaaw6664 (2020).
- [27] M. Pawłowski and N. Brunner, Semi-device-independent security of one-way quantum key distribution, *Phys. Rev. A* **84**, 010302(R) (2011).
- [28] T. Fritz, Quantum correlations in the temporal Clauser-Horne-Shimony-Holt (CHSH) scenario, *New J. Phys.* **12**, 083055 (2010).
- [29] J. Hoffmann, C. Spee, O. Gühne, and C. Budroni, Structure of temporal correlations of a qubit, *New J. Phys.* **20**, 102001 (2018).
- [30] C. Budroni, G. Fagundes, and M. Kleinmann, Memory cost of temporal correlations, *New J. Phys.* **21**, 093018 (2019).
- [31] P. Mironowicz and M. Pawłowski, Experimentally feasible semi-device-independent certification of four-outcome positive-operator-valued measurements, *Phys. Rev. A* **100**, 030301 (2019).
- [32] A. Tavakoli, J. Kaniewski, T. Vértesi, D. Rosset, and N. Brunner, Self-testing quantum states and measurements in the prepare-and-measure scenario, *Phys. Rev. A* **98**, 062307 (2018).
- [33] M. Farkas and J. Kaniewski, Self-testing mutually unbiased bases in the prepare-and-measure scenario, *Phys. Rev. A* **99**, 032316 (2019).
- [34] M. Ozmaniec, L. Guerini, P. Wittek, and A. Acín, Simulating Positive-Operator-Valued Measures with Projective Measurements, *Phys. Rev. Lett.* **119**, 190501 (2017).
- [35] A. Ambainis, D. Leung, L. Mancinska, and M. Ozols, Quantum random access codes with shared randomness, [arXiv:0810.2937](https://arxiv.org/abs/0810.2937).
- [36] T. Heinosaari and M. Ziman, *The Mathematical Language of Quantum Theory: From Uncertainty to Entanglement* (Cambridge University Press, 2011).
- [37] M. Navascués and T. Vértesi, Bounding the Set of Finite Dimensional Quantum Correlations, *Phys. Rev. Lett.* **115**, 020501 (2015).
- [38] M. Navascués, A. Feix, M. Araújo, and T. Vértesi, Characterizing finite-dimensional quantum behavior, *Phys. Rev. A* **92**, 042117 (2015).
- [39] A. Chaturvedi, M. Ray, R. Veynar, and M. Pawłowski, On the security of semi-device-independent QKD protocols, *Quantum Inf. Process.* **17**, 131 (2018).
- [40] S. Wagner, J.-D. Bancal, N. Sangouard, and P. Sekatski, Device-independent characterization of generalized measurements, *Quantum* **4**, 243 (2020).
- [41] K. Mohan, A. Tavakoli, and N. Brunner, Sequential random access codes and self-testing of quantum measurement instruments, *New J. Phys.* **21**, 083034 (2019).
- [42] K.-C. Toh, M. J. Todd, and R. H. Tütüncü, SDPT3: A MATLAB software package for semidefinite programming, version 1.3, *Optim. Methods Software* **11**, 545 (1999).
- [43] J. Löfberg, YALMIP: A toolbox for modeling and optimization in MATLAB, in *Proceedings of the 2004 IEEE International Conference on Robotics and Automation (IEEE Cat. No.04CH37508)* (IEEE, Piscataway, NJ, 2004), pp. 284–289.
- [44] E. Schmidt, Zur theorie der linearen und nicht linearen integralgleichungen. zweite abhandlung: Auflösung der allgemeinen linearen integralgleichung, in *Integralgleichungen und Gleichungen mit unendlich vielen Unbekannten* (Springer, Berlin, 1989), pp. 234–248.
- [45] J. B. Lasserre, Convergent SDP-relaxations in polynomial optimization with sparsity, *SIAM J. Optim.* **17**, 822 (2006).
- [46] R. F. Werner and M. M. Wolf, Bell inequalities and entanglement, *Quantum Inf. Comput.* **1**, 125 (2001).