Rapid Communications

# Experimentally feasible semi-device-independent certification of four-outcome positive-operator-valued measurements

Piotr Mironowicz[1,2,3,*] and Marcin Pawłowski[2,3]

[1]*Department of Algorithms and System Modeling, Faculty of Electronics, Telecommunications and Informatics, Gdańsk University of Technology, 80-233 Gdańsk, Poland*

[2]*Institute of Theoretical Physics and Astrophysics, National Quantum Information Centre, Faculty of Mathematics, Physics and Informatics, University of Gdańsk, Wita Stwosza 57, 80-308 Gdańsk, Poland*

[3]*International Centre for Theory of Quantum Technologies, University of Gdańsk, Wita Stwosza 57, 80-308 Gdańsk, Poland*

(Received 21 December 2018; published 6 September 2019)

Recently the quantum information science community devoted a lot of attention to the theoretical and practical aspects of generalized measurements, the formalism of all possible quantum operations leading to acquisition of classical information. On the other hand, due to imperfections present in quantum devices, and limited thrust to them, a trend of formulating quantum information tasks in a semi-device-independent manner emerged. In this Rapid Communication we use the concept of quantum random access codes to construct a protocol able to certify the presence of the generalized measurements in a semi-device-independent way without employing quantum entanglement. We use semidefinite programming methods to show robustness of the protocol and characterize its statistical properties. We conclude that it allows for experimental realizations using technology currently available in laboratories.

DOI: 10.1103/PhysRevA.100.030301

*Introduction.* Measurements lay in the heart of all physical sciences. The formalism of quantum mechanics defines them as projections on vectors in some abstract Hilbert space, yet they remain one of the most mysterious notions of modern physics.

Even though the formalism was elaborated many years ago [1], the development of quantum information science led to its significant enhancement, when so-called positive-operator-valued measure (POVM) or generalized measurements have been introduced [2–4], originating in the problem of nonorthogonal states discrimination.

The importance of POVMs stems from the fact that they formalize the most general way we can acquire information from physical systems. Their analysis improves our understanding of which quantities can be potentially measured with what accuracy and which information processing tasks can be performed, e.g., the mentioned task of state discrimination or state tomography [5,6]. The problem how generalized measurements are related to projective ones supplied with additional resources, is also closely related to fundamental issues [7,8].

A recent trend in quantum information, related to security and reliability issues, tries to formulate physical problems, protocols, and experiments in a so-called device-independent (DI) way [9], where one derives all conclusions about some phenomenon based only on the observed results, not making assumptions regarding the internal construction of the involved setup. This approach is motivated by the limited thrust that may be devoted to quantum apparatuses one uses. In (almost) all physical experiments some imperfections occur, e.g., a quantum measurement can be conducted in a slightly different way than assumed in theory. DI formulation often allows for some conclusive results, even if considered devices are not working in an entirely correct way. What is more, with the DI approach one is sometimes able to gain positive results even if employed devices are intended by a malevolent vendor to work in a misleading way, as is sometimes assumed in cryptography.

A popular relaxation of the DI approach is called semi-device-independent (SDI) [10], where some assumptions regarding devices are made. The most common assumption is a constraint on the dimension of quantum systems communicated between parts of the considered setup. The motivation is that quite often DI protocols are not suitable for practical application. This happens because they usually tolerate only small imperfections, and require scenarios involving resources that are difficult to be attained, like close to perfect quantum entanglement. It revealed that when using a relatively simple assumption the requirements for protocols are significantly lessened.

From the interest in these two topics, i.e., measurements and DI protocols, emerged a problem of SDI certification that some of the measurements performed by devices used in an experiment cannot be projective. Surprisingly, the problem was revealed to be very demanding. The first experiment certifying the presence of generalized measurements [11] was based on a scheme involving entangled quantum states. Later a similar approach was used to generate randomness from POVM outcomes [12]. Yet, the way to certify the presence of generalized measurements without entangled states is not known.

The result of this Rapid Communication is an SDI protocol using a prepare and measure scheme that is able to certify

*piotr.mironowicz@gmail.com

 

the presence of a four-outcome POVM in dimension two. The advantage of the proposed protocol in comparison to the one introduced in [11] is that no quantum entanglement is required to realize it, and thus experimental implementations are potentially easier to perform. Indeed, we show that the robustness of the protocol makes it feasible for experimental realizations.

The aim of this Rapid Communication is not only to show that a POVM was implemented in an experiment,[1] but to prove that it was genuinely four-outcome, viz., not a convex combination of measurements with less outcomes. Note, that in order to gather a probabilistic description of a black-box use of the device, one has to repeat experimental runs many times and count particular events, in a form: *For the settings* $(x, y)$ *the result* $b$ *occurred* $n_{b,x,y}$ *times*.

This way it can happen that for the measurement setting under investigation all four outcomes $b = 1, 2, 3, 4$ have been observed in some events. On the other hand, it still does not mean that a four-outcome measurement was performed in any of the runs. It could happen that, e.g., in even runs only outcomes 1 and 2, and in odd runs only outcomes 3 and 4 were (potentially) possible. Thus, we cannot *a priori* say that in some experiment a *genuine* four-outcome measurement was performed. The aim of this Rapid Communication is to circumvent this problem.

We note that the experiment reported in [11] was able to certify only a (genuine) three-outcome POVM, and certification of four outcomes would require very high visibility (above 0.993) that is more difficult to attain with quantum entanglement than in the prepare and measure scheme used in this Rapid Communication. Moreover, the latter approach is able to achieve higher generation rates, which is important from an application point of view, such as randomness generation using generalized measurements [12].

*Quantum random access codes.* The key tool we use in this Rapid Communication is so-called random access codes (RACs). They were first introduced in the field of quantum information as conjugate coding in 1983 by Wiesner [13], and then reintroduced in [14,15] (see [16] for an overview). In an $n^d \to 1$ RAC Alice is provided a uniformly distributed string of $n$ dits, $\mathbf{x} = x_1 x_2 \cdots x_n$. Her task is to encode the string into a single dit message $m(\mathbf{x})$, in such a way that Bob is able to recover any of the $n$ dits with high probability. Bob receives Alice's message $m$, and a referee provides him a uniformly distributed input $y \in [n]$, where $[n] \equiv \{1, 2, \ldots, n\}$. After this Bob performs classical (possibly probabilistic) computations of some function $b(y, m)$. We say that the protocol succeeded when $b(y, m(\mathbf{x})) = x_y$.

The quantum analogs of RACs are quantumrandom access codes (QRACs) [13,14]. In $n^d \to 1$ QRAC Alice encodes the $n$-dit input $\mathbf{x}$ into a $d$-dimensional quantum system $\rho_{\mathbf{x}}$, that is then transmitted to Bob. He afterwards performs one of his $n$ measurements (depending on the input $y$) to give his guess $b$ for $x_y$. Thus he outputs $b$ with probability given by $\mathrm{Tr}[\rho_{\mathbf{x}} M_b^y]$, where the operators $M_b^y$ are POVMs, i.e., positive and $\forall y \sum_b M_b^y = \mathbb{1}_d$, and $\mathbb{1}_d$ is the identity operator in dimension $d$. In this Rapid Communication we consider degenerated POVMs, where some of the operators are allowed to be null.

Note that Alice's only optimal strategy is to send a state $\rho_{\mathbf{x}}$ maximizing the value of $\mathrm{Tr}[\rho_{\mathbf{x}}(\sum_{y\in[n]} M_{x_y}^y)]$. This is obtained if the state is in the subspace of vectors with maximal eigenvalue of the operator $\sum_{y\in[n]} M_{x_y}^y$.

In both RACs and QRACs we consider the probability that Bob returns outcome $b$ when his input is $y$, and Alice's input is $x$. We denote this probability by $P(b|x, y)$. The average success probability for RACs and QRACs is thus given by

$$\frac{1}{nd^n} \sum_{\mathbf{x}\in[d]^n} \sum_{y\in[n]} P(x_y|\mathbf{x}, y). \tag{1}$$

*Reduction of* $3^2 \to 1$ *QRAC and its self-testing.* Now, let us focus on a $3^2 \to 1$ QRAC. In [17] it has been shown that this protocol possesses a robust self-testing property [18], meaning that there exists a unique set of optimal quantum states and measurements that maximizes it (up to some elementary transformations), and that if the experiment is close to the maximal value, then the states and measurements are close to the optimal ones. Let

$$\{\tilde{\rho}_{\mathbf{x}}\} \text{ and } \left\{\tilde{M}_b^y\right\} \tag{2}$$

be these optimal states and measurements, respectively.

To be more specific, Alice obtains here one of eight possible inputs, and prepares one of eight relevant qubits. In the perfect case of success probability

$$S_3 = \frac{1}{2}\left(1 + \frac{\sqrt{3}}{3}\right) \approx 0.788\,68, \tag{3}$$

Bob performs a measurement in one of three mutually unbiased bases in dimension 2, corresponding in this case to measuring observables given by Pauli operators $\{\sigma_x, \sigma_y, \sigma_z\}$.

From our observation regarding Alice's optimal encodings, we find the unique preparation states maximizing the success probability. One can check [16] that the Bloch sphere representations of states $\{\tilde{\rho}_{000}, \tilde{\rho}_{011}, \tilde{\rho}_{101}, \tilde{\rho}_{110}\}$ and $\{\tilde{\rho}_{111}, \tilde{\rho}_{100}, \tilde{\rho}_{010}, \tilde{\rho}_{001}\}$ are located on the edges of regular tetrahedra, with relevant edges antipodal to each other. The explicit representation of the former set of states is as follows:

$$\tilde{\rho}_{000} = \begin{bmatrix} 1-\alpha & \beta(1+i) \\ \beta(1-i) & \alpha \end{bmatrix}, \tag{4a}$$

$$\tilde{\rho}_{011} = \begin{bmatrix} \alpha & \beta(1-i) \\ \beta(1+i) & 1-\alpha \end{bmatrix}, \tag{4b}$$

$$\tilde{\rho}_{101} = \begin{bmatrix} 1-\alpha & \beta(-1+i) \\ \beta(-1-i) & \alpha \end{bmatrix}, \tag{4c}$$

$$\tilde{\rho}_{110} = \begin{bmatrix} 1-\alpha & \beta(-1-i) \\ \beta(-1+i) & \alpha \end{bmatrix}, \tag{4d}$$

where $\alpha \equiv \frac{3-\sqrt{3}}{6}$ and $\beta \equiv \frac{\sqrt{3}}{6}$.

Now, we apply the method of the so-called reduction of symmetric dimension witnesses introduced by us in [19] to show that the following expression (that is not a QRAC)

[1] This task would be trivial, as the measure of projective measurements is 0, effectively meaning that all practical measurements are POVMs.

possesses a self-testing property:

$$\frac{1}{12}\sum_{\mathbf{x}\in\{000,011,101,110\}}\sum_{y\in[3]}P(x_y|\mathbf{x},y). \tag{5}$$

Indeed, let us assume that there exists a set of measurements of Bob $\{M_b^y\}$ and states prepared by Alice $\{\rho_{\mathbf{x}}\}_{\mathbf{x}=000,011,101,110}$ optimal for (5) and different from $\{\tilde{M}_b^y\}$ and $\{\tilde{\rho}_{\mathbf{x}}\}_{\mathbf{x}=000,011,101,110}$. Without loss of generality we may assume that $\mathrm{Tr}\,M_b^y = 1$ for all $b$ and $y$ [17].

Let us now define $\rho_{111} \equiv \mathbb{1}_2 - \rho_{000}$, $\rho_{100} \equiv \mathbb{1}_2 - \rho_{011}$, $\rho_{010} \equiv \mathbb{1}_2 - \rho_{101}$, and $\rho_{001} \equiv \mathbb{1}_2 - \rho_{110}$. One can easily check that these states together with $\{M_b^y\}$ maximize the expression complementary to (5), i.e.,

$$\frac{1}{12}\sum_{\mathbf{x}\in\{111,100,010,001\}}\sum_{y\in[3]}P(x_y|\mathbf{x},y). \tag{6}$$

One can verify that the states $\{\tilde{\rho}_{\mathbf{x}}\}$ and measurements $\{\tilde{M}_b^y\}$ from (2) used for expressions (5) and (6) give for both cases success probability $S_3$, and the average of these game expressions is exactly $3^2 \to 1$ QRAC. From its self-testing property, the assumption that states $\{\rho_{\mathbf{x}}\}$ and measurements $\{M_b^y\}$ are not equal to these leads to contradiction, showing the self-testing property of both games (5) and (6).

We briefly note here that an immediate consequence of the above construction is the possibility of deriving also the robustness of the self-testing of expressions (5) and (6) directly from robustness of the $3^2 \to 1$ QRAC [17]. Indeed, consider the maximal distance $\delta_1$ of states and measurements from (2) that allows one to reach the value $S_3 - \epsilon$ by $3^2 \to 1$ QRAC, where to express the distance an arbitrary isotropic metric is used.

Let $\delta_2$ be the maximal distance from (2) that allows one to reach the value $S_3 - \epsilon$ in the reduced game (5). From isotropy of the metric we get the same maximal distance $\delta_2$ for the reduced game (6), and we see that the same measurements can be used for both of these reduced games. From this and from the fact that $3^2 \to 1$ QRAC is the average of (5) and (6) we see that $\delta_2 \leqslant \delta_1$.

*Robust POVM certification.* Let us now consider a more complicated task, where Alice and Bob are not only maximizing expression (5) (i.e., the reduced $3^2 \to 1$ QRAC), but also minimizing probability of some other events. Let us introduce an additional fourth input of Bob, related to a four-outcome measurement (with outcomes labeled 1,2,3,4). The new expression we consider is

$$\frac{1}{12}\left[\sum_{\mathbf{x}\in\{000,011,101,110\}}\sum_{y\in[3]}P(x_y|\mathbf{x},y) - kG^4\right], \tag{7}$$

where $k > 0$, and

$$G^4 \equiv P(1|000,4) + P(2|011,4) + P(3|101,4) + P(4|110,4). \tag{8}$$

One can easily see that expression (7) cannot obtain a value greater than $S_3$, and the value would be obtained only when the states $\{\tilde{\rho}_{\mathbf{x}}\}$ and measurements $\{\tilde{M}_b^y\}$ are used, and the part $G^4$ is equal to 0. From this it follows that each operator $\{M_i^4\}$ has to be orthogonal to relevant state $\{\tilde{\rho}_{000}, \tilde{\rho}_{011}, \tilde{\rho}_{101}, \tilde{\rho}_{110}\}$. Direct calculation shows that the fourth measurement is a POVM given by

$$M_1^4 = \frac{1}{2}\begin{bmatrix}\alpha & \beta(-1-i)\\ \beta(-1+i) & 1-\alpha\end{bmatrix}, \tag{9a}$$

$$M_2^4 = \frac{1}{2}\begin{bmatrix}1-\alpha & \beta(-1+i)\\ \beta(-1-i) & \alpha\end{bmatrix}, \tag{9b}$$

$$M_3^4 = \frac{1}{2}\begin{bmatrix}1-\alpha & \beta(1-i)\\ \beta(1+i) & \alpha\end{bmatrix}, \tag{9c}$$

$$M_4^4 = \frac{1}{2}\begin{bmatrix}\alpha & \beta(1+i)\\ \beta(1-i) & 1-\alpha\end{bmatrix}. \tag{9d}$$

All these considerations refer to the perfect case when the maximal value $S_3$ of expression (7) is observed. In real-world experiments this will not be the case due to experimental imperfections. Thus, to provide an experimentally feasible certificate that a measurement is a genuine four-outcome POVM, we need to establish the robustness of the certification protocol. We note here, that in order to perform a conclusive experiment one does not need to calculate full robustness properties including distances of the states and measurements to the perfect ones depending on the certificate value. For the purpose of the experiment it suffices to establish the scope of values that certifies the presence of four- or three-outcome POVM.

In order to model the experimental imperfections we use the visibility of quantum states. The visibility $\nu$ means that whenever the state prepared in the perfect situation is $\rho$, the state occurring in the experiment is modeled as $\nu\rho + \frac{1-\nu}{d}\mathbb{1}_d$. This parameter represents the impact of the proper state in comparison to the white noise. Let $N(k)$ be the value of the certificate (7) when $\nu = 1$, i.e., for all input settings the transmitted state is the white noise. We have

$$N(k) = \tfrac{1}{12}(12 \times 0.5 - k \times 4 \times 0.25). \tag{10}$$

Let $g_j(k)$ denote the maximal value of expression (7) when the fourth measurement has $j$ outcomes, $j = 2, 3, 4$. We have $g_4(k) = S_3$ for all $k \geqslant 0$. The critical visibility $\nu_j(k)$ needed to certify that $j$ ($j = 3, 4$) outcomes are necessary to reproduce

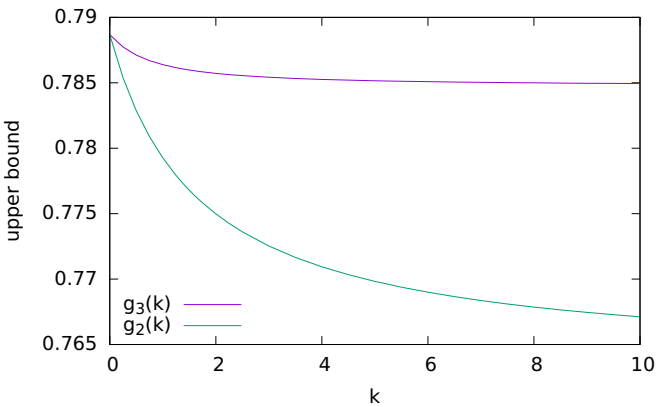


FIG. 1. The values of upper bounds $g_3(k)$ and $g_2(k)$ for the game (7) possible to be obtained with three- and two-outcome POVMs, respectively, for different values of $k$.

TABLE I. The probabilities obtained using the see-saw method for the case when fourth measurement is assumed to have only *two outcomes* with nonzero probabilities and $k = 1$. The bold values are the ones that occur in (7).

| x | $P(0\|\mathbf{x}, 1)$ | $P(1\|\mathbf{x}, 1)$ | $P(0\|\mathbf{x}, 2)$ | $P(1\|\mathbf{x}, 2)$ | $P(0\|\mathbf{x}, 3)$ | $P(1\|\mathbf{x}, 3)$ | $P(1\|\mathbf{x}, 4)$ | $P(2\|\mathbf{x}, 4)$ | $P(3\|\mathbf{x}, 4)$ | $P(4\|\mathbf{x}, 4)$ |
|---|---|---|---|---|---|---|---|---|---|---|
| 000 | **0.684** | 0.316 | **0.854** | 0.146 | **0.854** | 0.146 | **0.035** | 0.965 | 0 | 0 |
| 011 | **0.684** | 0.316 | 0.146 | **0.854** | 0.146 | **0.854** | 0.965 | **0.035** | 0 | 0 |
| 101 | 0.195 | **0.805** | **0.757** | 0.243 | 0.243 | **0.757** | 0.500 | 0.500 | **0** | 0 |
| 110 | 0.195 | **0.805** | 0.243 | **0.757** | **0.757** | 0.243 | 0.500 | 0.500 | 0 | **0** |

the experimental value is given by the expression

$$\nu_j(k) = \frac{g_{j-1}(k) - N}{S_3 - N}. \tag{11}$$

There exist a couple of methods of optimization of quantum expression with dimension constraints. One of them is the see-saw method [20], that optimizes within the interior of the quantum theory, and is able to provide explicit forms of states and measurements realizing the resulting value. The result of a maximization provides a lower bound on the proper quantum value. The see-saw optimizations have been performed using OCTAVE [21] with SDPT3 solver [22,23] and YALMIP toolbox [24]. Some other methods [19,25,26] optimize from the exterior of the quantum theory (i.e., they provide relaxations of the quantum formalism). They give upper bounds on quantum values.

The results we obtained using the second level of the Mironowicz-Li-Pawłowski (MLP) relaxation [19] for different values of $k$ for functions $g_3(k)$ and $g_2(k)$ are shown in Fig. 1. Recall that the assumed dimension constraint is two. We have $g_3(1) = 0.7864$ and $g_2(1) = 0.7793$, relating to visibilities $\nu_4(1) = 0.9938$ and $\nu_3(1) = 0.9747$, respectively. The MLP relaxation values have been calculated using the NCPOL2SPDA package [27].

The value $g_2(1)$ is derived also in the see-saw method giving lower bounds on the values of dimension constrained quantum scenarios, thus this value is exact. In the see-saw approximation of $g_3(1)$ we obtained after multiple executions with random seeds the value 0.7856, thus establishing the scope of the possible exact value. For the sake of completeness the details of the probability distribution obtained using see-saw are given in Tables I and II for $k = 1$.

Now, let $g_{\text{obs}}(k)$ be the observed value of the game (7) for some $k$, and $r$ be the ratio of runs of the experiment using genuine four-outcome POVMs. Let $g_{\text{exp}}^{(4)}$ and $g_{\text{exp}}^{(<4)}$ be the average values of the game in genuine four-outcome POVM runs, and runs with measurements with less than four possible outcomes, respectively. Obviously

$$g_{\text{obs}}(k) = r g_{\text{exp}}^{(4)} + (1-r) g_{\text{exp}}^{(<4)} \leqslant r g_4 + (1-r) g_3(k). \tag{12}$$

From this it follows that

$$r \geqslant r_0(k) \equiv \frac{g_{\text{obs}}(k) - g_3(k)}{g_4 - g_3(k)}. \tag{13}$$

Thus, if $g_{\text{obs}}(k)$ is the observed average value of expression (7) for some $k > 0$, under assumption that the dimension of the quantum system is two, then at least in the $r_0(k)$ part of runs of the experiment a genuine four-outcome POVM occurred.

Our results mean that whenever in an experiment one obtains the average value greater than $g_3(k)$ [$g_2(k)$], then a genuine four(three)-outcome POVM is certified to be used, at least in some runs of the experiment. The main conclusion of the Rapid Communication may be summarized in the following way.

*Corollary 1.* For all $k > 0$, under the assumption that qubits are sent and a three-outcome POVM is measured the quantity (7) obeys an upper bound $g_3(k)$ that can be beaten with a four-outcome POVM to the value $g_4(k) > g_3(k)$. These allow one to certify a presence of a four-outcome POVM in an experiment.

*Conclusions.* In this Rapid Communication we have presented a prepare and measure SDI protocol able to certify the occurrence of a genuine four-outcome generalized measurement in dimension two. The robustness of the protocol allows for using it in real-world experiments in laboratories [28]. The special role of four-outcome POVMs in dimension two stems from the fact that they are information complete [29].

Even though the construction of the protocol was based on the reduction of QRACs, the resulting states and measurements are closely related to the so-called elegant Bell inequality [30] (EBI), whose self-testing properties were shown recently [31]. Using the methods of [19] it is possible to convert EBI to a prepare and measure protocol and, after the reduction operation, derive the same result as those presented above.

The problem of how to certify generalized measurements in different dimensions and with arbitrary number of outcomes remains open. The above construction suggests that a possible way to tackle this issue is related to similar QRAC

TABLE II. The probabilities obtained using the see-saw method for the case when fourth measurement is assumed to have *three outcomes* with nonzero probabilities and $k = 1$. The bold values are the ones that occur in (7).

| x | $P(0\|\mathbf{x}, 1)$ | $P(1\|\mathbf{x}, 1)$ | $P(0\|\mathbf{x}, 2)$ | $P(1\|\mathbf{x}, 2)$ | $P(0\|\mathbf{x}, 3)$ | $P(1\|\mathbf{x}, 3)$ | $P(1\|\mathbf{x}, 4)$ | $P(2\|\mathbf{x}, 4)$ | $P(3\|\mathbf{x}, 4)$ | $P(4\|\mathbf{x}, 4)$ |
|---|---|---|---|---|---|---|---|---|---|---|
| 000 | **0.765** | 0.235 | **0.765** | 0.235 | **0.856** | 0.144 | **0.008** | 0.496 | 0.496 | 0 |
| 011 | **0.765** | 0.235 | 0.144 | **0.856** | 0.235 | **0.765** | 0.496 | **0.008** | 0.496 | 0 |
| 101 | 0.144 | **0.856** | **0.765** | 0.235 | 0.235 | **0.765** | 0.496 | 0.496 | **0.008** | 0 |
| 110 | 0.235 | **0.765** | 0.235 | **0.765** | **0.765** | 0.235 | 0.333 | 0.333 | 0.333 | **0** |

constructions [32,33]. This shows the benefit of using the above method in comparison to a simple conversion from an existing entangled protocol using EBI.

*Note added.* Recently, we became aware of an independent work [28] focused on self-testing of qubit POVMs.

*Acknowledgments*. This work was supported by National Science Centre (NCN) Grant No. 2014/14/E/ST2/00020, First TEAM Grant No. First TEAM/2016-1/5, and DS Programs of the Faculty of Electronics, Telecommunications and Informatics, Gdańsk University of Technology. The International Centre for Theory of Quantum Technologies project is carried out within the International Research Agendas Programme of the Foundation for Polish Science co-financed by the European Union from the funds of the Smart Growth Operational Programme, axis IV: Increasing the research potential (Measure 4.3). The authors are grateful to Professor Ryszard Horodecki, the Director of National Quantum Information Centre, where a large part of this work was created.

[1] P. Dirac, *The Principles of Quantum Mechanics* (Oxford University Press, United Kingdom, 1930).
[2] C. W. Helstrom, *Quantum Detection and Estimation Theory* (Academic, New York, 1976).
[3] I. D. Ivanovic, How to differentiate between non-orthogonal states, Phys. Lett. A **123**, 257 (1987).
[4] A. Peres, How to differentiate between non-orthogonal states, Phys. Lett. A **128**, 19 (1988).
[5] D. Petz and L. Ruppert, Optimal quantum-state tomography with known parameters, J. Phys. A: Math. Theor. **45**, 085306 (2012).
[6] H. Lyyra, T. Kuusela, and T. Heinosaari, Obtaining conclusive information from incomplete experimental tomography, Phys. Rev. A **99**, 042335 (2019).
[7] M. Oszmaniec, L. Guerini, P. Wittek, and A. Acín, Simulating Positive-Operator-Valued Measures with Projective Measurements, Phys. Rev. Lett. **119**, 190501 (2017).
[8] M. Oszmaniec, F. B. Maciejewski, and Z. Puchała, All quantum measurements can be simulated using projective measurements and postselection, Phys. Rev. A **100**, 012351 (2019).
[9] D. Mayers and A. Yao, Quantum cryptography with imperfect apparatus, IEEE Symposium on Foundations of Computer Science, 1998 (unpublished).
[10] M. Pawłowski and N. Brunner, Semi-device-independent security of one-way quantum key distribution, Phys. Rev. A **84**, 010302(R) (2011).
[11] E. S. Gómez, S. Gómez, P. Gonzalez, G. Cañas, J. F. Barra, A. Delgado, G. B. Xavier, A. Cabello, M. Kleinmann, T. Vértesi, and G. Lima, Device-Independent Certification of a Nonprojective Qubit Measurement, Phys. Rev. Lett. **117**, 260401 (2016).
[12] S. Gómez, A. Mattar, E. S. Gómez, D. Cavalcanti, O. J. Farías, A. Acín, and G. Lima, Experimental nonlocality-based randomness generation with non-projective measurements, Phys. Rev. A **97**, 040102(R) (2018).
[13] S. Wiesner, Conjugate coding, SIGACT News **15**, 78 (1983).
[14] A. Ambainis, A. Nayak, A. Ta-Shma, and U. Vazirani, Dense quantum coding and a lower bound for 1-way quantum automata, in *Proceedings of the 31st Annual ACM Symposium on Theory of Computing* (ACM Press, New York, 1999), pp. 376–383.
[15] A. Ambainis, A. Nayak, A. Ta-Shma, and U. Vazirani, Dense quantum coding and quantum finite automata, J. ACM **49**, 496 (2002).
[16] A. Ambainis, D. Leung, L. Mancinska, and M. Ozols, Quantum random access codes with shared randomness, arXiv:0810.2937.
[17] 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).
[18] A. Coladangelo, K. T. Goh, and V. Scarani, All pure bipartite entangled states can be self-tested, Nat. Commun. **8**, 15485 (2017).
[19] P. Mironowicz, H.-W. Li, and M. Pawłowski, Properties of dimension witnesses and their semi-definite programming relaxations, Phys. Rev. A **90**, 022322 (2014).
[20] K. F. Pal and T. Vértesi, Maximal violation of a bipartite three-setting, two-outcome Bell inequality using infinite-dimensional quantum systems, Phys. Rev. A **82**, 022116 (2010).
[21] J. W. Eaton, D. Bateman, S. Hauberg, and R. Wehbring, GNU Octave version 5.1.0 manual: A high-level interactive language for numerical computations (2019), https://www.gnu.org/software/octave/doc/v5.1.0/.
[22] K. C. Toh, M. Todd, and R. H. Tütüncü, SDPT3—A MATLAB software package for semidefinite programming, Opt. Methods Softw. **11**, 545 (1999).
[23] R. H. Tütüncü, K. C. Toh, and M. J. Todd, Solving semi-definite-quadratic-linear programs using SDPT3, Math. Program. **95**, 189 (2003).
[24] J. Löfberg, YALMIP: A toolbox for modeling and optimization in MATLAB, in *Proceedings of the 2004 IEEE International Conference on Robotics and Automation* (IEEE, Piscataway, NJ, 2004).
[25] M. Navascués, G. de la Torre, and T. Vértesi, Characterization of Quantum Correlations with Local Dimension Constraints and its Device-Independent Applications, Phys. Rev. X **4**, 011011 (2014).
[26] M. Navascués and T. Vértesi, Bounding the Set of Finite Dimensional Quantum Correlations, Phys. Rev. Lett. **115**, 020501 (2015).
[27] P. Wittek, Algorithm 950: Ncpol2sdpa—Sparse semidefinite programming relaxations for polynomial optimization problems of noncommuting variables, ACM Trans. Math. Software **41**, 21 (2015).
[28] A. Tavakoli, M. Smania, T. Vértesi, N. Brunner, and M. Bourennane, Self-testing non-projective measurements, arXiv:1811.12712.
[29] M. Smania, M. Nawareg, P. Mironowicz, A. Cabello, M. Pawłowski, and M. Bourennane, Experimental device-independent certification of a symmetric, informationally complete, positive operator-valued measure, arXiv:1811.12851.
[30] N. Gisin, Bell Inequalities: Many Questions, a Few Answers, in *Quantum Reality, Relativistic Causality, and Closing the*

*Epistemic Circle*, The Western Ontario Series in Philosophy of Science, Vol. 73 (Springer, Dordrecht, 2009), pp. 125–138.

[31] O. Andersson, P. Badziąg, I. Bengtsson, I. Dumitru, and A. Cabello, Self-testing properties of Gisin's elegant Bell inequality, Phys. Rev. A **96**, 032119 (2017).

[32] M. Farkas and J. Kaniewski, Self-testing mutually unbiased bases in the prepare-and-measure scenario, Phys. Rev. A **99**, 032316 (2019).

[33] P. Mironowicz *et al.* (unpublished).