Experimental certification of an informationally complete quantum measurement in a device-independent protocol

Massimiliano Smania,[1, *] Piotr Mironowicz,[2, 3, 4, †] Mohamed Nawareg,[1]
Marcin Pawłowski,[3, 4] Adán Cabello,[5, 6] and Mohamed Bourennane[1, ‡]

[1]*Department of Physics, Stockholm University, S-10691 Stockholm, Sweden*
[2]*Department of Algorithms and System Modeling, Faculty of Electronics,*
Telecommunications and Informatics, Gdańsk University of Technology
[3]*National Quantum Information Centre in Gdańsk, Sopot 81-824, Poland*
[4]*International Centre for Theory of Quantum Technologies,*
University of Gdańsk, Wita Stwosza 57, 80-308 Gdańsk, Poland
[5]*Departamento de Física Aplicada II, Universidad de Sevilla, E-41012 Sevilla, Spain*
[6]*Instituto Carlos I de Física Teórica y Computacional, Universidad de Sevilla, E-41012 Sevilla, Spain*

Minimal informationally complete positive operator-valued measures (MIC-POVMs) are special kinds of measurement in quantum theory in which the statistics of their d^2-outcomes are enough to reconstruct any d-dimensional quantum state. For this reason, MIC-POVMs are referred to as standard measurements for quantum information. Here, we report an experiment with entangled photon pairs that certifies, for what we believe is the first time, a MIC-POVM for qubits following a device-independent protocol (i.e., modeling the state preparation and the measurement devices as black boxes, and using only the statistics of the inputs and outputs). Our certification is achieved under the assumption of freedom of choice, no communication, and fair sampling.

INTRODUCTION

A minimal informationally complete positive operator-valued measure (MIC-POVM) [1, 2] is a measurement on a d-dimensional quantum system that: (i) is informationally complete (IC), i.e., its statistics determine completely any quantum state and allow for a simple state-reconstruction and (ii) is minimal, since it has the minimum number of outcomes a measurement must have to be IC, namely, d^2 [3]. MIC-POVMs are fundamental in quantum information. For example, they are crucial for optimal quantum state tomography [4, 5], quantum key distribution with optimal trade-off between security and key rate [6], device-independent certification of optimal randomness from one bit of entanglement [7, 8], and optimal entanglement detection [9]. Arguably, MIC-POVMs are the "standard" measurements in quantum information [10] and thus have a privileged role in information-theoretic reconstructions of quantum theory [10].

Experimentally, MIC-POVMs have been aimed at in photonic experiments of qubit [11], qutrit [12, 13], and two-qubit [14] tomography, quantum key distribution [11], and generalized measurements using quantum walks [14, 15]. However, all these experiments made assumptions about the state preparation and the functioning of the measurement devices and therefore have limited applicability to cryptographic scenarios.

Here, we address the problem of experimentally certifying a MIC-POVM for qubits following a "device independent" (DI) protocol [7, 8, 16, 17]. That is, modeling the state preparation and the measurement devices as black boxes and using only the statistics of the inputs and outputs obtained within a Bell inequality experiment. The idea behind the experiment is to integrate the MIC-POVM within a Bell inequality experiment and use it to produce correlations that, according to quantum theory, are only attainable with a MIC-POVM for qubits. Our results not only allow us to certify a MIC-POVM for qubits in a DI protocol, but also constitute the first experimental observation of "qubit correlations which can only be explained by four-outcome non-projective measurements" [18].

CERTIFICATION METHODS

To certify a four-outcome MIC-POVM in a DI way, we use the bipartite Bell scenario shown in Fig. 1. There, in the middle, is a source emitting pairs of particles. One of the particles is measured by one party, Alice, and the other particle is measured by the other party, Bob. Alice chooses her measurement from a set of four measurements: three two-outcome measurements A_x, with $x \in \{1, 2, 3\}$, and one four-outcome measurement A_4. Bob chooses his measurement from a set of four two-outcome measurements B_y, with $y \in \{1, 2, 3, 4\}$. The possible outcomes of the two-outcome measurements are $+1$ and -1, and the possible outcomes of the four-outcome measurements are $1, 2, 3$, and 4. The outcomes of A_x and B_y are denoted by a and b, respectively. From the experimental results, we obtain the set of conditional probabilities $\{P(a, b|x, y)\}$.

In our experiment, we are interested in the conditional probabilities appearing in the following Bell inequality introduced in Ref. [7]:

$$\beta_{\text{el}}^{\text{m}} = \beta_{\text{el}} - k \sum_{i=1}^{4} P(a = i, b = +1|x = 4, y = i), \quad (1)$$
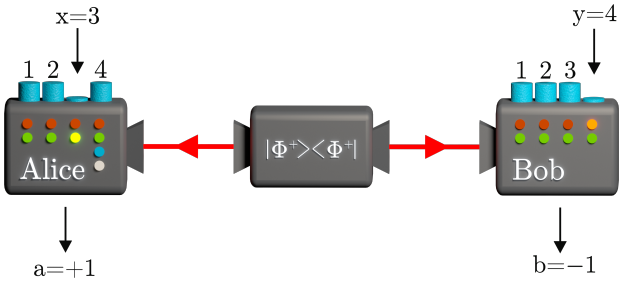
FIG. 1. The scenario considered in our experiment consists of two parties, Alice and Bob, who perform local measurements on maximally entangled pairs of qubits. See further details in the text.

where β_{el} is the Bell operator of the so-called "elegant Bell inequality" [7, 8, 19], namely,

$$\beta_{\text{el}} = E_{11} + E_{12} - E_{13} - E_{14} + E_{21} - E_{22} \\ + E_{23} - E_{24} + E_{31} - E_{32} - E_{33} + E_{34}, \quad (2)$$

where $E_{xy} = \sum_{a,b} ab P(a,b|x,y)$. For local hidden variable theories, β_{el} is upper-bounded by 6. In contrast, in quantum theory β_{el} is upper-bounded by $4\sqrt{3} \approx 6.928$. The quantum maximum can be achieved with pairs of qubits in state $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ and the following projective measurements:

$$A_1 = \sigma_x, \quad B_1 = \frac{1}{\sqrt{3}}(\sigma_x - \sigma_y + \sigma_z),$$
$$A_2 = \sigma_y, \quad B_2 = \frac{1}{\sqrt{3}}(\sigma_x + \sigma_y - \sigma_z),$$
$$A_3 = \sigma_z, \quad B_3 = \frac{1}{\sqrt{3}}(-\sigma_x - \sigma_y - \sigma_z), \quad (3)$$
$$B_4 = \frac{1}{\sqrt{3}}(-\sigma_x + \sigma_y + \sigma_z),$$

where σ_i are the Pauli matrices.

According to quantum theory, our target Bell operator $\beta_{\text{el}}^{\text{m}}$ is also upper-bounded by $4\sqrt{3}$. This quantum maximum can be attained with state $|\Phi^+\rangle$ and the measurements in Eq. (3). However, in this case, the second term in Eq. (1) is zero if and only if A_4 is a qubit symmetric MIC-POVM whose elements are anti-aligned with Bob's measurements B_y in Eq. (3). That is, if A_4 is the four-outcome POVM, defined by the following elements:

$$A_{4,1} = \frac{1}{2}\begin{pmatrix} \alpha & -\beta(1+i) \\ \beta(-1+i) & 1-\alpha \end{pmatrix},$$
$$A_{4,2} = \frac{1}{2}\begin{pmatrix} 1-\alpha & \beta(-1+i) \\ -\beta(1+i) & \alpha \end{pmatrix},$$
$$A_{4,3} = \frac{1}{2}\begin{pmatrix} 1-\alpha & \beta(1-i) \\ \beta(1+i) & \alpha \end{pmatrix}, \quad (4)$$
$$A_{4,4} = \frac{1}{2}\begin{pmatrix} \alpha & \beta(1+i) \\ \beta(1-i) & 1-\alpha \end{pmatrix},$$

where $\alpha = \frac{3-\sqrt{3}}{6}$ and $\beta = \frac{\sqrt{3}}{6}$. In this case, the extremes of the four unit vectors associated to the elements of A_4 define a regular tetrahedron within the Bloch sphere.

Any measurement different than the one defined in Eq. (4) will produce a smaller value for $\beta_{\text{el}}^{\text{m}}$. While certifying a *symmetric* MIC-POVM requires ideal conditions, we can use the property above to test whether a genuine four-outcome, MIC-POVM has indeed been realized in the experiment, by computing the maximum of $\beta_{\text{el}}^{\text{m}}$ that can be obtained using three-outcome measurements. In order to do this, let us consider the following generalization of $\beta_{\text{el}}^{\text{m}}$:

$$\sum_{x=1}^{3}\sum_{y=1}^{4} \gamma_{xy} E_{xy} - k \sum_{y=1}^{4}\sum_{a=1}^{4}\sum_{b=\pm 1} \gamma_{bxy} P(a,b|4,y). \quad (5)$$

We compute the maximum value of Eq. (5) that can be obtained using three-outcome measurements. That is, the maximum value of

$$\max_{j=1,2,3,4} \left[\sum_{x=1}^{3}\sum_{y=1}^{4} \gamma_{xy} E_{xy} \\ -k \sum_{y=1}^{4}\sum_{a\neq j}\sum_{b=\pm 1} \gamma_{bxy} P(a,b|4,y) \right]. \quad (6)$$

Each of the maximizations within Eq. (6) are taken with a constraint that the jth outcome of Alice's A_4 measurement has probability 0. The larger the gap between the experimental value of Eq. (5) and the maximum possible value of Eq. (6), the more confident we can be that indeed a genuine four-outcome POVM has been performed.

Most crucially, as we show in the Supplemental Material, four irreducible outcomes in dimension 2 imply information completeness, which is arguably the most important feature of a quantum measurement.

Finally, while Bell scenarios can in general be useful for measurement certification, it is important to point out that the Bell inequality in the protocol above is tailored to the specific measurement targeted in our certification. In order to use the same procedure for an arbitrary measurement, a different Bell inequality would in general be required. In fact, finding the optimal Bell inequality for certifying in a device-independent protocol a given generalized measurement is, in general, a difficult problem.

EXPERIMENT

Experimental setup

A type-I spontaneous parametric down-conversion source is used to generate entangled photon pairs in state $|\Phi^+\rangle = 1/\sqrt{2}(|HH\rangle + |VV\rangle)$, where H and V denote horizontal and vertical polarization, respectively.

Pairs of entangled photons at 780 nm are produced in two orthogonally oriented 2 mm thick beta barium borate (BBO) crystals, pumped with a femto-second laser at 390 nm. As shown in Fig. 2, these photons go through 1 nm spectral bandpass filters (SF), and are then coupled into single-mode fibers (SMF) to have perfect spatial mode overlap between the two polarizations. These SMFs then bring the photons to Alice's and Bob's measurement stations. Whenever projective measurements are performed on both sides (i.e., whenever $x \in \{1, 2, 3\}$ and $y \in \{1, 2, 3, 4\}$), the two measurement stations are identically composed by a lambda-half wave plate (HWP), a lambda-quarter wave plate (QWP), and a polarization beam-splitter (PBS). Multi-mode fibers (MMF) finally collect the photons at the four outcomes and bring them to the single-photon avalanche photodiodes (APDs). In addition, Bob's station includes a phase plate (PP).

In order to implement the four-outcome POVM, Alice's measurement station couples the two-dimensional polarization space with a counter-propagating two-path Sagnac interferometer, which makes transformations in an effectively four-dimensional space possible using two HWPs. At the two outputs of the interferometer, PPs, HWPs and QWPs are used in combination with PBSs to perform the POVM (for more details, see Supplemental Material). MMFs connected to APDs again gather photons at the four outcomes. Detection counting is performed with a coincidence unit (CU) using 1.6 ns coincidence windows.

A two-photon rate of about 150 coincidences per second was maintained throughout the experiment. Each measurement setting lasted 30 seconds, and all measurements were repeated a total of 23 times. This was done in order to decrease the repeatability error of the motorized wave plate mounts.

Results

The maximization of Eq. (6) for fixed coefficients γ_{xy} and γ_{bxy} should be made over the set of probabilities allowed by quantum theory. To obtain an upper bound on its value, we use the semi-definite programming method of Navascués, Pironio, and Acín (NPA) [20] implemented in the Python package Ncpol2spda [21].

To identify the values of γ_{xy} and γ_{bxy} that provide the largest gap between the experimental value of (5) and the maximum possible value of (6), we performed a series of numerical optimizations using the Nelder-Mead method [22], with target function defined as the difference between experimental value of (5) and a bound of (6), with variable coefficients γ_{xy} and γ_{bxy} and fixed values of k. As a result, we obtained the following Bell operator:

$$
\begin{aligned}
& 0.9541 E_{11} + 0.9917 E_{12} - 0.9767 E_{13} - 1.0064 E_{14} \\
& + 0.9514 E_{21} - 0.9921 E_{22} + 0.8211 E_{23} - 1.0237 E_{24} \\
& + 1.0641 E_{31} - 1.0044 E_{32} - 1.0579 E_{33} + 1.1563 E_{34} \\
& - 3[1.2068 P(1,1|4,1) - 0.0374 P(1,2|4,1) - 0.0034 P(2,1|4,1) + 0.0140 P(2,2|4,1) \\
& + 0.0006 P(3,1|4,1) + 0.0268 P(3,2|4,1) - 0.0163 P(4,1|4,1) - 0.0155 P(4,2|4,1) \\
& - 0.0033 P(1,1|4,2) + 0.0184 P(1,2|4,2) + 1.1156 P(2,1|4,2) - 0.0046 P(2,2|4,2) \\
& - 0.0125 P(3,1|4,2) + 0.0401 P(3,2|4,2) - 0.0175 P(4,1|4,2) - 0.0240 P(4,2|4,2) \\
& - 0.0108 P(1,1|4,3) + 0.0153 P(1,2|4,3) - 0.1195 P(2,1|4,3) + 0.1752 P(2,2|4,3) \\
& + 0.6201 P(3,1|4,3) + 0.0149 P(3,2|4,3) - 0.0399 P(4,1|4,3) + 0.0527 P(4,2|4,3) \\
& + 0.0058 P(1,1|4,4) - 0.0149 P(1,2|4,4) + 0.0025 P(2,1|4,4) + 0.0205 P(2,2|4,4) \\
& + 0.0150 P(3,1|4,4) + 0.0212 P(3,2|4,4) + 0.9565 P(4,1|4,4) - 0.0023 P(4,2|4,4)].
\end{aligned}
\tag{7}
$$

The upper bounds on the maximum possible value of β_{IC} in Eq. (7), obtained using the third level of the NPA method, in case of three-outcome measurements and in case of any quantum measurement are:

$$
\beta_{\mathrm{IC}} \overset{\text{3-outcome}}{\leq} 6.8782 \overset{\text{Quantum}}{\leq} 6.9883, \tag{8}
$$

whereas our experimental result is:

$$
\beta_{\mathrm{IC}}^{\exp} = 6.960 \pm 0.007 \tag{9}
$$

(more detailed results are provided in Tables I and II). Therefore, the experimental value violates the three-outcome bound by more than 11 standard deviations, certifying that Alice's A_4 measurement was indeed an irreducible four-outcome measurement, under the assumption that the system at Alice's laboratory is a qubit. In order to remove this assumption, we used the SWAP method [23] to calculate the two-qubit state fidelity with the maximally entangled Bell state $|\Phi^+\rangle$ certified by the experimental data contained in Tab. I for β_{el} in Eq. (2).
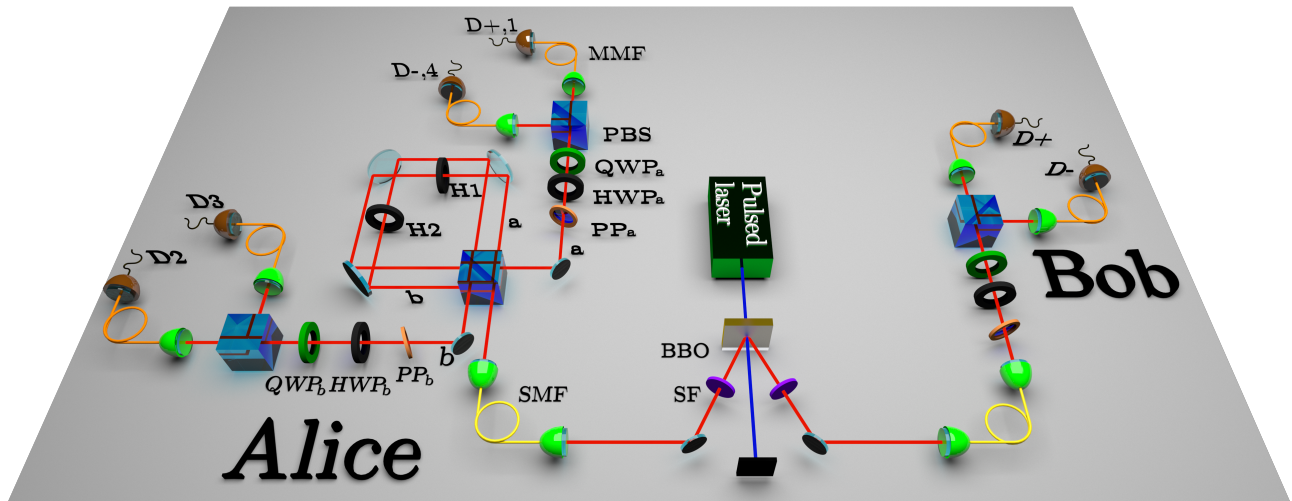
FIG. 2. Experimental setup. The following components are used: a beta-barium borate non-linear crystal (BBO), 3 nm narrow spectral filters (SF), single-mode optical fibers (SMF), phase plates (PP), lambda-half wave plates (HWP), lambda-quarter wave plates (QWP), polarizing beam splitters (PBS), multi-mode optical fibers (MMF), and single-photon detectors (DET).
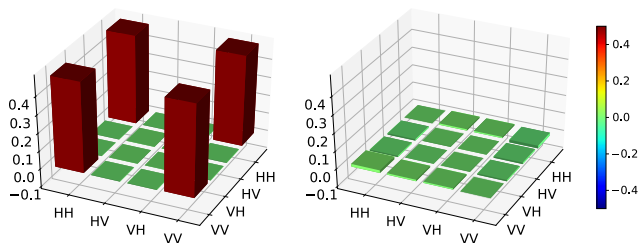

FIG. 3. Tomography of the prepared maximally entangled state. Real (left) and imaginary (right) parts.

To this end we employed the level $3 + AABB$ of the NPA hierarchy [20]. The resulting fidelity was 0.947.

This means that a qubit measurement occurs in at least 94.7% of times. The only alternative to a qubit MIC-POVM is that in 0.947 of the cases a three-outcome measurement on a qubit was used and in the remaining 0.053 of the cases a four-outcome measurement on a higher-dimensional system was used. However, in such a case, the maximal possible value to be observed is not greater than $0.947 \times 6.8782 + 0.053 \times 6.9883 \approx 6.8840$, which is smaller than the experimental value, namely, 6.960. Similarly, one can calculate that the critical fidelity η_{crit} to two dimensional state for MIC-POVMs is given by: $(6.9883 - \beta_{exp})/(6.9883 - 6.8782) \approx 0.257$.

Even though our DI protocol relies on this method, we can provide additional, non DI arguments, which suggest that the actual state fidelity was considerably higher. Firstly, we tested the quality of the polarization entanglement by performing a complete nine-measurement state tomography of the Alice-Bob system. The tomography of the joint state is shown in Fig. 3. The experimental fidelity with state $|\Phi^+\rangle$ was near optimal at $(99.6 \pm 0.1)\%$.

Secondly, our measured value of the Bell operator of the Elegant Bell Inequality was $\beta_{el} = 6.909 \pm 0.007$, which corresponds to 99.7% of the quantum bound and is less than three standard deviations away from it. As mentioned above, a result equal to the quantum bound would imply that the joint state is a maximally entangled qubit-qubit state [7, 8].

As a final remark, although our protocol is DI, we have assumed freedom-of-choice, fair-sampling and no-communication in our experiment. As we show in the Supplemental Material, closing the detection loophole would require overall system efficiencies above 94%, outside the reach of state of the art photonics experiments.

Setting	Theory	Experiment
E_{11}	$1/\sqrt{3} \approx 0.577$	0.553 ± 0.002
E_{12}	0.577	0.573 ± 0.002
E_{13}	-0.577	-0.581 ± 0.002
E_{14}	-0.577	-0.543 ± 0.002
E_{21}	0.577	0.589 ± 0.002
E_{22}	-0.577	-0.599 ± 0.002
E_{23}	0.577	0.529 ± 0.002
E_{24}	-0.577	-0.579 ± 0.002
E_{31}	0.577	0.584 ± 0.002
E_{32}	-0.577	-0.557 ± 0.002
E_{33}	-0.577	-0.621 ± 0.002
E_{34}	0.577	0.601 ± 0.002
β_{el}	$4\sqrt{3} \approx 6.928$	6.909 ± 0.007

TABLE I. Experimental values for the combinations of settings needed to test the elegant Bell inequality.

$P(a=i, b=+1|x=4, y=i)$	Theory	Experiment
$P(1,+1|4,1)$	0	0.0021 ± 0.0001
$P(2,+1|4,2)$	0	0.0020 ± 0.0001
$P(3,+1|4,3)$	0	0.0025 ± 0.0001
$P(4,+1|4,4)$	0	0.0025 ± 0.0001
Sum	0	0.0091 ± 0.0002

TABLE II. Experimental values for the probabilities of the outcomes of the MIC-POVM that are most relevant to the DI certification protocol [see Eq. (1)].

State tomography with the MIC-POVM

In order to test the tomographic capabilities of our certified MIC-POVM against the standard tomographic methods based on projective measurements, we reconstructed eight different Alice's local qubit states (those naturally occurring in our Bell scenario when we condition Alice's state to Bob's measurements and results) using both methods. Firstly, a standard tomographic analysis from the experimental statistics of *three* projective measurements (in our case, A_1, A_2, and A_3; that is, σ_x, σ_y, and σ_z). Secondly, using only the experimental statistics of our *single* four-outcome measurement. The resulting reconstructed local states should be identical for both methods and, ideally, must point to the corners of a regular tetrahedron in the Bloch sphere. In the case of the MIC-POVM, a simple formula connects the four experimental frequencies produced by the single measurement with the tomographic reconstruction:

$$\vec{s} = 3 \sum_{j=1}^{4} f_j \vec{A}_j, \qquad (10)$$

where $\vec{s}$ is the unknown Bloch vector, each $\vec{A}_j$ is one of the four elements of the symmetric MIC-POVM set (see Eq. (4)), and f_j is its corresponding measured frequency [5]. On the other hand, the six experimental frequencies provided by the three projective measurements were used, through linear inversion [24], to reconstruct the same states. The results of both methods are presented in Fig. 4.

The fidelity between corresponding vectors was in all eight cases equal to or greater than 99.5%, indicating that the two tomographic methods yielded near-optimally overlapping results, and the four-outcome POVM is informationally complete and effectively symmetric. More detailed results are provided in the Supplemental Material.

All the experimental uncertainties reported were calculated with *a priori* evaluation of known sources of error, and subsequent propagation in the results. The sources of errors included in our analysis were: photon counting statistics, precision of wave plate rotation, detector dark counts, and higher order down-conversion events
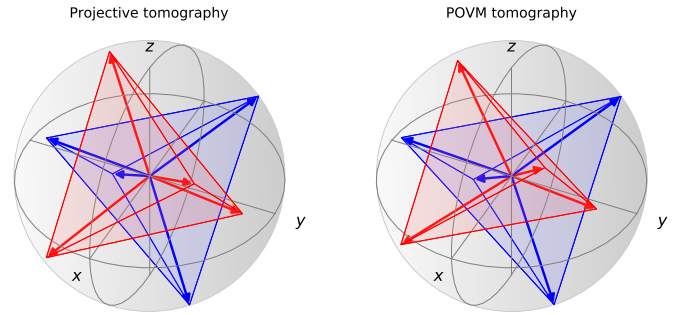

FIG. 4. Reconstruction of eight Alice's local qubit states, conditioned on Bob's setting and outcome, as obtained from standard projective tomography (left) and MIC-POVM tomography (right).

(see Supplemental Material for more details).

CONCLUSIONS

Quantum information identifies MIC-POVMs as the standard quantum measurements for information processing tasks as they are informationally complete and optimal for tomographic and cryptographic purposes. On the other hand, the device-independent paradigm provides the arguably optimal way to test quantum devices, as it reduces the assumptions to the minimum. Device-independent tests are especially important within cryptographic scenarios and constitute, in a sense, the highest level of certification attainable with quantum theory. Here, we have reported the results of an experiment certifying for the first time a MIC-POVM for qubits following a device-independent protocol. For that, we have produced correlations between separated photons that, as we have proven, are only attributable to an informationally complete four-outcome measurement on qubits. Our results pave the way towards realistic applications requiring device-independent certification of MIC-POVMs, and show how very refined concepts of quantum information are now experimentally attainable and can transform communication and information processing technologies.

DISCLOSURES

The authors declare no conflicts of interest.

See Supplemental Material for supporting content.

————————

* massimiliano.smania@fysik.su.se
† piotr.mironowicz@gmail.com
‡ boure@fysik.su.se

[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] S. Weigert, "Simple minimal informationaly complete measurements for qudits," Int. J. Mod. Phys. B **20**, 1942 (2006).

[3] G. Chiribella, G. M. D'Ariano, and D. Schlingemann, "How continuous quantum measurements in finite dimensions are actually discrete," Phys. Rev. Lett. **98**, 190403 (2007).

[4] C. M. Caves, C. A. Fuchs, and R. Schack, "Unknown quantum states: The quantum de finetti representation," J. Math. Phys. **43**, 4537 (2002).

[5] J. Řeháček, B.-G. Englert, and D. Kaszlikowski, "Minimal qubit tomography," Phys. Rev. A **70**, 052321 (2004).

[6] C. A. Fuchs and M. Sasaki, "Squeezing quantum information through a classical channel: Measuring the "quantumness" of a set of quantum states," Quant. Info. Comp. **3**, 377 (2003).

[7] A. Acín, S. Pironio, T. Vértesi, and P. Wittek, "Optimal randomness certification from one entangled bit," Phys. Rev. A **93**, 040102(R) (2016).

[8] O. Andersson, P. Badziąg, I. Dumitru, and A. Cabello, "Device-independent certification of two bits of randomness from one entangled bit and gisin's elegant bell inequality," Phys. Rev. A **97**, 012314 (2018).

[9] J. Shang, A. Asadian, H. Zhu, and O. Gühne, "Enhanced entanglement criterion via symmetric informationally complete measurements," Phys. Rev. A **98**, 022309 (2018).

[10] C. A. Fuchs, "Quantum mechanics as quantum information and only a little more," https://arxiv.org/abs/quant-ph/0205039 (2002).

[11] T. Durt, C. Kurtsiefer, A. Lamas-Linares, and A. Ling, "Wigner tomography of two-qubit states and quantum cryptography," Phys. Rev. A **78**, 042338 (2008).

[12] Z. E. D. Medendorp, F. A. Torres-Ruiz, L. K. Shalm, G. N. M. Tabia, C. A. Fuchs, and A. M. Steinberg, "Experimental characterization of qutrits using symmetric informationally complete positive operator-valued measurements," Phys. Rev. A **83**, 051801(R) (2011).

[13] W. M. Pimenta, B. Marques, T. O. Maciel, R. O. Vianna, A. Delgado, C. Saavedra, and S. Pádua, "Minimum tomography of two entangled qutrits using local measurements of one-qutrit symmetric informationally complete positive operator-valued measure," Phys. Rev. A **88**, 012112 (2013).

[14] Z. Hou, J.-F. Tang, J. Shang, H. Zhu, J. Li, Y. Yuan, K.-D. Wu, G.-Y. Xiang, C.-F. Li, and G.-C. Guo, "Deterministic realization of collective measurements via photonic quantum walks," Nat. Commun. **9**, 1414 (2018).

[15] Y.-Y. Zhao, N.-K. Yu, P. Kurzyński, G.-Y. Xiang, C.-F. Li, and G.-C. Guo, "Experimental realization of generalized qubit measurements based on quantum walks," Phys. Rev. A **91**, 042101 (2015).

[16] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, "Device-independent security of quantum cryptography against collective attacks," Phys. Rev. Lett. **98**, 230501 (2007).

[17] A. Acín and L. Masanes, "Certified randomness in quantum physics," Nature **540**, 213 (2016).

[18] E. S. Gómez, S. Gómez, P. González, 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).

[19] Nicolas Gisin, "Bell inequalities: Many questions, a few answers," in *Quantum Reality, Relativistic Causality, and Closing the Epistemic Circle*, edited by Wayne C. Myrvold and Joy Christian (Springer, 2009) pp. 125–138.

[20] M. Navascués, S. Pironio, and A. Acín, "A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations," New J. Phys. **10**, 073013 (2008).

[21] P. Wittek, "Algorithm 950: ncpol2sdpa–sparse semidefinite programming relaxations for polynomial optimization problems of noncommuting variables," ACM Trans. Math. Softw. **41**, 21 (2015).

[22] J. A. Nelder and R. Mead, "A simplex method for function minimization," The Computer Journal **7**, 308 (1965).

[23] T. H. Yang, T. Vertesi, J.-D. Bancal, V. Scarani, and M. Navascues, "Robust and versatile black-box certification of quantum devices," Phys. Rev. Lett. **113**, 040401 (2014).

[24] C. Schwemmer, L. Knips, D. Richart, H. Weinfurter, T. Moroder, M. Kleinmann, and O. Gühne, "Systematic errors in current quantum state tomography tools," Phys. Rev. Lett. **114**, 080403 (2015).

[25] M. Czechlewski and M. Pawłowski, "The influence of the choice of post-processing method on bell inequalities," Phys. Rev. A **97**, 062123 (2018).

SUPPLEMENTAL MATERIAL

Here we provide supplementary information to the manuscript above. In particular, the following will be presented: details on the experimental realization of non-projective measurements, proof of information completeness, results of tomographic reconstruction of Alice's eight local states and details on error estimation.

Experimental realization of Alice's POVM

We will derive in this section the Kraus operators corresponding to the four outcomes of Alice's non-projective measurement (Eq. (4) in main paper). In order to get to them, we shall work with a four dimensional Hilbert space on Alice's side, which includes the usual polarization space (with basis vectors $|H\rangle$ and $|V\rangle$) and the additional path degree of freedom added by the Sagnac interferometer. Referring to Fig. 2 in the main paper, we denote by $|a\rangle$ the mode transmitted by the polarizing beam splitter (PBS) at the entrance of the interferometer, passing through lambda-half wave plate (HWP) H1, and transmitted again by the PBS. Counter-propagating to it, and going through HWP H2, is instead mode $|b\rangle$.

We can then describe any four-dimensional state $|\Psi\rangle_A$ as a vector with basis $\{|H\rangle|a\rangle, |H\rangle|b\rangle, |V\rangle|a\rangle, |V\rangle|b\rangle\}$, where each element refers to one polarization-path combined mode. In this context, a PBS can be described as:

$$U_{PBS} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & i \\ 0 & 0 & 1 & 0 \\ 0 & i & 0 & 0 \end{pmatrix}, \tag{11}$$

while HWP, lambda-quarter wave plates (QWP) and phase plates (PP) as:

$$U_H(\theta) = \begin{pmatrix} \cos 2\theta & \sin 2\theta \\ \sin 2\theta & -\cos 2\theta \end{pmatrix},$$
$$U_Q(\theta) = \begin{pmatrix} \cos^2\theta + i\sin^2\theta & (1-i)\sin\theta\cos\theta \\ (1-i)\sin\theta\cos\theta & i\cos^2\theta + \sin^2\theta \end{pmatrix}, \tag{12}$$
$$U_{PP}(\theta) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix}.$$

The HWPs inside the interferometer act as:

$$U_{H1H2} = U_H(\theta_{H1}) \oplus U_H(\theta_{H2}) =$$
$$\begin{pmatrix} \cos 2\theta_{H1} & \sin 2\theta_{H1} & 0 & 0 \\ \sin 2\theta_{H1} & -\cos 2\theta_{H1} & 0 & 0 \\ 0 & 0 & \cos 2\theta_{H2} & \sin 2\theta_{H2} \\ 0 & 0 & \sin 2\theta_{H2} & -\cos 2\theta_{H2} \end{pmatrix} \tag{13}$$

and the whole interferometer is thus given by $U_{int}(\theta_{H1}, \theta_{H2}) = U_{PBS}U_{H1H2}U_{PBS}$.

After the Sagnac interferometer, each of the two output paths includes a combination of PP, HWP and QWP, PBS and two single photon detectors. Referring to Fig. 2 in the main paper, we can then express the transformations in polarization space for outcomes $j = \{1, 2, 3, 4\}$ in terms of Kraus operators as:

$$A_1 = \langle a|U_{PBS}U_Q(\theta_{Qa})U_H(\theta_{Ha})U_{PP}(\theta_{Pa})|a\rangle\langle a|U_{int}|a\rangle,$$
$$A_2 = \langle a|U_{PBS}U_Q(\theta_{Qb})U_H(\theta_{Hb})U_{PP}(\theta_{Pb})|a\rangle\langle b|U_{int}|a\rangle,$$
$$A_3 = \langle b|U_{PBS}U_Q(\theta_{Qb})U_H(\theta_{Hb})U_{PP}(\theta_{Pb})|a\rangle\langle b|U_{int}|a\rangle,$$
$$A_4 = \langle b|U_{PBS}U_Q(\theta_{Qa})U_H(\theta_{Ha})U_{PP}(\theta_{Pa})|a\rangle\langle a|U_{int}|a\rangle, \tag{14}$$

so that Alice's qubit undergoes the operation $|\psi\rangle_A \to A_j|\psi\rangle_A$, and each of her non-projective measurement operators (in Eq. (4) in the main paper) is described by $A_{4,j} = A_j^\dagger A_j$. As a side note, while a combination of HWP and QWP at each interferometer output would in principle be sufficient, adding the PPs allows for "standard" σ_x and σ_y measurement settings to be used, together with a fixed phase given by the PPs. Moreover, since the relative phase between the interferometer's arms is fixed but unknown, the additional PP simplifies the experimental task of compensating for this additional phase.

Because of the effectively redundant PPs, there are several combinations of settings that lead to optimal violation of Eq. (5). In our experimental realization, we used the following: $\theta_{H1} = 31.32°$, $\theta_{H2} = 13.68°$, $\theta_{Pa} = 45°$, $\theta_{Ha} = 0°$, $\theta_{Qa} = 45°$, $\theta_{Pb} = 135°$, $\theta_{Hb} = 22.5°$, $\theta_{Qb} = 0°$.

Information completeness of 4-outcome POVMs in dimension 2

We will now show that if a 4-outcome POVM is implemented in dimension 2, then the information retrieved from the quantum system is complete.

Note that a system of dimension 2 contains 3 independent parameters. Thus, in order to show that a 4-outcome POVM obtains these parameters we need to show that it consists of 3 linearly independent operators.

Let us assume that a POVM contains only 2 linearly independent operators. Without loss of generality we can write it in one of the forms:

$$(A, B, \alpha A + \beta B, \mathbb{1} - (1+\alpha)A - (1+\beta)B), \tag{15}$$

or

$$(A, B, \alpha A - \beta B, \mathbb{1} - (1+\alpha)A - (1-\beta)B), \tag{16}$$

with $\alpha, \beta \geq 0$. We now show that POVMs in (15) and (16) can be expressed as a convex combination of POVMs with at most 3 outcomes.

Indeed, for (15) we have:

$$(A, B, \alpha A + \beta B, \mathbb{1} - (1+\alpha)A - (1+\beta)B)$$
$$= \frac{1}{(1+\alpha)(1+\beta)} \left((1+\alpha)A, (1+\beta)B, 0, R \right)$$
$$+ \frac{\alpha}{(1+\alpha)(1+\beta)} \left(0, (1+\alpha)A, (1+\beta)B, R \right)$$
$$+ \frac{\beta}{(1+\alpha)(1+\beta)} \left((1+\alpha)A, 0, (1+\beta)B, R \right)$$
$$+ \frac{\alpha\beta}{(1+\alpha)(1+\beta)} \left(0, 0, (1+\alpha)A + (1+\beta)B, R \right), \tag{17}$$

where $R = \mathbb{1} - (1+\alpha)A - (1+\beta)B$.

Similarly, for (16) we have:

$$(A, B, \alpha A - \beta B, \mathbb{1} - (1+\alpha)A - (1-\beta)B)$$
$$= \frac{\alpha^2}{(\alpha+\beta)(1+\alpha)} \left(0, \left(1+\frac{\beta}{\alpha}\right)B, \right.$$
$$\left. \left(1+\frac{1}{\alpha}\right)(\alpha A - \beta B), R' \right)$$
$$+ \frac{\alpha}{(\alpha+\beta)(1+\alpha)} \left(\left(1+\frac{1}{\alpha}\right)(\alpha A - \beta B), \right.$$
$$\left. \left(1+\frac{\beta}{\alpha}\right)B, 0, R' \right)$$
$$+ \frac{\alpha\beta}{(\alpha+\beta)(1+\alpha)} \left(\left(1+\frac{\beta}{\alpha}\right)B, 0, \right.$$
$$\left. \left(1+\frac{1}{\alpha}\right)(\alpha A - \beta B), R' \right)$$
$$+ \frac{\beta}{(\alpha+\beta)(1+\alpha)} \left((1+\alpha)A + (1-\beta)B, 0, 0, R' \right), \tag{18}$$

where $R' = \mathbb{1} - (1+\alpha)A - (1-\beta)B$.

Detection efficiency

In order to calculate critical detection efficiency of the modified elegant Bell expression (Eq. (7) in the main paper), we first calculated its local hidden variables bound. To this end we enumerated all possible deterministic strategies. This revealed that the strategy assigning outcomes + for Alice's measurements 1 and 3, − for Alice's measurement 2, 2 for the POVM measurement, + for Bob's measurements 1, 2 and 4 and − for his measurement 3 yields the value 6.1652.

For detection efficiency calculations we assumed that, in post-processing of the experimental data whenever no-click events occur, an outcome from the optimal LHV strategy above is assigned. The critical detection efficiency calculated using the method in Ref. [25] is equal to 0.9439.

Tomographic reconstruction of Alice's eight local states

In Table III we report the eight qubit states, in Bloch vector notation, reconstructed using both standard projective tomography $(\sigma_x, \sigma_y, \sigma_z)$, and with single-setting MIC-POVM tomography. These states are the local states of Alice's qubit, conditioned on Bob's measurement settings and outcomes. The pairwise fidelity is also reported.

Error estimation

Here we provide a more comprehensive description of the errors considered in the experiment.

Counting statistics

Whenever (coincident) events with a constant rate are counted for some amount of time, the distribution of the final amount is in very good approximation Poissonian. We therefore considered all our empirical counts to have an uncertainty equal to their square root, and propagated it in the results. This is, by far, the predominant contribution to the final uncertainties in our experiment, giving errors of the order of $2 \cdot 10^{-3}$ and 10^{-4} on each E_{ab} and $P(a=i, b=+1 | x=4, y=i)$ term, respectively.

Motor precision

All measurement wave plates were rotated by motorized mounts controlled by a computer. The step motors have a precision equivalent to $0.02°$. This results in errors of the same order of the Poissonian ones. In order to reduce their contribution, each setting was repeated 23 times, therefore decreasing the uncertainties by almost a factor of 5.

Detector dark counts

Each of the single photon detectors used in the measurements have dark count rates of about 500 detections per second. The chances of a coincident event stemming from a true detection and a dark count, with the rates used, was as low as 10^{-11}, thus negligible.

Higher order down-conversion events

The rate of accidental coincidences $ac_{m,ij}$ coming from multiple down-conversion events in a single pulse, for

Projective tomography	SIC-POVM tomography	Fidelity
$(0.561 \; 0.601 \; 0.570)$	$(0.544 \; 0.508 \; 0.668)$	$0.995^{+0.004}_{-0.004}$
$(0.570 \; -0.589 \; -0.574)$	$(0.506 \; -0.681 \; -0.530)$	$0.996^{+0.003}_{-0.004}$
$(-0.572 \; 0.525 \; -0.630)$	$(-0.572 \; 0.525 \; -0.630)$	$0.997^{+0.002}_{-0.003}$
$(-0.551 \; -0.590 \; 0.591)$	$(-0.526 \; -0.695 \; 0.490)$	$0.995^{+0.002}_{-0.005}$
$(-0.548 \; -0.581 \; -0.601)$	$(-0.518 \; -0.574 \; -0.634)$	$0.999^{+0.001}_{-0.001}$
$(-0.577 \; 0.611 \; 0.541)$	$(-0.658 \; 0.586 \; 0.474)$	$0.997^{+0.002}_{-0.002}$
$(0.588 \; -0.532 \; 0.610)$	$(0.560 \; -0.603 \; 0.569)$	$0.998^{+0.001}_{-0.001}$
$(0.540 \; 0.573 \; -0.616)$	$(0.480 \; 0.570 \; -0.667)$	$0.998^{+0.001}_{-0.002}$

TABLE III. Tomographic reconstruction of the states depicted in Fig. 4 in the main text, using both projective and MIC-POVM tomography, and their pairwise fidelities. Uncertainties represent 15.9% and 84.1% quantiles of the respective results' distributions.

measurement setting m and detectors (i, j), can be estimated with the formula

$$ac_{m,ij} = \frac{S_{m,i} S_{m,j} \Delta t}{T}, \qquad (19)$$

where $S_{m,k}$ are the total (single) events on detector k during measurement time T, when coincidence windows of length Δt are used. While the resulting rates are fairly minimal (of the order of 10^{-3} events per second), they can still worsen, although slightly, the results obtained. Since the DI certification protocol can, in principle, work even if the state and measurements are not characterized, we chose not to correct our evaluations for this type of error. In the case of the full state tomography, the derived fidelity of 99.6% (and corresponding uncertainty), did not change whether we took accidental counts into consideration or not, due to their very low rate.