Self-Testing of a Single Quantum System: Theory and Experiment

Xiao-Min Hu
University of Science and Technology of China

Yi Xie
College of Science, National University of Defense Technology

Atul Arora
Centre for Quantum Information & Communication, Université libre de Bruxelles

Ming-Zhong Ai
University of Science and Technology of China

Kishor Bharti
iHPC, Singapore

Jie Zhang
National University of Defense Technology

Wei Wu
National University of Defense Technology

Chen pingxing
National University of Defense Technology

Jin-Ming Cui
https://orcid.org/0000-0002-5785-4248

Bi-Heng Liu
CAS Key Laboratory of Quantum Information, University of Science and Technology of China, Hefei, 230026, People's Republic of China

Yun-Feng Huang
University of Science and Technology of China

Chuan-Feng Li
University of Science and Technology of China

Guangcan Guo
University of Science and Technology of China

Jeremie Roland
Université Libre de Bruxelles

Adan Cabello
Universidad de Sevilla

Leong Chuan Kwek (cqtklc@nus.edu.sg)
National University of Singapore
Self-Testing of a Single Quantum System: Theory and Experiment

Xiao-Min Hu,1,2,3,* Yi Xie,4,5,* Atul Singh Arora,6,7,* Ming-Zhong Ai,1,2,3,* Kishor Bharti,8,9,10,* Jie Zhang,4,5 Wei Wu,4,5 Ping-Xing Chen,4,5,† Jin-Ming Cui,1,2,3 Bi-Heng Liu,1,2,3,‡ Yun-Feng Huang,1,2,3,§ Chuan-Feng Li,1,2,3 Guang-Can Guo,1,2,3 Jérémie Roland,6 Adán Cabello,11,12,¶ and Leong-Chuan Kwek8,13,14,∗∗

1 CAS Key Laboratory of Quantum Information, University of Science and Technology of China, Hefei, 230026, China
2 CAS Center For Excellence in Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei, 230026, China
3 Hefei National Laboratory, University of Science and Technology of China, Hefei, 230088, China
4 Department of Physics, College of Liberal Arts and Sciences, National University of Defense Technology, Changsha 410073, Hunan, China
5 Interdisciplinary Center for Quantum Information, National University of Defense Technology, Changsha 410073, Hunan, China
6 Centre for Quantum Information & Communication, Université libre de Bruxelles, B-1050 Bruxelles, Belgium
7 Institute of Quantum Information and Matter, Department of Computing and Mathematical Sciences, California Institute of Technology, USA
8 Centre for Quantum Technologies, National University of Singapore, Singapore
9 Joint Center for Quantum Information and Computer Science and Joint Quantum Institute, NIST/University of Maryland, College Park, Maryland 20742, USA
10 Institute of High Performance Computing, Agency for Science, Technology and Research (A*STAR), 1 Fusionopolis Way, Connexis, Singapore 138632, Singapore
11 Departamento de Física Aplicada II, Universidad de Sevilla, E-41012 Sevilla, Spain
12 Instituto Carlos I de Física Teórica y Computacional, Universidad de Sevilla, E-41012 Sevilla, Spain
13 MayaLab, CNRS-UNS-NUS-NTU International Joint Research Unit, Singapore UMI 3634, Singapore
14 National Institute of Education, Nanyang Technological University, Singapore 637616, Singapore

Self-testing allows for characterising quantum systems under minimal assumptions. However, existing schemes rely on quantum non-locality and cannot be applied to systems that are not entangled. Here, we introduce a robust method that achieves self-testing of individual systems by taking advantage of contextuality. The scheme is based on the simplest contextuality witness for the simplest contextual quantum system—the Klyachko-Can-Binicioğlu-Shumovsky inequality for the qutrit. We establish a lower bound on the fidelity of the state and the measurements as a function of the value of the witness under a pragmatic assumption on the measurements. We apply the method in an experiment on a single trapped 40Ca+ and using randomly chosen measurements and perfect detection efficiency. Using the observed statistics, we obtain the first experimental demonstration of self-testing of a single quantum system with negligible deviations from the assumptions.

I. INTRODUCTION

There is strong reason to believe that quantum devices can outperform their classical counterparts, on various fronts [1]. Yet, certifying that a quantum device is functioning as intended (or claimed), becomes challenging as the device becomes

* These five authors contributed equally to this work.
† pxchen@nudt.edu.cn
‡ bhliu@ustc.edu.cn
§ hyf@ustc.edu.cn
¶ adan@us.es
∗∗ kwekleongchuan@nus.edu.sg
increasingly complex [2]. More concretely, consider the two traditional methods for characterising a quantum system—
tomography and classical simulation. Both methods fail for large systems. Tomography requires resources which scale
*exponentially* (in the size of the quantum system being characterised) [3]. Similarly, since we have strong evidence showing
that quantum computations are intractable for classical computers, characterisation by classical simulation also fails for
large systems [4]. Thus, methods for characterising quantum systems are crucial for building useful large scale quantum
devices. Many such methods are known with varying strengths and weaknesses. Restricting to efficient methods, one
can classify them according to several parameters, such as the assumptions they make about the system (the weaker the
better) and the knowledge they provide about the system (the more the better). In this work, we focus on self-testing and
related methods, which solely aim to minimise the assumptions needed.

Self-testing is a property of a configuration—a state and a set of measurements—which requires that every other
configuration which produces the same measurement statistics is, in fact, identical to it, up to (local) isometries. Clearly,
without some assumption about the underlying system, no configuration can be self-tested. One of these assumptions is
that the system is bipartite and the two parts of the system cannot communicate. Indeed, the term “self-testing” was coined
in 2004 by [5] who showed that (in the bipartite no-communication setting) this property holds for a pair of maximally
entangled qubits. The underlying ideas, however, were already present in earlier works [6–10]. Self-testing has since been
an area of active investigation [11] and the notion has been extended to various settings, such as, bipartite (all pure states
can be self-tested [12–14]), multi-partite (various families can be self-tested [15–18]), Bell state measurement [19, 20],
predict-and-measure [21, 22], steering [23–25], among others.

Returning to device characterisation, a central technological challenge of our times is the construction of a large-scale
quantum computer—a single complex quantum system, where the aforementioned results do not hold. Thus, it is natural
to ask if one can extend self-testing to the single system setting.

II. RESULTS

Here, we tackle this question by approaching self-testing via non-contextuality inequalities—linear inequalities [26, 27],
similar to Bell inequalities, the experimental violation of which [28, 29] can be used to witness non-classicality. Their
advantage is precisely that they can be tested in a single system. Unlike, the aforementioned self-testing schemes based
on Bell nonlocality which assume no-communication (between parts of the device), we make a mild assumption on the
measurements that we call *KCBS orthogonality*. Similar self-testing schemes, based on non-contextuality inequalities, have
recently been proposed [30–33]. However, these works can only be applied when the experimental statistics *exactly* match
the ideal statistics. We remedy this stiffing shortcoming by providing the first contextuality self-testing *robustness curve*,
which enables one to self-test single quantum systems in the laboratory—the curve quantifies the fidelity of the system’s
configuration (to the ideal configuration) as a function of the deviation of the observed statistics (from the ideal statistics).
We then perform an experiment on a single $^{40}\text{Ca}^+$ ion and apply this self-test scheme to characterise the system. We
find that our characterisation is consistent with that obtained by conventional tomography. We emphasise that, even though
our self-test scheme was designed to minimise the assumptions one needs to make, it is nevertheless crucial to ensure
that these are satisfied by the experiment. In addition to the KCBS orthogonality condition, one must ensure that the
detection efficiency is nearly perfect and that the measurement settings are chosen randomly. In our experimental setup,
we quantify the deviation from these requirements and find that they are, indeed, negligible (see Section I in SM [35]).

---

1 Self-testing initially was defined to be a property of a quantum state alone (and not the measurements).
2 This is simply because the device could classically store and reproduce whatever statistics the self-test is required to satisfy.
3 While some of the works prove that their self test is “robust” in principle, they fail to show how to apply their result for any experiment
   which even mildly deviates from the ideal case.
4 To assure that non-contextual models are not simulating contextual correlations [34].
A. Overview and organisation

Figure II.1.  **LEFT.** The $^{40}\text{Ca}^+$ ion system and the measurement scheme. (a) The energy level diagram of the $^{40}\text{Ca}^+$ ion. (b) A schematic of the experimental setup. (c) The sequence of operations used in our experiment to measure $p_i$ via $\Pr(10|ij)$, i.e., the probability of obtaining $(a, b) = (1, 0)$ when $M_i$ and $M_j$ are measured. We choose $(i, j) \in E$ (edges of a five cycle graph) at random using a quantum random number generator. Each measurement $M_i$ is implemented by performing a rotation $U_i$, a fluorescence measurement (performed using a photo-multiplier tube), and undoing the rotation. For each measurement, the experiment is repeated over 10000 times.

**RIGHT.** The $x$-axis represents $\sum_k p_k$ (which we call the KCBS value) while the $y$-axis represents the total fidelity, $F$, to the ideal KCBS configuration. Recall that $I = Q - \sum_k p_k$. The bottom curve (blue), obtained by solving a semidefinite program, lower bounds $F$ as a function of $\sum_k p_k$. The top curve (orange) is similarly obtained by assuming, in addition, that $p_1 = p_2 = \cdots = p_5$. The points represent various experiments which (nearly) satisfy Assumption 1. The $x$ coordinates of these points represent $\sum_k p_k$, while the $y$ coordinate is evaluated by performing tomography and computing the fidelity to the ideal KCBS configuration. We note that $\sum_k p_k$ exceeds $\sqrt{5}$ (the maximum quantum value for projective measurements). This is warranted because our experiments are nearly perfect, and even small deviations from the underlying assumptions cause the KCBS value to deviate from the ideal one. It is worth noting that the left end of the error bar, however, is well within the $\sqrt{5}$ limit.

We first outline our theoretical contributions (Section II C). We informally introduced self-testing but did not explain the KCBS orthogonality condition (Assumption 1). Informally, for any odd number $n$ of measurements, the condition requires that the measurements are projective and satisfy the relations of orthogonality corresponding to an $n$-cycle graph (vertices represent measurements and edges relations of orthogonality). For simplicity, we henceforth implicitly take $^5 n = 5$. We denote our self-test by $I$ (Equation II.1) which is a linear expression in the input/output probabilities associated with the device. $I$ can be made 0 by a quantum device but every classical device must yield $I \geq Q - C > 0$, where $Q$ and $C$ are

---

5 It turns out that, in this setup, $n = 5$ is the smallest cyclic graph which separates quantum behaviour from its classical counterpart.
Consider a configuration for which $I$ is close to zero. To quantify the closeness of it to the KCBS configuration, we define the total fidelity, $F$ (Equation II.5). $F = 6$ for the KCBS configuration. We give a lower bound on $F$ as a function of $I$. The expression for $F$ when $I > 0$ becomes an optimisation problem which can be relaxed to a hierarchy of semidefinite programs (SDPs). This in turn can be solved numerically to obtain lower bounds on $F$. The details of the proof appear in Subsection IV A and those of the numerical solution in Subsection IV D. Obtaining the numerical solution was challenging. This is primarily because the description of the SDP we obtained is implicit. Therefore, we first find this explicit description by performing symbolic computation and subsequently, solve the resulting SDP (with over 15,000 constraints).

We now outline the experiment (Section II D). We apply this self-test to an experimental setup based on a single trapped $^{40}$Ca$^+$ ion. The KCBS configuration can be realised using a qutrit and projective measurements (see Figure II.2). In the experiment, the three levels of the qutrit are formed by the ground state, and the first excited state which is further split by the presence of a magnetic field. The measurements are executed by rotating between the ground state and the excited state using 729 nm lasers, performing a photon number measurement (via fluorescence detection), followed by an inverse of the rotation (see Figure II.1, LEFT and Subsection II D 1). The initial state and the rotation angles can be chosen such that they correspond directly to the KCBS configuration (Subsection II D 2). The actual experimental setup, of course, requires numerous details to be first addressed (Subsection II D 1) for this correspondence to work. Using this setup, we perform two types of experiments (Subsection II D 3), both of which are deviations from the KCBS configuration, constructed to ensure the KCBS orthogonality condition (Assumption 1) still holds. First, we leave the measurements unchanged but progressively depolarise the initial state. Second, we change the measurement settings, parametrised by

\[ F = n + 1 \]
Table I. A comparison of our experiment to previous experimental results on contextuality (see Section IV in SM [35]).

| Year | System         | Self-test | Compatibility | Sharp measurement | Random basis selection | Detection loophole |
|------|----------------|-----------|---------------|-------------------|------------------------|-------------------|
| 2011 | Photon [29]    | ×         | quantified    | not checked        | ×                      | not addressed     |
| 2013 | Yb+ ion [38]   | ×         | quantified    | not checked        | ×                      | closed            |
| 2016 | Superconducting [39] | ×         | quantified    | not checked        | ×                      | closed            |
| 2017 | Photon [40]    | ×         | quantified    | not checked        | ×                      | not addressed     |
| 2018 | Ca+ ion [41]   | ×         | quantified    | not checked        | ×                      | closed            |
| 2019 | Photon [42]    | ×         | quantified    | not checked        | ×                      | closed            |
| 2020 | Ba+ ion [43]   | ×         | quantified    | not checked        | ×                      | closed            |
| 2022 | Ca+ ion [this work] | ✓         | quantified    | quantified         | ✓                      | closed            |

Before delving into the details, we give a brief comparison to prior works.

Comparison to another single system self-testing scheme. In a breakthrough result, a self-testing scheme for a single quantum system was introduced by [36] which relied on cryptographic assumptions, instead of no-communication (as in the Bell case) or some requirement on the measurements (as in the case of contextuality). Arguably, this approach makes a qualitatively weaker assumption about the device. Yet, despite the theoretical appeal, they remain elusive with current technologies—the cryptographic functions involved in such schemes, seem to require at least 1,000 qubits\(^8\) which need to be held coherent for about 10,000 layers of gates (estimate based on [37]). This limitation is circumvented by our contextuality based self-test which can be already be implemented on a qutrit (viz. a three-level system).

Comparison to other contextuality experiments. Works on contextuality conventionally use an operational (i.e. theory independent) language to formulate the associated concepts. In this work, however, we take a more pragmatic approach and work directly under the assumption that quantum mechanics governs the behaviour of our devices. Consequently, the terminology we use to characterise our experiment is slightly different from prior works. More precisely, the analogue of our KCBS orthogonality requirement, in the operational perspective may be thought of as compatibility and sharpness of measurements (see Section I in the supplementary material (SM) [35]). In our experiment, we simultaneously quantify and minimise divergence from the basic assumptions—perfect detection, random selection of measurements, compatibility and sharpness—which, to the best of our knowledge, makes it the most comprehensive contextuality experiment to be reported (see Table I).

Swap isometry. One of our theoretical constructions (the swap isometry, explained in Subsection IV A) is motivated by the corresponding construction in [44]. While the construction in [44] works for Bell scenarios, our construction applies to the single party setting.

\(^8\) The number of qubits serves as the security parameter; higher the number, harder it is for a classical machine to break the underlying cryptographic scheme. The estimate ensures today’s classical computers will not be able to break the scheme. Proof of principle experiments may be possible with fewer qubits but they may be seen as having “computational loopholes”—classical computers will be able to spoof such tests.
C. The self-test scheme

Suppose we have a set of (independent) identical devices each of which takes a string as input and produces a string as output. Let \( p_i \) denote the probability of event \( i \), where an event is an instance of an input-output. Let \( I := \sum_i q_i p_i \) denote a linear combination of these probabilities, where \( q_i \in \mathbb{R} \). We say that \( (I, c) \), for some \( c \in \mathbb{R} \), self-tests the device\(^9\) if the following holds—if the device satisfies \( I = c \), then the device is uniquely described as containing a specific quantum state, the inputs corresponding to selecting specific measurements, the outputs correspond to the action of the measurement on the aforementioned quantum state, up to a global isometry.

As stated earlier, no self-test can exist without additional assumptions. We make the following assumption about the device we wish to self-test. To describe it, we setup some notation. We denote the \( i \)th binary measurement by \( M_i := (\Pi_{0|i}, \Pi_{1|i}) \), where \( \Pi_{0|i} \) denotes the measurement operator corresponding to the zeroth output and \( \Pi_{1|i} \) denotes that corresponding to the first output. Being measurement operators, they satisfy the probability conservation condition \( \Pi_{0|i}^\dagger \Pi_{0|i} + \Pi_{1|i}^\dagger \Pi_{1|i} = \mathbb{1} \). We say the binary measurement is repeatable and Hermitian if \( \Pi_{b|i}^\dagger = \Pi_{b|i} \) for \( b \in \{0, 1\} \) and \( \Pi_{b|i} = \Pi_{b|i}^\dagger \), respectively.

**Assumption 1.** For an odd \( n \), the quantum state in the device is \( \rho \) and the measurements \( M_1, M_2, \ldots, M_n \) are repeatable and Hermitian binary measurements (as described above) satisfying \( \Pi_{1|i} \cdot \Pi_{1|j} = 0 \) for \( i, j \in \{1, 2, \ldots, n - 1, n\} \), \{\( n, 1 \}\} := E.

At first, one might think that restricting to projective measurements, instead of POVMs, is without loss of generality due to Naimark’s theorem (according to which the statistics of any quantum measurement can also be obtained using a projective measurement, since any a positive-operator-valued measure can be seen as a projective-valued measure in a larger Hilbert space). However, this conclusion no longer holds for sequential measurements where post-measurement states become relevant.\(^10\) In any case, the aforementioned is a mild requirement and our experimental setup almost perfectly satisfies it (see Section I in SM [35]).

For a device satisfying Assumption 1, we consider the self-test\(^11\) \( I \)

\[
I := Q_n - \sum_{i=1}^{n} p_i, \tag{II.1}
\]

where \( p_i := \text{tr}(\Pi_i \rho) = \langle \Pi_i \rangle \) and \( Q_n := \frac{n \cos(\pi/n)}{1 + \cos(\pi/n)} \) is the “quantum value”.\(^12\) This quantum value is achieved by \( \sum_i (\Pi_i) \) for the KCBS configuration \((\rho_\text{KCBS}, \{\Pi_i^\text{KCBS}\})\), where \( \rho_\text{KCBS} \) is a qutrit in a pure state and \( \Pi_i^\text{KCBS} \) are projectors (see Definition 3 below), yielding \( I = 0 \).

**Definition 2** (An ideal KCBS configuration). Consider a three-dimensional Hilbert space spanned by the basis \( \{|0\rangle, |1\rangle, |2\rangle\} \). Let

\[
|u_l\rangle := \cos \theta |0\rangle + \sin \theta \sin \phi_l |1\rangle + \sin \theta \cos \phi_l |2\rangle, \tag{II.2}
\]

---

\(^9\) Later, we use “self-tests the device” to succinctly say “self-tests the configuration in the device”.

\(^10\) To properly address this issue, one must consider quantum instruments instead and define the notion of orthogonality accordingly. In the present work, we do not pursue this direction.

\(^11\) This particular form is of interest because, informally, any classical (i.e., non-contextual) model satisfying Assumption 1 cannot result in \( \sum_{i=1}^{n} p_i > C_n \) where \( C_n := (n - 1)/2 \) while quantumly, for the KCBS configuration (see Definition 3) one obtains \( \sum_{i=1}^{n} p_i = Q_n \), the highest possible [45]. The self-test measures how close one is to the maximum quantum value, \( Q_n \).

\(^12\) The maximum value of \( \sum_i p_i \) that is classically achievable (i.e., when all measurements commute) is \( (n - 1)/2 \).
where \( \phi_l := l\pi(n - 1)/n \) for \( 1 \leq l \leq n \) and \( \cos^2 \theta = \frac{\cos(\pi/n)}{1 + \cos(\pi/n)} \). Define
\[
|\psi^{\text{KCBS}}\rangle := |0\rangle, \\
\Pi_i^{\text{KCBS}} := |u_i\rangle \langle u_i|.
\] (II.3)

(II.4)

It was shown in [30] that any quantum realisation \( (\rho, \{\Pi_i\}) \) which satisfies Assumption 1 and yields \( \mathcal{I} = 0 \), must be the same as the KCBS configuration, up to a global isometry.\(^{13}\)

Recall that for clarity, we restricted to \( n = 5 \) but the arguments readily generalise. Suppose the device corresponds to a quantum realisation \( (\rho, \{\Pi_i\}) \) for which \( \mathcal{I} = \epsilon \) is small but not exactly zero. In this case, we derive a lower bound on the fidelity of \( (\rho, \{\Pi_i\}) \) to \((\rho^{\text{KCBS}}, \{\Pi_i^{\text{KCBS}}\}) \) (up to a global isometry). More precisely, we lower bound the value of the following function
\[
F := \min_{\rho, \{\Pi_i\}} \max_V \left[ \sum_{i=1}^5 F(\text{tr}_\mathcal{H}[V\Pi_i\rho\Pi_i^d], \Pi_i^{\text{KCBS}}\rho^{\text{KCBS}}\Pi_i^{\text{KCBS}}) + F(\text{tr}_\mathcal{H}[V\rho\Pi_i^d], \rho^{\text{KCBS}}) \right],
\] (II.5)

where \((\rho, \{\Pi_i\})_{i=1}^5\) is a quantum realisation of \( \{p_i\}_{i=1}^5 \) satisfying \( \mathcal{I} = \epsilon \), \( V \) is an isometry from \( \mathcal{H} \) to \( \mathcal{H} \otimes \mathcal{H}^{\text{KCBS}} \), i.e., from the space on which \( \rho, \{\Pi_i\}_{i=1}^5 \) are defined, to itself tensored with the 3-dimensional space where \( \rho^{\text{KCBS}}, \{\Pi_i^{\text{KCBS}}\}_{i=1}^5 \) are defined, and \( F(\sigma, \tau) := \text{tr} \sqrt{[\sigma^{1/2}\tau^{1/2}]^2} \) is the fidelity of \( \rho \geq 0 \) to \( \sigma \geq 0 \). This lower bound can be approximated by a sequence of semi-definite programs and can be evaluated for any\(^{14} \) \( \mathcal{I} = \epsilon \), yielding the robustness curve (see Figure II.1). We defer the detailed analysis to Subsection IV A.

### D. Experiment

#### 1. The setup

We describe our experimental setup which is designed to realise the ideal KCBS configuration. We use a \(^{40}\text{Ca}^+\) ion trapped in a blade-shaped Paul trap. The qutrit basis states are encoded into three Zeeman sub-levels of the \(^{40}\text{Ca}^+\) ion, with
\[
|0\rangle = |S_{1/2}, m_J = -1/2\rangle, \\
|1\rangle = |D_{5/2}, m_J = -3/2\rangle, \\
|2\rangle = |D_{5/2}, m_J = -1/2\rangle.
\] (II.6)

(II.7)

(II.8)

as shown in Figure II.1a. Unitary operations on these qutrits are performed by shining a linear polarised narrow-linewidth 729 nm laser beam, propagating along the trap axis, at an angle of 45° with respect to the quantization axis. For \( k \in \{1, 2\} \), the laser can be frequency modulated to be on resonance with the specific transition between the states \( |0\rangle \) and \( |k\rangle \) by an acousto-optic modulator (AOM). The coupling strength \( \Omega_k \), duration \( t \) and phase \( \phi_k \) of this laser pulse then can be controlled by the AOM to perform a rotation, \( R_k(\theta_k, \phi_k) \) between the states \( |0\rangle \) and \( |k\rangle \), where \( \theta_k = \Omega_k t \) and \( \phi_k \) represent

\(^{13}\) In fact, they also showed that if \( \mathcal{I} = \epsilon \) is close to zero, then the quantum realisation must be close to the KCBS configuration. However, their analysis did not yield the exact function corresponding to equation II.5—they only had an asymptotic bound (on the fidelity to the KCBS configuration) of the form \( O(\sqrt{\epsilon}) \).

\(^{14}\) Instead of the sum \( \sum_i p_i \), one could impose constraints on the values of \( p_i \) individually. In fact, this is what we do in our analysis as it yields a better bound.
the polar angle and the azimuthal angle respectively, i.e.,

\[
R_1(\theta_1, \phi_1) = \begin{pmatrix}
\cos \frac{\theta_1}{2} & -i\sin \frac{\theta_1}{2} e^{-i\phi_1} & 0 \\
-i\sin \frac{\theta_1}{2} e^{i\phi_1} & \cos \frac{\theta_1}{2} & 0 \\
0 & 0 & 1
\end{pmatrix},
\]

(II.9)

\[
R_2(\theta_2, \phi_2) = \begin{pmatrix}
\cos \frac{\theta_2}{2} & 0 & -i\sin \frac{\theta_2}{2} e^{-i\phi_2} \\
0 & 1 & 0 \\
-i\sin \frac{\theta_2}{2} e^{i\phi_2} & 0 & \cos \frac{\theta_2}{2}
\end{pmatrix}.
\]

(II.10)

The parameters of the rotation are controlled by varying the duration and phase of the corresponding laser pulse under constant intensity via the acoustic-optic modulator with high fidelity. Using \(R_1\) and \(R_2\), one can perform an arbitrary rotation in the qutrit space. Measurements in our setup are performed by fluorescence detection, i.e., counting photons.

2. Realising the KCBS configuration

The preceding operations can be combined to perform various experiments that (nearly) satisfy Assumption 1. Here, we describe, at a high level, the procedure for realising the KCBS configuration (see Definition 3). Detailed experimental steps are deferred to Subsection IV.B.

Using the notation introduced in Assumption 1, we denote the binary measurements of interest by \(M_i := (\Pi_{0|i}, \Pi_{1|i})\) and the quantum state of our system by \(\rho\). To realise the KCBS configuration, we require \(\Pi_{1|i} = |u_i\rangle\langle u_i|\) and \(\rho = |0\rangle\langle 0|\).

To implement the measurement \(\Pi_{1|i}\), as a composition of the operations our setup permits, we first compute a qutrit rotation \(U_i\) which maps \(|u_i\rangle\) to \(|0\rangle\). This, in turn, is used to compute the parameters \(\theta_{1,i}, \theta_{2,i}\) and \(\phi_{1,i}, \phi_{2,i}\) such that \(U_i = R_2(\theta_{2,i}, \phi_{2,i}) \cdot R_1(\theta_{1,i}, \phi_{1,i})\). Observe that defining \(\Pi_{1|i} := U_i |0\rangle \langle 0| U_i^\dagger\) and \(\Pi_{0|i} := U_i (|1\rangle \langle 1| + |0\rangle \langle 0|) U_i^\dagger\) results in the KCBS configuration.

Neglecting experimental imperfections (which are indeed negligible in our experiment; see Section I in SM [35]), it is evident that Assumption 1 is satisfied, i.e., \(\Pi_{1|i} \cdot \Pi_{1|j} = 0\) for \((i, j) \in E\) and \(\Pi_{1|i}^2 = \Pi_{1|i}\). Further, it is clear that

\[
p_i = \Pr(1|i) = \Pr(10|ij) = \text{tr}(\Pi_{0|j} \cdot \Pi_{1|i} \rho \Pi_{1|i}^\dagger \cdot \Pi_{0|j}^\dagger),
\]

(II.11)

where \(\Pr(ab|ij)\) denotes the probability of obtaining outcomes \((a, b)\) when measurements \((M_i, M_j)\) are performed and \(\Pr(a|i)\) denotes the probability of obtaining outcome \(a\) given \(M_i\) was measured. Finally, we note that \(\Pr(10|ij) = \Pr(01|ji)\).

As illustrated in Figure II.1, \(\sum_k p_k\) is estimated by randomly (using a quantum random number generator; see Section I in SM [35]) choosing \((i, j) \in E\), measuring \(M_i\) followed by \(M_j\) and counting \(N(10|ij)\), the number of times the output was \((1, 0)\), i.e.,

\[
p_i \approx \frac{N(10|ij)}{\sum_{a,b \in \{0,1\}} N(ab|ij)},
\]

(II.12)

3. Experiments that are self-tested

To study the self-testing property of a device, we perform experiments which deviate from the standard KCBS configuration, in two qualitatively different ways.
(a) \( p \)-configuration. Consider the realisation \( (\rho'(\rho), \{M_i\}) \) parametrised by \( 0 \leq p \leq 1 \). Here, \( M_i \) correspond to projectors along \(|u_i\rangle\) as before, but instead of initialising the state of the device to \( \rho = |0\rangle\langle0| \), we initialise it to a mixture of \( \rho \) and the maximally mixed state, i.e.,

\[
\rho'(\rho) := (1 - p)|0\rangle\langle0| + \frac{p}{9}. \tag{II.13}
\]

For \( p = 0 \), we recover the ideal KCBS configuration for which \( \mathcal{I} = 0 \). However, for \( p > 0 \), Assumption 1 still holds (neglecting the imperfections in the measurements) but \( \mathcal{I} = \epsilon > 0 \). The experiment was performed for \( p = 0.01, 0.2 \).

(b) \( \theta \)-configuration. Consider the realisation \( (|u'_0\rangle\langle u'_0|, \{M'_i(\theta)\}) \) parametrised by the vector \(|u'_0\rangle\) and the angle \( \theta \). Here, unlike the previous case, the state is pure. Further, the measurements \( M'_i = (\Pi'_{i|\theta}, \Pi'_{0|i}) \) now correspond to projections on \( |u'_\theta\rangle \) for \( i \in \{1, 2 \ldots 5\} \). These vectors \(|u'_\theta\rangle\) are chosen to be

\[
|u'_1\rangle = (1, 0, 0)^T, \tag{II.14}
\]
\[
|u'_2\rangle = (0, 0, 1)^T, \tag{II.15}
\]
\[
|u'_3\rangle = (-\cos(\theta), \sin(\theta), 0)^T, \tag{II.16}
\]
\[
|u'_4\rangle = \frac{(\sin(\theta), \cos(\theta), \sin(\theta))^T}{\sqrt{1 + \sin^2(\theta)}}, \tag{II.17}
\]
\[
|u'_5\rangle = (0, \sin(\theta), -\cos(\theta))^T, \tag{II.18}
\]

which ensures that Assumption 1 holds for all angles \( \theta \). We take \(|u'_0\rangle\) to be the eigenvector of \( \sum_k \Pi'_k \) with the largest eigenvalue. We performed the experiment for \( \theta = 22.041 \) and 150.612.

Table II summarises our findings for experiments implementing both \( p \) and \( \theta \)-configurations which are in agreement with our theoretical results. Here, we briefly explain how the data was obtained and analysed, deferring the details to Subsection IV C.

For a given configuration, we performed 10,000 sequential measurements and used Equation II.12 to estimate the mean \( \mu(p_i) \) and standard deviation \( \sigma(p_i) \) for each \( p_i \). Note, for instance, to measure \( p_2 \), one could measure in normal order: \( M_2 \) followed by \( M_3 \), or in reverse order: \( M_2 \) followed by \( M_1 \). We used a quantum random number generator to choose the measurement and its order.

To apply our self-test, we have two options: impose the constraint corresponding to either (1) \( \sum_k p_k \) or (2) \( p_k \) for each \( k \) individually. Option (2) would be unequivocally better than option (1) if \( \sigma \) was 0 (illustrated by the orange curve in Figure II.1, Right). As \( \sigma > 0 \), we use both methods and pick the best performing among them. When \( \sigma > 0 \) for a random variable, we evaluate \( \mu - 1.96\sigma \) to get an estimate for the random variable which lower bounds its value with over 95 percent confidence (assuming the data is normally distributed). When such an estimate is used, sometimes option (1) can give a better bound than option (2).

III. DISCUSSION

Quantifying deviations from assumptions. In all self-testing experiments, deviations from the assumptions must be quantitatively accounted for in the robustness curve. All reported self-test scheme, to the best of our knowledge, have

\[ \text{defined exactly as } M_i \text{ was defined using } |u_i\rangle; \Pi'_{i|\theta} = U'_i|0\rangle\langle0|U'_i† \text{ and } \Pi'_{0|i} = U_i(1 - |0\rangle\langle0|)U_i† \text{ with } U'_i \text{ encoding a rotation from } |u'_\theta\rangle \text{ to } |0\rangle. \]
| Configuration | \( \sum p_k \) | Fidelity (tomography) | Fidelity (lower bound) using \( \mu - 1.96\sigma \) | \( \sigma \) | \( \mu - 1.96\sigma \) |
|--------------|----------------|----------------------|----------------------------------|---------|------------------|
| \( p = 0 \) | 2.249 | 0.009 | 2.233 | 5.965 | 0.016 | 5.933 | 5.296 | 4.170 |
| \( p = 0 \) | 2.255 | 0.011 | 2.236 | 5.965 | 0.016 | 5.933 | 5.892 | 4.026 |
| \( p = 0.1 \) | 2.207 | 0.011 | 2.186 | 5.901 | 0.016 | 5.870 | 2.934 | 3.002 |
| \( p = 0.1 \) | 2.203 | 0.011 | 2.182 | 5.901 | 0.016 | 5.870 | 2.842 | 2.933 |
| \( p = 0.2 \) | 2.140 | 0.011 | 2.118 | 5.812 | 0.019 | 5.775 | 1.654 | 2.343 |
| \( p = 0.2 \) | 2.145 | 0.011 | 2.124 | 5.812 | 0.019 | 5.775 | 1.753 | 2.386 |
| \( \theta = 22.021 \) | 2.078 | 0.010 | 2.058 | 3.989 | 0.017 | 3.956 | 0.740 | 2.561 |
| \( \theta = 22.041 \) | 2.077 | 0.010 | 2.057 | 3.989 | 0.017 | 3.956 | 0.726 | 2.579 |
| \( \theta = 150.612 \) | 2.062 | 0.010 | 2.043 | 4.050 | 0.017 | 4.017 | 0.533 | 2.222 |
| \( \theta = 150.612 \) | 2.068 | 0.010 | 2.048 | 4.050 | 0.017 | 4.017 | 0.601 | 2.579 |

Table II. The above table shows a summary of our experimental and numerical results. Configuration refers to the \( p \) and \( \theta \) configurations discussed in Subsection II D 3. Each row represents the statistics obtained after running 10,000 experiments. White (grey) rows represent normal (reverse) order (again, see Subsection II D 3). The values in the last two columns show lower bounds on the total fidelity obtained using our self-test scheme (i.e., solving the semidefinite programme in Algorithm 6), evaluated in two slightly different ways. These arise as we consider \( \mu - 1.96\sigma \) (where \( \mu \) is the mean and \( \sigma \) is the standard deviation) to estimate the smallest possible value of our observed variables, with 95 percent confidence. Note the lower bounds on fidelity (last two columns) are satisfied by the value obtained using conventional tomography.

neglected this aspect in their analysis.

In more detail, for our setting, the lower bounds on total fidelity obtained using semi-definite programming only hold when Assumption 1 is satisfied. Relaxing this assumption (see Section I in SM [35]) to allow for measurements with errors \( \epsilon \) in repeatability (i.e., quantifying \( ||\Pi_{a[i]} - \Pi_{a[i]}|| \)) and \( \delta \) in orthogonality (i.e., quantifying \( ||\Pi_{1[i]} \cdot \Pi_{1[i+1]}|| \)) is left as an open question. A full analysis should yield a lower bound on the total fidelity as a function of the KCBS value, \( \delta \) and \( \epsilon \).

Note that the experimental points in Figure II.1 lie above our robustness curve. The robustness curve obtained via the full analysis cannot be above the present curve and thus will still lower bound the total fidelity for the experimental data points. Similarly, the existing robustness curves in Bell setting also only consider fidelity lower bound as a function of quantum value. Their analogous full analysis ought to include errors emanating from detection and locality loopholes.

A naïve application of current techniques fails because Algorithm 4 no longer yields a valid isometry. Complementary to this, improving the sharpness (i.e., projectiveness) and exclusivity of measurements in the experiment is also an obvious yet important goal, which if properly achieved, may render the aforesaid irrelevant.

**Future directions.** Extending the analysis to \( n > 5 \) (by making the algorithm more efficient), adapting it to more involved settings (possibly to anti-cycles), dropping the IID assumption (perhaps by using martingale analysis), obtaining analytic bounds (possibly via techniques from convex optimisation), we believe, are interesting avenues for further exploration.
IV. METHODS

A. Lower bound using an SDP relaxation

We briefly describe our algorithm for estimating $F$ and outline an argument which shows that this algorithm always yields a lower bound (on $F$). First, we drop the maximisation over $V$ in Equation II.5 and replace it with a particular isometry $V$ which is expressed in terms of $\rho, \{\Pi_i\}_{i=1}^5$. Then, as we shall see, the expression for the fidelity appears as a sum of terms of the following form. Let $w$ be a word created from the letters $\{I, \Pi_1, \Pi_2, \ldots, \Pi_5, P\}$, with $P^\dagger P = I$, $\Pi_i^2 = \Pi_i$, and $\Pi_i \Pi_j = 0$ if $(i, j) \in E$, i.e., when $i, j$ are exclusive.\textsuperscript{16} The fidelity is a linear combination of these words, i.e., $F = \min_{\{w\}} \sum_w \alpha_w \langle w \rangle$, where $\text{tr}[w\rho] = \langle w \rangle$, subject to the constraint that $\{\langle w \rangle\}_w$ corresponds to a quantum realisation. The advantage of casting the problem in this form is that one can now relax the problem to a sequence of semi-definite programs.\textsuperscript{17} The idea is simple to state. Treat $\{\{w\}_w\}$ as a vector. Denote by $Q$ the set of all such vectors which correspond to a quantum realisation (of $\{p_i\}_{i=1}^5$). It turns out that one can impose constraints on words with $k$ letters, for instance. Under these constraints, denote by $Q_k$ the set that is obtained. Note that $\lim_{k \to \infty} Q_k = Q$. Further, it is clear that $F = \min_{\{w\}_w \epsilon Q} \sum_w \alpha_w \langle w \rangle \geq \min_{\{w\}_w \epsilon Q_k} \sum_w \alpha_w \langle w \rangle$ as we are minimising over a larger set on the right hand side.

We now proceed formally. We begin with defining the ideal KCBS configuration, referred to above.

**Definition 3** (An ideal KCBS configuration). Consider a three-dimensional Hilbert space spanned by the basis $\{\{0\}, \{1\}, \{2\}\}$. Let

$$|u_l\rangle := \cos \theta |0\rangle + \sin \theta \sin \phi_l |1\rangle + \sin \theta \cos \phi_l |2\rangle, \quad (IV.1)$$

where $\phi_l := l\pi(n-1)/n$ for $1 \leq l \leq n$ and $\cos^2 \theta = \frac{\cos (\pi/n)}{1 + \cos (\pi/n)}$. Define

$$|\psi^{KCBS}\rangle := |0\rangle, \quad II^{KCBS}_i := |u_i\rangle \langle u_i| \quad (IV.2)$$

For concreteness, we first consider a unitary $U_{SWAP}$ instead of an isometry, which acts on two spaces $A$ and $A'$, i.e., $U_{SWAP} : A \otimes A' \rightarrow A \otimes A'$. The space $A'$ is three-dimensional and $A$ is an arbitrary Hilbert space. Informally, we want to construct the unitary $U_{SWAP}$ to be such that it takes a realisation in $A$ and maps it to a realisation in $A'$ which has a large overlap with the KCBS configuration. To this end, we first assume that $A$ is three-dimensional. In particular, suppose that the $A$ register is in the state

$$\sigma \in \{|\psi^{KCBS}\rangle \langle \psi^{KCBS}|\} \cup \{II^{KCBS}_i |\psi^{KCBS}\rangle \langle \psi^{KCBS}| II^{KCBS}_i\}_{i=1}^5 \quad (IV.4)$$

Then, at the very least, we want $U_{SWAP}$ to map $\sigma_A \otimes |0\rangle \langle 0|_A'$ to $|0\rangle \langle 0|_A \otimes \sigma_{A'}$ (see Figure II.2). Our strategy is to construct $U_{SWAP}$ in this seemingly trivial case and then express it in terms of the state and measurement operators on $A$. The rationale is that by construction, $U_{SWAP}$ will work for the ideal case and therefore should also work for cases close to ideal. This should become clear momentarily. Note that any circuit that swaps two qutrits should let us achieve our simplified goal (because all elements of $SKCBS$ are defined on a three dimensional Hilbert space). One possible qutrit

\textsuperscript{16} We introduced $\hat{P}$ for completeness; its role is explained later.

\textsuperscript{17} I.e., construct an NPA-like hierarchy [40].
swapping unitary/circuit (a special case of the general qudit swapping unitary/circuit defined in [44]) may be defined as
\[ S^{''}_{\text{SWAP}} := TUVU , \]
where
\[ T := \mathbb{I}_A \otimes \sum_{k=0}^{2} |−k⟩ ⟨ k|_{A'} , \]
\[ U := \sum_{k=0}^{2} P_k^A \otimes |k⟩ ⟨ k|_{A'} , \]
\[ V := \sum_{k=0}^{2} |\bar{k}⟩ ⟨ \bar{k}|_{A'} \otimes P_{A'}^{-k} , \]
and
\[ P := \sum_{i=0}^{2} |k⟩ ⟨ k| \]
is a translation operator, the arithmetic operations are modulo 3 and \{\bar{0}, \bar{1}, \bar{2}\} is a basis for the qutrit space \(A\). We omit the proof that \(S^{''}_{\text{SWAP}}\) indeed performs a swap operation (for a proof see [44]).

To generalise this idea and to construct an isometry, we relax the assumption that \(A\) is a three dimensional Hilbert space. We re-express/replace the operations in \(T, U, V\) which act on the \(A'\) space by linear combinations of monomials in \(\{\Pi_i\}_{i=1}^{5}\).

We obtain the coefficients used in these linear combinations by assuming the space \(A'\) is three dimensional. The idea is simply that this map reduces to a swap operation when we re-impose the assumptions and for cases close to it, we expect it to behave appropriately. We describe this procedure more precisely below.

**Algorithm 4** (Constructing an isometry). Let
- \(A'\) be a three-dimensional Hilbert space spanned by an orthonormal basis \(\{|0⟩_{A'}, |1⟩_{A'}, |2⟩_{A'}\}\),
- \(\rho^{KCBS}, \{\Pi_i^{KCBS}\}_{i=1}^{5}\) be an ideal KCBS configuration (see Definition 3) on \(A'\),
- \(A\) be a Hilbert space with dimension at least 3 containing orthonormal vectors \(\{|\bar{0}\rangle_A, |\bar{1}\rangle_A, |\bar{2}\rangle_A\}\),
- \(\rho, \{\Pi_i\}_{i=1}^{5}\) be an arbitrary quantum realisation defined on \(A\).

Define \(T, U, V\) as in Equation IV.5 and let \(S^{''}_{\text{SWAP}} := TUVU\) with the following changes. Let
\[ W^{KCBS} := \{\{\Pi_i^{KCBS}\}_{i=1}^{5}, \{\Pi_i^{KCBS}\Pi_j^{KCBS}\}_{i,j=1}^{5}, \ldots \} \]
and
\[ W := \{\{\Pi_i\}_{i=1}^{5}, \{\Pi_i\Pi_j\}_{i,j=1}^{5}, \ldots \} \]
be the set of “words” formed by the KCBS projectors and those of the arbitrary quantum realisation, respectively.

1. **Translation operator:**
   (a) Express \(P_{A'}\) as a linear combination of elements in \(W\), i.e., \(P_{A'} = \sum_{l \in W_{KCBS}} \alpha_l^{KCBS} \).
   (b) Define \(P_A := \sum_{l \in W} \alpha_l I\).

2. **Basis projectors:** Formally replace, in \(V\), the operators
   (a) \(|\bar{0}\rangle_{A'}\) by \(\Pi_1\),
   (b) \(|\bar{1}\rangle_{A'}\) by \(\Pi_2\), and
   (c) \(|\bar{2}\rangle_{A'}\) by \((I - \Pi_1)(I - \Pi_2)\).
Thus, \( V \) now becomes \( \Pi_1 \otimes I_{A'} + \Pi_2 \otimes P_{A'}^{-1} + (\Pi - \Pi_1)(\Pi - \Pi_2) \otimes P_{A'}^{-2} \).

We found an explicit linear combination for step 1 (a) of Algorithm 4.\(^{18}\) Thus, the algorithm always succeeds at constructing \( S'_\text{SWAP} \). We must show that \( S'_\text{SWAP} \) is in fact an isometry. This is important because of the following reason. Recall that our objective was to lower bound the fidelity given in Equation (II.2) of the main text. To this end, we said that there is some solution (which we expect should also work reasonably). Combining these, we can construct \( S'_\text{SWAP} \) is not an isometry. In fact, \( P_A \) as produced by the algorithm is not necessarily unitary (viz. \( P_A^T P_A = I_A \) may not hold).

To address this, we use the localising matrix technique introduced in [47]. Let \( \hat{P}_A \) be unitary matrix satisfying \( PP \geq 0 \), where we dropped the subscript for clarity. Consider the case where \( P \) is not unitary. In that case, one can use polar decomposition to write \( P = |P|U \) (not to be confused with the \( U \) above; where \( |P| \geq 0 \) and \( UU = I \) ) so choosing \( \hat{P} = U^\dagger \) satisfies \( PP \geq 0 \). Thus for each \( P \), the constraint can be satisfied. Consider the other case, i.e., where \( P = U \) is unitary. Then,\(^{19}\) \( \hat{P} = U^\dagger \). Thus, in the ideal case, we recover the same unitary and for the case close to ideal, we are guaranteed that there is some solution (which we expect should also work reasonably). Combining these, we can construct \( S \), which is an isometry.

**Lemma 5** (\( S \) is indeed an isometry). Let \( S'_\text{SWAP} \) be the map produced by Algorithm 4 and define \( S \text{SWAP} \) to be \( S'_\text{SWAP} \) with \( P_A \) replaced by \( \hat{P}_A \). Then \( S \text{SWAP} \) is an isometry if the following conditions hold

\[
\hat{P}_A^\dagger \hat{P}_A = I_A, \\
\hat{P}_A \hat{P}_A \geq 0.
\]

**Proof.** It suffices to show that \( \langle \psi|_{A',A} S_{\text{SWAP}}^I S_{\text{SWAP}}^I_{A',A} |\psi\rangle_{A',A} = 1 \) for all normalised \( |\psi\rangle_{A',A} \). We express \( S_{\text{SWAP}} = TUV \), where \( T \) is as in Equation IV.5, \( U := \sum_{k=0}^{2} \hat{P}_A^\dagger \otimes |k\rangle \langle k|_{A'} \), and \( V := \Pi_1 \otimes I_{A'} + \Pi_2 \otimes P_{A'}^{-1} + (\Pi - \Pi_1)(\Pi - \Pi_2) \otimes P_{A'}^{-2} \).

Observe that \( T^\dagger T = I_{A',A} = U^\dagger U \) since \( \hat{P}_A^\dagger \hat{P}_A = I_A \). Further, we have that

\[
V^\dagger V = \Pi_1 \otimes I_{A'} + \Pi_2 \otimes I_{A'} + (\Pi - \Pi_1)(\Pi - \Pi_2) \otimes I_{A'}.
\]

Hence, \( S_{\text{SWAP}}^I S_{\text{SWAP}}^I = I_{A,A'} \) establishing that \( S \) is in fact unitary and thus also an isometry. \( \square \)

We can now combine all the pieces to write the final optimisation problem we solve. We use \( G(\{a_i\}) \) to denote the set of all letters.

**Algorithm 6** (The SDP for lower bounding the fidelity of a given realisation with the ideal KCBS realisation). The algorithm proceeds in two parts.

**Notation:** Let

- \( \mathcal{A} \) represent an arbitrary Hilbert space and \( \mathcal{A}' \) represent a three dimensional Hilbert space,
- \( \mathcal{W} \) be the set of "words" constructed using \( \{\Pi_i\}_{i=1}^5 \), \( \hat{P} \) and \( \hat{P}^\dagger \), i.e., \( \mathcal{W} = G(\{\Pi_i\}_{i=1}^5, \hat{P}, \hat{P}^\dagger) \), and
- define \( \langle w \rangle := tr_{\mathcal{A}}(pw) \) and assume\(^{20}\) \( \rho = |\psi\rangle \langle \psi| \) so that \( \langle w \rangle = \langle \psi| w |\psi\rangle \) for all \( w \in \mathcal{W} \).

\(^ {18}\) Using prior results, we expect one can prove the existence of such a linear combination, but we do not pursue this here.

\(^ {19}\) To see this, write the polar decomposition of \( \hat{P} = |\hat{P}| E \) (where \( |\hat{P}| \geq 0 \) and \( E^\dagger E = I \)). Then, \( \hat{P}U = |\hat{P}| EU \), which is a polar decomposition of \( \hat{P}U \). The polar decomposition of a positive semi-definite matrix \( M \) always has the form \( M\mathbb{I} \). Using \( M = \hat{P}U \), and identifying \( EU \) with \( I \), we have \( E = U^\dagger \).

\(^ {20}\) Without loss of generality, one can purify a state by increasing the dimension and have the operators leave that space unaffected (for any given quantum realisation).
Input:

- (Implicit) \( \Pi_i, \Pi_j = 0 \) for all \( i, j \in E(G) \), where \( G \) is a five cycle graph and \( E \) are its edges, indexed \([1, 2, \ldots, 5]\).
- Observed statistics:\( \sum_i p_i = \sum_i \langle \Pi_i \rangle = c \).

Evaluation | Part 1.

- Evaluate \( S_{SWAP} \) as described in Lemma 5 using Algorithm 4.
- Define the objective function \( f \) as
  \[
  f \left( \rho, \{\Pi_i\}_{i=1}^5 \right) = \sum_{i=1}^5 F \left( tr_A \left[ S_{SWAP} (\Pi_i \rho_A \Pi_i \otimes |0\rangle \langle 0|_{\mathcal{A}'}) S_{SWAP}^\dagger \right], \Pi_i^{KCBS} \rho_{\mathcal{A}'}, \Pi_i^{KCBS} \right)
  \]
  \[
  + F \left( tr_A \left[ S_{SWAP} (\rho_A \otimes |0\rangle \langle 0|_{\mathcal{A}'}) S_{SWAP}^\dagger \right], \rho_{\mathcal{A}'}, \Pi_i^{KCBS} \right)
  \]
  and evaluate the coefficients \( f_w \) so that
  \[
  f = \sum_{w \in \mathcal{W}} f_w \langle w \rangle.
  \]
- Again, from Algorithm 4, evaluate \( P_A \) as a linear combination of \( \langle w \rangle \).

Evaluation | Part 2. Solve the following SDP:

\[
F_{\text{noiseless}} = \min_{\{\langle w \rangle\}_{w \in \mathcal{W}}} \sum_{w \in \mathcal{W}} f_w \langle w \rangle
\]

s.t. \( \Gamma^{(k)}(\Pi) \geq 0 \quad \because \text{all gram matrices are } \geq 0 \)

\[
\Gamma^{(k)}(\Pi)_{v,w} = \Gamma^{(k)}(\Pi)_{v',w'}
\]

\[
\Gamma^{(k)}(\hat{P}_A P_A) \geq 0
\]

\[
\Gamma^{(k)}(\hat{P}_A P_A)_{v,w} = \Gamma^{(k)}(\hat{P}_A P_A)_{v',w'}
\]

\[
\sum_{i=1}^5 \langle \Pi_i \rangle = c \quad \text{(observed statistic)}
\]

where \( \Gamma^{(k)}(X) \) is a matrix which is

- indexed by letters \( w \),
- whose matrix elements are given by \( \Gamma^{(k)}(X)_{v,w} = \langle \psi | v^\dagger X w | \psi \rangle \),
- where \( k \) defines the maximum number of letters that appear in the words \( w \) which index the matrix \( \Gamma^{(k)} \), and,

where in the first two equality constraints, we use the following relations:

\[21\] To obtain a better bound, one can add more fine-grained statistics as well such as the values of \( p_i \) individually for each \( i \).

\[22\] This was done using symbolic computation.
\[ \Pi_i \Pi_j = 0 \text{ for all } i,j \in E(G) \text{ and} \]
\[ \hat{P}_A^1 \hat{P}_A = \hat{P}_A \hat{P}_A^1 = I_A. \]

**Output:** \( F_{\text{noiseless}}(c) \).

**Remark 7.** Note that \( \hat{P} \hat{P} \geq 0 \implies \Gamma^{(k)}(\hat{P} \hat{P}) \geq 0 \). This follows readily by letting \( A^\dagger A = \hat{P} \hat{P} \) for some \( A \) (which must exist for any positive semi-definite matrix; one can use spectral decomposition). Then \( \Gamma^{(k)}(A^\dagger A) \) is a Gram matrix and thus \( \geq 0 \).

**Remark 8.** We solved this SDP with \( \langle w \rangle \) restricted to being real, but it has been shown that this is without loss of generality (see, e.g., §V.A in [44]).

We thus have an algorithm which can calculate the required lower bound on fidelity, given the observed value of the KCBS operator.

### B. Experimental setup

The calcium ions, in which two dark states and one bright state are chosen to encode the states \{|1\}, \{|2\}\} and \{|0\}, respectively. Every experimental sequence starts with 1 ms Doppler cooling using a 397 nm laser and a resonant 866 nm laser. The 397 nm laser is red detuned approximately half a natural linewidth from resonant with the cycling transition between \( S_{1/2} \) and \( P_{1/2} \) manifolds. This is followed by 300 \( \mu s \) electromagnetically-induced transparency (EIT) cooling sequence which cools the ion down to the motional ground state. After that, 10 \( \mu s \) optical pumping laser is applied to initialise the qutrit to the \{|0\} state with 99.5% fidelity. When needed, 729 nm pulse sequence is applied to prepare a certain initial state. Measurements of the observables \{\( A_i \}\} are performed through coherent rotations \( R_2(\theta_2, \phi_2) R_1(\theta_1, \phi_1) \), a fluorescence detection followed by the operation \( R_1^\dagger(\theta_1, \phi_1) R_2^\dagger(\theta_2, \phi_2) \) which undoes the previous rotation. The first fluorescence detection lasts for 220 \( \mu s \) and uses laser settings close to those of Doppler cooling, to minimise the motional heating due to photon recoil (in case of a bright state). However, this brings the temperature of the bright state close to the Doppler limit. Therefore, a 150 \( \mu s \) EIT cooling sequence followed by 10 \( \mu s \) optical pumping pulses is applied to cool the bright state ion. The detection and cooling time are greatly suppressed to minimise the random phase accumulation between the sequential measurement. Neither fluorescence detection nor EIT cooling process affects the temperature of a dark state ion, which is slightly heated at a rate of 140 quanta per second due to electronic noise. The second fluorescence detection uses resonant laser pulse and 300 \( \mu s \) integrating time, which lowers detection error. The result is acquired by counting the number of photons collected from photo multiplier tube (PMT) within the detection time. The statistical probability is calculated by repeating the same measurement 10,000 times.

In our experiments the 2\( \pi \) pulse time for both transitions are adjusted to around 142 \( \mu s \); that is, the Rabi frequency is as low as \( \Omega_{1/2} = (2\pi)7 \) KHz, making the AC-Stark shift below 100 Hz. The separation between \{|1\} and \{|2\} is \( \omega_2 - \omega_1 = (2\pi)8.69 \) MHz with corresponding magnetic field \( B = 5.18 \) G. The maximum probability of off-resonant excitation \( \Omega^2/(\omega_2 - \omega_1)^2 \) is about \( 6.5 \times 10^{-7} \), small enough to ensure the independence of each Rabi oscillation [48, 49].

### C. Analysing the data

**The data.** The complete dataset can be accessed on GitHub [50], which was summarised in Table II. For the normal (reverse) ordered case, the results are plotted in Figure II.1 (Figure S1 in SM [35]).

**Why two curves?** As noted earlier, there are two robustness curves the aforementioned figures. We now detail why. Notice that the observed statistic constraint in the SDP corresponding to Algorithm 6 can be tightened by specifying the value of each \( \langle \Pi_i \rangle \) term. Obviously, if one specifies the value of \( \langle \Pi_i \rangle \), the value for their sum automatically gets fixed. Based on the experimental data, we have access to the value of each of the \( \langle \Pi_i \rangle \) and thus we can always obtain a tighter
bound compared with the bound obtained via the sum constraint in the SDP for Algorithm 6. We illustrate this by plotting the robustness curve obtained in the special case $p_1 = p_2 = p_3 = p_4 = p_5$ ($p_i$ and (II) are interchangeable). One could have just as easily taken a different choice for the values of $p_i$ such that their sum remains equal to the appropriate KCBS value and obtain a different robustness curve. All such curves, obtained by providing the value for $p$s, will be lower bounded by the curve obtained via the sum constraint (the blue curve). For our experimental data point with mean $\mu$ and standard deviation $\sigma$, we base our analysis on $\mu - 1.96\sigma$, which is the smallest possible value with 95 percent confidence for a normally distributed data.

Analyzing the $p$-configuration. As mentioned above, we base our analysis on $\mu - 1.96\sigma$ for the appropriate values of $\mu$ and $\sigma$. This, however, has consequences on the constraint that we impose via the observed statistics. For our experimental data, we observe that $\sum_i (\mu (p_i) - 1.96\sigma (p_i))$ is upper bounded by $\mu (\sum_i p_i) - 1.96\sigma (\sum_i p_i)$. Since our robustness curves are very sensitive to minor changes near the region of maximum KCBS value ($\sum_i p_i$), the lower bound on the fidelity provided by the sum constraint can be better than the (nearly) equal statistic constraint ($p_1 \approx p_2 \approx p_3 \approx p_4 \approx p_5$). Since our goal is to provide tight lower bounds, we take the largest value, which is the one obtained from sum constraint close to the region of maximum KCBS value. Away from the maximum KCBS value region, (nearly) equal statistic constraint provides a better estimate (as is evident from the plots in Figure II.1). We also computed the fidelity of these quantum realisations to the ideal KCBS configuration by performing state and measurement tomography. We found that the self-testing lower bounds are satisfied.

Results for $p$-configuration. For $p = 0.0, 0.1, and 0.2$, we obtained $\sum_k p_k$ to be 2.233, 2.186, and 2.118, respectively for the normal ordered case. By solving the SDP outputted by Algorithm 6 with these values as inputs, the self-testing lower bounds on the total fidelity of these realisations to the KCBS configuration are 5.296, 3.002, and 2.343 respectively. For the reverse ordered experiments the corresponding values for $\sum_k p_k$ are 2.236, 2.182, and 2.124, respectively. The self-testing lower bound on the total fidelity for these cases were 5.892, 2.933, and 2.386 respectively. On the other hand, conventional tomography yielded 5.965, 5.901, and 5.812 respectively. The values are same for normal and reverse ordered experiments (because an experiment being normal or reverse is determined by quantum random number generator and has no explicit difference otherwise at the level of measurements and the state involved). As expected, the total fidelity obtained from conventional tomography is indeed above by the lower bound on it, obtained using our self-test.

Analyzing the $\theta$-configuration. To obtain the self-test lower bounds, we proceeded as before. However, finding a lower bound on the fidelity using conventional tomography, is slightly more involved in this case. The idea is to first find the fidelity between the experimental setup and the $\theta$ configuration and then between $\theta$ configuration and the KCBS configuration (up to an isometry). Using a form of a triangle inequality, one can lowerbound the total fidelity.

In more detail, our goal is to find the total fidelity of the experimentally realised configuration with a configuration which is related to the KCBS configuration via an isometry. In the previous case, this isometry was an identity matrix (a trivial isometry). Since the optimal configuration is unique up to an isometry, any configuration which is related to the KCBS configuration via an isometry can be considered an optimal configuration. Our goal is to calculate the total fidelity of the experimental realisation of $\{|u_0^E\rangle \langle u_0^E|, \{|u_1^E\rangle \langle u_1^E|\}_{i=1}^5\}$, say $(\rho_0^E, \{M_i^E\}_{i=1}^5)$ to an optimal configuration, say $(\{|u_0^O\rangle \langle u_0^O|, \{|u_1^O\rangle \langle u_1^O|\}_{i=1}^5\})$. Let us denote the fidelity of $|u_i^E\rangle$ to $|u_i^O\rangle$ as $F_{i}^{E,O}$. Here, $F_{i}^{E,O}$ denotes the fidelity of the $i$th component of the experimental realisation to that of the ideal configuration. Similarly, other fidelities are denoted by $F_{i}^{E,\theta}$ and $F_{i}^{\theta,O}$. We know that fidelity is not a valid metric, and hence, we will not be able to apply triangle inequality directly. However, we can use trace distance as a proxy to relate the aforementioned three configurations. After some simple calculation, we obtain the following expression for the lower bound on the total fidelity $\left(\sum_{i=0}^{5} F_{i}^{E,O}\right)$ (see SM [35] for details).

$$\sum_{i=0}^{5} F_{i}^{E,I} \geq 6 - \left(\sum_{i=0}^{5} \sqrt{1 - F_{i}^{E,\theta}}\right) - \left(\sum_{i=0}^{5} \sqrt{1 - F_{i}^{\theta,O}}\right).$$  (IV.15)
Based on the experimental data, we can calculate $\left( \sum_{i=0}^{5} \sqrt{1 - F_{i}^{E,\theta}} \right)$. The second total fidelity expression $\left( \sum_{i=0}^{5} \sqrt{1 - F_{i}^{\theta,O}} \right)$ can be evaluated using numerical optimization.

**Results for the $\theta$-configuration.** We obtained $\sum_{k} p_{k}$ to be 2.058 and 2.043, respectively, for the normal ordered case. For the reverse ordered experiments, the corresponding values were 2.057 and 2.048, respectively. The self-testing lower bound on the total fidelity for the normal ordered case was 2.561, 2.222 and the corresponding values for the reverse ordered case were 2.579 and 2.579, respectively. Conventional tomography, on the other hand, yielded 3.956, 4.050, respectively (for both normal normal and reverse order). Again, the self-testing lower bounds are satisfied, as expected.

**D. Numerics to evaluate fidelity lower bounds**

As previously stated, obtaining the numerical solution was quite involved, owing to the fact that the description of the semidefinite program we obtain is implicit. Consequently, one first needs to find this explicit description through symbolic computation and then solve the resulting semidefinite program. After performing the symbolic computation to find the objective and constraints, we solve an SDP over a $192 \times 192$ matrix with 16,859 constraints. The terms in the objective function must appear in the SDP matrix in order for us to impose appropriate constraints. This is because the optimisation program would otherwise be undefined. The unusually large size of the SDP matrices (compared to similar self-test schemes) reflects the complexity of the objective function in our case, which would have been difficult to obtain without symbolic computation. To capture all the terms that appear in the objective, we needed words with three letters (the matrices involved scale exponentially in the number of letters). Further, we require 769 localising matrix constraints.

We used Jupyter notebooks (based on python) as our programming environment. We used sympy for symbolic computations and cvxpy for translating the resulting SDP into an instance which MOSEK (an SDP solver) could solve. Our implementation is available on GitHub.

**ACKNOWLEDGEMENTS**

This work was supported by the National Key Research and Development Program of China (No. 2017YFA0304100, No. 2021YFE0113100), NSFC (No. 11734015, No. 11874345, No. 11821404, No. 11904357, No. 12174367, No. 11904402, No. 12074433, No. 12174447, No. 12004430, and No. 12174448), Innovation Program for Quantum Science and Technology (No. 2021ZD0301200), the Fundamental Research Funds for the Central Universities, USTC Tang Scholarship, Science and Technological Fund of Anhui Province for Outstanding Young (2008085J02). AC is supported by Project Qdisc (Project No. US-15097, Universidad e Sevilla), with FEDER funds, QuantERA grant SECRET, by MINECO (Project No. PCI2019-111885-2), MICINN (Project No. PID2020-113738GB-I00), and by the EU-funded FoQaCiA project. LCK thanks the Ministry of Education, Singapore and the National Research Foundation Singapore for their support. KB acknowledges funding by AFOSR, DoE QSA, NSF QLCI (award No. OMA-2120757), DoE ASCR Accelerated Research in Quantum Computing program (award No. DE-SC0020312), NSF PFCQC program, the DoE ASCR Quantum Testbed Pathfinder program (award No. DE-SC0019040), U.S. Department of Energy Award No. DE-SC0019449, ARO MURI, AFOSR MURI, and DARPA SAVaN T ADVENT. ASA acknowledges funding provided by the Institute for Quantum Information and Matter. A substantial part of the work was done while ASA was at the Université Libre de Bruxelles and was supported by the Belgian Fonds pour la Formation à la Recherche dans l’Industrie 4959 et dans l’Agriculture - FRIA, under grant No. 1.E.081.17F. ASA and JR were supported by the Belgian Fonds de la Recherche Scientifique – FNRS, under grant no R.50.05.18.F (QuantAlgo). The QuantAlgo project has received funding from the QuantERA European Research Area Network (ERA-NET) Cofund in Quantum Technologies implemented within the European Union’s Horizon 2020 program. We would like to express our gratitude to Jonathan Lau for his logistical assistance with computer-related matters. We
thank Tobias Haug for various discussions.

[1] Ivan H Deutsch. Harnessing the power of the second quantum revolution. *PRX Quantum*, 1(2):020101, 2020.
[2] Jens Eisert, Dominik Hangleiter, Nathan Walk, Ingo Roth, Damian Markham, Rhea Parekh, Ulysse Chabaud, and Elham Kashefi. Quantum certification and benchmarking. *Nature Reviews Physics*, 2(7):382–390, 2020.
[3] Ryan O’Donnell and John Wright. Efficient quantum tomography. In *Proceedings of the forty-eighth annual ACM symposium on Theory of Computing*, pages 899–912, 2016.
[4] J. Ignacio Cirac, David Pérez-García, Norbert Schuch, and Frank Verstraete. Matrix product states and projected entangled pair states: Concepts, symmetries, theorems. *Rev. Mod. Phys.*, 93:045003, Dec 2021.
[5] Dominic Mayers and Andrew Yao. Self testing quantum apparatus. *Quantum Info. Comput.*, 4(4):273–286, July 2004.
[6] Boris S Tisre’son. Quantum analogues of the bell inequalities. the case of two spatially separated domains. *Journal of Soviet Mathematics*, 36(4):557–570, 1987.
[7] Stephen J Summers and Reinhard Werner. Bell’s inequalities and quantum field theory. i. general setting. *J. Math. Phys.*, 28(10):2440–2447, 1987.
[8] Sandu Popescu and Daniel Rohrlich. Generic quantum nonlocality. *Phys. Lett. A*, 166(5-6):293–297, 1992.
[9] Samuel I Braunstein, Ady Mann, and Michael Revzen. Maximal violation of bell inequalities for mixed states. *Physical Review Letters*, 68(22):3259, 1992.
[10] Dominic Mayers and Andrew Yao. Quantum cryptography with imperfect apparatus. In *Proceedings 39th Annual Symposium on Foundations of Computer Science (Cat. No. 98CB36280)*, pages 503–509. IEEE, 1998.
[11] Ivan Šupić and Joseph Bowles. Self-testing of quantum systems: a review. *Quantum*, 4:337, 2020.
[51] Aaron Meurer, Christopher P. Smith, Mateusz Paprocki, Ondřej Čertík, Sergey B. Kirpichev, Matthew Rocklin, AMiT Kumar, Sergiu Ivanov, Jason K. Moore, Sartaj Singh, Thilina Rathnayake, Sean Vig, Brian E. Granger, Richard P. Muller, Francesco Bonazzi, Harsh Gupta, Shivam Vats, Fredrik Johansson, Fabian Pedregosa, Matthew J. Curry, Andy R. Terrel, Štěpán Roučka, Ashutosh Saboo, Isuru Fernando, Sumith Kulal, Robert Cimrman, and Anthony Scopatz. Sympy: symbolic computing in python. PeerJ Computer Science, 3:e103, January 2017.

[52] Steven Diamond and Stephen Boyd. CVXPY: A Python-embedded modeling language for convex optimization. Journal of Machine Learning Research, 17(83):1–5, 2016.

[53] Akshay Agrawal, Robin Verschueren, Steven Diamond, and Stephen Boyd. A rewriting system for convex optimization problems. Journal of Control and Decision, 5(1):42–60, 2018.
Supplementary Files

This is a list of supplementary files associated with this preprint. Click to download.

- Kweksupp.pdf