nature physics

Article

https://doi.org/10.1038/s41567-024-02584-z

All real projective measurements can be self-tested

Received: 8 July 2023

Accepted: 12 June 2024

Published online: 1 August 2024

Check for updates

Ranyiliu Chen [1] ✉, Laura Mančinska[1] & Jurij Volčič [2]

Entangled quantum systems feature non-local correlations that are stronger than could be realized classically. This property makes it possible to perform self-testing, the strongest form of quantum functionality verification, which allows a classical user to deduce the quantum state and measurements used to produce a given set of measurement statistics. While self-testing of quantum states is well understood, self-testing of measurements, especially in high dimensions, remains relatively unexplored. Here we prove that every real projective measurement can be self-tested. Our approach employs the idea that existing self-tests can be extended to verify additional untrusted measurements, known as post-hoc self-testing. We formalize the method of post-hoc self-testing and establish the condition under which it can be applied. Using this condition, we construct self-tests for all real projective measurements. We build on this result to develop an iterative self-testing technique that provides a clear methodology for constructing new self-tests from pre-existing ones.

Consider a scenario where a classical user, Victor, engages with a quantum device by posing questions $x \in \mathcal{I}$ and receiving answers $a \in \mathcal{O}$, where $\mathcal{I}$ and $\mathcal{O}$ are two finite sets of labels. Lacking any prior knowledge of the device's internal workings, Victor models its behaviour as a state preparation $|\psi\rangle$, accompanied by quantum measurements $\{M_{a|x}, \sum_a M_{a|x} = I\}$ where I is the identity matrix. In response to question x, the device executes measurement $\{M_a|_x\}_a$ on the state $|\psi\rangle$ and outputs the resulting measurement output a. While it is straightforward to predict the device's output statistics from $|\psi\rangle$ and $\{M_{a|x}\}$ using Born's rule[1] $p(a|x) = \langle\psi|M_{a|x}|\psi\rangle$, it is impossible to deduce $|\psi\rangle$ and $\{M_{a|x}\}$ solely from the statistics $p(a|x)$. Indeed, different states $|\psi\rangle$ and $\{M_{a|x}\}$ can yield the same $p(a|x)$. In this setting, even a classical computer is always able to simulate the quantum process, if its running time is not limited.

Intriguingly, deducing the quantum functionality from the resulting classical statistics becomes possible in the so-called bipartite Bell scenario[2,3] (Fig. 1). Here, Victor interacts with two spatially separated quantum devices, named Alice and Bob. He poses questions $x \in \mathcal{I}_A$ and $y \in \mathcal{I}_B$ to Alice and Bob respectively, who in turn provide answers, $a \in \mathcal{O}_A$ and $b \in \mathcal{O}_B$. While Alice and Bob cannot communicate during this interaction, they may share an entangled quantum state $|\psi\rangle_{AB}$, which they can measure locally using measurements $\{M_{a|x} : a \in \mathcal{O}_A, x \in \mathcal{I}_A\}$ and $\{N_{b|y} : b \in \mathcal{O}_B, y \in \mathcal{I}_B\}$ to obtain outputs a and b. The statistics observed by Victor then follow the distribution $p(a,b|x,y) = \langle\psi|M_{a|x} \otimes N_{b|y}|\psi\rangle$. Some statistics $p(a,b|x,y)$ can exclusively be produced by a specific set of measurements $\{M_{a|x}\}$ and $\{N_{b|y}\}$ on a specific entangled state $|\psi\rangle_{AB}$ (up to a change of a local frame of reference). This phenomenon is known as self-testing[4] and it relies on key features of quantum theory such as entanglement[5] and incompatibility of measurements[6]. Self-testing represents the strongest form of verification as it requires minimal assumptions, namely, no-communication between Alice's and Bob's measuring devices and the validity of the quantum theory. In particular, in self-testing we do not require access to any trusted or fully characterized quantum devices, a condition also known as device independence[7].

The quantum mechanical description of the devices in a bipartite Bell scenario is given by what we call a strategy. Formally, such a strategy $\mathcal{S}$ is a tuple:

$$\mathcal{S} = \left(|\psi\rangle_{AB}, \{M_{a|x} : a \in \mathcal{O}_A, x \in \mathcal{I}_A\}, \{N_{b|y} : b \in \mathcal{O}_B, y \in \mathcal{I}_B\}\right),$$

where $|\psi\rangle_{AB} \in \mathcal{H}_A \otimes \mathcal{H}_B$ is the shared state and $\mathcal{M}_x = \{M_{a|x}\} \subseteq \mathcal{L}(\mathcal{H}_A)$ and $\mathcal{N}_b = \{N_{b|y}\} \subseteq \mathcal{L}(\mathcal{H}_B)$ are the positive operator-valued measures

[1]QMATH, Department of Mathematical Sciences, University of Copenhagen, Copenhagen, Denmark. [2]Department of Mathematics, Drexel University, Philadelphia, PA, USA. ✉e-mail: rc@math.ku.dk

https://doi.org/10.1038/s41567-024-02584-z

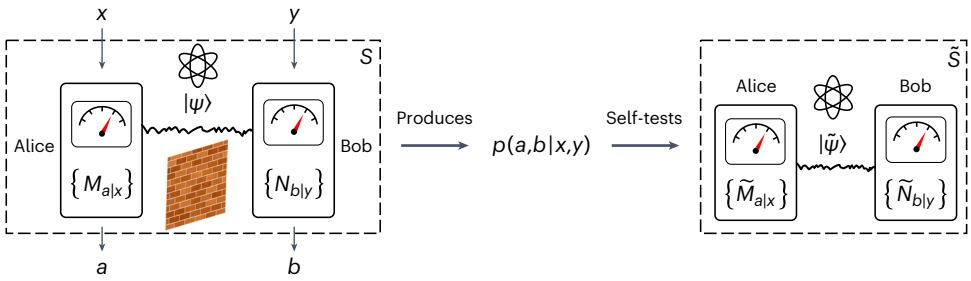

Fig. 1 | Self-testing in a Bell scenario. Spatially separated, Alice and Bob perform local measurements on a shared state (left, described by $\mathcal{S}$), giving rise to correlation $p(a,b|x,y)$. In the case of self-testing (right), Victor can classically verify Alice and Bob: the only way for Alice and Bob to produce the correct correlation is by adhering to the prescribed specification $\tilde{\mathcal{S}}$.

(POVMs) of Alice and Bob respectively. Here $\mathcal{H}_A/\mathcal{H}_B$ denotes the Hilbert space of Alice/Bob, and $\mathcal{L}(\mathcal{H})$ is the space of linear operators on $\mathcal{H}$. The resulting measurement statistics:

$$p(a,b|x,y) = \langle\psi|M_{a|x} \otimes N_{b|y}|\psi\rangle$$

is commonly referred to as correlation. In self-testing, we can recover the description of the state and measurements comprising $\mathcal{S}$ from merely observing the measurement statistics p that it produces. So whenever self-testing holds, we can verify the involved state-preparation and measurement functionalities without any prior knowledge of the inner workings of the employed quantum devices. This leads us to the following fundamental question of self-testing:

Question. *Which quantum states and which measurements can be self-tested?*

In other words, the above question asks which state-preparation and measurement functionalities can be verified by a classical user with no access to trusted quantum devices. To verify (self-test) a given state-preparation or measurement functionality, we need to construct a strategy $\mathcal{S}$ that incorporates this functionality and is moreover determined (self-tested) by the correlation it produces.

In the bipartite scenario, the question regarding self-testable states has been answered by a milestone result[8] that allowed any pure bipartite entangled state to be self-tested. Recent work showed that in the network setting[9] it is possible to self-test any entangled multiparty state[10]. In contrast to this relatively complete picture for self-testing of quantum states, the self-testing of general measurements has remained elusive. Existing protocols primarily focus on low-dimensional quantum systems or specific higher-dimensional measurements. In the case of a two-level system, we know how to self-test Pauli measurements[4], and subsequent work has shown that any two-dimensional projective measurement is self-testable[11]. In refs. 12,13 tensor-products of Pauli matrices were self-tested, and ref. 14 presented a self-test for a particular pair of d-output measurements. In refs. 15,16, constant-sized self-testing of measurements satisfying some special property is demonstrated. The verification of measurements has also been considered in more general scenarios, including verification of POVM measurements in one-sided device-independent settings[17] and verification of entangled measurements in structured networks[18]. Self-testing of arbitrary higher-dimensional measurements in the standard bipartite Bell scenario, however, has remained out of reach.

The issue of complex measurements

If a strategy uses complex measurements (measurements with complex matrix entries in a Schmidt basis of the shared state), we can take the complex conjugate to obtain a different strategy that yields the same statistics:

$$\left\langle\psi|\overline{M}_{a|x} \otimes \overline{N}_{b|y}|\psi\right\rangle = \langle\psi|M_{a|x} \otimes N_{b|y}|\psi\rangle\,.$$

In general, the complex conjugated strategy $(|\psi\rangle_{AB}, \{\overline{M}_{a|x}\}, \{\overline{N}_{b|y}\})$ cannot be obtained from the original strategy by a local change of basis. Unlike a change of reference frame, complex conjugation does not have a natural physical interpretation. Hence, complex conjugation is a fundamental obstruction to the verification of complex measurements in the strongest possible sense in the standard two-party Bell scenario. To verify complex measurements, the usual approach is to weaken the self-testing definition and consider equivalence up to both the change of local frame of reference and the complex conjugate[19–22]. More generally, this approach aligns with the concept of convex self-testing[23], allowing Alice and Bob to employ a convex combination of strategies (in the case of self-testing strategies with complex entries, a reference strategy and its complex conjugate). In this work our goal is to identify which measurements can be verified (self-tested) in the strongest form—that is, only up to a change of local frame of reference, which is not met by complex measurements. A recent work[24] showed that only projective measurements fulfil this strict self-testing criterion. Our findings therefore offer a comprehensive self-testing protocol for all measurements that are potentially self-testable.

In this work we study the self-testing of measurements in a comprehensive (as opposed to example-based) manner, and provide initial general results for self-testing of measurements. Our specific contributions include the following:

First, we put forth a fully explicit self-testing protocol for any real projective measurement. Our construction has a question set of cubic size in d, the dimension of the measurement to be self-tested, and a constant-sized answer set. Our self-test is also robust to noise.

Second, we formalize the method of post-hoc self-testing and identify the condition for its application. Post-hoc self-testing occurs when we can extend a previously self-tested strategy to include an additional measurement. While there are sporadic examples of this method in the literature, a comprehensive understanding of this phenomenon and when it occurs was lacking. To remedy this, we identified a condition under which an initial self-test of a given $\mathcal{S}$ can be extended to include an additional $\mathcal{M}$. Applying this criterion to an initial strategy from recent work[15] allows us to obtain our explicit self-testing construction for any real projective measurement.

Finally, we develop a new technique of iterative self-testing that involves the sequential application of post-hoc self-testing. Starting from any established self-test, we use Jordan algebra to characterize the set of measurements that can be verified via iterative self-testing. Iterative self-testing is inspired by the formalization of post-hoc self-testing, and offers a way of developing new self-tests based on pre-existing ones.

Set-up

The observable picture of measurements

In many cases, especially when the measurement is projective (that is, all operators in the POVMs are projections), it can be more convenient to work with generalized observables than with operators of POVMs.

Given a POVM $\{M_a : a \in [0, |\mathcal{O}_A| - 1]\}$, its generalized observables are contractions given by:

$$A^{(j)} := \sum_{a=0}^{|\mathcal{O}_A|-1} \omega^{aj} M_a, j \in [0, |\mathcal{O}_A| - 1]$$

where $\omega = e^{i2\pi/|\mathcal{O}_A|}$. Note that $\{M_a\}$ can be recovered from $\{A^{(j)}\}$ by $M_a = \frac{1}{|\mathcal{O}_A|}\sum_{j=0}^{|\mathcal{O}_A|-1} \omega^{-aj} A_x^{(j)}$. So $\{A^{(j)}\}$ provides an alternative, yet full, description of the measurement $\{M_a\}$. One important property of generalized observables is that a measurement $\{M_a\}$ is projective if, and only if, the corresponding $A := A^{(1)}$ is a unitary matrix of order $|\mathcal{O}_A|$ (see ref. 25 for a proof; here, the order of A is the smallest integer n such that $A^n = I$). In this case $A^{(j)} = A^j$ is the jth power of A, implying that every projective measurement $\{M_a\}$ is fully characterized by a single operator $A = \sum_a \omega^a M_a$. Therefore, we call A the observable of $\{M_a\}$ whenever $\{M_a\}$ is a projective measurement.

In this work we specify quantum strategies by the tuple:

$$\mathcal{S} = \left(|\psi\rangle_{AB}, \left\{A_x^{(j)} : x \in \mathcal{I}_A, j \in \mathcal{O}_A\right\}, \left\{B_y^{(k)} : y \in \mathcal{I}_B, k \in \mathcal{O}_B\right\}\right),$$

where $A_x^{(j)} = \sum_{a=0}^{|\mathcal{O}_A|-1} \omega_A^{aj} M_{a|x}$, $\omega_A = e^{i2\pi/|\mathcal{O}_A|}$, $B_y^{(k)} = \sum_{b=0}^{|\mathcal{O}_B|-1} \omega_B^{bk} N_{b|y}$ and $\omega_B = e^{i2\pi/|\mathcal{O}_B|}$. The correlation is also conveniently specified via

$$\left\{\left\langle\psi\middle|A_x^{(j)} \otimes B_y^{(k)}\middle|\psi\right\rangle\right\}_{j,k,x,y} = \left\{\sum_{a,b} \omega_A^{aj}\omega_B^{bk} p(ab|xy)\right\}_{j,k,x,y}.$$

Furthermore, we call $\mathcal{S}$ projective if all the measurements in $\mathcal{S}$ are projective, and denote it by $\mathcal{S} = (|\psi\rangle_{AB}, \{A_x : x \in \mathcal{I}_A\}, \{B_y : y \in \mathcal{I}_B\})$ for simplicity. In this work we shall present our results in terms of observables.

Self-testing

In a self-testing protocol the verifier Victor wishes to infer the underlying quantum strategy from his observation of correlations, so it is desired that the strategy generating a given correlation is to some extent unique. However, there are at least two types of manipulation of the strategy that do not affect the correlation. First, if we only choose a different basis, then strategies $\mathcal{S} = (|\psi\rangle_{AB}, \{A_x^{(j)}\}, \{B_y^{(k)}\})$ and $\mathcal{S}' = (U_A \otimes U_B|\psi\rangle_{AB}, \{U_A A_x^{(j)} U_A^\dagger\}, \{U_B B_y^{(k)} U_B^\dagger\})$ produce the same correlation for any local unitaries U_A, U_B. Second, if we attach a bipartite auxiliary state $|\text{aux}\rangle_{A'B'}$ on which the measurements act trivially, then strategies $\mathcal{S} = (|\psi\rangle_{AB}, \{A_x^{(j)}\}, \{B_y^{(k)}\})$ and $\mathcal{S}' = (|\text{aux}\rangle_{A'B'} \otimes |\psi\rangle_{AB}, \{I \otimes A_x^{(j)}\}, \{I \otimes B_y^{(k)}\})$ produce the same correlation. Motivated by the above two manipulations, we say that $\tilde{\mathcal{S}}$ is a local dilation of $\mathcal{S}$ if up to a change of local bases $\mathcal{S}$ is $\tilde{\mathcal{S}}$ plus some trivial auxiliary state. We are now ready to define self-testing.

Definition 1. A strategy $\tilde{\mathcal{S}} = (|\tilde{\psi}\rangle, \{\tilde{A}_x^{(j)}\}, \{\tilde{B}_y^{(k)}\})$ is self-tested if any strategy $\mathcal{S} = (|\psi\rangle, \{A_x^{(j)}\}, \{B_y^{(k)}\})$ producing the same correlation as $\tilde{\mathcal{S}}$ must be locally dilated to $\tilde{\mathcal{S}}$; that is, up to change of local bases, $A_x^{(j)} = I \otimes \tilde{A}_x^{(j)}$, $B_y^{(k)} = I \otimes \tilde{B}_y^{(k)}$ and $|\psi\rangle = |\text{aux}\rangle \otimes |\tilde{\psi}\rangle$ for some auxiliary state $|\text{aux}\rangle$.

Results

We begin by presenting our main result: the self-testing of any real projective measurement. Next, we introduce the methodology employed to establish this result and outline its proof. Lastly, we propose the method of iterative self-testing and offer a criterion for its application.

Self-testing of any real projective measurement

We now show how to self-test an arbitrary real projective measurement. Specifically, we construct the following self-tested strategy:

Theorem 1. *Let $|\Phi_d\rangle = \sum_{j=0}^{d-1} |jj\rangle/\sqrt{d}$ be the (canonical) maximally entangled state in dimension d. For any $d \geq 2$, we construct d-dimensional binary observables $\tilde{T}_0, \ldots, \tilde{T}_{d(d+1)/2}$ such that for any d-dimensional real projective measurement given by its observable $\tilde{O}$, the strategy:*

$$\tilde{S} = \left(|\phi_d\rangle, \overbrace{\{\tilde{T}_0, \ldots, \tilde{T}_d, \tilde{O}\}}^{\text{Alice's measurements}}, \overbrace{\{\tilde{T}_0, \ldots \tilde{T}_d, \tilde{T}_{d+1}, \ldots, \tilde{T}_{d(d+1)/2-1}\}}^{\text{Bob's measurements}}\right)$$

is self-tested.

The binary observables $\tilde{T}_0, \ldots, \tilde{T}_{d(d+1)/2-1}$ correspond to rank-1 projections coming from vectors forming the standard $(d+1)$-simplex centred at the origin (their explicit construction is described in Supplementary Section 3.1). But let us briefly discuss a few key points about Theorem 1. First, the observables $\{\tilde{T}_j\}$ are independent of the specific d-dimensional observable $\tilde{O}$ that Victor wishes to self-test, as long as d is fixed. One can therefore simultaneously incorporate several new projective measurements. Second, all $\tilde{T}_j$ are binary measurements (have two outputs), which means that the size of the question set $\mathcal{I}_A \times \mathcal{I}_B$ is in $O(d^3)$, while the answer set is constant-sized. Third, the self-test from Theorem 1 is robust to noise: if a strategy produces a correlation close to that of $\tilde{\mathcal{S}}$, then it must be close to $\tilde{\mathcal{S}}$ up to a basis change and enlargement by some trivial auxiliary state. The robust version of Theorem 2 can be found in Supplementary Section 2.2.

Condition for post-hoc self-testing

The concept of post-hoc self-testing has been implicitly employed in previous works, such as self-testing of graph states[26], randomness certification[27,28] and one-sided self-testing[17,29]. A review paper[30] summarized this technique and referred to it as post-hoc self-testing. In this section, we formalize the idea of post-hoc self-testing and establish the necessary condition for its application.

In post-hoc self-testing we consider a scenario where we have self-tested strategy $\tilde{\mathcal{S}} = (|\tilde{\psi}\rangle, \{\tilde{A}_x^{(j)}\}_x, \{\tilde{B}_y^{(k)}\}_y)$, and we would like to self-test an additional measurement $\{\tilde{O}^{(\ell)}\}$, where ℓ denotes the outcome of the additional measurement. We are interested to ask when $\{\tilde{O}^{(\ell)}\}$ can be self-tested by extending $\tilde{\mathcal{S}}$. In particular, when is $\tilde{\mathcal{S}}' = (|\tilde{\psi}\rangle, \{\tilde{A}_x^{(j)}\}_x, \{\tilde{B}_y^{(k)}, \tilde{O}^{(\ell)}\}_y)$ self-tested by the correlation it produces (Fig. 2)? As $\tilde{\mathcal{S}}$ is self-tested, Alice has to honestly perform some measurement that is a local dilation of $\{\tilde{A}_x^{(j)}\}$, producing correlations $\{\langle\tilde{\psi}|(\tilde{A}_x^{(j)} \otimes \tilde{O}^{(\ell)})|\tilde{\psi}\rangle\}_x$ between $\tilde{A}_x^{(j)}$ and $\tilde{O}^{(\ell)}$. Now if $\{\langle\tilde{\psi}|(\tilde{A}_x^{(j)} \otimes \tilde{O}^{(\ell)})|\tilde{\psi}\rangle\}_x$ can fully characterize $\{\tilde{O}^{(\ell)}\}$ for all ℓ then Bob also has no choice but to honestly perform a local dilation of $\tilde{O}^{(\ell)}$, and $\tilde{S}'$ remains self-tested consequently. Whether $\{\langle\tilde{\psi}|\tilde{A}_x^{(j)} \otimes \tilde{O}^{(\ell)}|\tilde{\psi}\rangle\}_x$ fully characterizes $\tilde{O}^{(\ell)}$ will depend on $\{\tilde{A}_x^{(j)}\}$, $|\tilde{\psi}\rangle$, and $\tilde{O}^{(\ell)}$. The following theorem provides a criterion for post-hoc self-testing when the measurements are projective.

Theorem 2. *A criterion for post-hoc self-testing. Let $\tilde{\mathcal{S}} = (|\tilde{\psi}\rangle, \{\tilde{A}_x\}_x, \{\tilde{B}_y\}_y)$ be a self-tested projective strategy, and let $\tilde{O}$ be the observable of an L-output projective measurement. Then $\tilde{\mathcal{S}}' = (|\tilde{\psi}\rangle, \{\tilde{A}_x\}_x, \{\tilde{B}_y, \tilde{O}\}_y)$ remains self-tested, if the following holds: for each $\ell \in [0, L-1]$, there exists a positive-definite operator P_ℓ such that:*

$$\overline{\tilde{O}^\ell} P_\ell \in \text{span}_{\mathbb{C}}\left\{D\tilde{A}_x^j D : x, j\right\}, \quad (1)$$

where D is the diagonal matrix $D = \text{diag}(\lambda_1, \ldots, \lambda_d)$, and λ_j are the Schmidt coefficients of $|\tilde{\psi}\rangle$.

https://doi.org/10.1038/s41567-024-02584-z

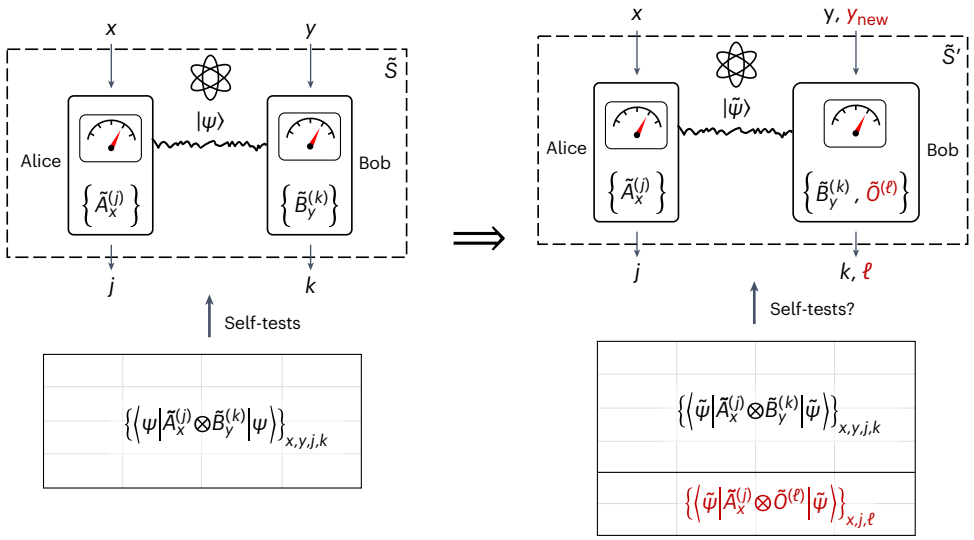

Fig. 2 | Post-hoc self-testing. Starting from a self-tested strategy $\tilde{S}$ (left), if it is feasible to infer the new measurement $\tilde{O}^{(\ell)}$ with input y_{new} and output ℓ from correlations $\{\langle\psi|A_x^{(j)} \otimes O^{(\ell)}|\psi\rangle\}$, then extended strategy $\tilde{S}'$ (right) remains self-tested.

The key steps towards Theorem 2 are twisting the tracial inner product between operators with D, inducing a conformal pairing of vectors with P_ℓ and then leveraging the metric properties of observables and isometries to recover $\tilde{O}^{(\ell)}$. While the positive definite P_ℓ renders condition (1) nonlinear, its existence can be determined via semi-definite optimization.

While condition (1) can be checked through a semi-definite program, the existential nature of Theorem 2 can make it cumbersome to work with in some applications. To address this issue, we present a closed-form variant of Theorem 2 for the special case where $|\tilde{\psi}\rangle = |\boldsymbol{\Phi}_d\rangle$ is the maximally entangled state and $\tilde{A}_x$ and $\tilde{O}$ are binary measurements. This particular form not only facilitates the proof of Theorem 1, but also proves useful in the context of iterative self-testing.

Proposition 3. *A closed-form criterion for post-hoc self-testing. Let* $\tilde{S} = (|\Phi_d\rangle, \{\tilde{A}_x\}_x, \{\tilde{B}_y\}_y)$ *be a self-tested projective strategy where* $\{\tilde{A}_x\}_x$ *are binary, and let* $\tilde{O}$ *be the observable of a binary real projective measurement. Then* $\tilde{S}' = (|\tilde{\psi}\rangle, \{\tilde{A}_x\}_x, \{\tilde{B}_y, \tilde{O}\}_y)$ *remains self-tested whenever*:

$$\tilde{O} \in \text{sgn}\,(\text{span}_{\mathbb{R}}\{I, \tilde{A}_x : x\}),$$

where sgn *is the extension of the sign function via functional calculus. Namely, it is given by* $\text{sgn} : H = \sum_j \lambda_j |v_j\rangle\langle v_j| \mapsto \sum_j \text{sgn}(\lambda_j)|v_j\rangle\langle v_j|$ *where* $\{|v_j\rangle\}_j$ *is an orthonormal basis of eigenvectors for* H.

The proofs of Theorem 2 and Proposition 3 can be found in the Supplementary Information. We note that the sgn function is crucial, as it produces observables outside the span.

Proof outline of Theorem 1

The self-testing result of Theorem 1 follows by applying Proposition 3 to an initial self-tested strategy chosen from ref. 15. Specifically, in ref. 15 the authors show that the strategy:

$$\tilde{S}^{(0)} = \left(|\Phi_d\rangle, \{\tilde{T}_x\}_{x=0}^{d}, \{\tilde{T}_y\}_{y=0}^{d}\right)$$

is robustly self-tested. Here $\tilde{T}_j$ are certain binary observables, the same as the ones in Theorem 1. We introduce the following additional observables for Bob:

$$\{\tilde{T}_y\}_{y=d+1}^{\frac{d(d+1)}{2}-1} = \{\text{sgn}\,(\tilde{T}_j + \tilde{T}_k) : 1 \le j < k \le d\} \setminus \{\text{sgn}\,(\tilde{T}_1 + \tilde{T}_2)\}.$$

We then use Proposition 3 to conclude that the extended strategy:

$$\tilde{S}^{(1)} = \left(|\Phi_d\rangle, \{\tilde{T}_x\}_{x=0}^{d}, \{\tilde{T}_y\}_{y=0}^{\frac{d(d+1)}{2}-1}\right)$$

remains self-tested.

Next we show that the observables on Bob's side from strategy $\tilde{S}^{(1)}$ span the space of all $d \times d$ symmetric matrices. Therefore, for any binary observable $\tilde{O}_{\text{binary}}$, we have $\tilde{O}_{\text{binary}} \in \text{sgn}\,(\text{span}_{\mathbb{R}}\{I, \tilde{T}_y\}_{y=0}^{\frac{d(d+1)}{2}-1})$. By incorporating $\tilde{O}$ into Alice's set of observables, the strategy:

$$\tilde{S}^{(2)} = \left(|\Phi_d\rangle, \{\tilde{T}_x, \tilde{O}_{\text{binary}}\}_{x=0}^{d}, \{\tilde{T}_y\}_{y=0}^{\frac{d(d+1)}{2}-1}\right)$$

remains self-tested. Finally, if any binary observable can be self-tested, then any multiple-output one can also be self-tested by regarding it as a collection of binary observables. Specifically, given any L-output observable $\tilde{O} = \sum_{a=0}^{L-1} e^{i2\pi a/L}\tilde{M}_a$, consider binary observables $\{2\tilde{M}_a - I\}_{a=0}^{L-1}$. As every binary observable $2\tilde{M}_a - I$ can be self-tested, $\tilde{O}$ can be self-tested as well. This holds for any $L \ge 2$, so we conclude that:

$$\tilde{S}^{(3)} = \left(|\Phi_d\rangle, \{\tilde{T}_x, \tilde{O}\}_{x=0}^{d}, \{\tilde{T}_y\}_{y=0}^{\frac{d(d+1)}{2}-1}\right)$$

is self-tested for any d-dimensional real projective measurement $\tilde{O}$, thus finishing the proof of Theorem 1.

Iterative self-testing

In the proof of Theorem 1 we sequentially applied post-hoc self-testing two times to get the final self-testing protocol. In general, given initial strategy $\tilde{S} = (\Phi_d, \{\tilde{A}_x\}, \{\tilde{B}_y\})$, if we post-hoc self-test $\tilde{O} \in \text{sgn}\,(\text{span}\{I, \tilde{A}_x\})$ on Bob's side, then we can use $\{\tilde{B}_y, \tilde{O}\}$ to post-hoc self-test another measurement $\tilde{O}' \in \text{sgn}\,(\text{span}\{I, \tilde{B}_y, \tilde{O}\})$ for Alice. By doing this in several rounds, starting from a small set of observables $\{\tilde{A}_x\}$ we may eventually self-test many additional observables. We call this process iterative self-testing. A priori it is unclear exactly which measurements can be reached starting from a fixed self-tested strategy $\tilde{S}$ after many rounds of iterative self-testing. The main goal of this section is to provide an easy-to-use criterion for a measurement $\tilde{O}$ to be reachable after an arbitrary number of rounds of iterative self-testing.

Given an initial strategy $\tilde{\mathcal{S}} = (|\Phi_d\rangle, \{\tilde{A}_x\}, \{\tilde{B}_y\})$, let S_j be the set of binary observables that can be obtained in the jth iteration of post-hoc self-testing via Proposition 3. Note that $S_1 = \mathrm{sgn}\,(\mathrm{span}_{\mathbb{R}}\{I, \tilde{A}_x : x\})$ and $S_{j+1} = \mathrm{sgn}\,(\mathrm{span}_{\mathbb{R}}(S_j))$ for $j \geq 1$. Furthermore, we have $S_j \subseteq S_{j+1}$ since $\mathrm{sgn}\,(\tilde{O}) = \tilde{O}$ for any binary observable $\tilde{O}$. Therefore, by iteratively using this technique, we enlarge the set of self-tested binary observables, S_j, in each step.

Define $V_j := \mathrm{span}_{\mathbb{R}}(S_j)$. Then $\{V_j\}_j$ is an increasing sequence of subspaces of the finite-dimensional real Hermitian matrix space, $H_d(\mathbb{R})$, and eventually stabilizes at $V_\infty = \lim_{j\to\infty} V_j$. Given initial binary observables $\{\tilde{A}_x\}, \{\tilde{B}_y\}$, it is natural to ask: what is V_∞? In the Supplementary Information we show that V_∞ is the real Jordan algebra generated by $\{\tilde{A}_x\}$ (ref. 31). Recall that a (unital) Jordan algebra is a vector subspace of an associative algebra that contains the identity and is closed under the Jordan product $a \star b = \frac{1}{2}(ab + ba)$.

This yields the following theorem:

Theorem 4. *Let $\tilde{\mathcal{S}} = (|\Phi_d\rangle, \{\tilde{A}_x\}, \{\tilde{B}_y\})$ be a self-tested strategy using maximally entangled state and binary real projective measurements. A binary real projective measurement $\tilde{O}$ can be iteratively self-tested if $\tilde{O} \in \mathcal{JA}(\{\tilde{A}_x\})$, where $\mathcal{JA}(\{\tilde{A}_x\})$ is the real Jordan algebra generated by $\{\tilde{A}_x\}$. Moreover, the upper bound on the number of the iterations is determined by $\lceil 2\log_2 d \rceil$.*

To argue about many-output (rather than just binary-output) measurements, we can proceed in a manner similar to that used in the proof of Theorem 1. This leads us to conclude that every L-output measurement $\{\tilde{M}_\ell, \ell \in [0, L-1]\}$ satisfying:

$$\tilde{M}_\ell \in \mathcal{JA}(\{\tilde{A}_x\}) \quad \forall \ell \in [0, L-1]$$

can be iteratively self-tested when starting from a self-tested strategy $\tilde{\mathcal{S}}$. In particular, if $\mathcal{JA}(\{\tilde{A}_x\}) = H_d(\mathbb{R})$, *that is* $\{\tilde{A}_x\}$ generates the whole real Jordan algebra of symmetric $d \times d$ matrices, then every d-dimensional measurement can be self-tested. We show that the condition $\mathcal{JA}(\{\tilde{A}_x\}) = H_d(\mathbb{R})$ is equivalent to $\{\tilde{A}_x\}$ having a trivial centralizer, which can be checked efficiently.

Discussion

We have addressed the problem of self-testing an arbitrary real projective measurement by constructing a self-testing protocol using binary measurements and maximally entangled states. Our protocol remains the same for any real projective measurement, provided that the dimension d is fixed. The protocol has a $O(d^3)$-sized question set and a constant-sized answer set. We show that our protocol is, in principle, robust. While the obtained robustness could be sufficient for further theoretical results, our analysis is not tight enough to tolerate realistic noise in current experiments. To obtain experimentally relevant robustness, one should perform a tailored analysis of a carefully selected set-up, as it is highly unlikely that any analysis that applies to arbitrary set-ups will ever be sufficiently tight for experimental purposes.

Another contribution of this work is the technique of iterative self-testing. This offers a convenient method for establishing new self-tests based on pre-existing ones. Our results show that the set of self-testable observables includes the real Jordan algebra generated by the observables that we use for iterative self-testing.

We leave a few open questions and improvements for future work. Now that we know that all real projective measurements can be self-tested, one outstanding challenge is to enhance the efficiency—specifically, the size and robustness of the protocols. It is known that some high-dimensional states and measurements admit constant-sized self-tests (for example, see refs. 15,16 and refs. 14,32 with constant-sized question sets). Is it the case that all states and measurements can be self-tested by a constant-sized protocol? Another open question is whether numerical techniques, such as the numerical swap method[33], could yield better robustness estimates when our protocol is applied to concrete target measurements. This could have applications in verifiable distributed quantum computation[34].

Lastly, from a theoretical standpoint, iterative self-testing is applicable to strategies with partially entangled states, but the underlying algebraic structure remains to be understood. It would also be interesting to explore beyond the two-party Bell scenario and investigate whether there are more general scenarios that allow self-testing of complex measurements in a stronger sense, for example, where only a measurement and its conjugate are allowed but not any combination of them[35,36].

Online content

Any methods, additional references, Nature Portfolio reporting summaries, source data, extended data, supplementary information, acknowledgements, peer review information; details of author contributions and competing interests; and statements of data and code availability are available at https://doi.org/10.1038/s41567-024-02584-z.

References

1. Born, M. On the quantum mechanics of collisions. *Z. Phys.* **37**, 863–867 (1926).
2. Brunner, N., Cavalcanti, D., Pironio, S., Scarani, V. & Wehner, S. Bell nonlocality. *Rev. Mod. Phys.* **86**, 419–478 (2014).
3. Bell, J. S. On the Einstein Podolsky Rosen paradox. *Phys. Phys. Fiz.* **1**, 195–200 (1964).
4. Mayers, D. & Yao, A. Self testing quantum apparatus. *Quantum Inf. Comput.* **4**, 273–286 (2004).
5. Gisin, N. & Peres, A. Maximal violation of Bell's inequality for arbitrarily large spin. *Phys. Lett. A* **162**, 15–17 (1992).
6. Wolf, M. M., Perez-Garcia, D. & Fernandez, C. Measurements incompatible in quantum theory cannot be measured jointly in any other no-signaling theory. *Phys. Rev. Lett.* **103**, 230402 (2009).
7. Acín, A. et al. Device-independent security of quantum cryptography against collective attacks. *Phys. Rev. Lett.* **98**, 230501 (2007).
8. Coladangelo, A., Goh, K. T. & Scarani, V. All pure bipartite entangled states can be self-tested. *Nat. Commun.* **8**, 15485 (2017).
9. Tavakoli, A., Pozas-Kerstjens, A., Luo, M.-X. & Renou, M.-O. Bell nonlocality in networks. *Rep. Progr. Phys.***85**, 056001 (2022).
10. Šupić, I., Bowles, J., Renou, M.-O., Acín, A. & Hoban, M. J. Quantum networks self-test all entangled states. *Nat. Phys.* **19**, 670–675 (2023).
11. Yang, T. H. & Navascués, M. Robust self-testing of unknown quantum systems into any entangled two-qubit states. *Phys. Rev. A* **87**, 050102(R) (2013).
12. McKague, M. Self-testing in parallel with CHSH. *Quantum* **1**, 1 (2017).
13. Coladangelo, A. Parallel self-testing of (tilted) EPR pairs via copies of (tilted) CHSH and the magic square game. *Quantum Inf. Comput.* **17**, 831–865 (2017).
14. Sarkar, S., Saha, D., Kaniewski, J. & Augusiak, R. Self-testing quantum systems of arbitrary local dimension with minimal number of measurements. *npj Quantum Inf.* https://doi.org/10.1038/s41534-021-00490-3 (2021).
15. Mančinska, L., Prakash, J. & Schafhauser, C. Constant-sized robust self-tests for states and measurements of unbounded dimension. Preprint at https://arxiv.org/abs/2103.01729 (2021).
16. Fu, H. Constant-sized correlations are sufficient to self-test maximally entangled states with unbounded dimension. *Quantum* **6**, 614 (2022).
17. Sarkar, S., Saha, D. & Augusiak, R. Certification of incompatible measurements using quantum steering. *Phys. Rev. A* **106**, 040402 (2022).

18. Renou, M. O., Kaniewski, J. & Brunner, N. Self-testing entangled measurements in quantum networks. *Phys. Rev. Lett.* **121**, 250507 (2018).
19. McKague, M. & Mosca, M. in *Theory of Quantum Computation, Communication, and Cryptography* (eds Dam, W. et al.) 113–130 (Springer, 2011).
20. Acín, A., Pironio, S., Vértesi, T. & Wittek, P. Optimal randomness certification from one entangled bit. *Phys. Rev. A* **93**, 040102 (2016).
21. Bowles, J., Šupić, I., Cavalcanti, D. & Acín, A. Self-testing of pauli observables for device-independent entanglement certification. *Phys. Rev. A* **98**, 042336 (2018).
22. Jain, R., Miller, C. A. & Shi, Y. Parallel device-independent quantum key distribution. *IEEE Trans. Inf. Theory* **66**, 5567–5584 (2020).
23. Mančinska, L., Nielsen, T. G. & Prakash, J. Glued magic games self-test maximally entangled states. Preprint at https://arxiv.org/abs/2105.10658 (2021).
24. Baptista, P. et al. A mathematical foundation for self-testing: lifting common assumptions. Preprint at https://arxiv.org/abs/2310.12662 (2023).
25. Kaniewski, J. et al. Maximal nonlocality from maximal entanglement and mutually unbiased bases, and self-testing of two-qutrit quantum systems. *Quantum* **3**, 198 (2019).
26. McKague, M. Interactive proofs for BQP via self-tested graph states. *Theory Comput.* https://doi.org/10.4086/toc.2016.v012a003 (2016).
27. Andersson, O., Badziag, P., Dumitru, I. & Cabello, A. Device-independent certification of two bits of randomness from one entangled bit and Gisin's elegant bell inequality. *Phys. Rev. A* **97**, 012314 (2018).
28. Woodhead, E. et al. Maximal randomness from partially entangled states. *Phys. Rev. Res.* **2**, 042028 (2020).
29. Sarkar, S. et al. Self-testing of any pure entangled state with the minimal number of measurements and optimal randomness certification in a one-sided device-independent scenario. *Phys. Rev. Appl.* **19**, 034038 (2023).
30. Šupić, I. & Bowles, J. Self-testing of quantum systems: a review. *Quantum* **4**, 337 (2020).
31. Jacobson, N. *Structure and Representations of Jordan Algebras* Colloquium Publications Vol. 39 (American Mathematical Society, 1968).
32. Šupić, I., Cavalcanti, D. & Bowles, J. Device-independent certification of tensor products of quantum states using single-copy self-testing protocols. *Quantum* **5**, 418 (2021).
33. Yang, T. H., Vértesi, T., Bancal, J.-D., Scarani, V. & Navascués, M. Robust and versatile black-box certification of quantum devices. *Phys. Rev. Lett.* **113**, 040401 (2014).
34. Reichardt, B. W., Unger, F. & Vazirani, U. Classical command of quantum systems. *Nature* **496**, 456–460 (2013).
35. Renou, M.-O. et al. Quantum theory based on real numbers can be experimentally falsified. *Nature* **600**, 625–629 (2021).
36. Sarkar, S., Orthey, A. C. Jr & Augusiak, R. A universal scheme to self-test any quantum state and measurement. Preprint at https://arxiv.org/abs/2312.04405 (2023).

Data availability
This work does not have any associated data.

Acknowledgements
This work is funded by the European Research Council under grant agreement number 101078107 (QInteract) (L.M.), QuantERA project under grant agreement number 101017733 (VERIqTAS) (R.C. and L.M.), VILLUM FONDEN via QMATH Centre of Excellence grant number 10059 (R.C., L.M. and J.V.), Villum Young Investigator grant number 37532 (R.C., L.M. and J.V.) and NSF grant number DMS-1954709, DMS-2348720 (J.V.).

Author contributions
R.C., L.M. and J.V. conceived the idea, crafted the proofs and prepared the manuscript.

Competing interests
The authors declare no competing interests.

Additional information
Supplementary information The online version contains supplementary material available at https://doi.org/10.1038/s41567-024-02584-z.

Correspondence and requests for materials should be addressed to Ranyiliu Chen.

Peer review information *Nature Physics* thanks the anonymous reviewers for their contribution to the peer review of this work.