arXiv:2306.13498v2 [quant-ph] 15 Mar 2024

Constant-sized self-tests for maximally entangled states and single local projective measurements

Jurij Volčič

Department of Mathematics, Drexel University, Pennsylvania

Self-testing is a powerful certification of quantum systems relying on measured, classical statistics. This paper considers self-testing in bipartite Bell scenarios with small number of inputs and outputs, but with quantum states and measurements of arbitrarily large dimension. The contributions are twofold. Firstly, it is shown that every maximally entangled state can be self-tested with four binary measurements per party. This result extends the earlier work of Mančinska-Prakash-Schafhauser (2021), which applies to maximally entangled states of odd dimensions only. Secondly, it is shown that every single local binary projective measurement can be self-tested with five binary measurements per party. A similar statement holds for self-testing of local projective measurements with more than two outputs. These results are enabled by the representation theory of quadruples of projections that add to a scalar multiple of the identity. Structure of irreducible representations, analysis of their spectral features and post-hoc self-testing are the primary methods for constructing the new self-tests with small number of inputs and outputs.

1 Introduction

Thanks to non-locality of quantum theory, unknown non-communicating quantum devices measuring an unknown shared entangled state can sometimes be identified based on classical statistic of their outputs. This phenomenon is called *self-testing*, and is the strongest form of device-independent certification of quantum systems. Self-testing was introduced in [20], and has been a heavily studied subject ever since; see [26] for a comprehensive review of major advances on this topic. The immense interest attracted by self-testing originates from its applications in device-independent quantum cryptography [1, 12], delegated quantum computation [11],

Jurij Volčič: jurij.volcic@drexel.edu, Supported by the NSF grant DMS-1954709.

randomness generation [22, 2], entanglement detection [5], and computational complexity [13, 17]. For experimental developments, see [16, 25].

This paper focuses on self-testing in bipartite Bell scenarios [6], where two parties randomly perform measurements on a shared quantum state without communicating. From these measurements, joint probability distribution of inputs and outputs of both parties can be constructed as classical data describing the system. Suppose that each party can perform N measurements, each of them with K outcomes. Borrowing terminology from quantum games, we model this setup with bipartite quantum *strategies*. Namely, an N-input K-output strategy $\mathcal{S}$ of two parties (subsystems) A and B consists of a bipartite quantum state $|\psi\rangle$ in the tensor product of Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$, a measurement $(\mathcal{M}_{i,a})_{a=1}^K$ of positive operators on $\mathcal{H}_A$ for each $i = 1, \dots, N$, and a measurement $(\mathcal{N}_{j,b})_{b=1}^K$ of positive operators on $\mathcal{H}_B$ for each $j = 1, \dots, N$. The *correlation* of $\mathcal{S}$ is the array p of probabilities given by the Born rule $p(a, b|i, j) = \langle\psi| \mathcal{M}_{i,a} \otimes \mathcal{N}_{j,b} |\psi\rangle$, and is the classically observable data induced by $\mathcal{S}$. There are two trivial modifications of the strategy $\mathcal{S}$ that do not affect its correlation: one is a unitary change of local bases, and the other is extending the state with an ancillary state on which the measurements act trivially. If any other strategy with correlation p is obtained from $\mathcal{S}$ using these trivial modifications, then we say that $\mathcal{S}$ is *self-tested* by p. That is, the state and measurements in a self-tested strategy are essentially uniquely determined by the correlation. The most renowned example of a self-tested strategy (with 2 inputs and 2 outputs) consists of maximally entangled qubits and two pairs of Pauli measurements, which give the maximal quantum violation of the famous CHSH inequality [8, 28, 20].

The following is a fundamental self-testing problem:

($\star$) *Which states and which measurements can be self-tested, i.e., appear in a strategy that is self-tested by its correlation? Furthermore, how complex is such a strategy, e.g., how many inputs and outputs per party are required?*

The breakthrough on ($\star$) for quantum states was achieved in [10], where the authors showed that every entangled bipartite state can be self-tested. The number of inputs in the provided self-tests *grows with the local dimension* n of the quantum state under investigation, which makes these self-tests rather complicated in large dimensions. The existence result of [10] was later not only extended to multipartite states in quantum networks [27] and refined in one-sided device-independent scenarios [23], but also improved in terms of inputs and outputs needed to self-test certain states. In [24], the authors show that an n-dimensional maximally entangled bipartite state can be self-tested using 2 inputs and n outputs. The paper [14] was the first to provide *constant-sized* self-tests for some infinite families of maximally entangled states of *even* dimension (but not constant-sized self-tests for all maximally entangled states of even dimension). This result was complemented by [19], where the authors establish that maximally entangled state of *any odd* dimension can be self-tested using 4 inputs and 2 outputs.

In comparison with states, the progress on ($\star$) for measurements has been more constrained. All two-dimensional projective measurements have been self-tested [29], and likewise tensor products of Pauli measurements [21, 9]. Recently, it has been established that every projective measurement can be self-tested [7]. Actually, the self-tests derived in [7] allow for arbitrary real ensembles of projective measurements to be self-tested simultaneously. However, self-testing an n-dimensional projective measurement in this manner requires roughly n^2 inputs.

Contributions

This paper provides self-tests for *all maximally entangled states* and *all single local projective measurements*, respectively, that are *uniform* in number of both inputs and outputs. The first main result concerns maximally entangled states.

Theorem A (Corollary 5.4)**.** Maximally entangled bipartite state of any local dimension d can be self-tested using 4 inputs and 2 outputs.

The strategies of Theorem A are given in Definition 5.1. Their construction and self-testing feature arises from the one-parametric family of universal C*-algebras $\mathcal{A}_{2-\frac{1}{n}}$ generated by four projections adding up to $2-\frac{1}{n}$ times the identity. Remarkable results about representations of these algebras were established by Kruglyak-Rabanovich-Samoĭlenko using Coxeter functors between representation categories [18]. Their theory is essential in the proof of Theorem A. Representations of C*-algebras of this type have already been leveraged in [19]. However, their work uses a different family of parameters ($2-\frac{2}{n}$ for odd n, instead of $2-\frac{1}{n}$ for natural n) that leads to simple C*-algebras, and maximally entangled states of odd dimensions only. On the other hand, exploiting algebras $\mathcal{A}_{2-\frac{1}{n}}$ for self-testing purposes requires a more sophisticated analysis of their representations, but applies to all maximally entangled states.

The second main result of this paper provides constant-sized self-tests for single local projective measurements with 2 outputs, i.e., *binary* projective measurements. Note that a local binary projective measurement $(P, I-P)$ is, up to unitary change of local basis, given by a real matrix, and determined by the dimension n and the rank r of the projection P.

Theorem B (Corollary 5.11)**.** A single local binary projective measurement of any dimension n and rank r appears in a 5-input 2-output strategy that is self-tested by its correlation.

See Definition 5.9 for the explicit strategies used in Theorem B. A generalization of Theorem B for local non-binary projective measurements is given in Corollary 5.13. It is important to stress both the significance and the limitation of Theorem B. Given a single projective measurement, Theorem B provides a small self-testing strategy that contains this measurement. Note that up to a choice of coordinate

system, a given projective measurement always admits a real matrix presentation. However, Theorem B does not address self-testing of *ensembles* of projective measurements; from this perspective, it is weaker than [7], which provides (large) self-tests for all real ensembles of projective measurements. The strategies of Theorem B are obtained from the strategies of Theorem A by the principle of *post-hoc self-testing* [26]. A broad sufficiency criterion for applicability of post-hoc self-testing was presented in [7]. To apply this criterion in the proof of Theorem B, certain spectral aspects of representations of $\mathcal{A}_{2-\frac{1}{n}}$ need to be resolved. Namely, we determine the spectrum of the sum of pairs of projections arising from representations of $\mathcal{A}_{2-\frac{1}{n}}$.

While the derivation of the newly presented self-tests might seem rather abstract, the resulting correlations admit closed-form expressions, and the corresponding strategies can recursively constructed using basic tools from linear algebra (see Appendix A for examples).

Reader's guide

Section 2 reviews the standard terminology and notation on quantum strategies and self-testing. Section 3 presents a construction of four $n \times n$ projections that add to $2 - \frac{1}{n}$ times identity, and their basic properties; these projections are central to this paper, and provide local projective measurements for the new self-tested strategies. Section 4 establishes certain spectral results about these projections, which are critical for demonstrating self-testing in this paper. While this section provides the main new mathematical insight into what is required to establish the new self-testing results, a reader only interested in main statements may skip this section. Section 5 presents the new self-tested strategies and their correlations. Section 6 addresses obstructions to constant-sized self-testing of arbitrary entangled states and pairs of projective measurements. Lastly, Appendix A explicitly constructs the distinguished projections appearing in self-tests for local dimensions up to 6.

Acknowledgments

The author thanks Ken Dykema for inspiring conversations about self-testing, and Ricardo Gutierrez-Jauregui for sharing his expertise on experimental aspects of quantum theory.

2 Preliminaries

This section introduces notation and terminology on quantum strategies and self-testing, following the conventions presented in [19]. For a comprehensive overview, see [26].

Let $K \in \mathbb{N}$. A K-tuple of operators $(P_a)_{a=1}^K$ acting on a Hilbert space $\mathcal{H}$ is a *positive operator-valued measure (K-POVM)* if $P_a \succeq 0$ and $\sum_{a=1}^K P_a = I$. If all P_a are projections, then $(P_a)_{a=1}^K$ is a *projection-valued measure (K-PVM)*, or a *projective measurement*. Note that, up to a unitary basis change, a PVM $(P_a)_{a=1}^K$ is uniquely determined by the ranks $\operatorname{rk} P_a$ for $a = 1, \dots, K$. That is, every K-PVM with ranks of projections $r_1, \dots, r_K$ is unitarily equivalent to

$$\left(I_{r_1} \oplus 0_{r_2+\cdots+r_K}, 0_{r_1} \oplus I_{r_2} \oplus 0_{r_3+\cdots+r_K}, \dots, 0_{r_1+\cdots+r_{K-1}} \oplus I_{r_K}\right).$$

A 2-POVM is also called a *binary* measurement. Observe that a binary PVM is simply a pair $(P, I-P)$ where P is a projection, and is determined by the dimension and the rank of P up to a unitary basis change.

A *(pure bipartite) state* $|\psi\rangle$ is a unit vector in $\mathcal{H}_A \otimes \mathcal{H}_B$, where $\mathcal{H}_A, \mathcal{H}_B$ are Hilbert spaces. We say that $|\psi\rangle$ has *full Schmidt rank* if $P \otimes I |\psi\rangle = I \otimes Q |\psi\rangle = 0$ for some projections P, Q implies $P = 0$ and $Q = 0$. In this case, the Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$ are isomorphic. For $n \in \mathbb{N}$, the (canonical) *maximally entangled state* of local dimension n is $|\phi_n\rangle = \frac{1}{\sqrt{n}} \sum_{i=1}^n |i\rangle|i\rangle \in \mathbb{C}^n \otimes \mathbb{C}^n$. For $A, B \in \mathrm{M}_n(\mathbb{C})$,

$$\langle \phi_n | A \otimes B |\phi_n\rangle = \tau(AB^{\mathrm{t}}) = \frac{1}{n} \operatorname{tr}(AB^{\mathrm{t}}),$$

where τ denotes the normalized trace on $\mathrm{M}_n(\mathbb{C})$.

Let $K_A, K_B, N_A, N_B \in \mathbb{N}$. An (N_A, N_B)*-input* (K_A, K_B)*-output bipartite quantum strategy* $\mathcal{S}$ is a triple

$$\mathcal{S} = (|\psi\rangle; \mathcal{M}_1, \dots, \mathcal{M}_{N_A}; \mathcal{N}_1, \dots, \mathcal{N}_{N_B})$$

where $\mathcal{M}_i$ are K_A-POVMs on a finite-dimensional Hilbert space $\mathcal{H}_A$, $\mathcal{N}_j$ are K_B-POVMs on a finite-dimensional Hilbert space $\mathcal{H}_B$, and $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ is a state. When $K = K_A = K_B$ and $N = N_A = N_B$, we simply say that $\mathcal{S}$ is a N*-input* K*-output bipartite strategy*. The *correlation* of $\mathcal{S}$ is the $N_A \times N_B \times K_A \times K_B$ array p with entries

$$p(a, b|i, j) = \langle \psi | \mathcal{M}_{i,a} \otimes \mathcal{N}_{j,b} |\psi\rangle \qquad \begin{aligned} &1 \le a \le K_A,\ 1 \le b \le K_B, \\ &1 \le i \le N_A,\ 1 \le j \le N_B. \end{aligned}$$

Since $\mathcal{S}$ in particular models non-communication between parties, the correlation p is *non-signalling*, meaning that $p(a|i) := \sum_{b=1}^{K_B} p(a, b|i, j)$ and $p(b|j) := \sum_{a=1}^{K_A} p(a, b|i, j)$ are well-defined (the first sum is independent of j and the second sum is independent of i). A correlation p is called *synchronous* if $K_A = K_B$, $N_A = N_B$ and $p(a, b|i, i) = 0$ for all i and $a \neq b$.

Let $\mathcal{S}$ and $\widetilde{\mathcal{S}}$ be (N_A, N_B)-input (K_A, K_B)-output strategies. Then $\widetilde{\mathcal{S}}$ is a *local dilation* if $\mathcal{S}$ there exist finite-dimensional Hilbert spaces $\mathcal{K}_A, \mathcal{K}_B$, a state $|\mathrm{aux}\rangle \in \mathcal{K}_A \otimes \mathcal{K}_B$ and isometries $U_A : \mathcal{H}_A \to \widetilde{\mathcal{H}}_A \otimes \mathcal{K}_A$ and $U_B : \mathcal{H}_B \to \widetilde{\mathcal{H}}_B \otimes \mathcal{K}_B$ such that

$$(U_A \otimes U_B)(\mathcal{M}_{i,a} \otimes \mathcal{N}_{j,b}) |\psi\rangle = (\widetilde{\mathcal{M}}_{i,a} \otimes \widetilde{\mathcal{N}}_{j,b}) |\widetilde{\psi}\rangle \otimes |\mathrm{aux}\rangle \tag{1}$$

for all a, b, i, j. There is a slight abuse of notation in (1); namely, we identify

$$(\widetilde{\mathcal{H}}_A \otimes \mathcal{K}_A) \otimes (\widetilde{\mathcal{H}}_B \otimes \mathcal{K}_B) \equiv (\widetilde{\mathcal{H}}_A \otimes \widetilde{\mathcal{H}}_B) \otimes (\mathcal{K}_A \otimes \mathcal{K}_B).$$

Note that if $\widetilde{\mathcal{S}}$ is a local dilation of $\mathcal{S}$, then the correlations of $\mathcal{S}$ and $\widetilde{\mathcal{S}}$ coincide. Finally, we say that a strategy $\widetilde{\mathcal{S}}$ is *self-tested* by its correlation if it is a local dilation of any other strategy with the same correlation.

3 Quadruples of projections adding to a scalar multiple of the identity

In [18], the authors derive several profound results on tuples of projections that add to a scalar multiple of the identity operator. This is achieved by studying certain functors between categories of their representations, which are also the cornerstone of this paper. For our purposes, we focus on projections P_1, P_2, P_3, P_4 that add to $(2-\frac{1}{n})I$, where n is a natural number. First we adopt the language of representations of C*-algebras, at least to the extent required in this paper. Then we review the construction of the aforementioned functors from [18, Section 1.2]. Finally, we refine a part of [18, Proposition 3] to obtain further properties about the projections P_i as above (Proposition 3.1).

For $\alpha \in \mathbb{R}$ define the universal C*-algebra

$$\mathcal{A}_\alpha = \mathrm{C}^* \left\langle x_1, x_2, x_3, x_4 \colon x_i = x_i^* = x_i^2,\ x_1 + x_2 + x_3 + x_4 = \alpha \right\rangle,$$

and let Rep_α denote the category of representations of $\mathcal{A}_\alpha$. That is, objects of Rep_α are representations of $\mathcal{A}_\alpha$ on Hilbert spaces, and morphisms of Rep_α are equivariant maps, i.e., bounded linear operators between Hilbert spaces that intertwine the actions of representations. For a comprehensive source on C*-algebras and their representations, see [3]. While the above terminology offers a suitable mathematical framework for the technical steps in the proofs of this paper, let us extract the main meaning behind it, sufficient for comprehending the proofs. Without addressing precisely what a universal C*-algebra is, we can still say what its representations are. A representation π of $\mathcal{A}_\alpha$ is a quadruple of projections X_1, X_2, X_3, X_4 on a Hilbert space $\mathcal{H}$ that satisfy $X_1 + X_2 + X_3 + X_4 = \alpha I$. Thus Rep_α is foremost a collection of such quadruples; one could think of $\mathcal{A}_\alpha$ as their abstract model. For a $\pi \in \mathrm{Rep}_\alpha$ as above we write $\pi(x_i) = X_i$, and we assign to it a 6-tuple of numbers $[\pi] = (\alpha; n; d_1, d_2, d_3, d_4)$ where $n = \dim \mathcal{H}$ and $d_i = \operatorname{rk} \pi(x_i)$, the dimension of the range of X_i (if $\mathcal{H}$ is infinite-dimensional, then $n = \infty$; likewise, d_i can be infinite).

Note that representations may be related to each other in several ways. For example, let $\pi \in \mathcal{A}_\alpha$ is given by projections $X_1, \ldots, X_4$ on a Hilbert space $\mathcal{H}$ and $\rho \in \mathcal{A}_\alpha$ is given by projections $Y_1, \ldots, Y_4$ on a Hilbert space $\mathcal{K}$. Then the projections $X_1 \oplus Y_1, \ldots, X_4 \oplus Y_4$ act on $\mathcal{H} \oplus \mathcal{K}$ and add to α times identity, so they determine representation of $\mathcal{A}_\alpha$, called the *direct sum* of π and ρ. Next, we say that π and ρ are

unitarily equivalent if there is a unitary (that is, an isometric invertible linear map) $U : \mathcal{H} \to \mathcal{K}$ such that $Y_i = UX_iU^*$ for $i = 1, \dots, 4$. Finally, we say that $\pi \in \mathrm{Rep}_\alpha$ is *irreducible* if it is not unitarily equivalent to a direct sum of representations. Irreducible representations can be viewed as the building blocks of Rep_α; namely, every representation is unitarily equivalent to a (possibly infinite) direct sum of irreducible representations. Without going into technical details, viewing Rep_α as a category instead of merely a set encapsulates these relations between representations (e.g., that some of them are unitarily equivalent, some are direct sums of others, and some are irreducible).

In this paper, representations of $\mathcal{A}_\alpha$ (for certain choices of α) give rise to the projective measurements in self-tested strategies presented in Section 5. To establish the self-testing property, it is imperative to have a good handle on Rep_α (concretely, on the irreducible representations within). This is straightforward for $\alpha = 0$ and $\alpha = 1$. Indeed, the only quadruples of projections adding to 0 are tuples of zero operators; these are all direct sums of the trivial representation τ given by $\tau(x_j) = 0$ acting on the one-dimensional Hilbert space. Hence Rep_0 contains a unique irreducible representation. On the other hand, quadruples of projections adding to 1 are necessarily diagonalizable, and thus unitarily equivalent to direct sums of $(1,0,0,0)$, $(0,1,0,0)$, $(0,0,1,0)$, $(0,0,0,1)$ acting on the one-dimensional Hilbert space. Thus Rep_1 contains exactly four unitarily non-equivalent irreducible representations. For general α, representations of $\mathcal{A}_\alpha$ are not yet well-understood; however, the aim of the next subsection is to leverage the knowledge of the very simple Rep_1 to study Rep_α for certain values of α.

3.1 Functors between representation categories

In this subsection we define two functors $T = T_\alpha : \mathrm{Rep}_\alpha \to \mathrm{Rep}_{4-\alpha}$ (linear reflection) and $S = S_\alpha : \mathrm{Rep}_\alpha \to \mathrm{Rep}_{\frac{\alpha}{\alpha-1}}$ (hyperbolic reflection). The subscripts are omitted when clear from the context. Before defining T and S, let us mention what a reader should imagine under this terminology. A functor from Rep_α to Rep_β is primarily a mapping, that takes each quadruple of projections adding to α times identity to a quadruple of projections adding to β times identity. However, being a functor means that this mapping has to respect the additional structure of the categories Rep_α and Rep_β; in particular, it needs to preserve direct sums, and map unitarily equivalent representations to unitarily equivalent representations. Technically, one encapsulates this by saying that a functor consists of a map between objects of categories and a (well-behaved) map between morphisms of categories.

(T): Given a representation π of $\mathcal{A}_\alpha$ let $T(\pi)$ be the representation of $\mathcal{A}_{4-\alpha}$ determined by $T(\pi)(x_i) := I - \pi(x_i)$. Note that T commutes with equivariant maps between representations, so it extends to a functor $T : \mathrm{Rep}_\alpha \to \mathrm{Rep}_{4-\alpha}$. If $[\pi] = (\alpha; n; d_i)$ then $[T(\pi)] = (4-\alpha; n; n-d_i)$.

(S): Suppose $\alpha \notin \{0, 1\}$, and let π be a representation of $\mathcal{A}_\alpha$ on $\mathcal{H}$. Denote

$\widehat{\mathcal{H}} = \bigoplus_i \operatorname{ran}\pi(x_i)$. Let $w_i : \operatorname{ran}\pi(x_i) \to \widehat{\mathcal{H}}$ be the canonical injections, and let $u_i : \operatorname{ran}\pi(x_i) \to \mathcal{H}$ be inclusions. Then

$$u = \frac{1}{\sqrt{\alpha}} \begin{pmatrix} u_1^* \\ \vdots \\ u_4^* \end{pmatrix} : \mathcal{H} \to \widehat{\mathcal{H}}$$

is an isometry by definition of the algebra $\mathcal{A}_\alpha$. Let $\mathcal{K} = \operatorname{ran}(I - uu^*)$, with inclusion $v : \mathcal{K} \to \widehat{\mathcal{H}}$. Note that $\dim \mathcal{K} = \dim \widehat{\mathcal{H}} - \dim \mathcal{H}$. Define

$$S(\pi)(x_i) := \frac{\alpha}{\alpha - 1} v^* w_i w_i^* v.$$

Then

$$\begin{aligned}
(S(\pi)(x_i))^2 &= \frac{\alpha^2}{(\alpha-1)^2} v^* w_i w_i^* v v^* w_i w_i^* v = \frac{\alpha^2}{(\alpha-1)^2} v^* w_i w_i^* (I - uu^*) w_i w_i^* v \\
&= \frac{\alpha^2}{(\alpha-1)^2} v^* w_i \left(I - \frac{1}{\alpha} u_i^* u_i \right) w_i^* v = \frac{\alpha^2}{(\alpha-1)^2} \left(1 - \frac{1}{\alpha} \right) v^* w_i w_i^* v \\
&= S(\pi)(x_i)
\end{aligned}$$

and

$$\sum_{i=1}^4 S(\pi)(x_i) = \sum_{i=1}^4 \frac{\alpha}{\alpha-1} v^* w_i w_i^* v = \frac{\alpha}{\alpha-1} v^* \left(\sum_{i=1}^4 w_i w_i^* \right) v = \frac{\alpha}{\alpha-1} v^* v = \frac{\alpha}{\alpha-1} I.$$

Therefore $S(\pi)(x_1), \ldots, S(\pi)(x_4)$ are projections that give rise to a representation $S(\pi)$ of $\mathcal{A}_{\frac{\alpha}{\alpha-1}}$ on $\mathcal{K}$. As described in [18, Section 1.2], one can also extend S to equivariant maps, resulting in a functor $S : \mathrm{Rep}_\alpha \to \mathrm{Rep}_{\frac{\alpha}{\alpha-1}}$. If $[\pi] = (\alpha; n; d_i)$ then $[S(\pi)] = (\frac{\alpha}{\alpha-1}; \sum_i d_i - n; d_i)$.

3.2 Distinguished quadruples of projections

For $\alpha \in (0, 3)$, the (Coxeter) functor

$$\Phi^+ = S \circ T = S_{4-\alpha} \circ T_\alpha : \mathrm{Rep}_\alpha \to \mathrm{Rep}_{1+\frac{1}{3-\alpha}}$$

define an equivalence of categories (with inverse $T \circ S$) by [18, Theorem 2]. In particular, Φ^+ is a bijection between representations of $\mathcal{A}_\alpha$ and $\mathcal{A}_{1+\frac{1}{3-\alpha}}$, which maps irreducible ones to irreducible ones. If $[\pi] = (\alpha, n, d_1, \ldots, d_4)$ then $[\Phi^+(\pi)] = (1 + \frac{1}{3-\alpha}; 3n - \sum_i d_i; n - d_i)$. The functor Φ^+ plays an implicit yet crucial role in [18, Proposition 3] that describes the category $\mathrm{Rep}_{2-\frac{1}{n}}$. For the sake of completeness, we provide the proof of the part of [18, Proposition 3], and refine it to extract the additional information needed in this paper. Given a real number β let $\lfloor \beta \rfloor$ denote the largest integer that is not larger than β.

The main statement of this section shows that starting with the easily-understood Rep_1 and then repeatedly applying the functor Φ^+, one obtains a good grasp on $\mathrm{Rep}_{2-\frac{1}{n}}$ for every $n \in \mathbb{N}$.

Proposition 3.1 ([18, Proposition 3(c)])**.** *Let $n \in \mathbb{N}$. The C*-algebra $\mathcal{A}_{2-\frac{1}{n}}$ has precisely four unitarily non-equivalent irreducible representations.*
More concretely, there are projections $\mathfrak{P}_1^{(n)}, \dots, \mathfrak{P}_4^{(n)} \in \mathrm{M}_n(\mathbb{R})$ with $\operatorname{rk} \mathfrak{P}_1^{(n)} = \lfloor \frac{n}{2} \rfloor - (-1)^n$ and $\operatorname{rk} \mathfrak{P}_i^{(n)} = \lfloor \frac{n}{2} \rfloor$ for $i = 2, 3, 4$, such that given an irreducible representation of $\mathcal{A}_{2-\frac{1}{n}}$, the quadruple $(\pi(x_1), \dots, \pi(x_4))$ is unitarily equivalent to one of the

$$(\mathfrak{P}_1^{(n)}, \mathfrak{P}_2^{(n)}, \mathfrak{P}_3^{(n)}, \mathfrak{P}_4^{(n)}), \quad (\mathfrak{P}_4^{(n)}, \mathfrak{P}_1^{(n)}, \mathfrak{P}_2^{(n)}, \mathfrak{P}_3^{(n)}),$$
$$(\mathfrak{P}_3^{(n)}, \mathfrak{P}_4^{(n)}, \mathfrak{P}_1^{(n)}, \mathfrak{P}_2^{(n)}), \quad (\mathfrak{P}_2^{(n)}, \mathfrak{P}_3^{(n)}, \mathfrak{P}_4^{(n)}, \mathfrak{P}_1^{(n)}).$$

Proof. We prove the statement by induction on n. If $n = 1$, then $\mathfrak{P}_1^{(1)} = 1$ and $\mathfrak{P}_i^{(1)} = 0$ for $i = 2, 3, 4$ are the desired 1×1 projections, giving rise to a representation $\mathcal{A}_1 \to \mathbb{C}$. Now suppose projections $\mathfrak{P}_i^{(n)} \in \mathrm{M}_n(\mathbb{R})$ possess the desired properties. Then they define an irreducible representation of $\mathcal{A}_{2-\frac{1}{n}}$ given by $\pi(x_i) = \mathfrak{P}_i^{(n)}$, and the other three irreducible representations up to unitary equivalence are obtained by cyclically permuting the generators. Now let $\mathfrak{P}_i^{(n+1)} := \Phi^+(\pi)(x_i)$. Since $\Phi^+ : \mathrm{Rep}_{2-\frac{1}{n}} \to \mathrm{Rep}_{2-\frac{1}{n+1}}$ is an equivalence of categories, $\Phi^+(\pi)$ is an irreducible representation of $\mathcal{A}_{2-\frac{1}{n}}$, and the other three irreducible representations up unitary equivalence are obtained via cyclic permutations of generators. The rank values are determined by comparing $[\pi]$ and $[\Phi^+(\pi)]$. □

Projections $\mathfrak{P}_i^{(n)}$ are central to the self-testing results in this paper. The intuition behind their applicability to self-tests is the following: if we momentarily forget irreducibility, they are characterized by having certain traces and satisfying a linear equation. In a quantum strategy with a maximally entangled state and projective measurements, traces and linear relations among the PVMs are encoded by the correlation. This makes strategies with maximally entangled states and measurements $(\mathfrak{P}_i^{(n)}, I - \mathfrak{P}_i^{(n)})$ very natural candidates for the self-testing phenomenon.

Remark 3.2. Proposition 3.1 does not provide a closed-form expression for projections $\mathfrak{P}_1^{(n)}, \dots, \mathfrak{P}_4^{(n)} \in \mathrm{M}_n(\mathbb{R})$ as functions of n. Nevertheless, definitions of functors T and S give rise to a recursive procedure for constructing $\mathfrak{P}_i^{(n)} \in \mathrm{M}_n(\mathbb{R})$ from $\mathfrak{P}_i^{(n-1)} \in \mathrm{M}_{n-1}(\mathbb{R})$. This procedure requires only matrix arithmetic and Gram-Schmidt orthogonalization.
Basis of recursion $n = 1$: set $\mathfrak{P}_1^{(1)} := 1$ and $\mathfrak{P}_i^{(1)} := 0$ for $i = 2, 3, 4$.
Recursive step $n \to n + 1$: given $\mathfrak{P}_1^{(n)}, \dots, \mathfrak{P}_4^{(n)}$ let

- U_i be an $n \times \operatorname{rk}(n - \mathfrak{P}_i^{(n)})$ matrix whose columns form an orthonormal basis of the column space of $I - \mathfrak{P}_i^{(n)}$;
- V_i be an $(\operatorname{rk} \mathfrak{P}_i^{(n)}) \times (n + 1)$ matrix such that the columns of

$$\begin{pmatrix} V_1 \\ \vdots \\ V_4 \end{pmatrix}$$

form an orthonormal basis of the column space of

$$I - \frac{1}{2+\frac{1}{n}} \begin{pmatrix} U_1^* \\ \vdots \\ U_4^* \end{pmatrix} \begin{pmatrix} U_1 & \cdots & U_4 \end{pmatrix}.$$

Then set $\mathfrak{P}_i^{(n+1)} := (2 - \frac{1}{n+1}) V_i^* V_i$.

Using the above procedure, we obtain the following projections for $n = 1, 2, 3$:

$$\mathfrak{P}_1^{(1)} = (1),\ \mathfrak{P}_2^{(1)} = (0),\ \mathfrak{P}_3^{(1)} = (0),\ \mathfrak{P}_4^{(1)} = (0)$$

$$\mathfrak{P}_1^{(2)} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},\ \mathfrak{P}_2^{(2)} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix},\ \mathfrak{P}_3^{(2)} = \begin{pmatrix} \frac{1}{4} & \frac{-\sqrt{3}}{4} \\ \frac{-\sqrt{3}}{4} & \frac{3}{4} \end{pmatrix},\ \mathfrak{P}_4^{(2)} = \begin{pmatrix} \frac{1}{4} & \frac{\sqrt{3}}{4} \\ \frac{\sqrt{3}}{4} & \frac{3}{4} \end{pmatrix}$$

$$\mathfrak{P}_1^{(3)} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix},\ \mathfrak{P}_2^{(3)} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & \frac{4}{9} & \frac{-2\sqrt{5}}{9} \\ 0 & \frac{-2\sqrt{5}}{9} & \frac{5}{9} \end{pmatrix},$$

$$\mathfrak{P}_3^{(3)} = \begin{pmatrix} \frac{1}{3} & \frac{1}{3\sqrt{3}} & \frac{\sqrt{5}}{3\sqrt{3}} \\ \frac{1}{3\sqrt{3}} & \frac{1}{9} & \frac{\sqrt{5}}{9} \\ \frac{\sqrt{5}}{3\sqrt{3}} & \frac{\sqrt{5}}{9} & \frac{5}{9} \end{pmatrix},\ \mathfrak{P}_4^{(3)} = \begin{pmatrix} \frac{1}{3} & \frac{-1}{3\sqrt{3}} & \frac{-\sqrt{5}}{3\sqrt{3}} \\ \frac{-1}{3\sqrt{3}} & \frac{1}{9} & \frac{\sqrt{5}}{9} \\ \frac{-\sqrt{5}}{3\sqrt{3}} & \frac{\sqrt{5}}{9} & \frac{5}{9} \end{pmatrix}$$

The linear-algebraic nature of this procedure allows for a feasible implementation using exact arithmetic. For concrete matrices in cases $n = 4, 5, 6$, see Appendix A.

For later use we record a technical fact.

Lemma 3.3. *The* 4×4 *matrix*

$$\begin{pmatrix} \operatorname{rk}\mathfrak{P}_1^{(n)} & \operatorname{rk}\mathfrak{P}_2^{(n)} & \operatorname{rk}\mathfrak{P}_3^{(n)} & \operatorname{rk}\mathfrak{P}_4^{(n)} \\ \operatorname{rk}\mathfrak{P}_4^{(n)} & \operatorname{rk}\mathfrak{P}_1^{(n)} & \operatorname{rk}\mathfrak{P}_2^{(n)} & \operatorname{rk}\mathfrak{P}_3^{(n)} \\ \operatorname{rk}\mathfrak{P}_3^{(n)} & \operatorname{rk}\mathfrak{P}_4^{(n)} & \operatorname{rk}\mathfrak{P}_1^{(n)} & \operatorname{rk}\mathfrak{P}_2^{(n)} \\ \operatorname{rk}\mathfrak{P}_2^{(n)} & \operatorname{rk}\mathfrak{P}_3^{(n)} & \operatorname{rk}\mathfrak{P}_4^{(n)} & \operatorname{rk}\mathfrak{P}_1^{(n)} \end{pmatrix} = -(-1)^n I_4 + \left\lfloor \frac{n}{2} \right\rfloor \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}$$

is invertible for every $n \in \mathbb{N}$.

Remark 3.4. Let us determine the normalized traces of $\mathfrak{P}_i^{(n)}$ and their products; these values will appear in the self-testing correlations of this paper. Clearly,

$$\tau\left(\mathfrak{P}_1^{(n)}\right) = \frac{1}{2} - \frac{1 + 3(-1)^n}{4n}, \qquad \tau\left(\mathfrak{P}_i^{(n)}\right) = \frac{1}{2} - \frac{1 - (-1)^n}{4n}, \quad \text{for } i = 2, 3, 4.$$

Next, by Proposition 3.1, for every permutation σ of $\{2, 3, 4\}$ there exists a unitary $U \in \mathrm{M}_n(\mathbb{C})$ such that

$$U\mathfrak{P}_1^{(n)}U^* = \mathfrak{P}_1^{(n)}, \qquad U\mathfrak{P}_i^{(n)}U^* = \mathfrak{P}_{\sigma(i)}^{(n)}, \quad \text{for } i = 2, 3, 4.$$

Therefore $\tau(\mathfrak{P}_1^{(n)}\mathfrak{P}_i^{(n)})$ is independent of $i \in \{2,3,4\}$, and $\tau(\mathfrak{P}_i^{(n)}\mathfrak{P}_j^{(n)})$ is independent of $i,j \in \{2,3,4\}$ with $i \neq j$. From the equation $\sum_{j=1}^4 \mathfrak{P}_i^{(n)}\mathfrak{P}_j^{(n)} = (2-\frac{1}{n})\mathfrak{P}_i^{(n)}$ for $i = 1,\dots,4$ we then obtain

$$\tau\left(\mathfrak{P}_1^{(n)}\mathfrak{P}_i^{(n)}\right) = \frac{1}{3}\left(1-\frac{1}{n}\right)\tau\left(\mathfrak{P}_1^{(n)}\right) \quad \text{for } i = 2,3,4,$$
$$\tau\left(\mathfrak{P}_i^{(n)}\mathfrak{P}_j^{(n)}\right) = \frac{1}{2}\left(1-\frac{1}{n}\right)\left(\tau\left(\mathfrak{P}_i^{(n)}\right) - \frac{1}{3}\tau\left(\mathfrak{P}_1^{(n)}\right)\right) \quad \text{for } i,j = 2,3,4 \text{ and } i \neq j.$$

4 Spectral results

Let $n \in \mathbb{N}$. The projections $\mathfrak{P}_1^{(n)},\dots,\mathfrak{P}_4^{(n)}$ of Proposition 3.1 play a central role in self-tests of Section 5 below. Namely, they appear as projective measurements in a self-tested strategy in Subsection 5.1; the fact that they are determined by a linear relation $\mathfrak{P}_1^{(n)} + \cdots + \mathfrak{P}_4^{(n)} = (2-\frac{1}{n})I$ is beneficial for deducing the measurements from the correlation. Nevertheless, to obtain a self-test, one still needs to be able to deduce the quantum state from the correlation. Furthermore, in Subsection 5.2, the presented strategies contain an additional projective measurement, which, while related to the $\mathfrak{P}_i^{(n)}$, is itself not a part of quadruple adding to a scalar multiple of identity. To help with the identification of the quantum state and the additional measurements from the correlation, we first require some information on eigenvalues and eigenvectors of certain tensor combinations and sums of pairs of the matrices $\mathfrak{P}_i^{(n)}$. Concretely, Proposition 4.2 shows how the maximally entangled state is related to $\mathfrak{P}_1^{(n)},\dots,\mathfrak{P}_4^{(n)}$, and Proposition 4.4 shows that $\mathfrak{P}_3^{(n)} + \mathfrak{P}_4^{(n)}$ has pairwise distinct eigenvalues, which enables post-hoc self-testing techniques [26, 7].

4.1 Role of the maximally entangled state

First, we identify the largest eigenvalue of $\sum_i \mathfrak{P}_i^{(n)} \otimes \mathfrak{P}_i^{(n)}$ and the corresponding eigenvector (cf. [19, Lemma 5.7]), and bound the spectrum of $\sum_i \mathfrak{P}_i^{(n)} \otimes \mathfrak{P}_{\sigma(i)}^{(n)}$ for a nontrivial cyclic permutation σ of $(1,2,3,4)$. Given $|\psi\rangle = \sum_{i,j} \alpha_{ij} |i\rangle|j\rangle \in \mathbb{C}^n \otimes \mathbb{C}^n$ let $\mathrm{mat}(|\psi\rangle) = \sum_{i,j} \alpha_{ij} |i\rangle\langle j| \in \mathrm{M}_n(\mathbb{C})$ denote its matricization; note that $\mathrm{mat}(|\phi_n\rangle) = \frac{1}{\sqrt{n}} I$, and

$$\mathrm{mat}\left(A \otimes B\,|\psi\rangle\right) = A\,\mathrm{mat}(|\psi\rangle)B^{\mathrm{t}}$$

for $A, B \in \mathrm{M}_n(\mathbb{C})$.

Lemma 4.1. *Let $n \in \mathbb{N}$ and let σ be a cyclic permutation σ of $(1,2,3,4)$. Denote $M = \frac{n}{2n-1}\sum_{i=1}^4 \mathfrak{P}_i^{(n)} \otimes \mathfrak{P}_{\sigma(i)}^{(n)}$.*

(i) If $\sigma = \mathrm{id}$, then the largest eigenvalue of M is 1, with the eigenspace $\mathbb{C}\,|\phi_n\rangle$.

(ii) If $\sigma \neq \mathrm{id}$, then all eigenvalues of M are strictly smaller than 1.

Proof. Let $|\psi\rangle \in \mathbb{C}^n \otimes \mathbb{C}^n$ be an arbitrary state. Then

$$\begin{aligned} \langle\psi| I \otimes I - M |\psi\rangle &\geq \langle\psi| I \otimes I - \frac{n}{2n-1} \sum_{i=1}^{4} \mathfrak{P}_i^{(n)} \otimes I |\psi\rangle \\ &= \langle\psi| \left(I - \frac{n}{2n-1} \sum_{i=1}^{4} \mathfrak{P}_i^{(n)} \right) \otimes I |\psi\rangle = 0. \end{aligned} \tag{2}$$

Therefore the largest eigenvalue of M is at most 1. Since

$$\langle\phi_n| I \otimes I - \frac{n}{2n-1} \sum_{i=1}^{4} \mathfrak{P}_i^{(n)} \otimes \mathfrak{P}_i^{(n)} |\phi_n\rangle = \tau \left(I - \frac{n}{2n-1} \sum_{i=1}^{4} \mathfrak{P}_i^{(n)} \right) = 0,$$

$|\phi_n\rangle$ is an eigenvector of M for eigenvalue 1 if $\sigma = \mathrm{id}$. Suppose $|\psi\rangle \in \mathbb{C}^n \otimes \mathbb{C}^n$ satisfies $M |\psi\rangle = |\psi\rangle$. Then (2) gives

$$\langle\psi| M |\psi\rangle = \langle\psi| \frac{n}{2n-1} \sum_{i=1}^{4} \mathfrak{P}_i^{(n)} \otimes I |\psi\rangle$$

and therefore

$$\langle\psi| \sum_{i=1}^{4} \mathfrak{P}_i^{(n)} \otimes (I - \mathfrak{P}_{\sigma(i)}^{(n)}) |\psi\rangle = 0.$$

Positive semidefinitness then implies $\mathfrak{P}_i^{(n)} \otimes (I - \mathfrak{P}_{\sigma(i)}^{(n)}) |\psi\rangle = 0$, and analogously $(I - \mathfrak{P}_i^{(n)}) \otimes \mathfrak{P}_{\sigma(i)}^{(n)} |\psi\rangle = 0$. In particular, $\mathfrak{P}_i^{(n)} \otimes I |\psi\rangle = I \otimes \mathfrak{P}_{\sigma(i)}^{(n)} |\psi\rangle$ for $i = 1, \ldots, 4$. Therefore

$$\mathfrak{P}_i^{(n)} \operatorname{mat}(|\psi\rangle) = \operatorname{mat}(|\psi\rangle) \mathfrak{P}_{\sigma(i)}^{(n)} \qquad \text{for } i = 1, \ldots, 4. \tag{3}$$

Note that $\mathfrak{P}_1^{(n)}, \ldots, \mathfrak{P}_4^{(n)}$ and $\mathfrak{P}_{\sigma(1)}^{(n)}, \ldots, \mathfrak{P}_{\sigma(4)}^{(n)}$ give rise to two irreducible representations of $\mathcal{A}_{2-\frac{1}{n}}$ by Proposition 3.1, which are unitarily equivalent if and only if $\sigma = \mathrm{id}$. Since $\operatorname{mat}(|\psi\rangle)$ intertwines these two irreducible representations, Schur's lemma implies that $\operatorname{mat} |\psi\rangle = \gamma I$ for some $\gamma \in \mathbb{C}$ if $\sigma = \mathrm{id}$, and $\operatorname{mat} |\psi\rangle = 0$ if if $\sigma \neq \mathrm{id}$. Therefore $|\psi\rangle$ is a scalar multiple of $|\phi_n\rangle$ if $\sigma = \mathrm{id}$, and 1 is not an eigenvalue of M if $\sigma \neq \mathrm{id}$. □

The following proposition shows how the maximally entangled state $|\phi_n\rangle$ is intrinsically connected to representations of $\mathcal{A}_{2-\frac{1}{n}}$.

Proposition 4.2. *Let $n \in \mathbb{N}$, let $a_1, \ldots, a_4, b_1, \ldots, b_4$ be nonnegative integers with $a_1 + \cdots + a_4 = b_1 + \cdots + b_4$, and let $\sigma_1, \ldots, \sigma_4$ be the distinct cyclic permutations of $(1, 2, 3, 4)$. Consider the identification*

$$\mathbb{C}^{(a_1+\cdots+a_4)n} \otimes \mathbb{C}^{(b_1+\cdots+b_4)n} \equiv \left(\bigoplus_{j,k=1}^{4} \mathbb{C}^{a_j} \otimes \mathbb{C}^{b_k} \right) \otimes (\mathbb{C}^n \otimes \mathbb{C}^n).$$

Then the largest eigenvalue of

$$\frac{n}{2n-1} \sum_{i=1}^{4} \left(\bigoplus_{j=1}^{4} I_{a_j} \otimes \mathfrak{P}_{\sigma_j(i)}^{(n)} \right) \otimes \left(\bigoplus_{j=1}^{4} I_{b_j} \otimes \mathfrak{P}_{\sigma_j(i)}^{(n)} \right)$$

is 1, with the eigenspace

$$\left\{ \Big(|\mathrm{aux}_1\rangle \oplus |\mathrm{aux}_2\rangle \oplus |\mathrm{aux}_3\rangle \oplus |\mathrm{aux}_4\rangle \Big) \otimes |\phi_n\rangle : \ |\mathrm{aux}_j\rangle \in \mathbb{C}^{a_j} \otimes \mathbb{C}^{b_j} \right\}.$$

Proof. Follows from the distributivity of tensor product over direct sum, and Lemma 4.1. □

4.2 Spectrum of the sum of two distinguished projections

Next, we analyze the spectrum of the matrix $\mathfrak{P}_3^{(n)} + \mathfrak{P}_4^{(n)}$ for every n. To do this, we return to the functors between categories Rep_α. Given a finite-dimensional representation π of $\mathcal{A}_\alpha$, let $\Lambda_\pi \subset [0,2]$ denote the set of eigenvalues of $\pi(x_3 + x_4)$.

Lemma 4.3. *Let π be an n-dimensional representation of $\mathcal{A}_\alpha$.*

(i) $\Lambda_{T(\pi)} = 2 - \Lambda_\pi$.

(ii) Let $\alpha \notin \{0, 1\}$.

(ii.a) If $\operatorname{rk}\pi(x_1) + \operatorname{rk}\pi(x_2) > n = \operatorname{rk}\pi(x_3) + \operatorname{rk}\pi(x_4)$ *then*

$$\Lambda_{S(\pi)} = \{0\} \cup \left(\tfrac{\alpha}{\alpha-1} - \tfrac{1}{\alpha-1}\Lambda_\pi \right).$$

(ii.b) If $\operatorname{rk}\pi(x_3) + \operatorname{rk}\pi(x_4) > n = \operatorname{rk}\pi(x_1) + \operatorname{rk}\pi(x_2)$ *then*

$$\Lambda_{S(\pi)} = \left\{ \tfrac{\alpha}{\alpha-1} \right\} \cup \left(\tfrac{\alpha}{\alpha-1} - \tfrac{1}{\alpha-1}\Lambda_\pi \right).$$

(iii) Let $\alpha \in (0, 3)$.

(iii.a) If $\operatorname{rk}\pi(x_1) + \operatorname{rk}\pi(x_2) < n = \operatorname{rk}\pi(x_3) + \operatorname{rk}\pi(x_4)$ *then*

$$\Lambda_{\Phi^+(\pi)} = \{0\} \cup \left(1 - \tfrac{1}{3-\alpha} + \tfrac{1}{3-\alpha}\Lambda_\pi \right).$$

(iii.b) If $\operatorname{rk}\pi(x_3) + \operatorname{rk}\pi(x_4) < n = \operatorname{rk}\pi(x_1) + \operatorname{rk}\pi(x_2)$ *then*

$$\Lambda_{\Phi^+(\pi)} = \left\{ 1 + \tfrac{1}{3-\alpha} \right\} \cup \left(1 - \tfrac{1}{3-\alpha} + \tfrac{1}{3-\alpha}\Lambda_\pi \right).$$

Proof. Equation (i) follows immediately from $T(\pi)(x_i) = I - \pi(x_i)$. Equations (iii) are consequences of (i) and (ii) because $\Phi^+ = S \circ T$.

Equations (ii): Suppose π act on $\mathcal{H}$ with $\dim \mathcal{H} = n$, and let

$$\begin{aligned} u_i &: \operatorname{ran}\pi(x_i) \to \mathcal{H}, \\ w_i &: \operatorname{ran}\pi(x_i) \to \operatorname{ran}\pi(x_1) \oplus \cdots \oplus \operatorname{ran}\pi(x_4), \\ v = \begin{pmatrix} v_1 \\ \vdots \\ v_4 \end{pmatrix} &: \operatorname{ran}\left(I - \frac{1}{\alpha} \begin{pmatrix} u_1^* \\ \vdots \\ u_4^* \end{pmatrix} \begin{pmatrix} u_1 & \cdots & u_4 \end{pmatrix} \right) \to \operatorname{ran}\pi(x_1) \oplus \cdots \oplus \operatorname{ran}\pi(x_4) \end{aligned}$$

be inclusions as in the construction of S. Then $S(\pi)(x_i) = \frac{\alpha}{\alpha-1} v^* w_i w_i^* v$, and the characteristic polynomial of $S(\pi)(x_3 + x_4)$ equals

$$\begin{aligned}
&\det\left(\lambda I - S(\pi)(x_3+x_4)\right)\\
&= \det\left(\lambda I - \tfrac{\alpha}{\alpha-1} v^*(w_3 w_3^* + w_4 w_4^*)v\right)\\
&= \det\left(\lambda I - \tfrac{\alpha}{\alpha-1} \begin{pmatrix} v_3^* & v_4^* \end{pmatrix} \begin{pmatrix} v_3 \\ v_4 \end{pmatrix}\right)\\
&= \lambda^{\operatorname{rk}\pi(x_1)+\operatorname{rk}\pi(x_2)-n} \det\left(\lambda I - \tfrac{\alpha}{\alpha-1} \begin{pmatrix} v_3 \\ v_4 \end{pmatrix} \begin{pmatrix} v_3^* & v_4^* \end{pmatrix}\right)\\
&= \lambda^{\operatorname{rk}\pi(x_1)+\operatorname{rk}\pi(x_2)-n} \det\left(\lambda I - \tfrac{\alpha}{\alpha-1} \left(I - \tfrac{1}{\alpha} \begin{pmatrix} u_3^* \\ u_4^* \end{pmatrix} \begin{pmatrix} u_3 & u_4 \end{pmatrix}\right)\right)\\
&= \lambda^{\operatorname{rk}\pi(x_1)+\operatorname{rk}\pi(x_2)-n} \det\left(\left(\lambda - \tfrac{\alpha}{\alpha-1}\right) I + \tfrac{1}{\alpha-1} \begin{pmatrix} u_3^* \\ u_4^* \end{pmatrix} \begin{pmatrix} u_3 & u_4 \end{pmatrix}\right)\\
&= \lambda^{\operatorname{rk}\pi(x_1)+\operatorname{rk}\pi(x_2)-n} \left(\lambda - \tfrac{\alpha}{\alpha-1}\right)^{\operatorname{rk}\pi(x_3)+\operatorname{rk}\pi(x_4)-n} \det\left(\left(\lambda - \tfrac{\alpha}{\alpha-1}\right) I + \tfrac{1}{\alpha-1} \begin{pmatrix} u_3 & u_4 \end{pmatrix} \begin{pmatrix} u_3^* \\ u_4^* \end{pmatrix}\right)\\
&= \lambda^{\operatorname{rk}\pi(x_1)+\operatorname{rk}\pi(x_2)-n} \left(\lambda - \tfrac{\alpha}{\alpha-1}\right)^{\operatorname{rk}\pi(x_3)+\operatorname{rk}\pi(x_4)-n} \det\left(\left(\lambda - \tfrac{\alpha}{\alpha-1}\right) I + \tfrac{1}{\alpha-1}\pi(x_3+x_4)\right).
\end{aligned}$$

Therefore

$$\Lambda_{S(\pi)} = \{0\} \cup \left(\tfrac{\alpha}{\alpha-1} - \tfrac{1}{\alpha-1}\Lambda_\pi\right)$$

if $\operatorname{rk}\pi(x_1) + \operatorname{rk}\pi(x_2) > n = \operatorname{rk}\pi(x_3) + \operatorname{rk}\pi(x_4)$, and

$$\Lambda_{S(\pi)} = \left\{\tfrac{\alpha}{\alpha-1}\right\} \cup \left(\tfrac{\alpha}{\alpha-1} - \tfrac{1}{\alpha-1}\Lambda_\pi\right)$$

if $\operatorname{rk}\pi(x_3) + \operatorname{rk}\pi(x_4) > n = \operatorname{rk}\pi(x_1) + \operatorname{rk}\pi(x_2)$. □

The following proposition identifies all eigenvalues of the matrix $\mathfrak{P}_3^{(n)} + \mathfrak{P}_4^{(n)}$; in particular, they are all simple (pairwise distinct).

Proposition 4.4. *Eigenvalues of* $n(\mathfrak{P}_3^{(n)} + \mathfrak{P}_4^{(n)})$ *are* $\{0, 2, \ldots, 2n-2\}$ *if* n *is odd, and* $\{1, 3, \ldots, 2n-1\}$ *if* n *is even.*

Proof. Let $\pi_1 : \mathcal{A}_1 \to \mathbb{C}$ be given as $\pi_1(x_1) = 1$ and $\pi_1(x_2) = \pi(x_3) = \pi(x_4) = 0$. For $n \geq 2$ denote $\pi_n = \Phi^+(\pi_1)$. By Proposition 3.1 we have $\operatorname{rk}\pi_n(x_1) + \operatorname{rk}\pi_n(x_2) < n = \operatorname{rk}\pi_n(x_3) + \operatorname{rk}\pi_n(x_4)$ if n is even, and $\operatorname{rk}\pi_n(x_3) + \operatorname{rk}\pi_n(x_4) < n = \operatorname{rk}\pi_n(x_1) + \operatorname{rk}\pi_n(x_2)$ if n is odd. By Lemma 4.3,

$$\begin{aligned}
\Lambda_{\pi_{n+1}} &= \{0\} \cup \left(\tfrac{1}{n+1} + \tfrac{n}{n+1}\Lambda_{\pi_n}\right) && \text{if } n \text{ is even,}\\
\Lambda_{\pi_{n+1}} &= \{2 - \tfrac{1}{n+1}\} \cup \left(\tfrac{1}{n+1} + \tfrac{n}{n+1}\Lambda_{\pi_n}\right) && \text{if } n \text{ is odd.}
\end{aligned}$$

Therefore

$$\begin{aligned}
(n+1)\Lambda_{\pi_{n+1}} &= \{0\} \cup (1 + n\Lambda_{\pi_n}) && \text{if } n \text{ is even,}\\
(n+1)\Lambda_{\pi_{n+1}} &= \{2n+1\} \cup (1 + n\Lambda_{\pi_n}) && \text{if } n \text{ is odd.}
\end{aligned}$$

Since $\Lambda_{\pi_1} = \{0\}$, induction on n shows that

$$\begin{aligned}
n\Lambda_{\pi_n} &= \{0, 2, \ldots, 2n-2\} && \text{if } n \text{ is odd,}\\
n\Lambda_{\pi_n} &= \{1, 3, \ldots, 2n-1\} && \text{if } n \text{ is even.}
\end{aligned}$$

Finally, $\mathfrak{P}_3^{(n)}, \mathfrak{P}_4^{(n)}$ are simultaneously unitarily equivalent to $\pi_n(x_3), \pi_n(x_4)$. □

Lastly, we determine how eigenvectors of $\mathfrak{P}_3^{(n)}+\mathfrak{P}_4^{(n)}$ interact with $\mathfrak{P}_1^{(n)}$ and $\mathfrak{P}_2^{(n)}$.

Proposition 4.5. *Let λ be an eigenvalue of $\mathfrak{P}_3^{(n)}+\mathfrak{P}_4^{(n)}$, with a corresponding unit eigenvector $|e\rangle \in \mathbb{R}^n$.*

(i) If $\lambda \neq 1-\frac{1}{n}$ then

$$\langle e|\,\mathfrak{P}_1^{(n)}\,|e\rangle = \langle e|\,\mathfrak{P}_2^{(n)}\,|e\rangle = 1-\frac{1}{2n}-\frac{\lambda}{2}.$$

(ii) If $\lambda = 1-\frac{1}{n}$ then

$$\langle e|\,\mathfrak{P}_1^{(n)}\,|e\rangle = \begin{cases} 0 & \text{if } n \text{ even,} \\ 1 & \text{if } n \text{ odd,} \end{cases} \qquad \langle e|\,\mathfrak{P}_2^{(n)}\,|e\rangle = \begin{cases} 1 & \text{if } n \text{ even,} \\ 0 & \text{if } n \text{ odd.} \end{cases}$$

Proof. (i) By the defining relation of $\mathfrak{P}_i^{(n)}$,

$$\mathfrak{P}_1^{(n)}\,|e\rangle + \mathfrak{P}_2^{(n)}\,|e\rangle + \lambda\,|e\rangle = \left(2-\frac{1}{n}\right)|e\rangle\,. \tag{4}$$

Multiplying (4) on the left with $\langle e|\,\mathfrak{P}_i^{(n)}$ for $i=1,2$ results in

$$\begin{aligned} \langle e|\,\mathfrak{P}_1^{(n)}\,|e\rangle + \langle e|\,\mathfrak{P}_1^{(n)}\mathfrak{P}_2^{(n)}\,|e\rangle &= \left(2-\frac{1}{n}-\lambda\right)\langle e|\,\mathfrak{P}_1^{(n)}\,|e\rangle\,, \\ \langle e|\,\mathfrak{P}_2^{(n)}\mathfrak{P}_1^{(n)}\,|e\rangle + |e\rangle\,\mathfrak{P}_2^{(n)}\,|e\rangle &= \left(2-\frac{1}{n}-\lambda\right)\langle e|\,\mathfrak{P}_2^{(n)}\,|e\rangle\,. \end{aligned}$$

Therefore $\langle e|\,\mathfrak{P}_1^{(n)}\,|e\rangle = \langle e|\,\mathfrak{P}_2^{(n)}\,|e\rangle$ if $\lambda \neq 1-\frac{1}{n}$. Multiplying (4) on the left with $\langle e|$ then gives $\langle e|\,\mathfrak{P}_1^{(n)}\,|e\rangle = \langle e|\,\mathfrak{P}_2^{(n)}\,|e\rangle = 1-\frac{1}{2n}-\frac{\lambda}{2}$.

(ii) Note that $\mathfrak{P}_3^{(n)}+\mathfrak{P}_4^{(n)}$ admits n orthonormal eigenvectors $|e_1\rangle, \ldots, |e_n\rangle \in \mathbb{R}^n$ by Proposition 4.4. Hence

$$\operatorname{tr}\mathfrak{P}_i^{(n)} = \sum_{k=1}^{n}\langle e_k|\,\mathfrak{P}_i^{(n)}\,|e_k\rangle$$

for $i=1,2$. By (ii) and Proposition 3.1 we therefore have

$$\begin{aligned} \langle e|\,\mathfrak{P}_i^{(n)}\,|e\rangle &= \operatorname{tr}\mathfrak{P}_i^{(n)} - (n-1)\left(1-\frac{1}{2n}\right) + \frac{1}{2}\left(\operatorname{tr}\left(\mathfrak{P}_3^{(n)}+\mathfrak{P}_4^{(n)}\right)-1+\frac{1}{n}\right) \\ &= 2\left\lfloor\frac{n}{2}\right\rfloor - n + 1 - \begin{cases} (-1)^n & \text{if } i=1 \\ 0 & \text{if } i=2 \end{cases} \end{aligned}$$

since $\operatorname{tr}\mathfrak{P}_i^{(n)} = \operatorname{rk}\mathfrak{P}_i^{(n)}$. □

5 Constant-sized self-tests

In this section we derive the main results of the paper: every maximally entangled state is self-tested by a 4-input 2-output strategy (Subsection 5.1), and every single binary PVM is self-tested by a 5-input 2-output strategy (Subsection 5.2).

5.1 Self-testing maximally entangled states

First we introduce a family of 4-input 2-output strategies that self-test maximally entangled states of all dimensions (Theorem 5.2).

Definition 5.1. For $n \in \mathbb{N}$ let $\mathfrak{P}_i^{(n)}$ be the $n \times n$ projections as in Proposition 3.1. Let $\mathcal{S}_n$ be the 4-input 2-output bipartite strategy

$$\mathcal{S}_n = \left(|\phi_n\rangle ; \left(\mathfrak{P}_i^{(n)}, I - \mathfrak{P}_i^{(n)}\right)_{i=1}^4 ; \left(\mathfrak{P}_i^{(n)}, I - \mathfrak{P}_i^{(n)}\right)_{i=1}^4 \right).$$

Note that the correlation of $\mathcal{S}_n$ is synchronous, $p(a,b|i,i) = \tau\left(\mathfrak{P}_i^{(n)}(I - \mathfrak{P}_i^{(n)})\right) = 0$ for $a \neq b$. Furthermore,

$$p(1,1|i,j) = \langle\phi_n| \mathfrak{P}_i^{(n)} \otimes \mathfrak{P}_j^{(n)} |\phi_n\rangle = \tau\left(\mathfrak{P}_i^{(n)}\mathfrak{P}_j^{(n)}\right),$$
$$p(1|i) = \langle\phi_n| \mathfrak{P}_i^{(n)} \otimes I |\phi_n\rangle = \langle\phi_n| I \otimes \mathfrak{P}_i^{(n)} |\phi_n\rangle = \tau\left(\mathfrak{P}_i^{(n)}\right)$$

for $i,j = 1,\dots,4$, and these values are computed in Remark 3.4. Comprising everything together, the correlation of $\mathcal{S}_n$ is determined by the vector

$$\left(p(1|i)\right)_{i=1}^4 = \left(\tfrac{\lfloor \frac{n}{2} \rfloor - (-1)^n}{n} \quad \tfrac{\lfloor \frac{n}{2} \rfloor}{n} \quad \tfrac{\lfloor \frac{n}{2} \rfloor}{n} \quad \tfrac{\lfloor \frac{n}{2} \rfloor}{n}\right)$$

and the symmetric matrix $\left(p(1,1|i,j)\right)_{i,j=1}^4$

$$\begin{pmatrix} \frac{\lfloor \frac{n}{2} \rfloor - (-1)^n}{n} & \frac{(n-1)(\lfloor \frac{n}{2} \rfloor - (-1)^n)}{3n^2} & \frac{(n-1)(\lfloor \frac{n}{2} \rfloor - (-1)^n)}{3n^2} & \frac{(n-1)(\lfloor \frac{n}{2} \rfloor - (-1)^n)}{3n^2} \\ . & \frac{\lfloor \frac{n}{2} \rfloor}{n} & \frac{(n-1)(2n-1+3(-1)^n)}{12n^2} & \frac{(n-1)(2n-1+3(-1)^n)}{12n^2} \\ . & . & \frac{\lfloor \frac{n}{2} \rfloor}{n} & \frac{(n-1)(2n-1+3(-1)^n)}{12n^2} \\ . & . & . & \frac{\lfloor \frac{n}{2} \rfloor}{n} \end{pmatrix}.$$

Notice that while a closed-form expression for the strategy $\mathcal{S}_n$ has not been given (instead, the projections in $\mathcal{S}_n$ can be recursively constructed as in Remark 3.2), its correlation admits a closed-form expression (as a function of n).

The next theorem establishes that $\mathcal{S}_n$ is a local dilation of any strategy $\mathcal{S}$ that produces the same correlation as $\mathcal{S}_n$. The blueprint for the proof is threefold. Firstly, the correlation manages to encode the defining linear relation of measurements in $\mathcal{S}_n$, which leads to measurements of $\mathcal{S}$ essentially forming a representation of $\mathcal{A}_{2-\frac{1}{n}}$. Secondly, the established relationship between the maximally entangled state and representations of $\mathcal{A}_{2-\frac{1}{n}}$ (Proposition 4.2) allows one to identify the state in $\mathcal{S}$. Thirdly, the finer look at the correlation shows that the representation of $\mathcal{A}_{2-\frac{1}{n}}$ arising from measurements of $\mathcal{S}$ cannot be an direct sum of the different irreducible representations, but is actually a direct copy of the irreducible representation coming from $\mathcal{S}_n$.

Theorem 5.2. *The strategy $\mathcal{S}_n$ is self-tested by its correlation for every $n \in \mathbb{N}$.*

Proof. Let p be the correlation of $\mathcal{S}_n$. Suppose

$$\mathcal{S} = \left(|\psi\rangle\,; (P_i, I - P_i)_{i=1}^4; (Q_i, I - Q_i)_{i=1}^4\right)$$

is another strategy with the correlation p. Since p is synchronous and local dilations are transitive, by [19, Lemma 4.9 and Corollary 3.6] it suffices to assume that the state $|\psi\rangle \in \mathcal{H} \otimes \mathcal{H}$ has full Schmidt rank, P_i, Q_i are projections on $\mathcal{H}$, and

$$P_i \otimes I\,|\psi\rangle = I \otimes Q_i\,|\psi\rangle \tag{5}$$

for $i = 1, \ldots, 4$. By equality of correlations and (5),

$$\begin{aligned}
&\langle\psi| \left(\frac{2n-1}{n} I - \sum_{i=1}^4 P_i\right)^2 \otimes I\,|\psi\rangle \\
&= \langle\psi| \left(\frac{2n-1}{n} I - \sum_{i=1}^4 P_i\right) \otimes \left(\frac{2n-1}{n} I - \sum_{i=1}^4 Q_i\right) |\psi\rangle \\
&= \langle\phi_n| \left(\frac{2n-1}{n} I - \sum_{i=1}^4 \mathfrak{P}_i^{(n)}\right) \otimes \left(\frac{2n-1}{n} I - \sum_{i=1}^4 \mathfrak{P}_i^{(n)}\right) |\phi_n\rangle = 0,
\end{aligned}$$

and analogously for Q_i. Since $|\psi\rangle$ has full rank, we obtain

$$\frac{2n-1}{n} I - \sum_{i=1}^4 P_i = 0 = \frac{2n-1}{n} I - \sum_{i=1}^4 Q_i. \tag{6}$$

Furthermore,

$$\langle\psi|\, \frac{n}{2n-1} \sum_{i=1}^4 P_i \otimes Q_i\,|\psi\rangle = \langle\phi_n|\, \frac{n}{2n-1} \sum_{i=1}^4 \mathfrak{P}_i^{(n)} \otimes \mathfrak{P}_i^{(n)}\,|\phi_n\rangle = 1. \tag{7}$$

Let $\sigma_1, \ldots, \sigma_4$ be the distinct cyclic permutations of $(1, 2, 3, 4)$, with $\sigma_1 = \mathrm{id}$. By (6) and Proposition 3.1 there exist nonnegative integers $a_1, \ldots, a_4, b_1, \ldots, b_4$ with $a_1 + \cdots + a_4 = b_1 + \cdots + b_4$, and unitaries U and V on $\mathcal{H}$, such that

$$UP_iU^* = \bigoplus_{j=1}^4 I_{a_j} \otimes \mathfrak{P}_{\sigma_j(i)}^{(n)}, \qquad VQ_iV^* = \bigoplus_{j=1}^4 I_{b_j} \otimes \mathfrak{P}_{\sigma_j(i)}^{(n)}$$

for $i = 1, \ldots, 4$. By (7) and Proposition 4.2,

$$U \otimes V\,|\psi\rangle = \Big(\,|\mathrm{aux}_1\rangle \oplus |\mathrm{aux}_2\rangle \oplus |\mathrm{aux}_3\rangle \oplus |\mathrm{aux}_4\rangle\,\Big) \otimes |\phi_n\rangle$$

for some $|\mathrm{aux}_j\rangle \in \mathbb{C}^{a_j} \otimes \mathbb{C}^{b_j}$, where we identified

$$\mathcal{H} \otimes \mathcal{H} \equiv \left(\bigoplus_{j,k=1}^4 \mathbb{C}^{a_j} \otimes \mathbb{C}^{b_k}\right) \otimes (\mathbb{C}^n \otimes \mathbb{C}^n).$$

Then

$$\langle\phi_n|\, \mathfrak{P}_i^{(n)} \otimes I\,|\phi_n\rangle = \langle\psi|\, P_i \otimes I\,|\psi\rangle = \sum_{j=1}^4 \langle \mathrm{aux}_j|\mathrm{aux}_j\rangle\, \langle\phi_n|\, \mathfrak{P}_{\sigma_j(i)}^{(n)} \otimes I\,|\phi_n\rangle$$

gives rise to a linear system of equations in $\langle \mathrm{aux}_j | \mathrm{aux}_j \rangle$,

$$\operatorname{rk} \mathfrak{P}_i^{(n)} = \sum_{j=1}^{4} \operatorname{rk} \mathfrak{P}_{\sigma_j(i)}^{(n)} \cdot \langle \mathrm{aux}_j | \mathrm{aux}_j \rangle \qquad \text{for } i = 1, 2, 3, 4. \tag{8}$$

By Lemma 3.3, the system (8) has a unique solution; since $\sigma_1 = \mathrm{id}$, we obtain $\langle \mathrm{aux}_1 | \mathrm{aux}_1 \rangle = 1$ and $\langle \mathrm{aux}_j | \mathrm{aux}_j \rangle = 0$ for $j = 2, 3, 4$. Since $|\psi\rangle$ is a faithful state, it follows that $a_j = b_j = 0$ for $j = 2, 3, 4$, and $a_1 = b_1$. Therefore

$$U P_i U^* = I_{a_1} \otimes \mathfrak{P}_i^{(n)}, \qquad V Q_i V^* = I_{a_1} \otimes \mathfrak{P}_i^{(n)}, \qquad U \otimes V \, |\psi\rangle = |\mathrm{aux}_1\rangle \otimes |\phi_n\rangle \,,$$

so $\mathcal{S}_n$ is a local dilation of $\mathcal{S}$. □

Remark 5.3. The proof of Theorem 5.2 follows the core ideas of the proof of [19, Corollary 7.1], which treats maximally entangled states of odd dimension. The main difference arises from applying the representation theory of C*-algebras $\mathcal{A}_\alpha$ for different values of α. Namely, in [19] the authors focus on $\mathcal{A}_{2-\frac{2}{n}}$ for odd n (and their analogs on more than four generators), since $\mathcal{A}_{2-\frac{2}{n}}$ for odd n is simple and isomorphic to $\mathrm{M}_n(\mathbb{C})$ (i.e., it has a unique irreducible representation, which is n-dimensional). On the other hand, algebras $\mathcal{A}_{2-\frac{1}{n}}$ for $n \in \mathbb{N}$ are not simple, as they are isomorphic to $\mathbb{C}^4 \otimes \mathrm{M}_n(\mathbb{C})$. Non-simplicity is the origin of intricacies in the proof of Theorem 5.2 and auxiliary results.

Finally, with a considerable effort, the authors of [19] also establish that their self-tests are *robust*. Such robustness analysis is omitted in this paper; nevertheless, there is no obstruction for the techniques of [19, Section 6] to imply robust versions of the newly presented self-tests.

Corollary 5.4. *The following states and binary projective measurements can be self-tested by 4-input 2-output bipartite strategies for every $n \in \mathbb{N}$:*

(a) maximally entangled state of local dimension n;

(b) binary projective measurement determined by an $n \times n$ projection with rank in

$$\left\{ \left\lceil \frac{n}{2} \right\rceil, \ \left\lfloor \frac{n}{2} \right\rfloor - (-1)^n, \ \left\lceil \frac{n}{2} \right\rceil + (-1)^n \right\}.$$

5.2 Self-testing local projective measurements

Next we introduce a two-parametric family of 5-input 2-output strategies that self-test binary PVMs of all dimensions and ranks (Theorem 5.10). These strategies are obtained from the 4-input 2-output strategies of Subsection 5.1 by adding an additional binary PVM. The phenomenon, where a self-tested strategy is extended to a new one while preserving the self-testing feature, is called post-hoc self-testing [26]. The key sufficiency condition for post-hoc self-testing was derived in [7], and is presented next.

Given an invertible hermitian matrix $X \in \mathrm{M}_n(\mathbb{C})$ let $\mathrm{sgn}(X) \in \mathrm{M}_n(\mathbb{C})$ be the unique hermitian unitary matrix that commutes with X, and $\mathrm{sgn}(X)X \succ 0$. Equivalently, $\mathrm{sgn}(X)$ is the unitary part of the polar decomposition of X. In other words, sgn is the matrix extension of the usual sign function via functional calculus. This map plays a role in the following post-hoc self-testing criterion established in [7].

Proposition 5.5. *[7, Proposition 3.7] Suppose $P, P_i, Q_j \in \mathrm{M}_n(\mathbb{R})$ for $i = 1, \ldots, N_A$ and $j = 1, \ldots, N_B$ are projections, and the (N_A, N_B)-input $(2,2)$-output strategy*

$$\Big(|\phi_n\rangle\,; (P_i, I - P_i)_{i=1}^{N_A}\,; (Q_i, I - Q_i)_{i=1}^{N_B}\Big)$$

is self-tested by its correlation. If

$$2P - I \in \mathrm{sgn}\left(\mathrm{GL}_n(\mathbb{R}) \cap \mathrm{span}_{\mathbb{R}}\{I, Q_1, \ldots, Q_{N_B}\}\right),$$

then the $(N_A + 1, N_B)$-input $(2,2)$-output strategy

$$\Big(|\phi_n\rangle\,; (P_i, I - P_i)_{i=1}^{N_A}, (P, I - P); (Q_i, I - Q_i)_{i=1}^{N_B}\Big)$$

is self-tested by its correlation.

As mentioned at the beginning of the subsection, Proposition 5.5 will be used to obtain a self-tested strategy by extending $\mathcal{S}_n$ from Subsection 5.1. Recall that $\mathfrak{P}_3^{(n)} + \mathfrak{P}_4^{(n)}$ has pairwise distinct eigenvalues by Proposition 4.4. This gives rise to a family of projections that satisfy the sufficiency condition in Proposition 5.5.

Proposition 5.6. *Let $n, r \in \mathbb{N}$ with $r \leq n$. The matrix*

$$\mathfrak{Q}^{(n,r)} := \frac{1}{2}\left(I + \mathrm{sgn}\left((2r - \tfrac{1}{2})I - n\Big(\mathfrak{P}_3^{(n)} + \mathfrak{P}_4^{(n)}\Big)\right)\right) \in \mathrm{M}_n(\mathbb{R})$$

is a projection of rank r, and satisfies

$$2\mathfrak{Q}^{(n,r)} - I \in \mathrm{sgn}\left(\mathrm{GL}_n(\mathbb{R}) \cap \mathrm{span}_{\mathbb{R}}\{I, \mathfrak{P}_3^{(n)}, \mathfrak{P}_4^{(n)}\}\right).$$

Proof. The matrix $\mathfrak{Q}^{(n,r)}$ is a projection by definition of the map sgn. By Proposition 4.4, the matrix $n(\mathfrak{P}_3^{(n)} + \mathfrak{P}_4^{(n)})$ has eigenvalues $\{0, 2, \ldots, 2n-2\}$ if n is odd and $\{1, 3, \ldots, 2n-1\}$ if n is even. Therefore $(2r - \frac{1}{2})I - n(\mathfrak{P}_3^{(n)} + \mathfrak{P}_4^{(n)})$ has r positive eigenvalues and $n - r$ negative eigenvalues. Consequently, the multiplicities of eigenvalues 1 and -1 of $\mathrm{sgn}((2r - \frac{1}{2})I - n(\mathfrak{P}_3^{(n)} + \mathfrak{P}_4^{(n)}))$ are r and $n - r$, respectively. Hence the rank of $\mathfrak{Q}^{(n,r)}$ is r. □

Remark 5.7. For $r \leq n$ let $|e_1\rangle, \ldots, |e_r\rangle \in \mathbb{R}^n$ be unit eigenvectors of $\mathfrak{P}_3^{(n)} + \mathfrak{P}_4^{(n)}$ corresponding to the smallest r eigenvalues in increasing order (note that $|e_i\rangle$ are uniquely determined up to a sign because $\mathfrak{P}_3^{(n)} + \mathfrak{P}_4^{(n)}$ has n distinct eigenvalues). Then

$$\mathfrak{Q}^{(n,r)} = |e_1\rangle\langle e_1| + \cdots + |e_r\rangle\langle e_r|\,.$$

For concrete matrix representations of $\mathfrak{Q}^{(n,r)}$ when $1 \leq r < n \leq 6$, see Appendix A. While this is arguably a simpler and computationally more available definition of $\mathfrak{Q}^{(n,r)}$ than the original in Proposition 5.6, the presentation in terms of the sgn map is critical in establishing the self-test of Theorem 5.10 below.

Remark 5.8. Let us determine the normalized traces of $\mathfrak{P}_i^{(n)}\mathfrak{Q}^{(n,r)}$ for $r < \frac{n}{2}$. Clearly, $\tau\left(\mathfrak{Q}^{(n,r)}\right) = \frac{r}{n}$. By Proposition 3.1 there exists a unitary $U \in \mathrm{M}_n(\mathbb{C})$ such that $U\mathfrak{P}_3^{(n)}U^* = \mathfrak{P}_4^{(n)}$ and $U\mathfrak{P}_4^{(n)}U^* = \mathfrak{P}_3^{(n)}$, and therefore $\mathrm{tr}\left(\mathfrak{P}_3^{(n)}\mathfrak{Q}^{(n,r)}\right) = \mathrm{tr}\left(\mathfrak{P}_4^{(n)}\mathfrak{Q}^{(n,r)}\right)$. Thus

$$\tau\left(\mathfrak{P}_i^{(n)}\mathfrak{Q}^{(n,r)}\right) = \frac{1}{2}\tau\left(\mathfrak{Q}^{(n,r)}\left(\mathfrak{P}_3^{(n)} + \mathfrak{P}_4^{(n)}\right)\mathfrak{Q}^{(n,r)}\right) = \frac{r}{2n^2}\left(r - \frac{1-(-1)^n}{2}\right)$$

for $i = 3, 4$ by Proposition 4.4, since $\mathrm{tr}(\mathfrak{Q}^{(n,r)}(\mathfrak{P}_3^{(n)} + \mathfrak{P}_4^{(n)})\mathfrak{Q}^{(n,r)})$ is the sum of smallest r eigenvalues of $\mathfrak{P}_3^{(n)} + \mathfrak{P}_4^{(n)}$ by Remark 5.7. Since $r < \frac{n}{2}$, Proposition 4.5 and Remark 5.7 imply $\mathrm{tr}(\mathfrak{Q}^{(n,r)}\mathfrak{P}_1^{(n)}\mathfrak{Q}^{(n,r)}) = \mathrm{tr}(\mathfrak{Q}^{(n,r)}\mathfrak{P}_2^{(n)}\mathfrak{Q}^{(n,r)})$. By the defining relation of $\mathfrak{P}_i^{(n)}$ we then obtain

$$\tau\left(\mathfrak{P}_i^{(n)}\mathfrak{Q}^{(n,r)}\right) = \frac{1}{2}\left(\left(2 - \frac{1}{n}\right)\tau\left(\mathfrak{Q}^{(n,r)}\right) - \tau\left(\mathfrak{P}_3^{(n)}\mathfrak{Q}^{(n,r)}\right) - \tau\left(\mathfrak{P}_4^{(n)}\mathfrak{Q}^{(n,r)}\right)\right)$$

for $i = 1, 2$.

Definition 5.9. Given $n, r \in \mathbb{N}$ with $r < n$, let $\mathfrak{P}_i^{(n)}$ be as in Proposition 3.1, and let $\mathfrak{Q}^{(n,r)}$ be as in Proposition 5.6. Let $\mathcal{S}_{n,r}$ be the $(5,4)$-input $(2,2)$-output bipartite strategy

$$\left(|\phi_n\rangle\,; \left(\mathfrak{P}_i^{(n)}, I - \mathfrak{P}_i^{(n)}\right)_{i=1}^4, (\mathfrak{Q}^{(n,r)}, I - \mathfrak{Q}^{(n,r)}); \left(\mathfrak{P}_i^{(n)}, I - \mathfrak{P}_i^{(n)}\right)_{i=1}^4\right).$$

Since $\mathcal{S}_{n,r}$ is an extension of $\mathcal{S}_n$, its correlation is determined by that of $\mathcal{S}_n$ and

$$\begin{aligned} p(1|5) &= \langle\phi_n|\,\mathfrak{Q}^{(n,r)} \otimes I\,|\phi_n\rangle = \tau\left(\mathfrak{Q}^{(n,r)}\right), \\ p(1,1|i,5) &= \langle\phi_n|\,\mathfrak{Q}^{(n,r)} \otimes \mathfrak{P}_j^{(n)}\,|\phi_n\rangle = \tau\left(\mathfrak{P}_i^{(n)}\mathfrak{Q}^{(n,r)}\right) \end{aligned}$$

for $i = 1, \ldots, 4$, which are computed in Remark 5.8.

Let $n, r \in \mathbb{N}$ with $r < n$. If $r = \frac{n}{2}$, then a binary projective measurement of dimension n and rank r is up to a unitary basis change contained in the self-tested strategy $\mathcal{S}_n$. Otherwise, a binary projective measurement of dimension n and rank r is contained, up to a unitary basis change and a reordering of outputs, in $\mathcal{S}_{n,r}$ or $\mathcal{S}_{n,n-r}$. For this reason, let us explicitly determine the correlation of $\mathcal{S}_{n,r}$ only for $r < \frac{n}{2}$. Since $\mathcal{S}_{n,r}$ is an extension of $\mathcal{S}_n$ (whose correlation is given in Subsection 5.1) and Remark 5.8 computes the additional inner products (for $r < \frac{n}{2}$), the correlation of $\mathcal{S}_{n,r}$ is determined by the vector

$$\left(p(1|j)\right)_{j=1}^5 = \left(\frac{\lfloor\frac{n}{2}\rfloor - (-1)^n}{n} \quad \frac{\lfloor\frac{n}{2}\rfloor}{n} \quad \frac{\lfloor\frac{n}{2}\rfloor}{n} \quad \frac{\lfloor\frac{n}{2}\rfloor}{n} \quad \frac{r}{n}\right)$$

and the 5×4 matrix $\left(p(1,1|i,j)\right)_{i,j}$

$$\begin{pmatrix} \frac{\lfloor \frac{n}{2} \rfloor - (-1)^n}{n} & \frac{(n-1)(\lfloor \frac{n}{2} \rfloor - (-1)^n)}{3n^2} & \frac{(n-1)(\lfloor \frac{n}{2} \rfloor - (-1)^n)}{3n^2} & \frac{(n-1)(\lfloor \frac{n}{2} \rfloor - (-1)^n)}{3n^2} \\ . & \frac{\lfloor \frac{n}{2} \rfloor}{n} & \frac{(n-1)(2n-1+3(-1)^n)}{12n^2} & \frac{(n-1)(2n-1+3(-1)^n)}{12n^2} \\ . & . & \frac{\lfloor \frac{n}{2} \rfloor}{n} & \frac{(n-1)(2n-1+3(-1)^n)}{12n^2} \\ . & . & . & \frac{\lfloor \frac{n}{2} \rfloor}{n} \\ \frac{r(4n-2r-1-(-1)^n)}{4n^2} & \frac{r(4n-2r-1-(-1)^n)}{4n^2} & \frac{r(2r-1+(-1)^n)}{4n^2} & \frac{r(2r-1+(-1)^n)}{4n^2} \end{pmatrix}$$

where the missing entries are determined by $p(1,1|i,j) = p(1,1|j,i)$ for $i,j \leq 4$.

Theorem 5.10. *The strategy $\mathcal{S}_{n,r}$ is self-tested by its correlation for all $n, r \in \mathbb{N}$ with $r < n$.*

Proof. By Theorem 5.2, the strategy $\mathcal{S}_n$ is self-tested by its correlation. Note that the projection $\mathfrak{Q}^{(n,r)}$ lies in the image of the span of $\{\mathfrak{P}_i^{(n)}\}_{i=1}^4$ under the map sgn. Therefore $\mathcal{S}_{n,r}$ is self-tested by its correlation by Proposition 5.5. □

Corollary 5.11. *Every local binary projective measurement appears in a 5-input 2-output strategy that is self-tested by its correlation.*

Proof. Every binary PVM is, up to unitary basis change, determined by its dimension and ranks of its projections. Therefore it suffices to consider measurements $(\mathfrak{Q}^{(n,r)}, I - \mathfrak{Q}^{(n,r)})$, and these appear in the 5-input 2-output strategies $\mathcal{S}_{n,r}$, self-tested by Theorem 5.10. □

Finally, we generalize Theorem 5.10 to arbitrary K-PVMs. Given $r_1, \ldots, r_K, n \in \mathbb{N}$ with $n = r_1 + \cdots + r_K$, Remark 5.7 shows that

$$\mathfrak{Q}_a^{(r_1,\ldots,r_K)} := \mathfrak{Q}^{(n, r_1+\cdots+r_a)} - \mathfrak{Q}^{(n, r_1+\cdots+r_{a-1})}$$

is a projection of rank r_a for every $a = 1, \ldots, K$, and

$$\left(\mathfrak{Q}_a^{(r_1,\ldots,r_K)}\right)_{a=1}^K$$

is a K-PVM. To it we assign a certain bipartite strategy with a mixed number of inputs and outputs.

Definition 5.12. Let $r_1, \ldots, r_K, n \in \mathbb{N}$ with $n = r_1 + \cdots + r_K$. We define a bipartite strategy $\mathcal{S}_{r_1,\ldots,r_K}$ that has 4 inputs with 2 outputs and 1 input with K outputs for the first party, and 4 inputs with 2 outputs for the second party:

$$\mathcal{S}_{r_1,\ldots,r_K} = \left(|\phi_n\rangle ; \left(\mathfrak{P}_i^{(n)}, I - \mathfrak{P}_i^{(n)}\right)_{i=1}^4, \left(\mathfrak{Q}_a^{(r_1,\ldots,r_K)}\right)_{a=1}^K ; \left(\mathfrak{P}_i^{(n)}, I - \mathfrak{P}_i^{(n)}\right)_{i=1}^4 \right).$$

As for the correlation of $\mathcal{S}_{n,r}$ from Definition 5.9, one can derive similar (yet more involved) formulae for the correlation of $\mathcal{S}_{r_1,\ldots,r_K}$ using Remark 5.7, and Propositions 4.4 and 4.5.

Corollary 5.13. *Let $r_1, \dots, r_K, n \in \mathbb{N}$ with $n = r_1 + \cdots + r_K$ be arbitrary. Then the strategy $\mathcal{S}_{r_1,\dots,r_K}$ is self-tested by its correlation.*

In particular, every single local K-PVM appears in a self-tested strategy that has 8 inputs with 2 outputs and 1 input with K outputs.

Proof. Let

$$\mathcal{S} = \left(|\psi\rangle\,; (P_i, I - P_i)_{i=1}^4\,, (R_a)_{a=1}^K\,; (Q_i, I - Q_i)_{i=1}^4\right)$$

be a bipartite strategy with the same correlation as $\mathcal{S}_{r_1,\dots,r_K}$. Define bipartite strategies that have $3 + K$ inputs with 2 outputs for the first party, and 4 inputs with 2 outputs for the second party:

$$\begin{aligned}\widetilde{\mathcal{S}} = \Big(|\phi_n\rangle\,; \left(\mathfrak{P}_i^{(n)}, I - \mathfrak{P}_i^{(n)}\right)_{i=1}^4\,, \left(\mathfrak{Q}_a^{(n,r_1+\cdots+r_a)}, I - \mathfrak{Q}_a^{(n,r_1+\cdots+r_a)}\right)_{a=1}^{K-1}\,; \\ \left(\mathfrak{P}_i^{(n)}, I - \mathfrak{P}_i^{(n)}\right)_{i=1}^4\Big)\,,\end{aligned}$$

$$\begin{aligned}\mathcal{S}' = \Big(|\psi\rangle\,; (P_i, I - P_i)_{i=1}^4\,, (R_1 + \cdots + R_a, I - (R_1 + \cdots + R_a))_{a=1}^{K-1}\,; \\ (Q_i, I - Q_i)_{i=1}^4\Big)\,.\end{aligned}$$

Since the projections $\mathfrak{Q}^{(n,r_1+\cdots+r_a)}$ lie in the image of the span of $\{\mathfrak{P}_i^{(n)}\}_{i=1}^4$ under the map sgn by Proposition 5.6, and the strategy $\mathcal{S}_n$ is self-tested by Theorem 5.2, the strategy $\widetilde{\mathcal{S}}$ is self-tested by a repeated application of Proposition 5.5. Therefore $\widetilde{\mathcal{S}}$ is a local dilation of $\mathcal{S}'$. The same local isometries and the ancillary state show that $\mathcal{S}_{r_1,\dots,r_K}$ is a local dilation of $\mathcal{S}$. □

6 Obstructions to constant-sized self-tests

In a sense, maximally entangled states of all dimensions and single binary projective measurements of all dimensions and ranks can be self-tested with a constant number of inputs and outputs because they form discrete families of objects (i.e., they are parameterized by one and two natural parameters, respectively). On the other hand, there are no constant-sized self-tests for all entangled states, nor for all pairs of binary projective measurements, as implied by the results of this section (for self-tests with varying numbers of inputs, see [11] and [7]). The local dimension of subsystems in a quantum strategy is not directly responsible for the absence of constant-sized self-tests; rather, dimensions of parameter spaces describing states and pairs of binary projective measurements are the obstructions to existence of uniform self-tests. The proofs of statements in this section rely on notions from real algebraic geometry [4].

By the singular value decomposition, every bipartite $|\psi\rangle \in \mathbb{C}^n \otimes \mathbb{C}^n$ is, up to a left-right unitary basis change, equal to

$$\sum_{i=1}^n c_i\,|i\rangle|i\rangle$$

for $c_i \geq 0$ and $\sum_{i=1}^n c_i^2 = 1$. The numbers c_i are the *Schmidt coefficients* of $|\psi\rangle$. For example, all the Schmidt coefficients of $|\phi_n\rangle$ are $\frac{1}{\sqrt{n}}$. Note that $|\psi\rangle$ has full Schmidt rank if and only if $c_i > 0$ for all i.

Proposition 6.1. *Let $L, K, N \in \mathbb{N}$ satisfy*

$$L > (N(K-1)+1)^2.$$

Then for all $d_1, \ldots, d_L \in \mathbb{N}$ there exists a bipartite state with L distinct Schmidt coefficients of multiplicities $d_1, \ldots, d_L$ that cannot be self-tested by N-inputs and K-outputs.

Proof. Let $\mathbf{A}$ denote the set of all N-input K-output bipartite quantum strategies whose states are of the form

$$|\psi\rangle = \sum_{\ell=1}^{L} \lambda_\ell \sum_{i=d_{\ell-1}+1}^{d_\ell} |i\rangle|i\rangle\,, \qquad \lambda_1 < \cdots < \lambda_L \tag{9}$$

where $d_0 := 0$. In particular, the states in strategies from $\mathbf{A}$ have full Schmidt rank and L distinct Schmidt coefficients of multiplicities $d_1, \ldots, d_L$. Consider the action of $G := \mathrm{U}_{d_1}(\mathbb{C}) \times \cdots \times \mathrm{U}_{d_L}(\mathbb{C})$ on $\mathbf{A}$, given by

$$U \cdot \Big(|\psi\rangle\,; (\mathcal{M}_i)_i; (\mathcal{N}_j)_j \Big) = \Big(U \otimes U\,|\psi\rangle\,; (U\mathcal{M}_i U^*)_i; (U\mathcal{N}_j U^*)_j \Big)$$

for $U = \oplus_{\ell=1}^L U_\ell \in G$. Note that G encodes precisely all actions of local unitaries that preserve the form (9) of states in strategies from $\mathcal{S}$. Let $\mathbf{B}$ be the quotient of $\mathbf{A}$ with respect to the action of G, and let $\pi : \mathbf{A} \to \mathbf{B}$ be the canonical projection. Given $\mathcal{S} \in \mathbf{A}$ let $f(\mathcal{S}) \in \mathbb{R}^{d_1+\cdots+d_L} \otimes \mathbb{R}^{d_1+\cdots+d_L}$ be its state (i.e., f is the projection onto the first component of the strategy). To $\mathcal{S} = (|\psi\rangle\,; (\mathcal{M}_i)_i; (\mathcal{N}_j)_j)$ we also assign a tuple $g(\mathcal{S}) \in \mathbb{R}^{(N(K-1)+1)^2-1}$ consisting of

$$\begin{aligned}
&\langle\psi|\,\mathcal{M}_{i,a} \otimes \mathcal{N}_{j,b}\,|\psi\rangle\,, \qquad i,j = 1,\ldots,N,\ a,b = 1,\ldots,K-1,\\
&\langle\psi|\,\mathcal{M}_{i,a} \otimes I\,|\psi\rangle\,, \qquad i = 1,\ldots,N,\ a = 1,\ldots,K-1,\\
&\langle\psi|\,I \otimes \mathcal{N}_{j,b}\,|\psi\rangle\,, \qquad j = 1,\ldots,N,\ b = 1,\ldots,K-1.
\end{aligned}$$

Note that $g(\mathcal{S})$ determines the correlation of $\mathcal{S}$. The set $\mathbf{A}$ is semialgebraic and the maps f, g are semialgebraic [4, Section 2]. Furthermore, $\mathbf{B}$ is semialgebraic by [4, Proposition 2.2.4] since G is a semialgebraic group. The maps f, g factor through π, in the sense that there are semialgebraic maps f', g' on $\mathbf{B}$ satisfying $f' \circ \pi = f$ and $g' \circ \pi = g$. Let $\mathbf{C} \subseteq \mathbf{B}$ be the set of equivalence classes $[\mathcal{S}]$ such that $g'^{-1}(\{g'([\mathcal{S}])\}) = \{[\mathcal{S}]\}$. Then $\mathbf{C}$ is also semialgebraic by [4, Proposition 2.2.4]. Note that if $\mathcal{S} \in \mathbf{A}$ is self-tested by its correlation then $\pi(\mathcal{S}) \in \mathbf{C}$. Observe that $\dim f'(\mathbf{B}) = L - 1$, and $\dim \mathbf{C} = \dim g'(\mathbf{C}) \leq (N(K-1)+1)^2 - 1$ by [4, Theorem 2.8.8] since $g'|_{\mathbf{C}}$ is injective. Surjectivity of $f'|_{\mathbf{C}}$ would imply $\dim \mathbf{C} \geq L - 1$, contradicting $L - 1 > (N(K-1)+1)^2 - 1$. Therefore $f'|_{\mathbf{C}}$ is not surjective. In

particular, there exists a state $|\psi\rangle$ of the form (9) such that $\pi(\mathcal{S}) \notin \mathbf{C}$ for every $\mathcal{S} \in f^{-1}(\{|\psi\rangle\})$. In particular, no N-input K-output strategy containing $|\psi\rangle$ is self-tested by its correlation. □

By the renowned theorem of Halmos [15], a pair of projections $P_1, P_2 \in \mathrm{M}_n(\mathbb{C})$ is, up ot a unitary basis change, equal to

$$\begin{aligned} P_1 &= \varepsilon_1 \oplus \cdots \oplus \varepsilon_o \oplus \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \oplus \cdots \oplus \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \\ P_2 &= \varepsilon_1' \oplus \cdots \oplus \varepsilon_o' \oplus \begin{pmatrix} \frac{1+\cos\alpha_1}{2} & \frac{\sin\alpha_1}{2} \\ \frac{\sin\alpha_1}{2} & \frac{1-\cos\alpha_1}{2} \end{pmatrix} \oplus \cdots \oplus \begin{pmatrix} \frac{1+\cos\alpha_L}{2} & \frac{\sin\alpha_L}{2} \\ \frac{\sin\alpha_L}{2} & \frac{1-\cos\alpha_L}{2} \end{pmatrix}, \end{aligned} \tag{10}$$

where $\varepsilon_i, \varepsilon_i' \in \{0,1\}$ and $\alpha_\ell \in (0, \frac{\pi}{2})$. The number of distinct 2×2 blocks in (10) equals the number of distinct positive eigenvalues of $i(P_1P_2 - P_2P_1)$.

Proposition 6.2. *Let $L, N \in \mathbb{N}$ satisfy $L{+}1 > (N{+}1)^2$. Then for all $d_0, d_1, \ldots, d_L \in \mathbb{N}$ there exists a pair of binary projective measurements $(P_1, I-P_1), (P_2, I-P_2)$ with L distinct 2×2 blocks in (10) with multiplicities $d_1, \ldots, d_L$ and d_0 1×1 blocks, that cannot be self-tested by N-inputs and 2-outputs.*

Proof. We proceed analogously as in the proof of Proposition 6.1. The set $\mathbf{A}$ consists of N-input 2-output strategies whose first two measurements are given by projections of the form (10) with L angles α_ℓ of multiplicities $d_1, \ldots, d_L$. Let $f : \mathbf{A} \to \mathrm{M}_{d_0+2(d_1+\cdots+d_L)}(\mathbb{R})^2$ be the projection onto the pair of projections defining the first two measurements in a strategy. The group G consists of all unitaries preserving the structure of (10). Then $g, \mathbf{B}, \mathbf{C}$ are defined similarly as in the proof of Proposition 6.1, and the same dimension arguments apply. □

A Distinguished projections in low dimensions

As a demonstration of Remark 3.2, we construct $\mathfrak{P}_1^{(n)}, \ldots \mathfrak{P}_4^{(n)}$ for $n \leq 6$.
$n = 1$: $(1), (0), (0), (0)$
$n = 2$:

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} \frac{1}{4} & \frac{-\sqrt{3}}{4} \\ \frac{-\sqrt{3}}{4} & \frac{3}{4} \end{pmatrix}, \begin{pmatrix} \frac{1}{4} & \frac{\sqrt{3}}{4} \\ \frac{\sqrt{3}}{4} & \frac{3}{4} \end{pmatrix}$$

$n = 3$:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 \\ 0 & \frac{4}{9} & \frac{-2\sqrt{5}}{9} \\ 0 & \frac{-2\sqrt{5}}{9} & \frac{5}{9} \end{pmatrix}, \begin{pmatrix} \frac{1}{3} & \frac{1}{3\sqrt{3}} & \frac{\sqrt{5}}{3\sqrt{3}} \\ \frac{1}{3\sqrt{3}} & \frac{1}{9} & \frac{\sqrt{5}}{9} \\ \frac{\sqrt{5}}{3\sqrt{3}} & \frac{\sqrt{5}}{9} & \frac{5}{9} \end{pmatrix}, \begin{pmatrix} \frac{1}{3} & \frac{-1}{3\sqrt{3}} & \frac{-\sqrt{5}}{3\sqrt{3}} \\ \frac{-1}{3\sqrt{3}} & \frac{1}{9} & \frac{\sqrt{5}}{9} \\ \frac{-\sqrt{5}}{3\sqrt{3}} & \frac{\sqrt{5}}{9} & \frac{5}{9} \end{pmatrix}$$

$n = 4$:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} \frac{1}{4} & 0 & \frac{-\sqrt{3}}{4} & 0 \\ 0 & 1 & 0 & 0 \\ \frac{-\sqrt{3}}{4} & 0 & \frac{3}{4} & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix},$$

$$\begin{pmatrix} \frac{1}{4} & \frac{-\sqrt{15}}{16} & \frac{\sqrt{3}}{8} & \frac{\sqrt{21}}{16} \\ \frac{-\sqrt{15}}{16} & \frac{3}{8} & \frac{-3\sqrt{5}}{16} & 0 \\ \frac{\sqrt{3}}{8} & \frac{-3\sqrt{5}}{16} & \frac{1}{2} & \frac{-\sqrt{7}}{16} \\ \frac{\sqrt{21}}{16} & 0 & \frac{-\sqrt{7}}{16} & \frac{7}{8} \end{pmatrix}, \begin{pmatrix} \frac{1}{4} & \frac{\sqrt{15}}{16} & \frac{\sqrt{3}}{8} & \frac{-\sqrt{21}}{16} \\ \frac{\sqrt{15}}{16} & \frac{3}{8} & \frac{3\sqrt{5}}{16} & 0 \\ \frac{\sqrt{3}}{8} & \frac{3\sqrt{5}}{16} & \frac{1}{2} & \frac{\sqrt{7}}{16} \\ \frac{-\sqrt{21}}{16} & 0 & \frac{\sqrt{7}}{16} & \frac{7}{8} \end{pmatrix}$$

$n = 5$:

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & \frac{4}{25} & 0 & \frac{-2\sqrt{21}}{25} & 0 \\ 0 & 0 & \frac{16}{25} & 0 & \frac{-12}{25} \\ 0 & \frac{-2\sqrt{21}}{25} & 0 & \frac{21}{25} & 0 \\ 0 & 0 & \frac{-12}{25} & 0 & \frac{9}{25} \end{pmatrix},$$

$$\begin{pmatrix} \frac{2}{5} & \frac{3}{5\sqrt{5}} & 0 & \frac{\sqrt{21}}{5\sqrt{5}} & 0 \\ \frac{3}{5\sqrt{5}} & \frac{8}{25} & \frac{\sqrt{7}}{25} & \frac{\sqrt{21}}{25} & \frac{3\sqrt{7}}{25} \\ 0 & \frac{\sqrt{7}}{25} & \frac{2}{25} & \frac{-\sqrt{3}}{25} & \frac{6}{25} \\ \frac{\sqrt{21}}{5\sqrt{5}} & \frac{\sqrt{21}}{25} & \frac{-\sqrt{3}}{25} & \frac{12}{25} & \frac{-3\sqrt{3}}{25} \\ 0 & \frac{3\sqrt{7}}{25} & \frac{6}{25} & \frac{-3\sqrt{3}}{25} & \frac{18}{25} \end{pmatrix}, \begin{pmatrix} \frac{2}{5} & \frac{-3}{5\sqrt{5}} & 0 & \frac{-\sqrt{21}}{5\sqrt{5}} & 0 \\ \frac{-3}{5\sqrt{5}} & \frac{8}{25} & \frac{-\sqrt{7}}{25} & \frac{\sqrt{21}}{25} & \frac{-3\sqrt{7}}{25} \\ 0 & \frac{-\sqrt{7}}{25} & \frac{2}{25} & \frac{\sqrt{3}}{25} & \frac{6}{25} \\ \frac{-\sqrt{21}}{5\sqrt{5}} & \frac{\sqrt{21}}{25} & \frac{\sqrt{3}}{25} & \frac{12}{25} & \frac{3\sqrt{3}}{25} \\ 0 & \frac{-3\sqrt{7}}{25} & \frac{6}{25} & \frac{3\sqrt{3}}{25} & \frac{18}{25} \end{pmatrix}$$

$n = 6$:

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} \frac{1}{9} & 0 & 0 & \frac{-2\sqrt{2}}{9} & 0 & 0 \\ 0 & \frac{4}{9} & 0 & 0 & \frac{-2\sqrt{5}}{9} & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ \frac{-2\sqrt{2}}{9} & 0 & 0 & \frac{8}{9} & 0 & 0 \\ 0 & \frac{-2\sqrt{5}}{9} & 0 & 0 & \frac{5}{9} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix},$$

$$\begin{pmatrix} \frac{13}{36} & \frac{1}{4\sqrt{3}} & \frac{-\sqrt{\frac{35}{3}}}{12} & \frac{\sqrt{2}}{9} & \frac{\sqrt{\frac{5}{3}}}{4} & 0 \\ \frac{1}{4\sqrt{3}} & \frac{7}{36} & 0 & \frac{-1}{4\sqrt{6}} & \frac{\sqrt{5}}{9} & \frac{\sqrt{\frac{55}{6}}}{12} \\ \frac{-\sqrt{\frac{35}{3}}}{12} & 0 & \frac{5}{12} & \frac{-\sqrt{\frac{35}{6}}}{6} & 0 & 0 \\ \frac{\sqrt{2}}{9} & \frac{-1}{4\sqrt{6}} & \frac{-\sqrt{\frac{35}{6}}}{6} & \frac{17}{36} & \frac{-\sqrt{\frac{5}{6}}}{4} & 0 \\ \frac{\sqrt{\frac{5}{3}}}{4} & \frac{\sqrt{5}}{9} & 0 & \frac{-\sqrt{\frac{5}{6}}}{4} & \frac{23}{36} & \frac{-\sqrt{\frac{11}{6}}}{12} \\ 0 & \frac{\sqrt{\frac{55}{6}}}{12} & 0 & 0 & \frac{-\sqrt{\frac{11}{6}}}{12} & \frac{11}{12} \end{pmatrix}, \begin{pmatrix} \frac{13}{36} & \frac{-1}{4\sqrt{3}} & \frac{\sqrt{\frac{35}{3}}}{12} & \frac{\sqrt{2}}{9} & \frac{-\sqrt{\frac{5}{3}}}{4} & 0 \\ \frac{-1}{4\sqrt{3}} & \frac{7}{36} & 0 & \frac{1}{4\sqrt{6}} & \frac{\sqrt{5}}{9} & \frac{-\sqrt{\frac{55}{6}}}{12} \\ \frac{\sqrt{\frac{35}{3}}}{12} & 0 & \frac{5}{12} & \frac{\sqrt{\frac{35}{6}}}{6} & 0 & 0 \\ \frac{\sqrt{2}}{9} & \frac{1}{4\sqrt{6}} & \frac{\sqrt{\frac{35}{6}}}{6} & \frac{17}{36} & \frac{\sqrt{\frac{5}{6}}}{4} & 0 \\ \frac{-\sqrt{\frac{5}{3}}}{4} & \frac{\sqrt{5}}{9} & 0 & \frac{\sqrt{\frac{5}{6}}}{4} & \frac{23}{36} & \frac{\sqrt{\frac{11}{6}}}{12} \\ 0 & \frac{-\sqrt{\frac{55}{6}}}{12} & 0 & 0 & \frac{\sqrt{\frac{11}{6}}}{12} & \frac{11}{12} \end{pmatrix}$$

To obtain $\mathfrak{Q}_{n,r}$, one computes $\mathfrak{Q}_{n,r} = \sum_{i=1}^{r} |e_i\rangle\langle e_i|$ where $|e_i\rangle$ are unit eigenvectors of $\mathfrak{P}_3^{(n)} + \mathfrak{P}_4^{(n)}$ corresponding to the r smallest eigenvalues in increasing order. Examples for $r < n \leq 5$ are given below.

$n = 2$, $r = 1$:

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

$n = 3$, $r = 1, 2$:

$$\begin{pmatrix} 0 & 0 & 0 \\ 0 & \frac{5}{6} & \frac{-\sqrt{5}}{6} \\ 0 & \frac{-\sqrt{5}}{6} & \frac{1}{6} \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & \frac{5}{6} & \frac{-\sqrt{5}}{6} \\ 0 & \frac{-\sqrt{5}}{6} & \frac{1}{6} \end{pmatrix}$$

$n = 4$, $r = 1, 2, 3$:

$$\begin{pmatrix} \frac{3}{4} & 0 & \frac{-\sqrt{3}}{4} & 0 \\ 0 & 0 & 0 & 0 \\ \frac{-\sqrt{3}}{4} & 0 & \frac{1}{4} & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} \frac{3}{4} & 0 & \frac{-\sqrt{3}}{4} & 0 \\ 0 & 1 & 0 & 0 \\ \frac{-\sqrt{3}}{4} & 0 & \frac{1}{4} & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

$n = 5$, $r = 1, 2, 3, 4$:

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \frac{9}{10} & 0 & \frac{-3}{10} \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \frac{-3}{10} & 0 & \frac{1}{10} \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & \frac{7}{10} & 0 & \frac{-\sqrt{21}}{10} & 0 \\ 0 & 0 & \frac{9}{10} & 0 & \frac{-3}{10} \\ 0 & \frac{-\sqrt{21}}{10} & 0 & \frac{3}{10} & 0 \\ 0 & 0 & \frac{-3}{10} & 0 & \frac{1}{10} \end{pmatrix},$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & \frac{7}{10} & 0 & \frac{-\sqrt{21}}{10} & 0 \\ 0 & 0 & \frac{9}{10} & 0 & \frac{-3}{10} \\ 0 & \frac{-\sqrt{21}}{10} & 0 & \frac{3}{10} & 0 \\ 0 & 0 & \frac{-3}{10} & 0 & \frac{1}{10} \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & \frac{9}{10} & 0 & \frac{-3}{10} \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & \frac{-3}{10} & 0 & \frac{1}{10} \end{pmatrix}$$

$n = 6$, $r = 1, 2, 3, 4, 5$:

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \frac{5}{6} & 0 & 0 & \frac{-\sqrt{5}}{6} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \frac{-\sqrt{5}}{6} & 0 & 0 & \frac{1}{6} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} \frac{2}{3} & 0 & 0 & \frac{-\sqrt{2}}{3} & 0 & 0 \\ 0 & \frac{5}{6} & 0 & 0 & \frac{-\sqrt{5}}{6} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ \frac{-\sqrt{2}}{3} & 0 & 0 & \frac{1}{3} & 0 & 0 \\ 0 & \frac{-\sqrt{5}}{6} & 0 & 0 & \frac{1}{6} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix},$$

$$\begin{pmatrix} \frac{2}{3} & 0 & 0 & \frac{-\sqrt{2}}{3} & 0 & 0 \\ 0 & \frac{5}{6} & 0 & 0 & \frac{-\sqrt{5}}{6} & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ \frac{-\sqrt{2}}{3} & 0 & 0 & \frac{1}{3} & 0 & 0 \\ 0 & \frac{-\sqrt{5}}{6} & 0 & 0 & \frac{1}{6} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & \frac{5}{6} & 0 & 0 & \frac{-\sqrt{5}}{6} & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & \frac{-\sqrt{5}}{6} & 0 & 0 & \frac{1}{6} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

References

[1] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani. Device-independent security of quantum cryptography against collective attacks. *Phys. Rev. Lett.*, 98:230501, 2007. https://doi.org/10.1103/PhysRevLett.98.230501.

[2] C. Bamps, S. Massar, and S. Pironio. Device-independent randomness generation with sublinear shared quantum resources. *Quantum*, 2(86):14 pp, 2018. https://doi.org/10.22331/q-2018-08-22-86.

[3] B. Blackadar. *Operator algebras*, volume 122 of *Encyclopaedia of Mathematical Sciences*. Springer-Verlag, Berlin, 2006. https://doi.org/10.1007/3-540-28517-2.

[4] J. Bochnak, M. Coste, and M.-F. Roy. *Real algebraic geometry*, volume 36 of *Results in Mathematics and Related Areas*. Springer-Verlag Berlin Heidelberg, 1998. https://doi.org/10.1007/978-3-662-03718-8.

[5] J. Bowles, I. Šupić, D. Cavalcanti, and A. Acín. Device-independent entanglement certification of all entangled states. *Phys. Rev. Lett.*, 121:180503, 2018. https://doi.org/10.1103/PhysRevLett.121.180503.

[6] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner. Bell nonlocality. *Rev. Mod. Phys.*, 86:419–478, 2014. https://doi.org/10.1103/RevModPhys.86.419.

[7] R. Chen, L. Mančinska, and J. Volčič. All real projective measurements can be self-tested. *arXiv*, 2302.00974:24 pp, 2023. https://doi.org/10.48550/arXiv.2302.00974.

[8] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.*, 23:880–884, 1969. https://doi.org/10.1103/PhysRevLett.23.880.

[9] A. Coladangelo. Parallel self-testing of (tilted) epr pairs via copies of (tilted) chsh and the magic square game. *Quantum Info. Comput.*, 17(9–10):831–865, 2017. https://doi.org/10.26421/QIC17.9-10-6.

[10] A. Coladangelo, K. T. Goh, and V. Scarani. All pure bipartite entangled states can be self-tested. *Nat. Commun.*, 8:15485, 2017. https://doi.org/10.1038/ncomms15485.

[11] A. Coladangelo, A. B. Grilo, S. Jeffery, and T. Vidick. Verifier-on-a-leash: new schemes for verifiable delegated quantum computation, with quasilinear resources. In *Advances in Cryptology – EUROCRYPT 2019*, pages 247–277. Springer International Publishing, 2019. https://doi.org/10.1007/978-3-030-17659-4_9.

[12] R. Faleiro and M. Goulão. Device-independent quantum authorization based on the clauser-horne-shimony-holt game. *Phys. Rev. A*, 103:022430, 2021. https://doi.org/10.1103/PhysRevA.103.022430.

[13] J. Fitzsimons, Z. Ji, T. Vidick, and H. Yuen. Quantum proof systems for iterated exponential time, and beyond. In *Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing*, STOC 2019, page 473–480. Association for Computing Machinery, 2019. https://doi.org/10.1145/3313276.3316343.

[14] H. Fu. Constant-sized correlations are sufficient to self-test maximally entangled states with unbounded dimension. *Quantum*, 6(614):16 pp, 2022. https://doi.org/10.22331/q-2022-01-03-614.

[15] P. R. Halmos. Two subspaces. *Trans. Amer. Math. Soc.*, 144:381–389, 1969. https://doi.org/10.2307/1995288.

[16] B. Hensen, H. Bernien, A. E. Dréau, A. Reiserer, N. Kalb, M. S. Blok, J. Ruitenberg, R. F. L. Vermeulen, R. N. Schouten, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, M. Markham, D. J. Twitchen, D. Elkouss, S. Wehner, T. H. Taminiau, and R. Hanson. Loophole-free bell inequality violation using electron spins separated by 1.3 kilometres. *Nature*, 526:682–686, 2015. https://doi.org/10.1038/nature15759.

[17] Z. Ji, A. Natarajan, T. Vidick, J. Wright, and H. Yuen. MIP* = RE. *Commun. ACM*, 64:131–138, 2021. https://doi.org/10.1145/3485628.

[18] S. A. Kruglyak, V. I. Rabanovich, and Y. S. Samoĭlenko. On sums of projections. *Funct. Anal. its Appl.*, 36(3):182–195, 2002. https://doi.org/10.1023/A:1020193804109.

[19] L. Mančinska, J. Prakash, and C. Schafhauser. Constant-sized robust self-tests for states and measurements of unbounded dimension. *arXiv*, 2103.01729:38 pp, 2021. https://doi.org/10.48550/arXiv.2103.01729.

[20] D. Mayers and A. Yao. Self testing quantum apparatus. *Quantum Info. Comput.*, 4(4):273–286, 2004. https://doi.org/10.48550/arXiv.quant-ph/0307205.

[21] M. McKague. Self-testing in parallel with chsh. *Quantum*, 1(1):8 pp, 2017. https://doi.org/10.22331/Q-2017-04-25-1.

[22] C. A. Miller and Y. Shi. Robust protocols for securely expanding randomness and distributing keys using untrusted quantum devices. *J. ACM*, 63(4), 2016. https://doi.org/10.1145/2885493.

[23] S. Sarkar, J. J. Borkała, C. Jebarathinam, O. Makuta, D. Saha, and R. Augusiak. 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. https://doi.org/10.1103/PhysRevApplied.19.034038.

[24] S. Sarkar, D. Saha, J. Kaniewski, and R. Augusiak. Self-testing quantum systems of arbitrary local dimension with minimal number of measurements. *Npj Quantum Inf.*, 7(151):5 pp, 2021. https://doi.org/10.1038/s41534-021-00490-3.

[25] S. Storz, J. Schär, A. Kulikov, P. Magnard, P. Kurpiers, J. Lütolf, T. Walter, A. Copetudo, K. Reuer, A. Akin, J.-C. Besse, M. Gabureac, G. J. Norris, A. Rosario, F. Martin, J. Martinez, W. Amaya, M. W. Mitchell, C. Abellan, J.-D. Bancal, N. Sangouard, B. Royer, A. Blais, and A. Wallraff. Loophole-free bell inequality violation with superconducting circuits. *Nature*, 617:265–270, 2023. https://doi.org/10.1038/s41586-023-05885-0.

[26] I. Šupić and J. Bowles. Self-testing of quantum systems: a review. *Quantum*, 4(337):62 pp, 2020. https://doi.org/10.22331/Q-2020-09-30-337.

[27] I. Šupić, J. Bowles, M.-O. Renou, A. Acín, and M. J. Hoban. Quantum networks self-test all entangled states. *Nat. Phys.*, 19(5):670–675, 2023. https://doi.org/10.1038/s41567-023-01945-4.

[28] B. S. Tsirel'son. Quantum analogues of the bell inequalities. the case of two spatially separated domains. *J. Sov. Math.*, 36:557–570, 1987. https://doi.org/10.1007/BF01663472.

[29] T. H. Yang and M. Navascués. Robust self-testing of unknown quantum systems into any entangled two-qubit states. *Phys. Rev. A*, 87:050102, 2013. https://doi.org/10.1103/PhysRevA.87.050102.