MAXIMAL DEVICE-INDEPENDENT RANDOMNESS IN EVERY DIMENSION

MÁTÉ FARKAS, JURIJ VOLČIČ, SIGURD A. L. STORGAARD, RANYILIU CHEN, AND LAURA MANČINSKA

ABSTRACT. Random numbers are used in a wide range of sciences. In many applications, generating unpredictable *private* random numbers is indispensable. Device-independent quantum random number generation is a framework that makes use of the intrinsic randomness of quantum processes to generate numbers that are fundamentally unpredictable according to our current understanding of physics. While device-independent quantum random number generation is an exceptional theoretical feat, the difficulty of controlling quantum systems makes it challenging to carry out in practice. It is therefore desirable to harness the full power of the quantum degrees of freedom (the dimension) that one can control. It is known that no more than $2\log(d)$ bits of private device-independent randomness can be extracted from a quantum system of local dimension d. In this paper we demonstrate that this bound can be achieved for all dimensions d by providing a family of explicit protocols. In order to obtain our result, we develop new certification techniques that can be of wider interest in device-independent applications for scenarios in which complete certification ('self-testing') is impossible or impractical.

CONTENTS

Date: July 25, 2025.

Key words and phrases. Randomness, conditional quantum entropy, device-independent certification, Bell inequalities, informationally complete positive operator-valued measures.

RC, LM, SS were in part supported by Villum Fonden via Villum Young Investigator grant (No 37532). LM and SS additionally acknowledge support from ERC grant (QInteract, Grant Agreement No 101078107). JV was supported by the NSF grant DMS-2348720.

1. Introduction

Randomness is an essential resource in many disciplines of science. It is useful for generating samples for simulation [KGV83] or training data, and various computational models rely on randomized algorithms [AB09]. For some of these applications, the *privacy* of the random numbers is not essential. That is, it is not a problem if third parties have access to the random numbers. In fact, in some cases deterministic *pseudo-random* numbers are advantageous for reproducibility. In other applications, however, truly unpredictable *private random numbers* are indispensable. This means that no third party should be able to a priori guess the random numbers. A prominent application is cryptography, where random numbers are widely used in encryption and decryption schemes [Sha48]. It is crucial for the security of such cryptographic protocols that these random numbers are private, and only the encoder and the decoder have access to them. In particular, no potential eavesdropper should be able to predict these numbers.

Any random number is ultimately generated by some physical process—a roll of a die, an output of a computer algorithm, atmospheric noise, etc. If this process is described by classical physics, then the generated number is technically pseudo-random: perfect knowledge of the initial conditions of the system generating the random numbers makes it possible to perfectly predict these numbers, due to the deterministic nature of classical physical laws. Therefore, to generate truly private random numbers, the underlying physical process must be quantum: the fundamentally probabilistic nature of quantum theory makes it impossible to predict the outcome of certain quantum mechanical experiments. Therefore, quantum measurements have the potential to generate private randomness.

Importantly, unpredictability for the user does not necessarily imply private randomness, even if quantum mechanical processes were used to generate the random numbers. Consider the case of generating randomness by measuring the quantum state $\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)$ in the basis $\{|0\rangle, |1\rangle\}$. The outcome of this measurement is a perfectly random bit. However, the privacy of this bit cannot be guaranteed unless the state and the measurement are characterized and trusted. Indeed, these measurement statistics are also compatible with measuring one half of a bipartite state $\frac{1}{\sqrt{2}}(|0\rangle\otimes|0\rangle+|1\rangle\otimes|1\rangle)$ in the basis $\{|0\rangle, |1\rangle\}$. An eavesdropper having access to the other half can then perfectly predict the outcome of this measurement by also measuring in the basis $\{|0\rangle, |1\rangle\}$, and thus the randomness is not private.

The framework that allows for certifying private randomness only from observed data (without a priori characterization of states and measurements) is called *device-independent quantum random number generation* (DIQRNG) [Col07; PAM+10; VV12]. This framework requires the use of a bipartite quantum system, and the private randomness of measurements performed on one half of the system can be certified based on the full bipartite measurement statistics. Crucially, this certification is based only on the correctness of quantum theory, and on the assumption that the two laboratories measuring the two systems do not leak information (a necessary assumption in any private randomness certification protocol). Importantly, DIQRNG replaces unverifiable computational assumptions (often used in classical cryptography [RSA78; Reg09], and in some quantum protocols [MDC+21; MBB+23]) with information-theoretic security.

Various DIQRNG protocols have been proposed and experimentally demonstrated [LZL+21; SZB+21; LLR+21], and less secure, device-*dependent*, variants are also available commercially [Qua24; Tos24]. One of the main challenges of true DIQRNG is its resource-intensity. In order to generate private random numbers, high-quality entangled quantum systems and quantum measurement devices need to be manufactured and operated reliably. We address the fundamental question of how much device-independent randomness can be generated using fixed quantum resources. Namely, we fix the controllable degrees of freedom—the *dimension*—of an entangled quantum state. Scaling up fully controllable dimensions is a major practical challenge in quantum technologies [AAB+19; MLA+22; AAA+23], and therefore taking full advantage of the available resources is crucial. Importantly, while we are interested in device-independent randomness that can be generated using systems of a fixed dimension, we do not assume the dimension of the system in the security proofs. We are simply interested in the certifiable device-independent randomness if the honest implementation is of a fixed dimension.

It is known that if a bipartite quantum state is locally d-dimensional, a fundamental upper bound on the certifiable private randomness is $2\log(d)$ bits[1]. Apart from the cases of $d = 2$ [APV+16] and $d = 3$ [BJS+22], however, it was previously unknown whether this fundamental limit can be achieved, and if so, what protocol should be used. In this work, we fully solve this problem. We show that the fundamental limit of $2\log(d)$ bits of private (device-independent) randomness can be extracted from locally d-dimensional systems in every dimension d. Moreover, our proof is constructive, providing an explicit protocol that certifies the maximal randomness. The techniques we employ are similar to *self-testing*, which is a powerful certification tool in quantum information theory [ŠB20]. While self-testing allows for essentially uniquely identifying quantum states and measurements from observed experimental statistics, our certification tools allow for more freedom, certifying only the properties essential for randomness certification. Furthermore, generating $2\log(d)$ bits of randomness from locally d-dimensional systems necessarily requires non-projective measurements[2], and therefore standard self-testing techniques cannot be applied. We believe that our framework opens up new possibilities

[1]This is the amount of randomness certifiable locally. Global randomness certification is not a straightforward extension of local randomness [BJS+22], and this manuscript is primarily concerned with local randomness.

[2]As projective measurements in dimension d have at most d outcomes, the randomness from them is limited to $\log(d)$ bits, and this limit can be achieved for every d, see e.g. Ref. [TFR+21].

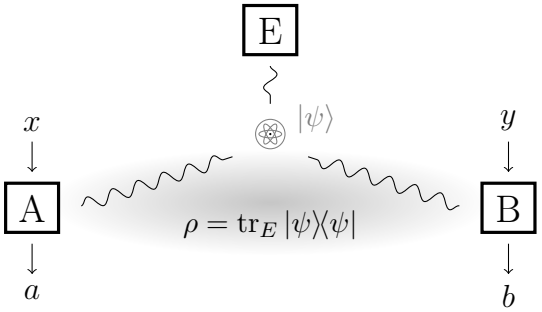

FIGURE 1. Bell scenario including an eavesdropper.

for practical device-independent certification methods in scenarios where self-testing is too demanding, unnecessary or impossible.

2. Preliminaries

The basic setup of DIQRNG is a so-called bipartite *Bell scenario* [BCP+14]. Two experimenters, commonly referred to as Alice and Bob, share a bipartite physical system and perform various measurements on their respective parts. They repeat the experiment many times in order to be able to estimate the outcome probabilities of the measurements. All conclusions of the experiment are drawn from the measurement statistics, and from the assumptions that quantum theory is correct and Alice's and Bob's laboratories do not leak any information. Crucially, Alice and Bob do not need any prior knowledge of the physical system or their measurement devices.

In quantum theory, physical systems are associated with a complex Hilbert space $\mathcal{H}$, which we assume to be finite-dimensional in this work. We will often refer to the set of matrices (linear operators) on a d-dimensional complex Hilbert space as $M_d(\mathbb{C})$. A bipartite system is associated with a tensor product of two Hilbert spaces, $\mathcal{H}_A \otimes \mathcal{H}_B$, and the state of the system is described by a positive semidefinite operator ρ on this Hilbert space with unit trace. Measurements on a Hilbert space are described by positive operator-valued measures (POVMs), which in our case correspond to a tuple of positive semidefinite operators that add up to the identity I. In a Bell scenario, Alice has various measurement settings labeled by x, and the possible outcomes of her measurements are labeled by a (the number of possible outcomes may depend on x). Similarly, Bob's settings are labeled by y and his outcomes by b. An experiment is characterized by the *correlation*, that is, the probabilities of Alice observing outcome a and Bob b, upon choosing measurement settings x and y. According to quantum theory, these probabilities are given by

$$p(a,b|x,y) = \mathrm{tr}[\rho(A_a^x \otimes B_b^y)], \tag{2.1}$$

where ρ is a quantum state on $\mathcal{H}_A \otimes \mathcal{H}_B$, $(A_a^x)_a$ is a POVM on $\mathcal{H}_A$ for all x and $(B_b^y)_b$ is a POVM on $\mathcal{H}_B$ for all y.

The aim of DIQRNG is to lower bound the randomness of certain measurement outcomes from the point of view of a potential eavesdropper, Eve, who holds part of a tripartite purification of ρ (see Figure 1 for a schematic representation). Moreover, this

bound must be solely based on the observed correlation. In this work, we are interested in the asymptotic rate of randomness of the outcome of a single setting x of Alice. This rate quantifies the randomness of a single measurement outcome of the measurement x, in the limit of Alice and Bob performing the experiment infinitely many times. Notice that while this setup is formulated under the assumption that the quantum state and measurements behave the same way in every experimental round (i.i.d. assumption), this assumption can be lifted in the asymptotic limit due to the entropy accumulation theorem [ADF+18; DFR20]. It is also worth noting that probability estimation techniques [ZKB18; ZFK20], which have been applied in the previously mentioned experimental demonstrations [LZL+21; SZB+21; LLR+21], can also be applied to our protocols.

It is well-known [TCR09] that the asymptotic rate of randomness is lower bounded by the conditional von Neumann entropy $H(\mathrm{A}|E)_{\rho_{\mathrm{A}E}}$ of the classical-quantum state

$$\rho_{\mathrm{A}E} = \sum_a |a\rangle\langle a|_{\mathrm{A}} \otimes \mathrm{tr}_{AB}[|\psi\rangle\langle\psi|(A_a^x \otimes I_B \otimes I_E)], \tag{2.2}$$

where $(A_a^x)_a$ is the POVM describing the measurement for setting x and $|\psi\rangle$ is a purification of the state ρ from Eq. (2.1). Note that we denote the classical register (post-measurement) of Alice by an upright A and the quantum register (pre-measurement) by an italic A. Since in a device-independent setting the only thing we assume is the observed correlation, $H(\mathrm{A}|E)_{\rho_{\mathrm{A}E}}$ needs to be minimized over all possible physical realizations compatible with the observed correlation $p(a,b|x,y)$ or with some function $f[p(a,b|x,y)]$ of it. That is, the minimization is taken over all possible Hilbert spaces $\mathcal{H}_A, \mathcal{H}_B$ and $\mathcal{H}_E$ and all states $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E$ and POVMs $(A_a^x)_a$ on $\mathcal{H}_A$ and $(B_b^y)_b$ on $\mathcal{H}_B$ such that

$$f[p(a,b|x,y)] = f[\langle\psi| \left(A_a^x \otimes B_b^y \otimes I_E\right) |\psi\rangle].$$

In general, this minimization is an extremely difficult task. In certain small and/or symmetric scenarios, analytic results exist, demonstrating that DIQRNG is possible in principle [Col07; PAM+10; VV12; ADF+18]. General methods for bounding the rate of randomness usually rely on numerics [BSS14; BFF21; BFF24], and scale rather badly with the number of measurement settings and outcomes.

In this work, we analytically carry out the above minimization for a class of correlations. In particular, we are interested in bounding the device-independent randomness from certain correlations that arise from measuring a quantum state that is locally d-dimensional, that is, $\mathcal{H}_A = \mathcal{H}_B = \mathbb{C}^d$ (note that while we are interested in correlations generated by locally d-dimensional states, we certify the randomness device-independently, that is, solely from the observed correlation). It is known that in this case the maximum possible certifiable device-independent randomness is upper bounded by $2\log(d)$ (see [APV+16] for a proof for the min-entropy), and we include a proof of this fact in Appendix A for completeness (for the von Neumann entropy). We prove that this fundamental bound can be achieved in every dimension d and we provide explicit protocols achieving this bound.

3. Setup and results

Our setup builds on the Bell scenario studied in [TFR+21]. The authors there propose a DIQRNG protocol and numerically prove that the protocol reaches close to 2 bits of randomness with locally 2-dimensional systems. For locally 3-dimensional systems, the authors can numerically certify approximately 3.03 bits of randomness, falling somewhat short of the fundamental bound $2\log(3) \approx 3.17$. Extending the numerical verification to larger dimensions is computationally extremely demanding. Moreover, extending the methods of [TFR+21] to arbitrary dimensions relies on the conjectured existence of symmetric informationally complete (SIC) POVMs in every dimension [Zau11].

To overcome previous limitations, we use the family of measurements that we introduce in this work, called *balanced informationally complete* (BIC) POVMs. Formally, a BIC-POVM in dimension d is a POVM of the form $\left(\frac{1}{d}P_j\right)_{j=1}^{d^2}$, where P_j are rank-1 projections that form a basis for $M_d(\mathbb{C})$. Unlike SIC-POVMs, BIC-POVMs exist in every dimension (see Appendix B), and may find broad use in other tasks where normally SIC-POVMs would be useful.

Our Bell scenario is parametrized by an integer $d \geq 2$ and a $d^2 \times d^2$ matrix $S = (s_{jk})_{j,k}$ that corresponds to a BIC-POVM. Specifically, we let $s_{jk} = \mathrm{tr}(P_j P_k)$ where $\left(\frac{1}{d}P_j\right)_{j=1}^{d^2}$ is a BIC-POVM. In our Bell scenario, Alice has $d^2(d^2-1)/2+1$ measurement settings. The first $d^2(d^2-1)/2$ settings are labeled by pairs jk such that $j,k \in [d^2]$ and $j<k$, where $[n] := \{1,\dots,n\}$, and these measurements have three outcomes each labeled by $a \in \{1,2,3\}$. The last measurement setting of Alice is labeled by $\mathbf{r}$ and this has d^2 outcomes labeled by $a \in [d^2]$. This is the measurement that Alice uses to generate randomness. On the other side, Bob has d^2 settings with two outcomes each, labeled by $b \in \{1,2\}$.

We introduce a *Bell function* (a linear function of correlations, equivalently referred to as a *Bell inequality*) with the aim that reaching its maximal value certifies the maximally entangled two-qudit state $|\varphi_d\rangle := \frac{1}{\sqrt{d}}\sum_{j=1}^{d}|j\rangle\otimes|j\rangle$ and a BIC-POVM $A_j^{\mathbf{r}} = \frac{1}{d}|e_j\rangle\langle e_j|$ such that $\left|\langle e_j|e_k\rangle\right|^2 = s_{jk}$ for all j,k. The function reads

$$
\begin{aligned}
&2\sum_{j<k}\sqrt{1-s_{jk}}\Big[p(1,1|jk,j)+p(2,1|jk,k)-p(1,1|jk,k)-p(2,1|jk,j)\Big]\\
&-\sum_{j<k}(1-s_{jk})\big[p_A(1|jk)+p_A(2|jk)\big]-d(d-2)\sum_{j=1}^{d^2}p_B(1|j)-\sum_{j=1}^{d^2}p(j,2|\mathbf{r},j),
\end{aligned}
\tag{3.1}
$$

where $\sum_{j<k}$ is short-hand for $\sum_{j=1}^{d^2-1}\sum_{k=j+1}^{d^2}$, and p_A and p_B are Alice's and Bob's marginal probabilities, respectively. For an explicit example of our construction in $d=2$, see Example C.1.

Every Bell function has a corresponding *Bell operator*, which is an operator-valued function of POVM elements A_a^x and B_b^y. In our case, the Bell operator reads

$$\begin{aligned} W_d := 2\sum_{j<k}\sqrt{1-s_{jk}}(A_1^{jk}-A_2^{jk})\otimes(B^j-B^k) - \sum_{j<k}(1-s_{jk})(A_1^{jk}+A_2^{jk})\otimes I \\ - d(d-2)\sum_{j=1}^{d^2} I\otimes B^j - \sum_{j=1}^{d^2} A_j^{\mathrm{r}}\otimes(I-B^j), \end{aligned} \tag{3.2}$$

where we introduced the notation $B^j := B_1^j$ (and therefore $B_2^j = I - B^j$). Note that in our notation we suppressed the dependence on the S matrix, as well as the fact W_d is a function of A_a^x and B_b^y. For a given set of POVMs with elements A_a^x and B_b^y and a given bipartite state ρ, the value of the Bell inequality is given by $\mathrm{tr}(W_d\rho)$.

One common way to show that some $\beta \in \mathbb{R}$ is an upper bound on the value of a Bell inequality is through a sum-of-squares decomposition of the *shifted* Bell operator $\beta I - W_d$. Specifically, if we can write

$$\beta I - W_d = \sum_i Q_i^* Q_i, \tag{3.3}$$

for some operator-valued functions Q_i of A_a^x and B_b^y (assuming that these form valid POVMs), then we have that for every set of POVMs with elements A_a^x and B_b^y and for every quantum state ρ,

$$\mathrm{tr}(W_d\rho) \leq \beta, \tag{3.4}$$

which is equivalent to saying that β is an upper bound on the value of the Bell inequality. The inequality in Eq. (3.4) comes from the fact that $Q_i^* Q_i$ is positive semidefinite for every A_a^x and B_b^y and that $\mathrm{tr}(\rho) = 1$ for every valid quantum state.

If Eq. (3.4) can be saturated then β is a tight bound. In this case, for every set of POVMs with elements A_a^x and B_b^y and every state ρ such that $\mathrm{tr}(W_d\rho) = \beta$ it must hold that $Q_i\rho = 0$ for all i. In some cases, these relations make it possible to essentially uniquely (up to local isometries) identify the quantum state and the POVMs that give rise to the maximal Bell violation. This is called *self-testing*, and it is a powerful tool in device-independent quantum information processing [ŠB20].

Importantly, in our DIQRNG protocol we would like to use a non-projective POVM (a BIC-POVM), and it is known that non-projective measurements cannot be self-tested due to Naimark's dilation theorem [BCK+23]. To certify our setup, we therefore develop new, weaker forms of self-testing. Based on the maximal value of our Bell inequalities we characterize the POVMs and the quantum state sufficiently so that we are able to bound the conditional von Neumann entropy of any state of the form in Eq. (2.2) compatible with the maximal value. Similar weaker forms of self-testing have been studied recently in the context of device-independent quantum information processing [Kan20; Far24]. Our techniques differ from these by certifying measurements *compressed onto the local support* of the state (see below), and by using the representation theory of measurement algebras. Crucially, we do not make any a priori assumptions on the state and measurements [BCK+23]. Our methods appear to be highly promising for further device-independent

applications beyond this work, in scenarios in which a complete self-testing statement is impossible or impractical.

Crucial in our analysis are the local supports of the state $\rho \in \mathrm{M}_{d_A}(\mathbb{C}) \otimes \mathrm{M}_{d_B}(\mathbb{C})$. We define $\mathrm{supp}_A\, \rho$ as the range of $\mathrm{tr}_B\, \rho \in \mathrm{M}_{d_A}(\mathbb{C})$, and $\mathrm{supp}_B\, \rho$ in an analogous way. We then define *compressions* onto the local supports. On Alice's Hilbert space, the compression of an operator X is defined as $\hat{X} := UXU^*$, where $U : \mathrm{supp}_A\, \rho \to \mathbb{C}^{d_A}$ is the inclusion, that is, U^*U is the identity on $\mathrm{supp}_A\, \rho$ and UU^* is the projection on $\mathbb{C}^{d_A}$ with range $\mathrm{supp}_A\, \rho$. Compressions on Bob's Hilbert space are defined analogously, also denoted by $\hat{X}$. The intuition behind considering compressed operators is that one cannot certify anything about the measurements outside the support of the state (the role of compressions onto the local support in self-testing of operators relative to the state [ŠB20] is elucidated in [BCK+23]).

The following proposition informally summarizes our certification results based on the maximal value of our Bell inequalities.

Proposition 3.1. *For every integer $d \geq 2$ and every S induced by a BIC-POVM, the maximum quantum value of the corresponding Bell inequality in Eq. (3.2) is d^2. Furthermore, if the value d^2 is reached using the state and measurements $\rho, A_a^{jk}, A_j^{\mathbf{r}}, B^j$, then*

i) ρ is supported on a Hilbert space $\bigoplus_\alpha \mathbb{C}^{e_\alpha} \otimes \mathbb{C}^{f_\alpha} \otimes \mathbb{C}^{r_\alpha d} \otimes \mathbb{C}^{r_\alpha d}$, where $e_\alpha, f_\alpha, r_\alpha \in \mathbb{N}$, and α is an element of a discrete index set. Up to local isometries, ρ is a mixture of states of the form

$$\bigoplus_\alpha |\chi_\alpha\rangle \otimes |\varphi_{r_\alpha d}\rangle\,, \qquad |\chi_\alpha\rangle \in \mathbb{C}^{e_\alpha} \otimes \mathbb{C}^{f_\alpha} \tag{3.5}$$

ii) Alice's and Bob's compressed operators satisfy

$$(\hat{A}_1^{jk})^2 = \hat{A}_1^{jk},\ (\hat{A}_2^{jk})^2 = \hat{A}_2^{jk},\ \hat{A}_1^{jk}\hat{A}_2^{jk} = 0 \quad \forall j < k, \tag{3.6}$$

$$(\hat{B}^j)^2 = \hat{B}^j \quad \forall j, \tag{3.7}$$

$$\sum_j \hat{B}^j = dI, \tag{3.8}$$

$$\hat{B}^j \hat{B}^k \hat{B}^j = s_{jk} \hat{B}^j \quad \forall j \neq k. \tag{3.9}$$

iii) Up to the same local isometry as for the state, the compressed elements of Alice's setting $\mathbf{r}$, acting on $\bigoplus_\alpha \mathbb{C}^{e_\alpha} \otimes \mathbb{C}^{r_\alpha d}$, are given by

$$\hat{A}_j^{\mathbf{r}} = \mathcal{N}_j + \bigoplus_\alpha \left(I_{e_\alpha} \otimes \frac{1}{d} \hat{C}_{j,\alpha} + W_{j,\alpha} \right) \tag{3.10}$$

where $\mathcal{N}_j$ acts on $\bigoplus_\alpha \mathbb{C}^{e_\alpha} \otimes \mathbb{C}^{r_\alpha d}$ and all of its diagonal (α, α)-blocks are zero. Moreover, we have $\mathrm{tr}_{\mathbb{C}^{r_\alpha d}}(W_{j,\alpha}) = 0$, and for every α the $\{\hat{C}_{j,\alpha}\}_j$ operators satisfy the same relations as the $\{\hat{B}^j\}_j$ operators, that is, Eqs. (3.7)–(3.9).

Note that d simply determines the number of inputs and outputs in the Bell inequality, and in deriving the maximal value we do not assume that the underlying state is locally d-dimensional. The proof is based on a sum-of-squares decomposition of the

shifted Bell operator (Appendix C) and on the representation theory of an algebra related to the associated BIC-POVM (Appendix D). The proof can be found in Appendix E.

Notice that we do not completely characterize the state up to local isometries. Instead, we certify the form in Eq. (3.5). Here, the index α labels the irreducible representations of the C*-algebra generated by the relations (3.7), (3.8) and (3.9). Both $\mathrm{supp}_A\,\rho$ and $\mathrm{supp}_B\,\rho$ decompose into a direct sum according to the irreducible representations, and we characterize the state on these subspaces. Notice in Eq. (3.5) that in every subspace we find a maximally entangled state of dimension $r_\alpha d$, tensored with some uncharacterized state $|\chi_\alpha\rangle$.

We also do not fully characterize the POVM $(A_j^{\mathbf{r}})_j$, as seen in Eq. (3.10). The characterization is, however, sufficient for certifying randomness. This is because $\hat{A}_j^{\mathbf{r}}$ acts trivially on the uncharacterized subspaces and subsystems of ρ, and acts like a BIC-POVM on the characterized part. Since on the characterized part the state is pure ($|\varphi_{r_\alpha d}\rangle$), no potential eavesdropper can be correlated to the state, since every purification of a pure state must be a product state. This intuition leads us to our main theorem:

Theorem 3.2. *Suppose the state ρ and measurement $(A_j^{\mathbf{r}})_j$ appear in an optimal quantum strategy for the Bell function (3.2), and let $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E$ be a purification of ρ. Then*

$$\sum_{j=1}^{d^2} |j\rangle\langle j|_{\mathrm{A}} \otimes \mathrm{tr}_{AB}\left[|\psi\rangle\langle\psi|(A_j^{\mathbf{r}} \otimes I_B \otimes I_E)\right] = \left(\frac{1}{d^2}\sum_{j=1}^{d^2} |j\rangle\langle j|\right) \otimes \sigma_E \tag{3.11}$$

for some state σ_E on $\mathcal{H}_E$.

In particular, the maximal value of the Bell inequality (3.2) certifies $2\log(d)$ bits of device-independent randomness from the outcome of the setting $\mathbf{r}$ of Alice. Since the maximal violation can be achieved using a locally d-dimensional state, the theoretical maximum device-independent randomness, $2\log(d)$ bits, can be achieved in every dimension d.

The proof of this theorem can be found in Appendix E. The value $2\log(d)$ comes from computing the conditional von Neumann entropy of the state in Eq. (3.11). A locally d-dimensional realization leading to the maximal value d^2 is given by $\rho = |\varphi_d\rangle\langle\varphi_d|$, $B^j = |e_j\rangle\langle e_j|$, where $\{\frac{1}{d}|e_j\rangle\langle e_j|\}_{j=1}^{d^2}$ form a BIC-POVM such that $\left|\langle e_j|e_k\rangle\right|^2 = s_{jk}$, $A_{1(2)}^{jk}$ being the transposition of the projection onto the eigenstate of $B^j - B^k$ with positive (negative) eigenvalue, and $A_j^{\mathbf{r}} = \frac{1}{d}|e_j\rangle\langle e_j|^{\mathrm{t}}$ (where all the transpositions are in the computational basis). In Proposition 3.1, this realization corresponds to a single value for the index α (let us denote this value by $\tilde{\alpha}$), and $e_{\tilde{\alpha}} = f_{\tilde{\alpha}} = r_{\tilde{\alpha}} = 1$, $\mathcal{N}_j = 0$, $W_{j,\tilde{\alpha}} = 0$, and $C_{j,\tilde{\alpha}} = |e_j\rangle\langle e_j|^{\mathrm{t}}$ for all j.

4. Discussion

Our main result establishes that the previously known fundamental bound on device-independent randomness can be achieved in every dimension. To prove this, we designed explicit protocols that reach the fundamental bound. Since the maximal randomness requires (by definition) non-projective POVMs, standard self-testing arguments do not

suffice for proving our result. As such, we developed new, weaker forms of self-testing, relying on the certification of compressed operators and the representation theory of measurement algebras. We expect our techniques to be highly useful in scenarios in which a full self-testing statement is not necessary, impossible, or impractical. This is particularly relevant in scenarios where non-projective measurements can be beneficial, or even optimal—such examples have been found e.g. in Bell non-locality [VB10] and quantum key distribution [Ben92; Ren04], and thus certifying non-projective measurements may find applications in these areas.

Let us address the practicality of physical implementations of non-projective measurements. Canonically, these are implemented by enlarging the Hilbert space with an ancillary system, and performing a joint projective measurement on the system and ancilla. As such, one might question whether our protocol is truly locally d-dimensional. Notice that importantly, the ancillary system is not shared between Alice and Bob but held only by Alice. Therefore, the entangled state is only locally d-dimensional. Moreover, in various standard physical implementations (e.g. spatial modes of photons) the ancillary system is purely a mathematical model, and there is no need to introduce an actual new physical system (e.g. a new photon) to implement a non-projective measurement [GTZ+23; GLV+24]. Therefore, in the sense of 'controllable degrees of freedom', our protocol can indeed be implemented using locally d dimensions.

Further regarding the practicality of our setup, one might notice that while the protocol generates $2\log(d)$ bits every time Alice measures $\mathbf{r}$, she has in total $d^2(d^2-1)/2+1$ measurement settings, which need to be chosen randomly. Notice, however, that these settings do not need to be chosen *uniformly* randomly. If Alice selects the setting $\mathbf{r}$ most of the time, she can generate arbitrarily close to $2\log(d)$ bits of randomness per measurement round. That is, she does not consume more randomness than what is generated. In fact, Alice only needs to consume a vanishing amount of randomness per measurement round. This approach is usually referred to as a spot-checking protocol [CVY13; MS17; LLR+21] and has been used in experimental demonstrations [LZL+21; SZB+21].

Our work opens up a couple of important future research directions, on top of the wider application of our certification methods. Following the discussion about the practicality, it would be desirable to work out the robustness of our protocol to experimental noise. This is a particularly promising research direction, since our protocol works with systems of arbitrary dimension, and it is known that systems of larger dimension could be more robust to noise [ZTV+21; DHM+21]. Moreover, the large freedom in the measurements (any BIC-POVM provides maximal randomness) provides ample potential candidate protocols. Since our certification is based on a Bell inequality (with quantifiable classical-quantum separation, see Appendix F), one possible avenue is to adapt robust self-testing techniques [BLM+09; YVB+14; Kan16; MPS24] to our certification methods. While it is plausible that this avenue is successful, quantifying the effect of noise on the representation-theoretic certification likely requires significant technical effort. As such, we leave the noise robustness quantification for a future study. Similarly, extending our analysis to the case of finite statistics is also of practical relevance, and should be the subject of a future work. At the same time, we note that numerical evidence supports the robustness of our protocols: for the SIC-POVM case in $d = 2$ and $d = 3$, Ref. [TFR+21]

contains semidefinite programming-based bounds on the min entropy in terms of the Bell inequality volation.

It would also be an interesting follow-up direction to figure out whether our protocols can be extended to certify maximal *global* device-independent randomness. That is, $2\log(d)$ bits on Alice's side and $2\log(d)$ bits on Bob's side. Proving this would require extending our certification methods to a new setting on Bob's side, corresponding to a BIC-POVM.

Last, the algebraic characterization of BIC-POVMs in Appendix B and G could provide new mathematical insights into the structure and famous existence problem of SIC-POVMs [Zau11], as SIC-POVMs are a class of BIC-POVMs. Further research into this algebraic characterization could also lead to other device-independent applications, similarly to what has been achieved with *mutually unbiased measurements* [TFR+21; CMF+22; FKN23].

Data availability

This work does not have any associated data.

APPENDICES

A. Fundamental bound on the device-independent randomness

The fundamental bound of $2\log(d)$ bits of device-independent randomness from locally d-dimensional states can be argued by considering *extremal* POVMs. In a fixed dimension, the set of POVMs forms a convex set. That is, one can take a convex combination of a POVM $(M_1,\dots,M_m)$ and $(N_1,\dots,N_m)$, given by $(\lambda M_1+(1-\lambda)N_1,\dots,\lambda M_m+(1-\lambda)N_m)$, which is again a POVM for every $\lambda\in[0,1]$. Furthermore, one can take convex combinations of POVMs with different numbers of outcomes, by appropriately padding the POVMs with zero operators. The set of POVMs endowed with this convex structure thus has extremal elements—POVMs that cannot be written as a non-trivial convex combination of two other POVMs. It is known from [DPP05] that extremal POVMs in dimension d can have at most d^2 non-zero elements. Consider then a correlation $p(a,b|x,y)=\mathrm{tr}[(A_a^x\otimes B_b^y)\rho]$ that can be realized in dimension d. In particular, by some locally d-dimensional entangled state ρ, and d-dimensional POVMs $\{(A_a^x)_a\}_x$ for Alice and $\{(B_b^y)_b\}_y$ for Bob. All POVMs decompose into extremal ones. In particular, for the POVM $(A_a^x)_a$ which we use for randomness extraction, we have $A_a^x=\sum_{e=0}^{k-1}p_eA_a^{x,e}$, where $\{p_e\}_e$ is a probability distribution and $\{(A_a^{x,e})_a\}_e$ are extremal POVMs and therefore have at most d^2 non-zero elements. Another realization of $p(a,b|x,y)$ is then given on the Hilbert space $\bigoplus_{e=0}^{k-1}\mathbb{C}^d\otimes\mathbb{C}^d$. The realization consists of a locally kd-dimensional state $\rho'=\bigoplus_{e=0}^{k-1}p_e\rho$ and kd-dimensional POVMs $(\tilde{A}_a^x)_a=\left(\bigoplus_{e=0}^{k-1}A_a^{x,e}\right)_a$ and $(\tilde{B}_b^y)_b=\left(\bigoplus_{e=0}^{k-1}B_b^y\right)_b$. A tripartite extension of ρ' is given by $\tilde{\rho}=\sum_{e=0}^{k-1}p_e\rho_e\otimes|e\rangle\langle e|$, where ρ_e equals ρ on the e-th copy of $\mathbb{C}^d\otimes\mathbb{C}^d$ and zero elsewhere, and $\{|e\rangle\}_{e=0}^{k-1}$ is an orthonormal basis on Eve's Hilbert space. While we could in principle consider a purification of $\tilde{\rho}$ to be fully consistent with (2.2), we will keep this mixed state for simplicity. Given this quantum realization of our observed correlation and the tripartite extension, the minimization of $H(\mathrm{A}|E)_{\rho_{\mathrm{A}E}}$ is upper bounded by $H(\mathrm{A}|E)_{\tilde{\rho}_{\mathrm{A}E}}$, where

$$\begin{aligned}\tilde{\rho}_{\mathrm{A}E}&=\sum_a|a\rangle\langle a|_{\mathrm{A}}\otimes\mathrm{tr}_{AB}[\tilde{\rho}(\tilde{A}_a^x\otimes I_B\otimes I_E)]\\&=\sum_a|a\rangle\langle a|_{\mathrm{A}}\otimes\left(\sum_{e=0}^{k-1}p_e\,\mathrm{tr}\left(\rho(A_a^{x,e}\otimes I_B)\right)|e\rangle\langle e|\right).\end{aligned}$$

The conditional entropy of this state is given by the conditional entropy of the classical distribution $q(a,e)=p_e\,\mathrm{tr}\left(\rho(A_a^{x,e}\otimes I_B)\right)$. That is,

$$\begin{aligned}H(\mathrm{A}|E)_{\tilde{\rho}_{\mathrm{A}E}}&=\sum_{e=0}^{k-1}p_eH(\mathrm{A}|E=e)=\sum_{e=0}^{k-1}p_eH\left(\left\{\mathrm{tr}\left(\rho(A_a^{x,e}\otimes I_B)\right)\right\}_a\right)\leq\sum_{e=0}^{k-1}p_e\log(d^2)\\&=2\log(d),\end{aligned}$$

where (with a slight abuse of notation) $H\left(\left\{\mathrm{tr}\left(\rho(A_a^{x,e}\otimes I_B)\right)\right\}_a\right)$ is the Shannon entropy of the distribution $\left\{\mathrm{tr}\left(\rho(A_a^{x,e}\otimes I_B)\right)\right\}_a$, which is upper bounded by $\log(d^2)$ due to the fact that at most d^2 elements of $(A_a^{x,e})_a$ are non-zero. The theoretical maximum device-independent randomness certifiable using locally d-dimensional states is therefore $2\log(d)$.

B. Balanced informationally complete POVMs

In this section we review the notion of (finite-dimensional) informationally complete POVMs and their construction following [DPS04; DPP05], and identify a sub-family of them that is the pillar of the scenario designed in this paper. Throughout the paper, given a matrix a we write a^*, a^{t} and $\overline{a}$ to denote its conjugate transpose, transpose and complex conjugate, respectively.

If elements of a POVM, $M_1,\dots,M_m$ on $\mathbb{C}^d$, span $\mathrm{M}_d(\mathbb{C})$, then $(M_j)_{j=1}^m$ is an *informationally complete POVM (IC-POVM)* on $\mathbb{C}^d$ (note that $m\geq d^2$ in this case). By [DPP05, Corollary 6], extremal d^2-outcome POVMs on $\mathbb{C}^d$ are IC-POVMs and consist of rank-one matrices. In this paper we focus on a special family of d^2-outcome rank-one IC-POVMs on $\mathbb{C}^d$. A *balanced IC-POVM (BIC-POVM)* on $\mathbb{C}^d$ is $(\frac{1}{d}P_j)_{j=1}^{d^2}$ where $P_1,\dots,P_{d^2}$ are rank-one projections that form a basis for $\mathrm{M}_d(\mathbb{C})$, and satisfy $\sum_{j=1}^{d^2}P_j=dI$. In the language of harmonic analysis, rank-one projections adding to a scalar multiple of the identity correspond to unit-norm tight frames [Wal18, Section 2]. For a parameterization of all BIC-POVMs on $\mathbb{C}^2$, see the first part of Example F.2 below.

Lemma B.1. *Let $(\frac{1}{d}P_j)_j$ be a BIC-POVM on $\mathbb{C}^d$. Then the $d^2\times d^2$ matrix $S=(\mathrm{tr}(P_jP_k))_{j,k}$ is positive definite, $s_{jj}=1$ for all j, $0\leq s_{jk}<1$ for all $j\neq k$, and $\sum_j s_{jk}=d$ for all k.*

Moreover, for every pair (j,k) there exists a sequence $j=i_1,\dots,i_N=k$ in $[d^2]$ such that $s_{i_ni_{n+1}}\neq 0$ for all $n=1,\dots,N-1$.

Proof. The matrix S is the Gram matrix of the basis $P_1,\dots,P_{d^2}$ with respect to the Frobenius inner product on $\mathrm{M}_d(\mathbb{C})$, and therefore positive definite. Since the P_j are rank-one projections, the diagonal entries of S equal 1. The off-diagonal entries of S lie in $[0,1)$ by the Cauchy-Schwarz inequality and linear independence of the P_j. Furthermore, for every k we have

$$\sum_{j=1}^{d^2}s_{jk}=\sum_{j=1}^{d^2}\mathrm{tr}(P_jP_k)=\mathrm{tr}\left(\left(\sum_{j=1}^{d^2}P_j\right)P_k\right)=d.$$

To prove the last part of the statement, consider the connectivity graph of S, i.e., the graph with vertices $[d^2]$, where there is an edge between j and k if and only if $s_{jk}\neq 0$. The assertion that we wish to prove is then equivalent to saying that any two vertices in this graph can be connected by a path. Suppose this is not true; then, the connectivity graph is not connected. One can then relabel its vertices in such a way that no vertex in $\{1,\dots,m\}$ has an edge to a vertex in $\{m+1,\dots,d^2\}$, for some $1\leq m<d^2$. This

means that $P_j P_k = 0$ for all $j \leq m$ and $k > m$. Let $V = \operatorname{ran} P_1 + \cdots + \operatorname{ran} P_m$. Then, $\operatorname{ran} P_{m+1} + \cdots + \operatorname{ran} P_{d^2} \subseteq V^\perp$, and in particular $V \neq \{0\}$ and $V \neq \mathbb{C}^d$. If $S \in \mathrm{M}_d(\mathbb{C})$ is any matrix that maps a nonzero vector from V to a nonzero vector from $V^\perp$ (and such S exists since V is a proper subspace of $\mathbb{C}^d$), then such S cannot be a linear combination of P_j (because the first m of them map V to V, and the rest map V to $\{0\}$). This contradicts the assumption that the P_j span the whole $\mathrm{M}_d(\mathbb{C})$. □

The matrix S in Lemma B.1 is said to be *induced* by the BIC-POVM. Its properties from Lemma B.1 are utilized frequently throughout the paper. In particular, the last part of Lemma B.1 asserts that while there may be zero entries in S, there cannot be too many; this is crucially used in Propositions D.1 and F.1.

To show the existence of IC-POVMs it is common to use group-theoretic tools [DPS04]. Consider the unitary projective representation of $\mathbb{Z}_d \times \mathbb{Z}_d$ on $\mathbb{P}(\mathbb{C}^d)$ given by the Weyl operators, *i.e.*,

$$U_{p,q} = \sum_{j=0}^{d-1} \omega^{jq} |j \oplus p\rangle\langle j| \qquad \text{for } (p,q) \in \mathbb{Z}_d \times \mathbb{Z}_d$$

where $\omega := e^{\frac{2\pi i}{d}}$ is the principal d^{th} root of unity and $\oplus$ is addition modulo d. If $|\psi\rangle \in \mathbb{C}^d$ is a unit vector then

$$(M_{p,q})_{(p,q)\in\mathbb{Z}_d\times\mathbb{Z}_d}, \quad \text{where} \quad M_{p,q} := \tfrac{1}{d} U_{p,q} |\psi\rangle\langle\psi| U_{p,q}^* \tag{B.1}$$

is a rank-one POVM. If furthermore $|\psi\rangle$ satisfies

$$\langle\psi| U_{p,q} |\psi\rangle \neq 0 \quad \text{for all } p, q \in \mathbb{Z}_d, \tag{B.2}$$

then $(M_{p,q})_{(p,q)}$ is a rank-one IC-POVM by [DPS04, Section 3], and furthermore a BIC-POVM. Notice that if we consider an arbitrary state $|\psi\rangle = \sum_{j=0}^{d-1} \psi_j |j\rangle$, where $\{|j\rangle\}_{j=0}^{d-1}$ is the standard orthonormal basis on $\mathbb{C}^d$, and we define the subnormalized vector $|\psi_p\rangle := \sum_{j=0}^{d-1} \overline{\psi_{j\oplus p}} \psi_j |j\rangle$, then

$$\langle\psi| U_{p,q} |\psi\rangle = \sum_{i,j,k=0}^{d-1} \omega^{jq} \psi_k \overline{\psi_i} \langle i|j \oplus p\rangle \langle j|k\rangle = \sum_{j=0}^{d-1} \omega^{jq} \overline{\psi_{j\oplus p}} \psi_j = \langle q| \mathcal{F}_d |\psi_p\rangle$$

where $\mathcal{F}_d$ denotes the quantum Fourier transform. The requirement (B.2) thus becomes

$$\langle q| \mathcal{F}_d |\psi_p\rangle \neq 0 \quad \text{for all } p, q \in \mathbb{Z}_d.$$

To construct BIC-POVMs on $\mathbb{C}^d$ for every $d \in \mathbb{N}$, we thus need to identify some unit vectors $|\psi\rangle \in \mathbb{C}^d$ satisfying the condition (B.2). In [DPS04; DPP05] it is asserted that states of the form $|\psi\rangle \propto \sum_k \alpha^k |k\rangle$, where $\alpha \in \mathbb{C}$ and $|\alpha| < 1$, fulfill the requirement (B.2). This assertion, however, needs some amendments: if d is even and $\alpha \in \mathbb{R}$, then $|\psi\rangle = \sum_k \alpha^k |k\rangle$ satisfies $\langle\psi| U_{d/2,1} |\psi\rangle = 0$ by a direct calculation. Thus we present the following sufficient criterion for $|\psi\rangle$ to satisfy (B.2).

Proposition B.2. *Let $d \in \mathbb{N}$, $r \in (0, \frac{1}{2})$, and $t \in \mathbb{R}$ if d is odd and $t \in \mathbb{R} \setminus \frac{1}{2d}\mathbb{Z}$ if d is even. Then $|\psi\rangle = \sum_{k=0}^{d-1} \alpha^k |k\rangle$ with $\alpha = re^{2\pi i t}$ satisfies $\langle\psi| U_{p,q} |\psi\rangle \neq 0$ for all $p, q \in \mathbb{Z}_d$.*

Proof. We expand

$$\begin{aligned}\langle\psi|\, U_{p,q}\, |\psi\rangle &= \sum_{k,\ell=0}^{d-1} \sum_{j\in\mathbb{Z}_d} \omega^{jq}\overline{\alpha}^k\alpha^\ell\, \langle k|j\oplus p\rangle\langle j|\ell\rangle \\ &= \sum_{\ell\le d-1-p} \omega^{\ell q}\overline{\alpha}^{\ell+p}\alpha^\ell + \sum_{\ell\ge d-p} \omega^{\ell q}\overline{\alpha}^{\ell+p-d}\alpha^\ell \\ &= e^{-2\pi i p t}\left(\sum_{\ell\le d-1-p} r^{2l+p}e^{2\pi i\frac{\ell q}{d}} + \sum_{\ell\ge d-p} r^{2l+p-d}e^{2\pi i(\frac{\ell q}{d}+dt)}\right).\end{aligned}$$

Therefore it suffices to see that

$$\sum_{\ell\le d-1-p} r^{2l+p}e^{2\pi i\frac{\ell q}{d}} + \sum_{\ell\ge d-p} r^{2l+p-d}e^{2\pi i(\frac{\ell q}{d}+dt)} \tag{B.3}$$

is nonzero for every $p, q \in \mathbb{Z}_d$. We shall reach this conclusion by observing that the largest absolute value of a term in (B.3) strictly dominates the sum of the other absolute values. Note that the largest absolute value equals r^m where $m = \min\{p, d-p\}$, and the smaller absolute values belong to $\{r^{m+1}, r^{m+2}, \dots\}$ if d is odd and to $\{r^{m+2}, r^{m+4}, \dots\}$ if d is even.

First assume that d is odd. Observe that the absolute values of terms in (B.3) are pairwise distinct. Since $r < \frac{1}{2}$ implies

$$r^{m+1} + r^{m+2} + \cdots < \frac{r}{1-r}r^m < r^m,$$

we see that (B.3) is nonzero. Now assume that d is even. Then the absolute values of terms in (B.3) are not all pair-wise distinct; rather, some appear once and others appear twice. If two terms in (B.3) have the same absolute value, then one appears in the first sum and the other appears in the second sum, and the difference of their arguments is $2\pi(\frac{q}{2} + dt)$. Observe that $\frac{q}{2} + dt \notin \frac{1}{2}\mathbb{Z}$ for every $q \in \{0, \dots, d-1\}$ by the assumption on t. In particular, $z = e^{2\pi i(\frac{q}{2}+dt)}$ satisfies $|z| = 1$, $z \neq -1$ and z is a ratio of any distinct two terms in (B.3) with the same absolute value. Since $r < \frac{1}{2} < \frac{1}{\sqrt{3}}$, we have

$$2(r^{m+2} + r^{m+4} + \cdots) \le \frac{2r^2}{1-r^2}r^m < r^m. \tag{B.4}$$

If $d \neq 2p$, then r^m appears once as an absolute value in (B.3), and the sum of other absolute values in (B.3) is strictly smaller than r^m by (B.4), so (B.3) is nonzero. If $d = 2p$, then all the absolute values of terms in (B.3) appear precisely twice, with the constant ratio $z \neq -1$. Thus, (B.3) becomes $(1+z)(r^m e^{i\alpha_0} + r^{m+2}e^{i\alpha_2} + r^{m+4}e^{i\alpha_4} + \cdots)$ for some angles α_j, and this expression is nonzero by (B.4). □

By Proposition B.2, there exists a state in $\mathbb{C}^d$ satisfying (B.2), for every $d \in \mathbb{N}$. Since (B.2) is a topologically open condition, in fact a generic state in $\mathbb{C}^d$ satisfies (B.2). Thus (B.1) can be used to produce a BIC-POVM from almost any state, which can then be employed in the scenario presented in Section C.

Finally, for the sake of completeness, let us comment on the connection to a famous open problem in quantum information theory, *i.e.*, the existence problem of *symmetric*

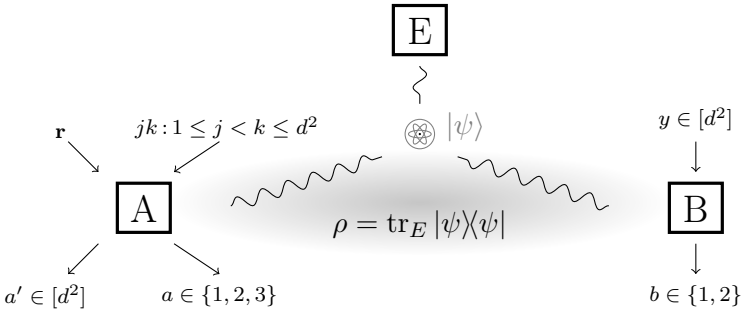

FIGURE 2. The Bell scenario with malicious eavesdropper Eve who is trying to guess Alice's outcome of her setting $\mathbf{r}$.

IC-POVMs (SIC-POVMs). It is straightforward to show that if

$$\left|\langle q|\, \mathcal{F}_d\, |\psi_p\rangle\right|^2 = \frac{1}{d+1} \quad \text{for all } (p,q) \neq (0,0), \tag{B.5}$$

then (B.1) is a SIC-POVM. Zauner famously conjectured in [Zau11] that SIC-POVMs exist in every finite dimension d. A state that fulfills (B.5) is called a *fiducial vector* and the SIC-POVM it induces is called covariant with respect to $\mathbb{Z}_d \times \mathbb{Z}_d$. Hence, one way to confirm Zauner's conjecture is to show the existence of fiducial vectors in every dimension. Fiducial vectors have been obtained in every dimension up to 67 [SG10]. Due to their uniform properties, SIC-POVMs have been widely used to design protocols in quantum information theory, for example for quantum key distribution [Ren05], quantum state tomography [BQT+15], entanglement detection [SAZ+18], certification of non-projective measurements [TRR19], and random number generation [TFR+21]. On the other hand, the protocol of this paper relies on more general BIC-POVMs, whose existence is unproblematic (in contrast to SIC-POVMs).

C. A Bell inequality

In this paper we investigate a variation of the scenario presented in [TFR+21]. For any integer $d \geq 2$, we consider the following Bell scenario (see Figure C). Alice has $d^2(d^2-1)/2 + 1$ measurement settings, where the first $d^2(d^2-1)/2$ settings have 3 outcomes, and the last one has d^2 outcomes. The first $d^2(d^2-1)/2$ settings are labaled by pairs jk such that $j, k \in [d^2]$ and $j < k$. The last of Alice's settings is labeled $\mathbf{r}$. We label the outcomes of the 3-outcome measurements by $a \in \{1, 2, 3\}$ and the outcome of the measurement $\mathbf{r}$ by $j \in [d^2]$. On the other side, Bob has d^2 measurement settings with two outcomes each, where the outcomes are labeled by $b \in \{1, 2\}$.

The overall goal in this paper is to show that the outcome of Alice's setting $\mathbf{r}$ is unpredictable for any eavesdropper Eve. We reach this conclusion in the device-independent setting, relying only on the observed correlation in the Bell scenario. We do this by constructing a Bell inequality whose maximal violation certifies certain desired properties of the measurements and the shared state. Since we aim to certify randomness coming from non-projective measurements, a fully assumption-free self-testing statement is impossible

[BCK+23, Theorem C]. As we will see, however, the maximal violation of our Bell inequality will certify enough about the state and the measurements to conclude that Eve cannot predict the outcome of Alice's measurement $\mathbf{r}$ better than a random guess.

We first simply state the Bell inequality, then the corresponding Bell operator and some intuition for why we chose this Bell inequality, in terms of the Bell operator. The inequality depends on d and on a fixed BIC-POVM coming from unit vectors $\{|e_j\rangle\}_{j=1}^{d^2}$. The inequality depends on the parameters $s_{jk} = \left|\langle e_j|e_k\rangle\right|^2$ (*i.e.*, the entries of the matrix S from Lemma B.1), and is given by

$$\begin{aligned} &2\sum_{j<k}\sqrt{1-s_{jk}}\Big[p(1,1|jk,j)+p(2,1|jk,k)-p(1,1|jk,k)-p(2,1|jk,j)\Big] \\ &-\sum_{j<k}(1-s_{jk})\big[p_A(1|jk)+p_A(2|jk)\big]-d(d-2)\sum_{j=1}^{d^2}p_B(1|j)-\sum_{j=1}^{d^2}p(j,2|\mathbf{r},j) \end{aligned} \tag{C.1}$$

where we use the shorthand notation $\sum_{j<k} = \sum_{j=1}^{d^2-1}\sum_{k=j+1}^{d^2}$. A quantum strategy for the above game consists of two finite-dimensional Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$, a bipartite state ρ on $\mathcal{H}_A \otimes \mathcal{H}_B$ given as a density matrix, POVMs $(A_1^{jk}, A_2^{jk}, I - A_1^{jk} - A_2^{jk})$ for $j < k \in [d^2]$ and $(A_1^{\mathbf{r}}, \ldots, A_{d^2}^{\mathbf{r}})$ on $\mathcal{H}_A$ (Alice's measurements), and POVMs $(B^j, I - B^j)$ for $j \in [d^2]$ on $\mathcal{H}_B$ (Bob's measurements). The corresponding Bell operator is given by

$$\begin{aligned} W_d := &2\sum_{j<k}\sqrt{1-s_{jk}}(A_1^{jk}-A_2^{jk})\otimes(B^j-B^k)-\sum_{j<k}(1-s_{jk})(A_1^{jk}+A_2^{jk})\otimes I \\ &-d(d-2)\sum_{j=1}^{d^2}I\otimes B^j-\sum_{j=1}^{d^2}A_j^{\mathbf{r}}\otimes(I-B^j), \end{aligned} \tag{C.2}$$

and the value attained by this quantum strategy is $\mathrm{tr}(W_d\rho)$. Note that W_d depends on the choice of a d-dimensional BIC-POVM, and not just on d; however, we index it with d because its maximal quantum value depends on d only, as seen in the remainder of the section. In the following, we will often omit the tensor products with the identity operator in the notation if it does not cause confusion. That is, we write A_a^{jk} instead of $A_a^{jk} \otimes I$ and B^j instead of $I \otimes B^j$.

The intuition for this Bell inequality comes from the aim of certifying a d-dimensional reference strategy (see section C.1). In this strategy, we use the maximally entangled state $|\varphi_d\rangle$, and the B^j operators are rank-1 projections, and therefore $B^j - B^k$ is rank-2. In order to certify this operator, we set $A_{1(2)}^{jk}$ to be the transposition of the projection onto the positive (negative) eigenvalue of $(B^j - B^k)$. Since the dimension is in general greater than 2, Alice's jk measurement must have a third outcome, occupying the remaining $d-2$ dimensions of her Hilbert space. That this third outcome occurs is enforced by the second term in W_d, penalizing Alice for outputting 1 or 2. The last term in W_d ensures correlation between Alice's measurement labeled by $\mathbf{r}$ and Bob's measurements. Specifically, in order to reach a large violation, if Alice chooses setting r and observes outcome j, then Bob, when simultaneously choosing setting j, should always observe outcome 2. The overlaps between Bob's measurements are certified using the s_{jk} dependence in the coefficients

in W_d. The precise form of these coefficients is a result of a simple sum-of-squares decomposition (see section C.2).

C.1. **Reference strategy.** We now consider a reference strategy in the quantum model reaching a score of d^2. Afterwards we proceed to show that d^2 is indeed optimal. Let Alice and Bob share the canonical maximally entangled state

$$|\varphi_d\rangle := \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} |kk\rangle \,.$$

Bob's measurements are given by $\tilde{B}^j := |\tilde{\psi}_j\rangle\langle\tilde{\psi}_j|$, where $\{\tilde{\psi}_j\}_j$ are unit vectors inducing the BIC-POVM. Now, the operator $\tilde{B}^j - \tilde{B}^k$ for $j \neq k$ is traceless, rank 2 and Hermitian. Hence, it has a spectral decomposition of the form

$$\tilde{B}^j - \tilde{B}^k = \gamma(|a_1^{jk}\rangle\langle a_1^{jk}| - |a_2^{jk}\rangle\langle a_2^{jk}|)$$

where $|a_1^{jk}\rangle\,, |a_2^{jk}\rangle$ are orthogonal unit vectors and $\gamma \in (0,2)$. Furthermore,

$$2\gamma^2 = \operatorname{tr}\left((\tilde{B}^j - \tilde{B}^k)^2\right) = \operatorname{tr}\left(\tilde{B}^j + \tilde{B}^k - \tilde{B}^j\tilde{B}^k - \tilde{B}^k\tilde{B}^j\right) = 2 - 2s_{jk}$$

so $\gamma = \sqrt{1 - s_{jk}}$. Let Alice's POVM associated with her 3-output measurement be given by $\tilde{A}_1^{jk} := (|a_1^{jk}\rangle\langle a_1^{jk}|)^{\mathrm{t}}$, $\tilde{A}_2^{jk} := (|a_2^{jk}\rangle\langle a_2^{jk}|)^{\mathrm{t}}$ and $\tilde{A}_3^{jk} := (I - |a_1^{jk}\rangle\langle a_1^{jk}| - |a_2^{jk}\rangle\langle a_2^{jk}|)^{\mathrm{t}}$. Notice in particular that we have the relations

$$\begin{aligned} \tilde{B}^j - \tilde{B}^k &= \sqrt{1 - s_{jk}}(\tilde{A}_1^{jk} - \tilde{A}_2^{jk})^{\mathrm{t}} \\ (\tilde{B}^j - \tilde{B}^k)^2 &= (1 - s_{jk})(\tilde{A}_1^{jk} + \tilde{A}_2^{jk})^{\mathrm{t}} \end{aligned} \tag{C.3}$$

Moreover, let $\tilde{A}_j^{\mathbf{r}} := \frac{1}{d}(\tilde{B}^j)^{\mathrm{t}}$.

Recall that since $|\varphi_d\rangle$ is the canonical maximally entangled state we have for any $X \in M_d(\mathbb{C})$ that $X \otimes I\,|\varphi_d\rangle = I \otimes X^{\mathrm{t}}\,|\varphi_d\rangle$. Then $\langle\varphi_d|\,W_d\,|\varphi_d\rangle$, the value of the Bell function (C.1) at this strategy,

$$\begin{aligned} &2\sum_{j<k} \sqrt{1 - s_{jk}}\,\langle\varphi_d|\,(\tilde{A}_1^{jk} - \tilde{A}_2^{jk}) \otimes (\tilde{B}^j - \tilde{B}^k)\,|\varphi_d\rangle - \sum_{j<k}(1 - s_{jk})\,\langle\varphi_d|\,(\tilde{A}_1^{jk} + \tilde{A}_2^{jk})\,|\varphi_d\rangle \\ &- d(d-2)\sum_{j=1}^{d^2}\langle\varphi_d|\,I \otimes \tilde{B}^j\,|\varphi_d\rangle - \sum_{j=1}^{d^2}\langle\varphi_d|\,\tilde{A}_j^{\mathbf{r}} \otimes (I - \tilde{B}^j)\,|\varphi_d\rangle\,, \end{aligned}$$

reduces to

$$\begin{aligned} &\sum_{j<k}\langle\varphi_d|\,I \otimes (\tilde{B}^j - \tilde{B}^k)^2\,|\varphi_d\rangle - d^2(d-2)\,\langle\varphi_d|\,I \otimes I\,|\varphi_d\rangle \\ &= \tfrac{1}{d}\sum_{j<k}\operatorname{tr}[(\tilde{B}^j - \tilde{B}^k)^2] - d^2(d-2) = \frac{2}{d}\sum_{j<k}(1 - s_{jk}) - d^2(d-2) \end{aligned}$$

using the relations (C.3), $\sum_j \tilde{B}^j = dI$ and $(\tilde{A}_j^{\mathbf{r}})^{\mathrm{t}}(I - \tilde{B}^j) = 0$. The sum $\sum_{j<k} s_{jk}$ is given by the sum of the upper triangle of the matrix S induced by the initial BIC-POVM. By

Lemma B.1 we have $\sum_{j<k} s_{jk} = \frac{d^3-d^2}{2}$ so $\langle\varphi_d| W_d |\varphi_d\rangle$ further simplifies to

$$\frac{2}{d}\left(\frac{d^4-d^2}{2} - \frac{d^3-d^2}{2}\right) - d^2(d-2) = d^2,$$

as desired.

Let us illustrate our construction with an explicit example generated by a BIC-POVM in $d = 2$.

Example C.1. Let us fix $d = 2$ and the BIC-POVM defined by

$$P_1 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad P_2 = \begin{pmatrix} \frac{1}{2} & -\frac{1}{2} \\ -\frac{1}{2} & \frac{1}{2} \end{pmatrix},$$
$$P_3 = \begin{pmatrix} \frac{1}{4} & \frac{1}{4} + i\frac{1}{2\sqrt{2}} \\ \frac{1}{4} - i\frac{1}{2\sqrt{2}} & \frac{3}{4} \end{pmatrix}, \quad P_4 = \begin{pmatrix} \frac{1}{4} & \frac{1}{4} - i\frac{1}{2\sqrt{2}} \\ \frac{1}{4} + i\frac{1}{2\sqrt{2}} & \frac{3}{4} \end{pmatrix},$$

which leads to the S matrix

$$S = \begin{pmatrix} 1 & \frac{1}{2} & \frac{1}{4} & \frac{1}{4} \\ \frac{1}{2} & 1 & \frac{1}{4} & \frac{1}{4} \\ \frac{1}{4} & \frac{1}{4} & 1 & \frac{1}{2} \\ \frac{1}{4} & \frac{1}{4} & \frac{1}{2} & 1 \end{pmatrix}$$

(note that this is a specific case of Example F.2 with $t_1 = t_2 = \frac{1}{4}$). The Bell function is then given by

$$\begin{aligned}
&\sqrt{2}\Big[p(1,1|12,1) + p(2,1|12,2) - p(1,1|12,2) - p(2,1|12,1)\Big] - \frac{1}{2}\big[p_A(1|12) + p_A(2|12)\big] \\
&+\sqrt{3}\Big[p(1,1|13,1) + p(2,1|13,3) - p(1,1|13,3) - p(2,1|13,1)\Big] - \frac{3}{4}\big[p_A(1|13) + p_A(2|13)\big] \\
&+\sqrt{3}\Big[p(1,1|14,1) + p(2,1|14,4) - p(1,1|14,4) - p(2,1|14,1)\Big] - \frac{3}{4}\big[p_A(1|14) + p_A(2|14)\big] \\
&+\sqrt{3}\Big[p(1,1|23,2) + p(2,1|23,3) - p(1,1|23,3) - p(2,1|23,2)\Big] - \frac{3}{4}\big[p_A(1|23) + p_A(2|23)\big] \\
&+\sqrt{3}\Big[p(1,1|24,2) + p(2,1|24,4) - p(1,1|24,4) - p(2,1|24,2)\Big] - \frac{3}{4}\big[p_A(1|24) + p_A(2|24)\big] \\
&+\sqrt{2}\Big[p(1,1|34,3) + p(2,1|34,4) - p(1,1|34,4) - p(2,1|34,3)\Big] - \frac{1}{2}\big[p_A(1|34) + p_A(2|34)\big] \\
&- \sum_{j=1}^{4} p(j,2|\mathbf{r},j),
\end{aligned}$$

(notice that the second to last term in the expression (C.1) vanishes when $d = 2$).

C.2. **Sum-of-squares decomposition of the Bell inequality.** In order to show that d^2 is the maximal quantum value of (C.1), or equivalently, a tight upper bound on the eigenvalues of the Bell operator W_d, we will need the following technical lemma.

Lemma C.2. *Let $X, Y \succeq 0$ satisfy $X+Y \preceq I$. Then $X+Y-(X-Y)^2 \succeq 0$. Furthermore, equality holds if and only if X, Y are projections orthogonal to each other.*

Proof. The inequality follows from rewriting $X + Y - (X - Y)^2$ as

$$(I - X + Y)X(I - X + Y) + (I + X - Y)Y(I + X - Y) + (X - Y)(I - X - Y)(X - Y),$$

where all three terms are positive semidefinite by construction.

Now suppose $X, Y \succeq 0$, $X + Y \preceq I$ and $X + Y - (X - Y)^2 = 0$. The above certificate for positive semidefinitenss of $X + Y - (X - Y)^2$ implies

$$(I - X + Y)X = 0, \qquad (I + X - Y)Y = 0.$$

In particular, XY is hermitian, so X and Y commute. Therefore they are jointly diagonalizable, with corresponding diagonal entries x_i and y_i, which satisfy for all i

$$x_i, y_i \geq 0, \quad x_i + y_i \leq 1, \quad (1 - x_i + y_i)x_i = 0, \quad (1 + x_i - y_i)y_i = 0. \tag{C.4}$$

A direct calculation shows that the solutions of (C.4) for a fixed i are $(0, 0), (1, 0), (0, 1)$. Therefore, X and Y are projections and $XY = 0$. □

Proposition C.3. *For any integer $d \geq 2$ and any choice of POVMs $\{A_a^{jk}\}_{jk}$, $\{A_j^{\mathbf{r}}\}$ and $\{B^j\}$ in the above scenario, we have*

$$d^2 I - W_d \succeq 0.$$

Proof. Let

$$\begin{aligned}
\Theta_d := &\sum_{j<k} \left[\sqrt{1 - s_{jk}}(A_1^{jk} - A_2^{jk}) - (B^j - B^k)\right]^2 + \left(dI - \sum_{j=1}^{d^2} B^j\right)^2 \\
&+ \sum_{j=1}^{d^2} A_j^{\mathbf{r}} \otimes (I - B^j) + d^2 \sum_{j=1}^{d^2} \left(B^j - (B^j)^2\right) \\
&+ \sum_{j<k} (1 - s_{jk}) \left[A_1^{jk} + A_2^{jk} - \left(A_1^{jk} - A_2^{jk}\right)^2\right].
\end{aligned} \tag{C.5}$$

The goal is to show that $W_d + \Theta_d = d^2 I$ and $\Theta_d \succeq 0$. First notice that if we expand the square in the first term of Θ_d we get

$$\begin{aligned}
&\left[\sqrt{1 - s_{jk}}(A_1^{jk} - A_2^{jk}) - (B^j - B^k)\right]^2 \\
&= (1 - s_{jk})(A_1^{jk} - A_2^{jk})^2 - 2\sqrt{1 - s_{jk}}(A_1^{jk} - A_2^{jk}) \otimes (B^j - B^k) \\
&\quad + \left[(B^j)^2 + (B^k)^2 - \{B^j, B^k\}\right].
\end{aligned} \tag{C.6}$$

The second term on the right hand side of Eq. (C.6) cancels with the first term of W_d in (C.2). The first term on the right hand side of Eq. (C.6) cancels with the last part of the last term of Θ_d. Notice also that the second term of W_d in (C.2) cancels with the first part of the last term of Θ_d, and that the terms involving $A_j^{\mathbf{r}}$ also cancel. Altogether we have reduced $W_d + \Theta_d$ to

$$\sum_{j<k} \left[(B^j)^2 + (B^k)^2 - \{B^j, B^k\}\right] + \left(dI - \sum_{j=1}^{d^2} B^j\right)^2 + d^2 \sum_{j=1}^{d^2} \left(B^j - (B^j)^2\right) - d(d-2) \sum_{j=1}^{d^2} B^j.$$

Using the fact that

$$\sum_{j<k}\left[(B^j)^2+(B^k)^2\right]=\tfrac{1}{2}\left(\sum_{j,k=1}^{d^2}\left[(B^j)^2+(B^k)^2\right]-2\sum_{\ell=1}^{d^2}(B^\ell)^2\right)=(d^2-1)\sum_{j=1}^{d^2}(B^j)^2,$$

we get

$$\begin{aligned}(d^2-1)\sum_{j=1}^{d^2}(B^j)^2-\sum_{j<k}\{B^j,B^k\}+\left(dI-\sum_{j=1}^{d^2}B^j\right)^2\\ +d^2\sum_{j=1}^{d^2}\left[B^j-(B^j)^2\right]-d(d-2)\sum_{j=1}^{d^2}B^j.\end{aligned}\tag{C.7}$$

Expanding the third term leads to

$$\begin{aligned}\left(dI-\sum_{j=1}^{d^2}B^j\right)^2&=d^2I+\sum_{j,k=1}^{d^2}B^jB^k-2d\sum_{j=1}^{d^2}B^j\\ &=d^2I+\sum_{j=1}^{d^2}(B^j)^2+\sum_{j<k}\{B^j,B^k\}-2d\sum_{j=1}^{d^2}B^j,\end{aligned}\tag{C.8}$$

where we have used

$$\sum_{j,k=1}^{d^2}B^jB^k=\sum_j(B^j)^2+\sum_{j<k}\{B^j,B^k\}.$$

Upon inserting Eq. (C.8) in the expression (C.7), one obtains d^2I after a straightforward simplification. We have thus shown $d^2I-W_d=\Theta_d$.

Notice that the first two terms of Θ_d are squares of Hermitian operators which means that they are positive semidefinite. The third and the fourth terms are also positive semidefinite which follows from the fact that the operators form POVMs. It follows by Lemma C.2 that the last term of Θ_d is positive semidefinite as well. We conclude that Θ_d is positive semidefinite and therefore $d^2I-W_d\succeq 0$, as desired. □

D. Representation-theoretic auxiliaries

Before analyzing strategies where the Bell function (C.1) attains the maximal quantum value d^2, we require a few intermediate results on operators satisfying the fundamental relations of BIC-POVMs, and a decomposition of states into maximally entangled ones. These results are obtained using techniques from C*-algebras and representation theory (for the general theory, see [Tak02] and [Pro07]), and might be of independent interest.

D.1. **A relevant C*-algebra.** This subsection introduces a C*-algebra whose representations lurk behind optimal strategies for the scenario in Section C. Let us first recall the necessary terminology on C*-algebras [Tak02, Chapter 1].

A unital *C*-algebra* $\mathcal{A}$ is a complex algebra with identity, an involution $*$ and a submultiplicative norm $\|\cdot\|$, such that $\mathcal{A}$ is a complete normed space and $\|a^*a\| = \|a\|^2$ for all $a \in \mathcal{A}$. A *representation* of $\mathcal{A}$ on a Hilbert space $\mathcal{H}$ is a map $\pi : \mathcal{A} \to \mathcal{B}(\mathcal{H})$, where $\mathcal{B}(\mathcal{H})$ are bounded operators on $\mathcal{H}$, that is additive, multiplicative, and respects $*$ (in other words, it is a $*$-homomorphism). When $\dim \mathcal{H} = D < \infty$, we identify $\mathcal{B}(\mathcal{H})$ with $\mathrm{M}_D(\mathbb{C})$, say that π is *finite-dimensional*, and write $\dim \pi = D$. A representation $\pi : \mathcal{A} \to \mathcal{B}(\mathcal{H})$ is *irreducible* if there is no closed subspace $\{0\} \neq \mathcal{K} \subset \mathcal{H}$ such that $\pi(a)\mathcal{K} \subseteq \mathcal{K}$ for all $a \in \mathcal{A}$. Given two representations $\pi : \mathcal{A} \to \mathcal{B}(\mathcal{H})$ and $\pi' : \mathcal{A} \to \mathcal{B}(\mathcal{H}')$, a *homomorphism* from π to π' is an operator $W : \mathcal{H} \to \mathcal{H}'$ such that $\pi'(a)W = W\pi(a)$ for all $a \in \mathcal{A}$. If there exists a unitary homomorphism from π to π', then π and π' are *unitarily equivalent*. Roughly speaking, unitarily equivalent representations are "equal" up to a unitary change of coordinates.

Finally, given a tuple $(a_1, \ldots, a_m)$ of self-adjoint operators on $\mathcal{H}$, we say that the tuple is irreducible if there is no subspace $\{0\} \neq \mathcal{K} \subset \mathcal{H}$ such that $a_j\mathcal{K} \subseteq \mathcal{K}$ for all j. If $(b_1, \ldots, b_m)$ is another tuple of self-adjoint operators on $\mathcal{H}'$, then an operator $W : \mathcal{H} \to \mathcal{H}'$ such that $b_j W = W a_j$ for all j is called a homomorphism from $(a_j)_j$ to $(b_j)_j$. This slight abuse of terminology is tailored to thinking of operator tuples in terms of C*-algebras they generate.

Let $S \in \mathrm{M}_{d^2}(\mathbb{R})$ be a matrix induced by a BIC-POVM. With it we associate the universal unital C*-algebra

$$\mathcal{A}_S = \mathrm{C}^*\left\langle x_1, \ldots, x_{d^2} : x_j = x_j^* = x_j^2 \ \forall j,\ \sum_{j=1}^{d^2} x_j = d,\ x_j x_k x_j = s_{jk} x_j \ \forall j, k \right\rangle,$$

that is, the "most general" C*-algebra generated by $x_1, \ldots x_{d^2}$ satisfying the above relations. Without invoking the subtleties of the full definition of a universal C*-algebra [Bla06, Section II.8.3], we can nevertheless precisely characterize its representations. Namely, a representation π of $\mathcal{A}_S$ on $\mathcal{H}$ corresponds to an ensemble of d^2 projections $\pi(x_1), \ldots, \pi(x_{d^2}) \in \mathcal{B}(\mathcal{H})$ that add up to d times identity, and satisfy $\pi(x_j)\pi(x_k)\pi(x_j) = s_{jk}\pi(x_j)$.

Proposition D.1. *Let π be a finite-dimensional representation of $\mathcal{A}_S$. Then $\dim \pi$ is divisible by d, $\operatorname{tr} \pi(x_j) = \frac{\dim \pi}{d}$ for all j, and $\pi(x_1), \ldots, \pi(x_{d^2})$ are linearly independent.*

Proof. Denote $X_j = \pi(x_j)$. For all $j \neq k$ we have $s_{jk} \operatorname{tr}(X_j) = \operatorname{tr}(X_j X_k) = s_{jk} \operatorname{tr}(X_k)$, and thus $\operatorname{tr}(X_j) = \operatorname{tr}(X_k)$ whenever $s_{jk} \neq 0$. By Lemma B.1 it follows that $\operatorname{tr}(X_1) = \cdots = \operatorname{tr}(X_{d^2})$. Then for all j,

$$d^2 \operatorname{tr}(X_j) = \sum_{k=1}^{d^2} \operatorname{tr}(X_k) = d \operatorname{tr} I$$

and so $d \operatorname{tr}(X_j) = \operatorname{tr} I = \dim \pi$. The Gram matrix of $\pi(x_1), \ldots, \pi(x_{d^2})$ with respect to the Frobenius inner product on $\mathrm{M}_{\dim \pi}(\mathbb{C})$ equals $(\operatorname{tr}(X_j X_k))_{j,k} = (\frac{\dim \pi}{d} s_{jk})_{j,k} = \frac{\dim \pi}{d} S$, which is invertible by Lemma B.1. Therefore $\pi(x_1), \ldots, \pi(x_{d^2})$ are linearly independent. □

Representations of $\mathcal{A}_S$ of minimal dimension mimic the properties of BIC-POVMs in the following sense.

Proposition D.2. *BIC-POVMs that induce S correspond to the d-dimensional representations of $\mathcal{A}_S$.*

Proof. If a BIC-POVM $\frac{1}{d}X_1, \dots, \frac{1}{d}X_{d^2}$ induces S, then the tuple $(X_j)_j$ gives rise to a d-dimensional representation π of $\mathcal{A}_S$. On the other hand, if π is a d-dimensional representation of $\mathcal{A}_S$, then $\operatorname{rk}\pi(x_j) = \operatorname{tr}\pi(x_j) = 1$ by Proposition D.1. Consequently $\operatorname{tr}(\pi(x_j)\pi(x_k)) = s_{jk}$ for all j, k, and so $\frac{1}{d}\pi(x_1), \dots, \frac{1}{d}\pi(x_{d^2})$ is a BIC-POVM inducing S. □

By Proposition D.2, every BIC-POVM inducing S gives rise to an irreducible representation of $\mathcal{A}_S$. However, $\mathcal{A}_S$ might have other irreducible representations (cf. Section G). Roughly speaking, this is an obstruction to the existence of "true" self-testing results in our setup; nevertheless, even the partial knowledge on representations of $\mathcal{A}_S$ turns out to be sufficient for our device-independent results from Section 3. We will also require an alternative definition of $\mathcal{A}_S$, as follows.

Lemma D.3. *The C*-algebra $\mathcal{A}_S$ equals*

$$\mathrm{C}^*\left\langle x_1, \dots, x_{d^2} \colon x_j = x_j^* = x_j^2 \ \forall j,\ \sum_{j=1}^{d^2} x_j = d,\ (1 - s_{jk})(x_j - x_k) = (x_j - x_k)^3 \ \forall j, k \right\rangle.$$

Proof. Let $\widetilde{\mathcal{A}}_S$ denote the new C*-algebra from the statement of Lemma D.3. Since

$$(x_j - x_k)^3 = (x_j - x_k) - (x_j x_k x_j - x_k x_j x_k)$$

for projections x_j, x_k, it follows that the relations $(1 - s_{jk})(x_j - x_k) = (x_j - x_k)^3$ in $\widetilde{\mathcal{A}}_S$ can be replaced with

$$x_j x_k x_j - s_{jk} x_j = x_k x_j x_k - s_{jk} x_k. \tag{D.1}$$

Thus, it is clear that the defining relations of $\mathcal{A}_S$ imply those of $\widetilde{\mathcal{A}}_S$ (because in $\mathcal{A}_S$, both sides of Eq. (D.1) are 0, and thus equal). It now suffices to see the converse; namely, that $x_j x_k x_j - s_{jk} x_j = 0$ holds in $\widetilde{\mathcal{A}}_S$. Firstly, observe that $x_j x_k x_j - s_{jk} x_j$ is positive semidefinite in $\widetilde{\mathcal{A}}_S$ for $j \neq k$ (and also trivially for $j = k$) since

$$x_j x_k x_j - s_{jk} x_j = \left(\tfrac{1}{\sqrt{1 - s_{jk}}} x_j x_k x_j - \tfrac{s_{jk}}{\sqrt{1 - s_{jk}}} x_j \right)^2$$

holds by Eq. (D.1). Next, for every j we have

$$\sum_k \left(x_j x_k x_j - s_{jk} x_j \right) = x_j \left(\sum_k x_k \right) x_j - \left(\sum_k s_{jk} \right) x_j = x_j \cdot d \cdot x_j - d x_j = 0.$$

Therefore $x_j x_k x_j - s_{jk} x_j = 0$ for all j, k by semidefiniteness, as desired. □

D.2. **Local support of a mixed bipartite state.** In this subsection we recall the definition of the local support of a mixed bipartite state, and highlight some of its features.

Given a mixed bipartite state $\rho \in \mathrm{M}_{d_A}(\mathbb{C}) \otimes \mathrm{M}_{d_B}(\mathbb{C})$, its *local support* on Alice's side $\operatorname{supp}_A \rho \subseteq \mathbb{C}^{d_A}$ is the range of $\operatorname{tr}_B \rho \in \mathrm{M}_{d_A}(\mathbb{C})$; here, tr_B denotes the partial trace over $\mathbb{C}^{d_B}$. The local support of ρ on Bob's side $\operatorname{supp}_B \rho \subseteq \mathbb{C}^{d_B}$ is defined analogously. Given an operator $X\colon \mathbb{C}^{d_A} \to \mathbb{C}^{d_A}$, its *compression* onto the local support of ρ is the operator $\hat{X}\colon \operatorname{supp}_A \rho \to \operatorname{supp}_A \rho$ given by $\hat{X} = U^* X U$ where $U\colon \operatorname{supp}_A \rho \to \mathbb{C}^{d_A}$ is the inclusion (that is, U^*U is the identity on $\operatorname{supp}_A \rho$, and UU^* is the projection acting on $\mathbb{C}^{d_A}$ whose range is $\operatorname{supp}_A \rho$). Analogously we define compressions onto $\operatorname{supp}_B \rho$ for operators on $\mathbb{C}^{d_B}$. The following lemma might be folklore (especially (i)), but we record it for the sake of completeness.

Lemma D.4. *Let $\rho \in \mathrm{M}_{d_A}(\mathbb{C}) \otimes \mathrm{M}_{d_B}(\mathbb{C})$ be a mixed bipartite state.*

(i) If $U\colon \operatorname{supp}_A \rho \to \mathbb{C}^{d_A}$ is the inclusion then $(UU^* \otimes I)\rho = \rho$.
(ii) If $Y \in \mathrm{M}_{d_B}(\mathbb{C})$ then $\operatorname{ran} \operatorname{tr}_B \big((I \otimes Y)\rho\big) \subseteq \operatorname{supp}_A \rho$.

Proof. First we check (i) and (ii) for a pure state ρ. After a local unitary basis change we can assume that $\rho = \sum_{i,j=0}^{r-1} \lambda_i \lambda_j |ii\rangle\langle jj|$ for $\lambda_i, \lambda_j > 0$. Then $\operatorname{tr}_B \rho = \sum_{i=0}^{r-1} \lambda_i^2 |i\rangle\langle i|$, so $UU^* = \sum_{i=0}^{r-1} |i\rangle\langle i|$ and (i) holds. The range of $\operatorname{tr}_B((I \otimes Y)\rho) = \sum_{i,j=0}^{r-1} \lambda_i \lambda_j \langle j| Y |i\rangle\, |i\rangle\langle j|$ is contained in the span of $\{|0\rangle, \dots, |r-1\rangle\}$, so (ii) holds.

If $\rho = \sum_k \gamma_k \rho_k$ where $\gamma_k > 0$ and ρ_k are pure states, then $\operatorname{supp}_A \rho = \sum_k \operatorname{supp}_A \rho_k$ by semidefiniteness. Thus $(UU^* \otimes I)\rho_k = \rho_k$ for all k. Also, the range of $\operatorname{tr}_B((I \otimes Y)\rho) = \sum_k \gamma_k \operatorname{tr}_B((I \otimes Y)\rho_k)$ is contained in $\operatorname{supp}_A \rho$ by the previous paragraph. Therefore (i) and (ii) hold for ρ. □

D.3. **Block-wise maximally entangled states.** In this subsection we see how a synchronicity condition on a mixed bipartite state ρ implies that ρ admits a block diagonal decomposition into maximally entangled states. This is achieved by invoking two basic facts about representations of the C*-algebras (see [Pro07] for a comprehensive source on representation theory). First, every representation breaks down into irreducible ones; second, there is a unique nonzero homomorphism between unitarily equivalent irreducible representations, and none between unitarily non-equivalent ones (Schur's lemma).

At a high level, Proposition D.5 below states the following: if Alice's measurements act on the shared state in the same way as Bob's (synchronicity condition (D.2)), then after a local unitary change the coordinates, the shared state decomposes into lower-dimensional maximally entangled states $|\varphi_{d_\alpha}\rangle$ (whose local dimensions d_α are determined by the measurements). Later in Section E, this result is applied to characterize the state of an optimal strategy for the scenario from Section C. Within Proposition D.5 and the rest of the paper, we often tacitly reshuffle the order of tensor factors for the sake of notation.

Proposition D.5. *Let $E_1, \dots, E_n \in \mathrm{M}_{d_A}(\mathbb{C})$ and $F_1, \dots, F_n \in \mathrm{M}_{d_B}(\mathbb{C})$ be hermitian matrices, and $\rho \in \mathrm{M}_{d_A}(\mathbb{C}) \otimes \mathrm{M}_{d_B}(\mathbb{C})$ a mixed bipartite state, such that*

$$(E_j \otimes I)\rho = (I \otimes F_j)\rho \qquad \text{for } j \in [n]. \tag{D.2}$$

Then there exist $L \in \mathbb{N}$, $d_\alpha, e_\alpha, f_\alpha \in \mathbb{N}$ *for* $\alpha \in [L]$, *and isometries* $U : \bigoplus_\alpha \mathbb{C}^{e_\alpha} \otimes \mathbb{C}^{d_\alpha} \to \mathbb{C}^{d_A}$, $V : \bigoplus_\alpha \mathbb{C}^{f_\alpha} \otimes \mathbb{C}^{d_\alpha} \to \mathbb{C}^{d_B}$ *such that:*

(i) $\operatorname{ran} U = \operatorname{supp}_A \rho$ *and* $\operatorname{ran} V = \operatorname{supp}_B \rho$*;*
(ii) $U^* E_j U \in \bigoplus_\alpha I_{e_\alpha} \otimes \mathrm{M}_{d_\alpha}(\mathbb{C})$ *and* $V^* F_j V \in \bigoplus_\alpha I_{f_\alpha} \otimes \mathrm{M}_{d_\alpha}(\mathbb{C})$ *for* $j \in [n]$*;*
(iii) $(U \otimes V)^* \rho (U \otimes V)$ *is a mixture of pure states of the form*

$$\bigoplus_\alpha |\chi_\alpha\rangle \otimes |\varphi_{d_\alpha}\rangle \in \bigoplus_\alpha \left(\mathbb{C}^{e_\alpha} \otimes \mathbb{C}^{f_\alpha}\right) \otimes \left(\mathbb{C}^{d_\alpha} \otimes \mathbb{C}^{d_\alpha}\right) \subset \left(\bigoplus_\alpha \mathbb{C}^{e_\alpha} \otimes \mathbb{C}^{r_\alpha d}\right) \otimes \left(\bigoplus_\alpha \mathbb{C}^{f_\alpha} \otimes \mathbb{C}^{r_\alpha d}\right);$$

(iv) if ρ *is pure then* $U^* E_j U = \left(V^* F_j V\right)^{\mathrm{t}}$ *for* $j \in [n]$.

Proof. Let $\hat{E}_j$ and $\hat{F}_j$ denote the compressions of E_j onto $\operatorname{supp}_A \rho$ and F_j onto $\operatorname{supp}_B \rho$, respectively. Also, let $\hat{\rho}$ denote the compression of ρ onto $\operatorname{supp}_A \rho \otimes \operatorname{supp}_B \rho$. Since $\hat{E}_j, \hat{F}_j$ are hermitian, the unital algebras generated by $\hat{E}_1, \ldots, \hat{E}_n$ and $\hat{F}_1, \ldots, \hat{F}_n$ are finite-dimensional C*-algebras. Let us identify $\operatorname{supp}_A \rho = \mathbb{C}^{N_A}, \operatorname{supp}_B \rho = \mathbb{C}^{N_B}$. By [Tak02, Theorem I.11.2], the algebras generated by $\hat{E}_j$ and $\hat{F}_j$ break up into irreducible representations; that is, one can find unitary changes of coordinates in which the tuples $(\hat{E}_j)_j$ and $(\hat{F}_j)_j$ are block-diagonal, with irreducible blocks. More explicitly, there exist unitaries $U \in \mathrm{M}_{N_A}(\mathbb{C}), V \in \mathrm{M}_{N_B}(\mathbb{C})$ and nonnegative integers $L, M', M'', e_\alpha, f_\alpha, d_\alpha, g'_\alpha$ and g''_α for all $\alpha \in [L]$ such that

$$\begin{aligned} \check{E}_j &:= U^* \hat{E}_j U = \bigoplus_{\alpha=1}^{L} X_{j,\alpha}^{\oplus e_\alpha} \oplus \bigoplus_{\alpha=1}^{M'} X'^{\oplus g'_\alpha}_{j,\alpha} \qquad \text{for } j \in [n], \\ \check{F}_j{}^{\mathrm{t}} &:= (V^* \hat{F}_j V)^{\mathrm{t}} = \bigoplus_{\alpha=1}^{L} X_{j,\alpha}^{\oplus f_\alpha} \oplus \bigoplus_{\alpha=1}^{M''} X''^{\oplus g''_\alpha}_{j,\alpha} \qquad \text{for } j \in [n], \end{aligned} \tag{D.3}$$

where $(X_{j,\alpha})_j, (X'_{j,\alpha})_j, (X''_{j,\alpha})_j$ are pairwise unitarily non-equivalent irreducible tuples, and $X_{j,\alpha} \in \mathrm{M}_{d_\alpha}(\mathbb{C})$.

Let $\check{\rho} := (U \otimes V)^* \hat{\rho} (U \otimes V) = \sum_{k=1}^K p_k |\psi_k\rangle\langle\psi_k|$ be a spectral decomposition of $\check{\rho}$, where $|\psi_1\rangle, \ldots, |\psi_K\rangle \in \mathbb{C}^{N_A} \otimes \mathbb{C}^{N_B}$ are orthogonal states, and $p_1, \ldots, p_K > 0$. Let **mat** denote the matricization operator[3] transforming vectors into matrices, determined by the linear extension of $\mathbf{mat}(|ab\rangle) = |a\rangle\langle b|$ defined on simple tensors. Then

$$\bigcap_{k=1}^{K} \ker \mathbf{mat}(|\psi_k\rangle) = 0, \qquad \bigcap_{k=1}^{K} \ker \mathbf{mat}(|\psi_k\rangle)^{\mathrm{t}} = 0 \tag{D.4}$$

since all operators and states have been compressed to $\operatorname{supp}_A \rho$ and $\operatorname{supp}_B \rho$. By Eq. (D.2) we have $(\check{E}_j \otimes I) |\psi_k\rangle = (I \otimes \check{F}_j) |\psi_k\rangle$, and therefore, applying **mat**(.) again,

$$\check{E}_j \mathbf{mat}(|\psi_k\rangle) = \mathbf{mat}(|\psi_k\rangle) \check{F}_j^{\mathrm{t}} \qquad \text{for } j \in [n],\ k \in [K]. \tag{D.5}$$

In particular, Eq. (D.5) means that the (α, β)-block of $\mathbf{mat}(|\psi_k\rangle)$ with respect to the block decomposition (D.3) determines a homomorphism between the diagonal α-block of

[3] For example, $\mathbf{mat}(\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)) = \frac{1}{\sqrt{2}}(|0\rangle\langle 0| + |1\rangle\langle 1|) = \frac{1}{\sqrt{2}} \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$.

$(\check{E}_j)_j$ and the β-block of $(\check{F}_j^{\mathrm{t}})_j$. Suppose $M' > 0$ holds in (D.3). By Eq. (D.5) and Schur's lemma [Pro07, Corollary 6.1.7], the $(L+1)^{\text{th}}$ block-row of $\mathbf{mat}(|\psi_k\rangle)$ is zero for every k, which contradicts Eq. (D.4). Therefore $M' = 0$, and analogously $M'' = 0$. Hence

$$\check{E}_j = \bigoplus_{\alpha=1}^{L} X_{j,\alpha}^{\oplus e_\alpha}, \qquad \check{F}_j^{\,\mathrm{t}} = \bigoplus_{\alpha=1}^{L} X_{j,\alpha}^{\oplus f_\alpha}, \tag{D.6}$$

and we can view $\mathbf{mat}(|\psi_k\rangle)$ as a block matrix with $\sum_\alpha e_\alpha$ block-rows and $\sum_\alpha f_\alpha$ block-columns according to decompositions (D.6). By Eq. (D.5), irreducibility of $(X_{j,\alpha})_j$ and another application of Schur's lemma, a block in $\mathbf{mat}(|\psi_k\rangle)$ is a nonzero scalar multiple of the identity matrix if the row and column correspond to the same $(X_{j,\alpha})_j$, and zero otherwise. Explicitly, $\mathbf{mat}(|\psi_k\rangle) = \bigoplus_\alpha R_{k,\alpha} \otimes I_{d_\alpha}$ for some $R_{k,\alpha} \in \mathbb{C}^{e_\alpha \times f_\alpha}$, and therefore

$$\check{\rho} = \sum_{k=1}^{K} p_k |\psi_k\rangle\langle\psi_k|, \qquad |\psi_k\rangle = \bigoplus_{\alpha=1}^{L} \sqrt{d_\alpha}\,\mathbf{mat}^{-1}(R_{k,\alpha}) \otimes |\varphi_{d_\alpha}\rangle\,.$$

Finally, assume that ρ is pure. Then $\check{\rho} = |\psi_1\rangle\langle\psi_1|$ and $\mathbf{mat}(\psi_1) = \bigoplus_\alpha R_{1,\alpha} \otimes I_{d_\alpha}$ is invertible by Eq. (D.4). This is only possible if $R_{1,\alpha}$ is invertible for every α. In particular, $R_{1,\alpha}$ has to be a square matrix, and therefore $e_\alpha = f_\alpha$ for all α. Hence $\check{E}_j = \check{F}_j^{\mathrm{t}}$ by (D.6). □

Remark D.6. Proposition D.5(iv) is a special case of [MPS24, Corollary 3.6]. On the other hand, purity in (iv) is essential. A counterexample with $n = 1$ and $d_A = d_B = 3$ is given by $E_1 = 1 \oplus 1 \oplus 0$, $F_1 = 1 \oplus 0 \oplus 0$ and $\rho = \frac{1}{2}(|\psi_1\rangle\langle\psi_1| + |\psi_2\rangle\langle\psi_2|)$ where $\psi_1 = \frac{1}{\sqrt{2}}(|00\rangle + |21\rangle)$ and $\psi_2 = \frac{1}{\sqrt{2}}(|10\rangle + |22\rangle)$.

E. Optimal strategy analysis

This section analyzes optimal strategies for the scenario in Section C, and establishes our main result on certifying maximal randomness (Theorem E.4). Throughout the section let $\mathcal{H}_A$ and $\mathcal{H}_B$ be finite-dimensional Hilbert spaces; ρ a mixed bipartite state on $\mathcal{H}_A \otimes \mathcal{H}_B$; $A_1^{jk}, A_2^{jk}, A_j^{\mathbf{r}}$ for $(j,k) \in [d^2] \times [d^2]$ with $j < k$ positive semidefinite contractions on $\mathcal{H}_A$ with $A_1^{jk} + A_2^{jk} \preceq I$; and B^j for $j \in [d^2]$ positive semidefinite contractions on $\mathcal{H}_B$. In other words, $\rho, A_a^{jk}, A_j^{\mathbf{r}}, B^j$ determine a quantum model strategy compatible with the scenario in Section C. Furthermore, given a measurement X on Alice's (or Bob's) side, its compression to $\operatorname{supp}_A \rho$ (or $\operatorname{supp}_B \rho$) is denoted $\hat{X}$.

E.1. Measurements in an optimal strategy.

We start by extracting properties of measurements B^j and A_a^{jk} in an optimal strategy for the Bell function (C.1).

Proposition E.1. *Assume the Bell function (C.1) attains d^2 at the strategy given by $\rho, A_a^{jk}, A_j^{\mathbf{r}}, B^j$. Then*

$$\sqrt{1 - s_{jk}}\big((A_1^{jk} - A_2^{jk}) \otimes I\big)\rho = \big(I \otimes (B^j - B^k)\big)\rho \quad \forall j < k, \tag{E.1}$$

$$\big(A_j^{\mathbf{r}} \otimes (I - B^j)\big)\rho = 0 \quad \forall j, \tag{E.2}$$

$A_1^{jk} - A_2^{jk}$ preserve $\operatorname{supp}_A \rho$ and B^j preserve $\operatorname{supp}_B \rho$, and the following hold for the compressions of measurements to the local support of ρ:

$$(\hat{B}^j)^2 = \hat{B}^j \quad \forall j, \tag{E.3}$$

$$\sum_j \hat{B}^j = dI, \tag{E.4}$$

$$(\hat{A}_1^{jk})^2 = \hat{A}_1^{jk},\ (\hat{A}_2^{jk})^2 = \hat{A}_2^{jk},\ \hat{A}_1^{jk}\hat{A}_2^{jk} = 0 \quad \forall j < k, \tag{E.5}$$

$$\hat{B}^j \hat{B}^k \hat{B}^j = s_{jk}\hat{B}^j \quad \forall j \neq k. \tag{E.6}$$

Proof. Attaining the maximal value at the given strategy is equivalent to saying that $\operatorname{tr}(W_d\rho) = d^2$, upon substituting Alice's and Bob's measurement operators into W_d. By Proposition C.3 and its proof, we have that $W_d = d^2 I - \Theta_d$, where $\Theta_d \succeq 0$ is given in (C.5). Attaining the value d^2 therefore implies $\operatorname{tr}(\Theta_d\rho) = 0$. This also implies $\Theta_d\rho = 0$ because Θ_d and ρ are positive semidefinite. Since Θ_d is a sum of hermitian squares in (C.5), it follows that each of the terms in the sum are zero, in particular we have Eqs. (E.1), (E.2) and

$$\Big(dI \otimes I - \sum_j I \otimes B^j\Big)\rho = 0, \tag{E.7}$$

$$\big[I \otimes (B^j - (B^j)^2)\big]\rho = 0, \tag{E.8}$$

$$\left(\left(A_1^{jk} + A_2^{jk} - (A_1^{jk} - A_2^{jk})^2\right) \otimes I\right)\rho = 0 \tag{E.9}$$

hold for all $j < k$. Next, notice that applying partial traces and Lemma D.4(ii) to Eq. (E.1) yields

$$(B^j - B^k)\operatorname{supp}_B \rho \subseteq \operatorname{supp}_B \rho, \quad (A_1^{jk} - A_2^{jk})\operatorname{supp}_A \rho \subseteq \operatorname{supp}_A \rho \qquad \text{for all } j < k. \tag{E.10}$$

In particular, the differences $B^j - B^k$ preserve $\operatorname{supp}_B \rho$ for all j, k. Thus the same holds for $\sum_k (B^j - B^k) = d^2 B^j - \sum_k B^k$, which acts as $d^2 B^j - dI$ on $\operatorname{supp}_B \rho$ by Eq. (E.7). Therefore

$$B^j \operatorname{supp}_B \rho \subseteq \operatorname{supp}_B \rho \qquad \text{for all } j, \tag{E.11}$$

and similarly,

$$A_j \operatorname{supp}_A \rho \subseteq \operatorname{supp}_A \rho \qquad \text{for all } j. \tag{E.12}$$

That is, these measurement operators preserve the local support of ρ. Thus, Eqs. (E.7), (E.8) and (E.9) can be restricted to the local support of ρ, and the marginal states on the local support are invertible by definition. Right-multiplying by appropriate inverses leads to

$$dI - \sum_j \hat{B}^j = 0, \tag{E.13}$$

$$\hat{B}^j - (\hat{B}^j)^2 = 0, \tag{E.14}$$

$$\hat{A}_1^{jk} + \hat{A}_2^{jk} - (\hat{A}_1^{jk} - \hat{A}_2^{jk})^2 = 0 \tag{E.15}$$

for all $j < k$ (more precisely, Eqs. (E.10) and (E.11) are needed because B^j and $A_1^{jk} - A_2^{jk}$ appear nonlinearly in Eqs. (E.8) and (E.9), respectively). In particular, Eqs. (E.3) and

(E.4) hold, and Eq. (E.5) follows by Eq. (E.15) and Lemma C.2. We are left with proving Eq. (E.6). Left-multiplying Eq. (E.1) by $\sqrt{1-s_{jk}}(A_1^{jk}-A_2^{jk})\otimes I$ yields

$$\begin{aligned}(1-s_{jk})\left((A_1^{jk}-A_2^{jk})^2\otimes I\right)\rho &= \sqrt{1-s_{jk}}\left((A_1^{jk}-A_2^{jk})\otimes(B^j-B^k)\right)\rho \\ &= \left(I\otimes(B^j-B^k)\right)\left(\sqrt{1-s_{jk}}(A_1^{jk}-A_2^{jk})\otimes I\right)\rho = \left(I\otimes(B^j-B^k)^2\right)\rho.\end{aligned} \tag{E.16}$$

We then left-multiply Eq. (E.16) by $\sqrt{1-s_jk}(A_1^{jk}-A_2^{jk})\otimes I$ one more time, and note that the projectivity and orthogonality of $\hat{A}_a^{jk}$ as in Eq. (E.5) imply that $(\hat{A}_1^{jk}-\hat{A}_2^{jk})^3 = \hat{A}_1^{jk}-\hat{A}_2^{jk}$. By Eq. (E.10) we therefore have

$$\left(\sqrt{1-s_{jk}}^3(A_1^{jk}-A_2^{jk})\otimes I\right)\rho = \left(I\otimes(B^j-B^k)^3\right)\rho,$$

which together with Eq. (E.1) yields

$$\left(I\otimes(1-s_{jk})(B^j-B^k)\right)\rho = \left(I\otimes(B^j-B^k)^3\right)\rho \tag{E.17}$$

for $j<k$. By Eq. (E.11) and symmetry we have

$$(1-s_{jk})(\hat{B}^j-\hat{B}^k) = (\hat{B}^j-\hat{B}^k)^3 \tag{E.18}$$

for all $j\neq k$. Then Eqs. (E.13), (E.14), (E.18) together with Lemma D.3 show that Eq. (E.6) holds. □

In particular, Proposition E.1 shows that the compressions of B^j from an optimal strategy determine a representation of the C*-algebra $\mathcal{A}_S$ from Section D.1. Next, we construct operators C_j on Alice's side whose compressions also determine a representation of $\mathcal{A}_S$. For $j\in[d^2]$ denote

$$C_j := \frac{1}{d^2}\left(dI + \sum_{k\neq j}\sqrt{1-s_{jk}}(A_1^{jk}-A_2^{jk})\right), \tag{E.19}$$

where we write $A_a^{jk}=A_a^{kj}$ for $k<j$. By Proposition E.1 we have

$$C_j \operatorname{supp}_A\rho \subseteq \operatorname{supp}_A\rho, \quad (C_j\otimes I)\rho = (I\otimes B^j)\rho \quad \forall j. \tag{E.20}$$

Then Eqs. (E.20), (E.3), (E.4), (E.6) imply that $\hat{C}_j$ are projections that add up to dI, and $\hat{C}_j\hat{C}_k\hat{C}_j = s_{jk}\hat{C}_j$, so $\hat{C}_j$ indeed determine a representation of $\mathcal{A}_S$. We can use these operators to deduce some partial information on the remaining measurements of Alice, that is, the $A_j^{\mathbf{r}}$ operators. Recall that every finite-dimensional representation of the C*-algebra $\mathcal{A}_S$ is a direct sum of irreducible ones, whose dimensions are multiples of d (Proposition D.1).

Proposition E.2. *Assume the Bell function (C.1) attains d^2 at the strategy given by $\rho, A_a^{jk}, A_j^{\mathbf{r}}, B^j$. Given Alice's operators $\hat{C}_j$ defined in Eq. (E.19), which determine a representation of $\mathcal{A}_S$, choose a basis of $\operatorname{supp}_A\rho$ such that*

$$\hat{C}_j = \bigoplus_{\alpha=1}^{L} I_{e_\alpha}\otimes\hat{C}_{j,\alpha}, \tag{E.21}$$

where $(\hat{C}_{j,\alpha})_j$ *determine pairwise non-isomorphic irreducible representations of* $\mathcal{A}_S$ *of dimension* $r_\alpha d$ *for* $r_\alpha \in \mathbb{N}$. *Then, with respect to the decomposition* (E.21), *for every* $\alpha \in [L]$ *the* (α,α)*-block of* $\hat{A}_j^{\mathbf{r}}$ *in* $\mathrm{M}_{e_\alpha}(\mathbb{C}) \otimes \mathrm{M}_{r_\alpha d}(\mathbb{C})$ *equals*

$$I_{e_\alpha} \otimes \frac{1}{d}\hat{C}_{j,\alpha} + W_{j,\alpha},$$

where $\mathrm{tr}_{\mathbb{C}^{r_\alpha d}}(W_{j,\alpha}) = 0 \in \mathrm{M}_{e_\alpha}(\mathbb{C})$.

Proof. Proposition E.1 implies

$$\begin{aligned}\Big(\big(A_j^{\mathbf{r}}(I - C_j)\big) \otimes I\Big)\,\rho &= \big(A_j^{\mathbf{r}} \otimes I\big)\,\big((I - C_j) \otimes I\big)\,\rho \\ &= \big(A_j^{\mathbf{r}} \otimes I\big)\,\Big(I \otimes (I - B^j)\Big)\,\rho \\ &= \Big(A_j^{\mathbf{r}} \otimes (I - B^j)\Big)\,\rho = 0\end{aligned}$$

and, since C_j preserves $\mathrm{supp}_A\,\rho$, one obtains $\hat{A}_j^{\mathbf{r}}(I - \hat{C}_j) = 0$. Since $\hat{A}_j^{\mathbf{r}}$ and $\hat{C}_j$ are hermitian, we obtain

$$\hat{A}_j^{\mathbf{r}}\hat{C}_j = \hat{A}_j^{\mathbf{r}} = \hat{C}_j\hat{A}_j^{\mathbf{r}} \quad \forall j. \tag{E.22}$$

Let $(X_{j\alpha pq})_{p,q=1}^{e_\alpha}$ denote the (α,α)-block of $\hat{A}_j^{\mathbf{r}}$ with respect to the decomposition (E.21). In other words, the (α,α)-block of $\hat{A}_j^{\mathbf{r}}$ is given by $\sum_{p,q=1}^{e_\alpha} |p\rangle\langle q| \otimes X_{j\alpha pq}$. Plugging this into Eq. (E.22) after projecting onto the (α,α) block, we obtain

$$X_{j\alpha pq}\hat{C}_{j,\alpha} = X_{j\alpha pq} = \hat{C}_{j,\alpha}X_{j\alpha pq} \tag{E.23}$$

for all j and $p,q \in [e_\alpha]$. Note that $\hat{C}_{1,\alpha},\dots,\hat{C}_{d^2,\alpha}$ have traces r_α and are linearly independent by Proposition D.1. Therefore

$$X_{j\alpha pq} = \sum_{k=1}^{d^2} \lambda_{j\alpha pq,k}\hat{C}_{k,\alpha} + W_{j\alpha pq} \tag{E.24}$$

for unique $\lambda_{j\alpha pq,k} \in \mathbb{C}$ and $W_{j\alpha pq} \in \mathrm{M}_{r_\alpha d}(\mathbb{C})$ satisfying $\mathrm{tr}(W_{j\alpha pq}\hat{C}_{\ell,\alpha}) = 0$ for all ℓ. In particular, $\mathrm{tr}(W_{j\alpha pq}) = 0$ because the $\hat{C}_{\ell,\alpha}$ add up to a multiple of identity. Then (E.23) and (E.24) together with $\hat{C}_{j,\alpha}\hat{C}_{k,\alpha}\hat{C}_{j,\alpha} = s_{jk}\hat{C}_{j,\alpha}$ imply

$$\begin{aligned} s_{\ell j}\,\mathrm{tr}\,X_{j\alpha pq} = \mathrm{tr}(\hat{C}_{j,\alpha}\hat{C}_{\ell,\alpha}\hat{C}_{j,\alpha}X_{j\alpha pq}) = \mathrm{tr}\left(\hat{C}_{\ell,\alpha}X_{j\alpha pq}\right) &= \sum_{k=1}^{d^2} \lambda_{j\alpha pq,k}\,\mathrm{tr}\left(\hat{C}_{\ell,\alpha}\hat{C}_{k,\alpha}\right) \\ &= \sum_{k=1}^{d^2} s_{\ell k} r_\alpha \lambda_{j\alpha pq,k} \end{aligned} \tag{E.25}$$

for all $\ell \in [d^2]$. Since the matrix S is invertible by Lemma B.1, the linear system (E.25) of d^2 equations in unknowns $\lambda_{j\alpha pq,1},\dots,\lambda_{j\alpha pq,d^2}$ has a unique solution, namely $\lambda_{j\alpha pq,j} = \frac{\mathrm{tr}\,X_{j\alpha pq}}{r_\alpha}$ and $\lambda_{j\alpha pq,k} = 0$ for $k \neq j$. Substituting this into Eq. (E.24), we have

$$X_{j\alpha pq} = \frac{\mathrm{tr}\,X_{j\alpha pq}}{r_\alpha}\hat{C}_{j,\alpha} + W_{j\alpha pq} \quad \forall j,p,q. \tag{E.26}$$

Since $\hat{A}_j^{\mathbf{r}}$ is a POVM, we have $\sum_j X_{j\alpha pp} = I$ and $\sum_j X_{j\alpha pq} = 0$ for $p \neq q$. Then (E.26), linear independence of the $\hat{C}_{j,\alpha}$, $\operatorname{span}\{\hat{C}_{j,\alpha}\}_j \cap \operatorname{span}\{W_{j\alpha pq}\}_{j,p,q} = \{0\}$ and the relation $\sum_j \frac{1}{d}\hat{C}_{j,\alpha} = I$ altogether imply $\frac{\operatorname{tr} X_{j\alpha pp}}{r_\alpha} = \frac{1}{d}$ and $\frac{\operatorname{tr} X_{j\alpha pq}}{r_\alpha} = 0$ for $p \neq q$. □

E.2. **State factorization.** The preceding characterization of measurements and state block decomposition allow us to prove that $2\log(d)$ bits of randomness can be extracted from the outcome of the setting $\mathbf{r}$ of Alice, by showing that a classical-quantum state between Alice and Eve necessarily factors (formally stated in Theorem E.4).

It is well known that if the partial trace of a bipartite pure state is pure, then the original state is a product state. In the proof of Theorem E.4 below, we require a variation of this fact for states in a tripartite system. The following technical lemma explains what can be deduced from the partial trace in the case where the subsystems decompose into direct sums, and the reduced state is highly structured with respect to these direct sums.

Lemma E.3. *Let $\mathcal{H}_C, \mathcal{H}_D, \mathcal{H}_E$ be finite-dimensional Hilbert spaces, with decompositions $\mathcal{H}_C = \bigoplus_\alpha \mathcal{H}_{C_\alpha}$ and $\mathcal{H}_D = \bigoplus_\alpha \mathcal{H}_{D_\alpha}$ indexed by a common index set. Suppose there are pure states $|\psi\rangle \in \mathcal{H}_C \otimes \mathcal{H}_D \otimes \mathcal{H}_E$ and $|\tau_\alpha\rangle \in \mathcal{H}_{C_\alpha}$ such that $\operatorname{tr}_E(|\psi\rangle\langle\psi|)$ is a mixture of pure states in*

$$\bigoplus_\alpha |\tau_\alpha\rangle \otimes \mathcal{H}_{D_\alpha}.$$

Then,

$$|\psi\rangle \in \bigoplus_\alpha |\tau_\alpha\rangle \otimes \mathcal{H}_{D_\alpha} \otimes \mathcal{H}_E.$$

Proof. First, we start with a basic observation on the interaction of tensor products and direct sums. Consider a pure state

$$|\xi\rangle \in \mathcal{H}_C \otimes \mathcal{H}_D = \bigoplus_{\alpha,\beta} \mathcal{H}_{C_\alpha} \otimes \mathcal{H}_{D_\beta}.$$

The density operator $|\xi\rangle\langle\xi|$ on $\mathcal{H}_C \otimes \mathcal{H}_D$ can be viewed as a block matrix indexed by pairs $\alpha\beta$ for α, β from the common index set, where the $(\alpha\beta, \alpha'\beta')$ block of $|\xi\rangle\langle\xi|$ is a map $\mathcal{H}_{C'_\alpha} \otimes \mathcal{H}_{D'_\beta} \to \mathcal{H}_{C_\alpha} \otimes \mathcal{H}_{D_\beta}$. If $|\xi\rangle$ is not an arbitrary vector of $\mathcal{H}_C \otimes \mathcal{H}_D$ but belongs to its "diagonal" subspace $\bigoplus_\alpha \mathcal{H}_{C_\alpha} \otimes \mathcal{H}_{D_\alpha}$, then the $(\alpha\beta, \alpha'\beta')$ block of $|\xi\rangle\langle\xi|$ is zero whenever $\alpha \neq \beta$ or $\alpha' \neq \beta'$.

Let us now turn to the proof of the statement.

With respect to the identification

$$\mathcal{H}_C \otimes \mathcal{H}_D \otimes \mathcal{H}_E = \bigoplus_{\alpha,\beta} \mathcal{H}_{C_\alpha} \otimes \mathcal{H}_{D_\beta} \otimes \mathcal{H}_E$$

we write $|\psi\rangle = \bigoplus_{\alpha,\beta} |\psi_{\alpha\beta}\rangle$ for $|\psi_{\alpha\beta}\rangle \in \mathcal{H}_{C_\alpha} \otimes \mathcal{H}_{D_\beta} \otimes \mathcal{H}_E$. Let us consider the diagonal blocks $|\psi_{\alpha\beta}\rangle\langle\psi_{\alpha\beta}|$ of $|\psi\rangle\langle\psi|$ with respect to this decomposition. If $\alpha \neq \beta$, then $\operatorname{tr}_E(|\psi_{\alpha\beta}\rangle\langle\psi_{\alpha\beta}|) = 0$ by the first paragraph because $\operatorname{tr}_E(|\psi\rangle\langle\psi|)$ is a mixture of pure states in $\bigoplus_\alpha \mathcal{H}_{C_\alpha} \otimes \mathcal{H}_{D_\alpha}$. Thus, $|\psi_{\alpha\beta}\rangle = 0$ for $\alpha \neq \beta$. If $\alpha = \beta$, then $\operatorname{tr}_E(|\psi_{\alpha\alpha}\rangle\langle\psi_{\alpha\alpha}|)$ is a mixture of pure states in $|\tau_\alpha\rangle \otimes \mathcal{H}_{D_\alpha}$. In particular, the further reduced (subnormalized) state $\operatorname{tr}_{D_\alpha E}(|\psi_{\alpha\alpha}\rangle\langle\psi_{\alpha\alpha}|)$ is proportional to the pure state $|\tau_\alpha\rangle\langle\tau_\alpha|$. Therefore, $|\psi_{\alpha\alpha}\rangle\langle\psi_{\alpha\alpha}|$ is

a (subnormalized) product bipartite state on $\mathcal{H}_{C_\alpha} \otimes (\mathcal{H}_{D_\alpha} \otimes \mathcal{H}_E)$, so $|\psi_{\alpha\alpha}\rangle = |\tau_\alpha\rangle \otimes |\chi_\alpha\rangle$ for some $|\chi_\alpha\rangle \in \mathcal{H}_{D_\alpha} \otimes \mathcal{H}_E$. Thus, $|\psi\rangle = \bigoplus_\alpha |\tau_\alpha\rangle \otimes |\chi_\alpha\rangle$. □

A pure tripartite state $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E$ is a purification of the mixed bipartite state ρ on $\mathcal{H}_A \otimes \mathcal{H}_B$ if $\rho = \mathrm{tr}_E(|\psi\rangle\langle\psi|)$. The device-independent randomness of the outcome of the setting $\mathbf{r}$ is bounded from below by the conditional von Neumann entropy $H(\mathrm{A}|E)_{\rho_{\mathrm{A}E}}$ of the classical-quantum state

$$\rho_{\mathrm{A}E} = \sum_{j=1}^{d^2} |j\rangle\langle j|_{\mathrm{A}} \otimes \mathrm{tr}_{AB}\left[|\psi\rangle\langle\psi|(A_j^{\mathbf{r}} \otimes I_B \otimes I_E)\right] \tag{E.27}$$

where $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E$ is the worst-case purification of ρ; that is, the purification of ρ that gives the lowest value of $H(\mathrm{A}|E)_{\rho_{\mathrm{A}E}}$.

Theorem E.4. *Suppose the state ρ and measurement $(A_j^{\mathbf{r}})_j$ appear in an optimal quantum strategy for the Bell function (C.1), and let $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E$ be a purification of ρ. Then*

$$\sum_{j=1}^{d^2} |j\rangle\langle j|_{\mathrm{A}} \otimes \mathrm{tr}_{AB}\left[|\psi\rangle\langle\psi|(A_j^{\mathbf{r}} \otimes I_B \otimes I_E)\right] = \left(\frac{1}{d^2}\sum_{j=1}^{d^2} |j\rangle\langle j|_{\mathrm{A}}\right) \otimes \sigma_E$$

for some state σ_E on $\mathcal{H}_E$.

In particular, the maximal violation of the Bell inequality (C.1) certifies $2\log(d)$ bits of device-independent randomness from the outcome of the setting $\mathbf{r}$ of Alice.

Proof. The operators $\hat{C}_j$ and $\hat{B}^j$ determine finite-dimensional representations of $\mathcal{A}_S$, which are direct sums of irreducible ones whose dimensions are multiples of d by Proposition D.1. By Eq. (E.20) and Proposition D.5 it then follows that there are isometries $U : \mathbb{C}^{D_A d} \to \mathcal{H}_A$ and $V : \mathbb{C}^{D_B d} \to \mathcal{H}_B$ with $\mathrm{ran}\, U = \mathrm{supp}_A\, \rho$ and $\mathrm{ran}\, V = \mathrm{supp}_B\, \rho$ such that

$$U^* C_j U \in \bigoplus_\alpha (I_{e_\alpha} \otimes \mathrm{M}_{r_\alpha d}(\mathbb{C})), \quad V^* B^j V \in \bigoplus_\alpha (I_{f_\alpha} \otimes \mathrm{M}_{r_\alpha d}(\mathbb{C})), \tag{E.28}$$

where $D_A = \sum_\alpha e_\alpha r_\alpha$ and $D_B = \sum_\alpha f_\alpha r_\alpha$. Furthermore, $(U \otimes V)^* \rho (U \otimes V)$ is a mixture of pure states in

$$\bigoplus_\alpha \left(\mathbb{C}^{e_\alpha} \otimes \mathbb{C}^{f_\alpha}\right) \otimes |\varphi_{r_\alpha d}\rangle\,. \tag{E.29}$$

With respect to the decomposition (E.28), let

$$U^* C_j U = \bigoplus_\alpha I_{e_\alpha} \otimes \hat{C}_{j,\alpha}$$

where $\mathrm{tr}\, \hat{C}_{j,\alpha} = r_\alpha$ due to Proposition D.1. By Proposition E.2, we have

$$U^* A_j^{\mathbf{r}} U = \mathcal{N}_j + \bigoplus_\alpha \left(I_{e_\alpha} \otimes \frac{1}{d}\hat{C}_{j,\alpha} + W_{j,\alpha}\right), \tag{E.30}$$

where $\mathrm{tr}_{\mathbb{C}^{r_\alpha d}}(W_{j,\alpha}) = 0$, and all diagonal (α,α)-blocks of $\mathcal{N}_j \in \mathrm{M}_{D_A d}(\mathbb{C})$ are zero.

Let $|\psi\rangle$ be a purification of ρ. Then $\rho = \mathrm{tr}_E(|\psi\rangle\langle\psi|)$ and so $(U\otimes V)^*\rho(U\otimes V) = \mathrm{tr}_E((U\otimes V\otimes I_E)^*|\psi\rangle\langle\psi|(U\otimes V\otimes I_E))$. By Lemma E.3 and recalling Eq. (E.29), up to a suitable shuffle of direct sums and tensor products we have

$$|\hat{\psi}\rangle := (U^*\otimes V^*\otimes I_E)\,|\psi\rangle = \bigoplus_\alpha |\chi_\alpha\rangle\otimes|\varphi_{r_\alpha d}\rangle$$

for some $|\chi_\alpha\rangle \in (\mathbb{C}^{e_\alpha}\otimes\mathbb{C}^{f_\alpha})\otimes\mathcal{H}_E$.

Let us record two observations on the block interactions of the decomposition (E.28). In the following calculations, equalities are valid up to a compatible shuffle of tensor products. Firstly, for all α and j we have

$$\begin{aligned}
&\mathrm{tr}_{AB}\left[\left(|\varphi_{r_\alpha d}\rangle\langle\varphi_{r_\alpha d}|\otimes|\chi_\alpha\rangle\langle\chi_\alpha|\right)\left(W_{j,\alpha}\otimes I_{f_\alpha r_\alpha d}\otimes I_E\right)\right]\\
&= \mathrm{tr}_{\mathbb{C}^{e_\alpha}\otimes\mathbb{C}^{f_\alpha}}\left[\mathrm{tr}_{\mathbb{C}^{r_\alpha d}\otimes\mathbb{C}^{r_\alpha d}}\left[\left(|\varphi_{r_\alpha d}\rangle\langle\varphi_{r_\alpha d}|\otimes|\chi_\alpha\rangle\langle\chi_\alpha|\right)\left(W_{j,\alpha}\otimes I_{f_\alpha r_\alpha d}\otimes I_E\right)\right]\right]\\
&= \mathrm{tr}_{\mathbb{C}^{e_\alpha}\otimes\mathbb{C}^{f_\alpha}}\left[|\chi_\alpha\rangle\langle\chi_\alpha|\left(\frac{1}{r_\alpha d}\,\mathrm{tr}_{\mathbb{C}^{r_\alpha d}}\left(W_{j,\alpha}\right)\otimes I_{f_\alpha}\otimes I_E\right)\right] = 0,
\end{aligned} \tag{E.31}$$

where (with a slight abuse of notation) we are looking at the subspace $\mathbb{C}^{e_\alpha r_\alpha d}$ of $\mathcal{H}_A$ after the isometry U and the subspace $\mathbb{C}^{f_\alpha r_\alpha d}$ of $\mathcal{H}_B$ after the isometry V, and we used $\mathrm{tr}_{\mathbb{C}^{r_\alpha d}}(W_{j,\alpha}) = 0$ from Proposition E.2. Secondly, for all j we have

$$\begin{aligned}
&\mathrm{tr}_{AB}\left[|\hat{\psi}\rangle\langle\hat{\psi}|\left(\mathcal{N}_j\otimes I_{D_B d}\otimes I_E\right)\right]\\
&= \mathrm{tr}_{AB}\left[\left(\bigoplus_{\alpha,\beta}|\varphi_{r_\alpha d}\rangle\langle\varphi_{r_\beta d}|\otimes|\chi_\alpha\rangle\langle\chi_\beta|\right)\left(\mathcal{N}_j\otimes I_{D_B d}\otimes I_E\right)\right]\\
&= \mathrm{tr}_{AB}\left[\left(\sum_\gamma\left(|\varphi_{r_\alpha d}\rangle\langle\varphi_{r_\gamma d}|\otimes|\chi_\alpha\rangle\langle\chi_\gamma|\right)\left((\mathcal{N}_j)_{\gamma,\beta}\otimes(I_{D_B d})_{\gamma,\beta}\otimes I_E\right)\right)_{\alpha,\beta}\right]\\
&= 0,
\end{aligned} \tag{E.32}$$

where in the third line we re-wrote the argument of the partial trace in terms of a block matrix with the blocks indexed by α and β, and in the last line we used the fact that $(\mathcal{N}_j)_{\alpha,\alpha} = 0$ for all α, and that $(I_{D_B d})_{\alpha,\beta} = 0$ for all $\alpha\neq\beta$.

For the sake of readability, I_B denotes the identity on Bob's system or its subsystems (depending on the context) in the following calculations. For every $j\in[d^2]$, we can use Eqs. (E.30), (E.31) and (E.32) together with $(UU^*\otimes VV^*\otimes I_E)\,|\psi\rangle = |\psi\rangle$ from Proposition

D.5 (and Lemma D.4(i)) to calculate

$$\begin{aligned}
&\mathrm{tr}_{AB}\left[|\psi\rangle\langle\psi|(A_j^{\mathbf{r}}\otimes I_B\otimes I_E)\right]\\
&=\mathrm{tr}_{AB}\left[(U^*\otimes V^*\otimes I_E)|\psi\rangle\langle\psi|(U\otimes V\otimes I_E)(U^*A_j^{\mathbf{r}}U\otimes I_B\otimes I_E)\right]\\
&=\mathrm{tr}_{AB}\left[|\hat{\psi}\rangle\langle\hat{\psi}|\left(\left(\mathcal{N}_j+\bigoplus_\alpha\left(I_{e_\alpha}\otimes\frac{1}{d}\hat{C}_{j,\alpha}+W_{j,\alpha}\right)\right)\otimes I_B\otimes I_E\right)\right]\\
&=\mathrm{tr}_{AB}\left[|\hat{\psi}\rangle\langle\hat{\psi}|\left(\left(\bigoplus_\alpha I_{e_\alpha}\otimes\frac{1}{d}\hat{C}_{j,\alpha}\right)\otimes I_B\otimes I_E\right)\right]\\
&=\sum_\alpha\mathrm{tr}_{AB}\left[\left(|\chi_\alpha\rangle\langle\chi_\alpha|\otimes|\varphi_{r_\alpha d}\rangle\langle\varphi_{r_\alpha d}|\right)\left(\left(I_{e_\alpha}\otimes\frac{\hat{C}_{j,\alpha}}{d}\right)\otimes I_B\otimes I_E\right)\right]\\
&=\sum_\alpha\mathrm{tr}\left(|\varphi_{r_\alpha d}\rangle\langle\varphi_{r_\alpha d}|\left(\frac{\hat{C}_{j,\alpha}}{d}\otimes I_{r_\alpha d}\right)\right)\mathrm{tr}_{\mathbb{C}^{e_\alpha}\otimes\mathbb{C}^{f_\alpha}}(|\chi_\alpha\rangle\langle\chi_\alpha|)\\
&=\sum_\alpha\frac{1}{r_\alpha d^2}\mathrm{tr}\left(\hat{C}_{j,\alpha}\right)\mathrm{tr}_{\mathbb{C}^{e_\alpha}\otimes\mathbb{C}^{f_\alpha}}(|\chi_\alpha\rangle\langle\chi_\alpha|)\\
&=\sum_\alpha\frac{1}{d^2}\mathrm{tr}_{\mathbb{C}^{e_\alpha}\otimes\mathbb{C}^{f_\alpha}}(|\chi_\alpha\rangle\langle\chi_\alpha|),
\end{aligned}$$

which is independent of j. Above, in the second line we used $(UU^*\otimes VV^*\otimes I_E)\,|\psi\rangle=|\psi\rangle$; in the third line we used Eq. (E.30); the fourth line comes from Eq. (E.32); the fifth line from the block structure of $|\hat{\psi}\rangle\langle\hat{\psi}|$ and the block-diagonal structure of the operator multiplying it; the sixth line is a re-grouping of the terms; and the seventh line uses the fact that $\mathrm{tr}(|\varphi_d\rangle\langle\varphi_d|(M\otimes I))=\frac{1}{d}\mathrm{tr}(M)$ for any operator M.

As a consequence of the above, the state $\rho_{\mathrm{A}E}$ in (E.27) can be written as

$$\begin{aligned}
\rho_{\mathrm{A}E}&=\sum_{j=1}^{d^2}|j\rangle\langle j|_{\mathrm{A}}\otimes\mathrm{tr}_{AB}\left[|\psi\rangle\langle\psi|(A_j^{\mathbf{r}}\otimes I_B\otimes I_E)\right]\\
&=\frac{1}{d^2}\sum_{j=1}^{d^2}|j\rangle\langle j|_{\mathrm{A}}\otimes\sigma_E
\end{aligned}$$

where $\sigma_E:=\sum_\alpha\mathrm{tr}_{\mathbb{C}^{e_\alpha}\otimes\mathbb{C}^{f_\alpha}}(|\chi_\alpha\rangle\langle\chi_\alpha|)$ is a state on $\mathcal{H}_E$. It therefore follows that

$$\begin{aligned}
H(\mathrm{A}|E)_{\rho_{\mathrm{A}E}}&=H(\mathrm{A}E)_{\rho_{\mathrm{A}E}}-H(E)_{\rho_{\mathrm{A}E}}=H\left(\frac{1}{d^2}\sum_{j=1}^{d^2}|j\rangle\langle j|_{\mathrm{A}}\otimes\sigma_E\right)-H(\sigma_E)\\
&=H\left(\frac{1}{d^2}\sum_{j=1}^{d^2}|j\rangle\langle j|_{\mathrm{A}}\right)+H(\sigma_E)-H(\sigma_E)=2\log(d)
\end{aligned}$$

for any purification $|\psi\rangle$ compatible with the observed correlation. □

F. Classical value of the BIC-POVM Bell function

Let $d \geq 2$, and let $S \in \mathrm{M}_{d^2}(\mathbb{R})$ be a matrix induced by a BIC-POVM. Consider the Bell function

$$\begin{aligned} &2\sum_{j<k}\sqrt{1-s_{jk}}\big[p(1,1|jk,j)+p(2,1|jk,k)-p(1,1|jk,k)-p(2,1|jk,j)\big] \\ &-\sum_{j<k}(1-s_{jk})\big[p_A(1|jk)+p_A(2|jk)\big]-d(d-2)\sum_{j=1}^{d^2}p_B(1|j)-\sum_{j=1}^{d^2}p(j,2|\mathbf{r},j) \end{aligned} \tag{F.1}$$

introduced in Section C. By Proposition C.3, its maximal quantum value equals d^2. In this section we provide an expression and an upper bound for its maximal classical value.

Proposition F.1. *Let $S \in \mathrm{M}_{d^2}(\mathbb{R})$ be a matrix induced by a BIC-POVM. Then the maximal classical value of the Bell function (F.1) equals*

$$\max_{\substack{J\subseteq[d^2],\\ 0<|J|<2d}}\left(-d(d-2)|J|+\sum_{j\in J,k\notin J}\left(2\sqrt{1-s_{jk}}-(1-s_{jk})\right)\right) \tag{F.2}$$

In particular, (F.1) is bounded from above by

$$d^2-\frac{1}{4}\left(\min_{\substack{J\subseteq[d^2],\\ 0<|J|<2d}}\sum_{j\in J,k\notin J}s_{jk}^2\right)<d^2.$$

Proof. Since maximizing (F.1) over all classical strategies is a convex optimization problem, its solution is attained at a deterministic strategy (since classical strategies are convex combinations of deterministic ones). Thus it suffices to solve the optimization problem

$$\begin{aligned} \max\quad & 2\sum_{j<k}\sqrt{1-s_{jk}}(a_1^{jk}-a_2^{jk})(b_j-b_k)-\sum_{j<k}(1-s_{jk})(a_1^{jk}+a_2^{jk}) \\ & -d(d-2)\sum_j b_j-\sum_j a_j^{\mathbf{r}}(1-b_j) \\ \text{subject to:}\quad & a_1^{jk},a_2^{jk},b_j,a_j^{\mathbf{r}}\in\{0,1\},\ a_1^{jk}a_2^{jk}=0,\ \text{exactly one of } a_j^{\mathbf{r}} \text{ is nonzero.} \end{aligned} \tag{F.3}$$

It is easier to analyze (F.3) with auxiliary notation $a_i^{jk}=a_i^{kj}$ for $j>k$ that makes (F.3) equivalent to

$$\begin{aligned} \max\quad & \sum_{j,k}\left(\sqrt{1-s_{jk}}(a_1^{jk}-a_2^{jk})(b_j-b_k)-\frac{1-s_{jk}}{2}(a_1^{jk}+a_2^{jk})\right) \\ & -d(d-2)\sum_j b_j-\sum_j a_j^{\mathbf{r}}(1-b_j) \\ \text{subject to:}\quad & a_1^{jk}=a_1^{kj},a_2^{jk}=a_2^{kj},b_j\in\{0,1\},\ a_1^{jk}a_2^{jk}=0,\ \text{exactly one of } a_j^{\mathbf{r}} \text{ is nonzero.} \end{aligned} \tag{F.4}$$

First, observe that $2\sqrt{1-t}-(1-t)$ is a monotone decreasing function $(0,1)\to(0,1)$. Let $J\subseteq[d^2]$ be arbitrary. Suppose we fix the b_j arguments in the objective function of (F.4) as $b_j=1$ if $j\in J$ and $b_j=0$ if $j\notin J$. To maximize the value of this partially evaluated objective function, it is then necessary to set:

- $a_1^{jk}=1$ if $j\in J$ and $k\notin J$,
- $a_2^{jk}=1$ if $j\notin J$ and $k\in J$,
- $a_1^{jk}=a_2^{jk}=0$ if $j,k\in J$ or $j,k\notin J$,
- $a_j^{\mathbf{r}}=1$ for some $j\in J$, unless $J=\emptyset$ in which case the choice of j is irrelevant.

For these arguments, the objective function of (F.4) evaluates as

$$v(J):=-d(d-2)|J|+\sum_{j\in J,k\notin J}\Big(2\sqrt{1-s_{jk}}-(1-s_{jk})\Big) \tag{F.5}$$

if $J\neq\emptyset$, and as -1 if $J=\emptyset$. By applying the estimate

$$1-t<2\sqrt{1-t}-(1-t)<1-\frac{t^2}{4}\qquad\text{for } t\in(0,1)$$

in (F.5) we see that

$$v(J)<-d(d-2)|J|+\sum_{j\in J,k\notin J}\Big(1-\tfrac{1}{4}s_{jk}^2\Big)=|J|(2d-|J|)-\tfrac{1}{4}\sum_{j\in J,k\notin J}s_{jk}^2.$$

In particular, $v(J)<0$ for $|J|=0$ and $|J|\geq 2d$. On the other hand, for $J=\{j\}$ one has

$$v(\{j\})=-d(d-2)+\sum_{k\neq j}\Big(2\sqrt{1-s_{jk}}-(1-s_{jk})\Big)>-d(d-2)+\sum_{k\neq j}(1-s_{jk})=d.$$

Therefore the classical value equals $\max_{0<|J|<2d}v(J)$. Moreover, the expression $|J|(2d-|J|)$ is at most d^2, leading to the following upper bound on the classical value,

$$d^2-\tfrac{1}{4}\min_{0<|J|<2d}\sum_{j\in J,k\notin J}s_{jk}^2.$$

Note that this value is strictly less than d^2 because $\sum_{j\in J,k\notin J}s_{jk}^2>0$ for every $0<|J|<d^2$ by Lemma B.1. □

Example F.2. Let us give a complete study of the classical value in the case of BIC-POVMs on $\mathbb{C}^2$. A routine calculation shows that up to unitary similarity, every quadruple of rank-one projections adding to $2I$ is of the form

$$P_1=\begin{pmatrix}1&0\\0&0\end{pmatrix},\quad P_2=\begin{pmatrix}1-t_1-t_2&-y_1-y_2\\-y_1-y_2&t_1+t_2\end{pmatrix},$$
$$P_3=\begin{pmatrix}t_1&y_1+iz\\y_1-iz&1-t_1\end{pmatrix},\quad P_4=\begin{pmatrix}t_2&y_2-iz\\y_2+iz&1-t_2\end{pmatrix},$$
$$y_j=\frac{t_j\sqrt{1-t_1-t_2}}{\sqrt{t_1+t_2}},\quad z=\pm\frac{\sqrt{t_1t_2}}{\sqrt{t_1+t_2}}$$

where $t_1, t_2 \geq 0$ and $t_1 + t_2 \leq 1$. Let $S = (\mathrm{tr}(P_j P_k))_{i,j=1}^4$. Then

$$S = \begin{pmatrix} 1 & 1-t_1-t_2 & t_1 & t_2 \\ 1-t_1-t_2 & 1 & t_2 & t_1 \\ t_1 & t_2 & 1 & 1-t_1-t_2 \\ t_2 & t_1 & 1-t_1-t_2 & 1 \end{pmatrix}$$

is invertible for $t_1, t_2, 1-t_1-t_2 \neq 0$. Therefore BIC-POVMs on $\mathbb{C}^2$ are (up to unitary similarity) given by $(\frac{1}{2}P_j)_j$ as above for parameters t_1, t_2 satisfying $t_1, t_2 > 0$ and $t_1 + t_2 < 1$. Note that $t_1 = t_2 = \frac{1}{3}$ yields a SIC-POVM. A case-by-case analysis of the formula in Proposition F.1 shows that the classical game value of the Bell function (F.1) associated with the BIC-POVM given by (t_1, t_2) equals

$$v(t_1,t_2) = 2 \cdot \begin{cases} t_1 + t_2 + 2(\sqrt{1-t_1} + \sqrt{1-t_2} - 1) & 0 < t_2 \leq \frac{1-t_1}{2},\ 0 < t_1 \leq \frac{1-t_2}{2}; \\ 2(\sqrt{1-t_1} + \sqrt{t_1+t_2}) - 1 - t_2 & 0 < t_1 \leq t_2,\ t_2 \geq \frac{1-t_1}{2},\ t_1 + t_2 < 1; \\ 2(\sqrt{1-t_2} + \sqrt{t_1+t_2}) - 1 - t_1 & 0 < t_2 \leq t_1,\ t_1 \geq \frac{1-t_2}{2},\ t_1 + t_2 < 1. \end{cases}$$

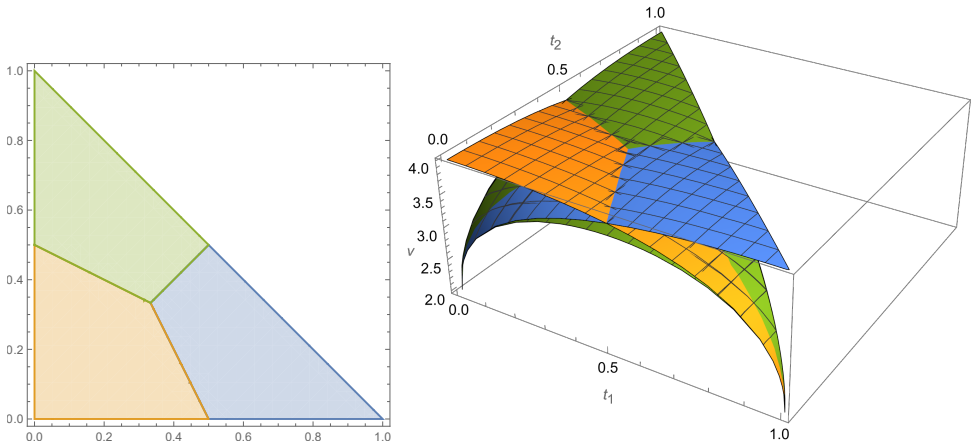

FIGURE 3. The regions and branches of the classical value function $v(t_1, t_2)$.

In particular, the formula for $v(t_1, t_2)$ leads to the following observations.

(i) $\lim_{t\to 0} v(t,t) = 4$, so the classical value can get arbitrarily close to the quantum value;
(ii) $\lim_{t\to\frac{1}{2}} v(t,t) = 1 + 2\sqrt{2} < \frac{8}{3}(\sqrt{6}-1) = v(\frac{1}{3},\frac{1}{3})$, so a SIC-POVM does not give the largest gap between quantum and classical value;
(iii) $1 + 2\sqrt{2} = \inf\{v(t_1,t_2) \colon t_1, t_2 > 0, t_1 + t_2 < 1\}$, so the gap between quantum and classical value is at most $3 - 2\sqrt{2} \approx 0.172$.

G. Further remarks on BIC-POVMs

This appendix collects examples and statements which, while not required for the derivation of the main results, are relevant to the broader theme of this paper.

G.1. **BIC-POVMs versus rank-one IC-POVMS.** By definition, a BIC-POVM on $\mathbb{C}^d$ is a d^2-outcome IC-POVM of rank-one matrices with trace $\frac{1}{d}$. The $\mathbb{Z}_d \times \mathbb{Z}_d$ covariant IC-POVMs from Section B are automatically BIC-POVMs, and moreover consists of pairwise non-orthogonal matrices. However, this is not the case for general rank-one IC-POVMs.

Example G.1. The quadruple

$$\begin{pmatrix} \frac{1}{2} & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} \frac{1}{8} & \frac{-i}{2\sqrt{6}} \\ \frac{i}{2\sqrt{6}} & \frac{1}{3} \end{pmatrix}, \begin{pmatrix} \frac{1}{8} & \frac{-1}{2\sqrt{6}} \\ \frac{-1}{2\sqrt{6}} & \frac{1}{3} \end{pmatrix}, \begin{pmatrix} \frac{1}{4} & \frac{1+i}{2\sqrt{6}} \\ \frac{1-i}{2\sqrt{6}} & \frac{1}{3} \end{pmatrix}$$

is a rank-one IC-POVM of pairwise non-orthogonal matrices, but not a BIC-POVM (since not all traces are the same).

Example G.2. Consider the states $|\psi_1\rangle, \ldots, |\psi_9\rangle \in \mathbb{C}^3$ given as

$$\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} \sqrt{\frac{2}{7}} \\ \sqrt{\frac{2}{7}} \\ \sqrt{\frac{3}{7}} \end{pmatrix}, \begin{pmatrix} -\sqrt{\frac{2}{7}} \\ \sqrt{\frac{2}{7}} \\ \sqrt{\frac{3}{7}} \end{pmatrix}, \begin{pmatrix} e^{2it_0}\sqrt{\frac{2}{7}} \\ e^{2it_1}\sqrt{\frac{2}{7}} \\ \sqrt{\frac{3}{7}} \end{pmatrix},$$

$$\begin{pmatrix} e^{-2it_0}\sqrt{\frac{2}{7}} \\ \sqrt{\frac{2}{7}} \\ \sqrt{\frac{3}{7}} \end{pmatrix}, \begin{pmatrix} -\sqrt{\frac{2}{7}} \\ e^{2it_1}\sqrt{\frac{2}{7}} \\ \sqrt{\frac{3}{7}} \end{pmatrix}, \begin{pmatrix} \sqrt{\frac{2}{7}} \\ e^{2it_2}\sqrt{\frac{2}{7}} \\ \sqrt{\frac{3}{7}} \end{pmatrix}, \begin{pmatrix} \sqrt{\frac{2}{7}} \\ e^{2it_3}\sqrt{\frac{2}{7}} \\ \sqrt{\frac{3}{7}} \end{pmatrix}$$

for

$$t_0 = \tfrac{\pi}{3},\ t_1 = \arctan(\tfrac{7}{\sqrt{3}}),\ t_2 = \arctan(\sqrt{3}(14+\sqrt{217})),\ t_3 = \arctan(\sqrt{3}(14-\sqrt{217})).$$

Then $M_j = \frac{1}{3}|\psi_j\rangle\langle\psi_j|$ form a BIC-POVM on $\mathbb{C}^3$ that does not arise from the construction in Section B since $M_1 M_2 = 0$.

Furthermore, d^2-outcome rank-one IC-POVMs on $\mathbb{C}^d$ without additional restrictions can be constructed in a very haphazard way. For example, if $|\psi_1\rangle, \ldots, |\psi_{d^2}\rangle \in \mathbb{C}^d$ are sufficiently generic, then $|\psi_1\rangle\langle\psi_1|, \ldots, |\psi_{d^2}\rangle\langle\psi_{d^2}|$ form a basis of $\mathrm{M}_d(\mathbb{C})$. Their sum is positive definite, and thus factors as K^2 for a positive definite $K \in \mathrm{M}_d(\mathbb{C})$. Then $K^{-1}|\psi_1\rangle\langle\psi_1|K^{-1}, \ldots, K^{-1}|\psi_{d^2}\rangle\langle\psi_{d^2}|K^{-1}$ is a rank-one IC-POVM.

Some more details are needed for a generic construction of BIC-POVMs. First observe that BIC-POVMs on $\mathbb{C}^d$ (up to unitary similarity) are in one-to-one correspondence with hermitian matrices $G \in \mathrm{M}_{d^2}(\mathbb{C})$ such that $G_{jj} = 1$ for all j, the Schur product of G and $\overline{G}$ is invertible, and $\frac{1}{d}G$ is a projection. Concretely, $(\frac{1}{d}|\psi_j\rangle\langle\psi_j|)_j$ is a BIC-POVM if and only if the matrix $G = (\langle\psi_j|\psi_k\rangle)_{j,k}$ satisfies the above properties. Thus one can construct BIC-POVMs as follows. Start with a full-rank $d^2 \times d$ complex matrix K_0. After column orthonormalization of K_0 we obtain K_1. Then $K_2 = K_1 K_1^*$ is a projection of rank d. Then there exists an effectively computable unitary $U \in \mathrm{M}_{d^2}(\mathbb{C})$ such that $K_3 = UK_2U^*$ has uniform diagonal entries $\frac{\operatorname{tr} K_2}{d^2} = \frac{1}{d}$. Let $G = dK_3$; if K_0 was sufficienly generic, the Schur product of G and $\overline{G}$ is invertible. Therefore G has the desired properties, and one can extract a BIC-POVM out of G using unitary diagonalization.

G.2. **BIC-POVM C*-algebra.** Let $S \in \mathrm{M}_{d^2}(\mathbb{R})$ be a matrix induced by a BIC-POVM. For the sake of simplicity let us furthermore assume that all the entries of S are nonzero (which is for example true for BIC-POVMs from Section B). In Section D.1 we introduced the C*-algebra $\mathcal{A}_S$ whose d-dimensional irreducible representations correspond to BIC-POVMs that induce S (Proposition D.2). However, $\mathcal{A}_S$ might have other irreducible representations when $d > 2$; see Example G.5 below. This motivates the introduction of the universal C*-algebra

$$\mathcal{B}_S = \mathrm{C}^*\Big\langle x_1, \dots, x_{d^2} \colon x_j = x_j^* = x_j^2 \ \forall j,\ \sum_{j=1}^{d^2} x_j = d,\ x_j x_k x_j = s_{jk} x_j \ \forall j,k,\ \big[x_1 x_{j_1} x_{j_2} x_1,\ x_1 x_{j_3} x_{j_4} x_1\big] = 0 \ \forall j_1, \dots, j_4 \Big\rangle.$$

Note that $\mathcal{B}_S$ is a quotient of $\mathcal{A}_S$. A straightforward inspection shows that $\mathcal{B}_S = \mathcal{A}_S$ for $d \leq 2$; however, $\mathcal{B}_S \neq \mathcal{A}_S$ in general (see Example G.5 below).

Lemma G.3. *The C*-subalgebra $x_1 \cdot \mathcal{B}_S \cdot x_1$ is abelian.*

Proof. Observe that $B = \{x_1 x_j x_k x_1 \colon j, k\}$ generates $x_1 \cdot \mathcal{B}_S \cdot x_1$ as a C*-algebra. Indeed, this follows by induction using $x_1 u x_j v x_1 = \frac{1}{s_{j1}} x_1 u x_j x_1 \cdot x_1 x_j v x_1$. Therefore $\mathcal{B}_S$ is abelian since B is a commuting family and $B = B^*$. □

Proposition G.4. *Irreducible representations of $\mathcal{B}_S$ correspond to BIC-POVMs that induce S.*

Proof. First observe that if π is a d-dimensional representation of $\mathcal{A}_S$, then $\pi(x_i)$ have rank one, so $\pi(x_j) M \pi(x_j)$ is a scalar multiple of $\pi(x_j)$ for every $M \in \mathrm{M}_d(\mathbb{C})$ and j. Therefore π is also a representation of $\mathcal{B}_S$. By Propositions D.1 and D.2 it thus suffices to show that every representation of $\mathcal{B}_S$ has a sub-representation of dimension d. Let $\pi : \mathcal{B}_S \to B(\mathcal{H})$ be a representation of $\mathcal{B}_S$ on a (nonzero) Hilbert space $\mathcal{H}$, and denote $X_j = \pi(x_j)$. Since the X_j add up to a multiple of the identity operator, at least one of them is nonzero; since $X_j X_1 X_j = s_{j1} X_j$ for all j, we in particular have $X_1 \neq 0$. Let $\mathcal{C} = x_1 \cdot \mathcal{B}_S \cdot x_1$. By Lemma G.3, the C*-algebra $\mathcal{C}$ is abelian, and nonzero since $X_1 \neq 0$. Therefore the restriction of π to $\mathcal{C}$ has a one-dimensional sub-representation. That is, there exists a unit vector $|\psi\rangle \in \mathcal{H}$ that is an eigenvector for every element of $\pi(\mathcal{C})$; namely, for every tuple $(j_1, \dots, j_m) \in \{1, \dots, d^2\}^m$ there is $\lambda_{j_1 \dots j_m} \in \mathbb{C}$ such that

$$X_1 X_{j_1} \cdots X_{j_m} X_1 |\psi\rangle = \lambda_{j_1 \dots j_m} |\psi\rangle .$$

In particular, $|\psi\rangle$ lies in the range of X_1. Let $\mathcal{K} \subset \mathcal{H}$ be the span of $\{X_1 |\psi\rangle , \cdots , X_{d^2} |\psi\rangle\}$.

Firstly, we claim that $\mathcal{K}$ is an invariant subspace for $X_1, \dots, X_{d^2}$, and therefore gives rise to a finite-dimensional sub-representation of π. Observe that $N \in B(\mathcal{H})$ is zero if and only if $X_1 X_j N = 0$ for $j = 1, \dots, d^2$ (because $X_j X_1 X_j = s_{j1} X_j$, and X_j add up to a nonzero multiple of the identity). Let $k, \ell \in \{1, \dots, d^2\}$ be arbitrary; we will show that

$$d X_k X_\ell |\psi\rangle = \sum_{j=1}^{d^2} \frac{\lambda_{jk\ell}}{s_{1j}} X_j |\psi\rangle . \tag{G.1}$$

By the preceding observation, (G.1) is equivalent to

$$dX_1X_iX_kX_\ell\left|\psi\right\rangle = \sum_{j=1}^{d^2} \frac{\lambda_{jk\ell}}{s_{1j}} X_1X_iX_j\left|\psi\right\rangle \qquad \text{for all } i = 1,\dots,d^2. \tag{G.2}$$

The choice of $\left|\psi\right\rangle = X_1\left|\psi\right\rangle$ and the defining relations for X_j imply

$$\begin{aligned}\sum_{j=1}^{d^2} \frac{\lambda_{jk\ell}}{s_{1j}} X_1X_iX_j\left|\psi\right\rangle &= \sum_{j=1}^{d^2} \frac{1}{s_{1j}} X_1X_iX_jX_1X_jX_kX_\ell X_1\left|\psi\right\rangle = \sum_{j=1}^{d^2} X_1X_iX_jX_kX_\ell X_1\left|\psi\right\rangle \\ &= X_1X_i\left(\sum_{j=1}^{d^2} X_j\right) X_kX_\ell X_1\left|\psi\right\rangle = dX_1X_iX_kX_\ell\left|\psi\right\rangle.\end{aligned}$$

Therefore (G.2) holds and consequently (G.1) holds, so $\mathcal{K}$ is an invariant subspace of $X_1,\dots,X_{d^2}$.

Secondly, we claim that $\dim\mathcal{K} = d$. Let $G = (\left\langle\psi\right| X_iX_j\left|\psi\right\rangle)_{i,j} = (\lambda_{ij})_{i,j} \in \mathrm{M}_{d^2}(\mathbb{C})$ be the Gram matrix of the spanning set of $\mathcal{K}$, and let $D \in \mathrm{M}_{d^2}(\mathbb{R})$ be the diagonal matrix whose k^{th} diagonal entry equals $\frac{1}{s_{1k}}$. Note that $\dim\mathcal{K} = \operatorname{rk} G$, and D is positive definite. Observe that $GDG = dG$. Indeed, the (i,j)-entry of GDG equals

$$\begin{aligned}\sum_{k=1}^{d^2} \frac{\lambda_{ik}\lambda_{kj}}{s_{1k}} &= \sum_{k=1}^{d^2} \frac{1}{s_{1k}} \left\langle\psi\right| X_1X_iX_kX_1X_kX_jX_1\left|\psi\right\rangle = \sum_{k=1}^{d^2} \left\langle\psi\right| X_1X_iX_kX_jX_1\left|\psi\right\rangle \\ &= \left\langle\psi\right| X_1X_i\left(\sum_{k=1}^{d^2} X_k\right) X_jX_1\left|\psi\right\rangle = \left\langle\psi\right| X_1X_iX_jX_1\left|\psi\right\rangle = d\lambda_{ij}.\end{aligned}$$

Therefore $\frac{1}{d}\sqrt{D}G\sqrt{D}$ is a projection, so

$$\begin{aligned}\dim\mathcal{K} = \operatorname{rk} G &= \operatorname{rk}\left(\frac{1}{d}\sqrt{D}G\sqrt{D}\right) = \operatorname{tr}\left(\frac{1}{d}\sqrt{D}G\sqrt{D}\right) = \frac{1}{d}\operatorname{tr}(GD) \\ &= \frac{1}{d}\sum_{j=1}^{d^2} \frac{\lambda_{jj}}{s_{1j}} = \frac{1}{d}\sum_{j=1}^{d^2} \frac{1}{s_{1j}} \left\langle\psi\right| X_1X_jX_1\left|\psi\right\rangle = \frac{1}{d}\left(\sum_{j=1}^{d^2} \left\langle\psi\right| X_1\left|\psi\right\rangle\right) = d,\end{aligned}$$

as desired. □

Let S be a $d^2 \times d^2$ matrix whose diagonal entries equal 1 and off-diagonal entries equal $\frac{1}{d+1}$. In view of Proposition G.4, irreducible representations of $\mathcal{B}_S$ are in one-to-one correspondence with SIC-POVMs (symmetric IC-POVMs). An analog of Proposition G.4 pertaining to mutually unbiased bases is given in [NPA12; GP24]. On the other hand, $\mathcal{A}_S$ may have representations that do not arise from SIC-POVMs, as it is shown by the following example.

Example G.5. Let $d = 3$ and let S be the 9×9 matrix with 1 on the diagonal and $\frac{1}{4}$ elsewhere. In other words, S is induced by a SIC-POVM on $\mathbb{C}^3$. We will show $\mathcal{A}_S \neq \mathcal{B}_S$ by producing a 6-dimensional irreducible representation of $\mathcal{A}_S$ (on the other hand, all

irreducible representations of $\mathcal{B}_S$ are 3-dimensional by Proposition G.4). Let $\xi = e^{\frac{\pi i}{12}}$ be the principal 24^{th} root of unity, and consider nine 6×6 matrices $X_1, \ldots, X_9$

$$I_2 \oplus 0_4, \begin{pmatrix} \frac{1}{4} & 0 & \frac{-\sqrt{3}}{4} & 0 & 0 & 0 \\ 0 & \frac{1}{4} & 0 & \frac{-\sqrt{3}}{4} & 0 & 0 \\ \frac{-\sqrt{3}}{4} & 0 & \frac{3}{4} & 0 & 0 & 0 \\ 0 & \frac{-\sqrt{3}}{4} & 0 & \frac{3}{4} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} \frac{1}{4} & 0 & \frac{\sqrt{3}}{4} & 0 & 0 & 0 \\ 0 & \frac{1}{4} & 0 & \frac{\sqrt{3}}{4} & 0 & 0 \\ \frac{\sqrt{3}}{4} & 0 & \frac{3}{4} & 0 & 0 & 0 \\ 0 & \frac{\sqrt{3}}{4} & 0 & \frac{3}{4} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix},$$

$$\begin{pmatrix} \frac{1}{4} & 0 & \frac{\xi^6}{4} & 0 & \frac{1}{\sqrt{8}\xi^5} & 0 \\ 0 & \frac{1}{4} & 0 & \frac{\xi^6}{4} & 0 & \frac{-1}{\sqrt{8}\xi^5} \\ \frac{1}{4\xi^6} & 0 & \frac{1}{4} & 0 & \frac{-\xi}{\sqrt{8}} & 0 \\ 0 & \frac{1}{4\xi^6} & 0 & \frac{1}{4} & 0 & \frac{\xi}{\sqrt{8}} \\ \frac{\xi^5}{\sqrt{8}} & 0 & \frac{-1}{\sqrt{8}\xi} & 0 & \frac{1}{2} & 0 \\ 0 & \frac{-\xi^5}{\sqrt{8}} & 0 & \frac{1}{\sqrt{8}\xi} & 0 & \frac{1}{2} \end{pmatrix}, \begin{pmatrix} \frac{1}{4} & 0 & \frac{1}{4\xi^6} & 0 & \frac{\xi^5}{\sqrt{8}} & 0 \\ 0 & \frac{1}{4} & 0 & \frac{1}{4\xi^6} & 0 & \frac{-\xi^5}{\sqrt{8}} \\ \frac{\xi^6}{4} & 0 & \frac{1}{4} & 0 & \frac{-1}{\sqrt{8}\xi} & 0 \\ 0 & \frac{\xi^6}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{\sqrt{8}\xi} \\ \frac{1}{\sqrt{8}\xi^5} & 0 & \frac{-\xi}{\sqrt{8}} & 0 & \frac{1}{2} & 0 \\ 0 & \frac{-1}{\sqrt{8}\xi^5} & 0 & \frac{\xi}{\sqrt{8}} & 0 & \frac{1}{2} \end{pmatrix},$$

$$\begin{pmatrix} \frac{1}{4} & 0 & 0 & \frac{\xi^6}{4} & \frac{1}{4} & \frac{1}{4\xi^6} \\ 0 & \frac{1}{4} & \frac{\xi^6}{4} & 0 & \frac{\xi^6}{4} & \frac{-1}{4} \\ 0 & \frac{1}{4\xi^6} & \frac{1}{4} & 0 & \frac{1}{4} & \frac{\xi^6}{4} \\ \frac{1}{4\xi^6} & 0 & 0 & \frac{1}{4} & \frac{1}{4\xi^6} & \frac{-1}{4} \\ \frac{1}{4} & \frac{1}{4\xi^6} & \frac{1}{4} & \frac{\xi^6}{4} & \frac{1}{2} & 0 \\ \frac{\xi^6}{4} & \frac{-1}{4} & \frac{1}{4\xi^6} & \frac{-1}{4} & 0 & \frac{1}{2} \end{pmatrix}, \begin{pmatrix} \frac{1}{4} & 0 & 0 & \frac{1}{4} & \frac{(-1-\sqrt{3})}{8} & \frac{(1-\sqrt{3})}{8} \\ 0 & \frac{1}{4} & \frac{-1}{4} & 0 & \frac{(1-\sqrt{3})}{8} & \frac{(1+\sqrt{3})}{8} \\ 0 & \frac{-1}{4} & \frac{1}{4} & 0 & \frac{(\sqrt{3}-1)}{8} & \frac{(-1-\sqrt{3})}{8} \\ \frac{1}{4} & 0 & 0 & \frac{1}{4} & \frac{(-1-\sqrt{3})}{8} & \frac{(1-\sqrt{3})}{8} \\ \frac{-1-\sqrt{3}}{8} & \frac{1-\sqrt{3}}{8} & \frac{\sqrt{3}-1}{8} & \frac{-1-\sqrt{3}}{8} & \frac{1}{2} & 0 \\ \frac{1-\sqrt{3}}{8} & \frac{1+\sqrt{3}}{8} & \frac{-1-\sqrt{3}}{8} & \frac{1-\sqrt{3}}{8} & 0 & \frac{1}{2} \end{pmatrix},$$

$$\begin{pmatrix} \frac{1}{4} & 0 & 0 & \frac{1}{4\xi^6} & \frac{1}{4} & \frac{\xi^6}{4} \\ 0 & \frac{1}{4} & \frac{1}{4\xi^6} & 0 & \frac{1}{4\xi^6} & \frac{-1}{4} \\ 0 & \frac{\xi^6}{4} & \frac{1}{4} & 0 & \frac{1}{4} & \frac{1}{4\xi^6} \\ \frac{\xi^6}{4} & 0 & 0 & \frac{1}{4} & \frac{\xi^6}{4} & \frac{-1}{4} \\ \frac{1}{4} & \frac{\xi^6}{4} & \frac{1}{4} & \frac{1}{4\xi^6} & \frac{1}{2} & 0 \\ \frac{1}{4\xi^6} & \frac{-1}{4} & \frac{\xi^6}{4} & \frac{-1}{4} & 0 & \frac{1}{2} \end{pmatrix}, \begin{pmatrix} \frac{1}{4} & 0 & 0 & \frac{-1}{4} & \frac{(-1-\sqrt{3})}{8} & \frac{(\sqrt{3}-1)}{8} \\ 0 & \frac{1}{4} & \frac{1}{4} & 0 & \frac{(\sqrt{3}-1)}{8} & \frac{(1+\sqrt{3})}{8} \\ 0 & \frac{1}{4} & \frac{1}{4} & 0 & \frac{(\sqrt{3}-1)}{8} & \frac{(1+\sqrt{3})}{8} \\ \frac{-1}{4} & 0 & 0 & \frac{1}{4} & \frac{(1+\sqrt{3})}{8} & \frac{(1-\sqrt{3})}{8} \\ \frac{-1-\sqrt{3}}{8} & \frac{\sqrt{3}-1}{8} & \frac{\sqrt{3}-1}{8} & \frac{1+\sqrt{3}}{8} & \frac{1}{2} & 0 \\ \frac{\sqrt{3}-1}{8} & \frac{1+\sqrt{3}}{8} & \frac{1+\sqrt{3}}{8} & \frac{1-\sqrt{3}}{8} & 0 & \frac{1}{2} \end{pmatrix}.$$

A direct yet tedious calculation shows that $X_1, \ldots, X_9$ are projections, $\sum_j X_j = 3I$ and $X_j X_k X_j = \frac{1}{4} X_j$ for $j \neq k$. Therefore $\pi(x_j) = X_j$ defines a representation $\pi : \mathcal{A}_S \to \mathrm{M}_6(\mathbb{C})$. Furthermore, one can verify that the span of $\{X_{j_1} X_{j_2} : 1 \leq j_1, j_2 \leq 9\}$ has dimension 25. Hence π is not a 2-fold inflation of a 3-dimensional representation or a direct sum of two 3-dimensional representations (since $25 > 9, 18$), so π is an irreducible representation by Proposition D.1.

References

[AAA+23] R. Acharya, I. Aleiner, R. Allen, et al. "Suppressing quantum errors by scaling a surface code logical qubit". In: *Nature* 614.7949 (2023), pp. 676–681.

[AAB+19] F. Arute, K. Arya, R. Babbush, et al. "Quantum supremacy using a programmable superconducting processor". In: *Nature* 574.7779 (2019), pp. 505–510.

[AB09] S. Arora and B. Barak. *Computational Complexity: A Modern Approach*. Cambridge University Press, 2009.

[ADF+18] R. Arnon-Friedman, F. Dupuis, O. Fawzi, et al. "Practical device-independent quantum cryptography via entropy accumulation". In: *Nat. Commun.* 9.1 (2018), p. 459.

[APV+16] A. Acín, S. Pironio, T. Vértesi, et al. "Optimal randomness certification from one entangled bit". In: *Phys. Rev. A* 93 (4 2016), p. 040102.

[BCK+23] P. Baptista, R. Chen, J. Kaniewski, et al. "A mathematical foundation for self-testing: Lifting common assumptions". In: *arXiv* 2310.12662 (2023).

[BCP+14] N. Brunner, D. Cavalcanti, S. Pironio, et al. "Bell nonlocality". In: *Rev. Mod. Phys.* 86 (2 2014), pp. 419–478.

[Ben92] C. H. Bennett. "Quantum cryptography using any two nonorthogonal states". In: *Phys. Rev. Lett.* 68 (21 1992), pp. 3121–3124.

[BFF21] P. Brown, H. Fawzi, and O. Fawzi. "Computing conditional entropies for quantum correlations". In: *Nat. Commun.* 12.1 (2021), p. 575.

[BFF24] P. Brown, H. Fawzi, and O. Fawzi. "Device-independent lower bounds on the conditional von Neumann entropy". In: *Quantum* 8 (2024), p. 1445.

[BJS+22] J. J. Borkała, C. Jebarathinam, S. Sarkar, et al. "Device-Independent Certification of Maximal Randomness from Pure Entangled Two-Qutrit States Using Non-Projective Measurements". In: *Entropy* 24.3 (2022).

[Bla06] B. Blackadar. *Operator algebras*. Vol. 122. Encyclopaedia of Mathematical Sciences. Springer-Verlag, Berlin, 2006.

[BLM+09] C.-E. Bardyn, T. C. H. Liew, S. Massar, et al. "Device-independent state estimation based on Bell's inequalities". In: *Phys. Rev. A* 80 (6 2009), p. 062327.

[BQT+15] N. Bent, H. Qassim, A. A. Tahir, et al. "Experimental Realization of Quantum Tomography of Photonic Qudits via Symmetric Informationally Complete Positive Operator-Valued Measures". In: *Phys. Rev. X* 5 (4 2015), p. 041006.

[BSS14] J.-D. Bancal, L. Sheridan, and V. Scarani. "More randomness from the same data". In: *New J. Phys.* 16.3 (2014), p. 033011.

[CMF+22] M. P. Colomer, L. Mortimer, I. Frérot, et al. "Three numerical approaches to find mutually unbiased bases using Bell inequalities". In: *Quantum* 6 (2022), p. 778.

[Col07] R. Colbeck. "Quantum And Relativistic Protocols For Secure Multi-Party Computation". PhD thesis. University of Cambridge, 2007.

[CVY13] M. Coudron, T. Vidick, and H. Yuen. "Robust Randomness Amplifiers: Upper and Lower Bounds". In: *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques*. Ed. by P. Raghavendra, S. Raskhodnikova, K. Jansen, et al. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 468–483.

[DFR20] F. Dupuis, O. Fawzi, and R. Renner. "Entropy Accumulation". In: *Comm. Math. Phys.* 379.3 (2020), pp. 867–913.

[DHM+21] M. Doda, M. Huber, G. Murta, et al. "Quantum Key Distribution Overcoming Extreme Noise: Simultaneous Subspace Coding Using High-Dimensional Entanglement". In: *Phys. Rev. Appl.* 15 (3 2021), p. 034003.

[DPP05] G. M. D'Ariano, P. L. Presti, and P. Perinotti. "Classical randomness in quantum measurements". In: *J. Phys. A* 38.26 (2005), p. 5979.

[DPS04] G. M. D'Ariano, P. Perinotti, and M. F. Sacchi. "Informationally complete measurements and group representation". In: *J. Opt. B* 6.6 (2004), S487.

[Far24] M. Farkas. "Unbounded Device-Independent Quantum Key Rates from Arbitrarily Small Nonlocality". In: *Phys. Rev. Lett.* 132 (21 2024), p. 210803.

[FKN23] M. Farkas, J. Kaniewski, and A. Nayak. "Mutually Unbiased Measurements, Hadamard Matrices, and Superdense Coding". In: *IEEE Trans. Inf. Theory* 69.6 (2023), pp. 3814–3824.

[GLV+24] S. Goel, S. Leedumrongwatthanakun, N. H. Valencia, et al. "Inverse design of high-dimensional quantum optical circuits in a complex medium". In: *Nat. Phys.* 20.2 (2024), pp. 232–239.

[GP24] S. Gribling and S. Polak. "Mutually unbiased bases: polynomial optimization and symmetry". In: *Quantum* 8 (2024), p. 1318.

[GTZ+23] S. Goel, M. Tyler, F. Zhu, et al. "Simultaneously Sorting Overlapping Quantum States of Light". In: *Phys. Rev. Lett.* 130 (14 2023), p. 143602.

[Kan16] J. Kaniewski. "Analytic and Nearly Optimal Self-Testing Bounds for the Clauser-Horne-Shimony-Holt and Mermin Inequalities". In: *Phys. Rev. Lett.* 117 (7 2016), p. 070402.

[Kan20] J. Kaniewski. "Weak form of self-testing". In: *Phys. Rev. Res.* 2 (3 2020), p. 033420.

[KGV83] S. Kirkpatrick, C. D. Gelatt, and M. P. Vecchi. "Optimization by Simulated Annealing". In: *Science* 220.4598 (1983), pp. 671–680.

[LLR+21] W.-Z. Liu, M.-H. Li, S. Ragy, et al. "Device-independent randomness expansion against quantum side information". In: *Nat. Phys.* 17.4 (2021), pp. 448–451.

[LZL+21] M.-H. Li, X. Zhang, W.-Z. Liu, et al. "Experimental Realization of Device-Independent Quantum Randomness Expansion". In: *Phys. Rev. Lett.* 126 (5 2021), p. 050503.

[MBB+23] F. Mazzoncini, B. Bauer, P. Brown, et al. "Hybrid Quantum Cryptography from Communication Complexity". In: *arXiv* 2311.09164 (2023).

[MDC+21] T. Metger, Y. Dulek, A. Coladangelo, et al. "Device-independent quantum key distribution from computational assumptions". In: *New J. Phys.* 23.12 (2021), p. 123021.

[MLA+22] L. S. Madsen, F. Laudenbach, M. F. Askarani, et al. "Quantum computational advantage with a programmable photonic processor". In: *Nature* 606.7912 (2022), pp. 75–81.

[MPS24] L. Mančinska, J. Prakash, and C. Schafhauser. "Constant-Sized Robust Self-Tests for States and Measurements of Unbounded Dimension". In: *Comm. Math. Phys.* 405.9 (2024), p. 221.

[MS17] C. A. Miller and Y. Shi. "Universal Security for Randomness Expansion from the Spot-Checking Protocol". In: *SIAM J. Comput.* 46.4 (2017), pp. 1304–1335.

[NPA12] M. Navascués, S. Pironio, and A. Acín. "SDP Relaxations for Non-Commutative Polynomial Optimization". In: *Handbook on Semidefinite, Conic and Polynomial Optimization*. New York, NY: Springer US, 2012, pp. 601–634.

[PAM+10] S. Pironio, A. Acín, S. Massar, et al. "Random numbers certified by Bell's theorem". In: *Nature* 464.7291 (2010), pp. 1021–1024.

[Pro07] C. Procesi. *Lie groups*. Universitext. An approach through invariants and representations. Springer, New York, 2007, pp. xxiv+596.

[Qua24] I. Quantique. *Quantum Random Number Generation*. `https://www.idquantique.com/random-number-generation/overview/`. Accessed: 04/09/2024. 2024.

[Reg09] O. Regev. "On lattices, learning with errors, random linear codes, and cryptography". In: *J. ACM* 56.6 (2009).

[Ren04] J. M. Renes. "Spherical-code key-distribution protocols for qubits". In: *Phys. Rev. A* 70 (5 2004), p. 052314.

[Ren05] J. M. Renes. "Equiangular spherical codes in quantum cryptography". In: *Quantum Info. Comput.* 5.1 (2005), pp. 81–92.

[RSA78] R. L. Rivest, A. Shamir, and L. Adleman. "A method for obtaining digital signatures and public-key cryptosystems". In: *Commun. ACM* 21.2 (1978), pp. 120–126.

[SAZ+18] J. Shang, A. Asadian, H. Zhu, et al. "Enhanced entanglement criterion via symmetric informationally complete measurements". In: *Phys. Rev. A* 98 (2 2018), p. 022309.

[ŠB20] I. Šupić and J. Bowles. "Self-testing of quantum systems: a review". In: *Quantum* 4 (2020), p. 337.

[SG10] A. J. Scott and M. Grassl. "Symmetric informationally complete positive-operator-valued measures: A new computer study". In: *J. Math. Phys.* 51.4 (2010).

[Sha48] C. E. Shannon. "A mathematical theory of communication". In: *Bell Syst. Tech. J.* 27.3 (1948), pp. 379–423.

[SZB+21] L. K. Shalm, Y. Zhang, J. C. Bienfang, et al. "Device-independent randomness expansion with entangled photons". In: *Nat. Phys.* 17.4 (2021), pp. 452–456.

[Tak02] M. Takesaki. *Theory of operator algebras. I.* Vol. 124. Encyclopaedia of Mathematical Sciences. Reprint of the first (1979) edition, Operator Algebras and Noncommutative Geometry, 5. Springer-Verlag, Berlin, 2002, pp. xx+415.

[TCR09] M. Tomamichel, R. Colbeck, and R. Renner. "A Fully Quantum Asymptotic Equipartition Property". In: *IEEE Trans. Inf. Theory* 55.12 (2009), pp. 5840–5847.

[TFR+21] A. Tavakoli, M. Farkas, D. Rosset, et al. "Mutually unbiased bases and symmetric informationally complete measurements in Bell experiments". In: *Sci. Adv.* 7.7 (2021), eabc3847.

[Tos24] Toshiba. *Quantum Random Number Generators*. `https://www.toshiba.eu/pages/eu/Cambridge-Research-Laboratory/quantum-random-number-generators`. Accessed: 04/09/2024. 2024.

[TRR19] A. Tavakoli, D. Rosset, and M.-O. Renou. "Enabling Computation of Correlation Bounds for Finite-Dimensional Quantum Systems via Symmetrization". In: *Phys. Rev. Lett.* 122 (7 2019), p. 070501.

[VB10] T. Vértesi and E. Bene. "Two-qubit Bell inequality for which positive operator-valued measurements are relevant". In: *Phys. Rev. A* 82 (6 2010), p. 062115.

[VV12] U. Vazirani and T. Vidick. "Certifiable quantum dice: or, true random number generation secure against quantum adversaries". In: *Proceedings of the ACM symposium on Theory of computing*. ACM New York, 2012, pp. 61–76.

[Wal18] S. F. D. Waldron. *An introduction to finite tight frames*. Applied and Numerical Harmonic Analysis. Birkhäuser/Springer, New York, 2018, pp. xx+587.

[YVB+14] T. H. Yang, T. Vértesi, J.-D. Bancal, et al. "Robust and Versatile Black-Box Certification of Quantum Devices". In: *Phys. Rev. Lett.* 113 (4 2014), p. 040401.

[Zau11] G. Zauner. "Quantum designs: foundations of a noncommutative design theory". In: *Int. J. Quantum Inf.* 09.01 (2011), pp. 445–507.

[ZFK20] Y. Zhang, H. Fu, and E. Knill. "Efficient randomness certification by quantum probability estimation". In: *Phys. Rev. Res.* 2 (1 Jan. 2020), p. 013016.

[ZKB18] Y. Zhang, E. Knill, and P. Bierhorst. "Certifying quantum randomness by probability estimation". In: *Phys. Rev. A* 98 (4 Oct. 2018), p. 040304.

[ZTV+21] F. Zhu, M. Tyler, N. H. Valencia, et al. "Is high-dimensional photonic entanglement robust to noise?" In: *AVS Quantum Science* 3.1 (2021), p. 011401.

Department of Mathematics, University of York, United Kingdom
Email address: mate.farkas@york.ac.uk

Department of Mathematics, University of Auckland, New Zealand
Email address: jurij.volcic@auckland.ac.nz

Department of Mathematical Sciences, University of Copenhagen, Denmark
Email address: sals@math.ku.dk

Quantum Science Center of Guangdong-Hong Kong-Macao Greater Bay Area, China, Department of Mathematical Sciences, University of Copenhagen, Denmark
Email address: chenranyiliu@quantumsc.cn

Department of Mathematical Sciences, University of Copenhagen, Denmark
Email address: mancinska@math.ku.dk