All Pure Bipartite Entangled States can be Self-Tested

Andrea Coladangelo,[1] Koon Tong Goh,[2] and Valerio Scarani[2,3]

[1] *Department of Computing and Mathematical Sciences, California Institute of Technology, 1200 E California Blvd, Pasadena, CA 91125, United States*

[2] *Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, Singapore 117543*

[3] *Department of Physics, National University of Singapore, 2 Science Drive 3, Singapore 117542*

Device-independent self-testing allows to uniquely charaterize the quantum state shared by untrusted parties (up to local isometries) by simply inspecting their correlations, and requiring only minimal assumptions, namely a no-signaling constraint on the untrusted parties and the validity of quantum mechanics. The device-independent approach exploits the fact that certain non-local correlations can be uniquely achieved by measurements on a particular quantum state. We can think of these correlations as a "classical fingerprint" of the self-tested quantum state. In this work, we show that all pure bipartite entangled states can be self-tested, by providing explicit self-testing correlations for each.

I. INTRODUCTION

Device-independent self-testing enables a completely classical verifier to characterize the joint quantum state shared by two potentially untrusted parties (the provers), up to local isometries, by simple inspection of the observed correlations. This approach requires minimal assumptions, namely a no-signaling constraint on the provers, and the validity of quantum mechanics. Thus, in a device-independent scenario [1], one can obtain guarantees on the functionality of a device without making assumptions on its inner-workings.

Self-testing is made possible by the existence of non-local correlations in quantum theory. While all correlations produced by classical provers are necessarily local, on the other hand, it is possible to produce non-local correlations by measuring a joint quantum state that is entangled [5]. It is well-known that certain entangled quantum states can be self-tested, meaning that a classical verifier can certify that such a state is shared by the two provers by observing the maximal violation of some Bell inequality, the ideal winning probability in some non-local game played by the provers, or simply by observing correlations that can be uniquely obtained by measurements on that state. The most celebrated example of a state that can be self-tested is the maximally entangled pair of qubits (the singlet). This is self-tested, for instance, by observing maximal violation of the well-known Clauser-Horne-Shimony-Holt (CHSH) inequality [19, 23].

The term "self-testing" in the context of Bell experiments was coined by Mayers and Yao [11], when they introduced a criterion to self-test the singlet state for the bipartite Bell scenario with three dichotomic measurements on each side. Since then, the self-testing of the two-qubit singlet has been made robust [14], then extended to sequential [20] and parallel certification of many copies [6–8, 13, 16, 25]; and the complete set of criteria that self-test that state with two dichotomic measurements has been provided [24]. Moreover, a variety of other quantum states have been proved to be self-testable: all partially entangled pure two-qubit states [4, 27], the maximally entangled pair of qutrits [21], the partially entangled pair of qutrits that violates maximally the CGLMP_3 inequality [2, 28], and a small class of higher dimensional partially entangled pairs of qudits, through results in parallel self-testing [7]. For the multi-partite case, it is known that the three-qubit W state [17, 26] and graph states [12, 17] can be self-tested. Hence, it is clear that self-testing is not an exclusive characteristic of maximally entangled states nor qubit states. However, little is known about self-testing of higher-dimensional entangled states (i.e. pairs of entangled qudits for $d > 2$).

In this paper, we consider the outstanding open question of whether all bipartite pure entangled quantum states can be self-tested. Building on the framework sketched by Yang and Navascués [27], we answer this question affirmatively with an explicit construction of a family of self-testing correlations.

On top of answering a fundamental question of quantum information science, our result has potential applications in protocols for Quantum Random Number Generation (QRNG) and for verification of delegated quantum computation. Several known protocols are in fact based on self-testing, usually on the rigidity of the CHSH game [9, 15, 20]; our work adds the flexibility of choosing the self-tested state in the bipartite scenario. The most direct application of our result may be in device-independent randomness expansion, the first device-independent QRNG scheme to be proposed, and the only to have been experimentally implemented [18]. There, guaranteed private randomness is generated from an initial random seed. Based on our self-testing procedure, a small random seed (two random trits per run) could provide up to $O(\log d)$ bits of private randomness, with d limited only by the experimental state-of-the-art. While this falls short of the infinite randomness expansion that was shown to be in principle possible with quantum theory [9, 15], such a randomness expansion protocol would use a single Bell setup and would thus become feasible as soon as one can realise loophole-free Bell tests with entangled states of dimension d. Of course, an analysis of the robustness

of our self-testing result is required to assess its applicability. We leave this to future work.

II. GENERAL FRAMEWORK

A. Preliminaries

In a bipartite Bell scenario, the two provers Alice and Bob receive inputs x and y respectively, corresponding to their choice of measurement settings, and their devices return outcomes a and b.
In the particular scenario that we will consider, which will allow us to produce the correlations needed to self-test any bipartite entangled state, Alice has three possible measurement settings and Bob has four, while the devices have d possible outcomes. So the inputs are $x \in \{0, 1, 2\}$ and $y \in \{0, 1, 2, 3\}$, and the outputs are $a, b \in \{0, 1, 2, \cdots, d-1\}$. We refer to this as a $[\{3, d\}, \{4, d\}]$ Bell scenario (see FIG. 1).

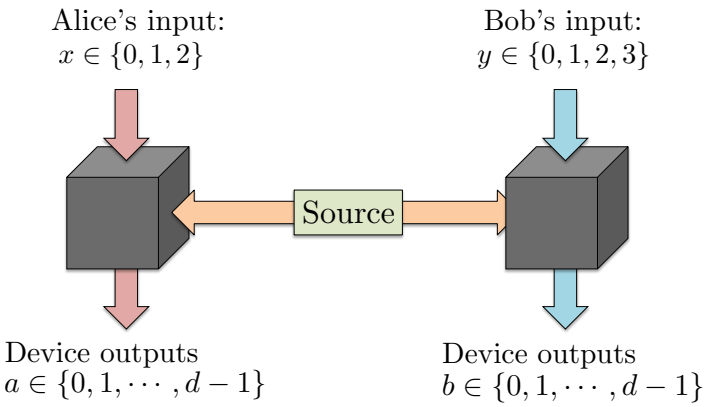

FIG. 1: A $[\{3, d\}, \{4, d\}]$ Bell scenario

The result of this Bell experiment can be fully described by the values of the conditional probabilities, $P(a, b|x, y)$. We can arrange these $P(a, b|x, y)$ in twelve $d \times d$ correlation tables, one for each pair of measurement settings, denoted by $T_{x,y}$.

$$T_{x,y} := \begin{array}{|c||c|c|c|c|} \hline a\backslash b & 0 & 1 & \cdots & d-1 \\ \hline\hline 0 & P(0,0|x,y) & P(0,1|x,y) & \cdots & P(0,d-1|x,y) \\ \hline 1 & P(1,0|x,y) & P(1,1|x,y) & \cdots & P(1,d-1|x,y) \\ \hline \vdots & \vdots & \vdots & \ddots & \vdots \\ \hline d-1 & P(d-1,0|x,y) & P(d-1,1|x,y) & \cdots & P(d-1,d-1|x,y) \\ \hline \end{array} \tag{1}$$

In the device-independent approach, the dimensionality of the measured system is not bounded a priori. Hence, the joint quantum state of the measured system can be assumed to be a pure state (denoted by $|\psi\rangle$) and the measurements made on the system to be projective, with $\Pi_a^{A_x}$ the projection corresponding to Alice obtaining outcome a on measurement setting x, and likewise for $\Pi_b^{B_y}$ on Bob's side. Moreover, any correlations produced by a bipartite mixed state can be reproduced by a bipartite pure state of the same dimension [22], which implies that bipartite mixed states cannot be self-tested. Hence, in the bipartite scenario, the best one can hope for is to self-test every pure state, and this is what we set out to do in the present work.

No further characterisation of either the state or the measurements is required, and estimating the $P(a, b|x, y)$ is all that has to be done in the lab. If the correlations $P(a, b|x, y)$ imply the existence of a local isometry Φ such that $\Phi(|\psi\rangle) = |\text{extra}\rangle \otimes |\psi_{\text{target}}\rangle$ i.e. Φ maps the unknown state $|\psi\rangle$ to the target state $|\psi_{\text{target}}\rangle$ tensored with a state $|\text{extra}\rangle$ that can be an arbitrary state, then we say that the correlations self-test $|\psi_{\text{target}}\rangle$. Our objective is to self-test all bipartite quantum states, and, using the Schmidt decomposition, this reduces to self-testing an arbitrary bipartite

quantum state of the form

$$|\psi_{\text{target}}\rangle := \sum_{i=0}^{d-1} c_i |ii\rangle \tag{2}$$

where $0 < c_i \leq 1$ for all i and $\sum_{i=0}^{d-1} c_i^2 = 1$.

B. Sufficient conditions for self-testing

In what follows, the subscript indicates the subsystem that an operator acts on (A for Alice and B for Bob).

Lemma 1. *(Yang-Navascués [27]) Let $|\psi_{target}\rangle = \sum_{i=0}^{d-1} c_i|ii\rangle$, where $0 < c_i \leq 1$ for all i and $\sum_{i=0}^{d-1} c_i^2 = 1$. Suppose there exist unitary operators $X_A^{(k)}, X_B^{(k)}, Z_A, Z_B$ and complete sets of orthogonal projections $\{P_A^{(k)}\}$ and $\{P_B^{(k)}\}$ satisfying the following conditions:*

$$Z_{A/B} = \sum_{k=0}^{d-1} \omega^k P_{A/B}^{(k)}, \tag{3}$$

$$P_A^{(k)}|\psi\rangle = P_B^{(k)}|\psi\rangle \ \ \forall k, \tag{4}$$

$$X_A^{(k)} P_B^{(k)}|\psi\rangle = \frac{c_k}{c_0}(X_B^{(k)})^\dagger P_A^{(0)}|\psi\rangle \tag{5}$$

where $\omega = e^{2\pi i/d}$. Then there exists a local isometry Φ such that $\Phi(|\psi\rangle) = |extra\rangle \otimes |\psi_{target}\rangle$, i.e. the state $|\psi_{target}\rangle$ is self-tested.

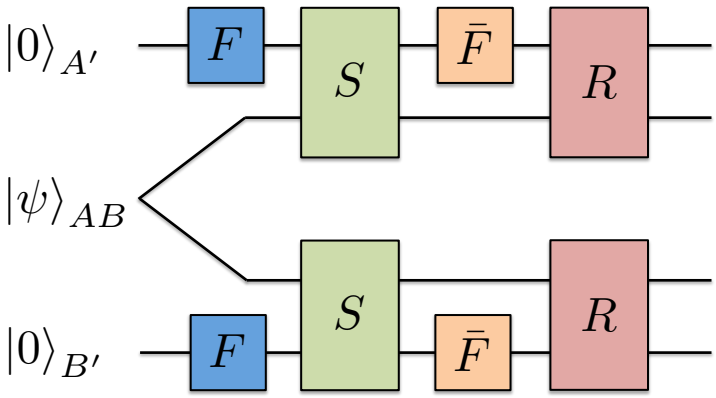

FIG. 2: Diagram of the isometry $\Phi(|\psi\rangle)$

The complete proof of this is given in the Appendix. Here we just describe how the local isometry Φ is constructed (Fig. 2). The local isometry adds two ancilla qudits in the zero state, and is a generalization of the SWAP isometry that is typically used in the qubit case. More precisely,

$$\Phi(|\psi\rangle) = (R_{A,A'} \otimes R_{B,B'})(\bar{F}_{A'} \otimes \bar{F}_{B'})(S_{AA'} \otimes S_{BB'})(F_{A'} \otimes F_{B'})|\psi\rangle_{AB}|0\rangle_{A'}|0\rangle_{B'} \tag{6}$$

where F is the quantum Fourier transform, $\bar{F}$ is the inverse quantum Fourier transform, $R_{AA'/BB'}$ is defined as $R_{AA'/BB'}|\psi\rangle_{AB}|k\rangle_{A/B} = X_{A/B}^{(k)}|\psi\rangle_{AB}|k\rangle_{A/B}$ and $S_{AA'/BB'}$ is defined as $S_{AA'/BB'}|\psi\rangle_{AB}|k\rangle_{A/B} = Z_{A/B}^k|\psi\rangle_{AB}|k\rangle_{A/B}$. Yang and Navascués [27] did not provide, or prove the existence of, correlations from which conditions (3)-(5) follow, and this is what we will contribute.

C. The idea behind our correlations

Here we give a sketch of the structure of the correlations that we will describe in full detail in the next section, and an intuition as to why they work. For clarity, in this paragraph we assume d to be even, but the proof will apply to odd d as well.
Recall that we wish to self-test the state $|\psi_{\text{target}}\rangle = \sum_{i=0}^{d-1} c_i|ii\rangle$, where $0 < c_i \leq 1$ for all i and $\sum_{i=0}^{d-1} c_i^2 = 1$. The approach, inspired by [27], is to use d-outcome measurements on Alice and Bob's side such that, for some measurement settings, the correlation tables $T_{x,y}$, as defined in (1), are block-diagonal with 2×2 blocks. More precisely, for measurement settings $x, y \in \{0, 1\}$, the 2×2 blocks will correspond to outcomes a, b respectively in $\{0, 1\}$, in $\{2, 3\}$,.., in $\{d-2, d-1\}$; and the idea is that the mth 2×2 block self-tests the portion $c_{2m}|2m\ 2m\rangle + c_{2m+1}|2m+1\ \ 2m+1\rangle$ of the target state. For measurement settings $x \in \{0, 2\}, y \in \{2, 3\}$, instead, the 2×2 blocks will correspond to outcomes a, b respectively in $\{1, 2\}$, in $\{3, 4\}$,.., in $\{d-1, 0\}$, again the idea being that the mth block "self-tests" the portion $c_{2m+1}|2m+1\ 2m+1\rangle + c_{2m+2}|2m+2\ \ 2m+2\rangle$.
See Fig. 3 for an illustration of the concept.

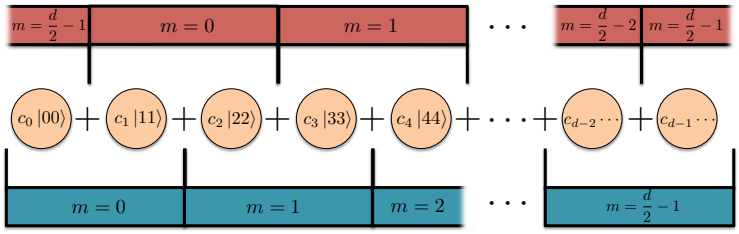

FIG. 3: In blue, the block-diagonal correlations for measurement settings $x, y \in \{0, 1\}$ "certify" the "even-odd" pairs, while, in red, the block-diagonal correlations for measurement settings $x \in \{0, 2\}, y \in \{2, 3\}$ certify the odd-even pairs.

In the following section, we will introduce explicit correlations that allow us to construct unitary operators satisfying the conditions of equations (3)-(5). These correlations use as a building block a known criterion for self-testing partially entangled states of two qubits, based on the *tilted CHSH inequality* [3]:

$$\left\langle \alpha \hat{A}_0 + \hat{A}_0\hat{B}_0 + \hat{A}_0\hat{B}_1 + \hat{A}_1\hat{B}_0 - \hat{A}_1\hat{B}_1 \right\rangle \leq 2 + \alpha \tag{7}$$

where $x, y, a, b \in \{0, 1\}$, $\alpha \in [0, 2)$, $\hat{A}_x = \Pi_0^{A_x} - \Pi_1^{A_x}$ and $\hat{B}_y = \Pi_0^{B_y} - \Pi_1^{B_y}$. The maximum quantum violation of the tilted-CHSH inequality is $\sqrt{8 + 2\alpha^2}$, and this self-tests the partially entangled pair of qubits $|\psi_\theta\rangle = \cos\theta|00\rangle + \sin\theta|11\rangle$ with $\sin(2\theta) = \sqrt{\frac{4-\alpha^2}{4+\alpha^2}}$ [4, 27]. The 2×2 blocks in our block-diagonal correlations will naturally correspond to ideal tilted CHSH correlations for appropriately chosen angles.

As we shall clarify later, this particular choice for the 2×2 blocks is not essential: although no other criterion for self-testing arbitrary partially entangled qubits is currently known, any other self-testing correlations from which we can deduce the existence of operators satisfying (37) and (38) could in principle be used in our proof.

III. PROOF OF SELF-TESTING

A. The correlations and their implications

In order to self-test the target state $|\psi_{\text{target}}\rangle = \sum_{i=0}^{d-1} c_i|ii\rangle$, where $0 < c_i \leq 1$, we won't need to specify the whole set of twelve correlations tables $T_{x,y}$, but it will be sufficient for us to specify the tables corresponding to measurement settings $x, y \in \{0, 1\}$, and those for settings $x \in \{0, 2\}, y \in \{2, 3\}$. The constraints we place on these will be sufficient to self-test $|\psi_{\text{target}}\rangle$.
Building on an idea of Yang and Navascués [27], our self-testing correlations will be block diagonal with 2×2 blocks. The tables for measurement settings $x, y \in \{0, 1\}$ are given in Tables I and II for even and odd d respectively. The 2×2 blocks $C_{x,y,m}$ are given by $(c_{2m}^2 + c_{2m+1}^2) \cdot C^{\text{ideal}}_{x,y,\theta_m}$ where the $C^{\text{ideal}}_{x,y,\theta_m}$ are the 2-by-2 correlation tables which correspond to the maximal violation of the tilted-CHSH inequality which self-tests the state $\cos(\theta_m)|00\rangle + \sin(\theta_m)|11\rangle$, where $\theta_m := \arctan\left(\frac{c_{2m+1}}{c_{2m}}\right) \in [0, \pi]$. They are given precisely in Tables III-V, with $\mu_m := \arctan(\sin(2\theta_m))$. The correlation

tables for measurement settings $x \in \{0,2\}, y \in \{2,3\}$, are presented later in Tables VI-X, after having derived some consequences of the correlations for measurement settings $x, y \in \{0,1\}$.

TABLE I: $T_{x,y}$ for $x, y \in \{0,1\}$ for even values of $d \geq 2$

$a\backslash b$	0	1	2	3	$\cdots$	$d-2$	$d-1$
0	$C_{x,y,m=0}$		0	0	$\cdots$	0	0
1			0	0	$\cdots$	0	0
2	0	0	$C_{x,y,m=1}$		$\cdots$	0	0
3	0	0			$\cdots$	0	0
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$
$d-2$	0	0	0	0	$\cdots$	$C_{x,y,m=\frac{d}{2}-1}$	
$d-1$	0	0	0	0	$\cdots$		

TABLE II: $T_{x,y}$ for $x, y \in \{0,1\}$ for odd values of $d \geq 3$

$a\backslash b$	0	1	2	3	$\cdots$	$d-3$	$d-2$	$d-1$
0	$C_{x,y,m=0}$		0	0	$\cdots$	0	0	0
1			0	0	$\cdots$	0	0	0
2	0	0	$C_{x,y,m=1}$		$\cdots$	0	0	0
3	0	0			$\cdots$	0	0	0
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$	0
$d-3$	0	0	0	0	$\cdots$	$C_{x,y,m=\frac{d-3}{2}}$		0
$d-2$	0	0	0	0	$\cdots$			0
$d-1$	0	0	0	0	$\cdots$	0	0	c_{d-1}^2

TABLE III: 2×2 block correlation table $C_{x=0,y=0,m}$ and $C_{x=0,y=1,m}$

$a\backslash b$	2m	2m+1
2m	$c_{2m}^2 \cos^2\left(\frac{\mu_m}{2}\right)$	$c_{2m}^2 \sin^2\left(\frac{\mu_m}{2}\right)$
2m+1	$c_{2m+1}^2 \sin^2\left(\frac{\mu_m}{2}\right)$	$c_{2m+1}^2 \cos^2\left(\frac{\mu_m}{2}\right)$

TABLE IV: 2×2 block correlation table $C_{x=1,y=0,m}$

$a\backslash b$	2m	2m+1
2m	$\frac{1}{2}(c_{2m}\cos\left(\frac{\mu_m}{2}\right) + c_{2m+1}\sin\left(\frac{\mu_m}{2}\right))^2$	$\frac{1}{2}(c_{2m+1}\cos\left(\frac{\mu_m}{2}\right) - c_{2m}\sin\left(\frac{\mu_m}{2}\right))^2$
2m+1	$\frac{1}{2}(c_{2m}\cos\left(\frac{\mu_m}{2}\right) - c_{2m+1}\sin\left(\frac{\mu_m}{2}\right))^2$	$\frac{1}{2}(c_{2m+1}\cos\left(\frac{\mu_m}{2}\right) + c_{2m}\sin\left(\frac{\mu_m}{2}\right))^2$

TABLE V: 2×2 block correlation table $C_{x=1,y=1,m}$

$a\backslash b$	2m	2m+1
2m	$\frac{1}{2}(c_{2m}\cos(\frac{\mu_m}{2}) - c_{2m+1}\sin(\frac{\mu_m}{2}))^2$	$\frac{1}{2}(c_{2m+1}\cos(\frac{\mu_m}{2}) + c_{2m}\sin(\frac{\mu_m}{2}))^2$
2m+1	$\frac{1}{2}(c_{2m}\cos(\frac{\mu_m}{2}) + c_{2m+1}\sin(\frac{\mu_m}{2}))^2$	$\frac{1}{2}(c_{2m+1}\cos(\frac{\mu_m}{2}) - c_{2m}\sin(\frac{\mu_m}{2}))^2$

Recall that $\Pi_i^{A_x}$ is the projection corresponding to Alice obtaining outcome i on measurement setting x, and similarly for $\Pi_i^{B_y}$ on Bob's side. We define the operators $\hat{A}_{x,m} = \Pi_{2m}^{A_x} - \Pi_{2m+1}^{A_x}$ and $\hat{B}_{y,m} = \Pi_{2m}^{B_y} - \Pi_{2m+1}^{B_y}$ for $x, y \in \{0,1\}$. Clearly, $(\hat{A}_{x,m})^2 = \Pi_{2m}^{A_x} + \Pi_{2m+1}^{A_x} := \mathbb{1}_m^{A_x}$ and $(\hat{B}_{y,m})^2 = \Pi_{2m}^{B_y} + \Pi_{2m+1}^{B_y} := \mathbb{1}_m^{B_y}$.
Now, $\|\Pi_{2m}^{A_0}|\psi\rangle\| = \sqrt{\langle\psi|\Pi_{2m}^{A_0}|\psi\rangle} = \sqrt{\langle\psi|\Pi_{2m}^{A_0}\cdot\sum_{i=0}^{d-1}\Pi_i^{B_0}|\psi\rangle} = \sqrt{c_{2m}^2\cos^2(\frac{\mu_m}{2}) + c_{2m}^2\sin^2(\frac{\mu_m}{2})} = c_{2m}$, and $\|\Pi_{2m+1}^{A_0}|\psi\rangle\| = c_{2m+1}$. With similar other calculations we deduce that

$$\|\mathbb{1}_m^{A_i}|\psi\rangle\| = \|\mathbb{1}_m^{B_j}|\psi\rangle\| = \sqrt{c_{2m}^2 + c_{2m+1}^2} \quad \forall i,j \in \{0,1\}\,. \tag{8}$$

Moreover, notice that $\langle\psi|\mathbb{1}_m^{A_i}\mathbb{1}_m^{B_j}|\psi\rangle = c_{2m}^2 + c_{2m+1}^2 = \|\mathbb{1}_m^{A_i}|\psi\rangle\|\cdot\|\mathbb{1}_m^{B_j}|\psi\rangle\|$. Hence, by Cauchy-Schwarz, it must be the case that

$$\mathbb{1}_m^{A_i}|\psi\rangle = \mathbb{1}_m^{B_j}|\psi\rangle \quad \forall i,j \in \{0,1\}\,. \tag{9}$$

By design, the correlations are such that

$$\langle\psi|\alpha_m\hat{A}_{0,m} + \hat{A}_{0,m}\hat{B}_{0,m} + \hat{A}_{0,m}\hat{B}_{1,m} + \hat{A}_{1,m}\hat{B}_{0,m} - \hat{A}_{1,m}\hat{B}_{1,m}|\psi\rangle = \sqrt{8+2\alpha_m^2}\cdot(c_{2m}^2 + c_{2m+1}^2) \tag{10}$$

where $\alpha_m = \frac{2}{\sqrt{1+2\tan^2(2\theta_m)}}$. As such, this is not a maximal violation of the tilted CHSH inequality (since $|\psi\rangle$ has unit norm). However, we can get around this by defining the normalised state $|\psi'_m\rangle = \frac{\mathbb{1}_m^{A_0}|\psi\rangle}{\sqrt{c_{2m}^2+c_{2m+1}^2}}$. Since $\hat{A}_{i,m}|\psi\rangle = \hat{A}_{i,m}\mathbb{1}_m^{A_i}|\psi\rangle = \hat{A}_{i,m}\mathbb{1}_m^{A_0}|\psi\rangle$, and $\hat{B}_{i,m}|\psi\rangle = \hat{B}_{i,m}\mathbb{1}_m^{B_i}|\psi\rangle = \hat{B}_{i,m}\mathbb{1}_m^{A_0}|\psi\rangle$, by (9), then (10) implies

$$\langle\psi'_m|\alpha_m\hat{A}_{0,m} + \hat{A}_{0,m}\hat{B}_{0,m} + \hat{A}_{0,m}\hat{B}_{1,m} + \hat{A}_{1,m}\hat{B}_{0,m} - \hat{A}_{1,m}\hat{B}_{1,m}|\psi'_m\rangle = \sqrt{8+2\alpha_m^2} \tag{11}$$

Bamps and Pironio [4] proved that such a maximal violation of the tilted-CHSH inequality implies that, letting $\tilde{Z}_{A,m} := \hat{A}_{0,m}$, $\tilde{X}_{A,m} := \hat{A}_{1,m}$, $\tilde{\tilde{Z}}_{B,m} := \frac{\hat{B}_{0,m}+\hat{B}_{1,m}}{2\cos(\mu_m)}$, $\tilde{\tilde{X}}_{B,m} := \frac{\hat{B}_{0,m}-\hat{B}_{1,m}}{2\sin(\mu_m)}$, and then letting $\tilde{Z}_{B,m} := \frac{\tilde{\tilde{Z}}_{B,m}}{|\tilde{\tilde{Z}}_{B,m}|}$ and $\tilde{X}_{B,m} := \frac{\tilde{\tilde{X}}_{B,m}}{|\tilde{\tilde{X}}_{B,m}|}$, we have

$$\tilde{Z}_{A,m}|\psi'_m\rangle = \tilde{Z}_{B,m}|\psi'_m\rangle \tag{12}$$

$$\tilde{X}_{A,m}(\mathbb{1}_m^{A_0} - \tilde{Z}_{A,m})|\psi'_m\rangle = \tan(\theta_m)\tilde{X}_{B,m}(\mathbb{1}_m^{A_0} + \tilde{Z}_{A,m})|\psi'_m\rangle \tag{13}$$

Here, we are slightly abusing notation in $\frac{\tilde{\tilde{Z}}_{B,m}}{|\tilde{\tilde{Z}}_{B,m}|}$ and $\frac{\tilde{\tilde{X}}_{B,m}}{|\tilde{\tilde{X}}_{B,m}|}$, and hence we clarify how these quantities are defined.
They are obtained via the following steps. First notice that all non-zero eigenvalues of $\tilde{\tilde{Z}}_{B,m}$ and $\tilde{\tilde{X}}_{B,m}$ necessarily correspond to eigenvectors in the subspace $\mathcal{B}_m = \text{range}(\mathbb{1}_m^{B_0}) + \text{range}(\mathbb{1}_m^{B_1})$. We divide these eigenvalues by their moduli. Then, we replace 0 eigenvalues with 1 if they correspond to eigenvectors in the subspace $\mathcal{B}_m$. The remaining 0 eigenvalues are left as they are. We remark that we defined the operators $\tilde{Z}_{B,m}$ and $\tilde{X}_{B,m}$ slightly differently than in [4], since we replaced, with 1, only the 0 eigenvalues corresponding to eigenvectors in $\mathcal{B}_m$, rather than *all* 0 eigenvalues, but it is clear that this change doesn't affect the conclusion of Bamps and Pironio [4] that we appealed to, since $|\psi'_m\rangle$ has no support outside of $\mathcal{B}_m$. As a consequence, $\tilde{Z}_{B,m}$ and $\tilde{X}_{B,m}$ are not unitary, and we have instead $(\tilde{Z}_{A,m})^2 = \mathbb{1}_m^{A_0}$, $(\tilde{X}_{A,m})^2 = \mathbb{1}_m^{A_1}$ and $(\tilde{Z}_{B,m})^2 = (\tilde{X}_{B,m})^2 = \mathbb{1}_{\mathcal{B}_m}$, where the latter is the projection onto the subspace $\mathcal{B}_m$.

Note that, importantly, (12) and (13) also imply

$$\tilde{Z}_{A,m}|\psi\rangle = \tilde{Z}_{B,m}|\psi\rangle \tag{14}$$

$$\tilde{X}_{A,m}(\mathbb{1}_m^{A_0} - \tilde{Z}_{A,m})|\psi\rangle = \tan(\theta_m)\tilde{X}_{B,m}(\mathbb{1}_m^{A_0} + \tilde{Z}_{A,m})|\psi\rangle \tag{15}$$

and this is because $\tilde{Z}_{A,m}|\psi'_m\rangle = \frac{1}{\sqrt{c_{2m}^2+c_{2m+1}^2}}\tilde{Z}_{A,m}\mathbb{1}_m^{A_0}|\psi\rangle = \frac{1}{\sqrt{c_{2m}^2+c_{2m+1}^2}}\tilde{Z}_{A,m}|\psi\rangle$, and also

$$\tilde{Z}_{B,m}|\psi'_m\rangle = \frac{1}{\sqrt{c_{2m}^2+c_{2m+1}^2}}\tilde{Z}_{B,m}\mathbb{1}_m^{A_0}|\psi\rangle = \frac{1}{\sqrt{c_{2m}^2+c_{2m+1}^2}}\tilde{Z}_{B,m}|\psi\rangle \tag{16}$$

where we have used (9) and the fact that

$$\mathbb{1}_m^{B_0}|\psi\rangle = \mathbb{1}_m^{B_1}|\psi\rangle \implies \mathbb{1}_{\mathcal{B}_m}|\psi\rangle = \mathbb{1}_m^{B_i}|\psi\rangle\,. \tag{17}$$

Now, we similarly make the correlations $T_{x,y}$ between measurement settings $x \in \{0,2\}$ and $y \in \{2,3\}$ be also block-diagonal, but "shifted down" appropriately by one measurement outcome. The 2×2 blocks are $D_{x,y,m}$ (corresponding to outcomes $2m+1$ and $2m+2$) for $x \in \{0,2\}$ and $y \in \{2,3\}$, defined as $D_{x,y,m} := (c_{2m+1}^2 + c_{2m+2}^2)\cdot C^{ideal}_{f(x),g(y);\theta'_m}$, where $\theta'_m := \arctan\left(\frac{c_{2m+2}}{c_{2m+1}}\right) \in [0,\pi]$, and $f(0)=0, f(2)=1, g(2)=0, g(3)=1$. The correlations, $T_{x,y}$, for $x \in \{0,2\}$ and $y \in \{2,3\}$ are given precisely in Tables VI to X where $\mu'_m := \arctan(\sin(2\theta'_m))$. We will proceed in a similar fashion to what we did above.

TABLE VI: $T_{x,y}$ for $x \in \{0,2\}$ and $y \in \{2,3\}$, for even values of $d \geq 2$

$a\backslash b$	1	2	3	4	$\cdots$	$d-1$	0
1	$D_{x,y,m=0}$		0	0	$\cdots$	0	0
2			0	0	$\cdots$	0	0
3	0	0	$D_{x,y,m=1}$		$\cdots$	0	0
4	0	0			$\cdots$	0	0
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$
$d-1$	0	0	0	0	$\cdots$	$D_{x,y,m=\frac{d}{2}-1}$	
0	0	0	0	0	$\cdots$		

TABLE VII: $T_{x,y}$ for $x \in \{0,2\}$ and $y \in \{2,3\}$, for odd values of $d \geq 3$

$a\backslash b$	1	2	3	4	$\cdots$	$d-2$	$d-1$	0
1	$D_{x,y,m=0}$		0	0	$\cdots$	0	0	0
2			0	0	$\cdots$	0	0	0
3	0	0	$D_{x,y,m=1}$		$\cdots$	0	0	0
4	0	0			$\cdots$	0	0	0
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$	0
$d-2$	0	0	0	0	$\cdots$	$D_{x,y,m=\frac{d-3}{2}}$		0
$d-1$	0	0	0	0	$\cdots$			0
0	0	0	0	0	$\cdots$	0	0	c_0^2

TABLE VIII: 2×2 block correlation table $D_{x=0,y=2,m}$ and $D_{x=0,y=3,m}$

$a\backslash b$	2m+1	2m+2
2m+1	$c_{2m+1}^2 \cos^2(\frac{\mu_m'}{2})$	$c_{2m+1}^2 \sin^2(\frac{\mu_m'}{2})$
2m+2	$c_{2m+2}^2 \sin^2(\frac{\mu_m}{2})$	$c_{2m+2}^2 \cos^2(\frac{\mu_m}{2})$

TABLE IX: 2×2 block correlation table $D_{x=2,y=2,m}$

$a\backslash b$	2m+1	2m+2
2m+1	$\frac{1}{2}(c_{2m+1}\cos(\frac{\mu_m'}{2}) + c_{2m+2}\sin(\frac{\mu_m'}{2}))^2$	$\frac{1}{2}(c_{2m+2}\cos(\frac{\mu_m'}{2}) - c_{2m+1}\sin(\frac{\mu_m'}{2}))^2$
2m+2	$\frac{1}{2}(c_{2m+1}\cos(\frac{\mu_m}{2}) - c_{2m+2}\sin(\frac{\mu_m}{2}))^2$	$\frac{1}{2}(c_{2m+2}\cos(\frac{\mu_m}{2}) + c_{2m+1}\sin(\frac{\mu_m}{2}))^2$

TABLE X: 2×2 block correlation table $D_{x=2,y=3,m}$

$a\backslash b$	2m+1	2m+2
2m+1	$\frac{1}{2}(c_{2m+1}\cos(\frac{\mu_m'}{2}) - c_{2m+2}\sin(\frac{\mu_m'}{2}))^2$	$\frac{1}{2}(c_{2m+2}\cos(\frac{\mu_m'}{2}) + c_{2m+1}\sin(\frac{\mu_m'}{2}))^2$
2m+2	$\frac{1}{2}(c_{2m+1}\cos(\frac{\mu_m}{2}) + c_{2m+2}\sin(\frac{\mu_m}{2}))^2$	$\frac{1}{2}(c_{2m+2}\cos(\frac{\mu_m}{2}) - c_{2m+1}\sin(\frac{\mu_m}{2}))^2$

We can define the operators $\hat{A}'_{0,m} = \Pi_{2m+1}^{A_0} - \Pi_{2m+2}^{A_0}$, $\hat{A}'_{1,m} = \Pi_{2m+1}^{A_2} - \Pi_{2m+2}^{A_2}$ $\hat{B}'_{0,m} = \Pi_{2m+1}^{B_2} - \Pi_{2m+2}^{B_2}$, $\hat{B}'_{1,m} = \Pi_{2m+1}^{B_3} - \Pi_{2m+2}^{B_3}$, and $\mathbb{1}_m^{A'_x} = \left(\hat{A}'_{x,m}\right)^2$ and $\mathbb{1}_m^{B'_y} = \left(\hat{B}'_{y,m}\right)^2$. We also define the subspace $\mathcal{B}'_m = \text{range}(\mathbb{1}_m^{B'_0}) + \text{range}(\mathbb{1}_m^{B'_1})$. Using the argument employed earlier and following the same procedure, we can similarly construct operators $\tilde{Z}'_{A,m}$, $\tilde{X}'_{A,m}$, $\tilde{Z}'_{B,m}$ and $\tilde{X}'_{B,m}$ from operators $\hat{A}'_{x,m}$ and $\hat{B}'_{y,m}$ such that $(\tilde{Z}'_{A,m})^2 = \mathbb{1}_m^{A'_0}$, $(\tilde{X}'_{A,m})^2 = \mathbb{1}_m^{A'_1}$ and $(\tilde{Z}'_{B,m})^2 = (\tilde{X}'_{B,m})^2 = \mathbb{1}_{\mathcal{B}'_m}$, where the latter is the projection onto the subspace $\mathcal{B}'_m$ and

$$\tilde{Z}'_{A,m}|\psi\rangle = \tilde{Z}'_{B,m}|\psi\rangle \tag{18}$$

$$\tilde{X}'_{A,m}(\mathbb{1}_m^{A'_0} - \tilde{Z}'_{A,m})|\psi\rangle = \tan(\theta'_m)\tilde{X}'_{B,m}(\mathbb{1}_m^{A'_0} + \tilde{Z}'_{A,m})|\psi\rangle \tag{19}$$

We remark that the correlations we described in Tables I-V and VI-X are indeed quantum correlations, meaning that they can be achieved by some measurements on a quantum state. In fact, they are naturally achieved when the joint state of the two provers is $|\psi_{\text{target}}\rangle$, and the observables on Alice and Bob's side are direct sums of 2×2 observables that are ideal for the appropriate tilted CHSH correlations.

B. Testing each block

Inspired by [27], we are ready to define the "flip" operators $X'_{A,m}$, $X'_{B,m}$, $Y'_{A,m}$ and $Y'_{B,m}$. Recall that we ultimately wish to produce unitary operators satisfying condition (5), namely (restating it for clarity) $X_A^{(i)} P_B^{(i)}|\psi\rangle = \frac{c_i}{c_0}(X_B^{(i)})^\dagger P_A^{(0)}|\psi\rangle$. Intuitively, the flip operator $X'_{A,m}$ will be a unitary operator whose role is to act on $P_A^{(2m+1)}|\psi\rangle$ (which is equal to $P_B^{(2m+1)}|\psi\rangle$ when condition (4) is satisfied) and turn it into $X'_{B,m}P_A^{(2m)}|\psi\rangle$, up to an appropriate factor. On the other hand, the flip operator $Y'_{A,m}$ will turn $P_A^{(2m)}|\psi\rangle$ into $Y'_{B,m}P_A^{(2m-1)}|\psi\rangle$, up to a factor. The idea is, then, that the appropriate alternating product of the unitary flip operators $X'_{A,m}$, $Y'_{A,m}$ will turn $P_A^{(i)}|\psi\rangle$ into precisely $\frac{c_i}{c_0}(X_B^{(i)})^\dagger P_A^{(0)}|\psi\rangle$, and we will let these alternating products be the $X_A^{(i)}$ and $X_B^{(i)}$ required by condition (5).

We define the X' flip operators as

$$X'_{A,m} = \tilde{X}_{A,m} + \mathbb{1} - \mathbb{1}_m^{A_1} \tag{20}$$
$$X'_{B,m} = \tilde{X}_{B,m} + \mathbb{1} - \mathbb{1}_{\mathcal{B}_m} \tag{21}$$

Clearly $X'_{A,m}$ and $X'_{B,m}$ are hermitian. They are also unitary:

$$\begin{aligned}(X'_{A,m})^2 &= (\tilde{X}_{A,m})^2 + \tilde{X}_{A,m}(\mathbb{1} - \mathbb{1}_m^{A_1}) + (\mathbb{1} - \mathbb{1}_m^{A_1})\tilde{X}_{A,m} + \mathbb{1} - \mathbb{1}_m^{A_1} \\ &= (\tilde{X}_{A,m})^2 + \mathbb{1} - \mathbb{1}_m^{A_1} = \mathbb{1}_m^{A_1} + \mathbb{1} - \mathbb{1}_m^{A_1} = \mathbb{1} \qquad (22)\\ (X'_{B,m})^2 &= (\tilde{X}_{B,m})^2 + \tilde{X}_{B,m}(\mathbb{1} - \mathbb{1}_{\mathcal{B}_m}) + (\mathbb{1} - \mathbb{1}_{\mathcal{B}_m})\tilde{X}_{B,m} + \mathbb{1} - \mathbb{1}_{\mathcal{B}_m} \\ &= (\tilde{X}_{B,m})^2 + \mathbb{1} - \mathbb{1}_{\mathcal{B}_m} = \mathbb{1}_{\mathcal{B}_m} + \mathbb{1} - \mathbb{1}_{\mathcal{B}_m} = \mathbb{1}\,. \qquad (23)\end{aligned}$$

Moreover, we still have

$$X'_{A,m}(\mathbb{1}_m^{A_0} - \tilde{Z}_{A,m})|\psi\rangle = \tan(\theta_m) X'_{B,m}(\mathbb{1}_m^{A_0} + \tilde{Z}_{A,m})|\psi\rangle\,. \tag{24}$$

Indeed, this follows from combining (13) with

$$\begin{aligned}(\mathbb{1} - \mathbb{1}_m^{A_1})(\mathbb{1}_m^{A_0} - \tilde{Z}_{A,m})|\psi\rangle &= (\mathbb{1} - \mathbb{1}_m^{A_1})(\mathbb{1}_m^{B_0} - \tilde{Z}_{B,m})|\psi\rangle \\ &= (\mathbb{1}_m^{B_0} - \tilde{Z}_{B,m})(\mathbb{1} - \mathbb{1}_m^{A_0})|\psi\rangle \\ &= (\mathbb{1} - \mathbb{1}_m^{A_0})(\mathbb{1}_m^{A_0} - \tilde{Z}_{A,m})|\psi\rangle = 0 \end{aligned} \tag{25}$$

and with

$$\begin{aligned}\big(\mathbb{1} - \mathbb{1}_{\mathcal{B}_m}\big)(\mathbb{1}_m^{A_0} + \tilde{Z}_{A,m})|\psi\rangle &= (\mathbb{1}_m^{A_0} + \tilde{Z}_{A,m})\big(\mathbb{1} - \mathbb{1}_{\mathcal{B}_m}\big)|\psi\rangle \\ &= (\mathbb{1}_m^{A_0} + \tilde{Z}_{A,m})(\mathbb{1} - \mathbb{1}_m^{B_0})|\psi\rangle \\ &= (\mathbb{1}_m^{A_0} + \tilde{Z}_{A,m})(\mathbb{1} - \mathbb{1}_m^{A_0})|\psi\rangle = 0 \end{aligned} \tag{26}$$

where the second last line uses (17). In particular, it follows from (24) that

$$X'_{A,m}\Pi_{2m+1}^{A_0}|\psi\rangle = \tan(\theta_m) X'_{B,m}\Pi_{2m}^{A_0}|\psi\rangle = \frac{c_{2m+1}}{c_{2m}} X'_{B,m}\Pi_{2m}^{A_0}|\psi\rangle \tag{27}$$

This concludes the description of the properties of the X' flip operators. Similarly, we define

$$Y'_{A,m} = \tilde{X}'_{A,m} + \mathbb{1} - \mathbb{1}_m^{A'_1} \tag{28}$$
$$Y'_{B,m} = \tilde{X}'_{B,m} + \mathbb{1} - \mathbb{1}_{\mathcal{B}'_m} \tag{29}$$

which are unitary, hermitian and satisfying

$$Y'_{A,m}\Pi_{2m+2}^{A_0}|\psi\rangle = \tan(\theta'_m) Y'_{B,m}\Pi_{2m+1}^{A_0}|\psi\rangle = \frac{c_{2m+2}}{c_{2m+1}} Y'_{B,m}\Pi_{2m+1}^{A_0}|\psi\rangle \tag{30}$$

C. Connecting the blocks

First, we need to define our $P_{A/B}^{(k)}$. Let $P_A^{(2m)} := (\mathbb{1}_m^{A_0} + \tilde{Z}_{A,m})/2 = \Pi_{2m}^{A_0}$, $P_A^{(2m+1)} := (\mathbb{1}_m^{A_0} - \tilde{Z}_{A,m})/2 = \Pi_{2m+1}^{A_0}$, $P_B^{(2m)} := (\mathbb{1}_{\mathcal{B}_m} + \tilde{Z}_{B,m})/2$ and $P_B^{(2m+1)} := (\mathbb{1}_{\mathcal{B}_m} - \tilde{Z}_{B,m})/2$. It holds, for $k = 2m, 2m+1$, that

$$\begin{aligned}P_A^{(k)}|\psi\rangle = (\mathbb{1}_m^{A_0} + (-1)^k \tilde{Z}_{A,m})/2|\psi\rangle &= (\mathbb{1}_m^{B_0} + (-1)^k \tilde{Z}_{A,m})/2|\psi\rangle \\ &= (\mathbb{1}_{\mathcal{B}_m} + (-1)^k \tilde{Z}_{B,m})/2|\psi\rangle = P_B^k|\psi\rangle \end{aligned} \tag{31}$$

where the last step uses (12). Hence, $P_A^{(k)}|\psi\rangle = P_B^{(k)}|\psi\rangle$ for $k = 0, .., d-1$.
Then, let $Z_{A/B} := \sum_{i=0}^{d-1} w^i P_{A/B}^{(i)}$.

Next, we will define $X_{A/B}^{(k)}$ as follows:

$$X_A^{(k)} = \begin{cases} \mathbb{1}, & \text{if } k = 0 \\ X'_{A,0}Y'_{A,0}X'_{A,1}Y'_{A,1}\dots X'_{A,m-1}Y'_{A,m-1}X'_{A,m} & \text{if } k = 2m+1 \\ X'_{A,0}Y'_{A,0}X'_{A,1}Y'_{A,1}\dots X'_{A,m-1}Y'_{A,m-1}, & \text{if } k = 2m \end{cases} \tag{32}$$

and

$$X_B^{(k)} = \begin{cases} \mathbb{1}, & \text{if } k = 0 \\ X'_{B,0}Y'_{B,0}X'_{B,1}Y'_{B,1}\dots X'_{B,m-1}Y'_{B,m-1}X'_{B,m} & \text{if } k = 2m+1 \\ X'_{B,0}Y'_{B,0}X'_{B,1}Y'_{B,1}\dots X'_{B,m-1}Y'_{B,m-1}, & \text{if } k = 2m \end{cases} \tag{33}$$

Again, $X_A^{(k)}$ and $X_B^{(k)}$ are unitary since they are product of unitaries. Finally we need to check that the last required condition is met, namely

$$X_A^{(k)}P_B^{(k)}|\psi\rangle = \frac{c_k}{c_0}(X_B^{(k)})^\dagger P_A^{(0)}|\psi\rangle \tag{34}$$

The case $k = 0$,

$$\begin{aligned} X_A^{(0)}P_B^{(0)}|\psi\rangle &= \mathbb{1}P_A^{(0)}|\psi\rangle \\ &= \frac{c_0}{c_0}X_B^{(0)}P_A^{(0)}|\psi\rangle. \end{aligned} \tag{35}$$

For $k = 2m+1$,

$$\begin{aligned} X_A^{(k)}P_B^{(k)}|\psi\rangle &= X_A^{(k)}P_A^{(k)}|\psi\rangle \\ &= X'_{A,0}Y'_{A,0}X'_{A,1}Y'_{A,1}\dots X'_{A,m-1}Y'_{A,m-1}X'_{A,m}\Pi_{2m+1}^{A_0}|\psi\rangle \\ &\overset{(27)}{=} \frac{c_{2m+1}}{c_{2m}}X'_{A,0}Y'_{A,0}X'_{A,1}Y'_{A,1}\dots X'_{A,m-1}Y'_{A,m-1}X'_{B,m}\Pi_{2m}^{A_0}|\psi\rangle \\ &= \frac{c_{2m+1}}{c_{2m}}X'_{B,m}X'_{A,0}Y'_{A,0}X'_{A,1}Y'_{A,1}\dots X'_{A,m-1}Y'_{A,m-1}\Pi_{2m}^{A_0}|\psi\rangle \\ &\overset{(30)}{=} \frac{c_{2m+1}}{c_{2m}}\cdot\frac{c_{2m}}{c_{2m-1}}X'_{B,m}X'_{A,0}Y'_{A,0}X'_{A,1}Y'_{A,1}\dots X'_{A,m-1}Y'_{B,m-1}\Pi_{2m-1}^{A_0}|\psi\rangle \\ &= \frac{c_{2m+1}}{c_{2m}}\cdot\frac{c_{2m}}{c_{2m-1}}X'_{B,m}Y'_{B,m-1}X'_{A,0}Y'_{A,0}X'_{A,1}Y'_{A,1}\dots X'_{A,m-1}\Pi_{2m-1}^{A_0}|\psi\rangle \\ &= \dots \\ &= \frac{c_{2m+1}}{\cancel{c_{2m}}}\cdot\frac{\cancel{c_{2m}}}{\cancel{c_{2m-1}}}\dots\frac{\cancel{c_2}}{\cancel{c_1}}\cdot\frac{\cancel{c_1}}{c_0}X'_{B,m}Y'_{B,m-1}X'_{B,m-1}\dots Y'_{B,1}X'_{B,1}Y'_{B,0}X'_{B,0}\Pi_0^{A_0}|\psi\rangle \\ &= \frac{c_{2m+1}}{c_0}(X_B^{(k)})^\dagger P_A(0)|\psi\rangle \end{aligned} \tag{36}$$

which is indeed (34) as $2m+1 = k$. The case $k = 2m$ is treated similarly. This concludes the proof.

IV. DISCUSSION

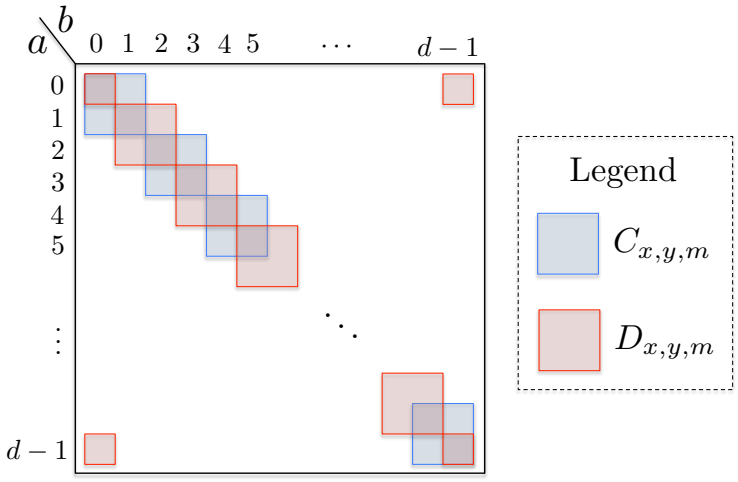

FIG. 4: Block diagonal correlations required for self-testing

In our proof, we described explicit self-testing correlations for the 2×2 blocks, in Tables III-V and VIII-X. However, we remark that this is not the only choice of correlations that can be made to self-test all bipartite entangled states. In fact, as a natural consequence of our work, it is the case that any block-diagonal correlations (as in Fig. 4) suffice as long the 2×2 "un-normalized" correlations $C_{x,y,m}$ and $D_{x,y,m}$ imply the existence of reflections Z_A, X_A on Alice's side and Z_B, X_B on Bob's side such that

$$Z_A|\psi\rangle = Z_B|\psi\rangle \tag{37}$$

$$X_A(\mathbb{1} - Z_A)|\psi\rangle = \tan(\theta) X_B(\mathbb{1} + Z_A)|\psi\rangle \tag{38}$$

for appropriate angles θ. For instance, in order to self-test bipartite maximally entangled states, we can invoke any correlation in the class given by Wang et al. [24] where $A_0|\psi\rangle = B_0|\psi\rangle$ (in the notation of Ref [24], $\alpha_{00} = 0$). These correlations fulfil equations (37) and (38) for $\tan\theta = 1$: thus, they can be used to self-test the maximally entangled pair of qudits, for any d, as is suggested by Yang and Navascués [27]. For these correlations, notice, moreover, that for $x = 0, y = 0$, the correlation table is diagonal and hence, we can drop Bob's fourth measurement setting because a diagonal correlation can fulfil its role as both $C_{x,y,m}$ and $D_{x,y,m}$. Thus, one can self-test maximally entangled states of arbitrary dimension within a $[\{3, d\}, \{3, d\}]$ Bell scenario.

We remark, that our analysis in the present work is limited to exact correlations: a natural follow-up to our work is to derive robustness bounds on our self-tests. While we believe that some robutsness bounds can be derived, existing analytical tools produce notoriously unsatisfying bounds, and the numerical tools that give much better bounds can only be applied to few examples. In this situation, we'd rather wait for the progress in analytical tools of the kind found in [10].

V. CONCLUSION AND OUTLOOK

In this work, we addressed the outstanding open question of whether all bipartite entangled quantum states can be self-tested. We presented a framework inspired by the work of Yang and Navascués [27], and provided explicit correlations that self-test all bipartite entangled pure states, thus answering the question affirmatively. These are indeed all the bipartite states that one can hope to self-test, since any correlations achieved by mixed states can also be achieved by pure states of the same dimension [22]. Our work provides new flexibility in choosing a bipartite quantum state for proofs of certification of randomness and of quantum computing; it also opens to the possibility of generating up to $\log(d)$ bits of private randomness with a seed consisting of two random trits per run, in a single Bell experiment setup. We leave this exploration for future work.

Acknowledgements

We thank Matthew McKague and Thomas Vidick for comments on earlier drafts, and acknowledge discussions with them as well as with Miguel Navascués and Xingyao Wu.

This research is supported by the Singapore Ministry of Education Academic Research Fund Tier 3 (Grant No. MOE2012-T3-1-009); by the National Research Fund and the Ministry of Education, Singapore, under the Research Centres of Excellence programme. A.C. is supported by AFOSR YIP award number FA9550-16-1-0495.

[1] Acín, A., Brunner, N., Gisin, N., Massar, S., Pironio, S., and Scarani, V., Phys. Rev. Lett. **98**, 230501 (2007).
[2] Acín, A., Durt, T., Gisin, N., and Latorre, J. I., Phys. Rev. A **65**, 052325 (2002).
[3] Acín, A., Massar, S., and Pironio, S., Phys. Rev. Lett. **108**, 100402 (2012).
[4] Bamps, C. and Pironio, S., Phys. Rev. A **91**, 052111 (2015).
[5] Bell, J. S., Physics (Long Island City, N.Y.) **1**, 195 (1964).
[6] Chao, R., Reichardt, B. W., Sutherland, C., and Vidick, T., arXiv preprint arXiv:1610.00771 (2016).
[7] Coladangelo, A. W., arXiv preprint arXiv:1609.03687 (2016).
[8] Coudron, M. and Natarajan, A., arXiv preprint arXiv:1609.06306 (2016).
[9] Coudron, M. and Yuen, H., arXiv preprint arXiv:1310.6755 (2013).
[10] Kaniewski, J., Phys. Rev. Lett. **117**, 070402 (2016).
[11] Mayers, D. and Yao, A., Quantum Inf. Comput. **4**, 273 (2004).
[12] McKague, M., in *Conference on Quantum Computation, Communication, and Cryptography* (Springer, 2011) pp. 104–120.
[13] McKague, M., New Journal of Physics **18**, 045013 (2016).
[14] McKague, M., Yang, T. H., and Scarani, V., J. Phys. A: Math. Theor. **45**, 455304 (2012).
[15] Miller, C. A. and Shi, Y., Journal of the ACM **63**, 33 (2016).
[16] Natarajan, A. and Vidick, T., arXiv preprint arXiv:1610.03574 (2016).
[17] Pál, K. F., Vértesi, T., and Navascués, M., Phys. Rev. A **90**, 042340 (2014).
[18] Pironio, S., Acín, A., Massar, S., de la Giroday, A. B., Matsukevich, D. N., Maunz, P., Olmschenk, S., Hayes, D., Luo, L., Manning, T. A., and Monroe, C., Nature **464**, 1021 (2010).
[19] Popescu, S. and Rohrlich, D., Phys. Lett. A **169**, 411 (1992).
[20] Reichardt, B. W., Unger, F., and Vazirani, U., Nature **496**, 456 (2013).
[21] Salavrakos, A., Augusiak, R., Tura, J., Wittek, P., Acín, A., and Pironio, S., arXiv preprint arXiv:1607.04578 (2016).
[22] Sikora, J., Varvitsiotis, A., and Wei, Z., Phys. Rev. Lett. **117**, 060401 (2016).
[23] Summers, S. J. and Werner, R., J. Math. Phys. **28**, 2440 (1987).
[24] Wang, Y., Wu, X., and Scarani, V., New Journal of Physics **18**, 025021 (2016).
[25] Wu, X., Bancal, J.-D., McKague, M., and Scarani, V., Phys. Rev. A **93**, 062121 (2016).
[26] Wu, X., Cai, Y., Yang, T. H., Le, H. N., Bancal, J.-D., and Scarani, V., Phys. Rev. A **90**, 042339 (2014).
[27] Yang, T. H. and Navascués, M., Phys. Rev. A **87**, 050102 (2013).
[28] Yang, T. H., Vértesi, T., Bancal, J.-D., Scarani, V., and Navascués, M., Phys. Rev. Lett. **113**, 040401 (2014).

Appendix A: Proof of the Yang-Navascués self-testing criterion

In this section, we will show that Yang-Navascués criteria is indeed sufficient to prove self-testing for any bipartite entangled state. Recall that it suffice to prove the existence of a local isometry $\Phi(\cdot)$ such that $P(a,b|x,y) = \langle\psi|\Pi_a^{A_x} \otimes \Pi_b^{B_y}|\psi\rangle \implies \Phi(|\psi\rangle) = |\text{extra}\rangle \otimes |\psi_{\text{target}}\rangle$. In this case, the ideal target state is given by $|\psi_{\text{target}}\rangle = \sum_{i=0}^{d-1} c_i|ii\rangle$ where $0 \le c_i \le 1$ for all i and $\sum_{i=0}^{d-1} c_i^2 = 1$.

Proof. We will compute the local isometry given by

$$(R_{A,A'} \otimes R_{B,B'})(\bar{F}_{A'} \otimes \bar{F}_{B'})(S_{AA'} \otimes S_{BB'})(F_{A'} \otimes F_{B'})|\psi\rangle_{AB}|0\rangle_{A'}|0\rangle_{B'} \tag{A1}$$

where F is the quantum Fourier transform, $\bar{F}$ is the inverse quantum Fourier transform, $R_{AA'/BB'}$ is defined as $R_{AA'/BB'}|\psi\rangle_{AB}|k\rangle_{A/B} = X_{A/B}^{(k)}|\psi\rangle_{AB}|k\rangle_{A/B}$ and $S_{AA'/BB'}$ is defined as $S_{AA'/BB'}|\psi\rangle_{AB}|k\rangle_{A/B} = Z_{A/B}^{k}|\psi\rangle_{AB}|k\rangle_{A/B}$. Also, the operators $X_{A/B}^{(k)}$ and $Z_{A/B}$ are unitary and satisfy the following criteria:

$$Z_{A/B} = \sum_{i=0}^{d-1} \omega^i P_{A/B}^{(i)}, \tag{A2}$$

$$P_A^{(i)}|\psi\rangle = P_B^{(i)}|\psi\rangle \ \ \forall i, \tag{A3}$$

$$X_A^{(i)} P_B^{(i)}|\psi\rangle = \frac{c_i}{c_0}(X_B^{(i)})^\dagger P_A^{(0)}|\psi\rangle \tag{A4}$$

where $\{P_{A/B}^{(i)}\}$ forms a complete orthogonal basis. The computation gives

$$|\psi\rangle_{AB}|0\rangle_{A'}|0\rangle_{B'} \xrightarrow{F_{A'}\otimes F_{B'}} \frac{1}{d}\sum_{k,k'}|\psi\rangle_{AB}|k\rangle_{A'}|k'\rangle_{B'} \tag{A5}$$

$$\xrightarrow{S_{A,A'}\otimes S_{B,B'}} \frac{1}{d}\sum_{k,k'}\left(\sum_j \omega^j P_A^{(j)}\right)^k \left(\sum_{j'} \omega^{j'} P_B^{(j')}\right)^{k'} |\psi\rangle_{AB}|k\rangle_{A'}|k'\rangle_{B'} \tag{A6}$$

$$= \frac{1}{d}\sum_{k,k',j,j'} \omega^{jk}\omega^{j'k'} P_A^{(j)} P_B^{(j')}|\psi\rangle_{AB}|k\rangle_{A'}|k'\rangle_{B'} \tag{A7}$$

$$= \frac{1}{d}\sum_{k,k',j,j'} \omega^{jk}\omega^{j'k'} P_A^{(j)} P_A^{(j')}|\psi\rangle_{AB}|k\rangle_{A'}|k'\rangle_{B'} \tag{A8}$$

$$= \frac{1}{d}\sum_{k,k',j} \omega^{j(k+k')} P_A^{(j)}|\psi\rangle_{AB}|k\rangle_{A'}|k'\rangle_{B'} \tag{A9}$$

$$\xrightarrow{\bar{F}_{A'}\otimes\bar{F}_{B'}} \frac{1}{d^2}\sum_{k,k',j,l,l'} \omega^{j(k+k')}\omega^{-lk}\omega^{-l'k'} P_A^{(j)}|\psi\rangle_{AB}|l\rangle_{A'}|l'\rangle_{B'} \tag{A10}$$

$$= \frac{1}{d^2}\sum_{k,k',j,l,l'} \omega^{k(j-l)}\omega^{k'(j-l')} P_A^{(j)}|\psi\rangle_{AB}|l\rangle_{A'}|l'\rangle_{B'} \tag{A11}$$

$$= \sum_j P_B^{(j)}|\psi\rangle_{AB}|j\rangle_{A'}|j\rangle_{B'} \tag{A12}$$

$$\xrightarrow{R_{A,A'}\otimes R_{B,B'}} \sum_j X_B^{(j)} X_A^{(j)} P_B^{(j)}|\psi\rangle_{AB}|j\rangle_{A'}|j\rangle_{B'} \tag{A13}$$

$$= \sum_j \frac{c_i}{c_0} X_B^{(j)}(X_B^{(j)})^\dagger P_A^{(0)}|\psi\rangle_{AB}|j\rangle_{A'}|j\rangle_{B'} \tag{A14}$$

$$= \sum_j P_A^{(0)}\frac{c_j}{c_0} X_B^{(j)}(X_B^{(j)})^\dagger|\psi\rangle_{AB}|j\rangle_{A'}|j\rangle_{B'} \tag{A15}$$

$$= \sum_j P_A^{(0)}\frac{c_j}{c_0}|\psi\rangle_{AB}|j\rangle_{A'}|j\rangle_{B'} \tag{A16}$$

$$= \frac{1}{c_0} P_A^{(0)} |\psi\rangle_{AB} \otimes \sum_j c_j |j\rangle_{A'} |j\rangle_{B'} \tag{A17}$$

$$= |\text{extra}\rangle \otimes |\psi_{\text{target}}\rangle \tag{A18}$$

□