

Self-test prime dimensional EPR pairs with constant alphabet

Honghao Fu¹ and Carl Miller^{1,2}

¹*Department of Computer Science, Institute for Advanced Computer Studies, and Joint Center for Quantum Information and Computer Science, University of Maryland, College Park, MD 20742, USA*

²*National Institute of Standards and Technology, 100 Bureau Dr., Gaithersburg, MD 20899, USA*

December 15, 2018

1 Preliminaries and notations

We use $[n]$ to denote the set $\{0, 1 \dots n-1\}$. We denote the group commutator of A and B , i.e. $ABA^{-1}B^{-1}$, by $[A, B]$.

The EPR pair. Our goal is to self-test maximally entangled state of local dimension d , denoted by

$$|EPR^{(d)}\rangle = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |ii\rangle. \quad (1)$$

The superscript (d) is to stress the local dimension and we follow this convention through this paper.

The Pauli operators. We self-test $|EPR^{(d)}\rangle$ by verify that Alice and Bob has operators behave like the d -dimensional Pauli operators which are defined by

$$\sigma_x^{(d)} = \sum_{i=0}^{d-1} |i+1\rangle\langle i| \quad \sigma_z^{(d)} = \sum_{i=0}^{d-1} \omega_d^i |i\rangle\langle i| \quad (2)$$

where $\omega_d = e^{i\pi/d}$ is the primitive d th root of unity and the addition is taken modulo d .

The weighted CHSH inequality [AMP12]. The first building-block of our result is a robust self-testing result based on the weighted CHSH inequality. The weighted CHSH operator is defined as

$$\mathcal{I}_\alpha = \alpha(A_0B_0 + A_0B_1) + A_1B_0 - A_1B_1, \quad (3)$$

where A_x, B_y for $x, y = 0, 1$ are Binary observables on Hilbert space \mathcal{H}_A and \mathcal{H}_B respectively. If Alice and Bob share product state $|\phi\rangle = |\phi_A\rangle \otimes |\phi_B\rangle$, we have

$$\langle \phi | \mathcal{I}_\alpha | \phi \rangle \leq 2\alpha. \quad (4)$$

However, If they share entangled state $|\psi\rangle$, the maximal violation is

$$\langle \psi | \mathcal{I}_\alpha | \psi \rangle \leq 2\sqrt{1 + \alpha^2}. \quad (5)$$

Definition 1 (Ideal strategy for \mathcal{I}_α). Define $\mu = \arctan(1/\alpha)$. The ideal strategy for weighted CHSH with parameter α (i.e. achieving maximal violation of eq. (5)) consists of the joint state $|EPR^{(2)}\rangle$ and observables $A_0 = \sigma_z^{(2)}$, $A_1 = \sigma_x^{(2)}$, $B_0 = \cos(\mu)\sigma_z^{(2)} + \sin(\mu)\sigma_x^{(2)}$ and $B_1 = \cos(\mu)\sigma_z^{(2)} - \sin(\mu)\sigma_x^{(2)}$.

We take an approach introduced in Ref. [BP15] and prove the following robust self-testing result.

Theorem 2. Suppose the quantum strategy $(|\psi\rangle, \{\tilde{A}_x\}_{x \in [2]}, \{\tilde{B}_y\}_{y \in [2]})$ satisfies that

$$\langle \psi | \mathcal{I}_\alpha | \psi \rangle \geq 2\sqrt{1 + \alpha^2} - \epsilon \quad (6)$$

for some α , then there exists a local isometry $\Phi = \Phi_A \otimes \Phi_B$ and an auxiliary state $|aux\rangle$ such that

$$\|\Phi(\tilde{A}_x \otimes \tilde{B}_y |\psi\rangle) - |aux\rangle \otimes (A_x \otimes B_y) |EPR^{(2)}\rangle\| = O(\sqrt{\epsilon}) \quad (7)$$

for $x, y \in \{-1, 0, 1\}$ where the subscript -1 refers to the identity operator and where A_x, B_y are from the ideal strategy.

We defer the proof of Theorem 2 till Appendix A. After proving the robust self-testing result, we take one step further and observed some interesting behaviour of the observable $\tilde{B}_0 \tilde{B}_1$.

Proposition 3. Suppose a quantum strategy $(|\psi\rangle, \{\tilde{A}_x\}_{x \in [2]}, \{\tilde{B}_y\}_{y \in [2]})$ achieves the maximal value of $\langle \psi | \mathcal{I}_{-\cot(\pi/2d)} | \psi \rangle$, then there exists a 2-dimensional Hilbert space which is spanned by eigenvectors of $\tilde{B}_0 \tilde{B}_1$ of eigenvalue ω_d and ω_d^{-1} .

Proof of Proposition 3. By Theorem 2, the condition that the strategy $(|\psi\rangle, \{\tilde{A}_x\}_{x \in [2]}, \{\tilde{B}_y\}_{y \in [2]})$ achieves the maximal value of $\langle \psi | \mathcal{I}_\alpha | \psi \rangle$ implies that there exists state $|u_0\rangle, |u_1\rangle$ such that

$$\begin{aligned} (\tilde{B}_0 + \tilde{B}_1)|u_0\rangle &= 2\cos(\pi/2d)|u_0\rangle \\ (\tilde{B}_0 + \tilde{B}_1)|u_1\rangle &= -2\cos(\pi/2d)|u_1\rangle \\ (\tilde{B}_0 - \tilde{B}_1)|u_0\rangle &= -2\sin(\pi/2d)|u_1\rangle \\ (\tilde{B}_0 - \tilde{B}_1)|u_1\rangle &= -2\sin(\pi/2d)|u_0\rangle. \end{aligned}$$

It is straightforward to calculate that

$$\tilde{B}_0 \tilde{B}_1 |u_0\rangle = \cos(\pi/d)|u_0\rangle - \sin(\pi/d)|u_1\rangle \quad (8)$$

$$\tilde{B}_0 \tilde{B}_1 |u_1\rangle = \sin(\pi/d)|u_0\rangle + \cos(\pi/d)|u_1\rangle. \quad (9)$$

We can conclude that

$$\tilde{B}_0 \tilde{B}_1 (|u_0\rangle + i|u_1\rangle) = e^{i\frac{\pi}{d}} (|u_0\rangle + i|u_1\rangle) \quad (10)$$

$$\tilde{B}_0 \tilde{B}_1 (|u_0\rangle - i|u_1\rangle) = e^{-i\frac{\pi}{d}} (|u_0\rangle - i|u_1\rangle). \quad (11)$$

□

Nonlocal game. The two players of a nonlocal game are Alice and Bob. Each of them is requested to give answer for a chosen question. We denote Alice's question set by X and answer set by A . Similarly, Bob's question set is denoted by Y and his answer set is denoted by B . The nonlocal game also comes with two functions: $\pi : X \times Y \rightarrow [0, 1]$, which is the probability distribution over the questions, and $V : A \times B \times X \times Y \rightarrow \mathbb{R}$, which is the scoring function. Such games are nonlocal

because Alice and Bob cannot communicate after getting their questions but they may share some strategy before the start of the game. Note that in the literature, the typical scoring function of a nonlocal game maps the input-output pair to $\{0,1\}$ which corresponds to losing and winning. Allowing the score to be any real number is the key ingredient to our new nonlocal game.

The quantum strategy of a game G consists of projective measurements $\{\{A_x^a\}_a\}$ on Alice's side and $\{\{B_y^b\}_b\}$ on Bob's side, and a shared state $|\psi\rangle$. Then the behaviour of Alice and Bob is described by the conditional probability

$$P(ab|xy) = \langle \psi | A_x^a \otimes B_y^b | \psi \rangle \text{ for } (a, b, x, y) \in A \times B \times X \times Y, \quad (12)$$

where $(A_x^a)^2 = A_x^a = (A_x^a)^\dagger$ and $(B_y^b)^2 = B_y^b = (B_y^b)^\dagger$. The *value* of a strategy is given by

$$\omega(G, p) = \sum_{a,b,x,y} \pi(x, y) P(ab|xy) V(a, b, x, y). \quad (13)$$

The main contribution of our work is the construction of a nonlocal game $G^{(d)}$ that can be used to self-test $|EPR^{(d)}\rangle$ where d is an arbitrary odd prime number. In fact, our nonlocal game self-tests $\sigma_x^{(d)}$ and $\sigma_z^{(d)}$ too, just implicitly. The nonlocal game is a linear system game with modifications. We introduce the definition of self-testing first and then the definition of linear system game, which come from Ref. [CS17, Slo17].

Definition 4 (Self-testing). We say that a nonlocal game self-tests a quantum state $|\Psi\rangle$ if any quantum strategy S that achieves the optimal quantum value uses a shared state equivalent up to local isometry to $|\Psi\rangle$.

Definition 5 (Linear system game). Let $Ax = b$ be an $m \times n$ linear system over \mathbb{Z}_d . The associated linear system game has two players Alice and Bob, where Alice is given a equation number $1 \leq x \leq m$ and replies with $a \in \mathbb{Z}_d^{\times n}$, and Bob is given a variable y and replies with an assignment $y \in \mathbb{Z}_d$. The winning condition is

$$a(y) = b \quad (\text{Consistency})$$

$$\sum_{y=1}^n A_{xy} a(y) \equiv b(x) \pmod{d}. \quad (\text{Constraint satisfaction})$$

The scoring function of linear system games always maps an input-output pair to $\{0,1\}$, so later when we say a quantum strategy wins a linear system game perfectly, we mean that $V(a, b, x, y) = 0$ implies that $P(ab|xy) = 0$.

The main tool to understand linear system game is through its solution group over \mathbb{Z}_d .

Definition 6 (Solution group over \mathbb{Z}_d [CS17]). For the linear system game associated with $Ax = b$ over \mathbb{Z}_d , its solution group $\Gamma(A, b, \mathbb{Z}_d)$ has one generator for each variable and one relation for each equation and relations enforcing that the variables in the same equation commutes. The set of local commutativity relations is denoted by R_c and defined by

$$R_c := \{[x_i, x_j] | A_{li} \neq 0 \neq A_{lj} \text{ for some } 1 \leq l \leq m\}. \quad (14)$$

The set of constraint satisfaction relations is denoted by R_{eq} and defined by.

$$R_{eq} := \{\mathcal{J}^{-b(l)} \prod_{i=1}^n x_i^{A_{li}} | 1 \leq l \leq m\} \quad (15)$$

Then the solution group has presentation

$$\Gamma(A, b, \mathbb{Z}_d) := \langle \{x_i\}_{i=1}^n \cup \{\mathcal{J}\} : R_c \cup R_{eq} \cup \{(x_i)^d, \mathcal{J}^d | 1 \leq i \leq n\} \rangle. \quad (16)$$

Note that the relations $(x_i)^d$ and \mathcal{J}^d ensure that we have solutions over \mathbb{Z}_d . Then the operator solution of $\Gamma(A, b, \mathbb{Z}_d)$ is given below.

Definition 7 (Operator solution). *An operator solution for the linear system game associated with $Ax = b$ over \mathbb{Z}_d is a unitary representation τ of $\Gamma(A, b, \mathbb{Z}_d)$ such that $\tau(\mathcal{J}) = \omega_d \mathbb{1}$. A conjugate operator solution is a unitary representation mapping \mathcal{J} to $\overline{\omega_d} \mathbb{1}$.*

What has been established in Ref.[CLS17, CS17] is that we can construct a perfect strategy of a linear system game from its operator solution and vice versa.

2 Components of $G^{(d)}$

Suppose we would like to self-test $|EPR^{(d)}\rangle$ with $G^{(d)}$, where d is prime and has primitive root 2. Later we will see how to deal with general prime numbers and why there are infinitely many prime dimensional EPR pairs that can be self-tested by a variant of $G^{(d)}$.

2.1 The linear system game

The main component of $G^{(d)}$ is a linear system game LS , whose solution group is derived from the following group

$$\mathcal{P}_{LS} = \langle u, x : uxu^{-1} = x^2 \rangle. \quad (17)$$

See Appendix B for details.

2.2 The extended weighted CHSH game

The extended weighted CHSH game is added to make sure that some of Alice and Bob's observables have eigenvalues ω_d and ω_d^{d-1} . The notation for the extended weighted CHSH game that enforces the eigenvalues of the observable U is $CHSH_U^{(d)}$, where the superscript d means that the rules of this game depends on d . Intuitively, this is one step towards verifying Alice and Bob use $\sigma_x^{(d)}$ and $\sigma_z^{(d)}$ in their operator solution.

In this game, Alice and Bob each gets a question $x, y \in \{0, 1, *\}$ and they answer with $a, b \in \{0, 1, \diamond, \perp\}$. The scoring rules are

- **Case 1:** $x = y = *$, Alice and Bob should answer with $a, b \in \{\diamond, \perp\}$ and they score only if $a = b$;
- **Case 2a:** $x, y \in \{0, 1\}$ and they answer with $a, b \in \{0, 1\}$, then their answers are scored according to $I_{-\cot(\pi/2d)}$
- **Case 2b:** $x, y \in \{0, 1\}$ and Alice answer with \perp , then all possible outputs from Bob are discarded;
- **Case 3:** $x \in 0, 1, y = *$, when Bob answers \diamond , Alice should answer with $\{0, 1\}$ but not \perp , when Bob answers \perp Alice should answer \perp too;
- **Case 4:** other combination of inputs are not scored.

In the ideal strategy, Alice and Bob share the state $|\psi\rangle = 1/\sqrt{d} \sum_{i=0}^{d-1} |u_i\rangle|u_i\rangle$. We define two subspaces $V = \text{span}\{|u_1\rangle, |u_{d-1}\rangle\}$ and $V^\perp = \mathbb{C}^d \setminus \text{span}\{|u_1\rangle, |u_{d-1}\rangle\}$ and define Π_V and Π_V^\perp to be the corresponding projectors. Note that V is the subspace on which they should maximize $\langle I_{-\cot(\pi/2d)} \rangle$.

We summarize the projectors of the ideal strategy and the ideal correlation in the following two charts. Note that we don't explicitly calculate the conditional probabilities of the form $P(\perp 0|xy)$ because they are irrelevant

		$x = *$	
		$a = \diamond$	$a = \perp$
$y = *$	$b = \diamond$	2/d	0
	$b = \perp$	0	(d-2)/d

Table 1: Alice and Bob's behaviour when $x = y = *$.

		$x = 0$			$x = 1$		
		$a = 0$	$a = 1$	$a = \perp$	$a = 0$	$a = 1$	$a = \perp$
$y = 0$	$b = 0$	$\frac{\cos^2(\pi/4d)}{d}$	$\frac{\sin^2(\pi/4d)}{d}$	$P(\perp 0 00)$	$\frac{1+\sin(\pi/2d)}{2d}$	$\frac{1-\sin(\pi/2d)}{2d}$	$P(\perp 0 10)$
	$b = 1$	$\frac{\sin^2(\pi/4d)}{d}$	$\frac{\cos^2(\pi/4d)}{d}$	$\frac{d-2}{d} - P(\perp 0 00)$	$\frac{1-\sin(\pi/2d)}{2d}$	$\frac{1+\sin(\pi/2d)}{2d}$	$\frac{d-2}{d} - P(\perp 0 10)$
$y = 1$	$b = 0$	$\frac{\cos^2(\pi/4d)}{d}$	$\frac{\sin^2(\pi/4d)}{d}$	$P(\perp 0 01)$	$\frac{1-\sin(\pi/2d)}{2d}$	$\frac{1+\sin(\pi/2d)}{2d}$	$P(\perp 0 11)$
	$b = 1$	$\frac{\sin^2(\pi/4d)}{d}$	$\frac{\cos^2(\pi/4d)}{d}$	$\frac{d-2}{d} - P(\perp 0 01)$	$\frac{1+\sin(\pi/2d)}{2d}$	$\frac{1-\sin(\pi/2d)}{2d}$	$\frac{d-2}{d} - P(\perp 0 11)$

Table 2: Alice and Bob's behaviour when $x, y \in [2]$.

		$x = 0$			$x = 1$		
		$a = 0$	$a = 1$	$a = \perp$	$a = 0$	$a = 1$	$a = \perp$
$y = *$	$b = \diamond$	1/d	1/d	0	1/d	1/d	0
	$b = \perp$	0	0	$\frac{d-2}{d}$	0	0	$\frac{d-2}{d}$

Table 3: Alice and Bob's behaviour when $x \in [2]$ and $y = *$.

Alice's projectors are

$$A_*^\diamond = \Pi_V, A_*^\perp = \Pi_V^\perp$$

$$A_0^0 = |u_1\rangle\langle u_1|, A_0^1 = |u_{d-1}\rangle\langle u_{d-1}|, A_0^\perp = \Pi_V^\perp$$

$$A_1^0 = \frac{1}{2}(|u_1\rangle + |u_{d-1}\rangle)(\langle u_1| + \langle u_{d-1}|), A_1^1 = \frac{1}{2}(|u_1\rangle - |u_{d-1}\rangle)(\langle u_1| - \langle u_{d-1}|), A_1^\perp = \Pi_V^\perp$$

Bob's projectors are

$$\begin{aligned}
B_*^\diamond &= \Pi_V, B_*^\perp = \Pi_V^\perp \\
B_0^0|_V &= \left(\cos\left(\frac{\pi}{4d}\right)|u_1\rangle + \sin\left(\frac{\pi}{4d}\right)|u_{d-1}\rangle \right) \left(\cos\left(\frac{\pi}{4d}\right)\langle u_1| + \sin\left(\frac{\pi}{4d}\right)\langle u_{d-1}| \right) \\
B_0^1|_V &= \left(\sin\left(\frac{\pi}{4d}\right)|u_1\rangle - \cos\left(\frac{\pi}{4d}\right)|u_{d-1}\rangle \right) \left(\sin\left(\frac{\pi}{4d}\right)\langle u_1| - \cos\left(\frac{\pi}{4d}\right)\langle u_{d-1}| \right) \\
B_1^0|_V &= \left(\cos\left(\frac{\pi}{4d}\right)|u_1\rangle - \sin\left(\frac{\pi}{4d}\right)|u_{d-1}\rangle \right) \left(\cos\left(\frac{\pi}{4d}\right)\langle u_1| - \sin\left(\frac{\pi}{4d}\right)\langle u_{d-1}| \right) \\
B_1^1|_V &= \left(\sin\left(\frac{\pi}{4d}\right)|u_1\rangle + \cos\left(\frac{\pi}{4d}\right)|u_{d-1}\rangle \right) \left(\sin\left(\frac{\pi}{4d}\right)\langle u_1| + \cos\left(\frac{\pi}{4d}\right)\langle u_{d-1}| \right).
\end{aligned}$$

About Bob's projectors for input $y \in [2]$, we are only interested in their actions when restricted to the subspace V . Their actions on the subspace V^\perp is irrelevant in this game.

The importance of this game is summarized in the following lemma.

Lemma 8. *Suppose a quantum strategy $\left(\{ \{ \tilde{A}_x^a \}_a \}_x, \{ \{ \tilde{B}_y^b \}_b \}_y, |\tilde{\psi}\rangle \right)$ achieves the optimal correlation of $\text{CHSH}^{(d)}$, then there exists unitaries U_A and U_B such that*

$$\begin{aligned}
U_A \otimes U_B (\tilde{A}_*^\diamond \otimes \tilde{B}_*^\diamond |\tilde{\psi}\rangle) &= |\text{EPR}^{(2)}\rangle \\
U_A \otimes U_B \left[\left(\mathbb{1} \otimes \frac{\tilde{B}_0 + \tilde{B}_1}{2 \cos(\pi/2d)} \right) (\tilde{A}_*^\diamond \otimes \tilde{B}_*^\diamond |\tilde{\psi}\rangle) \right] &= \mathbb{1} \otimes \sigma_z^{(2)} |\text{EPR}^{(2)}\rangle \\
U_A \otimes U_B \left[\left(\mathbb{1} \otimes \frac{\tilde{B}_0 - \tilde{B}_1}{-2 \sin(\pi/2d)} \right) (\tilde{A}_*^\diamond \otimes \tilde{B}_*^\diamond |\tilde{\psi}\rangle) \right] &= \mathbb{1} \otimes \sigma_x^{(2)} |\text{EPR}^{(2)}\rangle
\end{aligned}$$

where $\tilde{B}_0 = \tilde{B}_0^0 - \tilde{B}_0^1$ and $\tilde{B}_1 = \tilde{B}_1^0 - \tilde{B}_1^1$.

Proof. Note that $\tilde{A}_x^a \tilde{B}_y^b$ means $\tilde{A}_x^a \otimes \tilde{B}_y^b$ in the following proof.

From the marginal distribution $P_B(\diamond|*) = P_A(0|0) + P_A(1|0) = 2/d$, we know $\|\tilde{B}_*^\diamond |\tilde{\psi}\rangle\| = \|(\tilde{A}_0^0 + \tilde{A}_0^1) |\tilde{\psi}\rangle\| = \sqrt{2/d}$. Since $P(0 \diamond |0*) + P(1 \diamond |0*) = 2/d$, we find that

$$\frac{\langle \tilde{\psi} | \tilde{B}_*^\diamond (\tilde{A}_0^0 + \tilde{A}_0^1) \tilde{B}_*^\diamond | \tilde{\psi} \rangle}{\|\tilde{B}_*^\diamond |\tilde{\psi}\rangle\|^2} = 1,$$

which means that

$$(\tilde{A}_0^0 + \tilde{A}_0^1) \tilde{B}_*^\diamond |\tilde{\psi}\rangle = \tilde{B}_*^\diamond |\tilde{\psi}\rangle. \tag{18}$$

Using the commutation relation between $(\tilde{A}_0^0 + \tilde{A}_0^1)$ and \tilde{B}_*^\diamond , we get

$$\frac{\langle \tilde{\psi} | (\tilde{A}_0^0 + \tilde{A}_0^1) \tilde{B}_*^\diamond (\tilde{A}_0^0 + \tilde{A}_0^1) | \tilde{\psi} \rangle}{\|(\tilde{A}_0^0 + \tilde{A}_0^1) |\tilde{\psi}\rangle\|^2} = 1,$$

Similar argument gives us that

$$\tilde{B}_*^\diamond (\tilde{A}_0^0 + \tilde{A}_0^1) |\tilde{\psi}\rangle = (\tilde{A}_0^0 + \tilde{A}_0^1) |\tilde{\psi}\rangle. \tag{19}$$

The two equations above can be chained by commutativity to reach the conclusion that

$$(\tilde{A}_0^0 + \tilde{A}_0^1) |\tilde{\psi}\rangle = \tilde{B}_*^\diamond |\tilde{\psi}\rangle. \tag{20}$$

Following the same line of argument, we can conclude that

$$\tilde{B}_*^\diamond|\tilde{\psi}\rangle = \tilde{A}_*^\diamond|\tilde{\psi}\rangle = (\tilde{A}_0^0 + \tilde{A}_0^1)|\tilde{\psi}\rangle = (\tilde{A}_1^0 + \tilde{A}_1^1)|\tilde{\psi}\rangle. \quad (21)$$

Looking at the marginal distribution when Alice and Bob output \perp , we conclude that

$$\tilde{B}_*^\perp|\tilde{\psi}\rangle = \tilde{A}_*^\perp|\tilde{\psi}\rangle = \tilde{A}_0^\perp|\tilde{\psi}\rangle = \tilde{A}_1^\perp|\tilde{\psi}\rangle, \quad (22)$$

with similar arguments.

Next we examine the CHSH-type correlation when $x, y \in [2]$,

$$\begin{aligned} \langle \tilde{\psi} | \tilde{A}_0^0 \tilde{B}_0^0 | \tilde{\psi} \rangle &= \langle \tilde{\psi} | (\tilde{A}_*^\diamond + \tilde{A}_*^\perp) \tilde{A}_0^0 \tilde{B}_0^0 (\tilde{A}_*^\diamond + \tilde{A}_*^\perp) | \tilde{\psi} \rangle \\ &= \langle \tilde{\psi} | \tilde{A}_*^\diamond \tilde{A}_0^0 \tilde{B}_0^0 \tilde{A}_*^\diamond | \tilde{\psi} \rangle + \langle \tilde{\psi} | \tilde{A}_*^\diamond \tilde{A}_0^0 \tilde{B}_0^0 \tilde{A}_*^\perp | \tilde{\psi} \rangle \\ &\quad + \langle \tilde{\psi} | \tilde{A}_*^\perp \tilde{A}_0^0 \tilde{B}_0^0 \tilde{A}_*^\diamond | \tilde{\psi} \rangle + \langle \tilde{\psi} | \tilde{A}_*^\perp \tilde{A}_0^0 \tilde{B}_0^0 \tilde{A}_*^\perp | \tilde{\psi} \rangle \\ &= \langle \tilde{\psi} | \tilde{B}_*^\diamond \tilde{A}_0^0 \tilde{B}_0^0 \tilde{B}_*^\diamond | \tilde{\psi} \rangle + \langle \tilde{\psi} | \tilde{A}_*^\diamond \tilde{A}_0^0 \tilde{B}_0^0 \tilde{A}_0^\perp | \tilde{\psi} \rangle \\ &\quad + \langle \tilde{\psi} | \tilde{A}_0^\perp \tilde{A}_0^0 \tilde{B}_0^0 \tilde{A}_*^\diamond | \tilde{\psi} \rangle + \langle \tilde{\psi} | \tilde{A}_0^\perp \tilde{A}_0^0 \tilde{B}_0^0 \tilde{A}_0^\perp | \tilde{\psi} \rangle \\ &= \langle \tilde{\psi} | \tilde{B}_*^\diamond \tilde{A}_0^0 \tilde{B}_0^0 \tilde{B}_*^\diamond | \tilde{\psi} \rangle, \end{aligned}$$

where we use the facts that $\tilde{B}_*^\diamond|\tilde{\psi}\rangle = \tilde{A}_*^\diamond|\tilde{\psi}\rangle$, $\tilde{A}_*^\perp|\tilde{\psi}\rangle = \tilde{A}_0^\perp|\tilde{\psi}\rangle$ and that $\text{span}(\tilde{A}_0^0) \cap \text{span}(\tilde{A}_0^\perp) = \emptyset$. This means that if Alice and Bob share the state $\tilde{B}_*^\diamond|\tilde{\psi}\rangle / \|\tilde{B}_*^\diamond|\tilde{\psi}\rangle\|$ and apply $\tilde{A}_0^0 \tilde{B}_0^0$, the conditional probability is

$$\frac{\langle \tilde{\psi} | \tilde{B}_*^\diamond \tilde{A}_0^0 \tilde{B}_0^0 \tilde{B}_*^\diamond | \tilde{\psi} \rangle}{\langle \tilde{\psi} | \tilde{B}_*^\diamond \tilde{B}_*^\diamond | \tilde{\psi} \rangle} = \frac{\cos^2(\pi/4d)}{2}. \quad (23)$$

We can re-normalize the other correlations of $a, b \in [2]$ when $x, y \in [2]$ similarly and get a new set of correlations which achieves the maximal value of $\langle \mathbb{1}_{-\cot(\pi/2d)} \rangle$. The conclusion of Lemma 8 follows the application of Theorem 2 on the state $\tilde{A}_*^\diamond \tilde{B}_*^\diamond |\tilde{\psi}\rangle / \|\tilde{A}_*^\diamond \tilde{B}_*^\diamond |\tilde{\psi}\rangle\|$ as $\tilde{A}_*^\diamond \tilde{B}_*^\diamond |\tilde{\psi}\rangle = \tilde{B}_*^\diamond |\tilde{\psi}\rangle$. \square

Note that the combination of Lemma 8 with Proposition 3 gives us that $\tilde{B}_0 \tilde{B}_1$ has eigenvalues ω_d and ω_d^{-1} .

2.3 The single value test

By the following test, we want to make sure that some unitary U has eigenvalue 1. In this test $X = \{\Delta\}$, $Y = \{0, 1, \Delta\}$, $A = \{\diamond, \perp\}$ and $B = \{0, 1, \diamond, \perp\}$. The scoring rules are

- **Case 1** $x = y = \Delta$: Alice and Bob should answer with $a, b \in \{\diamond, \perp\}$ and they score only if $a = b$;
- **Case 2** $x = \Delta$ and $y = 0$: when Alice answer \diamond , Bob should answer 0, when Alice answer \perp all answers of Bob are accepted;
- **Case 3** $x = \Delta$ and $y = 1$: when Alice answer \diamond , Bob should answer 0, when Alice answer \perp all answers of Bob are accepted.

Define the subspace $V = \text{span}\{|u_0\rangle\}$. The ideal strategy has projective measurement

$$\begin{aligned} A_\Delta^\diamond &= B_\Delta^\diamond = |u_0\rangle\langle u_0|, & A_\Delta^\perp &= B_\Delta^\perp = \mathbb{1} - |u_0\rangle\langle u_0|, \\ B_0^0|_V &= B_1^0|_V = |u_0\rangle\langle u_0|, & B_0^1|_V &= B_1^1|_V = 0. \end{aligned}$$

The shared state is

$$|\psi\rangle = \frac{1}{\sqrt{d}} \sum_{i \in [d]} |u_i\rangle |u_i\rangle. \quad (24)$$

Note that the shared state is the same as the one used in the extended weighted CHSH game. So are the observables B_0 and B_1 .

It is easy to calculate the ideal correlation, which is

		$y = \Delta$		$y = 0$		$y = 1$	
		$b = \diamond$	$b = \perp$	$b = 0$	$b = 1$	$b = 0$	$b = 1$
$x = \Delta$	$a = \diamond$	$1/d$	0	$1/d$	0	$1/d$	0
	$a = \perp$	0	$(d-1)/d$	$P(\perp 0 \Delta 0)$	$\frac{d-1}{d} - P(\perp 0 \Delta 0)$	$P(\perp 0 \Delta 1)$	$\frac{d-1}{d} - P(\perp 0 \Delta 0)$

Table 4: Ideal correlation of the single value test.

The reason we have $y = 0$ or $y = 1$ is that we want Bob to reuse operators from LS and we want to conclude that $B_0 B_1$ has eigenvalue 1.

Lemma 9. *If a quantum strategy $(\{\tilde{A}_\Delta^a\}_a, \{\{\tilde{B}_y^b\}_b\}_y, |\tilde{\psi}\rangle)$ has the same behaviour as the optimal one, then $(\tilde{B}_0^0 - \tilde{B}_1^1)(\tilde{B}_1^0 - \tilde{B}_0^1)$ has eigenvalue 1.*

Proof. By the marginal distribution we know that $\|\tilde{A}_\Delta^\diamond|\psi\rangle\| = \frac{1}{\sqrt{d}}$. From the condition that $P(\diamond 0|\Delta 0) = 1/d$, we know

$$\frac{\langle \psi | \tilde{A}_\Delta^\diamond \tilde{B}_0^0 | \psi \rangle}{\|\tilde{A}_\Delta^\diamond|\psi\rangle\|^2} = 1, \quad (25)$$

which implies that

$$\tilde{B}_0^0 \frac{\tilde{A}_\Delta^\diamond|\psi\rangle}{\|\tilde{A}_\Delta^\diamond|\psi\rangle\|} = \frac{\tilde{A}_\Delta^\diamond|\psi\rangle}{\|\tilde{A}_\Delta^\diamond|\psi\rangle\|}. \quad (26)$$

With similar reasoning, we get

$$\tilde{B}_1^0 \frac{\tilde{A}_\Delta^\diamond|\psi\rangle}{\|\tilde{A}_\Delta^\diamond|\psi\rangle\|} = \frac{\tilde{A}_\Delta^\diamond|\psi\rangle}{\|\tilde{A}_\Delta^\diamond|\psi\rangle\|}. \quad (27)$$

Hence $\frac{\tilde{A}_\Delta^\diamond|\psi\rangle}{\|\tilde{A}_\Delta^\diamond|\psi\rangle\|}$ is in the intersection of $\text{supp}(\tilde{B}_0^0)$ and $\text{supp}(\tilde{B}_1^0)$. Since $\text{supp}(\tilde{B}_y^0)$ and $\text{supp}(\tilde{B}_y^1)$ are disjoint, we know

$$(\tilde{B}_y^0 - \tilde{B}_y^1) \frac{\tilde{A}_\Delta^\diamond|\psi\rangle}{\|\tilde{A}_\Delta^\diamond|\psi\rangle\|} = \frac{\tilde{A}_\Delta^\diamond|\psi\rangle}{\|\tilde{A}_\Delta^\diamond|\psi\rangle\|} - 0 = \frac{\tilde{A}_\Delta^\diamond|\psi\rangle}{\|\tilde{A}_\Delta^\diamond|\psi\rangle\|}$$

for $y = 0, 1$. Therefor, we know $\frac{\tilde{A}_\Delta^\diamond|\psi\rangle}{\|\tilde{A}_\Delta^\diamond|\psi\rangle\|}$ is an eigenvector of $\tilde{B}_0 \tilde{B}_1$ with eigenvalue 1 because

$$\tilde{B}_0 \tilde{B}_1 \frac{\tilde{A}_\Delta^\diamond|\psi\rangle}{\|\tilde{A}_\Delta^\diamond|\psi\rangle\|} = \tilde{B}_0 \frac{\tilde{A}_\Delta^\diamond|\psi\rangle}{\|\tilde{A}_\Delta^\diamond|\psi\rangle\|} = \frac{\tilde{A}_\Delta^\diamond|\psi\rangle}{\|\tilde{A}_\Delta^\diamond|\psi\rangle\|}. \quad (28)$$

□

In the later section, when we apply this test to make sure some unitary U has eigenvalue 1, we denote the test by SVT_U .

3 Main result

3.1 The game $G^{(d)}$

Assume the linear system game has n variables and m equations. Alice receives $x \in \{1, \dots, m+4\}$ and Bob receives $y \in \{1, \dots, n+2\}$. The scoring rules are the following:

- when $x \in \{1, \dots, m\}$ and $y \in \{1, \dots, n\}$, they are scored according to the linear system game, LS ;
- when $x \in \{m+1, m+2, m+3\}$ and $y \in \{1, 2, n+1\}$, they are scored according to $CHSH_X^{(d)}$, where

$$*_A = m+1, \quad 0_A = m+2, \quad 1_A = m+3, \quad (29)$$

$$*_B = n+1, \quad 0_B = 1, \quad 1_A = 2, \quad (30)$$

are the inputs for the game $CHSH_X^{(d)}$ (The intuition behind is that $B_1 B_2 = X$);

- when $x = m+4$ and $y \in \{1, 2, n+2\}$, they are scored according to SVT_X , where

$$\Delta_A = m+4 \quad (31)$$

$$\Delta_B = n+2, \quad 1_B = 1, \quad 2_B = 2 \quad (32)$$

are the inputs for the game SVT_X ;

- otherwise, they score 0.

Note that the dimension d is defined in the rules of $CHSH_X^{(d)}$. Next we are going to prove that the strategy winning this game optimally can self-test d -dimensional EPR pair.

3.2 Proof

This subsection needs to be formalized. By Lemma 4.3 of [CS17], we can extract an operator solution from the perfect winning strategy of the linear system game: For each variable $\{x_i\}_{i=1}^n$, Alice and Bob has operators A_i and B_i respectively. The condition that they agree with assignment to variables means that

$$\langle \psi | A_i \otimes \bar{B}_i | \psi \rangle = 1 \Rightarrow A_i \otimes \bar{B}_i | \psi \rangle = | \psi \rangle \quad (33)$$

and the condition that Alice's assignments satisfy the constraint means that

$$\text{Tr}(\rho_A \Pi_{j:A_{ij} \neq 0} A_j) = \text{Tr}(\rho_A) \text{ for all } 1 \leq i \leq m \quad (34)$$

where $\rho_A = \text{Tr}_B(|\psi\rangle\langle\psi|)$, so for any $|v\rangle \in \text{supp}(\rho_A)$, we have

$$\Pi_{j:A_{ij} \neq 0} A_j |v\rangle = |v\rangle \text{ for all } 1 \leq i \leq m. \quad (35)$$

Since the relation $u^{-1}xu = x^2$ is embedded in this linear system game, we know

$$\sigma_A(u)^\dagger A_1 A_2 \sigma_A(u) |v\rangle = (A_1 A_2)^2 |v\rangle \text{ for all } |v\rangle \in \text{supp}(\rho_A). \quad (36)$$

For simplicity, we define $X = A_1 A_2$ and $U = \sigma_A(u)$. For simplicity, we define $X = A_1 A_2$ and $U = \sigma_A(u)$. The condition becomes

$$UXU^\dagger|v\rangle = X^2|v\rangle \text{ for all } |v\rangle \in \text{supp}(\rho_A). \quad (37)$$

On the subspace $\text{supp}(\rho_A)$, we have the equality

$$UXU^\dagger X^{-2} = \mathbb{1}. \quad (38)$$

We will come back to the implication of this condition later.

Suppose the support of \tilde{A}_*^\diamond is spanned by $|u_0\rangle$ and $|u_1\rangle$ and define $|x_1\rangle = 1/\sqrt{2}(|u_0\rangle + i|u_1\rangle)$. The test $CHSH_X^{(d)}$ tells that $|x_1\rangle$ is the eigenvector of X with eigenvalue $e^{i\pi/d} = \omega_d$. Similarly, define $|x_{d-1}\rangle = 1/\sqrt{2}(|u_0\rangle - i|u_1\rangle)$ such that $X|x_{d-1}\rangle = \omega_d^{d-1}|x_{d-1}\rangle$. We know

$$\tilde{A}_*^\diamond|\tilde{\psi}\rangle = \tilde{A}_*^\diamond \otimes \tilde{B}_*^\diamond|\tilde{\psi}\rangle = \frac{1}{\sqrt{d}}(|u_0\rangle|u_0\rangle + |u_1\rangle|u_1\rangle). \quad (39)$$

If we restrict to Alice's system, we get

$$\text{Tr}_B(\tilde{A}_*^\diamond|\tilde{\psi}\rangle\langle\tilde{\psi}|\tilde{A}_*^\diamond) = \tilde{A}_*^\diamond\rho_A\tilde{A}_*^\diamond = \frac{1}{d}|u_0\rangle\langle u_0| + |u_1\rangle\langle u_1| = \frac{1}{d}\tilde{A}_*^\diamond. \quad (40)$$

Hence ρ_A acts as $\mathbb{1}$ on $\text{supp}(\tilde{A}_*^\diamond)$. We also know that there exists local unitary U_A such that

$$U_A\tilde{A}_*^\diamond U_A^\dagger = |x_1\rangle\langle x_1| + |x_{d-1}\rangle\langle x_{d-1}| \quad (41)$$

and

$$\text{Tr}(|x_1\rangle\langle x_1|\rho_A) = \text{Tr}(U_A|u_0\rangle\langle u_0|U_A^\dagger\rho_A) = \frac{1}{d}\text{Tr}(U_A|u_0\rangle\langle u_0|U_A^\dagger) = \frac{1}{d}, \quad (42)$$

and similarly $\text{Tr}(|x_{d-1}\rangle\langle x_{d-1}|\rho_A) = 1/d$.

Next, we calculate the eigen-decomposition of X in $\text{supp}(\rho_A)$. Based on eq. (38), we know

$$XU^\dagger|x_1\rangle = U^\dagger X^2|x_1\rangle = \omega_d^2 U^\dagger|x_1\rangle, \quad (43)$$

so $U^\dagger|x_1\rangle$ is an eigenvector of X with eigenvalue ω_d^2 . By induction, we know $X(U^\dagger)^i|x_1\rangle = \omega_d^{2i}(U^\dagger)^i|x_1\rangle$. From the set $\{(U^\dagger)^i|x_1\rangle\}_{i=0}^{d-2}$, we can identify $|x_i\rangle$ for $i = 1 \dots d-1$ such that $X|x_i\rangle = \omega_d^i|x_i\rangle$. From the single value test, we know

$$\tilde{A}_\Delta^\diamond|\tilde{\psi}\rangle = \tilde{A}_\Delta^\diamond \otimes \tilde{B}_\Delta^\diamond|\tilde{\psi}\rangle = \frac{1}{\sqrt{d}}|x_0\rangle|x_0\rangle \quad (44)$$

where $X|x_0\rangle = |x_0\rangle$. The effect of $CHSH_X^{(d)}$ and SVT_X is that we have a set $\{|x_i\rangle\}_{i \in [d]} \in \text{supp}(\rho_A)$ such that

$$X|x_i\rangle = \omega_d^i|x_i\rangle. \quad (45)$$

The other effect of SVT_X is that we know

$$\tilde{A}_\Delta^\diamond\rho_A\tilde{A}_\Delta^\diamond = \frac{1}{d}|x_0\rangle\langle x_0| = \frac{1}{d}\tilde{A}_\Delta^\diamond. \quad (46)$$

Question: Can we show $\text{Tr}(|x_2\rangle\langle x_2|\rho_A) = 1/d$?

References

- [AMP12] Antonio Acín, Serge Massar, and Stefano Pironio. Randomness versus nonlocality and entanglement. *Physical review letters*, 108(10):100402, 2012.
- [BP15] Cédric Bamps and Stefano Pironio. Sum-of-squares decompositions for a family of clauser-horne-shimony-holt-like inequalities and their application to self-testing. *Physical Review A*, 91(5):052111, 2015.
- [CLS17] Richard Cleve, Li Liu, and William Slofstra. Perfect commuting-operator strategies for linear system games. *Journal of Mathematical Physics*, 58(1):012202, 2017.
- [CS17] Andrea Coladangelo and Jalex Stark. Robust self-testing for linear constraint system games. *arXiv preprint arXiv:1709.09267*, 2017.
- [Mur88] M Ram Murty. Artin’s conjecture for primitive roots. *The Mathematical Intelligencer*, 10(4):59–67, 1988.
- [Slo17] William Slofstra. The set of quantum correlations is not closed. *arXiv preprint arXiv:1703.08618*, 2017.

A Proof of Theorem 2

Proof. Following the techniques developed in Ref. [BP15], the first step is to find a sum-of-square decomposition of

$$\tilde{\mathcal{I}}_\alpha = 2\sqrt{\alpha^2 + 1}\mathbb{1} - \mathcal{I}_\alpha = \frac{2}{\sin(\mu)}\mathbb{1} - \frac{\cos(\mu)}{\sin(\mu)}(A_0B_0 + A_0B_1) - A_1B_0 + A_1B_1. \quad (47)$$

With the following notation

$$\begin{aligned} Z_A &= A_0 & X_A &= A_1 \\ Z_B &= \frac{B_0 + B_1}{2\cos(\mu)} & X_B &= \frac{B_0 - B_1}{2\sin(\mu)}, \end{aligned}$$

the two SOS decompositions that we use are

$$\tilde{\mathcal{I}}_\alpha = \frac{\sin(\mu)\tilde{\mathcal{I}}_\alpha^2 + 4\sin(\mu)\cos(\mu)^2(Z_AX_B + X_AZ_B)^2}{4}, \quad (48)$$

$$\tilde{\mathcal{I}}_\alpha = \frac{\cos^2(\mu)}{\sin(\mu)}(Z_A - Z_B)^2 + \sin(\mu)(X_A - X_B)^2. \quad (49)$$

The verification is omitted here.

Suppose the quantum strategy $(|\psi\rangle, \{\tilde{A}_x\}_{x \in [2]}, \{\tilde{B}_{y \in [2]}\})$ achieves that $\langle \psi | \tilde{\mathcal{I}}_\alpha | \psi \rangle \leq \epsilon$. The second step is to establish bounds of the following form

$$\|(\tilde{Z}_A - \tilde{Z}_B)|\psi\rangle\| \leq c_1\sqrt{\epsilon} \quad (50)$$

$$\|(\tilde{X}_A(\mathbb{1} + \tilde{Z}_B) - \tilde{X}_B(\mathbb{1} - \tilde{Z}_A))|\psi\rangle\| \leq c_2\sqrt{\epsilon} \quad (51)$$

$$\|(\tilde{X}_A - \tilde{X}_B)|\psi\rangle\| \leq c_3\sqrt{\epsilon} \quad (52)$$

$$\|(\tilde{Z}_A\tilde{X}_A + \tilde{X}_A\tilde{Z}_A)|\psi\rangle\| \leq c_4\sqrt{\epsilon}. \quad (53)$$

Now we write $s = \sin(\mu)$, $c = \cos(\mu)$ and define

$$\begin{aligned} S_1 &= \frac{\sqrt{s}}{2} \tilde{\mathcal{I}}_\alpha, & S_2 &= \sqrt{s}c(\tilde{Z}_A \tilde{X}_B + \tilde{X}_A \tilde{Z}_B), \\ S_3 &= \frac{c}{\sqrt{s}}(\tilde{Z}_A - \tilde{Z}_B), & S_4 &= \sqrt{s}(\tilde{X}_A - \tilde{X}_B) \end{aligned}$$

then $\tilde{\mathcal{I}}_\alpha = S_1^2 + S_2^2 = S_3^2 + S_4^2$ and $\langle \psi | \tilde{\mathcal{I}}_\alpha | \psi \rangle \leq \epsilon$ implies that $\langle \psi | S_i^2 | \psi \rangle \leq \epsilon$ and $\|S_i | \psi \rangle\| \leq \sqrt{\epsilon}$ for $i = 1, 2, 3, 4$. We can easily check that

$$c_1 = \frac{\sqrt{s}}{c}, \quad c_2 = \frac{1}{\sqrt{s}} + \frac{1}{c\sqrt{s}}, \quad c_3 = \frac{1}{\sqrt{s}}.$$

where we use the relation that $\tilde{X}_A(\mathbb{1} + \tilde{Z}_B) - \tilde{X}_B(\mathbb{1} - \tilde{Z}_A) = S_4/s^{1/2} + S_2/(cs^{1/2})$. To calculate c_4 , we use the relation

$$\tilde{Z}_A \tilde{X}_A + \tilde{X}_A \tilde{Z}_A = \frac{S_2}{c\sqrt{s}} + \frac{\sqrt{s}\tilde{X}_A S_3}{c} + \frac{\tilde{Z}_A S_4}{\sqrt{s}} \quad (54)$$

and reach the conclusion that

$$c_4 = \frac{1 + c + s}{c\sqrt{s}} \quad (55)$$

where we use that fact that \tilde{Z}_A, \tilde{X}_A are unitaries.

With appropriate substitutions, the rest of the proof follows the same derivation as that in Appendix A of Ref. [BP15], so we omit it here. \square

B Construction of $\Gamma(LS)$