Self-test EPR pair with constant alphabet

Honghao Fu[1] 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., Gaithersbug, MD 20899, USA*

December 7, 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

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

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

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

where $\omega_d = e^{i\pi/d}$ is the primitive dth 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

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

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

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

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

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

Definition 1 (Ideal strategy for $\mathcal{I}_\alpha$). *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*

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

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

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

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 the 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

$$\tilde{B}_0\tilde{B}_1|u_0\rangle = \cos(\pi/d)|u_0\rangle - \sin(\pi/d)|u_1\rangle \tag{8}$$
$$\tilde{B}_0\tilde{B}_1|u_1\rangle = \sin(\pi/d)|u_0\rangle + \cos(\pi/d)|u_1\rangle. \tag{9}$$

We can conclude that

$$\tilde{B}_0\tilde{B}_1(|u_0\rangle + i|u_1\rangle) = e^{i\frac{\pi}{d}}(|u_0\rangle + i|u_1\rangle) \tag{10}$$
$$\tilde{B}_0\tilde{B}_1(|u_0\rangle - i|u_1\rangle) = e^{-i\frac{\pi}{d}}(|u_0\rangle - i|u_1\rangle). \tag{11}$$

□

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: $\pi : X \times Y \to [0,1]$, which is the probability distribution over the questions, and $V : A \times B \times X \times Y \to \mathbb{R}$, 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 $\{\{B_y^b\}_b\}_y$ on Bob's side, and a shared state $|\psi\rangle$. Then the behaviour of Alice and Bob is described by the conditional probability

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

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

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

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*

$$a(y) = b \qquad \textit{(Consistency)}$$

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

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*

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

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

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

Then the solution group has presentation

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

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 $G^{(d)}$

2.1 The linear system game

The main component of $G^{(d)}$ is a linear system game LS, whose solution group is an embedding of the qudit Pauli group, which is defined as

$$\mathcal{P}_d = \langle x, z, \mathcal{J} : x^d = z^d = \mathcal{J}^d = e, zxz^{-1}x^{-1} = \mathcal{J}, x\mathcal{J}x^{-1}\mathcal{J}^{-1} = z\mathcal{J}z^{-1}\mathcal{J}^{-1} = e\rangle. \tag{17}$$

To construct LS, we introduce new generators u_x and u_z, and replace the relation $x^d = z^d = e$ by the following relations

$$u_x x u_x = x^2, \quad u_z z u_z = z^2. \tag{18}$$

With constraints imposed by other components of the whole game, the two conditions above imply that the eigenvalues of x and z are $\{\omega_d^k = e^{ik\pi/d}\}_{k=1}^d$ with d odd, prime and $\mathbb{Z}/(d\mathbb{Z})$ has primitive root 2 and the eigenspaces for different eigenvalues are of the same dimension. Later we will set the exponent to be $a \in \{2, 3, 5\}$ which is the primitive root of infinitely many prime numbers and construct a nonlocal game that can self-test infinitely many maximally entangled state. [1]

Secondly, we drop the relation $\mathcal{J}^d = e$ and make the value of $\mathcal{J}$ determined by x and z in the relation $xzx^{-1}z^{-1} = \mathcal{J}$.

It can be easily checked that the qudit Pauli-x and Pauli-z operators of dimension d satisfy the new relations above, where Pauli-x and Pauli-z operators are defined by

$$\sigma_x = \sum_{i=0}^{d-1} |i+1 \pmod{d}\rangle\langle i| \qquad \sigma_z = \sum_{i=0}^{d-1} \omega_d^i |i\rangle\langle i|. \tag{19}$$

Moreover, if $U_x\sigma_x U_x^\dagger = \sigma_x^2$ and $U_z\sigma_z U_z^\dagger = \sigma_z^2$, we can verify that

$$U_x U_z = \mathbb{1} = U_z U_x, \tag{20}$$

Hence, we define the new group by

$$\begin{aligned} \mathcal{P} = \langle x, z, u, \mathcal{J} : & zxz^{-1}x^{-1} = \mathcal{J}, [x, \mathcal{J}] = [z, \mathcal{J}] = [u, \mathcal{J}] = e, \\ & uxu^{-1} = x^2, u^{-1}zu = z^2\rangle. \end{aligned} \tag{21}$$

Since $\mathcal{P}_d$'s relations satisfy the relations of $\mathcal{P}$, can we say $\mathcal{P}_d$ is a subgroup of $\mathcal{P}$? This group will be embedded in a solution group, $\Gamma_{\mathcal{P}}$, following Slofstra's embedding techniques. See Appendix **??** for details.

[1] Figuring out what a is will take us one step closer to resolving Artin's Conjecture[Mur88].

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

$$\bar{\mathcal{I}}_\alpha = 2\sqrt{\alpha^2+1}\mathbb{1} - \mathcal{I}_\alpha = \frac{2}{\sin(\mu)}\mathbb{1} - \frac{\cos(\mu)}{\sin(\mu)}(A_0B_0 + A_0B_1) - A_1B_0 + A_1B_1. \tag{22}$$

With the following notation

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

the two SOS decompositions that we use are

$$\bar{\mathcal{I}}_\alpha = \frac{\sin(\mu)\bar{\mathcal{I}}_\alpha^2 + 4\sin(\mu)\cos(\mu)^2(Z_AX_B + X_AZ_B)^2}{4}, \tag{23}$$

$$\bar{\mathcal{I}}_\alpha = \frac{\cos^2(\mu)}{\sin(\mu)}(Z_A - Z_B)^2 + \sin(\mu)(X_A - X_B)^2. \tag{24}$$

The verification is omitted here.

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

$$\|(\tilde{Z}_A - \tilde{Z}_B)|\psi\rangle\| \leq c_1\sqrt{\epsilon} \tag{25}$$

$$\|(\tilde{X}_A(\mathbb{1} + \tilde{Z}_B) - \tilde{X}_B(\mathbb{1} - \tilde{Z}_A))|\psi\rangle\| \leq c_2\sqrt{\epsilon} \tag{26}$$

$$\|(\tilde{X}_A - \tilde{X}_B)|\psi\rangle\| \leq c_3\sqrt{\epsilon} \tag{27}$$

$$\|(\tilde{Z}_A\tilde{X}_A + \tilde{X}_A\tilde{Z}_A)|\psi\rangle\| \leq c_4\sqrt{\epsilon}. \tag{28}$$

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

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

then $\bar{\mathcal{I}}_\alpha = S_1^2 + S_2^2 = S_3^2 + S_4^2$ and $\langle\psi|\bar{\mathcal{I}}_\alpha|\psi\rangle \leq \epsilon$ 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

$$\tilde{Z}_A\tilde{X}_A + \tilde{X}_A\tilde{Z}_A = \frac{S_2}{c\sqrt{s}} + \frac{\sqrt{s}\tilde{X}_A S_3}{c} + \frac{\tilde{Z}_A S_4}{\sqrt{s}} \tag{29}$$

and reach the conclusion that

$$c_4 = \frac{1 + c + s}{c\sqrt{s}} \tag{30}$$

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. □