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 10, 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 $1 \le x \le m$ 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*

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

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

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*

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

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

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

Then the solution group has presentation

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

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 $G^{(d)}$

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 qudit Pauli group, which is defined as

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

The goal of our modification is to construct $\mathcal{P}_{LS}$ which has implicit d-dependence. We first introduce new generators u_x and u_z to $\mathcal{P}_d$, and replace the relation $x^d = z^d = e$ by the following relations

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

Consequently, the d dependency of $G^{(d)}$ comes from constraints imposed by other components of the game, [1] but the alphabet sizes are determined by $\mathcal{P}_{LS}$ and we will see why they are constant. Next, 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 $\sigma_x^{(d)}$ and $\sigma_z^{(d)}$ can be extended to a representation of $\mathcal{P}_{LS}$ where $\sigma_x^{(d)}$ and $\sigma_z^{(d)}$ are defined by

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

Moreover, if $U_x \sigma_x^{(d)} U_x^\dagger = (\sigma_x^{(d)})^2$ and $U_z \sigma_z^{(d)} U_z^\dagger = (\sigma_z^{(d)})^2$, we can verify that

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

Hence, we do not need both u_x and u_z as generators and we just need one of them. In the end, we define $\mathcal{P}_{LS}$ by

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

This group will be embedded in a solution group, $\Gamma(LS)$, following Slofstra's embedding techniques. The corresponding game LS has $n = 2351$ variables and $m = 1916$ equations. See Appendix B for details.

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

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 $V^\perp = \mathbb{C}^d \setminus \text{span}\{|u_1\rangle, |u_{d-1}\rangle\}$ amd define Π_V and $\Pi_V^\perp$ to be the corresponding projectors. Note that V is the subspace on which they should maximaize $\langle I_{-\cot(\pi/2d)}\rangle$.

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

$$A_*^{\diamond} = \Pi_V, A_*^{\perp} = \Pi_V^{\perp}$$
$$A_0^0 = |u_1\rangle\langle u_1|, A_0^1 = |u_{d-1}\rangle\langle u_{d-1}|, A_0^{\perp} = \Pi_V^{\perp}$$
$$A_1^0 = \frac{1}{2}(|u_1\rangle + |u_{d-1}\rangle)(\langle u_1| + \langle u_{d-1}|), A_0^1 = \frac{1}{2}(|u_1\rangle - |u_{d-1}\rangle)(\langle u_1| - \langle u_{d-1}|), A_0^{\perp} = \Pi_V^{\perp}$$

Bob's projectors are

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

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* $CHSH^{(d)}$*, then there exists unitaries* U_A *and* U_B *such that*

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

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

$$(\tilde{A}_0^0 + \tilde{A}_0^1)\tilde{B}_*^\diamond|\tilde{\psi}\rangle = \tilde{B}_*^\diamond|\tilde{\psi}\rangle. \tag{22}$$

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

$$\tilde{B}_*^\diamond(\tilde{A}_0^0 + \tilde{A}_0^1)|\tilde{\psi}\rangle = (\tilde{A}_0^0 + \tilde{A}_0^1)|\tilde{\psi}\rangle. \tag{23}$$

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

$$(\tilde{A}_0^0 + \tilde{A}_0^1)|\tilde{\psi}\rangle = \tilde{B}_*^\diamond|\tilde{\psi}\rangle. \tag{24}$$

Following the same line of argument, we can conclude that

$$\tilde{B}_*^\diamond|\tilde{\psi}\rangle = \tilde{A}_*^\diamond|\tilde{\psi}\rangle = (\tilde{A}_0^0 + \tilde{A}_0^1)|\tilde{\psi}\rangle = (\tilde{A}_1^0 + \tilde{A}_1^1)|\tilde{\psi}\rangle. \tag{25}$$

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

$$\tilde{B}_*^\perp|\tilde{\psi}\rangle = \tilde{A}_*^\perp|\tilde{\psi}\rangle = \tilde{A}_0^\perp|\tilde{\psi}\rangle = \tilde{A}_1^\perp|\tilde{\psi}\rangle, \tag{26}$$

with similar arguments.

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

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

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 $\mathrm{span}(\tilde{A}_0^0) \cap \mathrm{span}(\tilde{A}_0^\perp) = \emptyset$. 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

$$\frac{\langle\tilde{\psi}|\tilde{B}_*^\diamond\tilde{A}_0^0\tilde{B}_0^0\tilde{B}_*^\diamond|\tilde{\psi}\rangle}{\langle\tilde{\psi}|\tilde{B}_*^\diamond\tilde{B}_*^\diamond|\tilde{\psi}\rangle} = \frac{\cos^2(\pi/4d)}{2}. \tag{27}$$

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 $\tilde{A}_*^\diamond\tilde{B}_*^\diamond|\tilde{\psi}\rangle = \tilde{B}_*^\diamond|\tilde{\psi}\rangle$. □

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 $X = \{*\}$, $Y = \{0, 1, *\}$, $A = \{\diamond, \perp\}$ and $B = \{0, 1, \diamond, \perp\}$. 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 2** $x = *$ and $y = 0$: when Alice answer $\diamond$, Bob should answer 0, when Alice answer$\perp$ all answers of Bob are accepted;
- **Case 3** $x = *$ 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

$$A_*^\diamond = B_*^\diamond = |u_0\rangle\langle u_0|, \qquad A_*^\perp = B_*^\perp = \mathbb{1} - |u_0\rangle\langle u_0|,$$
$$B_0^0|_V = B_1^0|_V = |u_0\rangle\langle u_0|, \qquad B_0^1|_V = B_1^1|_V = 0.$$

The shared state is

$$|\psi\rangle = \frac{1}{\sqrt{d}} \sum_{i\in[d]} |u_i\rangle|u_i\rangle. \tag{28}$$

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

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

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

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

$$\frac{\langle\psi|\tilde{A}_*^\diamond \tilde{B}_0^0|\psi\rangle}{\|\tilde{A}_*^\diamond|\psi\rangle\|^2} = 1, \tag{29}$$

which implies that

$$\tilde{B}_0^0 \frac{\tilde{A}_*^\diamond|\psi\rangle}{\|\tilde{A}_*^\diamond|\psi\rangle\|} = \frac{\tilde{A}_*^\diamond|\psi\rangle}{\|\tilde{A}_*^\diamond|\psi\rangle\|}. \tag{30}$$

With similar reasoning, we get

$$\tilde{B}_1^0 \frac{\tilde{A}_*^\diamond|\psi\rangle}{\|\tilde{A}_*^\diamond|\psi\rangle\|} = \frac{\tilde{A}_*^\diamond|\psi\rangle}{\|\tilde{A}_*^\diamond|\psi\rangle\|}. \tag{31}$$

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

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

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

$$\tilde{B}_0\tilde{B}_1\frac{\tilde{A}_*^\diamond|\psi\rangle}{\|\tilde{A}_*^\diamond|\psi\rangle\|} = \tilde{B}_0\frac{\tilde{A}_*^\diamond|\psi\rangle}{\|\tilde{A}_*^\diamond|\psi\rangle\|} = \frac{\tilde{A}_*^\diamond|\psi\rangle}{\|\tilde{A}_*^\diamond|\psi\rangle\|}. \tag{32}$$

□

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.

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

$$\bar{\mathcal{I}}_\alpha = 2\sqrt{\alpha^2+1}\mathbb{1} - \mathcal{I}_\alpha = \frac{2}{\sin(\mu)}\mathbb{1} - \frac{\cos(\mu)}{\sin(\mu)}(A_0B_0 + A_0B_1) - A_1B_0 + A_1B_1. \tag{33}$$

With the following notation

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

the two SOS decompositions that we use are

$$\bar{\mathcal{I}}_\alpha = \frac{\sin(\mu)\bar{\mathcal{I}}_\alpha^2 + 4\sin(\mu)\cos(\mu)^2(Z_A X_B + X_A Z_B)^2}{4}, \tag{34}$$

$$\bar{\mathcal{I}}_\alpha = \frac{\cos^2(\mu)}{\sin(\mu)}(Z_A - Z_B)^2 + \sin(\mu)(X_A - X_B)^2. \tag{35}$$

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

$$\|(\tilde{Z}_A - \tilde{Z}_B)|\psi\rangle\| \leq c_1\sqrt{\epsilon} \tag{36}$$
$$\|(\tilde{X}_A(\mathbb{1} + \tilde{Z}_B) - \tilde{X}_B(\mathbb{1} - \tilde{Z}_A))|\psi\rangle\| \leq c_2\sqrt{\epsilon} \tag{37}$$
$$\|(\tilde{X}_A - \tilde{X}_B)|\psi\rangle\| \leq c_3\sqrt{\epsilon} \tag{38}$$
$$\|(\tilde{Z}_A\tilde{X}_A + \tilde{X}_A\tilde{Z}_A)|\psi\rangle\| \leq c_4\sqrt{\epsilon}. \tag{39}$$

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

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

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

$$\tilde{Z}_A\tilde{X}_A + \tilde{X}_A\tilde{Z}_A = \frac{S_2}{c\sqrt{s}} + \frac{\sqrt{s}\tilde{X}_A S_3}{c} + \frac{\tilde{Z}_A S_4}{\sqrt{s}} \tag{40}$$

and reach the conclusion that

$$c_4 = \frac{1 + c + s}{c\sqrt{s}} \tag{41}$$

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. □

B Construction of $\Gamma(LS)$

In this section, we are going to embed the group $\mathcal{P}_{LS}$ into a solution group $\Gamma(LS)$ of a linear system game. What we do is to write any generator with arbitrary order as a product of new order-2 generators and rewrite all the relations with the new generators. In the end, we can get rid of the generators y_i and u and all the remaining generators are order-2.

We first embed the relation $xzx^{-1}z^{-1} = \mathcal{J}$ in a linear system game very similar to the Magic Square game. It has been shown that the following relations embeds $xzx^{-1}z^{-1} = \mathcal{J}$ [2]. Let $y_3 = z$ and $y_7 = x$ and the linear relations are

$$\begin{aligned} &y_1y_2y_3 = e, && y_4y_5y_6 = e, && y_7y_8y_9 = e, \\ &y_1^{-1}y_4^{-1}y_7^{-1} = e, && y_2^{-1}y_5^{-1}y_8^{-1} = \mathcal{J}, && y_3^{-1}y_6^{-1}y_9^{-1} = e. \end{aligned}$$

We refer to these set of linear relations as the MS_l relations. The magic square game also introduces some commutation relations:

$$\begin{aligned} &[y_1, y_2] = [y_1, y_3] = [y_1, y_4] = [y_1, y_7] = e, \\ &[y_2, y_3] = [y_2, y_5] = [y_2, y_8] = e, \\ &[y_3, y_6] = [y_3, y_9] = e, \\ &[y_4, y_7] = [y_4, y_5] = [y_4, y_6] = e, \\ &[y_5, y_6] = [y_5, y_8] = e, \\ &[y_6, y_9] = e, \\ &[y_7, y_8] = [y_7, y_9] = e, \\ &[y_8, y_9] = e. \end{aligned}$$

The set of the commutation relations above is denoted by MS_c. So we redefine $\mathcal{P}_{LS}$ as

$$\mathcal{P}_{LS} = \langle \{y_i\}_{i=1}^9, u, \mathcal{J} : MS_l \cup MS_c \cup \{[\mathcal{J}, y_i] = [\mathcal{J}, u] = e, uy_7u^{-1} = y_7^2, u^{-1}y_3u = y_3^2\}\rangle. \tag{42}$$

Then we can use a procedure similar to the one used in the proof of Proposition 4.8 of Ref. [Slo17] to embed $\mathcal{P}_{LS}$ into a group with only order-2 generators except for $\mathcal{J}$, whose order is implicit.

We start by introducing $y_{3,1}$ and $y_{3,2}$ of order 2 such that $y_3 = y_{3,1}y_{3,2}$ and $y_{3,1}$ commutes with u, $\mathcal{J}$ and y_i for $i \neq 3$. Then the relation $uy_3u^{-1} = y_3^2$ is rewritten as $uy_{3,2}u^{-1} = y_{3,2}y_{3,1}y_{3,2}$ so we introduce $y_{3,3} = y_{3,2}y_{3,1}y_{3,2}$. The group $\mathcal{P}_{LS}$ becomes

$$\begin{aligned} \mathcal{P}_{LS} = \langle y_{3,1}, y_{3,2}, y_{3,3}, u, \{y_i\}_{i\neq 3}\mathcal{J} : & y_{3,1}^2 = y_{3,2}^2 = y_{3,3}^2 = e, \\ & \mathcal{J} \text{ commute with all the generators, } [y_i, y_{3,1}] = [u, y_{3,1}] = e \text{ for } i \neq 3, \\ & MS_c \text{ with } y_3 \text{ replaced by } y_{3,2}, MS_l \text{ with } y_3 \text{ replaced by } y_{3,1}y_{3,2}, \\ & u^{-1}y_7u = y_7^2, y_{3,3} = y_{3,2}y_{3,1}y_{3,2}, uy_{3,2}u^{-1} = y_{3,3}\rangle. \end{aligned} \tag{43}$$

Next, we introduce $y_{7,1}$ and $y_{7,2}$ of order 2 such that $y_7 = y_{7,1}y_{7,2}$ and $y_{7,1}$ commutes with u, $\mathcal{J}$ and y_i for $i \neq 3, 7$. Then the relation $u^{-1}y_7u = y_7^2$ is rewritten as $u^{-1}y_{7,2}u = y_{7,2}y_{7,1}y_{7,2}$ so we introduce $y_{7,3} = y_{7,2}y_{7,1}y_{7,2}$. The relation $y_7y_{3,1}y_7^{-1} = y_{3,1}$ is rewritten as $y_{7,2}y_{3,1}y_{7,2} = y_{7,1}y_{3,1}y_{7,1}$ so

[2] For example, Fig. 11 of Ref. [CS17] proves it in a group picture.

we introduce $y_{7,4} = y_{7,1}y_{3,1}y_{7,1}$. The group $\mathcal{P}_{LS}$ becomes

$$\begin{aligned}\mathcal{P}_{LS} = \langle \{y_{3,i}\}_{i=1}^{3}, \{y_{7,i}\}_{i=1}^{4}, \{y_i\}_{i\neq 3,7}, u, \mathcal{J} : & \{y_{3,i}\}_{i=1}^{3}\{y_{7,i}\}_{i=1}^{4} \text{ of order 2;} \\ & \mathcal{J} \text{ commutes with all the generators, } [u, y_{3,1}] = [u, y_{7,1}] = e, \\ & y_{3,1}, y_{7,1} \text{ commute with } y_i,\ i \neq 3,7, \\ & MS_c \text{ with } y_3, y_7 \text{ replaced by } y_{3,2}, y_{7,2}, \\ & MS_l \text{ with } y_3, y_7 \text{ replaced by } y_{3,1}y_{3,2} \text{ and } y_{7,1}y_{7,2} \\ & y_{3,3} = y_{3,2}y_{3,1}y_{3,2}, uy_{3,2}u^{-1} = y_{3,3}, \\ & y_{7,3} = y_{7,2}y_{7,1}y_{7,2}, u^{-1}y_{7,2}u = y_{7,3}, \\ & y_{7,4} = y_{7,1}y_{3,1}y_{7,1}, y_{7,2}y_{3,1}y_{7,2} = y_{7,4}\rangle \end{aligned} \tag{44}$$

To replace u, we introduce u_1, u_2 of order 2 such that $u = u_1u_2$ and u_1 commutes with y_i for $i \neq 3,7$ and $\mathcal{J}$. The conjugacy relations involving u are $uy_{3,2}u^{-1} = y_{3,3}$, $u^{-1}y_{7,2}u = y_{7,3}$, $uy_{3,1}u^{-1} = y_{3,1}$ and $uy_{7,1}u^{-1} = y_{7,1}$. So we need to introduce u_3, u_4, u_5, u_6 such that

$$\begin{aligned} u_3 &= u_2y_{3,2}u_2 = u_1y_{3,3}u_1, \\ u_4 &= u_1y_{7,2}u_1 = u_2y_{7,3}u_2, \\ u_5 &= u_2y_{3,1}u_2 = u_1y_{3,1}u_1, \\ u_6 &= u_2y_{7,1}u_2 = u_1y_{7,1}u_1. \end{aligned}$$

At this stage $\mathcal{P}_{LS}$ has generators $\{y_{3,i}\}_{i=1}^{3}, \{y_{7,i}\}_{i=1}^{4}, \{y_i\}_{i\neq 3,7}, \{u_i\}_{i=1}^{6}$ with 6 linear relations and 44 conjugacy relations.

For the remaining y_i's, we use y_1 as an example and the same steps apply to the other y_i's. The conjugacy relations involving y_1 are

$$y_1y_{3,1}y_1^{-1} = y_{3,1}, \qquad\qquad y_1y_{7,1}y_1^{-1} = y_{7,1}.$$

and 4 commutation relations from MS_c. So we need to introduce $y_{1,i}$ for $i = 1, 2 \ldots 8$ such that they all are of order 2 and

$$\begin{aligned} y_1 &= y_{1,1}y_{1,2} \\ y_{1,3} &= y_{1,2}y_{3,1}y_{1,2} = y_{1,1}y_{3,1}y_{1,1}, \\ y_{1,4} &= y_{1,2}y_{7,1}y_{1,2} = y_{1,1}y_{7,1}y_{1,1}, \\ y_{1,5} &= y_{1,2}y_2y_{1,2} = y_{1,1}y_2y_{1,1}, \\ y_{1,6} &= y_{1,2}y_{3,2}y_{1,2} = y_{1,1}y_{3,2}y_{1,1}, \\ y_{1,7} &= y_{1,2}y_4y_{1,2} = y_{1,1}y_4y_{1,1}, \\ y_{1,8} &= y_{1,2}y_{7,2}y_{1,2} = y_{1,1}y_{7,2}y_{1,1}. \end{aligned}$$

The new commutation relations are $y_{1,1}$ commutes with all the remaining y_j's and commutation relations from MS_c involving y_1 with y_1 replaced by $y_{1,2}$. Then we repeat this process with y_2. In summary, replacing $y_1, y_2, y_4, y_5, y_6, y_8, y_9$ introduces $8 + 9 + 10 + 11 + 12 + 13 + 14 = 77$ new variables and $12 + 14 + 16 + 18 + 20 + 22 + 24 = 126$ new conjugacy relations. In total $\mathcal{P}_{LS}$ has 90 variables excluding $\mathcal{J}$, 6 linear relations and 170 conjugacy relations.

Then following the recipe given in the proofs of Proposition 4.2 and Lemma 4.4 in Ref. [Slo17], we embed $\mathcal{P}_{LS}$ into the solution group $\Gamma(LS)$ with 2351 variables and 1916 linear relations. Alice's output alphabet is of size 64 and of size 2 for Bob.

Such linear system game has at the biggest size when $a = 5$ or the special relation is $uxu^{-1} = x^5$. The biggest game has 2465 variables and 2006 equations. We leave the derivation for curious readers.