Robust Self Testing for Linear Constraint Games

Andrea Coladangelo Jalex Stark

Department of Computing and Mathematical Sciences
California Institute of Technology

QIP 2018, 16 January 2017

Outline

What makes self testing work?

- Self-testing community has a bag of tricks that requires intuition and hard work to apply.

What makes self testing work?

- Self-testing community has a bag of tricks that requires intuition and hard work to apply.
- Thesis: Self-testing proofs run on algebra representations.

What makes self testing work?

- Self-testing community has a bag of tricks that requires intuition and hard work to apply.
- Thesis: Self-testing proofs run on algebra representations.
- We focus on the simplest possible new results with proofs using a representation-theoretic framework.

Outline

A pseudotelepathic self-testing result

Theorem ([Wu+16])

There is a two-prover nonlocal game with perfect completeness self-testing the maximally entangled state on two pairs of qubits. The self-test has $O(\varepsilon)$ robustness, i.e. if the provers win with probability $1 - \varepsilon$, then their state is $O(\varepsilon)$ close **in trace distance** *to the ideal state.*

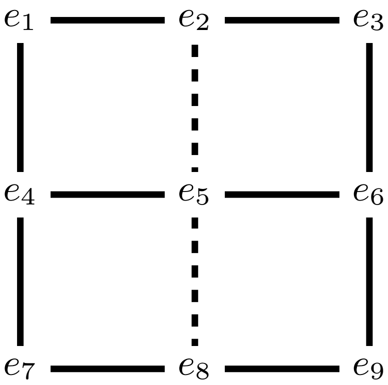
A pseudotelepathic self-testing result

Theorem ([Wu+16])

There is a two-prover nonlocal game with perfect completeness self-testing the maximally entangled state on two pairs of qubits. The self-test has $O(\varepsilon)$ robustness, i.e. if the provers win with probability $1-\varepsilon$, then their state is $O(\varepsilon)$ close **in trace distance** *to the ideal state.*

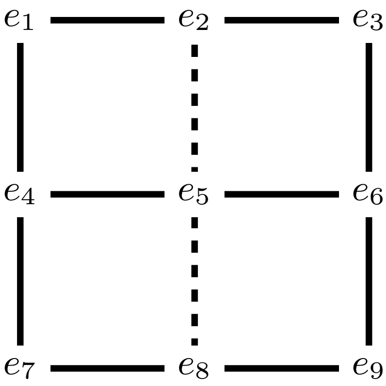
This was the first self-test using a *pseudotelepathy game*, i.e. a nonlocal game where ideal quantum provers win with probability 1 while any classical provers win with probability < 1.

The Mermin–Peres Magic Square equations



$$
\begin{aligned}
e_1 + e_2 + e_3 &= 0 \pmod{d} \\
e_4 + e_5 + e_6 &= 0 \pmod{d} \\
e_7 + e_8 + e_9 &= 0 \pmod{d} \\
-(e_2 + e_5 + e_8) &= 1 \pmod{d} \\
-(e_1 + e_4 + e_7) &= 0 \pmod{d} \\
-(e_3 + e_6 + e_9) &= 0 \pmod{d}
\end{aligned}
$$

The Mermin–Peres Magic Square equations



$$
\begin{aligned}
e_1 + e_2 + e_3 &= 0 \pmod{d} \\
e_4 + e_5 + e_6 &= 0 \pmod{d} \\
e_7 + e_8 + e_9 &= 0 \pmod{d} \\
-(e_2 + e_5 + e_8) &= 1 \pmod{d} \\
-(e_1 + e_4 + e_7) &= 0 \pmod{d} \\
-(e_3 + e_6 + e_9) &= 0 \pmod{d}
\end{aligned}
$$

Add up all equations: $0 = 1$.

The Magic Square game

1. Verifier asks Alice for an assignment to all the variables in a particular equation. Verifier asks Bob for an assignment to one variable in the same equation.

Transcript ($d = 3$)

Verifier	Alice, assign e_1, e_2, e_3.
	Bob, assign e_2.

The Magic Square game

1. Verifier asks Alice for an assignment to all the variables in a particular equation. Verifier asks Bob for an assignment to one variable in the same equation.
2. Without communicating with each other, Alice and Bob send answers to Verifier.

Transcript ($d = 3$)

Verifier	Alice, assign e_1, e_2, e_3. Bob, assign e_2.
Alice	$e_1 = 0, e_2 = 1, e_3 = 2$.
Bob	$e_2 = 1$.

The Magic Square game

1. Verifier asks Alice for an assignment to all the variables in a particular equation. Verifier asks Bob for an assignment to one variable in the same equation.
2. Without communicating with each other, Alice and Bob send answers to Verifier.
3. Verifier checks that Alice's assignment satisfies the relevant equation.
4. Verifier checks that Alice and Bob agree on their shared variable.

Transcript ($d = 3$)

Verifier	Alice, assign e_1, e_2, e_3. Bob, assign e_2.
Alice	$e_1 = 0, e_2 = 1, e_3 = 2$.
Bob	$e_2 = 1$.
Verifier	$0 + 1 + 2 = 0 \pmod 3$.
Verifier	$1 = 1$. **Alice and Bob win the game.**

Classical players can't overcome the contradiction

We could make a similar game starting from to any system of linear equations $\pmod{d}$. These are called *linear constraint system games* (LCS games).

Classical players can't overcome the contradiction

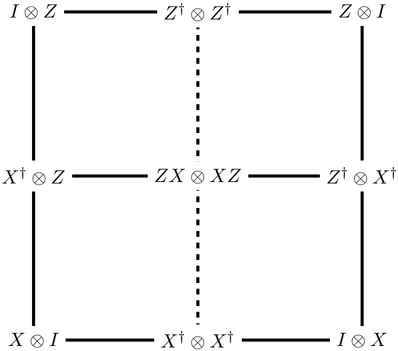
We could make a similar game starting from to any system of linear equations $\pmod{d}$. These are called *linear constraint system games* (LCS games).

Fact

If a system of equations has no solution, and Alice and Bob use a classical strategy in the corresponding LCS game, then they win with probability < 1.

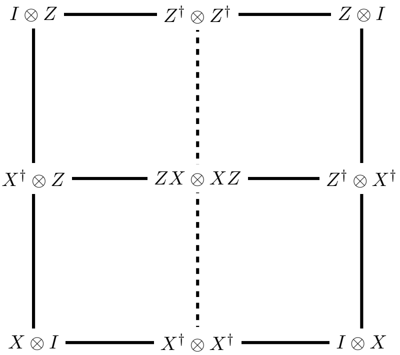
(In fact, they win with probability $\leq 1 - \frac{1}{\max(n,m)}$, where n, m are the number of equations and variables, respectively.)

The Mermin–Peres Magic Square operators, $d = 2$



$$X^2 = Z^2 = I$$
$$XZX^\dagger Z^\dagger = -I$$

The Mermin–Peres Magic Square operators, $d = 2$



$X^2 = Z^2 = I$

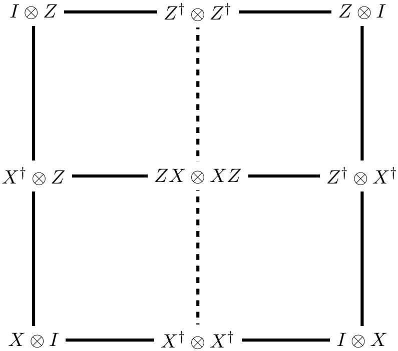
$XZX^\dagger Z^\dagger = -I$

On any line, the three operators commute

The product of operators on a solid line is I

The product of operators on the dashed line is $-I$

The Mermin–Peres Magic Square operators, $d = 2$



$X^2 = Z^2 = I$

$XZX^\dagger Z^\dagger = -I$

On any line, the three operators commute

The product of operators on a solid line is I

The product of operators on the dashed line is $-I$

If we replace $\{0, 1\}$ with $\{1, -1\}$ and replace addition with multiplication, then these operators satisfy the magic square equations! Call this an "operator solution" for the equations.

Winning the game with an operator solution, I

Suppose O_1, O_2, O_3 are commuting binary observables with $\langle\psi|O_1 O_2 O_3|\psi\rangle = (-1)^a$. If Alice measures O_1, O_2, O_3 to get results a_1, a_2, a_3, then she always has $a_1 + a_2 + a_3 = a$.

Winning the game with an operator solution, I

Suppose O_1, O_2, O_3 are commuting binary observables with $\langle\psi|O_1 O_2 O_3|\psi\rangle = (-1)^a$. If Alice measures O_1, O_2, O_3 to get results a_1, a_2, a_3, then she always has $a_1 + a_2 + a_3 = a$. Similarly, suppose that O_A and O_B satisfy $\langle\psi|O_A O_B^\dagger|\psi\rangle = 1$. If Alice measures O_A to get outcome a and Bob measures O_B to get outcome b, then $a - b = 0$ will always hold.

Winning the game with an operator solution, II

When asked for the value of a variable in the magic square, Alice measures the corresponding magic square operator. The multiplicative relations guarantee that Alice always satisfies her equations.

Winning the game with an operator solution, II

When asked for the value of a variable in the magic square, Alice measures the corresponding magic square operator. The multiplicative relations guarantee that Alice always satisfies her equations.

Similarly, Bob measures the conjugate of the magic square operator. Since $|\psi\rangle$ is maximally entangled, this guarantees that they give matching outputs.

Winning the game with an operator solution, II

When asked for the value of a variable in the magic square, Alice measures the corresponding magic square operator. The multiplicative relations guarantee that Alice always satisfies her equations.
Similarly, Bob measures the conjugate of the magic square operator. Since $|\psi\rangle$ is maximally entangled, this guarantees that they give matching outputs.

Theorem ([CLS16])

For any linear constraint game, if Alice and Bob share a maximally entangled state and make measurements according to an "operator solution" of the equations, then they will win with probability 1.

Winning the game with an operator solution, II

When asked for the value of a variable in the magic square, Alice measures the corresponding magic square operator. The multiplicative relations guarantee that Alice always satisfies her equations.
Similarly, Bob measures the conjugate of the magic square operator. Since $|\psi\rangle$ is maximally entangled, this guarantees that they give matching outputs.

Theorem ([CLS16])

For any linear constraint game, if Alice and Bob share a maximally entangled state and make measurements according to an "operator solution" of the equations, then they will win with probability 1.
Furthermore, this is the only way to always win an LCS game.

Outline

Find an isometry

Suppose we want to prove a self-testing result for the maximally entangled state of one pair of qubits, denote it $|\mathrm{EPR}_2\rangle$.

Find an isometry

Suppose we want to prove a self-testing result for the maximally entangled state of one pair of qubits, denote it $|\mathrm{EPR}_2\rangle$.

Let $|\psi\rangle_{AB}$ be the shared state used by Alice and Bob. We need to find isometries W_A and W_B such that

$$W_A \otimes W_B |\psi\rangle_{AB} = |\mathrm{EPR}_2\rangle_{A_1 B_1} \otimes |\mathrm{aux}\rangle_{A_2 B_2} . \tag{1}$$

How?

Reducing state self-testing to operator self-testing, I

Characterize the maximally entangled state via operators. Notice that $|\eta\rangle = |\mathrm{EPR}_2\rangle$ is the unique solution (up to global phase) to this set of equations:

$$\langle \eta | X \otimes X | \eta \rangle = 1,$$
$$\langle \eta | Z \otimes Z | \eta \rangle = 1.$$

Reducing state self-testing to operator self-testing, II

Let $W = W_A \otimes W_B$. If we want to ensure $W\left|\psi\right\rangle = \left|\mathrm{EPR}_2\right\rangle \otimes \left|\mathrm{aux}\right\rangle$, we can get that by ensuring

$$\langle\psi|W^\dagger(X_{A_1} \otimes X_{B_1} \otimes I_{A_2} \otimes I_{B_2})W|\psi\rangle = 1,$$
$$\langle\psi|W^\dagger(Z_{A_1} \otimes Z_{B_1} \otimes I_{A_2} \otimes I_{B_2})W|\psi\rangle = 1.$$

Reducing state self-testing to operator self-testing, II

Let $W = W_A \otimes W_B$. If we want to ensure $W\,|\psi\rangle = |\mathrm{EPR}_2\rangle \otimes |\mathrm{aux}\rangle$, we can get that by ensuring

$$\langle\psi|W^\dagger(X_{A_1} \otimes X_{B_1} \otimes I_{A_2} \otimes I_{B_2})W|\psi\rangle = 1,$$
$$\langle\psi|W^\dagger(Z_{A_1} \otimes Z_{B_1} \otimes I_{A_2} \otimes I_{B_2})W|\psi\rangle = 1.$$

Now suppose we have operators $\tilde{X}$ and $\tilde{Z}$ such that $X_{A_1} \otimes I_{A_2} = W_A \tilde{X}_A W_A^\dagger$ and $Z_{A_1} \otimes I_{A_2} = W_A \tilde{Z}_A W_A^\dagger$, and similarly for B.

Reducing state self-testing to operator self-testing, III

$X_{A_1} \otimes I_{A_2} = W_A \tilde{X}_A W_A^\dagger$ and $Z_{A_1} \otimes I_{A_2} = W_A \tilde{Z}_A W_A^\dagger$, and similarly for B, so we can substitute in our equation

$$\langle\psi|\tilde{X}_A \otimes \tilde{X}_B|\psi\rangle = 1,$$
$$\langle\psi|\tilde{Z}_A \otimes \tilde{Z}_B|\psi\rangle = 1.$$

Reducing state self-testing to operator self-testing, III

$X_{A_1} \otimes I_{A_2} = W_A \tilde{X}_A W_A^\dagger$ and $Z_{A_1} \otimes I_{A_2} = W_A \tilde{Z}_A W_A^\dagger$, and similarly for B, so we can substitute in our equation

$$\langle \psi | \tilde{X}_A \otimes \tilde{X}_B | \psi \rangle = 1,$$
$$\langle \psi | \tilde{Z}_A \otimes \tilde{Z}_B | \psi \rangle = 1.$$

If we let $\tilde{X}$ and $\tilde{Z}$ be the player's observables, then this equation can be guaranteed by winning a game with probability 1!

Reducing state self-testing to operator self-testing, III

$X_{A_1} \otimes I_{A_2} = W_A \tilde{X}_A W_A^\dagger$ and $Z_{A_1} \otimes I_{A_2} = W_A \tilde{Z}_A W_A^\dagger$, and similarly for B, so we can substitute in our equation

$$\langle\psi|\tilde{X}_A \otimes \tilde{X}_B|\psi\rangle = 1,$$
$$\langle\psi|\tilde{Z}_A \otimes \tilde{Z}_B|\psi\rangle = 1.$$

If we let $\tilde{X}$ and $\tilde{Z}$ be the player's observables, then this equation can be guaranteed by winning a game with probability 1!
To show self-testing, we show that some subset of the player's measurement operators are isometrically equivalent to the Pauli group.

Stability of the Pauli group

The algebraic relations of the Pauli operators determine the Pauli operators up to isometry.

Stability of the Pauli group

The algebraic relations of the Pauli operators determine the Pauli operators up to isometry.

Lemma

Suppose $\tilde{X}$ and $\tilde{Z}$ are operators on Hilbert space $\mathcal{H}$ with $\tilde{X}^2 = \tilde{Z}^2 = I$ and $\tilde{X}\tilde{Z}\tilde{X}\tilde{Z} = -I$. Then there is some isometry $W : \mathcal{H} \to \mathbb{C}^2 \otimes \mathcal{H}_{aux}$ such that $W\tilde{X}W^\dagger = X \otimes I$ and $W\tilde{Z}W^\dagger = Z \otimes I$.

Stability of the Pauli group

The algebraic relations of the Pauli operators determine the Pauli operators up to isometry.

Lemma

Suppose $\tilde{X}$ and $\tilde{Z}$ are operators on Hilbert space $\mathcal{H}$ with $\tilde{X}^2 = \tilde{Z}^2 = I$ and $\tilde{X}\tilde{Z}\tilde{X}\tilde{Z} = -I$. Then there is some isometry $W : \mathcal{H} \to \mathbb{C}^2 \otimes \mathcal{H}_{aux}$ such that $W\tilde{X}W^\dagger = X \otimes I$ and $W\tilde{Z}W^\dagger = Z \otimes I$.

Proof.

Build W "with our bare hands": find an explicit formula for W using sums and products of SWAP operators and projections onto the eigenspaces of $\tilde{X}, \tilde{Z}$. □

Outline

Main self-testing results

Theorem

The magic square game (mod d) self-tests its ideal strategy (which uses the maximally entangled state of local dimension d^2 together with the magic square of operators) with robustness $O(d^6\varepsilon)$.

Main self-testing results

Theorem

The magic square game (mod d) self-tests its ideal strategy (which uses the maximally entangled state of local dimension d^2 together with the magic square of operators) with robustness $O(d^6\varepsilon)$. Same for the magic pentagram, testing a state of dimension d^3.

Main self-testing results

Theorem

The magic square game (mod d) self-tests its ideal strategy (which uses the maximally entangled state of local dimension d^2 together with the magic square of operators) with robustness $O(d^6\varepsilon)$. Same for the magic pentagram, testing a state of dimension d^3.

Theorem

For integer n and d, there is an LCS game with $O(n^2)$ variables and equations self-testing its ideal strategy with robustness $O(d^6 n^{10}\varepsilon)$. (The game is a product of squares and pentagrams.)

Main self-testing results

Theorem

The magic square game (mod d) self-tests its ideal strategy (which uses the maximally entangled state of local dimension d^2 together with the magic square of operators) with robustness $O(d^6\varepsilon)$. Same for the magic pentagram, testing a state of dimension d^3.

Theorem

For integer n and d, there is an LCS game with $O(n^2)$ variables and equations self-testing its ideal strategy with robustness $O(d^6 n^{10}\varepsilon)$. (The game is a product of squares and pentagrams.) The strategy uses the maximally entangled state of local dimension d^n and observables which are n-qudit Paulis of weight at most 5.

Proof sketch.

- Show that a winning strategy for an LCS game is an *approximate operator solution* to the system of equations.

□

Proof sketch.

- Show that a winning strategy for an LCS game is an *approximate operator solution* to the system of equations.
- Show that approximate operator solutions are *approximate representations* of the game's *solution group* Γ.

$\square$

Proof sketch.

- Show that a winning strategy for an LCS game is an *approximate operator solution* to the system of equations.
- Show that approximate operator solutions are *approximate representations* of the game's *solution group* Γ.
- Show that every approximate representation of the solution group Γ is close to an exact representation of Γ. (This requires Γ to be finite.)

□

Proof sketch.

- Show that a winning strategy for an LCS game is an *approximate operator solution* to the system of equations.
- Show that approximate operator solutions are *approximate representations* of the game's *solution group* Γ.
- Show that every approximate representation of the solution group Γ is close to an exact representation of Γ. (This requires Γ to be finite.)
- Compute the solution group Γ of the game in question.

$\square$

Proof sketch.

- Show that a winning strategy for an LCS game is an *approximate operator solution* to the system of equations.
- Show that approximate operator solutions are *approximate representations* of the game's *solution group* Γ.
- Show that every approximate representation of the solution group Γ is close to an exact representation of Γ. (This requires Γ to be finite.)
- Compute the solution group Γ of the game in question.
- Show that only one exact representation of Γ serves as a winning strategy for the game.

□

Defining the solution group

We want to study the class of all sets of nine operators obeying the relations of the magic square. We forget the operators and focus on the multiplicative relations.

Defining the solution group

We want to study the class of all sets of nine operators obeying the relations of the magic square. We forget the operators and focus on the multiplicative relations.

The solution group Γ is given by

$$\Gamma = \langle S \mid R_{\text{equation}} \cup R_{\text{commutation}} \rangle, S = \{e_1, e_2, \ldots, e_9\}$$
$$R_{\text{equation}} = \left\{ e_1 e_2 e_3 = 1, \ldots e_3 e_6 e_9 = 1; e_1^d = 1, \ldots e_9^d = 1 \right\}$$
$$R_{\text{commutation}} = \{[e_1, e_2] = 1, [e_1, e_3] = 1, [e_2, e_3] = 1, \ldots\}$$

The elements of the group are finite strings of the letters e_i and their inverses e_i^{-1}. We allow to cancel words according to the equations in R.

Defining the solution group

We want to study the class of all sets of nine operators obeying the relations of the magic square. We forget the operators and focus on the multiplicative relations.
The solution group Γ is given by

$$\Gamma = \langle S \mid R_{\text{equation}} \cup R_{\text{commutation}} \rangle , S = \{e_1, e_2, \ldots, e_9\}$$
$$R_{\text{equation}} = \left\{ e_1 e_2 e_3 = 1, \ldots e_3 e_6 e_9 = 1; e_1^d = 1, \ldots e_9^d = 1 \right\}$$
$$R_{\text{commutation}} = \{[e_1, e_2] = 1, [e_1, e_3] = 1, [e_2, e_3] = 1, \ldots\}$$

The elements of the group are finite strings of the letters e_i and their inverses e_i^{-1}. We allow to cancel words according to the equations in R.
A *representation* of the solution group is a Hilbert space together with an assignment to each letter an operator on that Hilbert space. This is what we called an "operator solution" before.

Approximate representations

We could assign to each letter an operator, but not have the equations satisfied exactly. But if we satisfy them approximately, as in

$$\|A_1 A_2 A_3 - I\| \leq \varepsilon, \tag{2}$$

this will still allow us to succeed in the game.

A stability theorem for finite groups

Theorem ([GH15], [Vid17])

Let G be a finite group. Let ρ be a state on the Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$. Suppose that $f : G \to U(\mathcal{H}_A)$ be an "ε-approximate representation with respect to ρ", i.e.

$$\mathbb{E}_{x,y\in G} \left\| \left(f(x)f(y) \otimes I_B - f(xy) \otimes I_B \right) \sqrt{\rho} \right\|_2 \leq \varepsilon. \qquad (3)$$

A stability theorem for finite groups

Theorem ([GH15], [Vid17])

Let G be a finite group. Let ρ be a state on the Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$. Suppose that $f : G \to U(\mathcal{H}_A)$ be an "ε-approximate representation with respect to ρ", i.e.

$$\mathbb{E}_{x,y \in G} \left\| \left(f(x)f(y) \otimes I_B - f(xy) \otimes I_B \right) \sqrt{\rho} \right\|_2 \leq \varepsilon. \tag{3}$$

Then there is an isometry $V : \mathcal{H}_A \to \mathcal{H}_{A'}$ and an exact representation $\tau : G \to U(\mathcal{H}_{A'})$ such that

$$\mathbb{E}_x \left\| \left(f(x) \otimes I_B - V^\dagger \tau(x) V \otimes I_B \right) \sqrt{\rho} \right\|_2 \leq \varepsilon. \tag{4}$$

Stability theorem applied to one-qubit Paulis

Let $G = \{I, X, Z, XZ, -I, -X, -Z, -XZ\}$ be the one-qubit Weyl group. Suppose we have a operators $\tilde{X}, \tilde{Z}$ satisfying $\tilde{X}^2 \approx_\varepsilon I$, $\tilde{Z}^2 \approx_\varepsilon I$, and $\tilde{X}\tilde{Z}\tilde{X}\tilde{Z} \approx_\varepsilon -I$.

Stability theorem applied to one-qubit Paulis

Let $G = \{I, X, Z, XZ, -I, -X, -Z, -XZ\}$ be the one-qubit Weyl group. Suppose we have a operators $\tilde{X}, \tilde{Z}$ satisfying $\tilde{X}^2 \approx_\varepsilon I$, $\tilde{Z}^2 \approx_\varepsilon I$, and $\tilde{X}\tilde{Z}\tilde{X}\tilde{Z} \approx_\varepsilon -I$.
Define $f : G \to U(\mathbb{C}^d)$ starting with $f(I) = I$, $f(X) = \tilde{X}$, $f(Z) = \tilde{Z}$.

Stability theorem applied to one-qubit Paulis

Let $G = \{I, X, Z, XZ, -I, -X, -Z, -XZ\}$ be the one-qubit Weyl group. Suppose we have a operators $\tilde{X}, \tilde{Z}$ satisfying $\tilde{X}^2 \approx_\varepsilon I$, $\tilde{Z}^2 \approx_\varepsilon I$, and $\tilde{X}\tilde{Z}\tilde{X}\tilde{Z} \approx_\varepsilon -I$.
Define $f : G \to U(\mathbb{C}^d)$ starting with $f(I) = I$, $f(X) = \tilde{X}$, $f(Z) = \tilde{Z}$.
Extend f to all of G in some fashion:

$$f(XZ) = \tilde{X}\tilde{Z} \qquad f(-I) = \tilde{X}\tilde{Z}\tilde{X}\tilde{Z}$$

$$f(-X) = (\tilde{X}\tilde{Z}\tilde{X}\tilde{Z})\tilde{X} \qquad f(-Z) = (\tilde{X}\tilde{Z}\tilde{X}\tilde{Z})\tilde{Z}$$

$$f(-XZ) = (\tilde{X}\tilde{Z}\tilde{X}\tilde{Z})\tilde{X}\tilde{Z}$$

Stability theorem applied to one-qubit Paulis

Let $G = \{I, X, Z, XZ, -I, -X, -Z, -XZ\}$ be the one-qubit Weyl group. Suppose we have a operators $\tilde{X}, \tilde{Z}$ satisfying $\tilde{X}^2 \approx_\varepsilon I$, $\tilde{Z}^2 \approx_\varepsilon I$, and $\tilde{X}\tilde{Z}\tilde{X}\tilde{Z} \approx_\varepsilon -I$.
Define $f : G \to U(\mathbb{C}^d)$ starting with $f(I) = I$, $f(X) = \tilde{X}$, $f(Z) = \tilde{Z}$.
Extend f to all of G in some fashion:

$$f(XZ) = \tilde{X}\tilde{Z} \qquad f(-I) = \tilde{X}\tilde{Z}\tilde{X}\tilde{Z}$$
$$f(-X) = (\tilde{X}\tilde{Z}\tilde{X}\tilde{Z})\tilde{X} \qquad f(-Z) = (\tilde{X}\tilde{Z}\tilde{X}\tilde{Z})\tilde{Z}$$
$$f(-XZ) = (\tilde{X}\tilde{Z}\tilde{X}\tilde{Z})\tilde{X}\tilde{Z}$$

Check that all 64 equations of the form $f(x)f(y) \approx_\eta f(xy)$ hold with $\eta \leq 16\varepsilon$.

Outline

1. Motivation
   - The magic square
   - A conventional self-testing proof
2. Techniques
3. Open Questions

Better self-testing results with finite group theory

Any finite solution group with well-understood representation theory can be analyzed with these tools. Do any of them give self-testing results with better robustness?

Better self-testing results with finite group theory

Any finite solution group with well-understood representation theory can be analyzed with these tools. Do any of them give self-testing results with better robustness?
Conversely, can we use structure theorems about group representations to give no-go theorems?

Better self-testing results with finite group theory

Any finite solution group with well-understood representation theory can be analyzed with these tools. Do any of them give self-testing results with better robustness?
Conversely, can we use structure theorems about group representations to give no-go theorems?

Question

- *Exhibit a family of LCS games self-testing high-dimensional entanglement with constant completeness soundness gap, (reproving results of Natarajan and Vidick) or*

Better self-testing results with finite group theory

Any finite solution group with well-understood representation theory can be analyzed with these tools. Do any of them give self-testing results with better robustness?
Conversely, can we use structure theorems about group representations to give no-go theorems?

Question

- *Exhibit a family of LCS games self-testing high-dimensional entanglement with constant completeness soundness gap, (reproving results of Natarajan and Vidick) or*
- *Show that no family of LCS games satisfies the games qPCP conjecture.*

Structure of pseudotelepathy games

- Any LCS game which is pseudotelepathy must use a maximally entangled state for its winning strategies. [CM14] Are there two-prover pseudotelepathy games using different states?

Structure of pseudotelepathy games

- Any LCS game which is pseudotelepathy must use a maximally entangled state for its winning strategies. [CM14] Are there two-prover pseudotelepathy games using different states?
- We give two-player pseudotelepathy games with minimum dimension d^n for $d, n \geq 2$. [Cle+04] gives a two-player pseudotelepathy game with minimum dimension 3.

Structure of pseudotelepathy games

- Any LCS game which is pseudotelepathy must use a maximally entangled state for its winning strategies. [CM14] Are there two-prover pseudotelepathy games using different states?
- We give two-player pseudotelepathy games with minimum dimension d^n for $d, n \geq 2$. [Cle+04] gives a two-player pseudotelepathy game with minimum dimension 3.

  Is there such a game for prime dimension $p > 3$?

Structure of pseudotelepathy games

- Any LCS game which is pseudotelepathy must use a maximally entangled state for its winning strategies. [CM14] Are there two-prover pseudotelepathy games using different states?
- We give two-player pseudotelepathy games with minimum dimension d^n for $d, n \geq 2$. [Cle+04] gives a two-player pseudotelepathy game with minimum dimension 3.

  Is there such a game for prime dimension $p > 3$?

  How about dimension 6?

Structure of pseudotelepathy games

- Any LCS game which is pseudotelepathy must use a maximally entangled state for its winning strategies. [CM14] Are there two-prover pseudotelepathy games using different states?
- We give two-player pseudotelepathy games with minimum dimension d^n for $d, n \geq 2$. [Cle+04] gives a two-player pseudotelepathy game with minimum dimension 3.

  Is there such a game for prime dimension $p > 3$?

  How about dimension 6?
- Can we use representation-theoretic ideas to get self-testing for multi-prover games, e.g. with the LME construction of van Raamsdonk?

Algebraic self-testing outside of finite groups

- [DCOT17] prove a stability theorem for (infinite) amenable groups. Do any such groups correspond to self-testing linear constraint games?

Algebraic self-testing outside of finite groups

- [DCOT17] prove a stability theorem for (infinite) amenable groups. Do any such groups correspond to self-testing linear constraint games?
- Applying the solution group construction to games which are not linear constraint games yield solution *algebras* which are not necessarily group algebras. E.g. [LMR17] construct algebras related to graph isomorphism games. Can we understand self-testing for these games by representations of these algebras?

Questions?