Concluding remark

- Note that there is a natural isomorphism between states of $n$ pairs of qubits and states of a single pair of qu-Dits, for $D = 2^n$.

- If we are able to self-test $|\psi\rangle = \bigotimes_{i=1}^{n} \left( \cos \theta_i |00\rangle + \sin \theta_i |11\rangle \right)$, then we can also self-test some state of a single pair of qu-Dits.

- Hence, as a corollary of our result, we deduce that we can self-test an $n$ dimensional subfamily of the family of all partially entangled states of two qu-Dits, for $D = 2^n$.

- With a different approach, C. & Goh & Scarani show that all pure bipartite entangled states can be self-tested\textsuperscript{8}.

THANK YOU!

---

\textsuperscript{8}A. Coladangelo, K. T. Goh and V. Scarani (2016). All pure bipartite entangled states can be self-tested.
Rigidity of The Parallel Repeated Magic Square Game

Matthew Coudron, Anand Natarajan
MIT EECS/CSAIL, MIT CTP
QIP ‘17
The Magic Square Game

### Game Description

The Magic Square Game is a two-player game played on a $3 \times 3$ grid. Each player, $A$ and $B$, plays a move by placing tokens on the grid. The objective is to create a magical configuration where the sum of the tokens in any row, column, or diagonal equals a certain value.

### Game Mechanics

- **Tokens**: Two types of tokens are used, represented by $a$ and $b$.
- **Player Moves**: Player $A$ moves first, followed by player $B$, and so on.
- **Winning Condition**: The game ends when a player cannot make a move. The game is won by the player whose tokens create the magic configuration first.

### Game Parameters

- **Input**: A set of moves, $V(a,b|x,y)$, where $x$ and $y$ are the move coordinates.
- **Output**: A decision function $\text{V}(a,b|x,y)$ indicating the validity of a move under the current state.

### Example Move

- **Move**: $\text{V}(a,b|x,y)$
- **Result**: The move is valid if $a$ and $b$ satisfy the magic condition for the grid.

### Grid Layout

<table>
<thead>
<tr>
<th></th>
<th>Column 1</th>
<th>Column 2</th>
<th>Column 3</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Row 1</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Row 2</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Row 3</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Each row, column, and diagonal must sum to the magic constant for the game to be won.
The Magic Square Game

<table>
<thead>
<tr>
<th>Column 1</th>
<th>Column 2</th>
<th>Column 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Row 1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Row 2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Row 3</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

\[ V(a, b | x, y) \]
The Magic Square Game

\[ V(a,b|x,y) \]
The Magic Square Game

A

B

\[ V(a,b|x,y) \]

\[
\begin{array}{ccc}
\text{Row 1} & \text{Column 1} & \text{Column 2} & \text{Column 3} \\
\text{Row 2} &          &          &          \\
\text{Row 3} &          & 1        & 1        \\
\end{array}
\]
The Magic Square Game

<table>
<thead>
<tr>
<th></th>
<th>Column 1</th>
<th>Column 2</th>
<th>Column3</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Row 1</strong></td>
<td></td>
<td></td>
<td>-1</td>
</tr>
<tr>
<td><strong>Row 2</strong></td>
<td></td>
<td>1</td>
<td></td>
</tr>
<tr>
<td><strong>Row 3</strong></td>
<td>1</td>
<td>1</td>
<td>-1</td>
</tr>
</tbody>
</table>
The Magic Square Game: The Ideal Strategy

<table>
<thead>
<tr>
<th></th>
<th>Column 1</th>
<th>Column 2</th>
<th>Column 3</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Row 1</strong></td>
<td>$I \otimes \sigma_Z$</td>
<td>$\sigma_Z \otimes I$</td>
<td>$-\sigma_Z \otimes \sigma_Z$</td>
</tr>
<tr>
<td><strong>Row 2</strong></td>
<td>$\sigma_X \otimes I$</td>
<td>$I \otimes \sigma_X$</td>
<td>$-\sigma_X \otimes \sigma_X$</td>
</tr>
<tr>
<td><strong>Row 3</strong></td>
<td>$\sigma_X \otimes \sigma_Z$</td>
<td>$\sigma_Z \otimes \sigma_X$</td>
<td>$-\sigma_Y \otimes \sigma_Y$</td>
</tr>
</tbody>
</table>
Main Theorem

Rigidity of the $n$-round parallel repetition of the Magic Square game:

$$V(a^\otimes n, b^\otimes n \mid x^\otimes n y^\otimes n)$$
Main Theorem

Rigidity of the \( n \)-round parallel repetition of the Magic Square game:

- For any entangled strategy succeeding with probability \( 1 - \varepsilon \), the players’ shared state is \( O(\text{poly}(n\varepsilon)) \)-close to \( 2n \) EPR pairs under a local isometry.
Main Theorem

Rigidity of the n-round parallel repetition of the Magic Square game:

• For any entangled strategy succeeding with probability $1 - \epsilon$, the players’ shared state is $O(\text{poly}(n\epsilon))$-close to $2n$ EPR pairs under a local isometry.

• Furthermore, under local isometry, the players’ measurements must be $O(\text{poly}(n\epsilon))$-close to the “ideal” measurements when acting on the shared state.
Motivation

Rigidity Theorems and self-testing results are a critical component of many results in Quantum Information:
Motivation

Rigidity Theorems and self-testing results are a critical component of many results in Quantum Information:
  • Device independent protocols: QKD and randomness expansion ([VV12, CY13])
Motivation

Rigidity Theorems and self-testing results are a critical component of many results in Quantum Information:

- Device independent protocols: QKD and randomness expansion ([VV12, CY13])
- Interactive proofs for the local Hamiltonian problem ([FV14, NV16])
Rigidity Theorems and self-testing results are a critical component of many results in Quantum Information:

- Device independent protocols: QKD and randomness expansion ([VV12, CY13])
- Interactive proofs for the local Hamiltonian problem ([FV14, NV16])
- Delegating Quantum Computation for a classical verifier ([RUV12, NV16])
Background and Intuition

- Self-testing results for large games established in by McKague [McK15- “Self-testing in Parallel”]
Background and Intuition

• Self-testing results for large games established in by McKague [McK15- “Self-testing in Parallel”]
  • Gives a self-test for $n$ EPR pairs, with polynomial error dependence
Background and Intuition

• Self-testing results for large games established in by McKague [McK15- “Self-testing in Parallel”]
  • Gives a self-test for \( n \) EPR pairs, with polynomial error dependence
  • Gives a result for verifying \( n \)-qubit Pauli measurements, with exponential error dependence

\[ V(a \otimes n, b \otimes n | x \otimes n, y \otimes n) \]
Background and Intuition

- Self-testing results for large games established in by McKague [McK15- “Self-testing in Parallel”]
  - Gives a self-test for n EPR pairs, with polynomial error dependence
  - Gives a result for verifying n-qubit Pauli measurements, with exponential error dependence
- Improvement of classical verifier result to polynomial error dependence is prerequisite for applications in:

$$V(a^\otimes n, b^\otimes n \mid x^\otimes n y^\otimes n)$$
Background and Intuition

• Self-testing results for large games established in by McKague [McK15- “Self-testing in Parallel”]
  • Gives a self-test for n EPR pairs, with polynomial error dependence
  • Gives a result for verifying n-qubit Pauli measurements, with exponential error dependence

• Improvement of classical verifier result to polynomial error dependence is prerequisite for applications in:
  • Device independent protocols: QKD and randomness expansion

\[ V(a^\otimes n, b^\otimes n | x^\otimes n y^\otimes n) \]
Background and Intuition

• Self-testing results for large games established in by McKague [McK15- “Self-testing in Parallel”]
  • Gives a self-test for n EPR pairs, with polynomial error dependence
  • Gives a result for verifying n-qubit Pauli measurements, with exponential error dependence

• Improvement of classical verifier result to polynomial error dependence is prerequisite for applications in:
  • Device independent protocols: QKD and randomness expansion
  • Interactive proofs for the local Hamiltonian problem

\[ V(a \otimes n, b \otimes n \mid x \otimes n, y \otimes n) \]
Background and Intuition

- Self-testing results for large games established in by McKague [McK15- “Self-testing in Parallel”]
  - Gives a self-test for n EPR pairs, with polynomial error dependence
  - Gives a result for verifying n-qubit Pauli measurements, with exponential error dependence
- Improvement of classical verifier result to polynomial error dependence is prerequisite for applications in:
  - Device independent protocols: QKD and randomness expansion
  - Interactive proofs for the local Hamiltonian problem
  - Delegating Quantum Computation for a classical verifier
Proof Structure

Theorem A: Commutation and Anti-Commutation
Proof Structure

Theorem A: Commutation and Anti-Commutation

There exists a method for assembling Alice’s projectors into unitaries $\tilde{A}_{r,k}^c$ (resp. $\tilde{B}_{r,k}^c$), for $k \in [n]$ such that:

$V(a \otimes n, b \otimes n | x \otimes n, y \otimes n)$
Proof Structure

Theorem A: Commutation and Anti-Commutation
There exists a method for assembling Alice’s projectors into unitaries $\tilde{A}_{r,k}^c$ (resp. $\tilde{B}_{r,k}^c$), for $k \in [n]$ such that:

$$d_{\psi'}(\tilde{A}_{r,k}^c, \tilde{A}_{r',k'}^c, (-1)^{f(r,r',c,c')} \tilde{A}_{r',k}^c, \tilde{A}_{r,k}^c) \leq O(\sqrt{\epsilon})$$

and

$$d_{\psi'}(\tilde{A}_{r,k}^c, \tilde{A}_{r',k'}^c, \tilde{A}_{r',k'}^c, \tilde{A}_{r,k}^c) \leq O(\sqrt{\epsilon})$$
Theorem B: The Isometry
Proof Structure

Theorem B: The Isometry

• There exist unitary operators $W^A_{s,t}, W^B_{u,v}$ constructed from the $\tilde{A}_{r,k}^c$ and $\tilde{B}_{r,k}^c$ respectively.
Proof Structure

Theorem B: The Isometry

- There exist unitary operators $W^A_{s,t}$, $W^B_{u,v}$ constructed from the $\tilde{A}^c_{r,k}$ and $\tilde{B}^c_{r,k}$ respectively.
- And, there exists and isometry $V : \mathcal{H} \rightarrow \mathcal{H} \otimes \mathbb{C}^{2n} \otimes \mathbb{C}^{2n} \otimes \mathbb{C}^{2n} \otimes \mathbb{C}^{2n}$ and $|\phi\rangle \equiv V(|\psi\rangle)$ such that:

$$\left| \langle \phi | \sigma^A_X(s) \sigma^A_Z(t) \sigma^B_X(u) \sigma^B_Z(v) |\phi\rangle - \langle \psi | W^A_{s,t} W^B_{u,v} |\psi\rangle \right| \leq O(n^2 \sqrt{\varepsilon}).$$
Proof Structure

Theorem B: The Isometry

- There exist unitary operators $W^A_{s,t}$, $W^B_{u,v}$ constructed from the $\tilde{A}_{r,k}^c$ and $\tilde{B}_{r,k}^c$ respectively.
- And, there exists and isometry $V : \mathcal{H} \to \mathcal{H} \otimes \mathbb{C}^{2n} \otimes \mathbb{C}^{2n} \otimes \mathbb{C}^{2n} \otimes \mathbb{C}^{2n}$ and $|\phi\rangle \equiv V(|\psi\rangle)$ such that:

$$\left| \langle \phi | \sigma^A_X(s) \sigma^A_Z(t) \sigma^B_X(u) \sigma^B_Z(v) | \phi \rangle - \langle \psi | W^A_{s,t} W^B_{u,v} | \psi \rangle \right| \leq O(n^2 \sqrt{\varepsilon}).$$

- This type of isometry was pioneered in works of McKague [McKague16], [Wu, Bancal, McKague, Scarani 16]
Theorem B: The Isometry

- There exist unitary operators $W^A_{s,t}$, $W^B_{u,v}$ constructed from the $\tilde{A}^C_{r,k}$ and $\tilde{B}^C_{r,k}$ respectively.
- And, there exists an isometry $V : \mathcal{H} \rightarrow \mathcal{H} \otimes \mathbb{C}^{2n} \otimes \mathbb{C}^{2n} \otimes \mathbb{C}^{2n} \otimes \mathbb{C}^{2n}$ and $|\phi\rangle \equiv V(|\psi\rangle)$ such that:

$$\left|\langle \phi | \sigma^A_X(s)\sigma^A_Z(t)\sigma^B_X(u)\sigma^B_Z(v)|\phi\rangle - \langle \psi | W^A_{s,t}W^B_{u,v}|\psi\rangle\right| \leq O(n^2 \sqrt{\varepsilon}).$$

- This type of isometry was pioneered in works of McKague [McKague16], [Wu, Bancal, McKague, Scarani 16].
- This theorem overlaps with [Chao, Reichardt, Sutherland, Vidick 16].
Conclusion

• Rigidity theorem for the parallel repeated magic square game which:

\[ V(a \otimes n, b \otimes n \mid x \otimes n y \otimes n) \]
Conclusion

• Rigidity theorem for the parallel repeated magic square game which:
  • Self-tests $n$ EPR pairs with polynomial error dependence

\[
V(a \otimes n, b \otimes n \mid x \otimes n y \otimes n)
\]
Conclusion

• Rigidity theorem for the parallel repeated magic square game which:
  • Self-tests n EPR pairs with polynomial error dependence
  • Certifies Pauli-product measurements with polynomial error dependence
Conclusion

• Rigidity theorem for the parallel repeated magic square game which:
  • Self-tests n EPR pairs with polynomial error dependence
  • Certifies Pauli-product measurements with polynomial error dependence

• Open Problems:
Conclusion

• Rigidity theorem for the parallel repeated magic square game which:
  • Self-tests n EPR pairs with polynomial error dependence
  • Certifies Pauli-product measurements with polynomial error dependence

• Open Problems:
  • Reduce error dependence – [NV16]
Conclusion

• Rigidity theorem for the parallel repeated magic square game which:
  • Self-tests \( n \) EPR pairs with polynomial error dependence
  • Certifies Pauli-product measurements with polynomial error dependence

• Open Problems:
  • Reduce error dependence – [NV16]
  • Reduce input size – [CRSV16]
Conclusion

- Rigidity theorem for the parallel repeated magic square game which:
  - Self-tests n EPR pairs with polynomial error dependence
  - Certifies Pauli-product measurements with polynomial error dependence

- Open Problems:
  - Reduce error dependence – [NV16]
  - Reduce input size –[CRSV16]
  - Do both at the same time --- OPEN
Conclusion

• Rigidity theorem for the parallel repeated magic square game which:
  • Self-tests n EPR pairs with polynomial error dependence
  • Certifies Pauli-product measurements with polynomial error dependence

• Open Problems:
  • Reduce error dependence – [NV16]
  • Reduce input size – [CRSV16]
  • Do both at the same time --- OPEN
  • More applications to delegated quantum computation or interactive proofs for local Hamiltonian, randomness expansion.