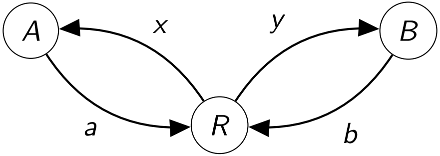
Glued magic games self-test maximally entangled states

Thor Gabelgaard Nielsen

28th June 2021

This presentation is based on [MNP21], which is co-authored with Laura Mančinska and Jitendra Prakash.

Nonlocal games



- A nonlocal game $G = (X, Y, A, B, V, \pi)$ is a cooperatively played game between two provers and a referee as follows:
- The referee selects a question pair (x, y) at random and sends it to the provers.
- Alice receives x, and Bob y, and are then not allowed to communicate in any way.
- They each send back their responses a and b, and the referee determine if they win.

The Magic Square game

- Consider a 3×3 board, which should be filled in so all rows and columns have even sum, except for the rightmost column.
  - A claimed solution can be tested using a nonlocal game.
  - One row/column is sent to Alice, one entry to Bob.
  - They win if Alice's assignments are satisfying, and are consistent with Bob's.
  - A perfect deterministic strategy is equivalent to a satisfying assignment.

e_1	e_2	e_3
e_4	e_5	e_6
e_7	e_8	e_9

- This can be interpreted as a system of equations over $\mathbb{Z}/2\mathbb{Z}$:

$$
\begin{aligned}
e_1 + e_2 + e_3 &= 0 & \qquad e_1 + e_4 + e_7 &= 0 \\
e_4 + e_5 + e_6 &= 0 & \qquad e_2 + e_5 + e_8 &= 0 \\
e_7 + e_8 + e_9 &= 0 & \qquad e_3 + e_6 + e_9 &= 1
\end{aligned}
$$

$$
\begin{tikzcd}
e_1 \arrow[r, dash] \arrow[d, dash] & e_2 \arrow[r, dash] \arrow[d, dash] & e_3 \arrow[d, dash, dashed] \\
e_4 \arrow[r, dash] \arrow[d, dash] & e_5 \arrow[r, dash] \arrow[d, dash] & e_6 \arrow[d, dash, dashed] \\
e_7 \arrow[r, dash] & e_8 \arrow[r, dash] & e_9
\end{tikzcd}
$$

Linear constraint system games

- Consider a system of linear equations in $e_1, \ldots, e_k$ over $\mathbb{Z}/2\mathbb{Z}$:

$$\sum_{j=1}^{k} \alpha_{i,j} e_j = \beta_i, \quad i \in [n].$$

- As with the Magic Square, we can define a corresponding nonlocal game:
  - Alice receives an equation, which she fills in.
  - Bob receives a variable, which he assigns a value to.
  - They win if the equation is true, and their assignment is consistent.
- Observe one can reformulate the equations multiplicatively, by the identification $\{0,1\} \ni b \mapsto (-1)^b$:

$$\prod_{j=1}^{k} e_j^{\alpha_{i,j}} = (-1)^{\beta_i}, i \in [n].$$

Strategies for nonlocal games

Definition (Quantum strategy)

Suppose $G = (X, Y, A, B, V, \pi)$ is a binary LCS game. A *quantum strategy* consists of a state and two sets of measurements given by observables,

$$\mathcal{S} = \left(|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B, \left\{ A_i^{(x)} \;\middle|\; x \in X \right\}_{i \in A}, \{B_j\}_{j \in B} \right),$$

where $\mathcal{H}_A$ and $\mathcal{H}_B$ are (possibly infinite dimensional) Hilbert spaces. Alice successively uses $A_1^{(x)}, \ldots, A_k^{(x)}$ to assign values to each variable, while Bob only uses B_j to determine his answer.

- For a perfect quantum strategy for a BLCS game, [CM14] found that:
  - $A_i^{(x)} = A_i^{(x')}$ for all $x, x' \in X$. Thus, we set $A_i := A_i^{(x)}$ for some x.
  - If e_i and e_j appear in the same equation, $[A_i, A_j] = 0 = [B_i, B_j]$.
  - The operators $\{A_i\}_i$ (resp. $\{B_j\}_j$) satisfy the equations of the game when written multiplicatively.

Convex combinations of strategies

Definition

Suppose for each $k \in [n]$ that $\mathcal{S}_k = \left(\left| \psi^{(k)} \right\rangle, \left\{ A_i^{(k)} \right\}_i, \left\{ B_j^{(k)} \right\}_j \right)$ are quantum strategies for some nonlocal game G, and $\{\alpha_k\}_{k=1}^n \subseteq [0,1]$ is a set of scalars satisfying $\sum_{k=1}^n \alpha_k^2 = 1$. The *corresponding convex combination* is the quantum strategy

$$\mathcal{S} := \sum_{k=1}^n \alpha_k \mathcal{S}_k := \left(|\psi\rangle, \{A_i\}_i, \{B_j\}_j \right),$$

where the state and the observables are given by

$$|\psi\rangle = \bigoplus_{k=1}^n \alpha_k \left| \psi^{(k)} \right\rangle, \qquad A_i = \bigoplus_{k=1}^n A_i^{(k)}, \qquad B_j = \bigoplus_{k=1}^n B_j^{(k)}.$$

Local dilations

Definition (Local dilation, [MPS21])

Suppose $\mathcal{S} = (|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B, \{A_i\}_i, \{B_j\}_j)$ and $\tilde{\mathcal{S}} = \left(\left|\tilde{\psi}\right\rangle \in \tilde{\mathcal{H}}_A \otimes \tilde{\mathcal{H}}_B, \{\tilde{A}_i\}_i, \{\tilde{B}_j\}_j\right)$ are two quantum strategies having the same number of observables for each party. We say that $\tilde{\mathcal{S}}$ is *a local dilation of* $\mathcal{S}$ if there exist Hilbert spaces $\mathcal{H}_{A,aux}$ and $\mathcal{H}_{B,aux}$, a state $|aux\rangle \in \mathcal{H}_{A,aux} \otimes \mathcal{H}_{B,aux}$ and isometries $U_A : \mathcal{H}_A \to \tilde{\mathcal{H}}_A \otimes \mathcal{H}_{A,aux}$ and $U_B : \mathcal{H}_A \to \tilde{\mathcal{H}}_B \otimes \mathcal{H}_{B,aux}$ such that with $U := U_A \otimes U_B$ it holds that for all i and j,

$$U\,|\psi\rangle = \left|\tilde{\psi}\right\rangle \otimes |aux\rangle\,,$$

$$U\,(A_i \otimes I)\,|\psi\rangle = \left(\tilde{A}_i \otimes I\right)\left|\tilde{\psi}\right\rangle \otimes |aux\rangle\,,$$

$$U\,(I \otimes B_j)\,|\psi\rangle = \left(I \otimes \tilde{B}_j\right)\left|\tilde{\psi}\right\rangle \otimes |aux\rangle\,.$$

Self-testing

Definition (Self-testing)

A nonlocal game G is a *self-test* for the ideal strategy $\tilde{\mathcal{S}}$ achieving the optimal quantum value, if for any other quantum strategy $\mathcal{S}$ achieving the optimal quantum value, $\tilde{\mathcal{S}}$ is a local dilation of $\mathcal{S}$.

- Allows one to completely characterise the possible optimal strategies.
- A common weaker result is that the above holds only for the state.
- Has two major limitations: Difficult to show, and does not apply for more than one optimal strategy.

Definition (Convex self-testing)

A nonlocal game G is a *convex self-test* for the ideal quantum strategies $\tilde{\mathcal{S}}_1, \ldots, \tilde{\mathcal{S}}_n$, if for any quantum strategy $\mathcal{S}$ achieving the optimal quantum value of G, there exists coefficients $\{\alpha_k\}_{k=1}^n \subseteq [0, 1]$ and a decomposition of $\mathcal{S}$ into the internal convex combination $\sum_{k=1}^n \alpha_k \mathcal{S}_k$ such that each of $\tilde{\mathcal{S}}_k$ is a local dilation of $\mathcal{S}_k$.

Self-testing

Theorem (Self-testing of Magic Square, [WBMS16])

The Magic Square game self-tests its ideal strategy $\mathcal{S}_{MS}$ which consists of nine observables for each party along with the state $|\psi_4\rangle = \frac{1}{2}\sum_{i=0}^{3}|ii\rangle$.

- Implies there exists a set of operators $\{A_i\}_{i\in[9]}$ satisfying the constraints of the game.

$$\begin{tikzcd}
A_1 \arrow[r, dash] \arrow[d, dash] & A_2 \arrow[r, dash] \arrow[d, dash] & A_3 \arrow[d, dash, dashed] \\
A_4 \arrow[r, dash] \arrow[d, dash] & A_5 \arrow[r, dash] \arrow[d, dash] & A_6 \arrow[d, dash, dashed] \\
A_7 \arrow[r, dash] & A_8 \arrow[r, dash] & A_9
\end{tikzcd}$$

Glued Magic Square

- If G and H are BLCS games each with one equation summing to 1, we can construct a new game by coalescing these two constraints to a single summing to 1.
  - Generalisation of the Glued Magic Square from [Cui+20].

$$
\begin{tikzcd}
e_1 \arrow[r, dash] \arrow[d, dash] & e_2 \arrow[r, dash] \arrow[d, dash] & e_3 \arrow[d, dash, dashed] & & \\
e_4 \arrow[r, dash] \arrow[d, dash] & e_5 \arrow[r, dash] \arrow[d, dash] & e_6 \arrow[d, dash, dashed] & & \\
e_7 \arrow[r, dash] & e_8 \arrow[r, dash] & e_9 \arrow[d, dash, dashed] & & \\
& & e_{10} \arrow[r, dash] \arrow[d, dash, dashed] & e_{11} \arrow[r, dash] \arrow[d, dash] & e_{12} \arrow[d, dash] \\
& & e_{13} \arrow[r, dash] \arrow[d, dash, dashed] & e_{14} \arrow[r, dash] \arrow[d, dash] & e_{15} \arrow[d, dash] \\
& & e_{16} \arrow[r, dash] & e_{17} \arrow[r, dash] & e_{18}
\end{tikzcd}
$$

Glued Magic Square

A note about some perfect strategies

- If $\left(|\psi\rangle, \{\tilde{A}_i\}_{i\in[9]}, \{\tilde{B}_j\}_{j\in[9]}\right)$ is a perfect strategy for Magic Square, then one obtains a perfect one for GMS by setting $\tilde{A}_i := \tilde{B}_i := I$, for $I \in \{10, \ldots, 18\}$.
  - This was originally observed in [Cui+20].
- Another perfect strategy appears by symmetry: Pairwisely swap operators for e_i and e_{19-i} (i.e. play Magic Square on the other Magic Square part).
- A different type of perfect strategy appears by taking a convex combination of the two previous ones.
  - An ad-hoc version of such a strategy appears in [Cui+20], and is inequivalent to the first one considered.
- Are there any other perfect strategies?

$$
\begin{tikzcd}
e_1 \arrow[r, no head] \arrow[d, no head] & e_2 \arrow[r, no head] \arrow[d, no head] & e_3 \arrow[d, no head, dashed] & & \\
e_4 \arrow[r, no head] \arrow[d, no head] & e_5 \arrow[r, no head] \arrow[d, no head] & e_6 \arrow[d, no head, dashed] & & \\
e_7 \arrow[r, no head] & e_8 \arrow[r, no head] & e_9 \arrow[d, no head, dashed] & & \\
 & & e_{10} \arrow[r, no head] \arrow[d, no head, dashed] & e_{11} \arrow[r, no head] \arrow[d, no head] & e_{12} \arrow[d, no head] \\
 & & e_{13} \arrow[r, no head] \arrow[d, no head, dashed] & e_{14} \arrow[r, no head] \arrow[d, no head] & e_{15} \arrow[d, no head] \\
 & & e_{16} \arrow[r, no head] & e_{17} \arrow[r, no head] & e_{18}
\end{tikzcd}
$$

Convex self-testing of Glued Magic Square

- For a perfect strategy $(|\psi\rangle, \{A_i\}_i, \{B_j\}_j)$, it holds that $A_3A_6A_9A_{10}A_{13}A_{16} = -I$.
  - Ideally, we would have $A_3A_6A_9 = -A_{10}A_{13}A_{16} = \pm I$. That implies we have a perfect Magic Square strategy on one Magic Square part.
  - It is not true in general – consider $A_i := \tilde{A}_i \oplus \tilde{A}_{19-i}$.
- While $A_3A_6A_9$ is not always $\pm I$, it is a central operator for all considered strategies.
- Exploiting the relations of the game, it can be shown that $[A_3A_6A_9, A_i] = 0$ for all $i \in [18]$.
- Thus, restricting A_i to either of the ± 1-eigenspace of $A_3A_6A_9$ is well-defined.
  - One can similarly restrict to the eigenspaces of $B_3B_6B_9$.

$$\begin{tikzcd}
A_1 \arrow[r, dash] \arrow[d, dash] & A_2 \arrow[r, dash] \arrow[d, dash] & A_3 \arrow[d, dash, dashed] & & \\
A_4 \arrow[r, dash] \arrow[d, dash] & A_5 \arrow[r, dash] \arrow[d, dash] & A_6 \arrow[d, dash, dashed] & & \\
A_7 \arrow[r, dash] & A_8 \arrow[r, dash] & A_9 \arrow[d, dash, dashed] & & \\
 & & A_{10} \arrow[r, dash] \arrow[d, dash, dashed] & A_{11} \arrow[r, dash] \arrow[d, dash] & A_{12} \arrow[d, dash] \\
 & & A_{13} \arrow[r, dash] \arrow[d, dash, dashed] & A_{14} \arrow[r, dash] \arrow[d, dash] & A_{15} \arrow[d, dash] \\
 & & A_{16} \arrow[r, dash] & A_{17} \arrow[r, dash] & A_{18}
\end{tikzcd}$$

Convex self-testing of Glued Magic Square

- Restricted to $(A_3A_6A_9)^-$ and $(B_3B_6B_9)^-$, we essentially get the following game:

$$\left.\begin{array}{ccccc} e_1 & \text{—} & e_2 & \text{—} & e_3 \\ | & & | & & \vdots \\ e_4 & \text{—} & e_5 & \text{—} & e_6 \\ | & & | & & \vdots \\ e_7 & \text{—} & e_8 & \text{—} & e_9 \end{array}\right\} = -I$$

$$= I \left\{\begin{array}{ccccc} e_{10} & \text{—} & e_{11} & \text{—} & e_{12} \\ \vdots & & | & & | \\ e_{13} & \text{—} & e_{14} & \text{—} & e_{15} \\ \vdots & & | & & | \\ e_{16} & \text{—} & e_{17} & \text{—} & e_{18} \end{array}\right.$$

Convex self-testing of Glued Magic Square

- Restricted to $(A_3A_6A_9)^-$ and $(B_3B_6B_9)^-$, we essentially get the following game:

$$
\begin{tikzcd}
e_1 \arrow[r, dash] \arrow[d, dash] & e_2 \arrow[r, dash] \arrow[d, dash] & e_3 \arrow[d, dash, dashed] \\
e_4 \arrow[r, dash] \arrow[d, dash] & e_5 \arrow[r, dash] \arrow[d, dash] & e_6 \arrow[d, dash, dashed] \\
e_7 \arrow[r, dash] & e_8 \arrow[r, dash] & e_9
\end{tikzcd}
$$

$$
\begin{tikzcd}
e_{10} \arrow[r, dash] \arrow[d, dash] & e_{11} \arrow[r, dash] \arrow[d, dash] & e_{12} \arrow[d, dash] \\
e_{13} \arrow[r, dash] \arrow[d, dash] & e_{14} \arrow[r, dash] \arrow[d, dash] & e_{15} \arrow[d, dash] \\
e_{16} \arrow[r, dash] & e_{17} \arrow[r, dash] & e_{18}
\end{tikzcd}
$$

Convex self-testing of Glued Magic Square

Analysing perfect strategies for subgames

- All operators can be derived from those corresponding to the blue variables.
- All blue operators pairwise commute.
  - Clear when sharing equations; can be readily derived when not (e.g. $A_{14}A_{18}A_{14}A_{18} = I$).
- This implies we get a representation of $(\mathbb{Z}/2\mathbb{Z})^{\times 4}$.

$$\begin{array}{ccccc} e_{10} & - & e_{11} & - & e_{12} \\ | & & | & & | \\ e_{13} & - & e_{14} & - & e_{15} \\ | & & | & & | \\ e_{16} & - & e_{17} & - & e_{18} \end{array}$$

Convex self-testing of Glued Magic Square

- Let S_1^σ be the strategy for GMS which is the ideal Magic Square strategy on the first part, and the representation σ of $(\mathbb{Z}/2\mathbb{Z})^{\times 4}$ on the second part.
- Let S_2^σ be as S_1^σ, except the operators for the first and second Magic Square part are swapped.
- Any perfect strategy for GMS decomposes into the above two types of strategies.
  - Thus, we get convex self-testing of the families

$$\hat{\mathcal{S}}_k = \left\{ \mathcal{S}_k^\sigma \mid \sigma \text{ is a representation of } (\mathbb{Z}/2\mathbb{Z})^{\times 4} \right\}, k \in [2].$$

- These all use the state $|\psi_4\rangle$, giving (ordinary) self-testing of the state.
- This generalises robustly.
- Replacing one or both parts with Magic Pentagram also works.

References I

Richard Cleve and Rajat Mittal. 'Characterization of binary constraint system games'. In: *International Colloquium on Automata, Languages, and Programming*. Springer. 2014, pp. 320–331.

David Cui, Arthur Mehta, Hamoon Mousavi and Seyed Sajjad Nezhadi. 'A generalization of CHSH and the algebraic structure of optimal strategies'. In: *Quantum* 4 (2020), p. 346.

Laura Mančinska, Thor Gabelgaard Nielsen and Jitendra Prakash. 'Glued magic games self-test maximally entangled states'. In: *arXiv preprint arXiv:2105.10658* (2021).

Laura Mančinska, Jitendra Prakash and Christopher Schafhauser. 'Constant-sized robust self-tests for states and measurements of unbounded dimension'. In: *arXiv e-print arXiv:2103.01729* (2021).

References II

Xingyao Wu, Jean-Daniel Bancal, Matthew McKague and Valerio Scarani. 'Device-independent parallel self-testing of two singlets'. In: *Physical Review A* 93.6 (2016), p. 062121.