Abstract

Self-testing is a method to verify that one has a particular quantum state from purely classical statistics. For applications such as device-independent delegated verifiable quantum computation, it is crucial that one tests multiple Bell states in parallel while keeping the quantum requirements of one side to a minimum. We use $3 \times n$ magic rectangle games to obtain a self-test for $n$ Bell states where one side need only make single-qubit Pauli measurements. It consumes little randomness, is robust, and requires only perfect correlations. To achieve this, we introduce a one-side-local quantum strategy for the magic square game that wins with certainty, generalise this to the family of $3 \times n$ magic rectangle games, and supplement these games with extra check rounds.

Magic square game

The magic square game is a nonlocal game played on a $3 \times 3$ grid [1].

- Alice and Bob are assigned (uniformly at random) a row and column.

Players must fill their row/column with $\pm 1$ according to certain rules:

1. The product of Alice's row must be positive.
2. The product of Bob's column must be negative.

\[
\begin{array}{ccc}
+ & + & + \\
+ & - & + \\
- & + & - \\
\end{array}
\]

Win condition: Values entered into the shared cell coincide.

Self-testing protocol: Three Bell states

Let $n = 3$ be the number of Bell states to be tested. In each round, a verifier chooses $c \in \{0, 1\}$ and $y \in \{1, \ldots, n\}$. The verifier sends Bob $(c, y)$ and, depending on $c$, runs one of the following subprotocols:

0. **Magic game.** Send Alice $x \in \{1, 2, 3\}$. Alice and Bob answer with $a_1, \ldots, a_n$ and $b_1, b_2, b_3$ in $\{+1, -1\}$ satisfying $b_1b_2b_3 = -1$. Accept if and only if $\prod_{k=1}^{n} a_k = b_c$.

1. **Local check.** Send Alice $x \in \{1, 3\}$. Alice and Bob answer with $a_1, \ldots, a_n$ and $b_1, b_2, b_3$ in $\{+1, -1\}$. If $x = 1$, accept if and only if $a_3 = b_3$. If $x = 3$, accept if and only if $a_1 = b_1$ for all $j \neq y$.

Self-testing protocol: Many Bell states

Let $n = 3 \mod 4$. The verifier chooses $c \in \{0, 1, 2\}$ and performs the previous protocol with an additional subprotocol if $c = 2$ is chosen:

2. **Pair check.** Send Alice $x \in \{1, 3\}$. Alice answers with $a_1, \ldots, a_n$. Bob answers with $n - 1$ bits $b_{x+1, y+1}$ and $b_{x, y+1}$ in $\{+1, -1\}$ (with addition taken modulo $n$) for all $k \in \{1, \ldots, n\}$. If $x = 1$, accept if and only if $a_3b_j = b_3a_j$ for all $i, j$. If $x = 3$, accept if and only if $a_1b_j = b_1a_j$ for all $i, j$.

Robustness and completeness

If a strategy is accepted with probability at least $1 - \varepsilon$, the protocol self-tests the state $|\Phi^{+}\rangle_{AB}$ with robustness $O(n^{3/2}/\sqrt{\varepsilon})$.

- **Subprotocol magic game** ensures a perfect $3 \times n$ strategy is used.
- **Local check** rules out entangled measurements for Alice.
- **Pair check** rules out deterministic extensions to single-qubit strategies using smaller $3 \times m$ magic rectangles.

There exist strategies (based on one-side-local magic game strategies) that are accepted with certainty (use only perfect correlations).

- In the honest case, Alice needs only single-qubit Pauli measurements, while Bob requires two-qubit, entangled measurements.

Comparison

The protocol simultaneously achieves several properties desirable in the client/server setting.

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Local Perf.</th>
<th>Err. tol.</th>
<th>Input size</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Alice</td>
<td>Bob</td>
<td></td>
</tr>
<tr>
<td>Alice</td>
<td>Yes</td>
<td>$O(n^{-3/2})$</td>
<td>$O(1)$</td>
</tr>
<tr>
<td>Bob</td>
<td>Yes</td>
<td>$O(\log n)$</td>
<td>$O(\log n)$</td>
</tr>
</tbody>
</table>

Šupić et al. (2021) as base test $N/A$ $O(1)$

Chao et al. (2018) $\frac{1}{3}$ No $O(n^{-3/2})$ $O(\log n)$

Natarajan and Vidick (2018) No Yes $O(\delta^3)$ $O(\log n)$

Natarajan and Vidick (2017) as CHSH/MS $O(\delta^3)$ $O(n)$

Coladangelo (2017): MS $O(n)$ No Yes $O(n^{-3/2})$ $O(n)$

Coladangelo (2017): CHSH $O(n)$ No Yes $O(n^{-3/2})$ $O(n)$

Mackeague (2016) $O(n)$ No Yes $O(n^{-3/2})$ $O(n)$

Sample comparisons with other protocols, including some based on the magic square (MS) game, are shown above.

Generalisation: Magic rectangle games

Magic rectangle games [2] are played on an $m \times n$ grid.

The rules are generalised accordingly:

1. The product of Alice's $i$th row must be $\alpha_i$.
2. The product of Bob's $j$th column must be $\beta_j$.

\[
\begin{array}{ccc}
\alpha_1 & \ldots & \alpha_m \\
\beta_1 & \ldots & \beta_n \\
\end{array}
\]

To avoid deterministic winning strategies, we also require

\[
\alpha_1 \ldots \alpha_m \cdot \beta_1 \ldots \beta_n = -1.
\]

The self-test uses 3 rows, 3 (mod 4) columns, $\alpha_i = +1$, and $\beta_j = -1$.

References
