Practical Parallel Self-testing of Bell States via Magic Rectangles*

Sean A. Adamson Petros Wallden

School of Informatics, University of Edinburgh

THE UNIVERSITY of EDINBURGH informatics

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 3×3 grid [1].

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

Players must fill their row/column with ± 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**.

+	+	+

	+	
	+	
	−	

	+	
+	+	+
	−	

Figure 1. Example for Alice (left) and Bob (middle). The players win (right).

Win condition: Values entered into the shared cell coincide.

One-side-local strategy

Optimal classical and quantum win probabilities $8/9$ and 1.

- Standard strategy has $|\Phi^+\rangle_{AB}^{\otimes 2}$ shared between Alice and Bob.
- Requires two-qubit *entangled* measurements upon some inputs.
- Alice needs only **single-qubit** measurements if $|\Phi^+\rangle_{AB}^{\otimes 3}$ shared.

X_1	X_1X_2	X_2
$-X_1Z_2$	Y_1Y_2	$-Z_1X_2$
Z_2	Z_1Z_2	Z_1

X_2X_3	X_1X_3	X_1X_2
Y_2Y_3	Y_1Y_3	Y_1Y_2
Z_2Z_3	Z_1Z_3	Z_1Z_2

Figure 2. The *standard* strategy (left) and *one-side-local* strategy (right).

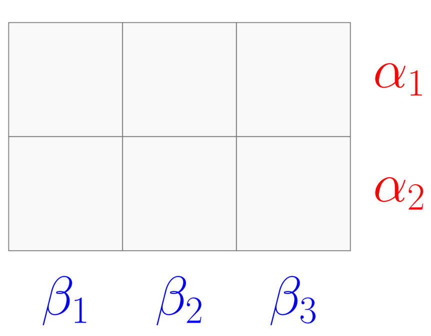
The **one-side-local** strategy generalises to $3 \times n$ *magic rectangle* games (for $n = 3 \mod 4$) and has a similar structure.

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 ith **row** must be α_i.
2. The product of Bob's jth **row** must be β_j.



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, $3 \pmod 4$ columns, $\alpha_i = +1$, and $\beta_j = -1$.

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 $b_1 b_2 b_3 = -1$. Accept if and only if $\prod_{k \neq y} a_k = b_x$.
1. Local check. Send Alice $x \in \{1, 3\}$. Alice and Bob answer with $a_1, \ldots, a_n$ and $b_1, \ldots, b_n$ in $\{+1, -1\}$. If $x = 1$, accept if and only if $a_y = b_y$. If $x = 3$, accept if and only if $a_j = b_j$ for all $j \neq y$.

Self-testing protocol: Many Bell states

Let $n = 3 \pmod 4$. 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 $b_{y-k,y+k}$ and $b'_{y-k,y+k}$ in $\{+1, -1\}$ (with addition taken modulo n) for all $k \in \{1, \ldots, \frac{n-1}{2}\}$. If $x = 1$, accept if and only if $a_i a_j = b_{i,j}$ for all i, j. If $x = 3$, accept if and only if $a_i a_j = b'_{i,j}$ for all i, j.

Robustness and completeness

If a strategy is accepted with probability at least $1 - \varepsilon$, the protocol self-tests the state $|\Phi^+\rangle_{AB}^{\otimes n}$ with robustness $O(n^{5/2}\sqrt{\varepsilon})$.

- 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 $3 \times n'$ 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.

Protocol	Local	Perf. corr.	Err. tol. $\varepsilon(n, \delta)$	Input size Alice	Input size Bob
This protocol	Alice	Yes	$O(n^{-5}\delta^2)$	$O(1)$	$O(\log n)$
Šupić et al. (2021)	As base test		N/A	$O(1)$	
Chao et al. (2018)	Yes	No	$O(n^{-5}\delta^2)$	$O(\log n)$	
Natarajan and Vidick (2018)	No	Yes	$O(\delta^c)$	$O(\log n)$	
Natarajan and Vidick (2017)	As CHSH/MS		$O(\delta^{16})$	$O(n)$	
Coladangelo (2017): MS	No	Yes	$O(n^{-3}\delta^2)$	$O(n)$	
Coladangelo (2017): CHSH	Yes	No	$O(n^{-3}\delta^2)$	$O(n)$	
Coudron and Natarajan (2016)	No	Yes	$O(n^{-4}\delta^4)$	$O(n)$	
McKague (2016)	Yes	No	$O(n^{-8}\delta^8)$	$O(\log \log n)$	

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

References

[1] Padmanabhan K. Aravind. Quantum mysteries revisited again. *Am. J. Phys.*, 72(10):1303–1307, 9 2004.

[2] Sean A. Adamson and Petros Wallden. Quantum magic rectangles: Characterization and application to certified randomness expansion. *Phys. Rev. Research*, 2(4):043317, 12 2020.