Rigidity of the magic pentagram game

Amir Kalev[1,*] and Carl A. Miller[1,2,†]

[1] *Joint Center for Quantum Information and Computer Science, University of Maryland, College Park, MD 20742-2420, USA*

[2] *National Institute of Standards and Technology, Gaithersburg, MD 20899, USA*

(Dated: November 3, 2017)

A game is rigid if a near-optimal score guarantees, under the sole assumption of the validity of quantum mechanics, that the players are using an approximately unique quantum strategy. Rigidity has a vital role in quantum cryptography as it permits a strictly classical user to trust behavior in the quantum realm. This property can be traced back as far as 1998 (Mayers and Yao) and has been proved for multiple classes of games. In this paper we prove ridigity for the magic pentagram game, a simple binary constraint satisfaction game involving two players, five clauses and ten variables. We show that all near-optimal strategies for the pentagram game are approximately equivalent to a unique strategy involving real Pauli measurements on three maximally-entangled qubit pairs.

I. INTRODUCTION

Quantum rigidity is a strengthening of the guarantee that quantum behavior is taking place. It essentially ascertains that observing certain correlations in a system, for example, correlations that violate Bell inequalities, is sufficient by itself to determine the quantum state and the measurements used to obtain these correlations. This notion was expressed in the work of Mayers and Yao on "self-checking quantum sources" [1] in 1998, and it can be traced back even earlier [2, 3]. Rigidity is a central tool for quantum computational protocols that involve untrusted devices, since it allows a user to verify the internal workings of a device based only on its external behavior (see, e.g., [4]).

Since its introduction the notion of rigidity has seen good deal of work, generally focused either on proving rigidity for particular classes of games, or proving that rigid games exist that self-test particular quantum states. Two-player games that are known to be rigid include the CHSH game [2, 5], the magic square game [6], the chained Bell inequalities [7], the Mayers-Yao criterion [1, 8], Hardy's test [9], the Hadamard-graph coloring game [10], and various classes of binary games [11–13]. New results on rigid games add to the tools available for protocols based on untrusted devices.

In the current paper we prove that the magic pentagram game (see Figure 1) is rigid. This game is a natural one to study: in particular, it was originally proposed alongside the magic square game [14], and it shares some of the same properties that make the magic square game useful in cryptography (in particular, it shares the property that an optimal strategy must yield a perfect shared key bit pair between two parties, which was exploited in [15]). From a resource standpoint, it also offers an improvement over the magic square game: whereas the magic square game requires 9 questions to self-test 2 EPR pairs, we will prove that the magic pentagram game self-tests 3 EPR pairs with 20 questions. If we compare the number of bits of randomness needed to generate the questions set to the number EPR pairs tested, the magic square has a ratio of $\frac{1}{2}\log_2 9 \approx 1.58$, while the magic pentagram game has a ratio of $\frac{1}{3}\log_2 20 \approx 1.44$.

The optimal strategy for the magic pentagram game is shown in Figure 2. Our main result is summarized below, and proved formally in Propositions 9, 10, 12, and Corollary 11.

Theorem 1 (Informal)**.** *Suppose that Alice and Bob have a strategy for the magic pentagram game that wins with probability $1-\epsilon$. Then, after the application of a local isometry on Alice's and Bob's systems, the following statements hold.*

1. *The shared state is within Euclidean distance $O(\sqrt{\epsilon})$ from a state of the form $(\Phi^+)^{\otimes 3} \otimes |junk\rangle$, where Φ^+ denotes a Bell state and $|junk\rangle$ denotes an arbitrary bipartite state. (Proposition 12.)*

2. *The post-measurement states under Alice's and Bob's measurements are approximated (up to $O(\sqrt{\epsilon})$) by the corresponding post-measurement states from the strategy in Figure 2. (Propositions 9–10 and Corollary 11.)*

Our proof is self-contained and borrows techniques from previous papers on rigidity [5, 6, 16]. One of the challenges for the magic pentagram game is that the first player may associate two different measurements to a single observable — for example, in Figure 1, Alice may use a different measurement for vertex 1 depending on whether the context is G or D. (This does not occur in the magic square game.) Our early technical work addresses this fact — see Propositions 5–6 and the discussion that follows.

The coefficients of the error terms $O(\sqrt{\epsilon})$ for Theorem 1 are not given explicitly, and optimizing these coefficients is left as an open problem. (Tracing through the steps of the current proof might yield coefficients in the thousands.)

* amirk@umd.edu

† camiller@umd.edu

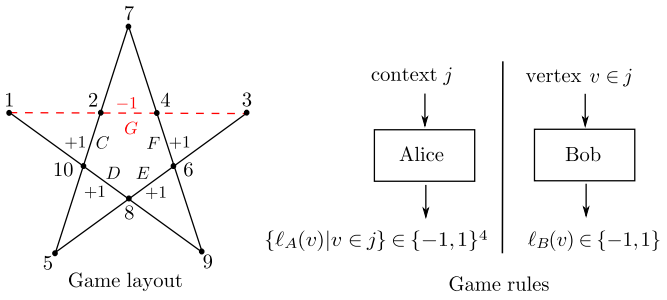

FIG. 1. **The pentagram game.**

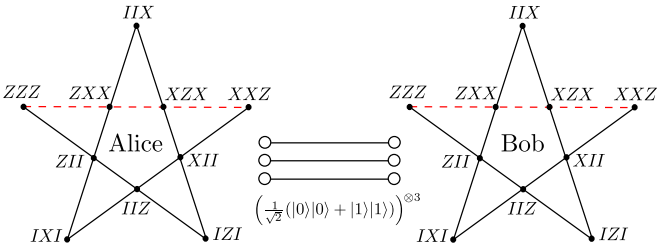

FIG. 2. **A winning strategy.**

In the larger picture, the magic square game and the magic pentagram game are examples of binary constraint satisfaction games [17]. Arkhipov [18] proved that a certain natural subclass of binary constraint satisfaction problems — specifically, those that are based on XOR clauses where every variable is in exactly two clauses — are all in a precise sense reducible to the magic square game and the magic pentagram game. This suggests that our result is a step towards a full classification of winning quantum strategies within this class.

II. THE MAGIC PENTAGRAM GAME

The pentagram game is a binary constraint satisfaction game between two parties, Alice and Bob. Its rules can be defined, as its name suggests, on a pentagram hypergraph, see Fig. 1. The five hyperedges of the pentagram (the clauses or contexts) are labeled C, D, E, F, G, and each contains four vertices. The hyperedges are each assigned a value: $\ell(C) = \ell(D) = \ell(E) = \ell(F) = 1$, and $\ell(G) = -1$. The rules of the games are as follows:

- A context j is chosen and a vertex $v \in j$ is chosen (both uniformly at random). The context j is given to Alice and the vertex v is given to Bob.
- Alice assigns either $+1$ or -1 to each vertex in the context j, and Bob assigns $+1$ or -1 to v.
- Alice and Bob can communicate and agree on a strategy prior to the beginning of the game, but are not allowed to communicate once the game has begun.

The game is won if the following two conditions both hold:

- The product of the values returned by Alice is equal to the pre-assigned value $\ell(j)$.
- Alice and Bob return the same value for v.

There is no classical strategy to win this game perfectly, as is easily verified. However, it can be won with probability 1 using quantum resources [14, 19]. A winning strategy is schematically shown in Fig. 2, with Z, X and I denoting the Pauli operators σ_z, σ_x, and the identity operator, respectively. They share six qubits, three at Alice's lab ($Q_1Q_2Q_3$) and three at Bob's ($Q_4Q_5Q_6$), prepared in the maximally entangled state

$$|\Phi^+\rangle^{\otimes 3} = \bigotimes_{i=1}^{3} \left(\frac{1}{\sqrt{2}}(|0\rangle_{Q_i}|0\rangle_{Q_{i+3}} + |1\rangle_{Q_i}|1\rangle_{Q_{i+3}}\right), \quad (1)$$

where $|0\rangle, |1\rangle$ are the eigenbasis of the Pauli Z operator. (When no confusion arises we drop the tensor product symbol and the subscript labels for Alice and Bob's subsystems.) Upon receiving a hyperedge label j, Alice measures the four Pauli observables associated with the four vertices of j on her three qubits, and then assigns to each vertex the value she obtains for the corresponding observable. These observables are reflection operators (i.e., Hermitian operators having eigenvalues in $\{-1, +1\}$) such that observables of adjacent vertices (vertices that are connected by the same hyperedge) all commute and thus can be measured simultaneously. Bob measures the observable of his input vertex on his three qubit system and assigns a $\{-1, +1\}$ value to the vertex according to the outcome of his measurement. By construction of this strategy, the winning conditions for this game, as listed above, are fulfilled for every input value j and v.

We note that in this strategy any two non-adjacent observables anti-commute. (This will become important in later proofs.)

III. STRATEGIES FOR THE MAGIC PENTAGRAM GAME

Our goal is to relate arbitrary strategies for the magic pentagram game to the strategy in Figure 2. The class of strategies that we study are captured in the following definition.

Definition 2. *A projective strategy for the magic pentagram game consists of the following data:*

1. ***The shared state:*** *Two finite-dimensional Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$, and a unit vector $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$.*
2. ***Alice's measurements:*** *For each $j \in \{C, D, E, F, G\}$, a projective measurement $\{M_t^j\}$*

on $\mathcal{H}_A$, where t varies over the set of all functions from j to $\{0,1\}$ whose parity is equal to $\ell(j)$.

3. ***Bob's measurements:*** *For vertex v, a projective measurement $\{N_v^s\}_{s\in 0,1}$.*

The functions obtained from these measurements specify the output values for Alice and Bob. Note that we could have allowed for the shared state to be mixed and for the measurements to be general positive-operator valued measures (POVMs). However standard techniques imply that any such strategy is a partial trace of one in the above form, so there is no generality lost.

Additionally, we make the following definition.

Definition 3. *A reflection is a Hermitian automorphism whose eigenvalues are contained in $\{-1,+1\}$. A reflection strategy for the magic pentagram game consists of the following data:*

1. ***The shared state:*** *Two finite-dimensional Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$, and a linear map $L\colon \mathcal{H}_B \to \mathcal{H}_A$ satisfying $\|L\|_2 = 1$.*

2. ***Alice's reflections:*** *Reflections*

$$\{R_v^j \mid j \in \{C,D,E,F,G\}, v \in j\}$$

on $\mathcal{H}_A$ such that the reflections that belong to any context j all commute ($[R_v^j, R_{v'}^j] = 0$) and their product is equal to $\ell(j)I$.

3. ***Bob's reflections:*** *Reflections $\{S_v\}_v$ on $\mathcal{H}_B$.*

Note that any projective strategy can be converted into a reflection strategy, and vice versa, via the relations

$$R_v^j = \sum_{t(v)=0} M_t^j - \sum_{t(v)=1} M_t^j, \tag{2}$$

$$S_v = N_v^0 - N_v^1 \tag{3}$$

$$L = \langle \Phi^B | \psi \rangle \tag{4}$$

where $|\Phi^B\rangle = \sum_i |ii\rangle$ on $\mathcal{H}_B$.

The probability distribution obtained from a projective measurement $\{O_1,\ldots,O_n\}$ on $\mathcal{H}_A$ is given by $(\|O_1 L\|_2^2, \ldots, \|O_n L\|_2^2)$, and the probability distribution obtained from a projective measurement $\{P_1,\ldots,P_n\}$ on $\mathcal{H}_B$ is given by $(\|LP_1\|_2^2, \ldots, \|LP_n\|_2^2)$. For any context j and any vertex $v \in j$, the probability that Alice and Bob will assign different values to the vertex v in a given reflection strategy is given by

$$\left\| \left(\frac{I+R_v^j}{2}\right) L \left(\frac{I-S_v}{2}\right) \right\|_2^2 + \left\| \left(\frac{I-R_v^j}{2}\right) L \left(\frac{I+S_v}{2}\right) \right\|_2^2.$$

Thus the losing probability (that is, one minus the expected score) for the reflection strategy is given by

$$\begin{aligned} p_{\text{lose}} &= \frac{1}{20} \sum_{v\in j} \left(\left\| \left(\frac{I+R_v^j}{2}\right) L \left(\frac{I-S_v}{2}\right) \right\|_2^2 \right. \\ &\quad \left. + \left\| \left(\frac{I-R_v^j}{2}\right) L \left(\frac{I+S_v}{2}\right) \right\|_2^2 \right) \\ &= \frac{1}{20} \sum_{v\in j} \left\| L - R_v^j L S_v \right\|_2^2 \\ &= \frac{1}{20} \sum_{v\in j} \left\| R_v^j L - L S_v \right\|_2^2 . \end{aligned}$$

Thus we have the following.

Proposition 4. *Let $(L, \{R_v^j\}, \{S_v\})$ be a reflection strategy for the magic pentagram game which achieves winning probability $1-\epsilon$. Then, for any context j and vertex $v \in j$,*

$$\left\| R_v^j L - L S_v \right\|_2 \leq O(\sqrt{\epsilon}), \tag{5}$$

Next we prove a series of properties for near-optimal strategies, all of which are consequences of Proposition 4.

Proposition 5 (Changing contexts)**.** *Let*

$$(L, \{R_v^j\}, \{S_v\})$$

be a reflection strategy with expected score $1-\epsilon$. Let $v_1,\ldots,v_n$ be a sequence of vertices and $j_1,\ldots,j_n$ and $j_1',\ldots,j_n'$ be sequences of contexts such that $v_i \in j_i \cap j_i'$ for all i. Then,

$$\left\| R_{v_1}^{j_1} R_{v_2}^{j_2} \cdots R_{v_n}^{j_n} L - R_{v_1}^{j_1'} R_{v_2}^{j_2'} \cdots R_{v_n}^{j_n'} L \right\|_2 \leq O(n\sqrt{\epsilon}).$$

Proof. Applying Proposition 4 inductively, we find that $R_{v_1}^{j_1} \cdots R_{v_n}^{j_n} L$ and $R_{v_1}^{j_1'} \cdots R_{v_n}^{j_n'} L$ are both within Euclidean distance $O(n\sqrt{\epsilon})$ from $L S_{v_1} \cdots S_{v_n}$. □

The next two propositions certify the relation between reflection operators in a strategy with expected score $1-\epsilon$. For convenience, hereafter we refer to sequences $T_1,\ldots,T_n$ of matrices satisfying $\|T_{i+1} - T_i\|_2 \leq \delta$ as *δ-approximate sequences.*

Proposition 6 (Approximate commutativity)**.** *Let $(L, \{R_v^j\}, \{S_v\})$ be a reflection strategy with expected score $1-\epsilon$. Let v and w be adjacent vertices, such that $v, w \in j$, and let $j' \neq j$ be the other hyperedge which contains w. Then,*

$$\left\| R_v^j R_w^{j'} L - R_w^{j'} R_v^j L \right\|_2 \leq O(\sqrt{\epsilon}) \tag{6}$$

$$\| L S_w S_v - L S_v S_w \|_2 \leq O(\sqrt{\epsilon}). \tag{7}$$

Proof. The desired result follows easily by applications of Proposition 4. □

Each vertex v has two reflection operators for Alice (R_v^j and R_v^k, where $j \cap k = \{v\}$). It is helpful for some of the proofs that follow to single out one distinguished reflection operator for each vertex. We therefore make the following (arbitrary) assignments,

$$\begin{array}{ll} R_1 := R_1^G & R_6 := R_6^E \\ R_2 := R_2^G & R_7 := R_7^F \\ R_3 := R_3^E & R_8 := R_8^D \\ R_4 := R_4^F & R_9 := R_9^D \\ R_5 := R_5^E & R_{10} := R_{10}^C . \end{array} \tag{8}$$

Proposition 7 (Approximate anti-commutativity)**.** *Let $(L, \{R_v^j\}, \{S_v\})$ be a reflection strategy with expected score $1-\epsilon$, and let $v \in j$ and $w \in j'$ be non-adjacent vertices (i.e., vertices that never occur in the same context). Then,*

$$\left\| R_v^j R_w^{j'} L + R_w^{j'} R_v^j L \right\|_2 \leq O(\sqrt{\epsilon}) \tag{9}$$

$$\left\| LS_wS_v + LS_vS_w \right\|_2 \leq O(\sqrt{\epsilon}). \tag{10}$$

Proof. By Proposition 5, it suffices to prove these relations with $R_v^j, R_w^{j'}$ replaced by R_v, R_w. We give a proof for $v = 7, w = 3$, which generalizes to cover all other cases by symmetry. The proof is inspired by the proof of rigidity for the magic square game [6]. Applying the rules for Alice's measurements from Definition 3 and the foregoing propositions, we find that the following sequence is an $O(\sqrt{\epsilon})$-approximate sequence:

$$\begin{aligned} &R_7R_3L, \\ &(R_4R_9R_6)(R_6R_8R_5)L, \\ &R_4R_9R_8R_5L, \\ &R_4(R_1R_{10}R_8)R_8R_5L, \\ &R_4R_1R_{10}R_5L, \\ &R_4R_1(R_2R_7)L, \\ &-R_3R_7L, \end{aligned}$$

and relation (10) follows similarly. □

The next proposition follows from Propositions 4, 6, and 7.

Proposition 8. *Let $v_1 \in j_1, v_2 \in j_2, \ldots, v_n \in j_n$ be a sequence of vertices and $i \in \{1, 2, \ldots, n-1\}$. Then,*

$$\begin{aligned} &\left\| R_{v_1}^{j_1} \cdots R_{v_i}^{j_i} R_{v_{i+1}}^{j_{i+1}} \cdots R_{v_n}^{j_n} L \right. \\ &\left. -bR_{v_1}^{j_1} \cdots R_{v_{i+1}}^{j_{i+1}} R_{v_i}^{j_i} \cdots R_{v_n}^{j_n} L \right\|_2 \leq O(n\sqrt{\epsilon}) \\ &\left\| LS_{v_1} \cdots S_{v_i} S_{v_{i+1}} \cdots S_{v_n} \right. \\ &\left. -bLS_{v_1} \cdots S_{v_{i+1}} S_{v_i} \cdots S_{v_n} \right\|_2 \leq O(n\sqrt{\epsilon}), \end{aligned}$$

where $b = 1$ if v_i, v_{i+1} are adjacent and $b = -1$ if v_i, v_{i+1} are non-adjacent. □

IV. RIGIDITY

In this section, we will use the following notation: $Q_1, \ldots, Q_6$ will denote qubit registers (each with a fixed isomorphism to $\mathbb{C}^2$). The linear maps $H_i \colon Q_i \to Q_i$ denote the Hadamard maps $|0\rangle \mapsto |+\rangle, |1\rangle \mapsto |-\rangle$, and the linear maps $X_i, Z_i \colon Q_i \to Q_i$ denote the Pauli operators. For any reflection U on $\mathcal{H}_A \otimes \mathcal{H}_B$, and $i \in \{1, 2, 3, 4, 5, 6\}$, let the map

$$C_i(U) \colon Q_i \otimes \mathcal{H}_A \otimes \mathcal{H}_B \to Q_i \otimes \mathcal{H}_A \otimes \mathcal{H}_B \tag{11}$$

denote the controlled operation $|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes U$. Note that these maps interact as follows:

$$X_iC_i(U)X_i = C_i(U)U = UC_i(U) \tag{12}$$

$$Z_iC_i(U) = C_i(-U) = C_i(U)Z_i \tag{13}$$

The next theorem asserts that some of the reflections in a near-optimal strategy for the magic pentagram game can be simulated by Pauli operators. Let

$$\begin{array}{ll} X_1' = R_6 & X_4' = S_6 \\ X_2' = R_5 & X_5' = S_5 \\ X_3' = R_7 & X_6' = S_7 \\ Z_1' = R_{10} & Z_4' = S_{10} \\ Z_2' = R_9 & Z_5' = S_9 \\ Z_3' = R_8 & Z_6' = S_8, \end{array} \tag{14}$$

where the Rs are given in Eq. (8). These operators are chosen so that for $i \in \{1, 2, 3\}$ (and similarly for $i \in \{4, 5, 6\}$) the pairs (X_i', Z_i'), belong to non-adjacent vertices, while all the other pairs of operators belong to adjacent vertices. Thus the approximate commutativity conditions and anti-commutativity conditions are what one would expect for the corresponding Pauli operators. We note that the particular choice of the X's and Z's here is not unique. The following results will hold for any choice of X's and Z's as long as they satisfy the required approximate commutation relations.

Proposition 9. *Let $(L, \{R_v^j\}, \{S_v\})$ be a reflection strategy with expected score $1-\epsilon$. Then, there exists an isometry Ψ_A from $\mathcal{H}_A$ to $\mathcal{H}_A \otimes Q_1 \otimes Q_2 \otimes Q_3$ such that for all $i \in \{1, 2, 3\}$,*

$$\|X_i\Psi_AL - \Psi_AX_i'L\|_2 \leq O(\sqrt{\epsilon}) \tag{15}$$

$$\|Z_i\Psi_AL - \Psi_AZ_i'L\|_2 \leq O(\sqrt{\epsilon}). \tag{16}$$

Proof. Our construction of the isometries follows previous papers on rigidity (e.g., [16]). For each $i \in \{1, 2, 3\}$ define

$$\Psi_i \colon \mathcal{H}_A \to \mathcal{H}_A \otimes Q_i \tag{17}$$

by

$$\Psi_i(z) = [C_i(X_i')]H_i[C_i(Z_i')](z \otimes |+\rangle). \tag{18}$$

Then, the following is an $O(\sqrt{\epsilon})$-approximate sequence:

$$\begin{aligned}
&X_i\Psi_i L,\\
&X_i[C_i(X_i')]H_i[C_i(Z_i')](L\otimes|+\rangle),\\
&[C_i(X_i')]X_i'X_iH_i[C_i(Z_i')](L\otimes|+\rangle),\\
&[C_i(X_i')]H_iZ_iX_i'[C_i(Z_i')](L\otimes|+\rangle),\\
&[C_i(X_i')]H_iZ_i[C_i(-Z_i')]X_i'(L\otimes|+\rangle),\\
&[C_i(X_i')]H_i[C_i(Z_i')]X_i'(L\otimes|+\rangle),\\
&\Psi_iX_i'L.
\end{aligned}$$

Thus,

$$\|X_i\Psi_iL-\Psi_iX_i'L\|_2\le O(\sqrt{\epsilon}).$$

Additionally, the following is an $O(\sqrt{\epsilon})$-approximate sequence:

$$\begin{aligned}
&Z_i\Psi_i L,\\
&Z_i[C_i(X_i')]H_i[C_i(Z_i')](L\otimes|+\rangle),\\
&[C_i(X_i')]Z_iH_i[C_i(Z_i')](L\otimes|+\rangle),\\
&[C_i(X_i')]H_iX_i[C_i(Z_i')](L\otimes|+\rangle),\\
&[C_i(X_i')]H_i[C_i(Z_i')]Z_i'X_i(L\otimes|+\rangle),\\
&[C_i(X_i')]H_i[C_i(Z_i')]Z_i'(L\otimes|+\rangle),\\
&\Psi_iZ_i'L.
\end{aligned}$$

Thus,

$$\|Z_i\Psi_iL-\Psi_iZ_i'L\|_2\le O(\sqrt{\epsilon}).$$

Also, if $i,k\in\{1,2,3\}$ with $k\neq i$, then by Proposition 6, the following is a $O(\sqrt{\epsilon})$-approximate sequence:

$$\begin{aligned}
&X_k'\Psi_i L,\\
&X_k'[C_i(X_i')]H_i[C_i(Z_i')](L\otimes|+\rangle),\\
&X_k'[C_i(X_i')]H_iL[C_i(Z_{i+3}')](I\otimes|+\rangle),\\
&X_k'[C_i(X_i')]LH_i[C_i(Z_{i+3}')](I\otimes|+\rangle),\\
&[C_i(X_i')]X_k'LH_i[C_i(Z_{i+3}')](I\otimes|+\rangle),\\
&[C_i(X_i')]X_k'H_i[C_i(Z_i')]L(I\otimes|+\rangle),\\
&[C_i(X_i')]H_i[C_i(Z_i')]X_k'L(I\otimes|+\rangle),\\
&\Psi_iX_k'L.
\end{aligned}$$

Therefore

$$\|X_k'\Psi_iL-\Psi_iX_k'L\|_2\le O(\sqrt{\epsilon}) \tag{19}$$

and by similar reasoning,

$$\|Z_k'\Psi_iL-\Psi_iZ_k'L\|_2\le O(\sqrt{\epsilon}). \tag{20}$$

Define $\Phi_i\colon\mathcal{H}_B\to\mathcal{H}_B\otimes Q_i$ by the same expression used to define Ψ_i, except with the operators X_i', Z_i' replaced with X_{i+3}', Z_{i+3}':

$$\Phi_i(z)=[C_i(X_{i+3}')]H_i[C_i(Z_{i+3}')](z\otimes|+\rangle). \tag{21}$$

Then, $\|\Psi_iL-L\Phi_i\|_2\le O(\sqrt{\epsilon})$ by Proposition 4. Let

$$\Psi_A=\Psi_1\Psi_2\Psi_3. \tag{22}$$

Then, the following is an $O(\sqrt{\epsilon})$-approximate sequence:

$$\begin{aligned}
&X_2\Psi_AL,\\
&X_2\Psi_1\Psi_2\Psi_3L,\\
&\Psi_1X_2\Psi_2\Psi_3L,\\
&\Psi_1X_2\Psi_2L\Phi_3,\\
&\Psi_1\Psi_2X_2'L\Phi_3,\\
&\Psi_1\Psi_2X_2'\Psi_3L,\\
&\Psi_1\Psi_2\Psi_3X_2'L.
\end{aligned}$$

Therefore,

$$\|X_2\Psi_AL-\Psi_AX_2'L\|_2\le O(\sqrt{\epsilon}). \tag{23}$$

The desired result for $i=1,3$ follows by similar reasoning. □

Likewise, we have the following.

Proposition 10. *Let $(L,\{R_v^j\},\{S_v\})$ be a reflection strategy with expected score $1-\epsilon$. Then, there exists an isometry Ψ_B from $\mathcal{H}_B$ to $\mathcal{H}_B\otimes Q_4\otimes Q_5\otimes Q_6$ such that for all $i\in\{4,5,6\}$,*

$$\left\|L\Psi_B^\dagger X_i-LX_i'\Psi_B^\dagger\right\|_2\le O(\sqrt{\epsilon}) \tag{24}$$

$$\left\|L\Psi_B^\dagger Z_i-LZ_i'\Psi_B^\dagger\right\|_2\le O(\sqrt{\epsilon}). \tag{25}$$

Proof. Define Ψ_i for $i\in\{4,5,6\}$ by the same expression (18) that was used in the previous proof, and let $\Psi_B=\Psi_4\Psi_5\Psi_6$. The desired result follows by the same reasoning that was used to prove Proposition 9. □

Note that Propositions 9 and 10 easily generalize to sequences of measurements — for example, the following is an $O(\sqrt{\epsilon})$-approximate sequence:

$$X_1X_2\Psi_AL, \tag{26}$$
$$X_1\Psi_AX_2'L, \tag{27}$$
$$X_1\Psi_ALX_5', \tag{28}$$
$$\Psi_AX_1'LX_5', \tag{29}$$
$$\Psi_AX_1'X_2'L. \tag{30}$$

Applying this method inductively, we have the following corollary.

Corollary 11. *The isometries from Proposition 9 and 10 satisfy the following. For any sequence $M_1',\dots,M_n'\in\{X_1',X_2',X_3',Z_1',Z_2',Z_3'\}$ and corresponding sequence $M_1,\dots,M_n\in\{X_1,X_2,X_3,Z_1,Z_2,Z_3\}$,*

$$\|M_1\cdots M_n\Psi_AL-\Psi_AM_1'\cdots M_n'L\|_2\le O(n\sqrt{\epsilon}).$$

For any sequence $N_1',\dots,N_n'\in\{X_4',X_5',X_6',Z_4',Z_5',Z_6'\}$ and corresponding sequence $N_1,\dots,N_n\in\{X_4,X_5,X_6,Z_4,Z_5,Z_6\}$,

$$\left\|L\Psi_B^\dagger N_n\cdots N_1-LN_n'\cdots N_1'\Psi_B^\dagger\right\|_2\le O(n\sqrt{\epsilon}).$$ □

Finally, we prove the following proposition, which addresses the image of the L under the isometry $\Psi_A \otimes \Psi_B$. For each $i \in \{1,2,3\}$, let

$$\phi_i^+ \colon Q_i \to Q_{i+3} \tag{31}$$

be defined by

$$\phi_i^+ = \begin{bmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} & 0 \\ 0 & \frac{1}{\sqrt{2}} \end{pmatrix} \end{bmatrix}. \tag{32}$$

(This is a matrix expression for an EPR pair.) Let

$$\phi_i^- = \begin{bmatrix} \frac{1}{\sqrt{2}} & 0 \\ 0 & -\frac{1}{\sqrt{2}} \end{bmatrix} \tag{33}$$

$$\psi_i^+ = \begin{bmatrix} \begin{pmatrix} 0 & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & 0 \end{pmatrix} \end{bmatrix} \tag{34}$$

$$\psi_i^- = \begin{bmatrix} 0 & \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} & 0 \end{bmatrix}. \tag{35}$$

Proposition 12. *Let L, Ψ_A, Ψ_B be the operators from Propositions 9 and 10. Then, for some $L' \colon \mathcal{H}_B \to \mathcal{H}_A$,*

$$\left\| L' \otimes \phi_1^+ \otimes \phi_2^+ \otimes \phi_3^+ - \Psi_A L \Psi_B^\dagger \right\|_2 \leq O(\sqrt{\epsilon}). \tag{36}$$

Proof. Let $P = \Psi_A L \Psi_B^\dagger$. By the score assumption,

$$\left\| X_i' L X_{i+3}' - L \right\|_2 \leq O(\sqrt{\epsilon}) \tag{37}$$

$$\left\| Z_i' L Z_{i+3}' - L \right\|_2 \leq O(\sqrt{\epsilon}), \tag{38}$$

for $i \in \{1,2,3\}$, therefore by Propositions 9 and 10,

$$\left\| X_i P X_{i+3} - P \right\|_2 \leq O(\sqrt{\epsilon}) \tag{39}$$

$$\left\| Z_i P Z_{i+3} - P \right\|_2 \leq O(\sqrt{\epsilon}), \tag{40}$$

Note that $X_i \phi_i^+ X_i = Z_i \phi_i^+ Z_i = \phi_i^+$, while the other Bell states fail significantly to satisfy the same equalities:

$$X_i \phi_i^- X_i = -\phi_i^- \tag{41}$$

$$Z_i \psi_i^+ Z_i = -\psi_i^+ \tag{42}$$

$$Z_i \psi_i^- Z_i = -\psi_i^-. \tag{43}$$

Write

$$P = \sum_{v_1, v_2, v_3} v_1 \otimes v_2 \otimes v_3 \otimes P_{v_1, v_2, v_3}, \tag{44}$$

where v_i varies over $\{\phi_i^+, \phi_i^-, \psi_i^+, \psi_i^-\}$. Conditions (39) and (40) imply that all components P_{v_1,v_2,v_3} except $P_{\phi_1^+,\phi_2^+,\phi_3^+}$ must have Euclidean norm less than $O(\sqrt{\epsilon})$. The desired result follows. □

V. SUMMARY AND CONCLUSIONS

Quantum rigidity allows a classical user to certify manipulations of quantum systems, thus enabling quantum cryptography in a scenario in which the user does not trust her quantum apparatus (device-independent quantum cryptography). In this paper we have expanded the toolbox for the device-independent setting by showing that the magic pentagram game is rigid. In particular, this means that it is possible to certify the existence of 3 ebits using a game that consists of only 20 questions.

In our style of proof we have reduced some of the arguments for rigidity to bare manipulations of sequences of operators (see the proofs in section IV). This style in particular allows us to cleanly handle conditions such as approximate commutativity and anti-commutativity. Such an approach could be useful for proving more general results.

A natural next step would be to try to parallelize our result (following [4, 16, 20–26]) to show that parallel copies of the magic pentagram game can be used to certify a maximally entangled state of arbitrary size. Then, we could try to choose a small subset of the questions from the parallelized game and prove that that subset is adequate to achieve rigidity.

The magic pentagram game is an example of a binary constraint satisfaction XOR game in which every variable appears in exactly two contexts. This class of games was studied in [18], and the author proved that any game in the class that exhibits pseudo-telepathy must in a sense contain either the magic square game or the magic pentagram game (as topological minors of its relational graph). An interesting further direction would be to explore further the consequences for our rigidity result (and [6]) for the class from [18].

ACKNOWLEDGMENTS

The authors would like to thank Cedric Lin for bringing Ref. [18] to our attention, and Matthew McKague for helpful technical discussions about our proofs. AK is funded by the US Department of Defense.

[1] D. Mayers and A. Yao, in *Foundations of Computer Science, 1998. Proceedings. 39th Annual Symposium on* (IEEE, 1998) pp. 503–509.
[2] S. Popescu and D. Rohrlich, Physics Letters A **169**, 411 (1992).
[3] S. J. Summers and R. Werner, Journal of Mathematical Physics **28**, 2440 (1987).
[4] B. W. Reichardt, F. Unger, and U. Vazirani, Nature **496**, 456 (2013).
[5] M. McKague, T. H. Yang, and V. Scarani, Journal of Physics A: Mathematical and Theoretical **45**, 455304 (2012).
[6] X. Wu, J.-D. Bancal, M. McKague, and V. Scarani, Physical Review A **93**, 062121 (2016).

[7] I. Šupić, R. Augusiak, A. Salavrakos, and A. Acín, New Journal of Physics **18**, 035013 (2016).

[8] F. Magniez, D. Mayers, M. Mosca, and H. Ollivier, "Self-testing of quantum circuits," in *Automata, Languages and Programming: 33rd International Colloquium, ICALP 2006, Venice, Italy, July 10-14, 2006, Proceedings, Part I*, edited by M. Bugliesi, B. Preneel, V. Sassone, and I. Wegener (Springer Berlin Heidelberg, Berlin, Heidelberg, 2006) pp. 72–83.

[9] R. Rabelo, L. Y. Zhi, and V. Scarani, Phys. Rev. Lett. **109**, 180401 (2012).

[10] L. Mančinska, "Maximally entangled states in pseudo-telepathy games," in *Computing with New Resources: Essays Dedicated to Jozef Gruska on the Occasion of His 80th Birthday*, edited by C. S. Calude, R. Freivalds, and I. Kazuo (Springer International Publishing, 2014) pp. 200–207.

[11] C. A. Miller and Y. Shi, in *8th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2013)*, Leibniz International Proceedings in Informatics (LIPIcs), Vol. 22, edited by S. Severini and F. Brandao (Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, Dagstuhl, Germany, 2013) pp. 254–262.

[12] Y. Wang, X. Wu, and V. Scarani, New Journal of Physics **18**, 025021 (2016).

[13] C. Bamps and S. Pironio, Phys. Rev. A **91**, 052111 (2015).

[14] N. D. Mermin, Physical Review Letters **65**, 3373 (1990).

[15] R. Jain, C. A. Miller, and Y. Shi, arXiv preprint arXiv:1703.05426v1 (2017).

[16] M. McKague, New Journal of Physics **18**, 045013 (2016).

[17] R. Cleve and R. Mittal, "Characterization of binary constraint system games," in *Automata, Languages, and Programming: 41st International Colloquium, ICALP 2014, Copenhagen, Denmark, July 8-11, 2014, Proceedings, Part I*, edited by J. Esparza, P. Fraigniaud, T. Husfeldt, and E. Koutsoupias (Springer Berlin Heidelberg, Berlin, Heidelberg, 2014) pp. 320–331.

[18] A. Arkhipov, arXiv preprint arXiv:1209.3819 (2012).

[19] N. D. Mermin, Reviews of Modern Physics **65**, 803 (1993).

[20] D. Ostrev, arXiv preprint arXiv:1506.00607 (2015).

[21] D. Ostrev and T. Vidick, arXiv preprint arXiv:1609.01652 (2016).

[22] A. W. Coladangelo, arXiv preprint arXiv:1609.03687 (2016).

[23] A. Natarajan and T. Vidick, in *Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing*, STOC 2017 (ACM, New York, NY, USA, 2017) pp. 1003–1015.

[24] M. McKague, Quantum **1**, 1 (2017).

[25] R. Chao, B. W. Reichardt, C. Sutherland, and T. Vidick, arXiv preprint arXiv:1610.00771 (2016).

[26] M. Coudron and A. Natarajan, arXiv preprint arXiv:1609.06306 (2016).