

A three-player coherent state embezzlement game

Zhengfeng Ji*

Debbie Leung[†]

Thomas Vidick[‡]

Abstract

We introduce a three-player nonlocal game, with a finite number of classical questions and answers, such that the optimal success probability of 1 in the game can only be achieved in the limit of strategies using arbitrarily high-dimensional entangled states. Precisely, there exists a constant $0 < c \leq 1$ such that to succeed with probability $1 - \epsilon$ in the game it is necessary to use an entangled state of at least $\Omega(\epsilon^{-c})$ qubits, and it is sufficient to use a state of at most $O(\epsilon^{-1})$ qubits.

The game is based on the coherent state exchange game of Leung et al. (CJTCS 2013). In our game, the task of the quantum verifier is delegated to a third player by a classical referee. Our results complement those of Slofstra (arXiv:1703.08618) and Dykema et al. (arXiv:1709.05032), who obtained two-player games with similar (though quantitatively weaker) properties based on the representation theory of finitely presented groups and C^* -algebras respectively.

A nonlocal game [CHTW04] is the description of a one-round interaction between a trusted referee, whose actions are prescribed by the game, and multiple spatially isolated players. The players cooperate to succeed in the game, but they are not allowed to communicate. The existence of simple games in which players can increase their odds of succeeding by sharing an entangled state as simple as an EPR pair (as opposed to only sharing classical randomness) has been demonstrated theoretically since the work of Bell [Bel64] in the 1960s and experimentally in a major line of works ranging from the first experiments by Aspect and collaborators [AGR81] in the 1980s to the first loophole-free violations demonstrated in 2015 [HBD⁺15, GVW⁺15, SMSC⁺15]. Aside from their experimental motivation as “tests for quantumness”, nonlocal games have been actively studied in computer science (complexity of interactive proof systems), cryptography (device independence), quantum field theory and functional analysis (commuting and tensor product models for nonlocal correlations).

An outstanding question in the theory of nonlocal games is the quantification of the amount of entanglement required to achieve, or even approach, optimality. For a long time, there was no explicit nonlocal game known for which any optimal strategy provably required more than one, or at most two, qubits of entanglement per player. More recently, a number of examples of nonlocal games requiring a large amount of entanglement have been found, see for example [BBT11, Slo11, Ji13, MV14, CRSV16, CS17b]. However, these games all require an increasing number of questions or answers. In [PV10] the authors identified a Bell inequality, the so-called I_{3322} inequality, that can also be formulated as a two-player game with 3 possible questions and 2 possible answers per player, and gave strong numerical evidence that the optimal violation of the inequality (equivalently, the maximum success probability of players sharing entanglement in the associated game) could only be reached in the limit of arbitrarily high-dimensional entanglement. However, an analytical proof of this fact has remained elusive.

*Centre for Quantum Software and Information, University of Technology Sydney, Australia

[†]University of Waterloo, Canada. Email: wcleung@uwaterloo.ca

[‡]California Institute of Technology, USA. Email: vidick@cms.caltech.edu

In Leung et al. [LTW13], motivated by the discovery of “embezzling states” [vdH03] and to gain insights in the amount of entanglement required of optimal strategies in multi-prover interactive proof systems, the authors introduced a game called the “coherent state exchange game” in which each player receives a 3-dimensional system and returns a qubit. They showed that an optimal success probability of 1 in this game could only be achieved in the limit of strategies using entangled states of arbitrarily large dimension; moreover, they provided precise trade-offs between success probability and dimension. The intuition for the game is simple: the players are tasked with coherently transforming a product state to an EPR pair. A simple application of Fannes’ inequality [Fan73] shows that this can only be accomplished by using an arbitrarily large “reservoir” of entanglement. Such “universal reservoirs”, the embezzlement states introduced in [vdH03], can be used to instantiate arbitrarily close to perfect strategies for the players.

The game considered in [LTW13] is not a nonlocal game in the orthodox sense of the term: in the game the referee is required to prepare a (small) entangled state, and exchange quantum states with the players. Was this a “cheat” that enabled the result, or a hint that a similar property should be achievable with nonlocal games with a classical referee? In [RV15] a step was taken in this direction by adapting the game to one in which questions remain quantum, but answers from the player are classical.

A breakthrough came in a sequence of two works by Slofstra [Slo16, Slo17], who introduced completely different techniques, based on the representation theory of finitely presented groups and a “universal embedding theorem” to obtain nonlocal games from groups. A consequence of Slofstra’s work is the resolution of a decades-old open question on the closure of the set of finite-dimensional quantum correlations, showing that this set is not closed. In particular, there exists a finite game such that the optimum success probability cannot be achieved in any finite dimension, resolving the aforementioned line of questioning in the affirmative.

A different proof for the non-closure of the set of quantum correlations has recently been obtained by Dykema et al. [DPP17]. Although the proof is arguably simpler and more direct (in particular, it yields a two-player game with only 5 questions per player!), it still relies on rather non-trivial mathematical results establishing the non-existence of non-trivial finite-dimensional representations for certain C^* -algebras associated with projections. A drawback of these and Slofstra’s methods is that it may not be obvious to formulate the resulting game explicitly, to gain insights on the physical reason why increasing amounts of entanglement can be required to win with higher probabilities, or to obtain good quantitative estimates on the achievable trade-offs between dimension and success probability (though a step in this direction was recently made by making a special case of Slofstra’s approach quantitative: see [SV17], on which we comment more below).

Our results. In this paper we return to the line of works [LTW13, RV15] exploring the properties of quantum embezzlement, and provide a different, arguably more direct and more intuitive construction of a nonlocal game, with classical questions and answers, whose optimal success probability of 1 can only be achieved in the limit of infinite-dimensional strategies. A benefit is that our construction is fully explicit, and we are able to obtain precise quantitative estimates on the trade-off between dimension and success probability of any strategy. Our analysis shows that any near-optimal strategy for the game we construct must contain, within itself, the ability to “embezzle” an EPR pair from a product state – a task that, according to Fannes’ inequality, can only be achieved with arbitrarily high accuracy using a family of ancilla entangled states that have unbounded entanglement entropy. The impossibility of perfect embezzlement using finite-dimensional entanglement thus provides a natural physical basis for the fact that the optimal success probability of 1 in our game can only be achieved in the limit of infinite-dimensional strategies.

As already mentioned, our starting point is the two-player embezzlement game [LTW13]. We modify the

two-player game with quantum referee into a three-player game with classical referee by turning the quantum referee in the original game into a third player in the new game. The classical referee in the new game classically “delegates” to the third player the preparation of the quantum referee’s messages to the other two players. The transformation follows a similar spirit as a family of more general transformations introduced by Ji [Ji16, Ji17]. It is not clear if the techniques from [Ji16, Ji17] could work here as a black-box. In addition, even if the constructions proposed in those works did lead to nonlocal games with the desired properties, the games would have at least four extra players, and the analysis would be non-trivial. Here, we give a more direct construction, with a simple analysis, that only requires a single additional player.

Our game, called 3EMB, is described in Figure 2. It satisfies the properties described in Theorem 1.

Theorem 1. *There exists a three-player game with the following properties:*

- *There are 12 possible questions to each player. One player replies with 3 bits and the other two each reply with 2 bits.*
- *For any $\varepsilon > 0$ there is $d = O(\varepsilon^{-1})$ and a strategy for the players that succeeds with probability $1 - \varepsilon$ using an entangled state with local dimension 8 for the first player and 2^{d+3} for each of the other two players.*
- *There is a constant $c > 0$ such that for any $\varepsilon > 0$, any strategy for the players that succeeds with probability at least $1 - \varepsilon$ in the game must use an entangled state of local dimension at least $2^{\Omega(\varepsilon^{-c})}$ for two of the players.*

Our game is smaller than the game from [SV17], but larger than the one from [DPP17]; in addition, it requires three players, instead of two for both of these results. Quantitatively, the trade-off between dimension and success probability we obtain is exponentially stronger than the one obtained in [SV17]. (An exponential trade-off of the kind we obtain has long been known for *families* of games, but of course the point of our result is that the trade-off is demonstrated for a single, finite game.)

Discussion. It remains an outstanding open question to determine the size of the smallest game such that the optimal success probability in the game can only be achieved in the limit of infinite-dimensional strategies. All games for which such a result has been shown so far have quantum value 1 (also called “pseudo-telepathy” games), whereas in the case of the I_{3322} inequality, the (still conjectural) separation is for a game with quantum value strictly less than 1. It is interesting to explore what features of entanglement cannot be demonstrated in pseudo-telepathy games.

Due to the fact that optimal strategies for the players in our game are required to perform coherent state embezzlement, the results of [CLP17] imply that there is no perfect infinite-dimensional strategy in the tensor product model, but there is one in the commuting-operator model.¹ As a consequence our game is not a candidate for separating the sets C_q and C_{qs} of correlations achievable using finite-dimensional and infinite-dimensional strategies in the tensor product model respectively; showing such a separation, sometimes referred to as “Tsirelson’s problem”, remains an open problem.

There are reasons to believe that the exponential trade-off between entanglement dimension and success probability demonstrated by our construction may be optimal. Indeed, even if one allows games whose size grows with ε^{-1} (equivalently, if one restricts to “not too small” values of ε), the best scaling known remains

¹We thank Laura Mančinska for pointing out this consequence.

exponential (see e.g. [OV16] for the best known in the case of XOR games). However, no upper bounds are known.

It remains an open question to obtain an exponential scaling for a two-player game. We have no reason to think this is not achievable using current techniques. More generally, it is interesting to investigate possible fundamental differences between properties of entanglement that can be evidenced in two-player games, versus games with three or more players.

Organization. The construction of the game, and its analysis, combines known rigidity results for the GHZ game and the Magic Square games. These games are described in Section 1.2 and combined in Section 2. In Section 3 we introduce the game 3EMB, give intuition for the construction, and prove Theorem 1.

1 Preliminaries

1.1 Notation

\mathcal{H} denotes a finite-dimensional Hilbert space, and $L(\mathcal{H})$ the linear operators on \mathcal{H} . We use indices $\mathcal{H}_A, \mathcal{H}_B$, etc., to index different spaces. We write

$$\sigma_i = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad \text{and} \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad (1)$$

for the standard single-qubit Pauli observables on \mathbb{C}^2 . We sometimes use an additional subscript, $\sigma_{w,R}$ for $w \in \{i, x, y, z\}$, to clarify the space on which a Pauli operator acts: $\sigma_{w,R}$ acts on $\mathcal{H}_R \simeq (\mathbb{C}^2)_R$. We write $|\text{EPR}\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$ for the EPR pair and $|\text{GHZ}\rangle = \frac{1}{\sqrt{2}}|000\rangle + \frac{1}{\sqrt{2}}|111\rangle$ for the 3-qubit GHZ state.

We use the following useful piece of notation:

Definition 2. For finite-dimensional Hilbert spaces $\mathcal{H}_A, \mathcal{H}_B$ and $\mathcal{H}_{A'}$, $\delta > 0$, and operators $R \in L(\mathcal{H}_A)$ and $S \in L(\mathcal{H}_{A'})$ we say that R and S are δ -isometric with respect to $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$, and write $R \simeq_\delta S$, if there exists an isometry $V : \mathcal{H}_A \rightarrow \mathcal{H}_{A'}$ such that

$$\|(R - V^\dagger S V) \otimes I_B |\psi\rangle\| = O(\delta).$$

If V is the identity, then we further say that R and S are δ -equivalent, and write $R \approx_\delta S$ for $\|(R - S) \otimes I_B |\psi\rangle\| = O(\delta)$.

Analogously, for a state $|\phi\rangle$ on $\mathcal{H}_{A'} \otimes \mathcal{H}_{B'}$ we write $|\psi\rangle \simeq_\delta |\phi\rangle$ when there exists isometries $V_A : \mathcal{H}_A \rightarrow \mathcal{H}_{A'}$ and $V_B : \mathcal{H}_B \rightarrow \mathcal{H}_{B'}$ such that $\| |\psi\rangle - V_A \otimes V_B |\phi\rangle \| = O(\delta)$, and $|\psi\rangle \approx_\delta |\phi\rangle$ whenever V_A and V_B are the identity.

The notation $R \simeq_\delta S$ carries some ambiguity, as it does not specify the state $|\psi\rangle$. The latter should always be clear from the context: we will often simply write that R and S are δ -isometric, without explicitly specifying $|\psi\rangle$ or the isometry. The relation is transitive, but not reflexive: the operator on the right will always act on a space of dimension at least as large as that on which the operator on the left acts. The notion of δ -equivalence is both transitive and reflexive, and we will use it as a measure of distance on linear operators.

1.2 Elementary tests

We use the language of tests to describe elementary building blocks used in the construction of our game. A test is a protocol describing an interaction between a trusted verifier and multiple untrusted players. In the test, the verifier selects a question for each player, according to a publicly known distribution. The (ordered) tuple of questions selected by the verifier is called a query. Upon receiving its question, each player has to provide an answer to the verifier. Finally, the verifier decides to accept (in which case we say that the players pass the test) or reject (the players fail), by evaluating a publicly known predicate on the query and the tuple of answers.

We recall two well-known tests. The first is a test such that any players that pass the test with probability close to 1 must use a shared entangled state that is isometric to a GHZ state (we say the test “self-tests” the GHZ state). The second is the Magic Square game, which self-tests two EPR pairs, as well as Pauli σ_x and σ_z measurements on that state.

Theorem 3 (GHZ test, Proposition 4 in [MS12]). *There exists a three-player test GHZ with the following properties.*

1. *The marginal distribution on questions to each player is uniform over $\{x, y\}$;*
2. *Each player replies with a single bit in $\{\pm 1\}$;*
3. *For any pair of anti-commuting binary observables X, Y on \mathcal{H}_i , for each player $i \in \{1, 2, 3\}$, there is a strategy for the players that succeeds with probability 1 and only requires that each player measures her share of an eigenvalue-1 eigenstate of the operator*

$$G(X, Y) = \frac{1}{4}(X \otimes X \otimes X - Y \otimes Y \otimes X - X \otimes Y \otimes Y - Y \otimes X \otimes Y) \in L(\mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \mathcal{H}_3) \quad (2)$$

using the binary observable indicated by her question;

4. *For any $\varepsilon \geq 0$ there is $\delta = O(\sqrt{\varepsilon})$ such that for any strategy with success probability at least $1 - \varepsilon$, there are local isometries on \mathcal{H}_i , $i \in \{1, 2, 3\}$, such that, under the isometries, $|\psi\rangle \simeq_\delta |\text{GHZ}\rangle_{123}|\psi'\rangle$, for some state $|\psi'\rangle$, and a player’s observable W on question $w \in \{x, y\}$ satisfies $W \simeq_\delta \sigma_w$, the Pauli observable acting on the player’s share of $|\text{GHZ}\rangle_{123}$.*

One realization of a game satisfying the above theorem can be stated as follows. The referee draws a random query from the set $\{(x, x, x), (y, y, x), (y, x, y), (x, y, y)\}$ and sends the i -th symbol in the query to the i -th player as her question. The players win if their answers multiply to 1 if the query is (x, x, x) and -1 otherwise.

In the GHZ game, we work with the GHZ state and observables σ_x and σ_y . Yet, when designing the main nonlocal game introduced later, it will be important for us to work with the GHZ state, and simultaneously have access to σ_x and σ_z observables by rigidity. For this reason, in Section 2 we introduce a game that requires two GHZ states and uses a construction motivated by the Magic Square game MS. In the following theorem, we recall some properties of the Magic Square game, a two-player game that self-tests two EPR pairs.

Theorem 4 (Magic Square test, Theorem 5.9 in [CS17a]). *There exists a two-player test MS with the following properties:*

1. Queries (q_1, q_2) in the game, where for $i \in \{1, 2\}$ question q_i goes to the i -th player, are drawn from $\mathcal{Q} \times \mathcal{Q}$, where

$$\mathcal{Q} = \{c_1, c_2, c_3, r_1, r_2, r_3\}. \quad (3)$$

The marginal distribution on questions to each player is uniform over \mathcal{Q} ;

2. Each player replies with 2 bits in $\{\pm 1\}^2$;
3. For each player labeled by $i \in \{1, 2\}$, let \mathcal{H}_i denote the Hilbert space associated with player i 's local system. For any two commuting pairs of anti-commuting binary observables (X_1^i, Z_1^i) and (X_2^i, Z_2^i) acting on \mathcal{H}_i , there is a strategy for the players that succeeds with probability 1 and only requires the measurement of observables obtained as the product of $X_1^i, Z_1^i, X_2^i, Z_2^i$ on an eigenvalue-1 eigenstate of the operator

$$\text{MS}(X, Z) = \frac{1}{2}(X_1^1 \otimes X_1^2 + Z_1^1 \otimes Z_1^2) \cdot \frac{1}{2}(X_2^1 \otimes X_2^2 + Z_2^1 \otimes Z_2^2) \in \text{L}(\mathcal{H}_1 \otimes \mathcal{H}_2);^2$$

4. For any $\varepsilon \geq 0$ there is a $\delta = O(\sqrt{\varepsilon})$ such that for any strategy with success probability at least $1 - \varepsilon$, there are local isometries on \mathcal{H}_i , $i \in \{1, 2\}$, such that, under the isometries, $|\psi\rangle \simeq_\delta |\text{EPR}\rangle_{A_1 B_1} \otimes |\text{EPR}\rangle_{A_2 B_2} \otimes |\psi'\rangle$, for some state $|\psi'\rangle$. In addition, let X_1 and X_2 (resp. Z_2 and Z_1) be the binary observables associated with a player's first and second answer bits on question $r_1 \in \mathcal{Q}$ (resp. $r_2 \in \mathcal{Q}$). Then for $j \in \{1, 2\}$ and $w \in \{x, z\}$, $W_j \simeq_\delta \sigma_{w,j}$, where $\sigma_{w,j}$ is the Pauli σ_w observable acting on the player's j -th qubit. Similar approximations hold for questions c_1 and c_2 , with the associated observables being close to $\sigma_{x,1}$ and $\sigma_{z,2}$, and $\sigma_{x,2}$ and $\sigma_{z,1}$ respectively.

To derive the variant of the Magic Square game used in Theorem 4, recall the standard formulation for the Magic Square as a matrix

$$\begin{bmatrix} xi & ix & xx \\ iz & zi & zz \\ xz & zx & yy \end{bmatrix}. \quad (4)$$

In the formulation of the game from e.g. [Ara04], the first player is sent a question which is a random entry in the matrix, and the second player a question which is a random row or column that contains the first player's question. The first player replies with one bit and the second player replies with 3 bits. The referee accepts if the answers are consistent, and the 3 answer bits of the second player multiply to 1 except if her question is c_3 (the column with entries xx, zz, yy), in which case the product should be -1 . If the players share two EPR pairs, and measure the observables corresponding to the symbols in their questions (turning ww' into the observable $\sigma_w \otimes \sigma_{w'}$) then they always succeed.

We consider the following modifications. First, the questions we consider are always a complete row or a column, and never a single entry of the magic square. This allows us to reduce the number of questions without changing the properties of the game. In addition, for simplicity we consider the uniform distribution on pairs of questions. When the query to the players consists of two copies of the same row or column, the referee checks that both answers from the players match. If two non-intersecting rows or columns are sampled, then the referee automatically accepts. Second, it is sufficient for the players to return the first 2

²In the definition of $\text{MS}(X, Z)$, for each i , for both $j = 1, 2$, the operators X_j^i, Z_j^i act on $H_1 \otimes H_2$, but only nontrivially on H_i . We do not write down the identity operator on $H_{\{1,2\} \setminus \{i\}}$ explicitly. Both $X_1^1 \otimes X_1^2 + Z_1^1 \otimes Z_1^2$ and $X_2^1 \otimes X_2^2 + Z_2^1 \otimes Z_2^2$ are operators in $\text{L}(\mathcal{H}_1 \otimes \mathcal{H}_2)$, and \cdot denotes their product. The subscript j can be interpreted as a label for systems within each player's local Hilbert space in the honest strategy.

bits out of the 3 she obtains, since the winning condition (known to the player) forces the 3rd answer bit to be a deterministic function of the first two.

Note that the soundness analysis (item 4.) only makes claims about the structure of a player's observables associated with the x and z symbols in the questions, not y . As explained in e.g. [RUV13], due to the existence of two inequivalent non-trivial irreducible representations of the Pauli group (related by complex conjugation), this is inevitable.

2 A 3-player rigidity test

In this section we introduce a 3-player test that can only be passed with probability 1 by players who share two copies of the GHZ state, and such that the players' observables associated to a subset of the questions in the test are isometric to σ_x and σ_z Pauli observables on their respective qubits. We obtain the test by combining the standard GHZ test with the MS (Magic Square) test described in the previous section. The reason for using two GHZ states is that the Magic Square test requires two EPR pairs to be passed with probability 1.

We call the resulting test the P3 test. In this test, each player is asked to measure the two commuting two-qubit Pauli operators that are indicated in the first two entries of the row or column of the magic square in Eq. (4) that she receives as her question, and return the outcomes as her answer. These answers are denoted by $a = (a_1, a_2)$, $b = (b_1, b_2)$, and $v = (v_1, v_2) \in \{\pm 1\}^2$ respectively. The row or column sent to each player is chosen independently and uniformly at random by the referee among the 6 possibilities. The referee then checks all possible parity constraints implied by the stabilizers of two GHZ states, among those that can be computed from the players' answers. Suppose those two GHZ states lie on registers $A_1 B_1 V_1$ and $A_2 B_2 V_2$. For example, if the query is (r_1, r_1, r_1) , the measurement outcomes a_1, a_2 correspond to xi, ix on $A_1 A_2$, b_1, b_2 correspond to xi, ix on $B_1 B_2$, v_1, v_2 correspond to xi, ix on $V_1 V_2$, so the referee checks that $a_1 b_1 v_1 = 1$ and $a_2 b_2 v_2 = 1$, which corresponds to the stabilizers $XIXIXI$ and $IXIXIX$ on $A_1 A_2 B_1 B_2 V_1 V_2$. If the query is (r_1, r_3, c_3) , a_1, a_2 correspond to xi, ix on $A_1 A_2$, b_1, b_2 correspond to xz, zx on $B_1 B_2$, v_1, v_2 correspond to xx, zz on $V_1 V_2$, so the referee checks $a_1 a_2 b_1 b_2 v_1 v_2 = -1$, for the corresponding stabilizer $XXYYYY$.

The complete test is described in Figure 1. Intuitively, the P3 test embeds the Magic Square test as a three-player test, where two players in P3 jointly play the role of a single player in the Magic Square game by measuring certain logical X, Z observables.

Theorem 5 (3-player Pauli test). *There exists a three-player test P3, described in Figure 1, with the following properties.*

1. *The marginal distribution on questions to each player is uniform over the set \mathcal{Q} defined in (3);*
2. *Each player replies with two bits in $\{\pm 1\}^2$;*
3. *For $i \in \{1, 2, 3\}$, let \mathcal{H}_i be a Hilbert space, and let (X_1, Y_1, Z_1) and (X_2, Y_2, Z_2) be any two commuting triples of observables satisfying the Pauli relations acting on \mathcal{H}_i . Then, there is a strategy for the players that succeeds with probability 1 and only requires the measurement of observables obtained as the product of $X_1, Y_1, Z_1, X_2, Y_2, Z_2$ on an eigenvalue-1 eigenstate of the operator $G(X_1, Y_1) \cdot G(X_2, Y_2)$, where $G(\cdot, \cdot)$ is as in (2);*
4. *For any $\varepsilon \geq 0$ there is $\delta = O(\varepsilon^{1/4})$ such that for any strategy with success probability at least $1 - \varepsilon$, there are local isometries on \mathcal{H}_i , $i \in \{1, 2, 3\}$, such that, under the isometries, $|\psi\rangle \simeq_\delta$*

Let \mathcal{Q} be the question set defined in (3). The referee selects a query (q_1, q_2, q_3) from $\mathcal{Q} \times \mathcal{Q} \times \mathcal{Q}$ uniformly at random, and sends one question to each player. Each player responds with two bits denoted by $a, b, v \in \{\pm 1\}^2$ respectively.

For each query $q \in \mathcal{Q}$, let G_q be the group generated by the commuting two-qubit Pauli operators indicated in the corresponding row or column of the magic square described in Eq. (4). The group G_q always contains four elements. Two of these elements are indexed by the first two entries in the row or column, and to these elements are associated the players' first two answers. In all cases except for the third column, the product of these elements is the third entry in the row or column, and to it the referee associates the product of the players' answers. For the case of the third column c_3 , the value associated to the last square is the opposite of the product of the players' answers.

If there is an operator $P \in G_{q_1} \times G_{q_2} \times G_{q_3}$ such that either P or $-P$ is a stabilizer of the tensor product of two GHZ states, the referee rejects whenever the associated parity computed from the players' answers does not equal $+1$ or -1 respectively. In all other cases, the verifier accepts.

Figure 1: Description of the test P3.

$|\text{GHZ}\rangle_{123}|\text{GHZ}\rangle_{123}|\psi'\rangle$ and for each player, the observables X_1, X_2 associated with the first and second answer bit to question r_1 and observables Z_2, Z_1 associated with the first and second answer bits to question r_2 satisfy $X_j \simeq_\delta \sigma_{x,j}$ and $Z_j \simeq_\delta \sigma_{z,j}$, where $\sigma_{w,j}$ is the Pauli σ_w observable acting on the player's j -th qubit for $w \in \{x, z\}$.

Remark 6. The soundness guarantees provided by Theorem 5 are analogous to those of Theorem 4, except that they apply to a 3-player test, two copies of the GHZ state, and the σ_x, σ_z observables. The soundness parameter δ has a worse dependence on ε , with an exponent $1/4$ instead of $1/2$. We did not try to optimize the exponent and expect it should be possible to improve it.

Proof. The first and second items are clear from the definition of the test in Figure 1. To show the third, we describe a successful strategy for the players. Since X_j, Y_j, Z_j satisfy the Pauli relations they are isomorphic to either the standard Pauli matrices (1) or their complex conjugate. For simplicity, assume the former, so that each of the three players, upon receiving the question q , measures the first two commuting two-qubit Pauli operators in the corresponding row or column. As the referee only verifies the constraints implied by the stabilizer of the two GHZ states, it is immediate that the players succeed with probability 1.

We now show item 4., soundness. Consider a strategy for the players, using an arbitrary shared state $|\psi\rangle$ and projective measurements on that state, that succeeds with probability at least $1 - \varepsilon$.

As the players' strategy uses projective measurement with four outcomes, they each define two observables. For each entry m in the magic square, we define two observables, R_m for the row and C_m for the column. For example, row observables R_{xi}, R_{ix} and R_{xx} are derived from the four-outcome measurement applied by a player upon receiving question r_1 . Similarly, observables C_{xx}, C_{zz} and C_{yy} are derived from the measurement applied by a player upon receiving question c_3 . By definition, observables R_m taken from the same row, or observables C_m taken from the same column, commute with each other.

We show that for any of the nine possible values for m , the two observables R_m and C_m are close in the state-dependent distance. That is, the observables are almost identical, irrespective of whether the entry was asked as part of a row or a column. We show this for the example of the entry $m = xz$ asked to the first player; all other cases follow by a similar argument.

The first step is to observe that it is always possible to select an element in the stabilizer group of $|\text{GHZ}\rangle^{\otimes 2}$ such that the first two tensor components (corresponding to the first qubit of each GHZ state) are $\sigma_{x,1}$ and $\sigma_{z,2}$. Here we can for example choose $\sigma_{x,1}\sigma_{z,2} \otimes \sigma_{x,1}\sigma_{z,2} \otimes \sigma_{x,1}\sigma_{i,2}$. In general, for any $m = rs$, we can find a stabilizer of $|\text{GHZ}\rangle$ with the first tensor component being σ_r , since the stabilizer group of $|\text{GHZ}\rangle$ includes $\sigma_x \otimes \sigma_x \otimes \sigma_x$ and $\sigma_z \otimes \sigma_z \otimes \sigma_i$, and similarly for σ_s . Tensoring these two stabilizers gives a stabilizer of $|\text{GHZ}\rangle^{\otimes 2}$ with $\sigma_{r,1}\sigma_{s,2}$ acting on the first qubits of the two GHZ states.

As a second step, for precisely the same reason the chosen stabilizer can always be recovered from two distinct queries, the first with a row question involving m to the first player, and the second with a column question involving m to the first player. Here, the two queries are (r_3, r_3, r_1) and (c_1, r_3, r_1) . For the case of (r_3, r_3, r_1) , one of the constraints verified by the referee is $a_1 b_1 v_1 = 1$, which implies that

$$R_{xz} \otimes I \otimes I \approx_{\sqrt{\epsilon}} I \otimes R_{xz} \otimes R_{xi}. \quad (5)$$

Similarly, for question (c_1, r_3, r_1) , the referee's check implies that

$$C_{xz} \otimes I \otimes I \approx_{\sqrt{\epsilon}} I \otimes R_{xz} \otimes R_{xi}.$$

Combining the above two equations establishes that

$$R_{xz} \approx_{\sqrt{\epsilon}} C_{xz}.$$

Having shown analogous relations for each possible entry m in the square, it follows that the set of operators R_m approximately satisfies all the algebraic constraints for the operators in the magic square (4), i.e. they approximately multiply to the identity or its opposite for each row or column, as required. For example, $R_{xi}R_{ix}R_{xx} = I$ follows simply by definition of these observables. On the other hand, $R_{xx}R_{zz}R_{yy} \approx -I$ follows from the same using the column observables, which holds by definition, and the approximation $R_m \approx C_m$ shown above.

It is then straightforward to devise a strategy for the two-player Magic Square test in which the first player determines her answers by measuring the observables R_m , and the role of the second player in the game is played by a joint strategy for the second and third players here, where each player measures the required observable that follows from using (5) and analogous relations that hold for each possible entry. From the previous analysis it follows that the resulting strategy succeeds in the Magic Square test with probability at least $1 - O(\sqrt{\epsilon})$. Applying Theorem 4 it follows that there exists a local isometry such that

$$R_{wi} \simeq_{\delta} \sigma_{w,1} \quad R_{iw} \simeq_{\delta} \sigma_{w,2},$$

for some $\delta = O(\epsilon^{1/4})$ and all $w \in x, z$.

To conclude, recall that by definition, $X_1 = R_{xi}$, $X_2 = R_{ix}$, $Z_1 = R_{zi}$ and $Z_2 = R_{iz}$. The characterization of the shared state claimed in item 4 follows from the form for X_j and Z_j described above, and the definition of the test, which in particular implies that the state is stabilized by $X_j \otimes X_j \otimes X_j$, $Z_j \otimes Z_j \otimes I$, and $I \otimes Z_j \otimes Z_j$, for $j \in \{1, 2\}$. \square

3 Coherent state exchange with three players

In this section we describe our main result, a three-player game between a classical referee and three players that has the property that the optimal success probability of 1 can only be achieved in the limit of arbitrarily

high-dimensional entanglement. The first player in the game is called the “virtual verifier”, P_V . The remaining two players are referred to using symbols P_A, P_B respectively. The game, called the 3EMB game, is described in Figure 2. We first give some intuition behind the game. In Section 3.1 we exhibit a family of strategies for the players in the game, using states of growing dimension and with success probability that goes to 1. In Section 3.2 we show that any strategy for the players with success close to 1 in the game must use an entangled state that has large local dimension.

The referee interacts with three players, labeled P_V, P_A and P_B . Each player receives a question taken from the set $\{0, 1\} \times \mathcal{Q}$, where \mathcal{Q} is specified in (3). We use the symbol π_V, π_A, π_B to denote the first component (lying in $\{0, 1\}$) of the question to P_V, P_A and P_B respectively. It will always be the case that $\pi_A = \pi_B = \pi$. In the game, P_V should reply with 3 bits $(u, v) \in \{0, 1\} \times \{\pm 1\}^2$, while P_A, P_B each reply with 2 bits $a, b \in \{\pm 1\}^2$ respectively. Let $v = (v_1, v_2), a = (a_1, a_2), b = (b_1, b_2)$.

The referee performs either of the following tests chosen at random with equal probability:

- (a) The referee sets $\pi_V = \pi = 0$. He executes the test P3 with the three players, inserting the question from P3 as the second component of their question, and checking validity of the triple (v, a, b) extracted from the players’ answers as would the verifier in P3.
- (b) The referee sets $\pi_V = 1$ and $\pi = 0$. The second component of P_V ’s question is chosen uniformly at random from \mathcal{Q} . The referee performs either of the following with equal probability:
 - (i) Send both P_A and P_B the question r_2 . Let a_1 and a_2 be the answers associated with entries iz and zi respectively. Reject if $a_1 = 1$ and $((u = 0$ and $a_2 = -1)$ or $(u = 1$ and $a_2 = 1))$. Accept in all other cases.
 - (ii) Send both P_A and P_B the question c_1 . Let a_1 and a_2 be the answers associated with entries xi and iz respectively. Reject if $a_2 = -1$ and $((u = 0$ and $a_1 b_1 = -1)$ or $(u = 1$ and $a_1 b_1 = 1))$. Accept in all other cases.
- (c) The referee sets $\pi_V = 1$ and $\pi = 0$. He sets the second component of P_V ’s question to r_2 . He sends both P_A and P_B the same question, r_2 . The referee rejects if $a_1 \neq v_2$ or $b_1 \neq v_2$.
- (d) The referee sets $\pi_V = \pi = 1$, and executes the test P3 as in part (a). If $u = 0$ the referee accepts if and only if the players’ answers (v, a, b) pass the test P3. If $u = 1$ the referee always accepts.

Figure 2: Description of the game 3EMB.

Before giving details of the analysis, we provide intuition behind the construction of the game. As in [LTW13, RV15] the referee’s goal in the game is to force P_V, P_A and P_B to perform the transformation (normalization omitted)

$$|0\rangle_V |00\rangle_{A_1 B_1} |00\rangle_{A_2 B_2} + |1\rangle_V |\text{EPR}\rangle_{A_1 B_1} |11\rangle_{A_2 B_2} \rightarrow |0\rangle_V |00\rangle_{A_1 A_2} |00\rangle_{B_1 B_2} + |1\rangle_V |11\rangle_{A_1 B_1} |11\rangle_{A_2 B_2}. \quad (6)$$

Due to the EPR pair having one e-bit of entanglement, as opposed to the state $|11\rangle$ being a product state, the transformation (6) can be performed using operations local to V, A and B *only* by exploiting a large ancilla register that is used to “embezzle” the e-bit of entanglement.

The game 3EMB has two overlapping sub-games, indicated by a bit $\pi_V \in \{0, 1\}$ for P_V , and $\pi = \pi_A =$

$\pi_B \in \{0, 1\}$ for P_A and P_B . The first sub-game, for $\pi_V = \pi = 0$ (part (a) in Figure 2), uses the test P3 to constrain the players to share two copies of the GHZ state, on which they measure σ_x and σ_z Pauli observables (embedded in questions in \mathcal{Q}).

When $\pi_V = 1$, player P_V is tasked to perform a special measurement, which is obtained by applying a controlled-Hadamard from the qubit associated with his share of the second GHZ state, to the qubit associated with the first, followed by a measurement of the first qubit in the σ_z basis. This yields the outcome labeled u . The goal of parts (b) and (c) of the game is to verify that P_V applies precisely this measurement.

In the case P_V obtained the measurement outcome $|0\rangle$ on the first qubit, it is a simple calculation (see Section 3.1) to verify that the three players share a state that is locally isometric to the state on the left-hand side of (6). Now, observe that if the referee sometimes requires the three players to execute the test P3 on the second and third copies of the GHZ state, then conditioned on $u = 0$, in order to have a chance to succeed P_A and P_B have to execute the transformation (6), which brings the second copy in a state that is locally isometric to a GHZ state. That they are able to achieve this is checked in part (d) of the game.

Note that the bits π_V and π are chosen so that P_V can distinguish part (a) from parts (b), (c) and (d), while P_A and P_B can distinguish parts (a), (b) and (c) from part (d). This allows the rigidity results obtained from the analysis of part (a) to carry over to the analysis of parts (b) and (c): even though P_V can distinguish those parts, P_A and P_B cannot, and P_V cannot cheat on his own. But now if P_V plays parts (b) and (c) honestly, using the fact that he cannot distinguish parts (b), (c) and (d), P_A and P_B have to play part (d) honestly as well.

3.1 Completeness

We specify a sequence of strategies with growing dimension whose success probability approaches 1. The strategies follow closely the intuition for the game described earlier.

Lemma 7. *For any integer $d \geq 1$ there exists a strategy for the players in 3EMB in which P_V has three qubits and P_A and P_B each has $d + 3$ qubits, such that the strategy is accepted with probability 1 in parts (a), (b) and (c) of the game, and with probability $1 - O(1/d)$ in part (d).*

For any integer $d \geq 1$, define an *embezzlement state*

$$|\Gamma_d\rangle_{A'B'} = \frac{1}{\sqrt{N_d}} \sum_{j=1}^d |11\rangle_{A'B'}^{\otimes j} |\text{EPR}\rangle_{A'B'}^{\otimes (d-j)},$$

where $|\text{EPR}\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$ and N_d is a normalization constant such that $\| |\Gamma_d\rangle \| = 1$. We think of $|\Gamma_d\rangle$ as a bipartite state on $\mathcal{H}_{A'} \otimes \mathcal{H}_{B'} \simeq (\mathbb{C}^2)_{A'}^{\otimes d} \otimes (\mathbb{C}^2)_{B'}^{\otimes d}$. This state has the property that there exists “left-shift” unitaries $W_{AA'}$ on $\mathbb{C}_A^2 \otimes \mathcal{H}_{A'}$ and $W_{BB'}$ on $\mathbb{C}_B^2 \otimes \mathcal{H}_{B'}$ such that

$$|\langle 11|_{AB} \langle \Gamma_d|_{A'B'} (W_{AA'} \otimes W_{BB'}) |\text{EPR}\rangle_{AB} |\Gamma_d\rangle_{A'B'}| \geq 1 - O(1/d). \quad (7)$$

Proof of Lemma 7. We define a strategy for the players in 3EMB. The players share

$$|\phi\rangle = |\text{GHZ}\rangle_{V_1 A_1 B_1} |\text{GHZ}\rangle_{V_2 A_2 B_2} |\text{GHZ}\rangle_{V_3 A_3 B_3} |\Gamma_d\rangle_{A'B'}. \quad (8)$$

Here each of the registers V_j , A_j and B_j , for $j \in \{1, 2, 3\}$, is isomorphic to \mathbb{C}^2 , and the registers A' and B' each has dimension 2^d . Player P_V holds registers $V_1 V_2 V_3$, P_A has $A_1 A_2 A_3 A'$, and P_B has $B_1 B_2 B_3 B'$.

When $\pi_V = \pi = 0$, each player follows the honest strategy for P3 using her first and second qubits (item 3. in Theorem 5).

If $\pi_V = 1$, P_V performs a projective measurement $\Pi = \{\Pi^0, \Pi^1\}$ on his registers $V_1 V_2$, where

$$\Pi^0 = |0\rangle\langle 0|_{V_1} \otimes |0\rangle\langle 0|_{V_2} + |+\rangle\langle +|_{V_1} \otimes |1\rangle\langle 1|_{V_2}, \quad \Pi^1 = |1\rangle\langle 1|_{V_1} \otimes |0\rangle\langle 0|_{V_2} + |-\rangle\langle -|_{V_1} \otimes |1\rangle\langle 1|_{V_2}. \quad (9)$$

The outcome determines her first answer bit $u \in \{0, 1\}$. The player then applies a Hadamard on register V_1 , controlled on register V_2 . (The measurement and the controlled-Hadamard have the same effect as a controlled-Hadamard followed by a measurement in the σ_z eigenbasis on V_1 .) We can already verify that this strategy succeeds with probability 1 in part (b) of the test, which only depends on P_V 's answer u . For $u = 0$ and 1, the post-measurement states of all players, after P_V has applied the controlled-Hadamard, are

$$|\phi_0\rangle = |0\rangle_{V_1} \otimes \frac{1}{\sqrt{2}} \left(|0\rangle_{V_2} |00\rangle_{A_1 B_1} |00\rangle_{A_2 B_2} + |1\rangle_{V_2} |\text{EPR}\rangle_{A_1 B_1} |11\rangle_{A_2 B_2} \right) \otimes |\text{GHZ}\rangle_{V_3 A_3 B_3} \otimes |\Gamma_d\rangle_{A'B'}, \quad (10)$$

$$|\phi_1\rangle = |1\rangle_{V_1} \otimes \frac{1}{\sqrt{2}} \left(|0\rangle_{V_2} |11\rangle_{A_1 B_1} |00\rangle_{A_2 B_2} + |1\rangle_{V_2} |\text{EPR}^-\rangle_{A_1 B_1} |11\rangle_{A_2 B_2} \right) \otimes |\text{GHZ}\rangle_{V_3 A_3 B_3} \otimes |\Gamma_d\rangle_{A'B'}, \quad (11)$$

where $|\text{EPR}^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$.

In case (i), assuming $a_1 = 1$ (projecting onto $|0\rangle_{A_2}$) then $a_2 = 1$ (having the state $|0\rangle_{A_1}$) with certainty and the referee accepts. In case (ii), assuming $a_2 = -1$ (projecting onto $|1\rangle_{A_2}$) we have $a_1 b_1 = 1$ with certainty (since $\sigma_x \otimes \sigma_x$ stabilizes $|\text{EPR}\rangle$), so again the referee accepts.

To analyze part (c) we complete the description of P_V 's strategy when $\pi_V = 1$. After the measurement to obtain u , P_V takes the second part of the question and applies the honest strategy in game P3 using the appropriate Pauli operators on his registers V_2 and V_3 . It is then straightforward to verify that in both cases, $u = 0$ or $u = 1$, the players are accepted with certainty (note that by definition P_V 's answer v_1 is obtained by measuring σ_z on register V_2).

Note that P_A and P_B play parts (a), (b) and (c) using the same strategy (indeed, they have to, since they cannot distinguish questions coming from either of those parts of the game).

Finally we analyze part (d) (when $\pi_V = \pi = 1$). First note that P_V necessarily plays as already described in part (c). Next we define a strategy for P_A and P_B . Since in part (d) the referee always accepts in case P_V reports $u = 1$, it suffices to examine the players' strategy in case $u = 0$. In this case, after P_V has measured using Π and applied the controlled-Hadamard, the post-measurement state of all players is as in (10). Player P_A (resp. P_B) performs a controlled-unitary $W_{A_1 A'}$ (resp. $W_{B_1 B'}$) as described in (7), controlled on the register A_2 (resp. B_2). By (7) the resulting state has overlap $1 - O(1/d)$ with the state

$$|0\rangle_{V_1} \otimes \frac{1}{\sqrt{2}} \left(|0\rangle_{V_2} |00\rangle_{A_1 A_2} |00\rangle_{B_1 B_2} + |1\rangle_{V_2} |11\rangle_{A_1 B_1} |11\rangle_{A_2 B_2} \right) \otimes |\text{GHZ}\rangle_{V_3 A_3 B_3} |\Gamma_d\rangle_{A'B'}.$$

The player then applies a controlled- σ_x operation on register A_1 (resp. B_1), controlled on A_2 (resp. B_2). This brings the state $O(1/d)$ -close to

$$|000\rangle_{V_1 A_1 B_1} \otimes \frac{1}{\sqrt{2}} \left(|0\rangle_{V_2} |0\rangle_{A_2} |0\rangle_{B_2} + |1\rangle_{V_2} |1\rangle_{A_2} |1\rangle_{B_2} \right) \otimes |\text{GHZ}\rangle_{V_3 A_3 B_3} |\Gamma_d\rangle_{A'B'}. \quad (12)$$

At this point the player applies the honest strategy for the test P3 on the second and third copies of $|\text{GHZ}\rangle$. Together with P_V 's strategy, due to the small discrepancy between the players' shared state and the ideal state in (12), the players succeed with probability $1 - O(1/d)$ in part (d). \square

3.2 Soundness

For the soundness analysis we rely on the following fact, implicit in [LTW13, Section 3] (building on results in [vdH03, Fan73]) and stated as Fact 5.7 in [RV15].

Fact 8. *Let n, t be integers, $U, V \in L(\mathbb{C}^n \otimes \mathbb{C}^t)$ arbitrary operators of norm at most 1, and $|\varphi\rangle \in \mathbb{C}^n \otimes \mathbb{C}^n$, $|\Psi\rangle \in \mathbb{C}^t \otimes \mathbb{C}^t$ of unit norm. Let S be the von Neumann entropy of the reduced density matrix of $|\varphi\rangle$ on any of the two subsystems, and assume $S \geq 1$. Then*

$$1 - |\langle \varphi | \langle \Psi | U \otimes V | 0^n 0^n \rangle | \Psi \rangle|^2 \geq \min \left\{ \frac{1}{4e^2}, \frac{S^2}{16 \log^2(3t)} \right\}.$$

We show the following.

Lemma 9. *Suppose a strategy for the players succeeds with probability at least $1 - \varepsilon$ in the three-player game 3EMB described in Figure 2. Then the players must use an entangled state such that the local dimension of players P_A and P_B is at least $2^{\Omega(\varepsilon^{-c})}$, for some constant $c > 0$.*

Proof. Fix a strategy for the players that succeeds with probability at least $1 - \varepsilon$ in the game. Let $|\psi\rangle_{VAB} \in \mathcal{H}_V \otimes \mathcal{H}_A \otimes \mathcal{H}_B$ be the players' entangled state. We examine the consequences of the players' strategy having success probability at least $1 - 4\varepsilon$ in each of the four parts of the game one after the other.

Part (a). Applying item 4. from Theorem 5, for $D \in \{V, A, B\}$ there exists an isometry $W_D : \mathcal{H}_D \rightarrow \mathbb{C}_{D_1}^2 \otimes \mathbb{C}_{D_2}^2 \otimes \mathcal{H}_{D'}$ such that, under this isometry, the four-outcome POVM applied by a player to determine answers to a question of the form $w_1 w_2 \in \mathcal{P}$ (when $\pi = 0$) is isometric to the four-outcome POVM induced by Pauli σ_{w_1} (when $w_1 \in \{x, z\}$) and σ_{w_2} (when $w_2 \in \{x, z\}$) acting on D_1 and D_2 respectively, up to an error $\delta_1 = O(\varepsilon^{1/4})$. Moreover, under all three isometries,

$$|\psi\rangle_{VAB} \simeq_{\delta_1} |\text{GHZ}\rangle_{V_1 A_1 B_1} |\text{GHZ}\rangle_{V_2 A_2 B_2} |\psi'\rangle_{V' A' B'} , \quad (13)$$

for some tripartite state $|\psi'\rangle$.

For the remainder of the proof we modify the players' strategy to incorporate the isometry, and change their shared state to match exactly the state on the right-hand side of (13); we keep the same notation $|\psi\rangle_{VAB}$ for the modified state. The success probability of this modified strategy in parts (b), (c) and (d) of the game is at least $1 - \varepsilon_1$ for some $\varepsilon_1 = O(\varepsilon + \delta_1) = O(\delta_1) = O(\varepsilon^{1/4})$.

Part (b). When $\pi_V = 1$, P_V applies an eight-outcome POVM measurement that we may assume to be projective. Let w denote the second component of the question to P_V . For any value for w , let $\Pi_{w,V} = \Pi_{w,V}^0 - \Pi_{w,V}^1$ denote a binary observable associated with P_V 's first answer bit, $u \in \{0, 1\}$.

Consider the binary observable defined on $\mathbb{C}_{A_1}^2 \otimes \mathbb{C}_{A_2}^2 \otimes \mathbb{C}_{B_1}^2 \otimes \mathbb{C}_{B_2}^2$ by

$$R_{AB} = \sigma_{z,A_1} \otimes |0\rangle\langle 0|_{A_2} + \sigma_{x,A_1} \otimes |1\rangle\langle 1|_{A_2} \otimes \sigma_{x,B_1} .$$

Then we claim that for any w ,

$$\Pi_{w,V} \otimes R_{AB} \approx_{\sqrt{\varepsilon_1}} I . \quad (14)$$

To show (14) we decompose the -1 eigenspace of the observable $\Pi_{w,V} \otimes R_{AB}$ into a sum of two components, such that the overlap of each component with $|\psi\rangle$ can be bounded from the assumption that the strategy succeeds with probability $1 - \varepsilon_1$ in part (b). The first component,

$$\Pi_{w,V}^1 \otimes \left(|0\rangle\langle 0|_{A_1} \otimes |0\rangle\langle 0|_{A_2} + (|++\rangle\langle ++|_{A_1 B_1} + |--\rangle\langle --|_{A_1 B_1}) \otimes |1\rangle\langle 1|_{A_2} \right),$$

corresponds to rejection for the $u = 1$ cases of (i) and (ii) in part (b). The second component,

$$\Pi_{w,V}^0 \otimes \left(|1\rangle\langle 1|_{A_1} \otimes |0\rangle\langle 0|_{A_2} + (|+-\rangle\langle +-|_{A_1 B_1} + |-+\rangle\langle -+|_{A_1 B_1}) \otimes |1\rangle\langle 1|_{A_2} \right),$$

corresponds to rejection for the $u = 0$ cases. This shows (14). Let $\Pi'_V = \sigma_{z,V_1} \otimes |0\rangle\langle 0|_{V_2} + \sigma_{x,V_1} \otimes |1\rangle\langle 1|_{V_2}$. Using the fact that the GHZ state is stabilized by $\sigma_{z,V_1} \otimes \sigma_{z,A_1}$ as well as by $\sigma_{x,V_1} \otimes \sigma_{x,A_1} \otimes \sigma_{x,B_1}$, it follows that $\Pi'_V \otimes R_{AB}|\psi\rangle = |\psi\rangle$. Together with (14), we have shown that $\Pi_{w,V} \approx_{\varepsilon_1} \Pi'_V$ for all w ; in particular $\Pi_{w,V}$ does not depend on w (to the extent that only its action on $|\psi\rangle$ is considered), and for the remainder of the proof we drop the subscript w .

Part (c). Let Z_1 be the observable associated with P_V 's outcome $v_2 \in \{\pm 1\}$ when the second component of his question is r_2 . Using the fact that $|\text{GHZ}\rangle_{V_2 A_2 B_2}$ is stabilized by $\sigma_z \otimes \sigma_z$ acting on $V_2 A_2$ or $V_2 B_2$, success $1 - \varepsilon_1$ in this part enforces that

$$Z_1 \approx_{\sqrt{\varepsilon_1}} \sigma_{z,V_2}. \quad (15)$$

Part (d). From the analysis of part (b) we deduce that conditioned on the referee choosing to execute part (d), and on the outcome $u = 0$ having been obtained from P_V , the joint state of the players (irrespective of the choice of question w to P_V) is

$$|\psi''\rangle \simeq_{\delta_2} \frac{1}{\sqrt{2}} (|00\rangle_{V_1 V_2} |00\rangle_{A_1 B_1} |00\rangle_{A_2 B_2} + |+\rangle_{V_1} |1\rangle_{V_2} |\text{EPR}\rangle_{A_1 B_1} |11\rangle_{A_2 B_2}) \otimes |\psi'\rangle_{V_A B'},$$

for some $\delta_2 = O(\sqrt{\varepsilon_1}) = O(\varepsilon^{1/8})$. From part (c) we also know that P_V 's observable Z_1 associated with answer v_2 to question r_2 satisfies (15). By item 4. from Theorem 5, for the players' strategy to succeed with probability $1 - \varepsilon_1$ in part (d) it is necessary that the observable X_1 associated with P_V 's answer v_1 on question r_1 approximately anti-commutes with Z_1 on $|\psi''\rangle$, up to an error $\varepsilon_2 = O(\varepsilon_1^{1/4}) = O(\varepsilon^{1/16})$. Using (15), it follows that $X_1 \approx_{\varepsilon_2} |0\rangle\langle 1|_{V_2} \otimes U + |1\rangle\langle 0|_{V_2} \otimes U^\dagger$, for some unitary U on $V_1 V'$. Using again item 4. of Theorem 5, success in part (d) also implies that $X_1 \otimes X_{1,A} \otimes X_{1,B}$ approximately stabilizes $|\psi''\rangle$, where $X_{1,A}$ and $X_{1,B}$ are observables associated with P_A and P_B 's outcome a_1 and b_1 on question x_{1,i_2} respectively. Thus

$$\left| \langle 0|_{V_1} \langle \psi' |_{V_A B'} \langle 11|_{A_2 B_2} \langle \text{EPR} |_{A_1 B_1} (U_{V_1 V'} \otimes X_{1,A} \otimes X_{1,B}) |00\rangle_{A_1 B_1} |00\rangle_{A_2 B_2} |\psi'\rangle_{V_A B'} |+\rangle_{V_1} \right| \geq 1 - \delta_3,$$

for some $\delta_3 = O(\delta_2 + \varepsilon_2) = O(\varepsilon^{1/16})$. Expanding out registers $V_1 V'$ of $|+\rangle_{V_1} |\psi'\rangle_{V_A B'}$ in the eigenbasis of U , we obtain a distribution $\{|\alpha_k|^2\}_k$ and a family of states $\{|\psi^{(k)}\rangle_{A' B'}\}_k$ such that

$$\sum_k |\alpha_k|^2 \left| \langle \psi^{(k)} |_{A' B'} \langle 11|_{A_2 B_2} \langle \text{EPR} |_{A_1 B_1} (X_{1,A} \otimes X_{1,B}) |00\rangle_{A_1 B_1} |00\rangle_{A_2 B_2} |\psi^{(k)}\rangle_{A' B'} \right| \geq 1 - O(\delta_3).$$

By Fact 8 applied with $n = 2$ and $|\varphi\rangle = |\text{EPR}\rangle$ we deduce the claimed lower bound on the dimension of the players' strategy. In particular, $\frac{1}{16 \log^2(3t)} \leq O(\delta_3) = O(\varepsilon^{1/16})$, so, $t = 2^{\Omega(\varepsilon^{-1/32})}$. \square

4 Acknowledgements

We thank William Sloftra and John Watrous for helpful discussions. Part of this work was conducted when ZJ was visiting the Institute for Quantum Computing in the University of Waterloo, and also when DL and TV were attending the “Quantum Physics of Information” program at the Kavli Institute for Theoretical Physics. This research was supported in part by the National Science Foundation under Grant No. NSF PHY 17-48958. DL is supported by an NSERC Discovery grant and a CIFAR research grant via the Quantum Information Science program. TV is supported by NSF CAREER Grant CCF-1553477, AFOSR YIP award number FA9550-16-1-0495, a CIFAR Azrieli Global Scholar award, and the IQIM, an NSF Physics Frontiers Center (NSF Grant PHY-1125565) with support of the Gordon and Betty Moore Foundation (GBMF-12500028).

References

- [AGR81] Alain Aspect, Philippe Grangier, and Gérard Roger. Experimental tests of realistic local theories via Bell’s theorem. *Physical review letters*, 47(7):460, 1981.
- [Ara04] PK Aravind. Quantum mysteries revisited again. *American Journal of Physics*, 72(10):1303–1307, 2004.
- [BBT11] Jop Briët, Harry Buhrman, and Ben Toner. A generalized Grothendieck inequality and non-local correlations that require high entanglement. *Communications in Mathematical Physics*, 305(3):827–843, 2011.
- [Bel64] John S. Bell. On the Einstein-Podolsky-Rosen paradox. *Physics*, 1:195–200, 1964.
- [CHTW04] Richard Cleve, Peter Hoyer, Benjamin Toner, and John Watrous. Consequences and limits of nonlocal strategies. In *Computational Complexity, 2004. Proceedings. 19th IEEE Annual Conference on*, pages 236–249. IEEE, 2004.
- [CLP17] Richard Cleve, Li Liu, and Vern I Paulsen. Perfect embezzlement of entanglement. *Journal of Mathematical Physics*, 58(1):012204, 2017.
- [CRSV16] Rui Chao, Ben W Reichardt, Chris Sutherland, and Thomas Vidick. Test for a large amount of entanglement, using few measurements. *arXiv preprint arXiv:1610.00771*, 2016.
- [CS17a] Andrea Coladangelo and Jalex Stark. Robust self-testing for linear constraint system games. *arXiv preprint arXiv:1709.09267*, 2017.
- [CS17b] Andrea Coladangelo and Jalex Stark. Separation of finite and infinite-dimensional quantum correlations, with infinite question or answer sets. *arXiv preprint arXiv:1708.06522*, 2017.
- [DPP17] Ken Dykema, Vern I Paulsen, and Jitendra Prakash. Non-closure of the set of quantum correlations via graphs. *arXiv preprint arXiv:1709.05032*, 2017.
- [Fan73] Mark Fannes. A continuity property of the entropy density for spin lattice systems. *Communications in Mathematical Physics*, 31(4):291–294, 1973.

- [GVW⁺15] Marissa Giustina, Marijn AM Versteegh, Sören Wengerowsky, Johannes Handsteiner, Armin Hochrainer, Kevin Phelan, Fabian Steinlechner, Johannes Kofler, Jan-Åke Larsson, Carlos Abellán, et al. Significant-loophole-free test of Bell’s theorem with entangled photons. *Physical review letters*, 115(25):250401, 2015.
- [HBD⁺15] Bas Hensen, H Bernien, AE Dréau, A Reiserer, N Kalb, MS Blok, J Ruitenbergh, RFL Vermeulen, RN Schouten, C Abellán, et al. Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres. *Nature*, 526(7575):682–686, 2015.
- [Ji13] Zhengfeng Ji. Binary Constraint System Games and Locally Commutative Reductions. *arXiv:1310.3794*, 2013.
- [Ji16] Zhengfeng Ji. Classical verification of quantum proofs. In *Proceedings of the forty-eighth annual ACM symposium on Theory of Computing*, pages 885–898. ACM, 2016.
- [Ji17] Zhengfeng Ji. Compression of quantum multi-prover interactive proofs. In *Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing*, STOC 2017, pages 289–302, New York, NY, USA, 2017. ACM.
- [LTW13] Debbie Leung, Ben Toner, and John Watrous. Coherent state exchange in multi-prover quantum interactive proof systems. *Chicago Journal of Theoretical Computer Science*, 11:1–18, 2013.
- [MS12] Carl A Miller and Yaoyun Shi. Optimal robust quantum self-testing by binary nonlocal XOR games. *arXiv preprint arXiv:1207.1819*, 2012.
- [MV14] Laura Mančinska and Thomas Vidick. Unbounded entanglement can be needed to achieve the optimal success probability. In *International Colloquium on Automata, Languages, and Programming*, pages 835–846. Springer, 2014.
- [OV16] Dimiter Ostrev and Thomas Vidick. Entanglement of approximate quantum strategies in XOR games. *arXiv preprint arXiv:1609.01652*, 2016.
- [PV10] Károly F Pál and Tamás Vértesi. Maximal violation of a bipartite three-setting, two-outcome bell inequality using infinite-dimensional quantum systems. *Physical Review A*, 82(2):022116, 2010.
- [RUV13] Ben W Reichardt, Falk Unger, and Umesh Vazirani. Classical command of quantum systems. *Nature*, 496(7446):456–460, 2013.
- [RV15] Oded Regev and Thomas Vidick. Quantum XOR games. *ACM Transactions on Computation Theory (ToCT)*, 7(4):15, 2015.
- [Slo11] William Slofstra. Lower bounds on the entanglement needed to play XOR non-local games. *Journal of Mathematical Physics*, 52(10):102202, 2011.
- [Slo16] William Slofstra. Tsirelson’s problem and an embedding theorem for groups arising from non-local games. *arXiv preprint arXiv:1606.03140*, 2016.
- [Slo17] William Slofstra. The set of quantum correlations is not closed. *arXiv preprint arXiv:1703.08618*, 2017.

- [SMSC⁺15] Lynden K Shalm, Evan Meyer-Scott, Bradley G Christensen, Peter Bierhorst, Michael A Wayne, Martin J Stevens, Thomas Gerrits, Scott Glancy, Deny R Hamel, Michael S Allman, et al. Strong loophole-free test of local realism. *Physical review letters*, 115(25):250402, 2015.
- [SV17] William Slofstra and Thomas Vidick. Entanglement in non-local games and the hyperlinear profile of groups. *arXiv preprint arXiv:1711.10676*, 2017.
- [vDH03] Wim van Dam and Patrick Hayden. Universal entanglement transformations without communication. *Physical Review A*, 67(6):060302, 2003.