Quantum Information and Computation, Vol. 18, No. 7&8 (2018) 0617–0631

ENTANGLEMENT OF APPROXIMATE QUANTUM STRATEGIES IN XOR GAMES

DIMITER OSTREV[a]
Interdisciplinary Center for Security, Reliability and Trust, University of Luxembourg, 6, Avenue de la Fonte, L-4364 Esch-sur-Alzette, Luxembourg

THOMAS VIDICK[b]
Department of Computing and Mathematical Sciences, California Institute of Technology 1200 E. California Blvd., MC 305-16, Pasadena, California 91125-2100, USA

Received December 28, 2017
Revised May 23, 2018

We characterize the amount of entanglement that is sufficient to play any XOR game near-optimally. We show that for any XOR game G and $\varepsilon > 0$ there is an ε-optimal strategy for G using $\lceil \varepsilon^{-1} \rceil$ ebits of entanglement, irrespective of the number of questions in the game. By considering the family of XOR games CHSH(n) introduced by Slofstra (Jour. Math. Phys. 2011), we show that this bound is nearly tight: for any $\varepsilon > 0$ there is an $n = \Theta(\varepsilon^{-1/5})$ such that $\Omega(\varepsilon^{-1/5})$ ebits are required for any strategy achieving bias that is at least a multiplicative factor $(1 - \varepsilon)$ from optimal in CHSH(n).

Keywords: non-local XOR games, entanglement, nearly-optimal strategies
Communicated by: R Cleve & R de Wolf

1 Introduction

Perhaps the most striking demonstration of the departure of quantum systems from classical behavior is given by the Bell test. Recent experiments [1, 2, 3] establish "all-loopholes-closed" validations of the simplest such test, the CHSH inequality [4]. Although they do not reach the maximum quantum bound of $2\sqrt{2}$, the observed violation and statistical confidence are high enough to provide a solid proof of quantumness of the underlying physical system.

Research in quantum cryptography and self-testing in recent years has established that a large violation of the CHSH inequality goes much further than a generic certificate of non-classical behavior: it can serve as a guarantee that the underlying quantum system is locally isometric to one that is in a Bell pair $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. This can be interpreted as a form of "self-test" for the Bell pair, which certifies its presence solely via observable correlations.

[a]Email address: dimiter.ostrev@uni.lu
[b]Email address: vidick@cms.caltech.edu

Can more complex entangled states similarly be verified by the violation of a suitable Bell inequality? Due to its importance for experiments as well as quantum cryptography, the question has been extensively studied. The most relevant state of the art for us is the following: for any dimension d there exists a Bell inequality whose maximum violation by a quantum system can only be achieved if the system is locally isometric to a d-dimensional maximally entangled state [5]. With the exception of the results from [6] and [7] (to which we return in more detail below), however, all known self-tests for d-dimensional entangled states require either a number of inputs [8, 9, 10, 11] or outputs [5, 12] that scales at least linearly with d, i.e. the test has size exponential in the number of ebits tested.

The situation is even less satisfying as soon as one attempts to certify an even slightly noisy system, where by noisy system we mean one that will only lead to a violation that approaches the quantum optimum up to a multiplicative factor $(1-\varepsilon)$ for some $\varepsilon > 0$. The performance of known tests scales poorly with the "robustness parameter" ε, which with the recent exception of [10] is required to be inverse exponential in the number of ebits tested before any consequence can be drawn.

We study the question in the context of the simplest kind of Bell inequalities, two-party binary output correlation inequalities. These are bipartite Bell inequalities where each site can be measured using any number of two-outcome local observables, but only expectation values of the correlators of the outcomes obtained at each site are taken into account. Such inequalities can be equivalently formulated using the language of two-player XOR games, that we adopt from now on. An XOR game is a two-player one-round game G in which the players' answers are restricted to be a single bit each, and the verifier's acceptance criterion only depends on the parity of these bits. Any binary output correlation inequality can be mapped into an XOR game and vice-versa. The bias β^* of the XOR game, defined as twice the maximum deviation from 1/2 of the players' success probability, is the quantity that plays the role of the quantum bound for the Bell inequality.

Results. Our main result is that XOR games can provide very efficient tests for high-dimensional entanglement, while at the same time being noise-robust — to some extent. In the positive direction we show that for any $\varepsilon > 0$, there exists an XOR game with $\Theta(\varepsilon^{-1/5})$ inputs for Alice and $\Theta(\varepsilon^{-2/5})$ inputs for Bob such that any strategy that comes within a multiplicative $(1-\varepsilon)$ of the optimal quantum bias requires the use of a state that is close to a tensor product of $\Omega(\varepsilon^{-1/5})$ EPR pairs. Thus both the number of settings and the certified number of ebits are inverse polynomial in ε. (The number of outcomes, of course, is only two.) In the negative direction we show that, up to the exponent $-1/5$, no XOR game can lead to a better scaling: for any XOR game and any $\varepsilon > 0$ there exists a strategy coming within a multiplicative factor $(1-\varepsilon)$ of the optimal bias that uses $O(\varepsilon^{-1})$ EPR pairs (irrespective of the number of inputs in the game).

For our positive result we consider a family of XOR games introduced by Slofstra [6].

Definition 1 *For an integer $n \geq 2$, the game*[c] $\mathrm{CHSH}(n)$ *has n possible questions for Alice, indexed by integers $i \in \{1, \ldots, n\}$, and $n(n-1)$ possible questions for Bob, indexed by pairs $(i,j) \in \{1,\ldots,n\}^2$ such that $i \neq j$. The game can be described as follows: the referee selects a pair $(i,j) \in \{1,\ldots,n\}^2$ such that $i < j$ and $(x,y) \in \{0,1\}^2$ uniformly at random. If $x = 0$*

[c] This game should not be confused with the CHSH_q game introduced in [13].

the referee sends i to Alice, and if $x = 1$ the referee sends her j. If $y = 0$ the referee sends (i, j) to Bob, and if $y = 1$ the referee sends him (j, i). The players have to provide answers $a, b \in \{0, 1\}$ such that $a \oplus b = x \wedge y$.

Note that CHSH(2) is the usual CHSH game, for which the optimal bias is $\beta^*(\mathrm{CHSH}) = \sqrt{2}/2$. Slofstra showed that $\beta^*(\mathrm{CHSH}(n)) = \sqrt{2}/2$ for all $n \geq 2$, and that strategies achieving the optimum bias in CHSH(n) require a Hilbert space of dimension $2^{\lfloor n/2 \rfloor}$. Our theorem implies a smooth degradation of this bound for $\varepsilon > 0$.

Theorem 1 *Let $\varepsilon > 0$, let $n = \Theta(\varepsilon^{-1/5})$ be an integer and $(A_i, B_{ij}, |\psi\rangle)$ a strategy in* CHSH(n) *achieving bias at least $(1 - \varepsilon)\beta^*(\mathrm{CHSH}(n))$. Then $|\psi\rangle$ has entanglement entropy $\Omega(\varepsilon^{-1/5})$.*

Switching the parameters around, Theorem 1 implies in particular that for any integer $n \geq 2$ and $\varepsilon = O(n^{-5})$, any ε-optimal strategy in CHSH(n) requires entanglement of dimension $2^{\Omega(n)}$. The proof of Theorem 1 in fact yields a stronger "rigidity" result for the game CHSH(n), showing that for any strategy achieving bias at least $(1 - \varepsilon)$ times the optimum in CHSH(n) and any $r \leq \lfloor n/3 \rfloor$ there are local isometries that map the strategy to one that is within distance $O(r^{5/2}\sqrt{\varepsilon})$ of a tensor product of r ideal strategies for the game CHSH(2).

The proof of Theorem 1 is given in Section 4. The proof proceeds in two steps. First we observe that CHSH(n) contains $\binom{n}{2}$ copies of the CHSH game embedded inside it, one for each pair $\{i, j\} \subseteq \{1, \ldots, n\}$. By applying well-known rigidity results for the CHSH game we obtain approximate anti-commutation relations between each pair of Alice's observables. Second, we show that any such n pairwise approximately anti-commuting observables can be used to construct $m = \lfloor n/3 \rfloor$ pairs (X_k, Z_k) of anti-commuting observables such that any two observables belonging to distinct pairs approximately commute. Finally, in the third and last step we apply a theorem due to [14] to show that the observables constructed in the second step are (up to a local isometry) close to commuting pairs of Pauli observables. The lower bound on entanglement entropy follows from an application of strong subadditivity and Fannes' inequality.

Our negative result complements the lower bound from Theorem 1. We prove the following:

Theorem 2 *Let $\varepsilon > 0$ and let G be an XOR game. Then there exists an ε-optimal strategy for G using a maximally entangled state in $2^{\lceil \varepsilon^{-1} \rceil}$ dimensions.*

The same result, with a slightly weaker upper bound $d = 2^{O(\varepsilon^{-2})}$, is attributed to Regev in [15]. The improvement from ε^{-2} to ε^{-1} requires a slightly more careful analysis of the performance of the randomly projected vectors in the semidefinite program associated to the XOR game. Although its implication for XOR games has not previously been spelled out, the improved bound is not new, and can be obtained in a number of different ways. For instance it follows from the analysis of Krivine rounding schemes in [16, Theorem 1.1], and was also obtained using Riesz's rounding technique in [17, Theorem 4]. We provide a different analysis based on a rounding technique which was used in [18] to analyze the non-commutative Grothendieck inequality and originates in Hirschman's proof [19] of the Hadamard three-line theorem in complex analysis. Details are given in Section 3.

Applications. Our result can be interpreted as a robust, efficient self-test for the tensor product of n EPR pairs: given any integer n, setting $\varepsilon = O(n^{-5})$ any strategy in CHSH($3n$) that achieves a bias at least $(1 - \varepsilon)$ times the optimal must be using a state that is close to an

n-qubit maximally entangled state. The game CHSH($3n$) only has $O(n^2)$ inputs per player, and it thus provides a very efficient test, with the number of inputs scaling only quadratically with the number of ebits tested.

The work of Reichardt et al. [20] demonstrates that self-testing results for the tensor product of many EPR pairs can form the basis for much more complex tasks, such as the classical delegation of an arbitrary quantum circuit to two isolated provers. It would be interesting to investigate whether the analysis of the CHSH(n) game that we give here could be leveraged to improve the efficiency of their protocol. Our self-testing result gives access to n mutually anti-commuting pairs of observables on Alice's system, which can be combined to create arbitrary Pauli operators. Paulis of high weight will require taking the product of many observables, yielding a corresponding loss in error. However, one can easily imagine modifying the CHSH(n) game by introducing inputs associated with specific Pauli operators one is interested in.

In [21] the game CHSH(n) is used to test effective anti-commutators, from which a form of device-independent uncertainty relation can be derived. The stronger guarantees that come out of our analysis may have further applications to device-independent cryptography.

Related works. The study of optimal strategies in XOR games was initiated by Tsirelson, who shows [22, 23] that for any XOR game with n and m inputs per party there is an optimal strategy that uses a maximally entangled state of dimension at most $2^{\lfloor r/2 \rfloor}$, where r is the largest integer that satisfies $\binom{r+1}{2} \leq n + m - 1$ and $r \leq \min(m, n)$. Slofstra [6] gives a slight variant of the CHSH(n) game with $m = n(n-1)/2$, that requires $\lfloor (n-1)/2 \rfloor$ ebits to play optimally and thus shows that Tsirelson's bound is asymptotically tight. [24, Section 3.3] gives a family of games that exactly match Tsirelson's bound.

In terms of nearly-optimal strategies in XOR games, the best prior lower bound on the dimension of the Hilbert space scales as $1/\varepsilon$; precisely $\lceil 1/(2\varepsilon) \rceil$ [25]. In [6] a slightly weaker lower bound of $\Omega(\varepsilon^{-1/12})$ is shown based on the theory of approximate representations of C^*-algebras, for the same family of games CHSH(n) as considered here.

In [7] an analogous result to Theorem 1 is proved, except that the result applies to a game that is not an XOR game. As already mentioned, the proof of Theorem 1 relies on the main technical component of [7]. The advantage of our result is that the game is slightly simpler and, as shown by Theorem 2, is nearly-tight for XOR games.

[26] analyzes nearly-optimal strategies for the CHSH(n) game from a representation theory point of view. That paper shows that an adaptation of the group-averaging construction gives an approximately intertwining operator between the canonical optimal strategy for CHSH(n) and any given nearly-optimal strategy.

We mention in passing that there seem to be at least three different ways to formalize the intuition that nearly optimal strategies must be close to optimal ones: showing that the defining relations for a certain algebra are approximately satisfied as in [6], constructing local isometries as in [27] and as we also do here, and constructing an approximately intertwining operator as in [26]. An interesting open problem is to establish relations between these three approaches.

2 Preliminaries

2.1 Notation

For a finite set S we write $\mathrm{E}_{i\in S}$ for $|S|^{-1}\sum_{i\in S}$. All Hilbert spaces in this paper are finite-dimensional; we use a calligraphic letter such as $\mathcal{H}, \mathcal{H}_\mathsf{A}, \mathcal{H}_\mathsf{B}$ to denote a finite-dimensional Hilbert space. Given $A \in \mathrm{L}(\mathcal{H})$,[d]the absolute value $|A|$ is defined as the unique positive square root of $A^\dagger A$. For $A \in \mathrm{L}(\mathcal{H})$ we write A^{-1} or (when there is no ambiguity) $\frac{1}{A}$ for the Moore-Penrose pseudo-inverse of A.

An observable is a Hermitian operator $A \in \mathrm{L}(\mathcal{H})$ that squares to identity. We will call an observable balanced if its 1-eigenspace and its (-1)-eigenspace have the same dimension. Note that the statement "A is a balanced observable" is equivalent to the statement "there exists an observable B that anti-commutes with A".

For two vectors $|\varphi\rangle, |\psi\rangle \in \mathcal{H}$ and $\delta > 0$, we write $|\varphi\rangle \approx_\delta |\psi\rangle$ to mean $\||\varphi\rangle - |\psi\rangle\| = O(\delta)$, where the implicit constant is universal.

We use $\{A, B\} = AB + BA$ and $[A, B] = AB - BA$ to denote the anti-commutator and commutator. We will often consider all four commutators between two pairs X, Z and X', Z' of anti-commuting observables. In order to avoid having to write $[X, X'], [X, Z'], [Z, X'], [Z, Z']$ all the time, we adopt the following notational convention: we write "$[P, Q']$, where each of P, Q stands for either X or Z". Thus, for example, "$\|[P, Q']|\psi\rangle\| < \varepsilon$, where each of P, Q stands for either X or Z", means

$$\|[X, X']|\psi\rangle\| < \varepsilon\ ,\ \text{ and }\ \|[X, Z']|\psi\rangle\| < \varepsilon\ ,\ \text{ and }\ \|[Z, X']|\psi\rangle\| < \varepsilon\ ,\ \text{ and }\ \|[Z, Z']|\psi\rangle\| < \varepsilon\ .$$

2.2 XOR games

For integers n and m, an $n \times m$ XOR game G is specified by a real $n \times m$ matrix, that we often also call G, such that $\sum_{i,j} |G_{i,j}| = 1$. A strategy for the players in G is given by finite-dimensional Hilbert spaces $\mathcal{H}_\mathsf{A}$ and $\mathcal{H}_\mathsf{B}$, a collection of n observables $A_i \in \mathrm{L}(\mathcal{H}_\mathsf{A})$ for the first player, m observables $B_j \in \mathrm{L}(\mathcal{H}_\mathsf{B})$ for the second player, and a state $|\psi\rangle \in \mathcal{H}_\mathsf{A} \otimes \mathcal{H}_\mathsf{B}$ (in any finite dimension). The bias of the strategy is defined as

$$\beta^*(G; A_i, B_j, |\psi\rangle) := \sum_{i,j} G_{i,j} \langle\psi|A_i \otimes B_j|\psi\rangle.$$

The bias of a game is the maximum bias achievable over any finite-dimensional strategy:

$$\beta^*(G) := \sup_{d, A_i, B_j, |\psi\rangle} \Big|\sum_{i,j} G_{i,j} \langle\psi|A_i \otimes B_j|\psi\rangle\Big|,$$

where the supremum is taken over all integers d, observables A_i, B_j in $\mathbb{C}^d$ and states $|\psi\rangle \in \mathbb{C}^d \otimes \mathbb{C}^d$. Given $\varepsilon > 0$ we say that a strategy $(A_i, B_j, |\psi\rangle)$ in G is ε-optimal if $\beta^*(G; A_i, B_j, |\psi\rangle) \geq (1 - \varepsilon)\beta^*(G)$.

Tsirelson [22] proved the following fact that will be relevant for our analysis: for any collection $x_i, y_j \in \mathbb{R}^d$ of real unit vectors there exists observables $A_i, B_j \in \mathrm{L}(\mathbb{C}^D)$ for $D \leq 2^{\lfloor d/2 \rfloor}$ and $|\psi\rangle = D^{-1/2} \sum_{i=1}^D |i\rangle|i\rangle$ such that $\langle\psi|A_i \otimes B_j|\psi\rangle = x_i \cdot y_j$ for every i, j. (Tsirelson's

[d] $\mathrm{L}(\mathcal{H})$ is the space of bounded linear operators on $\mathcal{H}$

construction is based on the use of a representation of the Clifford algebra.) This observation allows to prove that the following semidefinite relaxation of the bias is tight:

$$\begin{aligned} \beta^*(G) = \mathrm{SDP}(G) = \quad & \sup \sum_{i,j} G_{i,j}\, x_i \cdot y_j \\ & x_i, y_j \in \mathbb{R}^{m+n} \\ & \|x_i\| = \|y_j\| = 1. \end{aligned} \tag{1}$$

We refer to [15] for a proof of this fact.

For the game CHSH = CHSH(2) very good results are known characterizing the structure of ε-optimal strategies. We use the following lemma from [27] (see also [28, Lemma 4.2]).

Lemma 1 (CHSH rigidity) *Let $\delta > 0$ and $(\{A_0, A_1\}, \{B_0, B_1\}, |\psi\rangle)$ a δ-optimal strategy in* CHSH. *Then there exists local isometries U, V and a state $|\psi'\rangle$ such that, letting $|\phi^+\rangle = (1/\sqrt{2})(|00\rangle + |11\rangle)$ and X, Z the single-qubit Pauli operators,*

$$\|U \otimes V|\psi\rangle - |\phi^+\rangle|\psi'\rangle\| = O(\sqrt{\delta}), \tag{2}$$

$$\max\Big\{\|\big(A_0 - U^\dagger(X \otimes \mathrm{Id})U\big) \otimes \mathrm{Id}\,|\psi\rangle\|,\ \|\big(A_1 - U^\dagger(Z \otimes \mathrm{Id})U\big) \otimes \mathrm{Id}\,|\psi\rangle\|\Big\} = O(\sqrt{\delta}), \tag{3}$$

and letting $\tilde{A}_0 := \frac{B_0+B_1}{|B_0+B_1|}$ and $\tilde{A}_1 := \frac{B_0-B_1}{|B_0-B_1|}$,

$$\max\Big\{\big\|\big(A_0 \otimes \mathrm{Id} - \mathrm{Id} \otimes \tilde{A}_0\big)|\psi\rangle\big\|,\ \big\|\big(A_1 \otimes \mathrm{Id} - \mathrm{Id} \otimes \tilde{A}_1\big)|\psi\rangle\big\|\Big\} = O(\sqrt{\delta}), \tag{4}$$

$$\max\Big\{\big\|\,\mathrm{Id} \otimes \big(\tilde{A}_0 - V^\dagger(X \otimes \mathrm{Id})V\big)|\psi\rangle\big\|,\ \big\|\,\mathrm{Id} \otimes \big(\tilde{A}_1 - V^\dagger(Z \otimes \mathrm{Id})V\big)|\psi\rangle\big\|\Big\} = O(\sqrt{\delta}). \tag{5}$$

2.3 Overlapping qubits

The notion of "overlapping qubits" is introduced in [29]. Intuitively, a pair of overlapping qubits i and j is specified by two pairs of anti-commuting observables $\{X_i, Z_i\}$ and $\{X_j, Z_j\}$ such that $[P_i, Q_j] \approx 0$ where each of P, Q stands for either X or Z. The following theorem from [14] bounds the distance of partially overlapping qubits from exact qubits.

Theorem 3 (Theorem 2.1 in [14]) *Let $|\psi\rangle$ be a state in $\mathcal{H}_A \otimes \mathcal{H}_B$. Assume that for each $j \in \{1, \ldots, n\}$ there are observables $X_j, Z_j \in \mathrm{L}(\mathcal{H}_A)$ and $X'_j, Z'_j \in \mathrm{L}(\mathcal{H}_B)$ such that*

$$\begin{aligned} \forall j, \{X_j, Z_j\} = \{X'_j, Z'_j\} &= 0 \\ \forall i \neq j, \max\big\{\big\|[P_i, Q_j] \otimes \mathrm{Id}\,|\psi\rangle\big\|,\ \big\|\,\mathrm{Id} \otimes [P'_i, Q'_j]|\psi\rangle\big\|\big\} &\leq \eta \\ \forall j, \big\|P_j \otimes P'_j|\psi\rangle - |\psi\rangle\big\| &\leq \eta \end{aligned}$$

where each of P, Q stands for either X or Z.

Let

$$|\psi'\rangle = |\psi\rangle_{AB} \otimes |\phi^+\rangle^{\otimes n}_{A'A''} \otimes |\phi^+\rangle^{\otimes n}_{B'B''} \in \mathcal{H}_A \otimes (\mathbb{C}^2)^{\otimes n}_{A'} \otimes (\mathbb{C}^2)^{\otimes n}_{A''} \otimes \mathcal{H}_B \otimes (\mathbb{C}^2)^{\otimes n}_{B'} \otimes (\mathbb{C}^2)^{\otimes n}_{B''}\ ,$$

where $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Then there exist observables $\hat{X}_i, \hat{Z}_i \in \mathrm{L}(\mathcal{H}_A \otimes (\mathbb{C}^2)^{\otimes n}_{A'} \otimes (\mathbb{C}^2)^{\otimes n}_{A''})$

and $\hat{X}'_i, \hat{Z}'_i \in \mathrm{L}(\mathcal{H}_B \otimes (\mathbb{C}^2)^{\otimes n}_{B'} \otimes (\mathbb{C}^2)^{\otimes n}_{B''})$ *such that*

$$\begin{aligned}
\forall j, \{\hat{X}_j, \hat{Z}_j\} = \{\hat{X}'_j, \hat{Z}'_j\} &= 0 \\
\forall i \neq j, [\hat{P}_i, \hat{Q}_j] = [\hat{P}'_i, \hat{Q}'_j] &= 0 \\
\forall j, \max\left\{\|\left(\hat{P}_j - P_j \otimes \mathrm{Id}_{AA'A''}\right) \otimes \mathrm{Id}_{BB'B''} |\psi'\rangle\|, \|\mathrm{Id}_{AA'A''} \otimes \left(\hat{P}'_j - P'_j \otimes \mathrm{Id}_{B'B''}\right)|\psi'\rangle\|\right\} &= O(n\eta) \\
\forall j, \left\|\hat{P}_j \otimes \hat{P}'_j |\psi'\rangle - |\psi'\rangle\right\| &= O(n\eta)
\end{aligned}$$

where each of P, Q *stands for either* X *or* Z*.*

Using that the (anti-)commutation relations between observables $\{\hat{X}_i, \hat{Z}_i\}$ stated in the theorem suffice to characterize these operators, up to conjugation, as the Pauli $\{\sigma^x_i, \sigma^z_i\}$ observables, the theorem has the following immediate corollary.

Corollary 1 (Corollary 2.2 in [14]) *Under the assumptions of Theorem 3, there are unitaries* $U_{DD'D''} : \mathcal{H}_D \otimes (\mathbb{C}^2)^{\otimes n}_{D'} \otimes (\mathbb{C}^2)^{\otimes n}_{D''} \to \mathcal{H}_D \otimes (\mathbb{C}^2)^{\otimes n}_{D'} \otimes (\mathbb{C}^2)^{\otimes n}_{D''}$ *(where* D *stands for either* A *or* B*) and a state* $|\mathrm{extra}\rangle \in \mathcal{H}_A \otimes (\mathbb{C}^2)^{\otimes n}_{A''} \otimes \mathcal{H}_B \otimes (\mathbb{C}^2)^{\otimes n}_{B''}$ *such that*

$$\begin{aligned}
\left\|U_{AA'A''} \otimes U_{BB'B''} |\psi'\rangle - |\phi^+\rangle^{\otimes n}_{A'B'} \otimes |\mathrm{extra}\rangle_{AA''BB''}\right\| &= O(n^{3/2}\eta)\,, \\
\left\|(U_{DD'D''}((X_j)_D \otimes \mathrm{Id}_{D'D''})U^\dagger_{DD'D''} - (\sigma^x_j)_{D'} \otimes \mathrm{Id}_{DD''}) \otimes \mathrm{Id}_{otherside} |\phi^+\rangle^{\otimes n}_{A'B'} \otimes |\mathrm{extra}\rangle_{AA''BB''}\right\| &= O(n^{3/2}\eta)\,, \\
\left\|(U_{DD'D''}((Z_j)_D \otimes \mathrm{Id}_{D'D''})U^\dagger_{DD'D''} - (\sigma^z_j)_{D'} \otimes \mathrm{Id}_{DD''}) \otimes \mathrm{Id}_{otherside} |\phi^+\rangle^{\otimes n}_{A'B'} \otimes |\mathrm{extra}\rangle_{AA''BB''}\right\| &= O(n^{3/2}\eta)\ .
\end{aligned}$$

Theorem 3 requires observables that exactly anti-commute. The following lemma shows that approximately anti-commuting observables are never far from exactly anti-commuting ones.

Lemma 2 *Let* X, Z *be balanced obervables on a space* $\mathcal{H}_A$ *of even dimension and let* $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ *be such that* $\|\{X, Z\} \otimes \mathrm{Id}\,|\psi\rangle\| \leq \varepsilon$*. Then there exists a balanced observable* $\tilde{Z}$ *on* $\mathcal{H}_A$ *such that*

$$\|(Z - \tilde{Z}) \otimes \mathrm{Id}\,|\psi\rangle\| \leq \sqrt{3/2}\,\varepsilon,$$

and

$$\{X, \tilde{Z}\} = 0.$$

Proof. Let R, S be the projections on the 1 and -1 eigenspace of X. Consider RZS; from the singular value decomposition [30, Corollary 2.4], there exist an orthonormal basis $|u_1\rangle \ldots |u_n\rangle$ of $Im(R)$, an orthonormal basis $|v_1\rangle, \ldots |v_n\rangle$ of $Im(S)$, and non-negative real numbers $c_1, \ldots c_n$ such that

$$RZS = \sum_i c_i |u_i\rangle\langle v_i| \quad \text{and} \quad SZR = (RZS)^\dagger = \sum_i c_i |v_i\rangle\langle u_i|$$

We write the matrices for X and Z with respect to the basis $|u_1\rangle \ldots |u_n\rangle, |v_1\rangle, \ldots |v_n\rangle$ of $\mathcal{H}_A$; they are

$$X = \begin{pmatrix} \mathrm{Id} & 0 \\ 0 & -\mathrm{Id} \end{pmatrix} \qquad \text{and} \qquad Z = \begin{pmatrix} A & C \\ C & B \end{pmatrix},$$

where the size of the blocks is $n = dim(\mathcal{H}_\mathsf{A})/2$, and where $C = diag(c_1, \ldots, c_n)$. With this notation, we get

$$\{X, Z\}^2 = \begin{pmatrix} 4A^2 & 0 \\ 0 & 4B^2 \end{pmatrix}. \tag{6}$$

Let

$$\tilde{Z} = \begin{pmatrix} 0 & \mathrm{Id} \\ \mathrm{Id} & 0 \end{pmatrix}.$$

Then $\{X, \tilde{Z}\} = 0$, and it remains to show that $\|(Z - \tilde{Z}) \otimes \mathrm{Id}\,|\psi\rangle\| \leq \sqrt{3/2}\,\varepsilon$.

Using $Z^2 = \mathrm{Id}$, we get $C^2 = \mathrm{Id} - A^2$ and $C^2 = \mathrm{Id} - B^2$. Using $C^2 \leq \mathrm{Id}$ and the fact that C is diagonal with non-negative real entries, we get

$$(\mathrm{Id} - C)^2 \leq 2(\mathrm{Id} - C^2) \tag{7}$$

and from here we get

$$(\mathrm{Id} - C)^2 \leq 2A^2, \qquad (\mathrm{Id} - C)^2 \leq 2B^2. \tag{8}$$

We can then bound

$$\begin{aligned}(Z - \tilde{Z})^2 &\leq 2\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}^2 + 2\begin{pmatrix} 0 & C - \mathrm{Id} \\ C - \mathrm{Id} & 0 \end{pmatrix}^2 \\ &\leq \frac{1}{2}\{X, Z\}^2 + \{X, Z\}^2,\end{aligned}$$

where to bound the first term we used (6), and to bound the second we used (8) and (6). The lemma follows by evaluating both sides of the operator inequality on $\rho_\mathsf{A} = \mathrm{Tr}_\mathsf{B}|\psi\rangle\langle\psi|$. $\square$.

3 Upper bound: playing XOR games with low entanglement

We prove Theorem 2. Let G be an XOR game and $(A_s, B_t, |\psi\rangle)$ an optimal strategy for the players in G, where $|\psi\rangle \in \mathbb{C}^D \otimes \mathbb{C}^D$. Let

$$x_s = \langle\psi|A_s \otimes \mathrm{Id}, \qquad y_t = \langle\psi|\,\mathrm{Id} \otimes B_t,$$

and observe that x_s, y_t are complex D^2-dimensional unit vectors such that $\sum_{s,t} G_{s,t} x_s \cdot \overline{y_t} = \beta^*(G)$ (where for complex row vectors $x = (x_1, \ldots, x_l)$ and $y = (y_1, \ldots, y_l)$ we denote $x \cdot y = \sum_i x_i y_i$). Let d be an integer and $\{g_{kp}\}$, for $k \in \{1, \ldots, d\}$ and $p \in \{1, \ldots, D^2\}$, be independent and uniformly distributed in $\{1, -1, i, -i\}$. Define $x'_s, y'_t \in \mathbb{C}^d$ by

$$(x'_s)_k = \frac{1}{\sqrt{d}} \sum_p g_{kp}(x_s)_p, \qquad (y'_t)_k = \frac{1}{\sqrt{d}} \sum_p g_{kp}(y_t)_p,$$

for $k = 1, \ldots, d$. The vectors x'_s (resp. y'_t) can be thought of as being obtained from the x_s (resp. y_t) by "random projection", with $V = (g_{kp})_{1 \leq k \leq d, 1 \leq p \leq D^2}$ the "random projection matrix" (up to scaling and on expectation, $VV^\dagger \propto \mathrm{Id}$), that places the vectors in a favorable position for the analysis.

The goal of the analysis is to demonstrate that there exists a choice of coefficients that yields a large objective value, in spite of the vectors being of possibly much lower dimension than the initial set of vectors, coming from the quantum strategy. The main difficulty is

in dealing with the normalization of the x'_s and y'_t. For this we again apply a randomized rounding procedure, following a trick previously used in e.g. [18]. Let α be a real parameter distributed according to the hyperbolic secant distribution, with pdf $f(z) = \frac{1}{2}\mathrm{sech}(\frac{\pi}{2}z)$, where $\mathrm{sech}(z) = \frac{2}{e^z+e^{-z}}$ is the hyperbolic secant function. The only property of this distribution relevant for the analysis is that it satisfies that for any $a > 0$, $\mathrm{E}_\alpha[a^{i\alpha}] = 2a - \mathrm{E}_\alpha[a^{2+i\alpha}]$ (see e.g. [31, Sec. 23.11]. Using this relation we obtain

$$\mathrm{E}\Big[\sum_{s,t} G_{s,t}\frac{x'_s}{\|x'_s\|}\|x'_s\|^{i\alpha}\cdot\frac{\overline{y'_t}}{\|y'_t\|}\|y'_t\|^{i\alpha}\Big] = 2\sum_{s,t} G_{s,t}x_s\cdot\overline{y_t} - \mathrm{E}\Big[\sum_{s,t} G_{s,t}x'_s\|x'_t\|^{1+i\alpha}\cdot\overline{y'_t}\|y'_t\|^{1+i\alpha}\Big]. \tag{9}$$

We bound the second term on the right-hand side. For this we interpret $x'_s\|x'_s\|^{1+i\alpha}$ and $y'_t\|y'_t\|^{1-i\alpha}$ as a vector solution to the semidefinite program (1) associated to the XOR game G, where the vectors live in the infinite-dimensional space of random d-dimensional vectors over $\mathbb{C}$ with inner product $\langle X, Y\rangle = E(X\cdot\overline{Y})$.[e] Let $z \in \mathbb{C}^{D^2}$ be any vector among the x_s, y_t, and let z' be the associated random vector, $x'_s\|x'_s\|^{1+i\alpha}$ or $y'_t\|y'_t\|^{1-i\alpha}$. We compute

$$\begin{aligned}
\|z'\|^2 &= \frac{1}{d^2}\mathrm{E}\Big(\sum_{k=1}^{d}\Big|\sum_p g_{kp}z_p\Big|^2\Big)^2 \\
&= \frac{1}{d^2}\mathrm{E}\Big[\sum_{k,k'=1}^{d}\sum_{p,q,r,s=1}^{D^2} g_{kp}\overline{g_{kq}}g_{k'r}\overline{g_{k's}}\,z_p\overline{z_q}z_r\overline{z_s}\Big] \\
&= \frac{1}{d^2}\Big(d\sum_{p\neq q}|z_p|^2|z_q|^2 + d^2\sum_{p,q}|z_p|^2|z_q|^2\Big) \\
&\leq \frac{d^2+d}{d^2}\|z\|^4 = 1+\frac{1}{d}.
\end{aligned}$$

Using that the objective value of (1) scales linearly with the norm of the vectors, this bound lets us upper bound the modulus of the second term on the right-hand side in (9) by $(1 + 1/d)\beta^*(G)$, so that

$$\mathrm{E}\Big[\sum_{s,t} G_{s,t}\frac{x'_s}{\|x'_s\|}\|x'_s\|^{i\alpha}\cdot\frac{\overline{y'_t}}{\|y'_t\|}\|y'_t\|^{i\alpha}\Big] \geq \Big(1-\frac{1}{d}\Big)\beta^*(G).$$

In particular there must exist a choice of coefficients g_{kp} and real parameter α such that the complex d-dimensional unit vectors $\frac{x'_s}{\|x'_s\|}\|x'_s\|^{i\alpha}$ and $\frac{y'_t}{\|y'_t\|}\|y'_t\|^{-i\alpha}$ yield a value for the left-hand side of (9) that is at least $(1 - 1/d)\beta^*(G)$. Decomposing these vectors into real and imaginary parts as described earlier in footnote e we obtain a real vector solution of dimension $2d$ achieving bias $(1 - 1/d)\beta^*(G)$ in (1). Applying Tsirelson's construction (as described in Section 2.2) yields observables in dimension 2^d achieving the same value in G, proving Theorem 2.

[e] Although a priori SDP(G) considers a supremum over real finite-dimensional vectors, the extension to infinite-dimensional complex vectors does not allow for a larger value, as the vectors can always be projected down to their finite-dimensional span, and made real by considering $x \mapsto \Re(X) \oplus \Im(x)$ and $y \mapsto \Re(y) \oplus (-\Im(y))$.

4 Lower bound: rigidity for the CHSH(n) games

The goal of this section is to prove Theorem 1. We start by assuming without loss of generality that $\mathcal{H}_\mathsf{A}$, $\mathcal{H}_\mathsf{B}$ are finite dimensional Hilbert spaces of even dimension d each, and that Alice's observables are balanced; this assumption is technically required in the proof, and can always be satisfied by taking the direct sum with a space of appropriate dimension on which the state $|\psi\rangle$ has no support, and on which all operators are extended by taking the direct sum with an appropriate observable.

The proof of Theorem 1 has several steps, which we give in the following lemmas. Our first lemma shows that in any good strategy for the CHSH(n) game, Alice's observables must approximately pairwise anti-commute.

Lemma 3 *Take $n \geq 2$, $\varepsilon > 0$. Let $(A_i, B_{ij}, |\psi\rangle)$ be an ε-optimal strategy in* CHSH(n)*. For all $i < j$ let*

$$\tilde{A}_{ij} := \frac{B_{ij} + B_{ji}}{|B_{ij} + B_{ji}|}, \qquad \tilde{A}_{ji} := \frac{B_{ij} - B_{ji}}{|B_{ij} - B_{ji}|}.$$

Then the following hold:

$$\mathrm{E}_{i<j} \|\{A_i, A_j\} \otimes \mathrm{Id}\, |\psi\rangle\| = O(\sqrt{\varepsilon}), \qquad \mathrm{E}_{i<j} \|\, \mathrm{Id} \otimes \{\tilde{A}_{ij}, \tilde{A}_{ji}\} |\psi\rangle\| = O(\sqrt{\varepsilon}), \tag{10}$$

$$\max\Big\{ \mathrm{E}_{i<j} \big\| \big(A_i \otimes \mathrm{Id} - \mathrm{Id} \otimes \tilde{A}_{ij}\big) |\psi\rangle \big\|,\ \mathrm{E}_{i<j} \big\| \big(A_j \otimes \mathrm{Id} - \mathrm{Id} \otimes \tilde{A}_{ji}\big) |\psi\rangle \big\| \Big\} = O(\sqrt{\varepsilon}). \tag{11}$$

Proof. For any $(i, j) \in \{1, \ldots, n\}^2$ such that $i < j$ let ε_{ij} be such that the players' strategy achieves a bias $(1 - \varepsilon_{ij})\beta^*(\mathrm{CHSH})$ in the game, conditioned on the referee having selected the pair (i, j) in the first step of the game as described in Definition 1. Then $\mathrm{E}_{i<j}[\varepsilon_{ij}] = \varepsilon$, and for any $i < j$ the strategy $(A_i, A_j, B_{ij}, B_{ji}, |\psi\rangle)$ is an ε_{ij}-optimal strategy in the CHSH game.

The relation (11) then follows directly from (4) from the CHSH rigidity lemma (Lemma 1) and concavity of the square root function. To prove (10), write

$$\begin{aligned}
\{A_i, A_j\} \otimes \mathrm{Id}\, |\psi\rangle &\approx_{\sqrt{\varepsilon_{ij}}} (A_i \otimes \tilde{A}_{ji} + A_j \otimes \tilde{A}_{ij}) |\psi\rangle \\
&\approx_{\sqrt{\varepsilon_{ij}}} (U \otimes V)^\dagger \big((X \otimes Z + Z \otimes X) \otimes \mathrm{Id} \big) (U \otimes V) |\psi\rangle \\
&\approx_{\sqrt{\varepsilon_{ij}}} (U \otimes V)^\dagger \big((X \otimes Z + Z \otimes X) |\phi^+\rangle \big) \otimes |\psi'\rangle \\
&= 0,
\end{aligned}$$

where the first line uses (4), the second (3) and (5) (here the isometries U and V are allowed to depend on the pair (i, j)), the third (2) and the fourth is by definition of $|\phi^+\rangle$. Averaging over $i < j$ and using concavity of the square root function proves the first part of (10). The second part follows similarly (alternatively, from the first part using (11)). $\square$.

Given n pairwise perfectly anticommuting observables $A_1, \ldots, A_n$, we can define $m = \lfloor n/3 \rfloor$ pairs of observables

$$X_k = i A_{3k-2} A_{3k-1} \qquad \text{and} \qquad Z_k = i A_{3k-1} A_{3k},$$

for $k = 1, \ldots, \lfloor n/3 \rfloor$, such that $\{X_k, Z_k\} = 0$ and $[P_k, Q_\ell] = 0$ for $k \neq \ell$ and where each of P, Q stands for either X or Z. The following lemma shows that essentially the same construction also works in the approximate case.

Lemma 4 *Let $\delta > 0$ and $A_1, \ldots, A_n$ and $A'_1, \ldots, A'_n$ be observables such that*

$$\mathrm{E}_i \|(A_i \otimes \mathrm{Id} - \mathrm{Id} \otimes A'_i)|\psi\rangle\| \leq \delta \qquad \text{and} \qquad \mathrm{E}_{i \neq j} \|\{A_i, A_j\} \otimes \mathrm{Id}\,|\psi\rangle\| \leq \delta. \tag{12}$$

Then there exists $m = \lfloor n/3 \rfloor$ pairs of observables X_k, Z_k and X'_k, Z'_k such that for all k, $\{X_k, Z_k\} = \{X'_k, Z'_k\} = 0$ and

$$\mathrm{E}_{k \neq \ell} \|[P_k, Q_\ell] \otimes \mathrm{Id}\,|\psi\rangle\| = O(\delta), \qquad \mathrm{E}_{k \neq \ell} \|\mathrm{Id} \otimes [P'_k, Q'_\ell]|\psi\rangle\| = O(\delta), \tag{13}$$

and

$$\mathrm{E}_k \|(P_k \otimes \mathrm{Id} - \mathrm{Id} \otimes P'_k)|\psi\rangle\| = O(\delta) \tag{14}$$

where each of P, Q stands for either X or Z.

Proof. For $k \in \{1, \ldots, m\}$ we construct X_k, Z_k, X'_k, Z'_k in two stages. First, apply Lemma 2 independently to (A_{3k-1}, A_{3k-2}) and to (A_{3k-1}, A_{3k}) to obtain $\tilde{A}_{3k-2}$ and $\tilde{A}_{3k}$ that exactly anti-commute with A_{3k-1}. Next, let $X_k = i\tilde{A}_{3k-2}A_{3k-1}$ and $\tilde{Z}_k = iA_{3k-1}\tilde{A}_{3k}$. Then X_k, $\tilde{Z}_k$ are balanced observables and they satisfy

$$\begin{aligned}
\{X_k, \tilde{Z}_k\} \otimes \mathrm{Id}\,|\psi\rangle &= -\{\tilde{A}_{3k-2}, \tilde{A}_{3k}\} \otimes \mathrm{Id}\,|\psi\rangle \\
&\approx -(\tilde{A}_{3k-2}A_{3k} + \tilde{A}_{3k}A_{3k-2}) \otimes \mathrm{Id}\,|\psi\rangle \\
&\approx -\tilde{A}_{3k-2} \otimes A'_{3k}|\psi\rangle - \tilde{A}_{3k} \otimes A'_{3k-2}|\psi\rangle \\
&\approx -A_{3k-2} \otimes A'_{3k}|\psi\rangle - A_{3k} \otimes A'_{3k-2}|\psi\rangle \\
&\approx -\{A_{3k-2}, A_{3k}\} \otimes \mathrm{Id}\,|\psi\rangle \approx 0,
\end{aligned}$$

where the total error in the chain of approximations is at most

$$\begin{aligned}
&2\sqrt{3/2}\|\{A_{3k-2}, A_{3k-1}\} \otimes \mathrm{Id}\,|\psi\rangle\| + 2\sqrt{3/2}\|\{A_{3k-1}, A_{3k}\} \otimes \mathrm{Id}\,|\psi\rangle\| \\
&+ 2\|(A_{3k-2} \otimes \mathrm{Id} - \mathrm{Id} \otimes A'_{3k-2})|\psi\rangle\| + 2\|(A_{3k} \otimes \mathrm{Id} - \mathrm{Id} \otimes A'_{3k})|\psi\rangle\| + \|\{A_{3k-2}, A_{3k}\} \otimes \mathrm{Id}\,|\psi\rangle\|.
\end{aligned}$$

In a similar manner we can define $X'_k = i\tilde{A}'_{3k-2}A'_{3k-1}$ and $\tilde{Z}'_k = iA'_{3k-1}\tilde{A}'_{3k}$. Then X'_k, $\tilde{Z}'_k$ are balanced observables and we can obtain a similar bound on $\|\mathrm{Id} \otimes \{X'_k, \tilde{Z}'_k\}|\psi\rangle\|$.

In the second stage, we apply Lemma 2 to $X_k, \tilde{Z}_k$ to obtain exactly anti-commuting X_k, Z_k such that $\|(Z_k - \tilde{Z}_k) \otimes \mathrm{Id}\,|\psi\rangle\| \leq \|\{X_k, \tilde{Z}_k\} \otimes \mathrm{Id}\,|\psi\rangle\|$. Similarly, we apply Lemma 2 to $X'_k, \tilde{Z}'_k$ and obtain exactly anti-commuting X'_k, Z'_k such that $\|(Z'_k - \tilde{Z}'_k) \otimes \mathrm{Id}\,|\psi\rangle\| \leq \|\{X'_k, \tilde{Z}'_k\} \otimes \mathrm{Id}\,|\psi\rangle\|$. It remains to show that $X_k, Z_k, X'_k Z'_k$ satisfy the conclusions of Lemma 4.

For each $k \neq l$, we can bound $\|(P_k \otimes \mathrm{Id} - \mathrm{Id} \otimes P'_k)|\psi\rangle\|$, $\|\mathrm{Id} \otimes [P'_k, Q'_\ell]|\psi\rangle\|$, and $\|[P_k, Q_\ell] \otimes \mathrm{Id}\,|\psi\rangle\|$ (again, each of P, Q stands for either X or Z) using a similar chain of approximations to the one above. What is important here is that there is a small constant c such that for all $i \neq j$, the terms $\|(A_i \otimes \mathrm{Id} - \mathrm{Id} \otimes A'_i)|\psi\rangle\|$ and $\|\{A_i, A_j\} \otimes \mathrm{Id}\,|\psi\rangle\|$ appear at most c times in the different error bounds that we obtain from the chains of approximation. Therefore, we can average over $k \neq l$ and use the assumptions (12) to obtain the conclusions of Lemma 4. □.

Lemma 4 gives us qubits that approximately commute on average. On the other hand, we would like to apply Theorem 3, which requires there to be an absolute upper bound that holds for all commutators. In order to switch from the conclusions of Lemma 4 to the assumptions of Theorem 3, we prove the following combinatorial lemma:

Lemma 5 *Let K_n be the complete graph on n vertices. Suppose that to each vertex v, there are associated two non-negative weights, $w_1(v), w_2(v)$, such that $\mathrm{E}_v w_i(v) \leq \delta$ for $i = 1, 2$. Suppose further that to each edge e, there are associated eight non-negative weights $w_1(e), \ldots, w_8(e)$ such that $\mathrm{E}_e w_i(e) \leq \delta$ for $i = 1, \ldots 8$. Then, for each $a > 0$, there exists a subset S of the vertices of size at least*

$$\frac{(a-2)^2 n}{8a(n-1) + a(a-2)}$$

such that

$$\forall v \in S, \forall i = 1, 2, \;\; w_i(v) \leq a\delta \; ,$$
$$\forall e \in S \times S, \forall i = 1, \ldots 8, \;\; w_i(e) \leq a\delta \; .$$

Proof. First, delete any vertex v for which $w_1(v) > a\delta$ or $w_2(v) > a\delta$. Let n' be the number of remaining vertices. Then

$$(n - n')a\delta < \sum_v (w_1(v) + w_2(v)) \leq 2n\delta$$

so

$$n' > \frac{a-2}{a} n \; .$$

Next, delete any edge e for which $\forall i, w_i(e) \leq a\delta$. Let m' be the number of remaining edges. Then,

$$m' a\delta < \sum_e \sum_{i=1}^{8} w_i(e) \leq 8 \binom{n}{2} \delta \; ,$$

so

$$m' < \frac{8}{a} \binom{n}{2} \; .$$

Note that we have kept acceptable vertices and have deleted acceptable edges. Thus, we are interested in finding a large independent set among the remaining vertices. Recall the Theorem of Turan: if a graph $G = (V, E)$ has average degree $2|E|/|V|$ that is at most d, then G contains an independent set of size at least $|V|/(d+1)$.[f] Applying this theorem to our case gives an independent set of size at least

$$\frac{n'}{\frac{2m'}{n'} + 1} > \frac{\frac{a-2}{a} n}{\frac{8}{a-2}(n-1) + 1} = \frac{(a-2)^2 n}{8a(n-1) + a(a-2)}$$

as needed. □.

We will also need a lemma that demonstrates that if a state is close to a tensor product of a number of EPR pairs and an ancilla, then the state has high entanglement entropy.

Lemma 6 *Let $|\psi\rangle_{AA'BB'}$ be a state in $(\mathbb{C}^2 \otimes \mathbb{C}^2)_{AB}^{\otimes r} \otimes (\mathcal{H}_{A'} \otimes \mathcal{H}_{B'})$ such that*

$$\| |\psi\rangle_{AA'BB'} - |\phi^+\rangle_{AB}^{\otimes r} \otimes |\mathrm{extra}\rangle_{A'B'} \| \leq \delta/2 \tag{15}$$

Then, $|\psi\rangle_{AA'BB'}$ has entanglement entropy at least

$$r - 3\delta r + 2\delta \log(\delta)$$

[f] Proof: Go through the vertices in a random order. Add each vertex to the set if none of its neighbors are already in. The expected size of the independent set produced is $\sum_v 1/(d(v)+1) \geq |V|/(d+1)$.

Proof. We will use ρ with appropriate subscripts to denote reduced density matrices of $|\psi\rangle_{\mathsf{AA'BB'}}$ and σ with appropriate subscripts to denote reduced density matrices of $|\phi^+\rangle_{\mathsf{AB}}^{\otimes r} \otimes |\text{extra}\rangle_{\mathsf{A'B'}}$.

We will show that

$$S(\rho_{\mathsf{A}}) \geq r - \delta r + \delta \log(\delta) \tag{16}$$

and

$$S(\rho_{\mathsf{AB}}) \leq 2\delta r - \delta \log(\delta), \tag{17}$$

which using strong subadditivity as

$$S(\rho_{\mathsf{AA'}}) \geq S(\rho_{\mathsf{AA'B}}) + S(\rho_{\mathsf{A}}) - S(\rho_{\mathsf{AB}}) \geq S(\rho_{\mathsf{A}}) - S(\rho_{\mathsf{AB}})$$

will prove the result.

The trace distance between $|\psi\rangle\langle\psi|$ and $|\phi^+\rangle_{\mathsf{AB}}^{\otimes r} \otimes |\text{extra}\rangle_{\mathsf{A'B'}}\langle\phi^+|_{\mathsf{AB}}^{\otimes r} \otimes \langle\text{extra}|_{\mathsf{A'B'}}$ is at most δ. Take partial trace and get that the trace distance between ρ_{A} and σ_{A} is at most δ. Apply Fannes' inequality [30, Box 11.2]:

$$|S(\rho_A) - S(\sigma_A)| \leq Tr|\rho_A - \sigma_A| \log(dim(\mathcal{H}_A)) - Tr|\rho_A - \sigma_A| \log(Tr|\rho_A - \sigma_A|)$$

to get the bound (16). Similarly, the trace distance between ρ_{AB} and σ_{AB} is at most δ. Apply Fannes' inequality again and get the bound (17). This completes the proof of Lemma 6. □.

Theorem 1 follows from Lemma 3, Lemma 4, Lemma 5, Lemma 6 and Theorem 3.

Proof. [Proof of Theorem 1] Let $(A_i, B_{ij}, |\psi\rangle)$ be an ε-optimal strategy in CHSH(n). Apply Lemma 3 and get operators A_i, $\tilde{A}_{ij}$ satisfying (10) and (11).

Next, for each i, take A'_i to be that operator among $\tilde{A}_{i1}, \dots \tilde{A}_{i(i-1)}, \tilde{A}_{i(i+1)}, \dots \tilde{A}_{in}$ that makes $\|(A_i \otimes \mathrm{Id} - \mathrm{Id} \otimes A'_i)|\psi\rangle\|$ smallest. From (11) we obtain

$$\mathrm{E}_i \|(A_i \otimes \mathrm{Id} - \mathrm{Id} \otimes A'_i)|\psi\rangle\| = O(\sqrt{\varepsilon})$$

Next, apply Lemma 4 with $\delta = O(\sqrt{\varepsilon})$. We obtain $X_k, Z_k, X'_k, Z'_k, k = 1, \dots \lfloor n/3 \rfloor$ satisfying (13) and (14). We think of a complete graph on $m = \lfloor n/3 \rfloor$ vertices, and associate the two weights $\|(P_k \otimes \mathrm{Id} - \mathrm{Id} \otimes P'_k)|\psi\rangle\|$ to vertex k and the eight weights $\|[P_k, Q_l] \otimes \mathrm{Id}\,|\psi\rangle\|, \|\,\mathrm{Id} \otimes [P'_k, Q'_l]|\psi\rangle\|$ to edge (k, l) (again, each of P, Q stands for either X or Z). We apply Lemma 5 and obtain a subset of $\{1, \dots m\}$ of size at least

$$r = \frac{(a-2)^2 n}{8a(n-1) + a(a-2)}$$

such that the corresponding observables satisfy the assumptions of Theorem 3 with $\eta = O(a\sqrt{\varepsilon})$.

We apply Corollary 1, and get that the first bound in the corollary holds with error $\delta/2 = cr^{3/2}a\sqrt{\varepsilon}$. We apply Lemma 6 and get that the entanglement entropy of $|\psi\rangle$ is at least

$$r - 3\delta r + 2\delta \log(\delta)$$

We choose $a = \Theta(\varepsilon^{-1/5})$ so that $r = \Theta(\varepsilon^{-1/5})$ and $\delta = 1/100$. For this choice, the lower bound on the entanglement entropy of $|\psi\rangle$ is $\Omega(\varepsilon^{-1/5})$ as needed. □.

Acknowledgements

We would like to thank the referees for their valuable comments; the presentation was much improved as a result. Work on this article was performed while Dimiter Ostrev was at the Department of Mathematics, Massachusetts Institute of Technology, Cambridge, Massachusetts, USA. Thomas Vidick 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

1. Bas Hensen, H Bernien, AE Dréau, A Reiserer, N Kalb, MS Blok, J Ruitenberg, 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.
2. 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.
3. 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.
4. John F. Clauser, Michael A. Horne, Abner Shimony, and Richard A. Holt. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.*, 23:880–884, 1969.
5. Tzyh Haur Yang and Miguel Navascués. Robust self-testing of unknown quantum systems into any entangled two-qubit states. *Physical Review A*, 87(5):050102, 2013.
6. William Slofstra. Lower bounds on the entanglement needed to play XOR non-local games. *Journal of Mathematical Physics*, 52(10):102202, 2011.
7. Rui Chao, Ben W. Reichardt, Chris Sutherland, and Thomas Vidick. Test for a large amount of entanglement, using few measurements. In *Proceedings of the 2017 Conference on Innovations in Theoretical Computer Science (ITCS)*, 2017.
8. Andrea Coladangelo. Parallel self-testing of (tilted) epr pairs via copies of (tilted) chsh and the magic square game. *Quantum Information and Computation*, 17(9-10):831–865, 2017.
9. Matthew Coudron and Anand Natarajan. The parallel-repeated magic square game is rigid. *arXiv preprint arXiv:1609.06306*, 2016.
10. Anand Natarajan and Thomas Vidick. A quantum linearity test for robustly verifying entanglement. In *Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing*, pages 1003–1015. ACM, 2017.
11. Andrea Coladangelo and Jalex Stark. Robust self-testing for linear constraint system games. *arXiv preprint arXiv:1709.09267*, 2017.
12. Matthew McKague. Self-testing high dimensional states using the generalized Magic Square game. *arXiv preprint arXiv:1605.09435*, 2016.
13. Mohammad Bavarian and Peter W. Shor. Information causality, Szemerédi-Trotter and algebraic variants of CHSH. In *Proceedings of the 2015 Conference on Innovations in Theoretical Computer Science*, pages 123–132. ACM, 2015.
14. 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.
15. Richard Cleve, Peter Høyer, Ben Toner, and John Watrous. Consequences and limits of nonlocal strategies. In *Proc. 19th IEEE Conf. on Computational Complexity (CCC'04)*, pages 236–249. IEEE Computer Society, 2004.
16. Assaf Naor and Oded Regev. Krivine schemes are optimal. *Proceedings of the American Mathe-*

matical Society, 142(12):4315–4320, 2014.
17. Andrea Montanari and Subhabrata Sen. Semidefinite programs on sparse random graphs and their application to community detection. In *Proc. 48th STOC*, pages 814–827. ACM, 2016.
18. Assaf Naor, Oded Regev, and Thomas Vidick. Efficient rounding for the noncommutative Grothendieck inequality. In *Proc. 45th STOC*, pages 71–80, New York, NY, USA, 2013. ACM.
19. Isidore Isaac Hirschman. A convexity theorem for certain groups of transformations. *Journal d'Analyse Mathématique*, 2(2):209–218, 1952.
20. Ben Reichardt, Falk Unger, and Umesh Vazirani. A classical leash for a quantum system: Command of quantum systems via rigidity of CHSH games. *Nature*, 496(7446):456–460, 2013.
21. Jedrzej Kaniewski, Marco Tomamichel, and Stephanie Wehner. Entropic uncertainty from effective anticommutators. *Physical Review A*, 90(1):012332, 2014.
22. Boris S Tsirelson. Quantum analogues of the bell inequalities. the case of two spatially separated domains. *Journal of Soviet Mathematics*, 36(4):557–570, 1987.
23. Boris S Tsirelson. Some results and problems on quantum bell-type inequalities. *Hadronic Journal Supplement*, 8(4):329–345, 1993.
24. Sander Gribling, David de Laat, and Monique Laurent. Matrices with high completely positive semidefinite rank. *Linear Algebra and its Applications*, 513:122–148, 2017.
25. Jop Briët, Harry Buhrman, and Ben Toner. A generalized Grothendieck inequality and nonlocal correlations that require high entanglement. *Comm. Mat. Phys.*, 305(3):827–843, 2011.
26. Dimiter Ostrev. The structure of nearly-optimal quantum strategies for the chsh (n) xor games. *Quantum Information & Computation*, 16(13-14):1191–1211, 2016.
27. Matthew McKague, Tzyr Haur Yang, and Valerio Scarani. Robust self-testing of the singlet. *Journal of Physics A: Mathematical and Theoretical*, 45(45):455304, 2012.
28. Ben W. Reichardt, Falk Unger, and Umesh Vazirani. A classical leash for a quantum system: Command of quantum systems via rigidity of CHSH games. In *Proc. 4th ITCS*, pages 321–322, New York, NY, USA, 2013. ACM.
29. Rui Chao, Ben W. Reichardt, Chris Sutherland, and Thomas Vidick. Overlapping qubits. In *Proceedings of the 2017 Conference on Innovations in Theoretical Computer Science (ITCS)*, 2017.
30. Michael A Nielsen and Isaac L Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2010.
31. Norman L. Johnson, Samuel Kotz, and N. Balakrishnan. *Continuous Univariate Distributions*, volume 2. Wiley, 1995.