Quantum Strategies Are Better Than Classical in Almost Any XOR Game*

Andris Ambainis[1], Artūrs Bačkurs[1], Kaspars Balodis[1], Dmitrijs Kravčenko[1], Raitis Ozols[1], Juris Smotrovs[1], and Madars Virza[2]

[1] Faculty of Computing, University of Latvia, Raina bulv. 19, Riga, LV-1586, Latvia
{andris.ambainis,Juris.Smotrovs}@lu.lv,
{abackurs,kbalodis,kdmitry}@gmail.com, raitis.ozols@inbox.lv
[2] Computer Science and Artificial Intelligence Laboratory, Massachusetts Institute of Technology, 32 Vassar Street, Cambridge, MA 02139, USA
madars@gmail.com

Abstract. We initiate a study of random instances of nonlocal games. We show that quantum strategies are better than classical for almost any 2-player XOR game. More precisely, for large n, the entangled value of a random 2-player XOR game with n questions to every player is at least 1.21... times the classical value, for $1 - o(1)$ fraction of all 2-player XOR games.

1 Introduction

Quantum mechanics is strikingly different from classical physics. In the area of information processing, this difference can be seen through quantum algorithms which can be exponentially faster than conventional algorithms [27,25] and through quantum cryptography which offers degree of security that is impossible classically [5].

Another information-theoretic way of seeing the difference between quantum mechanics and the classical world is through non-local games. An example of a non-local game is the CHSH (Clauser-Horne-Shimony-Holt) game [10]. This is a game played by two players against a referee. The two players cannot communicate but can share common randomness or a common quantum state that is prepared before the beginning of the game. The referee sends an independent uniformly random bit to each of the two players. Each player responds by sending one bit back to the referee. Players win if $x \oplus y = i \wedge j$ where i, j are the bits that the referee sent to the player and x, y are players' responses. The maximum winning probability that can be achieved is 0.75 classically and $\frac{1}{2} + \frac{1}{2\sqrt{2}} = 0.85...$ quantumly.

There are several reasons why non-local games are interesting. First, CHSH game provides a very simple example to test the validity of quantum mechanics. If we have implemented the referee and the two players A, B by devices so that

* Supported by ESF project 2009/0216/1DP/1.1.1.2.0/09/APIA/VIAA/044 and FP7 FET-Open project QCS. Full version available as arXiv preprint arXiv:1112.3330.

A. Czumaj et al. (Eds.): ICALP 2012, Part I, LNCS 7391, pp. 25–37, 2012.

there is no communication possible between A and B and we observe the winning probability of 0.85..., there is no classical explanation possible. Second, non-local games have been used in device-independent cryptography [1,26].

Some non-local games show big gaps between the classical and the quantum winning probabilities. For example, Buhrman et al. [8] construct a 2-player quantum game where the referee and the players send values $x, y, i, j \in \{1, \ldots, n\}$ and the classical winning probability is $\frac{1}{2} + \Theta(\frac{1}{\sqrt{n}})$ while the quantum winning probability is 1. In contrast, Almeida et al. [2] construct a non-trivial example of a game in which quantum strategies provide no advantage at all.

Which of those is the typical behaviour? In this paper, we study this question by looking at random instances of non-local games.

More specifically, we study two-party XOR games with uniform distribution of inputs. This is a subclass of non-local games with 2 players, where the referee chooses inputs $i \in \{1, 2, \ldots, n\}$, $j \in \{1, 2, \ldots, k\}$ uniformly at random and sends them to the players. The players reply by sending bits x and y. The rules of the game are specified by an $n \times k$ matrix A whose entries are $+1$ and -1. To win, the players must produce x and y with $x = y$ if $A_{ij} = 1$ and x and y with $x \neq y$ if $A_{ij} = -1$.

We consider the case when the matrix A that specifies the rules of the game is chosen randomly against all ± 1-valued $n \times k$ matrices A. For the case when $n = k$, we show that

- The maximum winning probability p_q that can be achieved by a quantum strategy is $\frac{1}{2} + \frac{1 \pm o(1)}{\sqrt{n}}$ with a probability $1 - o(1)$;
- The maximum winning probability p_{cl} that can be achieved by a classical strategy satisfies

$$\frac{1}{2} + \frac{0.6394... - o(1)}{\sqrt{n}} \leq p_{cl} \leq \frac{1}{2} + \frac{0.8325... + o(1)}{\sqrt{n}}$$

  with a probability $1 - o(1)$.

In the literature on non-local games, one typically studies the difference between the winning probability p_q (p_{cl}) and the losing probability $1 - p_q$ ($1 - p_{cl}$): $\Delta_q = 2p_q - 1$ ($\Delta_{cl} = 2p_{cl} - 1$). The advantage of quantum strategies is then evaluated by the ratio $\frac{\Delta_q}{\Delta_{cl}}$. For random XOR games, our results imply that

$$1.2011... < \frac{\Delta_q}{\Delta_{cl}} < 1.5638...$$

for almost all games. Our computer experiments suggest that, for large n, $\frac{\Delta_q}{\Delta_{cl}} \approx 1.305...$. For comparison, the biggest advantage that can be achieved in any 2-player XOR game is equal to Grothendieck's constant K_G [14] about which we know that [16,23,6]

$$1.67696.... \leq K_G \leq 1.7822139781...$$

Thus, the quantum advantage in random XOR games is comparable to the maximum possible advantage for this class of non-local games.

We find this result quite surprising. Quantum-over-classical advantage usually makes use of a structure that is present in the computational problem (such as the algebraic structure that enables Shor's quantum algorithm for factoring [25]). Such structure is normally not present in random computational problems.

The methods that we use to prove our results are also quite interesting. The upper bounds are easy in both classical and quantum case but both lower bounds are fairly sophisticated. The lower bound for the entangled value requires proving a new version of Marčenko-Pastur law [19] for random matrices.

The classical value of random XOR games is equal to a natural quantity ($l_\infty \to l_1$ norm of a random matrix) that might be interesting for other purposes. The lower bound for it requires a subtle argument that reduces lower-bounding the classical value to analyzing a certain random walk.

Related Work. Junge and Palazuelos [17] and Briet and Vidick [7] have constructed non-local games with a big gap between the quantum (entangled) value and the classical value, via randomized constructions. The difference between this paper and [7,17] is as follows. The goal of [7,17] was to construct a big gap between the entangled value and the classical value of a non-local game and the probability distribution on non-local games and inputs was chosen so that this goal would be achieved.

Our goal is to study the behaviour of non-local games in the case when the conditions are random. We therefore choose a natural probability distribution on non-local games (without the goal of optimizing the quantum advantage) and study it. The surprising fact is that a substantial quantum advantage still exists in such setting.

2 Technical Preliminaries

We use $[n]$ to denote the set $\{1, 2, \ldots, n\}$.

In a 2-player XOR game, we have two players A and B playing against a referee. Players A and B cannot communicate but can share common random bits (in the classical case) or an entangled quantum state (in the quantum case). The referee randomly chooses values $i \in \{1, \ldots, n\}$ and $j \in \{1, \ldots, n\}$ and sends them to A and B, respectively. Players A and B respond by sending answers $x \in \{0, 1\}$ and $y \in \{0, 1\}$ to the referee.

Players win if answers x and y satisfy some winning condition $P(i, j, x, y)$. For XOR games, the condition may only depend on the parity $x \oplus y$ of players' responses. Then, it can be written as $P(i, j, x \oplus y)$.

For this paper, we also assume that, for any i, j, exactly one of $P(i, j, 0)$ and $P(i, j, 1)$ is true. Then, we can describe a game by an $n \times n$ matrix $(A_{ij})_{i,j=1}^n$ where $A_{ij} = 1$ means that, given i and j, players must output x, y with $x \oplus y = 0$ (equivalently, $x = y$) and $A_{ij} = -1$ means that players must output x, y with $x \oplus y = 1$ (equivalently, $x \neq y$).

Let $p_{S,win}$ be the probability that the players win if they use a strategy S and $p_{S,los} = 1 - p_{S,win}$ be the probability that they lose. We will be interested in the difference $\Delta_S = p_{S,win} - p_{S,los}$ between the winning and the losing probabilities. The *classical value* of a game, Δ_{cl}, is the maximum of Δ_S over all classical strategies S. The *entangled value* of a game, Δ_q, is the maximum of Δ_S over all quantum strategies S.

Let p_{ij} be the probability that the referee sends question i to player A and question j to player B. Then [11, section 5.3], the classical value of the game is equal to

$$\Delta_{cl} = \max_{u_1,\ldots,u_n \in \{-1,1\}} \max_{v_1,\ldots,v_n \in \{-1,1\}} \sum_{i,j=1}^{n} p_{ij} A_{ij} u_i v_j. \tag{1}$$

In the quantum case, Tsirelson's theorem [9] implies that

$$\Delta_q = \max_{u_i : \|u_i\|=1} \max_{v_j : \|v_j\|=1} \sum_{i,j=1}^{n} p_{ij} A_{ij} \langle u_i, v_j \rangle \tag{2}$$

where the maximization is over all tuples of unit-length vectors $u_1, \ldots, u_n \in R^d$, $v_1, \ldots, v_n \in R^d$ (in an arbitrary number of dimensions d).

We will assume that the probability distribution on the referee's questions i, j is uniform: $p_{ij} = \frac{1}{n^2}$ and study Δ_{cl} and Δ_q for the case when A is a random Bernoulli matrix (i.e., each entry A_{ij} is $+1$ with probability $1/2$ and -1 with probability $1/2$, independently of other entries).

Other probability distributions on referee's questions can be considered, as well. For example, one could choose y_{ij} to be normally distributed random variables with mean 0 and variance 1 and take $p_{ij} = \frac{|y_{ij}|}{\sum_{i,j=1}^{n} |y_{ij}|}$. Or, more generally, one could start with y_{ij} being i.i.d. random variables from some arbitrary distribution D and define p_{ij} in a similar way.

Most of our results are still true in this more general setting (with mild assumptions on the probability distribution D). Namely, Theorem 1 and the upper bound part of Theorem 4 remain unchanged. The only exception is the lower bound part of Theorem 4 which relies on the fact that the probability distribution p_{ij} is uniform. It might be possible to generalize our lower bound proof to other distributions D but the exact constant in such generalization of our lower bound could depend on the probability distribution D.

3 Quantum Upper and Lower Bound

Theorem 1. *For a random 2-player XOR game with n inputs for each player,*

$$\Delta_q = \frac{2 \pm o(1)}{\sqrt{n}}$$

with probability $1 - o(1)$.

Proof. Because of (2), proving our theorem is equivalent to showing that

$$\max_{\|u_i\|=\|v_j\|=1} \sum_{i=1}^{n}\sum_{j=1}^{n} A_{ij}\langle u_i, v_j\rangle = (2 \pm o(1))n^{3/2}$$

holds with probability $1 - o(1)$.

For the upper bound, we rewrite this expression as follows. Let u be a vector obtained by concatenating all vectors u_i and v be a vector obtained by concatenating all v_j. Since $\|u_i\| = \|v_j\| = 1$, we have $\|u\| = \|v\| = \sqrt{n}$. We have

$$\sum_{i=1}^{n}\sum_{j=1}^{n} A_{ij}\langle u_i, v_j\rangle = \langle u, (A \otimes I)v\rangle \leq \|u\| \cdot \|A \otimes I\| \cdot \|v\| \leq \|A\|n.$$

By known results on operator norms of random matrices [30], $\|A\| = (2+o(1))\sqrt{n}$ with a high probability.

For the lower bound, we note that

$$\max_{\|u_i\|=\|v_j\|=1} \sum_{i=1}^{n}\sum_{j=1}^{n} A_{ij}\langle u_i, v_j\rangle = \max_{\|u_i\|\leq 1, \|v_j\|\leq 1} \sum_{i=1}^{n}\sum_{j=1}^{n} A_{ij}\langle u_i, v_j\rangle.$$

We have

Theorem 2 (Marčenko-Pastur law, [19]). *Let A be a $n \times n$ random matrix whose entries A_{ij} are independent random variables with mean 0 and variance 1. Let $C \in [0, 2]$. With probability $1 - o(1)$, the number of singular values λ of A that satisfy $\lambda \geq C\sqrt{n}$ is $(f(C) - o(1))n$ where*

$$f(C) = \frac{1}{2\pi} \int_{x=C^2}^{4} \sqrt{\frac{4}{x} - 1}dx.$$

Let $\lambda_1, \ldots, \lambda_m$ be the singular values of A that satisfy $\lambda_i \geq (2 - \epsilon)\sqrt{n}$. With high probability, we have $m \in [(f(2 - \epsilon) - o(1))n, (f(2 - \epsilon) + o(1))n]$. We now assume that this is the case.

Let l_i and r_i be the corresponding left and right singular vectors: $Ar_i = \lambda_i l_i$. (Here, we choose l_i and r_i so that $\|l_i\| = \|r_i\| = 1$ for all i.) Let l_{ij} and r_{ij} be the components of l_i and r_i: $l_i = (l_{ij})_{j=1}^{n}$ and $r_i = (r_{ij})_{j=1}^{n}$.

We define u_j and v_j in a following way:

$$u_j = (l_{ij})_{i=1}^{m}, \quad v_j = (r_{ij})_{i=1}^{m}.$$

We have

$$\sum_{i=1}^{n}\sum_{j=1}^{n} A_{ij}\langle u_i, v_j\rangle = \sum_{i=1}^{n}\sum_{j=1}^{n}\sum_{k=1}^{m} A_{ij} l_{ki} r_{kj}$$

$$= \sum_{k=1}^{m} \langle l_k, Ar_k\rangle = \sum_{k=1}^{m} \lambda_k \geq (2 - \epsilon)m\sqrt{n}. \tag{3}$$

Since $\|l_i\| = \|r_i\| = 1$ and the vectors u_i and v_j are obtained by rearranging the entries of l_i and r_i, we have

$$\sum_{i=1}^{n} \|u_i\|^2 = \sum_{i=1}^{n} \|l_i\|^2 = m$$

and, similarly, $\sum_i \|v_i\|^2 = m$. If u_i and v_i all were of the same length, we would have $\|u_i\|^2 = \|v_i\|^2 = \frac{m}{n}$. Then, replacing u_i and v_i by $u'_i = \frac{u_i}{\|u_i\|}$ and $v'_i = \frac{v_i}{\|v_i\|}$ would increase each vector $\sqrt{\frac{n}{m}}$ times and result in

$$\sum_{i=1}^{n}\sum_{j=1}^{n} A_{ij}\langle u'_i, v'_j\rangle \geq (2-\epsilon)n^{3/2}.$$

To deal with the general case, we will show that almost all u_i and v_i are of roughly the same length. Then, a similar argument will be used. The key to our proof is a new modification of Marčenko-Pastur law.

Theorem 3 (Modified Marčenko-Pastur law). *Let A be an $n \times n$ random matrix whose entries A_{ij} are independent random variables with mean 0 and variance 1. Let $C \in [0,2]$. Let e_i be the i^{th} vector of the standard basis. Let P_C be the projector on the subspace spanned by the right singular vectors with singular values at least $C\sqrt{n}$. Then,*

$$Pr\left[\left|\|P_C e_i\|^2 - f(C)\right| > \epsilon\right] = O\left(\frac{1}{n}\right)$$

with the big-O constant depending on C and ϵ.

The same result also holds for the left singular vectors.

Proof. The proof is given in the full version of the paper. □

We now complete the proof, assuming the modified Marčenko-Pastur law. Since P_C is spanned by the right singular vectors $r_1, \ldots, r_m$, we have

$$\|P_C e_i\|^2 = \sum_{j=1}^{m} \langle r_j, e_i\rangle^2 = \sum_{j=1}^{m} r_{ji}^2 = \|v_i\|^2. \tag{4}$$

Therefore, the modified Marčenko-Pastur law means that

$$Pr[\|v_i\|^2 > f(2-\epsilon) + \delta] = O\left(\frac{1}{n}\right).$$

Thus, the expected number of $i \in \{1, \ldots, n\}$ for which $\|v_i\|^2 > f(2-\epsilon) + \delta$ is $O(1)$. We now apply the following transformations to vectors v_i:

1. For each v_i with $\|v_i\|^2 > f(2-\epsilon) + \delta$ (or u_i with $\|u_i\|^2 > f(2-\epsilon) + \delta$), we replace it by the zero vector $\overrightarrow{0}$;

2. We replace each v_i by
$$v_i' = \frac{v_i}{\sqrt{f(2-\epsilon)+\delta}}$$
and similarly for u_i.

After the first step $\|v_i\|^2 \leq f(2-\epsilon)+\delta$ for all i. Hence, after the second step, $\|v_i'\|^2 \leq 1$ for all i.

We now bound the effect of those two steps on the sum
$$\sum_{i=1}^{n}\sum_{j=1}^{n} A_{ij}\langle u_i, v_j\rangle.$$

Because of (3), the initial value of this sum is at least
$$(2-\epsilon)m\sqrt{n} \geq (2-\epsilon)(f(2-\epsilon)-o(1))n^{3/2}. \tag{5}$$

Because of (4), $\|v_j\|^2 = \|P_C e_j\|^2 \leq \|e_j\|^2 = 1$. Similarly, $\|u_i\|^2 \leq 1$. Hence, $|\langle u_i, v_j\rangle| \leq 1$ and replacing one v_j (or u_i) by 0 changes the sum by at most $\sum_{i=1}^{n}|A_{ij}| = n$. Replacing $O(1)$ v_j's (or u_i's) changes it by $O(n)$. Since the sum (5) is of the order $\Theta(n^{3/2})$, this is a lower order change.

Replacing v_i's by v_i''s (and u_i's by similarly defined u_i''s) increases each inner product $\langle u_i, v_j\rangle$ $\frac{1}{f(2-\epsilon)+\delta}$ times and achieves
$$\sum_{i=1}^{n}\sum_{j=1}^{n} A_{ij}\langle u_i', v_j'\rangle \geq \frac{(2-\epsilon)(f(2-\epsilon)-o(1))}{f(2-\epsilon)+\delta} n^{3/2}.$$

Since this can be achieved for any fixed $\epsilon > 0$ and $\delta > 0$, we get that
$$\max_{\|u_i'\|\leq 1, \|v_j'\|\leq 1} \sum_{i=1}^{n}\sum_{j=1}^{n} A_{ij}\langle u_i', v_j'\rangle \geq (2-o(1))n^{3/2}.$$

□

4 Classical Upper and Lower Bound

In the classical case, we have to estimate
$$\Delta_{cl} = \max_{u_1,\ldots,u_n\in\{-1,1\}} \max_{v_1,\ldots,v_n\in\{-1,1\}} \sum_{i,j=1}^{n} A_{ij}u_i v_j. \tag{6}$$

There are several ways how one can interpret this expression and several contexts in which similar quantities have been studied before:

1. (6) is equal to the $l_\infty \to l_1$ norm of A (denoted $\|A\|_{\infty\to 1}$). It is known that, for a random matrix A, $\|A\|_{\infty\to 1} = \Theta(n\sqrt{n})$ (e.g., from [21] or [18]), but the exact constant under Θ is not known.

2. One can also interpret (6) combinatorially, as a problem of "unbalancing lights" [3]. In this interpretation, $n \times n$ matrix represents an array of lights, with each light being "on" ($A_{ij} = 1$) or "off" ($A_{ij} = -1$). We are allowed to choose a row or a column and switch all lights in this row or column. The task is to maximize the difference between the number of lights that are on and the number of lights that are off. It is known that for any $n \times n$ matrix A with ± 1 entries, (6) is at least $\sqrt{\frac{2}{\pi}} n^{3/2}$ [3, p.19]. We are not aware of any work on evaluating (6) for a random matrix A in this context.
3. In the context of statistical physics, there has been substantial work on determining the order of

$$\max_{u_1,\ldots,u_n \in \{-1,1\}} \sum_{i,j=1}^{n} A_{ij} u_i u_j \tag{7}$$

when A_{ij} is a symmetric Gaussian matrix (each $A_{ij} = A_{ji}$ is an independent Gaussian random variable with mean 0 and variance 1). It is known that (7) is equal to $(1.527... + o(1))n^{3/2}$ with probability $1 - o(1)$. This was first discovered in [24,22] and rigorously proven by Talagrand [29].

The quantities (6) and (7) are of similar flavour but are not identical and there is no clear relation between them.

Theorem 4. *For a random 2-player XOR game, its classical value Δ_{cl} satisfies*

$$\frac{1.2789...}{\sqrt{n}} \leq \Delta_{cl} \leq \frac{2\sqrt{\ln 2} + o(1)}{\sqrt{n}} = \frac{1.6651... + o(1)}{\sqrt{n}}$$

with probability $1 - o(1)$.

This is equivalent to

$$1.2789...n^{3/2} \leq \|A\|_{\infty \to 1} \leq 1.6651...n^{3/2}$$

for a Bernoulli random matrix A.

In computer experiments, the ratio $\frac{\|A\|_{\infty \to 1}}{n^{3/2}}$ grows with n and reaches 1.4519... for $n = 26$. By fitting a formula $an^{3/2} + bn$ where the leading term is of the order $n^{3/2}$ and the largest correction term is of the order n to the data, we obtained that

$$\|A\|_{\infty \to 1} \approx 1.53274...n^{3/2} - 0.472806...n.$$

Figure 1 shows the fit. Curiously, the constant in front of $n^{3/2}$ is very close to the constant 1.527... for the sum (7). We do not know whether this is a coincidence or there is some connection between the asymptotic behaviour of the two sums.

Proof. The upper bound follows straightforwardly from Chernoff bounds (and is similar to the argument in [18] which provides an upper bound on (6) which holds with probability $1 - O(1/c^n)$). We use the following form of Chernoff inequality:

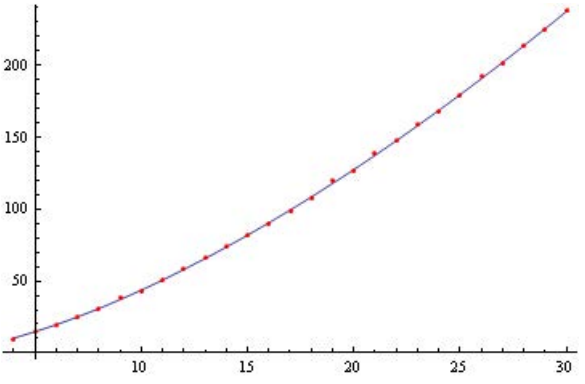

Fig. 1. $\|A\|_{\infty\to 1}$, for random $n \times n$ matrices A

Theorem 5. *[3, p.263] Let $X_1, \ldots, X_n$ be independent random variables with $Pr[X_i = 1] = Pr[X_i = -1] = \frac{1}{2}$ and let $X = X_1 + \ldots + X_n$. Then,*

$$Pr[X \geq a] < e^{-\frac{a^2}{2n}}.$$

Let $x_1, \ldots, x_n \in \{-1, 1\}$ and $y_1, \ldots, y_n \in \{-1, 1\}$ be arbitrary. If $A_{ij} \in \{-1, 1\}$ are uniformly random, then $A_{ij}x_iy_j \in \{-1, 1\}$ are also uniformly random. Hence, $\sum_{i,j} A_{ij}x_iy_j$ is a sum of n^2 uniformly random values from $\{-1, 1\}$. By Theorem 5,

$$\Pr\left[\sum_{i,j} A_{ij}x_iy_j > Cn^{\frac{3}{2}}\right] < e^{\frac{-\left(Cn^{\frac{3}{2}}\right)^2}{2n^2}} = \frac{1}{e^{\frac{C^2n}{2}}}.$$

By taking $C = 2\sqrt{\ln 2} + 2\frac{\sqrt{\ln n}}{\sqrt{n}}$, we can ensure that this probability is less than $\frac{1}{2^{2n}n^2}$. Then, by the union bound, the probability that $\sum_{i,j} A_{ij}x_iy_j > Cn^{\frac{3}{2}}$ for some choice of x_i's and y_j's is less than $2^{2n}\frac{1}{2^{2n}n^2} = \frac{1}{n^2}$.

We now prove the lower bound[1]. We first show

Lemma 1. *Let A be an $n \times n$ random Bernoulli matrix. Then,*

$$\mathrm{E}_A\left[\max_{u_i,v_j\in\{-1,1\}} \sum_{i,j} u_iv_jA_{ij}\right] \geq (1.2789... - o(1))n^{3/2}.$$

[1] This lower bound is not necessary for proving the advantage of quantum strategies which follows by combining the classical upper bound and the quantum lower bound. But it is interesting for two other reasons. First, it is necessary to show that, for a random XOR game, $\frac{\Delta_q}{\Delta_{cl}}$ is less than Grothendiek's constant. Second, as discussed at the beginning of this section, the classical value is equal to a natural quantity that comes up in several other settings.

Let $X = \max_{u_i, v_j \in \{-1,1\}} \sum_{i,j} u_i v_j A_{ij}$. By Lemma 1, $E[X] \geq (1.2789... - o(1))n^{3/2}$. To prove that $X \geq (1.2789... - o(1))n^{3/2}$ with probability $1 - o(1)$, we show that X is concentrated around $E[X]$.

Lemma 2. *Let $X = \max_{u_i, v_j \in \{-1,1\}} \sum_{i,j} u_i v_j A_{ij}$ for a random $n \times n$ matrix A. Then,*

$$Pr\left[|X - E[X]| \geq an\right] < 2e^{-a^2/8}.$$

We then apply Lemma 2 with $a = \log n$ (or with $a = f(n)$ for any other $f(n)$ that has $f(n) \to \infty$ when $n \to \infty$ and $f(n) = o(\sqrt{n})$) and combine it with Lemma 1.

It remains to prove the two lemmas.

Proof (of Lemma 1). Let A be a random ± 1 matrix. We choose u_i and v_j, according to Algorithm 1.

Because of the last step, we get that

$$\sum_{i=1}^{n} \sum_{j=1}^{n} u_i v_j A_{ij} = \sum_{j=1}^{n} |S_{n,j}|.$$

Each of $S_{n,j}$ is a random variable with an identical distribution. Hence,

$$E\left[\sum_{i=1}^{n} \sum_{j=1}^{n} u_i v_j A_{ij}\right] = \sum_{j=1}^{n} E|S_{n,j}| = nE|S_{n,1}|. \tag{8}$$

1. Set $u_1 = 1$.
2. For each $k = 2, \ldots, n$ do:
   (a) For each $j = 1, \ldots, n$, compute $S_{k-1,j} = \sum_{i=1}^{k-1} A_{ij} u_i$.
   (b) Let $a_k = (Z(S_{k-1,1}), Z(S_{k-1,2}), ..., Z(S_{k-1,n}))$ where $Z(x) = 1$ if $x > 0$, $Z(x) = -1$ if $x < 0$ and $Z(x) = 1$ or $Z(x) = -1$ with equal probability $\frac{1}{2}$ if $x = 0$.
   (c) Let $b_k = (A_{k1}, A_{k2}, ..., A_{kn})$.
   (d) Let $u_k \in \{+1, -1\}$ be such that a_k and $u_k b_k$ agree in the maximum number of positions.
3. For each $j = 1, \ldots, n$, let v_j be such that $v_j S_{n,j} \geq 0$ where $S_{n,j} = \sum_{i=1}^{n} A_{ij} u_i$.

Algorithm 1. Algorithm for choosing u_i and v_j for a given matrix A

We now consider a random walk with a reflecting boundary. The random walk starts at position 0. If it is at the position 0, it always moves to the position 1. If it is at the position $i > 0$, it moves to the position $i + 1$ with probability $\frac{1}{2} + \frac{\epsilon}{2}$ and position $i - 1$ with probability $\frac{1}{2} - \frac{\epsilon}{2}$. Let K_i^{ϵ} be the position of the walker after i steps.

Lemma 3. *$|S_{n,1}| = K_n^\epsilon$ for some $\epsilon = (1+o(1))\sqrt{\frac{2}{\pi n}}$.*

Proof. $b_i = (A_{i1}, \ldots, A_{in})$ is a vector consisting of random ± 1's that is independent of a_i. Hence, the expected number of agreements between a_i and $u_i b_i$ is $(\frac{1}{2} + \frac{\epsilon}{2})n$ where $\epsilon = (1+o(1))\sqrt{\frac{2}{\pi n}}$ [3, p.21]. Moreover, the probability of a_i and $u_i b_i$ agreeing in location j is the same for all j.

Hence, if $|S_{i-1,1}| > 0$, we have $|S_{i,1}| = |S_{i-1,1}| + 1$ with probability $\frac{1}{2} + \frac{\epsilon}{2}$ and $|S_{i,1}| = |S_{i-1,1}| - 1$ with probability $\frac{1}{2} - \frac{\epsilon}{2}$. If $|S_{i-1,1}| = 0$, then we always have $|S_{i,1}| = 1$. □

Lemma 4. *For a random walk with a reflecting boundary and $\epsilon = \frac{\alpha}{\sqrt{n}}$, we have $E[K_n^\epsilon] \geq (f(\alpha) - o(1))\sqrt{n}$ where*

$$f(\alpha) = \frac{1}{2}\left(e^{-\frac{\alpha^2}{2}}\sqrt{\frac{2}{\pi}} + \alpha + \left(\frac{1}{\alpha} + \alpha\right)\mathrm{Erf}\left(\frac{\alpha}{\sqrt{2}}\right)\right).$$

Proof. The proof is given in the full version of the paper. □

By combining (8) and Lemmas 3 and 4, the probability of winning minus the probability of losing in the classical case of a random XOR game is at least

$$f\left(\sqrt{\frac{2}{\pi}}\right)\sqrt{n} \cdot n \cdot \frac{1}{n^2} = \frac{2 + 2e^{-1/\pi} + (2+\pi)\mathrm{Erf}\left(\frac{1}{\sqrt{\pi}}\right)}{2\sqrt{2\pi}} n^{-\frac{1}{2}}$$

$$= 1.2789076012442957... n^{-\frac{1}{2}}.$$

□

Proof (of Lemma 2). Let

$$f(A_{11}, A_{12}, \ldots, A_{nn}) = \max_{u_i, v_j \in \{-1,1\}} \sum_{i,j} u_i v_j A_{ij}.$$

Then, changing one A_{ij} from $+1$ to -1 (or from -1 to $+1$) changes $\sum_{i,j} u_i v_j A_{ij}$ by at most 2. This means that $f(A_{11}, \ldots, A_{nn})$ changes by at most 2 as well. In other words, f is 2-Lipschitz. By applying Azuma's inequality [20, p. 303-305] with $c = 2$, $t = n^2$, $\lambda = \frac{a}{2}$, we get

$$Pr\left[|f(A_{11}, \ldots, A_{nn}) - E[f(A_{11}, \ldots, A_{nn})]| \geq an\right] < 2e^{-a^2/8}.$$

□

5 Conclusion

We showed that quantum strategies are better than classical for random instances of XOR games. We expect that similar results may be true for other classes of non-local games.

A possible difficulty with proving them is that the mathematical methods for analyzing other classes of non-local games are much less developed. There is a well developed mathematical framework for studying XOR games [9,11,31] which we used in our paper. But even with that, some of our proofs were quite involved. Proving a similar result for a less well-studied class of games would be even more difficult.

Acknowledgments. We thank Assaf Naor, Oded Regev, Stanislaw Szarek and several anonymous referees for useful comments and references to related work.

References

1. Acin, A., Brunner, N., Gisin, N., Massar, S., Pironio, S., Scarani, V.: Device-independent security of quantum cryptography against collective attacks. Physical Review Letters 98, 230501 (2007)
2. Almeida, M.L., Bancal, J.-D., Brunner, N., Acin, A., Gisin, N., Pironio, S.: Guess your neighbour's input: a multipartite non-local game with no quantum advantage. Physical Review Letters 104, 230404 (2010), also arXiv:1003.3844
3. Alon, N., Spencer, J.: The Probabilistic Method. Wiley (2000)
4. Bai, Z., Silverstein, J.: Spectral Analysis of Large Dimensional Random Matrices. Springer (2010)
5. Bennett, C.H., Brassard, G.: Quantum Cryptography: Public key distribution and coin tossing. In: Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, p. 175 (1984)
6. Braverman, M., Makarychev, K., Makarychev, Y., Naor, A.: The Groethendieck constant is strictly smaller than Krivine's bound. In: Proceedings of FOCS 2011, pp. 453–462 (2011)
7. Briet, J., Vidick, T.: Explicit lower and upper bounds on the entangled value of multiplayer XOR games, arxiv: 1108.5647
8. Buhrman, H., Regev, O., Scarpa, G., de Wolf, R.: Near-optimal and explicit Bell inequality violations. In: Proceedings of Complexity 2011, pp. 157–166 (2011); also arxiv: 1012.5403
9. Cirel'son, B. (Tsirelson): Quantum generalizations of Bell's inequality. Letters in Mathematical Physics 4, 93–100 (1980)
10. Clauser, J., Horne, M., Shimony, A., Holt, R.: Physical Review Letters 23, 880–884 (1969)
11. Cleve, R., Höyer, P., Toner, B., Watrous, J.: Consequences and limits of non-local strategies. In: Proceedings of CCC 2004, pp. 236–249 (2004); also quant-ph/0404076
12. Davidson, K., Szarek, S.: Local operator theory, random matrices and Banach spaces. In: Johnson, W.B., Lindenstrauss, J. (eds.) Handbook on the Geometry of Banach Spaces, vol. 1, pp. 317–366. Elsevier (2001)
13. Graham, R.L., Knuth, D.E., Patashnik, O.: Concrete Mathematics, 2nd edn. Addison-Wesley, Reading (1994)
14. Grothendieck, A.: Resume de la theorie metrique des produits tensoriels topologiques. Boletim Sociedade De Matematico de Sao Paulo 8, 1–79 (1953)
15. Grover, L.K.: A fast quantum mechanical algorithm for database search. In: Proceedings of STOC 1996, pp. 212–219 (1996)

16. Krivine, J.-L.: Sur la constante de Grothendieck. Comptes Rendus de l'Académie des Sciences, Series A-B 284, A445–A446 (1977)
17. Junge, M., Palazuelos, C.: Large violation of Bell inequalities with low entanglement. Communications in Mathematical Physics 306(3), 695–746 (2011); arXiv:1007.3043
18. Linial, N., Mendelson, S., Schechtman, G., Shraibman, A.: Complexity measures of sign matrices. Combinatorica 27(4), 439–463 (2007)
19. Marčenko, V.A., Pastur, L.A.: Distribution of eigenvalues for some sets of random matrices. Math. USSR Sbornik 1, 457–483 (1967)
20. Mitzenmacher, M., Upfal, E.: Probability and Computing. Randomized Algorithms and Their Analysis. Cambridge University Press (2005)
21. Montero, A.M., Tonge, A.M.: The Schur multiplication in tensor algebras. Studia Math. 68(1), 1–24 (1980)
22. Parisi, G.: The order parameter for spin glasses: a function on the interval 0-1. Journal of Physics A: Mathemathical and General 13, 1101–1112 (1980)
23. Reeds, J.A.: A new lower bound on the real Grothendieck constant (1991) (unpublished manuscript), `http://www.dtc.umn.edu/reedsj/bound2.dvi`
24. Sherrington, D., Kirkpatrick, S.: Infinite ranged models of spin glasses. Physical Review B 17, 4384–4403 (1978)
25. Shor, P.W.: Algorithms for quantum computation: Discrete logarithms and factoring. In: FOCS 1994, pp. 124–134. IEEE (1994)
26. Silman, J., Chailloux, A., Aharon, N., Kerenidis, I., Pironio, S., Massar, S.: Fully distrustful quantum cryptography. Physical Review Letters 106, 220501 (2011)
27. Simon, D.R.: On the power of quantum computation. In: FOCS 1994, pp. 116–123. IEEE (1994)
28. Stanley, R.: Enumerative Combinatorics, vol. 2. Cambridge University Press (1999)
29. Talagrand, M.: The generalized Parisi formula. Comptes Rendus de l'Académie des Sciences, Series I 337, 111–114 (2003)
30. Tao, T.: Topics in Random Matrix Theory, Draft of a book, `http://terrytao.files.wordpress.com/2011/02/matrix-book.pdf`
31. Wehner, S.: Tsirelson bounds for generalized Clauser-Horne-Shimony-Holt inequalities. Physical Review A 73, 022110 (2006)