Worst case analysis of non-local games *

Andris Ambainis[1], Artūrs Bačkurs[2], Kaspars Balodis[1], Agnis Škuškovniks[1], Juris Smotrovs[1], and Madars Virza[2]

[1] Faculty of Computing, University of Latvia, Raina bulv. 19, Riga, LV-1586, Latvia, e-mail: andris.ambainis@lu.lv, kbalodis@gmail.com, agnis.skuskovniks@gmail.com, Juris.Smotrovs@lu.lv

[2] Computer Science and Artificial Intelligence Laboratory, Massachusetts Institute of Technology, 32 Vassar Street, Cambridge, MA 02139, USA e-mail: abackurs@gmail.com, madars@gmail.com

Abstract. Non-local games are studied in quantum information because they provide a simple way for proving the difference between the classical world and the quantum world. A non-local game is a cooperative game played by 2 or more players against a referee. The players cannot communicate but may share common random bits or a common quantum state. A referee sends an input x_i to the i^{th} player who then responds by sending an answer a_i to the referee. The players win if the answers a_i satisfy a condition that may depend on the inputs x_i.
Typically, non-local games are studied in a framework where the referee picks the inputs from a known probability distribution. We initiate the study of non-local games in a worst-case scenario when the referee's probability distribution is unknown and study several non-local games in this scenario.

1 Overview

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 [18, 16] and through quantum cryptography which offers degree of security that is impossible classically [7].

Another way of seeing the difference between quantum mechanics and the classical world is through non-local games. An example of non-local game is the CHSH (Clauser-Horne-Shimonyi-Holt) game [11]. This is a game played by two parties against a referee. The two parties cannot communicate but can share common randomness or common quantum state that is prepared before the beginning of the game. The referee prepares two uniformly random bits x, y and gives one of them to each of two parties. The parties reply by sending bits a and b to the referee. They win if $a \oplus b = x \wedge y$. The maximum winning probability that can be achieved is 0.75 classically and $\frac{1}{2} + \frac{1}{2\sqrt{2}} = 0.85...$ quantumly.

* Supported by ESF project 2009/0216/1DP/1.1.1.2.0/09/APIA/VIAA/044 and FP7 FET-Open project QCS.

Other non-local games can be obtained by changing the winning conditions, replacing bits x, y with $x, y \in \{1, \ldots, m\}$ or changing the number of parties. The common feature is that all non-local games involve parties that cannot communicate but can share common random bits or a common quantum state.

There are several reasons why non-local games are interesting. First, CHSH game provides a very simple example to test validity of quantum mechanics. If we have implemented the referee and the two players by devices so that 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, 17].

Non-local games are typically analyzed with the referee acting according to some probability distribution. E. g., for the CHSH game, the referee chooses each of possible pairs of bits $(0, 0)$, $(0, 1)$, $(1, 0)$, $(1, 1)$ as (x, y) with equal probabilities $1/4$. This is quite natural if we think of the CHSH game as an experiment for testing the validity of quantum mechanics. Then, we can implement the device for the referee so that it uses the appropriate probability distribution.

On the other hand, most of theoretical computer science is based on the worst-case analysis of algorithms, including areas such as quantum communication complexity [20] and distributed computing [13] (which are both related to non-local games). Because of that, we think that it is also interesting to study non-local games in a worst case setting, when the players have to achieve winning probability at least p for every possible combination of input data (x, y)[1].

In this paper, we start a study of non-local games in the worst-case framework. We start with several simple observations (section 3). First, the maximum gap between quantum and classical winning probability in the worst-case scenario is at most the maximum gap for a fixed probability distribution. Second, many of the non-local games that achieve the biggest gaps for a fixed probability distribution (such as CHSH game for 2-player XOR games or Mermin-Ardehali game [15, 5] for n-player XOR games) also achieve the same gap in the worst-case scenario, due to natural symmetries present in those games.

Then, in section 4, we look at examples of non-local games for which the worst case is different from the average case under the most natural probability distribution, with two goals. First, we show natural examples of non-local games for which the worst-case behaviour is not a straightforward consequence of the average-case behaviour under the uniform distribution.

Second, at the same time, we develop methods for analyzing non-local games in the worst case. For non-local games under a fixed probability distribution, computing the best winning probability is at least NP-hard [14] in the general case but there are efficient algorithms for fairly broad special cases (such as 2-player XOR games [12]). Those algorithms crucially rely on the fact that non-local games are studied under a fixed probability distribution on inputs (x, y). This allows to reduce the maximum winning probability to a simple expression

[1] Also, when we give talks about non-local games to computer scientists who are not familiar with quantum computing, we often get a question: why don't you consider the worst case setting?

whose maximum can be computed by a polynomial time algorithm. (For example, for 2-player XOR games, this is done via semidefinite programming [12].)

These methods no longer work in the worst case scenario, where we have to develop new methods on case-by-case basis - for games that would have been easy to analyze with previous methods if the probability distribution was fixed.

2 Technical preliminaries

We will study non-local games of the following kind [12] in both classical and quantum settings. There are n cooperating players A_1, A_2, ..., A_n trying to maximize the game value (see below), and there is a referee. Before the game the players may share a common source of correlated random data: in the classical case, a common random variable R taking values in a finite set $\mathcal{R}$, and in the quantum case, an entangled n-part quantum state $|\psi\rangle \in \mathcal{A}_1 \otimes \ldots \otimes \mathcal{A}_n$ (where $\mathcal{A}_i$ is a finite-dimensional subspace corresponding to the part of the state available to A_i). During the game the players cannot communicate between themselves.

Each of the players (A_i) has a finite set of possible input data: X_i. At the start of the game the referee randomly picks values $(x_1, \ldots, x_n) = \mathbf{x} \in X_1 \times \ldots \times X_n$ according to some probability distribution π, and sends each of the players his input (i. e. A_i receives x_i).

Each of the players then must send the referee a response a_i which may depend on the input and the common random data source. In this paper we will consider only *binary games*, that is games where the responses are simply bits: $a_i \in \{0, 1\}$. We denote $(a_1, \ldots, a_n)$ by $\mathbf{a}$.

The referee checks whether the players have won by some predicate (known to all parties) depending on the players' inputs and outputs: $V(\mathbf{a} \mid \mathbf{x})$. For convenience in formulas, we will suppose that V takes value 1 when it is *true* and -1 when it is *false*. A binary game whose outcome depends only on the XOR of the players' responses: $V(\mathbf{a} \mid \mathbf{x}) = V'(\bigoplus_{i=1}^{n} a_i \mid \mathbf{x})$, is called an *XOR game*. A game whose outcome does not change after any permutation γ of the players (i. e. $V(\gamma(\mathbf{a}) \mid \gamma(\mathbf{x})) = V(\mathbf{a} \mid \mathbf{x})$ for any γ) is called a *symmetric game*.

The value ω of a non-local game G for given players' strategies is the difference between the probability that the players win and the probability that they lose:

$$\omega(G) = \Pr[V(\mathbf{a} \mid \mathbf{x}) = 1] - \Pr[V(\mathbf{a} \mid \mathbf{x}) = -1] \in [-1, 1].$$

The probability that the players win can then be expressed by the game value in this way: $\Pr[V(\mathbf{a} \mid \mathbf{x}) = 1] = \frac{1}{2} + \frac{1}{2}\omega(G)$.

In the classical case, the players' strategy is the random variable R and a set of functions $a_i : X_i \times \mathcal{R} \to \{0, 1\}$ determining the responses. The maximal classical game value achievable by the players for a given distribution π is thus:

$$\omega_c^{\pi}(G) = \sup_{R, \mathbf{a}} \sum_{r, \mathbf{x}} \pi(\mathbf{x}) \Pr[R = r] V(a_1(x_1, r), \ldots, a_n(x_n, r) \mid \mathbf{x}).$$

However, the use of random variable here is redundant, since in the expression it provides a convex combination of deterministic strategy game values, thus the

maximum is achieved by some deterministic strategy (with $a_i : X_i \to \{0,1\}$):

$$\omega_c^\pi(G) = \max_{\mathbf{a}} \sum_{\mathbf{x}} \pi(\mathbf{x}) V(a_1(x_1), \ldots, a_n(x_n) \mid \mathbf{x}).$$

In this paper we investigate the case when the players do not know the probability distribution π used by the referee, and must maximize the game value for the worst distribution the referee could choose, given the strategy picked by the players. We will call it the worst-case game value. The maximal classical worst-case game value ω_c achievable by the players is given by the formula

$$\omega_c(G) = \sup_{R,\mathbf{a}} \min_{\pi} \sum_{r,\mathbf{x}} \pi(\mathbf{x}) \Pr[R = r] V(a_1(x_1, r), \ldots, a_n(x_n, r) \mid \mathbf{x}).$$

Note that in the worst-case approach the optimal strategy cannot be a deterministic one, unless there is a deterministic strategy winning on *all* inputs: if there is an input on which the strategy loses, then the referee can supply it with certainty, and the players always lose. Clearly, $\omega_c(G) \leq \omega_c^\pi(G)$ for any π.

In the most of the studied examples π has been the uniform distribution. We will call it the average case and denote its maximum game value by $\omega_c^{\text{uni}}(G)$.

In the quantum case, the players' strategy is the state $|\psi\rangle$ and the measurements that the players pick depending on the received inputs and perform on their parts of $|\psi\rangle$ to determine their responses. Mathematically, the measurement performed by A_i after receiving input x_i is a pair of positive semidefinite $\dim \mathcal{A}_i$-dimensional matrices $M_i^{0|x_i}$, $M_i^{1|x_i}$ with $M_i^{0|x_i} + M_i^{1|x_i} = I$ where I is the identity matrix. We denote the collection of all measurements by $\mathbf{M}$.

The maximum quantum game value for a fixed distribution π is

$$\omega_q^\pi(G) = \sup_{|\psi\rangle,\mathbf{M}} \sum_{\mathbf{x},\mathbf{a}} \pi(\mathbf{x}) \langle\psi| \bigotimes_{i=1}^{n} M_i^{a_i|x_i} |\psi\rangle V(\mathbf{a} \mid \mathbf{x}),$$

and the maximum quantum worst-case game value is

$$\omega_q(G) = \sup_{|\psi\rangle,\mathbf{M}} \min_{\pi} \sum_{\mathbf{x},\mathbf{a}} \pi(\mathbf{x}) \langle\psi| \bigotimes_{i=1}^{n} M_i^{a_i|x_i} |\psi\rangle V(\mathbf{a} \mid \mathbf{x}).$$

Since the shared entangled state can be used to simulate a random variable, $\omega_q(G) \geq \omega_c(G)$ and for any π: $\omega_q^\pi(G) \geq \omega_c^\pi(G)$.

In the case of two player games ($n = 2$) we will use notation A, B for the players, X, Y for the input sets, x, y for the inputs, a, b for the responses.

3 Games with worst case equivalent to average case

3.1 Maximum quantum-classical gap

The advantage of quantum strategies is usually measured by the ratio $\frac{\omega_q^\pi(G)}{\omega_c^\pi(G)}$ (or $\frac{\omega_q(G)}{\omega_c(G)}$ in the worst-case setting) between the quantum value $\omega_q^\pi(G)$ and the

classical value $\omega_c^\pi(G)$. Finding non-local games with maximum $\frac{\omega_q^\pi(G)}{\omega_c^\pi(G)}$ has been an object of much research (e.g. [9, 8]).

We show that the maximum advantage in the worst-case scenario is never bigger than for the best choice of a fixed probability distribution.

Theorem 1 *For any game G,*

$$\frac{\omega_q(G)}{\omega_c(G)} \leq \max_\pi \frac{\omega_q^\pi(G)}{\omega_c^\pi(G)}.$$

Proof. By Yao's principle [21], $\omega_c(G)$ is equal to the minimum of $\omega_c^\pi(G)$ over all probability distributions π. Let π be the probability distribution that achieves this minimum. Then, $\omega_q^\pi(G) \geq \omega_q(G)$ (since knowing π can only make it easier to win in a non-local game) and, hence, $\frac{\omega_q^\pi(G)}{\omega_c^\pi(G)} \geq \frac{\omega_q(G)}{\omega_c(G)}$. □

For many natural games, $\max_\pi \frac{\omega_q^\pi(G)}{\omega_c^\pi(G)}$ is achieved by $\pi = uni$ and, often, there is a straightforward symmetry argument that shows that $\omega_c^{uni} = \omega_c$ or $\omega_q^{uni} = \omega_q$. Then, the uniform distribution on inputs is equivalent to the worst case. We show two examples of that in the next two subsections.

3.2 CHSH game

The CHSH game [11, 12] is a canonical example of a 2-player non-local game with a quantum advantage. It is a two player XOR game with $X = Y = \{0, 1\}$, $V(a, b \mid x, y) = a \oplus b \equiv x \wedge y$, and π the uniform distribution. It is easy to check that no deterministic strategy can win on all inputs, but the strategy $a(x) = 0$, $b(y) = 0$ wins on 3 inputs out of 4, so [12]: $\omega_c^{\text{uni}}(CHSH) = 0.75 - 0.25 = 0.5$.

Moreover, since out of the four strategies S_1: $a(x) = 0$, $b(y) = 0$; S_2: $a(x) = x$, $b(y) = 0$; S_3: $a(x) = 0$, $b(y) = y$; S_4: $a(x) = x$, $b(y) = \neg y$ each one loses on a different input, and wins on the 3 other ones, we have for any predetermined π: $\omega_c^\pi(CHSH) = 1 - 2\min_{x,y} \pi(x, y) \geq 0.5$. Indeed, one can pick the strategy losing on the input with the minimal value of π.

Theorem 2 *$\omega_c(CHSH) = 0.5$; $\omega_q(CHSH) = 1/\sqrt{2}$.*

Proof. If the players use a random variable R to pick one of the strategies S_1, S_2, S_3, S_4 mentioned above with equal probability (i. e. 0.25), then for any input x, y they will have a winning strategy with probability 0.75. Thus $\omega_c(CHSH) \geq 0.5$. On the other hand, $\omega_c(CHSH) \leq \omega_c^{\text{uni}}(CHSH) = 0.5$.

[12] shows that the winning probability in the quantum case is $\frac{1}{2} + \frac{1}{2\sqrt{2}}$ giving $\omega_q^{\text{uni}}(CHSH) = 1/\sqrt{2}$. Moreover, the used strategy achieves this value *on every input* x, y, therefore it gives also the worst-case value: $\omega_q(CHSH) = 1/\sqrt{2}$. □

3.3 Mermin-Ardehali game

Mermin-Ardehali (MA) game is an n-player XOR game that achieves the biggest quantum advantage among XOR games with 2 questions to each player ($X_1 = \ldots = X_n = \{0,1\}$). This game corresponds to Mermin-Ardehali n-partite Bell inequality [15, 5].

The winning condition for MA game is: $a_1 \oplus \ldots \oplus a_n = 0$ if $(x_1 + \ldots + x_n) \bmod 4 \in \{0,1\}$ and $a_1 \oplus \ldots \oplus a_n = 1$ if $(x_1 + \ldots + x_n) \bmod 4 \in \{2,3\}$.

For the uniform distribution on the inputs, we have $\omega_q^{uni}(MA) = \frac{1}{\sqrt{2}}$ and $\omega_c^{uni}(MA) = \frac{1}{2^{\lceil \frac{n}{2}-1 \rceil}}$ classically [15, 5, 4]. As shown by Werner and Wolf [19], no XOR game has a bigger quantum advantage.

Theorem 3 *[19] No n-party XOR game G with binary inputs x_i (with any input distribution π) achieves $\frac{\omega_q^\pi(G)}{\omega_c^\pi(G)} > 2^{\frac{n-1}{2}}$.*

This makes the worst-case analysis of Mermin-Ardehali game for even n quite straightforward. For the quantum case, the maximal game value $\frac{1}{\sqrt{2}}$ is given by a quantum strategy which achieves the corresponding winning probability $\frac{1}{2} + \frac{1}{2\sqrt{2}}$ *on every input* [15, 5, 4], thus

Theorem 4 *For all n: $\omega_q(MA) = 1/\sqrt{2}$.*

For the classical case, Theorems 1 and 3 together imply $\frac{\omega_q(MA)}{\omega_c(MA)} \leq 2^{\frac{n-1}{2}}$ and $\omega_c(MA) \geq \frac{1}{2^{n/2}}$. Thus,

$$\frac{1}{2^{n/2}} \leq \omega_c(MA) \leq \omega_c^{uni}(MA) \leq \frac{1}{2^{\lceil \frac{n-1}{2} \rceil}}.$$

For even n, the upper and lower bounds coincide, implying

Theorem 5 *For even n: $\omega_c(MA) = 2^{-\frac{n}{2}}$.*

Other examples. Other examples of well known non-local games with $\omega_c^{uni} = \omega_c$ and $\omega_q^{uni} = \omega_q$ are the Odd Cycle game of [12] and the Magic Square game of [6, 12]. Again, the natural symmetries present in these games which make the worst case equivalent to the average case.

4 Games with worst case different from average case

The goals of this section are:

- to present natural examples of non-local games for which the worst-case scenario is different from the average case;
- to develop methods for analyzing quantum games in the worst-case scenario (which is substantially more difficult than in the average case).

4.1 EQUAL-EQUAL game

We define EQUAL-EQUAL (EE_m) as a two-player XOR game with $X = Y = \{1, \ldots, m\}$ and $V(a, b \mid x, y) \stackrel{def}{=} (x = y) \equiv (a = b)$.

This is a natural variation of the Odd-Cycle game of [12]. For $m = 3$, the Odd-Cycle game can be viewed as a game in which the players try to prove to the referee that they have 3 bits $a_1, a_2, a_3 \in \{0, 1\}$ which all have different values.

This can be generalized to larger m in two ways. The first generalization is the Odd-Cycle game [12] in which the players attempt to prove to the referee that an m-cycle (for m odd) is 2-colorable. The second generalization is a game in which the players attempt to prove that they have m bits $a_1, \ldots, a_m \in \{0, 1\}$ which all have different values. This is our EQUAL-EQUAL game.

Theorem 6 *For even m: $\omega_c(EE_m) = \frac{m}{3m-4}$, and for odd m: $\omega_c(EE_m) = \frac{m+1}{3m-1}$.*

Proof. In the full version of paper [3]. □

Theorem 7 *For even m: $\omega_q(EE_m) = \frac{m}{3m-4}$, and for odd m: $\frac{m+1}{3m-1} \leq \omega_q(EE_m) \leq \frac{m^2+1}{(3m-1)(m-1)}$.*

Proof. The lower bounds follow from $\omega_q(EE_m) \geq \omega_c(EE_m)$. For the upper bounds, let $\pi_{\alpha,\beta}$ denote the probability distribution defined by $\pi_{\alpha,\beta}(i, i) = \alpha$ for any i and $\pi_{\alpha,\beta}(i, j) = \beta$ for any distinct i, j. Then, $\omega_q(EE_m) \leq \omega_q^{\pi_{\alpha,\beta}}(EE_m)$.

For the two-player XOR games where on every input exactly one of the cases $a \oplus b = 0$ and $a \oplus b = 1$ is winning, it is useful to introduce the matrix V with $V_{xy} = V(0, 0 \mid x, y)$, and to observe that $V(a, b \mid x, y) = (-1)^a(-1)^b V_{xy}$. Thus, for any distribution π

$$\omega_q^{\pi}(EE_m) = \sup_{|\psi\rangle, \mathbf{M}} \sum_{x,y,a,b} \pi(x, y) \langle\psi| M_1^{a|x} \otimes M_2^{b|y} |\psi\rangle (-1)^a (-1)^b V_{xy},$$

and by the Tsirelson's theorem [10] this game value is equal to

$$\sup_d \max_{u_i : \|u_i\|=1} \max_{v_j : \|v_j\|=1} \sum_{i=1}^{m} \sum_{j=1}^{m} \pi(i, j) V_{ij} (u_i, v_j)$$

where $u_1, \ldots, u_m, v_1, \ldots, v_m \in \mathbb{R}^d$ and (u_i, v_j) is the scalar product.

The part of the sum containing u_i is

$$\sum_{j=1}^{m} \pi(i, j) V_{ij} (u_i, v_j) = \left(u_i, \sum_{j=1}^{m} \pi(i, j) V_{ij} v_j \right).$$

To maximize the scalar product, u_i must be the unit vector in the direction of $\sum_{j=1}^{m} \pi(i, j) V_{ij} v_j$.

For the EQUAL-EQUAL game and the distribution $\pi_{\alpha,\beta}$ we have $V_{ij} = 1$ and $\pi_{\alpha,\beta}(i,j) = \alpha$ if $i = j$, $V_{ij} = -1$ and $\pi_{\alpha,\beta}(i,j) = \beta$ if $i \neq j$. So we have to maximize the sum

$$S = \sum_{i=1}^{m} \left\| \sum_{j=1}^{m} \pi_{\alpha,\beta}(i,j) V_{ij} v_j \right\| = \sum_{i=1}^{m} \left\| \alpha v_i - \beta \sum_{j=1, j\neq i}^{m} v_j \right\|.$$

Let us denote $s = \sum_{j=1}^{m} v_j$ and apply the inequality between the arithmetic and quadratic means (and use the fact that $\|v_i\| = 1$):

$$\begin{aligned}
S^2 &\leq m \sum_{i=1}^{m} \|\alpha v_i - \beta(s - v_i)\|^2 = m \sum_{i=1}^{m} \|(\alpha+\beta)v_i - \beta s\|^2 \\
&= m \left(\sum_{i=1}^{m} (\alpha+\beta)^2 \|v_i\|^2 - \sum_{i=1}^{m} 2(\alpha+\beta)\beta(v_i, s) + \sum_{i=1}^{m} \beta^2 \|s\|^2 \right) \\
&= m \left((\alpha+\beta)^2 m - 2(\alpha+\beta)\beta \left(\sum_{i=1}^{m} v_i, s \right) + m\beta^2 \|s\|^2 \right) \\
&= m((\alpha+\beta)^2 m - 2(\alpha+\beta)\beta \|s\|^2 + m\beta^2 \|s\|^2) \\
&= m^2(\alpha+\beta)^2 + \|s\|^2 m\beta(m\beta - 2(\alpha+\beta)).
\end{aligned}$$

With values of α and β

$$\alpha = \begin{cases} \frac{m-1}{m(3m-1)} & \text{if } m \text{ is odd,} \\ \frac{m-2}{m(3m-4)} & \text{if } m \text{ is even,} \end{cases} \quad \beta = \begin{cases} \frac{2}{(m-1)(3m-1)} & \text{if } m \text{ is odd,} \\ \frac{2}{m(3m-4)} & \text{if } m \text{ is even.} \end{cases} \tag{1}$$

one can calculate that the coefficient at $\|s\|^2$ is 0 for even m and $-\frac{4}{(m-1)^2(3m-1)^2}$ (negative) for odd m, so dropping this summand and extracting the square root we get $S \leq m(\alpha+\beta)$. Substituting the values of α and β according to equation (1) we get the desired estimations. □

Thus, for any even m the quantum strategy cannot achieve any advantage over the classical strategies (and for odd m there is no difference asymptotically). It was quite surprising for us. In the Appendix of full paper [3], we show a similar result for any of the symmetric distributions $\pi_{\alpha,\beta}$.

Theorem 8 *If m is even, then $\omega_q^{\pi_{\alpha,\beta}}(EE_m) = \omega_c^{\pi_{\alpha,\beta}}(EE_m)$. If m is odd, then*

$$0 \leq \omega_q^{\pi_{\alpha,\beta}}(EE_m) - \omega_c^{\pi_{\alpha,\beta}}(EE_m) \leq \frac{2}{m(3m-4)}.$$

While games with quantum advantage are common, there are only a few examples of games with no quantum advantage for an entire class of probability distributions. "Guess your neighbour's input" of [2] is one such example, with quantum strategies having no advantage for any probability distribution on the input. Our EQUAL-EQUAL game provides another natural example where quantum strategies have no advantage for a class of distributions.

Also in the Appendix of full paper [3], we show that quantum and classical values are the same for the uniform distribution.

Corollary 1 *For $m \geq 4$: $\omega_q^{\text{uni}}(EE_m) = \omega_c^{\text{uni}}(EE_m) = \frac{m-2}{m}$.*

4.2 n-party AND game

n-party AND game ($nAND$) is a symmetric XOR game with binary inputs $X_1 = \ldots = X_n = \{0,1\}$ and $V(\mathbf{a} \mid \mathbf{x}) = (\bigoplus_{i=1}^n a_i = \bigwedge_{i=1}^n x_i)$.

Although this is a natural generalization of the CHSH game (compare the winning conditions), it appears that this game has not been studied before. Possibly, this is due to the fact that in the average case the game can be won classically with a probability that is very close to 1 by a trivial strategy: all players always outputting $a_i = 0$. If this game is studied in the worst-case scenario, it becomes more interesting. The following theorem implies that $\lim_{n\to\infty} \omega_c(nAND) = 1/3$.

Theorem 9 $\omega_c(nAND) = 2^{n-2}/(3 \cdot 2^{n-2} - 1)$.

Proof. In the full version of paper [3]. □

In the quantum case, since the game is symmetric with binary inputs, we can introduce parameters c_i being equal to the value of $V((0,\ldots,0) \mid \mathbf{x})$ on any input $\mathbf{x}$ containing i ones and $n-i$ zeroes, and p_i being equal to the probability (determined by π) of such kind of input. According to [4], for such game G:

$$\omega_q^{\pi}(G) = \max_{z:|z|=1} \left| \sum_{i=0}^{n} p_i c_i z^i \right|$$

where z is a complex number. By Yao's principle,

$$\omega_q(G) = \min_{p_0,\ldots,p_n:\sum p_i=1} \max_{z:|z|=1} \left| \sum_{i=0}^{n} p_i c_i z^i \right|. \tag{2}$$

We have for the $nAND$ game: $c_0 = \ldots = c_{n-1} = 1$ and $c_n = -1$.

Theorem 10 $\lim_{n\to\infty} \omega_q(nAND) = 1/3$.

Proof. Since $\omega_q(nAND) \geq \omega_c(nAND) > 1/3$, it is sufficient to prove that $\omega_q(nAND) \leq 1/3 + o(1)$ by picking particular values of p_i and showing that with them the limit of the expression (2) does not exceed $1/3$. Such values are: $p_n = 1/3$, $p_i = pq^{n-i}$ for $i = 0,\ldots,n-1$ where $q = e^{-\frac{1}{\sqrt{n}}}$ and p is chosen so that $p\sum_{i=1}^{n} q^i = \frac{2}{3}$, i.e. $p = \frac{2}{3}\frac{1-q}{q(1-q^n)}$. The inequality to prove is

$$\lim_{n\to\infty} \max_{z:|z|=1} \left| p \sum_{i=0}^{n-1} q^{n-i} z^i - \frac{1}{3} z^n \right| \leq \frac{1}{3}.$$

Since $|z| = 1$, we can divide the expression within modulus by z^n and use the substitution $w = 1/z$. We obtain

$$\lim_{n\to\infty} \max_{w:|w|=1} \left| p \sum_{i=1}^{n} (qw)^i - \frac{1}{3} \right| = \lim_{n\to\infty} \max_{w:|w|=1} \left| \frac{2}{3} \frac{1-q}{1-q^n} \frac{w(1-q^n w^n)}{1-qw} - \frac{1}{3} \right|. \tag{3}$$

From $\lim_{n\to\infty} q^n = \lim_{n\to\infty} e^{-\sqrt{n}} = 0$ we get $\lim_{n\to\infty}(1-q^n) = 1$ and, since $|w| = 1$, $\lim_{n\to\infty}(1-q^n w^n) = 1$. Thus (3) is equal to

$$\lim_{n\to\infty} \max_{w:|w|=1} \left| \frac{2}{3}\frac{(1-q)w}{1-qw} - \frac{1}{3} \right|. \tag{4}$$

Claim 1 *For each $\epsilon > 0$ there exists δ_0 such that the inequality*

$$\left| \left| \frac{2\delta w}{1-(1-\delta)w} - 1 \right| - 1 \right| < \epsilon \tag{5}$$

holds where $0 < \delta < \delta_0$ and $z \in C$, and $|w| = 1$.

Now Claim 1 gives that (4) is equal to $1/3$. We used the fact that $\lim_{n\to\infty} e^{-\frac{1}{\sqrt{n}}} = 1$ and the substitution $1 - q = \delta$. □

Proof (of Claim 1).

The inequality (5) requires that there exists some number with absolute value 1 that is sufficiently close to $\frac{2\delta w}{1-(1-\delta)w} - 1$ or, equivalently, that there exists some number on a circle in the complex plane with its center at $1/2$ and a radius of $1/2$ that is sufficiently close to $\frac{\delta w}{1-(1-\delta)w} = \frac{1}{1+((1/w)-1)/\delta}$.

The numbers $\left\{ \frac{1}{1+((1/w)-1)/\delta} | w \in C \text{ and } |w| = 1 \right\}$ form a circle in the complex plane with its center on the real axis that has common points with the real axis at 1 and $\frac{1}{1-2/\delta} = \frac{\delta}{\delta-2}$. The latter circle is sufficiently close to the circle with its center at $1/2$ and radius of $1/2$ if we choose $\delta_0 > 0$ sufficiently small so that the value of $\frac{\delta}{\delta-2}$ is sufficiently close to 0. □

4.3 n-party MAJORITY game

By replacing the AND function with the MAJORITY function in the definition of the n-party AND game, we obtain the n-party MAJORITY game.

More formally, n-party MAJORITY game ($nMAJ$) is a symmetric XOR game with $X_1 = \ldots = X_n = \{0,1\}$ and $V(\mathbf{a} \mid \mathbf{x})$ demanding that $\bigoplus_{i=1}^{n} a_i$ is $true$ if at least half of x_i is $true$, and $false$ otherwise. Similarly as in the previous section, we introduce parameters c_i and p_i and use the expression for game value given in [4]. This time $c_0 = \ldots = c_{\lceil n/2 \rceil - 1} = 1$, $c_{\lceil n/2 \rceil} = \ldots = c_n = -1$.

We have

Theorem 11 $\lim_{n\to\infty} \omega_c(nAND) = \lim_{n\to\infty} \omega_q(nAND) = 0$.

Proof. Since $0 \le \omega_c(nMAJ) \le \omega_q(nMAJ)$, it suffices to prove $\lim_{n\to\infty} \omega_q(nAND) = 0$. Similarly as above, we can do it by picking particular values of p_i for which the limit of (2) is 0. Such values are as follows. If n is even, let $n = 2k$ and $p_{2k} = 0$, otherwise let $n = 2k-1$. Let $p_i = r_i/s$ where $r_i = r_{2k-1-i}$ and $r_i = 1/(2k-1-2i)$ for $0 \le i \le k-1$, and $s = 2\sum_{i=1}^{k} 1/(2i-1)$. We have to prove that

$$\lim_{k\to\infty} \max_{z:|z|=1} \left| \sum_{i=0}^{k-1} p_i z^i - \sum_{i=k}^{2k-1} p_i z^i \right| = 0.$$

Since $|z| = 1$, we can multiply the polynomial within the modulus by $z^{1/2-k}$ and use the substitution $w = z^{-1/2}$ obtaining:

$$\max_{z:|z|=1} \left| \sum_{i=0}^{k-1} p_i z^i - \sum_{i=k}^{2k-1} p_i z^i \right| = \max_{w:|w|=1} \left| \sum_{i=0}^{k-1} p_i w^{2k-1-2i} - \sum_{i=k}^{2k-1} p_i w^{2k-1-2i} \right|$$

$$= \frac{2}{s} \max_{w:|w|=1} \left| \mathrm{Im} \left(\sum_{i=0}^{k-1} r_i w^{2k-1-2i} \right) \right| = \frac{2}{s} \max_{\theta} \left| \sum_{i=1}^{k} \frac{\sin(2i-1)\theta}{2i-1} \right|$$

where $\mathrm{Im}(z)$ is the imaginary part of z and $w = e^{i\theta}$.

Since the function $\sum_{i=1}^{k} (\sin(2i-1)\theta)/(2i-1)$ is a partial sum of the Fourier series of a square wave function, we have

$$\max_{\theta} \left| \sum_{i=1}^{k} \frac{\sin(2i-1)\theta}{2i-1} \right| = O(1).$$

Also, $2/s = o(1)$ because $\lim_{k\to\infty} s = \infty$. The result follows. □

5 Games without common data

What happens if the players are not allowed to share neither common randomness nor common quantum state?

If the probability distribution on the inputs is fixed, this scenario is equivalent to two players with common randomness because common random bits can be always fixed to the value that achieves the best result for the two players. For this reason, the question above has never been studied.

In the worst-case setting, the situation changes. Players with no common randomness are no longer equivalent to players with shared randomness. For many games, not allowing shared randomness results in the players being unable to win the game with any probability $p > 1/2$.

Let $\omega_n(G)$ denote the value of a game G if no shared randomness is allowed. We have

Theorem 12 *Suppose G is a two-player XOR game (with sets of inputs X, Y of arbitrary size) where on every input (x, y) exactly one of the two possible values of $a \oplus b$ wins. If $\omega_n(G) > 0$ then $\omega_n(G) = 1$, i. e. then G can be won deterministically.*

If we do not restrict to XOR games, it becomes possible to have a game which can be won with probability more than $\frac{1}{2}$ but not with probability 1.

Theorem 13 *There is a two-player game G (with binary sets of inputs and outputs $X = Y = A = B = \{0, 1\}$) with $0 < \omega_n(G) = \left(\sqrt{5} - 2\right) < 1$.*

We give the proofs of both theorems in the full version of this paper [3].

References

1. A. Acin, N. Brunner, N. Gisin, S. Massar, S. Pironio, V. Scarani. Device-independent security of quantum cryptography against collective attacks. *Physical Review Letters*, 98:230501, 2007.
2. M. L. Almeida, J.-D. Bancal, N. Brunner, A. Acin, N. Gisin, S. Pironio. Guess your neighbour's input: a multipartite non-local game with no quantum advantage. *Physical Review Letters*, 104:230404, 2010.
3. A. Ambainis, A. Backurs, K. Balodis, A. Skuskovniks, J. Smotrovs, M. Virza Worst case analysis of non-local games. *Available as arXiv.org e-Print arXiv:1112.2856*
4. A. Ambainis, D. Kravchenko, N. Nahimovs, A. Rivosh. Nonlocal Quantum XOR Games for Large Number of Players. *Proceedings of TAMC'2010*, pp. 72-83.
5. M. Ardehali. Bell inequalities with a magnitude of violation that grows exponentially with the number of particles. *Physical Review A*, 46:5375-5378, 1992.
6. P. K. Aravind. The magic squares and Bell's theorem. Manuscript, 2002. Available as arXiv.org e-Print quant-ph/0206070.
7. C. H. Bennett and G. Brassard, Quantum Cryptography: Public key distribution and coin tossing, *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing*, Bangalore, p. 175 (1984).
8. J. Briet, T. Vidick. Explicit lower and upper bounds on the entangled value of multiplayer XOR games. arXiv:1108.5647.
9. H. Buhrman, O. Regev, G. Scarpa, R. de Wolf. Near-Optimal and Explicit Bell Inequality Violations. *Proceedings of CCC'2011*, pp. 157-166.
10. B. Cirelson (Tsirelson). Quantum generalizations of Bell's inequality. *Letters in Mathematical Physics*, 4:93–100, 1980.
11. J. Clauser, M. Horne, A. Shimony, and R. Holt, Proposed experiment to test local hidden-variable theories. *Physical Review Letters*, 23:880, 1969.
12. R. Cleve, P. Høyer, B. Toner, J. Watrous. Consequences and limits of nonlocal strategies. *Proceedings of CCC'2004*, pages 236–249, 2004. Also quant-ph/0404076.
13. C. Gavoille, A. Kosowski, M. Markiewicz. What Can Be Observed Locally? *Proceedings of DISC'2009*, pp. 243-257.
14. J. Kempe, H. Kobayashi, K. Matsumoto, B. Toner and T. Vidick, Entangled Games are Hard to Approximate. *Proceedings of FOCS'2008*, pp. 447-456.
15. D. Mermin. Extreme Quantum Entanglement in a Superposition of Macroscopically Distinct States. *Physical Review Letters*, 65: 15 (1990).
16. P. W. Shor. Algorithms for quantum computation: Discrete logarithms and factoring. In *FOCS'1994*, pages 124–134. IEEE.
17. J. Silman, A. Chailloux, N. Aharon, I. Kerenidis, S. Pironio, S. Massar. Fully distrustful quantum cryptography. *Physical Review Letters*, 106:220501, 2011.
18. D. R. Simon, On the power of quantum computation, *Proceedings of FOCS'1994*, pages 116–123. IEEE.
19. R.F. Werner, M.M. Wolf, Bell inequalities and Entanglement, *Quantum Information and Computation*, 1(3):1-25 (2001).
20. R. de Wolf. Quantum Communication and Complexity. *Theoretical Computer Science*, 287(1): 337-353, 2002.
21. A. Yao Probabilistic computations: Toward a unified measure of complexity *Proceedings of the 18th IEEE Symposium on Foundations of Computer Science (FOCS)*, pp. 222-227, 1977.