What Can Be Computed without Communications?

Heger Arfaoui and Pierre Fraigniaud*

LIAFA, CNRS and University Paris Diderot, France

Abstract. This paper addresses the following 2-player problem. Alice (resp., Bob) receives a boolean x (resp., y) as input, and must return a boolean a (resp., b) as output. A *game* between Alice and Bob is defined by a pair (δ, f) of boolean functions. The objective of Alice and Bob playing game (δ, f) is, for every inputs x and y, to output values a and b, respectively, satisfying $\delta(a, b) = f(x, y)$, in *absence of any communication* between the two players.It is known that, for XOR-games, that is, games equivalent, up to individual reversible transformations, to a game (δ, f) with $\delta(a, b) = a \oplus b$, the ability for the players to use entangled quantum bits (qbits) helps: there exist a distributed protocol for the CHSH game, using quantum correlations, for which the probability that the two players produce a successful output is higher than the maximum probability of success of any classical distributed protocol for that game, even when using shared randomness.

In this paper, we show that, apart from XOR-games, quantum correlations does not help, in the sense that, for every such game, there exists a classical protocol (using shared randomness) whose probability of success is at least as large as the one of any protocol using quantum correlations. This result holds for both worst case and average case analysis. It is achieved by considering a model stronger than quantum correlations, the *non-signaling model*, for which we show that, if the game is not an XOR-game, then shared randomness is a sufficient resource for the design of optimal protocols. These results provide an invitation to revisit the theory of distributed *checking*, a.k.a. distributed *verification*. Indeed, the literature dealing with this theory is mostly focusing on decision functions δ equivalent to the AND-operator. This paper demonstrates that such a decision function may not well be suited for taking benefit of the computational power of quantum correlations.

1 Introduction

1.1 Context and Objective

This paper addresses the following 2-player problem. Alice (resp., Bob) receives a boolean x (resp., y) as input, and must return a boolean a (resp., b) as output.

* Both authors are supported by the ANR projects DISPLEXITY and PROSE, and by the Interdisciplinary project "Algorithmique distribuée quantique" of University Paris Diderot. Additional support from the INRIA project GANG.

G. Even and M.M. Halldórsson (Eds.): SIROCCO 2012, LNCS 7355, pp. 135–146, 2012.

A *game* between Alice and Bob is defined by a pair (δ, f) of boolean functions. The objective of Alice and Bob playing game (δ, f) is, for every inputs x and y, to output values a and b satisfying

$$\delta(a, b) = f(x, y)$$

in *absence of any communication* between the two players. Obviously, the game is trivial whenever there exist two boolean functions α and β such that $\delta(\alpha(x), \beta(y)) = f(x, y)$ for every pair $(x, y) \in \{0, 1\}^2$. Indeed, for such games, there exists a deterministic distributed protocol solving the game, with Alice returning $\alpha(x)$ on input x, and Bob returning $\beta(y)$ on input y. Non-trivial games may still be solved, but only under some probabilistic guarantees. A game (δ, f) is said to be solvable with probability p if there exists a randomized distributed protocol such that Alice outputs a, and Bob outputs b, with

$$\Pr(\delta(a, b) = f(x, y)) \geq p \tag{1}$$

for every input pair $(x, y) \in \{0, 1\}^2$.

Different sources of randomness can then be considered. Classical[1] sources of randomness include the case where each of the two players are provided with individual independent sources of random bits. It also include shared randomness where, in addition to individual independent sources of random bits, the two players have access to a common source of random bits. Shared randomness enables to produce outputs satisfying

$$\Pr(a, b|x, y) = \sum_{\lambda \in \Omega} \Pr(a|x, \lambda) \cdot \Pr(b|y, \lambda) \cdot \Pr(\lambda) \tag{2}$$

where the random variable λ is drawn from some probability space Ω, and $\Pr(a, b|x, y)$ denotes the probability that Alice outputs a and Bob outputs b, given the fact that Alice receives x as input, and Bob receives y as input. It is known [3] that correlations on quantum entangled states enable to derive protocols whose output distribution cannot be modeled as Eq. 2. One evidence of this fact is the CHSH game [6]:

$$a \oplus b = x \wedge y$$

where $\oplus$ denotes the exclusive-or operator. CHSH can be solved with probability $\cos^2(\pi/8) > \frac{3}{4}$ with a quantum protocol [5], while every protocol using classical shared randomness cannot solve CHSH with probability more than $\frac{3}{4}$. One objective of this paper is to complete an exhaustive study of 2-player games in order to identify for which games quantum correlations help.

In fact, the literature dealing with 2-player games (see, e.g., [1,2,8,15], and the recent survey [4]) refers to objects called *boxes*. A box B is characterized by the probabilities $\Pr(a, b|x, y)$ of outputting pair (a, b) given the input pair (x, y), for all $a, b, x, y \in \{0, 1\}$. A box B is thus described by a set

$$\{\Pr(a, b|x, y),\ (x, y) \in \{0, 1\}^2\}$$

[1] I.e., not using quantum effects.

of four probability distributions, one for each pair $(x, y) \in \{0, 1\}^2$. Hence, there are infinitely many boxes, with different computational powers.

The absence of communication between the two players along with the assumption of causality are captured by the class of *non-signaling* boxes. A box B is non-signaling if and only if it satisfies that the marginal output distributions for Alice and Bob depend only on their respective inputs. Formally, a non-signaling box satisfies:

$$\begin{aligned} &\forall a, x,\ \textstyle\sum_b \Pr(a, b|x, 0) = \sum_b \Pr(a, b|x, 1), \\ \text{and } &\forall b, y,\ \textstyle\sum_a \Pr(a, b|0, y) = \sum_a \Pr(a, b|1, y) \end{aligned} \tag{3}$$

Non-signaling boxes satisfying Eq. 2 are called *local*, where "locality" is referring here to the physical science concept of *local hidden variables* [3,9]. Boxes that do not satisfy Eq. 3 are *signaling*. Signaling boxes are not considered physically realistic because they would imply instantaneous transmission of signals between two distant entities.

The set of all boxes has a geometric interpretation [1], for it forms a 12-dimensional convex polytope, including the (convex) polytope of non-signaling boxes, which includes in turn the (convex) local polytope. Fig. 1 provides an abstract representation of the non-signaling polytope. Each of the extremal vertices of the non-signaling polytope is equivalent (up to individual reversible transformations on the inputs and outputs) to the PR box [5,15], that is described by the distribution:

$$\Pr(a, b|x, y) = \begin{cases} \frac{1}{2} \text{ if } a \oplus b = x \wedge y \\ 0 \text{ otherwise.} \end{cases}$$

Notice that the PR box satisfies $\Pr(a \oplus b = x \wedge y) = 1$ for every input pair x, y. So, in particular, it solves the CHSH game with probability 1. Each of the extremal vertices of the local polytope can be implemented by a deterministic protocol: they are equivalent to the identity box ID described by $\Pr(a, b|x, y) = 1$ if and only if $a = x$ and $y = b$. Every non-extremal box B is a linear combinations of extremal boxes: $B = \sum_{i=1}^{k} \beta_i B_i$ where B_i is an extremal box, $\sum_{i=1}^{k} \beta_i = 1$, and $\beta_i > 0$ for every $i = 1, \ldots, k$. On Fig. 1, the doted line represents the limit of the class of boxes implementable by a quantum protocol. This latter class strictly contains the local boxes, and is strictly included in the class of non-signaling boxes, as witnessed by the CHSH game.

Our objective can thus be reformulated as follows. Given a box implementable by a quantum protocol, which games can be efficiently solved using this box? Stated differently, given a game, what are the boxes implementable by a quantum protocol that enable to solve that game with better guarantees than any local boxes?

1.2 Our Results

We show that, for every 2-player game (δ, f) different from an XOR-game, i.e., different from a game which is equal, up to individual reversible transformations,

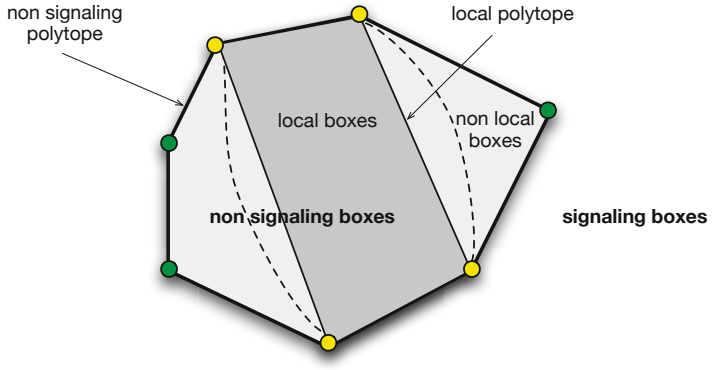

Fig. 1. Abstract representation of the non-signaling polytope

to a game (δ, f) with $\delta(a, b) = a \oplus b$, every box solving (δ, f) with probabilistic guarantee p greater that the probabilistic guarantee of any local box, is signaling. As a corollary, quantum correlations do not help for solving games different from XOR-games. Moreover, this result holds even the worst-case guarantee stated in Eq. 1 is replaced by the average-case guarantee

$$\frac{1}{4}\sum_{x,y} \Pr(\delta(a, b) = f(x, y)) \geq p \ .$$

The results in this paper open new perspectives in term of distributed *checking*, a.k.a. distributed *verification*, which consists in having a set of, say, n processes deciding whether their global state (defined as the union of the local state of every individual process) satisfies some prescribed property, or not. The literature on this latter topic (see, e.g., [7,10,11,13,14]) assumes a *decision* function δ which is applied to the set of individual decisions produced by the processes. Typically, each process should output a boolean b_i, and the global interpretation of the outputs is computed by

$$\delta(b_1, \ldots, b_n) = \bigwedge_{i=1}^{n} b_i \in \{\text{“yes”}, \text{“no”}\} \ .$$

The use of the AND operator is motivated by the requirement that the global state is valid if and only if all processes agree on some (local) validity condition. If this condition is locally violated somewhere in the system, then at least one process “rises an alarm” by outputting 0. However, recent advances in the theory of distributed checking [12] demonstrate that using other decision functions δ significantly increases the power of the “checker”, or “verifier”. Our results show that some functions δ, in particular the classical AND operator, do not enable to

use the power of quantum computing efficiently, compared to shared randomness, at least for 2-player games. In contrast, the exclusive-or operator is known to offer high potential, as far as distributed quantum computing is concerned. In particular, [2] proved that every boolean function f on n independent players can be implemented by a circuit of PR boxes that output booleans b_i, $i = 1, \ldots, n$, satisfying

$$\bigoplus_{i=1}^{n} b_i = f(x_1, \ldots, x_n) \ .$$

The results in this paper give one more evidence of the impact of the decision function δ on the ability of "deciding" boolean predicates f.

2 Equivalence Classes of Games

As introduced in the previous section, a game between Alice and Bob is described by a pair (δ, f) of boolean functions on two variables. Playing the game means for Alice (resp. Bob) to receive a boolean x (resp., y) as input, and to return a boolean a (resp., b) as output such that $\delta(a, b) = f(x, y)$ without communication between the two players. Examples of games are

$$\text{EQ}: \quad a \wedge b = \overline{x \oplus y} \quad \text{and} \quad \text{NEQ}: \quad a \wedge b = x \oplus y.$$

Another example of a game is :

$$\text{AMOS}: \quad a \wedge b = \overline{x \wedge y}.$$

In these three examples, one can view the games as Alice and Bob respectively deciding whether the equality $x = y$ holds, whether the non-equality $x \neq y$ holds, and whether there is "at most one selected" player (a selected player has input 1). Here, "deciding" means that if the answer is "yes" then both players should output "yes", while if the answer is "no" then at least one player should output "no". In fact, the three games EQ, NEQ, and AMOS, are AND-games. However, all games are not of that type. In particular, we shall see that the already mentioned CHSH game

$$a \oplus b = x \wedge y$$

is not an AND-game, for $\delta(a, b) \neq a \wedge b$. More precisely, for any game (δ, f), both functions δ and f can be rewritten as:

$$\delta(a, b) = \alpha_{1,1}ab + \alpha_{1,0}a + \alpha_{0,1}b + \alpha_{0,0} \ \text{ and } \ f(x, y) = \beta_{1,1}xy + \beta_{1,0}x + \beta_{0,1}y + \beta_{0,0}$$

where the $+$ symbol denotes the exclusive-or operator $\oplus$, the (omitted) $\cdot$ symbol denotes the and-operator $\wedge$, and all coefficients are in $\{0, 1\}$. We say that two games (δ, f) and (δ', f') are equivalent if

$$\delta(a, b) = \delta'(A, B) \ \text{ and } \ f(x, y) = f'(X, Y)$$

where A (resp., B, X, Y) is a degree-1 polynomial in a (resp., b, x, y) with coefficients in $\{0, 1\}$. Whenever two games are equivalent, any protocol solving one of the two games can be used for solving the other games, by performing individual reversible transformations on the inputs and outputs, and the probability of success for the two games will be identical. The same notion of equivalence can be defined for boxes. Now we can state formally that the CHSH game is not equivalent to any of the three AND-games: EQ, NEQ, or AMOS. This is because, as we will see further in the text, none of these latter games can be solved with probability 1 by a non-signaling box (as opposed to the CHSH game which can be solved with probability 1 by the PR box). Instead, EQ and NEQ are equivalent games. Indeed, for NEQ, $f(x, y) = x + y$, while, for EQ, $f(x, y) = x + (y + 1)$.

Definition 1. *A game (δ, f) is an* XOR*-game if and only if it is equivalent to a game (δ', f') where $\delta'(a, b) = a \oplus b$.*

3 On the Power of Quantum Correlations

In this paper, we establish our main result, stating that correlations on quantum entangled states do not help for solving 2-player games that are not equivalent to an XOR-games. In fact we establish a stronger result by showing that non-signaling boxes do not help for those games, compared to local boxes.

Theorem 1. *Let (δ, f) be a 2-player game that is not equivalent to any* XOR*-game. Let p be the largest success probability for (δ, f) over all local boxes. Then every box solving (δ, f) with probabilistic guarantee $> p$ is signaling.*

Proof. The proof is straightforward for games (δ, f) where δ does not depend on both a and b. Indeed, if δ is constant, say α, then the game is either impossible (whenever $\exists x, y : f(x, y) \neq \alpha$) or trivial (whenever $\forall x, y, f(x, y) = \alpha$). And if δ is a single-variable function, say $\delta(a, b) = a + \alpha$ for some α, then the game is again either impossible, or trivial, or equivalent to a single-player game where the player must compute a two-variable function $f(x, y)$ knowing only one of the variables. Games of that latter class are equivalent to either the game $a = y$ or the game $b = x$. Non-signaling boxes do not help for such games (the best probability of success is $\frac{1}{2}$). Therefore, we focus now on "true" 2-player games, i.e., games (δ, f) where δ depends on both a and b.

First, we show that every true 2-player game (δ, f) which is not equivalent to an XOR-game is either deterministic, or equivalent to NEQ or AMOS. To establish this claim, observe that if f is constant, or depends on only one of the the two inputs, then the game (δ, f) can be solved with probability 1, by a deterministic protocol. Indeed, assume, without loss of generality, that f depends only on x. (The case f constant is straightforward). Then Alice and Bob can agree beforehand on a fixed value b^* for b. It follows that, knowing b^*, f ,and δ, Alice can output a such that $\delta(a, b^*) = f(x)$.

We can now come to the interesting case, that is, when both δ and f depend on their two inputs. Any 2-variable boolean function g can be rewritten as :

$$g(u, v) = U + V \quad or \quad g(u, v) = UV \quad or \quad g(u, v) = UV + 1$$

where U (resp., V) is a polynomial in u (resp., v) of degree at most 1, with coefficients in $\{0,1\}$. Given that fact, we rewrite any game (δ, f) using two expressions from the above, one for δ, and the other for f. We thus get nine different types of games, which can be narrowed down to five types by noticing that games like $A + B = XY + 1$ are the same as games like $A' + B' = X'Y'$, up to the (reversible) transformation $B' = B + 1$. These five types of games are the following:

$$\begin{aligned}
\delta(a,b) = A + B = f(x,y) = X + Y \\
\delta(a,b) = A + B = f(x,y) = XY \\
\delta(a,b) = AB = f(x,y) = X + Y \\
\delta(a,b) = AB = f(x,y) = XY \\
\delta(a,b) = AB = f(x,y) = XY + 1
\end{aligned}$$

Since f (resp., δ) depends on both x and y (resp., both a and b), all polynomials in these five types of games are of degree exactly 1, hence making all transformations reversible. Therefore, if two games can be rewritten into the same type, then they are equivalent. Table 1 describes the equivalence classes over the set of games formed by the five types above, and provides a representative for each class.

Table 1. Equivalence classes for true 2-player games depending on both inputs. The first two classes of games are deterministic, i.e., can be solved by a deterministic protocol. Instead, the last three classes are not deterministic. No deterministic protocol can solve any of the games in these three classes.

	Form of the class	Representative of the class
Deterministic	$AB = XY$	PROD $a \wedge b = x \wedge y$
	$A + B = X + Y$	SUM $a \oplus b = x \oplus y$
Not deterministic	$A + B = XY$	CHSH $a \oplus b = x \wedge y$
	$AB = X + Y$	NEQ $a \wedge b = x \oplus y$
	$AB = XY + 1$	AMOS $a \wedge b = \neg(x \wedge y)$

The theorem holds for games PROD and SUM since both of them can be solved by a deterministic protocol. Every game that is neither equivalent to an XOR-game nor deterministic is equivalent to an AND-game: NEQ or AMOS. We now show that non-local boxes fail to solve AMOS or NEQ with higher probabilistic guarantee than what can be achieved with local boxes.

Let us first examine AMOS. We start by showing that any box that solves AMOS with probabilistic guarantee $p > \frac{2}{3}$ is signaling. Suppose that there exists a non-signaling box B, defined by the correlation $\Pr(a, b|x, y)$, that solves AMOS with probability p. On the one hand, for any probability distribution $\pi = \{\pi_{xy} | (x, y) \in \{0, 1\}^2\}$ of the inputs, we have

$$\sum_{xy} \pi_{xy} \Pr(\text{success for input } (x, y)) \geq p$$

On the other hand, we have

$$\sum_{xy} \pi_{xy} \Pr(\text{success for input } (x, y)) = \sum_{xy} \pi_{xy} \sum_{ab} \mathbb{1}_{\{a \wedge b = \neg(x \wedge y)\}} \Pr(a, b|x, y)$$

where $\mathbb{1}_{\{a \wedge b = \neg(x \wedge y)\}}$ denotes the boolean indicator function of whether $a \wedge b = \neg(x \wedge y)$ is true or not. Let us consider the following distribution π^*:

$$\pi^*_{00} = 0 \quad \text{and} \quad \pi^*_{xy} = \frac{1}{3} \text{ for all } (x, y) \neq (0, 0)$$

Let $p_{abxy} = \Pr(a, b|x, y)$ for box B. The probability of success with the input distribution π^* satisfies

$$\begin{aligned}
\sum_{xy} \pi^*_{xy} \Pr(\text{success for } (x, y)) &= \frac{1}{3} \sum_{xy \neq (0,0)} \mathbb{1}_{\{a \wedge b = \neg(x \wedge y)\}} p_{abxy} \\
&= \frac{1}{3} \left(p_{1101} + p_{1110} + \sum_{(ab) \neq (11)} p_{ab11} \right) \\
&= \frac{1}{3} \left(p_{1101} + p_{1110} + p_{0011} + p_{0111} + p_{1011} \right) \quad (4)
\end{aligned}$$

The non-signaling conditions (cf., Eq. 3) require that, for every a, b, x, y,

$$\begin{aligned}
p_{a0x0} + p_{a1x0} &= p_{a0x1} + p_{a1x1} \\
\text{and } p_{0b0y} + p_{1b0y} &= p_{0b1y} + p_{1b1y}
\end{aligned}$$

which gives a bound on the first two terms of Equation 4:

$$\begin{aligned}
p_{1101} &= p_{1111} + p_{0111} - p_{0101} \leq p_{1111} + p_{0111} \\
\text{and } p_{1110} &= p_{1111} + p_{1011} - p_{1010} \leq p_{1111} + p_{1011}
\end{aligned}$$

The probability p of success is therefore bounded by :

$$\begin{aligned}
p &\leq \frac{1}{3} \left(p_{1111} + p_{0111} + p_{1011} + p_{1111} + p_{0011} + p_{0111} + p_{1011} \right) \\
&\leq \frac{1}{3} \Big((2 \sum_{ab} p_{ab11}) - p_{1111} \Big) \\
&\leq \frac{2}{3}
\end{aligned}$$

as $\sum_{ab} p_{abxy} = 1$ for any fixed (x, y), and $p_{1111} \geq 0$. Therefore, every non-signaling box solves AMOS with success at most $\frac{2}{3}$.

Regarding NEQ, we observe that with distribution π^*, AMOS and NEQ become the same games:

$$f_{\text{AMOS}}(x, y) = f_{\text{NEQ}}(x, y)$$

for all $(x, y \neq (0, 0)$. As a consequence, the same bound $\frac{2}{3}$ holds for NEQ: every non-signaling box solves NEQ with success at most $\frac{2}{3}$.

We now show that the bound $\frac{2}{3}$ for AMOS and NEQ can be reached by local boxes. For this purpose, we describe a protocol using solely shared randomness, and reaches success probability $\frac{2}{3}$. Let a_0 and a_1 (resp., b_0 and b_1) be the outputs of Alice (resp. Bob) on the respective input $x = 0$ and $x = 1$ (resp., $y = 0$ and $y = 1$). AMOS translates into solving the system:

$$\begin{cases} a_0 \cdot b_0 = 1 \\ a_0 \cdot b_1 = 1 \\ a_1 \cdot b_0 = 1 \\ a_1 \cdot b_1 = 0 \end{cases} \tag{5}$$

and NEQ translates into :

$$\begin{cases} a_0 \cdot b_0 = 0 \\ a_0 \cdot b_1 = 1 \\ a_1 \cdot b_0 = 1 \\ a_1 \cdot b_1 = 0 \end{cases} \tag{6}$$

The second and third equations of the system for AMOS as well as for NEQ imply that $a_0 = a_1 = b_0 = b_1 = 1$, resulting in the last equation impossible to be satisfied in both games. Hence the last three equations of each system cannot be simultaneously satisfied. Instead, if one chooses to ignore one of them, then one can find a solution to the game. Playing any one of the two games using shared randomness, we allow Alice and Bob to have access, before knowing their inputs, to a shared random variable λ uniformly distributed in $\{1, 2, 3\}$, designating the equation to be ignored among the last three ones. Alice and Bob will fail to solve the game with probability at most $\frac{1}{3}$ (when the ignored equation is precisely the one corresponding to the actual inputs), making the success probability for any input (x, y) equal to $\frac{2}{3}$. This completes the proof of the theorem. □

It turns out that even relaxing the constraints placed on solving the game, by considering average case analysis, does not allow non-signaling boxes to perform better than local boxes on games not equivalent to XOR-games.

Theorem 2. *Let (δ, f) be a 2-player game that is not equivalent to any* XOR*-game. Let p be the largest* average *success probability for (δ, f) over all local boxes. Then every box solving (δ, f) with average probabilistic guarantee $> p$ is signaling.*

Proof. Using the same arguments as in the proof of Theorem 1, we limit the analysis to AMOS and NEQ. For average case analysis, we consider these two

games with input probability distribution $\pi_{xy} = \frac{1}{4}$ for every $(x, y) \in \{0, 1\}^2$. The success probability for Alice and Bob with this input distribution is then given by:

$$\Pr(\text{success}) = \frac{1}{4} \sum_{x,y} \sum_{a,b} \mathbb{1}_{\{\delta(a,b)=f(x,y)\}} \Pr(a, b|x, y)$$

First, we show that the protocol described in the proof of Theorem 1 for solving AMOS and NEQ has average success probability $\frac{3}{4}$. Indeed, the success probability of that protocol can be written as:

$$\Pr(\text{success}) = \frac{1}{4} \sum_{x,y} \Pr(\text{success}(x, y)) = \frac{1}{4}\Big(1 + \frac{2}{3} + \frac{2}{3} + \frac{2}{3}\Big) = \frac{3}{4}$$

because, the protocol always satisfies the first equation of both games, and satisfies each of the three other equations (of both games) with probability $\frac{2}{3}$.

Next, we show that a non-local box cannot solve AMOS or NEQ with average success probability greater than $\frac{3}{4}$. Indeed, we have

$$\Pr(\text{success}) = \frac{1}{4}\Big[\Big(\sum_{(x,y)\neq(0,0)} \sum_{a,b} \mathbb{1}_{\{\delta(a,b)=f(x,y)\}} \Pr(a, b|x, y)\Big) + \Big(\sum_{a,b} \mathbb{1}_{\{\delta(a,b)=f(0,0)\}} \Pr(a, b|0, 0)\Big)\Big]$$

The first term is the same as the one analyzed in the proof of Theorem 1, where it was proved to be at most 2. The second term is at most $\sum_{ab} \Pr(a, b|0, 0) \leq 1$. Therefore, the average success probability for non-local boxes is at most $\frac{3}{4}$. □

The practical interest of the previous two theorems comes from their consequence to distributed quantum computing:

Corollary 1. *Quantum correlations does not help for solving 2-player games that are not equivalent to any* XOR*-game. This limitation holds for both worst case, and average case analysis.*

4 Open Problem

One obvious generalization of the 2-player games is to consider games with more than two players, with IDs from 1 to $n \geq 2$. In the n-player game (δ, f), Player i receives boolean x_i as input, and must return a boolean a_i such that

$$\delta(a_1, \ldots, a_n) = f(x_1, \ldots, x_n)$$

in absence of communication between the players. As for two players, two classes of games deserve specific interest:

- XOR-games: $\delta(a_1, \ldots, a_n) = a_1 \oplus \ldots \oplus a_n$, for they generalize the CHSH game, and for they can be solved by a non-signaling box implementable by a circuit of PR boxes (see [2]);

– AND-games: $\delta(a_1, \ldots, a_n) = a_1 \wedge \ldots \wedge a_n$ for they correspond to the standard decision mechanism in the distributed computing literature (see, e.g., [14]).

In particular, the n-player variant of AMOS is:

$$\bigwedge_{i=1}^{n} a_i = \bigwedge_{i \neq j} (\overline{x_i \wedge x_j}).$$

There exists a randomized protocol (see [10]), that is using individual random coins, and solves AMOS with success guarantee $\frac{\sqrt{5}-1}{2} \geq 0.61 > 1/2$. In this protocol, every selected player (i.e., one with input 1) outputs 1 with probability p, to be fixed later, and 0 with probability $1-p$. Every non-selected player (i.e., one with input 0) systematically outputs 0. Hence, if no players are selected, then the protocol always outputs the right answer. If one player is selected, then the protocol fails with probability $1-p$, while if two or more players are selected then the protocol fails with probability at most p^2. Solving $p^2 = 1-p$ results in picking the optimal probability $p^* = \frac{\sqrt{5}-1}{2}$.

On the other hand, we have seen in this paper that AMOS can be solved with success guarantee $\frac{2}{3} > p^*$ by two players applying a probabilistic protocol using shared randomness. One can actually show that the same guarantee can be achieved with three players, by analyzing the following system

$$\begin{cases} a_0 \cdot b_0 \cdot c_0 = 1 \\ a_1 \cdot b_0 \cdot c_0 = 1 \\ a_0 \cdot b_1 \cdot c_0 = 1 \\ a_0 \cdot b_0 \cdot b_1 = 1 \\ a_1 \cdot b_1 \cdot c_0 = 0 \\ a_1 \cdot b_0 \cdot c_1 = 0 \\ a_0 \cdot b_1 \cdot c_1 = 0 \\ a_1 \cdot b_1 \cdot b_1 = 0 \end{cases}$$

which lists the eight equations for AMOS corresponding to the eight possible inputs of the games. Consider the protocol which solves that system after ignoring the second and seventh equations with probability $\frac{1}{3}$, the third and sixth with probability $\frac{1}{3}$, and the fourth and fifth with probability $\frac{1}{3}$. This protocol has success probability at least $\frac{2}{3}$ for every triple of inputs.

Unfortunately, the protocols for two and three players do not seem to extend easily to a higher number of players. For four players, we have designed an ad hoc probabilistic protocol using shared randomness, with success probability $\frac{9}{14} > \frac{\sqrt{5}-1}{2}$, but we failed to design a local protocol with success probability $\frac{2}{3}$. For more than four players, the ad hoc protocol could be generalized, but we have not identified a general pattern for it.

Instead, the lower bound $\frac{2}{3}$ on the probability of success for solving AMOS with non-signaling boxes established in this paper trivially extends to n players. We thus conclude by stating the following problem.

Open problem: Prove or disprove the existence of a shared-randomness probabilistic protocol that solves the n-player AMOS game with success probability $\frac{2}{3}$, for all $n \geq 2$.

References

1. Barrett, J., Linden, N., Massar, S., Pironio, S., Popescu, S., Roberts, D.: Nonlocal correlations as an information-theoretic resource. Physical Review A 71(2), 1–11 (2005)
2. Barrett, J., Pironio, S.: Popescu-Rohrlich correlations as a unit of nonlocality. Phys. Rev. Lett. 95(14) (2005)
3. Bell, J.S.: On the Einstein-Podolsky-Rosen paradox. Physics 1(3), 195–200 (1964)
4. Buhrman, H., Cleve, R., Massar, S., de Wolf, R.: Non-locality and communication complexity. Reviews of Modern Physics 82, 665–698 (2010)
5. Cirel'son, B.S.: Quantum generalizations of bell's inequality. Letters in Math. Phys. 4(2), 93–100 (1980)
6. Clauser, J.F., Horne, M.A., Shimony, A., Holt, R.A.: Proposed experiment to test local hidden-variable theories. Physical Review Letters 23(15), 880–884 (1969)
7. Das Sarma, A., Holzer, S., Kor, L., Korman, A., Nanongkai, D., Pandurangan, G., Peleg, D., Wattenhofer, R.: Distributed verification and hardness of distributed approximation. In: 43rd ACM Symp. on Theory of Computing, STOC (2011)
8. Dupuis, F., Gisin, N., Hasidim, A., Allan Méthot, A., Pilpel, H.: No nonlocal box is universal. J. Math. Phys. 48(082107) (2007)
9. Einstein, A., Podolsky, B., Rosen, N.: Can quantum-mechanical description of physical reality be considered complete? Physical Review 47(10), 777–780 (1935)
10. Fraigniaud, P., Korman, A., Peleg, D.: Local distributed decision. In: 52nd Annual IEEE Symposium on Foundations of Computer Science (FOCS), pp. 708–717 (2011)
11. Fraigniaud, P., Rajsbaum, S., Travers, C.: Locality and Checkability in Wait-Free Computing. In: Peleg, D. (ed.) DISC 2011. LNCS, vol. 6950, pp. 333–347. Springer, Heidelberg (2011)
12. Fraigniaud, P., Rajsbaum, S., Travers, C.: Universal distributed checkers and orientation-detection tasks (submitted, 2012)
13. Korman, A., Kutten, S., Peleg, D.: Proof labeling schemes. Distributed Computing 22, 215–233 (2010)
14. Naor, M., Stockmeyer, L.: What can be computed locally? SIAM J. Comput. 24(6), 1259–1277 (1995)
15. Popescu, S., Rohrlich, D.: Quantum nonlocality as an axiom. Foundations of Physics 24(3), 379–385 (1994)