University of Latvia

Quantum Games, Quantum States, Their Properties and Applications

by

Dmitry Kravchenko

Doctoral Thesis

Area: Computer Science
Sub-Area: Mathematical Foundations of Computer Science

Scientific Advisor:
Professor Andris Ambainis

2013, Riga

EIROPAS SOCIĀLAIS FONDS

EIROPAS SAVIENĪBA

IEGULDĪJUMS TAVĀ NĀKOTNĒ

LATVIJAS UNIVERSITATE
ANNO 1919

This work has been supported by the European Social Fund within the projects

- 2009/0138/1DP/1.1.2.1.2/09/IPIA/VIAA/004 «Support for Doctoral Studies at University of Latvia» and
- 2009/0216/1DP/1.1.1.2.0/09/APIA/VIAA/044 «Applications of Computer Science and its links to Quantum Physics»

Abstract

Quantum mechanics and game theory were developed at almost the same time, during the first half of 20th century.

Classical game theory is one of the most developed in mathematics and computer science. It has many applications in economics, biology, and different kinds of social science. In computer science, many cryptographic protocols are also based on the elements of game theory.

Quantum computing is a relatively new branch of computer science. It unites different aspects of complexity theory and quantum physics.

Our intention is to take it one step further and combine classical game theory with the acquired knowledge of quantum computing; in particular, to study the effects of using quantum information in the well-known problems of game theory.

In this thesis, we obtain several bounds on the values of some special classes of nonlocal quantum games, and we present a new scheme for games quantization.

Contents

List of Figures

Objectives and Results

The main goal of most research in the field of quantum information and quantum computing is to understand the new properties and characteristics of information that are inherent in a system, the behavior of which can be described by the laws of quantum mechanics. More importantly, because classical information and classical elements of computation are just special cases of quantum information and quantum computing, the goal is to find the benefits of the quantum model of computing when comparing it with the classical one. In this sense, our topic of research — quantum game theory — is not an exception.

Game theory itself attracts the interest of researchers from different fields of science primarily as a tool for modeling and studying the laws of interaction between two or more parties in different real processes, such as the adaptation of a species in its ecological niche, or traders' behavior in the market or on a stock exchange. As we know, the behavior of participants in such processes (in terms of game theory — the behavior of players in the game), generally speaking, is not the most effective — i.e., beneficial — for either the individual player, who makes the decision, or for the system as a whole. This inefficiency usually occurs because of insufficiently coordinated activity of two or more players. However, in some cases, the manipulation of quantum information leads to better coordination of players' behavior and thus, achieves better results.

The goal of this thesis is to identify those cases in which insufficient levels of coordination between players, who operate with classical information in their actions, can be improved by the use of quantum information. Particular attention is paid not to the specific examples of games that are interesting from this point of view, but to entire classes of games, where operations with photons or more complex quantum systems could provide a significant increase in the efficiency of the players' behavior.

Part I

Overview of Games and Their Quantum Models

Chapter 1

Elements of Game Theory

1.1 Introduction

Game theory as a scientific discipline started to develop in the 1920s. Traditionally, applications of this theory were characterized as one of two modes: on the one hand, games were considered as purely mathematical problems, and on the other, they were applied to study various economic and social problems.

The founder of game theory — eminent mathematician John von Neumann — considered the description of economic relations as the main task of his theory. However, the very nature of the tasks that he examined and the methods he used ask for arguments, which are purely mathematical.

A game, as we understand it, appeared at the same time as Homo sapiens species. It can be said that the most distinctive feature of the human mind is its capability for abstract thinking, but the game, from the moment it emerged and until nowadays, is a method of cognitive perception of the world through its modeling and abstraction from reality. Thus, any kind of a game is, in a way, a reflection of real life processes.

1.2 General principles of studying games

1.2.1 Introduction

In practice, there are often cases and situations with of two (or more) participating parties, each of which has different interests and the ability to apply different strategies to achieve their goals. Such cases and situations are usually named *conflict* cases and situations, or simply *conflicts*.

As a rule, any conflict situation taken from real life is quite complex. In studying such situations, additional difficulties are created by numerous very different obstacles, which do not necessarily provide any substantial influence either on the conflict development or on its resolution. Therefore, in order to make the analysis of conflict situations possible, it is necessary to abstract oneself from these secondary factors. Under certain circumstances, this will allow the to constructin of a simplified formalized conflict model, which is usually named the *game*, and which differs from the real conflict situation by the fact that it is conducted under certain rules.

Game theory uses scientific, i.e., mathematical means to analyze conflicts. In this chapter, we will present the characteristics of the basic features of games as models of these conflicts, describing them in mathematical terms and thus, offer formal definitions to the basic elements of games, which will be used in further chapters.

1.2.2 Uncertainty of the outcome of the game and its sources

Generally, conflicts (and consequently, games that have the character of competitions, which are models of conflicts or their imitations) can be characterized by the uncertainty of their outcome. This circumstance prompts the participants to enter consciously into the conflict and is attracts witnesses and spectators to it. Therefore, any decision taken by a player during the process of the game turns out to be a decision made in the circumstance of uncertainty.

From a purely qualitative point of view, the reasons for the uncertainty of the outcome of the game may be divided into three groups.

First, the rules of the game might allow such a variety of different plays that an initial prediction of the outcome of the game is practically impossible. The sources of uncertainty of this type might be defined as *combinatorial*, and those games where the uncertainty of the result is primarily caused by combinatorial reasons — defined as *combinatorial games*. An explicit example of a combinatorial game is chess.

Second, the source of uncertainty of the result of the game might be the influence of random factors. Random factors might appear in a game influenced by some kind of "spontaneous force" (dispersion in shooting, weather conditions, noise in communication channels, etc.), or as a result of conscious acts of persons participating in the game process, who conduct specially organized "randomized" activities (tossing coins or dice, using tables of random numbers, performing a measurement of a qubit, etc.). Games where the result is uncertain solely due to casual factors are called *games of chance*. Typical examples of games of chance are games of dice or roulette. In such games, there is no question of right or optimal behavior of a player, because the result of the game does not depend on his activities. The only decisions that he may take concern the reasonability of his participation or non-participation in this game or another, depending on its rules.

Of course, we can find games that combine features both of combinatorial games and of games of chance. One such game is backgammon, where the reason for uncertainty is the casual behavior of the dice, and the combinatorial complexity arises from the configurations made of the draughts that are on the board.

The third source of uncertainty of the result of a game has strategic origin; a player might be unaware of how his adversary acts. Unlike the two previous sources of uncertainty, this source is part of the game in its essence. It gives uncertainty that comes from the other participant of the game. Games, the run of which are uncertain owing to the strategic reason stated above, are named *strategic games*.

Curiously enough, strategic games in their pure form are not widespread. The most common example of a strategic game is one of the types of "pitch-and-toss" game, when two players, independently from each other, put a coin on the table. If the coins are placed with the same side up, the first player wins; otherwise the second player wins. This game, for all its primitiveness, is in some aspects "more difficult" than, for example, chess. In chess, the action takes place on the open board, and we can imagine, at least in the mind, an “ideal player” who sees all the possibilities hidden in each position. Every choice, considered by one of the players, is equally considered by his adversary. Intuitively, it is clear that such an ideal player could be described by a finite deterministic automaton, or at least a Turing machine. Unlike chess, in the described “pitch-and-toss” game, the player in principle cannot know what his adversary has done, and this circumstance makes this game strategic.

In this case, the question of the right and optimal behavior of the player is much more difficult than in the previous cases. It is clear that placing a coin with its front or reverse side uppermost cannot be considered as either good or bad behavior. In reality, in strategic games random behavior is considered the right behavior. With regard to the “pitch-and-toss” game, this means that placing a coin with this or that side uppermost is less reasonable than tossing it up and allowing the coin to fall on either side. In other words, deterministic behavior makes no sense in such games.

Strategic features of the game might be combined with combinatorial features (e.g., “sea battle” — a kind of chess, where each player plays on his board and views only his figures, and an intermediary takes them off when they are captured, announces checks, fixes mate or draws), with the features of games of chance (e.g., poker), and also with the features of combinatorial games and games of chance simultaneously (e.g., bridge).

1.2.3 Combinatorial games

As already mentioned, all uncertainties of a combinatorial type may be resolved by a deterministic automaton. This fact can be illustrated easily for so-called *positional games*. These games are where the status of play process may be fully described as a kind of position, and before taking a decision, each player is completely aware of the current position. (A classic example of such a game is chess; in reality, any game with open information could be attributed to this class of games.)

The main idea of this is to describe the set of all positions, for which sound play by the first player will bring him victory, irrespective of his adversary’s choices. Accordingly, the complement of this set will be the set of losing positions. Thus, from each winning position there exists a choice for a player that leads to a losing position for the opponent.

Conversely, each move from a losing position leads to a winning position for the opponent. The easiest way to distinguish between these two sets is just the above-mentioned recurrent definition with the set of *base cases* consisting of the final positions where no moves are available.

This solution is not difficult to implement for such games as, for example, the "tic-tac-toe" game; however, as the combinatorial complexity of the game increases, the explicit indication of such a set becomes increasingly problematic. For a game such as chess, it seems practically impossible.

1.2.4 Games of chance

A randomizing factor is determining in all games of chance. A classic example of such a game is dice. For a long time, different variants of this game have been a major source of work for probability theory. In addition, dice were used in fortune telling; this fact, generally speaking, emphasizes human inclination to follow the indications of randomizing devices in taking decisions.

If the goal of a player in a combinatorial game is to win, and optimal strategies for a player are those that provide that win, then in the case of a game of chance there are no such playing skills (of course, not going beyond the rules of play) that could guarantee him the desired outcome. That is why, receiving a fixed sum of money by a player cannot be considered as the goal, to achieve which he uses this or that strategy. Here, the goal turns to be more complex.

It seems most natural for a player to try to maximize the win that he *expects* to obtain. The question of the propriety of such an approach lies more in the sphere of philosophy, but there are some rational arguments in its favor.

Von Neumann and Morgenstern [NM53] describe the attitude to probabilistic events in such a way. Suppose an individuum has a comprehensive system of preferences, in other words, for any pair of possible events he has a distinct feeling of preference. That means, we suppose, that for any two alternative events that are presented to him as possibilities, he can identify the one he prefers. It would be a natural generalization of this picture to concede that this individuum could compare not only events, but also combinations of events with specified probabilities.

Suppose two events B and C are given, and for simplicity, let us consider the ratio of their probabilities as $50:50$. We expect that the given individuum has distinct ideas, i.e., he prefers event A to an equally probable combination of events B and C, or vice versa. It is clear that if A is more preferable to him than B and C, A will also be more preferable than the named combination; similarly, if both B and C are more preferable than A, he will prefer this combination. However, if for him A is more preferable than B, but less preferable than C, any assertion that now he prefers A to the combination includes essential new information. That is, if he currently prefers A to the equally probable combination of B and C, it gives reasons for quantitative evaluation of the fact that his preference for A, compared with B, exceeds his preference for C compared with A. In such a way, by changing the ratio of probabilities, we can quantitatively evaluate the distance between any two preferences. (It must be said that the same reasoning was provided by Euclid for disposition of points on a straight line; in fact, exactly this is the basis of its classic conclusion for the calculation of distances.)

One more argument in favor of considering the *expected value* as a kind of purpose can be formulated in the following way. Suppose a situation where a player receives numerous such “purposes” in succession. To be definite, let us take two equally probable events, for example, the loss of 1€, and the gain of 2€. It would not be difficult to determine that by performing consecutively a large number of these event combinations will lead to the average value of each of them being $\frac{1}{2}$€, with an arbitrarily large accuracy. Thereby, the influence of this feature of games of chance might be minimized.

Incidentally, based on these arguments, the notion of fair play may be formulated as a game, before the beginning of which the expected value of a win for each player is equal to zero (or some certain value, in the case where it is not a zero-sum game).

1.2.5 Strategic games and mixed strategies

It has already been said that strategic games suppose a situation where a player must take a decision in circumstances of incomplete awareness about the status of the game. In his article, von Neumann [Neu28] ascertains that in fact, players’ strategies are systems of possible actions in various informational conditions.

The cases when the number of participants of game N equals 0 or 1 are of no interest. The case when $N = 2$ is the simplest of nontrivial cases, but it is of principal importance for all game theory and is good enough to illustrate the principles of the solution of strategic games.

In [Neu28], Von Neumann gives a detailed description of a zero-sum game with two participants, the rules of which he formulated in the following way:

Each of the players S_1 and S_2 chooses, without knowing the other's choice, one of the numbers $1, 2, \ldots, \Sigma_1$ and $1, 2, \ldots, \Sigma_2$, respectively (where Σ_i stands for the number of strategies for player S_i). If they have chosen numbers x and y, they receive the sums $g(x, y)$ and $-g(x, y)$, respectively. Here, the function $g(x, y)$ may be absolutely arbitrary (defined for $x = 1, 2, \ldots, \Sigma_1$ and $y = 1, 2, \ldots, \Sigma_2$). This is followed by quite simple arguments, which constitute the main body of game theory as a separate discipline.

Player S_1, for any choice x receives the gain not less than $\min_y g(x, y)$, and for this reason he must choose x so as to maximize this minimum, i.e., to provide oneself with $\max_x \min_y g(x, y)$ received. Player S_2, for similar reasoning, is able not to give S_1 more gain than $\min_y \max_x g(x, y)$. The equality

$$v = \max_x \min_y g(x, y) = \min_y \max_x g(x, y)$$

does not leave any doubts about optimal strategies; player S_1 can provide himself a gain in the amount of at least v, and player S_2 is able not to allow him to win more. This is obvious for non-strategic games, but this is not always true in the case of strategic games. This circumstance is overcome in the so-called *mixed expansion* of the game, i.e., by the implementation of so-called mixed strategies. Player S_1 in a strategic game chooses not just strategy x, but a combination of several strategies $\xi = (\xi_1, \xi_2, \ldots, \xi_{\Sigma_1})$, where ξ_i is the probability of choosing the ith strategy (it is implied, of course, that all $\xi_i > 0$, and that $\xi_1 + \xi_2 + \ldots + \xi_{\Sigma_1} = 1$). In the same manner, player S_2 chooses a mixed strategy $\eta = (\eta_1, \eta_2, \ldots, \eta_{\Sigma_2})$. (For example, in the above-mentioned "pitch-and-toss" game, mixed strategy $\xi_{\text{opt}} = \left(\frac{1}{2}, \frac{1}{2}\right)$ will be the most appropriate for player S_1, and optimal strategy for player S_2 is the same: $\eta_{\text{opt}} = \left(\frac{1}{2}, \frac{1}{2}\right)$. If, for example, player S_1 chooses any other strategy $\xi = (\alpha, 1-\alpha)$, $\alpha \neq \frac{1}{2}$, then actually he can be "punished" by player S_2's pure strategy $\eta = (0,1)$ or $\eta = (1,0)$ — depending on the definition of the function $g(x,y)$. In this case, it is clear that the gain (or rather expected value of the gain) of player S_1 in this case will be equal to

$$h(\xi,\eta) = \sum_{p=1}^{\Sigma_1} \sum_{q=1}^{\Sigma_2} g(p,q)\, \xi_p \eta_q.$$

One of the most significant theorems in game theory is the equality

$$\max_{\xi} \min_{\eta} h(\xi,\eta) = \min_{\eta} \max_{\xi} h(\xi,\eta). \tag{1.1}$$

From this equality, it follows that any zero-sum game with two participants has at least one pure or mixed optimal strategy for each of the players.

1.2.6 Coalitions

To reveal completely the matter of uncertainty in the outcome of games, one more question should be mentioned. This question arises when more than two players participate in a game.

For example, consider the game between three players, by the rules of which player S_1 has more privileges than players S_2 and S_3. Would the "weak" players unite in this case to resist more successfully the "strong" one, or would one of the "weak" players try to come to an agreement with the "strong" player, in order to to minimize losses? If one such coalition happens, what will be the conditions for its participants?

General answers to these questions have not yet been found. There exist more or less probable theories for games with three, four and partially, with five players. In addition, the variants are considered where the consolidated gain of the players is a variable quantity, which depends on strategies chosen by players. In general, the problem of relations among an arbitrary number of players is not yet resolved.

1.2.7 Concept of strategy

When speaking about different kinds of players, one usually means how these players behave in different game situations. In game theory, this behavior is called *strategy*. Under a strategy, we understand the following.

We shall consider all possible *positions* of the given game (under the position, we shall understand any sequence of choices, starting from the very beginning that does not contradict the rules of game). In every such position, player P has certain information regarding the current position of the game, and makes a choice according to the rules. In games with open information, he is completely aware of the game position. In other cases he can only affirm that a game is in one of a certain set of positions. We shall name this set of positions the *informational state* of a player in position P, and mark it as D_P. For example, in the case of a game with open information, $D_P = (P)$; but in any case $P \in D_P$.

The player's strategy is function $S\,(D_P)$, which is defined for all D_P, whose values correspond to the choice of a player in the informational state D_P. It can be said that the number of strategies is the number of different programs that can ever be written for implementation by a player (different — meaning such programs that behave differently in at least one position of at least one game). If the number of positions is finite, and in every position, only a finite number of moves is possible, then the number of strategies in this game is finite, although enormously large as a rule. For example, if in the simple tick-tack-toe game there exist 255168 different plays, including 549946 different positions, then the number of different strategies for the first player in this game is about 10^{30000}, and for the second player — more than 10^{50000}.

For this reason, in most real games, the entire set of strategies is considered from a purely abstract point of view. However, quite often, there are situations that are modeled by games with a small number of strategies; among these are the so-called matrix games.

1.3 Matrix games

1.3.1 Introduction

When studying two-player games it is often convenient to represent the gain function as a table or matrix, the size of which corresponds to the number of different strategies for both players.

Consider, for example, a conflict situation, where each of two players has the following possibilities for choosing his mode of behavior:

- player S_1 can choose any of the strategies $1, 2, \ldots, \Sigma_1$;
- player S_2 can choose any of the strategies $1, 2, \ldots, \Sigma_2$.

By sequentially going over all the strategies of player S_1 and all the strategies of player S_2, it is possible to complete the table (or *matrix*) of gains for these players. In this case, for example, rows and columns answer to the choices of the first and second player, respectively.

The games, which are representable in such a manner, are called *matrix games*. In fact, any game between two players may be represented in the form of such a table; the only restricting factor is usually the huge number of strategies.

1.3.2 Zero-sum games with two players

The easiest case to analyze is so-called *zero-sum games*. It means that the total sum of gains of all the players equals zero. Therefore, if there are two players, the gain of one of them is equal to the other's loss.

To illustrate this, we shall consider a modified version of the pitch-and-toss game. The first player, independently from the second player, thinks of a number — 0 or 1 (i.e., "pitch" or "toss", respectively); the second player does the same thing. In the case where the numbers do not coincide, the second player wins, the second player wins and if they do coincide, the first player wins. Additionally, in the case where the two numbers equal 1, the first player receives double gain.

The outcome function for the first player can be represented as a table:

		Number of player 2	
		0	1
Number of player 1	0	+1	−1
	1	−1	+2

or as a matrix:

$$G = \begin{pmatrix} 1 & -1 \\ -1 & 2 \end{pmatrix}$$

In this case, optimal behavior for the first player would be the choice of strategy "0" with probability $\frac{3}{5}$ and of strategy "1" with probability $\frac{2}{5}$ (although this might seem strange). Then his expected gain will be $\frac{1}{5}$ irrespective of the second player's behavior. For the second player, optimal behavior would also be strategy "0" with probability $\frac{3}{5}$ and strategy "1" with probability $\frac{2}{5}$, and his expected loss would be $\frac{1}{5}$. That is,

$$\xi_{\text{opt}} = \eta_{\text{opt}} = \left(\frac{3}{5}, \frac{2}{5}\right),$$

and

$$h\left(\xi_{\text{opt}}, \eta_{\text{opt}}\right) = \frac{1}{5}.$$

It is easy to see that, in cases of deviation from his optimal strategy, a player could be punished with a decrease of his expected gain.

Problems of this kind are resolved using methods of linear programming and are considered completely analyzed for any reasonable number of strategies.

1.3.3 Non-zero-sum games

Previous considerations concerned the games of two participants, in which the interests of the players were absolutely opposite. Much more frequent are situations when the interests of the players, although not coincident, do not have to be absolutely opposite.

That is, sometimes players in such games could achieve better result by combining their efforts rather than declining the possibility of cooperation.

In this case, every joint choice of the players might be described by two functions. If player S_1 chooses strategy x, and player S_2 chooses strategy y, then as a result, the gain of player S_1 would equal a certain number $g_1(x, y)$, and generally, the gain of player S_2 would equal a certain other number $g_2(x, y)$. (Remember that in the case of zero-sum games $g_2(x, y) = -g_1(x, y)$.) The outcome function for the first and for the second players could be represented as two tables (or two matrices[1]).

As an example we shall consider probably the most popular game from experimental economics. In this game each player is asked to make a choice: take from the organizer of the game either 1€ for himself or 100€ for a partner. This game may be described in the following two tables:

First player's outcome function g_1

First player \ Second player	**100€**	**1€**
100€	*100€*	*0€*
1€	*101€*	*1€*

Second player's outcome function g_2

First player \ Second player	**100€**	**1€**
100€	*100€*	*101€*
1€	*0€*	*1€*

However, the results would be more obviously demonstrated as one table:

First player \ Second player	**100€**	**1€**
100€	*100€* to First player *100€* to Second player	*0€* to First player *101€* to Second player
1€	*101€* to First player *0€* to Second player	*1€* to First player *1€* to Second player

Suppose that player S_1 chooses strategy "100€ to partner" with probability p and strategy "1€ to oneself" with probability $1-p$. Similarly, player S_2 chooses strategy

[1]Such games are known as *bimatrix games*.

"100€ to partner" with probability q and strategy "1€ to oneself" with probability $1-q$. That is, $\xi = (p, 1-p)$ and $\eta = (q, 1-q)$.

Then, the expected gain of player S_1 would equal

$$h_1(p,q) = g_1(0,0)\,pq + g_1(0,1)\,p(1-q) + g_1(1,0)(1-p)\,q + g_1(1,1)(1-p)(1-q)\,,$$

and the expected gain of player S_2 would equal

$$h_2(p,q) = g_2(0,0)\,pq + g_2(0,1)\,p(1-q) + g_2(1,0)(1-p)\,q + g_2(1,1)(1-p)(1-q)$$

($0 \le p, q \le 1$; instead of the names of the strategies "100€ to partner" and "1€ to oneself", they are given numbers 0 and 1, respectively).

1.3.4 Points of equilibrium

Non-zero-sum games are a popular subject for discussion in economic and social philosophy, mainly because of their relation to issues of self-interest and cooperation (and for the same reasons, they often are confused with *cooperative games*). These topics will be illustrated and considered in more detail in further chapters (in Section 3.4, and then in Chapter 13), where we compare some non-zero-sum games with their quantum analogs. In this subsection, we introduce one important solution concept for non-zero-sum games, which prepares the ground for this kind of comparison and which will be used throughout most of the sections of Part III.

Let us consider a game, where both players S_1 and S_2 have a choice between strategy 0 and strategy 1. The probabilities of choosing strategy 0, as in the previous considerations, are marked as p and q, respectively, for players S_1 and S_2. That is, their mixed strategies would equal $\xi = (p, 1-p)$ and $\eta = (q, 1-q)$.

We shall say that a pair of numbers

$$(p^*, q^*)\,, \qquad 0 \le p^*, q^* \le 1$$

defines an *equilibrium situation*, if for any p and q $(0 \le p, q \le 1)$ the following two inequalities are simultaneously true:

$$h_1(p, q^*) \le h_1(p^*, q^*)\,, \qquad \text{and} \qquad h_2(p^*, q) \le h_2(p^*, q^*)\,.$$

These inequalities mean the following; a situation, defined by mixed strategy (p^*, q^*), is an equilibrium if a deviation from it by one of the players (assuming that the other player keeps his choice) cannot result in an increase of the gain of the player who deviated from the strategy. Therefore, it turns out that, if an equilibrium situation exists, deviation from it is not advantageous to any player himself.

Could such situations appear in a non-zero-sum game? According to the theorem on the points of equilibrium, proved by John Nash,

any non-zero-sum game has at least one equilibrium situation (point of equilibrium) in mixed strategies.

For example, in the game described in the end of the previous subsection (1.3.3), the only equilibrium situation would be choosing the pure strategy "1€ to oneself" for both players, that is, $p = q = 0$. In all other situations, for each of the players, it makes sense to deviate towards the strategy "1€ to oneself".

In other games, strategies in equilibrium situations might really be mixed, but we shall not dwell on proving this fact, as we shall not use it in our further analysis.

Equilibrium situations are interesting because they provide a rather good description of fixed points in the behavior of economic systems (recall that John Nash received his Nobel Memorial Prize in economic sciences.)

Like the von Neumann–Morgenstern theorem (1.1) for two-player zero-sum games, the Nash equilibrium is treated as the most important solution concept for non-zero-sum games. Finding the Nash equilibrium for different kinds of games is a topical problem in game theory. We refer to the book by Nisan, Roughgarden, Tardos, and Vazirani [NRTV07] for the latest achievements in solving this and related problems.

Chapter 2

Quantum Systems and Their States

2.1 Introduction

When studying different kinds of interactions, one usually bears in mind the fact that each participant possesses some amount of information. According to this information, the participant performs his actions. In particular, players in a game have some information about the choices of the other players. Furthermore, performing a move in the game is usually nothing more than announcing an appropriate decision, i.e., providing others with some information.

As we are studying interactions with the principles of the quantum mechanics involved, let us briefly describe what information is from the quantum mechanical point of view. An extended study on quantum information and related linear algebra can be found in [Sha80] or any other textbook in a similar area.

2.2 Quantum bits

2.2.1 States of qubits

Traditionally information is being measured (and sometimes represented) by ***bi**nary digi**t**s* or, shorter, *bits*. The basic unit of quantum information is called the ***qu**antum **bit*** or, shorter, the *qubit*. The fundamental differences between these two kinds of information are of special interest in the field known as quantum information processing.

A bit can have one of two values — 0 or 1. Similarly, a qubit can also be in one of two states. In the case of a qubit these two states are usually labeled as $|0\rangle$ and $|1\rangle$. Unlike a bit, a qubit can generally exist in a so-called *superposition* state, which is a linear combination of the basic states $|0\rangle$ and $|1\rangle$. Generally, a state of a qubit can be represented as

$$\alpha|0\rangle + \beta|1\rangle, \tag{2.1}$$

where α and β are called *amplitudes*, and their values are some complex numbers.

2.2.2 Measurement of qubits

One of the most intriguing features of quantum information is that given a qubit, an observer cannot determine its state; however, he can learn some information about it by performing a *measurement* on it.

If the qubit was in state (2.1) before, then after the measurement, it *collapses* to one of two states — $|0\rangle$ or $|1\rangle$, and the observer can recognize which of the two events occurred. The ratio of probabilities of collapsing to $|0\rangle$ and collapsing to $|1\rangle$, according to the laws of quantum mechanics, is $|\alpha|^2 : |\beta|^2$. In order to fit probability theory, the following restriction must be applied on the values of amplitudes α and β:

$$|\alpha|^2 + |\beta|^2 = 1. \tag{2.2}$$

Complex vector $\binom{\alpha}{\beta}$ which meets condition (2.2), is called a *unit vector.*

2.2.3 Unitary operations on qubits

In addition to the measurement, there are operations of another kind that change the state of a qubit. These operations are linear transformations defined on the set of 2-dimensional unit vectors. If such a linear transformation preserves the unity of a vector, then it is called *unitary.* Unitary transformations (or *unitary operators*), defined on the set 2-dimensional unit vectors, can naturally be described by 2×2 matrices, which also are called *unitary.*

For example, one very important set of four unitary operators in quantum computing is known as the *Pauli operators*. Probably the most common notation for them is σ_0, σ_x, σ_y and σ_z. These operators act on the basic states of a qubit $|0\rangle$ and $|1\rangle$ in the following way:

- $\sigma_0|0\rangle = |0\rangle$; $\qquad \sigma_0|1\rangle = |1\rangle$;
- $\sigma_x|0\rangle = |1\rangle$; $\qquad \sigma_x|1\rangle = |0\rangle$;
- $\sigma_y|0\rangle = -i|1\rangle$; $\qquad \sigma_y|1\rangle = i|0\rangle$;
- $\sigma_z|0\rangle = |0\rangle$; $\qquad \sigma_z|1\rangle = -|1\rangle$.

We can also represent σ_0, σ_x, σ_y and σ_z as 2×2 unitary matrices:

$$\sigma_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}; \qquad \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}; \qquad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}; \qquad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Another example is one special subset of unitary transformations described in [EWL99], which can be defined by the following two-parametric set of matrices:

$$\left\{ \widehat{U}(\theta, \phi) = \begin{pmatrix} e^{i\phi}\cos\theta & \sin\theta \\ -\sin\theta & e^{-i\phi}\cos\theta \end{pmatrix} : \theta, \phi \in \mathbb{R} \right\}.$$

2.3 Larger quantum systems

2.3.1 Quantum digits

In Subsection 2.2.1 we described the set of states for qubits, the simplest type of quantum systems, with just two basic states, $|0\rangle$ or $|1\rangle$. However, there are more complex quantum systems with more than two basic states.

For example, the so-called *qutrits* are three-level quantum systems with three basic states $|0\rangle$, $|1\rangle$, and $|2\rangle$; the general superposition state of a *qutrit* can be described as $\alpha|0\rangle + \beta|1\rangle + \gamma|2\rangle$, and of course, vector $\begin{pmatrix} \alpha \\ \beta \\ \gamma \end{pmatrix}$ should be unit: $|\alpha|^2 + |\beta|^2 + |\gamma|^2 = 1$.

Generally, an M-level quantum system has M basic states: $|0\rangle$, $|1\rangle$, $\ldots$, $|M\rangle$. Analogously, its state can be described by $\sum_{i=1}^{M} \alpha_i |i\rangle$, and vector

$$\begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_M \end{pmatrix} \tag{2.3}$$

should be a unit vector: $\sum_{i=1}^{M} |\alpha_i|^2 = 1$. Such a quantum system is sometimes called a ***qu**antum **dig**it* or, shorter, *qudit* (as it is a quantum analog of the classical digit from $\{1, 2, \ldots, M\}$).

2.3.2 Multipartite quantum systems

Sometimes it is useful to emphasize that a multilevel quantum system comprises several quantum subsystems.

For example, if a quantum system consists of two qubits, then its four basic states are four different tensor products of the qubits' basic states:

$$|0\rangle \otimes |0\rangle, \qquad |0\rangle \otimes |1\rangle, \qquad |1\rangle \otimes |0\rangle, \qquad \text{and} \qquad |1\rangle \otimes |1\rangle.$$

Usually, they are labeled as

$$|00\rangle, |01\rangle, |10\rangle, \text{ and } |11\rangle, \qquad \text{respectively.}$$

Its state can then be described as $\alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$, or by the unit vector $\begin{pmatrix} \alpha_{00} \\ \alpha_{01} \\ \alpha_{10} \\ \alpha_{11} \end{pmatrix}$ of length $|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1$.

If a quantum system consists of more than two qubits, say N qubits, then its 2^N basic states are usually labeled as $|b_1 b_2 \ldots b_N\rangle$, where $b_i \in \{0, 1\}$.

2.3.3 Unitary operations on quantum systems

As mentioned in Subsection 2.3.1, an M-level quantum system could be represented as a unit vector in form (2.3). Unitary operations on such a quantum system could then be represented as $M \times M$ unitary matrices.

There is a large variety of such matrices, and in the next subsection, we shall describe a specific example of a 4×4 unitary matrix, which will demonstrate an unusual effect of quantum mechanics.

2.3.4 Quantum entanglement

Another phenomenon of the quantum world, which sometimes does not fit in classical communication theory, is called *quantum entanglement*.

The simplest illustration of this phenomenon requires a two-qubit quantum system. Let us observe two qubits, both in basic state $|0\rangle$, as a single quantum system. As stated in Subsection 2.3.2, the state of such a quantum system is denoted as $|00\rangle$ and can be represented by the four-dimensional vector $\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$.

Let us now apply the linear unitary operator, which is represented by the unitary matrix $\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & -1 & 0 \\ 1 & 0 & 0 & -1 \end{pmatrix}$:

$$\begin{pmatrix} \frac{1}{\sqrt{2}} & 0 & 0 & \frac{1}{\sqrt{2}} \\ 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ 0 & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & 0 \\ \frac{1}{\sqrt{2}} & 0 & 0 & -\frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ \frac{1}{\sqrt{2}} \end{pmatrix}.$$

As one can follow, the resulting state is then the following sum: $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$. This is the so-called *Bell state* [1], and a pair of qubits in such a state is called the *EPR pair* (after the famous Einstein, Podolsky and Rosen paradox).

When measuring one qubit of the EPR pair, one will make it collapse equiprobably to one of the two basic states, $|0\rangle$ or $|1\rangle$. Surprisingly, measurement of another qubit will cause it to collapse to exactly the same state as the first measured qubit. Therefore, one could say that the two qubits of the EPR pair are *entangled*.

The effects of quantum entanglement have been studied extensively in quantum information science and in particular, they play a key role in quantum game theory.

[1] A similar state for ≥ 3 qubits — $\frac{1}{\sqrt{2}}|00\dots0\rangle + \frac{1}{\sqrt{2}}|11\dots1\rangle$ — is called the *GHZ state* (after Greenberger, Horne and Zeilinger, who discovered the extremely non-classical properties of such states in their joint work [GHZ89]).

Chapter 3

Overview and Examples of Quantum Games

3.1 Introduction

As many elements and ideas of game theory and quantum mechanics have some common ground, there have been several attempts to find interconnections between these topics. We could establish some of the reasons for such interest.

The element of uncertainty in many games is raised by some random events, and can be described in terms of probabilities. On the other hand, the concept of probability underlies quantum mechanics. Thus, quantum probability could be used to describe quantum versions of games that assume some classical randomness.

Correlations between measurement results within an entangled quantum system could be used for better cooperation between players. Apart from the fact that this serves as a great demonstration of the properties of the quantum world, it could also have also some useful applications.

There are some more interesting aspects in studying correlations between game theory and the behavior of quantum particles. However, this interest lies rather in the area of physics (e.g., crystallography). In this work, we shall concentrate mainly on information-theoretic aspects and ideas brought by the properties of quantum states.

The concept of quantum games has been developed since the late 1990s [Vai99, Mey99]. Many examples of them have been invented to illustrate how different are the circumstances in the microcosm from the classical. In this chapter we shall study several quantum games, which represent the most significant ideas in this area.

3.2 Vaidman's game

Vaidman [Vai99] was probably the first to speak about quantum protocol in terms of games. He illustrated the Greenberger-Horne-Zeilinger (GHZ) proof of the nonexistence of local hidden variables by presenting a 3-player game that cannot be won with confidence without using quantum theory.

Imagine three players are taken to three remote locations A, B and C. Then, at the same moment, each of them is asked one of two possible questions:

- What is X?

  or

- What is Y?

Whatever question a player was asked, he could only answer either "1" or "-1".

The rules of this game assume only two possible types of scenario:

1. All players are asked "What is X?".

   In this case, the players must answer with three numbers with product -1. That is, up to permutations, either with 1,1,-1 or with -1,-1,-1.

2. One player is asked "What is X?" and the other two players are asked "What is Y?".

   In this case, the players must answer with three numbers with product 1. That is, up to permutations, either with 1,1,1 or with 1,-1,-1.

3.2.1 Classical version

Actually, here, each player has only four possible choices:

1.	Asked	X,	answer	1;	asked	Y,	answer	1.
2.	Asked	X,	answer	1;	asked	Y,	answer	-1.
3.	Asked	X,	answer	-1;	asked	Y,	answer	1.
4.	Asked	X,	answer	-1;	asked	Y,	answer	-1.

Let us denote the answers to the question "What is X?" chosen by players A, B and C, as X_A, X_B and X_C, respectively, and the answers to the question "What is Y?" chosen by players A, B and C, as Y_A, Y_B and Y_C, respectively.

If there was a winning strategy $\{X_A,\ X_B,\ X_C,\ Y_A,\ Y_B,\ Y_C\}$ for the players, the following set of conditions should be satisfied:

$$X_A X_B X_C = -1$$

$$X_A Y_B Y_C = 1$$

$$Y_A X_B Y_C = 1$$

$$Y_A Y_B X_C = 1$$

Of course, it is impossible to satisfy all four conditions. The product of left-hand sides of these equations is positive, as it is the product of squares:

$$X_A^2 X_B^2 X_C^2 Y_A^2 Y_B^2 Y_C^2 = 1.$$

On the other hand, the product of the left-hand side of these equations is, evidently, -1.

This contradiction shows that there is no 100%-winning classical strategy.

3.2.2 Quantum version

In order to demonstrate quantum strategy for his game, Vaidman [Vai99] considers the following scenario:

1. Players are given an entangled three-qubit quantum system in initial state:

$$|GHZ\rangle = \frac{1}{\sqrt{2}} \left(|000\rangle - |111\rangle\right)$$

2. Players are asked their questions.

3. Each player performs a measurement on his qubit in some basis — according to the type of question he received.

4. Each player answers with $(-1)^{\text{[result of the measurement: 0 or 1]}}$

Let us look on this process from a slightly different point of view. For our further purposes, it will be suitable to consider local qubit operations instead of measuring them in different bases.

The precise quantum strategies for players could be defined as follows:

- Asked "What is X?", a player "flips" his qubit using transformation matrix
$$\widehat{X} = \begin{pmatrix} -\frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix}.$$
- Asked "What is Y?", a player "flips" his qubit using transformation matrix
$$\widehat{Y} = \begin{pmatrix} -\frac{i}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} & -\frac{i}{\sqrt{2}} \end{pmatrix}.$$
- After performing the respective transformations, each player measures his qubit in computational basis and answers with $(-1)^{\text{[result of the measurement: 0 or 1]}}$.

It is easy to check that the finite state after three local operations will be equal to

$$\widehat{X} \otimes \widehat{X} \otimes \widehat{X} \left(\frac{1}{\sqrt{2}}|000\rangle - \frac{1}{\sqrt{2}}|111\rangle \right) = \frac{1}{2} \left(|001\rangle + |010\rangle + |100\rangle + |111\rangle \right)$$

or (up to permutations of players)

$$\widehat{X} \otimes \widehat{Y} \otimes \widehat{Y} \left(\frac{1}{\sqrt{2}}|000\rangle - \frac{1}{\sqrt{2}}|111\rangle \right) = \frac{1}{2} \left(|000\rangle - |011\rangle + |101\rangle + |110\rangle \right)$$

In each case, the parity of 1's corresponds to the right answer, so this quantum strategy is 100%-winning.

3.3 CHSH game

Another cooperative game, which probably is the most studied in physical experiments (starting with [AGR81]), was initially described in [CHSH69]. This is a game between a referee from one side and players from the other side. The referee gives one bit to each player. Then he expects equal answers if at least one input bit was 0. If both input bits were 1, he expects different answers. Formally, the rules of this game could be expressed by the table:

$INPUT$	Right answer
$0, 0$	$0, 0$ or $1, 1$
$0, 1$	$0, 0$ or $1, 1$
$1, 0$	$0, 0$ or $1, 1$
$1, 1$	$0, 1$ or $1, 0$

or by the formula:

$$XOR\,(OUTPUT) = AND\,(INPUT)$$

3.3.1 Classical version

Assume that the referee gives to the players randomized (uniformly distributed) inputs from $\{(0,0), (0,1), (1,0), (1,1)\}$. For any pair of fixed (deterministic) players' strategies

$$(A:\ \{0,1\} \to \{0,1\}, \quad B:\ \{0,1\} \to \{0,1\})$$

the sum of their answers for all four different inputs

$$(A\,(0) + B\,(0)) + (A\,(0) + B\,(1)) + (A\,(1) + B\,(0)) + (A\,(1) + B\,(1))$$

is evidently even.

However, as the sum of right answers must be odd, any strategy pair will lead to at least one error in these four cases. (One might think that some kind of randomized strategy could give better results, but the answer is no; an average result of a randomized strategy is calculated as an average result of some set of fixed strategies.)

Therefore, the provably best average result is $\frac{3}{4} = 0.75$. This can be achieved by answering 0 and ignoring the input.

3.3.2 Quantum version

Surprisingly, there is a way to improve the classical result of 0.75 by permitting players to use an entangled quantum system before the start of the game.

Imagine players share a two-qubit system in entangled state

$$|\psi\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

Again, it is sufficient for players to use the same strategy:

- Given input x (0 or 1), a player "flips" his qubit using transformation matrix

$$\begin{pmatrix} \frac{e^{\frac{1-4x}{8}\pi i}}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{e^{\frac{4x-1}{8}\pi i}}{\sqrt{2}} \end{pmatrix}.$$

- Then he measures his qubit in computational basis and answers with the result of the measurement.

Let us estimate the outcome of the game in the case where players get input "a, b" (from the set $\{(0,0), (0,1), (1,0), (1,1)\}$). The product of the transformation matrices $\widehat{A}$ and $\widehat{B}$ is then equal to

$$\widehat{A}\otimes\widehat{B}=\begin{pmatrix}\boxed{\dfrac{e^{\frac{2-4a-4b}{8}\pi i}}{2}} & -\dfrac{e^{\frac{1-4a}{8}\pi i}}{2} & -\dfrac{e^{\frac{1-4b}{8}\pi i}}{2} & \boxed{\dfrac{1}{2}} \\ \dfrac{e^{\frac{1-4a}{8}\pi i}}{2} & \dfrac{e^{\frac{4b-4a}{8}\pi i}}{2} & -\dfrac{1}{2} & -\dfrac{e^{\frac{4b-1}{8}\pi i}}{2} \\ \dfrac{e^{\frac{1-4b}{8}\pi i}}{2} & -\dfrac{1}{2} & \dfrac{e^{\frac{4a-4b}{8}\pi i}}{2} & -\dfrac{e^{\frac{4a-1}{8}\pi i}}{2} \\ \boxed{\dfrac{1}{2}} & \dfrac{e^{\frac{4b-1}{8}\pi i}}{2} & \dfrac{e^{\frac{4a-1}{8}\pi i}}{2} & \boxed{\dfrac{e^{\frac{4a+4b-2}{8}\pi i}}{2}}\end{pmatrix}$$

In fact, there is no need to do all those boring calculations. Actually, it is sufficient for our further purposes to consider only the corner values of this matrix (these four values are marked with boxes).

As the initial state $\left(\dfrac{1}{\sqrt{2}}|00\rangle+\dfrac{1}{\sqrt{2}}|11\rangle\right)$ has only two non-zero amplitudes, we are actually only interested in two rows of matrix $\widehat{A}\otimes\widehat{B}$; namely, in the first and the last ones.

Let us now consider amplitudes of $|00\rangle$ and $|11\rangle$ of the final state. They depend only on two columns of matrix $\widehat{A}\otimes\widehat{B}$; namely, the first and the last ones.

If $A=B=1$, they both are equal to $\dfrac{e^{\pm\frac{6}{8}\pi i}+1}{2\sqrt{2}}$, and the probability of getting *losing* measurement results $(0,0)$ or $(1,1)$ is equal to

$$2\times\left|\frac{e^{\pm\frac{6}{8}\pi i}+1}{2\sqrt{2}}\right|^2=\cos^2\frac{3}{8}\pi=0.146\ldots$$

In the opposite case, if $a+b\leq 1$, they are both equal to $\dfrac{e^{\pm\frac{2}{8}\pi i}+1}{2\sqrt{2}}$, and the probability of getting *winning* measurement results $(0,0)$ or $(1,1)$ is equal to

$$2\times\left|\frac{e^{\pm\frac{2}{8}\pi i}+1}{2\sqrt{2}}\right|^2=\cos^2\frac{1}{8}\pi=0.8535\ldots$$

(To make these equalities evident, one can recall the fact that $\left|e^{pi}+e^{qi}\right|$ is just $2\cos\dfrac{p-q}{2}$, and in particular, $\left|e^{pi}+e^{0i}\right|=2\cos\dfrac{p}{2}$.)

Therefore, whatever input players received, they win with a probability of $\cos^2 \frac{1}{8}\pi = \frac{1}{2} + \frac{1}{2\sqrt{2}} = 0.8535\ldots$ and lose with a probability of $\cos^2 \frac{3}{8}\pi = \frac{1}{2} - \frac{1}{2\sqrt{2}} = 0.146\ldots$.

In fact, this is the best result that could be achieved in this game, as was shown in [Cir80].

Traditionally, quantum strategies for this game are described in a different way. In particular, players are offered the use of *different* strategies. The reason why we did not follow this tradition is ideological; the notion of symmetry is crucial for our further considerations, and given a symmetrical problem, we shall try to find symmetrical solutions for it.

3.4 Prisoner's Dilemma

Prisoner's Dilemma is one of the most popular non-zero-sum games. It is strategically completely equivalent to the economic game mentioned in Subsection 1.3.3. It is considered that the initial source of the idea of this game was discussions by Merrill Flood and Melvin Dresher in 1950, as part of the game theory investigations in the Rand Corporation during the Cold War. As Flood and Dresher did not publicize their ideas in external journal articles, there is no canonical formulation of the rules of this game. Let us quote from the website www.prisoners-dilemma.com, which is dedicated entirely to the Prisoner's Dilemma:

> You and a friend have committed a crime and have been caught. You are being held in separate cells. You are both offered a deal but have to decide what to do. But you are not allowed to communicate with your partner and you will not be told what they have decided until you have made a decision.
>
> Essentially the deal is this.
>
> - If you confess and your partner denies taking part in the crime, you go free and your partner goes to prison for five years.
> - If your partner confesses and you deny participating in the crime, you go to prison for five years and your partner goes free.
> - If you both confess you will serve four years each.
> - If you both deny taking part in the crime, you both go to prison for two years.

These rules could be represented as in Table 3.1.

Table 3.1: Players' payoffs in Prisoner's Dilemma

		Your partner: Confesses	Your partner: Denies
You	Confess	4 years for You, 4 years for Your partner	0 years for You, 5 years for Your partner
You	Deny	5 years for You, 0 years for Your partner	2 years for You, 2 years for Your partner

This game is a famous illustration of the fact that two rationally operating individuals sometimes might not cooperate, even if it is in their interest to do so. The phenomenon represented by this game became very popular among scientists of different areas, and it was investigated in many works and from many points of view. For the history of this idea we refer to one of the most significant books on this topic, which is dedicated entirely to the Prisoner's Dilemma [Pou92].

3.4.1 Classical version

Analysis of such games usually assumes the Nash equilibrium as a solution concept. This concept was described in Subsection 1.3.3, and very similar arguments in the case of the Prisoner's Dilemma show that rational players will confess and serve four years each.

One can formalize the game process in the following way (some redundant formalism here will be clarified later):

1. The game board consists of two numbers a and b from $[0, 1]$.
   Initially their values are $a_1 = b_1 = 0$.

2. Players independently choose (say linear) operators A and B and apply them to a and b, respectively.

Let us denote $a_2 = A(a_1)$ and $b_2 = B(b_1)$.

3. Resulting numbers a_2 and b_2 are treated as probabilities of choosing the second strategy, i.e., denying participation in the crime. (Obviously, $1 - a_2$ and $1 - b_2$ then will be the probabilities of choosing the first strategy, i.e., confessing.)

4. Players get their payoffs — respectively
$\$_1(a_2, b_2) = -4(1 - a_2)(1 - b_2) - 5a_2(1 - b_2) - 2a_2b_2 = 4b_2 - 4 - a_2(1 + b_2)$ and
$\$_2(a_2, b_2) = -4(1 - a_2)(1 - b_2) - 5(1 - a_2)b_2 - 2a_2b_2 = 4a_2 - 4 - b_2(1 + a_2)$.

Obviously,

$\max_A \$_1(A(0), b_2)$ (for any b_2) is achieved when $A(0) = 0$, and
$\max_B \$_2(a_2, B(0))$ (for any a_2) is achieved when $B(0) = 0$.

In other words, when players independently maximize their payoffs (by choosing identity operators $A = B = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$), they both get

$\$_1(0, 0) = \$_2(0, 0) = -4.$

On the other hand, the Pareto optimal decision would be to choose exchange operators $A = B = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ with payoffs

$\$_1(1, 1) = \$_2(1, 1) = -2.$

3.4.2 Quantum version

Jens Eisert, Martin Wilkens, and Maciej Lewenstein in [EWL99, EW00] investigated the quantization of non-zero-sum games and in particular Prisoner's Dilemma. The physical model proposed for quantum games assumes the following prerequisites:

- a system of multiple qubits in a given initial state (usually in an entangled one);
- two or more players, each of which is provided at least one qubit and the ability to act on these qubits;
- a device to measure the final state of the system, which determines the outcome for each of the players.

The proposed quantum game process is somewhat analogous to the classical one:

1. The game board consists of a two-qubit quantum system.
   Its initial state is $\psi_1 = |00\rangle$.

1_q Before all players' actions, an entangling operator

$$\widehat{J} \in \left\{ \exp\left(i\gamma \begin{pmatrix} 0001 \\ 0010 \\ 0100 \\ 1000 \end{pmatrix} \right) : \gamma \in \left[0, \frac{\pi}{4}\right] \right\}$$

is applied to the system, which gets "entangled" into state $\psi_{1_q} = \widehat{J}\psi_1$.

2. Players independently choose operators $\widehat{A} = \widehat{U}\left(\theta_A, \phi_A\right)$ and $\widehat{B} = \widehat{U}\left(\theta_B, \phi_B\right)$ and apply them to the first and the second qubits of the system, respectively. Its state changes to $\psi_2 = \left(\widehat{A} \otimes \widehat{B}\right) \psi_{1_q}$.

2_q After all the players' actions are done, an operator $\widehat{J}^\dagger$ is applied to the system.
Its state changes to $\psi_{2_q} = \widehat{J}^\dagger \psi_2$.
Let us denote $\psi_{2_q} = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$.

3. The resulting qubits are measured in computational basis, and absolute squares of probability amplitudes $|\alpha_{ab}|^2$ are treated as probabilities of choosing strategy a by the first player and strategy b by the second player (where $a, b \in \{0, 1\}$, strategy 0 corresponds to confessing and strategy 1 corresponds to denying participation in the crime).

4. Players get their payoffs — respectively
   $\$_1\left(\psi_{2_q}\right) = -4\left|\alpha_{00}\right|^2 - 5\left|\alpha_{10}\right|^2 - 2\left|\alpha_{11}\right|^2$ and
   $\$_2\left(\psi_{2_q}\right) = -4\left|\alpha_{00}\right|^2 - 5\left|\alpha_{01}\right|^2 - 2\left|\alpha_{11}\right|^2$

As one can see, the quantum scheme implies two additional steps 1_q and 2_q, which stand for the "quantum entangling" and "quantum disentangling" of quantum system, respectively.

The authors of [EWL99] argue that (a) these two steps together with (b) two additional variables ϕ_A and ϕ_B in step 2, essentially make all the difference between the classical and quantum versions of the game. Therefore, the quantum version of the Prisoner's Dilemma is somewhat a: (a) generalization and (b) "quantum-mixed" expansion of the original game.

The fact is that by fixing $\phi_A = \phi_B = 0$ makes the game completely equivalent to its classical version with $a = \sin^2\theta_A$ and $b = \sin^2\theta_B$ (and the same Nash equilibrium $\theta_A = \theta_B = 0$ with payoffs $\$_1 = \$_2 = -4$) [1].

Therewith, adjusting parameter γ for operator $\widehat{J}$ from step 1_q allows obtaining different degrees of quantum entanglement effect in the game. Thus, setting $\gamma = 0$ eliminates any quantum entanglement and leaves the Nash equilibrium at the point of mutual confessing and a four-year prison sentence. On the other hand, setting $\gamma = \frac{\pi}{4}$ provides maximal entanglement, and improves the players' behavior up to the Pareto optimal mutual denying participation in the crime. For example, the set of Nash equilibria in such a game contains a symmetric pair of strategies $\widehat{A} = \widehat{B} = \widehat{U}\left(0, \frac{\pi}{4}\right)$ with payoffs $\$_1 = \$_2 = -2$. (The idea is the following: for the first player choosing strategy $\widehat{A} = \widehat{U}\left(0, \frac{\pi}{4}\right)$ guarantees equity $|\alpha_{01}|^2 = |\alpha_{10}|^2 = \frac{\sin^2\theta_B}{2}$, so that $\$_1\left(\psi_{2_q}\right) = \$_2\left(\psi_{2_q}\right)$, and with certainty converts an adversary into an ally; a similar argument remains for choosing strategy $\widehat{B} = \widehat{U}\left(0, \frac{\pi}{4}\right)$ by the second player.)

[1] This "backward compatibility" with the set of classical strategies is assured by the constraint on $\widehat{J}$ in step 1_q.

Part II

Nonlocal XOR Games

Chapter 4

Introduction

4.1 Definition

In Vaidman's game use of an entangled quantum system allow players to construct 100%-winning strategies. In CHSH game players can use quantum strategies to achieve result, which exceeds classical optimum by over 10%. This improvement is possible because of correlations between measurement outcomes of different parts of quantum system In physics, these correlations are referred to as *nonlocality* or *quantum entanglement*. Therefore, such games are called *nonlocal* or *entangled*. Actually, CHSH is the most famous example of nonlocal games. But let us now give a general description of these games.

A nonlocal game is a cooperative game of two or more players. Given some information, the players must find a solution, but with no direct communication between any of them.

We can view nonlocal games as games between a *referee* and some number of *players*, where communication is available only between the referee and the players. Referee chooses settings of the game by telling some information (or *input*) x_i to each of the player.

After that, each player independently must give back some answer (or *output*) y_i. The rules of the game define a function $f(x_1, x_2, \ldots, y_1, y_2, \ldots)$ which determines whether the players have won or lost.

Players are not allowed to communicate among themselves. In the classical case, they can use shared common bits that are independent of the inputs $x_1, \ldots, x_N$ (one can interpret this fact in the following way: players are allowed to communicate *before* they have received their questions, but prohibited to communicate *after* that). In the quantum case, they can use a common multipartite quantum state $|\psi\rangle$ that is independent of $x_1, x_2, \ldots, x_N$. Each of players receives a part of $|\psi\rangle$ and is allowed to apply a measurement that depends on his input x_i to his part of $|\psi\rangle$. The advantage of quantum strategies is possible because of the non-classical correlations between the measurement outcomes of different parts of quantum system $|\psi\rangle$ (*entanglement* or *nonlocality*).

In general, the maximum winning probability in a nonlocal game is hard to compute. It is NP-hard to compute it for 2-player games with quantum inputs and outputs or for 3-player games classically [KKM$^+$08].

4.2 Nonlocal XOR games

Nonlocal games have been a very popular research topic (often, under the name of Bell inequalities [Bel64, Eke91]). Many nonlocal games have been studied and large gaps between classical and quantum winning probabilities have been discovered.

XOR games are the most widely studied class of nonlocal games. In a XOR game, players' outputs $y_1, y_2, \ldots, y_N$ are $\{0, 1\}$-valued. The condition describing whether the players have won can depend only on $x_1, x_2, \ldots, x_N$ and $y_1 \oplus y_2 \oplus \ldots \oplus y_N$. In particular, XOR games include the CHSH game.

For two-player XOR games (with inputs $x_1, x_2, \ldots, x_N$ being from an arbitrary set), we know that the maximum success probability of players can be described by a semidefinite program [Cir80] and, hence, can be calculated in polynomial time [CHTW04]. In contrast, computing the classical success probability is NP-hard.

For XOR games with more than two players, examples of specific games providing a quantum advantage are known [Mer90, Ard92, PWP$^+$08, BV12] and there is some theory in the framework of Bell inequalities [WW01a, WW01b, ZB02]. This theory, however, often focuses on questions other than computing classical and quantum winning probabilities — which is our main interest.

4.3 What we study here

In this part, we consider a restricted case of symmetric multiplayer XOR games. We shall study mainly those games, where each player should receive exactly one bit of input and answer exactly one bit of output, and is allowed to operate with one qubit of N-qubit quantum system. For this restricted case, we show that both classical and quantum winning probabilities can be easily calculated.

Werner and Wolf [WW01a] speaking about nonlocal games in terms of set of Bell inequalities, show that maximal violation of these inequalities can be achieved by using maximal entanglement. That is, the biggest effect is achieved when using maximally entangled state $|GHZ\rangle = \frac{1}{\sqrt{2}}|00\ldots0\rangle + \frac{1}{\sqrt{2}}|11\ldots1\rangle$ or equal states up to local unitary operations. When studying nonlocal games and having the similar interests, we'll also concentrate mainly on the case when players share a quantum system in state $|GHZ\rangle$.

In Chapter 5 we perform some analysis of optimal strategies for both classical and quantum versions of nonlocal XOR games. Namely, we specify relatively small subsets, which with certainty contain optimal strategies. These methods allow to perform both very efficient numerical and analytical investigations of such games.

In Chapter 6 we develop techniques (based on the results of Chapter 5) for evaluation of a random symmetric nonlocal XOR game. This analysis shows that for almost all such games the use of entangled quantum system allows players to improve their outcomes significantly.

In Chapter 7 we describe similar results (but obtained by using totally different techiques) for random two-player nonlocal XOR games. We follow that almost all such games show quantum-over-classical advantage which is comparable to the maximum possible advantage for this class of nonlocal games.

In Chapter 8 we apply our methods for analysis of symmetric nonlocal games to the particular case of Mermin-Ardehali's inequality [Mer90, Ard92]. The results coincide with [Ard92] but are obtained using different methods (which are more combinatorial in their nature). The advantage of our methods is that they can be easily applied to any symmetric XOR game while those of [Ard92] are tailored to the particular XOR game.

Finally, in Chapter 9 we apply a similar technique for analyzing the generalized version of CHSH game, where referee's choice is not restricted with uniform input distribution. Some subset of the results coincide with [LLP10], as the classes of games being analyzed here and in [LLP10] partially overlap. But again, we use different methods and have slightly different purposes.

4.4 Formalism of XOR games

A nonlocal N-player game is defined by a sequence of 2^N elements $[(I_{00\ldots0}, I_{00\ldots1}, \ldots, I_{11\ldots1})]$, where each element corresponds to some of 2^N inputs and describes all right answers for this input: $I_{x_1\ldots x_N} \subseteq \{0,1\}^N$. Players receive a uniformly random input $x_1, \ldots, x_N \in \{0,1\}$ with the i^{th} player receiving x_i. The i^{th} player then produces an output $y_i \in \{0,1\}$. No communication is allowed between the players but they can use shared randomness (in the classical case) or quantum entanglement (in the quantum case). Players win if $y_1 y_2 \ldots y_N \in I_{x_1 x_2 \ldots x_N}$ and lose otherwise.

For each $I_{x_1 x_2 \ldots x_N}$, there are 2^{2^N} possible values. Therefore, there are $\left(2^{2^N}\right)^{\left(2^N\right)} = 2^{2^{2N}}$ different games. This means 65536 games for $N = 2$, $\approx 1.8 \cdot 10^{19}$ games for $N = 3$ and practically not enumerable for $N > 3$.

We shall concentrate on that games, which are symmetrical with respect to permuting the players and whose outcome depends only on parity of the sum of the output (or Hamming weight of the output), i.e. on $XOR\,(|OUTPUT|)$. (Actually, this decision was based not on strict analytics, but rather on the results of numerical experiments: XOR games seem to be the most interesting in their quantum versions. See Section 6.2 for illustration of this fact.)

Each such XOR game can be described as a string of $N+1$ bits: $\Gamma_0 \Gamma_1 \ldots \Gamma_N$, where each bit Γ_i represents the correct right parity of the output sum in the case when the sum of input is i. Typical and important XOR game is the CHSH game: in our terms it can be defined as $\Gamma_0 \Gamma_1 \Gamma_2 = \text{“}{+}{+}{-}\text{”}$ (that is, an even answer if $|INPUT| = 0$ or 1 and an odd answer if $|INPUT| = 2$).

Chapter 5

Optimal Strategies for Symmetric XOR Games

5.1 Normalized classical strategies

In their classical versions XOR games are a good object for analysis and in most cases turn out to have a little outcome for players.

Imagine a classical version of XOR game, for which we want to find optimal classical strategies for players. Each player has 4 different choices: (00), (01), (10), (11); (where the first bit represents the answer to input 0, and the second bit represents the answer to input 1. Thus, (ab) denotes a choice to answer a to input 0 and to answer b to input 1).

Definition 5.1 (Classical normalized strategy) *A classical normalized strategy for N-player XOR game is one of the following* $2N+2$ *choice sequences:*

$$\begin{aligned}&(00)^{N-k}\ \ (01)^{k}\\&(00)^{N-1}\ \ (11)\\&(00)^{N-k}\ \ (01)^{k-1}\ \ (10)\,,\end{aligned}$$

where $k \in \{0, 1, \ldots N\}$*.*

Theorem 5.1 *[AKNR10] For any classical strategy for an N-player XOR game there exists a normalized strategy, such that these strategies on equal input answer equal parity.*

Proof:

First of all, remember, that we consider only symmetrical games with respect to players permutation. Therefore, we always will order players by their choices.

The second step is choice inversion for a pair of players. If we take any pair of choices and invert both of them, the parity of the output will not change. Thus, we can find the following pairs of choices and make the corresponding inversions:

$$\begin{aligned}(11)\ (11) &\to (00)\ (00)\\ (11)\ (10) &\to (00)\ (01)\\ (11)\ (01) &\to (00)\ (10)\\ (10)\ (10) &\to (01)\ (01)\end{aligned}$$

If it is impossible to find such pair, there is clearly no more than one choice from the set $\{(10)\,,\ (11)\}$, and presence of choice (11) follows that all other choices are (00). In other words, this strategy is normalized. $\square$

This trick allows very efficient search for an optimal strategy for classical version of a symmetric XOR game. Strategy of form

$$(00)^{N-k}\ (01)^k$$

has mean outcome

$$\mathit{Outcome}\left((00)^{N-k}\ (01)^k\right) = \frac{1}{2^N}\sum_{i=0}^{N}\sum_{j=0}^{i}(-1)^j\,\Gamma_i\binom{N-k}{i-j}\binom{k}{j}$$

(variable i here stands for the number of 1s in the input data, and variable j denotes the number of 1s given to the (01)-choice players).

All other normal strategies has mean outcomes computable as

$$\begin{aligned}\mathit{Outcome}\left((00)^{N-1}\ (11)\right) &= -\mathit{Outcome}\left((00)^N\right)\\ \mathit{Outcome}\left((00)^{N-k}\ (01)^{k-1}\ (10)\right) &= -\mathit{Outcome}\left((00)^k\ (01)^{N-k}\right).\end{aligned}$$

Indeed, given some game and some input data for players, whenever a strategy from the left side of an equality above wins the game, the corresponding strategy from the right side of the equality loses, and vice versa. These two equalities demonstate the fact that each normalized strategy has its sibling with the last players's choice bitwise inverted and with value of the mean outcome negated. From now on, we consider such pairs of strategies S and $\overline{S}$ together with a positive value of the mean outcome

$$|Outcome\,(S)| = \left|Outcome\left(\overline{S}\right)\right|.$$

In fact, the most useful strategies are $(00)^N$ and $(01)^N$. In our computer experiments, one of these strategies is optimal for $\approx 99\%$ symmetric XOR games. Our rigorous results in the next chapter imply that asymptotically (in the limit of large N) the fraction of games for which one of these symmetric strategies is optimal is $1 - o\,(1)$.

5.2 Optimal quantum strategies

Consider a possibly non-symmetric XOR game. Let $x_1, x_2, \ldots, x_N$ be the inputs to the players. Define $G_{x_1,x_2,\ldots,x_N} = 1$ if, to win for these inputs, players must output $y_1, y_2, \ldots, y_N$ with XOR being 1 and $G_{x_1,x_2,\ldots,x_N} = -1$ if players must output $y_1, y_2, \ldots, y_N$ with XOR being 0.

Werner and Wolf [WW01a, WW01b] have shown that, for any strategy in quantum version of an XOR game, its bias (the difference between the winning probability $\Pr_{win}$ and the losing probability $\Pr_{los}$) is equal to

$$f\,(\lambda_1, \lambda_2, \ldots, \lambda_N) = \left| \frac{1}{2^N} \sum_{x_1,x_2,\ldots,x_N \in \{0,1\}} G_{x_1,x_2,\ldots,x_N} \lambda_1^{x_1} \lambda_2^{x_2} \ldots \lambda_N^{x_N} \right| \tag{5.1}$$

for some $\lambda_1, \lambda_2, \ldots, \lambda_N$ satisfying $|\lambda_1| = |\lambda_2| = \ldots = |\lambda_N| = 1$. Conversely, for any such $\lambda_1, \lambda_2, \ldots, \lambda_N$, there is a winning strategy with the bias being $f\,(\lambda_1, \lambda_2, \ldots, \lambda_N)$.

Theorem 5.2 *[AKNR10] For symmetric XOR games, the maximum of $f\,(\lambda_1, \lambda_2, \ldots, \lambda_N)$ is achieved when $\lambda_1 = \lambda_2 = \ldots = \lambda_N$.*

Proof: We fix all but two of λ_i. To simplify the notation, we assume that $\lambda_3, \ldots, \lambda_N$ are the variables that have been fixed. Then, (5.1) becomes

$$a + b\lambda_1 + c\lambda_2 + d\lambda_1\lambda_2$$

for some a, b, c, d. Because of symmetry, we have $b = c$. Thus, we have to maximize

$$a + b\left(\lambda_1 + \lambda_2\right) + d\lambda_1\lambda_2. \tag{5.2}$$

Let $\lambda_1 = e^{i\theta_1}$ and $\lambda_2 = e^{i\theta_2}$. Let $\theta_+ = \dfrac{\theta_1 + \theta_2}{2}$ and $\theta_- = \dfrac{\theta_1 - \theta_2}{2}$. Then, (5.2) becomes $a + be^{i\theta_+}\left(e^{i\theta_-} + e^{-i\theta_-}\right) + de^{2i\theta_+} = A + B\cos\theta_-$ where $A = a + de^{2i\theta_+}$ and $B = 2be^{i\theta_+}$. If we fix θ_+, we have to maximize the expression $A + Bx$, $x \in [-1, 1]$. For any complex A, B, $A + Bx$ is either maximized by $x = 1$ (if the angle between A and B as vectors in the complex plane is at most $\frac{\pi}{2}$) or by $x = -1$ (if the angle between A and B is more than $\frac{\pi}{2}$). If $x = 1$, we have $\lambda_1 = \lambda_2 = \theta_+$. If $x = -1$, we have $\lambda_1 = \lambda_2 = -\theta_+$.

Thus, if $\lambda_1 \neq \lambda_2$, then the value of (5.1) can be increased by keeping the same $\theta_+ = \dfrac{\theta_1 + \theta_2}{2}$ but changing λ_1 and λ_2 so that they become equal. The same argument applies if $\lambda_i \neq \lambda_j$. $\square$

Thus, we can find the value of a symmetric XOR game by maximizing

$$f\left(\lambda\right) = \left|\frac{1}{2^N}\sum_{k=0}^{N}\binom{N}{k}\Gamma_k\lambda^k\right|. \tag{5.3}$$

The maximal $f\left(\lambda\right)$ is the maximum possible gap $\Pr_{win} - \Pr_{los}$ between the winning probability $\Pr_{win}$ and the losing probability $\Pr_{los}$. We have $\Pr_{win} = \dfrac{1 + f\left(\lambda\right)}{2}$ and $\Pr_{los} = \dfrac{1 - f\left(\lambda\right)}{2}$.

Chapter 6

Random Symmetric XOR Games

6.1 Introduction

Interest in studying symmetric XOR games was initially raised after the series of computer experiments indicating significant difference between classical and quantum versions of such games [AKNR10, AKN$^+$13]. As we shall see in the next sections, the difference in favor of "quantum" players is inherent among the vast majority of symmetric XOR games.

This chapter is dedicated entirely to the analysis of asymptotic behavior of the "classical" and "quantum" expected values of a random N-player XOR game.

We obtain a tight bound for the classical case and provide numerical evidence that quantum players can achieve better results.

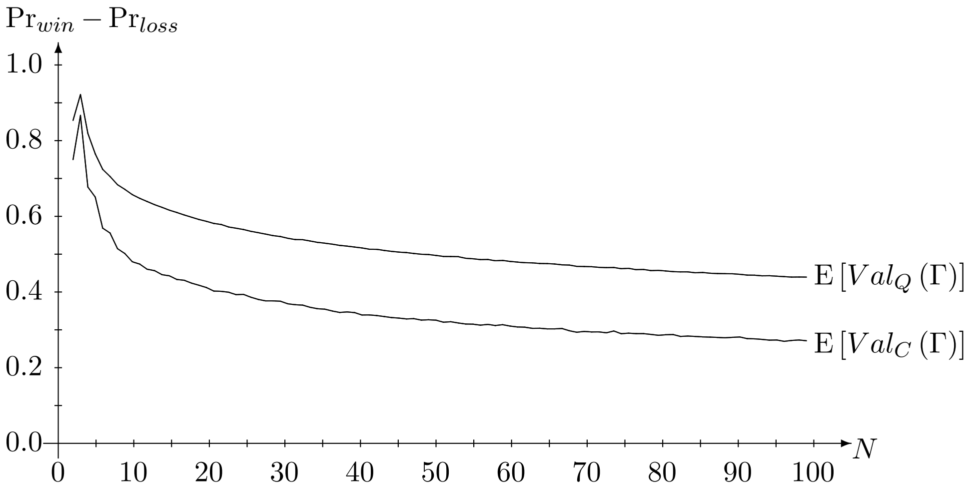
6.2 Computer experiments

In order to visualize the matter let us first represent the "behavior" of symmetric XOR games for different numbers of players.

Figure 6.1 shows the expected classical and quantum values for a randomly chosen symmetric XOR game with binary inputs, with the number of players N ranging between 2 and 101 [1].

[1]For $N \leq 16$ the graphs are precise, as for small number of players it was possible to analyze all 2^{N+1}

Figure 6.1: Expected values of quantum and classical XOR games



We see that there is a consistent quantum advantage for all N, and the question about the further behavior of these two graphs arises very naturally.

In the Figure 6.2, we provide some statistical data on the distribution of the game values (from 10^6 randomly selected games for $N = 64$). The first two histograms show the distribution of classical and quantum values, respectively. The last one shows the distribution of biases between the values of classical and quantum versions of a game.

We see that the quantum value of a game is more sharply concentrated than the classical value. There is a substantial number (around 30%) of games which have no quantum advantage (or almost no quantum advantage) [2]. For the remaining games, the gap between quantum and classical values is quite uniformly distributed over a large interval.

These results however are obtained by using numerical techniques and lack some theoretical ground.

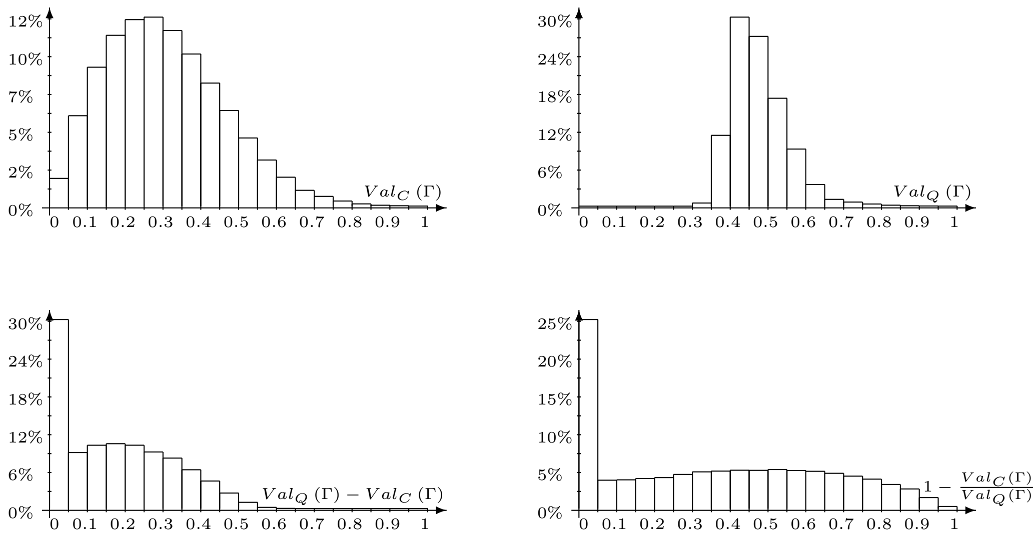
6.3 Some analysis of normalized strategies

In order to make a performance evaluation of classical strategies, let us analyze some statistical properties of each normalized strategy. Now we shall calculate the variance

games.

[2] However, our results in the next sections indicate that the fraction of such games will tend to 0 for larger N.

Figure 6.2: Histograms of 64-player games' values



of the mean outcome produced by a normalized strategy for a randomly chosen game.

We first consider the strategy $(00)^N$. As all players always answer 0, the mean outcome of this strategy is equal to

$$\left|Outcome\left((00)^N\right)\right| = \left|\sum_{j=0}^{N} \frac{\Gamma_j \binom{N}{j}}{2^N}\right| \tag{6.1}$$

For the strategy $(01)^N$, we have

$$\left|Outcome\left((01)^N\right)\right| = \left|\sum_{j=0}^{N} \frac{(-1)^j\, \Gamma_j \binom{N}{j}}{2^N}\right| \tag{6.2}$$

Since the variance of a sum is equal to the sum of variances of the summands, for both values (6.1) and (6.2) we have equal variances

$$\begin{aligned} \operatorname{Var}\left[\left|Outcome\left((00)^N\right)\right|\right] &= \operatorname{Var}\left[\left|Outcome\left((01)^N\right)\right|\right] \\ &= \operatorname{Var}\left[\sum_{j=0}^{N} \frac{\pm\binom{N}{j}}{2^N}\right] = \sum_{j=0}^{N} \operatorname{Var}\left[\frac{\pm\binom{N}{j}}{2^N}\right] = \sum_{j=0}^{N} \left(\frac{\binom{N}{j}}{2^N}\right)^2 = \frac{\binom{2N}{N}}{4^N}. \end{aligned}$$

Equity of these two variances could be also shown in the following way: $Outcome\left((00)^N\right)$ for the game $\Gamma_0\Gamma_1\Gamma_2\Gamma_3\Gamma_4\ldots$ is exactly the same as $Outcome\left((01)^N\right)$

for the game $\Gamma_0\overline{\Gamma_1}\Gamma_2\overline{\Gamma_3}\Gamma_4\ldots$, with all odd bits inverted.

More generally, assume that we have a strategy $(00)^k\,(01)^{N-k}$. We can invert the answers by all players for the case $x_i = 1$ (that is, substitute choices (00) with (01) and vice versa). Then, the overall parity of answers $\oplus_{i=1}^{N} y_i$ stays the same if an even number of players have received $x_i = 1$ and changes to opposite value if an odd number of players have received $x_i = 1$. If we simultaneously invert all odd-numbered bits Γ_i in the winning condition, the mean outcome does not change. From this, we conclude that for each k,

$$Outcome\left((00)^k\,(01)^{N-k}\right) = Outcome\left((00)^{N-k}\,(01)^k\right). \tag{6.3}$$

We now consider the value for the second strategy from Definition 5.1, $(00)^{N-1}\,(01)$, for a random symmetric XOR game.

Probability distributions of $\oplus_{i=0}^{N} y_i$ when $\sum_{i=0}^{N} x_i = j$ are listed in Table 6.1.

Table 6.1: Probability distributions for strategy $(00)^{N-1}\,(01)$

j	0	1	2	3	4	5	6	7	$\ldots$
$\Pr\left[\oplus_{i=0}^{N} y_i = 0\right]$	1	$\frac{1}{N}$	$\frac{N-2}{N}$	$\frac{3}{N}$	$\frac{N-4}{N}$	$\frac{5}{N}$	$\frac{N-6}{N}$	$\frac{7}{N}$	$\ldots$
$\Pr\left[\oplus_{i=0}^{N} y_i = 1\right]$	0	$\frac{N-1}{N}$	$\frac{2}{N}$	$\frac{N-3}{N}$	$\frac{4}{N}$	$\frac{N-5}{N}$	$\frac{6}{N}$	$\frac{N-7}{N}$	$\ldots$

Given input with $\sum_{i=0}^{N} x_i = j$, the strategy outputs even or odd answer, depending on whether or not the last player has received 1, i.e. with probabilities $\frac{N-j}{N}$ and $\frac{j}{N}$ (unlike 1 and 0 in the case of symmetric strategies).

Therefore, the variance of the mean outcome of the strategy $(00)^{N-1}\,(01)$ for input with $\sum_{i=0}^{N} x_i = j$ is $\left(\frac{N-j}{N} - \frac{j}{N}\right)^2 = \left(\frac{N-2j}{N}\right)^2$.

Summing up the variances for all possible j's, we get

$$\begin{aligned} \mathrm{Var}\left[Outcome\left((00)^{N-1}\,(01)\right)\right] &= \sum_{j=0}^{N} \mathrm{Var}\left[\frac{\pm\frac{N-2j}{N}\binom{N}{j}}{2^N}\right] \\ &= \sum_{j=0}^{N}\left(\frac{\pm\frac{N-2j}{N}\binom{N}{j}}{2^N}\right)^2 = \frac{\binom{2N}{N}}{4^N\,(2N-1)} \approx \frac{1}{\sqrt{\pi N}\,(2N-1)}, \end{aligned} \tag{6.4}$$

with the third equality following from Lemma 6.1, which we prove below (notation $\pm\frac{N-2j}{N}$ denotes a random variable with equiprobable values $+\frac{N-2j}{N}$ and $-\frac{N-2j}{N}$).

Due to (6.3), the value of strategy $(00)\,(01)^{N-1}$ has the same variance.

Lemma 6.1

$$\sum_{j=0}^{N}\left(\frac{N-2j}{N}\binom{N}{j}\right)^2=\frac{\binom{2N}{N}}{2N-1}$$

Proof:

$$\begin{aligned}
&\sum_{j=0}^{N}\left(\frac{N-2j}{N}\binom{N}{j}\right)^2\\
&=\sum_{j=0}^{N}\left(1-4\frac{j}{N}+4\frac{j^2}{N^2}\right)\binom{N}{j}^2\\
&=\sum_{j=0}^{N}\binom{N}{j}^2-4\sum_{j=1}^{N}\binom{N-1}{j-1}\binom{N}{j}+4\sum_{j=1}^{N}\binom{N-1}{j-1}^2\\
&=\binom{2N}{N}-4\binom{2N-1}{N-1}+4\binom{2N-2}{N-1}\\
&=\binom{2N}{N}-2\binom{2N}{N}+\frac{2N}{2N-1}\binom{2N}{N}\\
&=\frac{\binom{2N}{N}}{2N-1}
\end{aligned}$$

□

Other strategies of type $(00)^{N-k}\,(01)^k$ where $2\le k\le N-2$ have much smaller variances, which can be expressed as follows:

$$\begin{aligned}
\operatorname{Var}\left[Outcome\left((00)^{N-k}\,(01)^k\right)\right]&=\sum_{j=0}^{N}\left(\frac{\left(\sum_{l=0}^{j}(-1)^l\,\frac{\binom{k}{l}\binom{N-k}{j-l}}{\binom{N}{j}}\right)\binom{N}{j}}{2^N}\right)^2\\
&=\frac{\sum_{j=0}^{N}\left(\sum_{l=0}^{j}(-1)^l\binom{k}{l}\binom{N-k}{j-l}\right)^2}{4^N}.
\end{aligned}\qquad(6.5)$$

The expression $\sum_{l=0}^{j}(-1)^l\binom{k}{l}\binom{N-k}{j-l}$ inside (6.5) is the well known Kravchuk polynomial $K_j\,(k)$, whose square can be bounded by the strict inequality provided in [Kra01]:

$$\left(\sum_{l=0}^{j}(-1)^l\binom{k}{l}\binom{N-k}{j-l}\right)^2=(K_j\,(k))^2<2^N\binom{N}{j}\binom{N}{k}^{-1}.\qquad(6.6)$$

This inequality implies that

$$\begin{aligned}\operatorname{Var}\left[Outcome\left((00)^{N-k}(01)^{k}\right)\right] &= \frac{\sum_{j=0}^{N}\left(K_j(k)\right)^2}{4^N} \\ &< \frac{\sum_{j=0}^{N} 2^N \binom{N}{j}\binom{N}{k}^{-1}}{4^N} = \binom{N}{k}^{-1}.\end{aligned} \tag{6.7}$$

6.4 Symmetric classical strategies

Let us now obtain a tight bound on the value of strategies $(00)^N$ and $(01)^N$.

Theorem 6.2 *[AIKV12] For a random N-player symmetric XOR game with binary inputs,*

$$\mathrm{E}\left[\max\left(\left|Outcome\left((00)^N\right)\right|, \left|Outcome\left((01)^N\right)\right|\right)\right] = \frac{0.8475\ldots + o(1)}{\sqrt[4]{N}}. \tag{6.8}$$

Proof:

We need to find a bound for the maximum of (6.1) and (6.2):

$$\mathrm{E}\left[\max\left(\left|Outcome\left((00)^N\right)\right|, \left|Outcome\left((01)^N\right)\right|\right)\right]$$

$$= \mathrm{E}\left[\max\left(\left|\sum_{j=0}^{N}\frac{\Gamma_j\binom{N}{j}}{2^N}\right|, \left|\sum_{j=0}^{N}\frac{(-1)^j\,\Gamma_j\binom{N}{j}}{2^N}\right|\right)\right].$$

Among the summands of (6.1) and (6.2) let us first evaluate those which are equal for both of the sums, i.e. for even j's, and then for remaining summands, which have opposite values in the sums, i.e. for odd j's:

$$\mathrm{E}\left[\max\left(\left|Outcome\left((00)^N\right)\right|, \left|Outcome\left((01)^N\right)\right|\right)\right]$$

$$= \mathrm{E}\left[\max\left(\pm \sum_{\substack{0\le j\le N,\\ j \text{ is even}}} \frac{\Gamma_j \binom{N}{j}}{2^N} \pm \sum_{\substack{0\le j\le N,\\ j \text{ is odd}}} \frac{\Gamma_j \binom{N}{j}}{2^N}\right)\right]$$

$$= \mathrm{E}\left[\sum_{\substack{0\le j\le N,\\ j \text{ is even}}} \frac{\Gamma_j \binom{N}{j}}{2^N}\right] + \mathrm{E}\left[\sum_{\substack{0\le j\le N,\\ j \text{ is odd}}} \frac{\Gamma_j \binom{N}{j}}{2^N}\right] \tag{6.9}$$

Let Σ_{even} and Σ_{odd} be the two sums in (6.9). Then, we have

$$\mathrm{Var}\left[\Sigma_{even}\right] = \sum_{\substack{0\le j\le N,\\ j \text{ is even}}} \left(\frac{\binom{N}{j}}{2^N}\right)^2 = \frac{\binom{2N}{N}}{2\cdot 4^N}.$$

Similarly, $\mathrm{Var}\left[\Sigma_{odd}\right] = \frac{\binom{2N}{N}}{2\cdot 4^N}$. From the central limit theorem, in the limit of large N, each of random variables Σ_{even} and Σ_{odd} can be approximated by a normally distributed random variable with the same mean (which is 0) and variance. If X is a normally distributed random variable with $\mathrm{E}\left[X\right] = 0$, then $\mathrm{E}\left[|X|\right] = \sqrt{\frac{2}{\pi}}\sqrt{\mathrm{Var}\left[X\right]}$. Hence, (6.9) is equal to

$$\begin{aligned}
\mathrm{E}\left[|\Sigma_{even}|\right] + \mathrm{E}\left[|\Sigma_{odd}|\right] &= \sqrt{\frac{2}{\pi}}\left(1+o\left(1\right)\right)\sqrt{\mathrm{Var}\left[\Sigma_{even}\right]} + \sqrt{\frac{2}{\pi}}\left(1+o\left(1\right)\right)\sqrt{\mathrm{Var}\left[\Sigma_{odd}\right]} \\
&= \left(1+o\left(1\right)\right)\sqrt{\frac{2}{\pi}}\sqrt{\frac{\binom{2N}{N}}{2\cdot 4^N}} \times 2 \\
&= \left(1+o\left(1\right)\right)\sqrt[4]{\frac{16}{\pi^3}}\frac{1}{\sqrt[4]{N}} \\
&= \frac{0.8475\ldots + o\left(1\right)}{\sqrt[4]{N}},
\end{aligned}$$

where the third equality follows from the approximation of the binomial coefficients $\binom{2N}{N} = (1+o(1))\frac{4^N}{\sqrt{\pi N}}$. $\square$

6.5 Asymmetric classical strategies

In this section we show that with a high probability an asymmetric strategy of type $(00)^k (01)^{N-k}$ gives a weaker result than one provided in Theorem 6.2.

Theorem 6.3 *[AIKV12] For any $c > 0$,*

$$\Pr\left[\max_{k:1\le k\le N-1}\left|Outcome\left((00)^k (01)^{N-k}\right)\right| \ge \frac{c}{\sqrt[4]{N}}\right] = O\left(\frac{1}{N}\right). \tag{6.10}$$

Proof:

Among the strategies $(00)^k (01)^{N-k}$, $k \in \{1,\ldots,N-1\}$, two strategies (for $k=1$ and $k=N-1$) have variance $\approx \frac{1}{\sqrt{\pi N}(2N-1)}$ (due to (6.4)), and the remaining $N-3$ strategies have variance less than $\frac{1}{\binom{N}{k}}$ (due to (6.6)).

We now apply Chebyshev's inequality, using those two bounds on the variance. We have

$$\begin{aligned}&\Pr\left[\left|Outcome\left((00)^{N-1}(01)\right)\right| \ge \frac{\lambda}{\sqrt[4]{\pi N}\sqrt{2N-1}}\right]\\ &= \Pr\left[\left|Outcome\left((00)(01)^{N-1}\right)\right| \ge \frac{\lambda}{\sqrt[4]{\pi N}\sqrt{2N-1}}\right] \le \frac{1}{\lambda^2},\end{aligned} \tag{6.11}$$

and, for $2 \le k \le N-2$:

$$\Pr\left[\left|Outcome\left((00)^{N-k}(01)^k\right)\right| \ge \frac{\lambda}{\sqrt{\binom{N}{k}}}\right] \le \frac{1}{\lambda^2}. \tag{6.12}$$

We now combine the bounds (6.11) and (6.12) into one upper bound.

$$\begin{aligned}&\Pr\left[\max_{1\le k\le N-1}\left|Val\left((00)^{N-k}(01)^k\right)\right| \ge B\right] \le\\ &\le 2\times\frac{1}{\left(B\sqrt[4]{\pi N}\sqrt{2N-1}\right)^2} + \sum_{k=2}^{N-2}\frac{1}{\left(B\sqrt{\binom{N}{k}}\right)^2}\\ &= \frac{2}{B^2\sqrt{\pi N}(2N-1)} + O\left(\frac{1}{B^2N^3}\right),\end{aligned} \tag{6.13}$$

with the last equality following from $\binom{N}{k} \geq \binom{N}{2}$ and the fact that we are summing over $N-3$ values for k: $k \in \{2, \ldots, N-2\}$. Taking $B = \frac{c}{\sqrt[4]{N}}$ completes the proof. $\square$

6.6 Cumulative classical bound

In order to combine the results of Theorems 6.2 and 6.3, we can just substitute the constant c from (6.10) with constant $0.8475\ldots + o(1)$ from (6.8) and follow the inequality:

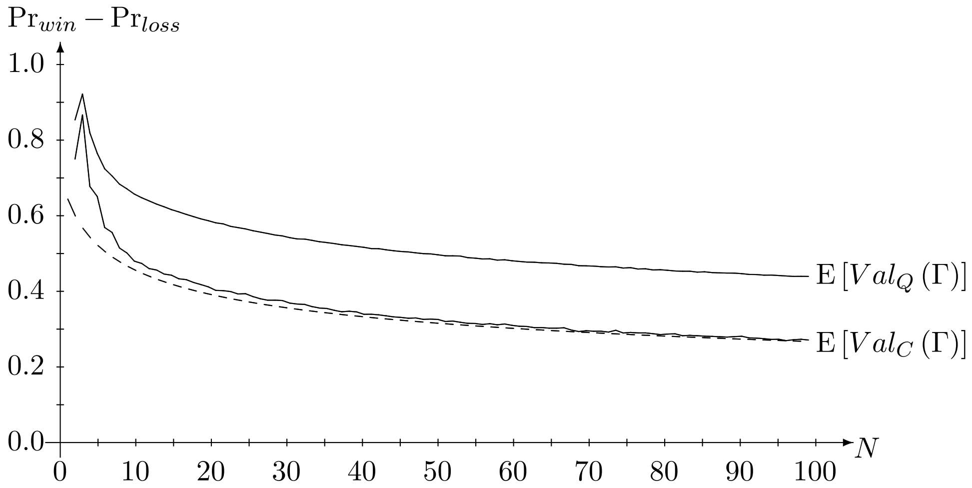
$$\begin{aligned} &\mathrm{E}\left[\max_k \left|Outcome\left((00)^k (01)^{N-k}\right)\right|\right] \\ &\quad\leq \frac{0.8475\ldots + o(1)}{\sqrt[4]{N}} + \Pr\left[\max_{k:1\leq k\leq N-1} \left|Outcome\left((00)^k (01)^{N-k}\right)\right| \geq \frac{0.8475\ldots + o(1)}{\sqrt[4]{N}}\right] \\ &\quad\leq \frac{0.8475\ldots + o(1)}{\sqrt[4]{N}} + O\left(\frac{1}{N}\right) = \frac{0.8475\ldots + o(1)}{\sqrt[4]{N}}. \end{aligned}$$

Thus, expected value (6.8) turns out to be also a tight bound for the expected value of a random classical symmetric XOR game:

$$\mathrm{E}\left[Val_C(\Gamma)\right] = \mathrm{E}\left[\max_k \left|Outcome\left((00)^k (01)^{N-k}\right)\right|\right] = \frac{0.8475\ldots + o(1)}{\sqrt[4]{N}}.$$

Let us now reillustrate Figure 6.1 together with this bound:

Figure 6.3: Expected values of quantum and classical XOR games + classical bound



6.7 Quantum bound

Next we turn to the quantum case. Due to the result proven in Section 5.2, we must evaluate

$$\mathrm{E}\left[Val_Q(\Gamma)\right] = \mathrm{E}\left[\max_{|\lambda|=1}\left|\sum_{k=0}^{N}\frac{\binom{N}{k}\Gamma_k\lambda^k}{2^N}\right|\right],$$

which is the mean value of a random game in quantum case.

So far, we have not been able to find a tight lower for this value. However, we provide some insights which could lead to a solution to the problem. We can bound the value from below by

$$\max_{|\lambda|=1}\left|\sum_{k=0}^{N}\frac{\binom{N}{k}\Gamma_k\lambda^k}{2^N}\right| \geq \max_{\alpha}\left|\sum_{k=0}^{N}\frac{\binom{N}{k}\Gamma_k\cos(k\alpha)}{2^N}\right| \tag{6.14}$$

The sum $\sum_{k=0}^{N} c_k\cos(k\alpha)$ where c_k are indepedent random variables with mean 0 and variance 1 has been being extensively studied over several decades under the name "*random trigonometric polynomials*" [SZ54, Hal73, Kas87, BL01]. Famous result of [SZ54] imply that there exist constants A and B such that

$$\lim_{M\to\infty}\Pr\left[A\sqrt{M\log M} \leq \max_{\alpha}\left|\sum_{k=0}^{M} c_k\cos(k\alpha)\right| \leq B\sqrt{M\log M}\right] = 1. \tag{6.15}$$

To apply (6.15), the crucial step is to reduce a sum of $\binom{N}{k}c_k\cos(k\alpha)$ with binomial coefficients to a sum of $c_k\cos(k\alpha)$ not containing binomial coefficients.

We propose the following non-rigorous approximation. We first drop the terms with $k \in \left[0, \frac{N}{2}-\sqrt{N}\right) \cup \left(\sqrt{N}+\frac{N}{2}, N\right]$. For the remaining terms, we replace $\binom{N}{j}$ with $\binom{N}{N/2}$ (since $\binom{N}{k} = \Theta\left(\binom{N}{N/2}\right)$ for $k \in \left[\frac{N}{2}-\sqrt{N}, \frac{N}{2}+\sqrt{N}\right]$). If this approximation can be justified, it reduces (6.14) to (6.15) with $M = 2\sqrt{N}$. This would lead to a lower bound of $\mathrm{E}\left[Val_Q(\Gamma)\right] = \Omega\left(\frac{\sqrt{\log M}}{\sqrt{M}}\right) = \Omega\left(\frac{\sqrt{\log N}}{\sqrt[4]{N}}\right)$.

Chapter 7

Random XOR Games for Two Players

7.1 Introduction

In Chapter 6 we illustrated a contribution that N entangled qubits can bring to interaction abilities of N players being apart from each other.

Yet another setting is in relevance to this topic. Let us modify the general rules of the game by allowing communication between some players. We then can figure out N' groups of players, such that inside every group players are allowed to communicate. One can observe such games just as N'-player games, where each player receives some predefined amount of bits and must answer with the same amount of bits.

The simplest nontrivial class of such games consists of games with $N' = 2$ (games with $N' = 1$ obviously are trivial, and games with $N' > 2$ are NP-hard to compute [KKM$^+$08]). Such two-player games are extensively studied in a number of papers. E.g. Buhrman et al. [BRSW11] construct a 2-player quantum game where the players receive numbers x_1, x_2 and answer with numbers y_1, y_2 ($x_1, x_2 \in \{1, \ldots, n\}$); the classical value of this game is $\frac{1}{2} + \Theta\left(\frac{1}{\sqrt{n}}\right)$ while the quantum value is 1. In contrast, Almeida et al. [ABB$^+$10] construct a non-trivial example of a game in which quantum strategies provide no advantage at all. We still do not know which of those two examples is the typical for two-player nonlocal games.

In this light nonlocal XOR games are of particular interest. Detailed analysis of two-player XOR games can be found in [CHTW04]. In this chapter we shall also concentrate on two-player symmetric XOR games. It turns out that quantum values of these games typically are significantly bigger than classical ones. All details can be found in [ABB+12], and in this chapter we shall just provide the main results.

7.2 Formalism

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 $P(i, j, x \oplus y)$.

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, $x \neq y$).

7.3 Results

7.3.1 Preliminaries

Let p_{ij} be the probability that the referee sends question i to player A and question j to player B. Then, by [CHTW04, section 5.3], the classical value of the game is equal to

$$\Delta_c = \max_{u_1, \ldots, u_n \in \{-1,1\}} \max_{v_1, \ldots, v_n \in \{-1,1\}} \sum_{i=1}^{n} \sum_{j=1}^{n} p_{ij} A_{ij} u_i v_j. \quad (7.1)$$

In the quantum case, Tsirelson's theorem [Cir80] implies that

$$\Delta_q = \max_{\|u_i\|=1} \max_{\|v_j\|=1} \sum_{i,j=1}^{n} p_{ij} A_{ij} \langle u_i, v_j \rangle \tag{7.2}$$

where the maximization is over all tuples of unit-length vectors $u_1, \ldots, u_n \in \mathbb{R}^d$, $v_1, \ldots, v_n \in \mathbb{R}^d$ (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_c and Δ_q for the case when A is a random Bernoulli matrix (i.e., each entry A_{ij} is $+1$ with probability $\frac{1}{2}$ and -1 with probability $\frac{1}{2}$, independently of other entries).

In [ABB+12] three bounds are proven: upper and lower bounds for Δ_c and one explicit bound for Δ_q.

7.3.2 Quantum bound

Theorem 7.1 *[ABB+12] For a random 2-player XOR game with n inputs for each player,*

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

with probability $1 - o(1)$.

This theorem relies on two facts for building upper and lower bounds for Δ_q.

One fact about operator norms of random matrices from [Tao11] implies that $\|A\| = (2 + o(1)) \sqrt{n}$ with a high probability, and consequently, the upper bound for Δ_q follows from the following inequality:

$$\sum_{i=1}^{n} \sum_{j=1}^{n} A_{ij} \langle u_i, v_j \rangle = \langle u, (A \otimes I) v \rangle \leq \|u\| \cdot \|A \otimes I\| \cdot \|v\| \leq \|A\| n = (2 + o(1)) n^{3/2}.$$

Another fact is derived similarly to the Marchenko-Pastur law [MP67] in random matrix theory, which bounds the number of big singular values for random $n \times n$ matrix with elements from $\{-1, 1\}$. In a similar manner one can bound (by $O\left(\frac{1}{n}\right)$) the number of long vectors

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

where l_i and r_i are respectively left and right singular vectors of matrix A (so that $Ar_i = \lambda_i l_i$). Zeroizing these long vectors and normalizing all remaining vectors result in $u'_1, \ldots, u'_n, v'_1, \ldots, v'_n$ with norms ≤ 1, such that $\sum_{i=1}^{n} \sum_{j=1}^{n} A_{ij} \langle u'_i, v'_j \rangle \geq (2 - o(1))\, n^{3/2}$. And this naturally implies the lower bound for Δ_q, since

$$\max_{\|u_i\|=\|v_j\|=1} \sum_{i=1}^{n} \sum_{j=1}^{n} A_{ij} \langle u_i, v_j \rangle = \max_{\|u_i\|\leq 1, \|v_j\|\leq 1} \sum_{i=1}^{n} \sum_{j=1}^{n} A_{ij} \langle u_i, v_j \rangle \geq \sum_{i=1}^{n} \sum_{j=1}^{n} A_{ij} \langle u'_i, v'_j \rangle.$$

7.3.3 Classical bound

Theorem 7.2 *[ABB+12] For a random 2-player XOR game, its classical value Δ_c satisfies*

$$\frac{1.2789\ldots}{\sqrt{n}} \leq \Delta_c \leq \frac{2\sqrt{\ln 2} + o(1)}{\sqrt{n}} = \frac{1.6651\ldots + o(1)}{\sqrt{n}}$$

with probability $1 - o(1)$.

The upper bound in this theorem follows just from Chernoff bounds.

The proof of the lower bound is constructive, since it follows from the evaluation of the expected value

$$\mathrm{E}\left[\sum_{i=1}^{n} \sum_{j=1}^{n} u_i v_j A_{ij}\right] \geq 1.2789\ldots n^{3/2},$$

where values of $u_1, \ldots, u_n, v_1, \ldots, v_n$ are calculated according to Algorithm 1.

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 $a_k = (Z(S_{k-1,1}), \ldots, Z(S_{k-1,n}))$, where $Z(x) = \begin{cases} +1, & \text{if } x > 0 \\ -1, & \text{if } x < 0 \\ \pm 1 \text{ (equiprobably)}, & \text{if } x = 0 \end{cases}$.
   (c) Let $b_k = (A_{k1}, A_{k2}, \ldots, A_{kn})$.
   (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.

7.3.4 The difference

In the literature on nonlocal games, one typically studies the ratio $\frac{\Delta_q}{\Delta_c}$. For random XOR games, our results imply that

$$1.2011\ldots < \frac{\Delta_q}{\Delta_c} < 1.5638\ldots$$

for almost all games. Our computer experiments suggest that, for large n, $\frac{\Delta_q}{\Delta_c} \approx 1.305\ldots$. For comparison, the biggest advantage that can be achieved in any 2-player XOR game is equal to Grothendieck's constant K_G [Gro53] about which we know that [Kri77, Ree91, BMMN11]

$$1.67696\ldots \leq K_G \leq 1.7822139781\ldots$$

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

Chapter 8

Mermin-Ardehali Game

8.1 Introduction

There are four quantum XOR games (equivalent to each other up to the input and/or output inversion), which give the biggest gap between "classical" and "quantum" outcomes. Those games were discovered in the context of Bell inequalities (physics notion closely related to nonlocal games) by Ardehali [Ard92], building on an earlier work by Mermin [Mer90].

They can be described as follows:

$$\begin{array}{c|ccccc} |INPUT| & 0 & 1 & 2 & 3 & \cdots & N \\ \hline \Gamma_{|INPUT|} & + & + & - & - & \cdots & \begin{cases} + & \text{if} \quad (N \bmod 4) \in \{0,1\} \\ - & \text{otherwise} \end{cases} \end{array} \tag{8.1}$$

$$\begin{array}{c|ccccc} |INPUT| & 0 & 1 & 2 & 3 & \cdots & N \\ \hline \Gamma_{|INPUT|} & + & - & - & + & \cdots & \begin{cases} + & \text{if} \quad (N \bmod 4) \in \{0,3\} \\ - & \text{otherwise} \end{cases} \end{array}$$

$$\begin{array}{c|ccccc} |INPUT| & 0 & 1 & 2 & 3 & \cdots & N \\ \hline \Gamma_{|INPUT|} & - & - & + & + & \cdots & \begin{cases} + & \text{if} \quad (N \bmod 4) \in \{2,3\} \\ - & \text{otherwise} \end{cases} \end{array}$$

$\|INPUT\|$	0	1	2	3	$\cdots$	N
$\Gamma_{\|INPUT\|}$	$-$	$+$	$+$	$-$	$\cdots$	$\begin{cases} + & \text{if} \quad (N \bmod 4) \in \{1,2\} \\ - & \text{otherwise} \end{cases}$

For each of those games, the classical and the quantum values are correspondingly $Val_C = 2^{-\lceil \frac{N-1}{2} \rceil}$ and $Val_Q = \frac{1}{\sqrt{2}}$.

Thus, if we take the ratio $\dfrac{Val_Q}{Val_C}$ as the measure of the quantum advantage, these games achieve the ratio of $2^{\lfloor \frac{N-1}{2} \rfloor}$. Werner and Wolf [WW01a] have shown that this ratio is the best possible among all XOR games. Similar ratio was earlier achieved by Mermin [Mer90] for a partial XOR game:

$\|INPUT\|$	0	1	2	3	$\cdots$	N
$\Gamma_{\|INPUT\|}$	$+$	*any*	$-$	*any*	$\cdots$	$\begin{cases} + & \text{if} \quad (N \bmod 4) \in \{0\} \\ - & \text{if} \quad (N \bmod 4) \in \{2\} \end{cases}$

In this game, the input of the players is chosen uniformly at random among all inputs with an even number of 1s.

We now derive the winning probabilities for Mermin-Ardehali game using our methods.

8.2 Classical version

Since all of them are symmetric to each other (with respect to inversion of input and/or output bits), we will consider only the first game (8.1). Any normalized strategy for a classical version of such game can be further simplified.

Lemma 8.1 *In Mermin-Ardehali game, if there are two players with strategies* (01) *and* (10)*, replacing their strategies by* (00) *and* (11) *does not change the average winning probability.*

Proof: Let us compare the outcome before and after a simplification of type (01) (01) $\rightarrow$ (00) (11). Imagine the situation, where the referee has already produced inputs for all except two players, whose choices are being changed. And he is ready to toss up his coin twice in order to decide what input to give to the remaining players.

If the coin will produce different inputs for these players, their answers will be the same: one will answer 0 and the other will answer 1, so the outcome will remain unchanged.

If the coin will produce equal inputs for players — 00 or 11 — it is a more tricky case. Let us notice first that the rules of the game require different answers for 00 and for 11. This can be seen from Table (8.1): changing $|INPUT|$ by 2, right answer changes to opposite value. The second fact to notice is that the strategy before the simplification resulted in equal answers on input 00 and on input 11, that is in one correct and one incorrect answer. The third fact is that the strategy after the simplification will do essentially the same (but in opposite sequence): one answer will be incorrect and the other one will be correct.

So, the total average is equal for both strategies. □

Finally, when none of the simplifications can be applied, then the strategy is one from the following set:

$$\left\{\begin{array}{l}(00)^N, \\ (00)^{N-1}\ (01), \\ (00)^{N-1}\ (10), \\ (00)^{N-1}\ (11)\end{array}\right\}$$

Theorem 8.2 *[AKN+13] For any N the optimal classical strategy has winning probability* $\frac{1}{2} + 2^{-\lceil \frac{N+1}{2} \rceil}$.

Proof: By $f(N, 01)$ we will denote the number of winning inputs (as a subset of all 2^N inputs) for N-player game with strategy $(00)^{N-1}(01)$. The value of f for $f(N, 00)$, $f(N, 10)$, $f(N, 11)$ will be defined similarly. We will use these two elementary facts extensively: $\binom{N}{k} = 0$ if k exceeds N or is less than zero, and $\binom{N}{k} + \binom{N}{k-1} = \binom{N+1}{k}$, which holds for any pair of N and k. Let's evaluate $f(N, 00)$. This strategy always produces XOR equal to zero, therefore $f(N, 00)$ is equal to the number of all N-bit strings, whose Hamming weight is 0 or 1 modulo 4. Counting over all Hamming weights we have $f(N, 00) = \binom{N}{0} + \binom{N}{1} + \binom{N}{4} + \binom{N}{5} + \ldots = \sum_{k=0}^{\infty} \binom{N}{4k} + \binom{N}{4k+1} = \sum_{k=0}^{\infty} \binom{N+1}{4k+1}$. The sum is bounded because of the first elementary fact. This infinity-based notation will be helpful later. Strategy $f(N,01)$ always produces XOR equal to the last bit of the input. If the last bit is zero, then for the strategy to give a correct answer, the Hamming weight of all other bits of the input must be 0 or 1 modulo 4 and there are $\sum_{k=0}^{\infty}\binom{N-1}{4k}+\binom{N-1}{4k+1}=\sum_{k=0}^{\infty}\binom{N}{4k+1}$ such inputs. If the last bit is one, then for the strategy to give a correct answer, the Hamming weight of all other bits of the input must be 1 or 2 modulo 4 and there are $\sum_{k=0}^{\infty}\binom{N-1}{4k+1}+\binom{N-1}{4k+2}=\sum_{k=0}^{\infty}\binom{N}{4k+2}$ such inputs. Taking these two facts together we have: $f(N,01)=\sum_{k=0}^{\infty}\binom{N}{4k+1}+\sum_{k=0}^{\infty}\binom{N}{4k+2}=\sum_{k=0}^{\infty}\binom{N+1}{4k+2}$. Analyzing the other two cases in a similar manner we get $f(N,10)=\sum_{k=0}^{\infty}\binom{N+1}{4k}$ and $f(N,11)=\sum_{k=0}^{\infty}\binom{N+1}{4k+3}$. Let us notice that $f(1,00)=2$, $f(1,01)=1$, $f(1,10)=1$, $f(1,11)=0$. Also notice that $f(N+1,00)=f(N,00)+f(N,10)$, $f(N+1,01)=f(N,01)+f(N,00)$, $f(N+1,10)=f(N,10)+f(N,11)$ and $f(N+1,11)=f(N,11)+f(N,01)$, which can be proved by using the second elementary fact. By using mathematical induction one can immediately prove that the number of winning inputs for each of four strategies can be characterized as follows:

$N \pmod 8$	(00)	(01)	(10)	(11)
0	$2^{\frac{N}{2}-1}+2^{N-1}$	$2^{N-1}-2^{\frac{N}{2}-1}$	$2^{\frac{N}{2}-1}+2^{N-1}$	$2^{N-1}-2^{\frac{N}{2}-1}$
1	$2^{\frac{N-1}{2}}+2^{N-1}$	2^{N-1}	2^{N-1}	$2^{N-1}-2^{\frac{N-1}{2}}$
2	$2^{\frac{N}{2}-1}+2^{N-1}$	$2^{\frac{N}{2}-1}+2^{N-1}$	$2^{N-1}-2^{\frac{N}{2}-1}$	$2^{N-1}-2^{\frac{N}{2}-1}$
3	2^{N-1}	$2^{\frac{N-1}{2}}+2^{N-1}$	$2^{N-1}-2^{\frac{N-1}{2}}$	2^{N-1}
4	$2^{N-1}-2^{\frac{N}{2}-1}$	$2^{\frac{N}{2}-1}+2^{N-1}$	$2^{N-1}-2^{\frac{N}{2}-1}$	$2^{\frac{N}{2}-1}+2^{N-1}$
5	$2^{N-1}-2^{\frac{N-1}{2}}$	2^{N-1}	2^{N-1}	$2^{\frac{N-1}{2}}+2^{N-1}$
6	$2^{N-1}-2^{\frac{N}{2}-1}$	$2^{N-1}-2^{\frac{N}{2}-1}$	$2^{\frac{N}{2}-1}+2^{N-1}$	$2^{\frac{N}{2}-1}+2^{N-1}$
7	2^{N-1}	$2^{N-1}-2^{\frac{N-1}{2}}$	$2^{\frac{N-1}{2}}+2^{N-1}$	2^{N-1}

This proves the fact that for any N the optimal strategy has $2^{\lfloor\frac{N-1}{2}\rfloor}+2^{N-1}$ winning inputs and therefore the winning probability is $\frac{1}{2}+2^{-\lceil\frac{N+1}{2}\rceil}$. $\square$

Our analysis of the game is different from the one in Ardehali's paper [Ard92]. Ardehali's analysis is based on a clever trick that reduces the winning probability to an expression involving complex numbers. This results in a proof that is fairly short but is specific to Mermin-Ardehali game.

Our method of evaluating a sum of binomial coefficients is applicable to any symmetric XOR game.

8.3 Quantum version

The value of the Mermin-Ardehali game can be obtained by maximizing the one-variable expression in equation (5.3). In the case of Mermin-Ardehali game, the maximum of this expression is $\frac{1}{\sqrt{2}}$ and it is achieved by $\lambda = e^{i\theta}$ where $\theta = \frac{(2N+1) \bmod 8}{N}\pi + k\frac{2\pi}{N}$.

The result $f(\lambda) = \frac{1}{\sqrt{2}}$ corresponds to the winning probability of $\Pr_{win} = \frac{1}{2} + \frac{1}{2\sqrt{2}}$. It has been known since [Ard92] that $\Pr_{win} = \frac{1}{2} + \frac{1}{2\sqrt{2}}$ but the advantage of our approach is that we obtain the maximum winning probability by an easy argument that is applicable to any symmetric XOR game.

The winning strategy can be obtained by reversing the argument of [WW01a] and going from λ to transformations for the N players. There are infinitely many possible sets of strategies for each of the given θ. One of these strategies is described in [Ard92]. We include an example of another strategy — of course, symmetric one — in Section 8.4.

The optimality of $\Pr_{win} = \frac{1}{2} + \frac{1}{2\sqrt{2}}$ can be also shown by a very simple argument, which does not involve any of the machinery above.

Theorem 8.3 *[AKNR10]* $\frac{1}{2} + \frac{1}{2\sqrt{2}}$ *is the best possible probability for quantum strategy.*

Proof: We modify the game by providing the inputs and the outputs of the first $N-2$ players to the $(N-1)^{\text{st}}$ and N^{th} players. Clearly, this makes the game easier: the last two players can still use the previous strategy, even if they have the extra knowledge.

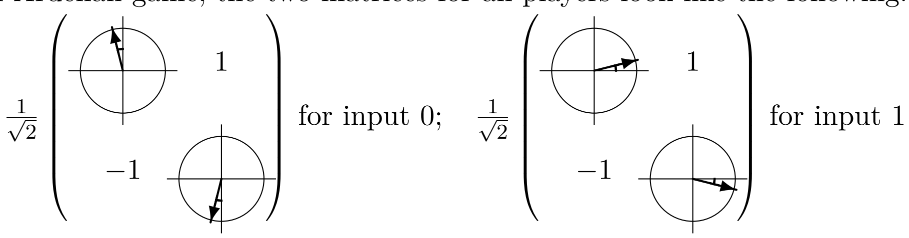
Let k be the number of 1s among the first $N-2$ inputs. Then, we have the following dependence of the result on the actions of the last two players.

$x_1 + x_2 + \ldots + x_{N-2}$	$x_{N-1} + x_N$			
	0	1	2	
k	$+$	$+$	$-$	if $k \bmod 4 = 0$
k	$+$	$-$	$-$	if $k \bmod 4 = 1$
k	$-$	$-$	$+$	if $k \bmod 4 = 2$
k	$-$	$+$	$+$	if $k \bmod 4 = 3$

In either of the four cases, we get a game (for the last two players) which is equivalent to the CHSH game and, therefore, cannot be won with probability more than $\frac{1}{2} + \frac{1}{2\sqrt{2}}$. □

8.4 Optimal quantum strategy

A common behavior for a player in a quantum nonlocal game is to perform some local operation on his qubit, perform a measurement in the standard basis and answer the result of the measurement. In other words, a choice for a player can be expressed with two matrices: one for input 0 and other for input 1. In fact, players may use equal strategies to achieve the best outcome. So optimal strategy for any quantum XOR game can be found and proved with numerical optimization quite simply. For quantum version of Mermin-Ardehali game, the two matrices for all players look like the following:



Complex numbers here are illustrated as vectors on the complex plane. Marked small angles between vectors and axes are equal to each other and their value γ depends on the number of players.

Let us assume x as a value of the input bit. Then these two matrices can be described as one:

$$\frac{1}{\sqrt{2}}\begin{pmatrix} e^{i\left(\frac{\pi}{2}\cdot(1-x)+\gamma\right)} & e^{0} \\ e^{i\pi} & e^{i\left(-\frac{\pi}{2}\cdot(1-x)-\gamma\right)} \end{pmatrix} \tag{8.2}$$

The value γ can be expressed by the table:

Number of players	Angle γ
2	$\frac{5}{8}\pi$
3	$\frac{7}{12}\pi$
4	$\frac{1}{16}\pi$
5	$\frac{3}{20}\pi$
6	$\frac{5}{24}\pi$
7	$\frac{7}{28}\pi$
8	$\frac{1}{32}\pi$
$\vdots$	$\vdots$
N	$\frac{(2N+1) \bmod 8}{4N}\pi$
$\vdots$	$\vdots$

Consider a quantum system in the initial state $|GHZ\rangle = \frac{1}{\sqrt{2}}|00\ldots0\rangle + \frac{1}{\sqrt{2}}|11\ldots1\rangle$. Let us express all local operations, that the players apply to their qubits during the play, as a tensor product of N matrices $M = C_1 \otimes C_2 \otimes \ldots \otimes C_N$ (where each C_k can be represented as in (8.2)). Each cell of M can be calculated as follows:

$$M_{[j_1 j_2 \ldots j_N,\, i_1 i_2 \ldots i_N]} = \prod_{k=1}^{N} C_{k\,[j_k,\, i_k]}$$

where $i_1, i_2, \ldots, i_N,\ j_1, j_2, \ldots, j_N \in \{0, 1\}$.

After all local operations are complete, let's express the final state directly as sum of its amplitudes

$$\sum_{y_1,\ldots,y_N \in \{0,1\}} \alpha_{y_1\ldots y_N} |y_1 \ldots y_N\rangle = M\left(\frac{1}{\sqrt{2}}|00\ldots0\rangle + \frac{1}{\sqrt{2}}|11\ldots1\rangle\right)$$

Consider the value of an arbitrary amplitude $\alpha_{y_1\ldots y_N}$. As there are only two nonzero amplitudes in the starting state, any $\alpha_{y_1\ldots y_N}$ will consist of two summands:

$$\alpha_{y_1\ldots y_N} = \frac{1}{\sqrt{2}}\prod_{k=1}^{N} C_{k\,[0,\, y_k]} + \frac{1}{\sqrt{2}}\prod_{k=1}^{N} C_{k\,[1,\, y_k]}$$

Assuming players got an N-bit input $x_1 \dots x_N$, let us substitute the values from (8.2) for each C_k:

$$\begin{aligned}
\alpha_{y_1\dots y_N} &= \frac{1}{\sqrt{2}}\prod_{k=1}^{N}\frac{1}{\sqrt{2}}e^{i\left(\left(\gamma+\frac{\pi}{2}(1-x_k)\right)\cdot(1-y_k)\right)} + \\
&\quad +\frac{1}{\sqrt{2}}\prod_{k=1}^{N}\frac{1}{\sqrt{2}}e^{i\left(\pi+\left(\frac{\pi}{2}-\gamma+\frac{\pi}{2}\cdot x_k\right)\cdot y_k\right)} = \\
&= \left(\frac{1}{\sqrt{2}}\right)^{N+1} e^{i\sum_{k=1}^{N}\left(\gamma+\frac{\pi}{2}(1-x_k)\right)\cdot(1-y_k)} \\
&\quad + \left(\frac{1}{\sqrt{2}}\right)^{N+1} e^{i\sum_{k=1}^{N}\left(\pi+\left(\frac{\pi}{2}-\gamma+\frac{\pi}{2}\cdot x_k\right)\cdot y_k\right)}
\end{aligned}$$

Now we are interested mainly in the difference between rotation angles on the complex plane for these two summands. That is,

$$\begin{aligned}
&\sum_{k=1}^{N}\left[\left(\gamma+\frac{\pi}{2}(1-x_k)\right)(1-y_k)-\left(\pi+\left(\frac{\pi}{2}-\gamma+\frac{\pi}{2}x_k\right)y_k\right)\right] \\
&= \sum_{k=1}^{N}\left[\left(\gamma+\frac{\pi}{2}-\frac{\pi}{2}x_k-\gamma y_k-\frac{\pi}{2}y_k+\frac{\pi}{2}x_k y_k\right)-\left(\pi+\frac{\pi}{2}y_k-\gamma y_k+\frac{\pi}{2}x_k y_k\right)\right] \\
&= \sum_{k=1}^{N}\left(\gamma+\frac{\pi}{2}-\frac{\pi}{2}x_k-\frac{\pi}{2}y_k-\pi-\frac{\pi}{2}y_k\right) \\
&= \sum_{k=1}^{N}\left(\gamma-\frac{\pi}{2}-\frac{\pi}{2}x_k-\pi y_k\right)
\end{aligned}$$

Let us now consider the case of $N = 4n$ and $\gamma = \frac{1}{4N}\pi$ (and similar reasoning holds for any N). In this case the difference is expressed by (throwing out $\frac{\pi}{2} \times N \equiv 0 \pmod{2\pi}$, which is now redundant)

$$\frac{1}{4}\pi - \frac{1}{2}\pi\sum_{k=1}^{N}(x_k + 2y_k)$$

By modulus 2π it is equal to the value from Table 8.1.

If the angle between two summands (both of the same length $\left(\frac{1}{\sqrt{2}}\right)^{N+1}$) is $\boxed{\pm\frac{1}{4}\pi}$, then their sum is

$$\left(\frac{1}{\sqrt{2}}\right)^{N-1}\cos\frac{\pi}{8} = \left(\frac{1}{\sqrt{2}}\right)^{N-1}\frac{\sqrt{2+\sqrt{2}}}{2}. \tag{8.3}$$

Table 8.1: Amplitude angle values for different inputs

$\|INPUT\|$ $= x_1 + x_2 + \ldots + x_N$	$\|OUTPUT\| = y_1 + y_2 + \ldots + y_N$ 0	1	2	3	$\ldots$
0	$\boxed{\frac{1}{4}\pi}$	$-\frac{3}{4}\pi$	$\boxed{\frac{1}{4}\pi}$	$-\frac{3}{4}\pi$	$\cdots$
1	$\boxed{-\frac{1}{4}\pi}$	$\frac{3}{4}\pi$	$\boxed{-\frac{1}{4}\pi}$	$\frac{3}{4}\pi$	$\cdots$
2	$-\frac{3}{4}\pi$	$\boxed{\frac{1}{4}\pi}$	$-\frac{3}{4}\pi$	$\boxed{\frac{1}{4}\pi}$	$\cdots$
3	$\frac{3}{4}\pi$	$\boxed{-\frac{1}{4}\pi}$	$\frac{3}{4}\pi$	$\boxed{-\frac{1}{4}\pi}$	$\cdots$
4	$\boxed{\frac{1}{4}\pi}$	$-\frac{3}{4}\pi$	$\boxed{\frac{1}{4}\pi}$	$-\frac{3}{4}\pi$	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

(Recall that the absolute value of the sum of two vectors of the same length x with angle ϕ between them is calculated as $\left|2x\cos\frac{\phi}{2}\right|$.)

If the angle between two summands (both of the same length $\left(\frac{1}{\sqrt{2}}\right)^{N+1}$) is $\pm\frac{3}{4}\pi$, then their sum is

$$\left(\frac{1}{\sqrt{2}}\right)^{N-1}\cos\frac{3\pi}{8} = \left(\frac{1}{\sqrt{2}}\right)^{N-1}\frac{\sqrt{2-\sqrt{2}}}{2}$$

As one can see from Table 8.1, bigger amplitudes always correspond to correct answers (and smaller amplitudes correspond to incorrect answers). The sum of the squares of formula (8.3), i.e., the result of the measurement for any fixed input, will give the probability of right answer:

$$\sum_{Angle=\boxed{\pm\frac{1}{4}\pi}}\left(\left(\frac{1}{\sqrt{2}}\right)^{N-1}\frac{\sqrt{2+\sqrt{2}}}{2}\right)^2 = 2^{N-1}\left(\frac{1}{\sqrt{2}}\right)^{2(N-1)}\left(\frac{\sqrt{2+\sqrt{2}}}{2}\right)^2$$
$$= \frac{1}{2}+\frac{1}{2\sqrt{2}}$$

Note that this probability is stable: it remains the same for all possible inputs from the referee.

Chapter 9

CHSH Game with Arbitrary Input Distribution

9.1 Introduction

CHSH game is a popular illustration of the difference between classical and quantum worlds. Namely, it shows violation of the original Bell's inequality. In terms of the CHSH game, the biggest such violation can be achieved by choosing uniformly distributed players' input.

It could be interesting however to study more general case, i.e. CHSH games with different input distributions.

9.2 Classical version

Let us start with the classical optimum for a CHSH game with arbitrary distribution of input.

First of all it is worth to recall the fact that no randomized strategy can give better results than optimal deterministic one does. So, it is sufficient to consider and evaluate finite number of different deterministic strategies only. Since each of two players has to determine his binary answer for two possible inputs, this number is $2^4 = 16$. But it turns out to be sufficient to consider only four of them in order to find an optimum.

The following four strategies belong to the set of optimal classical strategies for CHSH game with uniform distribution of input.

Answers of player 1		Answers of player 2		Inputs, for which strategy gives correct answer
Input 0	Input 1	Input 0	Input 1	
0	0	0	0	$0,0$ $0,1$ $1,0$ ~~$1,1$~~
0	1	0	0	$0,0$ $0,1$ ~~$1,0$~~ $1,1$
0	0	0	1	$0,0$ ~~$0,1$~~ $1,0$ $1,1$
0	1	1	0	~~$0,0$~~ $0,1$ $1,0$ $1,1$

Since each strategy in CHSH game results in an incorrect answer for at least one input, each of the other 12 strategies either is equivalent to one of the above-mentioned four strategies or is strictly dominated by one of them. Therefore it is sufficient to consider only the four above-mentioned strategies.

Suppose we have input distribution $(P_{00}, P_{01}, P_{10}, P_{11})$, where P_{ab} stands for the probability to receive input "a, b" from the referee. We must select any pair (a^*, b^*), such that

$$P_{a^*b^*} = \min_{a,b} P_{ab}$$

Then we must search for this pair crossed out in the rightmost column of the table (i.e. for "~~a^*, b^*~~") and select the respective strategy. This strategy will exploit differences of input distributions in the best possible way and will give outcome

$$1 - \min(P_{00}, P_{01}, P_{10}, P_{11})$$

which is evidently the best possible expected value for the given distribution.

We conclude that the classical outcome depends linearly on the input distribution and has the lowest expected value (0.75) for the uniform input distribution.

9.3 Analysis of quantum version

In this section we shall consider only those input distributions, which preserve symmetry of the game with respect to permutations of players. In other words, we shall assume that $P_{01} = P_{10} = \dfrac{1 - P_{00} - P_{11}}{2}$.

In order to find an optimal quantum strategy for the players in such symmetric game, we can make some useful restrictions:

1. Players always answer with the result of the measurement applied to their qubits.
2. Given x as an input, a player applies operation

$$\widehat{U_x} = \begin{pmatrix} \frac{e^{i\phi_x}}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} & \frac{e^{-i\phi_x}}{\sqrt{2}} \end{pmatrix}$$

   to his qubit and then makes a measurement.
3. Strategies for both players are the same.

Proof:

1. The first fact follows from the result of [WW01a], namely from the assumption that observables $A(0), A(1)$ for any player may be unitary.
2. The second fact also can be simply followed from [WW01a]. To figure out observables $A(0), A(1)$ for any player, one should calculate:

$$A(x) = \widehat{U_x}^{\dagger} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \widehat{U_x} = \begin{pmatrix} 0 & -e^{i\phi_x} \\ -e^{-i\phi_x} & 0 \end{pmatrix}$$

   Thus both observables $A(0)$ and $A(1)$, as well as their product

$$C = A(0)A(1) = \begin{pmatrix} e^{i(\phi_0-\phi_1)} & 0 \\ 0 & e^{i(\phi_1-\phi_0)} \end{pmatrix} \tag{9.1}$$

   can have any eigenvalue (from the set $\{\gamma : |\gamma| = 1\}$, depending on the values ϕ_0 and ϕ_1) needed to maximize the outcome of the game.
3. Equality of players' strategies could be proven in the similar way as in analysis of general XOR games.

□

Now let us perform some calculations in order to figure out the best outcome for the described set of quantum strategies.

Given an input "x, y", players perform the following transformation on their entangled quantum system:

$$\widehat{U_x} \otimes \widehat{U_y} = \begin{pmatrix} \frac{e^{i\phi_x}}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} & \frac{e^{-i\phi_x}}{\sqrt{2}} \end{pmatrix} \otimes \begin{pmatrix} \frac{e^{i\phi_y}}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} & \frac{e^{-i\phi_y}}{\sqrt{2}} \end{pmatrix}$$

$$= \begin{pmatrix} \boxed{\frac{e^{i(\phi_x+\phi_y)}}{2}} & \frac{e^{i\phi_x}}{2} & \frac{e^{i\phi_y}}{2} & \boxed{\frac{1}{2}} \\ -\frac{e^{i\phi_x}}{2} & \frac{e^{i(\phi_x-\phi_y)}}{2} & -\frac{1}{2} & \frac{e^{-i\phi_y}}{2} \\ -\frac{e^{i\phi_y}}{2} & -\frac{1}{2} & \frac{e^{i(\phi_y-\phi_x)}}{2} & \frac{e^{-i\phi_x}}{2} \\ \boxed{\frac{1}{2}} & -\frac{e^{-i\phi_y}}{2} & -\frac{e^{-i\phi_x}}{2} & \boxed{\frac{e^{-i(\phi_x+\phi_y)}}{2}} \end{pmatrix}$$

Just like in the analysis of an ordinary CHSH game, we only have to consider amplitudes of $|00\rangle$ and $|11\rangle$ of the initial state and on the same amplitudes of the final state, that is, the corner values of this matrix.

The winning probability for such a strategy is as follows:

$$\begin{aligned} Win(\phi_0, \phi_1) = \; & P_{00} \times \left(\left| \frac{e^{i(\phi_0+\phi_0)}}{2\sqrt{2}} + \frac{1}{2\sqrt{2}} \right|^2 + \left| \frac{1}{2\sqrt{2}} + \frac{e^{-i(\phi_0+\phi_0)}}{2\sqrt{2}} \right|^2 \right) + \\ & P_{01} \times \left(\left| \frac{e^{i(\phi_0+\phi_1)}}{2\sqrt{2}} + \frac{1}{2\sqrt{2}} \right|^2 + \left| \frac{1}{2\sqrt{2}} + \frac{e^{-i(\phi_0+\phi_1)}}{2\sqrt{2}} \right|^2 \right) + \\ & P_{10} \times \left(\left| \frac{e^{i(\phi_1+\phi_0)}}{2\sqrt{2}} + \frac{1}{2\sqrt{2}} \right|^2 + \left| \frac{1}{2\sqrt{2}} + \frac{e^{-i(\phi_1+\phi_0)}}{2\sqrt{2}} \right|^2 \right) + \\ & P_{11} \times \left(1 - \left| \frac{e^{i(\phi_1+\phi_1)}}{2\sqrt{2}} + \frac{1}{2\sqrt{2}} \right|^2 - \left| \frac{1}{2\sqrt{2}} + \frac{e^{-i(\phi_1+\phi_1)}}{2\sqrt{2}} \right|^2 \right) \end{aligned}$$

Since $\left|e^{i\phi} + 1\right| = \left|e^{-i\phi} + 1\right| = 2\cos\frac{\phi}{2}$, we can rewrite this expression as

$$\begin{aligned} Win(\phi_0, \phi_1) = \; & P_{00}\cos^2\phi_0 + \\ & (P_{01} + P_{10})\cos^2\frac{\phi_0+\phi_1}{2} + \\ & P_{11} - P_{11}\cos^2\phi_1 \end{aligned}$$

Since $\quad \cos^2 \phi = \dfrac{\cos 2\phi + 1}{2}$,

$$
\begin{aligned}
Win(\phi_0, \phi_1) &= \frac{P_{00}}{2}(\cos 2\phi_0 + 1) + \\
&\quad \frac{P_{01} + P_{10}}{2}(\cos(\phi_0 + \phi_1) + 1) + \\
&\quad P_{11} - \frac{P_{11}}{2}(\cos 2\phi_1 + 1) \\
&= \frac{P_{00}}{2}\cos 2\phi_0 + \frac{P_{01} + P_{10}}{2}\cos(\phi_0 + \phi_1) - \frac{P_{11}}{2}\cos 2\phi_1 + \\
&\quad \underbrace{\frac{P_{00} + P_{01} + P_{10} + P_{11}}{2}}_{=\frac{1}{2}}
\end{aligned}
$$

Finally, we define $Bias\,(\phi_0, \phi_1)$ as $Win\,(\phi_0, phi_1) - Loss\,(\phi_0, \phi_1)$:

$$
\begin{aligned}
Bias\,(\phi_0, \phi_1) &= Win\,(\phi_0, \phi_1) - Lose\,(\phi_0, \phi_1) \\
&= Win\,(\phi_0, \phi_1) - (1 - Win\,(\phi_0, \phi_1)) \\
&= 2 \times Win\,(\phi_0, \phi_1) - 1 \\
&= P_{00}\cos 2\phi_0 + (P_{01} + P_{10})\cos(\phi_0 + \phi_1) - P_{11}\cos 2\phi_1
\end{aligned}
$$

We notice that this expression does not depend on ratio of P_{01} and P_{10}, but depends only on their sum. This is not surprising: since players use the same strategy, expected value of the game must not depend on permutations of players. In further considerations it will be useful to replace $P_{01} + P_{10}$ with $1 - P_{00} - P_{11}$.

So, now our task is: given values P_{00} and P_{11}, just maximize the expression

$$
Bias\,(\phi_0, \phi_1) = P_{00}\cos 2\phi_0 + (1 - P_{00} - P_{11})\cos(\phi_0 + \phi_1) - P_{11}\cos 2\phi_1 \tag{9.2}
$$

This procedure turns out not to be so trivial. An extremum of function $Bias\,(\phi_0, \phi_1)$ requires the following two conditions to be satisfied:

$$
\begin{cases}
\dfrac{\mathrm{d}}{\mathrm{d}\phi_0} Bias\,(\phi_0, \phi_1) = 0 \\
\dfrac{\mathrm{d}}{\mathrm{d}\phi_1} Bias\,(\phi_0, \phi_1) = 0
\end{cases}
$$

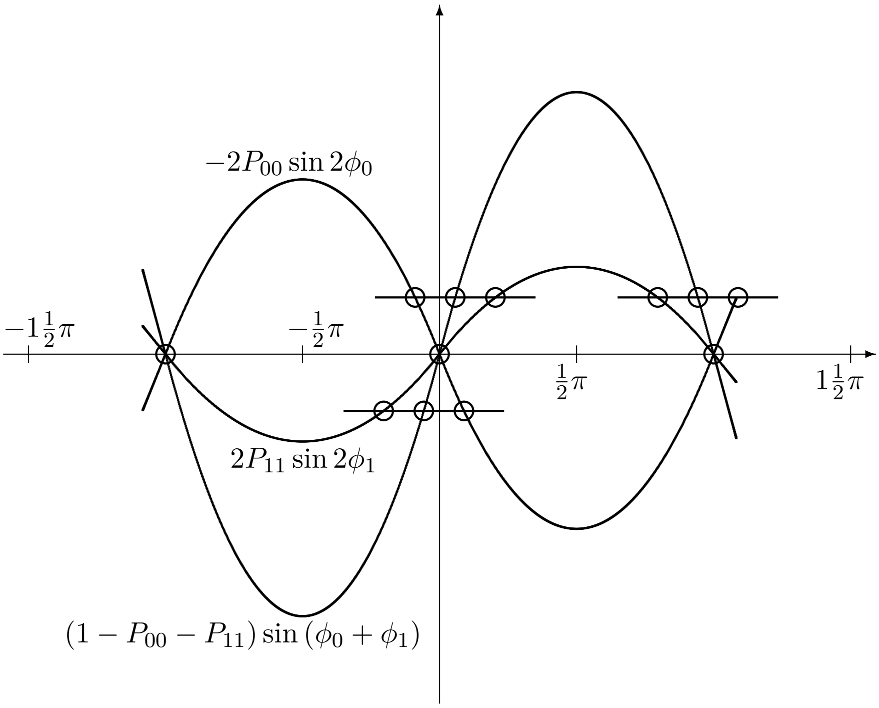
It follows that

$$
\begin{cases}
-(1 - P_{00} - P_{11})\sin(\phi_0 + \phi_1) - 2P_{00}\sin 2\phi_0 = 0 \\
-(1 - P_{00} - P_{11})\sin(\phi_0 + \phi_1) + 2P_{11}\sin 2\phi_1 = 0
\end{cases}
$$

And this could be rewritten in slightly more beautiful form:

$$(1 - P_{00} - P_{11}) \sin(\phi_0 + \phi_1) = -2P_{00} \sin 2\phi_0 = 2P_{11} \sin 2\phi_1 \tag{9.3}$$

In order to understand the following steps, it is worth to imagine what all that means when drawn on a diagram.



Here we tried to illustrate three functions

$$\begin{cases} f_1(\phi_0 + \phi_1) &= (1 - P_{00} - P_{11}) \sin(\phi_0 + \phi_1) \\ f_2(2\phi_0) &= -2P_{00} \sin 2\phi_0 \\ f_3(2\phi_1) &= 2P_{11} \sin 2\phi_1 \end{cases} \tag{9.4}$$

in such a way as if their arguments $\phi_0 + \phi_1$, $2\phi_0$, and $2\phi_1$ would be mutually independent. If they were really independent, then we would be interested in every triple of points of different curves, which lies on the same horizontal line: we could claim then that each of such triple corresponds to an extremum of (9.2).

Fortunately, there are not so many extremums. Now we are going to find all points, which meet restriction of equidistance: arguments of form $\phi_0 + \phi_1$, $2\phi_0$, and $2\phi_1$ follow that values of arguments $2\phi_0$ and $2\phi_1$ are equidistant from value of argument $\phi_0 + \phi_1$.

There are marked some triples on the diagram that meet both our conditions: values of the margin arguments are equidistant from the value of the middle argument, and values of all three respective functions are equal (we shall call them *correct* triples).

Actually, there are shown eight correct triples, three of which are collapsed into single points (namely, one point $2\phi_0 = \phi_0 + \phi_1 = 2\phi_1 = -\pi$; one point in 0; and one point in π). Additionally, there are marked triple $(2\phi_0, \phi_0 + \phi_1, 2\phi_1) = (-\pi, 0, \pi)$ and triple $(2\phi_0, \phi_0 + \phi_1, 2\phi_1) = (\pi, 0, -\pi)$. These five triples are correct for each input distribution $P_{00}, P_{01}, P_{10}, P_{11}$.

But we must consider also some specific correct triples. On the diagram there are marked three such triples, which do depend on values of P_{00} and P_{11} (from left to right):

1. $(2\phi_0, \phi_0 + \phi_1, 2\phi_1) = (0.28, -0.18, -0.64)$
2. $(2\phi_0, \phi_0 + \phi_1, 2\phi_1) = (-0.28, 0.18, 0.64)$
3. $(2\phi_0, \phi_0 + \phi_1, 2\phi_1) = (3.42, 2.96, 2.50)$

So, we can figure out eight function's $Bias\,(\phi_0, \phi_1)$ extremum points from this diagram. Actually, they are only candidates to extremums, as they could turn out to be, for example, saddle points (that is, correspond to $\min\limits_{\phi_0'} Bias\,(\phi_0', \phi_1) = \max\limits_{\phi_1'} Bias\,(\phi_0, \phi_1'))$. Then we won't have any interest in them. Besides that, they could turn out to be minimums, and then we also won't have any interest in them. But on the other hand, we can be sure that after we have found all correct triples, we won't miss any maximum. That is, we should check finite (and quite small) number of correct triples and figure out that triple, which correspond to the biggest value of $Bias\,(\phi_0, \phi_1)$.

How can we find all correct triples, which correspond to some given values P_{00} and P_{11}? In order to do this we are going to start with the condition of functions' equity, and then add the condition of arguments' equidistance.

But before it is worth to take a look on the diagram once again and try to imagine what could be the diagrams and solutions for arbitrary P_{00} and P_{11}. One could notice that the amplitudes of functions can vary, but functions should keep their signs, as $P_{00}, P_{01}, 1 - P_{00} - P_{11}$ all are positive numbers (unless one of them collapses to zero; that would immediately follow that the game is trivial and has 100%-winning classical strategy, as it was described in the analysis of classical case). That is, we can assume the diagram to consist of two "positive" sinusoids and one "negative" sinusoid. The second fact to notice is that none of these sinusoids can exceed 1 by its absolute value, since we can expect that $P_{00}, P_{01},$ and $1 - P_{00} - P_{11}$ all are ≤ 1.

Now, let us continue our search for correct triples and start with considering each horizontal line of the diagram. Say, let us fix a horizontal line at height H. We are only interested in horizontal lines that cross all three functions (9.4). That means,

$$|H| \leq \min\left(|1 - P_{00} - P_{11}|, |-2P_{00}|, |2P_{11}|\right) < 1$$

On the next step, let us add the condition of equidistance of the arguments. When expressed via function value H, values of arguments $\phi_0 + \phi_1$, $2\phi_0$, and $2\phi_1$ will look as follows:

$$\begin{cases} (1 - P_{00} - P_{11}) \sin(\phi_0 + \phi_1) = H & \Longrightarrow \quad \phi_0 + \phi_1 = \arcsin \dfrac{H}{1 - P_{00} - P_{11}} \\ -2P_{00} \sin 2\phi_0 = H & \Longrightarrow \quad 2\phi_0 = \arcsin \dfrac{H}{-2P_{00}} \\ 2P_{11} \sin 2\phi_1 = H & \Longrightarrow \quad 2\phi_1 = \arcsin \dfrac{H}{2P_{11}} \end{cases} \tag{9.5}$$

So, the condition of equidistance of the arguments for value H means that

$$2 \arcsin \frac{H}{1 - P_{00} - P_{11}} = \arcsin \frac{H}{-2P_{00}} + \arcsin \frac{H}{2P_{11}} \tag{9.6}$$

Unfortunately, last claim was not completely correct. There are some more cases, which can guarantee to meet the condition of equidistance of the arguments. Namely, in the equation (9.6) we can replace any of three components of form "$\arcsin X$" with "$\pi - \arcsin X$". Laws of trigonometry forces us here to spread our considerations into $2^3 = 8$ different threads (actually, less than eight, as some of them are completely equal, but definitely more than one).

But as all these threads are of quite similar nature, we shall limit ourselves with only that one described by (9.6).

Now let us solve (9.6) by considering sines of both sides:

$$2\arcsin\frac{H}{1-P_{00}-P_{11}} = \arcsin\frac{H}{-2P_{00}} + \arcsin\frac{H}{2P_{11}}$$

- -

$$\sin\left(2\arcsin\frac{H}{1-P_{00}-P_{11}}\right) = \sin\left(\arcsin\frac{H}{-2P_{00}} + \arcsin\frac{H}{2P_{11}}\right)$$

- -

$$\begin{aligned} 2\times\sin\left(\arcsin\frac{H}{1-P_{00}-P_{11}}\right) & & \sin\left(\arcsin\frac{H}{-2P_{00}}\right)\cos\left(\arcsin\frac{H}{2P_{11}}\right) \\ & = & \\ \times\cos\left(\arcsin\frac{H}{1-P_{00}-P_{11}}\right) & & +\cos\left(\arcsin\frac{H}{-2P_{00}}\right)\sin\left(\arcsin\frac{H}{2P_{11}}\right) \end{aligned}$$

- -

$$\frac{2H\sqrt{1-\frac{H^2}{(1-P_{00}-P_{11})^2}}}{1-P_{00}-P_{11}} = \frac{H\sqrt{1-\frac{H^2}{4P_{11}^2}}}{-2P_{00}} + \frac{H\sqrt{1-\frac{H^2}{4P_{00}^2}}}{2P_{11}}$$

This is quite heavy formula, but it is still computable. We shall not dive into simplifying these expressions, as this process is rather boring.

For each value H, which satisfies this equation, one must compute

$$\begin{cases} \phi_0 = \dfrac{\arcsin\frac{H}{-2P_{00}}}{2} \quad \text{or} \quad \dfrac{\pi-\arcsin\frac{H}{-2P_{00}}}{2} \\ \\ \phi_1 = \dfrac{\arcsin\frac{H}{2P_{11}}}{2} \quad \text{or} \quad \dfrac{\pi-\arcsin\frac{H}{2P_{11}}}{2} \end{cases} \tag{9.7}$$

and then check the (probably, extremal) value of $Bias\,(\phi_0, \phi_1)$ for corresponding ϕ_0 and ϕ_1. In this manner all extremums of function $Bias\,(\phi_0, \phi_1)$ would be observed and a maximum would be found among them. (Moreover, in this manner we could also find all minimums and all saddle points of this function, and thus make some estimations about what would happen, if players wanted to lose, or if one player wanted to lose and another wanted to win.)

9.4 Optimal quantum strategies

Luckily, there is a shorter way to find strategies for the quantum version of this game.

In order to do this, we shall find the upper bound for $Bias\left(\phi_0, \phi_1\right)$ by optimizing expression

$$\left|P_{00} + \left(1 - P_{00} - P_{11}\right)\lambda - P_{11}\lambda^2\right|$$

Direct calculations show that

$$\max_{|\lambda|=1}\left|P_{00} + \left(1 - P_{00} - P_{11}\right)\lambda - P_{11}\lambda^2\right| = \max_{|\lambda|=1}\sqrt{\begin{array}{l} -4P_{00}P_{11}\Re^2(\lambda) \\ +2\left(1 - P_{00} - P_{11}\right)\left(P_{00} - P_{11}\right)\Re(\lambda) \\ +1 - \left(1 - P_{00} - P_{11}\right)\left(P_{00} + P_{11}\right) \end{array}}$$

(by $\Re(\lambda)$ we denote the real part of complex number λ).

The quadratic function of $\Re\left(\lambda\right)$ under the square root achieves its maximum at the point where its derivative $-8P_{00}P_{11}\Re\left(\lambda\right) + 2\left(1 - P_{00} - P_{11}\right)\left(P_{00} - P_{11}\right)$ turns to zero, that is, at

$$\Re(\lambda) = \frac{\left(1 - P_{00} - P_{11}\right)\left(P_{00} - P_{11}\right)}{4P_{00}P_{11}} = \frac{1 - P_{00}}{4P_{11}} - \frac{1 - P_{11}}{4P_{00}}$$

and the closer is $\Re(\lambda)$ to this point, the bigger is the value of the function.

Since $|\lambda| = 1 \implies \Re(\lambda) \in [-1; 1]$, the closest possible value for $\Re(\lambda)$ is at

$$\Re(\lambda_{opt}) = \max\left(-1, \min\left(1, \frac{\left(1 - P_{00} - P_{11}\right)\left(P_{00} - P_{11}\right)}{4P_{00}P_{11}}\right)\right)$$

In this way we can find the exact value of λ_{opt}, which corresponds to the optimal eigenvalue of (9.1).

Phase of this eigenvalue $\arg\left(\lambda_{opt}\right)$ is just the difference between angles ϕ_0 and ϕ_1:

$$\phi_1 = \phi_0 + \arg\left(\lambda_{opt}\right) \tag{9.8}$$

Combining (9.8) with (9.5) we get the following equation:

$$H = \left(1 - P_{00} - P_{11}\right)\sin\left(\phi_0 + \phi_0 + \arg\left(\lambda_{opt}\right)\right) = -2P_{00}\sin 2\phi_0$$

Solving this equation will lead to the following result:

$$\sin 2\phi_0 = \pm\xi, \quad \text{where} \quad \xi = \frac{1}{\sqrt{\left(\frac{\cos\left(\arg\left(\lambda_{opt}\right)\right) + \frac{2P_{00}}{1-P_{00}-P_{11}}}{\sin\left(\arg\left(\lambda_{opt}\right)\right)}\right)^2 + 1}} \tag{9.9}$$

Checking results for four possible values of ϕ_0 ($\dfrac{\pm\arcsin\xi}{2}$ and $\dfrac{\pi\mp\arcsin\xi}{2}$) will provide us with optimal ϕ_0 and ϕ_1.

Of course, (9.9) can be further simplified, but let us limit our considerations only with the general principle of building this formula.

These results partly overlap with the work of Lawson et al. [LLP10], which also analyzes CHSH game under non-uniform distributions on the inputs. We, however, analyze different probability distributions and use different methods.

Chapter 10

Summary

Part II is dedicated to the so-called nonlocal games, which can be briefly defined as cooperative games of non-communicating players against a referee. These games are known as a simple but useful model which is widely used for displaying nonlocal properties of quantum mechanics. Among them XOR games (whose outcome depends only on the parity of players' answers) are of special interest, because they appear to have the biggest difference between their classical and quantum values. In order to show this we described our techniques for analyzing such games.

In Chapter 5 we initiated studying multiplayer nonlocal XOR games with $\{0,1\}$-valued players' input, which are symmetric w.r.t. permutation of players. We showed that for any such game there always exists a symmetric optimal quantum strategy, and defined quite small set, which with certainty contains an optimal classical strategy. These results provide an insight for efficient (polynomial-timed) calculating classical and quantum values of an arbitrary game from the above-mentioned class.

On the ground of these ideas we developed efficient algorithms for determining both classical and quantum values, and in Chapter 6 we presented statistical results of analysis of millions of games picked at random (part of these results were introduced in the joint work [AIKV12]). Additionally we built an explicit bound for the expected classical value of a random game, and made a hypothesis on the expected quantum value of a random game. These results demonstrate significant quantum-over-classical advantage for almost all multiplayer nonlocal XOR games.

In Chapter 7 we briefly introduced the results of the joint work [ABB+12], which is dedicated to the two-player nonlocal XOR games with large players' input. We performed study on general properties of a random game from that set. One can specify the rules of such game by an $n \times n$ matrix, whose entries are $+1$ and -1. Two classical bounds and one explicit quantum bound for the expected value of a random game follow from a large variety of techniques, most of which come from the theory of random matrices. These results also confirm that quantum-over-classical advantage is typical for nonlocal XOR games.

In Chapter 8 we studied the well known Mermin-Ardehali game, which demonstrate the biggest possible quantum-over-classical advantage in its class of games. We analyzed this game in the light of ideas from Chapter 5 and followed its known values (together with appropriate symmetric strategies) in different way, which (as we hope) is simpler than one in original works [Mer90, Ard92].

In Chapter 9 we performed analysis of modified CHSH games, where the referee may choose the probability distribution of players' input. We obtained quite heavy formulae for finding optimal players' strategies in these games. The overall result conforms to the immanent spirit of Part II: the more symmetric (i.e. uniform) the distribution of input is, the greater is the quantum-over-classical advantage in the game.

Part III

Games with Quantum Decisions

Chapter 11

Introduction

In Part II we studied nonlocal games. In these games players are provided with some settings and must declare their decisions in the form of common classical information.

This part is dedicated to another interesting class of games. In these games, unlike nonlocal ones, players are allowed to declare their decisions by providing a quantum system in some state, i.e. in the form of quantum information. Since this class of games seems not to have any conventional name so far, we proposed to call them "games with quantum decisions".

One of the most widely studied models of game quantization was initially proposed in [EWL99] and further developed in a number of works, up to physical implementation on a quantum computer [DLX$^+$01]. In this model the game process follows the predefined protocol, which consists of the following steps:

1. a referee prepares a multipartite quantum system (in an entangled state);
2. parts of this quantum system are being distributed among the players;
3. players perform arbitrary operations on their particles (by applying some unitary operators on their states);
4. the referee collects all the system together, applies some additional unitary operations and performs a measurement;
5. payoffs are being paid to the players according to the results of the measurement.

This is a general description of the protocol, which needs one significant remark. The fact is that when one builds a quantum version of a classical game, he might intend to keep the quantum game analogous to its classical version. In order to do so, he must properly define operations made by the referee.

Traditionally this model is being applied for quantization of non-cooperative games (such as Prisoner's Dilemma [EWL99] or Kolkata Restaurant Problem [SH11]), since they are comparatively easy analyzable. But it is also applicable for quantization of cooperative games, in which entanglement effects could affect also the process of forming coalitions.

Initially this model was demonstrated on the quantization of Prisoner's Dilemma (see Section 3.4 for details), which is a 2×2 matrix game. The one-dimensional space of the referee's operations

$$\widehat{J} \in \left\{ \exp\left(i\gamma \begin{pmatrix} 0001 \\ 0010 \\ 0100 \\ 1000 \end{pmatrix} \right) : \gamma \in \left[0, \frac{\pi}{4}\right] \right\} \tag{11.1}$$

(where parameter γ represents the amount of the initial entanglement and thus the power of the quantum effect in the game) was chosen in order to keep the same outcome of the game for (a) all four pure classical strategies and (b) all two-dimensional space of mixed strategies in the mixed expansion of the original Prisoner's Dilemma.

This model is very naturally applicable to a game with any number of players N, just by substituting the $\begin{pmatrix} 0001 \\ 0010 \\ 0100 \\ 1000 \end{pmatrix}$ with $2^N \times 2^N$ exchange matrix in (11.1) (e.g. similar technique was introduced in [BH01b]). On the other hand, this model has quite specific limitation on the amount of strategies for each player. Namely, each player in the classical version of a game should have exactly 2 strategies (and respectively one-dimensional space of strategies in the mixed expansion of this game, where the single parameter represents the probability of choosing one or another of the two options).

Probably the first step towards an M-choice generalization of an N-player game is done in [SH11] by constructing a quantum minority game, where three players use three-level quantum states.

In this part we introduce rather new approach to the generalizing similar scheme to the set of arbitrary multiplayer multichoice game. This approach has been published in our paper [Kra13].

Chapter 12 is dedicated to formal description of the quantization scheme, and in Chapter 13 we illustrate this technique on a specific example of voting game. The key idea is repeated in both chapters in order to keep them self contained to a certain degree, and to allow the reader to skip or just to run over one of them.

Finally, in Chapter 14 we discuss some known issues and comments on game quantization.

Chapter 12

Technical Details

12.1 Settings

Let us consider an arbitrary N-player game, where i^{th} player has arbitrary number (say M_i) of options (i.e. pure classical strategies).

We shall now treat this game in the spirit of the considerations applied to the Prisoner's Dilemma (see Section 3.4). Yet lifting of restrictions on the number of choices will lead to a different quantization method.

12.2 Classical formalism

We can formulate the settings of the game and the behavior of the players in terms of linear algebra in the following way:

1. The game board consists of N unit vectors, each from $\{0,1\}^{M_i}$ for $i \in \{1, 2, \ldots, N\}$. Initially their values are $a_{1i} = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$.
2. All players independently choose shift operators $A_1, A_2, \ldots, A_N$ and apply them one

by one to $a_{1\,1}, a_{1\,2}, \ldots, a_{1\,N}$. Thus the i^{th} player chooses $M_i \times M_i$ matrix

$$A_i \in \left\{ \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \ddots & 0 & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \ddots & 1 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & 0 & \cdots & 0 & 0 \end{pmatrix}^k = [m_{yx}] : m_{yx} = \begin{cases} 1 \text{ if } y+k \equiv x (\text{mod } N), \\ 0 \text{ otherwise} \end{cases}, k \in \mathbb{N} \right\} \tag{12.1}$$

and multiplies it with $a_{1\,i}$.

Let us denote $a_{2\,i} = A_i a_{1\,i}$ for $i \in \{1, 2, \ldots, N\}$.

3. Each resulting vector $a_{2\,i}$ is treated as probability distribution of choosing among M_i options available for the i^{th} player.

4. Players get their payoffs according to the table of payoffs.

12.3 Quantum formalism

We now propose the general scheme for constructing a quantum version of an arbitrary miltiplayer multichoice game. This scheme is somewhat an analog and an expansion of the classical scheme described in Section 12.2.

1. The game board consists of an N-qudit quantum system, where the i^{th} qudit is an M_i-level quantum subsystem.
   The initial state of the game board is $\psi_1 = |11\ldots1\rangle$ (and corresponds to choosing the first option by each of N players).

1_q Before all players' actions, an entangling operator $\widehat{J}$ (from the set, which we shall define later) is applied to the system, which gets "entangled" into state $\psi_{1_q} = \widehat{J}\psi_1$.

2. Players independently choose shift or any other unitary operators $\widehat{A}_1, \widehat{A}_2, \ldots, \widehat{A}_N$ and apply them one by one to the N qudits of the system.

Its state changes to $\psi_2 = \left(\widehat{A}_1 \otimes \widehat{A}_2 \otimes \ldots \otimes \widehat{A}_N\right) \psi_{1_q}$.

2_q After all players' actions are done, an operator $\widehat{J}^\dagger$ is applied to the system.
Its state changes to $\psi_{2_q} = \widehat{J}^\dagger \psi_2$.
Let us denote $\psi_{2_q} = \sum\limits_{k_1=1}^{M_1} \sum\limits_{k_2=1}^{M_2} \ldots \sum\limits_{k_N=1}^{M_N} \alpha_{k_1 k_2 \ldots k_N} |k_1 k_2 \ldots k_N\rangle$.

3. Resulting qubits are measured in the computational basis, and the absolute squares of the probability amplitudes $|\alpha_{k_1 k_2 \ldots k_N}|^2$ (of total number $\prod\limits_{i=1}^{N} M_i$) are treated as probabilities of simultaneous choosing options $k_1, k_2, \ldots, k_M$.

4. Players get their payoffs according to the table of payoffs.

In order to keep "backward compatibility" with the set of classical strategies (like in the Quantum Prisoner's Dilemma) we must apply special constraints on the entangling operator $\widehat{J}$ in step 2_q. Namely, we must ensure that steps 1_q and 2_q won't affect state ψ_{2_q} in the case where all players choose unitary operators from the set (12.1) which is "classical" subset of "quantum" set of strategies.

In terms of linear algebra this requirement is being defined as a set of $\prod\limits_{i=1}^{N} M_i$ equalities:

$$\widehat{J}^\dagger \left(\bigotimes_{i=1}^{N} \widehat{A}_i \right) \widehat{J} = \bigotimes_{i=1}^{N} \widehat{A}_i \quad \text{(where all } \widehat{A}_i \text{ are from the set (12.1))},$$

which has $\left(\prod\limits_{i=1}^{N} M_i\right)$-dimensional space of solutions:

$$\widehat{J} \in \left\{ \sum_{k_1=1}^{M_1} \sum_{k_2=1}^{M_2} \ldots \sum_{k_N=1}^{M_N} \lambda_{k_1 k_2 \ldots k_N} \left(\bigotimes_{j=1}^{N} E_{k_j} E_{k_j}^\dagger \right) : |\lambda_{k_1 k_2 \ldots k_N}| = 1 \right\},$$

where $E_{k_j} = \frac{1}{\sqrt{M_j}} \begin{pmatrix} \exp\left(2\pi i (k_j - 1) \frac{0}{M_j}\right) \\ \exp\left(2\pi i (k_j - 1) \frac{1}{M_j}\right) \\ \vdots \\ \exp\left(2\pi i (k_j - 1) \frac{M_j - 1}{M_j}\right) \end{pmatrix}$ is k_j^{th} eigenvector of $M_j \times M_j$ shift matrix.

Chapter 13

Voting Game

13.1 Introduction

Voting games are used as a model for analyzing different political processes, and in particular elections.

When more than two candidates are participating, voters sometimes have reason for the so-called *tactical voting.* Namely, a voter in some situations doesn't support the most preferred candidate, and acts just in order to prevent the undesirable candidate from winning an election.

There is a large variety of voting systems, including ones with rather exotic ballots and tallying methods. In this chapter we shall consider the basic case of a plurality voting system, where this tactical voting occurs in a quantum model of the game and brings a better outcome to all the voters.

Let us consider elections with 4 candidates and only 3 voters. Voters give their votes to exactly one candidate each, and the single winner (the candidate with the most votes) provides the appropriate payoffs to all voters according to his personal preferences. If there are more than one candidate with maximal number of votes, let us pick one of the leaders at random and assert him to be the winner (in this case we shall consider voters' payoffs as expected values).

It is convenient to call all the participants with appropriate names and represent the voters' payoffs for all four possible winning candidates as in Table 13.1:

Table 13.1: Voters' payoffs

		Candidates			
		Mr. A	Mr. B	Mr. C	Mr. Fairness
Voters	Mrs. A	3	0	0	2
	Mrs. B	0	3	0	2
	Mrs. C	0	0	3	2

13.2 Nash equilibria

When analyzing *plurality* (or *relative majority*) voting it is worth to mention that not all Nash equilibria can be treated as solutions.

E.g. let us consider such voting game with N voters. Each situation when at least $\lfloor \frac{N}{2} \rfloor + 2$ voters vote for one (possibly, very bad) candidate, formally speaking, is a Nash equilibrium: there is no a single voter who could improve his outcome by switching to another option (since a single vote is unable to affect the absolute majority). Of course, unanimous voting for an unfit candidate could not be considered as a stable one or even as making any common sense. What is the appropriate concept of decision in such situations?

For different practical purposes the so-called *refinements* must be applied on the set of Nash equilibria. E.g. in real voting processes a voter usually

- is not sure about other voters' decisions, especially when tactical voting makes sense;
- is not sure whether or not all the voters will participate in voting;
- is not sure whether or not some voters by accident will vote for undesired candidates or just spoil their voting bulletins;

- is not sure about how many mistakes will be made during checking and summing up the results of the voting;

At least some of these factors must be taken into account. In terms of game theoretical analysis it means applying the so-called *trembling hand refinement*. *Trembling hand perfect equilibrium* assumes a small probability ϵ for each player to change his choice to some different one [Sel74].

Thus in the voting game described above, *each* single vote has a chance to affect the majority, even if the probability of this effect is very small.

According to this refinement, let us assume that after voters completed their task, the tallying machine counts each voting bulletin properly with probability $1-3\epsilon$, and with probability 3ϵ makes mistake (in favor to one of the remaining candidates, with probability ϵ for each candidate).

Then the probabilities of winning in different cases of voting are as follows:

Table 13.2: Adjustment of winning probabilities for trembling hand perfect equilibrium

<table>
<tr><th>Combinations of votes</th><th>$\Pr\left[\substack{\text{Mr. A}\\ \text{wins}}\right]$</th><th>$\Pr\left[\substack{\text{Mr. B}\\ \text{wins}}\right]$</th><th>$\Pr\left[\substack{\text{Mr. C}\\ \text{wins}}\right]$</th><th>$\Pr\left[\substack{\text{Mr. Fairness}\\ \text{wins}}\right]$</th></tr>
<tr><td>3 × Mr. A</td><td>$1-21\epsilon^2+36\epsilon^3$</td><td colspan="3">$7\epsilon^2-12\epsilon^3$</td></tr>
<tr><td>2 × Mr. A,
1 × Mr. B</td><td>$1-4\frac{2}{3}\epsilon+9\frac{2}{3}\epsilon^2-12\epsilon^3$</td><td>$3\frac{1}{3}\epsilon-13\epsilon^2+14\frac{2}{3}\epsilon^3$</td><td colspan="2">$\frac{2}{3}\epsilon+1\frac{2}{3}\epsilon^2-1\frac{1}{3}\epsilon^3$</td></tr>
<tr><td>1 × Mr. A,
1 × Mr. B,
1 × Mr. C</td><td colspan="3">$\frac{1}{3}-\frac{1}{3}\epsilon+\frac{1}{3}\epsilon^2-1\frac{1}{3}\epsilon^3$</td><td>$\epsilon-\epsilon^2+4\epsilon^3$</td></tr>
</table>

All other cases are equivalent to above-stated ones up to permutation of candidates.

13.3 Classical version

Let us analyze the voting game with payoffs defined in Table 13.1.

The single trembling hand perfect equilibrium is “selfish voting”: it is easy to show that regardless of the other votes, Mrs. A’s best choice is to vote for Mr. A. Similar arguments will show that Mrs. B will vote for Mr. B, and Mrs. C will vote for Mr. C.

Mr. Fairness, whose leadership promises the biggest common benefit, will remain with no votes at all.

Summing up these arguments, we follow that Messrs. A, B and C will win with probabilities about $\frac{1}{3}$ each, thus providing Mesdames A, B and C with benefits about 1 for each of them [1] [2].

Let us now reformulate the process of voting game in terms of linear algebra, like it was done in Section 3.4 for Prisoner's Dilemma:

1. The game board consists of three unit vectors from $\{0,1\}^4$.
   Initially their values are $a_1 = b_1 = c_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$.

2. Voters independently choose shift operators A, B, C from $\left\{ \begin{pmatrix} 0&1&0&0 \\ 0&0&1&0 \\ 0&0&0&1 \\ 1&0&0&0 \end{pmatrix}^k : k \in \mathbb{N} \right\}$ and apply them respectively to a_1, b_1, c_1.
   Let us denote $a_2 = Aa_1, b_2 = Bb_1, c_2 = Cc_1$.

3. Resulting vectors a_2, b_2, c_2 are treated as probability distribution of choosing among four options available for voters.
   Note that the set of allowed operators in step 2 implement only pure strategies for voters. This restriction however is not crucial as in voting games use of mixed strategies generally makes no sense.

4. Winner is selected among the candidates according to Table 13.2, and voters get their payoffs according to Table 13.1.

Thus described above Nash equilibrium of our voting game asserts the following

[1] To be completely precise in accordance to Table 13.2, each voter's payoff is $1 + \epsilon - \epsilon^2 + 4\epsilon^3$, i.e. slightly bigger, because Nash equilibrium here is the worst decision in terms of common benefit, and deviation from this point (caused by *trembling hand*) improves the payoffs.

[2] Generally speaking, the set of Nash equilibria in such voting games might not consist of a single element (as it does in our case), but all Nash equilibria assume voters to use pure strategies (unlike general bimatrix or multimatrix games, where use of mixed strategies sometimes prevent players from big loss).

values:

$$a_1 = b_1 = c_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

$$A = \begin{pmatrix} 0&1&0&0 \\ 0&0&1&0 \\ 0&0&0&1 \\ 1&0&0&0 \end{pmatrix}^0 = \begin{pmatrix} 1&0&0&0 \\ 0&1&0&0 \\ 0&0&1&0 \\ 0&0&0&1 \end{pmatrix}, \quad B = \begin{pmatrix} 0&1&0&0 \\ 0&0&1&0 \\ 0&0&0&1 \\ 1&0&0&0 \end{pmatrix}^1 = \begin{pmatrix} 0&1&0&0 \\ 0&0&1&0 \\ 0&0&0&1 \\ 1&0&0&0 \end{pmatrix}, \quad C = \begin{pmatrix} 0&1&0&0 \\ 0&0&1&0 \\ 0&0&0&1 \\ 1&0&0&0 \end{pmatrix}^2 = \begin{pmatrix} 0&0&1&0 \\ 0&0&0&1 \\ 1&0&0&0 \\ 0&1&0&0 \end{pmatrix}$$

$$a_2 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \qquad b_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \qquad c_2 = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$$

13.4 Quantum version

We propose a quantization of this voting game by the general method described in Subsection 12.3. In the following voting scheme we numbered candidates from 0 to 3 as they appear in Table 13.1.

1. The game board consists of a three-qudit quantum system, where each qudit is a 4-level quantum subsystem.
   Initial state of the game board is $\psi_1 = |000\rangle$.

1_q Before all players' actions, an entangling operator $\widehat{J}$ (from the set, which we shall define later) is applied to the system, which gets "entangled" into state $\psi_{1_q} = \widehat{J}\psi_1$.

2. Players independently choose unitary operators $\widehat{A}, \widehat{B}, \widehat{C}$ and apply them one by one to the three qudits of the system. Its state changes to $\psi_2 = \left(\widehat{A} \otimes \widehat{B} \otimes \widehat{C}\right) \psi_{1_q}$.

2_q After all players' actions are done, an operator $\widehat{J}^\dagger$ is applied to the system.
Its state changes to $\psi_{2_q} = \widehat{J}^\dagger \psi_2$.
Let us denote $\psi_{2_q} = \sum_{i=0}^{3} \sum_{j=0}^{3} \sum_{k=0}^{3} \alpha_{ijk} |ijk\rangle$.

3. Resulting qubits are measured in computational basis, and the absolute squares of amplitudes $|\alpha_{ijk}|^2$ are treated as probabilities of voting for candidates i, j, k by the first, second and third voters respectively.

4. Winner is selected among the candidates according to Table 13.2, and voters get their

payoffs according to Table 13.1.

In order to keep "backward compatibility" with the set of classical strategies (like in the Prisoner's Dilemma) we must apply special constraints on the entangling operator $\widehat{J}$ in step 2_q. Namely, we must ensure that steps 1_q and 2_q won't affect state ψ_{2_q} in the case where all three voters choose unitary operators from the set $\left\{ \begin{pmatrix} 0&1&0&0\\ 0&0&1&0\\ 0&0&0&1\\ 1&0&0&0 \end{pmatrix}^k : k \in \mathbb{N} \right\}$, so that they are equivalent to shift operators from the classical version of game.

In terms of linear algebra this requirement is being defined as a set of $4^3 = 64$ equalities:

$$\widehat{J}^\dagger \left(\widehat{A} \otimes \widehat{B} \otimes \widehat{C} \right) \widehat{J} = \widehat{A} \otimes \widehat{B} \otimes \widehat{C}, \quad \text{where } \widehat{A}, \widehat{B}, \widehat{C} \in \left\{ \begin{pmatrix} 0&1&0&0\\ 0&0&1&0\\ 0&0&0&1\\ 1&0&0&0 \end{pmatrix}^k : k \in \mathbb{N} \right\},$$

which has 64-dimensional space of solutions:

$$\widehat{J} \in \left\{ \sum_{i=0}^{3} \sum_{j=0}^{3} \sum_{k=0}^{3} \lambda_{ijk} \left(E_i E_i^\dagger \otimes E_j E_j^\dagger \otimes E_k E_k^\dagger \right) : |\lambda_{ijk}| = 1 \right\},$$

where $E_0 = \frac{1}{2} \begin{pmatrix} 1\\1\\1\\1 \end{pmatrix}, E_1 = \frac{1}{2} \begin{pmatrix} 1\\i\\-1\\-i \end{pmatrix}, E_2 = \frac{1}{2} \begin{pmatrix} 1\\-1\\1\\-1 \end{pmatrix}, E_3 = \frac{1}{2} \begin{pmatrix} 1\\-i\\-1\\i \end{pmatrix}$ are eigenvectors of 4×4 shift matrices.

As an example we shall consider a symmetric bundle of λ's:

$$\lambda_{ijk} = \begin{cases} 1 & \text{if } i = j = k, \\ -1 & \text{otherwise,} \end{cases}$$

and corresponding 64×64 matrix

$$\widehat{J} = [m_{ij}], \qquad \text{where } m_{ij} = \begin{cases} -\frac{7}{8} & \text{if } i = j, \\ \frac{1}{8} & \text{if } i + \lfloor \frac{i}{4} \rfloor + \lfloor \frac{i}{16} \rfloor \equiv j + \lfloor \frac{j}{4} \rfloor + \lfloor \frac{j}{16} \rfloor \pmod 4, \\ 0 & \text{otherwise.} \end{cases}$$

13.5 Search for quantum Nash equilibrium

Although Nash equilibrium is known as the most important solution concept of non-zero-sum games, very little is known about efficient computing of Nash equilibria for an arbitrary game. For example, Megiddo and Papadimitriou [MP91] placed this problem for a *finite two-player game* into rather specific complexity class TFNP, and question about the precise computational complexity is still relevant.

Certainly, our problem for *infinite multiplayer game* is much less clear. In this chapter we shall only (a) show inconsistency of classical selfish voting in terms of Nash equilibrium and (b) provide a promising solution, which turns up, in a curious way, Pareto optimal.

All our considerations are based on numerical experiments, which model the process of iterative search for equilibrium point in the multidimensional space of strategies.

We start our search from an arbitrary point. So as to show inconsistency of classical Nash equilibrium, let us start with the selfish voting, i.e. with

$$\widehat{A} = \begin{pmatrix} 1&0&0&0\\ 0&1&0&0\\ 0&0&1&0\\ 0&0&0&1 \end{pmatrix}, \qquad \widehat{B} = \begin{pmatrix} 0&1&0&0\\ 0&0&1&0\\ 0&0&0&1\\ 1&0&0&0 \end{pmatrix}, \qquad \widehat{C} = \begin{pmatrix} 0&0&1&0\\ 0&0&0&1\\ 1&0&0&0\\ 0&1&0&0 \end{pmatrix}.$$

Then let us perform a series of the iterations. We first let Mrs. A slightly [3] change her unitary operator $\widehat{A}$ in order to increase her expected payoff (assuming $\widehat{B}$ and $\widehat{C}$ to remain unchanged). Then we make similar offer to Mrs. B, and then to Mrs. C. After that we repeat these three adjustments, starting again with Mrs. A, until some stable point is reached.

Changes of voters' payoffs during this iterative algorithm is displayed in Figure 13.1.

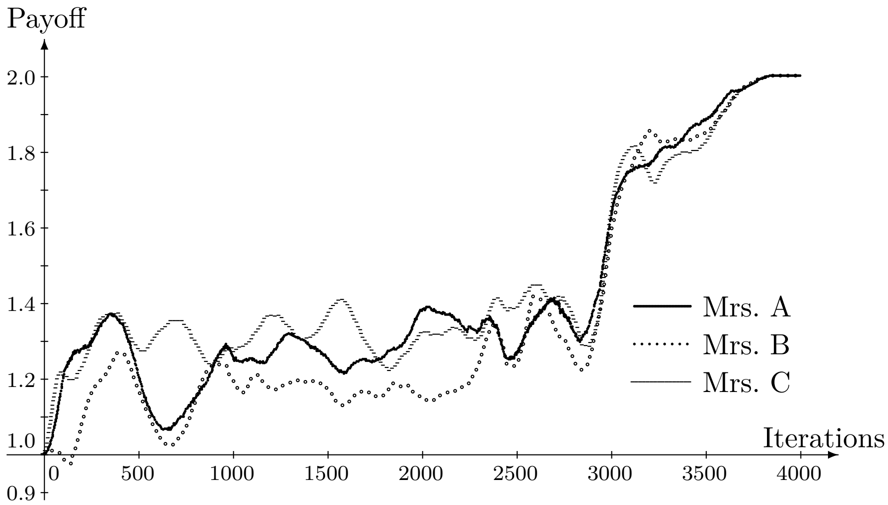
Sooner or later, voters' payoffs reach the neighborhood of a Pareto optimal point (and never leave it again), where each voter has payoff 2.

Basically, results of this (probably not the most efficient) algorithm suffice for both our purposes:

(a) It shows inconsistency of classical selfish voting in terms of Nash equilibrium. We can follow that if Mrs. B and Mrs. C stick to their classical optimal strategies, i.e.

[3] Say we can restrict $\max_{i,j} \left| \widehat{A}_{ij} - \widehat{A}'_{ij} \right| \leq 0.01$, where $\widehat{A}'$ is Mrs. A's operator after the change is made. Actually we just restricted the distance between $\widehat{A}$ and $\widehat{A}'$ in the parametrized space of $M \times M$ unitary operators.

Figure 13.1: Voters' payoffs during evolution



$\widehat{B} = \begin{pmatrix} 0&1&0&0\\ 0&0&1&0\\ 0&0&0&1\\ 1&0&0&0 \end{pmatrix}$ and $\widehat{C} = \begin{pmatrix} 0&0&1&0\\ 0&0&0&1\\ 1&0&0&0\\ 0&1&0&0 \end{pmatrix}$, then there exists a strategy for Mrs. A, which is significantly better than $\widehat{A} = I$. E.g. choosing $\widehat{A} = \begin{pmatrix} -1&0&0&0\\ 0&1&0&0\\ 0&0&1&0\\ 0&0&0&1 \end{pmatrix}$ will provide her with expected outcome $\frac{101}{64}$ (while Mrs. B will get $\frac{47}{64}$, and Mrs. C will get $\frac{53}{64}$).

(b) It provides us with a non-rigorous equilibrium, which probably could be proven analytically. We shall not go into greater detail, as this was just a specific example for illustration of the general game quantization method.

Chapter 14

Possible Issues

14.1 Objections on EWL scheme

In [EP02] van Enk and Pike provide some criticism on the quantum Prisoner's Dilemma constructed by Eisert et al. in [EWL99, EW00]. Namely, they argue that this generalization of classical Prisoner's Dilemma is somewhat equivalent to offering a new classical choice $\boldsymbol{Q}$ for each of the players, so that the payoff matrix in Table 3.1 is expanded as in Table 14.1.

Table 14.1: Players' payoffs in Prisoner's Dilemma with an extra choice $\boldsymbol{Q}$

		Your partner		
		Confesses	Denies	$\boldsymbol{Q}$s
You	Confess	4y. for You, 4y. for Your partner	0y. for You, 5y. for Your partner	**5y.** for You, **0y.** for Your partner
	Deny	5y. for You, 0y. for Your partner	2y. for You, 2y. for Your partner	**4y.** for You, **4y.** for Your partner
	$\boldsymbol{Q}$	**0y.** for You, **5y.** for Your partner	**4y.** for You, **4y.** for Your partner	**2y.** for You, **2y.** for Your partner

Obviously, a mutual choice of $\boldsymbol{Q}$ is the single Nash equilibrium.

Additionally, authors of [EP02] provide some arguments of rather philosophical nature. Namely, they treat step 2_q as an activity of an attorney or interrogator which actually helps the prisoners. Providing prisoners with such assistance certainly is counter to the spirit of the game.

Finally, Benjamin and Hayden [BH01a] showed that when the set of strategies is not restricted with two-parametric $\widehat{U}\left(\theta,\phi\right)$, and players are allowed to use any local unitary operator, then strategies $\widehat{A}=\widehat{B}=\widehat{U}\left(0,\frac{\pi}{4}\right)$ do not remain a Nash equilibrium. Moreover, they show that in such settings no Nash equilibrium for the quantum Prisoners' Dilemma exists.

This criticism, of course, should be taken into account when constructing a quantum version of a game. Although first two objections (by van Enk and Pike) seem not to be that relevant for the voting game (described in Chapter 13), the comment by Benjamin and Hayden is worth some complementary discussion.

14.2 Comment on Nash equilibria in quantized games

The fact is that quantization by [EWL99] is claimed to be a generalization of the *mixed expansion* of Prisoner's Dilemma. But, as it is noted in [BH01a], Nash's theorem may not work any more under these circumstances.

Unlike quantization of Prisoner's Dilemma with exactly two pure classical strategies per player, the more general quantization proposed in this part is claimed to be an expansion, which does not implement mixed strategies in the sense of classical probabilities [1]. It is not clear whether Nash's theorem works for this *quantum expansion* of the game. While it might not be relevant for the quantum voting game, overall situation needs some futher reasoning on existance of Nash equilibrium points.

For both quantization schemes (by [EWL99, EW00] and by Part III of this thesis) the following reasoning seems to be quite natural. Since sets of quantum strategies are

[1] This feature can be qualified as a drawback in comparison with EWL scheme, but our further considerations in this chapter show that it is not that significant. In fact, implementing mixed strategies appear to be obsolete, when speaking about Nash equilibria.

compact, and the payoff function is a continuous mapping to the compact (N-dimensional) space of payoffs, one can observe such quantum game as a basic case of classical game with infinite set of strategies. In game theory it is a well-known fact that for mixed expansion of such game exists a Nash equilibrium [Gli52]. In particular, for quantum Prisoner's Dilemma all Nash equilibrium points consist of mixed strategies. In general, search for a Nash equilibrium may require analysis of superoperators as players' strategies and mixed quantum states as objects for the final measurement of step 2_q.

From this point of view the only fundamental difference between the two quantization schemata is as follows:

(a) EWL scheme is a "quantum-over-mixed" expansion of an original classical game;

(b) our scheme is just a "quantum" expansion, which contains only *pure strategies* as a special case, and does not contain *mixed strategies* in the sense of classical probabilistic choice.

But in both cases, generally speaking, we need to apply further mixed expansion (one can call it "*mixed-over-quantum expansion*") of the resulting game in order to figure out its Nash equilibria.

Chapter 15

Summary

Part III is devoted to the analysis of players' interaction in a special but large class of quantum games, which we call *games with quantum decisions*. The strategies of the above-mentioned games are operations undertaken on qubits, whilst players' winnings are calculated taking into account the results of quantum system measurements. The classical choices of players account only for a limited ratio of various quantum operations, which often does not allow the maximally effective approach by rationally thinking players. The usage of quantum strategies makes it possible to sufficiently enlarge players' abilities to interact among themselves applying quite rational principles.

Quantum Prisoner's Dilemma (see Section 3.4 in Part I) may serve as a basic illustration of a game with quantum decisions. In Chapter 12 we provided a technique, which is of similar spirit but technically different, which allows quantization of games with arbitrary many players and arbitrary many players' choices.

In Chapter 13 we illustrated ideas of Chapter 12 by quantizing a specific noncooperative game, which models the process of elections. We also provided computer experiments modeling the behavior of participants in a system, which is working under the laws of quantum theory.

In Chapter 14 we study some objections on quantum Prisoner's Dilemma which arose after work [EWL99]. We analyzed these issues (by Benjamin and Hayden [BH01a], and by van Enk and Pike [EP02]), and evaluated their relevance to our proposed quantization scheme of Chapter 12 and to the specific quantized voting game of Chapter 13. We followed that although the above-mentioned objections may be not that relevant to the voting game, some of them must be born in mind when constructing new quantum versions of classical games.

Conclusion

The topic of quantum games began to attract the attention of researchers quite recently, following the works [Vai99, Mey99, EWL99]. Perhaps this interest could be explained by the relative affordability of these games for real physical experiments. The fact is that implementing most of these games only requires operations on separate qubits, and all the necessary technologies are already available in experimental quantum optics.

For example, Chinese physicists successfully conducted a number of physical experiments [DLX^{+}01] based on the theoretical model described in [EWL99]; thus, confirming the general applicability of the EWL scheme.

Another topic — nonlocal games — is of particular interest in quantum information. These games also are being successfully implemented in real physical experiments. Similar experiments in the context of Bell inequalities were performed long before the concept of quantum games (for example, in [AGR81]), but the results of these experiments could easily be interpreted as an argument in favor of the applicability of the concept of nonlocal quantum games. Today, these and similar experiments are still considered relevant, and one of the latest results in experimental physics, concerning the nature of the nonlocality effect is, for example, the work [MHS^{+}12].

Therefore, one can say that, despite its relative youth, the theory of quantum games is already confirmed experimentally and has good prospects for practical use (in particular, in the field of cryptography, see, e.g., [BB84, Eke91]). This fact distinguishes quantum games from other areas of quantum computing, which often require complex technologies to manipulate large quantum systems, and have not yet been confirmed in large-scale experiments.

On the other hand, studies of some theoretical aspects of quantum games remain insufficient.

For example, games with quantum decisions have so far been presented only as analogs of classic games with binary strategies. (Probably the only exception is the recently introduced quantum Kolkata Restaurant Problem [SH11] with three strategies for each player.) Chapters 12 and 13 of the thesis fill this gap, but they can only be considered as a first step on the way to studying quantum games with an arbitrary number of strategies.

The effects of quantum nonlocality are now being given much more attention. However, in this area there are still many open questions. For example, researchers still do not have a common understanding of the measure of entanglement of quantum subsystems (at least, for systems consisting of more than two qubits, there are several different entanglement measures, see, e.g., [DVC00]). Reaching a common understanding of this issue will perhaps help quantum game theory, where the equivalent open question is formulated as the advantage of quantum strategies over classical ones. In this sense, games discussed in Chapters 5 to 9 of the thesis represent estimates of the entanglement measure of a quantum system in GHZ state $\frac{1}{\sqrt{2}}\left(|0\rangle^{\otimes N} + |1\rangle^{\otimes N}\right)$. This state is often called “the most entangled”; however, authors of [PWP$^+$08] show that it does not always give the maximum benefit, which could be achieved with the use of the properties of quantum nonlocality.

These and other questions of quantum game theory require further consideration, and as practice shows, such issues often involve a wide range of different mathematical methods.

Bibliography

[ABB+10] 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, *Phys. Rev. Lett.*, 104:230404 (2010).

[ABB+12] A. Ambainis, A. Bačkurs, K. Balodis, D. Kravchenko, R. Ozols, J. Smotrovs, M. Virza. Quantum strategies are better than classical in almost any XOR game, *Proceedings of ICALP'2012*, 1:25–37 (2012).

[AGR81] A. Aspect, P. Grangier, G. Roger. Experimental tests of realistic local theories via Bell's theorem, *Phys. Rev. Lett.*, 47(7):460–463 (1981).

[AIKV12] A. Ambainis, J. Iraids, D. Kravchenko, M. Virza. Advantage of Quantum Strategies in Random Symmetric XOR Games, *Proceedings of MEMICS'2012*, 57–68 (2012).

[AKNR10] A. Ambainis, D. Kravchenko, N. Nahimovs, A. Rivosh. Quantum XOR games for large number of players, *Proceedings of TAMC'2010*, 72–83 (2010).

[AKN+13] A. Ambainis, D. Kravchenko, N. Nahimovs, A. Rivosh, M. Virza. On Symmetric Nonlocal Games, *Theoretical Computer Science*, 494:36–48 (2013).

[Ard92] M. Ardehali. Bell inequalities with a magnitude of violation that grows exponentially with the number of particles, *Phys. Rev. A*, 46:5375–5378 (1992).

[AGR81] A. Aspect, Ph. Grangier, G. Roger. Experimental Tests of Realistic Local Theories via Bell's Theorem, *Phys. Rev. Lett.*, 47:460–463 (1981).

[BB84] C.H. Bennett, G. Brassard. Quantum cryptography: Public key distribution and coin tossing, *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*, 175–179 (1984).

[Bel64] J. Bell. On the Einstein-Podolsky-Rosen paradox, *Physics*, 1(3):195–200 (1964).

[BH01a] S.C. Benjamin, P.M. Hayden. Comment on "Quantum Games and Quantum Strategies", *Phys. Rev. Lett.*, 87(6):069801 (2001).

[BH01b] S.C. Benjamin, P.M. Hayden. Multi-Player Quantum Games, *Phys. Rev. A*, 64(3):030301 (2001).

[BL01] P. Borwein, R. Lockhart. The Expected L_p Norm of Random Polynomials, *Proceedings of the American Mathematical Society*, 129(5):1463–1472 (2001).

[BMMN11] M. Braverman, K. Makarychev, Y. Makarychev, A. Naor. The Groethendieck constant is strictly smaller than Krivine's bound, *Proceedings of FOCS'2011*, 453–462 (2011).

[BRSW11] H. Buhrman, O. Regev, G. Scarpa, R. de Wolf. Near-optimal and explicit Bell inequality violations, *Proceedings of CCC'2011*, 157–166 (2011).

[BV12] J. Briët, T. Vidick. Explicit Lower and Upper Bounds on the Entangled Value of Multiplayer XOR Games. *Communications in Mathematical Physics*, Online First Articles (2012).

[CHSH69] J.F. Clauser, M.A. Horne, A. Shimony, R.A. Holt. Proposed Experiment to Test Local Hidden-Variable Theories, *Phys. Rev. Lett.*, 23:880 (1969).

[CHTW04] R. Cleve, P. Høyer, B. Toner, J. Watrous. Consequences and limits of nonlocal strategies, *Proceedings of CCC'2004*, 236–249 (2004).

[Cir80] B.S. Tsirelson. Quantum generalizations of Bell's inequality, *Letters in Mathematical Physics*, 4(2):93–100 (1980).

[DLX$^+$01] J. Du, H. Li, X. Xu, M. Shi, J. Wu, X. Zhou, R. Han. Experimental realization of quantum games on a quantum computer, *Phys. Rev. Lett.*, 88:137902 (2002).

[DVC00] W. Dür, G. Vidal, J.I. Cirac. Three qubits can be entangled in two inequivalent ways, *Phys. Rev. A*, 62:062314 (2000).

[Eke91] A.K. Ekert. Quantum cryptography based on Bell's theorem, *Phys. Rev. Lett.*, 67(6):661–663 (1991).

[EP02] S.J. van Enk, R. Pike. Classical Rules in Quantum Games, *Phys. Rev. A*, 66:024306 (2002).

[EW00] J. Eisert, M. Wilkens. Quantum Games, *Journal of Modern Optics*, 47:2543–2556 (2000).

[EWL99] J. Eisert, M. Wilkens, M. Lewenstein. Quantum Games and Quantum Strategies, *Phys. Rev. Lett.*, 83:3077 (1999).

[GHZ89] D.M. Greenberger, M.A. Horne, A. Zeilinger. Bell's theorem, Quantum Theory, and Conceptions of the Universe, *Kluwer Academic Publishers*, ISBN 0-792-30496-9, 37:69–72 (1989).

[Gli52] I.L. Glicksberg. A further generalization of the Kakutani fixed point theorem with application to Nash equilibrium points, *Proceedings of the American Mathematical Society*, 3:170–174 (1952).

[Gro53] A. Grothendieck. Résumé de la théorie métrique des produits tensoriels topologiques, *Boletim da Sociedade de Matemática de São Paulo*, 8:1–79 (1953).

[Hal73] G. Halász. On a result of Salem and Zygmund concerning random polynomials, *Studia Scientiarum Mathematicarum Hungarica*, 8:369–377 (1973).

[Kas87] B.S. Kashin. The properties of random polynomials with coefficients ±1, *Vestnik Moskovskogo Universiteta. Seriya 1. Matematika. Mekhanika*, 5:40–46 (1987).

[KKM+08] J. Kempe, H. Kobayashi, K. Matsumoto, B. Toner, T. Vidick. Entangled Games are Hard to Approximate, *Proceedings of FOCS'2008*, 447–456 (2008).

[Kra01] I. Krasikov. Nonnegative Quadratic Forms and Bounds on Orthogonal Polynomials, *Journal of Approximation Theory*, 111(1):31–49 (2001).

[Kra13] D. Kravchenko. A New Quantization Scheme for Classical Games, *Proceedings of Workshop on Quantum and Classical Complexity (Satellite event to ICALP'2013)*, 17–34 (2013).

[Kri77] J.-L. Krivine. Sur la constante de Grothendieck, *Comptes Rendus de l'Académie des Sciences, Series A–B*, 284:A445–A446 (1977).

[LLP10] T. Lawson, N. Linden, S. Popescu. Biased nonlocal quantum games, *arXiv:1011.6245v1* [quant-ph] (2010).

[Mer90] D. Mermin. Extreme Quantum Entanglement in a Superposition of Macroscopically Distinct States, *Phys. Rev. Lett.*, 65:15 (1990).

[Mey99] D.A. Meyer. Quantum strategies. *Phys. Rev. Lett.* 82:1052-1055 (1999).

[MHS+12] E. Megidish, A. Halevy, T. Shacham, T. Dvir, L. Dovrat, H.S. Eisenberg. Entanglement Between Photons that have Never Coexisted, *Frontiers in Optics Conference*, FTh2C:4 (2012).

[MP67] V.A. Marchenko, L.A. Pastur. Distribution of eigenvalues for some sets of random matrices, *Mathematics of the USSR. Sbornik*, 1:457–483 (1967).

[MP91] N. Megiddo, C. Papadimitriou. A note on total functions, existence theorems and complexity, *Theoretical Computer Science*, 81:317–324 (1991).

[Neu28] J. von Neumann. Zur Theorie der Gesellschaftspiele, *Mathematische Annalen*, 100(1):295–320 (1928).

[NM53] J. von Neumann, O. Morgenstern. Theory of games and economic behavior, *Princeton University Press* (1953).

[NRTV07] N. Nisan, T. Roughgarden, E. Tardos, V.V. Vazirani. Algorithmic Game Theory, *Cambridge University Press*, ISBN 0-521-87282-0 (2007).

[Pou92] W. Poundstone. Prisoner's Dilemma, *New York: Anchor Books*, ISBN 0-385-41580-X (1992).

[PWP+08] D. Perez-Garcia, M.M. Wolf, C. Palazuelos, I. Villanueva, M. Junge. Unbounded violation of tripartite Bell inequalities, *Communications in Mathematical Physics*, 279:455 (2008).

[Ree91] J.A. Reeds. A new lower bound on the real Grothendieck constant (unpublished manuscript,
available at `http://www.dtc.umn.edu/reedsj/bound2.dvi`, 1991).

[Sel74] R. Selten. Reexamination of the Perfectness Concept for Equilibrium Points in Extensive Games, *Institut für Mathematische Wirtschaftsforschung an der Universität Bielefeld*, Issue 23 of Working papers (available at `http://www.imw.uni-bielefeld.de/research/wp23.php`, 1974). Also *International Journal of Game Theory*, 4:25–55.

[SH11] P. Sharif, H. Heydari. Quantum solution to a three player Kolkata restaurant problem using entangled qutrits, *arXiv:1111.1962* [quant-ph] (2011).

[Sha80] R. Shankar. Principles of Quantum Mechanics, *Plenum Press*, ISBN 0-306-40397-8 (1980).

[SZ54] R. Salem, A. Zygmund. Some properties of trigonometric series whose terms have random signs, *Acta Mathematica*, 91:245–301 (1954).

[Tao11] T. Tao. Topics in Random Matrix Theory (draft of a book, available at http://terrytao.files.wordpress.com/2011/02/matrix-book.pdf, 2011).

[Vai99] L. Vaidman. Variations on the theme of the Greenberger-Horne-Zeilinger proof, *Foundations of Physics*, 29:615 (1999).

[WW01a] R.F. Werner, M.M. Wolf. Bell inequalities and Entanglement, *Quantum Information & Computation*, 1(3):1–25 (2001).

[WW01b] R.F. Werner, M.M. Wolf. All multipartite Bell correlation inequalities for two dichotomic observables per site, *Phys. Rev. A*, 64:032112 (2001).

[ZB02] M. Zukowski, C. Bruckner. Bell's theorem for general N-qubit states, *Phys. Rev. Lett.*, 88:210401 (2002).