Université de Montréal

Multi-Prover and Parallel Repetition in Non-Classical Interactive Games

par
Tommy Payette

Département d'informatique et de recherche opérationelle
Faculté des arts et des sciences

Mémoire présenté à la Faculté des arts et des sciences
en vue de l'obtention du grade de Maître ès sciences (M.Sc.)
en informatique

Août 2009

Université de Montréal
Faculté des arts et des sciences

Ce mémoire intitulé:

Multi-Prover and Parallel Repetition in Non-Classical Interactive Games

présenté par:

Tommy Payette

a été évalué par un jury composé des personnes suivantes:

Alain Tapp
président-rapporteur

Louis Salvail
directeur de recherche

Gilles Brassard
codirecteur

Geňa Hahn
membre du jury

Mémoire accepté le:

Résumé

Depuis l'introduction de la mécanique quantique, plusieurs mystères de la nature ont trouvé leurs explications. De plus en plus, les concepts de la mécanique quantique se sont entremêlés avec d'autres de la théorie de la complexité du calcul. De nouvelles idées et solutions ont été découvertes et élaborées dans le but de résoudre ces problèmes informatiques. En particulier, la mécanique quantique a secoué plusieurs preuves de sécurité de protocoles classiques.

Dans ce mémoire, nous faisons un étalage de résultats récents de l'implication de la mécanique quantique sur la complexité du calcul, et cela plus précisément dans le cas de classes avec interaction. Nous présentons ces travaux de recherches avec la nomenclature des jeux à information imparfaite avec coopération. Nous exposons les différences entre les théories classiques, quantiques et non-signalantes et les démontrons par l'exemple du jeu à cycle impair. Nous centralisons notre attention autour de deux grands thèmes : l'effet sur un jeu de l'ajout de joueurs et de la répétition parallèle. Nous observons que l'effet de ces modifications a des conséquences très différentes en fonction de la théorie physique considérée.

Mots clés: preuves intéractives à plusieurs prouveurs, jeux du cycle impair, nonlocalité, complexité du calcul quantique, intrication.

Abstract

Since the introduction of quantum mechanics, many mysteries of nature have found explanations. Many quantum-mechanical concepts have merged with the field of computational complexity theory. New ideas and solutions have been put forward to solve computational problems. In particular, quantum mechanics has struck down many security proofs of classical protocols.

In this thesis, we survey recent results regarding the implication of quantum mechanics to computational complexity and more precisely to classes with interaction. We present the work done in the framework of cooperative games with imperfect information. We give some differences between classical, quantum and no-signaling theories and apply them to the specific example of Odd Cycle Games. We center our attention on two different themes: the effect on a game of adding more players and of parallel repetition. We observe that depending of the physical theory considered, the consequences of these changes is very different.

Keywords: multi-prover interactive proofs, Odd Cycle Games, non-locality, quantum computational complexity, entanglement.

Contents

List of Symbols and Abbreviations

Abbreviation	Description	Definition
$\mathbb{Z}$	Set of natural number	
$\mathbb{R}$	Set of real numbers	
$\mathbb{C}$	Set of complex numbers	
$\|\psi\rangle$	Quantum State	page 5
I	Identity matrix	page 7
δ	Kronecker delta function	page 7
POVM	Positive Operator-Valued Measure	page 10
EPR	Einstein-Podolsky-Rosen	page 13
XOR	Exclusive-OR	page 23

List of Figures

Acknowledgements

I would like to thank my supervisors, Louis Salvail and Gilles Brassard, for their help and support. I would also like to thank my friends and my family for their encouragement, from which I found the motivation to complete this thesis.

Chapter 1

Introduction

Nowadays, information is a fundamental concept in computer science as well as in pure physics. Physicists and other scientists try to uncover the mysteries behind nature using physical phenomena that can be explained, or at least approximated, to certain degrees with mathematical equations. At the same time, computer scientists work on a more abstract level to understand the amount of computational resources necessary to solve a problem. The two fields meet each other because any information system is implemented by physical means and is governed by a physical model. The link between physics and computer science is becoming even more important as computer components decrease in size. Indeed, at the limits of the nanometer scale, the choice of the physical model has a deep impact on the analysis of the computational resources. The most successful physical theory, quantum mechanics, has grown in popularity and has successfully explained many phenomena of nature.

1.1 Incompleteness of Classical Theory

It was proven in 1964 that a purely classical explanation of physical phenomena was incompatible with the predictions of quantum mechanics [Bel64]. At that time, some physicists thought that it was impossible for an event to have an effect instantaneously on another one. A local hidden theory is a theory that follows these lines of ideas. Another theory, quantum mechanics, allows in certain situation instantaneous correlations. It was proven in [Bel64] that predictions from quantum mechanics could

not be explained by local hidden theories.

This had many implications in the field of computational complexity theory since classification was made only with classical resources. When quantum mechanical concepts are taken into account, many classes of resources have to be redefined and new consequences emerge.

In this thesis, we present recent results about the differences of already established computational classes when non-classical physical resources are considered. We center our attention on classes with interaction and only to those with classical communication between the parties. To demonstrate the results, we use the framework of games, which are well suited for this type of classes. In particular, we survey how the addition of more players affects the outcome of a game and what consequences parallel repetition has on games.

1.2 Related Works

We are mainly interested in how quantum mechanics changes the setting of computational complexity classes with interaction, classical messages and cooperative provers. Other classes are described with different properties than the one we are interested. We give a brief summary of the related work.

There exist complexity classes for which interaction is done through a quantum channel: the class *QIP* (Quantum Interactive Proofs) [Wat03, KW00] and its multi-prover analogue, the class *QMIP* (Quantum Multi-prover Interactive Proofs)[KM02]. It has recently been shown [JJUW09] that $QIP = PSPACE$.

Other interactive complexity classes related to the subject include the classes *RG* (Referee Games) in the classical setting [Pap85, KM90] and *QRG* (Quantum Referee Games) in the quantum setting [Gut05, GW04, GW07]. In both of these classes, the provers are in competition with each other.

Some have studied zero-knowledge interactive classes in the classical setting [GMW91, GMR89] and in the quantum setting [Wat02, Wat06, Kob07].

Finally, there are interesting results related to the hardness of approximation of the value of games in [IKP$^+$07, KRT07, KKM$^+$08].

1.3 Contribution

The thesis describes many results and presents them in an organized manner to help the reader understand how the physical theory considered affects computational classification. It is not meant to be a comprehensive survey since this topic is still very active. However, results are chosen to indicate possible future lines of work, to the best of our knowledge. The contribution of the author is to group the research papers in a concise and organized manner through a unified notation for clear understanding.

1.4 Structure of the Thesis

The remainder of this thesis is divided into five chapters. Chapter 2 introduces the notions of quantum mechanics needed for this thesis. Chapter 3 introduces the notions of computational complexity theory and serves as a motivation for the study of games. Chapter 4 gives a description of the game framework. Chapters 5 and 6 are selections of results from recent papers. Chapter 5 presents results for multi-prover games and chapter 6, results on parallel repetition. Each of these chapters is divided into three sections: classical theory, non-classical theory and a section with a specific example.

Chapter 2

Quantum Information

The purpose of the present chapter is to introduce the reader to the notions of quantum information. This chapter is not intended to be a comprehensive introduction to the topic but rather presents essential tools of quantum information needed to understand this thesis. For more information on the topic, the reader is encouraged to consult [NC00]. Note that we assume that the reader is familiar with basic notions of linear algebra.

2.1 The Qubits

Like the classical bits, quantum bits, or *qubits* for short, are parts of a mathematical representation of a physical system. This abstraction is similar to the concept of states *on* and *off* in electronics for the underlying voltage measures they represent. There are many ways to construct the physical implementation to produce qubits but these techniques are beyond the scope of this thesis.

Analogously to the values 0 and 1 of a classical bit, a qubit can take values $|0\rangle$ and $|1\rangle$. Although classical bits are uniquely restricted to values 0 and 1, qubits can be in superposition of states $|0\rangle$ and $|1\rangle$ as in

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

where $|\psi\rangle$ is used to describe the state and α and β are complex numbers with the restriction $|\alpha|^2 + |\beta|^2 = 1$. Qubits can, therefore, be represented in a two-dimensional complex vector space with orthonormal basis $|0\rangle$ and $|1\rangle$.

By the nature of quantum mechanics, it is not possible to measure directly the values α and β to get a complete description of the state $|\psi\rangle$. Rather, when a qubit is measured with respect to the orthonormal basis, the observation is 0 with probability $|\alpha|^2$ or 1 with probability $|\beta|^2$.

2.2 Systems of Qubits and their Evolution

In general, the state of an n-qubit system can be represented in a 2^n-dimensional vector space with complex inner product over $\mathbb{C}$.

The standard notation in quantum mechanics is called the Dirac notation. This notation represents a vector by $|\psi\rangle$ where ψ is a label for the vector. In this formalism, the object $|\psi\rangle$ is called a *ket* and the object $\langle\psi|$ is called a *bra*. The *ket* being a vector from a vector space, the *bra* is defined to be the conjugate transpose of the *ket*

$$\langle\psi| = |\bar{\psi}\rangle^T = |\psi\rangle^\dagger$$

where the *dagger* sign † indicates the conjugate transpose. We denote the inner and outer product between vector $|\varphi\rangle$ and $|\psi\rangle$ by $\langle\varphi|\psi\rangle$ and $|\varphi\rangle\langle\psi|$, respectively. The name *bra* and *ket* have been taken from the definition of the inner product $\langle\varphi|\psi\rangle$ that is the *bracket*.

We describe a method to enlarge vector spaces. This is often erroneously called the tensor product but it should be really called the Kronecker product. The Kronecker product $U \otimes V$ of two matrices U and V of dimension $M \times M$ and $N \times N$ is calculated as follows. First, we write

$$\begin{pmatrix} u_{11}V & u_{12}V & \dots & u_{1M}V \\ u_{21}V & u_{22}V & \dots & u_{2M}V \\ \vdots & \vdots & \ddots & \vdots \\ u_{M1}V & u_{M2}V & \dots & u_{MM}V \end{pmatrix} \tag{2.2}$$

where u_{ij} is the element in the i^{th} row and j^{th} column of the matrix U. Matrix (2.2) is a $M \times M$ matrix of $N \times N$ matrices. The final Kronecker product $U \otimes V$ is given by removing the parentheses for the matrices V in (2.2) producing an $MN \times MN$ matrix [Bra].

For notational convenience, when using the *ket* representation of vectors in Kronecker products, the symbol $\otimes$ can be dropped. For example, we can write the Kronecker product of $|0\rangle$ and $|0\rangle$ by $|0\rangle \otimes |0\rangle = |0\rangle|0\rangle = |00\rangle$.

It would be useless to describe the state of a physical system at a particular time without being able to observe its evolution through time. In

fact, the evolution of a closed system can be described by transformations (unitary).

A transformation on a state can be represented either with matrix notation or by a set of linear transformations on the basis of this state. For example, transformations on qubits are represented by

$$U = \begin{bmatrix} u_{00} & u_{01} \\ u_{10} & u_{11} \end{bmatrix}$$

or equivalently by the set of transformations

$$|0\rangle \overset{U}{\longmapsto} u_{00}|0\rangle + u_{10}|1\rangle$$

$$|1\rangle \overset{U}{\longmapsto} u_{01}|0\rangle + u_{11}|1\rangle$$

where $u_{ij} \in \mathbb{C}$ with the condition that U is unitary.

Definition 2.2.1. [Unitary Transformations] A transformation U is said unitary if

$$UU^\dagger = I$$

where I is the identity matrix with the same dimensions as matrix U.

Definition 2.2.1 is correct for finite Hilbert spaces. For infinite Hilbert spaces, we would also require $U^\dagger U = I$. Unitary transformations play an essential role in quantum mechanics. If the state of the system is $|\psi\rangle$ at time t_1 and $|\psi'\rangle$ at time t_2, then there exists a unitary transformation U that relates the two closed states by

$$|\psi'\rangle = U|\psi\rangle.$$

Note that quantum mechanics only indicate that the unitary transformation U exists; it does not indicate which unitary operator U it is.

It is worth mentioning at this point a very useful unitary transformation, the Hadamard transformation, defined by

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

and whose uses will be seen later.

In some cases, unitary transformations are not applied to the whole system. Take, for example, the case when the two qubits of a two-qubit system $|\psi\rangle$ are physically separated. If a unitary transformation U is applied on

the second qubit only, the effect on the system is given by unitary transformation $(I \otimes U)$. In general for a two-qubit system, applying a unitary operation U_1 on the first part of the system and U_2 on the second part of the system is equivalent to applying the unitary transformation $U_1 \otimes U_2$ on the whole system.

2.3 The Trace Function

A useful tool from linear algebra that will be used in this thesis is the trace function.

Definition 2.3.1 (Trace)**.** The trace of a matrix A is defined to be the sum of its diagonal elements:

$$\mathrm{tr}(A) = \sum_i A_{ii}.$$

The trace has two important properties. For two matrices A and B whose products AB and BA exist, and a complex number z, the trace is linear

$$\mathrm{tr}(zA + B) = z\mathrm{tr}(A) + \mathrm{tr}(B),$$

and it satisfies

$$\mathrm{tr}(AB) = \mathrm{tr}(BA). \tag{2.3}$$

For an operator A and a state $|\psi\rangle$, it can be shown that property (2.3) of the trace implies

$$\mathrm{tr}(A|\psi\rangle\langle\psi|) = \langle\psi|A|\psi\rangle. \tag{2.4}$$

For multi-qubit systems or systems of states, the trace can be taken only with respect to a certain qubit or state, this is called the partial trace. In this case, the qubit or the state in question is indicated as a subscript.

Definition 2.3.2 (Partial Trace)**.** Consider two states A and B with two vectors $|a_1\rangle, |a_2\rangle \in A$ and $|b_1\rangle, |b_2\rangle \in B$ from their appropriate state space and a state described by $\rho = |a_1\rangle\langle a_2| \otimes |b_1\rangle\langle b_2|$. Then the partial trace of ρ with respect to B is given by

$$\begin{aligned}\rho_A &= \mathrm{tr}_B(\rho) \\ &= |a_1\rangle\langle a_2|\mathrm{tr}(|b_1\rangle\langle b_2|) \\ &= |a_1\rangle\langle a_2|\langle b_1|b_2\rangle\end{aligned}$$

where ρ_A is the reduced state of ρ on system A. The definition of the partial trace can be generalized with linearity on its input.

2.4 Measurements

Now that we know that the state of a physical system can be represented by $|\psi\rangle$ and its evolution in time by a unitary transformation U, we need to describe a mechanism to get information from a state. We obtain it by measuring the state but the information gained is dependent on the measurement made. Measurements are described by a collection $\{M_m\}$ of measurement operators living in the space of the state to be measured where the index m refers to the outcome of the measurement. The measurement operators are subject to the completeness equation

$$\sum_m \quad M_m^\dagger M_m = I. \tag{2.5}$$

If the system is in state $|\psi\rangle$ immediately before measurement, then the probability that outcome m occurs after measurement is given by

$$\Pr_{|\psi\rangle}[m] = \langle\psi|M_m^\dagger M_m|\psi\rangle = \mathrm{tr}(M_m^\dagger M_m|\psi\rangle\langle\psi|). \tag{2.6}$$

The measurement changes the state of the system to

$$|\psi'\rangle = \frac{M_m|\psi\rangle}{\sqrt{\langle\psi|M_m^\dagger M_m|\psi\rangle}}$$

Before giving an example of a measurement on a state, we define two important properties that an operator can have.

Definition 2.4.1 (Hermitian Operator)**.** We say that an operator P is Hermitian if

$$P = P^\dagger. \tag{2.7}$$

Definition 2.4.2 (Orthogonal Operator)**.** We say that two operator P_m and $P_{m'}$ are orthogonal if

$$P_m P_{m'} = \delta_{m,m'} P_m \tag{2.8}$$

where $\delta_{m,m'}$ is the Kronecker delta function defined by

$$\delta_{m,m'} = \begin{cases} 1 & \text{if } m = m' \\ 0 & \text{if } m \neq m'. \end{cases} \tag{2.9}$$

To illustrate the effect of a measurement on a state, the example of the measurement of a qubit in the computational basis follows.

Recall that the state of the qubit can be given by equation $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ (equation (2.1)) subject to $|\alpha|^2 + |\beta|^2 = 1$. In the computational basis $\{|0\rangle, |1\rangle\}$, the outcomes $m \in \{0, 1\}$ are obtained with measurement operators $\{M_0, M_1\}$ defined by

$$M_0 = |0\rangle\langle 0|,$$

and

$$M_1 = |1\rangle\langle 1|.$$

Since M_0 and M_1 are Hermitian and $M = M^2$, the probability of getting measurement outcome 0 and 1 is given by

$$\Pr_{|\psi\rangle}[m = 0] = \langle\psi|M_0^\dagger M_0|\psi\rangle = \langle\psi|M_0|\psi\rangle = |\alpha|^2,$$

and

$$\Pr_{|\psi\rangle}[m = 1] = \langle\psi|M_1^\dagger M_1|\psi\rangle = \langle\psi|M_1|\psi\rangle = |\beta|^2.$$

The state after outcomes 0 and 1 are obtained will be:

$$|\psi'\rangle = \frac{M_0|\psi\rangle}{|\alpha|} = \frac{\alpha|0\rangle}{|\alpha|},$$

and

$$|\psi'\rangle = \frac{M_1|\psi\rangle}{|\beta|} = \frac{\beta|1\rangle}{|\beta|},$$

respectively. Since the statistics of the measurement of states $\frac{\alpha}{|\alpha|}|0\rangle$ and $|0\rangle$ and of states $\frac{\beta}{|\beta|}|1\rangle$ and $|1\rangle$ are the same, the global phase factor can effectively be ignored. After normalization, measuring a qubit in the state given by equation (2.1) with the computational basis $\{|0\rangle, |1\rangle\}$ will lead to the final state

$$|\psi'\rangle = |0\rangle \qquad \text{with probability } \Pr_{|\psi\rangle}[m = 0] = |\alpha|^2,$$

and

$$|\psi'\rangle = |1\rangle \qquad \text{with probability } \Pr_{|\psi\rangle}[m = 1] = |\beta|^2.$$

There are two cases of quantum measurements that are often seen in literature: projective measurements and POVM (Positive Operator-Valued Measures). In some case, the use of these special cases simplifies the analysis of a problem. Projective measurements with unitary transformations and auxiliary systems are POVM and POVM are equivalent to general measurements.

A projective measurement is described by an observable M that is a Hermitian operator with spectral decomposition

$$M = \sum_m m P_m$$

where P_m is the projector onto the eigenspace of M with eigenvalue m. The set of eigenvalues represents the set of possible outcomes. Similarly to general measurements, the outcome m occurs with probability

$$\Pr_{|\psi\rangle}[m] = \langle\psi|P_m|\psi\rangle$$

and after measurement, the state evolves to

$$|\psi'\rangle = \frac{P_m|\psi\rangle}{\sqrt{\Pr_{|\psi\rangle}[m]}}$$

Being a special case of general measurements, projective measurements have an important property: the operators $\{P_m\}_M$ are orthogonal projectors. This means that $\{P_m\}_M$ are Hermitian and orthogonal.

In order to describe an observable M, a complete set of orthogonal projectors $\{P_m\}_m$ is often given satisfying equations $\sum_m P_m = I$ as well as equations (2.7) and (2.8). Moreover, when it is said to "measure in a basis $\{|m\rangle\}_m$", this means to make the projective measurement with projectors $P_m = |m\rangle\langle m|$, where $M = \sum_m m P_m$.

POVM are a particularly useful formalism. Let M_m be a measurement operator such that $\sum_m M_m^\dagger M_m = I$ describes a measurement on quantum state $|\psi\rangle$ and define

$$E_m \stackrel{def}{=} M_m^\dagger M_m.$$

Then similarly to general measurements, $\{E_m\}_m$ satisfies the completeness relation (2.5). Each operator E_m, also called POVM element, is sufficient to determine the measurement outcomes and the set $\{E_m\}_m$ is called POVM.

The practicality of the POVM formalism can be illustrated with a simple example. Suppose we are given one of two quantum states, $|\psi_1\rangle = |0\rangle$ or $|\psi_2\rangle = \frac{(|0\rangle+|1\rangle)}{\sqrt{2}}$, which are indistinguishable with perfect reliability but we do not know which of the states it is. Although it is impossible to distinguish the two states with perfect reliability, we can nonetheless devise an experiment that will distinguish the states some of the time and never make an error of mis-identification. Consider the POVM $\{E_1, E_2, E_3\}$ defined by

$$E_1 = \frac{\sqrt{2}}{1+\sqrt{2}}|1\rangle\langle 1|, \tag{2.10}$$

$$E_2 = \frac{\sqrt{2}}{1+\sqrt{2}} \frac{(|0\rangle - |1\rangle)(\langle 0| - \langle 1|)}{2}, \tag{2.11}$$

$$E_3 = I - E_1 - E_2. \tag{2.12}$$

These are clearly POVM since each operator is positive and satisfies the completeness relation (2.5). When we measure the state, we have that

$$\langle \psi_1 | E_1 | \psi_1 \rangle = 0, \tag{2.13}$$

$$\langle \psi_2 | E_2 | \psi_2 \rangle = 0. \tag{2.14}$$

By equation (2.6), equations (2.13) and (2.14) mean that the probability of measuring E_1 and E_2 from the state $|\psi_1\rangle$ and $|\psi_2\rangle$ respectively is 0. Therefore, if the unknown state $|\psi\rangle$ was indeed $|\psi_1\rangle$ there is zero probability that E_1 will be observed and if the state was $|\psi_2\rangle$ there is zero probability that E_2 will be observed. In other words, if the result of the experiment is E_2, the state was $|\psi_1\rangle$ and if the results is E_1, the state was $|\psi_2\rangle$. When the result is E_3, it is impossible to know which state it was. In both cases, when $|\psi\rangle$ is $|\psi_1\rangle$ or $|\psi_2\rangle$, the probability of correctly identifying the unknown state $|\psi\rangle$ calculated from equation (2.6) is $\frac{1}{\sqrt{2}+2} \approx 0.29$. What is very interesting from the standpoint of POVM is that this probability is higher than it would be possible with projective measurements. This example concludes the demonstration of how useful the POVM formalism is.

2.5 Entanglement

So far, we have explained how to represent the evolution of the state of a system, how to measure it and what information can be extracted as well as how the measure changes the state of the system. This section presents one of the most puzzling concepts in quantum mechanics: entanglement.

Consider a composite system of $m + n$ qubits described by the state $|\psi\rangle$. If $|\psi\rangle$ can be written as $|\psi\rangle = |\psi_1\rangle|\psi_2\rangle$ with two separate states $|\psi_1\rangle$ and $|\psi_2\rangle$ of m and n qubits respectively, then it is called a product state. If the state cannot be separated in this manner, we say the state $|\psi\rangle$ is entangled. Entangled states play a crucial role in quantum information and it is probably the most astonishing phenomenon in quantum mechanics.

Well-known examples of entangled states in the literature are the two-qubit Bell states:

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle),$$

$$|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle),$$

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle),$$

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle),$$

where the last state is also called the Einstein-Podolsky-Rosen (EPR) pair, introduced in [EPR35].

To get a better understanding of the power of entanglement, an example will be used. Suppose Alice and Bob are separated and share an EPR pair where Alice keeps the first qubit and Bob keeps the second qubit. Suppose now that Alice measures her qubit. With probability $\frac{1}{2}$, she will get the outcome 0 and with probability $\frac{1}{2}$, she will get the outcome 1. By the nature of the EPR pair, Alice then knows that Bob will get measurement outcome 1 or 0 with perfect probability before he measures. However, from the perspective of Bob, who does not know if Alice has measured yet or not, his state is still the EPR pair. Only if Alice tells him the result she got, will he know that his state is in fact $|0\rangle$ (if Alice got outcome 1) or $|1\rangle$ (of Alice got outcome 0). The troubling effect is that no matter who measured first, they will still get opposite outcomes.

You might think that when Alice measures her state a signal is sent to the state of Bob. But experiments indicate that if this is the case, it would be supraluminal and would violate special relativity. In [Bra], a paradoxical scenario is described that indicates how signalling theory is problematic:

> [...]if the two particles are moving away from one another, relativity allows for a paradoxical situation in which each particle is measured after the other in its own space-time frame, and therefore it does not even make sense to say that the first-measured particle "decides" the outcome for both particles: neither particle is measured first! This whole concept revolted Einstein to such an extent that he called it "spooky action at a distance".

Another explanation of the strange phenomenon might be that quantum mechanics is wrong and that each particle is already determined to be in the state $|01\rangle$ or $|10\rangle$ before Bob and Alice receive it. That is, randomness occurs before separation. Again in [Bra], an experiment that was made is described in which each participant Bob and Alice apply the Hadamard transformation upon receiving their state. For details of the experiment,

consult [Bra]. It is shown that the resulting statistical outcomes would be different in the case that the state would be already $|01\rangle$ or $|10\rangle$ and the case that the state is changed at measurement. Experiments have shown that the state is in fact changed after measurement and not at the separation[FC72,ADR82,AGR82,TBG+98,TBZ+98].

All these results do not prove that quantum mechanics is correct but rather that a naïve classical interpretation is not sufficient. Can there be another classical explanation? This question puzzled Einstein, Podolsky and Rosen but it was not until 1964, that Bell's theorem ruled out any classical theory [Bel64].

Chapter 3

Computational Complexity Theory

This chapter gives motivations for the study of games in chapter 4. The notion of games that will be presented in this thesis is linked to the notion of multi-prover interactive proofs in computational complexity. This is the reason we devote an entire chapter to this topic.

A short reminder of relevant complexity classes will be presented. We assume the reader is familiar with basic notions of complexity theory. For more details on the topic, consult [Sip06] for an introduction to complexity theory and [Wat] for more information on complexity theory classes with quantum information.

3.1 Definitions and Non-Interactive Classes

Computational complexity theory is the science that studies the amount of resources required by an algorithm to solve a given computational problem. Common resources include time and space with respect to the size of the input, but also randomness, alternations, interaction and many more. The theory of computational complexity characterizes quantified amount of resources into computational classes.

Central elements in computational complexity theory are languages. A language is a set of strings (e.g.:{000110,1010}) over an alphabet Σ (e.g.:$\Sigma_1 = \{0, 1\}$). In this setting, we can study the problem of deciding whether of not a given string is in a language. An important set of

problems are decision problems: problems for which the solution is either *yes* or *no*. A particular set of decision problems, promise problems, are well suited for the game setting of the next chapter. A promise problem is a decision problem for which the input is a subset of all possible string Σ^*. We formalize the notion of promise problems with the following definition from [Wat].

Definition 3.1.1 (Promise Problems)**.** A promise problem is a pair $A = (A_{yes}, A_{no})$ where $A_{yes}, A_{no} \subseteq \Sigma^*$ are sets of strings satisfying $A_{yes} \cap A_{no} = \emptyset$. The sets A_{yes} and A_{no} are sets of *yes-instances* and *no-instances* having answers *yes* and *no* respectively.

Adding the condition $A_{yes} \cup A_{no} = \Sigma^*$ to the definition of promise problems gives the definition of a language. We can group any problems, and in particular promise problems, of related complexity into classes. In the remaining of this section we will give the description of different complexity classes with respect to promise problems rather than just languages. The motivation for this transition will be clear in the next chapter.

In complexity theory, we are also interested by relations between different classes. If there exists a function f so that for all $x \in A_{yes}, f(x) \in B_{yes}$ and for all $x \in A_{no}, f(x) \in B_{no}$ then we say there is a reduction from the class A to B, $A \leq B$. If there is as well a reduction from class B to A, $B \leq A$, we say that the two classes are equivalent. There are some restrictions for the type of functions for this to be true, but for the results presented you can assume the function f is a classical polynomial-time function on inputs in $A_{yes} \cup A_{no}$.

In the literature, classes of problems are described in terms of languages and not on promise problems. In this thesis however, we will follow non-standard definitions based on the promises problems. We give the definition of some classes with which the reader should be familiar.

Two of the most discussed classes are the class P and NP. Their definition with respect to promise problems is given [Wat].

Definition 3.1.2 (Class P)**.** A promise problem $A = (A_{yes}, A_{no})$ is in P if and only if there exists a deterministic Turing machine M in time polynomial in the length of the input $|x|$ that accepts every string $x \in A_{yes}$ and rejects every string $x \in A_{no}$.

Definition 3.1.3 (Class NP)**.** A promise problem $A = (A_{yes}, A_{no})$ is in NP if and only if there exists a polynomially bounded function $p(|x|)$ and a deterministic Turing machine M in time polynomial in the length of the

input $|x|$ with the following properties. For every string $x \in A_{yes}$, M accepts (x, y) for some $y \in \Sigma^{p(|x|)}$, and for every string $x \in A_{no}$, M rejects (x, y) for all strings $y \in \Sigma^{p(|x|)}$.

Nowadays, the list of classes is very large. Many results in complexity theory put in relation one class to another or prove the equivalence of two classes. We give the definition of three more fundamental classes: *PSPACE*, *EXP* and *NEXP*.

Definition 3.1.4 (Class *SPACE*)**.** A promise problem $A = (A_{yes}, A_{no})$ is in *PSPACE* if and only if there exists a deterministic Turing machine M running in space polynomial in $|x|$ that accepts every string $x \in A_{yes}$ and rejects every string $x \in A_{no}$.

Definition 3.1.5 (Class *EXP*)**.** A promise problem $A = (A_{yes}, A_{no})$ is in *EXP* if and only if there exists an deterministic Turing machine M in time exponential in the length of the input $|x|$ (meaning time bounded by $2^{p(|x|)}$, for some polynomial-bounded function $p(|x|)$), that accepts every string $x \in A_{yes}$ and rejects every string $x \in A_{no}$.

Definition 3.1.6 (Class *NEXP*)**.** A promise problem $A = (A_{yes}, A_{no})$ is in *NEXP* if and only if there exists a polynomially bounded function $p(|x|)$ and a deterministic Turing machine M in exponential time in the length of the input $|x|$ with the following properties. For every string $x \in A_{yes}$, M accepts (x, y) for some $y \in \Sigma^{2^{p(|x|)}}$, and for every string $x \in A_{no}$, M rejects (x, y) for all strings $y \in \Sigma^{2^{p(|x|)}}$.

Note that we do not introduce the class *NPSPACE* for nondeterministic polynomial space since it was shown that $PSPACE = NPSPACE$ in [Sav70]. Therefore, nondeterminism does not add more power to the class *PSPACE*. Figure (3.1) puts in relation the complexity classes described so far by drawing the more powerful complexity classes higher. Lines indicate containments; for example, *NP* contains *P*. Note that none of these containments are known to be strict.

Next, we give a brief overview of other classes along with some results that are going to be relevant to the rest of the thesis.

3.2 Interaction with a Single Prover

Introduced in [GMR85], an interactive proof system is a model of computation in which a polynomial number of messages are exchanged between

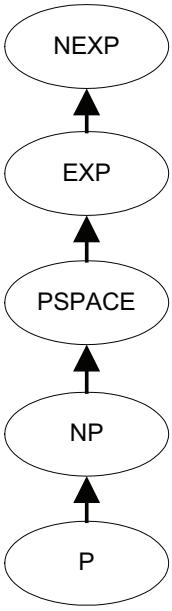

Figure 3.1: Hierarchy of Complexity Classes.

two parties: a prover and a verifier. We let the prover have unbounded computational power and the verifier be polynomial time but allowed to use randomness. The goal of the prover is to convince the verifier about the truth of a statement that might be beyond the reach of the verifier. The verifier wants to challenge the prover in order to verify his assertion. To do so, the verifier sends a question $q \in Q$ to the prover for which the prover answers $a \in A$ where Q and A are sets of possible questions and answers of polynomial size. A round of interaction is defined as a question from the verifier and an answer from the prover. After a certain number of rounds, based on the answers he received, the verifier either accepts or rejects the statement of the prover. If the answer is a member of the *yes-instances* A_{yes}, the verifier should accept it and if the answer is from the *no-instances* A_{no}, the verifier should reject it.

Sometimes, the verifier cannot be convinced without doubt of the truth of the statement using a polynomial number of messages. This is why we introduce the completeness and soundness probabilities. In the formalism of promise problems, if $x \in A_{yes}$, the completeness probability is the probability that the verifier accepts it, that it does not reject a true statement. If a $x \in A_{no}$, the soundness probability is the probability that the verifier accepts it, that he accepts a false statement. Formally, we define these two notions for interactive proofs with promise problems in the following

definitions.

Definition 3.2.1 (Completeness)**.** Given a promise problem $A = (A_{yes}, A_{no})$, the completeness probability c is the minimum probability for which the verifier V accepts any $x \in A_{yes}$

$$\Pr[V \text{ accepts } x] \geq c. \tag{3.1}$$

Definition 3.2.2 (Soundness)**.** Given a promise problem $A = (A_{yes}, A_{no})$, the soundness probability s is the maximum probability for which the verifier V accepts $x \in A_{no}$

$$\Pr[V \text{ accepts } x] \leq s. \tag{3.2}$$

We define the class *BPP* again with the non-standard promise problems formalism.

Definition 3.2.3 (Class *BPP*)**.** A promise problem $A = (A_{yes}, A_{no})$ is in *BPP* (Bounded-error, Probabilistic, Polynomial time) if and only if there exists a probabilistic Turing machine M in time polynomial in the length of the input $|x|$ with completeness probability $\frac{2}{3}$ and soundness probability $\frac{1}{3}$.

The interactive proof system described above with the verifier given the power of the class *BPP* characterizes the class IP.

Definition 3.2.4 (Class *IP*)**.** A promise problem $A = (A_{yes}, A_{no})$ is in *IP* (Interactive Proofs) if and only if there exists an interactive proof system for A given that the verifier has the power of the class *BPP* and the prover has unbounded computational power. The communication between the verifier and the prover remains classical.

Historically, some complexity theorists wanted to increase the power of the class *NP* by introducing interaction. It turns out that if the verifier is bounded by the class *P* only (without randomness), the resulting interactive class would be equal to the class *NP* [AB]. Therefore, having the power of *NP* with interaction does not add more power to the class. On the other hands, by letting the verifier be probabilistic as in the class *BPP*, it was shown that the class *IP=PSPACE* in [Sha92], which might increase the power of the class beyond *NP* and *BPP* if $NP \neq PSPACE$. It was also shown by non trivial arguments that restricting the completeness probability to be 1 does not change the power of the class. However, restricting the soundness probability to be 0 reduces the power of the class *IP* to the class *NP* because the verifier becomes deterministic [AB].

To illustrate the concept of the class *IP*, an illustrative scenario borrowed and adapted from [AB] is presented. Suppose that Alice has a friend Bob who claims that he can distinguish the taste of two similar soda drink *Cole* and *Petsi*. To verify that assertion, Alice is going to prepare one cup of each drink labelled 1 and 2 in the absence of Bob and then present them to him. If after tasting them, Bob can correctly identify each one, Alice is more convinced that Bob is telling the truth. The promise in this case is that exactly one of the bottle of Alice contains *Cole* and exactly one contains *Petsi*. The query (two cups) from Alice and the answer of Bob constitute one round of interaction. However, Bob could give a random answer and with probability $\frac{1}{2}$ give the right result. This is why Alice is encouraged to redo the test n times to increase her confidence level. At the end, Bob could have been lucky with probability only $(\frac{1}{2})^n$. Alice can choose the number n of repetitions until she is satisfied and thus can detect a cheating Bob with probability $1 - (\frac{1}{2})^n$. Since Alice knows which cup has which soda drink, the completeness probability is 1 (i.e.: she will accept every good answer given by Bob). The probability that Bob will cheat successfully Alice, the soundness probability, is $(\frac{1}{2})^n$.

3.3 Interaction with Many Provers

Interactive proofs were generalized to more than one prover, resulting in the class *MIP* (Multiprover Interactive Proofs) in [BOGKW88]. Cryptographic purposes were originally the motivation behind this class. With this generalization, all communication between any provers is forbidden as soon as interaction between provers and the verifier has started. However, since the provers are cooperative, they can initially agree on a shared strategy to convince the verifier. In the new paradigm, the verifier sends a question to each prover and makes his decision based on their answers. A round in multi-prover interactive proofs is a questions/answers tuple between the verifier and all provers.

Definition 3.3.1 (Class *MIP*)**.** A promise problem $A = (A_{yes}, A_{no})$ is in *MIP* (Multi-prover Interactive Proofs) if and only if there exists a k-prover interactive proof system with $k \geq 2$ for A, given that the verifier has the power of the class *BPP* and the provers have unbounded power. The communication between the verifier and the provers is classical and the provers cannot communicate once the interactive part of the protocol has started with the verifier.

For notational convention, $MIP_{c,s}[k, r]$ will be used to represent the class of interactive proof systems with k-provers ($k \geq 2$) and r-round ($r \geq 1$) with completeness probability c and soundness probability s. We write simply $MIP[k, r]$ when the specific values of c and s are not important and similarly. Similarly, we write $MIP[k]$ when the value of $r \geq 2$ is not important.

The original paper [BOGKW88] already demonstrated that increasing the number of provers to more than two does not change the power of the class, thus for any value $k \geq 2$, $MIP[k] = MIP[2]$. It was further shown that $NEXP = MIP[2, 1]$ [BFL90] and consequently that having more than one prover might increase the power of the class $IP = PSPACE$ to $MIP = NEXP$ (if $PSPACE \neq NEXP$). After an increasing interest in two-prover one-round interactive proofs, several refinements [CCL90, Fei91, LS91] lead to the proof that every language in $NEXP$ has a two-prover one-round interactive proof with perfect completeness and exponentially small soundness error [FL92]. Thus, the restriction of $MIP_{1,s}[2, 1]$ with exponentially small soundness error s is as powerful as the more general $MIP[k]$. Later, the parallel repetition theorem for two-prover one-round interactive proofs appeared [Raz98].

To understand why more provers are more powerful than one prover, let's revisit the experiment of distinguishing the taste of soda drinks *Cole* and *Petsi*. Let's introduce another participant, Charlie, to the test. Now Charlie and Bob claim that they both can distinguish the taste of *Cole* and *Petsi* and want to convince Alice about that statement. Alice wants to make sure that BOTH participants tell the truth. She could do as before with each participant separately and detect each cheating participant with probability $1 - (\frac{1}{2})^n$ after n repetition of the test. The probability that Alice detects both participants if they cheat would then be $\left(1 - (\frac{1}{2})^n\right)^2$ because the two events are independent of each other, enforced by the no-communication condition. In fact with two participants, to get the same probability as with one participant you just need to do more tests.

By looking at these results, one might think that two provers only affect the soundness of the experiment and by a right number of sequential repetitions it is possible to get the same results. If Alice does the experiment as mentioned, this is indeed so. However, with two provers, Alice could have less information and be as convinced as before. Suppose Alice has two bottles of *unidentified* cola. The promise is that one bottle contains *Cole* and the other contains *Petsi*. Now, Alice cannot verify the answers of the provers since she does not even know the answer herself. However, what she could do is to send the test to Bob and Charlie. Alice remembers which

liquid she had put in the two cup and gives one to Bob and the other to Charlie. If their answers do not contradict each other for a same cola noted by Alice, she is more convinced that they both tell the truth. If Alice had sent both cup to Bob, he could have cheated by comparing the first cup with the second one so that there is no contradiction. It does not prove that Bob can distinguish both liquids, it only proves that Bob can associate similar liquids from different queries. For example, Bob could have called the real *Cole*, *Petsi*, and the real *Petsi*, *Cole* and Alice would have not been able to verify the solution. When using Charlie to check the answers of Bob, we ensure that Bob makes less errors in misidentification by checking contradictions between the participants. It turns out that after n repetitions of the test, she will detect cheating provers with the same probability $\left(1 - (\frac{1}{2})^n\right)^2$ as before.

With this example, one could conjecture that the power of the class *MIP* is larger than *IP* since it is possible to prove more results than the single prover scenario. With a single prover, it would have been impossible for Alice to verify the answer from Bob which she does not know. In the literature, the corroboration of the answers from the two provers as in the above scenario is called oracularization. The second prover serves as an "oracle" to check the answers provided by the first prover. This is what gives power to the class *MIP*.

3.4 Interaction with Entanglement

All the definitions of complexity classes seen so far were made when quantum information concepts were not applied to complexity theory. This has the consequence that all previous results were assuming classical strategies whereas in fact, the provers could harness the power of quantum mechanics. This led to the introduction of new classes including MIP^* in [CHTW04]. The class MIP^* is the same as *MIP* except that in this case the provers are allowed to share arbitrarily many entangled qubits beforehand.

Definition 3.4.1 (Class MIP^*)**.** A promise problem $A = (A_{yes}, A_{no})$ is in MIP^* (Multi-prover Interactive Proofs) if and only if there exists a k-prover interactive proof system with $k \geq 2$ for A given that the verifier has the power of the class BPP and the provers have unbounded computational power. The communication between the verifier and the provers is classical and the provers cannot communicate once the protocol has started. However, the provers are allowed to share arbitrarily many entangled qubits.

Note that in MIP^*, the communication between the provers and verifier is purely classical as before. Other variants such as *QIP* and *QMIP* are defined with quantum provers/verifier communication but will not be discussed further in this thesis.

The interest in the class MIP^* is strengthened by the fact that although the verifier can ensure the physical separation of the provers, he has no way to control the sharing of entanglement between parties before the interaction begins. Because of this limitation, the power of the class MIP^* is of utmost importance to the field of cryptography. For example, entanglement has invalidated the security proof of previously believed-to-be secure protocols based on classical strategies [BOGKW88, May96, BCMS98].

Many results proved earlier for the class *MIP* are unknown to be valid for MIP^* such as the relation between $MIP^*[k, r]$, $MIP^*[2, r]$ and *NEXP* except the trivial inclusions $MIP^*[k, r] \subseteq MIP^*[k + 1, r]$ and $MIP^*[k, r] \subseteq MIP^*[k, r + 1]$. Increasing the number of rounds and provers have still to be studied in order to fully understand the power of MIP^*.

Much effort has been spent in order to establish the power of the class MIP^*. Two explanations for the difficulty of this problem are that 1) there is no bound for the amount of entanglement necessary for the player to have an optimal strategy and 2) the correlations emerging from entanglement are still not very well understood.

However, it was shown recently that the addition of a third player for MIP^* produces interesting results: $NP \subseteq MIP^*_{1,1/poly}[3, 1]$ [KKM$^+$08, IKP$^+$07] and $NEXP \subseteq MIP^*_{1,1-2^{-poly}}[3, 1]$[KKM$^+$08]. It is shown in [IKM08] that two-prover one-round interactive proof system for *PSPACE* still achieves exponential small soundness error with entangled provers (and more strongly, no-signalling provers). It is also shown that every language in *NEXP* has a two-prover one-round interactive proof system of perfect completeness, albeit with exponentially small gap between completeness and soundness, in which each prover responds with only two bits.

Along those lines of research, one complexity class derived from MIP^* has been widely studied and interesting results have been shown about it. The classical class $\oplus MIP[2, 1]$ with its entangled counterpart $\oplus MIP^*[2, 1]$ are similar to $MIP[2, 1]$ and $MIP^*[2, 1]$ with some restrictions. The verifier's output is a function of only the exclusif-OR (XOR) of the bits of the provers.

Definition 3.4.2 (Class $\oplus MIP$)**.** A promise problem $A = (A_{yes}, A_{no})$ is in $\oplus MIP$ if and only if there exists a one-round two-prover interactive proof system for A wherein the provers each send a single bit to the verifier, and

the verifiers decision to accept or reject is determined by the questions asked along with the XOR of these bits. The communication between the verifier and the provers is classical and the provers cannot communicate once the protocol has started. The verifier and provers remains classical all the time.

Definition 3.4.3 (Class $\oplus MIP^*$)**.** This class is similar to $\oplus MIP$, except that the provers may now share arbitrary entangled states.

It has been proven that classically $\oplus MIP_{c_1,s_1}[k,r] = NEXP$ for some $k \geq 2$ and $r \geq 1$ and for some choice of probabilities c_1 and s_1 [BGS98, Hås01]. With entanglements, it was shown that $\oplus MIP^*_{\frac{12}{16},\frac{11}{16}+\epsilon}[2,1] \subseteq NEXP$[CHTW04] for all $\epsilon \in (1, \frac{1}{16})$, which was further improved to $\oplus MIP^*[2] \subseteq EXP$[Weh06]. In [CGJ07], it was shown that $NP \subseteq \oplus MIP_{1-\epsilon,\frac{1}{2}+\epsilon}[2,1]$.

Returning to the *Cole* vs *Petsi* experiment, we could say that Charlie and Bob initially share two identical "magic" ice cubes. The cubes seem "magic" to the eye of Alice but in fact use the power of entanglement in a special manner. The ice cubes have the property that if they are put in a cola, they become red or blue with equal local probability. The magic of the ice cubes comes from the fact that if they are put in the same cola, they will be of the same colour and if they are put in a different cola, they will be of different colour. The power of these cubes will help Bob and Charlie make the difference between the tastes of the colas. Upon receiving their cup, Bob and Charlie randomly choose a cup and put the "magic" ice cube in. Charlie identifies a red cup by *Cole* and a blue cup by *Petsi*. Bob does the same procedure. Using this stratagem, they will be able to successfully answer the queries of Alice every time. If Alice is unaware of the stratagem, she could be completely misled by Charlie and Bob. Although the analogy required the use of "magic" ice cubes, it illustrates well the fact that Bob and Charlie can get extra information for the problem using quantum correlations. This extra information helps them to cheat Alice. In this analogy, Alice cannot prevent Bob and Charlie from using their ice cubes; all she can do is prevent the communication between them. The power of entanglement as it was explained in the previous chapter does not emit a signal and is therefore not a communicating tool. We will see in later sections that this does not necessarily extend to more than two provers.

We summarize the complexity classes discussed so far in figure 3.2.

This chapter concludes the motivation to study quantum mechanics from the perspective of complexity theory. In the next chapter, we will see that

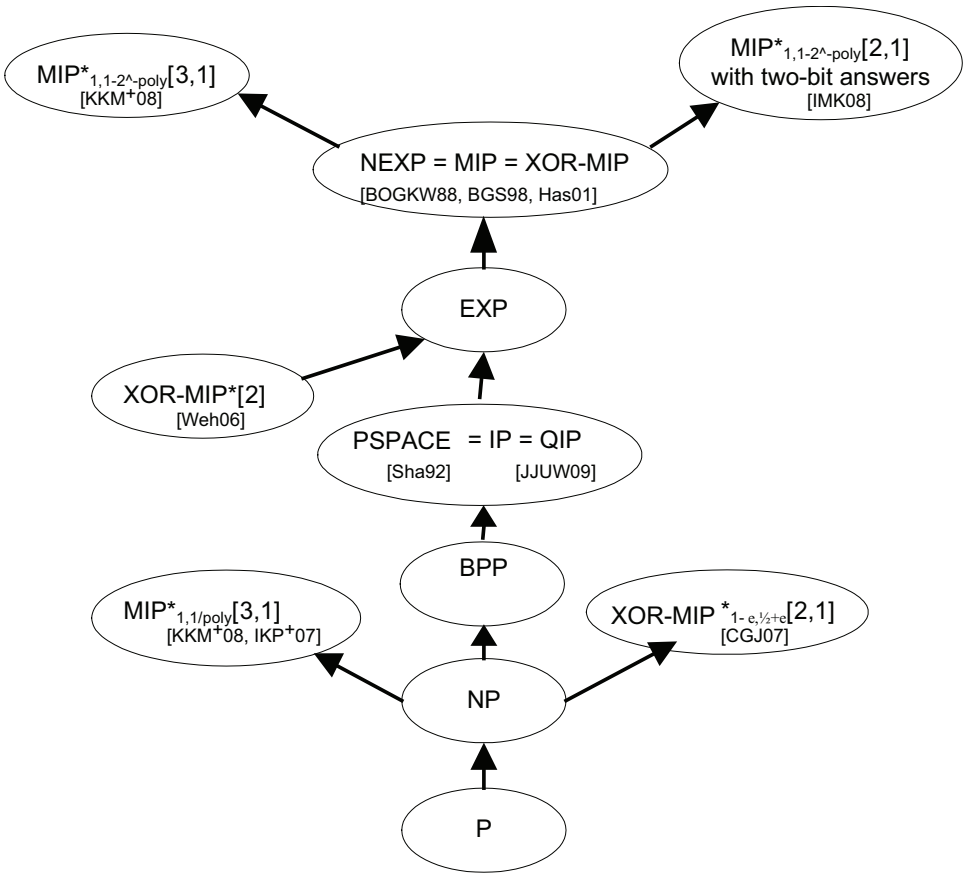

Figure 3.2: Updated Hierarchy of Complexity Classes.

the terminology of games is well adapted for the study of interactive classes with quantum mechanical concepts.

Chapter 4

Two-prover One-round Games

A better understanding of the effect of entanglement would give insight for the power of interactive classes extended with quantum mechanics. A natural framework to study these effects of nonlocality within interaction is through cooperative games with imperfect information. A cooperative game is a game in which players gain if they collaborate. The games studied have imperfect information, that is the players do not know the actions of the other players perfectly. In other words, no prover has access to the question that the other prover has received and therefore has to infer his likely actions. A game with perfect information is not interesting from the standpoint of information theory since the best actions are known in advance through the minimax decision rule [RN03]. In this thesis, we will concentrate on games with one round because of their simplicity. Note that in the game-theoretic framework, the verifier is in some cases referred to as the referee and the provers as the players.

In this chapter, we describe the framework of two-prover one-round games and explain its links with complexity theory, particularly with multi-prover interactive classes. This will serve as a basis to study the effect of quantum mechanics on these complexity classes. Following the work of [CHTW04], we prove the upper bound on the probability of winning in games for quantum provers in certain conditions. We then conclude the chapter with the description of a game that will serve as an example case in the forthcoming chapters.

4.1 Games Parameters

A two-prover one-round game is a game played by a verifier V against two provers P_1 and P_2 who cooperate with each other. The following definition describes a two-prover one-round game.

Definition 4.1.1 (Two-Prover One-Round Game)**.** A two-prover one-round game $G = (X, Y, A, B, R, \pi_{XY})$ is defined by

- Finite sets of questions X and Y,
- Finite sets of answers A and B,
- Winning Condition $R : X \times Y \times A \times B \to \{0, 1\}$ and
- Probability distribution π_{XY} on the question set $X \times Y$,

4.2 Strategies of the Provers

For a two-prover one-round game $G = (X, Y, A, B, R, \pi_{XY})$, the provers share a joint strategy before interaction begins. Once the verifier is ensured that the provers cannot communicate (e.g: by physical separation), interaction can occur. The verifier samples questions (x, y) from $X \times Y$ according to the probability distribution π_{XY}. He then sends the questions x and y to provers P_1 and P_2, who respond with $a \in A$ and $b \in B$, respectively. The provers win the game against the verifier if $R(x, y, a, b) = 1$, otherwise, the verifier wins against the provers; $R(x, y, a, b)$ is either 0 or 1. As a convention, the winning condition $R(x, y, a, b)$ is rewritten $R(a, b \mid x, y)$ to emphasize the fact that the answer (a, b) depends on the question (x, y). The provers can agree on a joint strategy for the game.

Definition 4.2.1 (Strategy)**.** A strategy for the provers consists in a set S of probability distributions $S_{(x,y)}$ over $A \times B$ indexed by $(x, y) \in X \times Y$

$$S = \{S_{(x,y)}\}_{(x,y) \in X \times Y.} \tag{4.1}$$

These can be interpreted as the provers giving joint answers $(a, b) \in A \times B$ to the questions $(x, y) \in X \times Y$ with probability $S(a, b \mid x, y)$. Given that P_1 has no access to question y and P_2 has not access to question x, not all probability distributions $S_{(x,y)}$ will be possible; we shall come back on this issue later. The probabilities are normalized so that for all questions (x, y):

$$\sum_{(a,b)} S(a,b \mid x,y) = 1.$$

We now introduce three classes of strategies based on the type of correlated resources that the provers possess. Although, the provers are given unlimited computational power, they nonetheless cannot communicate in the interactive part of the process. However, the initial resources they share give them a certain amount of possible correlation during interaction.

In the weakest class of strategies, the class of classical or unentangled strategies, the provers are allowed to share any classical random variables before the game starts as well as any private source of randomness they wish to use once the game has started. Formally, a classical strategy for the provers P_1 and P_2 is described for any question pair (x, y) and answer pair (a, b) by the following distributions

$$S(a,b \mid x,y) = \sum_{e} p(e) S(a \mid x,e) S(b \mid y,e). \tag{4.2}$$

where e can be seen as shared randomness. The optimal classical strategy is in fact deterministic since a probabilistic strategy is just a probability distribution over a finite set of deterministic strategies. So the provers can analyse every possible outcome of randomness and fix it so that it maximizes the winning probabilities of the game. We thus can see the set of classical strategies of P_1 and P_2 as a set of deterministic functions $a(x)$ and $b(y)$.

A stronger strategy class, the class of quantum strategies, encompasses strategies for which the provers are allowed to share a bipartite state $|\psi\rangle \in \mathbb{C}^{\Sigma\times\Gamma}$. The quantum strategies of each prover consist in performing a quantum measurement for each question over their share of the state and by answering by the outcome of the measurement. Using the POVM formalism, for each $x \in X$ prover P_1 has a POVM defined by

$$\{E_x^a : a \in A\} \subseteq \mathbb{C}^{\Sigma\times\Sigma}$$

and for each $y \in Y$ prover P_2 has a POVM defined by

$$\{E_y^b : b \in B\} \subseteq \mathbb{C}^{\Gamma\times\Gamma}$$

where each POVM satisfies completeness relation (2.5). Upon receiving the questions $(x, y) \in X \times Y$, the provers apply their POVM with respect to their question on their part of the state $|\psi\rangle$. The outcomes $(a, b) \in$

$A \times B$ of the measurements is sent to the verifier. From equation (2.6), the probability that the provers answers $(a, b) \in A \otimes B$ is given by

$$S(a, b \mid x, y) = \langle \psi | E_x^a \otimes E_y^b | \psi \rangle. \tag{4.3}$$

Finally, the class of no-signalling strategies, or behavior, includes any possible strategies that cannot be used by the provers to communicate. For example, each prover could have a magical black box that can give them a kind of correlation that cannot be implemented in the physical world, provided it cannot be used to communicate. More formally, a no-signalling strategy imposes on the prover P_1 that for any questions $x \in X$, $y, y' \in Y$ and answers $a \in A$, the marginal distributions

$$\sum_{b \in B} S(a, b \mid x, y) = \sum_{b \in B} S(a, b \mid x, y').$$

Similarly for the prover P_2, for any question $y \in Y$, $x, x' \in X$ and answers $b \in B$, the marginal distributions

$$\sum_{a \in A} S(a, b \mid x, y) = \sum_{b \in B} S(a, b \mid x', y).$$

The class of strategies available to the provers directly influences the winning probability of two-prover one-round games.

Definition 4.2.2 (Winning Probability of a Strategy)**.** In a two-prover one-round game $G = (X, Y, A, B, R, \pi_{XY})$, the winning probability $\tilde{\omega}(S_K)$of a strategy $S = \{S_{(x,y)}\}_{(x,y) \in X \times Y}$ is given by

$$\tilde{\omega}(S) = \sum_{(x,y) \in X \times Y} \left(\pi_{XY}(x, y) \sum_{(a,b) \in A \times B} R(a, b \mid x, y) S(a, b \mid x, y) \right).$$

Sometimes we will say that a game is a classical game, quantum game or no-signalling game to indicate the kind of strategy used by the provers.

4.3 Value of a Game

From the winning probability $\tilde{\omega}(S)$ of a strategy S, the value $\omega_K(G)$ of a two-prover one-round game G follows:

Definition 4.3.1 (Value of a Two-prover One-round Game)**.** The value of a two-prover one-round game $G = (X, Y, A, B, R, \pi_{XY})$ with strategy class K over strategy S is given by

$$\omega_K(G) = \sup_{S \in K} \sum_{(x,y) \in X \times Y} \left(\pi_{XY}(x,y) \sum_{(a,b) \in A \times B} R(a,b \mid x,y) S(a,b \mid x,y) \right).$$

In particular, the value of a two-prover one-round game G with classical strategy is described by $\omega_c(G)$, with quantum strategies by $\omega_q(G)$ and with no-signalling strategies by $\omega_{ns}(G)$. The trivial relationship among the different classes of strategies is

$$0 \leq \omega_c(G) \leq \omega_q(G) \leq \omega_{ns}(G) \leq 1. \tag{4.4}$$

We open a parenthesis here to look at the definition of the value $\omega_K(G)$ of a game G with respect to the class of strategies K. We find a solution for the value by solving a linear program in variables $S(a, b \mid x, y)$. The definition of the value constitutes the objective function. The constraints of the problem include positivity, normalization as well as the constraint imposed directly from the strategy class C. Positivity imposes that $S(a, b \mid x, y) \geq 1$ and normalization that for all pairs (x, y):$\sum_{(a,b)} S(a, b \mid x, y) = 1$. The last constraint comes directly from the definition of the class of strategy C.

As we said, the value of a game constitutes a linear programming problem referred to the primal problem. The problem of maximization in the primal problem with n variables and m constraints can be cast as a minimization problem. This is referred as the dual problem. In optimization theory, duality is the principle according to which the problem can be seen by either of the two perspectives: the primal or the dual problem. The dual problem is a linear combination of the m values in the primal problem that limit the constraints. In the dual problem, there are n dual constraints that make a lower bound on a linear combination of m dual variables. This means that even if we cannot solve the linear program, we can obtain an upper bound on the value of a game by constructing a solution to the dual program. Appendix A describes the formalism of mathematical optimization in more details.

We summarize the process of interactive games in figure (4.1). The three steps of the protocol are depicted: the non-interactive part, the interaction and the decision of the verifier.

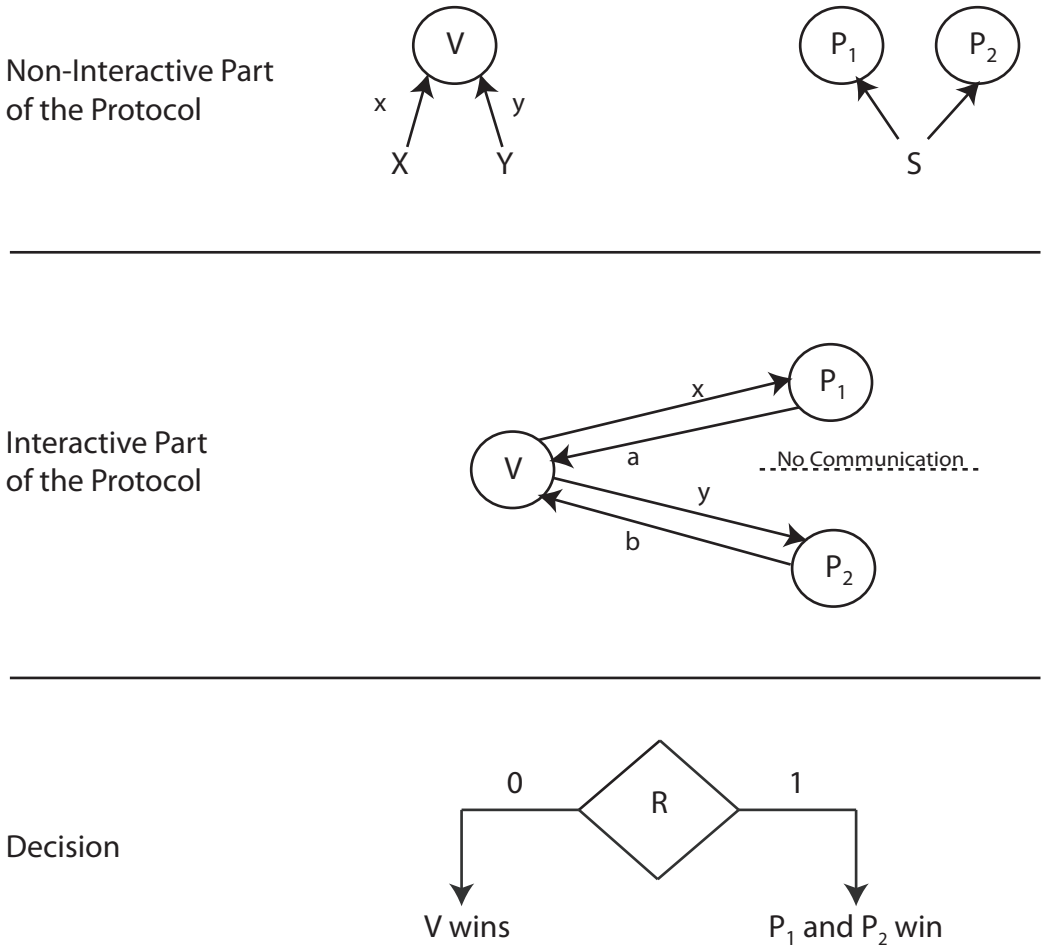

Figure 4.1: Two-Prover Interactive Game Protocol.

4.4 Relationship with Complexity Theory

Besides the classification of games with respect to strategies, games are also categorized by other parameters. Two of these characterizations are: binary games and XOR games. Binary games are games for which the answers of both provers are single bits (i.e.:$A = B = \{0, 1\}$). XOR games are binary games for which the function R is a function of $a \oplus b$ and not of a and b independently.

The relation with interactive complexity classes $MIP[2, 1]$, $\oplus MIP[2, 1]$, $MIP^*[2, 1]$ and $\oplus MIP^*[2, 1]$ should now seem evident. Consider a promise problem $A = (A_{yes}, A_{no})$ as introduced in definition (3.1.1). Given any string s and a game G, if $s \in A_{yes}$, the value $\omega_K(G)$ with respect to strategy class K will be close to 1 and if $s \in A_{no}$, the value $\omega_K(G)$ will be close to 0.

Non-signalling strategies are useful since they can sometimes give an upper bound for quantum strategies in the case this bound is not known. However, for the game to be a valid proof system, the soundness must not to be 1. Otherwise, the provers will be able to cheat the verifier every time. An upper bound on the value of a game will give insight on conditions for the associated complexity class.

Promise problems represent more generally the formalism of games compared to languages since it is possible that some inputs will never occur and therefore there is no need for the corresponding output to be defined. Languages have to be decision problems over all possible inputs.

Next, we prove an interesting result that puts an upper bound on the value of a XOR game with quantum strategies as a function of the classical value for that game. This upper bound will serve to prove the quantum value of the game in section 4.6.

4.5 Upper Bound for XOR Games

In [CHTW04], upper bounds for the value any XOR game with quantum strategies are proven. Preliminary to those results, it is demonstrated that the optimal value of two-prover binary games with quantum strategies is obtained by the provers doing projective measurements on their part of the shared state. Moreover, the parts of the shared state are of equal dimension. Therefore, in the search of an optimal strategy, only projective measurements have to be considered.

We describe the orthogonal projections M^0 and M^1 of prover P_1 subject to $M^0 + M^1 = I$ in terms of the observable $M = M^0 - M^1$ and similarly with $N = N^0 - N^1$ for prover P_2. The observables of the two-outcome projective measurement form a Hermitian matrix with eigenvalues $+1$ and -1 that can be mapped to answers 0 and 1 in that order.

A necessary result has to be stated before proving the bounds. The result in [Tsi87] relates the problem of finding the probability $\langle\psi|M_x^a \otimes N_y^b|\psi\rangle$ that the provers answer by $(a, b) \in A \otimes B$ to questions $(x, y) \in X \otimes Y$ to the classical problem of finding two real unit vectors.

Theorem 4.5.1 ([Tsi87])**.** *Let X and Y be finite sets and let $|\psi\rangle$ be a pure quantum state with support on a bipartite Hilbert space $\mathscr{H} = \mathscr{A} \otimes \mathscr{B}$ such that $\dim(\mathscr{A}) = \dim(\mathscr{B}) = n$. For each $x \in X$ and $y \in Y$, let M_x and N_y be observables on $\mathscr{A}$ and $\mathscr{B}$ respectively with eigenvalues ± 1. Then there exist*

real unit vectors u_x *and* v_y *in* $\mathbb{R}^{2n^2}$ *such that*

$$\langle\psi|M_x \otimes N_y|\psi\rangle = u_x \cdot v_y$$

for all $x \in X$ *and* $y \in Y$*, where "*$\cdot$*" denotes the scalar product of vectors.*

Conversely, suppose that X *and* Y *are finite sets, and* u_x *and* v_y *are unit vectors in* $\mathbb{R}^t$ *for each* $x \in X$ *and* $y \in Y$*. Let* $\mathscr{A}$ *and* $\mathscr{B}$ *be Hilbert spaces of dimension* $2^{\lceil t/2 \rceil}$*,* $\mathscr{H} = \mathscr{A} \otimes \mathscr{B}$ *and* $|\psi\rangle$ *be a maximally entangled state on* $\mathscr{H}$*. Then there exist observables* M_x *on* $\mathscr{A}$ *and* N_y *on* $\mathscr{B}$ *with eigenvalues* ± 1 *such that*

$$\langle\psi|M_x \otimes N_y|\psi\rangle = u_x \cdot v_y$$

for all $x \in X$ *and* $y \in Y$*.*

Therefore, by this theorem, we can characterize the optimal quantum strategy of the two provers by the right choice of unit vectors. This choice of unit vectors can be found using classical methods in time polynomial with respect to the question set sizes.

Consider a binary two-prover one-round game $G = (X, Y, A, B, R, \pi_{XY})$. Suppose the provers share an arbitrary entangled state $|\psi\rangle$ on $\mathscr{H} = \mathscr{A} \otimes \mathscr{B}$ where $\mathscr{A}$ and $\mathscr{B}$ are Hilbert spaces of dimension $2^{\lceil t/2 \rceil}$. Let M_x and N_y be the observables that describe projective measurements of each prover with eigenvalues $+1$ and -1 that can be mapped to outcomes 0 and 1 in that order. Then by theorem (4.5.1), there exist observables M_x on A and N_y on B such that

$$\langle\psi|M_x \otimes N_y|\psi\rangle = u_x \cdot v_y.$$

For XOR games, we sometimes write the winning condition $R(a, b \mid x, y)$ as $R(c \mid x, y)$ where $c = a \oplus b$. By equation (4.3) and by theorem 4.5.1, we have that the probability that $c = 0$ is

$$\begin{aligned}\langle\psi|(M_x^0 \otimes N_y^0 + M_x^1 \otimes N_y^1)|\psi\rangle &= \frac{1}{2}(1 + \langle\psi|M_x \otimes N_y|\psi\rangle) \\ &= \frac{1}{2}(1 + u_x \cdot v_y)\end{aligned}$$

and similarly, the probability that $c = 1$ is $\frac{1}{2}(1 - u_x \cdot v_y)$.

Therefore, by definition 4.3.1 of the value of a game and by theorem 4.5.1, we have that the quantum value of the two-prover one-round XOR game G is given by

$$\omega_q(G) = \sup_{u_x, v_y} \quad \frac{1}{2} \sum_{(x,y) \in X \times Y} (\pi_{XY}(x, y)\,(1 + (R(0 \mid x, y) - R(1 \mid x, y))\,u_x \cdot v_y)$$

where the supremum is over unit vectors

$$\{u_x \in \mathbb{R}^N : x \in X\} \cup \{v_y \in \mathbb{R}^N : y \in Y\}$$

and $N = \min(|X|, |Y|)$.

The necessary tools to prove an upper bound on the value of XOR games with quantum strategy have now all been described. In [CHTW04], the authors describe two upper bounds for the value of quantum games as a function of the classical value: one for weak strategies and one for strong strategies. By strong strategies, we mean that the optimal strategy produces a value near one and by weak strategies that the optimal strategy produces a value near zero. For the rest of this thesis, and in the next section, only the bounds for strong strategies will be considered. We therefore present the proof of the upper bound on the value of XOR games with quantum strategies.

Theorem 4.5.2 ([CHTW04])**.** *Let G be a two-prover one-round XOR game $G = (X, Y, A, B, R, \pi_{XY})$ with classical value $\omega_c(G)$. Then the quantum value $\omega_q(G)$ is bounded by*

$$\omega_q(G) \leq \begin{cases} \gamma_1 \omega_c(G) & \text{if } \omega_c(G) \leq \gamma_2 \\ sin^2(\frac{\pi}{2}\omega_c(G)) & \text{if } \omega_c(G) > \gamma_2, \end{cases}$$

for $\gamma_1 \approx 1.1382$ and $\gamma_2 \approx 0.74202$.

Proof. The quantum value $\omega_q(G)$ is obtained when the provers P_1 and P_2 share an arbitrary pure quantum state as in theorem (4.5.1) and when they measure with $\{M_x\}_x$ and $\{N_y\}_y$ respectively. We will construct a classical strategy from this quantum strategy with the use of theorem (4.5.1) to bound the quantum value as a function of the classical value.

Let the real unit vectors

$$\{u_x : x \in X\}, \{v_y : y \in Y\} \subset \mathbb{R}^t$$

be unit vectors from theorem (4.5.1) that maximize the difference between the quantum value $\omega_q(G)$ and the value of a trivial strategy that outputs bit $a \in A$ and $b \in B$ randomly and independently. A problem that seems to arise is that we do not know the size of t. But in fact, this is not a problem because the winning probability $\tilde{\omega}_q(S)$ of a strategy S depends only on the scalar product of the unit vectors. Therefore, the projection is on the span of $\{u_x : x \in X\} \cup \{v_y : y \in Y\}$ which has dimension $|X| + |Y|$. Since it is sufficient to project vectors $\{u_x : x \in X\}$ onto the span of the vectors

$\{v_y : y \in Y\}$ or vice versa, we have that $t = \min(|X|, |Y|)$. Finally, it is mentioned in [CHTW04], that u_x and v_y can be found using a semidefinite program (i.e.:a special case of convex optimization problems) in time polynomial in $|X| + |Y|$ within an additive error through the maximization.

Consider the classical strategy where u_x is given to prover P_1 and v_y is given to prover P_2 and they share a unit vector $\lambda \in \mathbb{R}^t$ chosen uniformly at random. When they receive their questions x and y, the provers P_1 and P_2 answer respectively $a' \in A$ and $b' \in B$ according to functions

$$a' = \frac{1 + sgn(u_x \cdot \lambda)}{2}$$

$$b' = \frac{1 + sgn(v_y \cdot \lambda)}{2}$$

where the sgn function is defined as usual by $sgn(x) = +1$ if $x \geq 0$ and -1 otherwise.

Next, we calculate the probability that the event $a' \oplus b' = 1$ occurs by introducing an azimuthal coordinate ϕ for λ. ϕ lies in the plane spanned by u_x and v_y such that u_x has coordinate $\phi = 0$ and v_y has coordinate $\phi = \theta_{xy} \equiv \cos^{-1}(u_x \cdot v_y) \in [0, \pi]$.

By geometry, it follows that

$$sgn(u_x \cdot \lambda) = \begin{cases} +1 & \text{if } \phi \in [\frac{-\pi}{2}, \frac{\pi}{2}] \\ -1 & \text{otherwise} \end{cases},$$

$$sgn(v_y \cdot \lambda) = \begin{cases} +1 & \text{if } \phi \in [\theta_{xy} - \frac{\pi}{2}, \theta_{xy} + \frac{\pi}{2}] \\ -1 & \text{otherwise.} \end{cases}$$

Because λ is chosen uniformly in $\mathbb{R}^t$, the azimuthal coordinate ϕ is uniformly distributed in $[0, 2\pi)$. Therefore, the probability that an optimal quantum strategy outputs $a' \oplus b' = 1$ is proportional to the measure that $sgn(u_x \cdot \lambda) = -sgn(v_y \cdot \lambda)$. The latter holds when $\phi \in [-\frac{\pi}{2}, \theta_{xy} - \frac{\pi}{2}] \cup [\frac{\pi}{2}, \theta_{xy} + \frac{\pi}{2}]$, that is with probability

$$Pr[a' \oplus b' = 1] = \frac{(\theta_{xy} - \frac{\pi}{2}) - (-\frac{\pi}{2}) + (\theta_{xy} + \frac{\pi}{2}) - (\frac{\pi}{2})}{2\pi} = \frac{\theta_{xy}}{\pi}. \tag{4.5}$$

With quantum strategies, the probability that $a \oplus b = 1$ is given by

$$\begin{aligned} Pr[a \oplus b = 1] &= \langle \psi | (M_x^0 N_y^1 + M_x^1 N_y^0) | \psi \rangle & (4.6) \\ &= \frac{1}{2}(1 - \langle \psi | M_x \otimes N_y | \psi \rangle) & \text{(by definition of observables)} \\ &= \frac{(1 - u_x \cdot v_y)}{2} & \text{(by theorem (4.5.1))} \end{aligned}$$

$$
\begin{aligned}
&= \frac{(1-\cos(\theta_{xy}))}{2} && \text{(by definition of } \theta\text{)} \\
&= \sin^2\left(\frac{\theta_{xy}}{2}\right) && \text{(because } \cos(2\alpha) = 1 - 2\sin^2(\alpha)\text{)} \\
&= \sin^2\left(\frac{\pi}{2} Pr[a' \oplus b' = 1]\right). && \text{(by equation (4.5))}
\end{aligned}
$$

Now, we want to place an upper bound on the last equality. We introduce a function $g : [0,1] \to [0,1]$ that is bounded below by $\sin^2(\frac{\pi}{2}x)$ and that is concave. The concavity restriction imposes that $g(x)$ must be bounded by the linear mapping $h(x) = \gamma_1 x$ tangent to $\sin^2(\frac{\pi}{2}x)$ at some point $0 < \gamma_2 < 1$ for some constants γ_1 and γ_2. Explicitly, concavity imposes that for some point $0 < \gamma_2 < 1$:

$$
\begin{aligned}
\sin^2\left(\frac{\pi}{2}\gamma_2\right) &= h(\gamma_2), \\
\frac{d}{dx}\sin^2\left(\frac{\pi}{2}x\right)\Big|_{x=\gamma_2} &= \frac{d}{dx}h(x)\Big|_{x=\gamma_2}.
\end{aligned}
$$

Solving this system of equations yields values $\gamma_1 \approx 1.1382$ and $\gamma_2 \approx 0.74202$.

By definition of g being concave on $\mathbb{C}$, given any two points $x, y \in \mathbb{C}$, we have

$$
\frac{g(x) + g(y)}{2} \leq g\left(\frac{x+y}{2}\right). \tag{4.7}
$$

This condition will be used in the rest of the proof.

From the definition of the function g and equation (4.6), we thus have the relation between the quantum strategy and the classical strategy

$$
Pr[a \oplus b = 1] \leq g(Pr[a' \oplus b' = 1]), \tag{4.8}
$$

and in a similar manner

$$
Pr[a \oplus b = 0] \leq g(Pr[a' \oplus b' = 0]). \tag{4.9}
$$

From these two results, if we denote the probability of any classical strategy S_c by $S_c(a, b|s, t)$ and the probability of quantum strategies S_q by $S_q(a, b|s, t)$ on questions $x, y \in X \times Y$ and answers $a, b \in A \times B$,we have that

$$
S_q(a, b \mid x, y) \leq g(S_c(a, b \mid x, y)). \tag{4.10}
$$

It follows that the winning probability of quantum strategies $\omega(S_q)$ is bounded by

$$
\omega(S_q) = \sum_{(x,y)} \left(\pi_{XY}(x, y) \sum_{(a,b)} R(a, b \mid x, y) S_q(a, b \mid x, y) \right)
$$

$$\leq \sum_{(x,y)} \left(\pi_{XY}(x,y) \sum_{(a,b)} R(a,b \mid x,y) g\big(S_c(a,b \mid x,y)\big) \right)$$

(by equation (4.10))

$$\leq g\left(\sum_{(x,y)} \left(\pi_{XY}(x,y) \sum_{(a,b)} R(a,b \mid x,y) S_c(a,b \mid x,y) \right) \right)$$

(by equation (4.7))

$$= g(\omega(S_c))$$

and therefore by definition (4.3.1) of the value of a game G with quantum strategies, $\omega_q(G)$ is bounded by

$$\begin{aligned} \omega_q(G) &= \sup_{S_q} \quad (\omega(S_q)) \\ &\leq \sup_{S_c} \quad (g(\omega(S_c))) \\ &\leq g\left(\sup_{S_c} \quad (\omega(S_c)) \right) \\ &= g(\omega_c(G)). \end{aligned}$$

□

4.6 Example: The Odd Cycle Game

In this section, we present a game that will serve as a representative example for the topics of this thesis. The game is called the Odd Cycle Game (OC game)[CHTW04], which is a variation of a game in [BC90] also discussed in [Vai01]. This game is a two-prover one-round game in which provers P_1 and P_2 want to convince a verifier that an odd cycle of length $m \geq 3$ is 2-colourable. In general, we say that a graph is c-coloured if each of its vertices can be assigned one of the c colours such that no adjacent vertices are of the same colour. It is obvious that an odd cycle of length $m \geq 3$ is not 2-colourable since n is odd, and therefore classical provers should not be able to win with probability 1. Figure (4.2) shows an example of odd cycle of length 5. As any odd cycle, the odd cycle depicted is not 2-colourable.

This game is a binary XOR games because the set of answers of the provers is binary and the winning condition is a XOR function of the answers of the provers.

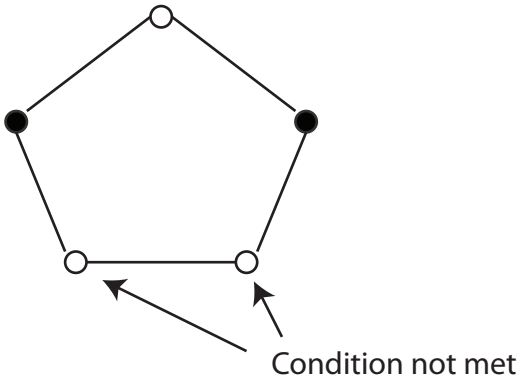

Figure 4.2: Impossibility of 2-Colourability of an Odd Cycle of Length 5.

In this game, the verifier sends a vertex of the cycle to each of the two provers, who are isolated from each other. The provers are then asked to give one of two colours to the verifier. The verifier wants to check that if the same vertex has been sent to the provers, the colours match and if the two vertices are adjacent, they are of different colours. If both conditions hold, it is an indication that the provers might be telling the truth.

In the formalism of games, an Odd Cycle Game G_{OC} of length $m = 2l + 1$ with $l \geq 1$ can be described as $G_{OC} = (X, Y, A, B, R, \pi_{XY})$ where $X = Y = \mathbb{Z}/m\mathbb{Z}$ and $A = B = \{0, 1\}$. The distribution π_{XY} is such that with probability $\frac{1}{2}$, $x = y$, and with probability $\frac{1}{2}$, $y = x + 1$ where addition is in $\mathbb{Z}/m\mathbb{Z}$. Note that for this probability distribution $\pi_{XY} \neq \pi_X \times \pi_Y$. The winning condition R is defined as

$$R(a, b \mid x, y) = \begin{cases} 1 & \text{if } a \oplus b = 0 \text{ when } x = y \\ 1 & \text{if } a \oplus b = 1 \text{ when } y = x + 1 \text{ mod(m)} \\ 0 & \text{otherwise} \end{cases} . \tag{4.11}$$

We will now prove the value that can be achieved for this game with classical and quantum strategies and will present an optimal strategy for both strategy classes.

Theorem 4.6.1 (Classical value of Odd Cycle Game[CHTW04])**.** *The value of the two-prover one-round Odd Cycle Game G_{OC} of length $m = 2\ell+1$ with $\ell \geq 1$ when provers are limited to classical strategies is $\omega_c(G_{OC}) \leq 1 - \frac{1}{2m}$.*

Proof. Consider a cycle of length $m = 2\ell + 1$ with $\ell \geq 1$. Obviously, one of the vertices cannot fulfill all the conditions for 2-colourability since m is odd. Therefore, there must exist two adjacent vertices of the same colour. Since

there are m possible questions to each prover, there are $2m$ possible different pairs (x, y) of questions. Because one of these questions cannot be satisfied and the distribution of questions is uniform over the $2m$ possible different unordered pairs (x, y), the provers must fail to answer with probability $\frac{1}{2m}$. This means that the value of the game is no more than $1 - \frac{1}{2m}$. □

The deterministic strategy consists of assigning a colour to each vertex of the cycle such that no adjacent vertices are of the same colour. As theorem (4.6.1) has shown, they cannot do better than failing for one of the questions. The next theorem presents an optimal deterministic strategy for the provers.

Theorem 4.6.2 (An Optimal Classical Strategy for Odd Cycle Game[CHTW04])**.** *The strategy in a two-prover one-round Odd Cycle Game G_{OC} of length $m = 2l + 1$ with $l \geq 1$ where prover P_1 answers $a \in A$ to the question $x \in X$ as follows*

$$a = x \mod (2)$$

and prover P_2 answers $b \in B$ to the question $y \in Y$ from the function

$$b = y \mod (2)$$

is an optimal classical strategy.

Proof. Consider an odd cycle of length $m = 2l + 1$ with $l \geq 1$. From the provers' strategy, we have $a + b = x + y \mod (2)$.

First, suppose $x = y$. Then we have $a + b = x + y \mod (2) = 2x \mod (2)$. Because for any choice of $x \in \mathbb{Z}/m\mathbb{Z}$ the product $2x$ is even, we have that $a + b = 0 \mod (2)$. This is equivalent to the mathematical formulation $a \oplus b = 0$ by the definition of the XOR function. By the definition (4.11) for the winning condition for the Odd Cycle Game, the verifier will accept the answers.

Second, suppose $y = x+1 \mod (m)$. Without loss of generality, suppose that we index each vertex from 0 to $m - 1$. We show that for any $x \in \{0, ..., m - 2\}$, the verifier accepts and for $x = m - 1$, the verifier rejects.

For any $x \in \{0, ..., m - 2\}$, we have $y = x + 1 < m$. The parity of y is different from that of x. We thus have $a + b = x + y \mod (2) = x + (x + 1) \mod (2) = 2x + 1 \mod (2)$. For any choice of x, the quantity $2x + 1$ is odd and therefore $a + b = 1 \mod (2)$, which is equivalent to $a \oplus b = 1$ and makes the verifier accept.

For $x = m - 1$, we have $y = x + 1 \mod (m) = m \mod (m) = 0$. Since m is odd and $x = m - 1$, we have that x is even; $y = 0$ is also even. We thus have $a + b = x + y \mod (2) = x \mod (2) = 0 \mod (2)$, which is equivalent to $a \oplus b = 0$ and makes the verifier rejects.

We have shown there is only one pair of questions $(x, y) = (m - 1, 0)$ from the distribution $\pi_{XY}$for which the verifier rejects. Since there is $2m$ possible questions, the verifier accepts with probability $1 - \frac{1}{2m}$, which is the optimal classical probability according to (4.6.1). Therefore, this strategy is optimal. □

The classical value of two-prover one-round Odd Cycle Game G_OD follows directly from theorem (4.6.1) and theorem (4.6.2). We expose it in the following corollary.

Theorem 4.6.3 (The value of Odd Cycle Game[CHTW04])**.** *The value of the two-prover one-round Odd Cycle Game G_{OC} of length $m = 2l + 1$ with $l \geq 1$ when provers are limited to classical strategies is $\omega_c(G_{OC}) = 1 - \frac{1}{2m}$.*

Now, we move on to the class of quantum strategies. We will present a quantum strategy for the provers and prove that this strategy is an optimal quantum strategy with the use of theorem (4.5.2) that puts an upper bound on the quantum value of XOR games as a function of the classical value.

Theorem 4.6.4 (An Optimal Quantum Strategy for Odd Cycle Games [CHTW04])**.** *There exists a family of quantum strategies S_q for provers in a two-prover one-round Odd Cycle Game G_{OC} of length $m \geq 3$ that achieves winning probability $\omega(S_q) = \cos^2\left(\frac{\pi}{4m}\right)$ by sharing a single EPR pair.*

Proof. The quantum strategy presented is taken from [CHTW04]. It consists in sharing a single EPR pair

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle).$$

Define the states $|\phi_0\rangle$ and $|\phi_1\rangle$ by

$$|\phi_0(\theta)\rangle = \cos(\theta)|0\rangle + \sin(\theta)|1\rangle,$$

and

$$|\phi_1(\theta)\rangle = -\sin(\theta)|0\rangle + \cos(\theta)|1\rangle.$$

Let the projective measurements M and N of prover P_1 and P_2 for $a, b \in \{0, 1\}$ be

$$M_x^a = |\phi_a(\alpha_x)\rangle\langle\phi_a(\alpha_x)|,$$

$$N_y^b = |\phi_b(\beta_y)\rangle\langle\phi_b(\beta_y)|,$$

respectively where the parameters α_x and β_y are defined by

$$\alpha_x = \left(\frac{\pi}{2} - \frac{\pi}{2m}\right) x + \frac{\pi}{4m},$$

and

$$\beta_y = \left(\frac{\pi}{2} - \frac{\pi}{2m}\right) y.$$

The probability that the provers answer the same bit is

$$\begin{aligned}
\Pr[a = b] &= \langle\Phi^+|M_x^a \otimes N_y^b|\Phi^+\rangle && \text{(by equation (2.6))} \\
&= \mathrm{tr}\left(M_x^a N_y^b|\Phi^+\rangle\langle\Phi^+|\right) && \text{(by equation (2.4))} \\
&= \frac{1}{2}\mathrm{tr}\left(M_x^a N_y^b\right) \\
&= \cos^2(\alpha_x - \beta_y)
\end{aligned}$$

and the probability that they answer differently is $1 - \cos^2(\alpha_x - \beta_y) = \sin^2(\alpha_x - \beta_y)$. If $x = y$, then the provers answer correctly with probability

$$\cos^2(\alpha_x - \beta_y) = \cos^2\left(\frac{\pi}{4m}\right).$$

If $y = x + 1 \mod (m)$, they answer correctly with probability

$$\begin{aligned}
\sin^2(\alpha_x - \beta_y) &= \sin^2\left(\frac{\pi}{4m} - \left(\frac{\pi}{2} - \frac{\pi}{2m}\right)\right) \\
&= \sin^2\left(\left(\frac{\pi}{2} - \frac{\pi}{2m}\right) - \frac{\pi}{4m}\right) && \text{(because } \sin(-x) = -\sin(x)\text{)} \\
&= \sin^2\left(\frac{\pi}{2} - \frac{\pi}{4m}\right) \\
&= \cos^2\left(\frac{\pi}{4m}\right). && \text{(because } sin\left(\tfrac{\pi}{2} - x\right) = \cos(x)\text{)}
\end{aligned}$$

Therefore, the provers will be able to achieve the two conditions of the Odd Cycle Game for any question pair $(x, y) \in X \times Y$ with probability $\cos^2(\frac{\pi}{4m})$ using this strategy. □

In the next theorem, we prove that the strategy used in theorem (4.6.4) is optimal and at the same time prove that the quantum value is $\omega_q(G_{OC}) = \cos^2(\frac{\pi}{4m})$.

Theorem 4.6.5 (Quantum Value of Odd Cycle Games [Ton09])**.** *The value of the two-prover one-round Odd Cycle Game G_{OC} of length $m = 2l + 1$ with $l \geq 1$ and quantum strategies is*

$$\omega_q(G_{OC}) = \cos^2\left(\frac{\pi}{4m}\right).$$

Proof. The Odd Cycle Game is a binary XOR game and the upper bound of theorem (4.5.2) applies. For any $m \geq 3$, we have $\omega_c(G_{OC}) > \gamma_2$ where γ_2 is defined in theorem (4.5.2). It follows that

$$\begin{aligned}
\omega_q(G_{OC}) &\leq \sin^2\left(\frac{\pi}{2}\omega_c\left(G_{OC}\right)\right) \\
&= \sin^2\left(\frac{\pi}{2} - \frac{\pi}{4m}\right) \\
&= \cos^2\left(\frac{\pi}{4m}\right). \qquad \text{(using } \sin\left(\tfrac{\pi}{2} - \theta\right) = \cos\left(\theta\right)\text{)}
\end{aligned}$$

By theorem (4.6.4), the upper bound can be achieved with a quantum strategy. Therefore, we have

$$\omega_q\left(G_{OC}\right) = \cos^2\left(\frac{\pi}{4m}\right).$$

□

In the remainder of the thesis, Odd cycle Games will be used as a particular example in the results demonstrated therein.

Chapter 5

The Power of Many Provers

In this section, the effect of adding more than two provers on the power of interactive proof systems with different classes of strategies is studied. A natural way to study these effects is through the game framework of last chapter. Using the game notation, it will be possible to investigate relation for the different classes with respect to the strategies in place.

It may seem natural to consider arbitrary k-prover games in which each provver would be given his own input and be expected some output. However, we are interested here in *extending* a *given* two-prover game to the multi-prover scenario. For this, we will follow the methodology described in [Ton09]. The method transforms a two-prover one-round game $G_2 = (X, Y, A, B, R, \pi_{XY})$ into a k-prover one-round game $G_k = (X, Y, A, B, R', \pi_{XY})$ with $k \geq 2$ where the subscript indicates the number of provers. Note that only the definition of the winning condition is modified when extending a two-prover game to a k-prover game and the probability distribution π_{XY} is the same. The idea in the game G_k is to sample $(x, y) \in X \times Y$ from π_{XY} and send $x \in X$ to prover P_1 and $y \in Y$ to prover P_2 as in G_2. The verifier also sends y to the $k-2$ remaining provers. The winning condition of the new game G_k imposes on provers P_1 and P_2 that they satisfy the winning condition R and that the answers b_i of all the other provers are equal to the answer b_1 of P_2. Formally, the winning condition of game G_k is

$$R'(a, b_1, ..., b_{k-1}|x, y) = R(a, b_1|x, y) \cap [b_1 = ... = b_{k-1}].$$

The protocol is illustrated in Figure (5.1).

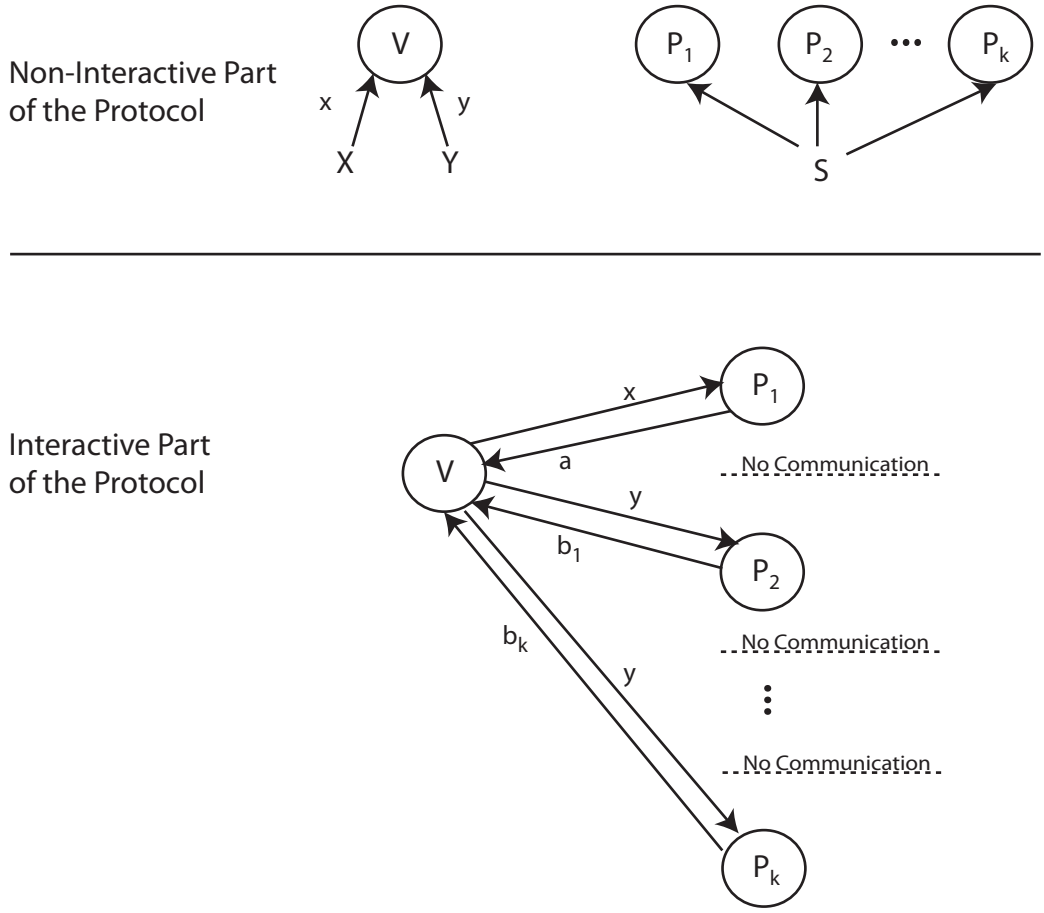

Figure 5.1: Multi-Prover Interactive Game Protocol.

5.1 Many-Prover Classical Games

In this section, we investigate multi-prover games with classical strategies for $k > 2$. We already mentioned the effective power of interactive proof systems with one prover. A result in 1992 stated that $IP = PSPACE$ [Sha92]. When the number of provers is increased to two, it has been shown that $NEXP = MIP[2, 1]$ [BFL90]. Two provers might therefore be

more powerful than one prover if *PSPACE* $\neq$ *NEXP*. This stems from the fact that the provers have a much limited way of cheating since they have to answer according to a shared strategy and are separated. Basically, the verifier takes one prover as an "oracle" to check the answer of the other. In fact, the power increases with the number of provers if the value of the game decreases as the number of provers increases. We will see what power is achievable with classical strategies in the following theorem:

Theorem 5.1.1 ([Ton09])**.** *The classical value* $\omega_c(G_2)$ *of a two-prover one-round game* $G_2 = (X, Y, A, B, R, \pi_{XY})$ *is equal to the classical value* $\omega_c(G_k)$ *of the game* $G_k = (X, Y, A, B, R', \pi_{XY})$ *with* $k \geq 2$ *provers.*

Proof. We want to prove that $\omega_c(G_2) = \omega_c(G_k)$ for $k \geq 2$. Consider an optimal classical strategy S_{opt} for G_2. This strategy is deterministic since any probabilistic strategy is a probability distribution over deterministic strategies. The strategy of each prover is a deterministic function of the question they receive. This gives deterministic functions to the other $k-2$ provers which use the same function as prover P_2.

Application of the deterministic function of prover P_2 by the other provers constitute a strategy for G_k. Since the other $k-2$ provers behave as P_2, the winning condition, for any questions $x, y \in X \times Y$ and answers $a, b_1, ..., b_{k-1} \in A \times B^{k-1}$, we have $S(a, b_1, b_2, ..., b_{k-1}|x, y) = S_{opt}(a, b_1|x, y)$ and $R' = 1$ only and only if $R = 1$. This is true because the equalities $b_1 = ... = b_{k-1}$ are enforced by the condition that the other $k-2$ provers action are the same as P_2. By the definition (4.3.1) of the value of a game, we have that

$$\begin{aligned}\omega_c(G_2) &= \sum_{(x,y)\in X\times Y} \pi_{XY}(x,y) \sum_{(a,b)\in A\times B} R(a,b|x,y) S_{opt}(a,b|x,y) \\ &= \omega_c(G_k)\end{aligned}$$

□

The result of theorem (5.1.1) shows that with classical strategies, adding more than two provers does not change the value of a two-prover one-round game and therefore does not improve the power of the associated proof system. Consequently, with classical strategies, adding more provers does not change the power of the class *MIP*[2]. In our illustrative example of the *Cole* vs *Petsi* experiment, adding more than two provers, therefore, yields the same value for classical provers. There is, therefore, no need to add more provers to the game to restrict how the provers behave.

We will now study the same conditions but with quantum and no-signalling strategies. We will see that results are different than those with classical strategies.

5.2 Many-Prover Non-Classical Games

We have seen that when the provers have quantum strategies, it can increase the value of games like the Odd Cycle Game [CHTW04]. However, does adding more than two provers in a game change the power of the class $MIP^*[2,1]$? Does it affect the value of a game? These are fundamental questions in complexity theory of interactive proofs for which there is no complete answers.

In presence of two provers with quantum strategies, oracularization, described in section 3.3, has not the same effectively as in the classical case. The Odd Cycle Game is a a clear example that oracularization, checking the corroboration of answers of the provers, is less efficient for the verifier in the quantum case. This is explained by the quantum value of this game which is greater than the classical value. However, this phenomenon is less trivial with more provers. The problem of having more provers is linked to how many entanglements the provers share and also to the size of the question and answer sets. As there is no standard on how to measure the amount of entanglements between more than two parties, the extrapolation to more than two provers is not known. Because of this, it is also extremely hard to infer bounds on the limit of the value these games can achieve.

As we will see, the efficiency of oracularization with quantum strategies will be restored as the classical case in presence of more than two provers. This can be explained by the fact that entanglements can be maximal in the case of two provers, something that is impossible to do with more than two provers. This is referred as monogamy of entanglement [Ton09]. With projective measurements, each prover wants to apply a projector to their part of the state as a function of the question and measure their state so as to obtain the right answer and without disturbing the reduced state of the other provers. For example, if provers A, B and C share a state $|\psi\rangle$, then when one prover has measured, the resulting state of the two other provers cannot be maximally entangled. If A and B are maximally entangled, then the qubits of C cannot be correlated maximally with both A and B; C will therefore be classically correlated with A and B. In other words, the more there are parties, the less they are entangled. This phenomenon is

particularly important for cryptographic purposes since it puts bounds on how much an eavesdropper C could learn about the communication between provers A and B using a quantum channel.

A dependency between the number of extra prover $k-2$ with the number of possible questions m to the second prover is made explicit with no-signalling strategies in [MAG06]. Preliminary results were made in [TDS03] based on the work of [Wer89] that proved similar result with quantum correlations. The next theorem states the results for no-signalling strategies which are even stronger than the case of quantum strategies and serves as a stronger upper bound. This is the reason it is presented with no-signalling strategies rather that quantum strategies.

Theorem 5.2.1 ([MAG06, Ton09])**.** *Let $G_2 = (X, Y, A, B, R, \pi_{XY})$ be a two-prover game with $m = |Y|$ and $G_{m+1} = (X, Y, A, B, R', \pi_{XY})$ be a $(m+1)$-prover game. Then the value with no-signalling strategies $\omega_{ns}(G_{m+1})$ is a nonincreasing sequence in m and*

$$\omega_{ns}(G_{m+1}) = \omega_c(G_2).$$

Proof. First of all, the no-signalling values $\omega_{ns}(G_{m+1})$ are non-increasing sequences in m since a strategy for $m+1$ provers would give a strategy for $2 \leq m' + 1 < m + 1$ provers by simply ignoring $m - m'$ provers.

Secondly, consider a no-signalling strategy for G_{m+1}, that is a set of probabilities $S(a, b_1, b_2, ..., b_m|x, y_1, y_2, ..., y_m)$. Here, we distinguish the questions y_i for each prover because the proof holds for any question y_i for . We now show that a two-prover classical strategy $S(a, b|x, y)$ can be built with the same probability distribution over the answers for each prover. We have that the distribution $S(a, b_1, b_2, ..., b_m|x, y_1, y_2, ..., y_m)$, can be constructed as well as the distributions $S(b_1, b_2, ..., b_m|y_1, y_2, ..., y_m)$ and $S(a|x, b_1, b_2, ..., b_m, y_1, y_2, ..., y_m)$. Let the provers share string $e = b_1, b_2, ..., b_m$ from the distribution $p(e) = S(b_1, b_2, ..., b_m|y_1, y_2, ..., y_m)$ when the corresponding inputs $y_1, y_2, ..., y_m$ are fixed. By the definition of conditional probability, we can construct a local model for $S(a, b|x, y)$. The two-prover classical strategy can be written as

$$\begin{aligned} S(a, b|x, y) = \sum_{b_1, b_2, ..., b_m} \Big[& S(b_1, b_2, ..., b_m|y_1, y_2, ..., y_m) \\ & \cdot S(a|x, b_1, b_2, ..., b_m, y_1, y_2, ..., y_m) \\ & \cdot S(b_1|x, b_1, b_2, ..., b_m, y_1, y_2, ..., y_m) \Big] \end{aligned}$$

$$
\begin{aligned}
&= \sum_e p(e) S(a|x,e) \delta_{b_1,y_1} \delta_{b_2,y_2} ... \delta_{b_m,y_m} \\
&\qquad\qquad (\delta_{m,m'} \text{ defined in equation (2.9)}) \\
&= \sum_e p(e) S(a|x,e) S(b|y,e) \qquad \text{(equation (4.2))} \\
&= \sum_e p(e) S(a|x,e) S(b_1|y_1,e) S(b_2|y_2,e) ... S(b_m|y_m,e) \\
&\qquad\qquad (\text{where } S(b|y,e) = S(b_i|y_i,e)) \\
&= S(a,b_1,b_2,...,b_m|x,y_1,y_2,...,y_m)
\end{aligned}
$$

where the last equation is the no-signalling probability distribution on $m+1$ provers. This is true because the probability distribution $p(e)$ is no-signalling and therefore all $S(b_i|y_i,e)$ are no-signalling as well. Because the theorem holds for any y_i, it holds for the special case where $y_1 = y_2 = ... = y_m$. □

For example, for any game two-prover game G_2 where $|A| = |B| = 2$, theorem (5.2.1) tell us that the no-signalling value with three provers $\omega_{ns}(G_3)$ is equal to a the classical value with two provers $\omega_c(G_2)$. By equation (4.4), we have that the quantum value $\omega_q(G_3)$ is also equal to $\omega_c(G_2)$.

However, as you can observe, theorem (5.2.1) does not cover all arbitrary cases of sizes of question sets. In general, the difference between the classical and no-signalling value for an arbitrary number of questions with three provers is not known.

This theorem has implication on the complexity of the class MIP^* and $\oplus MIP^*$. We know that $\oplus MIP_{c,s}[2,1] = NEXP$ for some choice of probabilities c and s [BGS98, Hås01]. However, the results that $\oplus MIP^*[2] \subseteq EXP$ [Weh06] cannot be generalized to any number of provers. This comes from the fact that for a particular number of questions and provers, quantum provers cannot cheat more than classical provers. In some situation, we have $\oplus MIP^*[2] = NEXP$. Theorem (5.2.1) gives also indications that the number of provers is not an independent parameter. To better understand the complexity of the class MIP^* and particularly $\oplus MIP^*$, we probably have to separate these classes into subclasses as a function of the number of questions as well as the number of provers.

In the section that follows, we will try to check how the addition of players affects the value of the game in the particular case of the Odd Cycle Game.

5.3 Many-Prover Odd Cycle Games

In this section, we apply the result of the last two sections to the Odd Cycle Game. We will see that for this specific game, we can improve earlier results.

In the case the provers are restricted to classical strategies, we have shown with theorem (5.1.1) that increasing the number of provers has no effect on the value of the game. It is easy to verify that the optimal classical strategy for the Odd Cycle Game in theorem (4.6.2) easily extend to $k \geq 2$ provers resulting in the same value $\omega_c(G_{OC,k}) = 1 - \frac{1}{2m}$ where we denote the Odd Cycle Game with k provers by $G_{OC,k}$.

With quantum strategies, more than two provers cannot share a maximally entangled state. This indicates that the value could be different from the two-prover case. We note that the value of the Odd Cycle Game increases slowly as the number of question m is increased. Therefore, the verifier has interest to keep the number of cycle m as low as possible to reduce the value of the game. Theorem (5.2.1) tell us that for an odd cycle of length m, $m+1$ provers are required to restrict the no-signalling and quantum value of the game to a classical one (e.g.: when $m = 3$, four provers are needed). For an arbitrary number of question m, however, the high number of prover required is impractical. An improved result with only three provers is demonstrated in [Ton09] to have the same effect for the case of the Odd Cycle Game.

Theorem 5.3.1. *The Odd Cycle Game $G_{OC,3} = (X, Y, A, B, R', \pi_{XYZ})$ of length m with three provers and no-signalling strategies has the same value as the Odd Cycle Game $G_{OC} = (X, Y, A, B, R, \pi_{XY})$ of length m with classical strategies*

$$\omega_{ns}(G_{OC,3}) = \omega_c(G_{OC}) = 1 - \frac{1}{2m}.$$

Proof. For notational preference, we have denoted the probability distribution π_{XYZ} in $G_{OC,3}$ to make explicit the three provers. However, the definition is as usual: for any x,y and z, $p_{XYZ}(x, y, z) = p_{XY}(x, y)\delta_{yz}$. Denote the questions set by Q such that $Q = X = Y = \{1, ..., m\}$ and answer set by A such that $A = B = \{0, 1\}$. We want to maximize the probability $S(a, b, c|x, y, z)$ where $a, b, c \in A$ and $x, y, z \in Q$ where provers (P_1, P_2, P_3) receive question (x, y, z) and answer by (a, b, c) respectively. The maximization over strategy family S can be cast as a linear problem.

First, we introduce a set of symmetries that are going to reduce the problem. Then, we write the constraints for maximization and finally we

write the dual problem as in A. An optimal solution to the dual problem will give the best lower bound of the problem.

The following set of symmetries does not change the value of the game and help to reduce the problem

1. all parties can flip the binary value of their outputs, and/or
2. all parties can add an integer to their inputs, and/or
3. Provers P_2 and P_3 can exchange roles.

The value of a XOR game is invariant under these symmetry by the nature of the function XOR.

Using symmetry 1 and 2, we can restrict our attention to the case $a = 0$ and $x = 0$ without loss of generality. Because it does not change $S(a, b, c|x, y, z)$, we have that $S(a, b, c|x, y, z) = S(0, b, c|0, y, z)$ which we denote by $r(b, c|y, z) = S(0, b, c|0, y, z)$. Symmetry 3 is later used to add a new constraint to the optimization problem.

The case where provers P_1 and P_2 have the same question which imposes that their answer is the same is represented by $r(0, 0|0, 0)$. The case where provers P_1 and P_2 does not have the same question which means that they must answer by a different colour by the nature of the odd cycle game is represented by $r(0, 0|0, 0)$. It is sufficient to consider only these questions to prover P_2 to cover evenly the probability distribution of the Odd Cycle Game by the symmetry 1 and 2. The method used to add more provers to a game imposes that the questions and answers of P_2 and P_3 are the same. We can therefore write the no-signalling value of $G_{OC,3}$ as

$$\omega_{ns}(G_{OD,3}) = \sup_r \left(\frac{1}{2}[r(0, 0|0, 0) + r(1, 1|1, 1)] \right).$$

This defines the objective function of the primal problem to maximize.

The constraints for the objective function of the primal problem are listed along with the labeling of the constraints for the dual problem as in [Ton09]:

- Normalization constrain $n(y, z)$:
  $\sum_{b,c} r(b, c|x, y) = 1$, for $0 \leq j$ and $k < m$.
- Symmetry constrain $s(b, c|y, z)$:
  $r(b, c|y, z) = r(c, b|z, y)$, for $b, c \in \{0, 1\}$ and $0 \leq j$ and $k < m$. This constraint comes from symmetry 3.

- No-signalling constraints:

  1. P_1 to P_2 and P_3, $y(d|y,z)$:
     $r(0,d|y,y+z)+r(1,1-d|y,y+z)=r(0,d|0,z)+r(1,1-d|0,z)$,
     for $d\in\{0,1\}$ and $1\leq j<m$ and $0\leq k<m$.
  2. P_2 to P_1 and P_3, $z(d|y,z)$:
     $r(0,d|y,z)+r(1,d|y,z)=r(0,d|0,z)+r(1,d|0,z)$, for $d\in\{0,1\}$ and $1\leq j<m$ and $0\leq k<m$.

The no-signalling conditions P_2 and P_3 to P_1 and P_1 and P_3 to P_2 do not further constrain the solution of the objective function.

Having defined the primal of the problem with its constraints, we write the objective function of the dual as the minimization of

$$\frac{1}{2m}\sum_{j,k} n(j,k) \tag{5.1}$$

Constraints of the dual problem are

1. $\mu(0,0|0,0)\geq n$
2. $\mu(1,1|1,1)\geq n$
3. $\mu(b,c|y,z)>0$

for all $b,c\in\{0,1\}$ and for $0\leq j,k\leq n$ where the function $\mu(b,c|y,z)$ is defined as

$$\begin{aligned}\mu(b,c|y,z) = n(j,k) &+ s(b,c|y,z) - s(c,b|z,y)\\ &+ [y=0]\sum_{y'=1}^{m-1}\left(y\left(\frac{1-bc}{2}|y,z\right)+z(c|y',z)\right)\\ &- [y\neq 0]\left(y\left(\frac{1-bc}{2}|y,z-y\right)+z(c|y,z)\right)\end{aligned}$$

A solution of the dual problem is given in B. Although, the non-zero variables for the solution were found numerically, the solution can be checked analytically.

By substituting the solution of the dual problem from B, equation (5.1) gives $\omega_{ns}(G_{OC,3})\leq 1-\frac{1}{2m}$. Since the classical value $\omega_c(G_{OC})=1-\frac{1}{2m}$ is a lower bound, we have that $\omega_{ns}(G_{OC,3})=\omega_c(G_{OC})=1-\frac{1}{2m}$. □

Since we know that the value $\omega_q(G_{OC,3})$ is bounded above $\omega_c(G_{OC,3})$ and below $\omega_{ns}(G_{OC,3})$ by equation (4.4), it follows that

Corollary 5.3.1. *The Odd Cycle Game $G_{OC,3}$ of length m with three provers and quantum strategies has the same value as with classical strategies:*

$$\omega_q(G_{OC,3}) = \omega_c(G_{OC}) = 1 - \frac{1}{2m}.$$

Therefore, adding one prover to the two-prover Odd Cycle Game restrict the set of strategy to classical strategies. This is an improvement over theorem (5.2.1) since it says that for any m, only three provers are required for $\omega_q(G_{OC,3}) = \omega_c(G_{OC})$ instead of the previous $m + 1$ provers.

In [BHK05], the addition of a third prover has already been used to limit the information that an eavesdropper (i.e.: the third prover) would gain from a key distribution. The authors prove that even with a post-quantum theory, if the first and second provers do no violate a Bell inequality, the third prover can get all information between them using post-quantum states that are deterministic and local. On the other hand, if the first and second provers violate a Bell inequality, then some of the post-quantum state of the third prover must be nonlocal. Since determinism and nonlocality in a state allow signalling, the third prover will not be able to obtain perfect information.

Finally, in [AGM06], it has been proven that more provers in a Quantum Key Distribution (QKD) protocol is provably secure against non signalling provers.

Chapter 6

Parallel Repetition of Two-Prover One-Round Games

In what follows, we discuss another important modification to two-prover one-round games: parallel repetition. Sequential repetition was discussed earlier and we have seen that it increases the soundness probabilities. Informally, parallel repetition of a two-prover one-round game G is a game G^n where the provers try to win $n \geq 1$ instances of the game G simultaneously.

More formally, the games $G_1, ..., G_n$ in parallel is described by $\wedge_{j=1}^{n} G_j$. The verifier sends $x_1, ..., x_n \in X_1 \times ... \times X_n$ to the first prover and $y_1, ..., y_n \in Y_1 \times ... \times Y_n$ to the second prover where each pair (x_i, y_i) is chosen independently from he original distribution $\pi_{X_i Y_i}$ from each game G_i. Then prover P_1 answers with $a_1, ..., a_n \in A_1 \times ... \times A_n$ and prover P_2 with $b_1, ..., b_k \in B_1 \times ... \times B_n$. They win the game $\wedge_{j=1}^{n} G_j$ if and only if they win each instances of game G_i. This means that they win if for every $0 \leq i \leq n$, $R(a_i, b_i | x_i, y_i) = 1$.

The protocol for n games in parallel is illustrated in Figure (6.1).

It is obvious that any kind of repetition has an effect on the value of the repeated game. Sequential repetition of a two-prover one-round game decrease the probability of winning by the provers exponentially but requires multiple rounds. The advantage of parallel repetition is that it preserves the number of rounds of a game. Trivially, for games $G_1, ..., G_n$ in parallel, we have that

$$\omega_q(\wedge_{j=1}^{n} G_j) \geq \prod_{j=1}^{n} \omega(G)^n \tag{6.1}$$

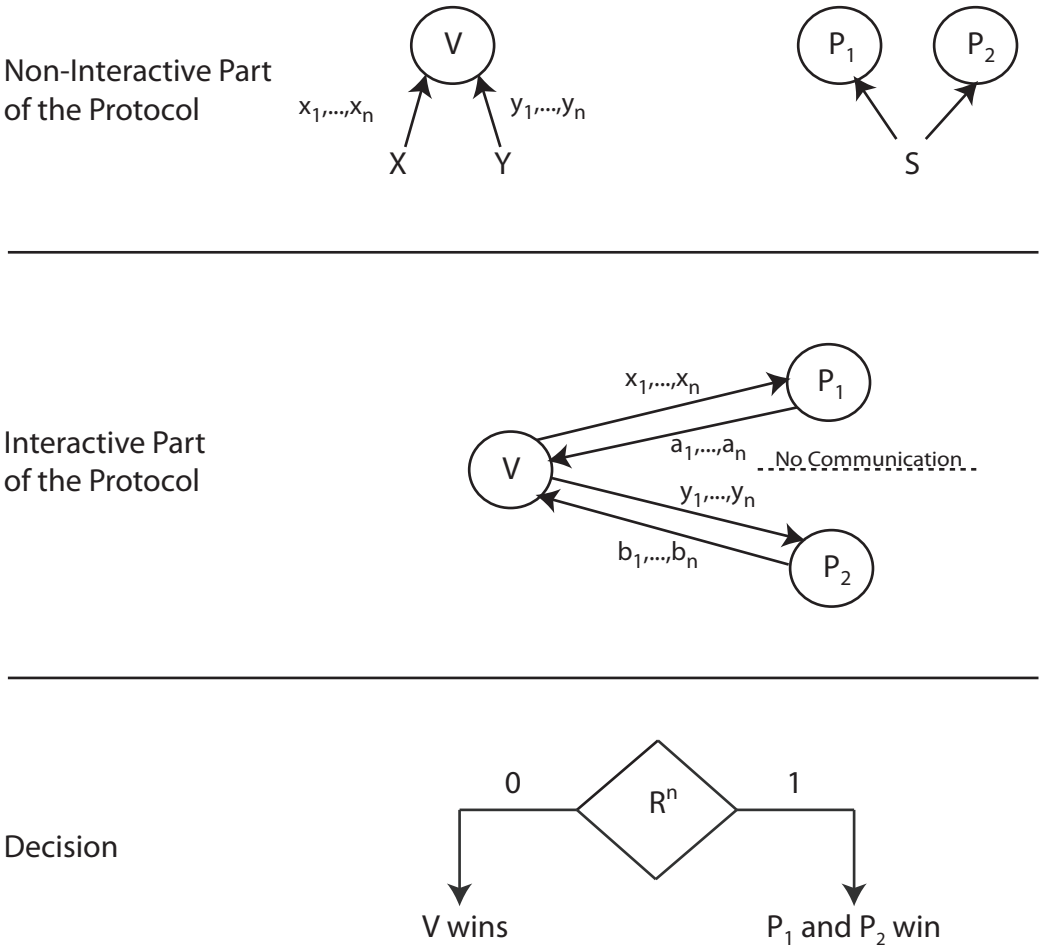

Figure 6.1: Two-Prover Interactive Game with Parallel Repetition.

because each player could play each instance of each game independently using an optimal strategy for each instance. In particular, when all the games are the same, we have use the notation $\wedge_{j=1}^{n} G_j = G^n$ and we have

$$\omega(G^n) \geq \omega(G)^n.$$

In the following section, we review the results obtained for parallel repetition with classical, quantum and no-signalling strategies and analyse its effect on the Odd Cycle Game.

6.1 Parallel Repetition of Classical Games

When computational theorist started to study parallel repetition, it was falsely believed that it could achieve the same exponential decrease in prob-

ability of winning for the provers [FRS88, FRS90]. A counterexample of this was shown in [For89]. Later,a simplified problem was studied where the probability distribution over the question sets is independent of each prover (i.e.:$\pi_{XY} = \pi_X \times \pi_Y$). Games based on these independent distributions are called no-information games. Otherwise, they are called games of partial-information. It was proved in [CCL90] that in the case of no-information games, n parallel repetitions would decrease the probability of error exponentially like sequential repetition. This bound was further improved in [LS91, Pel90, Fei91, Alo91].

After many years, it was not known whether parallel repetition could make the probability of error arbitrary small for a general case of unrestricted probability distribution. Then, it was proven in the general case that the probability of error can be made arbitrary small but without giving constructive bounds for the number of repetitions required to decrease the probability of error below a given bound [Ver94]. Finally, it was in [Raz98] that this number of repetition was made clear. It was shown that for a game G with value $\omega_c(G) = 1 - \epsilon$, where ϵ is the probability of failing by the provers, that the game G^n has value $\omega_c(G^n) \leq (1 - \epsilon^k)^{\Omega(n/s)}$, where s is the size of an answer (i.e: 1 for binary games) and k is an universal constant (i.e.: explicitly $k = 32$ in [Raz98]). This result was further improved and simplified in [Hol07] with a constant of $k = 3$. Tight results were shown with $k = 2$ for XOR games in [FKO07] and for other types of games, unique and projection games, in [Rao08]. It was also shown in [FV96] that the dependency on s for this bound is necessary.

The bound of $\omega_c(G^n) \leq (1 - \epsilon)^{\Omega(n/s)}$, with universal constant $k = 1$ was stated as a open problem in [FKO07] and conjectured in [MS07] with positive answer for special cases. This bound is usually referred as the Strong Parallel Repetition Problem.

A recent motivation for the study of parallel repetition is that a positive answer for the Strong Parallel Repetition Problem would imply the equivalence of the unique game conjecture [Kho02] with the hardness of approximation of the Max-Cut problem. The relation between the problems is explained in [Raz08]. The Strong Parallel Repetition Problem or any bounds with constant $k < 2$ would prove the unique game conjecture. But a counterexample of the Strong Parallel Repetition Problem was presented in [Raz08] and therefore that the unique game conjecture cannot be proven by improving the bounds on parallel repetitions alone.

The proof of the classical upper bound obtained in [Raz98] which is improved in [Hol07] is too extensive to include in this thesis. Rather, we will

present two two-prover one-round games G that satisfy $\omega_c(G^2) > \omega_c(G)^2$. The strict inequality shows that there are some games with parallel repetition for which there exist a better strategy than playing each game independently.

The first game presented is a game of partial-information and was proposed in [Fei91, For89]. The game is described by $G_F = (X, Y, A, B, R, \pi_{XY})$ where $X = Y = A = B = \{0, 1\}$ and π_{XY} is uniform over the pairs $(0, 0)$,$(0, 1)$ and $(1, 0)$. The winning condition R is

$$R(a, b|x, y) = \begin{cases} 1 & \text{if } x \vee a \neq y \vee b \\ 0 & \text{otherwise.} \end{cases}$$

Reminder that for any classical strategies, an optimal strategy is deterministic. For this game, the deterministic function $f(q)$ of the question q of each prover is either to copy the bit $f(q) = q$ of the questions or to do a bit flip $f(q) = \bar{q}$. Because this game is played by two provers, there is a total of four strategies to analyse. A simple case analysis for the game G_F reveals that its value is $\omega_c(G_F) = \frac{2}{3}$ when the provers answer with the question bit.

Next, we show what effects parallel repetition with two repetitions has on the classical value of this game of partial-information.

Theorem 6.1.1 ([Fei91])**.** *The classical value of the game G_F^2 with two parallel repetitions is*

$$\omega_c(G_F^2) > \omega_c(G_F)^2.$$

Proof. We show a strategy for G_F^2 that achieve this lower bound. In a game with two parallel repetitions, each prover receives a question pair and answer by an answer pair. The first element a pair corresponds to the first game and the other to the second game. Consider a strategy where each prover answers by the pair $(0, 0)$ if they receive the question pair $(0, 0)$ and answers $(1, 1)$ otherwise. A case analysis over all possible question pairs reveals that the probability of winning by the prover is $\frac{2}{3}$ for this strategy. Therefore,

$$\omega_c(G_F^2) \geq \frac{2}{3} = \omega_c(G_F) > \omega_c(G_F)^2.$$

which proves that this strategy is strictly better that playing each game independently with an optimal strategy on G_F. □

Note that the proof of theorem (6.1.1) uses a strategy that could not be optimal. Consequently, there could be strategies that achieve better results from the perspective of the provers. In fact, it is stated as a proposition in [Fei91] that this strategy is optimal: $\omega_c(G_F^2) = \frac{2}{3}$.

We have just shown an example of game of partial-information for which $\omega_c(G^2) > \omega_c(G)^2$. Can this result be extended for more general no-information games? We answer positively with the following example of no-information game again from [Fei91].

The game is described by $G_{F'} = (X, Y, A, B, R', \pi'_{XY})$ where $X = Y = A = B = \{0, 1\}$ and π'_{XY} is uniform over the pairs $(0, 0)$,$(0, 1)$,$(1, 0)$ and $(1, 1)$. The winning condition R' is

$$R'(a, b|x, y) = \begin{cases} 1 & \text{if } (x \wedge y) \vee (x \vee a \neq y \vee b), \\ 0 & \text{otherwise.} \end{cases}$$

The game $G_{F'}$ is a slight modification of the game G_F. The probability distribution is now uniform over the whole set $X \times Y$ and the winning condition $R' = 1$ if the question pair $(1, 1)$ is sent to the provers for any choice of answers by the provers. It is easy to see that the value of the game $G_{F'}$ is $\omega_c(G'_F) = \frac{3}{4}$. An optimal strategy is simply the same as G_F. When the provers are asked questions $(1, 1)$ they win disregarding the answers they give.

We show what effect parallel repetition with two repetitions has on the classical value of this no-information game.

Theorem 6.1.2 ([Fei91])**.** *The classical value of the above two-prover one-round no-information game G_F with two parallel repetitions is*

$$\omega_c(G^2_{F'}) > \omega_c(G_{F'})^2.$$

Proof. Consider the following strategy for $G^2_{F'}$. Upon receiving questions $(0, 0)$, prover P_1 answers $(0, 1)$ and player P_2 answer $(1, 0)$, otherwise they both respond by $(0, 0)$. A case analysis reveals for this strategy reveals that the prover will win with probability $= \frac{10}{16}$. Since the value of $\omega_c(G_{F'}) = \frac{3}{4}$, we have that

$$\omega_c(G^2_{F'}) \geq \frac{10}{16} > \omega_c(G_{F'})^2 = \frac{9}{16}.$$

which proves the theorem. □

Theorem (6.1.2) shows that even for no-information games it is possible for the provers to win more often by playing by a different strategy than the optimal strategy of a single instance of the game. This proves that the conclusion we have obtained from the previous game are not caused by the nature of the probability distribution. In [Fei91], it is stated as a proposition that $\omega_c(G^2_{F'}) = \omega_c(G'_F)^2$.

From what we have observed from the above theorems, the following corollary is easily deduced:

Corollary 6.1.1. *For the two-prover one-round game G_F (and similarly for $G_{F'}$), $\omega_c(G_F^2) > \omega_c(G_F)^2$ implies that $\omega_c(G_F^n) > \omega_c(G_F)^n$ for any number n of parallel repetition.*

What we learn from this corollary is that the verifier has therefore no interest in doing parallel repetition for these two games since it could help the provers to have a better strategy.

To conclude this section and to establish a link with complexity theory, note that parallel repetition of a game has an effect on the soundness of some repeated game with classical strategies. There exists an upper bound in [Hol07] for unrestricted game as a function of the question size, the number of repetition and a universal constant. For XOR games, it is shown in [FKO07] that the universal constant can be made smaller and the upper bound is more restrictive.

6.2 Parallel Repetition of Non-Classical Games

This section deals with parallel repetition when quantum and no-signalling strategies are allowed. It is essential to know if the same bounds can be achieved with these strategy classes. For general games, this is yet unknown.

In the settings of XOR games with quantum strategies, a proof in [CSUU07] shows that the Strong Parallel Repetition Theorem holds with two provers. In [Hol07], an upper bound is indicated for the no-signalling value of any two-prover games with parallel repetitions. Trivially, this bound is less restrictive than the classical case as it does not depend on the size of the question which was mandatory in the classical case. This latter upper bound is good for any kind of game as opposed to the Strong Parallel Repetition Theorem for XOR games. We leave the derivation of this upper bound to another discussion and we present instead the derivation of the Strong Parallel Repetition Theorem for XOR games.

The proof of the Strong Parallel Repetition for XOR games relies on the sum of XOR games. For any two XOR games $G = (X, Y, A, B, R, \pi_{XY})$ and $G' = (X', Y', A', B', R', \pi'_{X'Y'})$, define the sum (mod 2) as the XOR game

$$G'' = G \oplus G' = (X \times X', Y \times Y', A'', B'', R \oplus R', \pi_{XY} \times \pi'_{XY})$$

For this game, the verifier sample $(x, y), (x', y') \in (X \times Y) \times (X' \times Y')$ from the distribution $\pi_{XY} \times \pi_{X'Y'}$. He then sends (x, x') to prover P_1 and (y, y') to prover P_2. Prover $P1$ answers with $a'' \in A''$ and prover $P2$ with $b'' \in B''$ which are a binary functions of the answers $a, a' \in A \times A'$ and

$b, b' \in B \times B'$ respectively. More precisely, it must satisfies $a'' \oplus b'' = f(a, b|x, y) \oplus f'(a', b'|x', y')$ where the function f and f' are defined from the winning condition of the XOR games such that $a \oplus b = f(x, y)$ and $a' \oplus b' = f'(x', y')$. A natural question is whether the outputs $a'' = a \oplus a'$ and $b'' = b \oplus b'$ make an optimal strategy. The probability of winning for the provers with this strategy $S_\oplus$ is

$$\tilde{\omega}(S_\oplus) = \omega(G)\omega(G') + (1 - \omega(G))(1 - \omega(G')) \tag{6.2}$$

The first term in the addition represents the probability of winning both games for the provers and the second term is the probability of failing both games for the provers.

It turns out that $S_\oplus$ is not optimal for classical strategies. The authors in [CSUU07] give the example of the CHSH game as a counterexample. This game is defined by $G_{CHSH} = (X, Y, A, B, R, \pi_{XY})$ where $X = Y = A = B = \{1, 2\}$ and the winning condition is

$$R(a, b|x, y) = \begin{cases} 1 & \text{if } a \oplus b = x \wedge y \\ 0 & \text{otherwise} \end{cases}$$

It is proven in [CHTW04] that the classical value is $\omega_c(G_{CHSH}) = \frac{3}{4}$. According to (6.2), the winning probability of strategy $S_\oplus$ for this game with two parallel repetitions would be $\frac{10}{16}$. However, it can be shown that if the provers answer with $a'' = a \wedge a'$ and $b'' = b \wedge b'$, the winning probability of this strategy is $\frac{3}{4} > \frac{10}{16}$.

Before continuing with the main proof of this section, we define a useful quantity: the quantum bias of a XOR game.

Definition 6.2.1 (Quantum Bias [CSUU07])**.** The quantum bias $\varepsilon_q(G)$ of a XOR game G is a quantity defined by

$$\varepsilon_q(G) = 2\omega_q(G) - 1.$$

For a XOR game G, we denote the XOR game G^T, the transpose of G, to be the game where prover P_1 and P_2 exchange roles. Moreover, for $0 \leq \lambda \leq 1$, we define the convex combination of two XOR games G and G' by $\lambda G + (1 - \lambda)G'$. The convex combination of two games is a game in which with probability λ the game G is played and with probability $(1 - \lambda)$ the game G' is played.

We now state some properties of the bias of a game with the following proposition.

Proposition 6.2.1 ([CSUU07]). *Consider any XOR game G,G' and G''. The quantum bias satisfies*

1. $\varepsilon_q(G \oplus G') = \varepsilon_q(G' \oplus G)$,
2. $\varepsilon_q(G) = \varepsilon_q(G^T)$,
3. *For all* $0 \leq \lambda \leq 1$, $\varepsilon_q(\lambda G \oplus (1-\lambda)G') = \lambda\varepsilon_q(G) + (1-\lambda)\varepsilon_q(G')$,
4. *For all* $0 \leq \lambda \leq 1$, $G \oplus (\lambda G' + (1-\lambda)G'') = \lambda(G \oplus G') + (1-\lambda)(G \oplus G'')$.

Before showing that the strategy $S_\oplus$ for XOR games is optimal with quantum strategies, we state a lemma from [CSUU07].

Lemma 6.2.1 ([CSUU07]). *If G and G' are two XOR games, then*

$$\varepsilon_q\left(\left(\frac{1}{2}G + \frac{1}{2}G^T\right) \oplus \left(\frac{1}{2}G' + \frac{1}{2}G'^T\right)\right) \leq \varepsilon_q(G)\varepsilon_q(G').$$

The proof of this lemma is made in [CSUU07] using semidefinite programming and will not be presented here. We now proceed to the proof that $S_\oplus$ is optimal with quantum strategies for XOR games.

Theorem 6.2.1 ([CSUU07]). *For any XOR games $G = (X, Y, A, B, R, \pi_{XY})$ and $G' = (X', Y', A', B', R', \pi'_{X'Y'})$, the optimal quantum strategy for $G \oplus G'$ is a strategy family $S_\oplus$ where each prover plays G and G' independently as follows. They play G and G', each with an optimal strategy. They calculate $a, b \in A \times B$ and $a', b' \in A' \times B'$ respectively and output $a'' = a \oplus a'$ and $b'' = b \oplus b'$ respectively to the game $G \oplus G'$.*

Proof. By definition (6.2.1) of the bias, the proof reduces to showing that $\varepsilon_q(G \oplus G') = \varepsilon_q(G)\varepsilon_q(G')$.

Trivially, we have that $\varepsilon_q(G \oplus G') \geq \varepsilon_q(G)\varepsilon_q(G')$ since the provers can play each game with their optimal strategy and take the parity of the bit as their answer. The rest of the proof deals with the reverse inequality.

As indicated in chapter 4, the quantum strategy for the provers consists in sharing a state $|\psi\rangle$ and to apply a set of observable M_x and N_y. Using the vector characterization from theorem (4.5.1), we can write the equation for the quantum bias for the XOR game G as

$$\varepsilon_q(G) = \sum_{x,y} \pi_{XY}(-1)^{f(x,y)} \langle\psi| M_x \otimes N_y |\psi\rangle \tag{6.3}$$

$$= \sup_{\{u_x\},\{v_y\}} \sum_{x,y} \pi_{XY}(-1)^{f(x,y)} u_x \cdot v_y, \tag{6.4}$$

for unit vector $\{u_x\}_{x\in X}$ and $\{v_y\}_{y\in Y}$ where $f(x,y)$ is defined in the winning condition R as $a \oplus b = f(x,y)$. Therefore, it is possible to find an optimal solution to (6.3) like we do for the value of a game.

Using proposition (6.2.1) and lemma (6.2.1), we have

$$\begin{aligned}
\varepsilon_q(G \oplus G') &\geq \varepsilon_q(G)\varepsilon(G') \\
&\geq \varepsilon_q\left(\left(\frac{1}{2}G + \frac{1}{2}G^T\right) \oplus \left(\frac{1}{2}G' + \frac{1}{2}G'^T\right)\right) \\
&= \varepsilon_q\left(\frac{1}{4}(G \oplus G') + \frac{1}{4}(G \oplus G'^T) + \frac{1}{4}(G^T \oplus G') + \frac{1}{4}(G^T \oplus G'^T)\right) \\
&= \varepsilon_q\Bigg(\frac{1}{2}\left[\frac{1}{2}(G \oplus G') + \frac{1}{2}(G \oplus G'^T)\right] \\
&\qquad + \frac{1}{2}\left[\frac{1}{2}(G \oplus G') + \frac{1}{2}(G \oplus G'^T)\right]^T\Bigg) \\
&= \frac{1}{2}\varepsilon_q(G \oplus G') + \frac{1}{2}\varepsilon_q(G \oplus G'^T).
\end{aligned}$$

From the last results, we have that $\varepsilon_q(G \oplus G') \geq \varepsilon_q(G \oplus G'^T)$ and by proposition (6.2.1), $\varepsilon_q(G \oplus G'^T) \geq \varepsilon_q(G \oplus G')$. Therefore $\varepsilon_q(G \oplus G') = \varepsilon_q(G \oplus G'^T)$ and all inequalities above can be replaced by equalities. In particular, the first two lines state that $\varepsilon_q(G \oplus G') = \varepsilon_q(G)\varepsilon(G')$ which proves the theorem. □

We now have proved that for the optimal strategy for the sum $G \oplus G'$ of games G and G' with quantum strategies is to play each game independently with their optimal strategy. This results is necessary to prove the Strong Parallel Repetition Theorem for XOR games with quantum strategies. We now give the proof of two more lemmas before giving the main proof of this section.

Lemma 6.2.2 ([CSUU07])**.** *For any sequence of binary random variables* $X_1, X_2, ..., X_n$*,*

$$\frac{1}{2^n}\sum_{M\subseteq[n]} E\left[(-1)^{\oplus_{j\in M}X_j}\right] = Pr[X_1...X_n = 0...0].$$

Proof.

$$\frac{1}{2^n}\sum_{M\subseteq[n]} E\left[(-1)^{\oplus_{j\in M}X_j}\right] = E\left[\frac{1}{2^n}\sum_{M\subseteq[n]}(-1)^{\oplus_{j\in M}X_j}\right]$$

$$= E\left[\prod_{j=1}^{n}\left(\frac{1+(-1)_j^X}{2}\right)\right].$$

Because the quantity $\prod_{j=1}^{n}\left(1+(-1)^{X_j}\right)$ is non-zero only when $X_1...X_n = 0...0$, we have

$$E\left[\prod_{j=1}^{n}\left(\frac{1+(-1)^{X_j}}{2}\right)\right] = Pr[X_1...X_n = 0...0] \tag{6.5}$$

□

We introduce a new terminology for the bias of a strategy S and a game G. First, we describe the terminology for the winning probability $\tilde{\omega}(S)$ of a strategy S for a game G by $\tilde{\omega}(S,G)$.We indicate the bias of strategy S on a game G from definition (6.2.1) of the bias by

$$\tilde{\varepsilon}(S,G) = 2\tilde{\omega}_q(S,G) - 1. \tag{6.6}$$

In particular, for an optimal strategy S_{opt} for game G, we obtain the definition of the bias $\tilde{\varepsilon}(S_{opt},G) = \varepsilon(G)$.

Lemma 6.2.3 ([CSUU07])**.** *For any XOR game G_i, we have*

$$\frac{1}{2^n}\sum_{M\subseteq[n]}\tilde{\varepsilon}(S_M, \oplus_{j\in M}G_j) = \tilde{\omega}(S, \wedge_{j=1}^{n}G_j).$$

where n is the number of repetitions and S_M is the strategy that the provers answer by the sum of the answer of each game independently using strategy S.

Proof. For all $j \in [n]$, we use the function of the provers $a_j \oplus b_j = f_j(x_j, y_j)$ from winning condition R_j of a game $G_j = (A_j, B_j, X_j, Y_j, R_j, \pi_{X_jY_j})$ and define the binary random variables $X_j = a_j \oplus b_j \oplus f_j(x_j, y_j)$. When $X_j = 0$ the game G_j is won by the provers.

We have that

$$E[(-1)^{\oplus_{j\in M}X_j}] = \tilde{\varepsilon}(S_M, \oplus_{j\in M}G_j),$$

and that

$$Pr[X_1...X_n = 0...0] = \tilde{\omega}(S, \wedge_{j=1}^{n}G_j)$$

and from lemma (6.2.2), the two equations are equal. □

From lemma (6.2.3), we deduce the following corollary

Corollary 6.2.1 ([CSUU07])**.**

$$\omega_q(\wedge_{j=1}^n G_j) \leq \frac{1}{2^n} \sum_{M\subseteq[n]} \varepsilon_q(\oplus_{j\in M} G_j)$$

We are now in possession of all the necessary tools to proceed with the proof of the Strong Parallel Repetition Theorem for XOR games.

Theorem 6.2.2 (Strong Parallel Repetition Theorem for XOR games [CSUU07])**.** *For any XOR games $G_1, ..., G_n$, we have that the value $\omega_q(\wedge_{j=1}^n G_j)$ of all the games in parallel is*

$$\omega_q(\wedge_{j=1}^n G_j) = \prod_{j=1}^n \omega_q(G_j).$$

Proof. We know from equation (6.1) that the value $\omega_q(\wedge_{j=1}^n G_j)$ of any games $G_1, ..., G_n$ in parallel is lower bounded by

$$\omega_q(\wedge_{j=1}^n G_j) \geq \prod_{j=1}^n \omega_q(G_j).$$

This means that the value of the games in parallel cannot be lower than playing each game independently with their appropriate optimal strategy. The rest of the proof deals with the upper bound. We have that

$$\begin{aligned}
\omega_q(\wedge_{j=1}^n G_j) &\leq \frac{1}{2^n} \sum_{M\subseteq[n]} \varepsilon_q(\oplus_{j\in M} G_j) && \text{(by corollary (6.2.1))} \\
&= \frac{1}{2^n} \sum_{M\subseteq[n]} \prod_{j\in M} \varepsilon_q(G_j) && \text{(by theorem (6.2.1))} \\
&= \prod_{j=1}^n \left(\frac{1+\varepsilon_q(G_j)}{2}\right) \\
&= \prod_{j=1}^n \omega_q(G_j) && \text{(by the bias definition)}
\end{aligned}$$

Since we have $\prod_{j=1}^n \omega_q(G_j) \leq \omega_q(\wedge_{j=1}^n G_j) \leq \prod_{j=1}^n \omega_q(G_j)$, it follows that $\omega_q(\wedge_{j=1}^n G_j) = \prod_{j=1}^n \omega_q(G_j)$. □

The consequence of the above proof is that for XOR games the verifier has no advantages of doing parallel repetition when the provers use quantum strategies. By simplicity, he would then do no parallel repetition of the game.

For other games than XOR games, unique games or projections games, there are no known results for parallel repetition in the quantum settings beside the upper bound in [Hol07] for no-signalling strategies. In those cases, it could be possible that the provers can win more often using the quantum or no-signalling strategies.

6.3 Parallel Repetition of Odd Cycle Games

The upper bound in [Hol07] for the value of games with parallel repetition with classical and no-signalling strategies can be applied to the Odd Cycle Game. Moreover, since the Odd Cycle Game is a XOR game, the Strong Parallel Theorem of [CSUU07] for quantum strategies is also valid. However, those results are not specific to the Odd Cycle Game.

A classical result in [Raz08] puts a lower bound on the value of the two-prover Odd Cycle Game G_{OC}^n with n repetitions and with classical strategies

$$\omega_c(G_{OC}^n) \geq 1 - \frac{1}{m}O(\sqrt{n}).$$

This results is particularly important since it is a proof that the bound for the Strong Parallel Theorem for XOR games cannot be achieved classically.

Another important result appeared in [FKO07] and puts an upper bound on the classical value of the Odd Cycle Game with n repetitions as follows

$$\omega_c(G_{OC}^n) \leq 1 - \frac{1}{m}O(\sqrt{\frac{n}{log(n)}}).$$

An improved result for this bound would require improvements on the Foam Problem in physics discussed in [FKO07]. Finally, for n repetitions, the perfect repetition theorem does not work for classical strategies for this game with cycles of length m [FKO07]. That is

$$\omega_c(G_{OC}^n) > (1 - \frac{1}{2m})^n.$$

for some $n \leq m^2 log(m)$. However, the proof is not included in the preliminary version of the paper.

We now proceed with the proof in [Raz08] that the Odd Cycle Game of length $\omega_c(G_{OC}^n)$ with classical strategies and n parallel repetitions is lower bounded by $\omega_c(G_{OC}^n) \geq 1 - \frac{1}{m}O(\sqrt{n})$.

Theorem 6.3.1 ([Raz08]). *The value of the Odd Cycle Game G_{OC} of length m with classical strategies and n parallel repetitions is*

$$\omega_c(G_{OC}^n) \geq 1 - \frac{1}{m}O(\sqrt{n}).$$

For the upcoming proof, we introduce a special notation. For integers $i \leq j$, we write $[i, j]$ for the set of integer $\{i, i+1, ..., j\}$. Let $m = 2k+1$ be an odd integer and define the set $I = [-k, k]$ of size m. Let the arithmetics on those sets will be taken modulo m.

Before going on with the proof itself, the authors prove the following technical lemma:

Lemma 6.3.1 ([Raz08]). *There exists a probability distribution $f : I \to \mathbb{R}$, such that:*

1. *For every $i \in I, f(i) > 0$,*
2. *$f(k), f(-k) \leq O\left(\frac{1}{m^3}\right)$,*
3. *$\sum_{i \in I} \frac{f(i)^2}{f(i+1)} + \frac{f(i)^2}{f(i-1)} \leq 2 + O\left(\frac{1}{m^2}\right)$.*

Proof. Let the probability distribution be defined by

$$f(i) = \gamma \cdot (k + 1 - |i|)^2,$$

where $\gamma = \Theta\left(\frac{1}{m^3}\right)$.

The first and second requirements hold by the definition of the normalization factor γ. We now prove the third requirement:

For any $j \geq 2$, we have that

$$\frac{j^2}{(j+1)^2} + \frac{j^2}{(j-1)^2} \leq 2 + O\left(\frac{1}{j^2}\right).$$

By defining $j = k + 1 - |i|$ we have three cases that have to be dealt separately:

1. For $i \in I \backslash \{-k, 0, k\}$,

$$\begin{aligned} \frac{f(i)^2}{f(i+1)} + \frac{f(i)^2}{f(i-1)} &= f(i) \cdot \left(\frac{f(i)}{f(i+1)} + \frac{f(i)}{f(i-1)}\right) \\ &= 2f(i) + O(\gamma) \end{aligned}$$

2. For $i = 0$,

$$\begin{aligned}\frac{f(0)^2}{f(1)} + \frac{f(0)^2}{f(-1)} &= 2f(0) \cdot \frac{(k+1)^2}{k^2} \\ &= 2f(0) \cdot \left(1 + O\left(\frac{1}{k}\right)\right) \\ &= 2f(0) + O\left(\frac{1}{m^2}\right)\end{aligned}$$

3. For $i \in \{-k, k\}$,

$$\begin{aligned}\frac{f(i)^2}{f(i+1)} + \frac{f(i)^2}{f(i-1)} &= f(i) \cdot O(1) \\ &= O(\gamma)\end{aligned}$$

Therefore, the third requirement is verified over all the domain of the function f. □

Let $m = 2k + 1$ be an odd integer and define the Odd Cycle Game as usual by $G_{OC} = (X, Y, A, B, R, \pi_{XY})$. Define the question sets X and Y by $U = [-k, k]$ of size m to an ordering of the nodes of the cycle. Denote $E = \{\{i, i+1\} : i \in X\}$ to be the set of edges in the cycle. Each edge in the cycle is named by the node opposite to it (e.g.: the edge $\{i, i+1\}$ is named by $i + \frac{(m+1)}{2}$).

Let $x = (x_1, x_2, ..., x_n) \in X^n$ be the questions to prover P_1 and $y = (y_1, y_2, ..., y_n) \in Y^n$ be the questions to prover P_2 where each pair (x_i, y_i) is chosen from the distribution π_{XY}.

Consider the probability distribution given by lemma (6.3.1). For every node $u \in U$, define a probability distribution $P_u : E \to \mathbb{R}$ over the edges $e \in E$ by

$$P_u(e) = f(e - u)$$

where each e and u is from the set $[-k, k]$ and the arithmetic is taken modulo m. In a similar manner, for each $u = (u_1, ..., u_n) \in U^n$, define a probability distribution $P_u : E^n \to \mathbb{R}$ over the n edges $(e_1, ...e_n) \in E^n$ by

$$P_u(e_1, ..., e_n) = \prod_{i=1}^{n} P_{u_i}(e_i) = \prod_{i=1}^{n} f(e_i - u_i).$$

Returning to the Odd Cycle Game, we have two distributions P_x and P_y given by the above. We define the l_1 distance between two vectors $u =$

$u_1, ..., u_n$ and $v = v_1, ..., v_n$ is defined by

$$||u - v||_1 = \sum_i |u_i - v_i|.$$

The next lemma bounds the l_1 distance of those two distributions.

Lemma 6.3.2 ([Raz08]). $E_{x,y}||P_x - P_y||_1 \leq \frac{1}{m} \cdot O\left(\sqrt{n}\right)$

Proof. First of all, consider only the case where $n < \alpha m^2$ for some constant $\alpha > 0$ since otherwise the theorem holds trivially (i.e: $\frac{1}{m} \cdot \sqrt{n} \geq \Omega(1)$). Moreover, by symmetry, $E_y||P_x - P_y||_1$ is the same for every x. Thus, we can fix a particular $x = \bar{0} = (0, ..., 0)$ without loss of generality. It is thus enough to bound $E_z||P_{\bar{0}} - P_z||_1$ for $z = (z_1, ...z_n) \in [-1, 1]^n$ where each z_i is chosen independently from the distribution π_z such that $\pi_z(0) = \frac{1}{2}$, $\pi_z(1) = \frac{1}{4}$ and $\pi_z(-1) = \frac{1}{4}$. We therefore have

$$\begin{aligned}
E_{x,y}||P_x - P_y||_1 &= (E_z||P_{\bar{0}} - P_z||_1)^2 \\
&= \left(E_z \sum_{e \in E^n} |P_{\bar{0}}(e) - P_z(e)|\right)^2 \\
&\qquad \text{(by definition of the } l_1 \text{ distance)} \\
&= \left(E_z \sum_{e \in E^n} P_z(e) \left|\frac{P_{\bar{0}}(e)}{P_z(e)} - 1\right|\right)^2 \\
&\leq E_z \sum_{e \in E^n} P_z(e) \left(\frac{P_{\bar{0}}(e)}{P_z(e)} - 1\right)^2 \quad \text{(by Jensen's inequality)} \\
&= E_z \sum_{e \in E^n} \left(P_z(e) - 2P_{\bar{0}}(e) + \frac{P_{\bar{0}}(e)^2}{P_z(e)}\right) \\
&= 1 - 2 + E_z \sum_{e \in E^n} \frac{P_{\bar{0}}(e)^2}{P_z(e)} \\
&\qquad \text{(because } P_{\bar{0}} \text{ and } P_z \text{ are probability distributions)} \\
&= -1 + E_{z_1,...,z_n} \sum_{e_1,...,e_n} \prod_{i=1}^{n} \frac{f(e_i)^2}{f(e_i - z_i)} \\
&= -1 + \prod_{i=1}^{n} \left(E_{z_i} \sum_{e_i} \frac{f(e_i)^2}{f(e_i - z_i)}\right) \\
&= -1 + \prod_{i=1}^{n} \left(\sum_{e_i} \frac{1}{2} \frac{f(e_i)^2}{f(e_i)} + \frac{1}{4} \frac{f(e_i)^2}{f(e_i + 1)} + \frac{1}{4} \frac{f(e_i)^2}{f(e_i - 1)}\right)
\end{aligned}$$

$$= -1 + \prod_{i=1}^{n} \left(1 + O\left(\frac{1}{m^2}\right)\right)$$

(because f is a probability distribution and by lemma (6.3.1))

$$= O\left(\frac{1}{m^2}\right) \cdot O(n)$$

$$= \frac{1}{m^2} \cdot O(n)$$

□

The proof of theorem (6.3.1) follows from the above lemmas and another lemma in [Hol07]. We present the last necessary lemma restated in [Raz08].

Lemma 6.3.3 ([Raz08])**.** *Let W be a finite set. Assume that prover P_1 knows a distribution $P_A : W \to \mathbb{R}$ and prover P_2 knows a distribution $P_B : W \to \mathbb{R}$, such that*

$$||P_A - P_B||_1 \leq \delta.$$

Then, using a shared random string, prover P_1 can choose $w_A \in W$ distributed according to P_A, and prover P_2 can choose $w_B \in W$ distributed according to P_B, such that

$$w_A = w_B,$$

with probability at least $1 - O(\delta)$.

The proof of this lemma will not be presented in this paper but the reader is encouraged to consult [Hol07] for the proof. We give the proof of theorem (6.3.1) based on the results shown. Theorem (6.3.1) stated that the value of the Odd Cycle Game G_{OC} of length m with classical strategies and n parallel repetitions is

$$\omega_c(G_{OC}^n) \geq 1 - \frac{1}{m} O(\sqrt{n}).$$

Proof. We show a probabilistic protocol that achieves the desired lower bound on the value of the Odd Cycle Game with classical strategies. Since a probabilistic protocol is a convex combination of deterministic protocol, there exist a deterministic protocol that achieves the same value.

Upon receiving questions x and y from the verifier, prover P_1 gets probability distribution P_x and similarly prover P_2 gets probability distribution P_y. By lemma (6.3.2) and (6.3.3), P_1 can choose $e = (e_1, ..., e_n) \in E^n$ from P_x and P_2 can choose $e' = (e'_1, ..., e'_n) \in E^n$ from P_y such that $e = e'$ with probability at least $1 - \frac{1}{m} O(\sqrt{n})$.

Now, the prover uses this shared sequence of edges e to win the game as follows. From lemma (6.3.1), the probability that the edge e_i touches the node x_i is at most $O\left(\frac{1}{m}\right)$ which is negligible. They have joint sequence of edges such that it does not touch the node in the question. Thus if the each prover colours the cycle with 0 for the two nodes touching edge e and the rest of the nodes with 1 and 0 alternatively, they will have a share cycle that will be 2-coloured correctly except at edge e. But we have said that the probability that the edge e touches x is negligible. Therefore, if the prover use this probabilistic classical strategy, they will achieve a value of $\omega_c(G^n_{OC}) \geq 1 - \frac{1}{m}O(\sqrt{k})$ □

For $n \geq \Omega(m^2)$, it is explained in [Raz08] that the value of the repeated Odd Cycle Game is $\omega_c(G^n_{OC}) = (1-(\frac{1}{2m})^2)^{O(n)}$ which give a negative answer for the Strong Parallel Theorem Problem in the case of XOR games (as well as unique and projection games).

Chapter 7

Conclusion

In this thesis, we presented the effects of adding more provers to a multi-prover one-round game. We analysed the differences when the strategy of the provers is classical, quantum and no-signalling.

We have shown that with classical strategies, the value of the game is not changed with the addition of more that two provers. We have seen that in a situation where the number of provers is $k = m+1$ for m possible questions to the second prover, the value of the game is the same for classical, quantum and no-signalling strategies. In particular, we have shown that in the case of the Odd Cycle Game only three provers instead of $k = m + 1$ are necessary to reduce the value of the no-signalling and quantum games to a classical one.

With parallel repetition, we also noticed differences between strategy classes. In the classical setting, we noticed that there exist games with parallel repetition for which there is a better strategy than playing each instance of the game with an optimal strategy. Classically, this was shown for partial-information games and no-information games. With quantum strategies, we have shown that in the case of XOR games, the best strategy for a game with parallel repetition is to play each instance with an optimal strategy. This is clear demonstration of the difference between classical and quantum strategies for game with parallel repetition. Finally, we have presented a lower bound on the value of the Odd Cycle game with parallel repetition, which is a counterexample to strong parallel repetition with classical strategies.

The contribution of this thesis was to gather recent results on these topics and organize them in an unified manner. Results were selected to

emphasize the effect of the choice of the strategy class on the value of games. This could help to understand the power of the multi-prover interactive proof system with quantum and no signalling theories.

7.1 Future Work

When adding more provers to a two-prover game with no-signalling strategies, it would be interesting to know if there are relations between the number of possible questions to the second prover and the number of provers other than the one presented. For example, if $k \neq m+1$, the effect of adding more prover with quantum strategies is currently unknown for unrestricted games. Another interesting question is what is the effect on the value of a multi-prover one-round game with quantum strategies when the provers are allowed to receive different questions. Understanding the power of the multi-prover interactive proof system with quantum strategies is essential to give a correct security proof of many protocols.

The classical and no-signalling upper bounds for generalized games with parallel repetition might be reduced. For games other that XOR games, it is an important question to know what effects has parallel repetition. For example, whether of not, the best strategy is to play each instance with the optimal strategy of the game or if there is a better strategy. For the Odd Cycle Game, it would be interesting to have a strong bound on the value with parallel repetition for a certain number of repetition.

Finally, more differences between classical and quantum strategies could emerge from the addition of more players to a two-prover one-round game combined with parallel repetition. This is a very interesting question.

Bibliography

[AB] S. Arora and B. Barak. Computational complexity: A modern approach. Preliminary Draft, 2006. [cited at p. 19, 20]

[AGM06] A. Acin, N. Gisin, and L. Masanes. From Bell's theorem to secure quantum key distribution. *Physical Review Letters*, 97:120405, 2006. [cited at p. 54]

[Alo91] N. Alon. Probabilistic methods in extremal finite set theory. In *Mikls Eds.), Bolyai Society Mathematical Studies,3, Visegrd*, pages 39–57, 1991. [cited at p. 57]

[BC90] S. Braunstein and C. Caves. Wringing out better Bell inequalities. *Annals of Physics*, 202:22 – 56, 1990. [cited at p. 38]

[BCMS98] G. Brassard, C. Crepeau, D. Mayers, and L. Salvail. Defeating classical bit commitments with a quantum computer, 1998. [cited at p. 23]

[Bel64] J. S. Bell. On the einstein podolsky rosen paradox. *Physics*, 1(3):195 – 200, 1964. [cited at p. 1, 14]

[BFL90] L. Babai, L. Fortnow, and C. Lund. Nondeterministic exponential time has two-prover interactive protocols. In *SFCS '90: Proceedings of the 31st Annual Symposium on Foundations of Computer Science*, pages 16–25 vol.1, Washington, DC, USA, 1990. IEEE Computer Society. [cited at p. 21, 46]

[BGS98] M. Bellare, O. Goldreich, and M. Sudan. Free bits, pcps, and nonapproximability—towards tight results. *SIAM J. Comput.*, 27(3):804–915, 1998. [cited at p. 24, 50]

[BHK05] J. Barrett, L. Hardy, and A. Kent. No signalling and quantum key distribution. *Physical Review Letters*, 95:010503, 2005. [cited at p. 54]

[BOGKW88] M. Ben-Or, S. Goldwasser, J. Kilian, and A. Wigderson. Multi-prover interactive proofs: how to remove intractability assumptions. In *STOC '88: Proceedings of the twentieth annual ACM symposium on Theory of computing*, pages 113–131, New York, NY, USA, 1988. ACM. [cited at p. 20, 21, 23]

[Bra] G. Brassard. Quantum information processing for computer scientists. Preliminary and Fragmentary Draft, 2006. [cited at p. 6, 13, 14]

[BV04] S. Boyd and L. Vandenberghe. *Convex Optimization*. Cambridge University Press, March 2004. [cited at p. 85, 86, 87, 88, 89, 90]

[CCL90] J. Cai, A. Condon, and R. J. Lipton. On bounded round multi-prover interactive proof systems. *In Fifth Annual conference on Structure in Complexity Theory*, pages 45 – 54, 1990. [cited at p. 21, 57]

[CGJ07] R. Cleve, D. Gavinsky, and R. Jain. Entanglement-resistant two-prover interactive proof systems and non-adaptive private information retrieval systems, 2007. [cited at p. 24]

[CHTW04] R. Cleve, P. Hoyer, B. Toner, and J. Watrous. Consequences and limits of nonlocal strategies. In *CCC '04: Proceedings of the 19th IEEE Annual Conference on Computational Complexity*, pages 236–249, Washington, DC, USA, 2004. IEEE Computer Society. http://arxiv.org/abs/quant-ph/0404076. [cited at p. 22, 24, 27, 33, 35, 36, 38, 39, 40, 41, 48, 61]

[CSUU07] R. Cleve, W. Slofstra, F. Unger, and S. Upadhyay. Perfect parallel repetition theorem for quantum xor proof systems. In *CCC '07: Proceedings of the Twenty-Second Annual IEEE Conference on Computational Complexity*, pages 109–114, Washington, DC, USA, 2007. IEEE Computer Society. [cited at p. 60, 61, 62, 63, 64, 65, 66]

[EPR35] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Physical Review*, 47:777 – 780, 1935. [cited at p. 13]

[Fei91] U. Feige. On the success probability of two provers in one-round proof systems. In *Proc. 6th IEEE Structure in Complexity Theory*, pages 116–123, 1991. [cited at p. 21, 57, 58, 59]

[FKO07] U. Feige, G. Kindler, and R. O'Donnell. Understanding parallel repetition requires understanding foams. In *CCC '07: Proceedings of the Twenty-Second Annual IEEE Conference on Computational Complexity*, pages 179–192, Washington, DC, USA, 2007. IEEE Computer Society. [cited at p. 57, 60, 66]

[FL92] U. Feige and L. Lovász. Two-prover one-round proof systems: their power and their problems (extended abstract). In *STOC '92: Proceedings of the twenty-fourth annual ACM symposium on Theory of computing*, pages 733–744, New York, NY, USA, 1992. ACM. [cited at p. 21]

[For89] L. Fortnow. *Complexity-Theoretic Aspects of Interactive Proof Systems.* PhD thesis, MIT/LCS/TR-447, 1989. [cited at p. 57, 58]

[FRS88] L. Fortnow, J. Rompel, and M. Sipser. On the power of multi-prover interactive protocols. In *Structures*, pages 156–161, 1988. [cited at p. 57]

[FRS90] L. Fortnow, J. Rompel, and M. Sipser. Errata for on the power of multi-prover interactive protocols. In *Structures*, pages 318–319, 1990. [cited at p. 57]

[FV96] U. Feige and O. Verbitsky. Error reduction by parallel repetition - a negative result. In *CCC '96: Proceedings of the 11th Annual IEEE Conference on Computational Complexity*, page 70, Washington, DC, USA, 1996. IEEE Computer Society. [cited at p. 57]

[GMR85] S Goldwasser, S Micali, and C Rackoff. The knowledge complexity of interactive proof-systems. In *STOC '85: Proceedings of the seventeenth annual ACM symposium on Theory of computing*, pages 291–304, New York, NY, USA, 1985. ACM. [cited at p. 17]

[GMR89] S. Goldwasser, S. Micali, and C. Rackoff. The knowledge complexity of interactive proof systems. *SIAM J. Comput.*, 18(1):186–208, 1989. [cited at p. 2]

[GMW91] O. Goldreich, S. Micali, and A. Wigderson. Proofs that yield nothing but their validity or all languages in np have zero-knowledge proof systems. *J. ACM*, 38(3):690–728, 1991. [cited at p. 2]

[Gut05] G. Gutoski. Upper bounds for quantum interactive proofs with competing provers. In *CCC '05: Proceedings of the 20th Annual IEEE Conference on Computational Complexity*, pages 334–343, Washington, DC, USA, 2005. IEEE Computer Society. [cited at p. 2]

[GW04] G. Gutoski and J. Watrous. Quantum interactive proofs with competing provers. *CoRR*, abs/cs/0412102, 2004. [cited at p. 2]

[GW07] G. Gutoski and J. Watrous. Toward a general theory of quantum games. In *STOC '07: Proceedings of the thirty-ninth annual ACM symposium on Theory of computing*, pages 565–574, New York, NY, USA, 2007. ACM. [cited at p. 2]

[Hås01] J. Håstad. Some optimal inapproximability results. *J. ACM*, 48(4):798–859, 2001. [cited at p. 24, 50]

[Hol07] T. Holenstein. Parallel repetition: simplifications and the no-signaling case. In *STOC '07: Proceedings of the thirty-ninth annual ACM symposium on Theory of computing*, pages 411–419, New York, NY, USA, 2007. ACM. [cited at p. 57, 60, 66, 70]

[IKM08] T. Ito, H. Kobayashi, and K. Matsumoto. Oracularization and two-prover one-round interactive proofs against nonlocal strategies, 2008. [cited at p. 23]

[IKP+07] T. Ito, H. Kobayashi, D. Preda, X. Sun, and A. C. C. Yao. Generalized tsirelson inequalities, commuting-operator provers, and multi-prover interactive proof systems, 2007. [cited at p. 2, 23]

[JJUW09] R. Jain, Z. Ji, S. Upadhyay, and J. Watrous. Qip = pspace, 2009. [cited at p. 2]

[Kho02] S. Khot. On the power of unique 2-prover 1-round games. In *STOC '02: Proceedings of the thirty-fourth annual ACM symposium on Theory of computing*, pages 767–775, New York, NY, USA, 2002. ACM. [cited at p. 57]

[KKM+08] J. Kempe, H. Kobayashi, K. Matsumoto, B. Toner, and T. Vidick. Entangled games are hard to approximate. In *FOCS '08: Proceedings of the 2008 49th Annual IEEE Symposium on Foundations of Computer Science*, pages 447–456, Washington, DC, USA, 2008. IEEE Computer Society. [cited at p. 2, 23]

[KM90] D. Koller and N. Megiddo. The complexity of two-person zero-sum games in extensive form. *Games and Economic Behavior*, 4:528–552, 1990. [cited at p. 2]

[KM02] H. Kobayashi and K. Matsumoto. Quantum multi-prover interactive proof systems with limited prior entanglement. In *ISAAC '02: Proceedings of the 13th International Symposium on Algorithms*

and Computation, pages 115–127, London, UK, 2002. Springer-Verlag. [cited at p. 2]

[Kob07] H. Kobayashi. General properties of quantum zero-knowledge proofs, 2007. [cited at p. 2]

[KRT07] J. Kempe, O. Regev, and B. Toner. The unique games conjecture with entangled provers is false, 2007. [cited at p. 2]

[KW00] A. Kitaev and J. Watrous. Parallelization, amplification, and exponential time simulation of quantum interactive proof systems. In *STOC '00: Proceedings of the thirty-second annual ACM symposium on Theory of computing*, pages 608–617, New York, NY, USA, 2000. ACM. [cited at p. 2]

[LS91] D. Lapidot and A. Shamir. Fully parallelized multi prover protocols for nexp-time (extended abstract). In *SFCS '91: Proceedings of the 32nd annual symposium on Foundations of computer science*, pages 13–18, Washington, DC, USA, 1991. IEEE Computer Society. [cited at p. 21, 57]

[MAG06] L. Masanes, A. Acin, and N. Gisin. General properties of nonsignaling theories. *Physical Review A*, 73:012112, 2006. [cited at p. 49]

[May96] D. Mayers. Unconditionally secure quantum bit commitment is impossible, 1996. [cited at p. 23]

[MS07] O. Schwartz M. Safra. On parallel-repetition, unique-game and max-cut, 2007. [cited at p. 57]

[NC00] M. A. Nielsen and I. L. Chuang. *Quantum computation and quantum information*. Cambridge University Press, New York, NY, USA, 2000. [cited at p. 5]

[Pap85] C. H. Papadimitriou. Games against nature. *J. Comput. Syst. Sci.*, 31(2):288–301, 1985. [cited at p. 2]

[Pel90] D. Peleg. On the maximal number of ones in zero-one matrices with no forbidden rectangles, 1990. [cited at p. 57]

[Rao08] A. Rao. Parallel repetition in projection games and a concentration bound. In *STOC '08: Proceedings of the 40th annual ACM symposium on Theory of computing*, pages 1–10, New York, NY, USA, 2008. ACM. [cited at p. 57]

[Raz98] R. Raz. A parallel repetition theorem. *SIAM J. Comput.*, 27(3):763–803, 1998. [cited at p. 21, 57]

[Raz08] R. Raz. A counterexample to strong parallel repetition. In *FOCS '08: Proceedings of the 2008 49th Annual IEEE Symposium on Foundations of Computer Science*, pages 369–373, Washington, DC, USA, 2008. IEEE Computer Society. [cited at p. 57, 66, 67, 69, 70, 71]

[RN03] S. J. Russell and P. Norvig. *Artificial Intelligence: A Modern Approach*. Pearson Education, 2003. [cited at p. 27]

[Sav70] W.J. Savitch. Relationship between nondeterministic and deterministic tape classes. *Journal of Computer and System Sciences*, 4:177 – 192, 1970. [cited at p. 17]

[Sha92] A. Shamir. Ip = pspace. *J. ACM*, 39(4):869–877, 1992. [cited at p. 19, 46]

[Sip06] M. Sipser. *Introduction to the Theory of Computation*. Thomson Course Technology, 2nd edition, 2006. [cited at p. 15]

[TDS03] B. M. Terhal, A. C. Doherty, and D. Schwab. Local hidden variable theories for quantum states. *Physical Review Letters*, 90:157903, 2003. [cited at p. 49]

[Ton09] B. Toner. Monogamy of nonlocal quantum correlations. *PROC.R.SOC.A*, 465:59, 2009. [cited at p. 42, 45, 47, 48, 49, 51, 52]

[Tsi87] B. S. Tsirelson. Quantum analogues of the Bell inequalities: The case of two spatially separated domains. *Journal of Soviet Mathematics*, 36:557 – 570, 1987. [cited at p. 33]

[Vai01] L. Vaidman. Tests of Bell inequalities. 2001. [cited at p. 38]

[Ver94] O. Verbitsky. Toward the parallel repetition conjecture. In *Structures*, 1994. [cited at p. 57]

[Wat] J. Watrous. Quantum computational complexity. Manuscript, 2008. http://arxiv.org/abs/0804.3401. [cited at p. 15, 16]

[Wat02] J. Watrous. Limits on the power of quantum statistical zero-knowledge. In *In Proceedings of the 43rd Annual Symposium on Foundations of Computer Science*, pages 459–468. IEEE Computer Society, 2002. [cited at p. 2]

[Wat03] J. Watrous. Pspace has constant-round quantum interactive proof systems. *Theor. Comput. Sci.*, 292(3):575–588, 2003. [cited at p. 2]

[Wat06] J. Watrous. Zero-knowledge against quantum attacks. In *STOC '06: Proceedings of the thirty-eighth annual ACM symposium on Theory of computing*, pages 296–305, New York, NY, USA, 2006. ACM. [cited at p. 2]

[Weh06] S. Wehner. Entanglement in interactive proof systems with binary answers. *LNCS*, 3884:162, 2006. [cited at p. 24, 50]

[Wer89] R. F. Werner. An application of Bell's inequalities to a quantum state extension problem. *Letters in Mathematical Physics*, 17:359–363, May 1989. [cited at p. 49]

Appendices

Appendix A

Mathematical Optimization

In this section, we review the notions of mathematical optimization and more precisely of convex and linear optimization problems [BV04]. We also explain the notion of duality, useful for finding a lower bound on an optimization problem.

A.1 Optimization Problems

In optimization, the goal is to find a solution to a minimization or maximization problem. We begin by giving the general description of optimization problems.

Definition A.1.1 (Optimization problems [BV04])**.** Optimization problems have the form

$$\begin{array}{ll} \text{minimize} & f_0(x) \\ \text{subject to} & f_i(x) \leq b_i \qquad i = 1, ..., m \end{array}$$

where $x = (x_1, ..., x_n)$ is the optimization variable, $f_0 : \mathbb{R}^n \to \mathbb{R}$ is the objective function, $f_i : \mathbb{R}^n \to \mathbb{R}$, $i = 1, ..., m$, are the constraint functions and $b_1, ..., b_m$ are bounds for the constraints.

A solution to an optimization problem is a vector x^* that has the smallest objective value that satisfies the constraints. In other words, a solution x^* is defined by $f_0(z) \geq f_0(x^*)$ for any z such that $f_1(z) \leq b_1, ..., f_m(z) \leq b_m$. Note that we can transform a minimization problem into a maximization problem by changing the objective function f_0 by $-f_0$.

Optimization problems are divided into classes characterized by the form of the objection function and constraint functions. One of these classes is the class of linear problems or linear programs.A linear program has the form

$$f_i(\alpha x + \beta y) = \alpha f_i(x) + \beta f_i(y)$$

for all $x, y \in \mathbb{R}^n$ and all $\alpha, \beta \in \mathbb{R}$. A linear program is special case of convex optimization problems. Convex optimization problems is another class of optimization problems. For those problems, the objective and constraint functions have the special form

$$f_i(\alpha x + \beta y) \leq \alpha f_i(x) + \beta f_i(y)$$

for all $x, y \in \mathbb{R}^n$ and all $\alpha, \beta \in \mathbb{R}$ with $\alpha + \beta = 1$, $\alpha \geq 0, \beta \geq 0$.

There is no simple analytical formula for the solution of an optimization problems. On the other hand, there are a variety of methods to solve them based of the form of the objective and constraints functions [BV04].

In the next section, we focus our attention on convex optimization problems, and more specifically on linear programs.

A.1.1 Convex Optimization Problems

We describe a convex optimization problem as follows.

Definition A.1.1 (Convex Optimization Problems [BV04])**.** Convex optimization problems have the form

$$\begin{array}{lll} \text{minimize} & f_0(x) & \\ \text{subject to} & f_i(x) \leq 0 & i = 1, ..., m \\ & h_i(x) = 0 & i = 1, ..., p \end{array}$$

where $x \in \mathbb{R}^n$, $f_i : \mathbb{R}^n \to \mathbb{R}$ are inequality constraints and $h_i : \mathbb{R}^n \to \mathbb{R}$ are the equality constraints.

If there is no constraints (i.e.: $m = p = 0$), we say that the problem is unconstrained.

We define the domain of the optimization problem $\mathscr{D}$ as the set of points where the objective function and the constraint function are defined:

$$\mathscr{D} = \bigcap_{i=0}^{m} \operatorname{dom} f_i \cap \bigcap_{i=0}^{p} \operatorname{dom} h_i.$$

A point $x \in \mathscr{D}$ is said to feasible if it satisfies all inequality and equality constraints. We say that the problem is feasible if it has at least one feasible point.

We define the optimal value p^* of the problem as

$$p^* = \inf\{f_0(x) | f_i(x) \leq 0, i = 0, ..., m \quad h_i(x) = 0, i = 1, ..., p\}$$

If a problem is infeasible, we have $p^* = \infty$ and if there are feasible points x_k for which $f_0(x_k) \to -\infty$ as $k \to \infty$, we have $p^* = -\infty$ and we say the problem is unbounded below.

We say that a point x^* is optimal if it is feasible and $f(x^*) = p^*$. The set of optimal points is denoted by

$$X_{opt} = \{x | f_i(x) \leq 0, i = 0, ..., m \quad h_i(x) = 0, i = 1, ..., p, \quad f_0(x) = p^*\}.$$

If there exists an optimal point, we say that the optimal value is attained or achieved and that the problem is solvable. Otherwise, we say that the optimal point is not achievable. Note that when we refer to an optimal point, we mean a global optimal point. The definition of a local optimal point is given in [BV04].

A.1.2 Linear Optimization Problems

We describe a subclass of convex optimization problem, the class of linear optimization problems or simply linear programs as follows. A linear program has affine objective and constraint functions.

Definition A.1.2 (Linear Optimization Problems [BV04])**.** A general linear program has the form

$$\begin{array}{ll} \text{minimize} & a^T x + d \\ \text{subject to} & Gx \preceq h \\ & Ax = b \end{array}$$

where $G \in R^{m \times n}$,$A \in R^{p \times n}$ and the symbol $\preceq$ (and its strict form $\prec$) denote the generalized inequality.

The generalized inequality between vectors represents the componentwise inequality and between symmetric matrices, it represents matrix inequality. Note that the value d can be omitted in the definition of the problem because it does not affect the feasible set. The maximization problem of the objective function $-c^T x - d$ is also a linear program.

A linear program can be in the standard form or the inequality form. In the standard form, the only inequalities are the componentwise nonnegativity constraints $x \succeq 0$:

$$\begin{array}{ll} \text{minimize} & a^T x + d \\ \text{subject to} & Ax = b \\ & x \succeq 0. \end{array}$$

In the inequality form, the linear program has no equality constraints:

$$\begin{array}{ll} \text{minimize} & a^T x + d \\ \text{subject to} & Ax \succeq b. \end{array}$$

For more details on conversion to the standard form, consult [BV04].

A.2 Duality

A.2.1 The Lagrange Dual Function

Consider an optimization problem (not necessary convex) in the standard form as follows

$$\begin{array}{lll} \text{minimize} & f_0(x) & \\ \text{subject to} & f_i(x) \leq 0 & i = 1, ..., m \\ & h_i(x) = 0 & i = 1, ..., p \end{array}$$

We define the Lagrangian of associated with the optimization problem.

Definition A.2.1 (The Lagrangian [BV04])**.** We define the Lagrangian $L : \mathbb{R}^n \times \mathbb{R}^m \times \mathbb{R}^p \to \mathbb{R}$ as

$$L(x, \lambda, \nu) = f_0(x) + \sum_{i=1}^{m} \lambda_i f_i(x) + \sum_{i=1}^{p} \nu_i h_i(x)$$

where dom $\mathscr{D} \times \mathbb{R}^m \times \mathbb{R}^p$.

The vectors λ and ν refers to the dual variables or Lagrange multiplier vectors. The idea behind the Lagrangian is to take the constraints into account in the objective function in the form of a weighted sum. We define the dual function from the Lagrangian as follows.

Definition A.2.2 (The Dual Function[BV04])**.** We define the dual function $g : \mathbb{R}^m \times \mathbb{R}^p \to \mathbb{R}$ as the minimum value of the Lagrangian over x: for $\lambda \in \mathbb{R}^m$,$\nu \in \mathbb{R}^p$,

$$g(\lambda, \nu) = \inf_{x \in \mathscr{D}} L(x, \lambda, \nu) = \inf_{x \in \mathscr{D}} \left(f_0(x) + \sum_{i=1}^{m} \lambda_i f_i(x) + \sum_{i=1}^{p} \nu_i h_i(x) \right)$$

An important property of the dual function is that it is concave even if the problem is not convex.The dual function is an interesting function because it yields lower bounds on the optimal value p^* of the problem. We state this affirmation in the following theorem.

Definition A.2.1. *For any $\lambda \succeq 0$ and any ν, we have*

$$g(\lambda, \nu) \leq p^*$$

Proof. Suppose $\tilde{x}$ is any feasible point (i.e: $f_i(\tilde{x}) \leq 0$, $h_i(\tilde{x}) = 0$ and $\lambda \succeq 0$). The Lagrangian is therefore

$$\begin{aligned} L(\tilde{x}, \lambda, \nu) &= f_0(\tilde{x}) + \sum_{i=1}^{m} \lambda_i f_i(\tilde{x}) + \sum_{i=1}^{p} \nu_i h_i(\tilde{x}) \\ &\leq f_0(\tilde{x}) \end{aligned}$$

because

$$\sum_{i=1}^{m} \lambda_i f_i(\tilde{x}) + \sum_{i=1}^{p} \nu_i h_i(\tilde{x}) \leq 0.$$

Hence,

$$g(\lambda, \nu) = \inf_{x \in \mathscr{D}} L(x, \lambda, \nu) \leq L(\tilde{x}, \lambda, \nu) \leq f_0(\tilde{x})$$

Since the last equation does not depend on the choice of a particular $\tilde{x}$, it holds for every feasible points and the inequality follows. □

A.2.2 Dual Problems

We have proved that for each pair (λ, ν) with $\lambda \succeq 0$, the Lagrange dual function is a lower bound on p^* of an optimization problem. A natural question is which dual function achieves the best lower bound? This problem is refered to the Lagrange dual problem and can be formalized as the optimization problem

$$\text{maximize} \qquad g(\lambda, \nu)$$

$$\text{subject to} \qquad \lambda \succeq 0.$$

We observe that this problem is a convex optimization problem since the objective function is concave and the constraint is convex.

The definitions of the optimization problems we have seen before are referred as primal problems. We denote by (λ^*, ν^*) the dual optimal or optimal Lagrange multipliers if they are optimal for the problem. Note that even if the primal is not an optimization problem, the dual is.

Let d^* be the optimal value of the dual problem that is the best lower bound on p^*. There is two types of duality that we define in the following two definitions.

Definition A.2.1 (Weak Duality [BV04])**.** Weak duality is the inequality

$$d^* \leq p^* \tag{A.1}$$

where p^* is the optimal value of the primal and d^* is the optimal value of the dual.This inequality holds even if the primal problem is not convex.

Definition A.2.2 (Strong Duality [BV04])**.** Strong duality is the equality

$$d^* = p^* \tag{A.2}$$

where p^* is the optimal value of the primal and d^* is the optimal value of the dual.

Strong duality means that the best bound that can be obtained from the Lagrange dual is tight. This equality is not true in general.

Appendix B

A Solution to the Dual Problem

Non-zeros variables of the numerical solution of the dual problem for the Odd Cycle Game $G_{OC,3}$ with three provers and no-signaling strategies presented in theorem (5.3.1):

$$
\begin{aligned}
&n(0,0) = 2m-1 \\
&s(0,1|0,0) = \frac{3m}{2} \\
&s(0,1|1,0) = -m+1 \\
&s(0,0|0,1) = -m+1 \\
&s(0,1|1,1) = -\frac{m}{2} \\
&s(0,0|y,y+1) = (-1)^y && \text{for y=1,2,...,m-1} \\
&s(0,1|y,y+1) = -(-1)^y && \text{for y=1,2,...,m-1} \\
&y(0|1,0) = -2m+3 \\
&y(0|1,z) = -m+z+\frac{5}{2}+\frac{(-1)^z}{2} && \text{for z=1,2,...,m-1} \\
&y(1|1,0) = 3-\frac{3m}{2} \\
&y(1|1,1) = -m+4 \\
&y(1|y,1) = -(-1)^y && \text{for y=2,...,m-1} \\
&y(1|1,z) = -m+z+\frac{5}{2}+\frac{(-1)^z}{2} && \text{for z=2,...,m-2} \\
&y(1|1,m-1) = -m+3 \\
&y(1|j,m-1) = 1-(-1)^y && \text{for y=2,3,...,m-1}
\end{aligned}
$$

$$z(0|1,0) = m - 3$$

$$z(0|1,1) = 2m - 3$$

$$z(0|1,2) = m - 4$$

$$z(0|y, y-1) = -1 \qquad \text{for y=2,3,...,m-1}$$

$$z(0|y, y+1) = (-1)^y \qquad \text{for y=2,3,...,m-1}$$

$$z(0|1,z) = m - z - \frac{3}{2} + \frac{(-1)^z}{2} \qquad \text{for z=3,4,...,m-1}$$

$$z(1|y, y-1) = -1 + (-1)^y \qquad \text{for y=1,2,...,m-1}$$

$$z(1|1,z) = m - z - \frac{3}{2} + \frac{(-1)^z}{2} \qquad \text{for z=1,2,...,m-1}$$