Parallel Repetition of Prover-Verifier Quantum Interactions

by

Abel Molina Prieto

A thesis
presented to the University of Waterloo
in fulfillment of the
thesis requirement for the degree of
Master of Mathematics
in
Computer Science

Waterloo, Ontario, Canada, 2011

I hereby declare that I am the sole author of this thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

Abstract

In this thesis, we answer several questions about the behaviour of prover-verifier interactions under parallel repetition when quantum information is allowed, and the verifier acts independently in them.

We first consider the case in which a value is associated with each of the possible outcomes of an interaction. We prove that it is not possible for the prover to improve on the optimum average value per repetition by repeating the protocol multiple times in parallel.

We look then at games in which the outcomes are classified into two types, winning outcomes and losing outcomes. We ask what is the optimal probability for the prover of winning at least k times out of n parallel repetitions, given that the optimal probability of winning when only one repetition is considered is p. A reasonable conjecture for the answer would be $\sum_{m \geq k} \binom{n}{m} p^m (1-p)^{n-m}$, as that is the answer when it is optimal for the prover to act independently. This is known to be the correct answer when $k = n$. We will show how this cannot be extended to the general case, presenting an example of an interaction with $k = 1, n = 2$ in which $p \approx 0.85$, but it is possible to always win at least once. We will then give some upper bounds on the optimal probability for the prover of winning k times out of n parallel repetitions. These bounds are expressed as a function of p.

Finally, we connect our results to the study of error reduction for quantum interactive proofs using parallel repetition.

Acknowledgements

The work presented in this thesis has been performed while I was enrolled as a Masters student at the University of Waterloo. This work has been performed under the supervision of John Watrous.

I would like to thank my friends for all I have learned from them along these years, and for keeping me relatively sane.

I would like to thank my family for supporting me, specially when I decided to transfer abroad during the middle of my undergraduate degree.

I would like to thank John Watrous for all his support, specially for giving me the opportunity to learn from him when I approached him as an undergraduate student that did not know much.

I would like to thank Ray Laflamme and Michele Mosca for creating the Institute for Quantum Computing, and make it the leading institution in research that it is today. I would like as well to thank Mike and Ophelia Lazaridis for their continued support for the institution.

Finally, I would like to thank the readers of the thesis, Richard Cleve and Ashwin Nayak, for their time and their useful comments. I would also like to thank Gus Gutoski for his help with figures 3.1 and 3.2 in this thesis, and David Rhee for his help at analyzing the objective value of the last dual solution in Chapter 6.

Contents

1 Introduction 1

2 Background 7

2.1 Linear algebra 7

2.2 Quantum Information 9

2.3 Semidefinite programming 9

3 Mathematical formalization 13

4 Optimal expected value under parallel repetition 19

5 Optimal strategies in risk-minimizing parallel repetition 29

5.1 Counterexample to the independence of acting optimally for Bob 32

5.2 Analysis in the classical case 35

6 Quantitative bounds to hedging phenomena 41

7 Error reduction for interactive proof systems 47

8 Conclusion 53

Bibliography 55

Chapter 1

Introduction

We will give now an abstract description of the kind of interaction that we consider, without giving details about the corresponding underlying theories or mathematical structures. In our prover-verifier interaction, one individual (the prover) subjects another individual (the verifier) to a test. Following the standard convention for two-party interactions in quantum information, we will call them Alice and Bob, respectively. They could also be named Arthur and Merlin, following the convention in computational complexity for prover-verifier interactions. Of course, Alice and Bob might correspond to devices instead of individuals in a real life instance of this kind of interaction.

The interaction corresponding to our tests is of the following form:

1. Alice prepares a *question* and sends it to Bob.
2. Bob responds by sending an *answer* to Alice.
3. The previous steps are repeated an arbitrary number of times. At any point, Alice and Bob can use whatever memory they have of the interaction to determine what question or answer to send.
4. Based on the last answer from Bob, as well as whatever memory Alice has of Bob's previous answers and her own questions, Alice assigns an outcome to the test.

An interaction is specified by the process by which Alice operates. We assume that Bob has access to a complete description of this process. In a classical setting, the messages exchange between Alice and Bob are purely classical, that is, they can be modelled as a sequence of bits. The process by which Alice operates can then be modelled as a given probabilistic process, where the questions are selected from some probability distribution conditioned on previous parts of the interaction, and the final decision might also involve the use of randomness. In the quantum case, Alice's questions might take the form of quantum information, and so might the answers that she expects from Bob. The process by which Alice operates is then at each step a given map from quantum states to quantum states. This process transforms Alice's memory and the last answer he received from Bob to Alice's next question and the next state of her memory. Note that this implies that Alice's questions can be entangled with Alice's memory.

The behaviour of Bob is not part of the description of the test. Indeed, the questions we explore in this thesis are mostly concerned with looking at what behaviour is desirable for Bob in different cases. Typically Bob is allowed to perform an arbitrary probabilistic process in the classical case, and an arbitrary quantum process in the quantum case. In the same way as the process for Alice, this process can be conditioned on previous parts of the interaction, and in the quantum case Bob can entangle his answers with his memory.

Note also that there is no loss of generality involved in assuming that the protocol begins with a message from Alice. This is because we can simulate a similar protocol in which the first message is sent by Bob with a protocol of the kind described here in which the first message is sent by Alice, and it is an empty message.

The formalism necessary to study these interactions in a rigorous way is presented in Chapters 2 and 3. Chapter 2 presents some useful linear algebra, optimization and quantum information facts and terms. Chapter 3 shows how these can be applied to obtain a quantitative description of the interactions that we are studying.

As the original results of this thesis, we answer several questions related to the repetition in parallel of these interactions. They follow the theme of looking at the optimality for Bob of treating different repetitions of an interaction independently when the interaction is repeated in parallel. That is, we consider the case in which Alice instantiates n independent copies of her test: she follows exactly the same procedure in all of the n parallel repetitions when determining what questions to send. The processes followed to determine the outcome of the interactions are completely independent as well.

There are several questions that one might ask concerning what is Bob's optimal behaviour when a protocol is repeated several times in this way, depending on what does Bob want to optimize. In Chapter 4, we consider the setting in which a value is assigned by Bob to each of the outcomes, letting v denote the best expected value that he can obtain as the outcome of an interaction. Formally speaking, and without a reference to any particular mathematical model for our interaction, this is the supremum over all possible processes by which Bob can operate of the expected value corresponding to the outcome of the protocol, when Bob follows that particular process. In both the classical and quantum models, the supremum will always be achieved, so that it may safely be replaced by the maximum.

Now, we consider the case in which Bob is trying to maximize the sum of the values obtained from r repetitions of an interaction. We ask then the question:

> What is the optimum expected value per repetition that can be obtained for Bob when he considers all of the n interactions?

One might think that given the fact that Alice is instantiating independently the copies of her test, the answer to this question is v, as this is the answer when Bob acts independently in the different repetitions. As we prove, this is indeed the correct answer.

In Chapter 5, we look at the behaviour for Bob when he only cares about obtaining certain outcomes. Then, for a fixed choice of Alices test and a particular choice of outcome, let p denote the optimal probability for Bob of obtaining one of those outcomes. We identify these outcomes as the "winning" outcomes. In the same way as in the definition of v, p is more formally defined as the supremum of the probability that Bob achieves a winning outcome over all the processes by which Bob can operate. In the same way again as we have for v, in both our classical and quantum models this supremum can be safely replaced by a maximum.

When Bob is trying to optimize the average number of repetitions in which he obtains a winning outcome, the best he can do is to play independently his optimal strategy for achieving a winning outcome. This can be seen from assigning value 1 to the winning outcomes and value 0 to all other outcomes, and considering our result in Chapter 4. However, we can also consider the case in which Bob is not concerned with optimizing the average number of repetitions in which he obtains a winning outcome, but rather with making sure that the number of repetitions in which he obtains a winning outcome is above a certain threshold. We ask then the question:

> What is the optimum probability for Bob of achieving a winning outcome in at least k of the n interactions?

Following the same reasoning as in the previous question, one might think that given the fact that Alice is instantiating independently the copies of her test, the answer to this question is $\sum_{k\leq t\leq n}\binom{n}{t}p^t(1-p)^{n-t}$. The reason is that this is the answer when Bob acts independently in the different repetitions.

This is indeed the correct answer in the classical case. This can be proved from the observation that an optimal strategy for Bob in a classical model is always deterministic, and we will discuss later how it also follows as a special case of our analysis in the quantum case.

It is also known that in the special case in which $k = n$, the answer to this question is indeed $\sum_{k \leq t \leq n} \binom{n}{t} p^t (1-p)^{n-t}$, which in this case equals p^n. In what is probably the most significant contribution in this thesis, we show how $\sum_{k \leq t \leq n} \binom{n}{t} p^t (1-p)^{n-t}$ is in fact not in general the correct answer to this question. First, we show how the proof for the case in which $k = n$ fails to be generalized in a straightforward way in this case. Then, we give an explicit example of a test in which Bob can pass at least one of two repetitions with probability 1, despite the fact that $p < 1$. In our example, Bob's optimal probability of winning for a single repetition of the interaction is $\cos^2(\pi/8) \approx 0.85$.

The ability of Bob to correlate his answers can be seen as a form of hedging, as we illustrate in a highly fictitious scenario. In our scenario, Bob is offered the opportunity to take part in two potentially very lucrative but involving some risks games of chance, organized by Alice. These two games are completely identical to each other, and run independently. To earn the right to play in each of the games, Bob must contribute \$1 million of his own money, and he has an 85% chance of winning if he plays optimally. For each game he wins, Bob receives a price of \$3 million, with a total \$2 million gain over his initial investment. If Bob does not win, he loses his \$1 million investment.

Many people, if put in the place of Bob, would not hesitate to play both of the games, even taking out a \$2 million loan if necessary to do so. The expected gain from each of the games is \$1,550,000, and the only time that Bob loses money as an overall result is when Bob loses in both of the games. If we treat the games independently, the chance for a loss in both is 2.25%. However, Bob could be a highly risk-averse person. He would greatly enjoy being a millionaire, but cannot or does not want to risk a 2.25% chance of losing \$2 million. If the games run by Alice can be modelled classically, there is no way Bob can avoid this risk. However, if the two games have a model using quantum information with the same properties as the one in our example, Bob can be guaranteed to win in at least one of the games, and therefore obtain at least a total \$1 million gain. A choice of an appropriate quantum strategy allows Bob to hedge his bets perfectly.

There are other settings in which quantum effects that are not possible in the classical world have been discovered to be possible in an interaction between two parties that allows for quantum behaviour. However, our setting differs from some of the best-known such situations, such as the CHSH game [CHSH69] and the Mermin-Peres magic squares game [Mer90, Per90]. In our setting, we do not have two parties collaborating to achieve a non-classical outcome. Instead, we have a prover-verifier setting, in which Bob is trying to convince Alice in order to achieve the winning outcome for an interaction.

In Chapter 6, we continue examining the same question as in Chapter 5. As we said, we establish in Chapter 5 that it is not necessarily optimal for Bob to play independently when he is trying to win in at least a certain number of interactions. However, it still seems reasonable to think that how well Bob can do when he is trying to win in at least a certain number of repetitions should be somehow related to how well Bob can do when the interaction only occurs once, and he is trying to obtain the winning outcome. For example, it is clear that if Bob can make sure that he wins when the interaction only occurs once, then he is capable of making sure that he wins in at least a certain number of repetitions (since in fact, he can make sure that he wins in all repetitions). It is also possible to prove that if Bob does not have any chance of winning when the interaction only occurs once, then he does not have any chance of winning any number of interactions larger than zero when the game is played several times. This follows as a special case of our analysis for the quantum case. It can also be proved by contradiction starting from the observation that when only one repetition of the interaction is considered, Bob could simulate the setting in which several interactions are repeated in paralle, by simulating what would be the actions of Alice in the fictional copies of the interaction.

It is then a reasonable aim to obtain general quantitative relations that express this idea. With this goal in mind, we try to upper bound the optimum probability for Bob of achieving the winning outcome in at least k of the n interactions as a function of p. We will see how it is not hard to obtain from our formalization an upper bound of $\sum_{k \leq t \leq n} \binom{n}{t} p^t$. Using a more involved analysis, we obtain an improved upper bound of $p^k \binom{n}{k-1}$.

In Chapter 7, we apply the results from the previous section to the study of error reduction for quantum interactive proof systems. These, generally speaking, are a particular case of the kind of interaction that we consider here. In this new situation, there is a *string* x known to Alice and Bob, which might or might not be a member of a *language* L.

We also have an interaction of the form that we consider in our work, such that whenever $x \in L$ Bob can pass the test with probability at least α, while whenever $x \notin L$ Bob can pass the test with probability at most $\beta < \alpha$. Note that the fact that the value of x is known to Alice and Bob implies that they can use this value to make decisions during their operation.

Assuming Bob is playing to maximize his chance of passing, Alice can then use the outcome of the test to make a guess about whether $x \in L$ or not. We can see that it is easy to make a guess that will be correct with high probability whenever α is close to 1 and β is close to 0. Error reduction corresponds then to obtaining another test with smaller β and larger α. In a natural conjecture for a possible way of reducing error, this new better test simply consists of a number of independent instantiations of the original test. The new test accepts if and only if some suitably chosen fraction of these independent tests (e.g. $\frac{\alpha+\beta}{2}$) lead to Bob passing the test. This would improve on the more complicated strategy for reducing error in this situation that is known in the literature [JUW09].

If if was true that it is optimal for Bob to answer independently, that would easily prove the correctness of this natural strategy to reduce error. Indeed, under this assumption, the number of repetitions with a winning outcome when Bob plays optimally is described as a binomial distribution parametrized by p and n. Using the properties of the binomial distribution (e.g. using a Chernoff Bound), it would be then possible to prove that the probability that the new test produces a wrong guess about whether $x \in L$ decreases exponentially fast as a function of n.

Unfortunately, our results in Chapter 5 shows that a proof method that uses the optimality of independent answers for Bob to prove the correctness of the natural strategy to reduce error would start with an incorrect assumption. On the other hand, maybe it is possible to prove the correctness of the natural strategy to reduce error while replacing that incorrect assumption about Bob's optimal behaviour with a weaker one. We will show how this is indeed the case for a limited range of values of α and β (more exactly, whenever $\beta < 2^{-\frac{H(\alpha)}{\alpha}} < \alpha$), using our results from Chapter 6.

Chapter 2

Background

In this section we provide a summary of the mathematical background needed to develop the content of this thesis. Its main purpose is to unify the notation for the content of this thesis, and not to be completely exhaustive, but just to highlight concepts that might be less familiar to some readers.

2.1 Linear algebra

We establish here the notation for linear algebra terms that will be used in this thesis. We assume familiarity with basic linear algebra concepts such as Hilbert spaces, positive semidefiniteness and tensor products. For any finite-dimensional complex Hilbert space $\mathcal{X}$ we write $\mathrm{L}(\mathcal{X})$ to denote the set of linear operators acting on $\mathcal{X}$, we write $\mathbb{I}_{\mathcal{X}}$ to denote the identity operator acting on $\mathcal{X}$, we write $\mathrm{Herm}(\mathcal{X})$ to denote the set of Hermitian operators acting on $\mathcal{X}$, we write $\mathrm{Pos}(\mathcal{X})$ to denote the set of positive semidefinite operators acting on $\mathcal{X}$, and we write $\mathrm{Pd}(\mathcal{X})$ to denote the set of positive definite operators acting on $\mathcal{X}$. We write $\mathrm{D}(\mathcal{X})$ to denote the set of density operators (positive semidefinite operators with unit trace) acting on $\mathcal{X}$.

For Hermitian operators $A, B \in \mathrm{Herm}(\mathcal{X})$ the notations $A \geq B$ and $B \leq A$ indicate that $A - B$ is positive semidefinite, and the notations $A > B$ and $B < A$ indicate that $A - B$ is positive definite.

An inner product can be given to $\mathrm{L}(\mathcal{X})$, defined as $\langle A, B\rangle = \mathrm{Tr}(A^* B)$. If $A, B \in \mathrm{Herm}(\mathcal{X})$, it holds that $\langle A, B\rangle$ is a real number and satisfies $\langle A, B\rangle = \langle B, A\rangle$. For every choice of finite-dimensional complex Hilbert space $\mathcal{X}$ and $\mathcal{Y}$, and for a given linear mapping of the form $\Phi : \mathrm{L}(\mathcal{X}) \to \mathrm{L}(\mathcal{Y})$, there is a unique mapping $\Phi^* : \mathrm{L}(\mathcal{Y}) \to \mathrm{L}(\mathcal{X})$ (known as the *adjoint* of Φ) that satisfies $\langle Y, \Phi(X)\rangle = \langle \Phi^*(Y), X\rangle$ for all $X \in \mathrm{L}(\mathcal{X})$ and $Y \in \mathrm{L}(\mathcal{Y})$.

We write the tensor product of a Hilbert space $\mathcal{X}$ with itself n times, $\mathcal{X} \otimes \mathcal{X} \ldots \otimes \mathcal{X}$, as $\mathcal{X}^{\otimes n}$. We often consider several Hilbert spaces, all denoted by a common symbol (say $\mathcal{X}$), but with different subindices, corresponding to natural numbers in some range. We write $\mathcal{X}_{i \ldots j}$ to denote the tensor product $\mathcal{X}_i \otimes \ldots \otimes \mathcal{X}_j$ of a series of these spaces spanned by a sequence of consecutive subindices going from i to j, inclusive.

During our exposition, we slightly abuse notation by identifying the tensor product of several Hilbert spaces with their tensor product in a different order. For example, we might write something like $\mathrm{Tr}_{\mathcal{Y}_2}(P) = \mathbb{I}_{X_2} \otimes Q$, where $P \in \mathrm{L}(\mathcal{X}_{1\ldots 2} \otimes \mathcal{Y}_{1\ldots 2})$ and $Q \in \mathrm{L}(\mathcal{X}_1 \otimes \mathcal{Y}_1)$. We implicitly assume then that one of the sides in our equality is conjugated with an unitary operator that appropriately transposes the order of the spaces in the tensor product (for example, in this case we might conjugate $\mathrm{Tr}_{\mathcal{Y}_2}(P)$ with the operator that sends $x \otimes z \otimes y$ to $z \otimes x \otimes y$ for all $x \in \mathcal{X}_1, y \in \mathcal{Y}_1, z \in X_2$).

We define now the Choi-Jamiołkowski representation of a linear mapping from $\mathrm{L}(\mathcal{X})$ to $\mathrm{L}(\mathcal{Y})$. To do so, suppose $\dim(\mathcal{X}) = n$ and assume that a standard orthonormal basis $\{v_i : 1 \le i \le n\}$ of $\mathcal{X}$ has been selected. With respect to this basis, one defines the Choi-Jamiołkowski operator $J(\Phi) \in \mathrm{L}(\mathcal{Y} \otimes \mathcal{X})$ of a linear mapping $\Phi : \mathrm{L}(\mathcal{X}) \to \mathrm{L}(\mathcal{Y})$ as

$$J(\Phi) = \sum_{1 \le i,j \le n} \Phi(v_i v_j^*) \otimes v_i v_j^*$$

The mapping J is a linear bijection from the space of mappings of the form $\Phi : \mathrm{L}(\mathcal{X}) \to \mathrm{L}(\mathcal{Y})$ to the operator space $\mathrm{L}(\mathcal{Y} \otimes \mathcal{X})$. It has the property that that Φ is completely positive if and only if $J(\Phi) \in \mathrm{Pos}(\mathcal{Y} \otimes \mathcal{X})$, and that Φ is trace-preserving if and only if $\mathrm{Tr}_{\mathcal{Y}}(J(\Phi)) = \mathbb{I}_{\mathcal{X}}$ [Cho75, Jam72].

Some properties of the elements in our formalism that we will use very often are the following:

1. If $A \in \mathrm{L}(\mathcal{X}_1 \otimes \mathcal{Y}_1)$ and $B \in \mathrm{L}(\mathcal{X}_2 \otimes \mathcal{Y}_2)$, then $\mathrm{Tr}_{\mathcal{X}_1 \otimes \mathcal{X}_2}(A \otimes B) = \mathrm{Tr}_{\mathcal{X}_1}(A) \otimes \mathrm{Tr}_{\mathcal{X}_2}(B)$
2. $A \ge B$ and $C \ge D$ implies $A \otimes C \ge B \otimes D$ for any choice of positive semidefinite operators A, B, C and D.
3. If we have two maps $\Phi_1 : \mathrm{L}(\mathcal{X}_1) \to \mathrm{L}(\mathcal{Y}_1)$ and $\Phi_2 : \mathrm{L}(\mathcal{X}_2) \to \mathrm{L}(\mathcal{Y}_2)$, then $J(\Phi_1 \otimes \Phi_2) = J(\Phi_1) \otimes J(\Phi_2)$.

2.2 Quantum Information

We introduce now some concepts concerning our mathematical modelling of quantum information processing. See [NC00] for a comprehensive introduction to a formal treatment of quantum information processing.

A *register* is a hypothetical device that stores quantum information. Associated with a register X is a finite-dimensional complex Hilbert space $\mathcal{X}$, and each quantum state of X is described by a density operator $\rho \in \mathrm{D}(\mathcal{X})$. *Qubits* are registers for which $\dim(\mathcal{X}) = 2$. A *measurement* of X is described by a set of positive semidefinite operators $\{P_a : a \in \Sigma\} \subset \mathrm{Pos}(\mathcal{X})$, indexed by a finite non-empty set of measurement outcomes Σ, and satisfying the constraint $\sum_{a\in\Sigma} P_a = \mathbb{I}_{\mathcal{X}}$ (the identity operator on $\mathcal{X}$). If such a measurement is performed on X while it is in the state ρ, each outcome $a \in \Sigma$ results with probability $\langle P_a, \rho\rangle$.

We can also consider information stored across several registers. If these registers are associated with finite-dimensional complex Hilbert spaces $\mathcal{X}_1 \ldots \mathcal{X}_n$, the finite-dimensional complex Hilbert space associated with their joint state is $\mathcal{X}_{1\ldots n}$. Their joint state is then described by a density operator $\sigma \in \mathrm{D}(\mathcal{X}_{1\ldots n})$.

A *quantum channel* is a completely positive and trace-preserving linear mapping of the form $\Phi : \mathrm{L}(\mathcal{X}) \to \mathrm{L}(\mathcal{Y})$. This describes a hypothetical physical process that transforms each state ρ of a register X into the state $\Phi(\rho)$ of another register Y. The set of all channels of this form is denoted $\mathrm{C}(\mathcal{X}, \mathcal{Y})$. The identity channel that does nothing to a register X is denoted $\mathbb{I}_{\mathrm{L}(\mathcal{X})}$.

2.3 Semidefinite programming

Semidefinite programming is an area of optimization which has been extensively used within quantum information theory in the last few years (see for example [CSUU07, JJUW10, LMR+11, NPA08] for a few recent uses). More comprehensive discussions about semidefinite programming can be found in [VB96, Lov03, dK02, BV04], for instance. We provide here the basic definitions and theorems used in our work.

Definition 1. A semidefinite program is specified by complex finite-dimensional Hilbert spaces $\mathcal{X}$ and $\mathcal{Y}$, and operators Φ, A and B, where:

1. $\Phi : \mathrm{L}(\mathcal{X}) \to \mathrm{L}(\mathcal{Y})$ is a Hermiticity-preserving linear mapping, and
2. $A \in \mathrm{Herm}(\mathcal{X})$ and $B \in \mathrm{Herm}(\mathcal{Y})$ are Hermitian operators,

for some choice of finite-dimensional complex Hilbert spaces $\mathcal{X}$ and $\mathcal{Y}$.

We associate with these operators two optimization problems, called the *primal* and *dual* problems:

Primal problem

$$\begin{aligned} \text{maximize:}\quad & \langle A, X\rangle \\ \text{subject to:}\quad & \Phi(X) = B, \\ & X \in \mathrm{Pos}\,(\mathcal{X})\,. \end{aligned}$$

Dual problem

$$\begin{aligned} \text{minimize:}\quad & \langle B, Y\rangle \\ \text{subject to:}\quad & \Phi^*(Y) \geq A, \\ & Y \in \mathrm{Herm}\,(\mathcal{Y})\,. \end{aligned}$$

The optimal primal value of this semidefinite program is

$$\alpha = \sup\{\langle A, X\rangle \,:\, X \in \mathrm{Pos}\,(\mathcal{X})\,,\, \Phi(X) = B\}$$

and the optimal dual value is

$$\beta = \inf\{\langle B, Y\rangle \,:\, Y \in \mathrm{Herm}\,(\mathcal{Y})\,,\, \Phi^*(Y) \geq A\}.$$

(It is to be understood that the supremum over an empty set is $-\infty$ and the infimum over an empty set is ∞, so α and β are well-defined values in the set $\mathbb{R} \cup \{-\infty, \infty\}$. In this thesis, however, we will only consider semidefinite programs for which α and β are finite).

One of the most useful facts about a semidefinite program is that it always holds that $\alpha \leq \beta$. This is known as *weak duality.* The stronger condition $\alpha = \beta$, which is known as *strong duality*, does not hold for every semidefinite program. However, it is known that there are simple conditions under which it does hold. The following theorem provides us with an example of such conditions:

Theorem 2 (Slater's theorem for semidefinite programs)**.** *Let (Φ, A, B) be the operators in our definition of a semidefinite program, and let α and β be the optimal primal and dual values for the program.*

1. *If the dual problem is feasible and there exists a positive definite operator $X \in \mathrm{Pd}\,(\mathcal{X})$ for which $\Phi(X) = B$, then $\alpha = \beta$ and there exists an operator $Y \in \mathrm{Herm}\,(\mathcal{Y})$ such that $\Phi^*(Y) \geq A$ and $\langle B, Y\rangle = \beta$.*
2. *If the primal problem is feasible and there exists a Hermitian operator $Y \in \mathrm{Herm}\,(\mathcal{Y})$ for which $\Phi^*(Y) > A$, then $\alpha = \beta$ and there exists a positive semidefinite operator $X \in \mathrm{Pos}\,(\mathcal{X})$ such that $\Phi(X) = B$ and $\langle A, X\rangle = \alpha$.*

This theorem states then in the first item that if there is a solution to the dual problem, as well as a positive definite solution to the primal problem, then strong duality holds, and an optimal dual solution is achievable. The second item gives us a similar condition, but reversing the role of the primal and dual problems. And X such as the one in the first item and a Y such as the one in the second item are called *Slater points*.

Chapter 3

Mathematical formalization

We give now a presentation of the formalism that allows us to express the questions we ask in terms of semidefinite programs. This formalism was originally developed in [GW07] and [Gut09]. A related formalism for studying a similar kind of interaction was developed in [CDP09].

The following definition formally defines an interaction of the kind that we described in the introduction. The interaction is assumed to have r rounds (that is, r questions from Alice to Bob) and t different outcomes, which are indexed from 0 to $t-1$:

Definition 3. An interaction of the kind we study is defined by:

1. A series of r quantum registers in which Alice writes her questions, which are then sent to Bob. The finite-dimensional complex Hilbert spaces associated with these registers are denoted by $\mathcal{X}_1 \ldots \mathcal{X}_r$.
2. A series of r quantum registers registers in which Bob writes his answers, which are then sent to Alice. The finite-dimensional complex Hilbert spaces associated with these registers are denoted by $\mathcal{Y}_1 \ldots \mathcal{Y}_r$.
3. A series of $r+1$ quantum registers registers that Alice uses to store her memory between the different points of the interaction. The finite-dimensional complex Hilbert spaces associated with these registers are denoted by $\mathcal{Z}_1 \ldots \mathcal{Z}_{r+1}$.
4. A quantum state that represents the first question sent by Alice to Bob, as well as the state of her initial memory. This state corresponds to a density matrix $\sigma \in \mathrm{D}\left(\mathcal{X}_1 \otimes \mathcal{Z}_1\right)$.
5. A series of $r-1$ quantum channels that correspond to the process by which Alice decides what question to ask. They produce a new question from Alice's memory and

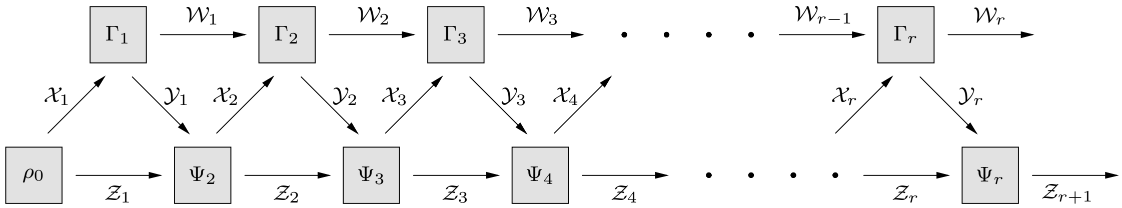

Figure 3.1: The interactions between Alice and Bob that we study

Bob's answer from the last question. We denote them by $\Psi_2 \dots \Psi_r$, with Ψ_i sending elements of $\mathrm{L}(\mathcal{Y}_{i-1} \otimes \mathcal{Z}_{i-1})$ to elements of $\mathrm{L}(\mathcal{X}_i)$.

6. A quantum channel Ψ_{r+1}, sending elements of $\mathrm{L}(\mathcal{Y}_r \otimes \mathcal{Z}_r)$ to elements of $\mathrm{L}(\mathcal{Z}_{r+1})$, the memory space for Alice after she receives the last answer.
7. A projective measurement $\{Q_i : 0 \leq i \leq k-1\}$ by which Alice decides the outcome of the interaction. This measurement is performed on $\mathcal{Z}_{r+1}$. The positive semidefinite operator corresponding to outcome k is given by Q_k.

Note that elements 6 and 7 could be merged together in a POVM measurement, but it will be more convenient for a later discussion to present the interaction in this way.

We formally define now the processes by which Bob can operate:

Definition 4. A possible process by which Bob can operate is given by:

1. A series of $r-1$ quantum registers registers that Bob uses to store his memory between sending an answer to Alice and receiving the next question. The finite-dimensional complex Hilbert spaces associated with these registers are denoted by $\mathcal{W}_1 \dots \mathcal{W}_{r-1}$.
2. A series of r quantum channels that correspond to the process by which Bob decides his answers. They produce an answer from Alice's question and Bob's memory. We denote them by $\Gamma_1 \dots \Gamma_r$. If $r = 1$, Γ_1 sends elements of $\mathrm{L}(\mathcal{X}_1)$ to elements of $\mathrm{L}(\mathcal{Y}_1)$. If $r > 1$, Γ_1 sends elements of $\mathrm{L}(\mathcal{X}_1)$ to elements of $\mathrm{L}(\mathcal{Y}_1 \otimes \mathcal{W}_1)$, Γ_i for $1 < i < r$ sends elements of $\mathrm{L}(\mathcal{X}_i \otimes \mathcal{W}_{i-1})$ to elements of $\mathrm{L}(\mathcal{Y}_r \otimes \mathcal{W}_r)$, and Γ_r sends elements of $\mathrm{L}(\mathcal{X}_r \otimes \mathcal{W}_{r-1})$ to elements of $\mathrm{L}(\mathcal{Y}_r)$.

A graphical representation of these definitions can be seen in Figure 3.1

The main result that allows us to express our questions in terms of semidefinite programs, which originally appeared in [Gut09], is the following one:

Lemma 5. *There exists operators* $P_0, \ldots, P_{t-1} \in \mathrm{Pos}\left(\mathcal{Y}_{1\ldots r} \otimes \mathcal{X}_{1\ldots r}\right)$ *, and a map from the set of possible processes by which Bob can operate to* $\mathrm{Pos}\left(\mathcal{Y}_{1\ldots r} \otimes \mathcal{X}_{1\ldots r}\right)$*, such that the probability that outcome* i *is obtained by the behaviour of Bob corresponding to* $X \in \mathrm{Pos}\left(\mathcal{Y}_{1\ldots r} \otimes \mathcal{X}_{1\ldots r}\right)$ *is* $\langle P_i, X\rangle$*.*

Moreover,

1. *The subset of* $\mathrm{Pos}\left(\mathcal{Y}_{1\ldots r} \otimes \mathcal{X}_{1\ldots r}\right)$ *to which the possible strategies for Bob are sent is composed by the elements* X *such that there exist* $X_1, \ldots, X_{r-1}$*, with* $\mathcal{X}_i \in \mathrm{Pos}\left(\mathcal{Y}_{1\ldots i} \otimes \mathcal{X}_{1\ldots i}\right)$*, satisfying:*

$$\begin{aligned}
&\mathrm{Tr}_{\mathcal{Y}_1}(X_1) = \mathbb{I}_{\mathcal{X}_1} \\
&\mathrm{Tr}_{\mathcal{Y}_2}(X_2) - X_1 \otimes \mathbb{I}_{\mathcal{X}_2} = 0 \\
&\vdots \\
&\mathrm{Tr}_{\mathcal{Y}_r}(X) - X_{r-1} \otimes \mathbb{I}_{\mathcal{X}_r} = 0
\end{aligned}$$

2. *The operators* $P_0, \ldots, P_{t-1}$ *are such that there exist* $\{P_i^j \in \mathrm{Pos}\left(\mathcal{Y}_{1\ldots j} \otimes \mathcal{X}_{1\ldots j}\right) \ : \ 0 \leq i \leq t-1, 1 \leq j \leq r-1\}$*,* $\rho \in \mathrm{D}\left(\mathcal{X}_1\right)$*, and* $\{R_j \in \mathrm{Pos}\left(\mathcal{Y}_{1\ldots j-1} \otimes \mathcal{X}_{1\ldots j}\right) : 2 \leq j \leq r\}$*, satisfying:*

$$\begin{aligned}
&\sum_{0 \leq i \leq t-1} P_i^1 = \mathbb{I}_{\mathcal{Y}_1} \otimes \rho \\
&\mathrm{Tr}_{\mathcal{X}_2}(R_2) = \sum_{0 \leq i \leq t-1} P_i^1 \\
&\sum_{0 \leq i \leq t-1} P_i^2 = \mathbb{I}_{\mathcal{Y}_2} \otimes R_2 \\
&\vdots \\
&\mathrm{Tr}_{\mathcal{X}_r}(R_r) = \sum_{0 \leq i \leq t-1} P_i^{r-1} \\
&\sum_{0 \leq i \leq t-1} P_i = \mathbb{I}_{\mathcal{Y}_r} \otimes R_r
\end{aligned}$$

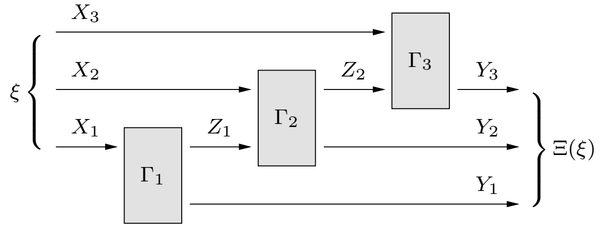

Figure 3.2: The map from $\mathrm{L}\left(\mathcal{X}_1 \otimes \ldots \mathcal{X}_r\right)$ to $\mathrm{L}\left(\mathcal{Y}_1 \otimes \ldots \otimes \mathcal{Y}_r\right)$ corresponding to the actions of Bob, in the particular case $r = 3$

This will allow us to express the questions we examine in the next chapters as questions about semidefinite programs. We will not give a proof of this Lemma here. However, we will mention the main ideas behind it. This will motivate how does the formalism apply to the case in which an interaction is repeated several times in parallel, with Alice acting independently. The main idea to prove this Lemma consists of looking at all the actions of Alice together as an operator Ξ_A from $\mathrm{L}\left(\mathcal{Y}_1 \otimes \ldots \otimes \mathcal{Y}_r\right)$ to $\mathrm{L}\left(\mathcal{X}_1 \otimes \ldots \otimes \mathcal{X}_r \otimes \mathcal{Z}_{r+1}\right)$, followed by a projective measurement $\{Q_k\}$ of $\mathcal{Z}_{r+1}$, and tracing out $\mathcal{Z}_{r+1}$. Similarly, we look at the actions of Bob as an operator Ξ_B from $\mathrm{L}\left(\mathcal{X}_1 \otimes \ldots \mathcal{X}_r\right)$ to $\mathrm{L}\left(\mathcal{Y}_1 \otimes \ldots \otimes \mathcal{Y}_r\right)$, as can be seen in figure 3.2.Then, $J(\Xi_B)$ is the object to which the actions of Bob map in the previous lemma, and P_k is given by $J\left(\left(\mathrm{Tr}_{\mathcal{Z}_{r+1}}\left(Q_k \Xi_A\right)\right)^*\right)$. The restrictions on such operators that appear in Lemma 5 are then the conditions that $J\left(\left(\mathrm{Tr}_{\mathcal{Z}_{r+1}}\left(Q_k \Xi_A\right)\right)^*\right)$and $J(\Xi_B)$ satisfy for operations Ξ_A and Ξ_B following the causal structure in our description of an interaction, as it is proved in [GW07] and [Gut09], with the operators X_i and R_j corresponding to the first rounds of the interaction.

Now, when we consider parallel repetition with Alice acting independently, we have that the new operator for Alice is given by

$$\begin{aligned} J\left(\left(\mathrm{Tr}_{\mathcal{Z}_{r+1}^{\otimes n}}\left(Q_{i_1} Q_{i_2} \ldots Q_{i_n} \Xi_A^{\otimes n}\right)\right)^*\right) &= J\left(\left(\mathrm{Tr}_{\mathcal{Z}_{r+1}}\left(Q_{i_1} \Xi_A\right)\right)^* \otimes \ldots \otimes \left(\mathrm{Tr}_{\mathcal{Z}_{r+1}}\left(Q_{i_n} \Xi_A\right)\right)^*\right) \\ &= J\left(\left(\mathrm{Tr}_{\mathcal{Z}_{r+1}}\left(Q_{i_1} \Xi_A\right)\right)^*\right) \otimes \ldots \otimes J\left(\left(\mathrm{Tr}_{\mathcal{Z}_{r+1}}\left(Q_{i_n} \Xi_A\right)\right)^*\right) \\ &= P_{i_1} \otimes \ldots \otimes P_{i_n}, \end{aligned}$$

using the properties of tensor products mentioned in Chapter 2. This motivates then the following Lemma:

Lemma 6. *Consider the case in which an interaction of the kind we consider here is repeated in parallel n times. Then, if we let $P_0, \ldots, P_{t-1}$ be the operators in the previous lemma, now there is a map from the set of possible strategies for Bob to* $\mathrm{Pos}\left((\mathcal{Y}_{1\ldots r} \otimes \mathcal{X}_{1\ldots r})^{\otimes n}\right)$ *such that the probability that outcomes $\{i_j : j \in 1 \ldots n\}$ are obtained in the n different repetitions when the behaviour of Bob corresponds to X is given by $\langle P_{i_1} \otimes P_{i_2} \otimes \ldots \otimes P_{i_n}, X\rangle$. Moreover, the subset of* $\mathrm{Pos}\left(\mathcal{Y}_{1\ldots r} \otimes \mathcal{X}_{1\ldots r}\right)$ *to which the possible strategies for Bob are sent is composed by the elements X such that there exist $X_1, \ldots, X_{r-1}$, with $X_i \in \mathrm{Pos}\left(\mathcal{Y}_{1\ldots i}^{\otimes n} \otimes \mathcal{X}_{1\ldots i}^{\otimes n}\right)$, satisfying:*

$$\begin{aligned}
&\mathrm{Tr}_{\mathcal{Y}_1^{\otimes n}}(X_1) = \mathbb{I}_{\mathcal{X}_1^{\otimes n}}\\
&\mathrm{Tr}_{\mathcal{Y}_2^{\otimes n}}(X_2) - X_1 \otimes \mathbb{I}_{\mathcal{X}_2^{\otimes n}} = 0\\
&\vdots\\
&\mathrm{Tr}_{\mathcal{Y}_r^{\otimes n}}(X) - X_{r-1} \otimes \mathbb{I}_{\mathcal{X}_r^{\otimes n}} = 0
\end{aligned}$$

To model the situation when only classical information is being exchanged inside this more general model, it is enough to assume that Alice appends a completely dephasing channel before and after each of her actions, and her measurement corresponds as well to a set of diagonal matrices. The completely dephasing channel just makes equal to zero all non-diagonal elements from the density matrix representing its input state, and leaves the diagonal elements unmodified, making sure then that only classical information is being sent. In this case, it is not hard to see that $J\left(\left(\mathrm{Tr}_{\mathcal{Z}_{r+1}}\left(Q_k \Xi_A\right)\right)^*\right)$ will be a diagonal matrix, since for the terms of the Choi-Jamiołkowski representation corresponding to a non-diagonal input we have that the channel Ξ_A will map them to 0, and for all the other ones, we have that they are mapped to a classical state, that is, a diagonal matrix. ρ and the R_i are diagonal as well, since they can be given a similar interpretation in terms of the Choi-Jamiołkowski representations for the actions of Alice when we ignore her measurement and shorten the length of the interaction, as it is shown in [GW07] and [Gut09].

Chapter 4

Optimal expected value under parallel repetition

We study in this chapter the situation where each outcome $i \in \{0 \ldots t-1\}$ of an interaction is associated with a value v_i, and Bob is concerned with maximizing the expected value that he obtains from the interaction. We prove that when an interaction is instantiated several times in parallel, it is optimal for Bob to act independently when is he trying to maximize the expected value per instantiation.

To express this situation formally, consider a fixed interaction, described using our formalism in Chapter 3, and a fixed process by which Bob can operate, represented by $X \in \mathrm{Pos}\left(\mathcal{Y}_{1\ldots r} \otimes \mathcal{X}_{1\ldots r}\right)$. As the probability that outcome i is obtained is $\langle P_i, X \rangle$, the expected value obtained by Bob for an interaction when following a process represented by X is $\sum_i v_i \langle P_i, X \rangle$. Therefore, this is the objective function that Bob is trying to maximize in the situation studied in this chapter. We obtain then that the following optimization problem corresponds to the problem of finding the optimal strategy for Bob in the setting where he is trying to maximize the expected value of the outcome:

Primal Problem 1

$$\begin{aligned}
\text{maximize:} \quad & \sum_i v_i \langle P_i, X \rangle \\
\text{subject to:} \quad & \mathrm{Tr}_{\mathcal{Y}_1}(X_1) = \mathbb{I}_{\mathcal{X}_1} \\
& \mathrm{Tr}_{\mathcal{Y}_2}(X_2) - X_1 \otimes \mathbb{I}_{\mathcal{X}_2} = 0 \\
& \vdots \\
& \mathrm{Tr}_{\mathcal{Y}_r}(X) - X_{r-1} \otimes \mathbb{I}_{\mathcal{X}_r} = 0 \\
& X \in \mathrm{Pos}\left(\mathcal{Y}_{1\ldots r} \otimes \mathcal{X}_{1\ldots r}\right), X_i \in \mathrm{Pos}\left(\mathcal{Y}_{1\ldots i} \otimes \mathcal{X}_{1\ldots i}\right)
\end{aligned}$$

To compute the dual, we express this is in the exact same form that appears in our definition of semidefinite program:

Primal Problem 2

$$\text{maximize:} \left\langle \begin{pmatrix} 0 & & & 0 \\ & 0 & & \\ & & \ddots & \\ 0 & & & \sum_i v_i P_i \end{pmatrix}, \begin{pmatrix} X_1 & & & \\ & X_2 & & \\ & & \ddots & \\ & & & X \end{pmatrix} \right\rangle$$

$$\text{subject to:} \begin{pmatrix} \mathrm{Tr}_{\mathcal{Y}_1}(X_1) & & & 0 \\ & \mathrm{Tr}_{\mathcal{Y}_2}(X_2) - X_1 \otimes \mathbb{I}_{\mathcal{X}_2} & & \\ & & \ddots & \\ 0 & & & \mathrm{Tr}_{\mathcal{Y}_r}(X) - X_{r-1} \otimes \mathbb{I}_{\mathcal{X}_r} \end{pmatrix} = \begin{pmatrix} \mathbb{I}_{\mathcal{X}_1} & & & 0 \\ & 0 & & \\ & & \ddots & \\ 0 & & & 0 \end{pmatrix}$$

$$\begin{pmatrix} X_1 & & & \\ & X_2 & & \\ & & \ddots & \\ & & & X \end{pmatrix} \in \mathrm{Pos}\left((\mathcal{Y}_1 \otimes \mathcal{X}_1) \oplus (\mathcal{Y}_{1\ldots 2} \otimes \mathcal{X}_{1\ldots 2}) \ldots \oplus (\mathcal{Y}_{1\ldots r} \otimes \mathcal{X}_{1\ldots r})\right)$$

Note that we are ignoring the non-diagonal blocks of the solution. The reason why we can ignore them is that they are ignored by both the function that we are trying to optimize and the constraint Φ of the semidefinite program. Their presence does not alter either the set of $X, \{X_i\}$ that represent feasible solutions, since for any feasible solution to this new problem, its blocks along the diagonal will be positive semidefinite, and for any positive semidefinite $X, \{X_i\}$, leaving the non-diagonal blocks as zero will give us a positive semidefinite matrix.

As Φ is represented by the action

$$\begin{pmatrix} X_1 & & & \\ & X_2 & & \\ & & \ddots & \\ & & & X \end{pmatrix} \to \begin{pmatrix} \mathrm{Tr}_{\mathcal{Y}_1}(X_1) & & & 0 \\ & \mathrm{Tr}_{\mathcal{Y}_2}(X_2) - X_1 \otimes \mathbb{I}_{\mathcal{X}_2} & & \\ & & \ddots & \\ 0 & & & \mathrm{Tr}_{\mathcal{Y}_r}(X) - X_{r-1} \otimes \mathbb{I}_{\mathcal{X}_r} \end{pmatrix},$$

its adjoint Φ^* corresponds to the action

$$\begin{pmatrix} Y_1 & & & \\ & Y_2 & & \\ & & \ddots & \\ & & & Y \end{pmatrix} \to \begin{pmatrix} Y_1 \otimes \mathbb{I}_{\mathcal{Y}_1} - \mathrm{Tr}_{\mathcal{X}_2}(Y_2) & & & \\ & Y_2 \otimes \mathbb{I}_{\mathcal{Y}_2} - \mathrm{Tr}_{\mathcal{X}_3}(Y_3) & & \\ & & \ddots & \\ & & & Y \otimes \mathbb{I}_{\mathcal{Y}_r} \end{pmatrix},$$

as can be verified by a simple computation.

The dual problem for our situation will correspond then to:

Dual Problem 1

minimize: $\left\langle \begin{pmatrix} \mathbb{I}_{\mathcal{X}_1} & & & 0 \\ & 0 & & \\ & & \ddots & \\ 0 & & & 0 \end{pmatrix}, \begin{pmatrix} Y & & & \\ & Y_2 & & \\ & & \ddots & \\ & & & Y_r \end{pmatrix} \right\rangle$

subject to: $\begin{pmatrix} Y \otimes \mathbb{I}_{\mathcal{Y}_1} - \mathrm{Tr}_{\mathcal{X}_2}(Y_2) & & & \\ & Y_2 \otimes \mathbb{I}_{\mathcal{Y}_2} - \mathrm{Tr}_{\mathcal{X}_3}(Y_3) & & \\ & & \ddots & \\ & & & Y_r \otimes \mathbb{I}_{\mathcal{Y}_r} \end{pmatrix} \geq \begin{pmatrix} 0 & & & 0 \\ & 0 & & \\ & & \ddots & \\ 0 & & & \sum_i v_i P_i \end{pmatrix}$

$\begin{pmatrix} Y & & & \\ & Y_2 & & \\ & & \ddots & \\ & & & Y_r \end{pmatrix} \in \mathrm{Herm}\left(\mathcal{X}_1 \oplus (\mathcal{Y}_1 \otimes X_{1\ldots2}) \ldots \oplus (\mathcal{Y}_{1\ldots r-1} \oplus \mathcal{X}_{1\ldots r})\right)$

We can simplify this and write it as:

Dual Problem 2

$$\begin{aligned} \text{minimize:}\ & \operatorname{Tr}(Y) \\ \text{subject to:}\ & Y \otimes \mathbb{I}_{\mathcal{Y}_1} - \operatorname{Tr}_{\mathcal{X}_2}(Y_2) \geq 0 \\ & Y_2 \otimes \mathbb{I}_{\mathcal{Y}_2} - \operatorname{Tr}_{\mathcal{X}_3}(Y_3) \geq 0 \\ & \vdots \\ & Y_r \otimes \mathbb{I}_{\mathcal{Y}_r} \geq \sum_i v_i P_i \\ & Y \in \operatorname{Herm}(\mathcal{X}_1), Y_i \in \operatorname{Herm}(\mathcal{Y}_{1\ldots i-1} \otimes \mathcal{X}_{1\ldots i}) \end{aligned}$$

Note that even if we only explicitly require $Y \in \operatorname{Herm}(\mathcal{X}_1, Y_i), Y_i \in \operatorname{Herm}(\mathcal{Y}_{1\ldots i-1} \otimes \mathcal{X}_{1\ldots i})$, it must actually be the case that $Y \in \operatorname{Pos}(\mathcal{X}_1), Y_i \in \operatorname{Pos}(\mathcal{Y}_{1\ldots i-1} \otimes \mathcal{X}_{1\ldots i})$. In the case of Y_r, this is because the fact that the last constraint is satisfied implies that Y_r is $\geq$ than a positive semidefinite operator. Feasibility for the second to last constraint implies then that Y_{r-1} is positive semidefinite, and so on. This will actually be the case for all the dual problems that consider in this thesis.

We prove now that both statements in Theorem 2 apply, so there are optimal primal and dual solutions to our semidefinite program, and they have the same value. Indeed,

1. For the form of the primal problem that follows the definition of semidefinite program (Primal Problem 2), we have that there is a positive definition solution, which can be obtained by letting each of the diagonal blocks of our solution be an appropriate multiple of the identity. For example, we can have:

$$X_1 = \frac{\mathbb{I}_{\mathcal{Y}_1 \otimes \mathcal{X}_1}}{\dim Y_1},\ X_2 = \frac{\mathbb{I}_{\mathcal{Y}_{1\ldots 2} \otimes \mathcal{X}_{1\ldots 2}}}{\dim Y_1 * \dim Y_2}, \ldots, X = \frac{\mathbb{I}_{\mathcal{Y}_{1\ldots r} \otimes \mathcal{X}_{1\ldots r}}}{\dim Y_1 * \dim Y_2 * \ldots \dim Y_r}$$

2. For the form of the dual problem that follows the definition of semidefinite program (Dual Problem 2), we have that there is a solution that strictly satisfies the constraint, which can be obtained again by letting each of the diagonal blocks of our solution be an appropriate multiple of the identity. For example, we can have:

$$
\begin{aligned}
Y_r &= \left(\left\|\sum_i v_i P_i\right\| + 1\right) \mathbb{I}_{\mathcal{Y}_{1\ldots r-1}\otimes\mathcal{X}_{1\ldots r}} \\
Y_{r-1} &= 2\dim\mathcal{X}_r \left(\left\|\sum_i v_i P_i\right\| + 1\right) \mathbb{I}_{\mathcal{Y}_{1\ldots r-2}\otimes\mathcal{X}_{1\ldots r-1}} \\
Y_{r-2} &= 4\dim\mathcal{X}_{r-1}\dim\mathcal{X}_r \left(\left\|\sum_i v_i P_i\right\| + 1\right) \mathbb{I}_{\mathcal{Y}_{1\ldots r-3}\otimes\mathcal{X}_{1\ldots r-2}} \\
&\vdots \\
Y &= 2^{r-1}\dim\mathcal{X}_2\ldots\dim\mathcal{X}_{r-1}\dim\mathcal{X}_r \left(\left\|\sum_i v_i P_i\right\| + 1\right) \mathbb{I}_{\mathcal{X}_1}
\end{aligned}
$$

We will then write v to refer to the optimal value of these optimizations problems.

We consider now the situation in which n copies of the same interaction occur, with Alice acting independently, while Bob is free to correlate his actions in the different repetitions. Bob is trying to maximize the expected value per repetition that he achieves, with the value of a series of outcomes being the sum of their individual values. Using the characterization of the possible processes by which Bob can operate in a parallel repetition situation from Lemma 6, we obtain that this corresponds to the optimization problem:

$$
\begin{aligned}
&\underline{\text{Primal Problem 3}} \\
\text{maximize:}\quad & \sum_{i_1,i_2,\ldots,i_n} \frac{1}{n}\left(v_{i_1}+v_{i_2}+\ldots+v_{i_n}\right)\langle P_{i_1}\otimes P_{i_2}\otimes\ldots\otimes P_{i_n}, X\rangle \\
\text{subject to:}\quad & \operatorname{Tr}_{\mathcal{Y}_1^{\otimes n}}(X_1) = \mathbb{I}_{\mathcal{X}_1^{\otimes n}} \\
& \operatorname{Tr}_{\mathcal{Y}_2^{\otimes n}}(X_2) - X_1\otimes\mathbb{I}_{\mathcal{X}_2^{\otimes n}} = 0 \\
& \vdots \\
& \operatorname{Tr}_{\mathcal{Y}_r^{\otimes n}}(X) - X_{r-1}\otimes\mathbb{I}_{\mathcal{X}_r^{\otimes n}} = 0 \\
& X \in \operatorname{Pos}\left(\mathcal{Y}_{1\ldots r}^{\otimes n}\otimes\mathcal{X}_{1\ldots r}^{\otimes n}\right), X_i \in \operatorname{Pos}\left(\mathcal{Y}_{1\ldots i}^{\otimes n}\otimes\mathcal{X}_{1\ldots i}^{\otimes n}\right)
\end{aligned}
$$

Going through the same process to obtain a simplified version of the dual as in the case with a single repetition, we have that the dual of this optimization problem is:

Dual Problem 3

$$\begin{aligned}
\text{minimize: } & \operatorname{Tr}(Y) \\
\text{subject to: } & Y \otimes \mathbb{I}_{\mathcal{Y}_1^{\otimes n}} - \operatorname{Tr}_{\mathcal{X}_2^{\otimes n}}(Y_2) \geq 0 \\
& Y_2 \otimes \mathbb{I}_{\mathcal{Y}_2^{\otimes n}} - \operatorname{Tr}_{\mathcal{X}_3^{\otimes n}}(Y_3) \geq 0 \\
& \vdots \\
& Y_r \otimes \mathbb{I}_{\mathcal{Y}_r^{\otimes n}} \geq \sum_{i_1, i_2, \ldots, i_n} \frac{1}{n} \left(v_{i_1} + v_{i_2} + \ldots + v_{i_n}\right) \left(P_{i_1} \otimes P_{i_2} \otimes \ldots \otimes P_{i_n}\right) \\
& Y \in \operatorname{Herm}\left(\mathcal{X}_1^{\otimes n}\right), Y_i \in \operatorname{Herm}\left(\mathcal{Y}_{1 \ldots i-1}^{\otimes n} \otimes \mathcal{X}_{1 \ldots i}^{\otimes n}\right)
\end{aligned}$$

We again have that strong duality holds, and there are optimal solutions for both the primal and dual problems. To see this, we can adapt the forms of the primal and dual problems in the same way that we did for the case with one single repetition, and obtain Slater points by letting the diagonal blocks of our solutions be multiples of the identity. We write v' then to refer to the optimal value of these optimizations problems.

We can now formally phrase the question

> Can Bob improve on his expected value per interaction when n interactions are played in parallel, as opposed to a single interaction?

as

> Is $v = v'$?

We will see now that the answer to this question is affirmative. Informally, it is clear that $v' \geq v$, since if Bob just plays his optimal strategy for one repetition in an independent way, his expected value per repetition will be the optimum expected value when only one single repetition occurs. And indeed, let $X, \{X_i\}$ represent an optimal solution to the primal version of the optimization problem for a single repetition (Primal Problem 1). Then, I claim that $X^{\otimes n}$, $\{X_i^{\otimes n}\}$ represent a feasible solution to the primal optimization problem for more than one repetition (Primal Problem 3), with value v. Indeed, using the properties of the tensor product that we stated in Chapter 2, we have:

- If we consider a random variable V that takes value v_i with probability $\langle P_i, X \rangle$, we have that

$$\begin{aligned}
& \sum_{i_1,i_2,\ldots,i_n} \frac{1}{n}\left(v_{i_1}+v_{i_2}+\ldots+v_{i_n}\right)\left\langle P_{i_1}\otimes P_{i_2}\otimes\ldots\otimes P_{i_n}, X^{\otimes n}\right\rangle \\
= \; & \frac{1}{n}\sum_{i_1,i_2,\ldots,i_n}\left(v_{i_1}+v_{i_2}+\ldots+v_{i_n}\right)\left\langle P_{i_1}, X\right\rangle\left\langle P_{i_2}, X\right\rangle\ldots\left\langle P_{i_n}, X\right\rangle \\
= \; & \frac{1}{n}\mathrm{E}[nV] = \frac{1}{n}n\mathrm{E}[V] = \mathrm{E}[V] = v
\end{aligned}$$

- $\mathrm{Tr}_{\mathcal{Y}_1^{\otimes n}}(X_1^{\otimes n}) = (\mathrm{Tr}_{\mathcal{Y}_1}(X_1))^{\otimes n} = \mathbb{I}_{\mathcal{X}_1}^{\otimes n} = \mathbb{I}_{\mathcal{X}_1^{\otimes n}}$

  $$\begin{aligned}
  \mathrm{Tr}_{\mathcal{Y}_2^{\otimes n}}(X_2^{\otimes n}) - X_1^{\otimes n}\otimes\mathbb{I}_{\mathcal{X}_2^{\otimes n}} &= (\mathrm{Tr}_{\mathcal{Y}_1}(X_2))^{\otimes n} - (X_1\otimes\mathbb{I}_{\mathcal{X}_2})^{\otimes n} \\
  &= (X_1\otimes\mathbb{I}_{\mathcal{X}_2})^{\otimes n} - (X_1\otimes\mathbb{I}_{\mathcal{X}_2})^{\otimes n} = 0
  \end{aligned}$$

  $$\vdots$$

  $$\begin{aligned}
  \mathrm{Tr}_{\mathcal{Y}_r^{\otimes n}}(X^{\otimes n}) - X_{r-1}^{\otimes n}\otimes\mathbb{I}_{\mathcal{X}_r^{\otimes n}} &= \mathrm{Tr}_{\mathcal{Y}_r}(X)^{\otimes n} - (X_{r-1}\otimes\mathbb{I}_{\mathcal{X}_r})^{\otimes n} \\
  &= (X_{r-1}\otimes\mathbb{I}_{\mathcal{X}_r})^{\otimes n} - (X_{r-1}\otimes\mathbb{I}_{\mathcal{X}_r})^{\otimes n} = 0
  \end{aligned}$$
- As $X \geq 0$ and $X_i \geq 0$, $X^{\otimes n} \geq 0$ and $X_i^{\otimes n} \geq 0$.

It is harder to come up with an intuitive reason for why $v' \leq v$. A possible informal argument would be that if Bob can obtain a value better than v as the expected value per repetition, then in one of his repetitions his expected value is better than v. Then, to obtain a expected value better than v when only one repetition is considered, he could simulate a setting in which multiple repetitions are considered, and let the "real" repetition of those be the one in which he obtains a value better than v. To give a formal argument for the fact that $v' \leq v$, we simply derive a solution to the dual problem for multiple repetitions (Dual Problem 3) with value v. Let then Y, $\{Y_i\}$ represent an optimal solution to Dual Problem 1. Then, I claim that

$$\frac{1}{n}\left(Y\otimes\rho\otimes\ldots\otimes\rho+\ldots+\rho\otimes\rho\otimes\ldots\otimes Y\right), \left\{\frac{1}{n}\left(Y_i\otimes R_i\otimes R_i\otimes R_i+\ldots+R_i\otimes R_i\otimes\ldots\otimes Y_i\right)\right\}$$

represents a feasible solution to the dual optimization problem for more than one repetition (Dual Problem 3) with value v. Indeed, using again the properties of the tensor product that we stated in Chapter 2, we have:

- $\mathrm{Tr}\left(\frac{1}{n}\left(Y \otimes \rho \otimes \ldots \otimes \rho + \ldots + \rho \otimes \rho \otimes \ldots \otimes Y\right)\right) = \frac{1}{n} n \, \mathrm{Tr}(Y) \, \mathrm{Tr}(\rho)^{n-1} = \mathrm{Tr}(Y) = v$
- For the first constraint of the dual problem, we have:

$$\begin{aligned}
&\frac{1}{n}\left(Y \otimes \rho \otimes \ldots \otimes \rho + \ldots + \rho \otimes \rho \otimes \ldots \otimes Y\right) \otimes \mathbb{I}_{\mathcal{Y}_1^{\otimes n}} - \\
&\mathrm{Tr}_{\mathcal{X}_2^{\otimes n}}\left(\frac{1}{n}\left(Y_2 \otimes R_2 \otimes \ldots \otimes R_2 + \ldots + R_2 \otimes R_2 \otimes \ldots \otimes Y_2\right)\right) \\
&= \frac{1}{n}\left((Y \otimes \mathbb{I}_{\mathcal{Y}_1}) \otimes (\rho \otimes \mathbb{I}_{\mathcal{Y}_1}) \otimes \ldots \otimes (\rho \otimes \mathbb{I}_{\mathcal{Y}_1}) - \mathrm{Tr}_{\mathcal{X}_2}(Y_2) \otimes \mathrm{Tr}_{\mathcal{X}_2}(R_2) \otimes \ldots \otimes \mathrm{Tr}_{\mathcal{X}_2}(R_2)\right) + \ldots \\
&+ \frac{1}{n}\left((\rho \otimes \mathbb{I}_{\mathcal{Y}_1}) \otimes \ldots \otimes (\rho \otimes \mathbb{I}_{\mathcal{Y}_1}) \otimes (Y \otimes \mathbb{I}_{\mathcal{Y}_1}) - \mathrm{Tr}_{\mathcal{X}_2}(R_2) \otimes \ldots \otimes \mathrm{Tr}_{\mathcal{X}_2}(R_2) \otimes \mathrm{Tr}_{\mathcal{X}_2}(Y_2)\right) \\
&\geq 0, \text{as } \rho \otimes \mathbb{I}_{\mathcal{Y}_1} = \mathrm{Tr}_{\mathcal{X}_2}(R_2) \text{ and } Y \otimes \mathbb{I}_{\mathcal{Y}_1} \geq \mathrm{Tr}_{\mathcal{X}_2}(Y_2)
\end{aligned}$$

- For successive constraints, we have:

$$\begin{aligned}
& \frac{1}{n}\left(Y_i \otimes R_i \otimes \ldots \otimes R_i + \ldots + R_i \otimes R_i \otimes \ldots \otimes Y\right) \otimes \mathbb{I}_{\mathcal{Y}_i^{\otimes n}} - \\
& \mathrm{Tr}_{\mathcal{X}_{i+1}^{\otimes n}}\left(\frac{1}{n}\left(Y_{i+1} \otimes R_{i+1} \otimes \ldots \otimes R_{i+1} + \ldots + R_{i+1} \otimes R_{i+1} \otimes \ldots \otimes Y_{i+1}\right)\right) \\
= \; & \frac{1}{n}\left(Y_i \otimes \mathbb{I}_{\mathcal{Y}_i}\right) \otimes \left(R_i \otimes \mathbb{I}_{\mathcal{Y}_i}\right) \otimes \ldots \otimes \left(R_i \otimes \mathbb{I}_{\mathcal{Y}_i}\right) \\
& - \frac{1}{n} \mathrm{Tr}_{\mathcal{X}_{i+1}}(Y_{i+1}) \otimes \mathrm{Tr}_{\mathcal{X}_{i+1}}(R_{i+1}) \otimes \ldots \otimes \mathrm{Tr}_{\mathcal{X}_{i+1}}(R_{i+1}) + \ldots \\
& + \frac{1}{n}\left(R_i \otimes \mathbb{I}_{\mathcal{Y}_i}\right) \otimes \ldots \otimes \left(R_i \otimes \mathbb{I}_{\mathcal{Y}_i}\right) \otimes \left(Y_i \otimes \mathbb{I}_{\mathcal{Y}_i}\right) \\
& - \frac{1}{n} \mathrm{Tr}_{\mathcal{X}_{i+1}}(R_{i+1}) \otimes \ldots \otimes \mathrm{Tr}_{\mathcal{X}_{i+1}}(R_{i+1}) \otimes \mathrm{Tr}_{\mathcal{X}_{i+1}}(Y_{i+1}) \\
\geq \; & 0, \text{as } R_i \otimes \mathbb{I}_{\mathcal{Y}_i} = \mathrm{Tr}_{\mathcal{X}_{i+1}}(R_{i+1}) \text{ and } Y_i \otimes \mathbb{I}_{\mathcal{Y}_i} \geq \mathrm{Tr}_{\mathcal{X}_{i+1}}(Y_{i+1})
\end{aligned}$$

- For the last constraint, As $Y_r \otimes \mathbb{I}_{\mathcal{Y}_r} \geq \sum_i v_i P_i$, and $R_r \otimes \mathbb{I}_{\mathcal{Y}_r} = \sum_i P^i$ we have that

$$\left(R_r \otimes \mathbb{I}_{\mathcal{Y}_r}\right)^{\otimes k-1} \otimes \left(Y_r \otimes \mathbb{I}_{\mathcal{Y}_r}\right) \otimes \left(R_r \otimes \mathbb{I}_{\mathcal{Y}_r}\right)^{\otimes n-k} \geq \sum_{i_1, i_2, \ldots, i_n} v_{i_k}\left(P_{i_1} \otimes P_{i_2} \otimes \ldots \otimes P_{i_n}\right)$$

Therefore,

$$\begin{aligned}
& \frac{1}{n} \sum_k \left(R_r \otimes \mathbb{I}_{\mathcal{Y}_r}\right)^{\otimes k-1} \otimes \left(Y_r \otimes \mathbb{I}_{\mathcal{Y}_r}\right) \otimes \left(R_r \otimes \mathbb{I}_{\mathcal{Y}_r}\right)^{\otimes n-k} \\
\geq \; & \sum_{i_1, i_2, \ldots, i_n} \frac{1}{n}\left(v_{i_1} + \ldots + v_{i_n}\right)\left(P_{i_1} \otimes P_{i_2} \otimes \ldots \otimes P_{i_n}\right)
\end{aligned}$$

Note that this implies that the answer to our question when only classical information is allowed is positive as well, as the classical case is a particular case of the quantum one.

Chapter 5

Optimal strategies in risk-minimizing parallel repetition

We consider here the situation in which the outcomes are split into two groups, *winning* outcomes and *losing* outcomes, and Bob desires to obtain winning outcomes

When Bob is trying to optimize the expected number of repetitions in which he obtains a winning outcome, the best he can do is to play independently several copies of his optimal strategy for achieving a winning outcome when only one repetition is considered. This can be seen from assigning value 1 to the winning outcome and value 0 to all other outcomes, and considering our result in the previous chapter. However, we can also consider the case in which Bob is not concerned with optimizing the number of repetitions in which he obtains the winning outcome, but rather with making sure that the number of repetitions in which he obtains the winning outcome is above a certain threshold. We can ask whether it is still optimal for Bob to play independently in this case.

To answer this question, note that we can assume without loss of generality that there are only two outcomes, by grouping together all the outcomes that correspond to a winning situation, and grouping also together all outcomes that correspond to a losing situation. To express this situation formally, consider a specific description of a game in the way presented in Chapter 3, with P_0 and P_1 being the operators from Lemma 5 that corresponds to the losing and winning outcome, respectively. We have than that determining the optimal process for Bob when he is trying to maximize the probability that he obtains the winning outcome, and only one repetition of the interaction is considered, corresponds to the following optimization problem:

Primal Problem 4

$$\begin{aligned}
\text{maximize: } & \langle P_1, X\rangle \\
\text{subject to: } & \operatorname{Tr}_{\mathcal{Y}_1}(X_1) = \mathbb{I}_{\mathcal{X}_1} \\
& \operatorname{Tr}_{\mathcal{Y}_2}(X_2) - X_1 \otimes \mathbb{I}_{\mathcal{X}_2} = 0 \\
& \vdots \\
& \operatorname{Tr}_{\mathcal{Y}_r}(X) - X_{r-1} \otimes \mathbb{I}_{\mathcal{X}_r} = 0 \\
& X \in \operatorname{Pos}\left(\mathcal{Y}_{1\ldots r} \otimes \mathcal{X}_{1\ldots r}\right), X_i \in \operatorname{Pos}\left(\mathcal{Y}_{1\ldots i} \otimes \mathcal{X}_{1\ldots i}\right)
\end{aligned}$$

The process of computing the dual is identical to the one one in Chapter 4, and we obtain as a result the dual problem:

Dual Problem 4

$$\begin{aligned}
\text{minimize: } & \operatorname{Tr}(Y) \\
\text{subject to: } & Y \otimes \mathbb{I}_{\mathcal{Y}_1} - \operatorname{Tr}_{\mathcal{X}_2}(Y_2) \geq 0 \\
& Y_2 \otimes \mathbb{I}_{\mathcal{Y}_2} - \operatorname{Tr}_{\mathcal{X}_3}(Y_3) \geq 0 \\
& \vdots \\
& Y_r \otimes \mathbb{I}_{\mathcal{Y}_r} \geq P_1 \\
& Y \in \operatorname{Herm}\left(\mathcal{X}_1\right), Y_i \in \operatorname{Herm}\left(\mathcal{Y}_{1\ldots i-1} \otimes \mathcal{X}_{1\ldots i}\right)
\end{aligned}$$

We have again strong duality, with optimal solutions existing for both the primal and the dual problem. To see this, we can just notice that these programs are a particular case of the ones for the situation in Chapter 4. We will then denote by p the optimal value of these semidefinite programs.

We consider now the situation in which several independent copies of the same interaction occur in parallel, and Bob is trying to optimize his probability of obtaining a winning outcome in at least k of then. In our analysis of the situation, we will use Σ_k^n to denote the subset of $\{0,1\}^n$ corresponding to the elements with exactly k 1s, and $\Sigma_{\geq k}^n$ to denote the subset of $\{0,1\}^n$ corresponding to the elements with at least k 1s. From Lemma 6, we obtain then that this situation corresponds to the following optimization problem:

Primal Problem 5

$$\begin{aligned}
\text{maximize:} \quad & \sum_{(i_1,i_2,\ldots,i_n)\in\Sigma^n_{\geq k}} \langle P_{i_1}\otimes P_{i_2}\otimes\ldots\otimes P_{i_n}, X\rangle \\
\text{subject to:} \quad & \mathrm{Tr}_{\mathcal{Y}_1^{\otimes n}}(X_1) = \mathbb{I}_{\mathcal{X}_1^{\otimes n}} \\
& \mathrm{Tr}_{\mathcal{Y}_2^{\otimes n}}(X_2) - X_1\otimes\mathbb{I}_{\mathcal{X}_2^{\otimes n}} = 0 \\
& \vdots \\
& \mathrm{Tr}_{\mathcal{Y}_r^{\otimes n}}(X) - X_{r-1}\otimes\mathbb{I}_{\mathcal{X}_r^{\otimes n}} = 0 \\
& X\in\mathrm{Pos}\left(\mathcal{Y}^{\otimes n}_{1\ldots r}\otimes\mathcal{X}^{\otimes n}_{1\ldots r}\right), X_i\in\mathrm{Pos}\left(\mathcal{Y}^{\otimes n}_{1\ldots i}\otimes\mathcal{X}^{\otimes n}_{1\ldots i}\right)
\end{aligned}$$

The process to obtain a simplified version of the dual as in the case with a single repetition gives us now:

Dual Problem 5

$$\begin{aligned}
\text{minimize:} \quad & \mathrm{Tr}(Y) \\
\text{subject to:} \quad & Y\otimes\mathbb{I}_{\mathcal{Y}_1^{\otimes n}} - \mathrm{Tr}_{\mathcal{X}_2^{\otimes n}}(Y_2)\geq 0 \\
& Y_2\otimes\mathbb{I}_{\mathcal{Y}_2^{\otimes n}} - \mathrm{Tr}_{\mathcal{X}_3^{\otimes n}}(Y_3)\geq 0 \\
& \vdots \\
& Y_r\otimes\mathbb{I}_{\mathcal{Y}_r^{\otimes n}} \geq \sum_{(i_1,i_2,\ldots,i_n)\in\Sigma^n_{\geq k}} P_{i_1}\otimes P_{i_2}\otimes\ldots\otimes P_{i_n} \\
& Y\in\mathrm{Herm}\left(\mathcal{X}_1^{\otimes n}\right), Y_i\in\mathrm{Herm}\left(\mathcal{Y}^{\otimes n}_{1\ldots i-1}\otimes\mathcal{X}^{\otimes n}_{1\ldots i}\right)
\end{aligned}$$

We have again strong duality with optimal solutions being achieved, as can be seen in the same way as for the problems in Chapter 4, that is, making each of the elements of our solution be a block of a larger matrix so that we have programs in the form in which we state the theorem for the existence of Slater points, and then letting the Slater points correspond to multiples of the identity. We will then denote by p' the optimal value of these problems.

Intuitively, the value of p' will be at least $\sum_{k\leq t\leq n}\binom{n}{t}p^t(1-p)^{n-t}$, since that is what a process for Bob that repeats n independent copies of the optimal process for one interaction would achieve. And indeed, if we let a solution to Primal Problem 4 be given by X, $\{X_i\}$, then $X^{\otimes n}$, $\{X_i^{\otimes n}\}$ gives us a solution to Primal Problem 5 with value $\sum_{k\leq t\leq n}\binom{n}{t}p^t(1-p)^{n-t}$. We can then formally phrase the question:

Is it optimal for Bob to play independently when trying to force a certain outcome in at least k out of n independent parallel copies of an interaction?

as

Is $p' = \sum_{k \leq t \leq n} \binom{n}{t} p^t (1-p)^{n-t}$?

This has been established in the literature to be the case when $k = n$ [Gut09, MS07]. The way in which this is done is by letting an optimal solution to Dual Problem 4 be given by $Y, \{Y_i\}$, and then considering the solution $Y^{\otimes n}, \{Y_i^{\otimes n}\}$ to Dual Problem 5. As the right hand side of the last constraint is $P_1^{\otimes n} \geq \mathbb{I}_{\mathcal{Y}_r} \otimes Y \geq 0$, the properties of the tensor product that we mention in Chapter 2 are enough to determine that $Y^{\otimes n}, \{Y_i^{\otimes n}\}$ is indeed a feasible solution, with value p^n. A natural way to extend this to the case in which $k < n$ would be to let our solution be

$$\sum_{(i_1,\ldots,i_n) \in \Sigma^n_{\geq k}} f(i_1) \otimes \ldots \otimes f(i_n), \left\{ \sum_{(i_1,\ldots,i_n) \in \Sigma^n_{\geq k}} f_i(i_1) \otimes \ldots \otimes f_i(i_n) \right\},$$

where $f(0) = \rho - Y$, $f(1) = Y$, $f_i(0) = R_i - Y_i$ and $f_i(1) = Y_i$. It is not clear that this would be a feasible solution. However, if we make the assumption that all the constraints except the last one are satisfied with equality in the Dual Problem 4 for $Y^{\otimes n}, \{Y_i^{\otimes n}\}$, which from Lemma 3.13 in [Gut09] is a valid assumption to make, we will have that all the constraints except the last one of Dual Problem 5 are satisfied by this solution. However, it is still not clear how to prove that the proposed solution does actually satisfy the last constraint. If at this point we could make the additional assumption that $Y \leq \rho$ and $Y_i \leq R_i$, the proof that we will give later for the classical case would give us that the candidate we are considering is indeed a feasible solution. However, there are cases in which it is not possible to make this assumption, as it follows from the existence of the counterexample to $p' = \sum_{k \leq t \leq n} \binom{n}{t} p^t (1-p)^{n-t}$ that we show now.

5.1 Counterexample to the independence of acting optimally for Bob

It is indeed possible to find a simple example, with $n = 2$, $r = 1$ and $k = 1$, in which the value of p is $\cos^2(\pi/8) \approx 0.85$, but the optimal probability for Bob to obtain a winning outcome in one of at least two repetitions of the interaction is not $\cos^2(\pi/8) + 2\cos^2(\pi/8)\sin^2(\pi/8) \approx 0.98$. Instead, it is equal to 1. A single repetition of the interaction corresponding to this example follows the following process:

1. Alice prepares a pair of qubits (X, Z) in the state

$$u = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle \in \mathcal{X} \otimes \mathcal{Z},$$

   and sends X to Bob.

2. Bob applies a quantum channel of his choice to X, obtaining a qubit Y that he sends back to Alice. After this action, the pair (Y, Z) will be in some particular state $\sigma \in \mathrm{D}(\mathcal{Y} \otimes \mathcal{Z})$.

3. Alice measures (Y, Z) with respect to the projective measurement $\{\Pi_0, \Pi_1\}$, where Π_0 corresponds to the losing outcome, while Π_1 corresponds to the winning outcome. $\Pi_0 = \mathbb{I} - \Pi_1$ and $\Pi_1 = vv^*$, for

$$v = \cos(\pi/8)|00\rangle + \sin(\pi/8)|11\rangle.$$

The probability that Bob obtains the winning outcome is

$$\langle \Pi_1, \sigma \rangle = \mathrm{F}(vv^*, \sigma)^2,$$

where $\mathrm{F}(\cdot, \cdot)$ denotes the *fidelity* function $\mathrm{F}(P, Q) = \left\| \sqrt{P}\sqrt{Q} \right\|_1$ and we have the equality from the fact that vv^* is pure.

Now, if Bob makes $\sigma \in \mathrm{D}(\mathcal{Y} \otimes \mathcal{Z})$ be the state after step 2, it must hold that

$$\mathrm{Tr}_{\mathcal{Y}}(\sigma) = \mathrm{Tr}_{\mathcal{X}}(uu^*) = \frac{1}{2}\mathbb{I}_{\mathcal{Z}}.$$

It is known that the fidelity function is monotone under partial tracing, so we have then that

$$\mathrm{F}(vv^*, \sigma)^2 \leq \mathrm{F}\left(\mathrm{Tr}_{\mathcal{Y}}(vv^*), \mathrm{Tr}_{\mathcal{Y}}(\sigma)\right)^2 = \mathrm{F}(Q, R)^2$$

for

$$Q = \begin{pmatrix} \cos^2(\pi/8) & 0 \\ 0 & \sin^2(\pi/8) \end{pmatrix} \qquad \text{and} \qquad R = \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{pmatrix}.$$

Computing $\sqrt{Q}\sqrt{R}$, we have then that

$$\begin{aligned}
\mathrm{F}(Q,R)^2 &= \left\| \sqrt{Q}\sqrt{R} \right\|_1^2 = \frac{1}{2}\left(\cos(\pi/8)+\sin(\pi/8)\right)^2 \\
&= \frac{1+\sin(\pi/4)}{2} = \frac{1+\cos(\pi/4)}{2} = \cos^2(\pi/8),
\end{aligned}$$

using the trigonometrical identity $\cos(\alpha/2) = \sqrt{\frac{1+\cos\alpha}{2}}$ in the last equality, and the identity $\sin(2\alpha) = 2\sin(\alpha)\cos(\alpha)$ in the third equality. We have then that the optimal probability for Bob of achieving the winning outcome is at most $\cos^2(\pi/8) \approx 0.85$. This bound is actually tight, since if Bob acts as the identity, he achieves the winning outcome with probability

$$\langle vv^*, uu^* \rangle^2 = \frac{\left(\cos(\pi/8)+\sin(\pi/8)\right)^2}{2} = \cos^2(\pi/8).$$

Now, for two instantiations of the interaction described above in which Alice operates independently, we consider what happens when Bob applies the phase flip $|00\rangle \mapsto -|00\rangle$, $|01\rangle \mapsto |01\rangle$, $|10\rangle \mapsto |10\rangle$, $|11\rangle \mapsto |11\rangle$ on the two qubits he receives. The state he receives is

$$\frac{1}{2}|0000\rangle + \frac{1}{2}|0011\rangle + \frac{1}{2}|1100\rangle + \frac{1}{2}|1111\rangle$$

and Bob's phase flip transforms this state to

$$-\frac{1}{2}|0000\rangle + \frac{1}{2}|0011\rangle + \frac{1}{2}|1100\rangle + \frac{1}{2}|1111\rangle.$$

Writing

$$w = -\sin(\pi/8)|00\rangle + \cos(\pi/8)|11\rangle$$

we find that

$$-\frac{1}{2}|0000\rangle + \frac{1}{2}|0011\rangle + \frac{1}{2}|1100\rangle + \frac{1}{2}|1111\rangle = \frac{1}{\sqrt{2}} v \otimes w + \frac{1}{\sqrt{2}} w \otimes v.$$

When Alice measures this state with respect to the measurement $\{\Pi_0, \Pi_1\}$, there will then be exactly one winning outcome and one failing outcome. Bob passes (and fails) exactly one of the two tests with certainty. The ability of Bob to correlate his answers in this way is suggestive of a perfect form of hedging, where the risk of a loss in one game of chance is perfectly offset the actions in a second game.

Note that any strategy for Bob in which he does better that playing independently when trying to win at least k times out of n will imply the existence of a hedging phenomenon, in the sense that for this strategy there will be a k' for which Bob will do worse than when playing independently at winning at least k' times out of n. This follows from our result of Chapter 4 that it is optimal for Bob to play independently if he is trying to maximize his expected number of wins.

5.2 Analysis in the classical case

In the classical case, it is not possible to find an example like the one we just presented. This can be derived from our analysis of the situation using semidefinite programs, observing first that in the classical case there exists an optimal dual solution $Y, \{Y_i\}$ to Dual Problem 4 in which all of the blocks in our solution are diagonal matrices. To see this, consider an arbitrary solution $Y', \{Y_i'\}$ to Dual Problem 4. Now, I claim that $\Lambda(Y'), \{\Lambda(Y_i')\}$ is a feasible solution with the same value, where the dephasing channel Λ sets the non-diagonal entries of the input to zero, and leaves the diagonal entries unaltered, giving then as the output an operator represented by a diagonal matrix. Indeed, we have that

- $\mathrm{Tr}(\Lambda(Y)) = \mathrm{Tr}(Y)$, since the diagonal elements of the corresponding matrices are the same.
- Λ is a positive operator, since the diagonal elements of a positive semidefinite matrix are non-negative. Then, as Λ commutes with the partial trace, $\Lambda(P_1) = P_1$, and $\Lambda(\mathbb{I} \otimes A) = \mathbb{I} \otimes \Lambda(A)$ for any operator A, we have that all the constraints are satisfied. This is because then we can write them as $\Lambda(A - B) \geq 0$, with $A \geq B$, and the constraint being therefore satisfied.

Now that we make the assumption that $Y, \{Y_i\}$ correspond to diagonal matrices (remember that P_0, P_1, $\{R_i\}$ and ρ do as well), we have that we can make the additional assumption that $Y \leq \rho, Y_i \leq R_i$. Indeed, consider any solution to Dual Problem 4 with operators $Y, \{Y_i\}$ that correspond to diagonal matrices. Then, I claim that if we let Y' be the element-wise minimum of Y and ρ, and Y_i' be the element-wise minimum of Y_i and R_i (note that then $Y' \leq \rho$ and $Y_i' \leq R_i$) , $Y', \{Y_i'\}$ is a feasible solution to Dual Problem 4 with a value equal to at most the one of $Y, \{Y_i\}$. Indeed, we have

- $Y' \leq Y$, so $\mathrm{Tr}(Y') \leq \mathrm{Tr}(Y)$.

- An element along the diagonal of the matrix for $Y' \otimes \mathbb{I}_{\mathcal{Y}_1}$ is equal either to the element in the same position for $Y \otimes \mathbb{I}_{\mathcal{Y}_1}$, or to the element in the same position for $\rho \otimes \mathbb{I}_{\mathcal{Y}_1}$.

  In case it is equal to the corresponding element of $Y \otimes \mathbb{I}_{\mathcal{Y}_1}$, from the feasibility of $Y, \{Y_i\}$ we have that this is at least the corresponding element of $\mathrm{Tr}_{\mathcal{X}_2}(Y_2)$, which will be at least the corresponding element of $\mathrm{Tr}_{\mathcal{X}_2}(Y_2')$, since $Y_2 \geq Y_2'$. We have then that in this case the element that we are considering of the matrix for $Y' \otimes \mathbb{I}_{\mathcal{Y}_1}$ will be at least equal to the element in the same position for the matrix for $\mathrm{Tr}_{\mathcal{X}_2}(Y_2')$

  In case it is equal to the corresponding element of $\rho \otimes \mathbb{I}_{\mathcal{Y}_1}$, we have that it then equal to the element in the same position for $\mathrm{Tr}_{\mathcal{X}_2}(R_2)$. This is at least equal to the corresponding element for $\mathrm{Tr}_{\mathcal{X}_2}(Y_2')$, from the definition of Y_2'. We have then again that the element that we are considering of the matrix for $Y' \otimes \mathbb{I}_{\mathcal{Y}_1}$ will be at least equal to the element in the same position for the matrix for $\mathrm{Tr}_{\mathcal{X}_2}(Y_2')$.

  As we are dealing with diagonal matrices, this establishes that the first constraint is satisfied. A similar argument (replacing Y by Y_i and ρ by R_i) gives us that all other constraints except the last one are satisfied.

- An element along the diagonal of the matrix for $Y_r' \otimes \mathbb{I}_{\mathcal{Y}_r}$ is equal either to the element in the same position for $Y_r \otimes \mathbb{I}_{\mathcal{Y}_r}$, or to the element in the same position for $R_r \otimes \mathbb{I}_{\mathcal{Y}_r}$.

  In case it is equal to the corresponding element of $Y_r \otimes \mathbb{I}_{\mathcal{Y}_r}$, from the feasibility of $Y, \{Y_i\}$ we have that this is at least the corresponding element of P_1.

  In case it is equal to the corresponding element for $R_r \otimes \mathbb{I}_{\mathcal{Y}_r}$, we have that as $P_1 \leq R_r \otimes \mathbb{I}_{\mathcal{Y}_r}$, the element we are considering of the matrix for $Y_r \otimes \mathbb{I}_{\mathcal{Y}_r}$ is at least equal to the corresponding element for P_1.

Making then all these assumptions about $Y, \{Y_i\}$, we have that we can prove that

$$\sum_{(i_1,\ldots,i_n)\in\Sigma^n_{\geq k}} f(i_1) \otimes \ldots \otimes f(i_n), \left\{ \sum_{(i_1,\ldots,i_n)\in\Sigma^n_{\geq k}} f_i(i_1) \otimes \ldots \otimes f_i(i_n) \right\}$$

is actually a feasible solution to Dual Problem 5, deriving then that

$$p' = \sum_{k\leq t\leq n} \binom{n}{t} p^t (1-p)^{n-t},$$

as desired. To prove that the solution is indeed feasible, we need the following Lemma:

Lemma 7. *Assume all of $A_0, A_1, R, B_1 = A_1 + R, B_0 = A_0 - R$ are positive semidefinite operators. Then for every choice of integers $n \geq 1$, $k \in \{0, \ldots, n\}$, it holds that*

$$\sum_{(i_1,\ldots,i_n)\in\Sigma^n_{\geq k}} B_{i_1} \otimes \ldots \otimes B_{i_n} \geq \sum_{(i_1,\ldots,i_n)\in\Sigma^n_{\geq k}} A_{i_1} \otimes \ldots \otimes A_{i_n}$$

Proof. (by induction on n)

- For $n = 1$, we must consider the cases $k = 0$ and $k = 1$.

  For $k = 0$ we have

  $$B_0 + B_1 = (A_0 - R) + (A_1 + R) = A_0 + A_1$$

  and for $k = 1$ we have

  $$B_1 = A_1 + R \geq A_1,$$

  as required.

- For $n > 1$, we have

  $$\begin{aligned}\sum_{(i_1,\ldots,i_n)\in\Sigma^n_{\geq k}} B_{i_1} \otimes \ldots \otimes B_{i_n} \quad &= \sum_{(i_1,\ldots,i_{n-1})\in\Sigma^{n-1}_{\geq k}} B_{i_1} \otimes \ldots \otimes B_{i_{n-1}} \otimes B_0 \\ &+ \sum_{(i_1,\ldots,i_{n-1})\in\Sigma^{n-1}_{\geq k-1}} B_{i_1} \otimes \ldots \otimes B_{i_{n-1}} \otimes B_1\end{aligned}$$

  Applying the induction hypothesis, we obtain

$$\begin{aligned}
\sum_{(i_1,\ldots,i_n)\in\Sigma^n_{\geq k}} B_{i_1}\otimes\ldots\otimes B_{i_n} \geq & \sum_{(i_1,\ldots,i_{n-1})\in\Sigma^{n-1}_{\geq k}} A_{i_1}\otimes\ldots\otimes A_{i_{n-1}}\otimes(A_0-R) \\
& + \sum_{(i_1,\ldots,i_{n-1})\in\Sigma^{n-1}_{\geq k-1}} A_{i_1}\otimes\ldots\otimes A_{i_{n-1}}\otimes(A_1+R) \\
= & \sum_{(i_1,\ldots,i_n)\in\Sigma^n_{\geq k}} A_{i_1}\otimes\ldots\otimes A_{i_n} \\
& + \sum_{(i_1,\ldots,i_{n-1})\in\Sigma^{n-1}_{k-1}} A_{i_1}\otimes\ldots\otimes A_{i_{n-1}}\otimes R \\
\geq & \sum_{(i_1,\ldots,i_n)\in\Sigma^n_{\geq k}} A_{i_1}\otimes\ldots\otimes A_{i_n},
\end{aligned}$$

as required.

Note that if we substitute the set of binary strings with at least k ones by any other monotone subset of $\{0,1\}^n$, the proof still holds.

□

Using this Lemma, we can prove now the feasibility of the proposed solution to Dual Problem 5:

- The fact that our proposed solution to Dual Problem 5 satisfies the first constraint follows from the Lemma, with $A_0 = \mathrm{Tr}_{\mathcal{X}_2}(R_2 - Y_2)$, $A_1 = \mathrm{Tr}_{\mathcal{X}_2}(Y_2)$, and $R = \mathbb{I}_{\mathcal{Y}_1}\otimes Y - \mathrm{Tr}_{\mathcal{X}_2}(Y_2)$, with B_0 being then $\mathrm{Tr}_{\mathcal{X}_2}(R_2) - \mathbb{I}_{\mathcal{Y}_1}\otimes Y = \mathbb{I}_{\mathcal{Y}_1}\otimes(\rho - Y)$, and B_1 being $\mathbb{I}_{\mathcal{Y}_1}\otimes Y$. That $B_0 \geq 0$ follows from our assumption that $Y \leq \rho$. That A_1 is ≥ 0 follows from the observation that we made before that all blocks of a feasible solution to the dual problems that we consider have to be positive semidefinite.
- The fact that our proposed solution to Dual Problem 5 satisfies all constraints from the second to the second last one follows from the Lemma in the same way, with $A_0 = \mathrm{Tr}_{\mathcal{X}_{i+1}}(R_{i+1} - Y_{i+1})$, $A_1 = \mathrm{Tr}_{\mathcal{X}_{i+1}}(Y_{i+1})$, and $R = \mathbb{I}_{\mathcal{Y}_i}\otimes Y_i - \mathrm{Tr}_{\mathcal{X}_{i+1}}(Y_{i+1})$. B_0 is now $\mathbb{I}_{\mathcal{Y}_i}\otimes(R_i - Y_i)$, and B_1 is $\mathbb{I}_{\mathcal{Y}_i}\otimes Y_i$. That $B_0 \geq 0$ follows from our assumption that $Y_i \leq R_i$. That A_1 is ≥ 0 follows from the observation that we made before that all blocks of a feasible solution to the dual problems that we consider have to be positive semidefinite.

- The fact that our proposed solution to Dual Problem 5 satisfies the last constraint follows from the Lemma as well, with $A_0 = P_0$, $A_1 = P_1$, and $R = \mathbb{I}_{\mathcal{Y}_r} \otimes Y_r - P_1$. B_0 is then $P_0 + P_1 - \mathbb{I}_{\mathcal{Y}_r} \otimes Y_r = \mathbb{I}_{\mathcal{Y}_1} \otimes (R_r - Y_r)$, and B_1 is $\mathbb{I}_{\mathcal{Y}_r} \otimes Y_r$. That $B_0 \geq 0$ follows from our assumption that $Y_r \leq R_r$.

We have then that our proposed solution to Dual Problem 5 is feasible in the classical case, as desired.

Chapter 6

Quantitative bounds to hedging phenomena

As we saw in Chapter 5, the naive upper bound for the optimum probability for Bob of achieving the winning outcome in at least k of n independent copies of an interaction as a function of p, his optimum probability to win when only one copy is considered, does not actually hold. However, it is still possible to establish weaker bounds. We will do so in this chapter, proving first a bound of

$$\sum_{t=k}^{n} \binom{n}{t} p^t,$$

and modifying then our method to prove a stronger bound of

$$p^k \binom{n}{k}.$$

The procedure that we will follow to obtain these bounds will be based on building a feasible solution to Dual Program 5 from an optimal solution to Dual Problem 4. Let then Y, $\{Y_i\}$ represent an optimal solution to Dual Problem 4. I claim that it holds that a feasible solution to Dual Problem 5 is given by

$$\sum_{(i_1,\ldots,i_n)\in\Sigma^n_{\geq k}} f(i_1)\otimes\ldots\otimes f(i_n), \left\{ \sum_{(i_1,\ldots,i_n)\in\Sigma^n_{\geq k}} f_i(i_1)\otimes\ldots\otimes f_i(i_n) \right\},$$

where $f(0) = \rho$, $f(1) = Y$, $f_i(0) = R_i$ and $f_i(1) = Y_i$, and that this solution has value $\sum_{t=k}^{n} \binom{n}{t} p^t$. Indeed, we can see that

$$\operatorname{Tr}\left(\sum_{(i_1,\dots,i_n)\in\Sigma_k^n} f(i_1) \otimes \ldots \otimes f(i_n) \right) = \sum_{t=k}^{n} |\Sigma_t^n| \operatorname{Tr}(Y)^t 1^{n-t} = \sum_{t=k}^{n} \binom{n}{t} p^t.$$

As far as feasibility is concerned, for all the conditions except the last $\geq$ inequality in the Dual Problem 5, it follows that they are satisfied using the same analysis as the one we performed in Chapter 4 to prove that our solution to Dual Problem 3 was feasible. For the last condition, we have that as

$$f_r(1) \otimes \mathbb{I}_{\mathcal{Y}_r} = R_r \geq P_1 \text{ and } f_r(0) \otimes \mathbb{I}_{\mathcal{Y}_r} = P_0 + P_1 \geq P_0,$$

then

$$\sum_{(i_1,\dots,i_n)\in\Sigma_{\geq k}^n} f_r(i_1) \otimes \ldots \otimes f_r(i_n) \geq \sum_{(i_1,\dots,i_n)\in\Sigma_{\geq k}^n} P_{i_1} \otimes \ldots \otimes P_{i_n}.$$

This is because then the terms at the left hand side of the last constraint can be paired to the terms at the right hand side, in such a way that the term at the left hand side is $\geq$ than the term at the right hand side.

To improve the analysis, one approach would be then obtaining a solution in which the terms at the left hand side in the last constraints can still be paired with the terms at the right hand side in this way (and the other constraints are also still satisfied), but the trace for the operator in our solution belonging to $\operatorname{Pos}(\mathcal{X}_1)$ is smaller. However, attempts at that approach have been unsuccessful so far at giving us a better value as a function of p. A possible way of doing so would be letting $Y', \{Y_i'\}$ denote a solution to the dual problem corresponding to the situation in which Bob is trying to maximize his probability of obtaining outcome 0, and then letting $f(0)$ be Y', and $f_i(0)$ be Y_i'. Then, as

$$f_r(0) \otimes \mathbb{I}_{\mathcal{Y}_r} = Y_r' \otimes \mathbb{I}_{\mathcal{Y}_r} \geq P_0,$$

we would still have a solution that satisfies the last constraint (and as can be checked again with an analysis similar to the one in Chapter 4, the other constraints are satisfied as well). The value of this solution would be

$$\sum_{t=k}^{n} \binom{n}{t} p^t \operatorname{Tr}(Y')^{n-t}.$$

However, the value of $\operatorname{Tr}(Y')$ does not in principle bear any relationship with p, and it might as well be 1, so this is not necessarily a better bound than the one we already obtained.

We can try then an alternative approach, in which we assign several terms of the right hand side in the last inequality to a term in the left hand side. For example, if we had $n = 3$ and $k = 2$, in the solution to Dual Problem 5 corresponding to our bound of $\sum_{t=k}^{n} \binom{n}{t} p^t$, the right hand side of the last constraint would contain $P_0 \otimes P_1 \otimes P_1$ and $P_1 \otimes P_1 \otimes P_1$, matched at the left hand side by $R_r \otimes \mathbb{I}_{\mathcal{Y}_r} \otimes Y_r \otimes \mathbb{I}_{\mathcal{Y}_r} \otimes Y_r \otimes \mathbb{I}_{\mathcal{Y}_r}$ and $Y_r \otimes \mathbb{I}_{\mathcal{Y}_r} \otimes Y_r \otimes \mathbb{I}_{\mathcal{Y}_r} \otimes Y_r \otimes \mathbb{I}_{\mathcal{Y}_r}$. However, it would be enough to have $R_r \otimes \mathbb{I}_{\mathcal{Y}_r} \otimes Y_r \otimes \mathbb{I}_{\mathcal{Y}_r} \otimes Y_r \otimes \mathbb{I}_{\mathcal{Y}_r}$ at the left hand side, since

$$P_0 \otimes P_1 \otimes P_1 + P_1 \otimes P_1 \otimes P_1 = (P_0 + P_1) \otimes P_1 \otimes P_1 = R_r \otimes \mathbb{I}_{\mathcal{Y}_r} \otimes P_1 \otimes P_1$$

Based on this idea, we build the following solution $S^{n,k}$ to Dual Problem 5, defined recursively as a function of n and k:

- If $k = 0$, then the solution is $S^{n,k} = \rho^{\otimes n}, \{R_i^{\otimes n}\}$
- If $k = n$, then the solution is $S^{n,k} = Y^{\otimes n}, \{Y_i^{\otimes n}\}$
- If $0 < k < n$, then the solution is

$$\begin{aligned} S^{n,k} \;=\; & (\rho, \{R_i\}) \otimes S^{n-1,k} \\ & +(Y \otimes \sum_{(i_1,\ldots,i_{n-1}) \in \Sigma_{k-1}^{n-1}} f(i_1) \otimes \ldots \otimes f(i_{n-1}), \\ & \left\{ Y_i \otimes \sum_{(i_1,\ldots,i_{n-1}) \in \Sigma_{k-1}^{n-1}} f_i(i_1) \otimes \ldots \otimes f_i(i_{n-1}) \right\}) \end{aligned}$$

, where the tensor product with $S^{n-1,k}$ and the sum between the first row and the second row are taken block-wise.

Now, we have that the value of this solution is $p^k\binom{n}{k}$. Indeed,

- If $k = 0$, then the value is $\operatorname{Tr}(\rho)^n = p^0\binom{n}{0}$.
- If $k = n$, then the value is $\operatorname{Tr}(Y)^n = p^n = p^n\binom{n}{n}$.
- If $0 < k < n$, we can use induction on n, with the base case being $n = 1$, covered by the previous two cases. We have then that the value is

$$\begin{aligned} & \operatorname{Tr}(\rho)p^k\binom{n-1}{k} + \operatorname{Tr}(Y)\binom{n-1}{k-1}\operatorname{Tr}(Y)^{k-1}\operatorname{Tr}(\rho)^{n-k} \\ = \; & p^k\binom{n-1}{k} + p\binom{n-1}{k-1}p^{k-1} = p^k\binom{n}{k} \end{aligned}$$

We also have that the solution is actually feasible. We prove in the same way as for the previous solutions we consider to Dual Problem 5 that all $\geq$ constraints except the last one are satisfied, using that if one of the blocks of our solution includes $f_i(i_1) \otimes \ldots \otimes f_i(i_n)$, the previous one will include $f_{i-1}(i_1) \otimes \ldots \otimes f_{i-1}(i_n)$ (with f instead of f_{i-1} if $i = 2$). For the last constraint, we have that

- If $k = 0$, then

$$R_r^{\otimes n} \otimes \mathbb{I}_{\mathcal{Y}_r^{\otimes n}} = (P_0 + P_1)^{\otimes n} = \sum_{(i_1,\ldots,i_n)\in\Sigma^n_{\geq 0}} P_{i_1} \otimes \ldots \otimes P_{i_n}$$

- If $k = n$, then

$$Y_r^{\otimes n} \otimes \mathbb{I}_{\mathcal{Y}_r^{\otimes n}} = (Y_r \otimes \mathbb{I}_{\mathcal{Y}_r})^{\otimes n} \geq P_1^{\otimes n} = \sum_{(i_1,\ldots,i_n)\in\Sigma^n_{\geq n}} P_{i_1} \otimes \ldots \otimes P_{i_n}$$

- If $0 < k < n$, we can use induction on n, in the same way as in our calculation of the value of the solution. We have then that, using the fact that $S^{n-1,k}$ is feasible for the corresponding program, the value at the left hand side of the last constraint is

$$\begin{aligned}
\geq\ & R_r \otimes \mathbb{I}_{\mathcal{Y}_r} \otimes \sum_{(i_1,\ldots,i_{n-1}) \in \Sigma^{n-1}_{\geq k}} P_{i_1} \otimes \ldots \otimes P_{i_{n-1}} \\
& + Y_r \otimes \sum_{(i_1,\ldots,i_{n-1}) \in \Sigma^{n-1}_{k-1}} f_i(i_1) \otimes \ldots \otimes f_i(i_{n-1}) \otimes \mathbb{I}_{\mathcal{Y}_r^{\otimes n}} \\
\geq\ & (P_0 + P_1) \otimes \sum_{(i_1,\ldots,i_{n-1}) \in \Sigma^{n-1}_{\geq k}} P_{i_1} \otimes \ldots \otimes P_{i_{n-1}} + P_1 \otimes \sum_{(i_1,\ldots,i_{n-1}) \in \Sigma^{n-1}_{k-1}} P_{i_1} \otimes \ldots \otimes P_{i_{n-1}} \\
=\ & \sum_{(i_1,\ldots,i_n) \in \{0,1\} \times \Sigma^{n-1}_{\geq k} \cup \{1\} \times \Sigma^{n-1}_{k-1}} P_{i_1} \otimes \ldots \otimes P_{i_n}
\end{aligned}$$

Decomposing $\Sigma^n_{\geq k}$ into two subsets, the one with at least k 1s in the last $n-1$ symbols, and the one with exactly $k-1$ 1s in the last $n-1$ symbols, we have that the last formula in our chain of inequalities is indeed

$$\sum_{(i_1,\ldots,i_n) \in \Sigma^n_{\geq k}} P_{i_1} \otimes \ldots \otimes P_{i_n}$$

, so our solution to Dual Problem 5 satisfies the last constraint, as desired.

Chapter 7

Error reduction for interactive proof systems

An interactive proof system is a situation in which an object belonging to one of two disjoint sets $(L_{\text{yes}}, L_{\text{no}})$ is known to two parties, one of which is trying to convince the other that the object belongs in L_{yes}. If the object does indeed belong in L_{yes}, the probability that the second individual is successfully convinced will be higher than if it does not. As it is standard to do in theoretical computer science, we will assume that the objects in the sets $(L_{\text{yes}}, L_{\text{no}})$ are modelled as binary strings. Several variations of this setting have been widely studied in complexity theory (see e.g. [BM88, GMR89] for two foundational papers in the area), as it is possible to defined complexity classes in terms of sets of objects for which such an interaction exists.

The model for these interactions is similar to the one we have considered in this thesis. In this chapter, we will then go back to referring to the party we have called Alice as the verifier and the party we have called Bob as the *prover*. There will be two outcomes for the interaction between them, one of them called the *accepting* outcome, and the other one called the *rejecting* outcome. We say that the verifier accepts whenever the outcome of the interaction is the accepting outcome, and that the verifier rejects whenever the outcome of the interaction is the rejecting outcome. We also place the additional restriction that the process by which the verifier operates must be an efficient process, so its computational ability is restricted to quantum (or probabilistic, in the classical case) polynomial time in the size of the shared object. The prover's computational ability is still unrestricted.

For an interactive proof system to be good, it should be possible for the verifier to make a reasonable guess about whether $x \in L_{\text{yes}}$ from the outcome of the interaction. Then, we say that an interactive proof is valid for a problem specified by $(L_{\text{yes}}, L_{\text{no}})$, with parameters α and β, $\beta < \alpha$, whenever

1. If $x \in L_{\text{yes}}$, it is possible for the prover to convince the verifier to accept with probability at least α. This is called the *completeness* condition, and corresponds to the condition in formal logic that true statements can be proved. $1-\alpha$ is called then the *completeness error.*
2. If $x \in L_{\text{no}}$, the verifier always accepts with probability at most β, regardless of the prover's actions. This is called the *soundness* condition, and corresponds to the condition in formal logic that false statements cannot be proved. β is called then the *soundness error.*

We might have for example that $\alpha = 1/2 + \delta$ and $\beta = 1/2 - \delta$, for some small $\delta > 0$. However, the verifier would be able to make a better guess about whether $x \in L_{\text{yes}}$ from the outcome of the interaction if we had $\alpha = 1 - \epsilon$ and $\beta = \epsilon$, for a small value of $\epsilon > 0$. The process of specifying a new interactive proof system from another one in a way that improves on the value of α and β is called then *error reduction.*

A natural procedure to perform for error reduction would be the same one that is usually performed in the case of probabilistic algorithms. That is, the verifier could repeat the interaction several times, and accept if and only if the number of accepting outcomes that are obtained is above a certain threshold. In the situation under consideration, one is to understand that it is important for the new verifier to run these independent tests in parallel (as opposed to requiring the prover to respond sequentially to the individual tests). A motivation for this comes for the fact that in the complexity classes defined in terms of quantum interactive proofs, the number of rounds is often considered to be a fixed constant, so one increasing the number of rounds might not be a possibility.

However, the analysis that proves that this intuitive procedure works in the case of probabilistic algorithms relies in the fact that the analysis of the different repetitions can be made in an independent way. It is not clear that we could do this in our analysis, since as we saw in Chapter 5, it might not be optimal for a hypothetical prover that interacts with many independent executions of an interactive proof system to respect the independence of these executions when the objective of the prover is to get a number of accepting outcomes past a certain threshold.

Note however that, as we saw in Chapter 5, in the classical case we can indeed assume that the prover respects the independence of the executions. And it is indeed well-known in that case that the same argument that is used for probabilistic algorithms can be extended, and error reduction based on parallel repetition and a threshold value computation works perfectly for (single-prover) interactive proof systems. [1] By this we mean that not only parallel repetition and a threshold value computation can be used for error reduction, but that as it follows from the behaviour in the classical case that we described in Chapter 5, we have the stronger statement that if p is the optimal probability for the original verifier to obtain an accepting outcome for some x, then the optimal probability to cause at least t acceptances out of k independent repetitions of the original interaction is

$$\sum_{j=t}^{k} \binom{k}{j} p^j (1-p)^{k-j}.$$

Using this and standard Chernoff bounds, we have that our suggested strategy for error reduction does quickly reduce the error. Our example in Chapter 5 shows that this perfect behaviour for parallel repetition does not always hold in the quantum case. However, it might still be the case that an strategy based on parallel repetition and a threshold value computation can be used for error reduction. This would provide a simpler strategy for performing error reduction in quantum interactive proofs that the ones that are known in the literature [JUW09, KW00].

We will show now then, using our results from Chapter 6, that the natural procedure that we suggest for error reduction does indeed work for a certain range of values for the α and β parameters. More formally, we prove the following Theorem:

Theorem 8. *Let the parameters α and β for a quantum interactive proof system be constant real numbers, with $0 \leq \beta < 2^{-\frac{H(\alpha)}{\alpha}} < \alpha \leq 1$. Then, a strategy based on parallel repetition followed by a threshold value computation will bring the soundness and completeness errors below ϵ in $O(\log \frac{1}{\epsilon})$ rounds.*

Proof. Let p be the optimal probability for the prover to obtain an accepting outcome with the case, and c be a constant rational number $\frac{c1}{c2}$ strictly smaller than α (we will further restrict the value of c later). We will let the threshold for the error reduction procedure be $k = \lfloor cn \rfloor$.

We start by looking at the completeness error, corresponding to the situation in which $x \in L_{\text{yes}}$ and $p \geq \alpha$. Consider an strategy for the prover which just plays the optimal strategy for a single repetition independently in each of the independent interactions. The

[1] The situation is very different for *multi-prover* interactive proof systems, wherein the subject of parallel repetition is complicated [Raz98, Hol09, Raz08].

probability that this strategy obtains a given number of accepting outcomes will be given then by a binomial distribution with parameters p and n, and this distribution follows the Chernoff bound

$$P(X \leq pn(1-\lambda)) \leq \exp\left(-\frac{pn\lambda^2}{2}\right)$$

As the probability that the number of accepting outcomes falls below the threshold is equal to the probability that it is at most cn, we have then that this probability is bounded by

$$\exp\left(\frac{-pn\left(1-\frac{cn}{pn}\right)^2}{2}\right) = \exp\left(\frac{-pn\left(1-\frac{c}{p}\right)^2}{2}\right)$$

As $c < \alpha \leq p$, this is an exponentially decreasing function of n, so it is indeed enough to repeat the interaction in parallel $O(\log \frac{1}{\epsilon})$ times to obtain a completeness error below ϵ.

We look now at the soundness error, corresponding to the situation in which $x \in L_{\text{no}}$ and $p \leq \beta$. Then, from our results in Chapter 6, we have that the probability that the prover can obtain a number of accepting outcomes above the threshold is upper bounded by

$$p^k \binom{n}{k}$$

To analyze this expression, we take its logarithm, which is equal to

$$k \lg p + \lg n! - \lg k! - \lg{(n-k)!}$$

Now, we can obtain lower and upper bounds for $\lg n! = \sum_{i=1}^{n} \lg i$ by integrating lg. The lower bound is $n \lg n - \frac{n+1}{\ln 2}$, while the upper bound is $(n+1)\lg(n+1) - \frac{n}{\ln 2}$. Using these bounds, we obtain an upper bound on the previous expression of

$$\begin{aligned} & p \lg k + (n+1)\lg(n+1) - \frac{n}{\ln 2} - k \lg k + \frac{k+1}{\ln 2} - (n-k)\lg(n-k) + \frac{n-k+1}{\ln 2} \\ = \; & p \lg k + \lg(n+1) + n \lg(n+1) - k \lg k - (n-k)\lg(n-k) + \frac{2}{\lg 2} \end{aligned}$$

If we write $k = \lfloor cn \rfloor = \left\lfloor \frac{c_1}{c_2} n \right\rfloor$ as $cn - \frac{c_1 n \mod c_2}{c_2} = n\left(c - \frac{c_1 n \mod c_2}{c_2 n}\right)$, this is equal to

$$\begin{aligned}&\left(cn - \frac{c_1 n \mod c_2}{c_2}\right)\lg p + \lg(n+1) + n\lg n + n\lg(1+\frac{1}{n}) - \left(cn - \frac{c_1 n \mod c_2}{c_2}\right)\lg n \\ &- \left(cn - \frac{c_1 n \mod c_2}{c_2}\right)\lg\left(c - \frac{c_1 n \mod c_2}{c_2 n}\right) - \left((1-c)n + \frac{c_1 n \mod c_2}{c_2}\right)\lg n \\ &- \left((1-c)n + \frac{c_1 n \mod c_2}{c_2}\right)\lg\left((1-c) + \frac{c_1 n \mod c_2}{c_2 n}\right) + \frac{2}{\lg 2}\end{aligned}$$

We can see that the terms in $n \log n$ cancel each other, and the previous expression can then be written as

$$\begin{aligned}&n\left[c\lg p + \lg(1+\frac{1}{n}) - c\lg\left(c - \frac{c_1 n \mod c_2}{c_2 n}\right) - (1-c)\lg\left((1-c) + \frac{c_1 n \mod c_2}{c_2 n}\right)\right] \\ &-\frac{c_1 n \mod c_2}{c_2}\lg p + \lg(n+1) + \frac{c_1 n \mod c_2}{c_2}\lg\left(c - \frac{c_1 n \mod c_2}{c_2 n}\right) \\ &-\frac{c_1 n \mod c_2}{c_2}\lg\left((1-c) + \frac{c_1 n \mod c_2}{c_2 n}\right)\end{aligned}$$

that is, as

$$n\left[c\lg p + \lg(1+\frac{1}{n}) - c\lg\left(c - \frac{c_1 n \mod c_2}{c_2 n}\right) - (1-c)\lg\left((1-c) + \frac{c_1 n \mod c_2}{c_2 n}\right)\right] + o(n)$$

As n goes to infinity, the coefficient for n goes to $c\lg p - H(c)$, which will be negative if $\frac{H(c)}{c} > \lg p$. Now, we have $\lg p \leq \lg \beta < \frac{H(\alpha)}{\alpha}$. As $\frac{H(x)}{x}$ is a continuous function in the interval $(0,1]$, we can then pick c as a constant close enough to α that $\lg \beta < \frac{H(c)}{c}$, and therefore $\frac{H(c)}{c} > \lg p$. We have then that there is a positive integer constant n_1 and a positive real constant λ_1 such that for all $n \geq n_1$, the coefficient for n in the previous expression is upper-bounded by λ_1. Taking also into account the $o(n)$ term, we have then that for n greater or equal than a constant n_2, the logarithm of our bound of the soundness

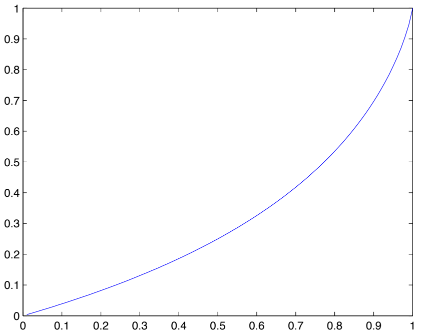

Figure 7.1: Graph for $2^{\frac{-H(x)}{x}}$

error is upper bounded by $-\lambda_2 n$ for some positive real λ_2, obtaining then the asymptotic result that the soundness error can be reduced to ϵ in $O(\log \frac{1}{\epsilon})$ rounds.

□

We can see in Figure 7.1 that the condition $\beta < 2^{-\frac{H(\alpha)}{\alpha}}$ is meaningful, in the sense that there seems to be a wide range of values of β and α for which it holds that $\beta < 2^{-\frac{H(\alpha)}{\alpha}}$. Indeed, it is possible to prove that $2^{-\frac{H(\alpha)}{\alpha}} > \alpha/3$, so for $\beta < \alpha/3$ the condition $\beta < 2^{-\frac{H(\alpha)}{\alpha}}$ will hold.

Chapter 8

Conclusion

This thesis has considered several questions related to the parallel repetition of a simple kind of interaction, broadly centered around the relevance of correlations arising in the quantum information theoretic versions of these interactions.

We have seen in Chapter 4 how the presence of those correlations does not affect the optimality for Bob of acting independently in the different repetitions whenever he associates a value to each outcome, and is trying to optimize the value obtained by repetition. However, when Bob is trying to force a certain outcome to occur a number of times past a given threshold, then we have seen in Chapter 5 that the correlations that are possible between the actions of Bob for different repetitions can give rise to a strikingly non-classical hedging type of behaviour.

Our work may have then relevance in settings considered in cryptography, where certain protocols might very well be abstracted as tests of the sort we have considered (this is the case, for example, for quantum money [Mol11], and quantum coin-flipping [GW07]).

The extent to which a dishonest individual can attack such protocols by correlating independent executions is an important security consideration that some would-be cryptographers might fail to consider. Our results in Chapter 5 demonstrate then that quantum attacks to such protocols may exhibit striking non-classical and counter-intuitive properties, and should therefore be given very careful consideration.

We have then established in Chapter 6 certain quantitative bounds to the hedging type of behaviour that we have observed. And finally, we have discussed in Chapter 7 the connection of our results with certain techniques for error reduction in quantum interactive proofs.

The main three questions left open in our work and that remain to be answered are the following ones:

1. Is it possible to improve our bounds in Chapter 6 concerning the optimum probability for Bob of achieving a winning outcome in at least k of the n interactions?
2. If the answer to the previous question is positive, can these improvements be used to prove that the naive way of parallel repetition discussed in Chapter 7 does always work?
3. If the answer to the previous questions is positive, how fast does the naive way of parallel repetition reduce the error?

Ideally, there would be an exponential decay in the optimum probability for Bob of achieving a winning outcome in a fraction of the interactions above pn, as a function of the number of repetitions n. That would answer both of the first questions in a positive way, and would establish that the naive way of parallel repetition does indeed reduce the error quickly in an asymptotical sense.

Bibliography

[BM88] L. Babai and S. Moran. Arthur-Merlin games: a randomized proof system, and a hierarchy of complexity classes. *Journal of Computer and System Sciences*, 36(2):254–276, 1988.

[BV04] S. Boyd and L. Vandenberghe. *Convex Optimization.* Cambridge University Press, 2004.

[CDP09] G. Chiribella, G. D'Ariano, and P. Perinotti. Theoretical framework for quantum networks. *Physical Review A*, 80(2):022339, 2009.

[Cho75] M.-D. Choi. Completely positive linear maps on complex matrices. *Linear Algebra and Its Applications*, 10(3):285–290, 1975.

[CHSH69] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt. Proposed experiment to test local hidden-variable theories. *Physical Review Letters*, 23:880–884, 1969.

[CSUU07] R. Cleve, W. Slofstra, F. Unger, and S. Upadhyay. Perfect parallel repetition theorem for quantum XOR proof systems. In *Twenty-Second Annual IEEE Conference on Computational Complexity*, pages 109–114, 2007.

[dK02] E. de Klerk. *Aspects of Semidefinite Programming – Interior Point Algorithms and Selected Applications*, volume 65 of *Applied Optimization.* Kluwer Academic Publishers, Dordrecht, 2002.

[GMR89] S. Goldwasser, S. Micali, and C. Rackoff. The knowledge complexity of interactive proof systems. *SIAM Journal on Computing*, 18(1):186–208, 1989.

[Gut09] G. Gutoski. Quantum strategies and local operations. PhD thesis, University of Waterloo. Available as arXiv 1003:0038v1, 2009.

[GW07] G. Gutoski and J. Watrous. Toward a general theory of quantum games. In *Proceedings of the 39th Annual ACM Symposium on Theory of Computing*, pages 565–574, 2007.

[Hol09] Thomas Holenstein. Parallel repetition: Simplifications and the no-signaling case. *Theory of Computing*, 5:141–172, 2009.

[Jam72] A. Jamiołkowski. Linear transformations which preserve trace and positive semidefiniteness of operators. *Reports on Mathematical Physics*, 3(4):275–278, 1972.

[JJUW10] R. Jain, Z. Ji, S. Upadhyay, and J. Watrous. QIP = PSPACE. In *Proceedings of the 42nd Annual ACM Symposium on Theory of Computing*, pages 573–582, 2010.

[JUW09] R. Jain, S. Upadhyay, and J. Watrous. Two-message quantum interactive proofs are in PSPACE. In *Proceedings of the 50th Annual IEEE Symposium on Foundations of Computer Science*, pages 534–543, 2009.

[KW00] A. Kitaev and J. Watrous. Parallelization, amplification, and exponential time simulation of quantum interactive proof system. In *Proceedings of the 32nd Annual ACM Symposium on Theory of Computing*, pages 608–617, 2000.

[LMR$^+$11] T. Lee, R. Mittal, B. Reichardt, R. Špalek, and M. Szegedy. Quantum query complexity of state conversion. In *52nd IEEE Symposium on Foundations of Computer Science*, 2011.

[Lov03] L. Lovász. Semidefinite programs and combinatorial optimization. *Recent Advances in Algorithms and Combinatorics*, 2003.

[Mer90] N. D. Mermin. Simple unified form for no-hidden variables theorems. *Physical Review Letters*, 65:3373–6, 1990.

[Mol11] A. Molina, 2011. Theoretical Physics Stack Exchange. URL: http://theoreticalphysics.stackexchange.com/questions/370/(version: 2011-12-08).

[MS07] R. Mittal and M. Szegedy. Product rules in semidefinite programming. In *Fundamentals of Computation Theory*, volume 4639 of *Lecture Notes in Computer Science*, pages 435–445. Springer-Verlag, 2007.

[NC00] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

[NPA08] M. Navascués, S. Pironio, and A. Acín. A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations. (073013), 2008.

[Per90] A. Peres. Incompatible results of quantum measurements. *Physical Review A*, 151:107–8, 1990.

[Raz98] R. Raz. A parallel repetition theorem. *SIAM Journal on Computing*, 27(3):763–803, 1998.

[Raz08] R. Raz. A counterexample to strong parallel repetition. In *49th Annual IEEE Symposium on Foundations of Computer Science*, pages 369–373, 2008.

[VB96] L. Vandenberghe and S. Boyd. Semidefinite programming. *SIAM Review*, 38(1):49–95, 1996.