Two-player interaction in quantum computing: cryptographic primitives & query complexity

Thèse présentée par
Loïck Magnin

en vue de l'obtention des grades

Docteur en Sciences, spécialité Informatique
Université Paris-Sud 11

et

Docteur en Sciences de l'Ingénieur
Université Libre de Bruxelles

Soutenue le 5 décembre 2011 devant le jury composé de

Alain Denise	Président
Peter Høyer	Rapporteur
Pascal Koiran	Rapporteur
Alain Dubus	Examinateur
Marc Haelterman	Examinateur
Jérémie Roland	Examinateur
Nicolas J. Cerf	Directeur de thèse
Frédéric Magniez	Directeur de thèse

À ma famille.

Résumé

Cette thèse étudie deux aspects d'interaction entre deux joueurs dans le modèle du calcul et de la communication quantique.

Premièrement, elle étudie deux primitives cryptographiques quantiques, des briques de base pour construire des protocoles cryptographiques complexes entre deux joueurs, comme par exemple un protocole d'identification.

La première primitive est la "mise en gage quantique". Cette primitive ne peut pas être réalisée de manière inconditionnellement sûre, mais il est possible d'avoir une sécurité lorsque les deux parties sont soumises à certaines contraintes additionnelles. Nous étudions cette primitive dans le cas où les deux joueurs sont limités à l'utilisation d'états et d'opérations gaussiennes, un sous-ensemble de la physique quantique central en optique, donc parfaitement adapté pour la communication via fibres optiques. Nous montrons que cette restriction ne permet malheureusement pas la réalisation de la mise en gage sûre. Pour parvenir à ce résultat, nous introduisons la notion de purification intrinsèque, qui permet de contourner l'utilisation du théorème de Uhlman, en particulier dans le cas gaussien.

Nous examinons ensuite une primitive cryptographique plus faible, le "tirage faible à pile ou face", dans le modèle standard du calcul quantique. Carlos Mochon a donné une preuve d'existence d'un tel protocole avec un biais arbitrairement petit. Nous donnons une interprétation claire de sa preuve, ce qui nous permet de la simplifier et de la raccourcir grandement.

La seconde partie de cette thèse concerne l'étude de méthodes pour prouver des bornes inférieures dans le modèle de la complexité en requête. Il s'agit d'un modèle de complexité central en calcul quantique dans lequel de nombreux résultats majeurs ont été obtenus. Dans ce modèle, un algorithme ne peut accéder à l'entrée uniquement qu'en effectuant des requêtes sur chacune des variables de l'entrée. Nous considérons une extension de ce modèle dans lequel un algorithme ne calcule pas une fonction, mais doit générer un état quantique.

Cette généralisation nous permet de comparer les différentes méthodes pour prouver des bornes inférieures dans ce modèle. Nous montrons d'abord que la méthode par adversaire "multiplicative" est plus forte que la méthode "additive". Nous montrons ensuite une réduction de la méthode polynomiale à la méthode multiplicative, ce qui permet de conclure à la supériorité de la méthode par adversaire multiplicative sur toutes les autres méthodes.

Les méthodes par adversaires sont en revanche souvent difficiles à utiliser car elles nécessitent le calcul de normes de matrices de très grandes tailles. Nous montrons comment l'étude des symétries d'un problème simplifie grandement ces calculs.

Enfin, nous appliquons ces formules pour prouver la borne inférieure optimale du problème Index Erasure, un problème de génération d'état quantique lié au célèbre problème Isomorphisme de Graphes.

Abstract

This dissertation studies two different aspects of two-player interaction in the model of quantum communication and quantum computation.

First, we study two cryptographic primitives, that are used as basic blocks to construct sophisticated cryptographic protocols between two players, e.g. identification protocols.

The first primitive is "quantum bit commitment". This primitive cannot be done in an unconditionally secure way. However, security can be obtained by restraining the power of the two players. We study this primitive when the two players can only create quantum Gaussian states and perform Gaussian operations. These operations are a subset of what is allowed by quantum physics, and plays a central role in quantum optics. Hence, it is an accurate model of communication through optical fibers. We show that unfortunately this restriction does not allow secure bit commitment. The proof of this result is based on the notion of "intrinsic purification" that we introduce to circumvent the use of Uhlman's theorem when the quantum states are Gaussian.

We then examine a weaker primitive, "quantum weak coin flipping", in the standard model of quantum computation. Mochon has showed that there exists such a protocol with arbitrarily small bias. We give a clear and meaningful interpretation of his proof. That allows us to present a drastically shorter and simplified proof.

The second part of the dissertation deals with different methods of proving lower bounds on the quantum query complexity. This is a very important model in quantum complexity in which numerous results have been proved. In this model, an algorithm has restricted access to the input: it can only query individual variables. We consider a generalization of the standard model, where an algorithm does not compute a classical function, but generates a quantum state.

This generalization allows us to compare the strength of the different methods used to prove lower bounds in this model. We first prove that the "multiplicative adversary method" is stronger than the "additive adversary method". We then show a reduction from the "polynomial method" to the multiplicative adversary method. Hence, we prove that the multiplicative adversary method is the strongest one.

Adversary methods are usually difficult to use since they involve the computation of norms of matrices with very large size. We show how studying the symmetries of a problem can largely simplify these computations.

Last, using these principles we prove the tight lower bound of the Index Erasure problem. This a quantum state generation problem that has links with the famous Graph Isomorphism problem.

Acknowledgements

When I started my thesis I knew I would end somewhere one day. I knew I was beginning a journey, but I had no idea how difficult it would be, where it would lead me, and what I would end up discovering about sciences and about myself. But I knew I would neither get lost, neither give up, because I was not alone. And I wish here to acknowledge people and organizations that helped me.

First of all, I want to thank my two supervisors, Frédéric Magniez and Nicolas Cerf. Nicolas introduced me to the fascinating field of quantum cryptography with continuous variables that I immediately appreciated. Nicolas also taught me the importance of physical intuition over mathematical formalism to explore new territories. He was of constant support and eager to follow me to discover them. This passion for exploration was also shared by Frédéric, and he helped me to always move forward and discover the greater picture. He helped me to organize my thoughts and to try to keep a clear mind focused and sharp.

I really appreciated how they both let me a great freedom and encourage me to challenge myself: I was able to choose my research subjects and my coauthors, and discover other way to perform research in the numerous travels they fully supported: USA, Canada, Spain, Japan, Egypt, Singapore, Switzerland. This really was an amazing journey!

I want to acknowledge the support of the Région Île-de-France for my travels between Paris and Brussels and thus making me feel part of both teams: the Algo group in Paris and the QuIC in Brussels.

In Paris and Brussels, I had a great pleasure to share office, ideas and laughters with Raúl, Joachim, Julien, Louis-Philippe, Xavier, Marc, Mathieu, Antoine and André.

I also want express my gratitude to all the members of the jury, in particular to Pascal Koiran and Peter Høyer, for reading carefully this manuscript and giving to me a very valuable feedback.

My gratitude goes to all my collaborators. Each of them brought me something and had faith in me: Anthony Leverrier, Andris Ambainis, Martin Rötteler, Jérémie Roland, Dorit Aharonov, Maor Ganz, Iordanis Kerenidis, and of course Nicolas Cerf and Frédéric Magniez.

In particular, I want to thank Jérémie Roland again. He was in the same office than me when I started my PhD, and I then went to meet him five times in the USA. During two summers I was intern at NEC Laboratories America under his supervision. These were two marvelous summers, full of joy and productivity.

Last, I would not be able to finish this thesis without the love and support from my family and my friends.

List of publications

This dissertation is based on the following publications:

[MMLC10] Loïck Magnin, Frédéric Magniez, Anthony Leverrier, and Nicolas J. Cerf. Strong no-go theorem for Gaussian quantum bit commitment. *Physical Review A*, Rapid communications, 81:010302, 2010. arXiv:0905.3419, doi:10.1103/PhysRevA.81.010302

[ACG+11] Dorit Aharonov, André Chailloux, Maor Ganz, Iordanis Kerenidis and Loïck Magnin. A simpler proof of existence of quantum weak coin flipping with arbitrarily small bias. *In submission*, 2011.

[AMR+11] Andris Ambainis, Loïck Magnin, Martin Roetteler, and Jérémie Roland. Symmetry-assisted adversaries for quantum state generation. In *Proceedings of the 26th Annual IEEE Conference on Computational Complexity*, pages 167–177, 2011. IEEE Computer Society. arXiv:1012.2112, doi:10.1109/CCC.2011.24

[MR11] Loïck Magnin and Jérémie Roland. Quantum adversary lower bounds by polynomials. *Technical report* 2011-TR080, NEC Laboratories America, Inc., 2011

Contents

1 Introduction

1.1 Quantum disruption in information sciences

The first time that quantum physics poked around information sciences was in 1970 when Stephen Wiesner proposed a scheme for unforgeable "quantum" banknotes. This idea got mostly ignored and published only in 1983 [Wie83] but inspired the design of quantum key distribution, one of the greatest success of quantum cryptography.

The other active branch of quantum information takes its root in a proposal by Richard Feynman to use quantum effects to speed up some computational tasks. He actually proposed to use some quantum systems in order to perform efficient simulations of some other quantum systems for which classical computers seemed unable to do in a reasonable time [Fey82]. The consequences of this idea reach much further than the domain of numerical simulation. What he proposed is actually another model of computation.

Quantum information brought a new view on many aspects of computer sciences and revealed unsuspected possibilities.

1.1.1 Spooky

Quantum computation differs from classical computation at its very core level: it does not manipulate bits, but a quantum equivalent, qubits, that have "spooky" properties. A bit, can takes only two values, that we will denote by $|0\rangle$ and $|1\rangle$. A randomized algorithm, i.e. an algorithm that will use some random bits as resources, like the Miller-Rabin primality test [Rab80], is mathematically described by a probabilistic bit, that takes value $|0\rangle$ with probability p and value $|1\rangle$ with probability $1 - p$.

> A bit can be compared to an on/off switch that takes only two values 0 or 1, whereas a probabilistic bit will be a dimmer switch that can take all the values between 0 and 1.

Quantum bits, or qubits, are a generalization of probabilistic bits: instead of being constrained in one dimension, they are two-dimensional objects in a space where $|0\rangle$ and $|1\rangle$ are interpreted as orthonormal vectors, and are described by the *superposition* $\alpha|0\rangle + \beta|1\rangle$ with $|\alpha|^2 + |\beta|^2 = 1$. Note that the parameters α and β do not represent probabilities hence can be negative.[1]

> To continue the switch metaphor, a qubit can be compared to a wheel with a mark that one would see from the side. The wheel switch is "1" when the mark is on top, "0" when the mark is at the bottom. The main difference with the dimmer switch is that to go from "1" to "0", there are now two distinct paths depending if the wheel turns clockwise or not. (See Figure 1.1)

[1] actually they are even complex numbers, but we do not discuss it here for the simplicity of the example.

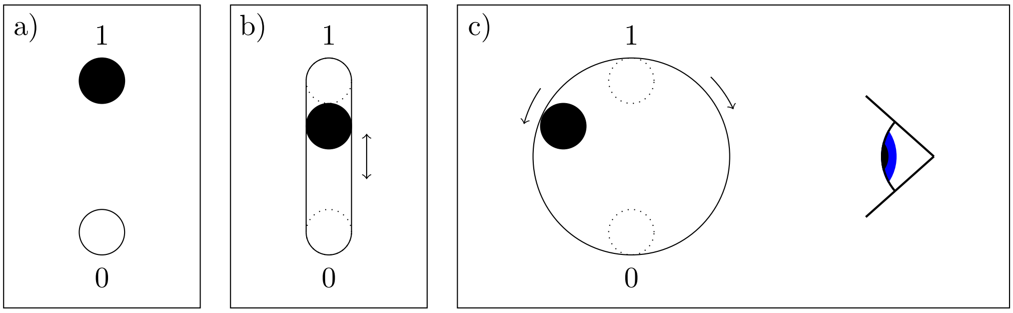


Figure 1.1: a) Schematic representation of an on/off switch on the 1 position. b) Representation of a dimmer switch in an intermediate position between 0 and 1. c) Representation of a "quantum wheel" switch. When seen from the side a quantum wheel switch seems identical to a dimmer switch.

Although in many aspects, quantum bits and probabilistic bits seem to have similar behaviors, they are not equivalent. For example, it is possible to create a $\sqrt{\text{NOT}}$ gate with quantum bits.

> We want to find an operation on the switch that when we applied it twice inverts the position of the switch. A switch in position 0 will ends up in position 1. After a few thoughts, it is easy to realize that no such operation can exist with determinist or probabilistic switches. But we can create it with a quantum switch: rotate the disc by an angle of 90°. When applied twice, the disc makes a half turn, thus turning a 0 into a 1.

This notation can be extended to strings: a classical string s is denoted by $|s\rangle$ and a quantum string is in general a superposition of classical strings. A quantum string is of the form $\sum_s \alpha_s |s\rangle$ with $\sum |\alpha_s|^2 = 1$, for example this is a 4-qubit string composed of the superposition of two 4-bit strings: $1/\sqrt{2}|0000\rangle + 1/\sqrt{2}|1111\rangle$.

The most spooky behavior though, is the EPR paradox, named after Einstein, Podolsky and Rosen who first published about it [EPR35].

> Two entangled discs can be represented as two spatially separate discs in the same position but it is impossible to describe the positions of the two discs individually. It is only known that they are in the same position. For example the state of the two discs after a person made a rotation on one disc is exactly the same as if the rotation would have been applied to the other disc.

Einstein, Podolsky and Rosen called this phenomenon a "spooky action at a distance" and even concluded that we were missing parameters, a hidden variable, in the study of quantum systems. Bell later showed that this was not the case and that quantum physics defeats one's imagination [Bel64].

This is then not surprising that entanglement is one of the most useful resource in quantum computation since the interactions between two players can be enhanced by it.

1.1.2 Surprise

In 1984, Charles Bennett and Gilles Brassard published a quantum key distribution (QKD) protocol in which two parties, usually called Alice and Bob, can communicate over a channel with unconditional security if they both have some quantum resources [BB84]. Even if the complete proof of the unconditional security took more than two decades to be fully completed [SP00, Ren05], the simplicity of the protocol and the elegance of the ideas behind it were powerful enough to start the field now known as quantum cryptography. To really understand why this announcement was such a surprise, one has to realize that up to that time, unconditional security has been considered as an impossible task to achieve, and the security of the protocols were always relying on hardness assumptions, e.g. on the hardness of FACTORING and DISCRETE LOG, or human trust.

Entanglement A surprising fact about the BB84 protocol is that the interaction between Alice and Bob does not use entangled states. Although Ekert proposed another protocol for QKD [Eke91] in which the main resource is entangled states shared between Alice and Bob, this formulation was later shown to be equivalent to the BB84 protocol and the proofs of security are generally based on this approach. For a recent review on QKD, one could read [SBPC+09].

1.1.3 Enthusiasm and fear

Communication is not the only domain in which quantum resources proved to be powerful; they also play an important role in computation. Undoubtedly the main result in quantum computation is the seminal algorithm by Peter Shor to factorize an integer in polynomial time [Sho94], whereas no classical polynomial time algorithms are known. As an immediate consequence, anyone with a quantum computer can break all of the current cryptographic protocols that are based on the hardness assumption of FACTORING or DISCRETE LOG. The FACTORING problem is not believed to be in P, but is neither NP-complete nor coNP-complete (unless a cataclysmic collapse of the polynomial hierarchy occurs). Thus we do not know for certain that a quantum computer is more powerful for factoring integers. Proving the higher computational power of a quantum computer over a classical one is done by finding *separations*, i.e. problems for which we can prove that a quantum algorithm exists with lower complexity than any classical algorithm. Proving separations for time complexity is probably the biggest challenge in theoretical computer science nowadays. This is why, as a first step, it is interesting to prove separations in more constrained models.

The other major results that shaped up the field is the discovery in 1996 by Lov Grover of an algorithm to find an element in a unordered list [Gro96] quadratically faster than any classical algorithm.

Quantum computation also proved to be efficient for evaluating tree formulae. The objective is to evaluate a Boolean formula where the inputs are given by the leaves of a tree, and the nodes are Boolean gates. Consider for example the balanced NAND-tree formula with N leaves, (all the branches of the tree have the same size, and the nodes are NAND gates), the deterministic complexity is $\Theta(N)$, the randomized one is $\Theta(N^{0.754})$ [SW86] and the quantum one $\Theta(N^{0.5})$ [FGG08, Amb09].

1.2 Scope and motivations

1.2.1 Gaussian quantum key distribution

Quantum key distribution started to shape up the field of quantum cryptography. There are currently many competing protocols, hundreds of papers devoted to prove the security of the many variants, a dozen of teams building hardware to create QKD enabled networks (optical fibers, quantum memory, repeaters, lasers) for large-scale deployment. In the last decade some startups started selling QKD devices for some niche markets. As a witness that this field has gained maturity, some researchers are now trying to hack theses devices, that is finding errors in the *implementation* of QKD protocols [GLLL+11].

The theoretical work on perfect QKD protocol is very mature currently, so the efforts are now focused on proposing and analyzing real life schemes. A new set of problems are emerging from this shift of focus, for example how to bypass the low efficiency of single photon detectors. A first answer has been proposed independently by Ralph [Ral99], Hillery [Hil00] and Reid [Rei00] who introduced protocols using continuous variables. This idea comes from physicists for whom it is very natural to manipulate quantum systems described by continuous variables whereas computer scientists are more used to discrete variables. As a matter of fact, many physical quantities are accurately described by continuous variables such as the position and the momentum of a particle or the amplitude of the electromagnetic field.

The key idea of using continuous variables (CV) and the so-called *homodyne* detection that measures the amplitude of a pulse of light with high accuracy and efficiency whereas all the previous protocols required photon detectors that are quite inefficient. Nicolas Cerf, Marc Lévy and Gilles Van Assche proposed a protocol that uses only Gaussian states [CLVA01] to performed quantum key distribution, that was later refined by Frédéric Grosshans and Philippe Grangier [GG02]. Gaussian states are a subset of CV states that have many advantages for practical implementation as for theoretic analysis: they are produced by a laser and can be transmitted using current telecom technologies, they can be easily manipulated in a laboratory, at least for a restricted set of operations, unimaginatively called Gaussian operations, and have a very well defined mathematical formalism. Indeed, Gaussian states can be represented by a “small” number of parameters whereas in general a CV state is characterized by an infinite number of parameters. Good introductions to quantum information with continuous variables can be found in [BvL05, CLP07].

This is how I came to study continuous variables and most noticeably Gaussian variables. Several variations of GG02 have been introduced, one of them in [WLB+04]. During my master thesis I studied a restricted class of attacks [Mag06] against this protocol, later turned into an article [SMGPSC07]. Complete security has subsequently been proved in [GPS07, RC09].

Contrarily to cryptographic purposes for which Gaussian states and operations enable perfect key distribution, Gaussian states and operations are not useful for computational tasks. Indeed they are not universal for quantum computation and can be simulated in polynomial time with classical computers [BS02, BSBN02].

1.2.2 Cryptographic primitives

Quantum cryptography is not limited to key distribution. Another important task is secure two-party function evaluation (2PFE). Unlike in QKD the two players, Alice and Bob, do not trust each other. Alice has an input x_A and Bob x_B and they want to compute $f(x_A, x_B)$ without revealing their inputs [Yao82].

> A popular example is the Millionaire's problem. Alice and Bob are two millionaires and they want to determine which one is the richest, without revealing how much each of them own.

The range of applications to secure two-party function evaluation is gigantic in our Internet era: secure authentication, identification, voting, and function evaluation, to cite a few. In order to create protocols for general 2PFE, we use subroutine protocols that perform a restricted class of secure function evaluation. These protocols are then used as building blocks for creating more general protocols.

We want to pinpoint that two-party secure computation can be implemented in a totally secure manner if there is a trusted third party, though it is of crucial importance not to rely on this trick since third parties can be bribed or corrupted. All current cryptography on the Internet is based on trusted third parties, and History shows we cannot rely on them. The latest example being the DigiNotar affair. DigiNotar signs identification certificates. When a user visits a website over SSL, the website sends a certificate to prove its authenticity. If the certificate is signed by a trusted authority, the browser lets its user go. DigiNotar servers got hacked and fraudulent certificates have been issued, that have been actively used to spy on people[2].

1.2.3 Query complexity

The most studied model in quantum computing other than time is the query complexity model. This model can be described as a two-player interaction. Player A, the algorithm, wants to compute a function f on an input x known only by Player B, the oracle. The communication between the algorithm and the oracle is strongly constrained: the algorithm can only ask questions of the form "what is the i-th bit of x?" and has to pay a 1$ fee per question (query). In a quantum setting, the queries can be made in superposition. The *query complexity of an algorithm* that computes a function f is the amount of money payed by the algorithm to the oracle. The *query complexity of a function* f is the minimum over all the algorithms of their query complexity, hence the query complexity of an algorithm is an upper bound on the query complexity of the function. Note that this is a worst-case complexity scenario: we are interested in the complexity of computing $f(x)$ for every x. This model restricts the design of algorithms in a certain way for which we can prove lower bounds. It proved itself extremely useful for showing separations and the optimality of certain algorithms, both in classical and quantum computing. For instance, consider the problem of sorting n elements. If an algorithm can only make comparisons between two elements, then it has to make $\Omega(n \log n)$ comparisons to sort them all.

First results in quantum query complexity The first separation came around the same time as BB84, when David Deutsch exhibited [Deu85] a (very artificial) problem, now known as the Deutsch's problem: a quantum computer can solve it in one single query, whereas two queries are needed by a classical one. This separation is not dramatic, but was the first one

[2] http://www.vasco.com/company/press_room/news_archive/2011/news_diginotar_reports_security_incident.aspx

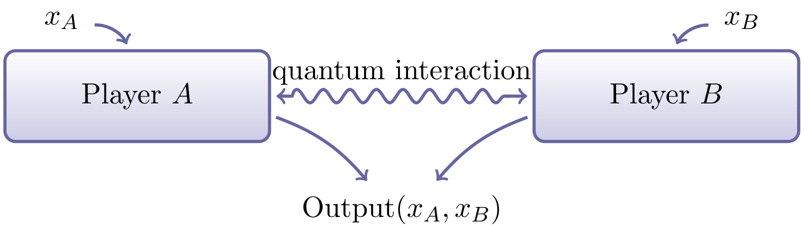
to be exhibited. It has been generalized by Deutsch and Josza [DJ92] and is now known in the improved form by Cleve *et al.* [CEMM98] as the Deutsch-Josza's problem: the input is a Boolean string x of length N with the promise that x is either a constant string (all the bits of the string are identical) either balanced (half of them are 0, half of them 1). The goal of the algorithm is to determine which one it is. They show that there is a one-query quantum algorithm that solves it with no error, whereas classically $N/2+1$ queries are needed. Unfortunately this huge separation does not hold in the probabilistic case when allowing bounded error, for which the separation is constant.

Similar problems with their quantum algorithms were later introduced, for example the Bernstein-Vazirani algorithm [BV97] which is the first exponential separation in query complexity between a quantum algorithm and a probabilistic one, or Simon algorithm [Sim97]. The main tool of Simon algorithm is the Fourier transform over the groups $\mathbb{Z}_2^k$. Shor's algorithm for factoring integers previously mentioned generalizes this idea to Fourier transform over $\mathbb{Z}_n$. All of these problems can be seen as instances of a more general problem, called the Hidden Subgroup problem (See e.g. [Joz98]).

Quantum proofs for classical problems Another implication of the study of quantum complexity, which will not be considered in this manuscript but is worth mentioning, is the fact that quantum arguments can help understanding classical computing. Some purely classical results have quantum proofs much simpler than their classical counterparts ([DdW11] is a good survey on this topic). This is even true by considering continuous variables like the very recent proof of #P completeness of the permanent by Scott Aaronson [Aar11] which uses linear optics arguments, in strong contrast with the arithmetic proof in the celebrated paper by Valiant [Val79].

1.2.4 Outline of this dissertation

In this dissertation, we will analyze two-player quantum interaction from two different points of view: cryptographic primitives and query complexity. As a matter of fact, even if these two domains may look different, they can be cast in the following very general setting: two players A and B each have an input x_A and x_B and they want to output a common answer $output(x_A, x_B)$. This output can be a quantum state $|\psi(x_A, x_B)\rangle$, a distribution $\mu(x_A, x_B)$, or a deterministic value $f(x_A, x_B)$. This thus encompasses quantum state generation problems, computing a function, and even two-party secure function evaluation. This is schematically represented by the following figure:



In Chapter 2, we successively introduce the models of quantum computation that we will consider in this dissertation, namely discrete variables (the standard model of quantum computation), the continuous variables model and its interesting subset: Gaussian variables.

Part I is devoted to analyze cryptographic primitives. In this setting, there is no restriction on the quantum interaction, but some security properties should be satisfied, for example if one player is dishonest, the outcome should remains correct. We examine two primitives: bit commitment in Chapter 3 for which we extend the impossibility from the discrete variable model to the Gaussian one. We then examine a weaker primitive, weak coin flipping, in Chapter 4 and prove the existence of a protocol with arbitrary small bias. These results are summarized in Section 1.3.

Part II studies lower bounds in quantum query complexity. In this setting, player A represents the algorithm, and player B the oracle, the only player to have an input. The quantum interaction is limited to queries to the oracle. In Chapter 5 we examine the different methods used for proving lower bounds on the quantum query complexity and give relationships between them. Finally in the last Chapter we compute a tight lower bound for a problem called Index Erasure. These results are summarized in Section 1.4.

1.3 Quantum primitives

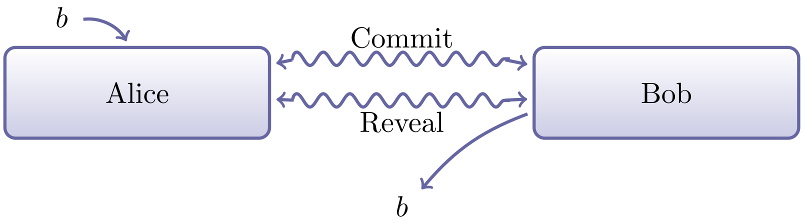
In this dissertation, we are interested in two-party primitives involving dishonest players, without the help of a third-party. There is no notion of privacy against an eavesdropper here. This is a different setup from key distribution where two honest players are trying to prevent a third one to spy on them. We focus our study on two primitives, bit commitment and coin flipping.

1.3.1 Bit commitment

Bit commitment (BC) is a universal primitive in quantum computing. It means that if one uses a perfectly secure BC protocol, one can do perfectly secure two-party function evaluation for any function. This situation is rather surprising since BC is not universal in classical computing. However, there exists another primitive, called oblivious transfer, that is universal for both, classical and quantum computation [BBCS92]. Bit commitment is a protocol that happens in two steps. In the first one, called the *commit phase*, Alice commits to a bit to Bob that she later reveals in the second phase, the *revealing phase*. A bit commitment protocol is said to be secure if it prevents both players to cheat, namely, during the revealing phase Alice cannot change the value of the bit she had committed to, and Bob cannot learn information about that bit before Alice reveals it. A traditional picture for this protocol is as follows:

> Alice locks a secret bit into a safe that she gives to Bob; then, when she wants to reveal her secret, she simply hands over the key of the safe to Bob. The protocol is secure if Bob cannot open the safe without the key, and if Alice cannot change her secret while Bob has the safe, for example using a remote false bottom system.

Bit commitment is an instance of our model of two-player interaction with two security properties: Bob cannot know b at the end of the commit phase, and he outputs b even if Alice cheats.



No-go theorem This primitive has been exhaustively studied in classical cryptography, where the security relies on unproven computational assumptions [Nao91, Cha87]. The idea of quantum bit commitment (QBC) was first introduced by Bennett and Brassard in 1984 [BB84], together with their quantum key distribution protocol. There were hopes that the ideas that made QKD possible would also work for QBC, although they also exhibited an attack on this first protocol. In 1993, Brassard *et al.* proposed a QBC protocol known as BCJL [BCJL93], which was believed to be secure until 1997, when Mayers [May97] and independently Lo and Chau [LC97] proved that it was not the case. Their proof involved a reduction of the BCJL protocol to a purified protocol, which cannot be perfectly secure against both Alice and Bob. A few months later, it has been realized that this reduction is general enough and applies to all QBC protocols. It ruled out the existence of an unconditionally secure QBC protocol. Because of the complexity of this reduction, however, it was not universally accepted (see, e.g., [Yue00]) until 2007, when d'Ariano *et al.* provided a complete, formal description of QBC protocols that definitely closed the question [DKSW07]. The proof was written for discrete variables, but it appeared that it was also valid for continuous variables. This result is known as the *no-go theorem* for quantum bit commitment.

This theorem is in fact a lower bound on the relation between the degree of concealment and bindingness, whereas insecure protocols provide upper bounds. The optimal security parameter with a quantum bit commitment attaining it have been proven by Chailloux and Kerenidis [CK11].

Circumventing the limitations The role of the *model* of security is a central notion: the no-go theorem is proven under the strong assumption that Alice and Bob have all the resources allowed by quantum mechanics. The no-go theorem is not true in other models, for example if one uses special relativity [Ken99, Ken11], or difficulties in building the hardware necessary to perform QBC. This is a very active research area and one of the greatest results are in the so-called bounded storage [Sch07] and noisy storage models [WST08]. The basic idea is obtained from a key observation: if Bob measures the quantum state he has at the end of the commit phase, the entanglement between Alice and Bob is broken, thus limiting her ability to cheat. Hence there are protocols for which forcing Bob to make a measurement are secure. The incentive to measure is done by considering practical implementation constraints, in this case the difficulty to construct efficient memories. The bounded storage model considers that Bob does not have enough memory to store all the qubits exchanged during the committing phase, thus needs to measure the ones he cannot store. The noisy storage model is a refinement of the latter: by knowing some practical limitations of the memory, mainly the amount and type of noise it adds per unit of time, it is possible to bound the amount of information that Bob loses and thus to perform a secure protocol.

Contributions We are considering a scenario quite similar to the bounded storage model, based on restraining Alice's and Bob's abilities, but the impossibility result remains here. In Chapter 3, guided by the ease of implementation of Gaussian variables, we investigate Gaussian quantum bit commitment. The original idea begins with the observation that with current technologies, only Gaussian deterministic operations are easily accessible. Thus, this limits the cheating capabilities of dishonest players, and the no-go theorem may not apply with this additional restriction. We consider the model in which Alice and Bob have at their disposal only Gaussian resources. We show that unfortunately the impossibility of bit commitment remains in this fully Gaussian model.

The result by Mayers, Lo and Chau starts by transforming any protocol into an equivalent protocol in term of security. Such protocol is non-interactive and happens as follows: first, Alice prepares a bipartite state $|\psi_b\rangle$ if she wants to commit to the bit b, and sends one part to Bob as the commit phase. The revealing phase consists of Alice sending the other part of $|\psi_b\rangle$. Thus, as the end of the protocol Bob holds $|\psi_0\rangle$ if Alice is committed to "0" or $|\psi_1\rangle$ otherwise. The protocol ends by Bob measuring the state he is holding.

The degree of concealment of the protocol, intuitively the probability that Bob can cheat, is related to Bob's efficiency to distinguish if he received a part of $|\psi_0\rangle$ or $|\psi_1\rangle$. Since Bob does not hold the entire state, he only has a partial view on it. We will later formalize this notion by the concept of *mixed states*. The less distinguishable the partial views of these two parts, the more concealing the protocol. Conversely, the more those partial views are distinguishable, the less Alice can convince Bob of the other outcome. There are different ways to express the distinguishability of two states (we detail some of them in Section 2.4), one is the fidelity. This is a mathematical function that quantifies how alike two states are. The fidelity of two identical states is 1, when they are totally distinguishable the fidelity between them is 0.

The proof of the insecurity is first performed for perfectly concealing protocols. Using direct techniques, Mayers, Lo and Chau proved that in this case, Alice has total control over the outcome of the protocol by applying the right transformation of the qubits she kept. The general case, not perfectly concealing protocols, is then reduced to the previous one. The main mathematical tool is Uhlmann's theorem who states that given two partial views ρ_0, ρ_1 of two different states, there exist two quantum states $|\psi_0\rangle$ and $|\psi_1\rangle$, such that ρ_0 and ρ_1 are also respectively the partial views of $|\psi_0\rangle$ and $|\psi_1\rangle$, and moreover they have the same distinguishability than $|\psi_0\rangle$ and $|\psi_1\rangle$. Those two states are the states that Alice needs to prepare in order to have a successful cheating strategy.

Our proof of the impossibility of Gaussian quantum bit commitment follows the same footsteps. Using the power of Gaussian formalism, we first prove the perfect case (Section 3.2.1) and we then perform a reduction from the approximate case to the perfect one (Section 3.2.2). This is where our proof differs from the previously published one. We cannot use Uhlmann theorem for one main reason, contrary to the discrete case, there is no constructive proof of the purifications. This has two consequences: we cannot exhibit a cheating strategy in this case, we simply have its existence, and we are not able to prove that the cheating strategy is Gaussian.

To overcome this problem we introduce a new notion of *intrinsic purifications* in Section 3.1 with the two properties we need: intrinsic purifications of Gaussian states are Gaussian, and the fidelity between two states is roughly the same than the one between their intrinsic purifications (Theorem 3.1). Although our theorem is a bit weaker than Uhlmann's theorem, we are able to prove the same level of security than previous proofs.

This work was started during my master thesis [Mag07] and completed with the joint work of Frédéric Magniez, Anthony Leverrier and Nicolas J. Cerf [MMLC10].

1.3.2 Coin flipping

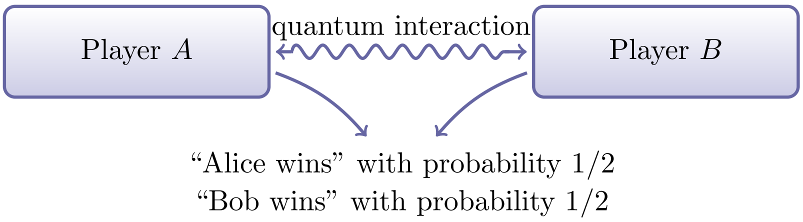
The impossibility result of quantum bit commitment is a bit disappointing since the extra power offered by quantum physics is of no use there. Happily, we can use it to perform a weaker cryptographic primitive, coin flipping. We say that a primitive P is weaker than Q if we can construct a secure protocol for P from a secure protocol for Q. This is why in this dissertation we focus on weak coin flipping.

Strong and weak Coin flipping comes in two flavors. In a *weak coin flipping* protocol, Alice and Bob should flip a coin (or a bit) at distance, it means that all their communications are done through a (quantum) channel. Originally this primitive has been referred as coin flipping by telephone. Alice wins if the outcome of the protocol is 0, Bob if it is 1. The folklore metaphor to explain weak CF is the following:

> Alice and Bob's love story has ended and they now live in separate houses. Both of them want to keep the car, so decide to flip a coin to determine a winner. Bob refuses to use an attorney to do it, afraid that Alice may bribe him. They decide to flip the coin on the phone.

The protocol is *sound* if when both players are honest, the probability that each of them wins is 1/2. The bias of the protocol is defined by the excess of probability that one player wins when the other player follows the protocol (i.e. the other player is honest). The protocol is *ε-secure* if there is the bias is at most ε.

Once again, a weak coin flipping protocol, can be viewed in our model of quantum interaction. The security property is now that the probability of one of the players to win remains close to 1/2 even if he cheats.


Player A
quantum interaction
Player B
"Alice wins" with probability 1/2
"Bob wins" with probability 1/2

This primitive is called *weak* since there are no constraints on the bias when losing, a protocol can be secure even though Alice could force the outcome to be 1, i.e. Alice decides to let Bob win. A *strong* coin flipping protocol adds such a constraint. As a consequence of this definition, weak coin flipping is weaker than strong coin flipping, and thus also weaker than bit commitment since there is a short reduction from strong coin flipping to BC: Alice randomly picks a bit a and commits to it. Bob picks a random bit b and publicly announces it, finally Alice unveils a, and the outcome of the protocol is the random bit $a \oplus b$.

In the classical setting, coin flipping has first been introduced by Blum [Blu83] and the security of classical protocols relies on computational assumptions, exactly like bit commitment. Without this requirement a cheating player could always decide the outcome of the protocol against a honest player.

	Classical	Quantum
Bit commitment	$1/2$	$0.239+\varepsilon$
Strong coin flipping	$1/2$	$0.207+\varepsilon$
Weak coin flipping	$1/2$	ε

Table 1.1: Optimal bias for three cryptographic primitives, in classical and quantum settings for unconditional security (no restriction on the model). The parameter ε can be arbitrary small.

Bounds for quantum coin flipping The study of the bias of coin flipping protocols in the quantum setting is particularly interesting. Lo and Chau [LC98] proved the impossibility of perfect strong coin flipping protocols, that is protocols with bias 0, whether protocols with bias guaranteed to be less than 1/2 (no player can cheat perfectly) exist remained open.

Ambainis proved that a weak coin flipping protocol with bias ε should have a least $\Omega(\log\log\frac{1}{\varepsilon})$ rounds, thus ruling out the possibility of perfect weak coin flipping. On the positive side, there were several simple protocols with bias 1/4 [SR01, Amb04, KN04]. Spekkens and Rudolph were the first ones to have a protocol with a smaller bias since they found a protocol with cheating probability $1/\sqrt{2}$ [SR02]. In a remarkable series of work, Carlos Mochon first discovered protocols with bias 1/6 [Moc05] and even a “protocol” that achieves arbitrarily small bias [Moc07].

The status of the paper by Mochon [Moc07] is quite peculiar. It is an 80-page long paper, extremely technical and never peer-reviewed. Inspired by techniques from Kitaev, Mochon writes the bias of weak coin flipping protocols as semidefinite programs and their duals. He then shows that these duals are equivalent to another model he calls *point games*. In a last step he exhibits a point game achieving arbitrarily small bias. There is a way to turn a point game into a protocol but Mochon actually never does it, since it is too complicated and the protocol would have no possibility of practical implementation. Moreover the protocol would not give any intuition on the reason why it performs so well.

For strong coin flipping, Aharonov *et al.* [ATSVY00] first discovered a protocol with bias 0.41, thus showing the superiority of quantum over classical cryptography. This result got improved to 1/4 achieved by many protocols [Amb04, SR01, NS03, KN04]. On the lower bound side, Kitaev [Kit03] proved that no protocol can have a bias smaller than $1/\sqrt{2}-1/2$ using semidefinite programming. A simple proof can be found in [ABDR04]. This gap has been closed by Chailloux and Kerenidis [CK09] when they showed a classical reduction from any weak coin flipping with bias ε to a strong coin flipping protocol with bias at most $1\sqrt{2}-1/2+2\varepsilon$. This result reinforced the motivation to have a clearer proof of the possibility of weak coin flipping than the current writing of Mochon. We summarize the tights bounds on the bias for bit commitment, strong and weak coin flipping in classical and quantum settings in Table 1.1.

Contributions Checking the validity of the proof of arbitrary small bias weak CF protocol [Moc07] is beneficiary to the community since it has not been, neither will be, submitted to peer-review. This result was almost not understood at all and the scientific community urged to see a simpler proof of Mochon's quantum weak coin flipping.

In Chapter 4 we present an arguably clearer and simpler proof of the existence of quantum weak coin flipping. The original proof is in two parts: first, a model equivalent to weak coin flipping protocols called *time independent point games* is introduced; and the existence of a protocol with arbitrary small bias is shown in this model. This dissertation deals the many steps to prove the equivalence between these two models, the construction of game is left unchanged.

The first step is the introduction of the concept of point games. Consider a protocol, its bias can be expressed as a semidefinite program, that is an optimization over a set of matrices, a *dual feasible point*, that satisfies some constraints. Each dual feasible points leads to an upper bound on the bias of the protocol, and thus is interpreted as a witness of the bias of the protocol. A point game is a graphical representation of a protocol and a dual feasible point. Informally, a point game is a succession of moves of points on a plane, called *transitions*. A point game created from a protocol and a dual feasible points obeys some rules: it starts with two points at coordinates $[0, 1]$ and $[1, 0]$, points can move either horizontally or vertically at every turn, and a the end of the game, there is only one point at coordinate $[1/2 + \varepsilon, 1/2 + \varepsilon]$ where u is an upper bound on the bias of the protocol.

By construction of a point game, the transitions obey a rule called *expressible by matrices* (EBM), and we show that at every point game with EBM transitions and final point $[1/2 + \varepsilon, 1/2 + \varepsilon]$ corresponds a weak coin flipping protocol with bias at most ε. In other words, we construct a protocol and a dual feasible point from a point game. We thus reduce the task of finding a protocol with bias ε to the task of finding a point game with EBM transitions with final point $[1/2 + \varepsilon, 1/2 + \varepsilon]$.

Unfortunately, EBM transitions have one main disadvantage: they are not easy to manipulate, so proving that a transition is EBM is quite a challenge. The problem is mainly that EBM transitions are described by a pair of matrices and a vector, hence it is difficult to give general properties of them. This difficulty is overcome by seeing transitions as functions with finite support. As a matter of fact, EBM functions have an interesting topological property: they form a convex cone. We interpret the dual of this cone as the set of operator monotone functions, and we call *valid functions* the dual of the operator monotone functions. We then show that *valid transitions*, i.e. transitions described by a valid function, are essentially the same as EBM functions. Valid functions have a very simple analytical characterization and checking that a given transition is valid corresponds to checking two simple mathematical statements.

Finally, we introduce the model of *time independent point games* by removing the ordering on the transitions. This can be done easily once again by seeing transitions as functions.

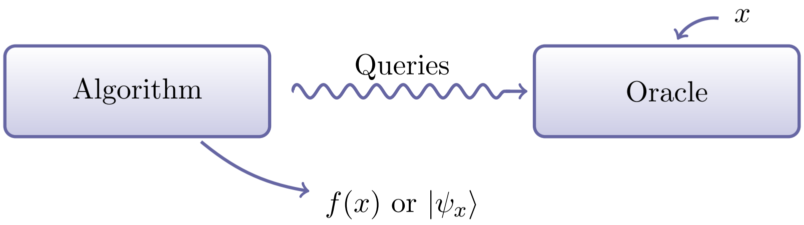
In [Moc07], point games are directly introduced with valid transitions. In this dissertation, we explain how point games with EBM transitions naturally arise and that they should be considered as the equivalent model to protocols with an associated dual feasible point. This observation is at the heart of the new work presented here. As a matter of fact, we now have an explanation on why operator monotone functions pop up, whereas in previous work they just came out of the blue. Moreover with this natural interpretation of valid functions as the bidual of EBM functions, we prove the equivalence between games with EBM transitions and games with valid transitions in about 3 pages with clear topological arguments, whereas the previous proof was a 20-page long appendix full of fairly advanced analysis. Furthermore the fact that we give a reason why we should consider transitions as functions leads to the introduction of time independent point games in a much more meaningful way. Our proof of the equivalence between the different models of point games and protocols is not only shorter and simpler, it also carries a clear explanation of the relation between the different models, their strength and why we need to consider them. We believe that this new proof will help other researchers understand the ideas behind Mochon's result.

For the sake of completeness, Appendix C presents Carlos Mochon's construction of a point game achieving an arbitrarily small bias.

This work is a collaboration with Dorit Aharonov, André Chailloux, Maor Ganz, and Iordanis Kerenidis [ACG+11].

1.4 Lower bounds for quantum query complexity

The query complexity model is also an instance of two-player quantum interaction, where the algorithm aims to compute a function f on a input x accessible only via queries to the oracle. In this dissertation, we generalize this model by considering algorithms that create a quantum state $|\psi_x\rangle$.



There are two main families of methods to prove lower bounds on the quantum query complexity: the adversary methods and the polynomial method. These methods are used to prove lower bounds for computing only a single instance of a function. A related problem is how the number of queries scales if one wants to compute k independent instances of the same function, and will see how to answer that question.

1.4.1 Direct sum and product theorems

The question of the resources needed to compute k instances is interesting and has a very practical importance, for instance for computers that perform very repetitive tasks like web servers that query their database. For example, in order to decrease the load of the database server, queries from independent and simultaneous users could be combined in smart ways. Roughly speaking, direct sum and products theorems are impossibility results on these strategies.

A function is said to obey a *direct sum theorem* if computing k independent instances requires at least $\Omega(k)$ times the amount of resources needed for one instance. In general the resources can be time, memory, communication or queries. In this dissertation, we are focusing our study on the latter. Assume that a problem needs T queries to be solved with success probability σ, then by performing the algorithm k times in parallel, hence using kT queries, the success probability is σ^k and thus decreases exponentially in k. A direct sum theorem leave the possibility that the success probability could decrease slower than exponentially, and thus there may be some gain to combine the queries. If this is not the case, the function obeys a *strong direct product theorem* (SDPT), that is the best strategy to compute k independent instances of the function is simply to repeat the algorithm k times.

There was a plethora of results concerning strong direct product theorems for query complexity in 2011! Andrew Drucker showed that the randomized query complexity of any function obeys a SDPT [Dru11]. Troy Lee and Jérémie Roland using totally different techniques proved the same result for quantum query complexity [LR11]. Alexander Sherstov proved direct product for quantum communication complexity and that the polynomial method, a method to prove lower bounds in the quantum query complexity model, also satisfies a strong direct product theorem [She11].

1.4.2 Adversaries

The basic idea behind the quantum adversary method and its variations is to define a progress function that monotonically changes from an initial value (before any query) to a final value (after the last query), when the algorithm is ready to tell its outcome. The progress function has one main property: its value changes only when the oracle is queried. Then, a lower bound on the quantum query complexity of the problem can be obtained by bounding the amount of progress done by one query.

Original additive The first adversary method was introduced by Ambainis [Amb00] and we will refer to it has the *original adversary* method as a generalization of the "hybrid argument" [BBBV97]. Other adversary methods that are variations on the same principle were subsequently proposed [HNS08, Amb06, BS04, LM08], but were later proved to be all equivalent [ŠS06]. They all rely on optimizing an adversary matrix Γ assigning non-negative weights Γ_{xy} to different pairs of inputs (x, y) to the problem. Consider two inputs x and y such that $f(x) \neq f(y)$ and an algorithm computing the function f. The quantum states corresponding to x and y gradually diverge at each step of the algorithm towards their final value $f(x)$ and $f(y)$, i.e. their scalar product decreases. The progress function is defined as the measurement of this divergence as the weighted average of this scalar products, thus a high weight should be put on pairs of functions hard to distinguish.

It was known that this method cannot always be used to prove tight lower bounds on any problems, since it is limited by the so-called "certificate complexity barrier" [Zha05, ŠS06], that is $\mathrm{ADV}(f) \leq \sqrt{C_0(f)C_1(f)}$ where $\mathrm{ADV}(f)$ denotes the best lower bound proved by the original adversary, and $C_b(f)$ denotes the certificate complexity of f for $f(x) = b$. Let us consider the case of the Element Distinctness problem: given a string of length N, are all the letters of the string distinct? For this problem, the original adversary method cannot prove lower bounds better than $\Omega(N^{1/2})$, since the certificate for a negative instance is a pair of positions of two identical letters, and the one for positive instance is the string itself.

General additive method While originally this method only considered non-negative weights, Høyer, Lee and Špalek later showed that negative weights also lead to a lower bound, which can actually be stronger in some cases [HLŠ07]. In particular, they exhibited an example where this *general additive* method breaks the certificate complexity barrier. A series of work [FGG08, ACR$^+$10, RŠ08, Rei11, LMR$^+$11] culminated by showing that the general adversary bound is tight for the bounded-error quantum query complexity, thus showing the relevance of the general additive adversary method.

The general additive adversary method also suffers from one main drawback: it cannot prove lower bounds for very small success probability and thus cannot be used to prove a strong direct product theorem for the quantum query complexity.

Multiplicative method To circumvent it, Robert Špalek introduced the *multiplicative* adversary method [Špa08] that generalizes some previous ad-hoc methods [Amb05, AŠdW07].

However, Špalek left unanswered the question of how multiplicative and additive methods relate in the case of high success probability. Since the multiplicative adversary method can prove lower bounds for small success probability, Špalek has been able to prove that the bound obtained with this method obeys a strong direct product theorem, but he did not answer the key question, wether or not the quantum query complexity does.

1.4.3 Polynomial method

Method The other main technique to prove lower bounds in the quantum query complexity model is the polynomial method introduced by Beals *et al.* [BBC$^+$01]. Contrarily to the adversary method, the polynomial method can only prove lower bounds for Boolean functions, but has nevertheless achieved tremendous success. One of the most noticeable is, for sure, that the quantum query complexity of a total function cannot be less than $q^{1/6}$ where q is the classical query complexity. In other words, there is no exponential separation between the randomized and the quantum query complexity for total functions.

The polynomial method has also been used to prove lower bounds for specific problems, some of them are not very natural like the *Ambainis function* [Amb06], but it is currently the only method from which lower bounds for Element Distinctness and Collision were derived by Scott Aaronson and Yaoyun Shi [Aar02, Shi02, AS04]. Unfortunately, one issue with those bounds proved by the polynomial method is that they are not very flexible, in the sense that they cannot be adapted to prove lower bounds on natural variations of these problems such that k-Element Distinctness: given a string on some alphabet, is there a letter that appears at least k times?

Other impressive results range from Time-Space trade-offs [KŠdW07], lower bounds for Abelian Hidden Subgroup [KNP07] to a strong direct product theorem for lower bounds obtained by the polynomial method [She11].

Relationship with the adversary methods Since the general additive adversary method is tight for bounded-error quantum query complexity, it is known that the general additive method is stronger than the polynomial method. However an explicit reduction was unknown before the work presented in this dissertation.

It was also known that the polynomial method and the original adversary method were not comparable. Indeed, Aaronson and Shi [AS04] were able to prove a $\Omega(N^{2/3})$ lower bound for Element Distinctness using the polynomial method which breaks the certificate complexity barrier. On the other hand, it is known that the adversary method can sometimes give better lower bounds than the polynomial method, in [Amb06] Ambainis exhibits a function with polynomial degree d and adversary bound $\Omega(d^{1.3})$.

Other cases for which the original adversary bound is stronger than the polynomial bound can be obtained by considering a weaker kind of oracles. Up to now, we have been considering *evaluation* oracles (an oracle returns the value of a letter of the input). It is possible de define a weaker kind of oracles, the *test* oracles. A query to a test oracle is of the form "Is the i-th letter of x the letter a?" The lower bounds obtained by the polynomial method are the same in both cases. Using this observation, Pierre Phillips demonstrated that some problems are easier in an "evaluation" model than in a "test" model, and thus that the original additive is sometimes stronger than the polynomial method [Phi03].

1.4.4 Quantum state generation problems

Even if one is interested in proving lower bounds for functions, it appears that studying a more complex model can actually be very useful. We study a generalization of the query model to include problems in which the input is still a black box, however, the output is no longer a classical value but a *quantum* state.

An example of quantum state generation problem is Index Erasure. Here the input is a string x of length N on an alphabet of size M with the promise that all the letters in the string are different. The task is to prepare the quantum state $\frac{1}{\sqrt{N}}\sum_{i=1}^{N}|x_i\rangle$ using as few queries to x as possible. The name "index erasure" came from the observation that while it is straightforward to prepare the (at first glance perhaps similar looking) state $\frac{1}{\sqrt{N}}\sum_{x=1}^{N}|i\rangle|x_i\rangle$ using a single quatum query, it is quite challenging to forget ("erase") the contents of the first register of this state which carries the input ("index") of the letter.

In particular, quantum state generation has been considered in [AT03] to solve statistical zero knowledge problems, one ultimate goal being to tackle Graph Isomorphism. The quantum state generation problem resulting from the well-known reduction of Graph Isomorphism to Index Erasure would be to generate the uniform superposition of all the permutations of a rigid graph $\mathcal{G}$:

$$|\mathrm{unif}(\mathcal{G})\rangle = \frac{1}{\sqrt{n!}}\sum_{\pi\in S_n}|\mathcal{G}\text{ permuted by }\pi\rangle.$$

By coherently generating this state for two given graphs, one could then use the standard SWAP-test [BCWdW01] to check whether the two states are equal or orthogonal, and therefore decide whether the graphs are isomorphic or not.

Such a method for solving Graph Isomorphism would be drastically different from more standard approaches based on the reduction to the Hidden Subgroup problem, and might therefore provide a way around serious limitations of the coset state approach [HMR+06]. As a matter of fact, Graph Isomorphism is quite a mystery in complexity. Like Factoring this problem is supposed to be NP-intermediate and reduces to an instance of Hidden Subgroup (however Factoring is an instance of Hidden Subgroup problem (HSP) on the cyclic group, but Graph Isomorphism is an instance of HSP on the symmetric group). But there is no known polynomial time quantum algorithm for solving Graph Isomorphism.

1.4.5 Contributions

Quantum state generation The chief technical innovation is the extension of the general additive and the multiplicative adversary methods to quantum state generation problems in Section 5.3. This provides to us a newer view on the adversary method: instead of getting focused on pairs of inputs and their weights in the adversary matrix Γ, we understand that the eigenspaces of the adversary matrix Γ are the key. The progress function can now be seen as a function that monitors the progress done by an algorithm, by looking at which subspaces are supporting the internal state of the algorithm. As a by-product we give elementary and arguably more intuitive proofs of the additive and multiplicative methods, contrasting with some rather technical proofs e.g. in [HLŠ07, Špa08]. This is a crucial observation to prove that the multiplicative method is stronger than both, the general additive method and the polynomial method.

Additive versus multiplicative To compare the strength of the additive and multiplicative adversary methods, we introduce yet another flavor of adversary method which we call *intermediate* adversary method. This method provides lower bounds for quantum state generation problems as well as for classical problems. The intermediate adversary method is a hybridization of the additive and multiplicative methods that uses “multiplicative” arguments in an “additive” setup: it is equivalent to the additive method for large success probability, but is also able to prove non-trivial lower-bounds for small success probability, overcoming the concern [Špa08] that the additive adversary method might fail in this case.

In Section 5.4, we show that for any problem, the intermediate adversary bound lies between the additive and multiplicative adversary bounds, answering Špalek's open question about the relative power of these methods [Špa08]. By considering the Search problem for exponentially small success probability in Chapter 6, we also conclude that the powers of the three methods are *strictly* increasing, since the corresponding lower bounds scale differently as a function of the success probability in that regime.

Polynomial versus multiplicative In Section 5.6.4, we give an explicit reduction from the polynomial method to the multiplicative adversary method. In order to do so, once again an intermediate method, the max-adversary method, yet another type of adversary method whose strength lies between the polynomial method and the multiplicative method.

Directly inspired by the new interpretation of the progress function, this method does not have an adversary matrix, but relies on a sequence of subspaces. The idea behind the max-adversary method is the following: define an ordered set of orthogonal subspaces ($\mathcal{S}_k : 0 \leq k \leq K$) such that any query can only transfer weight from subspace $\mathcal{S}_k$ to its immediate neighbors (i.e. $\mathcal{S}_{k-1}$ and $\mathcal{S}_{k+1}$) and that the initial state of the algorithm has only overlap on $\mathcal{S}_0$. If the final state should have non-zero overlap on subspace $\mathcal{S}_T$ in order to compute a function f accurately, this implies that T is a lower bound on the quantum query complexity of f.

The reduction from the max-adversary method to the multiplicative adversary method follows by considering the multiplicative adversary matrix $\Gamma = \sum_k \lambda^k \Pi_k$, where Π_k is the projector on $\mathcal{S}_k$, and showing that the corresponding multiplicative adversary bound tends to the max-adversary bound when $\lambda \to \infty$. The reduction from the polynomial method to the max-adversary method is done by showing that we can choose $\mathcal{S}_k$ to be a subspace characterized by polynomials of degree k; more precisely, we choose $\mathcal{S}_k$ to be the subspace spanned by the vectors of the Fourier basis of weight k. Let us also note that for any Boolean function, the adversary matrix leading to the same lower bound as the polynomial method does not depend on the function itself. This gives new insight on why the polynomial method does not always provide tight lower bounds.

If we restrict the progress function of the multiplicative adversary to increase by a factor at most c per query, the multiplicative bound can be written as a semidefinite program [LR11]. The best bound is then obtained by maximizing the value of this semidefinite program over all possible c. The reduction from the general additive to the multiplicative method shows that the multiplicative bound degrades into the additive bound in the limit $c \to 1$. In contrast, we can obtain the max-adversary bound by taking the limit $c \to \infty$, which therefore completes the picture of the relations between the different lower bound methods in quantum query complexity (see Fig. 1.2), and shows in particular that all these methods reduce to the multiplicative adversary method.

Our reduction from the polynomial method to the multiplicative adversary method gives

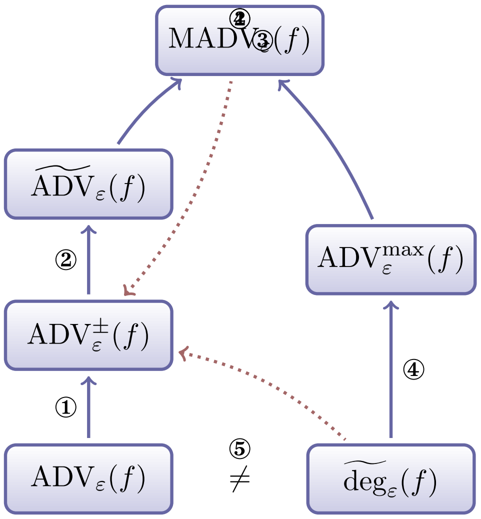

②
MADV③(f)
$\widetilde{\mathrm{ADV}}_\varepsilon(f)$
②
$\mathrm{ADV}^{\max}_\varepsilon(f)$
$\mathrm{ADV}^{\pm}_\varepsilon(f)$
④
①
$\mathrm{ADV}_\varepsilon(f)$
⑤
$\neq$
$\widetilde{\deg}_\varepsilon(f)$

Figure 1.2: Relations between the different methods to prove lower bounds for quantum query complexity. An arrow from method A to method B implies that any lower bound that can be proved with A can also be proved with B (i.e., B is stronger than A). A solid blue arrow means that the reduction is constructive, i.e., we can obtain a witness for B from a witness for A. ① [HLŠ07] ② Section 5.4 ③ [Rei11, LMR+11] ④ Section 5.6.4 ⑤ [Zha05, ŠS06, AS04, Amb06]

new hope to prove lower bounds for problems related to Collision and Element Distinctness. Variations of this problem have practical applications in post quantum cryptography, see e.g. recent schemes for secure communications where the security is based on the hardness of Element Distinctness-type problems [BHK+11].

This work was done in collaboration with Jérémie Roland [AMRR11, MR11].

Applications In Chapter 6 we present two applications of our results. First, we extend the strong direct product theorem for the multiplicative adversary bound [Špa08] to quantum state generation problems (Section 6.1). Since we have clarified the relation between the additive and multiplicative adversary methods, this also brings us closer to a similar theorem for the additive adversary method. The most important consequence would be for the quantum query complexity of functions, which would therefore also satisfy a strong direct product theorem since the additive adversary bound is tight in this case [LMR+11].

Secondly we focus on proving lower bounds using the adversary method. As it has been previously pointed out many interesting problems have strong symmetries [Amb05, AŠdW07, Špa08]. Section 6.2 shows how studying these symmetries helps to address the two main difficulties of the usage the adversary method, namely, how to choose a good adversary matrix Γ and how to bound the progress done by one query. Following the *automorphism principle* of [HLŠ07], we define the automorphism group G of a problem (function evaluation or quantum state generation). To do so, we reduce the adversary method from an algebraic problem to the study of the representations of the automorphism group G.

Finally, we validate our methodology by proving a lower bound of $\Omega(\sqrt{N})$ for the quantum query complexity of Index Erasure in Section 6.4 which is tight due to the matching upper bound based on Grover's algorithm, therefore closing the open problem stated by Shi [Shi02].

To the best of our knowledge, this is the first lower bound directly proved for the query complexity of a quantum state generation problem. The previous bound for Index Erasure was $\Omega(\sqrt[5]{N/\log N})$, proved by a classical reduction to the Set Equality problem [Mid04], which consists in deciding whether two sets of size N are equal or disjoint or, equivalently, whether two injective functions over a domain of size N have equal or disjoint images.

2 Models of quantum information

This Chapter presents two models for encoding quantum information, the standard model using discrete variables (DV), and the so-called continuous variables (CV) model. They share a lot of similarities but are expressed in two different mathematical frameworks: the DV model is in *finite* dimensional Hilbert spaces, whereas the CV model is in *separable infinite dimensional* Hilbert spaces.

2.1 Discrete variables

2.1.1 The Hilbert space $\mathbb{C}^n$

The Hilbert space $\mathbb{C}^n$ is the vector space of n-dimensional complex column vectors with the canonical inner product:

$$\begin{pmatrix} \psi_0 \\ \vdots \\ \psi_{n-1} \end{pmatrix}, \begin{pmatrix} \phi_0 \\ \vdots \\ \phi_{n-1} \end{pmatrix} \mapsto \sum_{i=0}^{n-1} \psi_i^* \phi_i = (\psi_0^*, \ldots, \psi_{n-1}^*) \cdot \begin{pmatrix} \phi_0 \\ \vdots \\ \phi_{n-1} \end{pmatrix},$$

where ψ_i^* denotes the complex conjugate of ψ_i.

In quantum mechanics, vectors and inner products are denoted following the Dirac notation. A column vector $\psi \in \mathbb{C}^n$ is denoted by the ket $|\psi\rangle$ and the complex conjugate row vector ψ^* by the bra $\langle\psi|$. As a consequence $\langle\psi|\phi\rangle$ is the inner product between ψ and ϕ, $|\phi\rangle\langle\psi|$ is the outer product, which is defined as the linear map: $|\chi\rangle \mapsto \langle\psi|\chi\rangle|\phi\rangle$. The projector onto the one-dimensional space spanned by $|\psi\rangle$ is thus denoted by $|\psi\rangle\langle\psi|$.

For $i = 0, 1, \ldots, n-1$, we denote by $|i\rangle$ the vector $(0\ 0 \cdots 0\ 1\ 0 \cdots 0)^T$ where the "1" is in the i-th position. We have $\langle i|j\rangle = \delta_{i,j}$, so $\{|i\rangle,\ 0 \leq i \leq n-1\}$ is an orthonormal basis of $\mathbb{C}^n$. This basis is called the *computational basis* of $\mathbb{C}^n$. Thus a vector $|\psi\rangle$ can be decomposed on the computation basis as $|\psi\rangle = \sum_{i=0}^{n-1} \alpha_i |i\rangle$ with complex probability amplitudes α_i. We will mostly consider spaces whose dimension is a power of 2, and in this case we often alternate between writing the index of a vector in the canonical basis in base 10 and in base 2, for example we could have written the previous decomposition $|\psi\rangle = \sum_{x\in\{0,1\}^{\log n}} \alpha_x |x\rangle$.

Tensor products For $0 \leq i \leq m-1$ and $0 \leq j \leq n-1$, the tensor product between $|i\rangle$ and $|j\rangle$ is the vector $|k\rangle = |i\rangle \otimes |j\rangle$ of the space $\mathbb{C}^m \otimes \mathbb{C}^n \cong \mathbb{C}^{mn}$ where $k = 2^n i + j$, that is the concatenation of the binary expansion of i and j. For example $|010\rangle \otimes |10\rangle = |01010\rangle$. The tensor product is extended by bilinearity to the full spaces $\mathbb{C}^m$ and $\mathbb{C}^n$ by: $(\sum_i \alpha_i|i\rangle) \otimes (\sum_j \beta_j|j\rangle) = \sum_{ij} \alpha_i\beta_j|i\rangle \otimes |j\rangle = \sum_{ij} \alpha_i\beta_j|i, j\rangle$.

Linear operators Given a Hilbert space $\mathcal{H}$, we denote by $\mathcal{L}(\mathcal{H})$ the set of linear operators on $\mathcal{H}$. When $\mathcal{H} = \mathbb{C}^n$, the linear operators are the matrices of size $n \times n$. The adjoint of an operator A is the operator denoted by $A^\dagger$ defined by being the unique linear operator such that for all $|\psi\rangle$ and $|\phi\rangle$ of $\mathcal{H}$, $\langle A^\dagger\psi|\phi\rangle = \langle\psi|A\phi\rangle$. A *Hermitian* operator A is its own adjoint $A = A^\dagger$. In the case where $\mathcal{H} = \mathbb{C}^n$, A is a matrix of size $n \times n$ and $A^\dagger$ is the transpose of

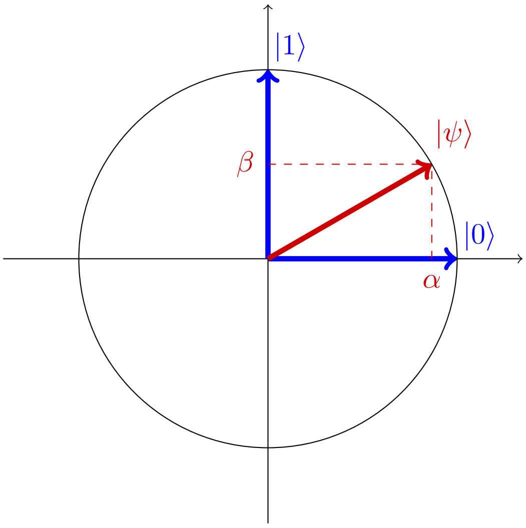


Figure 2.1: Representation (in red) of a qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ when α and β are real values in the plane spanned by the basis vectors $|0\rangle$ and $|1\rangle$ (in blue).

the complex conjugate of A. Hermitian matrices with non-negative eigenvalues are *positive semidefinite*. This defines a partial order on Hermitian matrices: $A \preceq B$ if $B - A$ is positive semidefinite. In particular $A \succeq 0$ means that A is positive semidefinite.

2.1.2 States

A *pure one-qubit state* is a normalized vector of $\mathbb{C}^2$:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad \text{with } |\alpha|^2 + |\beta|^2 = 1.$$

When α and β are real, it can be easily represented in a real plane, see Figure 2.1. This can be generalized to states on n qubits:

Definition 2.1 (n-qubit pure state) *A n-qubit* pure state *is a normalized vector of $\mathbb{C}^{2^n}$, and can be written $|\psi\rangle = \sum_{x\in\{0,1\}^n} \alpha_x|x\rangle$ with $\sum_{x\in\{0,1\}^n} |\alpha_x|^2 = 1$.*

Entanglement Note that all n-qubit pure states $|\psi\rangle$ cannot be written as the tensor product between two pure states $|\psi_A\rangle \otimes |\psi_B\rangle$, as for example the state $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. States that are not product of two states are called *entangled states*, in opposition to *product states*. Entangled states play a crucial role in quantum computing, and we will use entangled states as the primary resource all along this manuscript. For instance they naturally arise in cryptographic primitive, when the state shared by Alice and Bob exhibits correlations between them. This is the quantum generalization of shared randomness when Alice and Bob share a common probability distribution.

Mixed states Mixed states are a generalization of pure states and are probabilistic mixtures of pure states, that is a mixed state behaves like a state $|\psi_i\rangle$ with probability p_i. A mixed state cannot be described by a unit vector anymore, and is represented by a trace-one positive semidefinite matrix:

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|.$$

This matrix is called a *density matrix*, and this is how every quantum state is represented:

Definition 2.2 (Density matrix) *A n-qubit state ρ is a positive semidefinite matrix of size $2^n \times 2^n$ such that* $\mathrm{tr}(\rho) = 1$.

The density matrix of a pure state $|\psi\rangle$ is $\rho = |\psi\rangle\langle\psi|$, and we can easily characterize the density matrices of pure state:

Lemma 2.3 *ρ is a pure state if and only if* $\mathrm{tr}(\rho^2) = 1$.

Two different mixtures of pure states can lead to the same density matrix. For example, one can check that $\frac{1}{2}|\psi_a\rangle\langle\psi_a| + \frac{1}{2}|\psi_b\rangle\langle\psi_b| = \frac{3}{4}|0\rangle\langle 0| + \frac{1}{4}|1\rangle\langle 1|$ where $|\psi_a\rangle = \sqrt{\frac{3}{4}}|0\rangle + \sqrt{\frac{1}{4}}|1\rangle$ and $|\psi_b\rangle = \sqrt{\frac{3}{4}}|0\rangle - \sqrt{\frac{1}{4}}|1\rangle$. Nevertheless, the density matrix is the most complete description of a quantum states from a physical point of view since two states with the same density matrix are indistinguishable. In particular, since a density matrix ρ in dimension 2 is always diagonalizable $\rho = p|\varphi_0\rangle\langle\varphi_0| + (1-p)|\varphi_1\rangle\langle\varphi_1|$ for $0 \leq p \leq 1$, any mixed state is indistinguishable from a mixture of two pure orthogonal states.

Classical mixture of quantum states and quantum superposition should not be confused. For instance the state $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ has a density matrix $\begin{pmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{pmatrix}$ whereas the mixture $\frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|$ has a density matrix $\begin{pmatrix} 1/2 & 0 \\ 0 & 1/2 \end{pmatrix}$.

Furthermore, we can remark that the states $|\psi\rangle$ and $e^{i\theta}|\psi\rangle$ have the same density matrix, so they are indistinguishable, which means that pure states are defined up to a phase.

Bipartite quantum states Mixed states can be viewed as "parts" of bigger states. More formally for a bipartite quantum state, that is a state on more than 1 qubit, the description of each possible subsystem is in general a mixed state. The density matrix of a subsystem from the density matrix of the global system is computed using the partial trace:

Definition 2.4 (Partial trace) *Given two finite-dimensional Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$, the partial trace over B is the linear mapping from $\mathcal{L}(\mathcal{H}_A \otimes \mathcal{H}_B)$ to $\mathcal{L}(\mathcal{H}_A)$ such that:*

$$\forall A \in \mathcal{L}(\mathcal{H}_A),\ \forall B \in \mathcal{L}(\mathcal{H}_B),\ \mathrm{tr}_B(A \otimes B) = \mathrm{tr}(B)A.$$

The definition of the partial trace gives an explicit formulation only for product states $A \otimes B$, but the linearity condition ensures that this mapping is perfectly defined for all operators in $\mathcal{H}_A \otimes \mathcal{H}_B$.

A mixed state can always been seen as a part of (possibly bigger) pure state:

Lemma 2.5 *Let ρ be a n-qubit state. There exist a pure state m-qubit $|\psi\rangle$ such that $\rho = \mathrm{tr}_B(|\psi\rangle\langle\psi|)$ with $m \leq 2n$.*

Such a pure state is called a *purification* of ρ. As a sketch of a proof, consider a mixed state ρ written in its diagonal basis $\rho = \sum_i \lambda_i |\psi_i\rangle\langle\psi_i|$ with $\lambda_i \geq 0$ and $\sum_i \lambda_i = 1$. Then $|\psi\rangle = \sum_i \sqrt{\lambda_i}|\psi_i\rangle|\psi_i\rangle$ is a purification of ρ.

A useful mathematical tool to analyze pure states and their partial trace is the Schmidt decomposition:

Theorem 2.6 (Schmidt decomposition) *Let $|\psi\rangle$ be a pure state in $\mathbb{C}^{2^n} \otimes \mathbb{C}^{2^m}$. There exists an orthonormal basis $\{|u_i\rangle\}_i$ of $\mathbb{C}^{2^n}$ and $\{|v_j\rangle\}_j$ of $\mathbb{C}^{2^m}$ such that*

$$|\psi\rangle = \sum_{i=0}^{\min(2^n,2^m)-1} \sqrt{p_i}|u_i\rangle|v_i\rangle,$$

with $\sum_i p_i = 1$.

Corollary 2.7 *Consider a pure bipartite state $|\psi_{AB}\rangle \in \mathbb{C}^{2^n} \otimes \mathbb{C}^{2^n}$. Its Schmidt decomposition is $|\psi_{AB}\rangle = \sum_{i=0}^{2^n-1} \sqrt{p_i}|u_i\rangle|v_i\rangle$, thus the two mixed states $\rho_A = \mathrm{tr}_B|\psi_{AB}\rangle\langle\psi_{AB}|$ and $\rho_B = \mathrm{tr}_A|\psi_{AB}\rangle\langle\psi_{AB}|$ have the same spectrum $\{p_i\}_i$.*

2.1.3 Operations

There are two kinds of operation in quantum mechanics: unitary operations, responsible for the evolution of the quantum state, and measurements.

Definition 2.8 (Unitary matrix) *A unitary matrix U acting on n qubits is a $2^n \times 2^n$ matrix such that $UU^\dagger = \mathbb{I}$.*

A unitary operation U acts on a state ρ by: $\rho \mapsto U\rho U^\dagger$, and a pure state $|\psi\rangle$ by: $|\psi\rangle \mapsto U|\psi\rangle$. Quantum evolution shares similarities with stochastic evolution where the latter is modeled by stochastic matrices that preserve the 1-norm of probability distributions, whereas unitaries preserve their 2-norm. Moreover unitary matrices are always invertible, so every quantum computation is be reversible. Unlike classical computing it is not possible to compute functions that are non 1-to-1, but any function $f : \{0,1\}^n \to \{0,1\}^m$ can be converted into a unitary operation by appending qubits: $|x\rangle|s\rangle \mapsto |x\rangle|s \oplus f(x)\rangle$ is a reversible operation on $m+n$ qubits where $\oplus$ is the bitwise XOR.

It is sometimes useful to consider a more general type of operation on a quantum state:

Definition 2.9 (CPTP map) *Let $\mathcal{H}_1$ and $\mathcal{H}_2$ be two Hilbert spaces. The linear map $\mathcal{E} : \mathcal{L}(\mathcal{H}_1) \to \mathcal{L}(\mathcal{H}_2)$ is* completely positive trace preserving *if for all $k \geq 1$, for all positive semidefinite matrix $A \in \mathcal{L}(\mathbb{C}^k) \otimes \mathcal{L}(\mathcal{H}_1)$, $(\mathbb{I}_{\mathcal{L}(\mathbb{C}^k)} \otimes \mathcal{E})(A) \succeq 0$ and for all positive semidefinite matrix $A \in \mathcal{L}(\mathcal{H}_1)$, $\mathrm{tr}(\mathcal{E}(A)) = \mathrm{tr}(A)$.*

However, this does not allow extra power to the model of quantum computation, since a CPTP map can be implemented by a unitary on a larger Hilbert space:

Lemma 2.10 (Stinespring's dilation) *Let $\mathcal{E}$ be a completely positive trace preserving map from $\mathcal{L}(\mathcal{H}_1)$ to $\mathcal{L}(\mathcal{H}_2)$. There exist two Hilbert spaces $\mathcal{H}'_1$ and $\mathcal{H}'_2$ such that $\mathcal{H}_1 \otimes \mathcal{H}'_1 \cong \mathcal{H}_2 \otimes \mathcal{H}'_2$, a unitary U acting on $\mathcal{H}_1 \otimes \mathcal{H}'_1$ and a pure state $|\varphi\rangle \in \mathcal{H}'_1$ such that $\forall \rho \in \mathcal{L}(\mathcal{H}_1)$, $\mathcal{E}(\rho) = \mathrm{tr}_{\mathcal{H}'_2}[U(\rho \otimes |\varphi\rangle\langle\varphi|)U^\dagger]$.*

Measurement The projective measurement of a n-qubit pure state is defined by an orthonormal basis $\{|\psi_i\rangle\}$ of $\mathbb{C}^{2^n}$. After the measurement, a state $|\psi\rangle$ will be transformed into $|\psi_i\rangle$ with probability $|\langle\psi|\psi_i\rangle|^2$. This phenomenon is referred to as the "collapse of the wave function".

To extend this notion of measure to mixed states and partial measurements, a more general framework is for analyzing measurements is the following one:

Definition 2.11 (Positive Operator Valued Measure) *A POVM is a finite set of Hermitian positive semidefinite operators $\{E_i\}$ such that $\sum_i E_i = \mathbb{I}_{\mathcal{H}}$. The value of the measure of a state $\rho \in \mathcal{B}(\mathcal{H})$ is "i" with probability* $\mathrm{tr}[E_i\rho]$*, the resulting state is $\rho' = \frac{M_i \rho M_i}{\mathrm{tr}(M_i \rho M_i)}$ with $M_i = E_i^{1/2}$.*

Physicists tend to use a slightly different and weaker point of view on measurement through the notion of observable

Definition 2.12 (Observable) *Let M be a Hermitian matrix that can be diagonalized $M = \sum_{m \in \mathrm{sp}(M)} \Pi^{[m]}$. The value of the measurement of a state ρ using the observable M is "m" with probability* $\mathrm{tr}[\Pi^{[m]}\rho]$ *and the resulting state is $\rho' = \frac{\Pi^{[m]}\rho\Pi^{[m]}}{\mathrm{tr}(\Pi^{[m]}\rho\Pi^{[m]})}$.*

2.2 Continuous variables

Although we will not deal with physical implementations of qubits in the manuscript, one should never forget a qubit is encoded into two levels of one degree of liberty of a quantum state, like the spin of an electron or the polarization of a photon. However, quantum states can usually have more degrees of liberty and many more levels in them. Indeed, all elementary quantum systems cannot be represented by finite dimensional Hilbert spaces; *e.g.* position and momentum of a particle or the amplitude of an electromagnetic (EM) field. Let us insist that a qubit is a density matrix on a 2-dimensional Hilbert space, and that this Hilbert space can be embedded into another Hilbert space that can be infinite dimensional, see e.g. [GKP01].

The content of this section is to give a clear mathematical model for continuous variable systems, their evolution and their measurements.

2.2.1 The Hilbert space $L^2(\mathbb{R}^n)$

Let us first recall the definition of the Hilbert space $L^2(\mathbb{R})$. This is the quotient space $\mathcal{L}^2(\mathbb{R})/\sim$ where $\sim$ is the equivalence relation: two function ψ and ϕ are equivalent if they are equal almost everywhere, and $\mathcal{L}^2(\mathbb{R}) = \{\phi : \mathbb{R} \to \mathbb{C} \mid \int_{\mathbb{R}} |\phi(x)|^2 \mathrm{d}x < \infty\}$ is the set of square integrable functions. For any functions ϕ, ψ in $L^2(\mathbb{R})$, the canonical inner product on this space is defined by:

$$(\psi, \phi) = \int_{\mathbb{R}} \psi^*(x)\phi(x)\mathrm{d}x,$$

where ψ^* is the complex conjugate of ψ and the norm associated to it is:

$$\|\phi\| = \sqrt{(\phi, \phi)}.$$

When a tensor product structure is involved, we will abuse notations between the two isomorphic spaces $L^2(\mathbb{R}^n) \cong L^2(\mathbb{R})^{\otimes n}$.

One of the main property of $L^2(\mathbb{R}^n)$ is that it admits a countable basis:

Definition 2.13 (Hilbert basis, separable Hilbert space) *A* Hilbert basis *of an infinite-dimensional Hilbert space $\mathcal{H}$ is a countable set of orthonormal vectors $\{|v_i\rangle, i \in \mathbb{N}\}$ such that the space spanned by finite linear combinations of $|v_i\rangle$ is dense in $\mathcal{H}$. A Hilbert space with a Hilbert basis is* separable*.*

As a consequence, all separable Hilbert spaces are isomorphic, in particular L^2 and ℓ^2, the Hilbert space of square-summable sequences. In this manuscript, we will exclusivity use L^2

since we want to capture the "continuous" nature of the electromagnetic field that is more easily expressed in this setting. From now on, all the Hilbert spaces we will use are separable.

The Dirac notation can also be used in this case. A function ψ of L^2 is denoted by the ket $|\psi\rangle$ and the linear form $\phi \in L^2 \mapsto \int_{\mathbb{R}^n} \psi^*(x)\phi(x)\mathrm{d}x$ by $|\psi\rangle$. Please note that there are other linear form that the ones generated by functions of L^2 such as Dirac distributions, but we will carefully avoid to use them in this manuscript since it can lead to errors. The inner product on L^2 between ψ and ϕ can thus be denoted by $\langle\psi|\phi\rangle$ and the linear map $|\chi\rangle \mapsto \langle\psi|\chi\rangle|\phi\rangle$ by $|\phi\rangle\langle\psi|$.

Contrarily to the finite dimensional case, all linear operators on a infinite-dimensional separable Hilbert space $\mathcal{H}$ do not have an adjoint, but bounded linear operator do. A linear operator A is *bounded* if for all vector $|u\rangle$ of $\mathcal{H}$, the norm $\||A|u\rangle\|$ is finite. This restriction will not cause any problems, since unitaries and density operators are all bounded.

2.2.2 States

When dealing with infinite dimensional Hilbert spaces to study quantum systems, we are in a territory controlled by physicists, and the vocabulary is often dictated by historical and empirical reasons. For example an infinite dimensional state is often called a *mode* even if its physical support is not a mode of an electromagnetic field, and conversely the observable associated to the amplitude of an EM field is called *position* observable since the equation governing it is mathematically identical to the one of the position of a particle.

Definition 2.14 (CV states, modes) *A pure n-*mode state *is a vector of $L^2(\mathbb{R}^n)$ of norm 1.*

Contrarily to the finite dimensional case, the trace and the partial trace of an operator do not necessarily exist, this is why we will restrict ourselves to a smaller class of operators for which we can define the trace:

Definition 2.15 (Compact, trace-class operators, trace) *An operator A on a separable Hilbert space $\mathcal{H}$ is said* compact *if it can be written*

$$A = \sum_{n=0}^{\infty} \lambda_n |a_n\rangle\langle b_n|,$$

where the λ_n is a converging sequence of positive real numbers of limit 0*, $\{|a_n\rangle\}$ and $\{|b_n\rangle\}$ are two Hilbert basis of $\mathcal{H}$. The operator is* trace-class *if*

$$\sum_{n=0}^{\infty} \lambda_n < \infty.$$

The Banach space of trace-class operators on $\mathcal{H}$ is denoted $\mathcal{T}(\mathcal{H})$, and the trace *is the linear functional from $\mathcal{T}(\mathcal{H})$ to $\mathbb{R}$ defined by:*

$$\mathrm{tr}(A) = \sum_{k=0}^{\infty} \langle\psi_k|A|\psi_k\rangle,$$

where $\{|\psi_k\rangle\}$ is any Hilbert basis of $\mathcal{H}$.

Properties of trace-class operators

- If A and B are trace-class, then AB and BA are also trace-class.
- If A is trace-class, then $A^\dagger$ is trace-class.

This definition of the trace is the correct notion since the usual properties of the trace for matrices are also true for operators of $\mathcal{T}(\mathcal{H})$: $\operatorname{tr}(AB) = \operatorname{tr}(BA)$ and the trace does not depend of the choice of the basis. It is also straightforward to extend this definition to the partial trace of trace-class operators:

Definition 2.16 (Partial trace) *Given two separable Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$, the partial trace over B is the linear mapping from $\mathcal{T}(\mathcal{H}_A \otimes \mathcal{H}_B)$ to $\mathcal{T}(\mathcal{H}_A)$ such that by:*

$$\forall A \in \mathcal{T}(\mathcal{H}_A), B \in \mathcal{T}(\mathcal{H}_B),\ \operatorname{tr}_B(A \otimes B) = \operatorname{tr}(B)A.$$

A state with n modes will thus be represented by a density operator, the CV analog of the density matrix:

Definition 2.17 (n-mode state) *A n-mode state ρ is a positive semidefinite trace-class operator of $L^2(\mathbb{R}^n)$ such that $\operatorname{tr}(\rho) = 1$. The density operator ρ of pure state $|\psi\rangle$ is $\rho = |\psi\rangle\langle\psi|$.*

Lemma 2.18 *A state ρ is pure if and only if $\operatorname{tr}(\rho^2) = 1$.*

Since density operators are compact Hermitian operators, we can diagonalize them in a very similar manner than matrices: they have a discrete spectrum of real positive numbers:

Theorem 2.19 (Spectral Theorem) *Let A be a compact positive semidefinite Hermitian operator on L^2. There exists a sequence λ_n of real positive numbers converging to 0, and a Hilbert basis $|a_n\rangle$ of L^2 such that:*

$$A = \sum_n \lambda_n |a_n\rangle\langle a_n|.$$

When dealing with continuous variable states, it is often easier to use a different formalism than the one introduced here, the phase space formalism which is briefly introduced in Appendix A. The special case of Gaussian states in phase space is the focus of Section 2.3. Nevertheless, some operations are more easily done in the state space using a Hilbert basis. The most famous Hilbert basis is probably the Fourier basis, but this basis will be of no use in this work, instead we will the Fock basis which is of terrific importance, since the most useful Gaussian states can be easily expressed in it.

Definition 2.20 (Fock states) *For all integer $k \in \mathbb{N}$, we define the k-th Fock state $|k\rangle$ by the function*

$$|k\rangle : x \mapsto \left(\pi^{1/2} 2^k k!\right)^{-\frac{1}{2}} H_k(x) e^{-\frac{x^2}{2}},$$

where H_k is the k-th Hermite polynomial defined by: $H_k : x \mapsto (-1)^k e^{x^2} \frac{\mathrm{d}^k}{\mathrm{d}x^k} e^{-x^2}$.

Theorem 2.21 (Fock Basis) *The set of Fock states is a Hilbert basis of $L^2(\mathbb{R})$.*

This definition can seem a bit arid, but those states are the eigenstates of the harmonic oscillator, one of the most basic model in quantum mechanics. Moreover the state $|k\rangle$ represents number state of exactly k coherent photons produced by a laser. In realistic settings, lasers produce Gaussian states that are superposition of Fock states according to a Poisson distribution. We will decompose some of the Gaussian states in the Fock basis in Section 2.3.2.

When dealing with n modes, we use bold notation to denote a n-index $\mathbf{i} = i_1 \dots i_n \in \mathbb{N}^n$. The set $\{|\mathbf{i}\rangle, \mathbf{i} \in \mathbb{N}^n\}$ defined by $|\mathbf{i}\rangle = |i_1\rangle \cdots |i_n\rangle$ will be also called the Fock basis of $L^2(\mathbb{R}^n)$.

2.2.3 Operations

According to the axioms of quantum mechanics, the states will evolve with unitary operations:

Definition 2.22 (Unitary operator) *An operator U acting a Hilbert space $\mathcal{H}$ is* unitary *if $UU^\dagger = U^\dagger U = \mathbb{I}_{\mathcal{H}}$.*

We emphasize that contrary to the finite case, the existence of a right inverse does not imply the existence of a left inverse. For example, given a Hilbert basis $\{|\phi_k\rangle\}$, the shift operator $S : |\phi_k\rangle \mapsto |\phi_{k+1}\rangle$ has a left inverse, but no right inverse.

Measurements on the other hand are far more complex with continuous variables and expressed in the formalism of “observables”. An observable is simply an Hermitian operator and can have discrete or continuous spectrum, being bounded or not. We do not introduce the general case here but we give a straightforward generalization of Definition 2.12

Definition 2.23 (Observable with discrete spectrum) *A Hermitian operator M is an observable with discrete spectrum if there exists a countable set of projectors $\{\Pi^{[m]}\}$ such that $M = \sum_m m\Pi^{[m]}$. Measuring a state ρ with M will result to outcome “m” with probability $\mathrm{tr}[\Pi^{[m]}\rho]$. The resulting state is $\rho' = \frac{\Pi^{[m]}\rho\Pi^{[m]}}{\mathrm{tr}[\Pi^{[m]}\rho\Pi^{[m]}]}$.*

The other fundamental case, that has no discrete equivalent, comes from using an observable with a fully continuous spectrum. Phase space is the best formalism to describe such a measurement, but we nonetheless give the definition of one of them, the position measurement:

Definition 2.24 (Position observable) *Let $\rho = \sum_{m,n} \rho_{m,n}|m\rangle\langle n|$ be a one-mode state. The outcome of measuring ρ with the position observable and error Δ is x_0 with probability*

$$\sum_{m,n} \rho_{m,n} \int_{x_0-\Delta}^{x_0+\Delta} n(x)m(x)\mathrm{d}x,$$

where m and n are the m-th and n-th Fock functions.

We did not specify the resulting state after the measurement since we will never consider it in this dissertation, and in practical implementations this measurement is destructive: the light is absorbed by the measurement apparatus.

In the limit $\Delta \to 0$, this measurement appears to be fully continuous, thus giving the name *continuous variables* to quantum state expressed in infinite dimensional Hilbert spaces. In the laboratory, this measure can be perform efficiently for very small Δ, which is why this measure is the very root of considering CV state as a resource in quantum computing. Indeed when considering light pulses, this correspond to measuring their amplitude.

2.3 Gaussian model

In this dissertation, we restrict ourselves to a class of continuous variables states and operations called Gaussian states and Gaussian operations. In this Section, we introduce their formalism based on covariance and symplectic matrices. This is quite different from the previous sections since the states and operations are considered from a different point of view, called the phase space and not from the Hilbert space $L^2(\mathbb{R}^n)$ which is called the state space. We present a first connexion between the two formalisms by giving the decomposition of some of the usual Gaussian states in the Fock basis. The formal construction of the phase space and why states are described by covariance matrices is postponed to Appendix A since this is not needed for understanding the results presented in this manuscript.

2.3.1 Covariance and symplectic matrices

In this Section, we introduce the two mathematical objects at the heart of the study of Gaussian states and operations, covariance and symplectic matrices.

Definition 2.25 (Covariance matrix) *A covariance matrix is a $2n \times 2n$ real symmetric positive semi-definite matrix.*

Definition 2.26 (Symplectic matrix) *A symplectic matrix is a $2n \times 2n$ real matrix that satisfies*

$$S\Omega S^T = \Omega,$$

where Ω is the block diagonal matrix $\Omega = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^{\oplus n}$.

Properties of symplectic matrices:

- If S and T are symplectic, ST and TS are also symplectic;
- If S is symplectic, S is invertible and $S^{-1} = -\Omega S^T \Omega$;
- $\det S = 1$;
- Ω is symplectic and $\Omega^{-1} = \Omega^T = -\Omega$.

Covariance matrices can be "diagonalized" by the action of symplectic matrices. Of course, this is not a diagonalization in the usual sense since symplectic matrices are not unitary in general.

Theorem 2.27 (Williamson's decomposition [SCS99]) *Let γ be a covariance matrix. There exists a symplectic matrix S and a diagonal matrix $D = \mathrm{diag}(\nu_1, \nu_1, \nu_2, \nu_2 \ldots, \nu_n, \nu_n)$ such that:*

$$\nu_i \geq 0 \quad \textit{and} \quad \gamma = SDS^T.$$

The $\{\nu_i\}$ are called the symplectic values *of γ and are independent of S up to a permutation.*

2.3.2 Gaussian states

Definitions Let us now make the connection between covariance matrices and Gaussian states.

Definition 2.28 (Gaussian state) *An n-*mode Gaussian state *is described by a $2n$-dimensional real vector μ called the* mean vector *and $2n \times 2n$ covariance matrix γ with the additional constraint $\gamma + i\Omega \succeq 0$.*

As a consequence a Gaussian state is described by less than n^2 real parameters. This is in strong contrast with general CV states for which each mode can require an infinite number of parameters. It is also noteworthy that the set of Gaussian states does not have a linear structure: the superposition of Gaussian states is in general not a Gaussian state.

Informally, covariance matrices play a role quite similar to the one played by density operators in state space, and the symplectic values the one of eigenvalues. The condition $\gamma + i\Omega \succeq 0$ is in fact a condition on the symplectic values implies that all the symplectic values are at least one. To continue further this analogy, there is a characterization of pure Gaussian states quite similar to Lemma 2.18 and Lemma 2.3:

Lemma 2.29 (Symplectic values of a Gaussian state) *The symplectic values of a Gaussian state are greater or equal to 1. They are all equal to one if and only if the state is pure.*

Some Gaussian states Some Gaussian states play extremely important roles, such as the thermal states which are mixed Gaussian states and can be compared to totally mixed states of one qubit, and the two-mode squeezed states that are the Gaussian equivalent of EPR pairs on two qubits.

Definition 2.30 (Coherent and thermal states)

- *A* thermal state of variance ν *is a one-mode state with* $\mu = (0,0)$ *and* $\gamma = \nu\mathbb{I}$ *with* $\nu \geq 1$.
- *A* coherent state $|\alpha\rangle$ *is a pure one-mode state with* $\mu = \frac{1}{\sqrt{2}}(\Re(\alpha), \mathrm{Im}(\alpha))$ *and* $\gamma = \mathbb{I}_2$.
- *The* vacuum state *is the Fock state* $|0\rangle$. *It is a special case of coherent state (centered in* $\mu = (0,0)$*) and thermal state of variance* $\nu = 1$.

One other state plays a central role in the study of Gaussian states, the *two-mode squeezed state*, since it is the Gaussian equivalent of the EPR pair. A two-mode squeezed state of squeezing r is the Gaussian state of mean vector $\mu = (0,0,0,0)$ and covariance matrix:

$$\begin{pmatrix} \nu & 0 & \sqrt{\nu^2-1} & 0 \\ 0 & \nu & 0 & -\sqrt{\nu^2-1} \\ \sqrt{\nu^2-1} & 0 & \nu & 0 \\ 0 & -\sqrt{\nu^2-1} & 0 & \nu \end{pmatrix}$$

with the variance $\nu = \cosh(2r)$.

The partial trace of Gaussian states can also be expressed in a very simple way in phase space

Theorem 2.31 (Partial trace of a Gaussian state) *Let* ρ_{AB} *be a bipartite Gaussian state with* $n+m$ *modes. It is described by a* $2n \times 2m$ *covariance matrix* $\gamma_{AB} = \begin{pmatrix} \gamma_A & C \\ C^T & \gamma_B \end{pmatrix}$ *and a mean vector* $\mu = \mu_A \oplus \mu_B \in \mathbb{R}^{2n+2m}$, *then the state* $\rho_A = \mathrm{tr}_B(\rho_{AB})$ *is described by the covariance matrix* γ_A *and the mean vector* μ_A.

This proves that the mixed state obtained by tracing out one of the mode of a two-mode squeezed state of squeezing r is a thermal state of variance $\nu = \cosh(2r)$, thus making the connection with totally mixed states.

Relation with the Fock basis Although it is difficult to write any Gaussian state in the Fock basis, we know the expansion of these examples. A coherent state $|\alpha\rangle$ can be written as:

$$|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_{i=0}^{\infty} \frac{\alpha^i}{\sqrt{i!}} |i\rangle,$$

a two-mode squeezed state with squeezing r as:

$$|TMS(r)\rangle = (\cosh(r))^{-1/2} \sum \tanh(r)^i |i\rangle|i\rangle, \tag{2.1}$$

and as a consequence a thermal state of variance $\nu = \cosh(2r)$ as:

$$\rho_{\mathrm{th}(\nu)} = \sum_{i=0}^{\infty} \left(\frac{\nu-1}{\nu+1}\right)^i |i\rangle\langle i|. \tag{2.2}$$

2.3.3 Gaussian operations

Definition 2.32 (Gaussian operation) *A Gaussian operation is a linear map that maps any Gaussian state into a Gaussian state.*

This definition is not quite useful since it does not give a characterization of Gaussian operations in phase space. For unitary operation, there exist a simple characterization in phase space [Fiu01]:

Lemma 2.33 *The set of Gaussian unitaries acting on n modes is in one-to-one correspondence with the set $\{(S, d)\}$ for all $2n \times 2n$ symplectic matrix S and real vector d of $\mathbb{R}^{2n}$.*

In Appendix A, we explain how a Gaussian unitary acts on any CV state in phase space. This has a very simple formulation when considering only Gaussian states:

Corollary 2.34 *Let ρ be a Gaussian state with covariance matrix γ and mean vector μ and a Gaussian unitary U described in phase space by a symplectic matrix S and a displacement vector d, then the action of U in phase space is:*

$$(\gamma, \mu) \mapsto (S\gamma S^T, S\mu + d).$$

Normal mode decomposition One of the main mathematical tool for analyzing bipartite Gaussian states, is the normal mode decomposition [BR03], which is the Gaussian equivalent of the Schmidt decomposition:

Theorem 2.35 (Normal form) *Let γ_{AB} be the covariance matrix of a pure bipartite Gaussian state. γ_{AB} can be decomposed:*

$$(S_A \oplus S_B)\gamma_{AB}(S_A^T \oplus S_B^T) = \begin{pmatrix} D & \sqrt{D^2 - \mathbb{I}}Z_n \\ \sqrt{D^2 - \mathbb{I}}Z_n & D \end{pmatrix} \tag{2.3}$$

where D is the diagonal matrix of the symplectic values of γ_A, $Z_n = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)^{\oplus n}$, and S_A and S_B are two symplectic matrix acting respectively on Alice's and Bob's modes.

Physically, this theorem states if Alice and Bob share n modes of a pure Gaussian state, by applying local Gaussian unitary operations only, they can transfer it into n shared two-mode squeezed states.

2.4 Norms and distinguishability

This section introduces different norms that are used in this manuscript and focuses on how to use them for distinguishing states. Distinguishability between states has been extensively studied by Christopher A. Fuchs [Fuc96]. All the notions defined here are valid for separable Hilbert spaces, finite or infinite dimensional, this is why we omit to specify the dimensions.

First, the measure induced by the scalar product on the linear operator is the operator norm, sometimes called the spectral norm:

Definition 2.36 (Operator norm) *Let $A \in \mathcal{B}(\mathcal{H})$. The* operator norm *of A is defined by:*

$$\|A\| = \sup_{|v\rangle} \frac{\|A|v\rangle\|}{\||v\rangle\|}.$$

This norm appears quite naturally in many derivations, but does not have an operational meaning for distinguishability. This is why the trace norm is used:

Definition 2.37 (Trace norm) *Let $A \in \mathcal{T}(\mathcal{H})$, its trace norm is:*

$$\|A\|_{\mathrm{tr}} = \mathrm{tr}\sqrt{A^\dagger A}.$$

The trace norm gives the optimal probability p of distinguishing two equiprobable states ρ and σ:

$$p = \frac{1}{2} + \frac{1}{4}\|\rho - \sigma\|_{\mathrm{tr}}.$$

It is sometimes easier to define the trace distance between two states ρ and σ by

$$D_{\mathrm{tr}}(\rho, \sigma) = \frac{1}{2}\|\rho - \sigma\|_{\mathrm{tr}}.$$

The constant $1/2$ is chosen so that two orthogonal states have distance 1.

When dealing with trace norm, we will use the following lemmata:

Lemma 2.38 (Hölder's inequality) *For any $A, B \in \mathcal{T}(\mathcal{H})$, we have $\|AB\|_{\mathrm{tr}} \leq \|A\|_{\mathrm{F}} \cdot \|B\|_{\mathrm{F}}$, where $\|A\|_{\mathrm{F}}$ is the Frobenius norm defined by: $\|A\|_{\mathrm{F}} = \sqrt{\mathrm{tr}(A^\dagger A)}$.*

Lemma 2.39 *For any $A, B \in \mathcal{T}(\mathcal{H})$, we have $\mathrm{tr}(AB) \leq \|A\| \cdot \|B\|_{\mathrm{tr}}$.*

Lemma 2.40 *For any A, B Hermitian positive definite, we have $\left\|A^{\frac{1}{2}}BA^{\frac{1}{2}}\right\| = \left\|A^{\frac{1}{2}}B^{\frac{1}{2}}\right\|^2 = \left\|B^{\frac{1}{2}}A^{\frac{1}{2}}\right\|^2$, and $\left\|A^{\frac{1}{2}}B^{-\frac{1}{2}}\right\|^2 = \min\{c \text{ such that } A \preceq cB\}$.*

The other quantity that we will often use when dealing with distinguishability of two states is the fidelity.

Definition 2.41 (Fidelity) *The* fidelity *between to quantum states ρ and σ is defined by:*

$$\mathcal{F}(\rho, \sigma) = \mathrm{tr}\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}}.$$

When dealing with pure states, the fidelity is sometimes called the "transition probability" (see e.g. [Uhl76]), the term fidelity seems to come from an article by Josza [Joz94], but he uses the square of this quantity, since it can be understood as a probability. However in their book, Nielsen and Chuang [NC04] used this definition and has been used since in the computer science community. Physicists tend to use the original definition.[1]

The fidelity and the trace norm have some useful properties in common: they are symmetric, invariant under the action of unitary operations, and simpler expression for pure states $\rho = |\psi\rangle\langle\psi|$ and $\sigma = |\phi\rangle\langle\phi|$ can be derived:

$$\mathcal{F}(\rho,\sigma) = |\langle\psi|\phi\rangle| \quad \text{and} \quad \|\rho-\sigma\|_{\mathrm{tr}} = 2\sqrt{1-|\langle\psi|\phi\rangle|}.$$

Fidelity and trace distance also capture the fact that it is more difficult to distinguish mixed states than their purifications. Let $|\psi\rangle$ and $|\phi\rangle$ be two bipartite pure states in $\mathcal{T}(\mathcal{H}_A \otimes \mathcal{H}_B)$ and $\rho_A = \mathrm{tr}_B(|\psi\rangle\langle\psi|)$ and $\sigma_A = \mathrm{tr}_B(|\phi\rangle\langle\phi|)$ their partial traces over $\mathcal{H}_B$ then:

$$\mathcal{F}(\rho_A,\sigma_A) \geq \mathcal{F}(|\psi\rangle\langle\psi|, |\phi\rangle\langle\phi|) \quad \text{and} \quad D_{\mathrm{tr}}(\rho_A,\sigma_A) \leq D_{\mathrm{tr}}(|\psi\rangle\langle\psi|, |\phi\rangle\langle\phi|).$$

The first inequality can always be saturated, this is the content of Uhlmann's theorem:

Theorem 2.42 (Uhlmann's theorem) *Let ρ and σ be two quantum states and $|\psi\rangle$ a purification of ρ. Then*

$$\mathcal{F}(\rho,\sigma) = \max_{|\varphi\rangle} |\langle\psi|\varphi\rangle|\,,$$

where the maximum is taken over all purifications $|\varphi\rangle$ of σ.

There is a first proof of the theorem in [Uhl76] for discrete variables as well as for continuous variables. This proof is difficult to read and is non constructive. Richard Jozsa gave a simple constructive proof for the discrete variable case [Joz94]. To the best of our knowledge there is no continuous variable equivalent.

As written above, fidelity and trace distance have a strong relationship. It is possible to have a formal statement:

Lemma 2.43 *Let ρ and σ two quantum states. Then*

$$1-\mathcal{F}(\rho,\sigma) \leq D_{\mathrm{tr}}(\rho,\sigma) \leq \sqrt{1-\mathcal{F}(\rho,\sigma)^2}.$$

Quantum Chernoff bound and Bhattacharyya bound The quantum Chernoff bound [ACMT+07] is an upper bound on the minimal error done when distinguishing between two states when there are k copies of them and reads,

$$P_{\mathrm{err}} \leq \frac{1}{2}\left(\inf_{0<s<1} \mathrm{tr}\left[\rho^s\sigma^{1-s}\right]\right)^k.$$

The Bhattacharyya bound [Kai67, PL08] is the special case $s = 1/2$ of the Chernoff bound. In this manuscript, we will only consider that bound when $k = 1$, and by writing P_{err} in term of trace distance, we get:

Lemma 2.44 (Bhattacharyya bound) *For all state ρ and σ:*

$$1 - D_{\mathrm{tr}}(\rho,\sigma) \leq \mathrm{tr}\left[\sqrt{\rho}\sqrt{\sigma}\right].$$

[1] and they are probably right, but the primary focus of this dissertation is mostly computer scientists who are used to the definition introduced here.

2.5 Summary

In this Chapter, we gave a quick overview of the standard model of quantum computing in a finite-dimensional Hilbert space. We then extended it to continuous variables by considering the separable Hilbert space of square integrable functions. We underlined a few key differences, like the necessity to restrict ourselves to trace-class operators and the existence of “continuous” measurements.

We then focused on a subclass of CV states, called Gaussian states and their formalism coming from an formalism in another space. Gaussian states that can be concisely described by covariance matrices and Gaussian unitaries by symplectic matrices.

Let us summarize an informal connection between CV states in state space and Gaussian states in phase space (for clarity the mean vector of Gaussian states is omitted)

	n qubits	n modes	n Gaussian modes
Basis	$\|x\rangle,\ x \in \{0,1\}^n$	$\|\mathbf{i}\rangle,\ \mathbf{i} \in \mathbb{N}^n$	no basis
State	density matrix	density operator	covariance matrix
Size	$2^n \times 2^n$	infinite dimensional	$2n \times 2n$
Eigenvalues	$\sum_{i=1}^{2^n} \lambda_i = 1,\ \lambda_i \geq 0$	$\sum_{i=1}^{\infty} \lambda_i = 1,\ \lambda_i \geq 0$	$(\nu_1, \nu_1, \nu_2, \nu_2, \cdots, \nu_n, \nu_n),\ \nu_i \geq 1$
Unitary	$UU^\dagger = \mathbb{I}$	$UU^\dagger = U^\dagger U = \mathbb{I}$	$S\Omega S^T = \Omega$
Acts by	$\rho \mapsto U\rho U^\dagger$	$\rho \mapsto U\rho U^\dagger$	$\gamma \mapsto S\gamma S^T$

We finally examined two different notions to quantify the distinguishability between two states, the trace distance and the fidelity.

Part I

Cryptographic primitives

3 Gaussian quantum bit commitment

In this Chapter, we address quantum bit commitment protocols with *continuous variables*, and explore whether such protocols may be found secure when both parties are restricted to use Gaussian states and operations. We answer by the negative in Section 3.2. The main ingredient of the proof is the introduction of what we call *intrinsic purifications* that are introduced and studied in the first Section.

At the heart of the impossibility proof of quantum bit commitment lies Uhlmann's theorem (Theorem 2.42). For Gaussian quantum bit commitment, one would need a Gaussian version of this theorem, namely that if two Gaussian states have a certain fidelity between them, then there are two Gaussian purifications of them with the same fidelity. We do not resolve the question of stating if such theorem exists or not. As a matter of fact this question seems extremely difficult to answer. However an approximate version of Uhlmann is sufficient to prove the no-go theorem. This is the strategy we are following in this Chapter. By relaxing slightly the condition on the fidelity (we do not require that the fidelity of the purifications is exactly the same than the mixed states, but close enough) we can construct Gaussian purifications. Our approach is even a bit more general and it is called intrinsic purifications.

Moreover, the use of intrinsic purifications instead of Uhlmann's theorem allows us to provide a constructive attack for any CV QBC protocol, whereas constructive attacks were previously known for finite dimensions only.

3.1 Intrinsic purifications

In this Chapter, A^* (resp. A^T) denotes the complex conjugate (resp. the transpose) of any linear operator A **relatively to the Fock basis**, defined as $\langle \mathbf{i}|A^*|\mathbf{j}\rangle = \langle \mathbf{i}|A|\mathbf{j}\rangle^*$ and $\langle \mathbf{i}|A^T|\mathbf{j}\rangle = \langle \mathbf{j}|A|\mathbf{i}\rangle$.

This section is devoted to prove the following theorem:

Theorem 3.1 *For all n-mode state ρ there exists a $2n$-mode purification $|\psi(\rho)\rangle$ of ρ such that:*

- *If ρ is a Gaussian state, then $|\psi(\rho)\rangle$ is also a Gaussian state,*
- *For every n-mode states ρ_0 and ρ_1, we have*

$$1 - \sqrt{1 - \mathcal{F}(\rho_0, \rho_1)^2} \leq \mathcal{F}\Big(|\psi(\rho_0)\rangle\langle\psi(\rho_0)|,\ |\psi(\rho_1)\rangle\langle\psi(\rho_1)|\Big).$$

The proof of the theorem is based on the notion of *intrinsic purifications* :

Definition 3.2 (Intrinsic purifications) *Let ρ be an n-mode state and U be a diagonalization of ρ in the Fock basis, that is, U is a unitary operator such that $\langle \mathbf{i}|U^\dagger \rho U|\mathbf{j}\rangle = p_\mathbf{i}\,\delta_{\mathbf{ij}}$, where $\delta_{\mathbf{ij}}$ is the Kronecker delta. We then define an intrinsic purification $|\psi\rangle$ of ρ as*

$$|\psi\rangle = (U^* \otimes U) \sum_{\mathbf{i}} \sqrt{p_\mathbf{i}}|\mathbf{i}\rangle|\mathbf{i}\rangle.$$

Note that this purification is not uniquely defined, since there exist many diagonalizations of a state, one can for example permute the ordering of the extra modes. Contrary to Uhlmann's purifications for which it is not known wether they can be Gaussian for Gaussian states, we can make a statement for intrinsic purifications:

Lemma 3.3 *A Gaussian state has a Gaussian intrinsic purification.*

Proof. By Williamson's decomposition (Theorem 2.27), there exists a Gaussian unitary V such that $V\rho V^\dagger$ is a tensor product of n thermal states with variances ν_k, i.e. it can be written in the Fock basis by tensoring Equation (2.2):

$$V\rho V^\dagger = \bigotimes_{k=1}^{n}\sum_{i=0}^{\infty}\left(\frac{\nu_k-1}{\nu_k+1}\right)^i |i\rangle\langle i| = \sum_{\mathbf{i}\in\mathbb{N}^k} p_{\mathbf{i}}|\mathbf{i}\rangle\langle\mathbf{i}|,$$

with $p_{\mathbf{i}} = \prod_{k=1}^{n}\left(\frac{\nu_k-1}{\nu_k+1}\right)^{\mathbf{i}_k}$. The unitary V is a diagonalization of ρ in the Fock basis.

Our goal is to show that the state

$$(V^*\otimes V)\sum_{\mathbf{i}\in\mathbb{N}^k}\sqrt{p_{\mathbf{i}}}|\mathbf{i}\rangle|\mathbf{i}\rangle$$

is Gaussian. First of all, according to Equation (2.1), the state $\sum_{\mathbf{i}\in\mathbb{N}^k}\sqrt{p_{\mathbf{i}}}|\mathbf{i}\rangle|\mathbf{i}\rangle$ is a two-mode squeezed state, so is Gaussian. Since V comes from the Williamson's decomposition, V is also Gaussian. The remaining piece is to prove that V^* is also Gaussian.

V^* **is Gaussian** Our strategy is look at the action on V^* on any Gaussian state, and show it corresponds to apply a certain symplectic matrix in phase space. Let us take an arbitrary n-mode Gaussian state τ with covariance matrix γ_τ and mean vector μ_τ. Let us also denote the action of V by its symplectic matrix S and displacement vector d.

Define $Z_n = \bigoplus_{k=1}^{n} Z = \bigoplus_{k=1}^{n}\left(\begin{smallmatrix}1 & 0\\ 0 & -1\end{smallmatrix}\right)$. We want to show that applying V^* to τ is equivalent to applying the symplectic matrix Z_nSZ_n and the displacement Z_nd in phase space. First, remark that $V^* = (V^\dagger)^T$ and observe that $V^*\tau V^{*\dagger} = (V\tau^T V^\dagger)^T$.

The transposition relatively to the Fock basis has a simple expression in phase space for Gaussian states [Sim00]: let σ be a Gaussian state with covariance matrix γ_σ and mean vector μ_σ, then σ^T is a Gaussian state with covariance matrix $Z_n\gamma_\sigma Z_n$ and mean vector $Z_n\mu_\sigma$.

As a consequence, we get

$$\begin{aligned}
\tau^T &\quad \text{is described by} \quad Z_n\gamma_\tau Z_n \quad \text{and} \quad Z_n\mu_\tau\\
V\tau^T V^\dagger &\quad \text{is described by} \quad (SZ_n)\gamma_\tau(Z_nS^T) \quad \text{and} \quad (SZ_n)\mu_\tau - d\\
V^*\tau^T V^{*\dagger} &\quad \text{is described by} \quad (Z_nSZ_n)\gamma_\tau(Z_nSZ_n)^T \quad \text{and} \quad (Z_nSZ_n)\mu_\tau - Z_nd
\end{aligned}$$

Finally, we can conclude that (Z_nSZ_n) is a symplectic matrix, even though Z_n is not. First remark that $Z_n\Omega Z_n = -\Omega$, this leads us to:

$$(Z_nSZ_n)\Omega(Z_nSZ_n)^T = \Omega.$$

□

Proof of Theorem 3.1. Let $|\psi_0\rangle = (U_0^* \otimes U_0) \sum_i \sqrt{p_i}|i\rangle|i\rangle$ be an intrinsic purification of ρ_0 and $|\psi_1\rangle = (U_1^* \otimes U_1) \sum_i \sqrt{q_i}|i\rangle|i\rangle$ an intrinsic purification of ρ_1. According to the Bhattacharyya bound, we have

$$1 - \sqrt{1 - \mathcal{F}(\rho_0, \rho_1)^2} \leq \mathrm{tr}[\sqrt{\rho_0}\sqrt{\rho_1}],$$

so proving that

$$\mathrm{tr}[\sqrt{\rho_0}\sqrt{\rho_1}] = \mathcal{F}\big(|\psi_0\rangle\langle\psi_0|, |\psi_1\rangle\langle\psi_1|\big),$$

will conclude the proof. This equality is a property of intrinsic purifications.

Let us compute $\mathrm{tr}[\sqrt{\rho_0}\sqrt{\rho_1}]$ by taking the trace in the basis $\{U_0|\mathbf{k}\rangle\}_\mathbf{k}$:

$$\begin{aligned}
\mathrm{tr}[\sqrt{\rho_0}\sqrt{\rho_1}] &= \mathrm{tr}\left[U_0 \sum_{\mathbf{i}} \sqrt{p_\mathbf{i}}|\mathbf{i}\rangle\langle\mathbf{i}|U_0^\dagger U_1 \sum_{\mathbf{j}} \sqrt{q_\mathbf{j}}|\mathbf{j}\rangle\langle\mathbf{j}|U_1^\dagger\right] \\
&= \sum_{\mathbf{i},\mathbf{j},\mathbf{k}} \sqrt{p_\mathbf{i} q_\mathbf{j}}\ (\langle\mathbf{k}|U_0^\dagger)U_0|\mathbf{i}\rangle\langle\mathbf{i}|U_0^\dagger U_1|\mathbf{j}\rangle\langle\mathbf{j}|U_1^\dagger(U_0|\mathbf{k}\rangle) \\
&= \sum_{\mathbf{i},\mathbf{j}} \sqrt{p_\mathbf{i} q_\mathbf{j}}\langle\mathbf{i}|U_0^\dagger U_1|\mathbf{j}\rangle\langle\mathbf{j}|U_1^\dagger U_0|\mathbf{i}\rangle \\
&= \sum_{\mathbf{i},\mathbf{j}} \sqrt{p_\mathbf{i} q_\mathbf{j}} \left|\langle\mathbf{i}|U_0^\dagger U_1|\mathbf{j}\rangle\right|^2
\end{aligned}$$

On the other hand:

$$\mathcal{F}(|\psi_0\rangle\langle\psi_0|, |\psi_1\rangle\langle\psi_1|) = |\langle\psi_0|\psi_1\rangle| = \left|\sum_{\mathbf{i},\mathbf{j}} \sqrt{p_\mathbf{i} q_\mathbf{j}}\ \langle\mathbf{i}|(U_0^\dagger U_1)^*|\mathbf{j}\rangle\langle\mathbf{i}|U_0^\dagger U_1|\mathbf{j}\rangle\right|.$$

According to the definition of the conjugation relatively to the Fock basis, we can conclude that

$$\mathrm{tr}(\sqrt{\rho_0}\sqrt{\rho_1}) = \mathcal{F}(|\psi_0\rangle\langle\psi_0|, |\psi_1\rangle\langle\psi_1|).$$

This proof holds for any intrinsic purifications, so in particular, if ρ_0 and ρ_1 are Gaussian states, we can choose $|\psi_0\rangle$ and $|\psi_1\rangle$ to be Gaussian. □

This theorem can also be reformulated using the trace distance instead of the fidelity:

Corollary 3.4 *Given two n-mode states ρ_0 and ρ_1, there exist $2n$-mode purifications $|\psi_0\rangle$ of ρ_0 and $|\psi_1\rangle$ of ρ_1 such that*

$$D_{\mathrm{tr}}(|\psi_0\rangle\langle\psi_0|, |\psi_1\rangle\langle\psi_1|) \leq \sqrt{2D_{\mathrm{tr}}(\rho_0, \rho_1)}$$

Moreover, if ρ_0 and ρ_1 are Gaussian states, so are their purifications $|\psi_0\rangle$ and $|\psi_1\rangle$.

Relation to Uhlmann's theorem Our theorem is weaker than Uhlmann's theorem when stated in term of fidelity, but not in term of trace distance like in Corollary 3.4. However, our theorem has some advantages. First, our proof is constructive, whereas Uhlmann is not constructive for CV states, and secondly, we are able to prove the Gaussianity of the purifications, which was our first motivation. Another consequence that we reflected in the term "intrinsic" is that the purifications do not depend of both states ρ_0 and ρ_1. Thus we can purified several close states, and guarantee that their purification will also be close:

Corollary 3.5 *Let $\rho_1, \dots, \rho_t$ be t quantum states, and note $d_{i,j}$ the trace distance between ρ_i and ρ_j. Then, for all $i \in [t]$, there exists purification $|\psi_i\rangle$ of ρ_i such that*

$$\forall i, j \in [t],\ \frac{1}{2} \left\| |\psi_i\rangle\langle\psi_i| - |\psi_j\rangle\langle\psi_j| \right\|_{\mathrm{tr}} \leq \sqrt{2 d_{i,j}}.$$

Moreover, if $\rho_1, \dots, \rho_t$ are Gaussian states, the purifications are also Gaussian.

3.2 No-go theorem

In [May97, LC97] it has been shown that any QBC protocol, no matter how complicated are the commit and the reveal phases is equivalent to a *purified* protocol in terms of security.

Definition 3.6 (Purified quantum bit commitment protocol) *A* purified *quantum bit commitment protocol is an interactive protocol between two players Alice and Bob with two phases:*

Commit phase *Alice encodes her bit b into a pure bipartite state $|\psi_b\rangle$ and sends one half to Bob. At the end of the committing phase, Bob holds either $\rho_0 = \mathrm{tr}_A |\psi_0\rangle\langle\psi_0|$ or $\rho_1 = \mathrm{tr}_A |\psi_1\rangle\langle\psi_1|$ if Alice wants to commit to 0 or 1, respectively.*

Reveal phase *Alice sends the other half of $|\psi_b\rangle$.*

The reduction is done by remarking that all the measurements happening during each of the phases can be postponed to the end of the phases. When a full protocol involves only Gaussian states and Gaussian operations, the purified protocol uses only Gaussian states. This is why we will consider that $|\psi_b\rangle$ are Gaussian states from now on, and we will show that such a protocol is insecure, more precisely, we will show that the more concealing the protocol, the more powerful the cheating strategies.

Definition 3.7 (ε-concealing) *The protocol is referred to as* ε-concealing *if $\|\rho_0 - \rho_1\|_{\mathrm{tr}} \leq 2\varepsilon$, which means that Bob cannot learn the value of b, except with probability ε*

Definition 3.8 (δ-cheating strategy) *In a* δ-cheating strategy, *Alice sends a state $\rho^\sharp$ in the committing phase and then decides to follow a strategy leading to a final state of her choice, $|\psi_0^\sharp\rangle$ or $|\psi_1^\sharp\rangle$, so that Bob should not be able to distinguish this strategy from a honest strategy with a probability greater than δ. This means that $\left\|\rho^\sharp - \rho_b\right\|_{\mathrm{tr}} \leq 2\delta$ and $\left\|\psi_b^\sharp - \psi_b\right\|_{\mathrm{tr}} \leq 2\delta$.*

Now, let us state our main result:

Theorem 3.9 *Given any ε-concealing Gaussian quantum bit commitment protocol to Bob, there exists a Gaussian $\sqrt{2\varepsilon}$-cheating strategy for Alice.*

Here, we will only consider the simple strategy in which $\rho^\sharp = \rho_0$ and $|\psi_0^\sharp\rangle = |\psi_0\rangle$. Thus, $|\psi_1^\sharp\rangle$ will correspond to Alice initially committing to a zero and then cheating so to make it a one. This is sufficient to prove the no-go theorem. Without loss of generality, we will also consider that $|\psi_b\rangle$ are $2n$-mode states and ρ_b are n-mode states.

3.2.1 Perfectly concealing protocols

Let us first have a look at what happens when the protocol is perfectly concealing. In this case Alice has a perfect cheating strategy.

Lemma 3.10 *Let $|\psi_0\rangle$ and $|\psi_1\rangle$ be $2n$-mode Gaussian states such that $\mathrm{tr}_A|\psi_0\rangle\langle\psi_0| = \mathrm{tr}_A|\psi_1\rangle\langle\psi_1|$. There exists a Gaussian unitary operator U acting on n modes such that $(U \otimes \mathbb{I})|\psi_0\rangle = |\psi_1\rangle$, where $\mathbb{I}$ is the identity on n modes.*

Proof. For $b \in \{0,1\}$, denote by $\mu_b = \begin{pmatrix} \mu_b^A \\ \mu_b^B \end{pmatrix}$ and $\gamma_b = \begin{pmatrix} \gamma_b^A & C_b \\ C_b^T & \gamma_b^B \end{pmatrix}$ the covariance matrix and mean vector of $|\psi_b\rangle$. According to Theorem 2.31, the condition $\mathrm{tr}_A|\psi_0\rangle\langle\psi_0| = \mathrm{tr}_A|\psi_1\rangle\langle\psi_1|$ implies that $\mu_0^B = \mu_1^B$ and $\gamma_0^B = \gamma_1^B$.

As a consequence, γ_0^A and γ_1^A have the same symplectic spectra, so that, by applying the normal mode decomposition on γ_0 and γ_1 we know that there exist symplectic matrices S_b^j such that:

$$\gamma_0 = (S_0^A \oplus S_0^B)\tilde{\gamma}_0(S_0^A \oplus S_0^B)^t,$$
$$\gamma_1 = (S_1^A \oplus S_1^B)\tilde{\gamma}_1(S_1^A \oplus S_1^B)^t,$$

where $\tilde{\gamma}_b = \begin{pmatrix} D_b & d \\ d & D_b \end{pmatrix}$. The matrices D_0 and D_1 are diagonal matrices with the same values. It is then possible to choose the symplectic matrices S_b^j such that $D_0 = D_1$, hence $\tilde{\gamma}_0 = \tilde{\gamma}_1 = \tilde{\gamma}$. The symplectic matrix $S^\sharp = S_1^A(S_0^A)^{-1} \oplus \mathbb{I}_{2n}$ transforms γ_0 into γ_1 by acting on Alice's modes only. Similarly, the displacement $\mu_1 - S^\sharp\mu_0$ transforms μ_0 into μ_1 by acting on Alice's side only, which proves Lemma 3.10. □

The previous theorem is exactly what we needed to prove the no-go theorem for perfectly concealing protocol. Alice's cheating strategy is well-known, she first starts the protocol as she wanted to commit to 0, and she simply applies an appropriate unitary operation to her half of $|\psi_b\rangle$ between the two stages of the protocol if she decides to actually reveal 1. This allows her to convert $|\psi_0\rangle$ into $|\psi_1\rangle$. In the case of Gaussian QBC, Lemma 3.10 implies that this cheating unitary is Gaussian.

3.2.2 ε-concealing protocols

We now investigate the realistic case where the protocol is not perfectly concealing, which will finally lead us to the proof of Theorem 3.9. This proof is a reduction to the perfectly concealing case that is done using intrinsic purifications. (See Figure 3.1)

Proof of Theorem 3.9. We want to find an explicit Gaussian $\sqrt{2\varepsilon}$-cheating strategy for Alice against a ε-concealing QBC protocol. In the first stage of the protocol, Alice creates the state $|\psi_0\rangle$ and sends ρ_0 to Bob. In the second stage, if Alice wants to reveal the bit 0, she sends her half of $|\psi_0\rangle$ to Bob, while if she decides to reveal the bit 1, she applies a Gaussian unitary operation to her half of $|\psi_0\rangle$, mapping it to $|\psi_1^\sharp\rangle$, and then sends it to Bob.

As a consequence of Lemma 3.1, there exist Gaussian purifications $|\phi_0\rangle$ of ρ_0 and $|\phi_1\rangle$ of ρ_1 such that $D(\phi_0, \phi_1) \leq \sqrt{2D(\rho_0, \rho_1)}$. Moreover $|\psi_0\rangle$ and $|\phi_0\rangle$ (resp. $|\psi_1\rangle$ and $|\phi_1\rangle$) are

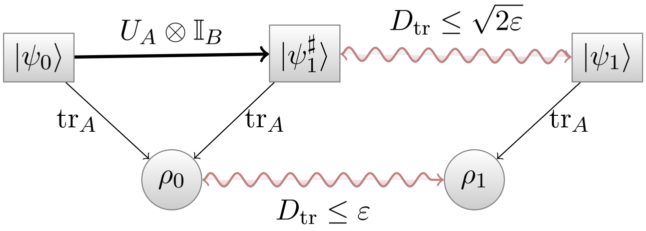


Figure 3.1: Overview of the proof. Square represent pure states, circles mixed state. The thick arrow denotes the action of a unitary, the thin arrows tracing over Alice's modes and the "snake" arrow is used to indicate the trace distance.

two Gaussian purifications of the same Gaussian state ρ_0 (resp. ρ_1), so that, according to Lemma 3.10, there exists a Gaussian unitary operator U_0 (resp. U_1) such that $(U_0 \otimes \mathbb{I})|\psi_0\rangle = |\phi_0\rangle$ (resp. $(U_1 \otimes \mathbb{I})|\psi_1\rangle = |\phi_1\rangle$). We note $|\psi_1^\sharp\rangle = (U_1^{-1}U_0 \otimes \mathbb{I})|\psi_0\rangle = (U_1^{-1} \otimes \mathbb{I})|\phi_0\rangle$. By unitary invariance of the trace distance, one has $D(\psi_1^\sharp, \psi_1) = D(\phi_0, \phi_1)$. Thus, for ε-concealing protocols, we have $D(\psi_1^\sharp, \psi_1) \leq \sqrt{2\varepsilon}$. □

We have thus obtained a stronger result than the standard no-go theorem since we have shown that QBC remains impossible even if Alice and Bob are restricted to manipulate Gaussian states. Although Lemma 3.1 can be seen as a weak version of Uhlmann's theorem in the sense that the intrinsic purification does not reach Uhlmann's bound, it is sufficient here because the quantities of interest in terms of guessing probability are not changed. Interestingly, the question of whether the purifications that saturate Uhlmann's bound could both be chosen Gaussian if the states are Gaussian is still open (although partial results in this direction have been obtained in [MM07]). Note also that we have an explicit construction of Alice's cheating purifications for any CV QBC protocol, Gaussian or not. This is done by noting that the Gaussian constraint can be relaxed in the proof of Lemma 3.1, and that Lemma 3.10 can be replaced by the usual Schmidt decomposition.

3.3 Is physics informational?

With the emergence of computers, devices that manipulate information, the concept that "information is physical" got widely accepted and formulated in a series of papers by Landauer (e.g. see [Lan92]). But in recent years, this concept got challenged [Fuc01, Fuc02, Bra05] and presented as the Fuchs-Brassard conjecture. This conjecture tries to build the theory of quantum physics on axioms from information theory instead of mechanics. Fuchs and Brassard conjectured that a theory in which key distribution is possible, and bit commitment is not is the theory of quantum physics. It was later proven wrong, but Clifton *et al.* proved instead that the assumptions of no-signalling, no-broadcasting, and the impossibility of bit commitment make it work within the framework of C^*-algebras [CBH03]. This is known as the CBH theorem.

One of the consequence of this strong no-go theorem is that it provides us with a natural and elegant counter-example of the Brassard and Fuchs conjecture as well as another input on the importance of the C^*-algebra framework for CBH. As a matter of fact, consider the subset of quantum mechanics where only Gaussian states and operations are allowed. As a result of our no-go theorem, this Gaussian model forbids bit commitment while it allows unconditional secret key distribution [RC09]. Interestingly, however, it is strictly included in quantum mechanics since, for instance, Bell inequalities cannot be violated with Gaussian states and measurements. This is in contradiction with the Brassard-Fuchs conjecture. Furthermore, according to the CBH theorem [CBH03], quantum mechanics can be rederived from the sole assumptions that signaling, broadcasting, and bit commitment are impossible in Nature. While this idea is very appealing, the Gaussian model again provides a natural counter-example to it.

The reason is that the CBH theorem actually requires the further assumption that the physical description of Nature is done within the framework of C^*-algebras. Although Smolin [Smo05] and latter Spekkens [Spe07] found toy models compatible with CBH but distinct from quantum mechanics, our counter-example is physically grounded.

3.4 Summary

We have addressed continuous variable quantum bit commitment, and have proved a strong version of the standard no-go theorem in which Alice and Bob are restricted to Gaussian states and operations. The main technical innovation of our proof is the introduction of “intrinsic purifications”, for which we are able to prove a Gaussian analog to Uhlmann’s theorem.

4 Weak coin flipping

The Chapter aims at proving the existence of a way coin flipping protocol with arbitrarily small bias. More precisely we study a model called *time independent point game*. We show that a time independent point game is equivalent to weak quantum coin flipping protocol and a witness on its bias. The construction of a time independent point game leading to a protocol with arbitrarily small bias is presented in Appendix C. This construction is due to Carlos Mochon [Moc07].

To prove the equivalence between a time independent point game and a protocol with a witness on its bias, we consider different intermediate models. Let us give a big picture overview of this Chapter. Section 4.1 formally introduces coin flipping protocols and their bias. We also show that the optimal bias of a protocol can be expressed as a semidefinite program, and that the points in this dual, *dual feasible points* are a witness on the bias of this protocol. In Section 4.2, we show the equivalence between a protocol and its dual feasible points on one side, and a *point game* on the other side. Roughly speaking, a point game is a game composed of succession of moves of points, called *transitions*. The game ends when only one point remains. We prove that the coordinates of that final point gives an upper bound on the cheating probabilities. Thus finding a point game with final point $[1/2+\varepsilon, 1/2+\varepsilon]$ gives us the existence of a quantum weak coin flipping protocol with bias ε. We consider 3 variations of point games, namely point games with *EBM transitions*, *valid transitions* and *time independent* point games, each model being a little bit easier to manipulate mathematically. We summarize the succession of models in Figure 4.1.

4.1 Coin flipping and semidefinite programming

4.1.1 Definitions

The role of the next couple of definitions is to formally define weak coin flipping protocols.

Definition 4.1 (Coin flipping protocol) *For n even, an n-message coin flipping protocol between two players, Alice and Bob, is described by:*

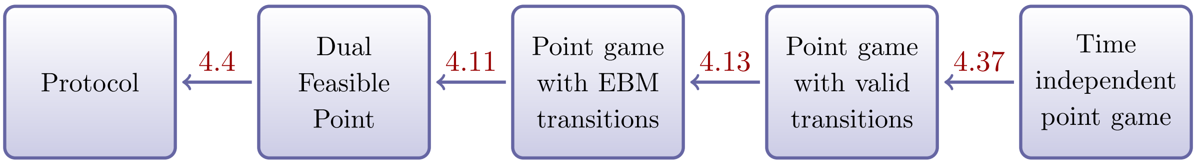

Protocol
4.4
Dual Feasible Point
4.11
Point game with EBM transitions
4.13
Point game with valid transitions
4.37
Time independent point game

Figure 4.1: The succession of models we will consider. An arrow from model A to model B means that proving the existence of an ε biased protocol in A implies the existence of an $\varepsilon + \varepsilon'$ biased protocol in B (for all $\varepsilon, \varepsilon' > 0$). The numbers on top of the arrows refer to the theorem proving that reduction.

- *Three Hilbert spaces $\mathcal{A}, \mathcal{B}$ corresponding to Alice and Bob private workspaces (Bob does not have any access to $\mathcal{A}$ and Alice to $\mathcal{B}$), and a message space $\mathcal{M}$.*
- *An initial product state $|\psi_0\rangle = |\psi_{A,0}\rangle \otimes |\psi_{M,0}\rangle \otimes |\psi_{B,0}\rangle \in \mathcal{A} \otimes \mathcal{M} \otimes \mathcal{B}$.*
- *A set of n unitaries $\{U_1, \ldots, U_n\}$ acting on $\mathcal{A} \otimes \mathcal{M} \otimes \mathcal{B}$, with $U_i = U_{A,i} \otimes \mathbb{I}_{\mathcal{B}}$ for i odd, and $U_i = \mathbb{I}_{\mathcal{A}} \otimes U_{B,i}$ for i even.*
- *A set of* honest states *$\{|\psi_i\rangle,\ i \in [n]\}$ defined by $|\psi_i\rangle = U_i U_{i-1} \cdots U_1 |\psi_0\rangle$.*
- *A set of n projectors $\{E_1, \ldots, E_n\}$ acting on $\mathcal{A} \otimes \mathcal{M} \otimes \mathcal{B}$, with $E_i = E_{A,i} \otimes \mathbb{I}_{\mathcal{B}}$ for i odd, and $E_i = \mathbb{I}_{\mathcal{A}} \otimes E_{B,i}$ for i even, such that $E_i|\psi_i\rangle = |\psi_i\rangle$.*
- *Two final POVM $\left\{\Pi_A^{(0)}, \Pi_A^{(1)}\right\}$ acting on $\mathcal{A}$ and $\left\{\Pi_B^{(0)}, \Pi_B^{(1)}\right\}$ acting on $\mathcal{B}$.*

The protocol is the following:

1. *In the beginning, Alice holds $|\psi_{A,0}\rangle|\psi_{M,0}\rangle$ and Bob $|\psi_{B,0}\rangle$.*
2. *For $i = 1$ to n:*
   — If i is odd, Alice applies U_i and measures the resulting state with the POVM $\{E_i, \mathbb{I} - E_i\}$. On the first outcome, Alice sends the message qubits to Bob; on the second outcome, she ends the protocol by outputting "0", i.e. Alice declares herself winner.
   — If i is even, Bob applies U_i and measures the resulting state with the POVM $\{E_i, \mathbb{I} - E_i\}$. On the first outcome, Bob sends the message qubits to Alice; on the second outcome, he ends the protocol by outputting "1", i.e. Bob declares himself winner.
3. *Alice and Bob measure their part of the state with the final POVM and output the outcome of their measurements. Alice wins on outcome "0" and Bob on outcome "1".*

Definition 4.2 (Weak coin flipping protocol with bias ε) *A weak coin flipping protocol with bias ε is a coin flipping protocol with the following properties:*

- ***Correctness**: When both players are honest, Alice and Bob's outcomes are always the same:*
  $\Pi_A^{(0)} \otimes \mathbb{I}_{\mathcal{M}} \otimes \Pi_B^{(1)}|\psi_n\rangle = \Pi_A^{(1)} \otimes \mathbb{I}_{\mathcal{M}} \otimes \Pi_B^{(0)}|\psi_n\rangle = 0.$
- ***Balanced:** When both players are honest, they win with probability 1/2:*
  $P_A = \left\|\Pi_A^{(0)} \otimes \mathbb{I}_{\mathcal{M}} \otimes \Pi_B^{(0)}|\psi_n\rangle\right\|^2 = \frac{1}{2}$ *and* $P_B = \left\|\Pi_A^{(1)} \otimes \mathbb{I}_{\mathcal{M}} \otimes \Pi_B^{(1)}|\psi_n\rangle\right\|^2 = \frac{1}{2}$.
- *ε **biased:** When Alice is honest, the probability that both players agree on Bob winning is $P_B^* \leq 1/2 + \varepsilon$. And conversely, if Bob is honest, the probability that both players agree on Alice winning is $P_A^* \leq 1/2 + \varepsilon$.*

The definition of a weak coin flipping protocol differs from the usual one in the fact that we added the projections $\{E_i\}$. The goal of these projections is to catch if the other player is cheating since they do not change the honest states. Intuitively they can only decrease the bias compared to a protocol without them. This can be proved, but it is not necessary in our case since we will directly prove upper bounds on the cheating probabilities for this specific type of protocols.

4.1.2 Cheating probabilities as SDPs

The cheating probabilities P_A^* and P_B^* cannot be easily computed from the definitions above. Kitaev showed that they can be expressed as semidefinite programs (SDP) [Kit03] and a written proof can be found in [ABDR04].

Fix a weak coin flipping protocol, and assume that Alice is honest. We describe a semidefinite program with variables the states $\rho_{AM,i}$, ie. the states at round i after Bob's workspace is traced out. The probability that Bob wins is the probability that Alice outputs "1" when applying the POVM $\left\{\Pi_A^{(0)}, \Pi_A^{(1)}\right\}$ to her part of the final state, or equivalently $\mathrm{tr}((\Pi_A^{(1)} \otimes \mathbb{I}_{\mathcal{M}})\rho_{AM,n})$. Since Alice is honest, the state in her workspace is not arbitrary, but rather satisfies some constraints. In the beginning of the protocol, Alice held the state $\mathrm{tr}_{\mathcal{M}}(\rho_{AM,0}) = |\psi_{A,0}\rangle\langle\psi_{A,0}|$. Moreover, the evolution of Alice's state is only due to her own actions, namely $\mathrm{tr}_{\mathcal{M}}(\rho_{AM,i}) = \mathrm{tr}_{\mathcal{M}}(\rho_{AM,i-1})$ if i is even and $\mathrm{tr}_{\mathcal{M}}(\rho_{AM,i}) = \mathrm{tr}_{\mathcal{M}}(E_i U_i \rho_{AM,i-1} U_i^\dagger E_i)$ if i is odd. Bob's cheating probability is the maximum over all his strategies, i.e. over all states $\{\rho_{AM,i}\}$ that satisfy these constraints.

The evolution of the states $\rho_{AM,i}$ is not unitary due to the presence of the projections, so they are not necessary normalized. However $\mathrm{tr}((\Pi_A^{(1)} \otimes \mathbb{I})\rho_{AM,n})$ represents the probability that Alice and Bob agree on Bob winning when Alice is honest. If Bob got caught cheating by the projections, Alice already declared herself the winner. The non-normalization of the states $\rho_{AM,i}$ reflects the probability that the protocol ended prematurely by one of the players declaring oneself winner.

This reasoning leads to the following two semidefinite programs:

Theorem 4.3 (Primal)
$P_B^* = \max \mathrm{tr}((\Pi_A^{(1)} \otimes \mathbb{I})\rho_{AM,n})$ *over all* $\rho_{AM,i}$ *satisfying the constraints:*

- $\mathrm{tr}_{\mathcal{M}}(\rho_{AM,0}) = \mathrm{tr}_{\mathcal{MB}}(|\psi_0\rangle\langle\psi_0|) = |\psi_{A,0}\rangle\langle\psi_{A,0}|$,
- *for i odd,* $\mathrm{tr}_{\mathcal{M}}(\rho_{AM,i}) = \mathrm{tr}_{\mathcal{M}}(E_i U_i \rho_{AM,i-1} U_i^\dagger E_i)$,
- *for i even,* $\mathrm{tr}_{\mathcal{M}}(\rho_{AM,i}) = \mathrm{tr}_{\mathcal{M}}(\rho_{AM,i-1})$.

$P_A^* = \max \mathrm{tr}((\mathbb{I} \otimes \Pi_B^{(0)})\rho_{MB,n})$ *over all* $\rho_{BM,i}$ *satisfying the constraints:*

- $\mathrm{tr}_{\mathcal{M}}(\rho_{MB,0}) = \mathrm{tr}_{\mathcal{AM}}(|\psi_0\rangle\langle\psi_0|) = |\psi_{B,0}\rangle\langle\psi_{B,0}|$,
- *for i even* $\mathrm{tr}_{\mathcal{M}}(\rho_{MB,i}) = \mathrm{tr}_{\mathcal{M}}(E_i U_i \rho_{MB,i-1} U_i^\dagger E_i)$,
- *for i odd* $\mathrm{tr}_{\mathcal{M}}(\rho_{MB,i}) = \mathrm{tr}_{\mathcal{M}}(\rho_{MB,i-1})$.

4.1.3 Upper bounds on the cheating probabilities via the dual SDPs

We wish to prove upper bounds on the cheating probabilities P_A^* and P_B^*. Using the primal is not suitable for this task since the cheating probabilities are defined by a maximization: any set of matrices $\{\rho_i\}$ that satisfies the constraints will lead to a lower bound on the cheating probabilities. We circumvent this problem by dualizing these SDPs.

Theorem 4.4 (Dual)
$P_B^* = \min \mathrm{tr}(Z_{A,0}|\psi_{A,0}\rangle\langle\psi_{A,0}|)$ *over all* $Z_{A,i}$ *under the constraints:*

① $\forall i,\ Z_{A,i} \succeq 0$,

② *for i odd,* $Z_{A,i-1} \otimes \mathbb{I}_{\mathcal{M}} \succeq U_{A,i}^{\dagger} E_{A,i}(Z_{A,i} \otimes \mathbb{I}_{\mathcal{M}}) E_{A,i} U_{A,i}$,

③ *for i even,* $Z_{A,i-1} = Z_{A,i}$,

④ $Z_{A,n} = \Pi_A^{(1)}$,

$P_A^* = \min \operatorname{tr}(Z_{B,0}|\psi_{B,0}\rangle\langle\psi_{B,0}|)$ *over all $Z_{B,i}$ under the constraints:*

① $\forall i,\ Z_{B,i} \succeq 0$,

② *for i even* $\mathbb{I}_{\mathcal{M}} \otimes Z_{B,i-1} \succeq U_{B,i}^{\dagger} E_{B,i}(\mathbb{I}_{\mathcal{M}} \otimes Z_{B,i}) E_{B,i} U_{B,i}$,

③ *for i odd,* $Z_{B,i-1} = Z_{B,i}$,

④ $Z_{B,n} = \Pi_B^{(0)}$,

A proof of this theorem can be found in [Kit03, ABDR04].
Let us now add one more constraint on the above dual SDPs:

⑤ $Z_{A,0}|\psi_{A,0}\rangle = \beta|\psi_{A,0}\rangle$ i.e. $|\psi_{A,0}\rangle$ is an eigenvector of $Z_{A,0}$ with eigenvalue $\beta > 0$,
⑤ $Z_{B,0}|\psi_{B,0}\rangle = \alpha|\psi_{B,0}\rangle$ i.e. $|\psi_{B,0}\rangle$ is an eigenvector of $Z_{B,0}$ with eigenvalue $\alpha > 0$.

Definition 4.5 (Dual feasible point) *A* dual feasible point *is a set of matrices $\{Z_0, \ldots, Z_n\}$ with $Z_i = Z_{A,i} \otimes \mathbb{I}_{\mathcal{M}} \otimes Z_{B,i}$ satisfying conditions ① to ⑤.*

Notice that $\operatorname{tr}(Z_{A,0}|\psi_{A,0}\rangle\langle\psi_{A,0}|) = \beta$ and $\operatorname{tr}(Z_{B,0}|\psi_{B,0}\rangle\langle\psi_{B,0}|) = \alpha$ and hence

Corollary 4.6 *Let $\{Z_i\}$ be a dual feasible point of a protocol, then $P_A^* \leq \alpha$ and $P_B^* \leq \beta$.*

Note that since we imposed a new constraint on the dual SDP, we may only be able to find a dual feasible point with larger values of α and β than before. However, we will show that still, we can make these values arbitrarily close to $1/2$. Moreover, one can, in fact, show that $P_A^* = \inf \alpha$ and $P_B^* = \inf \beta$ where the infimum is taken over all dual feasible points (see proof in Appendix B); therefore, we have not changed the value of the optimization problem.

Every dual feasible point produces an upper bound on the cheating probability: $P_A^* \leq \alpha$ and $P_B^* \leq \beta$. This is the magic of duality, a maximization problem has been turned into a minimization one.

Notice also that the dualization reversed the time ordering of the protocol. The primal formulation sets constraints on the evolution of ρ_i to ρ_{i+1} from a fixed state ρ_0, whereas in the dual formulation the initial constraint is on Z_n and the evolution concerns how Z_i is related to Z_{i-1}.

4.2 Point games

In the previous section we saw that we can upper bound the cheating probability of any weak coin flipping protocol by looking at the dual SDP formulation of the protocol and by providing a dual feasible point, namely a set of matrices $\{Z_0, \ldots, Z_n\}$ that satisfies a number of conditions. One can think of these matrices as a witness of the security of the protocol. However, it is not clear how to construct a protocol and, moreover, its dual feasible point.

Here, our goal is to find a graphical representation of a protocol together with its dual feasible point that will be easier to manipulate. This is the reason we introduce point games.

In high level, a point game is a set of points on a 2-dimensional plane together with a sequence of transitions between them. Instead of defining a point game at this point, we see how a protocol with cheating probabilities $P_A^* \leq \alpha$ and $P_B^* \leq \beta$ and a dual feasible point naturally gives rise to what we call a *point game expressible by matrices* with final point $[\beta, \alpha]$. More importantly, we will show that the reverse implication is also true and hence we will reduce the task of finding a coin flipping protocol and its dual feasible point to finding a point game expressible by matrices (EBM point game).

4.2.1 EBM point games

The dual SDP formulation of a coin flipping protocol enables us to calculate an upper bound on the cheating probabilities of Alice and Bob by finding a dual feasible point, i.e. a set of positive definite matrices $\{Z_0, \ldots, Z_n\}$, with $Z_i = Z_{A,i} \otimes \mathbb{I}_{\mathcal{M}} \otimes Z_{B,i}$ that satisfy a set of conditions. Then, the cheating probabilities of Alice and Bob are bounded by $\mathrm{tr}(Z_{A,0}\rho_{A,0}) = \alpha$ and $\mathrm{tr}(Z_{B,0}\rho_{B,0}) = \beta$, where $\rho_{A,0} = |\psi_{A,0}\rangle\langle\psi_{A,0}| = \mathrm{tr}_{\mathcal{MB}}|\psi_0\rangle\langle\psi_0|$ and $\rho_{B,0} = |\psi_{B,0}\rangle\langle\psi_{B,0}| = \mathrm{tr}_{\mathcal{AM}}|\psi_0\rangle\langle\psi_0|$ are the initial states of the protocol.

In fact, we need to be looking at the two cheating probabilities at the same time and hence we will be interested in their product (similar to Kitaev's lower bound for strong coin flipping) $\mathrm{tr}(Z_{A,0}\rho_{A,0}) \cdot \mathrm{tr}(Z_{B,0}\rho_{B,0}) = \mathrm{tr}(Z_{A,0} \otimes \mathbb{I}_{\mathcal{M}} \otimes Z_{B,0}|\psi_0\rangle\langle\psi_0|)$. Note that this equality holds only because the state $|\psi_0\rangle$ is a product state and it does not hold for the matrices Z_i and states $|\psi_i\rangle$ that correspond to the intermediate rounds of the protocol.

Nevertheless, the quantity $Z_{A,i} \otimes \mathbb{I}_{\mathcal{M}} \otimes Z_{B,i}|\psi_i\rangle\langle\psi_i|$ is exactly what we will represent as a set of points. In high level, for each pair of eigenspaces of $Z_{A,i}$ and $Z_{B,i}$ with corresponding eigenvalues $z_{A,i}$ and $z_{B,i}$ we define a point $[z_{A,i}, z_{B,i}]$ with weight equal to the projection of $|\psi_i\rangle$ on this pair of eigenspaces. When $|\psi_i\rangle$ is a unit vector, then this is a probability distribution. More formally,

Definition 4.7 (prob) *Let Z be a positive semidefinite matrix and note $\Pi^{[z]}$ the projector on the eigenspace of eigenvalue $z \in \mathrm{sp}(Z)$. We then have $Z = \sum_z z\Pi^{[z]}$. Let $|\psi\rangle$ be a (not necessarily unit) vector. We define* $\mathrm{prob}[Z, \psi]$ *as a function with finite support from* $[0, \infty) \to [0, \infty)$ *by:*

$$\mathrm{prob}[Z, \psi](z) = \begin{cases} \langle\psi|\Pi^{[z]}|\psi\rangle & \textit{if } z \in \mathrm{sp}(Z) \\ 0 & \textit{otherwise.} \end{cases}$$

If $Z = Z_A \otimes \mathbb{I}_{\mathcal{M}} \otimes Z_B$, using the same notation, we define $\mathrm{prob}[Z_A, Z_B, \psi]$ *as a 2-variate function with finite support from* $[0, \infty) \times [0, \infty) \to [0, \infty)$ *by:*

$$\mathrm{prob}[Z_A, Z_B, \psi](z_A, z_B) = \begin{cases} \langle\psi|\Pi^{[z_A]} \otimes \mathbb{I}_{\mathcal{M}} \otimes \Pi^{[z_B]}|\psi\rangle & \textit{if } (z_A, z_B) \in (\mathrm{Sp}(Z_A), \mathrm{Sp}(Z_B)) \\ 0 & \textit{otherwise.} \end{cases}$$

Hence, for every i, the positive semidefinite matrix $Z_i = Z_{A,i} \otimes \mathbb{I}_{\mathcal{M}} \otimes Z_{B,i}$ and the honest joint state $|\psi_i\rangle$ define the function $p_{n-i} = \mathrm{prob}[Z_{A,i}, Z_{B,i}, \psi_i]$ with finite support.

Notice that we have reversed the order of the protocol since this is a representation of the dual. The function p_0 represents the final state of the protocol, and p_n the protocol before any message. In other words, we have interpreted the dual feasible solution together with the honest states of the protocol as a sequence of functions with finite support $\{p_0, p_1, \ldots, p_n\}$.

A function with finite support can be equivalently represented by weighted points. Each value $(z_{A,i}, z_{B,i})$ in the support of the function is represented by a point of coordinates $[z_{A,i}, z_{B,i}]$ with weight $\langle\psi_i|\Pi^{[z_{A,i}]} \otimes \mathbb{I}_{\mathcal{M}} \otimes \Pi^{[z_{B,i}]}|\psi_i\rangle$. More formally, we denote by $[x_0, y_0]$ the function with finite support defined by $(x,y) \mapsto \delta_{x,x_0}\delta_{y,y_0}$. This function is graphically represented by a point of coordinates $[x_0,y_0]$ with weight 1. Then, the "point notation" of $\mathrm{prob}[Z_{A,i},Z_{B,i},\psi_i]$ is

$$\mathrm{prob}[Z_{A,i},Z_{B,i},\psi_i] = \sum_{(z_{A,i},z_{B,i})\in\big(\mathrm{sp}(Z_{A,i}),\mathrm{sp}(Z_{B,i})\big)} \langle\psi_i|\Pi^{[z_{A,i}]}\otimes\mathbb{I}_{\mathcal{M}}\otimes\Pi^{[z_{B,i}]}|\psi_i\rangle\ [z_{A,i},z_{B,i}].$$

We can now interpret the initial and final condition of the dual SDP in the language of point games and get:

$$\begin{aligned} p_0 &= \mathrm{prob}[Z_{A,n},Z_{B,n},\psi_n] = \mathrm{prob}[\Pi_A^{(1)},\Pi_B^{(0)},\psi_n] = \frac{1}{2}[1,0]+\frac{1}{2}[0,1] \\ p_n &= \mathrm{prob}[Z_{A,0},Z_{B,0},\psi_0] = 1[\beta,\alpha]. \end{aligned}$$

Recall that we added an extra condition in Theorem 4.4, namely that $|\psi_{A,0}\rangle$ is an eigenstate of $Z_{A,0}$. This condition ensures us that the game ends with one final point, and not several points.

The only thing that remains is to interpret the dual SDP condition for the intermediate round i in the language of point games, which will tell us how the points can move on the plane, in other words what type of *transitions* ($p_{n-i}\to p_{n-i+1}$) are allowed in our game.

Let us assume that i is odd. We know that the function p_{n-i} (resp. p_{n-i+1}) corresponds to the matrix Z_i (resp. Z_{i-1}) and the state $|\psi_i\rangle$ (resp. $|\psi_{i-1}\rangle$). Since i is odd, the conditions of the dual SDP state that $Z_{B,i}=Z_{B,i-1}$ and also $|\psi_i\rangle = E_{A,i}U_{A,i}\otimes\mathbb{I}_{\mathcal{B}}|\psi_{i-1}\rangle$. We claim that this implies that the points only move horizontally and moreover, the total weight on every horizontal line remains unchanged (thus so does the total weight).

We have

$$p_{n-i+1} = \sum_{(z_{A,i-1},z_{B,i-1})} \langle\psi_{i-1}|\Pi^{[z_{A,i-1}]}\otimes\mathbb{I}_{\mathcal{M}}\otimes\Pi^{[z_{B,i-1}]}|\psi_{i-1}\rangle\ [z_{A,i-1},z_{B,i-1}].$$

For p_{n-i}, we have

$$\begin{aligned} p_{n-i} &= \sum_{(z_{A,i},z_{B,i-1})} \langle\psi_i|\Pi^{[z_{A,i}]}\otimes\mathbb{I}_{\mathcal{M}}\otimes\Pi^{[z_{B,i-1}]}|\psi_i\rangle\ [z_{A,i},z_{B,i-1}] \\ &= \sum_{(z_{A,i},z_{B,i-1})} \langle\psi_{i-1}|U_{A,i}^\dagger E_{A,i}(\Pi^{[z_{A,i}]}\otimes\mathbb{I}_{\mathcal{M}})E_{A,i}U_{A,i}\otimes\Pi^{[z_{B,i-1}]}|\psi_{i-1}\rangle\ [z_{A,i},z_{B,i-1}]. \end{aligned}$$

First, notice that $\mathrm{sp}(Z_{B,i}) = \mathrm{sp}(Z_{B,i-1})$ and hence the possible values for the second coordinate of the points remain the same. Second, the sum of the weights of the points in each horizontal line with second coordinate $z_{B,i-1}$ remains the same and equal to $\langle\psi_{i-1}|\mathbb{I}_{\mathcal{A}}\otimes\mathbb{I}_{\mathcal{M}}\otimes\Pi^{[z_{B,i-1}]}|\psi_{i-1}\rangle$. Note also that for every $z_{B,i-1}$, i.e. for every horizontal line, we can define the functions

$$\begin{aligned} p_{n-i+1}(\cdot,z_{B,i-1}) &= \mathrm{prob}[Z_{A,i-1}\otimes\mathbb{I}_{\mathcal{M}}\otimes\Pi^{[z_{B,i-1}]},\psi_{i-1}], \\ p_{n-i}(\cdot,z_{B,i-1}) &= \mathrm{prob}[U_{A,i}^\dagger E_{A,i}(Z_{A,i}\otimes\mathbb{I}_{\mathcal{M}})E_{A,i}U_{A,i}\otimes\Pi^{[z_{B,i-1}]},\psi_{i-1}], \end{aligned}$$

and from the dual SDP condition we have $Z_{A,i-1}\otimes\mathbb{I}_{\mathcal{M}}\otimes\Pi^{[z_{B,i-1}]} \succeq U_{A,i}^\dagger E_{A,i}(Z_{A,i}\otimes\mathbb{I}_{\mathcal{M}})E_{A,i}U_{A,i}\otimes\Pi^{[z_{B,i-1}]}$. Similarly, for i even, the points move only vertically and the total weight on every vertical line remains unchanged.

We are now ready to define our point game. In plain words, a point game is a sequence of moves of weighted points. It starts with two points with weight $1/2$ at coordinates $[1,0]$ and $[0,1]$. Odd transitions are called horizontal transitions since the points seem to move horizontally, in the sense that the sum of the weights of the points on any horizontal line remains unchanged. Even transitions are called vertical transitions. At the end of the game, only one final point remains with weight 1 at coordinates $[\beta,\alpha]$. More formally,

Definition 4.8 (EBM line transition) *Let $l, r : [0,\infty) \to [0,\infty)$ be two functions with finite supports. The line transition $l \to r$ is* expressible by matrices *(EBM) if there exist positive semidefinite matrices $0 \preceq X \preceq Y$ and a (not necessarily unit) vector $|\psi\rangle$ such that $l = \mathrm{prob}[X,\psi]$ and $r = \mathrm{prob}[Y,\psi]$.*

We have already seen that any protocol and dual feasible point give rise only to EBM line transitions.

Definition 4.9 (EBM transition) *Let $p, q : [0,\infty) \times [0,\infty) \to [0,\infty)$ be two functions with finite supports. The transition $p \to q$ is an* EBM horizontal transition *if for all $y \in [0,\infty)$, $p(\cdot,y) \to q(\cdot,y)$ is an EBM line transition, and an* EBM vertical transition *if for all $x \in [0,\infty)$, $p(x,\cdot) \to q(x,\cdot)$ is an EBM line transition.*

Definition 4.10 (EBM point game) *An* EBM point game *is a sequence of functions $\{p_0, p_1, \cdots, p_n\}$ with finite support such that:*

- $p_0 = 1/2[0,1] + 1/2[1,0]$*;*
- *For all even i, $p_i \to p_{i+1}$ is an EBM vertical transition;*
- *For all odd i, $p_i \to p_{i+1}$ is an EBM horizontal transition;*
- $p_n = 1[\beta,\alpha]$*.*

We saw that a protocol with cheating probabilities $P_A^* \le \alpha$ and $P_B^* \le \beta$ and a dual feasible point give rise to an EBM point game with final point $[\beta,\alpha]$. Our goal is to show the reverse implication, namely that any EBM point game with final point $[\beta,\alpha]$ implies the existence of a protocol with cheating probabilities $P_A^* \le \alpha$ and $P_B^* \le \beta$.

Theorem 4.11 (EBM to Protocol) *From any EBM point game with final point $[\beta,\alpha]$, we can construct a weak coin flipping protocol with cheating probabilities $P_A^* \le \alpha$ and $P_B^* \le \beta$.*

Proof. Consider an EBM point game with transitions $p_0 \to p_1 \to \cdots \to p_n = [\beta,\alpha]$ and let us define the sets of all possible first and second coordinates z_A and z_B of all the points that appear in the game:

$$S_A = \{z_A \ge 0 \mid \exists i \in \{0,\dots,n\},\ \exists z_B \ge 0,\ p_i(z_A,z_B) > 0\}\,,$$
$$S_B = \{z_B \ge 0 \mid \exists i \in \{0,\dots,n\},\ \exists z_A \ge 0,\ p_i(z_A,z_B) > 0\}\,.$$

We wish to find a protocol (honest states, unitaries, projections) and a dual feasible point that guarantees that in this protocol Alice's and Bob's cheating probabilities are upper-bounded by α and β respectively. The idea is the following: every point $[z_A,z_B]$ of the game will be represented as an orthogonal state $|0,z_A\rangle|z_A,z_B\rangle|z_B,0\rangle \in \mathcal{A}\otimes\mathcal{M}\otimes\mathcal{B}$, where

$$\mathcal{A} = \mathrm{span}\{|b,z_A\rangle,\ b\in\{0,1\},\ z_A\in S_A\},$$
$$\mathcal{M} = \mathcal{A}'\otimes\mathcal{B}' = \mathrm{span}\{|z_A,z_B\rangle,\ z_A\in S_A,\ z_B\in S_B\},$$
$$\mathcal{B} = \mathrm{span}\{|z_B,b\rangle,\ b\in\{0,1\},\ z_B\in S_B\}.$$

The honest state $|\psi_i\rangle$ of the protocol at round i will be

$$|\psi_i\rangle = \sum_{z_A \in S_A, z_B \in S_B} \sqrt{p_{n-i}(z_A, z_B)}|0, z_A\rangle|z_A, z_B\rangle|z_B, 0\rangle.$$

The message space $\mathcal{M}$ contains the states that correspond to all the points of the game so that both players have alternate access to them and can manipulate their amplitudes by applying a unitary operation. The role of the unitary U_i is to transform the state $|\psi_{i-1}\rangle$ to the state $|\psi_i\rangle$, in other words $U_i|\psi_{i-1}\rangle = |\psi_i\rangle$. Moreover, we need to ensure that when Alice (resp. Bob) applies a unitary, then it corresponds to a horizontal (resp. vertical) line transition; in other words that the sum of the squares of the amplitudes of the states with a fixed second (resp. first) coordinate remains unchanged. The way to achieve this, is to force Alice to perform a unitary on the message space and her workspace which only uses the second coordinate of the points as a control (similarly we need to force Bob to perform a unitary which only uses the first coordinate of the points as a control). For this reason, Alice (resp. Bob) keeps a copy of the first (resp. second) coordinate of the points and each has a qubit that becomes 1 (via the unitary operation) when they catch the other player cheating, ie. not using the coordinate only as control. We define the cheating detection projections $E_{A,i} = E_A = \sum_{z_A} |0, z_A, z_A\rangle\langle 0, z_A, z_A| \otimes \mathbb{I}_{\mathcal{B}}$ and $E_{B,i} = E_B = \sum_{z_B} |0, z_B, z_B\rangle\langle 0, z_B, z_B| \otimes \mathbb{I}_{\mathcal{A}}$ that allow Alice and Bob to prematurely end the protocol and declare themselves winner. Note that these projections leave the honest states invariant.

It remains to find the unitaries U_i and the matrices Z_i. Let us assume that i is odd (similarly for i even), hence the transition $p_{n-i} \to p_{n-i+1}$ is horizontal; that is Alice applies the unitary $U_i = U_{A,i} \otimes \mathbb{I}_{\mathcal{B}}$. Since we want this unitary to use the second coordinate only as control we have $U_{A,i} = \sum_{z_B} U_{A,i}^{(z_B)} \otimes |z_B\rangle\langle z_B|$. Define the (non-normalized) states $|\psi_{i-1}^{(z_B)}\rangle = \sum_{z_A \in S_A} \sqrt{p_{n-i+1}(z_A, z_B)}|0, z_A, z_A\rangle$. Then in order to have $U_i|\psi_{i-1}\rangle = |\psi_i\rangle$, we need that $U_{A,i}^{(z_B)}|\psi_{i-1}^{(z_B)}\rangle = |\psi_i^{(z_B)}\rangle$.

We find the unitaries $U_{A,i}^{(z_B)}$ for $i = 1, \ldots, n$ and a single matrix $Z_A (= Z_{A,1} = \cdots = Z_{A,n-1})$ by expressing each EBM line transition $p_{n-i}(\cdot, z_B) \to p_{n-i+1}(\cdot, z_B)$ as $\mathrm{prob}[X, \psi] \to \mathrm{prob}[Y, \psi]$, where the matrices X, Y and the state $|\psi\rangle$ satisfy the properties of the following lemma:

Lemma 4.12 *Let $l \to r$ be an EBM line transition and denote by $\mathrm{supp}(l)$ and $\mathrm{supp}(r)$ the supports of l and r respectively. Let S be a set such that $\mathrm{supp}(l) \cup \mathrm{supp}(r) \subseteq S$ and $\Lambda > \max\{z : z \in S\}$. Given a set of orthonormal vectors $\{|z\rangle, z \in S\}$, there exists a family of $|S|$ orthonormal vectors $\{|\varphi(z)\rangle,\ z \in S\}$ in the $2|S|^2$-dimensional space $\mathrm{span}\{|b, z, z'\rangle,\ b \in \{0, 1\},\ z, z' \in S\}$ such that*

- *the state $|\psi\rangle = \sum_z \sqrt{r(z)}|0, z, z\rangle$ can be expressed as $|\psi\rangle = \sum_z \sqrt{l(z)}|\varphi(z)\rangle$,*
- *$l = \mathrm{prob}[X, \psi]$ and $r = \mathrm{prob}[Y, \psi]$, with*

$$Y = \sum_{z \in S} z|0, z, z\rangle\langle 0, z, z| + \Lambda \sum_{z \in S} |1, z, z\rangle\langle 1, z, z| \quad \textit{and} \quad X = \sum_{z \in S} z|\varphi(z)\rangle\langle\varphi(z)|.$$

We defer the proof of this lemma to the end of the section.

For each $z_B \in S_B$ and each EBM line transition $p_{n-i}(\cdot, z_B) \to p_{n-i-1}(\cdot, z_B)$, we apply Lemma 4.12 with $S = S_A$. This defines

$$\begin{aligned} X_i^{(z_B)} &= \sum_{z_A \in S_A} z_A |\varphi_i^{(z_B)}(z_A)\rangle\langle\varphi_i^{(z_B)}(z_A)| \\ Y &= \sum_{z_A \in S_A} z_A |0, z_A, z_A\rangle\langle 0, z_A, z_A| + \Lambda \sum_{z_A \in S_A} |1, z_A, z_A\rangle\langle 1, z_A, z_A| \\ |\psi_{i-1}^{(z_B)}\rangle &= \sum_{z_A \in S_A} \sqrt{p_{n-i+1}(z_A, z_B)} |0, z_A, z_A\rangle = \sum_{z_A} \sqrt{p_{n-i}(z_A, z_B)} |\varphi_i^{(z_B)}(z_A)\rangle \end{aligned}$$

We can now define the unitary $U_{A,i}^{(z_B)}$ by its action on a subspace of $\mathcal{A} \otimes \mathcal{A}'$:

$$U_{A,i}^{(z_B)} : |\varphi_i^{(z_B)}(z_A)\rangle \mapsto |0, z_A, z_A\rangle.$$

We complete $U_{A,i}^{(z_B)}$ so that it is a unitary on $\mathcal{A} \otimes \mathcal{A}'$. Note that we have:

$$\begin{aligned} U_{A,i}^{(z_B)} \sum_{z_A} \sqrt{p_{n-i+1}(z_A, z_B)} |0, z_A, z_A\rangle &= U_{A,i}^{(z_B)} \sum_{z_A} \sqrt{p_{n-i}(z_A, z_B)} |\varphi_i^{(z_B)}(z_A)\rangle \\ &= \sum_{z_A} \sqrt{p_{n-i}(z_A, z_B)} |0, z_A, z_A\rangle. \end{aligned}$$

and thus have $U_i|\psi_{i-1}\rangle = |\psi_i\rangle$. Moreover, by the definition of the unitary and the cheating detection projection, we can see that indeed Bob is forced to use the first coordinate only as control.

Last, we define $Z_A = \sum_{z_A \in S_A} z_A |0, z_A\rangle\langle 0, z_A| + \Lambda \sum_{z_A \in S_A} |1, z_A\rangle\langle 1, z_A|$. We need to verify that the Z_A's we defined are a dual feasible point. According to the constraints of the dual, we pick $Z_{A,n} = \Pi_A^{(1)} = |0, 1\rangle\langle 0, 1|$. Since the initial points of the point game are $[0, 1]$ and $[1, 0]$, then 1 is an eigenvalue of Z_A, so we have $\Pi_A^{(1)} \preceq Z_A$, i.e. $Z_{A,n} \preceq Z_{A,n-1}$. For $i = \{0, \dots, n-1\}$, we have

$$\begin{aligned} U_{A,i}^{\dagger} E_A (Z_A \otimes \mathbb{I}_{\mathcal{M}}) E_A U_{A,i} &= U_{A,i}^{\dagger} \left(\sum_{z_A} z_A |0, z_A, z_A\rangle\langle 0, z_A, z_A| \otimes \sum_{z_B} |z_B\rangle\langle z_B| \right) U_{A,i} \\ &= \sum_{z_B} \sum_{z_A} z_A U_{A,i}^{(z_B)\dagger} |0, z_A, z_A\rangle\langle 0, z_A, z_A| U_{A,i}^{(z_B)} \otimes |z_B\rangle\langle z_B| \\ &= \sum_{z_B} X_i^{(z_B)} \otimes |z_B\rangle\langle z_B| \\ &\preceq Y \otimes \mathbb{I}_{\mathcal{B}'} \\ &= \left(\sum_{z_A \in S_A} z_A |0, z_A, z_A\rangle\langle 0, z_A, z_A| + \Lambda |1, z_A, z_A\rangle\langle 1, z_A, z_A| \right) \otimes \mathbb{I}_{\mathcal{B}'} \\ &\preceq \left(\sum_{z_A, z_A' \in S_A} z_A |0, z_A, z_A'\rangle\langle 0, z_A, z_A'| + \Lambda |1, z_A, z_A'\rangle\langle 1, z_A, z_A'| \right) \otimes \mathbb{I}_{\mathcal{B}'} \\ &= Z_A \otimes \mathbb{I}_{\mathcal{M}}. \end{aligned}$$

To see that the first inequality is correct, consider a state $|\zeta\rangle$ in $\mathcal{A}\otimes\mathcal{M}$, $|\zeta\rangle = \sum_{z_B} |\zeta_{z_B}\rangle|z_B\rangle$. We get $\langle\zeta| \left(\sum_{z_B} X_i^{(z_B)} \otimes |z_B\rangle\langle z_B|\right) |\zeta\rangle = \sum_{z_B} \langle\zeta_{z_B}|X_i^{(z_B)}|\zeta_{z_B}\rangle \leq \sum_{z_B} \langle\zeta_{z_B}|Y|\zeta_{z_B}\rangle = \langle\zeta|Y \otimes \mathbb{I}_{\mathcal{B}'}|\zeta\rangle$ by Lemma 4.12, hence $\sum_{z_B} X_i^{(z_B)} \otimes |z_B\rangle\langle z_B| \preceq Y \otimes \mathbb{I}_{\mathcal{B}'}$. □

We remark that by the definition of the honest states, the projections, the unitaries and the dual feasible point, we have shown that any EBM line transition can be expressed as

$$\begin{aligned}
p_{n-i+1}(\cdot, z_B) &= \mathrm{prob}[Z_A \otimes \mathbb{I}_{\mathcal{A}'}, \psi_{i-1}^{(z_B)}] = \mathrm{prob}[Z_A \otimes \mathbb{I}_{\mathcal{M}} \otimes \Pi^{[z_B]}, \psi_{i-1}],\\
p_{n-i}(\cdot, z_B) &= \mathrm{prob}[U_{A,i}^{(z_B)\dagger} E_A (Z_A \otimes \mathbb{I}_{\mathcal{A}'}) E_A U_{A,i}^{z_B}, \psi_{i-1}^{(z_B)}]\\
&= \mathrm{prob}[U_{A,i}^{\dagger} E_A (Z_A \otimes \mathbb{I}_{\mathcal{M}}) E_A U_{A,i} \otimes \Pi^{[z_B]}, \psi_{i-1}].
\end{aligned}$$

This is precisely the type of EBM line transitions that arose when we started from a protocol and a dual feasible point.

Proof of Lemma 4.12. Let $l \to r$ be an EBM line transition, so by definition there exist two positive semidefinite matrices $X_0 \preceq Y_0$ and a vector $|\psi_0\rangle$ such that $l = \mathrm{prob}[X_0, \psi_0]$ and $r = \mathrm{prob}[Y_0, \psi_0]$. We will now make a succession of transformations to X_0, Y_0 and $|\psi_0\rangle$ in order to show that they can satisfy the properties of the Lemma.

Notice that the size of the matrices X_0 and Y_0 is unknown. We first see that we can decrease their size to at most $|S|$. We start by diagonalizing X_0 and Y_0:

$$X_0 = \sum_x x\Pi_{X_0}^{[x]} \qquad \text{and} \qquad Y_0 = \sum_y y\Pi_{Y_0}^{[y]}.$$

To remove the multiplicities of the eigenvalues, we go into the Hilbert space $\mathcal{H}$, spanned by $\{\Pi_{X_0}^{[x]}|\psi_0\rangle, \Pi_{Y_0}^{[y]}|\psi_0\rangle\}$. This space has dimension at most $|\mathrm{supp}(p) \cup \mathrm{supp}(q)| \leq |S|$. We define the new $|\psi\rangle = \Pi_{\mathcal{H}}|\psi_0\rangle$ as the projection of $|\psi_0\rangle$ on $\mathcal{H}$ and the matrices X and Y by

$$X = \sum_x x\Pi_X^{[x]} \quad \text{and} \quad Y = \sum_y y\Pi_Y^{[y]},$$

where $\Pi_X^{[x]}$ is the projector onto the one-dimensional space spanned by $\Pi_{X_0}^{[x]}|\psi_0\rangle$ and $\Pi_Y^{[y]}$ is the projector onto the one-dimensional space spanned by $\Pi_{Y_0}^{[y]}|\psi_0\rangle$. These matrices have size at most $|S|$. By construction, the matrices X, Y and the vector $|\psi\rangle$ satisfy the four properties

- $X \preceq Y$,
- $l = \mathrm{prob}[X, \psi]$ and $r = \mathrm{prob}[Y, \psi]$,
- The eigenvalues of X are in $\mathrm{supp}(l)$ with multiplicity 1,
- The eigenvalues of Y are in $\mathrm{supp}(r)$ with multiplicity 1.

Then, we will append the values in S that are not yet into the spectra of X and Y. This is done by increasing the dimension of the matrices and the vector $|\psi\rangle$ by the following algorithm: For each z in S do:

- if z is in the spectrum of X but not Y, $X \leftarrow X \oplus [0]$ and $Y \leftarrow Y \oplus [z]$;

- if z is in the spectrum of Y but not X, $X \leftarrow X \oplus [z]$ and $Y \leftarrow Y \oplus [\Lambda]$;
- if z is neither in the spectrum of X nor Y, $X \leftarrow X \oplus [z]$ and $Y \leftarrow Y \oplus [z]$.

The output of this algorithm are matrices of size less or equal to $2\,|S|$. We append extra 0 to X and extra Λ to Y until they have exactly size $2\,|S|$. We also increase the dimension of $|\psi\rangle$ by appending 0's.

We have constructed two matrices $0 \preceq X \preceq Y$ and a vector $|\psi\rangle$ of dimension $2\,|S|$ such that $l = \mathrm{prob}[X, \psi]$ and $r = \mathrm{prob}[Y, \psi]$. Moreover the spectrum of X is exactly $\{0\} \cup S$ and all non zero eigenvalues have multiplicity one; the spectrum of Y is exactly $S \cup \{\Lambda\}$ and all the eigenvalues in S have multiplicity one. Thus, they can be decomposed as:

$$X = \sum_{z \in S} z|u_z\rangle\langle u_z| \quad \text{and} \qquad Y = \sum_{z \in S} z|v_z\rangle\langle v_z| + \Lambda P,$$

where the $\{|u_z\rangle\}$ and $\{|v_z\rangle\}$ are orthonormal families of vectors and P is the projector onto the complement of $\mathrm{span}\{|v_z\rangle\}$.

We now increase the size of X, Y, and $|\psi\rangle$ by appending 0's to all of them until they reach size $2|S|^2$. In particular, we can write $X = \sum_{z\in S} z|u'_z\rangle\langle u'_z|$ and $Y = \sum_{z\in S} z|v'_z\rangle\langle v'_z| + \Lambda P'$ where $|u'_z\rangle = |u_z\rangle \otimes |0^S\rangle$, $|v'_z\rangle = |v_z\rangle \otimes |0^S\rangle$, and $P' = P \otimes |0^S\rangle\langle 0^S|$. As a consequence, P' is a projector on a $|S|$-dimensional subspace of the $2|S|^2$-dimensional space. Then, let U be a unitary that maps $|v'_z\rangle$ to $|0, z, z\rangle$ and sends P' to $\sum_z |1, z, z\rangle\langle 1, z, z|$ (Such unitary exists since P' is a projector onto a space of size $|S|$ orthogonal to the space spanned by the vectors $\{|u'_z\rangle,\ z \in S\}$). We define $|\varphi(z)\rangle = Ue^{i\theta_z}|u'_z\rangle$ so that applying U to X, Y, and $|\psi\rangle$ leads to:

$$X = \sum_{z\in S} z|\varphi(z)\rangle\langle\varphi(z)|\ ;\ Y = \sum_{z\in S} z|0, z, z\rangle\langle 0, z, z| + \Lambda|1, z, z\rangle\langle 1, z, z| \text{ and } |\psi\rangle = \sum_z \sqrt{l(z)}|\varphi(z)\rangle.$$

□

4.2.2 Valid point games

Here is where we stand now: we have defined points games as a sequence of EBM transitions, starting at points $1/2[0, 1] + 1/2[1, 0]$ and ending at some point $[\beta, \alpha]$. We have also shown that for each point game with final point $[\beta, \alpha]$, we can construct a balanced weak coin flipping protocol with cheating probabilities $P_A^* \leq \alpha$ and $P_B^* \leq \beta$. Our goal is thus to find a point game with final point $[\frac{1}{2} + \varepsilon, \frac{1}{2} + \varepsilon]$ for any $\varepsilon > 0$.

This task is quite a challenge and the formalism of EBM transitions (prob functions, matrices, vectors) is not very practical. As a matter of fact, to check that a transition is EBM, we need to check an existence property. The strategy we are following in this section is to turn the *existential* definition of EBM transitions into a *universal* characterization. The way we wish to accomplish that is by seeing the set of EBM transitions as a dual of another set. This is the main idea, however reality is a bit more complicated.

First, we change our point of view and we see the EBM line transitions as functions. In other words, instead of considering a line transition $l \to r$, we will manipulate the function with finite support $h = r - l$.

We will see in this section how the bidual of EBM functions allows us to define *valid functions* (and thus *valid transitions*). Unfortunately, the set of valid functions is a superset of the set of EBM functions, which means that all valid transitions are not necessarily EBM transitions. The main problem comes from the fact that the set of EBM functions is not closed while the set of valid functions is. On the other hand, valid transitions are much nicer to work with since they have a very simple characterization, as we will see in Section 4.2.2. The solution comes from the fact that even though not all valid transitions are EBM transitions, they can all be approximated by EBM transitions.

Theorem 4.13 (Valid to EBM) *Given a point game with valid transitions and final point $[\beta, \alpha]$ and any $\varepsilon > 0$, there is a point game with EBM transitions and final point $[\beta + \varepsilon, \alpha + \varepsilon]$.*

Hence our goal has become to find a point game with valid transitions and final point $[\frac{1}{2} + \varepsilon, \frac{1}{2} + \varepsilon]$ for any $\varepsilon > 0$. The following subsections are devoted to proving the above theorem.

EBM functions and EBM functions on $[0, \Lambda]$

Let us first describe the topological space we will be working in. This is the set V of functions from $[0, \infty)$ to $\mathbb{R}$ with finite support. V is an infinite dimensional vector space spanned by the canonical basis $\{[x]\}_{x\in[0,\infty)}$ where $[x](y) = \delta_{x,y}$ is the Kronecker delta function. Each element v of V can be written as $v = \sum_x v(x)[x]$. The usual norm on this space is the 1-norm, which is defined for any $v = \sum_x v(x)[x]$ as $\|v\|_1 = \sum_x |v(x)|$.

We now define the set K of EBM functions.

Definition 4.14 (K, EBM functions) *A function $h : [0, \infty) \to \mathbb{R}$ with finite support is an* EBM function *if the line transition $h^- \to h^+$ is expressible by matrices (EBM), where $h^+ : [0, \infty) \to [0, \infty)$ and $h^- : [0, \infty) \to [0, \infty)$ denotes respectively the positive and the negative part of h ($h = h^+ - h^-$). We denote by K the set of EBM functions.*

We would like to better characterize the set K. It is known, that for any closed convex cone $C \subset V$, we can define the space V' as the space of continuous functions from V to $\mathbb{R}$ and the dual cone C^* of C as

$$C^* = \{\Phi \in V', \ \forall h \in C, \Phi(h) \geq 0\}$$

Since C is a closed convex cone, C can be recovered from the dual cone $(C^*)^*$ of C^* as follows

Proposition 4.15 ([DR09]) *If C is a closed convex cone then*

$$C = \{h \in V, \ \forall \Phi \in C^*, \Phi(h) \geq 0\}$$

This provides a *universal* characterization of the set C.

We can show that K is a convex cone, but unfortunately it is not closed. However, if we restrict the support of elements of K to be on the closed interval $[0, \Lambda]$, then the resulting set is a closed convex cone.

Definition 4.16 (K_Λ) *A function $h : [0, \Lambda) \to \mathbb{R}$ with finite support is an* EBM function with support on $[0, \Lambda]$ *if the line transition $h^- \to h^+$ is expressible by matrices with spectrum in $[0, \Lambda]$, where h^+ and h^- denotes respectively the positive and the negative part of h. We denote by K_Λ the set of EBM functions with support on $[0, \Lambda]$.*

Note that when we restrict the spectrum of the matrices in the above definition to $[0, \Lambda]$, then the support of the corresponding function is also in $[0, \Lambda]$.

The proof that K_Λ is a closed convex cone follows from Lemma 4.17 and 4.18.

Lemma 4.17 *For any $\Lambda > 0$, K_Λ is a convex cone.*

Proof. Fix $\Lambda > 0$. Let $g, h \in K_\Lambda$, so $g^- \to g^+$ and $h^- \to h^+$ are two EBM line transitions, i.e. we can write them as: $g^- = \text{prob}[X_g, \psi_g]$, $g^+ = \text{prob}[Y_g, \psi_g]$, $h^- = \text{prob}[X_h, \psi_h]$ and $h^+ = \text{prob}[Y_h, \psi_h]$. (note that the dimensions of X_g and Y_g are not necessarily the same as the ones of X_h and Y_h)

K_Λ is a cone since for all $\lambda \geq 0$, $\lambda g = \lambda g^+ - \lambda g^- = \text{prob}[Y_g, \sqrt{\lambda}|\psi_g\rangle] - \text{prob}[X_g, \sqrt{\lambda}|\psi_g\rangle]$ and hence $\lambda g^- \to \lambda g^+$ is expressible by matrices with spectra in in $[0, \Lambda]$.

Let us finally show K_Λ is convex. It is enough to prove that $g + h \in K_\Lambda$. Construct $X = X_g \oplus X_h = \begin{bmatrix} X_g & 0 \\ 0 & X_h \end{bmatrix}$, $Y = Y_g \oplus Y_h = \begin{bmatrix} Y_g & 0 \\ 0 & Y_h \end{bmatrix}$ and $|\psi\rangle = |\psi_g\rangle \oplus |\psi_h\rangle = \begin{bmatrix} \psi_g \\ \psi_h \end{bmatrix}$. We now have

$$g^- + h^- = \text{prob}[X, \psi] \quad \text{and} \quad g^+ + h^+ = \text{prob}[Y, \psi].$$

Since we also have that $\text{sp}(X), \text{sp}(Y) \subset [0, \Lambda]$, we can conclude that K_Λ is convex. □

Lemma 4.18 *For any $\Lambda > 0$, K_Λ is closed.*

Proof. Fix $\Lambda > 0$. Let $\{t_i\}_{i \in \mathbb{N}}$ be a converging sequence of functions in K_Λ, and denote the limit of this sequence $t = \lim_{i \to \infty} t_i$. The rest of the proof is devoted to show that $t \in K_\Lambda$. Denote $t = \sum_x t(x)[x]$ and S the support of t, that is the set $S = \{x : t(x) \neq 0\}$. Note that t is an element of V so t has finite support. Since the t_i are EBM, we write $t_i = \text{prob}[Y_i, \psi_i] - \text{prob}[X_i, \psi_i]$, with $0 \preceq X_i \preceq Y_i$. Each of the X_i's and Y_i's can be diagonalized:

$$X_i = \sum_{x^{(i)}} x^{(i)} \Pi^{[x^{(i)}]} \quad \text{and} \quad Y_i = \sum_{y^{(i)}} y^{(i)} \Pi^{[y^{(i)}]},$$

where $\Pi^{[x^{(i)}]}$ is the projector onto the eigenspace of X_i with eigenvalue $x^{(i)}$. Since there will be no confusion, we drop the exponent (i) from now on. Let us define the matrices:

$$A_i = \sum_{x \in S} x\Pi^{[x]} + \sum_{x \notin S} 0 \cdot \Pi^{[x]} \quad \text{and} \quad B_i = \sum_{y \in S} y\Pi^{[y]} + \sum_{y \notin S} \Lambda \cdot \Pi^{[y]}.$$

First note that we immediately have $0 \preceq A_i \preceq X_i \preceq Y_i \preceq B_i$ so we can define an EBM function $t'_i = \text{prob}[B_i, \psi_i] - \text{prob}[A_i, \psi_i]$. The dimension of the matrices A_i are not necessarily identical, but this is not a problem. As done in the proof of Lemma 4.12 ("getting rid of the multiplicities" and "appending the missing eigenvalues"), we construct the positive semidefinite matrices A'_i, B'_i of size $s = 2|S|$ and the vectors $|\psi'_i\rangle$ also of dimension s such that $t'_i = \text{prob}[B'_i, \psi'_i] - \text{prob}[A'_i, \psi'_i]$. Notice also that the spectra of the A'_i and the B'_i are in the interval $[0, \Lambda]$.

We show that $\lim_{i \to \infty} t'_i = t$. We write each t_i as $t_i = u_i + v_i$, where $u_i = \sum_{x \in S} t_i(x)[x]$ and $v_i = \sum_{x \notin S} t_i(x)[x]$. Let $\varepsilon_i = \sum_{x \notin S} t_i(x)$. Since $\lim_{i \to \infty} t_i = t$, we have $\lim_{i \to \infty} \varepsilon_i = 0$. Our construction of t'_i implies that $t'_i = u_i + \varepsilon_i^+[\Lambda] - \varepsilon_i^-[0]$ with $\varepsilon_i^+ + \varepsilon_i^- = \varepsilon_i$. This means in particular that $\|t'_i - t_i\|_1 \leq \varepsilon_i$. Since $\lim_{i \to \infty} \varepsilon_i = 0$ and $\lim_{i \to \infty} t_i = t$, we conclude that $\lim_{i \to \infty} t'_i = t$.

We will now show that the limit of the sequence $\{t'_i\}_{i \in \mathbb{N}}$ is an element $t' \in K_\Lambda$ which will conclude the proof. We consider the sequence of triplets $\{(A'_i, B'_i, |\psi'_i\rangle)\}_{i \in \mathbb{N}}$. Let X^s_Λ the set of positive semidefinite matrices with spectrum in $[0, \Lambda]$ and Y^s the set of quantum states of dimension s. An element of the sequence is an element of $X^s_\Lambda \times X^s_\Lambda \times Y^s$. Since X^s_Λ and Y^s are two compact sets, $X^s_\Lambda \times X^s_\Lambda \times Y^s$ is also a compact set. This means that our sequence of triplets has an accumulation point $(A', B', |\psi'\rangle)$ even if this sequence does not necessarily converge.

Let us now define $t' = \text{prob}[B', \psi'] - \text{prob}[A', \psi']$. Since $0 \preceq A' \preceq B'$, we have $t' \in K_\Lambda$. We can also see that t' is an accumulation point of the sequence $\{t'_i\}_i$. Since the sequence of t'_i's converges to t, we conclude that $t = t'$ and $t \in K_\Lambda$. □

We proved that K_Λ is a convex cone. From Proposition 4.15, we have

Proposition 4.19 $K_\Lambda = \{h, \forall \Phi \in K^*_\Lambda, \Phi(h) \geq 0\}$

We now go back to the language of transitions and provide a characterization of an EBM line transition on $[0,\Lambda]$ (ie. a line transition expressible by matrices with spectra on $[0,\Lambda]$).

Proposition 4.20 *Let $l, r : [0,\Lambda] \to [0,\infty)$ be two functions with finite support on $[0,\Lambda]$. The line transition $l \to r$ is EBM on $[0,\Lambda]$ if and only if $\forall \Phi \in K^*_\Lambda, \Phi(r-l) \geq 0$.*

Proof. The forward direction follows immediately from Proposition 4.19. We now prove the opposite direction. This direction is immediately true from Proposition 4.19 if l and r have disjoint supports. We show that this still holds in the general case. Let l, r two non negative functions with finite support on $[0,\Lambda]$ such that $\forall \Phi \in K^*_\Lambda, \Phi(r-l) \geq 0$. Let $l = l' + \xi$ and $r = r' + \xi$ where ξ is a positive function and l' and r' have disjoint supports and are non negative.

For any $\Phi \in K^*_\Lambda$, we have $\Phi(r' - l') = \Phi(r-l) \geq 0$ hence $r' - l' \in K_\Lambda$ which means that $l' \to r'$ is an EBM line transition on $[0,\Lambda]$. In a similar flavor than in Lemma 4.17, we can append ξ to the EBM transition such that $l' + \xi \to r' + \xi$ is EBM on $[0,\Lambda]$. We conclude that $l \to r$ is EBM on $[0,\Lambda]$. □

EBM transitions and operator monotone functions

From the previous Proposition we have that a line transition $l \to r$ is EBM on $[0,\Lambda]$ if $\forall \Phi \in K^*_\Lambda, \Phi(r-l) \geq 0$. It is now the time to explicitly characterize the set K^*_Λ. Recall that

$$K^*_\Lambda = \{\Phi \in V', \forall h \in K_\Lambda, \Phi(h) \geq 0\}$$

There is a bijective mapping between Φ and f_Φ where f_Φ is a function on reals such that $\Phi([x]) = f_\Phi(x)$. This gives us by linearity of Φ that for a function $h = \sum_x h(x)[x]$ we have $\Phi(\sum_x h(x)[x]) = \sum_x h(x) f_\Phi(x)$. With this mapping, we can see elements of K^*_Λ as functions on reals.

We will show that up to this mapping, the set K^*_Λ is the set of operator monotone functions on $[0,\Lambda]$, which we define below.

Definition 4.21 (Operator monotone function) *A function $f : [0,\Lambda] \to \mathbb{R}$ is* operator monotone *on $[0,\Lambda]$ if for all positive semidefinite matrices $X \preceq Y$ with spectrum on $[0,\Lambda]$, we have $f(X) \preceq f(Y)$.*

A function $f : [0,\infty) \to \mathbb{R}$ is operator monotone *if for all positive semidefinite matrices $X \preceq Y$, we have $f(X) \preceq f(Y)$.*

Operator monotone functions have an analytic characterization:

Lemma 4.22 ([Bha97]) *Any operator monotone function $f : [0, \infty) \to \mathbb{R}$ can be written as*

$$f(t) = c_0 + c_1 t + \int_0^{+\infty} \frac{\lambda t}{\lambda + t} dw(\lambda)$$

for a measure w satisfying $\int_0^{+\infty} \frac{\lambda}{1+\lambda} dw(\lambda) < +\infty$.
Any operator monotone function $f : [0, \Lambda] \to \mathbb{R}$ can be written as

$$\tilde{f}(t) = c_0 + c_1 t + \int \frac{\lambda t}{\lambda + t} dw(\lambda)$$

with the integral ranging over $\lambda \in (-\infty, -\Lambda) \cup (0, +\infty)$.

Lemma 4.23 $\Phi \in K_\Lambda^* \Leftrightarrow f_\Phi$ *is operator monotone on* $[0, \Lambda]$.

Proof. Forward implication. We first notice that $\Phi \in K_\Lambda^*$ implies

$$\forall h \in K_\Lambda, \sum_x f_\Phi(x) h(x) \geq 0. \tag{4.1}$$

This is immediate from the definition of f_Φ. We now prove that a function f with finite support on $[0, \Lambda]$ satisfies (4.1) if and only if f is operator monotone on $[0, \Lambda]$. The proof of this equivalence is based on the following observation:

$$\sum_{x \in \mathrm{sp}(X)} f(x) \,\mathrm{prob}[X, \psi](x) = \sum_{x \in \mathrm{sp}(X)} f(x) \langle \psi | \Pi^{[x]} | \psi \rangle = \sum_{x \in \mathrm{sp}(X)} \langle \psi | f(x) \Pi^{[x]} | \psi \rangle = \langle \psi | f(X) | \psi \rangle.$$

Then,

$$\begin{aligned}
&\forall h \in K_\Lambda, \sum_x f(x) h(x) \geq 0 \\
&\quad \Leftrightarrow \forall |\psi\rangle, \ \forall\ 0 \preceq X \preceq Y \text{ with } \mathrm{sp}(X), \mathrm{sp}(Y) \subset [0, \Lambda], \\
&\qquad\quad \sum_x f(x) \left(\mathrm{prob}[Y, \psi](x) - \mathrm{prob}[X, \psi](x)\right) \geq 0 \\
&\quad \Leftrightarrow \forall |\psi\rangle, \ \forall\ 0 \preceq X \preceq Y \text{ with } \mathrm{sp}(X), \mathrm{sp}(Y) \subset [0, \Lambda], \ \langle \psi | f(X) | \psi \rangle \leq \langle \psi | f(Y) | \psi \rangle \\
&\quad \Leftrightarrow \forall\ 0 \preceq X \preceq Y \text{ with } \mathrm{sp}(X), \mathrm{sp}(Y) \subset [0, \Lambda], \ f(X) \preceq f(Y) \\
&\quad \Leftrightarrow f \text{ is operator monotone on } [0, \Lambda]
\end{aligned}$$

For the reverse implication, consider a pair (f_Φ, Φ) where f_Φ is a function with finite support on $[0, \Lambda]$ and Φ is its associated function in V'. Hence by the previous series of equivalence, we have $\forall h \in K_\Lambda, \ \Phi(h) \geq 0$. In order to prove that $\Phi \in K_\Lambda^*$ we need to show that Φ is continuous. Since f_Φ is operator monotone on $[0, \Lambda]$, f_Φ is increasing and $\forall x \in [0, \Lambda], \ f_\Phi(x) \in [f_\Phi(0), f_\Phi(\Lambda)]$, which means that $\|f_\Phi\|_\infty < +\infty$. Thus, for any $h = \sum_x h(x)[x]$, we have $\Phi_f(h) = \sum_x h(x) f_\Phi(x) \leq \|h\|_1 \|f_\Phi\|_\infty$, and hence Φ is continuous. □

Using Lemma 4.23 and Proposition 4.20, we have the following characterization of EBM line transitions on $[0, \Lambda]$.

Proposition 4.24 *Let $l, r : [0, \Lambda] \to [0, \infty)$ be two functions with finite support on $[0, \Lambda]$. The line transition $l \to r$ is EBM on $[0, \Lambda]$ if and only if $\forall f : [0, \Lambda] \to \mathbb{R}$ operator monotone on $[0, \Lambda]$, $\sum_x f(x) l(x) \leq \sum_x f(x) r(x)$.*

From the above proposition and Lemma 4.22, we have the following corollary

Corollary 4.25 *Let $l, r : [0,\Lambda] \to [0,\infty)$ be two functions with finite support on $[0,\Lambda]$. The line transition $l \to r$ is EBM on $[0,\Lambda]$ if and only if*

$$\sum_x l(x) = \sum_x r(x) \ ; \ \sum_x x(r(x) - l(x)) \geq 0 \ ; \ \forall \lambda \in (-\infty, -\Lambda] \cup (0,\infty), \ \sum_x \frac{\lambda x(r(x) - l(x))}{\lambda + x} \geq 0$$

Valid and strictly valid transitions

In the previous section, we gave a characterization of EBM line transitions on $[0,\Lambda]$ in terms of functions which are operator monotone on $[0,\Lambda]$. However, it is still not easy to manipulate this type of functions. Hence, we define a superset of EBM transitions, this time in terms of operator monotone functions (on $[0,\infty)$).

Definition 4.26 (Valid line transition) *Let $l, r : [0,\infty) \to [0,\infty)$ be two functions with finite supports. The line transition $l \to r$ is* valid *if for every operator monotone function $f : [0,\infty) \to \mathbb{R}$, we have $\sum_{x\in\text{supp}(l)} f(x)l(x) \leq \sum_{x\in\text{supp}(r)} f(x)r(x)$.*

Definition 4.27 (Valid transition) *Let $p, q : [0,\infty) \times [0,\infty) \to [0,\infty)$ be two functions with finite supports. The transition $p \to q$ is a* valid horizontal transition *if for all $y \in [0,\infty)$ the $p(\cdot, y) \to q(\cdot, y)$ is a valid line transition, and a* valid vertical transition *if for all $x \in [0,\infty)$ the $p(x,\cdot) \to q(x,\cdot)$ is a valid line transition.*

On the positive side, there is a simple way to verify whether a line transition is valid or not using the following Lemma:

Lemma 4.28 *Let l and r be two positive functions with finite support. $l \to r$ is a valid line transition if and only if $\sum_x l(x) = \sum_x r(x)$ and for all $\lambda > 0$, $\sum_x \frac{-1}{\lambda+x} r(x) \geq \sum_x \frac{-1}{\lambda+x} l(x)$.*

Proof. An immediate consequence of Lemma 4.22 and the definition of valid line transitions is that $l \to r$ is a valid line transition if and only if

❶ $\sum_x r(x) = \sum_x l(x)$

❷ for all $\lambda > 0$, $\sum_x \frac{\lambda x}{\lambda+x} r(x) \geq \sum_x \frac{\lambda x}{\lambda+x} l(x)$,

❸ $\sum_x x \cdot r(x) \geq \sum_x x \cdot l(x)$.

Condition ❸ is implied by condition ❷ in the limit $\lambda \to \infty$. Moreover, for all $\lambda > 0$ we have:

$$\sum_x \frac{\lambda x}{\lambda + x} r(x) \geq \sum_x \frac{\lambda x}{\lambda + x} l(x) \iff \sum_x \left(1 + \frac{-\lambda}{\lambda + x}\right) r(x) \geq \sum_x \left(1 + \frac{-\lambda}{\lambda + x}\right) l(x)$$
$$\iff \sum_x \frac{-1}{\lambda + x} r(x) \geq \sum_x \frac{-1}{\lambda + x} l(x)$$

by using property ❶. □

On the negative side, these transitions are indeed not necessarily EBM transitions. To circumvent this problem, we proceed as follows:

1. We consider a restriction of valid transitions, which we call strictly valid transitions and we show that such transitions are EBM transitions

2. From a point game with valid transitions and final point $[\beta, \alpha]$, we construct a point game with strictly valid transitions - and hence with EBM transitions - with final point $[\beta + \varepsilon, \alpha + \varepsilon]$, for all $\varepsilon > 0$.

Last, in the following Section, we will present a point game with valid transitions with final point $[\frac{1}{2} + \varepsilon, \frac{1}{2} + \varepsilon]$ for any $\varepsilon > 0$ which will, finally, imply the existence of a weak coin flipping protocol with arbitrarily small bias.

Strictly valid transitions

Definition 4.29 (Strictly valid line transition) *Let $l, r : [0, \infty) \to [0, \infty)$ be two functions with finite supports. The line transition $l \to r$ is* strictly valid *if it is a valid line transition and for every non-constant operator monotone function $f : [0, \infty) \to \mathbb{R}$, we have $\sum_{x \in \text{supp}(l)} f(x) l(x) < \sum_{x \in \text{supp}(r)} f(x) r(x)$.*

Using the characterization of operator monotone functions described in Lemma 4.22 and the same reasoning as in Lemma 4.28, we have

Corollary 4.30 *Let $l, r : [0, \infty) \to [0, \infty)$ be two functions with finite supports. The line transition $l \to r$ is* strictly valid *if*

$$\sum_x l(x) = \sum_x r(x) \ ; \ \sum_x x(r(x) - l(x)) > 0 \ ; \ \forall \lambda > 0, \ \sum_x \frac{\lambda x (r(x) - l(x))}{\lambda + x} > 0.$$

or equivalently if

$$\sum_x l(x) = \sum_x r(x) \ ; \ \forall \lambda > 0, \ \sum_x \frac{-1}{\lambda + x} r(x) > \sum_x \frac{-1}{\lambda + x} l(x).$$

Definition 4.31 (Strictly valid transition) *Let $p, q : [0, \infty) \times [0, \infty) \to [0, \infty)$ be two functions with finite supports. The transition $p \to q$ is a* strictly valid horizontal transition *if for all $y \in [0, \infty)$ with $\sum_x p'_i(x, y) = \sum_x p'_{i+1}(x, y) > 0$ the $p(\cdot, y) \to q(\cdot, y)$ is a strictly valid line transition, and a* strictly valid vertical transition *if for all $x \in [0, \infty)$ with $\sum_y p'_i(x, y) = \sum_y p'_{i+1}(x, y) > 0$ the $p(x, \cdot) \to q(x, \cdot)$ is a strictly valid line transition.*

Using Corollary 4.30, we can show the following

Lemma 4.32 *Any strictly valid transition is an EBM transition.*

Proof. We prove that for any strictly valid line transition, there exists a $\Lambda > 0$ such that the transition is an EBM line transition on $[0, \Lambda]$ and hence an EBM line transition. The proof easily extends to horizontal and vertical transitions.

Let $l \to r$ be a striclty valid line transition. The conditions of Corollary 4.30 are very close to the conditions in Corollary 4.25. We just need to show that there exists a Λ such that

$$\forall \lambda < -\Lambda, \ \sum_x \frac{\lambda x \ h(x)}{\lambda + x} \geq 0$$

We have

$$\lim_{\lambda \to -\infty} \sum_x \frac{\lambda x \ h(x)}{\lambda + x} = \sum_x x \ h(x) > 0.$$

If we consider $\sum_x \frac{\lambda x\ h(x)}{\lambda+x}$ as a function of λ, we have by continuity that there exists a $\Lambda > 0$ such that

$$\forall \lambda < -\Lambda, \quad \sum_x \frac{\lambda x\ h(x)}{\lambda + x} > 0,$$

which proves the Lemma. □

Approximating valid transitions with strictly valid transitions

Lemma 4.33 *Fix $\varepsilon > 0$. Given a point game with $2m$ valid transitions and final point $[\beta, \alpha]$, there exists a point game with $2m$ strictly valid transitions and final point $[\beta + \varepsilon, \alpha + \varepsilon]$.*

Proof. Consider a game with valid transitions $p_0 \to p_1 \to \cdots \to p_{2m}$. We will construct a new game with strictly valid transitions $p'_0 \to p'_1 \to \cdots \to p'_{2m}$. The idea to ensure strict validity, is to shift each point by an extra ε/m to the right for horizontal transitions and to the top for vertical transitions. After $2m$ transitions (m horizontal and m vertical), the final point will then be $[\beta + \varepsilon, \alpha + \varepsilon]$ as desired.

For all $i \neq 0$ and $\forall (x, y) \in \operatorname{supp}(p_i)$, we define the shifted points as:

$$\begin{aligned} p'_i(x + i\varepsilon/m, y + (i-1)\varepsilon/m) &= p_i(x, y) \quad \text{if } i \text{ is odd,} \\ p'_i(x + (i-1)\varepsilon/m, y + i\varepsilon/m) &= p_i(x, y) \quad \text{if } i \text{ is even.} \end{aligned}$$

Fix i even. We prove that the transition $p'_i \to \mathsf{p}'_{i+1}$ is a strictly valid horizontal transition by showing that for all $y \in [0, \infty)$ with $\sum_x p'_i(x, y) = \sum_x p'_{i+1}(x, y) > 0$ and for all non-constant operator monotones functions we have:

$$\begin{aligned} \sum_{x \in \operatorname{supp}(p'_{i+1})} p'_{i+1}(x, y) f(x) &= \sum_{x \in \operatorname{supp}(p'_{i+1})} p_{i+1}(x - (i+1)\varepsilon/m, y - i\varepsilon/m) f(x) \\ &= \sum_{x \in \operatorname{supp}(p_{i+1})} p_{i+1}(x, y - i\varepsilon/m) f(x + (i+1)\varepsilon/m) \\ &\geq \sum_{x \in \operatorname{supp}(p_i)} p_i(x, y - i\varepsilon/m) f(x + (i+1)\varepsilon/m) \\ &= \sum_{x \in \operatorname{supp}(p_i)} p'_i(x + (i-1)\varepsilon/m, y) f(x + (i+1)\varepsilon/m) \\ &= \sum_{x \in \operatorname{supp}(p'_i)} p'_i(x, y) f(x + 2\varepsilon/m) \\ &> \sum_{x \in \operatorname{supp}(p'_i)} p'_i(x, y) f(x) \end{aligned}$$

The first inequality follows from the validity of the transition $p_i \to p_{i+1}$ and by noticing that if $f(x)$ is an operator monotone function in x then $f(x+(i+1)\varepsilon/m)$ is also an operator monotone function in x. The second strict inequality follows from the fact that every no constant operator monotone function is strictly increasing. A similar proof holds for vertical transitions. □

Examples of valid line transitions

Point raise The transition $w[x] \to w[x']$ with $x' \geq x$ is a valid line transition.

We want to show that for all operator monotone functions f, $wf(x) \leq wf(x')$if and only if $x' \geq x$. By taking $f(x) = x$, we see that the condition is necessary. It is also sufficient since every operator monotone function is increasing.

Point merge The transition $w_1[x_1] + w_2[x_2] \to (w_1 + w_2)[x_3]$ is valid if and only if $x_3 \geq \frac{w_1 x_1 + w_2 x_2}{w_1 + w_2}$.

We want to show that for every operator monotone function, $w_1 f(x_1) + w_2 f(x_2) \leq (w_1 + w_2)[x_3]$ when $x_3 \geq \frac{w_1 x_1 + w_2 x_2}{w_1 + w_2}$. By taking $f(x) = x$, the above condition is necessary. This condition is also sufficient because operator monotone functions are concave.

Point split The transition $w[x] \to w_1[x_1] + w_2[x_2]$ with $w = w_1 + w_2$ is valid if and only if $\frac{w}{x} \geq \frac{w_1}{x_1} + \frac{w_2}{x_2}$.

We want to show that for every operator monotone function, $wf(x) \leq w_1 f(x_1) + w_2 f(x_2)$. By considering the function $f(x) = -\frac{1}{\lambda + x}$ and by considering the case where $\lambda \to 0$, we have $-\frac{w}{x} \leq -\frac{w_1}{x_1} - \frac{w_2}{x_2}$ which shows that the above condition is necessary.

We now show that the above condition is also sufficient. Assume that $\frac{w}{x} \geq \frac{w_1}{x_1} + \frac{w_2}{x_2}$. We want to verify that $wf(x) \leq w_1 f(x_1) + w_2 f(x_2)$ for $f(x) = -\frac{1}{\lambda + x}$. Let $q = \frac{1}{x}, q'_i = \frac{1}{x_i}$. Let a function $g(t) = -\frac{t}{1 + \lambda t}$. We have $-\frac{1}{\lambda + x} = g(w)$ and $-\frac{1}{\lambda + x_i} = g(w_i)$. This gives us

$$wf(x) = g(q) \leq g(\frac{w_1 q_1 + w_2 q_2}{w_1 + w_2}) \leq w_1 g(q_1) + w_2 g(q_2) = w_1 f(x_1) + w_2 f(x_2)$$

The first inequality holds because g is decreasing and the second inequality holds because g is convex. The special case of $f(x) = x$ follows by considering the limit $\lambda \to \infty$ when considering function $f(x) = \frac{\lambda x}{\lambda + x} = \lambda(1 + \lambda \cdot \frac{-1}{\lambda + x})$.

A last property that will be useful later on is that no valid point game puts any weight on the point $[0, 0]$.

Lemma 4.34 *A point game with valid transitions has no transition involving the point* $[0, 0]$.

Proof. It is sufficient to prove that there is no valid line transition $l \to w[0] + (1 - w)r$ where l and r are positive functions with finite support and $l(0) = r(0) = 0$. By contradiction, assume there exists such transition. In that case the second condition of Lemma 4.28 implies that for all $\lambda > 0$, we have $(1 - w)\sum_x \frac{-\lambda}{\lambda + x} r(x) - w \geq \sum_x \frac{-\lambda}{\lambda + x} l(x)$. The contradiction is obtained by taking the limit $\lambda \to 0$. □

4.2.3 Time independent point games

In the previous subsections, we showed that if there exists a point game with valid transitions and final point $[1/2 + \varepsilon, 1/2 + \varepsilon]$ for any $\varepsilon > 0$, then there exists a weak coin flipping protocol with arbitrarily small bias. We now introduce the last model, namely *time independent point games* (TIPG).

As its name suggests, the idea behind a time independent point game is to remove the time ordering of the transitions.In order to formally define time independent point games, we first extend the definition of valid functions, to 2-variable functions:

Definition 4.35 (Valid horizontal and vertical function) *Let $t : [0, \infty) \times [0, \infty) \to \mathbb{R}$ be a function with finite support.*

- *t is a* valid horizontal function *if for all $y \geq 0$, $t(\cdot, y)$ is a valid function;*
- *t is a* valid vertical function *if for all $x \geq 0$, $t(x, \cdot)$ is a valid function.*

The previous discussion leads to the following definition:

Definition 4.36 (Time independent point game) *A* time independent point game *is a valid horizontal function h and a valid vertical function v such that*

$$h + v = 1[\beta, \alpha] - \frac{1}{2}[0, 1] - \frac{1}{2}[1, 0].$$

We call the point $[\beta, \alpha]$ the final point of the game.

The interest of this model in comparison to point games with valid transitions is obvious: we only need to find two valid functions, instead of a sequence with an appropriate order. Even simpler, since $h + v = 0$ almost everywhere (except in $[0, 1]$, $[1, 0]$, and $[\beta, \alpha]$), it is enough to find a single valid function.

It is easy to construct a time independent point game with final point $[\beta, \alpha]$ from a point game with valid transitions and final point $[\beta, \alpha]$. As a matter of fact, h is the sum of the functions representing all the valid horizontal transitions, and v the sum of all the functions representing the vertical transitions. More interestingly, the reverse also holds:

Theorem 4.37 (TIPG to valid point games) *Assume there exists a time independent game with a valid horizontal function h and a valid vertical function v such that $h+v = 1[\beta, \alpha] - \frac{1}{2}[0, 1] - \frac{1}{2}[1, 0]$. Then, for all $\varepsilon > 0$, there exists a valid point game with final point $[\beta + \varepsilon, \alpha + \varepsilon]$.*

Before we prove the above theorem let us define *transitively valid transitions.*

Definition 4.38 (Transitively valid transition) *Let $p, q : [0, \infty) \times [0, \infty) \to [0, \infty)$ be two functions with finite support. The transition $p \to q$ is* transitively valid *if there exists a sequence of valid transitions $p_0 \to p_1, p_1 \to p_2, \cdots, p_{m-1} \to p_m$ such that $p = p_0$ and $q = p_m$.*

Proof (Theorem 4.37). We will show that for every $\varepsilon > 0$ the transition $\frac{1}{2}[0, 1] + \frac{1}{2}[1, 0] \to 1[\beta + \varepsilon, \alpha + \varepsilon]$ is transitively valid, which implies the theorem. Let us write $v = v^+ - v^-$, where v^+ and v^- are positive functions with disjoint supports and $h = h^+ - h^-$, where h^+ and h^- are again positive functions with disjoint supports. We first show the following

Lemma 4.39 $\frac{1}{2}[0, 1] + \frac{1}{2}[1, 0] + v^- \to [\beta, \alpha] + v^-$ *is transitively valid.*

Proof. By definition of v and h, $v^- \to v^+$ is a valid vertical transition and $h^- \to h^+$ is a valid horizontal transition. By adding the fixed points $\frac{1}{2}[0, 1] + \frac{1}{2}[1, 0]$ to the transition $v^- \to v^+$, we have that

$$\frac{1}{2}[0, 1] + \frac{1}{2}[1, 0] + v^- \to \frac{1}{2}[0, 1] + \frac{1}{2}[1, 0] + v^+$$

is a valid vertical transition. Let us now show that

$$\frac{1}{2}[0,1] + \frac{1}{2}[1,0] + v^+ \rightarrow [\beta,\alpha] + v^-$$

is a valid horizontal transition. First, remark that $h+v = (h^+ - h^-) + (v^+ - v^-) = -(\frac{1}{2}[0,1] + \frac{1}{2}[1,0]) + [\beta,\alpha]$ implies

$$\frac{1}{2}[0,1] + \frac{1}{2}[1,0] + v^+ = [\beta,\alpha] + h^- - h^+ + v^-.$$

Define the function with finite support $\zeta = [\beta,\alpha] - h^+ + v^-$. ζ is a positive function: the only place where ζ could be negative is on the support of h^+. But $\zeta + h^- = \frac{1}{2}[0,1] + \frac{1}{2}[1,0] + v^+$ is non negative and $\mathrm{supp}(h^+) \cap \mathrm{supp}(h^-) = \emptyset$ so ζ is non negative. This gives us $\zeta + h^- \rightarrow \zeta + h^+ = [\beta,\alpha] + v^-$ is a valid horizontal transition since $h^- \rightarrow h^+$ is a valid horizontal transition and ζ is non negative. This shows that $\frac{1}{2}[0,1] + \frac{1}{2}[1,0] + v^- \rightarrow [\beta,\alpha] + v^-$ is transitively valid. □

Our goal now is to get rid of this v^- function. We first show how to reduce the weight associated to v^- in the transition.

Lemma 4.40 *Suppose we have a transitively valid transition $p + \xi \rightarrow q + \xi$, then for any $\varepsilon > 0$, the transition $p + \varepsilon\xi \rightarrow q + \varepsilon\xi$ is transitively valid.*

Proof. First we remark that if $p' \rightarrow q'$ is a transitively valid transition and $\zeta : [0,\infty) \times [0,\infty) \rightarrow [0,\infty)$ is a positive function with finite support, then $p' + \zeta \rightarrow q' + \zeta$ is also a transitively valid transition. Pick ε' the inverse of an integer such that $\varepsilon > \varepsilon' > 0$, we write

$$\begin{aligned} p + \varepsilon'\xi &= (1-\varepsilon')p + \varepsilon'(p+\xi) \\ &\rightarrow (1-\varepsilon')p + \varepsilon'(q+\xi) = (p + \varepsilon'\xi) + \varepsilon'(q-p), \end{aligned}$$

where we used $p' = \varepsilon'(p+\xi)$, $q' = \varepsilon'(q+\xi)$ and $\zeta = (1-\varepsilon')p$. By repeating this process $1/\varepsilon'$ times, and adding on both side $(\varepsilon - \varepsilon')\xi$, we obtain that the transition $p + \varepsilon\xi \rightarrow q + \varepsilon\xi$ is transitively valid. □

From this Lemma, we have that $\forall \varepsilon > 0$, the following transition is transitively valid

$$\frac{1}{2}[0,1] + \frac{1}{2}[1,0] + \varepsilon v^- \rightarrow [\beta,\alpha] + \varepsilon v^- \tag{4.2}$$

We will now see how to create this tiny part εv^- by removing some weight from the points $[0,1]$ and $[1,0]$.

First note that by Lemma 4.34, $v^-(0,0) = 0$. Now let

$$m = \min_{(x,y)\in\mathrm{supp}(v^-)} \{\max\{x,y\}\}.$$

Then, we have $v^-(x,y) > 0 \implies x \geq m$ or $y \geq m$. From the previous remark, we have that $m > 0$. Then, by doing point raises, we have that there exists $a, b \geq 0$ such that the transition

$$a[0,m] + b[m,0] \rightarrow v^- \tag{4.3}$$

is transitively valid. This gives $\sum_{x,y} v^-(x,y) = a + b$.

Let us now assume that $m < 1$ (in fact, the case $m \geq 1$ is simpler and we will consider it afterwards). Let m_x, m_y such that $[0,1] \to \frac{am}{a+b}[0,m] + \frac{b+a(1-m)}{a+b}[0,m_y]$ and $[1,0] \to \frac{bm}{a+b}[m,0] + \frac{a+b(1-m)}{a+b}[m_x,0]$ are valid line transitions (such m_x, m_y always exist). For any $\delta > 0$, the transition

$$\begin{aligned}\frac{1}{2}[0,1] + \frac{1}{2}[1,0] \to &\frac{1-\delta}{2}[0,1] + \frac{\delta am}{2(a+b)}[0,m] + \frac{\delta(b+a(1-m))}{2(a+b)}[0,m_y] \\ &+ \frac{1-\delta}{2}[1,0] + \frac{\delta bm}{2(a+b)}[m,0] + \frac{\delta(a+b(1-m))}{2(a+b)}[m_x,0]\end{aligned}$$

is transitively valid by definition of m_x and m_y. Using Equation (4.3), we get that the following transition is transitively valid:

$$\begin{aligned}\frac{1}{2}[0,1] + \frac{1}{2}[1,0] \to &\frac{1-\delta}{2}[0,1] + \frac{1-\delta}{2}[1,0] + \frac{\delta m}{2(a+b)}v^- \\ &+ \frac{\delta(b+a(1-m))}{2(a+b)}[0,m_y] + \frac{\delta(a+b(1-m))}{2(a+b)}[m_x,0].\end{aligned}$$

Using Lemma 4.40 and Equation 4.2, we have that $(1-\delta)\left(\frac{1}{2}[0,1] + \frac{1}{2}[1,0] + \frac{\delta m}{2(1-\delta)(a+b)}v^-\right) \to (1-\delta)\left([\beta,\alpha] + \frac{\delta m}{2(1-\delta)(a+b)}v^-\right)$ is transitively valid. This gives that:

$$\frac{1}{2}[0,1] + \frac{1}{2}[1,0] \to (1-\delta)[\beta,\alpha] + \frac{\delta m}{2(a+b)}v^- + \frac{\delta(b+a(1-m))}{2(a+b)}[0,m_y] + \frac{\delta(a+b(1-m))}{2(a+b)}[m_x,0]$$

is transitively valid. Let $\xi = \frac{m}{2(a+b)}v^- + \frac{b+a(1-m)}{2(a+b)}[0,m_y] + \frac{a+b(1-m)}{2(a+b)}[m_x,0]$. The above transition can be rewritten as $\frac{1}{2}[1,0] + \frac{1}{2}[0,1] \to (1-\delta)[\beta,\alpha] + \delta\xi$. This holds for any $\delta > 0$.

For $m \geq 1$, we start by considering the raises $[0,1] \to [0,m]$ and $[1,0] \to [m,0]$ and then continue as above.

Our last goal is to get rid of this $\delta\xi$. To do this, we use the following Lemma.

Lemma 4.41 *Given $\varepsilon > 0$ and a function $\xi : [0,\infty) \times [0,\infty) \to [0,\infty)$ with finite support and $\sum_{(x,y)\in\mathrm{supp}(\xi)} \xi(x,y) = 1$, there exists $0 < \delta < 1$ such that $(1-\delta)[\beta,\alpha] + \delta\xi \to [\beta+\varepsilon, \alpha+\varepsilon]$ is transitively valid.*

Proof. By point raising, there exist values n_x and n_y such that $\xi \to [n_x, n_y]$ is transitively valid. Moreover, by further point raising, we can have $n_x > \beta + \varepsilon$ and $n_y > \alpha + \varepsilon$. We pick δ and δ' such that the following two line transitions are valid:

$$\begin{aligned}\delta'[n_x,\alpha] + \delta[n_x,n_y] &\to (\delta+\delta')[n_x,\alpha+\varepsilon], \\ (1-\delta-\delta')[\beta,\alpha+\varepsilon] + (\delta'+\delta)[n_x,\alpha+\varepsilon] &\to [\beta+\varepsilon,\alpha+\varepsilon].\end{aligned}$$

This is possible by taking $\delta, \delta' > 0$ that satisfy $\delta'\alpha + \delta n_y = (\delta+\delta')(\alpha+\varepsilon)$ and $(1-\delta-\delta')\beta + (\delta'+\delta)n_x = \beta + \varepsilon$. We conclude that

$$\begin{aligned}(1-\delta)[\beta,\alpha] + \delta\xi &\to (1-\delta)[\beta,\alpha] + \delta[n_x,n_y] && \text{is transitively valid} \\ &\to (1-\delta-\delta')[\beta,\alpha] + \delta'[n_x,\alpha] + \delta[n_x,n_y] && \text{is a valid point raise} \\ &\to (1-\delta-\delta')[\beta,\alpha] + (\delta'+\delta)[m_x,\alpha+\varepsilon] && \text{is a valid merge} \\ &\to (1-\delta-\delta')[\beta,\alpha+\varepsilon] + (\delta'+\delta)[m_x,\alpha+\varepsilon] && \text{is a valid point raise} \\ &\to [\beta+\varepsilon,\alpha+\varepsilon] && \text{is a valid merge.}\end{aligned}$$

□

This concludes the proof of the theorem. □

4.2.4 Unbalanced weak coin flipping

Unbalanced weak coin flipping is a generalization of the balanced version in which when both players are honest Alice wins with probability P_A and Bob with probability $P_B = 1 - P_A$ as defined in Definition 4.2, but we do not impose any longer that $P_A = P_B = 1/2$. All the point game formalism can be easily extended to handle unbalanced coin flipping. The initial points are then $P_A[1, 0] + P_B[0, 1]$ and we aim to have a final point $1[\beta, \alpha] = 1[P_B + \varepsilon, P_A + \varepsilon]$. As shown in [CK09], the existence of ε-biased unbalanced coin flipping implies the existence of an $1/\sqrt{2} - 1/2 + 2\varepsilon$-biased unbalanced coin flipping for all ε by composition of balanced protocols.

4.3 Summary

The objective of this Chapter is to prove the existence of weak coin flipping protocol with arbitrarily small bias. We have shown that this task can be reduced to finding a time independent point game with final point $[1/2 + \varepsilon, 1/2 + \varepsilon]$. Such game has already been constructed by Carlos Mochon (see Appendix C). Our major contribution is a strong clarification on the relationship between transitions expressible by matrices and valid transitions. The proof presented in this dissertation that strictly valid transitions are EBM is also totally new and uses topological arguments.

Part II

Query complexity

5 Adversaries and polynomials

This Chapter is devoted to the different methods used to prove lower bounds in the quantum query complexity model. The main result is that the multiplicative adversary method is stronger than any other known method, in particular the general additive method and the polynomial method. The key to prove this result is generalizing all the methods to be able to prove lower bounds on the query complexity of quantum state generation, and not simply classical functions. The methods then take a particularly nice geometric simplifications and simpler mathematical formulations that are thus used to compare their respective powers. We first introduce the notion of quantum query complexity for state generation before generalizing the methods.

5.1 Quantum query complexity

The query complexity model is a model of computation where the input of the a problem $\mathcal{P}$, a string x of length N over an alphabet Σ_O, can be accessed only through an oracle O_x.We will consider two types of oracles. A *register oracle* acts on two registers, the input register $\mathcal{I}$ and the output register $\mathcal{O}$, as:

$$|i\rangle_{\mathcal{I}}|s\rangle_{\mathcal{O}} \xrightarrow{O_x} |i\rangle_{\mathcal{I}}|s \oplus x_i\rangle_{\mathcal{O}},$$

where $i \in [N]$, $s, x_i \in \Sigma_O$ and $\oplus$ denotes the bitwise XOR.

When $\Sigma_O = \{0,1\}$, it is also possible to consider a *phase oracle*

$$\forall i, b \in \{0,1\},\ |i\rangle|b\rangle \mapsto (-1)^{bx_i}|i\rangle|b\rangle.$$

We denote by F the set of all possible inputs x that can be encoded into the oracle. We will consider three types of problems $\mathcal{P}$, a classical one and two quantum ones:

Function evaluation Given an oracle O_x, compute the classical output $\mathcal{P}(x)$. The success probability of an algorithm A solving $\mathcal{P}$ is $\min_{x\in F}\Pr[A(x) = \mathcal{P}(x)]$, where $A(x)$ is the classical output of the algorithm on oracle x.

Coherent quantum state generation Given an oracle O_x, generate a quantum state $|\mathcal{P}(x)\rangle = |\psi_x\rangle$ in some target register $\mathcal{T}$, and reset all other registers to a default state $|\bar{0}\rangle$. Let $|\psi_x^T\rangle$ be the final state of an algorithm A on oracle x, where $\Re(\langle\psi_x^T|(|\psi_x\rangle|\bar{0}\rangle)) \geq \sqrt{1-\varepsilon_x}$, where $\Re(z)$ denotes the real part of the complex number z. Then, the success probability of A is given by $\min_{x\in F}(1-\varepsilon_x)$.

Non-coherent quantum state generation Given an oracle O_x, generate a quantum state $|\mathcal{P}(x)\rangle = |\psi_x\rangle$ in some target register $\mathcal{T}$, while some x-dependent junk state may be generated in other registers. The success probability of an algorithm A solving $\mathcal{P}$ is given by $\min_{x\in F}\left\|\Pi_{|\psi_x\rangle}|\psi_x^T\rangle\right\|^2$, where $|\psi_x^T\rangle$ is the final state of the algorithm and $\Pi_{|\psi_x\rangle}$ is the projector on $|\psi_x\rangle$.

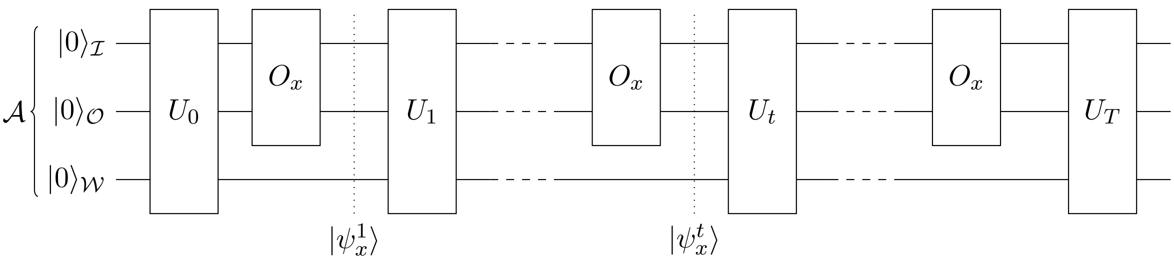


Figure 5.1: Schematic representation of a quantum algorithm that make use of an oracle O_x, an input register $\mathcal{I}$, an output register $\mathcal{O}$, and a register $\mathcal{W}$ for work space.

Definition 5.1 (Query complexity) *Fix one oracle and $\varepsilon \geq 0$. The query complexity $Q_\varepsilon(\mathcal{P})$ is the minimum number of queries to the oracle necessary to solve $\mathcal{P}$ with error probability ε over all possible algorithms.*

The two different model of oracle, phase oracle and register oracle, lead to equivalent notions of asymptotic query complexity (up to a constant), so we usually do not specify which one is used.

5.2 Adversary methods: general concepts

Before examining the differences between all the variations of the adversary method in the next Section, let us review the elements that are common in all of them.

Let us note that computing a function is a special case of non-coherent quantum state generation, where all states $|\mathcal{P}(x)\rangle$ are computational basis states. Indeed, no coherence is needed since the state is in this case measured right after its generation. However, when the quantum state generation is used as a subroutine in a quantum algorithm for another problem, coherence is typically needed to allow interferences between different states. This is in particular the case for solving Set Equality via reduction to Index Erasure, and similarly to solve Graph Isomorphism via the quantum state generation approach, since coherence is required to implement the SWAP-test.

Without loss of generality we can consider the algorithm as being a circuit $\mathcal{C}$ consisting of a sequence of unitaries $U_0, \ldots, U_T$ and oracle calls O_x acting on the "algorithm" Hilbert space $\mathcal{A}$. Decomposing $\mathcal{A}$ into three registers, the input register $\mathcal{I}$ and output register $\mathcal{O}$ for the oracle, as well as an additional workspace register $\mathcal{W}$, the circuit may be represented as in Fig. 5.1.

At the end of the circuit, a target register $\mathcal{T}$ holds the output of the algorithm. In the classical case, this register is measured to obtain the classical output, the string $A(x)$. In the quantum case, it holds the output state $A(x)$ (not necessarily pure).

In both cases, for a fixed algorithm, we note $|\psi_x^t\rangle$ the state of the algorithm after the t-th query. The idea behind the adversary methods is to consider that x is in fact an input to the oracle. We therefore introduce a function register $\mathcal{F}$ holding this input, and define a *super-oracle* O acting on registers $\mathcal{I} \otimes \mathcal{O} \otimes \mathcal{F}$ as

$$|i\rangle_{\mathcal{I}}|s\rangle_{\mathcal{O}}|x\rangle_{\mathcal{F}} \xrightarrow{O} |i\rangle_{\mathcal{I}}|s \oplus x_i\rangle_{\mathcal{O}}|x\rangle_{\mathcal{F}}.$$

We see that when the function register $\mathcal{F}$ is in state $|x\rangle$, O acts on $\mathcal{I} \otimes \mathcal{O}$ just as O_x. Suppose, just for the sake of analyzing the algorithm, that we prepare register $\mathcal{F}$ in the state $|\alpha\rangle =$

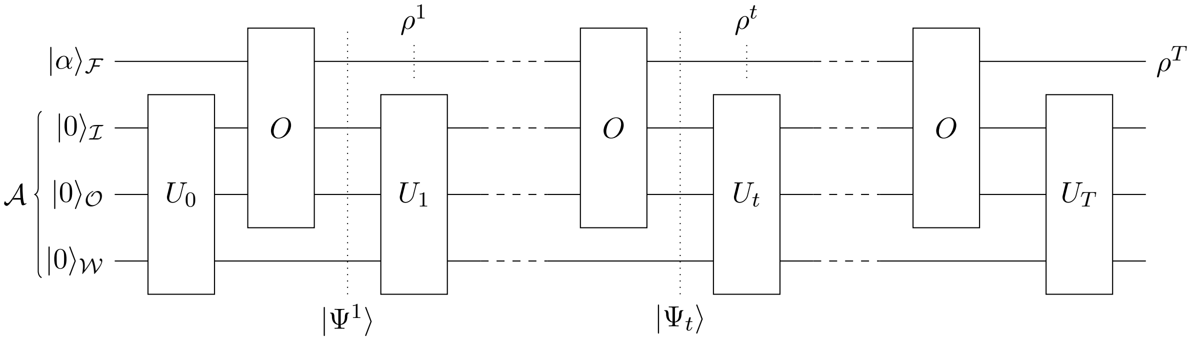

ρ^1
ρ^t
ρ^T
$|\alpha\rangle_{\mathcal{F}}$
$|0\rangle_{\mathcal{I}}$
$\mathcal{A}$
$|0\rangle_{\mathcal{O}}$
$|0\rangle_{\mathcal{W}}$
U_0
O
U_1
O
U_t
O
U_T
$|\Psi^1\rangle$
$|\Psi_t\rangle$

Figure 5.2: Schematic representation of a quantum algorithm that makes use of an oracle O_f, an input register $\mathcal{I}$, an output register $\mathcal{O}$, a register $\mathcal{W}$ for work space, and a virtual register $\mathcal{F}$ holding the input of the problem.

$\sum_{x\in F}\sqrt{\alpha_x}|x\rangle$ (with $\alpha_x \geq 0$), a superposition over the elements of F, and that we apply the same circuit as before, by replacing each call to O_x by a call to O. Intuitively, each oracle call introduces more entanglement between this new register and the algorithm register. The state of this new circuit after the t-th query is (see Figure 5.2)

$$|\Psi^t\rangle = \sum_{x\in F}\sqrt{\alpha_x}|\psi_x^t\rangle_{\mathcal{A}}|x\rangle_{\mathcal{F}}.$$

Note that only oracle calls can modify the state of the function register $\mathcal{F}$, since all other gates only affect the algorithm register $\mathcal{A} = \mathcal{I}\otimes\mathcal{O}\otimes\mathcal{W}$. After the t-th query, the state in the function register can be written as:

$$\rho^t = \mathrm{tr}_{\mathcal{A}}|\Psi^t\rangle\langle\Psi^t| = \sum_{x,x'\in F}\sqrt{\alpha_x\alpha_{x'}}\langle\psi_{x'}^t|\psi_f^t\rangle|x\rangle\langle x'|.$$

The general idea of all adversary methods is to study the evolution of the algorithm by looking at ρ^t. The algorithm starts with the state $\rho^0 = |\alpha\rangle\langle\alpha|$ and ends in a state ρ^T.

5.2.1 Adversary matrices and progress function

The adversary method studies how fast ρ^t can change from ρ^0 to ρ^T. We introduce a progress function in order to do so.

Definition 5.2 (Adversary, progress function) *An* adversary *is a couple* $(\Gamma, |\alpha\rangle)$ *where* Γ*, the* adversary matrix*, is a Hermitian matrix such that* $\mathrm{tr}[\Gamma|\alpha\rangle\langle\alpha|] = 1$*, and* $|\alpha\rangle$*, the* adversary state*, is a pure state. An* additive adversary matrix *also satisfies* $-\mathbb{I} \preceq \Gamma \preceq \mathbb{I}$ *(i.e.,* $\|\Gamma\| = 1$*), while a* multiplicative adversary matrix *satisfies* $\Gamma \succeq \mathbb{I}$*. In both cases, the* progress function *is defined as* $W^t = \mathrm{tr}\left[\Gamma\rho^t\right]$.

In order to analyze the variation of the progress function, let us define the action of an oracle in terms of matrices.

Definition 5.3 (D_i) *For a register oracle we define* D_i *as the (0-1)-matrix*

$$D_i = \sum_{x,x':x_i=x_i'}|x\rangle\langle x'|,$$

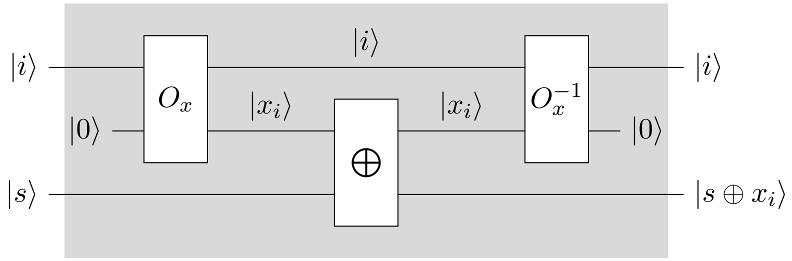


Figure 5.3: Schematic representation on the simulation of one register oracle (in gray) by one computing oracle call, a $|\Sigma_O|$ XOR gates and one uncomputing oracle call (in white).

and for a phase oracle as the $\{-1,1\}$*-valued matrix*

$$D_i = \sum_{x,x'} (-1)^{x_i + x'_i} |x\rangle\langle x'|.$$

Recall that the Hadamard product (entrywise product) between two matrices is denoted by $\circ$. We will show that the Hadamard product is closely related to oracle calls.

Definition 5.4 (Γ_i) *For any adversary matrix* Γ*, we denote by* Γ_i *the matrix* $\Gamma \circ D_i$*.*

For the rest of this Section, we only consider register oracles. Consider now that the input register is in a state $|i\rangle$, the oracle acts on the function register as the Hadamard product, denoted by $\circ$, with D_i. It is easy to check that this Hadamard product is a CPTP-map.

Fact 5.5 *The map* $\gamma \mapsto \gamma \circ D_i$ *is a CPTP-map and* $\gamma \circ D_i = \sum_y \Pi_y^i \gamma \Pi_y^i$ *with* $\Pi_y^i = \sum_{x:x_i=y} |x\rangle\langle x|$*.*

5.2.2 Effect of oracle calls

The basic idea of all adversary methods is to bound how much the value of the progress function can change by one oracle call. To study the action of one oracle call, we isolate the registers $\mathcal{I}$ and $\mathcal{O}$ holding the input and output of the oracle from the rest of the algorithm register. Without loss of generality, we may assume that for any oracle call, the output register $\mathcal{O}$ is in the state $|0\rangle_{\mathcal{O}}$ (*computing* oracle call) or $|x_i\rangle_{\mathcal{O}}$ (*uncomputing* oracle call). Indeed, an oracle call for any other state $|s\rangle_{\mathcal{O}}$ may be simulated by one computing oracle call, $\mathrm{O}(\log |\Sigma_O|)$ XOR gates and one uncomputing oracle call (See Figure 5.3). Therefore, this assumption only increases the query complexity by a factor at most 2.

Let us consider the action of the $(t+1)$-th register oracle call, which we assume to be of *computing* type (uncomputing oracle calls are treated similarly). Just before the $(t+1)$-th oracle call, the state can be written as:

$$|\Psi^t\rangle = \sum_{x,i} \sqrt{\alpha_x} |\psi_{x,i}^t\rangle_{\mathcal{W}} |i\rangle_{\mathcal{I}} |0\rangle_{\mathcal{O}} |x\rangle_{\mathcal{F}},$$

with $|\psi_{x,i}^t\rangle$ being non-normalized states. Let us consider the reduced density matrix $\tilde{\rho}^t = \mathrm{tr}_{\mathcal{W}} |\Psi^t\rangle\langle\Psi^t|$:

$$\tilde{\rho}^t = \sum_{x,x'} \sqrt{\alpha_x \alpha_{x'}} \left(\sum_{i,i'} \langle \psi_{x,i}^t | \psi_{x',i'}^t \rangle |i'\rangle\langle i| \right) \otimes |0\rangle\langle 0| \otimes |x'\rangle\langle x|. \tag{5.1}$$

and note that $\rho^t = \mathrm{tr}_{\mathcal{IO}}\left[\tilde{\rho}^t\right]$.

Lemma 5.6 *Let the t-th oracle call be of computing-type. Then, $W^t = \mathrm{tr}\left[\Upsilon\tilde{\rho}^t\right]$ and $W^{t+1} = \mathrm{tr}\left[\Upsilon'\tilde{\rho}^t\right]$, where*

$$\Upsilon = \sum_i |i\rangle\langle i| \otimes \sum_y |y\rangle\langle y| \otimes \Gamma = \bigoplus_{i,y} \Gamma, \tag{5.2}$$

$$\Upsilon' = \sum_i |i\rangle\langle i| \otimes \sum_y |y\rangle\langle y| \otimes \Gamma_i = \bigoplus_{i,y} \Gamma_i. \tag{5.3}$$

Note that for uncomputing oracle calls, it suffices to swap the roles of ρ^t and ρ^{t+1}.

Proof. Recall that the progress function is defined by $W^t = \mathrm{tr}[\Gamma\rho^t]$. From the definition of Υ and from the fact that $\rho^t = \mathrm{tr}_{\mathcal{IO}}\left[\tilde{\rho}^t\right]$, we get $W^t = \mathrm{tr}\left[\Upsilon\tilde{\rho}^t\right]$. Let us now consider what happens after one oracle call. An oracle call acts on the registers $\mathcal{I}\otimes\mathcal{O}\otimes\mathcal{F}$ as the operator

$$O = \sum_i |i\rangle\langle i| \sum_{x,s} |x_i \oplus s\rangle\langle s| \otimes |x\rangle\langle x|.$$

Before a computing oracle call, the output register $\mathcal{O}$ is in the state $|0\rangle$, as in Equation (5.1). Therefore, the state $\tilde{\rho}^{t+1} = O\tilde{\rho}^t O^\dagger$ just after the $(t+1)$-th oracle call is

$$\tilde{\rho}^{t+1} = \sum_{x,x',i,i'} \sqrt{\alpha_x\alpha_{x'}}\langle\psi^t_{x,i}|\psi^t_{x',i'}\rangle|i'\rangle\langle i| \otimes |x'_{i'}\rangle\langle x_i| \otimes |x'\rangle\langle x|$$

and

$$\rho^{t+1} = \mathrm{tr}_{\mathcal{IO}}\left[\tilde{\rho}^{t+1}\right] = \sum_i \rho^t_i \circ D_i, \tag{5.4}$$

where

$$\rho^t_i = \sum_{x,x'} \sqrt{\alpha_x\alpha_{x'}}\langle\psi^t_{x,i}|\psi^t_{x',i}\rangle|x'\rangle\langle x|. \tag{5.5}$$

Combining Equation (5.1) with Equation (5.3) we have:

$$\begin{aligned}
\mathrm{tr}\left[\Upsilon'\tilde{\rho}^t\right] &= \sum_{x,x',i,i'} \sqrt{\alpha_x\alpha_{x'}}\mathrm{tr}\left[\langle\psi^t_{x,i}|\psi^t_{x',i'}\rangle|i'\rangle\langle i| \otimes |0\rangle\langle 0| \otimes \Gamma_i|x'\rangle\langle x|\right] \\
&= \sum_i \mathrm{tr}\left[\Gamma_i \sum_{x,x'} \sqrt{\alpha_x\alpha_{x'}}\langle\psi^t_{x,i}|\psi^t_{x',i}\rangle|x'\rangle\langle x|\right] \\
&= \sum_i \mathrm{tr}\left[\Gamma_i\rho^t_i\right] \quad \text{by Equation (5.5)} \\
&= \sum_i \mathrm{tr}\left[(\Gamma\circ D_i)\rho^t_i\right] \\
&= \sum_i \mathrm{tr}\left[\Gamma(\rho^t_i\circ D_i)\right] \quad \text{using Fact 5.5 and } \mathrm{tr}(AB) = \mathrm{tr}(BA) \\
&= \mathrm{tr}\left[\Gamma\rho^{t+1}\right] \quad \text{by Equation (5.4).}
\end{aligned}$$

□

Notice that the action of querying i on ρ^t is the CPTP map $\rho \mapsto \rho^{t+1} = \rho\circ D_i$.

5.3 The different adversary methods

We first review the two main methods, namely the *general additive* and the *multiplicative* methods. These methods differ in two key points: firstly, the additive method bounds the absolute variation of the progress functions, whereas the multiplicative method bounds the relative progress done by one query; secondly the additive method imposes more conditions on the adversary matrix than the multiplicative method.

Then, we introduce the *intermediate* method, that is bound the absolute progress done by one query (additively) but uses the same conditions on the adversary matrices than the multiplicative method. We will later use this intermediate method as a "bridge" between the two other to compare their respective powers.

Moreover, we directly consider the case of quantum state generation since this formalism is the technical key in the proof of our main theorem. On of the main difference between generating a quantum state and a classical value is that the quantum state may be entangled with the environment. The query complexity should not depend of the state of the environment that we capture in a *junk matrix*. This is the role of the next couple of definitions.

To differentiate between the different methods, we will from now on denote additive adversary matrices by $\widetilde{\Gamma}$ and multiplicative adversary matrices by Γ. For the statement of the theorem, we will also need the following notions.

Definition 5.7 (Gram matrix) *A Gram matrix M of size $|F| \times |F|$ is a positive semidefinite matrix whose all diagonal entries are 1 ($M \circ \mathbb{I} = \mathbb{I}$). Equivalently, there exists a set $\{v_k : k \in [|F|]\}$ of unit-length vectors such that $M_{k,l} = \langle v_k | v_l \rangle$.*

Definition 5.8 ($\rho^{\odot}$, junk matrix) *For a quantum state generation problem $\mathcal{P}$ such that $|\mathcal{P}(x)\rangle = |\psi_x\rangle$, and a adversary state $|\alpha\rangle$, we denote by $\rho^{\odot}$ the* target *matrix*

$$\rho^{\odot} = \sum_{x,x' \in F} \sqrt{\alpha_x \alpha_{x'}} \langle \psi_x | \psi_{x'} \rangle |x'\rangle\!\langle x|.$$

In the non-coherent case, we call junk matrix *any Gram matrix M. In the coherent case we call junk matrix, the matrix J (the all-one matrix).*

5.3.1 General additive adversary method

Theorem 5.9 (Additive adversary method) *Let $\mathcal{P}$ be a problem, and $(\Gamma, |\alpha\rangle)$ be an additive adversary such that* $\mathrm{tr}\left[\widetilde{\Gamma}(\rho^{\odot} \circ M)\right] = 0$ *for any junk matrix M. Then,*

$$Q_\varepsilon(\mathcal{P}) \geq \frac{1 - C(\varepsilon)}{\max_i \left\|\widetilde{\Gamma}_i - \widetilde{\Gamma}\right\|} \quad \textit{where} \quad C(\varepsilon) = \varepsilon + 2\sqrt{\varepsilon(1-\varepsilon)}.$$

Proof. Consider an algorithm that solves $\mathcal{P}$ with probability at least $1 - \varepsilon$ in T queries. By definition of $\widetilde{\Gamma}$, the initial value of the progress function is $\widetilde{W}^0 = 1$. We now bound the decrease of the progress function for each query. We have from Lemma 5.6

$$\left|\widetilde{W}^{t+1} - \widetilde{W}^t\right| = \left|\mathrm{tr}[(\tilde{\Upsilon}' - \tilde{\Upsilon})\tilde{\rho}^t]\right| \leq \left\|\tilde{\Upsilon}' - \tilde{\Upsilon}\right\| = \max_i \left\|\widetilde{\Gamma}_i - \widetilde{\Gamma}\right\|.$$

To conclude, we need to upper-bound the value of the progress function at the end of the algorithm. Let us prove that $\widetilde{W}^T \leq C(\varepsilon)$. Let $|\psi_x\rangle$ be the state to be generated when the input is x (in particular, for a classical problem this will just be a computational basis state encoding the output of the function). The final state is:

$$|\Psi^T\rangle = \sum_{x\in F} \sqrt{\alpha_x}\left[\sqrt{1-\varepsilon_x}|\psi_x, \mathrm{junk}_x\rangle + \sqrt{\varepsilon_x}|\mathrm{err}_x\rangle\right]|x\rangle,$$

where $|\mathrm{junk}_x\rangle$ is the default state $|\bar{0}\rangle$ for a coherent quantum state generation problem, and any state otherwise. Since the algorithm has success probability $1-\varepsilon$, we have $0 \leq \varepsilon_x \leq \varepsilon, \forall x$ and the final state can be rewritten as:

$$|\Psi^T\rangle = \sum_{x\in F} \sqrt{\alpha_x}\left[\sqrt{1-\varepsilon}|\psi_x, \mathrm{junk}_x\rangle + \sqrt{\varepsilon}|\mathrm{error}_x\rangle\right]|x\rangle,$$

where $|\mathrm{error}_x\rangle$ is the (non-normalized) vector $\frac{\sqrt{1-\varepsilon_x}-\sqrt{1-\varepsilon}}{\sqrt{\varepsilon}}|\psi_x, \mathrm{junk}_x\rangle + \sqrt{\frac{\varepsilon_x}{\varepsilon}}|\mathrm{err}_x\rangle$.

Tracing over everything but the last register, we have

$$\rho^T = (1-\varepsilon)\left(\rho^{\odot}\circ M_{\mathrm{junk}}\right) + \varepsilon\tau + \sqrt{\varepsilon(1-\varepsilon)}(\sigma+\sigma^\dagger),$$

where

$$\begin{aligned} M_{\mathrm{junk}} &= \sum_{x,x'\in F} \langle \mathrm{junk}_x|\mathrm{junk}_{x'}\rangle |x'\rangle\langle x|,\\ \tau &= \sum_{x,x'\in F} \sqrt{\alpha_x\alpha_{x'}}\langle \mathrm{error}_x|\mathrm{error}_{x'}\rangle |x'\rangle\langle x|,\\ \sigma &= \sum_{x,x'\in F} \sqrt{\alpha_x\alpha_{x'}}\langle \psi_x, \mathrm{junk}_x|\mathrm{error}_{x'}\rangle |x'\rangle\langle x|. \end{aligned}$$

By assumption on $\widetilde{\Gamma}$, we have $\mathrm{tr}\left[\widetilde{\Gamma}(\rho^{\odot}\circ M_{\mathrm{junk}})\right] = 0$. Moreover, according to Lemma 2.39 we have $\mathrm{tr}\left[\widetilde{\Gamma}A\right] \leq \|\Gamma\|\,\|A\|_{\mathrm{tr}} = \|A\|_{\mathrm{tr}}$ for any operator A, so that

$$\begin{aligned} W^T &= (1-\varepsilon)\mathrm{tr}\left[\widetilde{\Gamma}(\rho^{\odot}\circ M_{\mathrm{junk}})\right] + \varepsilon\mathrm{tr}\left[\widetilde{\Gamma}\tau\right] + \sqrt{\varepsilon(1-\varepsilon)}\mathrm{tr}\left[\widetilde{\Gamma}(\sigma+\sigma^\dagger)\right]\\ &\leq \varepsilon\,\|\tau\|_{\mathrm{tr}} + \sqrt{\varepsilon(1-\varepsilon)}\left\|\sigma+\sigma^\dagger\right\|_{\mathrm{tr}}. \end{aligned}$$

It remains to show that $\|\tau\|_{\mathrm{tr}} \leq 1$ and $\left\|\sigma+\sigma^\dagger\right\|_{\mathrm{tr}} \leq 2$. Let us define the following matrices:

$$A = \sum_{x\in F}\sqrt{\alpha_x}|\psi_x, \mathrm{junk}_x\rangle\langle x|, \qquad B = \sum_{x\in F}\sqrt{\alpha_x}|\mathrm{error}_x\rangle\langle x|.$$

Then, we have $\sigma = (A^\dagger B)^t$ and therefore $\left\|\sigma+\sigma^\dagger\right\|_{\mathrm{tr}} \leq 2\,\|\sigma\|_{\mathrm{tr}} = 2\left\|A^\dagger B\right\|_{\mathrm{tr}} \leq 2\,\|A\|_{\mathrm{F}}\cdot\|B\|_{\mathrm{F}} \leq 2$, where we have used Hölder's inequality (Lemma 2.38) and the fact that $\|A\|_{\mathrm{F}} = 1$ since $|\psi_x, \mathrm{junk}_x\rangle$ is normalized, $\|B\|_{\mathrm{F}} \leq 1$, and $\langle \mathrm{error}_x|\mathrm{error}_x\rangle = \frac{1}{\varepsilon}\left(2-\varepsilon-2\sqrt{1-\varepsilon}\sqrt{1-\varepsilon_x}\right) \leq 1$ for $\varepsilon_x \leq \varepsilon$. Similarly, we have $\tau = (B^\dagger B)^t$ and therefore $\|\tau\|_{\mathrm{tr}} \leq \|B\|_{\mathrm{F}}^2 \leq 1$. □

For classical problems, we now prove that our method generalizes [HLŠ07]. Indeed, our condition on the adversary matrix is different, which allows us to also deal with quantum problems. However, for function evaluation the following lemma shows that the usual condition implies our modified condition. Let $\mathcal{P}(x)$ be the function to be computed.

Lemma 5.10 $\operatorname{tr}\left[\widetilde{\Gamma}(\rho^{\odot} \circ M)\right] = 0$ *for any matrix* M *if and only if* $\widetilde{\Gamma}_{xx'} = 0$ *for any* x, x' *such that* $\mathcal{P}(x) = \mathcal{P}(x')$.

Proof. Let $\widetilde{\Gamma}$ be such that $\operatorname{tr}\left[\widetilde{\Gamma}(\rho^{\odot} \circ M)\right] = 0$ for any matrix M, and x_0, x_0' be such that $\mathcal{P}(x_0) = \mathcal{P}(x_0')$. Choosing M such that $M_{x_0x_0'} = 1$ and $M_{yy'} = 0$ for any other element, we have $\rho^{\odot} \circ M = \sqrt{\alpha_{x_0}\alpha_{x_0'}}M$ and therefore $\widetilde{\Gamma}_{x_0x_0'} = 0$.

For the other direction, we obtain for any matrix M

$$\operatorname{tr}\left[\widetilde{\Gamma}(\rho^{\odot} \circ M)\right] = \sum_{x,x' \in F} \sqrt{\alpha_x\alpha_{x'}}\widetilde{\Gamma}_{xx'}\langle\mathcal{P}(x)|\mathcal{P}(x')\rangle M_{xx'} = 0$$

since $\widetilde{\Gamma}_{xx'} = 0$ whenever $\mathcal{P}(x) = \mathcal{P}(x')$, and $\langle\mathcal{P}(x)|\mathcal{P}(x')\rangle = 0$ whenever $\mathcal{P}(x) \neq \mathcal{P}(x')$. □

5.3.2 Multiplicative adversary method

The original adversary method can only prove a lower bound when $C(\varepsilon) < 1$, that is, when the success probability $1-\varepsilon > \frac{4}{5}$. For smaller success probability, we need to prove a stronger bound on the final value of the progress function W^T. Recall that this one of the main differences compared to the additive method. Since it is slightly more complicated than for the additive method, we first need to introduce the notion of *overlap on the bad subspace*:

Definition 5.11 (Good and bad multiplicative subspaces) *Let* Γ *be a multipliative adversary matrix and fix a threshold* $\lambda > 1$. *The eigenspaces of* Γ *are split into two spaces: the* good subspace V_{good} *is the direct sum of the eigenspaces of* Γ *with eigenvalues larger than* λ, *and the* bad subspace V_{bad} *is the direct sum of the eigenspaces of* Γ *with eigenvalues strictly smaller than* $\tilde{\lambda}$. *The projector on the bad subspace is denoted by* Π_{bad}.

Since the state of the algorithm ρ^T starts by being $\rho^0 = |\alpha\rangle\langle\alpha|$, it only has support on the bad subspace. Intuitively, $\rho^{\odot}$ should have a small support on it. This is quantified by

Definition 5.12 (Overlap on the bad subspace) *Let* $\mathcal{P}$ *be a problem,* $(\Gamma, |\alpha\rangle)$ *be an adversary (additive or multiplicative), and* λ *a threshold. The overlap of* $\rho^{\odot}$ *on the bad subspace set defined by* $\eta = \min_M \operatorname{tr}\left[\Pi_{\text{bad}}(\rho^{\odot} \circ M)\right]$ *over all junk matrix* M.

We can now state the multiplicative adversary method in a similar manner than the general additive adversary method:

Theorem 5.13 (Multiplicative adversary method) *Let* $\mathcal{P}$ *be a problem,* $(\Gamma, |\alpha\rangle)$ *be a multiplicative adversary, and* $\lambda > 1$ *a threshold. Denote by* η *the overlap of* $\rho^{\odot}$ *on the bad subspace. If* $\eta \leq 1 - \varepsilon$, *then we have:*

$$Q_\varepsilon(\mathcal{P}) \geq \frac{\log K(\eta, \lambda, \varepsilon)}{\log \max\left\{\left\|\Gamma_i^{\frac{1}{2}}\Gamma^{-\frac{1}{2}}\right\|^2, \left\|\Gamma^{\frac{1}{2}}\Gamma_i^{-\frac{1}{2}}\right\|^2 : \forall i \in \Sigma_I\right\}},$$

where $K(\eta, \lambda, \varepsilon) = 1 + (\lambda - 1)(\sqrt{1-\varepsilon} - \sqrt{\eta})^2$.

Proof. Consider an algorithm that solves $\mathcal{P}$ with probability at least $1 - \varepsilon$ in T queries. As done in the previous proof, the initial value of the progress function is $W^0 = 1$.

In this case we do not bound the difference of the progress function between two queries, but its quotient. From Fact 5.5, we note that Υ and Υ' are positive semidefinite. Then, using Lemma 5.6, we have

$$\begin{aligned}
\frac{W^{t+1}}{W^t} &= \frac{\operatorname{tr}\left[\Upsilon'\tilde{\rho}^t\right]}{\operatorname{tr}\left[\Upsilon\tilde{\rho}^t\right]} = \frac{\operatorname{tr}\left[\Upsilon'^{\frac{1}{2}}\Upsilon^{-\frac{1}{2}}\Upsilon^{\frac{1}{2}}\tilde{\rho}^t\Upsilon^{\frac{1}{2}}\Upsilon^{-\frac{1}{2}}\Upsilon'^{\frac{1}{2}}\right]}{\operatorname{tr}\left[\Upsilon^{\frac{1}{2}}\tilde{\rho}^t\Upsilon^{\frac{1}{2}}\right]} = \frac{\operatorname{tr}\left[\Upsilon^{-\frac{1}{2}}\Upsilon'\Upsilon^{-\frac{1}{2}}\Upsilon^{\frac{1}{2}}\tilde{\rho}^t\Upsilon^{\frac{1}{2}}\right]}{\operatorname{tr}\left[\Upsilon^{\frac{1}{2}}\tilde{\rho}^t\Upsilon^{\frac{1}{2}}\right]} \\
&\le \left\|\Upsilon^{-\frac{1}{2}}\Upsilon'\Upsilon^{-\frac{1}{2}}\right\| \quad \text{by to Lemma 2.39 and since } \operatorname{tr}[\Upsilon^{\frac{1}{2}}\tilde{\rho}^t\Upsilon^{\frac{1}{2}}] = \left\|\Upsilon^{\frac{1}{2}}\tilde{\rho}^t\Upsilon^{\frac{1}{2}}\right\|_{\operatorname{tr}} \\
&= \left\|\Upsilon'^{\frac{1}{2}}\Upsilon^{-\frac{1}{2}}\right\|^2 \quad \text{by Lemma 2.40} \\
&= \left\|\bigoplus_{i,y}\Gamma_i^{\frac{1}{2}}\Gamma^{-\frac{1}{2}}\right\|^2 = \max_i\left\|\Gamma_i^{\frac{1}{2}}\Gamma^{-\frac{1}{2}}\right\|^2.
\end{aligned}$$

If the $(t+1)$-th oracle call is of *uncomputing* type, we similarly obtain $\frac{W^{t+1}}{W^t} \le \max_x\left\|\Gamma^{\frac{1}{2}}\Gamma_i^{-\frac{1}{2}}\right\|^2$.

The second part of the proof is upper-bounding the final value of the progress function. Recall that by assumption, $|\Psi^T\rangle$ can be written

$$|\Psi^T\rangle = \sum_{x\in F}\sqrt{\alpha_x}\left[\sqrt{1-\varepsilon}|\psi_x,\mathrm{junk}_x\rangle + \sqrt{\varepsilon}|\mathrm{error}_x\rangle\right]|x\rangle.$$

The state $|\Psi\rangle = \sum_{x\in F}\sqrt{\alpha_x}|\psi_x,\mathrm{junk}_x\rangle|f\rangle$ satisfies $|\langle\Psi|\Psi^T\rangle| \ge \sqrt{1-\varepsilon}$, and $\operatorname{tr}_{\mathcal{A}}|\Psi\rangle\langle\Psi| = \rho^{\odot}\circ M_{\mathrm{junk}}$. Let $\beta = \left\|\Pi_{\mathrm{good}}|\Psi^T\rangle\right\|^2$, $|\Psi_{\mathrm{good}}\rangle = \Pi_{\mathrm{good}}|\Psi^T\rangle/\sqrt{\beta}$ and $|\Psi_{\mathrm{bad}}\rangle = \Pi_{\mathrm{bad}}|\Psi^T\rangle/\sqrt{1-\beta}$, so that

$$\begin{aligned}
\sqrt{1-\varepsilon} \le |\langle\Psi|\Psi^T\rangle| &= \sqrt{\beta}\ |\langle\Psi|\Psi_{\mathrm{good}}\rangle| + \sqrt{1-\beta}\ |\langle\Psi|\Psi_{\mathrm{bad}}\rangle| \\
&\le \sqrt{\beta}\ \|\Pi_{\mathrm{good}}|\Psi\rangle\| + \sqrt{1-\beta}\ \|\Pi_{\mathrm{bad}}|\Psi\rangle\| \\
&\le \sqrt{\beta} + \sqrt{1-\beta}\ \sqrt{\operatorname{tr}\left[\Pi_{\mathrm{bad}}(\rho^{\odot}\circ M_{\mathrm{junk}})\right]} \\
&\le \sqrt{\beta} + \sqrt{\eta}.
\end{aligned}$$

Since $\eta \le 1-\varepsilon$, we obtain that $\beta \ge (\sqrt{1-\varepsilon}-\sqrt{\eta})^2$. We are now ready to bound $W^T = \operatorname{tr}(\Gamma\rho^T)$, where

$$\rho^T = \beta\rho_{\mathrm{good}} + (1-\beta)\rho_{\mathrm{bad}} + \sqrt{\beta(1-\beta)}\left[\operatorname{tr}_A(|\Psi_{\mathrm{good}}\rangle\langle\Psi_{\mathrm{bad}}|) + \operatorname{tr}_A(|\Psi_{\mathrm{bad}}\rangle\langle\Psi_{\mathrm{good}}|)\right].$$

Since $\operatorname{tr}(\Gamma\rho_{\mathrm{good}}) \ge \lambda$, $\operatorname{tr}(\Gamma\rho_{\mathrm{bad}}) \ge 1$, and the off-diagonal terms are zero, we have

$$\begin{aligned}
\mathsf{W}^T &= \beta\ \operatorname{tr}(\Gamma\rho_{\mathrm{good}}) + (1-\beta)\ \operatorname{tr}(\Gamma\rho_{\mathrm{bad}}) && (5.6) \\
&\ge 1 + (\lambda-1)\beta \ge 1 + (\lambda-1)(\sqrt{1-\varepsilon}-\sqrt{\eta})^2. && (5.7)
\end{aligned}$$

The lower bound on the query complexity is a consequence of

$$\left(\max\left\{\left\|\Gamma_i^{\frac{1}{2}}\Gamma^{-\frac{1}{2}}\right\|^2, \left\|\Gamma^{\frac{1}{2}}\Gamma_i^{-\frac{1}{2}}\right\|^2 : \forall i\in\Sigma_I\right\}\right)^T \ge K(\eta,\lambda,\varepsilon).$$

□

For classical problems (function evaluation), we can use the following lemma:

Lemma 5.14 *Let Π_{bad} be the projector on V_{bad}, $\Pi_z = \sum_{\mathcal{P}(x)=z} |x\rangle\langle x|$, and assume that $\|\Pi_z \Pi_{\text{bad}}\|^2 \leq \eta$ for any z. Then, $\operatorname{tr}[\Pi_{\text{bad}}(\rho^{\odot} \circ M)] \leq \eta$ for any junk matrix M.*

Proof. For any junk matrix M, let us define the following purification of $\rho^{\odot} \circ M$,

$$|\psi_M^{\odot}\rangle = \sum_{x \in F} \sqrt{\alpha_x} |\mathcal{P}(x)\rangle |M_x\rangle |x\rangle,$$

where $|M_x\rangle$ are normalized states such that $\langle M_x | M_{x'}\rangle = \langle x|M|x'\rangle$. Let us also consider the operator $P = \sum_z |z\rangle\langle z| \otimes \mathbb{I}_{\text{junk}} \otimes \Pi_z$. Then, we have $P|\psi_M^{\odot}\rangle = |\psi_M^{\odot}\rangle$, so that

$$\operatorname{tr}\left[\Pi_{\text{bad}}(\rho^{\odot} \circ M)\right] = \left\|\Pi_{\text{bad}}|\psi_M^{\odot}\rangle\right\|^2 = \left\|\Pi_{\text{bad}} P |\psi_M^{\odot}\rangle\right\|^2 \leq \|\Pi_{\text{bad}} P\|^2 = \max_z \|\Pi_{\text{bad}} \Pi_z\|^2 \leq \eta.$$

□

This implies that our method is an extension of Špalek's original multiplicative adversary method [Špa08].

5.3.3 Intermediate adversary method

We now introduce the *intermediate adversary* method:

Definition 5.15 (Good and bad additive subspaces) *Let $\widetilde{\Gamma}$ be an additive adversary matrix and fix a threshold $0 < \tilde{\lambda} < 1$. The eigenspaces of $\widetilde{\Gamma}$ are split into two categories: the* good subspace *V_{good} is the direct sum of the eigenspaces of $\widetilde{\Gamma}$ with eigenvalues smaller than $\tilde{\lambda}$, and the* bad subspace *V_{bad} is the direct sum of the eigenspaces of $\widetilde{\Gamma}$ with eigenvalues strictly larger than $\tilde{\lambda}$. The projector on the bad subspace is denoted by Π_{bad}.*

Theorem 5.16 (Intermediate adversary method) *Let $\mathcal{P}$ be a problem, $(\widetilde{\Gamma}, |\alpha\rangle)$ be an additive adversary, and $0 < \tilde{\lambda} < 1$ be a threshold. Denote by η the overlap of $\rho^{\odot}$ on the bad subspace. If $\eta \leq 1 - \varepsilon$, then we have:*

$$Q_\varepsilon(\mathcal{P}) \geq \frac{\widetilde{K}(\eta, \tilde{\lambda}, \varepsilon)}{\max_i \left\|\widetilde{\Gamma}_i - \widetilde{\Gamma}\right\|} \quad \textit{where} \quad \widetilde{K}(\eta, \tilde{\lambda}, \varepsilon) = (1 - \tilde{\lambda})(\sqrt{1-\varepsilon} - \sqrt{\eta})^2.$$

Proof. The proof to bound the progress done by query is identical to the proof used for the general additive method, and the proof to lower-bound the final value of the progress function is identical to the proof of the multiplicative method up to Equation (5.6). Since $\operatorname{tr}(\widetilde{\Gamma}\rho_{\text{good}}) \leq \tilde{\lambda}$, $\operatorname{tr}(\widetilde{\Gamma}\rho_{\text{bad}}) \leq 1$, and the off-diagonal terms are zero, we have

$$\begin{aligned} \widetilde{W}^T &= \beta \operatorname{tr}(\widetilde{\Gamma}\rho_{\text{good}}) + (1-\beta) \operatorname{tr}(\widetilde{\Gamma}\rho_{\text{bad}}) && (5.8)\\ &\leq 1 - (1-\tilde{\lambda})\beta \leq 1 - (1-\tilde{\lambda})(\sqrt{1-\varepsilon} - \sqrt{\eta})^2. && (5.9) \end{aligned}$$

□

Note that since the condition on the adversary matrix is very similar as for the multiplicative adversary, we can also use an analogue of Lemma 5.14 to choose the adversary matrix in the special case of classical problems.

5.4 Comparison of the adversary methods

Definition 5.17 *We define the* additive adversary bound *and the* intermediate adversary bound *respectively as*

$$\mathrm{ADV}^{\pm}_{\varepsilon}(\mathcal{P}) = \max_{\widetilde{\Gamma},|\alpha\rangle} \frac{1-C(\varepsilon)}{\max_i \left\|\widetilde{\Gamma}-\widetilde{\Gamma}_i\right\|} \qquad \textit{and} \qquad \widetilde{\mathrm{ADV}}_{\varepsilon}(\mathcal{P}) = \max_{\widetilde{\Gamma},|\alpha\rangle,\tilde{\lambda}} \frac{\tilde{K}(\eta,\tilde{\lambda},\varepsilon)}{\max_i \left\|\widetilde{\Gamma}-\widetilde{\Gamma}_i\right\|}$$

where, for $\mathrm{ADV}^{\pm}$*, the maximum is taken over additive adversary* $(\widetilde{\Gamma},|\alpha\rangle)$ *such that* $\mathrm{tr}\left[\widetilde{\Gamma}(\rho^{\odot}\circ M)\right] = 0$ *for any junk matrix* M*, while for* $\widetilde{\mathrm{ADV}}$ *it is taken over all additive adversary matrices. Finally, we define the* multiplicative adversary bound *as*

$$\mathrm{MADV}_{\varepsilon}(\mathcal{P}) = \sup_{\lambda>1} \mathrm{MADV}^{(\lambda)}_{\varepsilon}(\mathcal{P}) \quad \textit{where} \quad \mathrm{MADV}^{(\lambda)}_{\varepsilon}(\mathcal{P}) = \sup_{\Gamma,|\alpha\rangle} \frac{\log K(\eta,\lambda,\varepsilon)}{\log\max\left\{\left\|\Gamma_i^{\frac{1}{2}}\Gamma^{-\frac{1}{2}}\right\|^2,\left\|\Gamma^{\frac{1}{2}}\Gamma_i^{-\frac{1}{2}}\right\|^2:\forall i\in\Sigma_I\right\}},$$

and the supremum is taken over all multiplicative adversary $(\Gamma,|\alpha\rangle)$*.*

Remark 5.18 (Alternate formulation) Moreover, using Lemma 2.40, the multiplicative adversary bound can be rewritten:

$$\mathrm{MADV}^{c}_{\varepsilon}(\mathcal{P}) = \sup_{\Gamma,|\alpha\rangle} \frac{\log K(\eta,\lambda,\varepsilon)}{\log c},$$
$$\mathrm{MADV}_{\varepsilon}(\mathcal{P}) = \sup_{c>1} \mathrm{MADV}^{c}_{\varepsilon}(\mathcal{P}),$$

where c satisfies $\Gamma_i \preceq c\Gamma$ for all $i\in\Sigma_I$. There is a implicit relation between c, λ and η that we do not specify in this dissertation. We will use this alternate form later on.

In this Section, we show that the three methods are progressively stronger (the two inequalities are proved independently in the next two sections).

Theorem 5.19 $\mathrm{MADV}_{\varepsilon}(\mathcal{P}) \geq \widetilde{\mathrm{ADV}}_{\varepsilon}(\mathcal{P}) \geq \mathrm{ADV}^{\pm}_{\varepsilon}(\mathcal{P})/60$*.*

In a nutshell, the multiplicative adversary bound is larger than the intermediate one since bounding the relative progress is more subtle than the absolute progress; and the intermediate adversary bound is larger than the general additive since the condition on the adversary matrix is more tight.

5.4.1 Additive versus intermediate

We show that the intermediate adversary method is at least as strong as the original additive one (up to a constant factor).

Lemma 5.20 $\widetilde{\mathrm{ADV}}_{\varepsilon}(\mathcal{P}) \geq \mathrm{ADV}^{\pm}_{\varepsilon}(\mathcal{P})/60$*.*

The proof of this lemma relies on the following.

Lemma 5.21 *Let* $(\widetilde{\Gamma},|\alpha\rangle)$ *be an additive adversary such that* $\mathrm{tr}\left[\widetilde{\Gamma}(\rho^{\odot}\circ M)\right] = 0$ *for any junk matrix* M*. Then, for any* $\tilde{\lambda},\varepsilon$ *such that* $\frac{\varepsilon}{1-\varepsilon} \leq \tilde{\lambda} \leq 1$*, we have*

$$\tilde{K}(\eta,\tilde{\lambda},\varepsilon) > (1-\tilde{\lambda})\left(\sqrt{1-\varepsilon} - \frac{1}{\sqrt{1+\tilde{\lambda}}}\right)^2.$$

Proof. From the definition of $\tilde{K}(\eta, \tilde{\lambda}, \varepsilon)$, it suffices to show that $\operatorname{tr}[\Pi_{\mathrm{bad}}(\rho^{\odot} \circ M)] < 1/(1 + \tilde{\lambda})$ for any junk matrix M. Let $p_{\mathrm{bad}} = \operatorname{tr}[\Pi_{\mathrm{bad}}(\rho^{\odot} \circ M)] = \left\|\Pi_{\mathrm{bad}}|\psi_M^{\odot}\rangle\right\|^2$, where $|\psi_M^{\odot}\rangle$ is defined as above. Let us also define the states $|\psi_{\mathrm{bad}}\rangle = \Pi_{\mathrm{bad}}|\psi_M^{\odot}\rangle/\sqrt{p_{\mathrm{bad}}}$ and $|\psi_{\mathrm{good}}\rangle = \Pi_{\mathrm{good}}|\psi_M^{\odot}\rangle/\sqrt{1-p_{\mathrm{bad}}}$, so that $|\psi_M^{\odot}\rangle = \sqrt{p_{\mathrm{bad}}}|\psi_{\mathrm{bad}}\rangle + \sqrt{1-p_{\mathrm{bad}}}|\psi_{\mathrm{good}}\rangle$. From the properties of the additive adversary matrix $\widetilde{\Gamma}$, we have

$$\begin{aligned}0 = \operatorname{tr}\left[\widetilde{\Gamma}(\rho^{\odot} \circ M)\right] &= \operatorname{tr}\left[\widetilde{\Gamma}|\psi_M^{\odot}\rangle\langle\psi_M^{\odot}|\right] = p_{\mathrm{bad}}\operatorname{tr}\left[\widetilde{\Gamma}|\psi_{\mathrm{bad}}\rangle\langle\psi_{\mathrm{bad}}|\right] + (1-p_{\mathrm{bad}})\operatorname{tr}\left[\widetilde{\Gamma}|\psi_{\mathrm{good}}\rangle\langle\psi_{\mathrm{good}}|\right]\\ &> p_{\mathrm{bad}}\tilde{\lambda} + (1-p_{\mathrm{bad}})(-1) = (\tilde{\lambda}+1)p_{\mathrm{bad}} - 1.\end{aligned}$$

This implies that $p_{\mathrm{bad}} < 1/(1+\tilde{\lambda})$. □

Proof of Lemma 5.20. This is immediate for $\varepsilon \geq 1/5$ as in this case, we have $\mathrm{ADV}_{\varepsilon}^{\pm}(\mathcal{P}) = 0$. Therefore, it suffices to show that for any additive adversary $(\widetilde{\Gamma}, |\alpha\rangle)$ and any $\varepsilon < 1/5$, we have $\max_{\tilde{\lambda}} \tilde{K}(\eta, \tilde{\lambda}, \varepsilon) \geq (1 - \varepsilon - 2\sqrt{\varepsilon(1-\varepsilon)})/60$. Let

$$\tilde{\lambda} = \left(\frac{4}{1-\varepsilon}\right)^{1/3} - 1,$$

and note that $\frac{\varepsilon}{1-\varepsilon} \leq \tilde{\lambda} \leq 1$ when $0 \leq \varepsilon \leq 1/2$. By Lemma 5.21, we then have

$$\max_{\tilde{\lambda}} \tilde{K}(\eta, \tilde{\lambda}, \varepsilon) \geq 1 - 2\varepsilon - 3(2-2\varepsilon)^{2/3} + 3(2-2\varepsilon)^{1/3} \geq (1 - \varepsilon - 2\sqrt{\varepsilon(1-\varepsilon)})/60,$$

for any $0 \leq \varepsilon \leq 1/2$. □

5.4.2 intermediate versus multiplicative

We now show that the multiplicative adversary method is at least as strong as the intermediate one.

Lemma 5.22 $\lim_{\lambda\to 1} \mathrm{MADV}_{\varepsilon}^{(\lambda)}(\mathcal{P}) \geq \widetilde{\mathrm{ADV}}_{\varepsilon}(\mathcal{P})$.

Using the alternate form of the multiplicative bound, it can be shown that this lemma reads, $\lim_{c\to 1} \mathrm{MADV}_{\varepsilon}^{c}(\mathcal{P}) \geq \widetilde{\mathrm{ADV}}_{\varepsilon}(\mathcal{P})$.

Proof. Let $(\widetilde{\Gamma}, |\alpha\rangle)$ be the additive adversary achieving $\widetilde{\mathrm{ADV}}_{\varepsilon}(\mathcal{P})$. Therefore, we have

$$\widetilde{\mathrm{ADV}}_{\varepsilon}(\mathcal{P}) = \frac{\tilde{K}(\eta, \tilde{\lambda}, \varepsilon)}{\max_i \left\|\widetilde{\Gamma} - \widetilde{\Gamma}_i\right\|}.$$

Let $\Gamma(\gamma) = \mathbb{I} + \gamma(\mathbb{I} - \widetilde{\Gamma})$. Since $\operatorname{tr}(\widetilde{\Gamma}|\alpha\rangle\langle\alpha|) = 1$ and $\left\|\widetilde{\Gamma}\right\| \leq 1$, we see that for any $\gamma > 0$, $\Gamma(\gamma)$ is definite positive with $\Gamma(\gamma) \succeq \mathbb{I}$ and $\operatorname{tr}(\Gamma(\gamma)|\alpha\rangle\langle\alpha|) = 1$, therefore it is a valid multiplicative adversary matrix. Moreover, Γ has eigenvalue at least $\lambda = 1 + \gamma(1 - \tilde{\lambda})$ over V_{good}. Therefore, $K(\eta, \lambda(\gamma), \varepsilon) = 1 + \gamma\tilde{K}(\eta, \tilde{\lambda}, \varepsilon)$ and, by definition of the multiplicative adversary bound,

$$\mathrm{MADV}_{\varepsilon}(\mathcal{P}) \geq \sup_{\gamma>0} \frac{\ln\left[1 + \gamma\tilde{K}(\eta, \tilde{\lambda}, \varepsilon)\right]}{\ln\max\left\{\left\|\Gamma_i^{\frac{1}{2}}(\gamma)\Gamma^{-\frac{1}{2}}(\gamma)\right\|^2, \left\|\Gamma^{\frac{1}{2}}(\gamma)\Gamma_i^{-\frac{1}{2}}(\gamma)\right\|^2 : \forall i \in \Sigma_I\right\}}.$$

We show that in the limit $\gamma \to 0^+$, the argument of the supremum is just $\widetilde{\mathrm{ADV}}_\varepsilon(\mathcal{P})$, which implies the lemma. For the numerator, we immediately have

$$\ln\left[1+\gamma\tilde{K}(\eta,\tilde{\lambda},\varepsilon)\right] = \gamma\tilde{K}(\eta,\tilde{\lambda},\varepsilon) + \mathrm{O}\big(\gamma^2\big)\,.$$

Also, since $\Gamma_i(\gamma) = \mathbb{I} + \gamma(\mathbb{I} - \widetilde{\Gamma}_i)$, we have

$$\begin{aligned}\left\|\Gamma_i^{\frac{1}{2}}(\gamma)\Gamma^{-\frac{1}{2}}(\gamma)\right\|^2 &= \left\|\mathbb{I} + \frac{\gamma}{2}(\widetilde{\Gamma} - \widetilde{\Gamma}_i)\right\|^2 + \mathrm{O}\big(\gamma^2\big)\,,\\ \left\|\Gamma^{\frac{1}{2}}(\gamma)\Gamma_i^{-\frac{1}{2}}(\gamma)\right\|^2 &= \left\|\mathbb{I} - \frac{\gamma}{2}(\widetilde{\Gamma} - \widetilde{\Gamma}_i)\right\|^2 + \mathrm{O}\big(\gamma^2\big)\,.\end{aligned}$$

Therefore, we have for the denominator

$$L(\gamma,i) \overset{\mathrm{def}}{=} \ln\max\left\{\left\|\Gamma_i^{\frac{1}{2}}(\gamma)\Gamma^{-\frac{1}{2}}(\gamma)\right\|^2, \left\|\Gamma^{\frac{1}{2}}(\gamma)\Gamma_i^{-\frac{1}{2}}(\gamma)\right\|^2\right\} = \gamma\left\|\widetilde{\Gamma} - \widetilde{\Gamma}_i\right\| + \mathrm{O}\big(\gamma^2\big)\,.$$

Since $\lim_{\gamma\to 0^+} L(\gamma,i)$ exists for all $i \in \Sigma_I$ and there are only a finite number of possible i, we can swap lim and max, which finally implies that:

$$\lim_{\gamma\to 0}\frac{\ln\left[1+\gamma\tilde{K}(\eta,\tilde{\lambda},\varepsilon)\right]}{\ln\max\left\{\left\|\Gamma_i^{\frac{1}{2}}(\gamma)\Gamma^{-\frac{1}{2}}(\gamma)\right\|^2, \left\|\Gamma^{\frac{1}{2}}(\gamma)\Gamma_i^{-\frac{1}{2}}(\gamma)\right\|^2 : \forall i \in \Sigma_I\right\}} = \widetilde{\mathrm{ADV}}_\varepsilon(\mathcal{P}).$$

□

5.5 Related work

In a follow-up work, Troy Lee and Jérémie Roland simplified and improved the understanding of the adversary methods. First, they separated the dependency of the adversary state $|\alpha\rangle$ from the density matrix ρ^t. As a matter of fact, for every t, the state of the algorithm can be decomposed:

$$\rho^t = M^t \circ |\alpha\rangle\langle\alpha|,$$

where M^t is the Gram matrix $[M^t]_{xx'} = \langle\psi_x^t|\psi_{x'}^t\rangle$. Since $\mathrm{tr}[\Gamma(\rho^t)] = \mathrm{tr}[\Gamma(M^t \circ |\alpha\rangle\langle\alpha|)] = \mathrm{tr}[(\Gamma \circ |\alpha\rangle\langle\alpha|)M^t]$, the dependency in $|\alpha\rangle$ can be transferred to the adversary matrix. As a consequence, instead of defining the progress function for a state ρ^t that depends of some arbitrary state $|\alpha\rangle$, it is possible to express it as a Gram matrix whose coefficients depends only on the problem. An algorithm start with the Gram matrix $M^0 = \mathbb{J}$, the all-one matrix, and in the zero-error case ends with the Gram matrix $M^\odot = \sum_{x,x'}\langle\psi_{x'}|\psi_x\rangle|x\rangle\langle x'|$. Since Gram matrix are Hermitian positive semidefinite, we still call them "states of the algorithm" even if they are not normalized.

Using the alternate formulation of the multiplicative adversary bound, and the previous remark, Lee and Roland gave a beautiful formulation of the multiplicative adversary bound in the zero-error case:

$$\begin{aligned}\mathrm{MADV}_0^c(M^\odot) &= \frac{1}{\ln c}\max_{\bar{\Gamma}\succeq 0}\left\{\log\mathrm{tr}[\bar{\Gamma}M^\odot] : \mathrm{tr}[\bar{\Gamma}\mathbb{J}] = 1, \bar{\Gamma}\circ D_i \preceq c\bar{\Gamma},\ \forall i \in \Sigma_I\right\},\\ \mathrm{MADV}_0(M^\odot) &= \sup_{c>1}\mathrm{MADV}_0^c(M^\odot).\end{aligned}$$

Since we now only impose to the adversary matrix to be positive semidefinite in this setup, we denote it by $\bar{\Gamma}$ in order to avoid confusions. For the general additive and the intermediate method, the dependency in $|\alpha\rangle$ cannot be completely removed.

They also revisited the output condition of an algorithm. Consider an algorithm that produces a Gram matrix N. What are the conditions that N should satisfy in order to solve $\mathcal{P}$ with probability larger than $1-\varepsilon$? It can be shown[1] that the original additive method considers as output states, any state N such that $\|N - M^{\odot}\|_{\infty} \leq 2\sqrt{\varepsilon}$, and the general additive method the states such that $\gamma_2(N - M^{\odot}) \leq 2\sqrt{\varepsilon}$. Troy Lee and Jérémie Roland interpreted the intermediate method and the multiplicative methods as using yet another output condition, based on the classical fidelity between the probability distributions of measuring N and $M^{\odot}$ with the observable Γ.

They even found the optimal output condition that the final Gram matrix of an algorithm should obeys to solve a problem with error ε. This condition involves the Hadamard product fidelity:

Definition 5.23 (Hadamard product fidelity) *The* Hadamard product fidelity $\mathcal{F}_H(A,B)$ *between two Gram matrices A and B is defined by:*

$$\mathcal{F}_H(A,B) = \min_{|\alpha\rangle : \||\alpha\rangle\|=1} \mathcal{F}(A \circ |\alpha\rangle\langle\alpha|, B \circ |\alpha\rangle\langle\alpha|).$$

When the Gram matrices are given by their vectors, computing the Hadamard product fidelity can be expressed by a maximization over unitaries:

Claim 5.24 ([LR11]) *Let $\{|a_x\rangle\}, \{|b_x\rangle\}$ be two sets of vectors, and A, B their corresponding Gram matrices. We have*

$$\max_V \min_x \Re(\langle a_x|V|b_x\rangle) = \mathcal{F}_H(A,B),$$

where the maximization is taken over all unitaries V.

Lemma 5.25 ([LR11]) *Let $M^{\odot}$ be a target state of a problem $\mathcal{P}$, An algorithm with final state M^T solve $\mathcal{P}$ with error at most ε if and only if $\mathcal{F}_H(M^T, M^{\odot}) \geq \sqrt{1-\varepsilon}$.*

As a consequence, in the approximate case, the multiplicative bound have also a very beautiful formulation:

$$\mathrm{MADV}_\varepsilon(M^{\odot}) = \min_N \left\{\mathrm{MADV}_0(N) : \mathcal{F}_H\big(M^{\odot}, N\big) \geq \sqrt{1-\varepsilon},\ N \succeq 0,\ N \circ \mathbb{I} = \mathbb{I}\right\}.$$

For the rest of this chapter, we will now use this definition since separating the output condition from the adversary matrix will be helpful.

5.6 Relation with the polynomial method

In this section we show an explicit reduction from the polynomial method to the multiplicative adversary. The polynomial has a more restrictive scope than the adversary method. We consider only the case of function evaluation, and more precisely Booleans functions. To mainstream the notations we will use f to denote $\mathcal{P}$. We also consider only inputs that are binary strings of size n.

Even with those restrictions, considering state generation as intermediate steps will simplify the proof.

[1] Personnal communication with Troy Lee and Jérémie Roland.

5.6.1 Polynomial method

Definition 5.26 (Approximate degree) *For any $\varepsilon \geq 0$, the* approximate degree $\widetilde{\deg}_\varepsilon(f)$ *of a function $f : \{0,1\}^n \to \mathbb{R}$ is defined as:*

$$\widetilde{\deg}_\varepsilon(f) = \min_p \{\deg(p) : \forall x \in \{0,1\}^n,\ |f(x) - p(x)| \leq \varepsilon\},$$

where the minimum is over n-variate polynomials $p : \mathbb{R}^n \to \mathbb{R}$.

Theorem 5.27 (Polynomial method [BBC+01]) *If f is a Boolean function, then $Q_\varepsilon(f) \geq \Omega\Big(\widetilde{\deg}_\varepsilon(f)\Big)$.*

To compare the polynomial bound and the multiplicative adversary bound, we introduce the *max-adversary* method, that is, once again, an intermediate method between the polynomial method and the multiplicative method. The main idea behind this method is to rewrite the polynomial method with a progress function: this progress function can increase by at most one at each query, exactly as the degree of the coefficients in the polynomial method.

5.6.2 Max-adversary method

Let us introduce a new adversary method that we call max-adversary method. The basic idea is to define an ordered set of orthogonal subspaces $(\mathcal{S}_k : 0 \leq k \leq K)$ such that any query can only transfer weight from subspace $\mathcal{S}_k$ to its immediate neighbors, i.e. on subspace $\mathcal{S}_{k'}$ if $|k - k'| \leq 1$. In that case, if the initial Gram matrix $\mathbb{J}$ only has overlap on $\mathcal{S}_0$ and the final Gram matrix $M^\odot$ has non-zero overlap on a subspace $\mathcal{S}_{k_0}$, then k_0 is a lower bound on the query complexity of $M^\odot$. This leads to the following adversary bound.

Definition 5.28 (Max-adversary bound) *Let $M^\odot$ be a Gram matrix specifying a quantum state generation problem. The zero-error max-adversary bound is:*

$$\mathrm{ADV}_0^{\max}(M^\odot) = \max_P \left\{k_0 : \mathrm{tr}(\Pi_{k_0} M^t) \neq 0\right\},$$

where the maximization is over ordered sets of projectors $P = (\Pi_k : 0 \leq k \leq K)$ satisfying the 3 following constraints:

① $\sum_k \Pi_k = \mathbb{I}_{\mathbb{C}^{2^n}}$,

② $\mathrm{tr}(\Pi_0 \mathbb{J}) = 2^n$,

③ $\forall i \in [1,n], \forall k, k'$ *such that* $|k - k'| > 1$, $\begin{cases} \Pi_{k'}(\Pi_k \circ D_i) = 0 \\ (\Pi_k \circ D_i)\Pi_{k'} = 0 \end{cases}$.

The bounded-error bound is defined as:

$$\mathrm{ADV}_\varepsilon^{\max}(M^\odot) = \min_N \left\{\mathrm{ADV}_0^{\max}(N) : \mathcal{F}_H\big(M^\odot, N\big) \geq \sqrt{1-\varepsilon},\ N \succeq 0,\ N \circ \mathbb{I} = \mathbb{I}\right\}.$$

The name *max*-adversary comes from the fact that we define the progress function as the index of the maximal eigenspace on which M^t has support, whereas in all the other adversary methods, the progress function is defined as an average over those indices.

Theorem 5.29 (Max-adversary) $Q_\varepsilon(M^\odot) \geq \mathrm{ADV}_\varepsilon^{\max}(M^\odot)$.

Proof. We track the change of a progress function

$$W[M^t] = \max_k \left\{k : \mathrm{tr}[\Pi_k M^t] \neq 0\right\}.$$

By condition ②, the first Gram matrix $M^0 = \mathbb{J}$ has only support on $\mathcal{S}_0$, so its initial value is 0. The final value is $\mathrm{ADV}^{\max}_\varepsilon(M^\odot)$. It suffices to show that one query increases the progress function by at most one.

Similarily to Equation (5.5), we decompose $M^t = \sum_i M^t_i$. This means that M^t_i is the reduced Gram matrix corresponding to the part of the state where the bit x_i is queried. Recall that after the t-th query, the Gram matrix of the algorithm will be $M^{t+1} = \sum_i M^t_i \circ D_i$. Let $k_0 = W[M^t]$. Remark that for all i, $W[M^t_i]$ is positive, thus by definition of k_0, we also have $W[M^t_i] \leq k_0$. Hence it is sufficient to prove that for all $k > k_0 + 1$, we have $\mathrm{tr}[\Pi_k M^t_i] = 0$ to conclude the proof. Fix $0 \leq k \leq K$, we get:

$$\mathrm{tr}[\Pi_k(M^t_i \circ D_i)] = \mathrm{tr}[(\Pi_k \circ D_i)M^t_i] = \sum_{l,m\leq k_0} \mathrm{tr}[(\Pi_k \circ D_i)\Pi_l M^t_i \Pi_m].$$

The last equality holds since M^t_i has no support on the spaces S_k for $k > k_0$ by definition of k_0. This quantity is null for all $k > k_0 + 1$, therefore the progress function can increase by at most one per query. □

5.6.3 Max versus multiplicative

We have previously shown that in the limit $c \to 1$, the multiplicative adversary bound $\mathrm{MADV}^c_0(M^\odot)$ is at least as strong as the additive adversary bound $\mathrm{ADV}^\pm(M^\odot)$. Here, we show that the max-adversary bound can be obtained by taking the limit $c \to \infty$.

There is a good intuitive explanation to this fact. Recall that the progress function $\mathrm{tr}[\bar{\Gamma} M^t] = \sum \lambda_k \mathrm{tr}[\Pi_k M^t]$ is the average weighted by the λ_k of M^t on the spaces spanned by the Π_k, whereas the max-adversary is simply the maximum of the index of those spaces, thus by taking weights that are increase exponentially, the average is then quite close to the maximum.

Theorem 5.30 *For any $\varepsilon \geq 0$ and any Gram matrix $M^\odot$, we have*

$$\lim_{c\to\infty} \mathrm{MADV}^c_0(M^\odot) \geq \mathrm{ADV}^{\max}_0(M^\odot).$$

This theorem is for the zero-error case, but since the ε-error case can be obtained for both bounds using the same optimization, we immediately obtain the following corollary.

Corollary 5.31 *For any $\varepsilon \geq 0$ and any Gram matrix $M^\odot$,*

$$\mathrm{MADV}_\varepsilon(M^\odot) \geq \mathrm{ADV}^{\max}_\varepsilon(M^\odot).$$

Proof of Theorem 5.30. Let $\{\Pi_k\}$ be a set of projectors such that $T = \mathrm{ADV}^{\max}_0(M^\odot)$. Therefore, we have $\mathrm{tr}(\Pi_0 \mathbb{J}) = 2^n$ and $\mathrm{tr}(\Pi_T M^\odot) \neq 0$. We construct the multiplicative adversary matrix

$$\bar{\Gamma} = \frac{1}{2^n} \sum_k \lambda^k \Pi_k,$$

for some $\lambda > 1$ (we will later take the limit $\lambda \to \infty$). Then $\bar{\Gamma}$ satisfies $\operatorname{tr}(\bar{\Gamma}\mathbb{J}) = 1$ and $\operatorname{tr}(\bar{\Gamma}M^{\odot}) \geq \lambda^T p_T > 0$, where we have defined $p_T = \operatorname{tr}(\Pi_T M^{\odot})/2^n > 0$.

We now show that for $c = 3\lambda$, we have $\bar{\Gamma}\circ D_i \preceq c\bar{\Gamma}$ for all i. We recall that for a phase oracle $D_i = \sum_{x,x'}(-1)^{x_i+x'_i}|x\rangle\langle x'|$, and for any matrix A, $A\circ D_i = U_i A U_i^\dagger$ where U_i is the diagonal unitary matrix $U_i = \sum_x (-1)^{x_i}|x\rangle\langle x|$. Let us first observe that $\forall k \in [1, K-1]$, $U_i\Pi_k U_i$ has eigenvalues at most one and support only on the spaces spanned by Π_{k-1}, Π_k, and Π_{k-1}. As a consequence we have $\lambda^k U_i\Pi_k U_i \preceq \lambda^k(\Pi_{k-1}+\Pi_k+\Pi_{k+1}) \preceq \lambda\left(\lambda^{k-1}\Pi_{k-1} + \lambda^k\Pi_k + \lambda^{k+1}\Pi_{k+1}\right)$. The cases $k=0$ and $k=K$ are handled in a similar manner. We also observe that $\Pi_k\circ D_i$ and $\Pi_{k+3}\circ D_i$ have no overlap, thus $\bar{\Gamma}_j = \sum_{k=0}^{\lfloor K/3\rfloor}\lambda^{3k+j}U_i\Pi_{3k+j}U_i \preceq \lambda\bar{\Gamma}$. By decomposing $\bar{\Gamma} = \bar{\Gamma}_0 + \bar{\Gamma}_1 + \bar{\Gamma}_2$ we get:

$$\forall i \in [n],\ \bar{\Gamma}\circ D_i \preceq 3\lambda\cdot\bar{\Gamma}.$$

Combining everything, we have:

$$\mathrm{MADV}_0^c(M^{\odot}) \geq \frac{\log \operatorname{tr}[\bar{\Gamma}M^{\odot}]}{\log c} \geq T\cdot\frac{\log(c/3)}{\log c} + \frac{\log p_T}{\log c} \xrightarrow[c\to\infty]{} T.$$

□

5.6.4 Polynomial versus max-adversary

This section compares the bounds obtained by the polynomial method and the max-adversary method. The common point between these two methods is that they both have a quantity that increases by at most one per query. For the max-adversary method, this quantity is the progress function; and for the polynomial method, it is the degree of the amplitudes of the basis states (see proof of the polynomial method [BBC+01]). The proof makes a formal link between these two quantities by defining spaces $\mathcal{S}_k$ characterizing polynomial of degree k with very little Fourier analysis on the Boolean cube.

For a Boolean function f, let us define the $\{1,-1\}$-valued function $\varphi : \{0,1\}^n \to \{1,-1\} : x \to (-1)^{f(x)}$. There are two natural quantum state generation problems associated to f, corresponding to the Gram matrices

$$F = \sum_{x,x'}\delta_{f(x),f(x')}|x\rangle\langle x'| \quad\text{and}\quad \Phi = \sum_{x,x'}\varphi(x)\varphi(x')|x'\rangle\langle x|.$$

Indeed, generating the Gram matrix F non-coherently is exactly the same problem as computing f, while generating the Gram matrix Φ coherently corresponds to *computing the function in the phase*, i.e., we need to generate the state $\varphi(x)|\bar{0}\rangle$. The bounded-error complexities of these problems are closely related:

Claim 5.32 ([LR11]) $Q_{(1-\sqrt{1-\varepsilon})/2+\varepsilon/4}(f) \leq Q_\varepsilon(\Phi) \leq 2Q_{(1-\sqrt{1-\varepsilon})/2}(f)$.

We insist that the problem corresponding to compute f is an **incoherent** quantum state generation problem, whereas computing f "in the phase" corresponds to the **coherent** state generation problem of the Gram matrix Φ.

This implies that to prove lower bounds on the bounded-error query complexity of f, it is sufficient to prove lower bounds on the query complexity of the related quantum state generation problem Φ, and this is precisely the approach that we will use in this section.

Theorem 5.33 *Let f be a Boolean function and Φ be the Gram matrix corresponding to computing f in the phase. For any $0 \leq \varepsilon < 1/2$, we have*

$$\mathrm{ADV}_{\varepsilon}^{\max}(\Phi) \geq \widetilde{\deg}_{\varepsilon}(f).$$

Combined with Claim 5.32 this immediately implies the polynomial lower bound as corollary.

Corollary 5.34 $Q_{(1-\sqrt{1-\varepsilon})/2}(f) \geq \frac{\widetilde{\deg}_{\varepsilon}(f)}{2}$.

The proof of Theorem 5.33 relies on the following property of the Hadamard product fidelity $\mathcal{F}_H$. Recall that $\Re(z)$ denotes the real part of the complex z.

Claim 5.35 *Let f be a Boolean function and Φ be the corresponding phase matrix. Then, for any Gram matrix N such that $\mathcal{F}_H(N, \Phi) \geq \sqrt{1-\varepsilon}$, we have $\left|\Re(N_{x,x'}) - \Phi_{x,x'}\right| \leq 2\varepsilon$ for all x, x'.*

Proof. By Claim 5.24, there exists a set of unit vectors $\{|n_x\rangle\}$ such that for all x, x', we have $N_{x,x'} = \langle n_x | n_{x'}\rangle$ and $\Re\langle n_x|\varphi(x)|\bar{0}\rangle \geq \sqrt{1-\varepsilon}$. For each x, let us define the scalar ε_x such that $\Re\langle n_x|\bar{0}\rangle = \varphi(x)\sqrt{1-\varepsilon_x}$ and the vector $|e_x\rangle = |n_x\rangle - \varphi(x)\sqrt{1-\varepsilon_x}|\bar{0}\rangle$. Therefore, we have by definition

$$|n_x\rangle = \varphi(x)\sqrt{1-\varepsilon_x}|\bar{0}\rangle + |e_x\rangle,$$

where $\Re\langle\bar{0}|e_x\rangle = 0$ and $\||e_x\rangle\| = \sqrt{\varepsilon_x} \leq \sqrt{\varepsilon}$. Finally, this implies

$$\varphi(x)\varphi(x')\Re\langle n_x|n_{x'}\rangle = \sqrt{(1-\varepsilon_x)(1-\varepsilon_{x'})} + \varphi(x)\varphi(x')\Re\langle e_x|e_{x'}\rangle \geq 1 - 2\varepsilon,$$

and in turn $|\Re\langle n_x|n_{x'}\rangle - \varphi(x)\varphi(x')| \leq 2\varepsilon$. □

The other main ingredient of the proof is basic properties of the Fourier basis on the Boolean cube (see e.g. [dW08]).

Definition 5.36 (Fourier basis) *For every subset $S \subseteq [n]$, we denote by $|\chi_S\rangle$ the Fourier state*

$$|\chi_S\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{S\cdot x}|x\rangle,$$

where $S \cdot x$ is the inner product of S and x when both are seen as vectors of $\mathbb{C}^{2^n}$, i.e. $S \cdot x = \sum_{i\in S} x_i$. The set $\{|\chi_S\rangle,\ S \subseteq [n]\}$ is an orthonormal basis of $\mathbb{C}^{2^n}$.

Lemma 5.37 *The set $\{\Pi_k\}$ where $\Pi_k = \sum_{S:|S|=k} |\chi_S\rangle\langle\chi_S|$ satisfies the 3 properties in Definition 5.28.*

Observe that this set is independent of any function f. This will lead to the fact that there exists a fixed multiplicative adversary matrix independent of the problem such that the multiplicative bound obtained by using this matrix is as stronger than the polynomial method.

Proof. The set $\{\Pi_k\}$ satisfies conditions ① and ②. Let us show that it also satisfies condition ③. For any $l \in [n-1]$ and $i \in [n]$, we have

$$\Pi_l \circ D_i = \frac{1}{2^n} \sum_{S:|S|=l} \sum_{x,x'} (-1)^{S\cdot(x+x')+x_i+x'_i} |x\rangle\langle x'| = \sum_{\substack{S:|S|=l+1 \\ i\in S}} |\chi_S\rangle\langle\chi_S| + \sum_{\substack{S:|S|=l-1 \\ i\notin S}} |\chi_S\rangle\langle\chi_S|.$$

We also have $\Pi_0 \circ D_i = |\chi_{\{i\}}\rangle\langle\chi_{\{i\}}|$ and $\Pi_n \circ D_i = |\chi_{[n]\setminus\{i\}}\rangle\langle\chi_{[n]\setminus\{i\}}|$. Condition ③ is then enforced.

□

We are now ready to prove that this adversary method leads to the same lower bound as the polynomial method.

Proof of Theorem 5.33. Recall that we associate to any Boolean function f the $\{-1,1\}$-valued function defined by $\varphi(x) = (-1)^{f(x)} = 1 - 2f(x)$. We then have $\deg(\varphi) = \deg(f)$.

We denote by $|\varphi\rangle = \sum_x (-1)^{f(x)}|x\rangle$ the non-normalized quantum state representing the function φ. For all $S \subseteq [n]$, the S-indexed *Fourier coefficient* $\hat{\varphi}(S)$ of the function φ is defined by $\hat{\varphi}(S) = \langle\chi_S|\varphi\rangle$. They have the property that $\hat{\varphi}(S) = 0$ if S has more elements than $\deg(\varphi)$. Hence, $|\varphi\rangle$ in the Fourier basis reads

$$|\varphi\rangle = \sum_{S:|S|\leq\deg(\varphi)} \hat{\varphi}(S)|\chi_S\rangle = \sum_{S:|S|\leq\deg(f)} \hat{\varphi}(S)|\chi_S\rangle.$$

. For the problem of computing the function f in the phase, the final Gram matrix is $\Phi = |\varphi\rangle\langle\varphi|$, hence $\mathrm{tr}(\Pi_d\Phi) \neq 0$ for $d = \deg(f)$ (see e.g. [dW08]), which immediately proves the theorem in the special case $\varepsilon = 0$ since this implies that $\mathrm{ADV}_0^{\max}(\Phi) \geq \deg(f)$.

Let us now fix $\varepsilon > 0$. We now show that for any Gram matrix N such that $\mathcal{F}_H(N,\Phi) \geq \sqrt{1-\varepsilon}$, there exists $T \geq \widetilde{\deg}_\varepsilon(f)$ such that $\mathrm{tr}(\Pi_T N) \neq 0$, which implies the theorem by definition of $\mathrm{ADV}_\varepsilon^{\max}(\Phi)$. Let N be any such matrix. Fix $x_0 \in \{0,1\}^n$ and define the multilinear polynomial p by

$$p(x) = \varphi(x_0)\Re\langle n_x|n_{x_0}\rangle.$$

By Claim 5.35, we have $|\Re(\langle n_x|n_{x_0}\rangle - \varphi(x_0)\varphi(x_0))| \leq 2\varepsilon$ for any x, therefore $\max_x |\varphi(x) - p(x)| \leq 2\varepsilon$. As a consequence the polynomial $q = (1+p)/2$ is an ε-approximation of f since $\varphi = 1-2f$.

Let $T = \max_k \{k : \mathrm{tr}(\Pi_k N) \neq 0\}$. Then, the matrix N can be written as $N = \sum_{S,S'} \alpha_{S,S'}|\chi_S\rangle\langle\chi_{S'}|$ where the sum is over all the sets of size at most T. Then the coefficient

$$N_{x_0,x} = \sum_S \left(\sum_{S'} \alpha_{S,S'}\chi_S(x_0)\right)\chi_{S'}(x)$$

is a polynomial of degree at most T in x, and so is p. Thus

$$\widetilde{\deg}_\varepsilon(f) \leq T = \max_k \{k : \mathrm{tr}(\Pi_k N) \neq 0\},$$

that is, there exists $T \geq \widetilde{\deg}_\varepsilon(f)$ such that $\mathrm{tr}(\Pi_T N) \neq 0$. □

5.7 Summary

We extended the multiplicative adversary method and the general adversary method to quantum state generation problems which is a generalization of their usual scope: computing functions. This generalization gives a clearer view on the adversary methods by considering that one should put weight on spaces instead of on pairs of inputs. This was used to prove that the multiplicative adversary is stronger that the general additive (by introducing another intermediate method: the intermediate adversary method). Considering quantum state generation problems was also very useful to give an explicit reduction from the polynomial method to the multiplicative method.

6 Applications

6.1 Strong direct product theorem

In this section we extend Špalek's strong direct product theorem [Špa08] to quantum state generation problems. We prove that for any problem which accepts a multiplicative adversary bound $\mathrm{MADV}_{\varepsilon}^{(\lambda)}(\mathcal{P})$, if one wants to solve $\mathcal{P}^{(k)}$, i.e., k independent instances of $\mathcal{P}$, using less than $\mathrm{O}(k)$ times the number of queries necessary to solve one instance with error ε, then the success probability for $\mathcal{P}^{(k)}$ is exponentially small in k.

Theorem 6.1 (Strong direct product) *For any $\varepsilon > 0$ and $\lambda > 1$ there exist a constant $0 < s < 1$ and two integers k_0, κ such that for any problem $\mathcal{P}$ and $k > k_0$:*

$$\mathrm{MADV}_{1-s^k}^{(\lambda)}(\mathcal{P}^{(k)}) \geq \frac{k}{\kappa} \cdot \mathrm{MADV}_{\varepsilon}^{(\lambda)}(\mathcal{P}).$$

Proof. This proof closely follows the footsteps of the one by Špalek in [Špa08, Section 5], which dealt with the special case of computing functions. Let us assume that the multiplicative adversary bound for $\mathcal{P}$ with threshold λ is obtained by the adversary $(\Gamma, |\alpha\rangle)$. For $\mathcal{P}^{(k)}$, we construct an adversary $(\Gamma' = \Gamma^{\otimes k}, |\alpha'\rangle = |\alpha\rangle^{\otimes k})$ and set the threshold at value $\lambda' = \lambda^{\frac{k}{\kappa}}$, where κ is an integer that will be fixed later.

First of all we observe that $\max_{i\in\Sigma_I, j\in[k]} \left\| \Gamma'^{\frac{1}{2}}_{i,j} \Gamma'^{-\frac{1}{2}} \right\| = \max_{i\in\Sigma_I} \left\| \Gamma_i^{\frac{1}{2}} \Gamma^{-\frac{1}{2}} \right\|$ where j is the index of the queried oracle and $\Gamma'_{i,j} = \Gamma' \circ (\mathbb{J}^{j-1} \otimes D_i \otimes \mathbb{J}^{k-j})$, $\mathbb{J}$ being the all-one matrix of size $|F| \times |F|$. The proof follows by noting that for all $i \in \Sigma_I$ and for all $j \in [k]$ we have

$$\begin{aligned} \Gamma'^{\frac{1}{2}}_{i,j} \Gamma'^{-\frac{1}{2}} &= \left(\Gamma^{\frac{1}{2}}{}^{\otimes j-1} \otimes \Gamma_i^{\frac{1}{2}} \otimes \Gamma^{\frac{1}{2}}{}^{\otimes k-j} \right) \left(\Gamma^{-\frac{1}{2}}{}^{\otimes j-1} \otimes \Gamma^{-\frac{1}{2}} \otimes \Gamma^{-\frac{1}{2}}{}^{\otimes k-j} \right) \\ &= \mathbb{I}^{\otimes j-1} \otimes \Gamma_i^{\frac{1}{2}} \Gamma^{-\frac{1}{2}} \otimes \mathbb{I}^{\otimes k-j}. \end{aligned}$$

The same calculation holds for the uncomputing oracle: $\Gamma'^{-\frac{1}{2}}_{i,j} \Gamma'^{\frac{1}{2}} = \mathbb{I}^{\otimes j-1} \otimes \Gamma_i^{-\frac{1}{2}} \Gamma^{\frac{1}{2}} \otimes \mathbb{I}^{\otimes k-j}$.

Let us now find an upper bound of $\max_M \mathrm{tr}[\Pi'_{\mathrm{bad}}(\rho^{\odot} \circ M)]$. The "bad" subspace V'_{bad} for the problem $\mathcal{P}^{(k)}$ is defined by the direct sum of eigenspaces of $\Gamma^{\otimes k}$ with eigenvalue at most $\lambda' = \lambda^{k/\kappa}$. While, we do not have in general $V'_{\mathrm{bad}} \subset V_{\mathrm{bad}}^{\otimes k}$ nor $V_{\mathrm{bad}}^{\otimes k} \subset V'_{\mathrm{bad}}$, we know that V'_{bad} is a subspace of the direct sum of spaces $\bigotimes_{j=1}^{k} V_{v_j}$ where $v \in \{\mathrm{good}, \mathrm{bad}\}^k$ and the number of good subspaces $|v|$ is at most $\frac{k}{\kappa}$. Indeed, any other eigenspace of Γ' has eigenvalue at least $1^{(\kappa-1)k/\kappa} \lambda^{k/\kappa} = \lambda'$ since the eigenvalues of Γ are greater than 1, and those associated to good subspaces are greater than $\lambda > 1$. Therefore, the projector Π'_{bad} on the bad subspace is such that $\Pi'_{\mathrm{bad}} = \Pi'_{\mathrm{bad}} \cdot \left(\bigoplus_{v:|v|<k/\kappa} \bigotimes_j \Pi_{v_j} \right)$. Let us consider a junk matrix M' for $\mathcal{P}^{(k)}$. Such a matrix can be written as $M' = \sum_l m_l \bigotimes_{j=1}^{k} M_{j,l}$ where $\sum_l m_l = 1$, and each $M_{j,l}$ is a junk

matrix for $\mathcal{P}$.

$$
\begin{aligned}
\mathrm{tr}[\Pi'_{\mathrm{bad}}(\rho^{\odot\otimes k} \circ M')] &\leq \sum_{v:|v|<k/\kappa} \sum_{l} m_l \mathrm{tr}\left[\bigotimes_{j=1}^{k} \Pi_{v_j}(\rho^{\odot} \circ M_{jl})\right] \\
&= \sum_{v:|v|<k/\kappa} \sum_{l} m_l \prod_{j} \mathrm{tr}[\Pi_{v_j}(\rho^{\odot} \circ M_{jl})] \\
&\leq \sum_{v:|v|<k/\kappa} \sum_{l} m_l \eta^{(\kappa-1)k/\kappa} \\
&= \eta^{(\kappa-1)k/\kappa} \sum_{v:|v|<k/\kappa} 1 \\
&\leq \eta^{(\kappa-1)k/\kappa} (\kappa e)^{k/\kappa} \\
&\leq \left[(\kappa e)^{1/\kappa} \eta^{(\kappa-1)/\kappa}\right]^k \\
&\leq \eta'^k,
\end{aligned}
$$

where $\eta' = (\kappa e)^{1/\kappa}(1-\varepsilon)^{(\kappa-1)/\kappa}$, and we choose a large enough integer κ so that $\eta' < 1$ (this is always possible as $1-\varepsilon < 1$). Let us also define the constant $\zeta' = \left(\frac{1+(\lambda-1)(1-\varepsilon)}{\lambda}\right)^{1/\kappa}$ and note that $\zeta' < 1$ since $\lambda > 1$ and $1-\varepsilon < 1$. Therefore, for large enough k_0, there exists a constant $0 < s < 1$ such that for all $k \geq k_0$, $\zeta'^{k/2} + \eta'^{k/2} \leq s^{k/2}$. For such k's, we choose $\varepsilon' = 1 - s^k$. With these choices, we have

$$
\begin{aligned}
K(\eta', \lambda', \varepsilon') = 1 + (\lambda'-1)(\sqrt{1-\varepsilon'}^{k/2} - \eta'^{k/2}) &\geq 1 + (\lambda'-1)\zeta'^k \\
\geq 1 + (1-\lambda^{-k/\kappa}) K(\eta, \lambda, \varepsilon)^{k/\kappa} &\geq K(\eta, \lambda, \varepsilon)^{k/\kappa},
\end{aligned}
$$

where we used the fact that $K(\eta, \lambda, \varepsilon) = 1 + (\lambda-1)(\sqrt{1-\varepsilon} - \sqrt{\eta})^2 \leq \lambda\zeta'^{\kappa} \leq \lambda$. Combining everything, we then have

$$
\begin{aligned}
\frac{k}{\kappa} \cdot \mathrm{MADV}_{\varepsilon}(\mathcal{P}) &= \frac{\ln K(\eta, \lambda, \varepsilon)^{k/\kappa}}{\ln \max\left\{\left\|\Gamma_i^{\frac{1}{2}}\Gamma^{-\frac{1}{2}}\right\|^2, \left\|\Gamma^{\frac{1}{2}}\Gamma_i^{-\frac{1}{2}}\right\|^2 : \forall i \in \Sigma_I\right\}} \\
&\leq \frac{\ln K(\eta', \lambda', \varepsilon')}{\ln \max\left\{\left\|\Gamma_i'^{\frac{1}{2}}\Gamma'^{-\frac{1}{2}}\right\|^2, \left\|\Gamma'^{\frac{1}{2}}\Gamma_i'^{-\frac{1}{2}}\right\|^2 : \forall i \in \Sigma_I\right\}} \leq \mathrm{MADV}_{\varepsilon'}(\mathcal{P}^{(k)}).
\end{aligned}
$$

□

Let us note that while we have proved that the multiplicative adversary method is stronger than the additive one, we cannot directly conclude that this strong direct product theorem also applies to the additive bound, in particular we cannot conclude that the bounded-error quantum query complexity of any function obeys a strong direct product theorem. This is because we can only prove that the multiplicative adversary method becomes stronger in the limit of λ going to 1, while in the same limit the constant s in the theorem also goes to 1. Therefore, this only implies a direct sum theorem for the additive adversary bound.

However, we made a significant step towards a proof that the quantum query complexity obeys a strong direct product theorem. In the special of functions, Troy Lee and Jérémie Roland filled up the missing part of the proof [LR11]. They overcame the issue by using the alternate formulation of the multiplicative bound (see Remark 5.18). More precisely they showed that there exists $c_0(\varepsilon) > 1$ such that for all $c < c_0(\varepsilon)$, $\mathrm{MADV}_\varepsilon^{(c)}(\mathcal{P}) \geq \mathrm{ADV}_\varepsilon^{\pm}(\mathcal{P})/60$ for any problem $\mathcal{P}$. The question wether the quantum query complexity obeys a SDPT for quantum state generation problems remains opened.

6.2 Using the representation theory

There are two main challenges to derive an adversary bound: first, one needs to find an optimal adversary, and then to compute the norm of $\Gamma_i - \Gamma$ in an additive setting or $\Gamma^{1/2}\Gamma_i^{-1/2}$ for the multiplicative bound.

In this section we study how we can leverage the symmetries of a problem in order to simplify these two tasks. This leads to a very elegant solution when a natural representation of its automorphism group is multiplicity-free. We recall that the set of inputs of length N over an alphabet of size M is denoted by F.

6.2.1 Symmetrization of the circuit

In this section we will study how the symmetries of the problem can help choosing the adversary matrix and in turn obtain the lower bounds. Let us consider permutations $(\pi, \tau) \in S_N \times S_M$ acting on $x \in F$ as

$$\forall i \in \Sigma_I,\ x^{\pi,\tau}(i) = \tau(x_{\pi(i)}).$$

Definition 6.2 (Automorphism group of $\mathcal{P}$) *We call a group $G \subseteq S_N \times S_M$ an* automorphism group *of a problem $\mathcal{P}$ if*

- *For any $(\pi, \tau) \in G$ and $x \in F$, we have $x^{\pi,\tau} \in F$.*
- *For any $(\pi, \tau) \in G$, there exists a unitary $V_{\pi,\tau}$ such that $V_{\pi,\tau}|\mathcal{P}(x)\rangle = |\mathcal{P}(x^{\pi,\tau})\rangle$ for all $x \in F$.*

Note that from an oracle for x, it is easy to simulate an oracle for $x^{\pi,\tau}$ by prefixing and appending the necessary permutations on the input and output registers. Consider for example a computing oracle call. Then, $O_{x^{\pi,\tau}}$ acts on $|i\rangle|0\rangle$ just as $(\pi^{-1} \otimes \tau)O_f(\pi \otimes \mathbb{I})$.

Therefore, if (π, τ) is an element of an automorphism G of $\mathcal{P}$, we can solve the problem with oracle x in the following indirect way:

1. Solve the problem for $x^{\pi,\tau}$, which will prepare a state close to $|\mathcal{P}(x^{\pi,\tau})\rangle$.
2. Apply $V_{\pi,\tau}^{\dagger}$ to map this state to a state close to $|\mathcal{P}(x)\rangle$.

Since we want the algorithm to work just as well for any possible x, we can use this property to symmetrize the circuit. The idea is to solve the algorithm for x by solving it for $x^{\pi,\tau}$ for all possible $(\pi, \tau) \in G$ simultaneously in superposition. Just as we considered $|x\rangle$ as an additional input to the circuit, we can also use the same mathematical trick and consider $|\pi, \tau\rangle$ as another input. We then run the algorithm on the superposition $\frac{1}{\sqrt{|G|}} \sum_{(\pi,\tau)\in G} |\pi, \tau\rangle$. Note that we can assume without loss of generality that the best algorithm for $\mathcal{P}$ is symmetrized. Indeed, for any algorithm for $\mathcal{P}$ with success probability p and query complexity T, the symmetrized version will have the same query complexity and a success probability at least p. For the same reason, we can also assume that the optimal adversary matrix satisfies a similar symmetry, in the following sense:

Lemma 6.3 *For all $(\pi, \tau) \in G$, let $U_{\pi,\tau}$ be the unitary that maps $|x\rangle$ to $|x^{\pi,\tau}\rangle$. Then, we can assume without loss of generality that the optimal adversary matrix Γ satisfies $U_{\pi,\tau}\Gamma U_{\pi,\tau}^\dagger = \Gamma$ for any $(\pi, \tau) \in G$.*

Proof. Let Γ be an adversary matrix that does not satisfy this property, and $|\alpha\rangle = \sum_x \sqrt{\alpha_x}|x\rangle$ be one of its eigenstates with eigenvalue 1.. We have $\Gamma|\alpha\rangle = |\alpha\rangle$, so in particular the condition $\mathrm{tr}[\Gamma|\alpha\rangle\langle\alpha|] = 1$. Let

$$\bar{\alpha}_x = \frac{1}{|G|}\sum_{(\pi,\tau)\in G} \alpha_{x^{\pi,\tau}}$$

and let us consider the following states and matrices

$$|\bar{\alpha}\rangle = \sum_x \sqrt{\bar{\alpha}_x}|x\rangle, \qquad |\bar{\alpha}\rangle = \sum_x \frac{1}{\sqrt{\bar{\alpha}_x}}|x\rangle,$$
$$\bar{\Gamma} = \frac{1}{|G|}\sum_{(\pi,\tau)\in G} U_{\pi,\tau}(\Gamma \circ |\alpha\rangle\langle\alpha| \circ |\bar{\alpha}\rangle\langle\bar{\alpha}|)U_{\pi,\tau}^\dagger, \qquad M^\odot = \sum_{x,x'}\langle\mathcal{P}(x)|\mathcal{P}(x')\rangle\ |x'\rangle\langle x|.$$

Let us note that any of the matrices $|\bar{\alpha}\rangle\langle\bar{\alpha}|, |\bar{\alpha}\rangle\langle\bar{\alpha}|, \bar{\Gamma}$ and $M^\odot$ satisfy the required symmetry under the action of G, i.e., $U_{\pi,\tau}\bar{\Gamma}U_{\pi,\tau}^\dagger = \bar{\Gamma}$ for any $(\pi, \tau) \in G$, and similarly for the other matrices. For $|\bar{\alpha}\rangle\langle\bar{\alpha}|, |\bar{\alpha}\rangle\langle\bar{\alpha}|$ and $\bar{\Gamma}$, it follows directly from their definition and the fact that $\bar{\alpha}_{x^{\pi,\tau}} = \bar{\alpha}_x$ for any $(\pi, \tau) \in G$, while for $M^\odot$, it follows from the definition of the automorphism group: for any $(\pi, \tau) \in G$, we have

$$\begin{aligned} U_{\pi,\tau}M^\odot U_{\pi,\tau}^\dagger &= \sum_{x,x'}\langle\mathcal{P}(x)|\mathcal{P}(x')\rangle\ |x'^{\pi,\tau}\rangle\langle x^{\pi,\tau}| = \sum_{x,x'}\langle\mathcal{P}(x^{\pi^{-1},\tau^{-1}})|\mathcal{P}(x'^{\pi^{-1},\tau^{-1}})\rangle\ |x'\rangle\langle x| \\ &= \sum_{x,x'}\langle\mathcal{P}(x)|V_{\pi,\tau}V_{\pi,\tau}^\dagger|\mathcal{P}(x')\rangle\ |x'\rangle\langle x| = M^\odot. \end{aligned}$$

Recall that we can assume without loss of generality that the optimal algorithm is symmetrized. In that case, the states $|\psi_x^t\rangle$ of the algorithm satisfy $\langle\psi_{x^{\pi,\tau}}^t|\psi_{x'^{\pi,\tau}}^t\rangle = \langle\psi_x^t|\psi_{x'}^t\rangle$ for any $(\pi, \tau) \in G$ at any time t. Therefore, the Gram matrix

$$M^t = \sum_{x,x'}\langle\psi_x^t|\psi_{x'}^t\rangle|x'\rangle\langle x|$$

also satisfies the symmetry $U_{\pi,\tau}M^tU_{\pi,\tau}^\dagger = \bar{\Gamma}$ for any $(\pi, \tau) \in G$ at any time t.

We now show that using the adversary matrix $\bar{\Gamma}$ with initial state $|\bar{\alpha}\rangle$ yields adversary bounds that are at least as strong as those obtained from Γ with initial state $|\alpha\rangle$. Intuitively, this follows from the fact that this choice leads to the same progress function for symmetrized algorithms. Indeed, for $\bar\rho^t = M^t \circ |\bar\alpha\rangle\langle\bar\alpha|$, we have

$$\begin{aligned}
\operatorname{tr}\left[\bar\Gamma\bar\rho^t\right] &= \frac{1}{|G|}\sum_{(\pi,\tau)\in G} \operatorname{tr}\left[U_{\pi,\tau}(\Gamma\circ|\alpha\rangle\langle\alpha|\circ|\bar\alpha\rangle\langle\bar\alpha|)U^\dagger_{\pi,\tau}(M^t\circ|\bar\alpha\rangle\langle\bar\alpha|)\right]\\
&= \frac{1}{|G|}\sum_{(\pi,\tau)\in G} \operatorname{tr}\left[(\Gamma\circ|\alpha\rangle\langle\alpha|\circ|\bar\alpha\rangle\langle\bar\alpha|)U^\dagger_{\pi,\tau}(M^t\circ|\bar\alpha\rangle\langle\bar\alpha|)U_{\pi,\tau}\right]\\
&= \operatorname{tr}\left[(\Gamma\circ|\alpha\rangle\langle\alpha|\circ|\bar\alpha\rangle\langle\bar\alpha|)(M^t\circ|\bar\alpha\rangle\langle\bar\alpha|)\right] = \operatorname{tr}\left[\Gamma(M^t\circ|\alpha\rangle\langle\alpha|)\right] = \operatorname{tr}\left[\Gamma\rho^t\right] \qquad (6.1)
\end{aligned}$$

where we used the fact that $|\bar\alpha\rangle\langle\bar\alpha|\circ|\bar\alpha\rangle\langle\bar\alpha| = \mathbb{J}$, the all-one matrix.

Let us now show more explicitly that this implies that the additive bound obtained from $\bar\Gamma$ is at least as strong as that obtained from Γ (the cases of the intermediate and multiplicative bounds are treated similarly). First, since $\bar\rho^0 = |\alpha\rangle\langle\bar\alpha|$ and $\rho^0 = |\alpha\rangle\langle\alpha|$, we immediately obtain from Equation (6.1) that $\operatorname{tr}\left[\bar\Gamma|\bar\alpha\rangle\langle\bar\alpha|\right] = \operatorname{tr}\left[\Gamma|\alpha\rangle\langle\alpha|\right] = 1$. Moreover, $\|\Gamma\| \leq 1$ is equivalent to $-\mathbb{I} \preceq \Gamma \preceq \mathbb{I}$ and therefore implies

$$\begin{aligned}
\Gamma \preceq \mathbb{I} &\Longrightarrow \Gamma\circ|\alpha\rangle\langle\alpha|\circ|\bar\alpha\rangle\langle\bar\alpha| \preceq \mathbb{I}\circ|\alpha\rangle\langle\alpha|\circ|\bar\alpha\rangle\langle\bar\alpha|\\
&\Longrightarrow \frac{1}{|G|}\sum_{(\pi,\tau)\in G} U_{\pi,\tau}(\Gamma\circ|\alpha\rangle\langle\alpha|\circ|\bar\alpha\rangle\langle\bar\alpha|)U^\dagger_{\pi,\tau} \preceq \frac{1}{|G|}\sum_{(\pi,\tau)\in G} U_{\pi,\tau}(\mathbb{I}\circ|\alpha\rangle\langle\alpha|\circ|\bar\alpha\rangle\langle\bar\alpha|)U^\dagger_{\pi,\tau}\\
&\Longrightarrow \bar\Gamma \preceq \mathbb{I}. \qquad (6.2)
\end{aligned}$$

Similarly, $\Gamma \succeq -\mathbb{I}$ implies $\bar\Gamma \succeq -\mathbb{I}$, and therefore $\left\|\bar\Gamma\right\| \leq 1$. Together with the fact that $\operatorname{tr}\left[\bar\Gamma|\bar\alpha\rangle\langle\bar\alpha|\right] = 1$, this implies that $\left\|\bar\Gamma\right\| = 1$ and $\bar\Gamma|\bar\alpha\rangle = |\bar\alpha\rangle$.

Second, we need to show that if Γ satisfies $\operatorname{tr}\left[\Gamma(\rho^\odot\circ M)\right] = 0$ for any junk matrix M, the same applies for $\bar\Gamma$ and $\bar\rho^\odot = M^\odot\circ|\bar\alpha\rangle\langle\bar\alpha|$. Following the same argument as for Equation (6.1), we have

$$\begin{aligned}
\operatorname{tr}\left[\bar\Gamma(\bar\rho^\odot\circ M)\right] &= \operatorname{tr}\left[(\Gamma\circ|\alpha\rangle\langle\alpha|\circ|\bar\alpha\rangle\langle\bar\alpha|)(M^\odot\circ|\bar\alpha\rangle\langle\bar\alpha|\circ\bar M)\right]\\
&= \operatorname{tr}\left[\Gamma(M^\odot\circ|\alpha\rangle\langle\alpha|\circ\bar M)\right] = \operatorname{tr}\left[\Gamma(\rho^\odot\circ\bar M)\right] = 0,
\end{aligned}$$

where $\bar M = \frac{1}{|G|}\sum_{(\pi,\tau)\in G} U_{\pi,\tau} M U^\dagger_{\pi,\tau}$ is the symmetrized version of M, which is also a junk matrix.

Third, we need to show that $\max_i \|\Gamma - \Gamma_i\| \leq c$ implies the same condition for $\bar\Gamma$ and $\bar\Gamma_i = \bar\Gamma\circ D_i$. Recall from Fact 5.5 that $\Gamma_i = \sum_y \Pi^i_y\Gamma\Pi^i_y$, and similarly for $\bar\Gamma_i$. By definition of Π^i_y, we have $U_{\pi,\tau}\Pi^i_y U^\dagger_{\pi,\tau} = \Pi^{\pi^{-1}(i)}_{\tau(y)}$ and in turn

$$\begin{aligned}
\bar\Gamma_i &= \frac{1}{|G|}\sum_y\sum_{(\pi,\tau)\in G} \Pi^i_y U_{\pi,\tau}(\Gamma\circ|\alpha\rangle\langle\alpha|\circ|\bar\alpha\rangle\langle\bar\alpha|)U^\dagger_{\pi,\tau}\Pi^i_y\\
&= \frac{1}{|G|}\sum_y\sum_{(\pi,\tau)\in G} U_{\pi,\tau}\Pi^{\pi(i)}_{\tau^{-1}(y)}(\Gamma\circ|\alpha\rangle\langle\alpha|\circ|\bar\alpha\rangle\langle\bar\alpha|)\Pi^{\pi(i)}_{\tau^{-1}(y)}U^\dagger_{\pi,\tau}\\
&= \frac{1}{|G|}\sum_{(\pi,\tau)\in G} U_{\pi,\tau}(\Gamma_{\pi(i)}\circ|\alpha\rangle\langle\alpha|\circ|\bar\alpha\rangle\langle\bar\alpha|)U^\dagger_{\pi,\tau}
\end{aligned}$$

Since $\max_i \|\Gamma - \Gamma_i\| \leq c$ can be rewritten as $-c\,\mathbb{I} \preceq \Gamma - \Gamma_i \preceq c\,\mathbb{I}$, we have, following the same argument as for Equation (6.2),

$$\begin{aligned}
\Gamma - \Gamma_{\pi(i)} \preceq c\,\mathbb{I} &\Leftrightarrow (\Gamma - \Gamma_{\pi(i)})\circ|\alpha\rangle\langle\alpha|\circ|\bar\alpha\rangle\langle\bar\alpha| \preceq c\,\mathbb{I}\circ|\alpha\rangle\langle\alpha|\circ|\bar\alpha\rangle\langle\bar\alpha|\\
&\Rightarrow \bar\Gamma - \bar\Gamma_i \preceq c\,\mathbb{I}.
\end{aligned}$$

Similarly, we also have $\bar{\Gamma} - \bar{\Gamma}_i \succeq -c\,\mathbb{I}$ and therefore $\|\bar{\Gamma} - \bar{\Gamma}_i\| \leq c$ for every i in Σ_I. □

Note that the mapping $\mathcal{U} : (\pi,\tau) \mapsto U_{\pi,\tau}$ defines a representation of the automorphism group G and that Lemma 6.3 implies that Γ commutes with $U_{\pi,\tau}$ for any $(\pi,\tau) \in G$. This means that the matrices $U_{\pi,\tau}$ and Γ block-diagonalize simultaneously in a common basis, where each block corresponds to a different irrep of G in $\mathcal{U}$. From now on, we will consider the special case where $\mathcal{U}$ is multiplicity-free. This happens for different interesting problems, such as t-fold search [AŠdW07, Špa08] and Index Erasure (see Section 6.4), as a consequence of the following lemma.

Lemma 6.4 *If, for any $x, x' \in F$, there exists $(\pi,\tau) \in G$ such that $x' = x^{\pi,\tau}$ and $x'^{\pi,\tau} = x$, then $\mathcal{U}$ is multiplicity-free.*

Proof. Let us consider the set of matrices $\mathcal{M} = \{A \in \mathbb{C}^{|F|\times|F|} : \forall(\pi,\tau) \in G,\ U_{\pi,\tau} A U_{\pi,\tau}^\dagger = A\}$. It is easy to see that for any $A, B \in \mathcal{M}$, we have $AB \in \mathcal{M}$, therefore $\mathcal{M}$ defines an algebra. Note that $\mathcal{U}$ is multiplicity-free if and only if $\mathcal{M}$ is commutative, in which case all matrices in $\mathcal{M}$ diagonalize in a common basis [Cam99, page 65]. For any matrix $A \in \mathcal{M}$, we have $A^t = A$ since there exists $(\pi,\tau) \in G$ such that $\langle f|A|g\rangle = \langle f|U_{\pi,\tau} A U_{\pi,\tau}^\dagger|g\rangle = \langle g|A|x\rangle$. This immediately implies that for any $A, B \in \mathcal{M}$, we have $AB = (AB)^t = B^t A^t = BA$, therefore $\mathcal{M}$ is a commutative algebra. (More precisely, $\mathcal{M}$ is a Bose-Mesner algebra associated to an association scheme [Bai04]) □

6.2.2 Symmetry of oracle calls

Recall that oracle calls are closely related to the Hadamard product with D_i. We show that the invariance of Γ under the action of a group G implies the invariance of $\Gamma_i = \Gamma \circ D_i$ under the action of the subgroup G_i of G that leaves i invariant.

Lemma 6.5 *For any $i \in \Sigma_I$ and $y \in \Sigma_O$, let us define the following subgroups of G*

$$\begin{aligned} G_{iy} &= \{(\pi,\tau) \in G : \pi(i) = i, \tau(y) = y\}, \\ G_i &= \{(\pi,\tau) \in G : \pi(i) = i\}. \end{aligned}$$

Then Π_y^i satisfies $U_{\pi,\tau}\Pi_y^i U_{\pi,\tau}^\dagger = \Pi_y^i$ for any $(\pi,\tau) \in G_{iy}$, and Γ_i satisfies $U_{\pi,\tau}\Gamma_i U_{\pi,\tau}^\dagger = \Gamma_i$ for any $(\pi,\tau) \in G_i$.

Proof. Recall that by definition of Π_y^i, we have $U_{\pi,\tau}\Pi_y^i U_{\pi,\tau}^\dagger = \Pi_{\tau(y)}^{\pi^{-1}(i)}$ for any $(\pi,\tau) \in G$. This immediately implies the first part of the lemma for $(\pi,\tau) \in G_{iy}$. Moreover, Fact 5.5 and Lemma 6.3 imply that $U_{\pi,\tau}\Gamma_i U_{\pi,\tau}^\dagger = \Gamma_{\pi^{-1}(i)}$ for any $(\pi,\tau) \in G$. This implies the second part of the lemma for $(\pi,\tau) \in G_i$. □

Since $\mathcal{U}$ is a representation of G, it is also a representation of the subgroup G_i. However, even if $\mathcal{U}$ is multiplicity-free with respect to G, it is typically not with respect to G_i. Indeed, when restricting G to G_i, multiplicities can happen due to two different mechanisms. First, an irrep can become reducible, and one of the new smaller irreps can be a copy of another irrep. Secondly, two irreps that are different for G could be the same when we restrict to the elements of G_i. Let us identify an irrep of G_i by three indices (k,l,m): the first index identifies the irrep k of G from which it originates, the second index identifies the irrep l of G_i, and the last index allows to discriminate betwen different copies of the same irrep of G_i. For example, two irreps having the same index l but different indices k are two copies of the same irrep of G_i originating from different irreps of G. Also, we denote by $V_{k,l,m}$ the subspace spanned by irrep (k,l,m). These subspaces are such that $\bigoplus_{l,m} V_{k,l,m} = V_k$, where V_k is the subspace spanned by the irrep k of G (we assume that $V_{k,l,m}$ is empty if (k,l,m) does not correspond to a valid irrep). In the following, it will also be useful to define $W_l = \bigoplus_{k,m} V_{k,l,m}$ which is sometimes called the isotypical component corresponding to l [Ser77].

Lemma 6.6 *Let $\mathcal{U}$ be multiplicity-free for G. Then, Γ can be written as $\Gamma = \sum_k \gamma_k \Pi_k$, where k indexes the irreps of G and Π_k is the projector onto the space V_k spanned by the irrep k. Also, Γ_i block-diagonalizes as $\Gamma_i = \sum_l \Gamma_i^l$, where l indexes the irreps of G_i, and, for each l, Γ_i^l is a matrix on the isotypical component $W_l = \bigoplus_{k,m} V_{k,l,m}$ of l. Moreover, Γ_i^l can be written as*

$$\Gamma_i^l = \sum_{k_1,m_1,k_2,m_2} \gamma^l_{x;k_1m_1;k_2m_2} \Pi^l_{k_1m_1\leftarrow k_2m_2},$$

where d_l is the dimension of irrep l, $\Pi^l_{k_1m_1\leftarrow k_2m_2}$ is the "transporter" *from V_{k_2,l,m_2} to V_{k_1,l,m_1}, i.e., the operator that maps any state in V_{k_2,l,m_2} to the corresponding state in V_{k_1,l,m_1}, and*

$$\gamma^l_{x;k_1m_1;k_2m_2} = \frac{1}{d_l}\mathrm{tr}\left[\Gamma_i \Pi^l_{k_2m_2\leftarrow k_1m_1}\right].$$

Proof. This directly follows from Lemmas 6.3 and 6.5 using the canonical decomposition of the representation $\mathcal{U}$ [Ser77]. □

6.2.3 Computing the adversary bounds

Lemma 6.6 tells us how to choose the adversary matrix: it suffices to assign weights γ_k to each irrep k of G, i.e., $\Gamma = \sum_k \gamma_k \Pi_k$. Moreover, it also implies that computing the associated adversary bounds boils down to bounding for each irrep l of G_i the norm of a small $m_l \times m_l$ matrix, where m_l is the multiplicity of irrep l.

Theorem 6.7 *Let $\mathcal{U}$ be multiplicity-free for G. Then, we have*

$$\left\|\widetilde{\Gamma}_i - \widetilde{\Gamma}\right\| = \max_l \left\|\tilde{\Delta}_i^l\right\|, \qquad \left\|\Gamma_i^{\frac{1}{2}}\Gamma^{-\frac{1}{2}}\right\|^2 = \max_l \left\|\Delta_i^l\right\|, \qquad \left\|\Gamma^{\frac{1}{2}}\Gamma_i^{-\frac{1}{2}}\right\|^2 = \max_l \left\|(\Delta_i^l)^{-1}\right\|,$$

where the maximums are over irreps l of G_i. For each irrep l, $\tilde{\Delta}_i^l$ and Δ_i^l are $m_l \times m_l$ matrices, where m_l is the multiplicity of l for G_i, with elements labeled by the different copies of the irrep and such that

$$(\tilde{\Delta}_i^l)_{k_1m_1,k_2m_2} = \frac{1}{d_l}\sum_{k,y} \gamma_k \mathrm{tr}\left[\Pi_y^i \Pi_k \Pi_y^i \Pi^l_{k_2m_2\leftarrow k_1m_1}\right] - \gamma_{k_1}\delta_{k_1,m_1;k_2,m_2}$$

$$(\Delta_i^l)_{k_1m_1,k_2m_2} = \frac{1}{d_l}\sum_{k,y} \frac{\gamma_k}{\sqrt{\gamma_{k_1}\gamma_{k_2}}}\mathrm{tr}\left[\Pi_y^i \Pi_k \Pi_y^i \Pi^l_{k_2m_2\leftarrow k_1m_1}\right].$$

Proof. Γ and Γ_i block-diagonalize in the spaces spanned by the irreps (k,l,m) of G_i, this implies that $\|\Gamma_i - \Gamma\| = \max_l \left\|\Gamma_i^l - \Gamma^l\right\|$ where

$$\Gamma^l = \bigoplus_{\substack{k,m:\\(k,l,m)\in\mathcal{U}}} \gamma_k \mathbb{I}_{d_l} = \mathbb{I}_{d_l} \otimes \left(\bigoplus_{\substack{k,m:\\(k,l,m)\in\mathcal{U}}} \gamma_k |k,l,m\rangle\langle k,l,m|\right).$$

and Lemma 6.6 gives us:

$$\Gamma_i^l - \Gamma^l = \mathbb{I}_{d_l} \otimes \left[\sum_{\substack{k_1,m_1\\k_2,m_2}} \underbrace{\left(\frac{1}{d_l} \mathrm{tr}\left[\Gamma_i \Pi^l_{k_2 m_2 \leftarrow k_1 m_1}\right] - \gamma_{k_1} \delta_{k_1,m_1;k_2,m_2} \right)}_{(\tilde{\Delta}_i^l)_{k_1 m_1, k_2 m_2}} |k_1, l, m_1\rangle\langle k_2, l, m_2| \right].$$

The multiplicative case is handled similarly after noting that $\left\| \Gamma_i^{\frac{1}{2}} \Gamma^{-\frac{1}{2}} \right\|^2 = \left\| \Gamma^{-\frac{1}{2}} \Gamma_i \Gamma^{-\frac{1}{2}} \right\|$ which leads to

$$(\Gamma^l)^{-\frac{1}{2}} \Gamma_i^l (\Gamma^l)^{-\frac{1}{2}} = \mathbb{I}_{d_l} \otimes \left[\sum_{\substack{k_1,m_1\\k_2,m_2}} \underbrace{\frac{\frac{1}{d_l} \mathrm{tr}\left[\Gamma_i \Pi^l_{k_2 m_2 \leftarrow k_1 m_1}\right]}{\sqrt{\gamma_{k_1} \gamma_{k_2}}}}_{(\Delta_i^l)_{k_1 m_1, k_2 m_2}} |k_1, l, m_1\rangle\langle k_2, l, m_2| \right].$$

□

We see that to obtain the adversary bounds, we need to compute the traces of products of four operators. Since G_{iy} is a subgroup of both G and G_i, each of these operators can be decomposed into a sum of projectors onto irreps of G_{iy} (or transporters from and to these irreps). To compute these traces, we can use the following lemma, which shows that it is sufficient to compute the traces of products of two projectors onto irreps of G_{iy}.

Lemma 6.8 *Let $\lambda, \mu, \nu_1, \nu_2$ denote irreps of G_{iy}. If any of μ, ν_1 or ν_2 is not isomorphic to λ, then* $\mathrm{tr}\left[\Pi_\lambda \Pi_\mu \Pi_\lambda \Pi_{\nu_1 \leftarrow \nu_2}\right] = 0$. *Otherwise, we have*

$$\mathrm{tr}\left[\Pi_\lambda \Pi_\mu \Pi_\lambda \Pi_{\nu_1 \leftarrow \nu_2}\right] = \frac{1}{d} \mathrm{tr}\left[\Pi_\lambda \Pi_\mu\right] \cdot \mathrm{tr}\left[\Pi_\lambda \Pi_{\nu_1 \leftarrow \nu_2}\right],$$
$$\left|\mathrm{tr}\left[\Pi_\lambda \Pi_{\nu_1 \leftarrow \nu_2}\right]\right| = \sqrt{\mathrm{tr}\left[\Pi_\lambda \Pi_{\nu_1}\right] \cdot \mathrm{tr}\left[\Pi_\lambda \Pi_{\nu_2}\right]},$$

where d is the dimension of the representation λ.

Proof. If two irreps are not isomorphic to each other, they belong to different isotypical subspaces of $\mathcal{U}$, and therefore the product of their projectors (or transporters) is zero. Let us now assume that all the irreps are isomorphic to λ, and therefore belong to the same isotypical subspace. Then, we can define isomorphic bases $\{|j\rangle\}_{j\in[d]}, \{|\psi_j\rangle\}_{j\in[d]}$, $\{|\phi_j^{(1)}\rangle\}_{j\in[d]}$ and $\{|\phi_j^{(2)}\rangle\}_{j\in[d]}$ for the subspaces spanned by irreps λ, μ, ν_1 and ν_2, respectively, such that

$$\Pi_\lambda = \sum_{j=1}^d |j\rangle\langle j|, \qquad \Pi_\mu = \sum_{j=1}^d |\psi_j\rangle\langle\psi_j|, \qquad \Pi_{\nu_1 \leftarrow \nu_2} = \sum_{j=1}^d |\phi_j^{(1)}\rangle\langle\phi_j^{(2)}|.$$

Let us also choose a basis $\{|j, j'\rangle\}_{(j,j')\in[d]\times[m]}$ for the whole $(d \times m)$-dimensional isotypical subspace, m being the multiplicity of the irreps. Without loss of generality, we may choose this basis such that $\{|j, 1\rangle\}_{j\in[d]} = \{|j\rangle\}_{j\in[d]}$ corresponds to λ itself, and, for any $j' \neq 1$,

$\{|j,j'\rangle\}_{j\in[d]}$ corresponds to a copy of λ. Since λ, μ, ν_1 and ν_2 are isomorphic, there exist coefficients $\{\alpha_{j'}\}_{j'\in[m]}$, $\{\beta^{(1)}_{j'}\}_{j'\in[m]}$ and $\{\beta^{(2)}_{j'}\}_{j'\in[m]}$ such that

$$|\psi_j\rangle = \sum_{j'=1}^{m} \alpha_{j'} |j,j'\rangle, \qquad |\phi_j^{(1)}\rangle = \sum_{j'=1}^{m} \beta^{(1)}_{j'} |j,j'\rangle, \qquad |\phi_j^{(2)}\rangle = \sum_{j'=1}^{m} \beta^{(2)}_{j'} |j,j'\rangle.$$

We now have

$$\begin{aligned}
\mathrm{tr}\left[\Pi_\lambda \Pi_\mu \Pi_\lambda \Pi_{\nu_1\leftarrow\nu_2}\right] &= \sum_{j=1}^{d} \langle j|\psi_j\rangle\langle\psi_j|j\rangle\langle j|\phi_j^{(1)}\rangle\langle\phi_j^{(2)}|j\rangle \\
&= d \cdot \langle 1|\psi_1\rangle\langle\psi_1|1\rangle\langle 1|\phi_1^{(1)}\rangle\langle\phi_1^{(2)}|1\rangle \\
&= \frac{1}{d}\sum_{i=1}^{d} \langle j|\psi_j\rangle\langle\psi_j|j\rangle \cdot \sum_{j=1}^{d}\langle j|\phi_j^{(1)}\rangle\langle\phi_j^{(2)}|j\rangle \\
&= \frac{1}{d}\mathrm{tr}\left[\Pi_\lambda\Pi_\mu\right] \cdot \mathrm{tr}\left[\Pi_\lambda \Pi_{\nu_1\leftarrow\nu_2}\right].
\end{aligned}$$

Similarly, we also have

$$\begin{aligned}
\mathrm{tr}\left[\Pi_\mu \Pi_{\nu_1\leftarrow\nu_2}\right] \cdot \mathrm{tr}\left[\Pi_\mu \Pi_{\nu_2\leftarrow\nu_1}\right] &= \sum_{j=1}^{d} \langle j|\phi_j^{(1)}\rangle\langle\phi_j^{(2)}|j\rangle \cdot \sum_{j=1}^{d} \langle j|\phi_j^{(2)}\rangle\langle\phi_j^{(1)}|j\rangle \\
&= d^2 \cdot \langle 1|\phi_1^{(1)}\rangle\langle\phi_1^{(2)}|1\rangle\langle 1|\phi_1^{(2)}\rangle\langle\phi_1^{(1)}|1\rangle \\
&= \sum_{j=1}^{d} \langle j|\phi_j^{(1)}\rangle\langle\phi_j^{(1)}|j\rangle \cdot \sum_{j=1}^{d} \langle j|\phi_j^{(2)}\rangle\langle\phi_j^{(2)}|j\rangle \\
&= \mathrm{tr}\left[\Pi_\mu\Pi_{\nu_1}\right] \cdot \mathrm{tr}\left[\Pi_\mu\Pi_{\nu_2}\right].
\end{aligned}$$

□

6.3 Lower bound for Search

In this Section, we consider Grover's Search problem [Gro96], which we denote $\textsc{Search}_n$: Given a string $x \in \{0,1\}^n$ with the promise that there exists a unique i such that $x_i = 1$, find this index. We can show that the inequalities in Theorem 5.19 are strict.

Theorem 6.9 *For any $0 < \varepsilon < 1 - \frac{1}{n}$, we have*

$$\begin{aligned}
\mathrm{ADV}^{\pm}_{\varepsilon}(\textsc{Search}_n) &= \Omega\left((1-\varepsilon-2\sqrt{\varepsilon(1-\varepsilon)})\sqrt{n}\right) \\
\widetilde{\mathrm{ADV}}_{\varepsilon}(\textsc{Search}_n) &= \Omega\left((\sqrt{1-\varepsilon}-1/\sqrt{n})^2\sqrt{n}\right) \\
\mathrm{MADV}_{\varepsilon}(\textsc{Search}_n) &= \Omega\left((\sqrt{1-\varepsilon}-1/\sqrt{n})\sqrt{n}\right).
\end{aligned}$$

In particular, for $\varepsilon > 1/5$, we have $\mathrm{MADV}_{\varepsilon}(\textsc{Search}_n) > \widetilde{\mathrm{ADV}}_{\varepsilon}(\textsc{Search}_n) > \mathrm{ADV}^{\pm}_{\varepsilon}(\textsc{Search}_n)$.

In order to illustrate our method, we will use representation theory to compute the adversary bounds, even though this is not really necessary for such a simple problem. The $\Omega(\sqrt{n})$

lower bound for large success probability is well-known (see e.g [BBBV97]), and the case of small success probability has been studied in [Amb05, Špa08] using the multiplicative adversary method. The fact that a non-trivial bound can also be found in this regime using an additive adversary method (our intermediate method) is new to the present work.

Proof. Let us denote by $x^{(j)}$ the oracle that marks element j, that is, $x_i^{(j)} = 1$ if $i = j$ and 0 otherwise. Let us consider the symmetric group S_n acting on x as $x_i^\pi = x_{(\pi(i))}$. This group forms an automorphism for $\textsc{Search}_n$, and the associated representation $\mathcal{U}$ corresponds to the natural representation acting on $[n]$. This representation decomposes into two irreps, the one-dimensional trivial representation on $V_0 = \text{Span}\{|\alpha\rangle\}$, where $|\alpha\rangle = (1/\sqrt{n})\sum_j |x^{(j)}\rangle$, and an $(n-1)$-dimensional irrep on $V_1 = V_0^\perp$. Following Lemma 6.3, we set $\Gamma = \Pi_0 + \gamma\Pi_1$.

Let us now fix some input $i \in [n]$ to the oracle (by symmetry, the calculation will be the same for any i). When restricting G to $G_i = \{\pi \in G : \pi(i) = i\}$, the second representation splits into two irreps, the first one being a second copy of the trivial representation, now acting on $V_{1,0} = \text{Span}\{|\alpha_i\rangle\}$, where $|\alpha_i\rangle = (|\alpha\rangle - \sqrt{n}|x^{(i)}\rangle)/\sqrt{n-1}$. Following our convention, we index the three irreps of G_i with labels (k,l) as $(0,0)$, $(1,0)$ and $(1,1)$ (no need for a third index as each irrep of G_i appears only once in a given irrep of G). Since we have one irrep with multiplicity two, and one irrep with multiplicity one, the matrix Γ_i will block-diagonalize into two blocks: one 2×2 block Γ_i^0 on $V_0 \oplus V_{1,0}$, and one $(n-2)\times(n-2)$ block Γ_i^1 on $V_{1,1}$.

Only the block corresponding to the trivial representation $l = 0$ is relevant. Indeed, since the other representation has multiplicity 1, the corresponding block is characterized by a single scalar, and it is straightforward to check that $\tilde{\Delta}_i^1 = 0$ and $\Delta_i^1 = 1$, so that the maximum in Theorem 6.7 will not be achieved by this block.

Let us now consider the other representation, corresponding to a 2×2 block. In order to compute matrices $\tilde{\Delta}_i^0$, and Δ_i^0, we first compute $\Pi_0 \circ D_i$ and $\Pi_1 \circ D_i$ using Fact 5.5. In the basis $\{|\alpha\rangle, |\alpha_i\rangle\}$, we obtain

$$\Pi_0 \circ D_i = \begin{pmatrix} 1-2\beta^2(1-\beta^2) & \beta\sqrt{1-\beta^2}(1-2\beta^2) \\ \beta\sqrt{1-\beta^2}(1-2\beta^2) & 2\beta^2(1-\beta^2) \end{pmatrix},$$

where $\beta = 1/\sqrt{n}$, and therefore $\Pi_1 \circ D_i = \mathbb{I} - \Pi_0 \circ D_i$. For the additive adversary methods, we then obtain from Theorem 6.7

$$\tilde{\Delta}_i^0 = (1-\gamma)\beta\sqrt{1-\beta}\begin{pmatrix} -2\beta\sqrt{1-\beta^2} & 1-2\beta^2 \\ 1-2\beta^2 & 2\beta\sqrt{1-\beta^2} \end{pmatrix}.$$

The matrix has eigenvalues ±1, so that $\left\|\tilde{\Delta}_i^0\right\| = (1-\gamma)\beta\sqrt{1-\beta}$.

For the usual additive adversary method, we need to choose γ such that $\text{tr}(\widetilde{\Gamma}(\rho^\odot \circ M)) = 0$ for any junk matrix M. Here, $\rho^\odot = \mathbb{I}/n$, therefore this condition reduces to $\text{tr}(\widetilde{\Gamma}) = 0$, which is satisfied for $\gamma = -1/(n-1)$. This yields $\left\|\tilde{\Delta}_i^0\right\| = 1/\sqrt{n-1}$, and therefore $\text{ADV}_\varepsilon^\pm(\textsc{Search}_n) = (1-\varepsilon-2\sqrt{\varepsilon(1-\varepsilon)})\sqrt{n-1}$, which is $\Omega(\sqrt{n})$ for $\varepsilon < 1/5$, but negative otherwise.

For the intermediate adversary method, we can choose $\tilde{\lambda} = \gamma$, so that $V_{\text{bad}} = V_0$ and $\eta = 1/n$. This implies that as soon as $\varepsilon < 1-1/n$, we have a non-trivial bound $\widehat{\text{ADV}}_\varepsilon(\textsc{Search}_n) = (\sqrt{1-\varepsilon} - 1/\sqrt{n})^2\sqrt{n-1}$.

For the multiplicative adversary method, we choose $\gamma > 1$ and $\lambda = \gamma$, so that $V_{\text{bad}} = V_0$ and $\eta = 1/n$. We then obtain similarly

$$\begin{aligned}\Delta_i^0 &= \begin{pmatrix} 1 + 2(\gamma-1)\beta^2(1-\beta^2) & -\frac{\gamma-1}{\sqrt{\gamma}}\beta\sqrt{1-\beta^2}(1-2\beta^2) \\ -\frac{\gamma-1}{\sqrt{\gamma}}\beta\sqrt{1-\beta^2}(1-2\beta^2) & 1-2\frac{\gamma-1}{\gamma}\beta^2(1-\beta^2)\end{pmatrix} \\ &= \begin{pmatrix} 1 & -\frac{\gamma-1}{\sqrt{\gamma}}\beta \\ -\frac{\gamma-1}{\sqrt{\gamma}}\beta & 1\end{pmatrix} + \mathrm{O}\big(\beta^2\big)\,.\end{aligned}$$

For a 2×2 matrix $\left(\begin{smallmatrix} a & b \\ c & d\end{smallmatrix}\right)$, Gershgorin circle theorem states the eigenvalues lie in $[b - |a|, b + |a|] \cup [d - |c|, d + |c|]$. In our case, the eigenvalues of $\begin{pmatrix} 1 & -\frac{\gamma-1}{\sqrt{\gamma}}\beta \\ -\frac{\gamma-1}{\sqrt{\gamma}}\beta & 1\end{pmatrix}$ lie in the range $[1 - \frac{\gamma-1}{\sqrt{\gamma n}}, 1 + \frac{\gamma-1}{\sqrt{\gamma n}}]$, so that

$$\mathrm{MADV}(\textsc{Search}_n) \geq \frac{\log[1+(\gamma-1)\zeta^2]}{\log[1+(\gamma-1)/\sqrt{\gamma n}]},$$

where $\zeta = \sqrt{1-\varepsilon} - 1/\sqrt{n}$. In the limit $\gamma \to 1^+$, we obtain the same bound as for the intermediate adversary method. However, for $\gamma = 1 + 1/\zeta^2$, we obtain

$$\mathrm{MADV}(\textsc{Search}_n) \geq (\log 2) \cdot \frac{\sqrt{\gamma n}}{\gamma - 1} = \Omega\left((\sqrt{1-\varepsilon} - 1/\sqrt{n})\sqrt{n}\right),$$

where we have used the fact that $\log(1+x) \leq x$. □

6.4 Lower bounds for Index Erasure

We recall the definition of Index Erasure:

Definition 6.10 (Index Erasure) *Let x be a string of length N on an alphabet of size $M > N$ with distinct letters, that is $x_i \neq x_j$ if $i \neq j$. Index Erasure is the problem of **coherently** generating the quantum state*

$$|\psi_x\rangle = \frac{1}{\sqrt{N}} \sum_{i=1}^{N} |x_i\rangle.$$

The goal of this section is to prove the optimal quantum query complexity of this problem:

Theorem 6.11 *For any $\varepsilon < 1 - \frac{N}{M}$, we have $Q_\varepsilon(\textsc{Index Erasure}) = \Theta(\sqrt{N})$.*

The upper bound has been proved by Shi [Shi02], we focus our work on the lower bound. The proof is rather long and takes the whole Section 6.4.2. Note that in general, we can see the input x as function $i \mapsto x_i$, and in the case of Index Erasure as an injective function from $[N]$ to $[M]$. Since it is easier to speak about "injective functions from $[N]$ to $[M]$" than "strings of length N with distinct letters over an alphabet of size M", we will mostly use this terminology.

6.4.1 Notations

We will consider irreps of the symmetric group S_N, *i.e., Young diagrams* and denote them by $\lambda_N, \lambda_N^+, \ldots$. Note that since a diagram λ_N necessarily contains N boxes, it is fully determined by its part λ below the first row, as we know that its first row must contain $N - |\lambda|$ boxes, where $|\lambda|$ is the number of boxes below the first row. This will lighten the notations. The dimension of the space spanned by an irrep of the symmetric group can be easily computed:

Lemma 6.12 (Hook-length formula [Sag01]) *For any Young diagram λ corresponding to an irrep of S_N, the dimension of the space spanned by this irrep is:*

$$d_\lambda^N = \frac{N!}{\prod_{(i,j)\in\lambda} h_N(i,j)},$$

where $h_N(i,j) = |\{(i,j') \in \lambda_N : j' > j\} \cup \{(i',j) \in \lambda_N : i' \geq i\}|$ is the hook-length.

More precisely, we will use the Hook-length formula to show that:

Lemma 6.13 *For $|\lambda| \leq \sqrt{N}$, we have:*

$$\frac{d_\lambda^N}{N d_\lambda^{N-1}} = \mathrm{O}\left(\frac{1}{N}\right).$$

Proof.

$$\frac{d_\lambda^N}{N d_\lambda^{N-1}} = \frac{N!}{N(N-1)!} \frac{H(\lambda)}{H(\lambda)} \prod_{i:(i,1)\in\lambda_{N-1}} \frac{h_N(i,1)-1}{h_N(i,1)},$$

where $H(\lambda)$ denotes the product of the Hook-length of the boxes below the first row. The other product is maximized when the Hook-lengths are small, i.e. when the Young diagrams have only two rows. It leads to:

$$\frac{d_\lambda^N}{N d_\lambda^{N-1}} \leq \prod_{i=2}^{N-2|\lambda|}\left(1-\frac{1}{i}\right) \prod_{i=N-2|\lambda|+2}^{N-|\lambda|+1}\left(1-\frac{1}{i}\right) = \frac{1}{N-2|\lambda|} \frac{N-2|\lambda|+1}{N-|\lambda|+1} = \mathrm{O}\left(\frac{1}{N}\right)$$

since $|\lambda| \leq \sqrt{N}$. □

6.4.2 Proof of the optimal lower bound for Index Erasure

Let $(\pi,\tau) \in S_N \times S_M$ act on the set F of injective functions from $[N]$ to $[M]$ (with $M \geq N^2$) by mapping x to $x^{\pi,\tau}$. Since we can obtain the state $|\psi_x\rangle$ from $|\psi_{x^{\pi,\tau}}\rangle$ by applying the permutation τ^{-1} on the target register, the whole group $G = S_N \times S_M$ defines an automorphism group for the problem.

Proof road map This proof is an illustration of the method we developed in Section 6.2, and thus relies heavily on the representation theory of the automorphism group $S_N \times S_M$.

First of all, we ensure that the irreps of the representation corresponding to the action G on the set of injective functions is multiplicity-free by using the necessary condition of Lemma 6.4. The irreps of the symmetric group S_N are represented by Young diagrams with N boxes (see e.g. [Sag01]), so the irreps of G are represented by pairs of Young diagrams with respectively

N and M boxes. We show that most of the irreps do not even occur in this representation. More precisely that only the irreps whose Young diagram for S_N is included into the one for S_M appear.

Secondly, we decompose ρ_0 and $\rho^{\odot}$ in the basis corresponding to those irreps. Since the Index Erasure problem is totally symmetric by permutation of the outputs, we choose $|\alpha\rangle$ as the uniform superposition over the set of injective functions, thus $\rho^0 = |\alpha\rangle\langle\alpha|$ as support only on the space V_0 corresponding to the trivial irrep which is represented by the pair of Young diagrams respectively with only one row of N boxes and M boxes. Meanwhile, we show that $\rho^{\odot}$ has overlap on two spaces: V_0 the one corresponding to the trivial irrep, and mostly on V_1, the space corresponding to the Young diagrams (λ_N, λ_M) where λ_N has only one row of N boxes, and λ_M has two rows with respectively $M-1$ and 1 boxes (See Figure 6.1).

Since we start from state ρ_0 and we want to reach the state $\rho^{\odot}$ which has a large weight over the space V_1, the strategy for the lower bound is to show that it is hard to transfer weight from V_0 to V_1. More precisely, we divide all irreps (and by consequence their corresponding subspaces) into two sets: one set of *bad* irreps containing all irreps represented by diagrams (λ_N, λ_M) where λ_N and λ_M only differ in their first row, and one set of *good* irreps containing all the other irreps (see Figure 6.2). According to Lemma 6.5, we pick the adversary matrix $\widetilde{\Gamma}$ diagonal in the basis of the irreps of the representation. We also choose the eigenvalues of $\widetilde{\Gamma}$ to be 0 on the good irrep so that the progress function for $\rho^{\odot}$ is small.

The last step uses Theorem 6.7. We show that three different cases arise for the matrices $\tilde{\Delta}^l_i$, and we handle them separately.

Multiplicities of representations Let us show that the representation $\mathcal{U}$ corresponding to the action of G on the set of injective functions F is multiplicity-free by using Lemma 6.4. We need to show that for any pair of functions $x, x' \in F$, there exists permutations $(\pi, \tau) \in S_M \times S_N$ such that $x^{\pi,\tau} = x'$ and $x'^{\pi,\tau} = x$. We first construct a permutation π acting on the input set. We denote by P_x (resp. $P_{x'}$) the preimage of the set $\mathrm{Im}(x) \cap \mathrm{Im}(x')$ by the function x (resp. by the function x'). We call *chain of length* $l+1$ a sequence of inputs $i_0 \to i_1 \to \cdots \to i_{l-1} \to i_l$ such that $x_{i_0} = x'_{i_1}, x_{i_1} = x'_{i_2}, \ldots, x_{i_{l-1}} = x'_{i_l}$. We only consider maximal chains, that is, chains that cannot be made longer by prepending or appending another chain. There are two types of maximal chains: the paths such that $i_0 \in P_x \backslash P_{x'}$, $i_1, \ldots, i_{l-1} \in P_x \cup P_{x'}$ and $i_l \in P_{x'} \backslash P_x$; and the cycles such that all the elements are in $P_x \cap P_{x'}$ and $i_0 = i_l$. The maximal chains are a partition of $P_x \cup P_{x'}$. We define the permutation π on each chain by $\pi(i_j) = i_{l-j}$, and for all $j \notin P_x \cup P_{x'}, \pi(j) = i$.

We define the permutation τ by:

$$\tau : \begin{cases} \forall i \in [N], & \tau(x_{\pi(j)}) = x'_i \\ \forall i \in [N], & \tau(x'_{\pi(j)}) = x_i \\ \forall y \notin \mathrm{Im}(x) \cup \mathrm{Im}(x'), & \tau(y) = y \end{cases}$$

The two first equations would imply that $x^{\pi,\tau} = x'$ and $x'^{\pi,\tau} = x$, but we need to check that they are consistent.

This is immediately the case for all $y \notin \mathrm{Im}(x) \cap \mathrm{Im}(x')$, therefore it remains to show that they are equivalent for $y \in \mathrm{Im}(x) \cap \mathrm{Im}(x')$. Let us consider such an output y, in which case there is a chain including inputs i_j and i_{j+1} such that $y = x_{i_j} = x'_{i_{j+1}}$. By definition of π, the same chain then also includes the inputs $\pi(i_{j+1})$ and $\pi(i_j)$, and we can define an output y' as $y' = x_{\pi(i_{j+1})} = x'_{\pi(i_j)}$. Therefore, the first equation in the definition of τ leads to

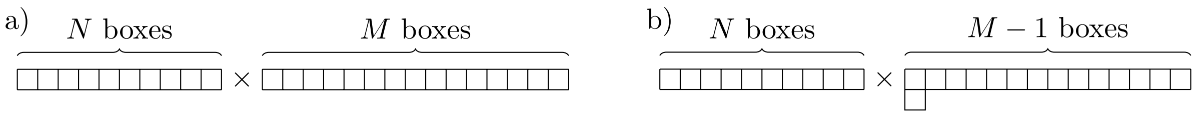


Figure 6.1: We use $N = 10$ and $M = 15$. a) Young diagrams corresponding to the one-dimensional space V_0. The initial state ρ^0 is the projector over V_0 ; b) Young diagrams corresponding to the $(M-1)$-dimensional space V_1. The target state $\rho^{\odot}$ has a large overlap $(1 - N/M)$ with the completely mixed state over V_1.

$\tau(y') = \tau(x_{\pi(i_{j+1})}) = x'_{i_{j+1}} = y$ while the second equations leads to $\tau(y') = \tau(x'_{\pi(i_j)}) = x_{i_j} = y$, i.e., both equations are consistent. By Lemma 6.4, this concludes the proof that the irreps in $\mathcal{U}$ have multiplicity 0 or 1.

Let us now show that many irreps do not appear at all. Recall that irreps of $G = S_N \times S_M$ can be represented by pairs of Young diagrams (λ_N, λ_M), where λ_N has N boxes, and λ_M has M boxes [Sag01]. We show that only irreps where the diagram λ_N is contained in the diagram λ_M can appear. We show this by induction on M, starting from $M = N$. For the base case, the set of injective functions F is isomorphic to the set of permutations in S_N, and $(\pi, \tau) \in S_N \times S_N$ acts on a permutation σ as $\tau\sigma\pi$. Therefore, the only irreps which occur in $\mathcal{U}$ are those where the two diagrams are the same, that is, $\lambda_N = \lambda_M$. When extending the range of functions in F from M to $M + 1$, we induce irreps of $S_N \times S_M$ to irreps of $S_N \times S_{M+1}$ by adding an extra box on the diagram corresponding to S_M. Since we start from a case where the two diagrams are the same, we can only obtain pairs of diagrams (λ_N, λ_M) where λ_N is contained inside λ_M.

Initial and target states The initial state is $\rho_0 = |x^{\pi,\tau}\rangle\langle x^{\pi,\tau}|$, where $|x^{\pi,\tau}\rangle = \frac{1}{\sqrt{|F|}} \sum_{x \in F} |x\rangle$ is the superposition over all injective functions, which is invariant under any element $(\pi, \tau) \in G$. Therefore, it corresponds to the trivial one-dimensional irrep of $S_N \times S_M$, represented by a pair of diagrams (λ_N, λ_M) where both diagrams contain only one row of N and M boxes, respectively (see Figure 6.1). Let $V_0 = \mathrm{Span}\{|x^{\pi,\tau}\rangle\}$ be the corresponding one-dimensional subspace. We now show that the target state $\rho^{\odot}$ is a mixed state over $V_0 \oplus V_1$, where $V_1 = \mathrm{Span}\{|\phi_y\rangle : y \in [M]\}$ is the $(M-1)$-dimensional subspace spanned by states $|\phi_y\rangle = \sqrt{1 - (N/M)}|\psi_y\rangle - \sqrt{N/M}|\bar{\psi}_y\rangle$, $|\psi_y\rangle$ being the uniform superposition over functions x such that $y \in \mathrm{Im}(x)$, and $|\bar{\psi}_y\rangle$ the uniform superposition over functions x such that $y \notin \mathrm{Im}(x)$. This subspace corresponds to the irrep represented by diagrams (λ_N, λ_M) where λ_N contains only one row of N boxes, and λ_M has $M - 1$ boxes on the first row and one box on the second (see Figure 6.1). We have for the target state

$$\begin{aligned}
\rho^{\odot} &= \frac{1}{F} \sum_{x,x' \in F} \langle \psi_x | \psi_{x'} \rangle |x'\rangle\langle x| = \frac{1}{F} \sum_{x,x' \in F} \frac{|\mathrm{Im}(x) \cap \mathrm{Im}(x')|}{N} |x'\rangle\langle x| \\
&= \frac{1}{M} \sum_{y=1}^{M} |\psi_y\rangle\langle\psi_y| = \frac{N}{M} |x^{\pi,\tau}\rangle\langle x^{\pi,\tau}| + \left(1 - \frac{N}{M}\right) \frac{1}{M} \sum_{y=1}^{M} |\phi_y\rangle\langle\phi_y| \\
&= \frac{N}{M}\rho_0 + \left(1 - \frac{N}{M}\right)\rho_1,
\end{aligned}$$

where ρ_0 and ρ_1 are the maximally mixed states over V_0 and V_1, respectively.

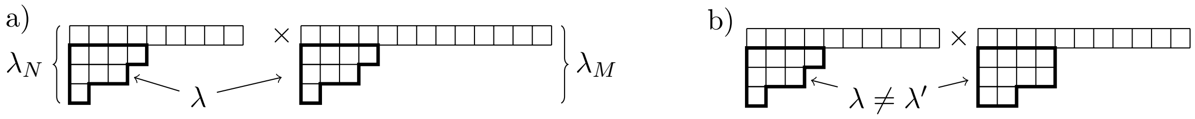


Figure 6.2: We use $N = 17$ and $M = 21$. a) Example of a "bad" irrep $\lambda_N \times \lambda_M$: the shape of the diagrams below the first row for S_N and S_M are the same λ ; b) Example of a "good" irrep: the shape of the diagram below the first line of S_N is strictly included into the one for S_M.

Adversary matrix Since we start from state ρ_0 and we want to reach state $\rho^{\odot}$ which has a large weight over ρ_1, the strategy for the lower bound is to show that it is hard to transfer weight from V_0 to V_1. More precisely, we divide all irreps (and by consequence their corresponding subspaces) into two sets: one set of *bad* irreps containing all irreps represented by diagrams (λ_N, λ_M) where λ_N and λ_M only differ in their first row, and one set of *good* irreps containing all the other irreps (see Figure 6.2). By this definition, the irrep corresponding to V_0 is bad, while the irrep corresponding to V_1 is good. The lower bound is based on the fact that it is hard to transfer weight onto good subspaces (in particular V_1) starting from V_0. As mentioned in Section 6.4.1, from now on, we note the irreps only by their part under the first row; (λ, λ') then denotes an irrep of $S_N \times S_M$. Therefore, bad irreps are precisely those such that $\lambda = \lambda'$. Recall from Lemma 6.5 that constructing an adversary matrix $\widetilde{\Gamma}$ amounts to assigning an eigenvalue to each irrep of G. We choose $\widetilde{\Gamma}$ such that it has eigenvalue 0 on good irreps, and eigenvalue $\gamma_{|\lambda|}$ on a bad irrep (λ, λ), which only depends on $|\lambda|$, i.e.,

$$\widetilde{\Gamma} = \sum_{\lambda} \gamma_{|\lambda|} \Pi_{(\lambda,\lambda)},$$

where $\Pi_{(\lambda,\lambda')}$ is the projector onto the subspace corresponding to the irrep (λ, λ'). We set

$$\gamma_{|\lambda|} = \begin{cases} 1 - \frac{|\lambda|}{\sqrt{N}} & \text{if } |\lambda| < \sqrt{N} \\ 0 & \text{otherwise.} \end{cases}$$

Therefore, we have $\gamma_0 = 1$ and $0 \leq \gamma_{|\lambda|} \leq 1$ for any λ, and $\widetilde{\Gamma}$ is a valid additive adversary matrix. Let V_{bad} denote the direct-sum of the bad subspaces. Since $\rho^{\odot}$ only has overlap N/M over V_{bad}, we have $\text{tr}(\Pi_{\text{bad}}\rho^{\odot}) \leq N/M$. Therefore, we can set the threshold eigenvalue $\tilde{\lambda} = 0$ and the base success probability $\eta = N/M$. This adversary matrix is thus a perfect candidate to prove a lower bound on the coherent version of INDEX ERASURE.

Discussion From Theorem 6.7, we see that we need to compute the norm of a matrix $\tilde{\Delta}_i^l$ for each irrep l of $G_i = S_{N-1} \times S_M$. We show that these matrices are non-zero only for three different types of irreps of G_i. Indeed, for irreps k of G and l of G_i, the quantity $\gamma_k \text{tr}\left[\Pi_y^i \Pi_k \Pi_y^i \Pi^l_{k_1 m_1 \leftarrow k_2 m_2}\right]$ is non-zero only if: ① k is a bad irrep (otherwise $\gamma_k = 0$); ② k and l restrict to a common irrep of $G_{iy} = S_{N-1} \times S_{M-1}$ (otherwise the product of the projectors is zero). The restrictions of an irrep (λ, λ') of G to G_{iy} are obtained by removing one box from each of the diagrams λ and λ'. Similarly, the restrictions of an irrep (λ, λ') of G_i to G_{iy} are obtained by removing one box from λ'. ③ Note that not all irreps of G_{iy} appear in the projector Π_y^i, as it projects on all injective functions such that $x_i = y$. Therefore, this set is isomorphic to the set of injective functions from $[N-1]$ to $[M-1]$, and we know that the irrep

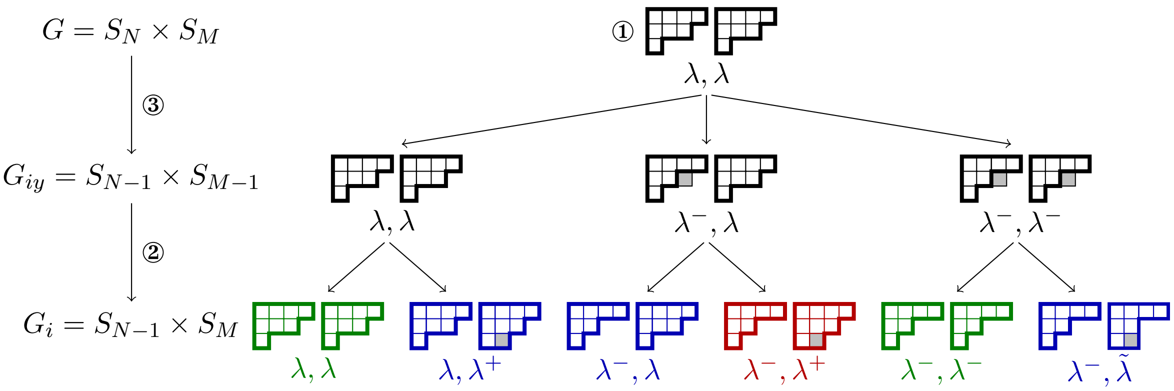


Figure 6.3: Following our convention, we draw only the part of the diagram below the first row. The condition ① imposes that the two diagrams for $S_N \times S_M$ (on top) have the same shape. When restricting from $S_N \times S_M$ to $S_{N-1} \times S_{M-1}$, one should remove one box from each diagram. When the removed box does not belong to the original irrep of $S_N \times S_M$, it is shown in light gray. The condition ③ imposes that the diagram for S_{N-1} (left) is included into the one for S_{M-1} (right). The condition ② gives the diagrams for $S_{N-1} \times S_M$ (at the bottom). Finally we have 3 "generic" types of irreps: case 1 (green) where the diagrams have the same shape; case 2 (blue) where the right diagram has one additional box; and case 3 (red) where the right diagram has 2 additional boxes.

$\mathcal{U}$ acting on this set is multiplicity-free, and that only irreps (λ, λ') where λ is contained in λ' can occur. Altogether, this implies that only three type of irreps of $G_i = S_{N-1} \times S_M$ lead to non-zero matrices (see Figure 6.3)

1. $l = (\lambda, \lambda)$: Same diagram for S_{N-1} and S_M below the first row. This irrep has multiplicity one since there is only one way to induce to a valid irrep of $S_N \times S_M$, by adding a box in the first row of the left diagram, leading to irrep $k = (\lambda, \lambda)$.

2. $l = (\lambda, \lambda^+)$: Diagram for S_M has one additional box below the first row. This irrep has multiplicity two since there are two ways to induce to a valid irrep of $S_N \times S_M$, by adding a box either in the first row, leading to $k = (\lambda, \lambda^+)$, or at the missing place below the first row, leading to $k = (\lambda^+, \lambda^+)$.

3. $l = (\lambda, \lambda^{++})$: Diagram for S_M has two additional boxes below the first row. This irrep has multiplicity three since there are three ways to induce to a valid irrep of $S_N \times S_M$, by adding a box either in the first row, leading to $k = (\lambda, \lambda^+)$, or at to one of the missing places below the first row, leading to $k = (\lambda^+, \lambda^{++})$.

Analysis of the three cases Let us now consider these three cases separately.

Case (λ, λ). Since this irrep has multiplicity one, we just need to compute a scalar. As an irrep of $S_{N-1} \times S_M$, (λ, λ) restricts to only one valid irrep of $S_{N-1} \times S_{M-1}$, by removing a box on the first row of the right diagram, therefore this irrep is also labeled (λ, λ). Inducing from this irrep of $S_{N-1} \times S_{M-1}$ to $S_N \times S_M$, we obtain three valid irreps, two "bad" ones, (λ, λ) and (λ^+, λ^+), and a good one, (λ, λ^+). To differentiate between projectors of irreps of the different

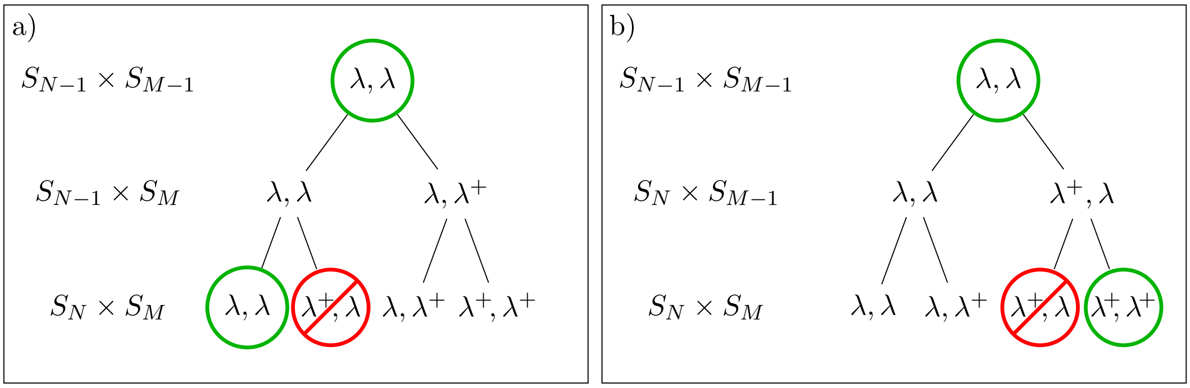


Figure 6.4: a) Justification of Equation (6.3). The irrep (λ, λ) of $S_{N-1} \times S_M$ only induces to one irrep of $S_N \times S_M$, since the other possible irrep is invalid (diagram λ^+ is not contained inside λ). b) Justification of Equation (6.4), using a similar argument.

groups, we will from now on use superscripts (for example $\Pi^{N,M}_{\lambda,\lambda}$ denotes a projector on the irrep (λ, λ) of $S_N \times S_M$). We therefore have from Theorem 6.7

$$\begin{aligned}\Delta_i^{\lambda,\lambda} =& \frac{\gamma_{|\lambda|}}{d^{N-1,M}_{\lambda,\lambda}} \sum_y \operatorname{tr}\left[\Pi^i_y \Pi^{N,M}_{\lambda,\lambda} \Pi^i_y \Pi^{N-1,M}_{\lambda,\lambda}\right] + \frac{\gamma_{|\lambda|+1}}{d^{N-1,M}_{\lambda,\lambda}} \sum_{y,\lambda^+} \operatorname{tr}\left[\Pi^i_y \Pi^{N,M}_{\lambda^+,\lambda^+} \Pi^i_y \Pi^{N-1,M}_{\lambda,\lambda}\right] - \gamma_{|\lambda|} \\ =& \frac{M\gamma_{|\lambda|}}{d^{N-1,M}_{\lambda,\lambda} d^{N-1,M-1}_{\lambda,\lambda}} \cdot \operatorname{tr}\left[\Pi^{N-1,M-1}_{\lambda,\lambda} \Pi^{N,M}_{\lambda,\lambda}\right] \cdot \operatorname{tr}\left[\Pi^{N-1,M-1}_{\lambda,\lambda} \Pi^{N-1,M}_{\lambda,\lambda}\right] \\ &+ \frac{M\gamma_{|\lambda|+1}}{d^{N-1,M}_{\lambda,\lambda} d^{N-1,M-1}_{\lambda,\lambda}} \sum_{\lambda^+} \operatorname{tr}\left[\Pi^{N-1,M-1}_{\lambda,\lambda} \Pi^{N,M}_{\lambda^+,\lambda^+}\right] \cdot \operatorname{tr}\left[\Pi^{N-1,M-1}_{\lambda,\lambda} \Pi^{N-1,M}_{\lambda,\lambda}\right] - \gamma_{|\lambda|},\end{aligned}$$

where we have used Lemma 6.8 and the fact that all terms in the sum over y are equal by symmetry.

From Figure 6.4, we see that

$$\operatorname{tr}\left[\Pi^{N-1,M-1}_{\lambda,\lambda} \Pi^{N,M}_{\lambda,\lambda}\right] = \operatorname{tr}\left[\Pi^{N-1,M-1}_{\lambda,\lambda} \Pi^{N-1,M}_{\lambda,\lambda}\right], \tag{6.3}$$

$$\operatorname{tr}\left[\Pi^{N-1,M-1}_{\lambda,\lambda} \Pi^{N,M}_{\lambda^+,\lambda^+}\right] = \operatorname{tr}\left[\Pi^{N-1,M-1}_{\lambda,\lambda} \Pi^{N,M-1}_{\lambda^+,\lambda}\right], \tag{6.4}$$

since the only way for (λ, λ) as an irrep of $S_N \times S_M$ to restrict to (λ, λ) as an irrep of $S_{N-1} \times S_{M-1}$ is to first restrict to (λ, λ) as an irrep of $S_{N-1} \times S_M$, and similarly for (λ^+, λ^+). Therefore, we only have two traces to compute. For the first one, we consider the maximally mixed state $\rho^{N-1,M-1}_{\lambda,\lambda}$ over the corresponding irrep. By inducing from S_{M-1} to S_M we find that its overlap over the irrep (λ, λ) of $S_{N-1} \times S_M$ is given by

$$\operatorname{tr}\left[\rho^{N-1,M-1}_{\lambda,\lambda} \Pi^{N-1,M}_{\lambda,\lambda}\right] = \frac{d^{N-1,M}_{\lambda,\lambda}}{M d^{N-1,M-1}_{\lambda,\lambda}} = \frac{d^M_\lambda}{M d^{M-1}_\lambda}.$$

For the second term, we use the fact that $\sum_{\lambda^+} \Pi^{N,M-1}_{\lambda^+,\lambda} = \mathbb{I} - \Pi^{N,M-1}_{\lambda,\lambda}$,

$$\sum_{\lambda^+} \operatorname{tr}\left[\rho^{N-1,M-1}_{\lambda,\lambda} \Pi^{N,M-1}_{\lambda^+,\lambda}\right] = 1 - \operatorname{tr}\left[\rho^{N-1,M-1}_{\lambda,\lambda} \Pi^{N,M-1}_{\lambda,\lambda}\right] = 1 - \frac{d^N_\lambda}{N d^{N-1}_\lambda},$$

and finally

$$\begin{aligned}\Delta_i^{\lambda,\lambda} &= \gamma_{|\lambda|}\frac{d_\lambda^M}{Md_\lambda^{M-1}} + \gamma_{|\lambda|+1}\left(1-\frac{d_\lambda^N}{Nd_\lambda^{N-1}}\right) - \gamma_{|\lambda|} \\ &= \frac{1}{\sqrt{N}} + \mathrm{O}\left(\frac{1}{N}+\frac{1}{M}\right),\end{aligned}$$

where we have used Lemma 6.13.

Case (λ,λ^+)**.** This irrep has multiplicity two, so we need to compute a 2×2 matrix. Let $(\lambda,\lambda^+,1)$ denote the copy of (λ,λ^+) irrep of $S_{N-1}\times S_M$ which is inside the (λ^+,λ^+) irrep of $S_N\times S_M$. Let $(\lambda,\lambda^+,2)$ denote the copy of (λ,λ^+) irrep of $S_{N-1}\times S_M$ which is inside the (λ,λ^+) irrep of $S_N\times S_M$. Let the first row and the first column of $\Delta_i^{\lambda,\lambda^+}$ be indexed by $(\lambda,\lambda^+,1)$ and the second row and the second column be indexed by $(\lambda,\lambda^+,2)$.

An irrep (λ,λ^+) of $S_{N-1}\times S_M$ restricts to two valid irreps of $S_{N-1}\times S_{M-1}$: (λ,λ) and (λ,λ^+). Those two irreps can be induced to the following bad irreps of $S_N\times S_M$: (λ,λ) and any irrep (λ',λ') which has one more square below the first row than λ. (λ' may be equal or different from λ^+.)

For brevity, we denote $\Delta_i^{\lambda,\lambda^+}$ simply by Δ. Since $(\lambda,\lambda^+,1)$ is contained inside a bad irrep of $S_N\times S_M$, we have

$$\begin{aligned}\Delta_{1,1} = {} & \frac{\gamma_{|\lambda|}}{d^{N-1,M}_{\lambda,\lambda^+}}\sum_y \mathrm{tr}\left[\Pi^i_y\Pi^{N,M}_{\lambda,\lambda}\Pi^i_y\Pi^{N-1,M}_{\lambda,\lambda^+,1}\right] + \frac{\gamma_{|\lambda|+1}}{d^{N-1,M}_{\lambda,\lambda^+}}\sum_{\lambda'}\sum_y \mathrm{tr}\left[\Pi^i_y\Pi^{N,M}_{\lambda',\lambda'}\Pi^i_y\Pi^{N-1,M}_{\lambda,\lambda^+,1}\right] - \gamma_{|\lambda|+1} \\ = {} & \frac{M\gamma_{|\lambda|}}{d^{N-1,M}_{\lambda,\lambda^+}d^{N-1,M-1}_{\lambda,\lambda}}\mathrm{tr}\left[\Pi^{N-1,M-1}_{\lambda,\lambda}\Pi^{N,M}_{\lambda,\lambda}\right]\mathrm{tr}\left[\Pi^{N-1,M-1}_{\lambda,\lambda}\Pi^{N-1,M}_{\lambda,\lambda^+,1}\right] \\ & + \frac{M\gamma_{|\lambda|+1}}{d^{N-1,M}_{\lambda,\lambda^+}d^{N-1,M-1}_{\lambda,\lambda}}\left(\sum_{\lambda'}\mathrm{tr}\left[\Pi^{N-1,M-1}_{\lambda,\lambda}\Pi^{N,M}_{\lambda',\lambda'}\right]\right)\mathrm{tr}\left[\Pi^{N-1,M-1}_{\lambda,\lambda}\Pi^{N-1,M}_{\lambda,\lambda^+,1}\right] \\ & + \frac{M\gamma_{|\lambda|+1}}{d^{N-1,M}_{\lambda,\lambda^+}d^{N-1,M-1}_{\lambda,\lambda^+}}\mathrm{tr}\left[\Pi^{N-1,M-1}_{\lambda,\lambda^+}\Pi^{N,M}_{\lambda^+,\lambda^+}\right]\mathrm{tr}\left[\Pi^{N-1,M-1}_{\lambda,\lambda^+}\Pi^{N-1,M}_{\lambda,\lambda^+,1}\right] - \gamma_{|\lambda|+1}\end{aligned}$$

We start by evaluating the sum

$$\sum_{\lambda'}\mathrm{tr}\left[\Pi^{N-1,M-1}_{\lambda,\lambda}\Pi^{N,M}_{\lambda',\lambda'}\right].$$

We consider the maximally mixed state $\rho^{N-1,M-1}_{\lambda,\lambda}$ over the corresponding irrep of $S_{N-1}\times S_{M-1}$. By inducing λ from S_{N-1} to S_N, we find that the dimension of the induced representation is Nd_λ^{N-1} and the induced representation decomposes into irrep λ of S_N, with dimension d_λ^N and irreps λ'. Therefore,

$$\sum_{\lambda'}\mathrm{tr}\left[\Pi^{N,M}_{\lambda',\lambda'}\rho^{N-1,M-1}_{\lambda,\lambda}\right] = 1-\frac{d_\lambda^N}{Nd_\lambda^{N-1}} \le 1-\frac{1}{N} \tag{6.5}$$

where the inequality follows by comparing the hook-length formulas of d_λ^N and d_λ^{N-1}. Similarly, we have

$$\mathrm{tr}\left[\Pi^{N,M}_{\lambda,\lambda}\rho^{N-1,M-1}_{\lambda,\lambda}\right] = \mathrm{O}\left(\frac{1}{N}\right). \tag{6.6}$$

We now evaluate a similar quantity for $\rho^{N-1,M-1}_{\lambda,\lambda^+}$. By inducing λ^+ from S_{M-1} to S_M, we find that the dimension of the induced representation is $Md^{M-1}_{\lambda^+}$ and the induced representation decomposes into irrep λ^+ of S_M, with dimension d^M_λ and irreps λ^{++} which have one more square below the first row than λ^+. Therefore,

$$\operatorname{tr}\left[\Pi^{N,M}_{\lambda^+,\lambda^+}\rho^{N-1,M-1}_{\lambda,\lambda^+}\right] = \frac{d^M_\lambda}{Md^{M-1}_\lambda} = \mathrm{O}\left(\frac{1}{M}\right). \tag{6.7}$$

By using Equations (6.5), (6.6) and (6.7), we have

$$\Delta_{1,1} = \frac{M\gamma_{|\lambda|+1}}{d^{N-1,M}_{\lambda,\lambda^+}}\operatorname{tr}\left[\Pi^{N-1,M-1}_{\lambda,\lambda}\Pi^{N-1,M}_{\lambda,\lambda^+,1}\right] + \mathrm{O}\left(\frac{1}{N}\right) - \gamma_{|\lambda|+1}. \tag{6.8}$$

We have

$$\operatorname{tr}\left[\Pi^{N-1,M-1}_{\lambda,\lambda}\Pi^{N-1,M}_{\lambda,\lambda^+,1}\right] = \operatorname{tr}\left[\Pi^{N-1,M-1}_{\lambda,\lambda}\Pi^{N,M}_{\lambda^+,\lambda^+}\right]$$

because the other irreps of $S_{N-1}\times S_M$ contained in the irrep (λ^+,λ^+) of $S_N\times S_M$ have no overlap with the irrep (λ,λ) of $S_{N-1}\times S_{M-1}$. Let $\rho^{N-1,M-1}_{\lambda,\lambda}$ be the completely mixed state over (λ,λ). Then,

$$\operatorname{tr}\left[\Pi^{N-1,M-1}_{\lambda,\lambda}\Pi^{N,M}_{\lambda^+,\lambda^+}\right] = d^{N-1,M-1}_{\lambda,\lambda}\operatorname{tr}\left[\Pi^{N,M}_{\lambda^+,\lambda^+}\rho^{N-1,M-1}_{\lambda,\lambda}\right] = d^{N-1,M-1}_{\lambda,\lambda}\frac{d^N_{\lambda^+}}{Nd^{N-1}_\lambda}.$$

Here, the second equality follows by inducing λ from S_{N-1} to S_N. We have

$$d^{N-1,M-1}_{\lambda,\lambda}\frac{d^N_{\lambda^+}}{Nd^{N-1}_\lambda} = d^{N-1}_\lambda d^{M-1}_\lambda\frac{d^N_{\lambda^+}}{Nd^{N-1}_\lambda} = \frac{d^{M-1}_\lambda d^N_{\lambda^+}}{N}.$$

By matching up the terms in hook-length formulas, we have

$$d^{M-1}_\lambda d^N_{\lambda^+} = \left(1+\mathrm{O}\left(\frac{1}{N}\right)\right)\frac{N}{M}d^{N-1}_\lambda d^M_{\lambda^+}. \tag{6.9}$$

Therefore,

$$\operatorname{tr}\left[\Pi^{N-1,M-1}_{\lambda,\lambda}\Pi^{N,M}_{\lambda^+,\lambda^+}\right] = \left(1+\mathrm{O}\left(\frac{1}{N}\right)\right)\frac{d^{N-1,M}_{\lambda,\lambda^+}}{M} \tag{6.10}$$

and

$$\Delta_{1,1} = \mathrm{O}\left(\frac{1}{N}\right)$$

Similarly to Equation (6.8), we have

$$\Delta_{2,2} = \frac{M\gamma_{|\lambda|+1}}{d^{N-1,M}_{\lambda,\lambda^+}}\operatorname{tr}\left[\Pi^{N-1,M-1}_{\lambda,\lambda}\Pi^{N-1,M}_{\lambda,\lambda^+,2}\right] + \mathrm{O}\left(\frac{1}{N}\right). \tag{6.11}$$

We have

$$\operatorname{tr}\left[\Pi^{N-1,M-1}_{\lambda,\lambda}\Pi^{N-1,M}_{\lambda,\lambda^+,2}\right] = \operatorname{tr}\left[\Pi^{N-1,M-1}_{\lambda,\lambda}\Pi^{N,M}_{\lambda,\lambda^+}\right] = d^{N-1,M-1}_{\lambda,\lambda}\operatorname{tr}\left[\Pi^{N,M}_{\lambda,\lambda^+}\rho^{N-1,M-1}_{\lambda,\lambda}\right],$$

because the other irreps of $S_{N-1} \times S_M$ contained in the irrep (λ, λ^+) of $S_N \times S_M$ have no overlap with the irrep (λ, λ) of $S_{N-1} \times S_{M-1}$.

By inducing λ from S_{M-1} to S_M, we get

$$\mathrm{tr}\left[\Pi^{N,M}_{\lambda,\lambda^+}\rho^{N-1,M-1}_{\lambda,\lambda}\right] + \mathrm{tr}\left[\Pi^{N,M}_{\lambda^+,\lambda^+}\rho^{N-1,M-1}_{\lambda,\lambda}\right] = \frac{d^M_{\lambda^+}}{M d^{M-1}_{\lambda}}. \tag{6.12}$$

By inducing λ from S_{N-1} to S_N, we get

$$\mathrm{tr}\left[\Pi^{N,M}_{\lambda^+,\lambda^+}\rho^{N-1,M-1}_{\lambda,\lambda}\right] = \frac{d^N_{\lambda^+}}{N d^{N-1}_{\lambda}}. \tag{6.13}$$

By subtracting Equation (6.13) from Equation (6.12), we get

$$\mathrm{tr}\left[\Pi^{N-1,M-1}_{\lambda,\lambda}\Pi^{N,M}_{\lambda,\lambda^+}\right] = \frac{d^M_{\lambda^+}d^{N-1}_{\lambda}}{M} - \frac{d^N_{\lambda^+}d^{M-1}_{\lambda}}{N}.$$

Because of Equation (6.9),

$$\mathrm{tr}\left[\Pi^{N-1,M-1}_{\lambda,\lambda}\Pi^{N,M}_{\lambda,\lambda^+}\right] = \mathrm{O}\left(\frac{d^M_{\lambda^+}d^{N-1}_{\lambda}}{MN}\right). \tag{6.14}$$

By substituting this into Equation (6.11), we get $\Delta_{2,2} = \mathrm{O}\left(\frac{1}{N}\right)$.

Last, we have to bound $\Delta_{1,2}$ and $\Delta_{2,1}$. Similarly to Equation (6.8), we have

$$\Delta_{i,j} = \frac{M\gamma_{|\lambda|+1}}{d^{N-1,M}_{\lambda,\lambda^+}}\mathrm{tr}\left[\Pi^{N-1,M-1}_{\lambda,\lambda}\Pi^{N-1,M}_{\lambda,\lambda^+,i\leftarrow j}\right] + \mathrm{O}\left(\frac{1}{N}\right).$$

By using Lemma 6.8 and Equations (6.10) and (6.14), we get

$$\Delta_{i,j} = \mathrm{O}\left(\frac{1}{\sqrt{N}}\right).$$

We have shown that $\Delta_{i,j} = \mathrm{O}\left(\frac{1}{\sqrt{N}}\right)$ for all i, j. Therefore, $\|\Delta\| = \mathrm{O}\left(\frac{1}{\sqrt{N}}\right)$.

Case (λ, λ^{++})**.** This irrep of $S_{N-1} \times S_M$ has multiplicity three, so we need to bound the elements of a 3×3 matrix. Let $(\lambda, \lambda^{++}, 1)$ denote the copy of the irrep that lies inside the irrep (λ, λ^{++}) of $(S_N \times S_M)$, $(\lambda, \lambda^{++}, 2)$ be the copy that lies inside the irrep $(\lambda^+, \lambda^{++})$ of $(S_N \times S_M)$, and $(\lambda, \lambda^{++}, 3)$ be the copy that lies inside the irrep $(\lambda'^+, \lambda^{++})$ of $(S_N \times S_M)$, where λ^+ and λ'^+ correspond to the two different ways a box can be added to λ. Since these two last copies have exactly the same structure, they can be treated similarly and we really need to compute only 4 different matrix elements (2 diagonal elements and 2 non-diagonal elements). Let us also note that none of these copies are contained in bad irreps of $S_N \times S_M$.

Let us now denote $\Delta^{\lambda,\lambda^{++}}_i$ by Δ, and index the rows and columns of this matrix by the three copies of the irrep. Note that the irrep (λ, λ^{++}) of $S_{N-1} \times S_M$ restricts to three valid irreps of $S_{N-1} \times S_{M-1}$: (λ, λ^{++}), (λ, λ^+) and (λ, λ'^+). Also only these last two irreps induce to bad irreps of $S_N \times S_M$, (λ^+,λ^+) and (λ'^+,λ'^+), respectively. Therefore, we have for the first diagonal element

$$\begin{aligned}\Delta_{1,1} &= \frac{\gamma_{|\lambda|+1}}{d^{N-1,M}_{\lambda,\lambda^{++}}}\sum_y \left\{\operatorname{tr}\left[\Pi^i_y\Pi^{N,M}_{\lambda^+,\lambda^+}\Pi^i_y\Pi^{N-1,M}_{\lambda,\lambda^{++},1}\right] + \operatorname{tr}\left[\Pi^i_y\Pi^{N,M}_{\lambda'^+,\lambda'^+}\Pi^i_y\Pi^{N-1,M}_{\lambda,\lambda^{++},1}\right]\right\}\\ &= \frac{2M\gamma_{|\lambda|+1}d^{N-1,M-1}_{\lambda,\lambda^+}}{d^{N-1,M}_{\lambda,\lambda^{++}}}\operatorname{tr}\left[\Pi^{N,M}_{\lambda^+,\lambda^+}\rho^{N-1,M-1}_{\lambda,\lambda^+}\right]\cdot\operatorname{tr}\left[\Pi^{N-1,M}_{\lambda,\lambda^{++},1}\rho^{N-1,M-1}_{\lambda,\lambda^+}\right].\end{aligned}$$

Studying as before the overlap of $\rho^{N-1,M-1}_{\lambda,\lambda^+}$ over the irreps of $S_N \times S_M$, we obtain for the two traces

$$\operatorname{tr}\left[\Pi^{N,M}_{\lambda^+,\lambda^+}\rho^{N-1,M-1}_{\lambda,\lambda^+}\right] \le \frac{d^M_{\lambda^+}}{Md^{M-1}_{\lambda^+}}, \tag{6.15}$$

$$\operatorname{tr}\left[\Pi^{N-1,M}_{\lambda,\lambda^{++},1}\rho^{N-1,M-1}_{\lambda,\lambda^+}\right] = \operatorname{tr}\left[\Pi^{N,M}_{\lambda,\lambda^{++}}\rho^{N-1,M-1}_{\lambda,\lambda^+}\right] \le \frac{d^N_{\lambda^+}}{Nd^{N-1}_{\lambda^+}}, \tag{6.16}$$

and in turn

$$\Delta_{1,1} \le \frac{2M\gamma_{|\lambda|+1}d^N_{\lambda^+}d^M_{\lambda^+}}{Nd^{N-1}_{\lambda^+}d^M_{\lambda^{++}}} = \mathrm{O}\left(\frac{1}{MN}\right).$$

For the second diagonal element, we find similarly

$$\begin{aligned}\Delta_{2,2} &= \frac{\gamma_{|\lambda|+1}}{d^{N-1,M}_{\lambda,\lambda^{++}}}\sum_y \left\{\operatorname{tr}\left[\Pi^i_y\Pi^{N,M}_{\lambda^+,\lambda^+}\Pi^i_y\Pi^{N-1,M}_{\lambda,\lambda^{++},2}\right] + \operatorname{tr}\left[\Pi^i_y\Pi^{N,M}_{\lambda'^+,\lambda'^+}\Pi^i_y\Pi^{N-1,M}_{\lambda,\lambda^{++},2}\right]\right\}\\ &= \frac{M\gamma_{|\lambda|+1}d^{N-1,M-1}_{\lambda,\lambda^+}}{d^{N-1,M}_{\lambda,\lambda^{++}}}\operatorname{tr}\left[\Pi^{N,M}_{\lambda^+,\lambda^+}\rho^{N-1,M-1}_{\lambda,\lambda^+}\right]\cdot\left\{\operatorname{tr}\left[\Pi^{N-1,M}_{\lambda,\lambda^{++},2}\rho^{N-1,M-1}_{\lambda,\lambda^+}\right] + \operatorname{tr}\left[\Pi^{N-1,M}_{\lambda,\lambda^{++},2}\rho^{N-1,M-1}_{\lambda,\lambda'^+}\right]\right\}\\ &\le \frac{2\gamma_{|\lambda|+1}d^M_{\lambda^+}}{d^M_{\lambda^{++}}} = \mathrm{O}\left(\frac{1}{M}\right),\end{aligned}$$

where we have used Equation (6.16) and the fact that the other overlaps are at most 1.

Using exactly the same arguments, we find for the non-diagonal elements

$$\begin{aligned}|\Delta_{1,2}| &\le \frac{2\gamma_{|\lambda|+1}d^M_{\lambda^+}}{d^M_{\lambda^{++}}}\sqrt{\frac{d^N_{\lambda^+}}{Nd^{N-1}_{\lambda^+}}} = \mathrm{O}\left(\frac{1}{M\sqrt{N}}\right),\\ |\Delta_{2,3}| &\le \frac{2\gamma_{|\lambda|+1}d^M_{\lambda^+}}{d^M_{\lambda^{++}}} = \mathrm{O}\left(\frac{1}{M}\right).\end{aligned}$$

Since the irreps $(\lambda,\lambda^{++},2)$ and $(\lambda,\lambda^{++},3)$ are of the same type, we also have $\Delta_{3,3} = \mathrm{O}(1/M)$ and $\Delta_{1,3} = \mathrm{O}\left(1/(M\sqrt{N})\right)$. Therefore, all elements of Δ are at most $\mathrm{O}(1/M)$, so that $\|\Delta\| = \mathrm{O}(1/M)$.

Finally, since the matrices corresponding to all irreps have norm at most $\mathrm{O}\left(1/\sqrt{N}\right)$, we have from Theorem 6.7 that $\left\|\widetilde{\Gamma}_i - \widetilde{\Gamma}\right\| = \mathrm{O}\left(1/\sqrt{N}\right)$, and in turn

$$Q_\varepsilon(\textsc{Index Erasure}) = \Omega\left((\sqrt{1-\varepsilon} - \sqrt{N/M})^2\sqrt{N}\right).$$

6.5 Summary

In this Chapter, we showed that the multiplicative adversary bound satisfies a strong direct product even for quantum state generation problems. We also examined how to use the adversary methods on specific problems, in particular we gave simple expressions when the automorphism group of a function is multiplicity-free. We then applied these formulas to re-derived the bounds for Search, (which gives an illustration of the differences between the adversary methods) and a tight lower bound for Index Erasure.

7 Perspectives

7.1 Cryptographic primitives

The quest is now to find practical schemes for implementing quantum primitives. Bit commitment and coin flipping face different challenges: indeed, we are interested in secure quantum bit commitment based on "reasonable" assumptions. In this manuscript we unfortunately proved that the physically grounded restriction to Gaussian states and Gaussian operations does not allow security. Let us give two other approaches that could lead to secure bit commitment under restrictions.

Gaussian bounded/noisy-storage model In a recent series of work, bit commitment and oblivious transfer have been shown to been secure when both player have bounded or deficient memories [DFSS08, WW08, WST08]. However, the proposed protocols involve qubits, single photon source and single photon detectors. Following the footsteps of quantum key distribution, proposing protocols with Gaussian variables could lead to efficient protocols. It appears that the study of security of such protocols requires new ideas. For example what is the good definition of "bounded" memory for continuous variables? If one tries to limit the number of modes, each of them being described by an infinite-dimensional vector, the overall Hilbert space is still unbounded, thus no real limitation is achieved. In these models, security can be proved by using a strong converse Shannon coding theorem [KW09]. Very few results are known in the continuous case, even for Gaussian channels. Such results would have strong impacts in the study of continuous variables cryptography.

Almost Gaussian bit commitment To go beyond Gaussian bit commitment we wish to find another model, with physical significance, that allows bit commitment. Mandilara and Cerf [MC11] proposed an extension to the Gaussian model by allowing a non-Gaussian gate (in this case photon subtraction) that only succeeds with bounded probability. They introduced a protocol which is more a proof-of-concept than a proposal for an actual protocol and proved as a first step that it is secure against Gaussian attacks. The full study of the security remains to be done and this idea deserves to be pushed further.

Let us point out that adding any non-Gaussian gate to Gaussian computation makes it universal for quantum computing [LB99]. This leads to the following extension: consider a set of gates that is not universal for quantum computing (e.g. Clifford operation for discrete variables, Gaussian operations for continuous variables) and one extra gate that makes the set universal (CNOT for DV, cubic gate for CV) but which can only be implemented with bounded probability. Can one construct a secure bit commitment protocol in this setting? The idea is that when preparing states, the probabilistic gate can be repeated as long a desired, but not when trying to cheat. Such a model is strongly grounded for the CV case and might also be relevant in the DV one.

Weak coin flipping The situation is quite different for weak coin flipping. If one tries to construct a protocol directly from the point games, it will be ridiculous in term of resources (qubits, circuit size, and number of rounds). Finding protocols with more constrained resources seems the next step. In particular, the recursive structure of the ladder seems to imply that such protocols may exist. Another direction is to prove better bounds on the number of rounds needed to achieve a bias ε than the current lower bound of $\log\log 1/\varepsilon$ [Amb04]. Only when such protocols will be discovered, it will be interesting to study practical questions that arise from implementation: detector efficiency, loss in the communication channel, imperfection of memories, etc. It would also be interesting to know if the proof of arbitrary small bias can still be adapted to take care of these effects, or if it will stay a Grail for unconditional security.

7.2 Query complexity

We proved that the multiplicative method is the strongest method we currently have to prove lower bounds for the quantum query complexity. Nevertheless this method is quite challenging to use, this is why we gave an easier formulation in term of representation theory when problems are multiplicity free.

Graph Isomorphism We extended the adversary methods to prove lower bounds for quantum state generation problems and demonstrated the power of our method by proving a tight lower bound for Index Erasure. This did not specifically address Graph Isomorphism since an exponential lower bound was already known using this approach. However we now have at our disposal a powerful new tool to rule out many more "state generation" approaches in the query complexity model. The next step is to consider more powerful approaches than Index Erasure for which we did not assume any structure to the problem. One elegant solution would be to prove lower bounds for the Component Superposition problem introduced in [Lut11]. This would have implication for Graph Isomorphism as well as on the study of counterfeiting quantum money [FGH+10].

Lower bound for Element Disctinctness The optimal lower bounds for Element Distinctness and Collision have been proved by the polynomial method [AS04]. Unfortunately it is not know how to extend those proofs to related problems like k-Element Distinctness. The reduction from the polynomial method to the multiplicative adversary method offers a new hope to prove those lower bounds. The first step is naturally to reprove the bound for Element Distinctness using the adversary method, and in a second step to generalize it.

Time-space tradeoff for Element Distinctness We made a significant step in proving that the quantum query complexity obeys a strong direct product theorem, the proof has then been completed in [LR11]. However this proof holds only for functions and not for quantum state generation problems. One possible application of this theorem is for proving a time-space tradeoff for Element Distinctness. Indeed, such tradeoff for multi output problems, such as Sorting, were proved using SDPTs. The k independent instances of a function f are encoded in Sorting such that the k outputs can be deduced from the sorted array. Then the space constraint combined to the SDPT gives the time-space tradeoff. For a decision problem however, such as Element Distinctness, this approach fails. One needs a measure on the progress based on the intermediate quantum states. We hope our approach can contribute to this quest.

Part III

Appendices

A Phase-space representation and Wigner function

In this Appendix we introduce another description of continuous variables states and operation: the phase-space description. This gives a formal justification to the introduction of covariance and symplectic matrices for Gaussian states.

A.1 Characteristic and Wigner functions

Definition A.1 (The operators X and P) *For $j \in [n]$, define the operators $X_j, P_j : L^2(\mathbb{R}^n) \to \mathbb{C}^{\mathbb{R}^n}$ that act on a function $\psi \in L^2(\mathbb{R}^n)$ by*

- $\forall (x_1, \dots, x_n) \in \mathbb{R}^n,\ X_j[\psi](x_1, \dots, x_n) = x_j \psi(x_1, \dots, x_n),$
- $\forall (x_1, \dots, x_n) \in \mathbb{R}^n,\ P_j[\psi](x_1, \dots, x_n) = -i \frac{\partial \psi}{\partial x_j}(x_1, \dots, x_n).$

Definition A.2 (Characteristic function) *Let $\xi = (\alpha_1, \beta_1, \dots, \alpha_n, \beta_n) \in \mathbb{R}^{2n}$. Define the Weyl operator V_ξ on $L^2(\mathbb{R}^n)$ by:*

$$V_\xi = \exp\left\{ \sum_{i=1}^{n} \alpha_i X_i + \beta_i P_i \right\}.$$

The characteristic function of a trace-class operator A is

$$\chi_A : \xi \mapsto \mathrm{tr}[A V_\xi].$$

The Weyl operator, is sometimes called the displacement operator. For example let $|\psi\rangle \in L^2(\mathbb{R})$, then $V_{(\alpha,0)}|\psi\rangle$ is the function: $x \mapsto \psi(x - \alpha)$. Consider another example: let ρ be a density operator on n modes, and ζ a $2n$-dimensional vector, the $\chi_{V_\zeta \rho V_\zeta^\dagger}(\xi) = \chi_\rho(\xi - \zeta)$. Details of these derivations can be found in [GPS07].

The vector ξ belongs to a $2n$-dimensional real space called the *phase-space*. The phase-space is actually a good model to analyze CV systems since any trace-class operator can be reconstructed from its characteristic function, this is the Weyl-Wigner isomorphism:

$$A = \frac{1}{(2\pi)^n} \int \chi_A(-\xi) V_\xi \mathrm{d}\xi.$$

Though all the computations in the phase-space can be done using the characteristic function, it is often easier to use the Wigner function which is its Fourier transform:

$$W_A(\xi) = \frac{1}{(2\pi)^n} \int \chi_A(\zeta) \exp\left\{ i \xi^T \Omega \zeta \right\} \mathrm{d}\zeta,$$

where $\Omega = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^{\oplus n}$.

It is also very useful to compute the trace of a state from its Wigner function. Let A and B be two trace-class operators, we have:

$$\begin{aligned}\mathrm{tr}[A] &= \int_{\mathbb{R}^{2n}} W_A(\xi)\mathrm{d}\xi,\\ \mathrm{tr}[AB] &= (2\pi)^n \int_{\mathbb{R}^{2n}} W_A(\xi)W_B(\xi)\mathrm{d}\xi.\end{aligned}$$

This latest formula has some practical implications. For example, it can be used to compute the purity of a state ρ by taking $A = B = \rho$, that is

$$\mathrm{tr}(\rho^2) = (2\pi)^n \int_{\mathbb{R}^{2n}} \mathrm{d}\xi W_\rho(\xi)^2,$$

or the fidelity between a mixed state ρ and a pure state $|\psi\rangle\langle\psi|$:

$$\mathcal{F}(\rho, |\psi\rangle\langle\psi|)^2 = \langle\psi|\rho|\psi\rangle = \mathrm{tr}[\rho|\psi\rangle\langle\psi|] = (2\pi)^n \int_{\mathbb{R}^{2n}} W_\rho(\xi)W_{|\psi\rangle\langle\psi|}(\xi)\mathrm{d}\xi.$$

This is also how is computed the Wigner function of the partial trace of an operator. Let ρ_{AB} be a bipartite state with $n+m$ modes and denote by $\rho_A = \mathrm{tr}_B(\rho_{AB})$, then

$$W_{\rho_A}(\xi_A) = \int_{\mathbb{R}^{2m}} W_{\rho_{AB}}\left(\begin{smallmatrix}\xi_A\\ \xi_B\end{smallmatrix}\right)\mathrm{d}\xi_B.$$

A.2 Gaussian states

Definition A.3 (Gaussian states) *An n-mode Gaussian state is a state whose Wigner function is a multivariate normal distribution, that is:*

$$W_\rho(\xi) = \frac{1}{\pi^n\sqrt{\det\gamma}}\exp\left\{-(\xi-\mu)^T\gamma^{-1}(\xi-\mu)\right\},$$

where γ is a covariance matrix satisfying $\gamma + i\Omega \succeq 0$ and μ is a $2n$-dimensional real vector called the mean vector.

Representing a 1-mode state in the phase-space requires a 3D-plotting. It is often easier to represent them in a 2-dimensional plane spanned by x and p with a contour plot. The plot represents the variance of a state, see e.g. Figure A.1.

Two-mode squeezed states Recall that a two mode squeezed state is given by a null mean vector and a covariance matrix

$$\begin{pmatrix} \nu & 0 & \sqrt{\nu^2-1} & 0\\ 0 & \nu & 0 & -\sqrt{\nu^2-1}\\ \sqrt{\nu^2-1} & 0 & \nu & 0\\ 0 & -\sqrt{\nu^2-1} & 0 & \nu \end{pmatrix}.$$

We can now understand why this state is similar to the EPR pair. In the limit $r \to \infty$, this Wigner function of the state would be given by Dirac deltas: $(x_1, p_1, x_2, p_2) \mapsto \delta(x_1 - x_2)\delta(p_1 + p_2)$, meaning that the value of x_1 and x_2 are perfectly correlated, as the value of any projective measurement of a shared EPR pair are perfectly correlated. Unfortunately such states do not exist since they would require an infinite squeezing, hence infinite energy. This is why using CV EPR pair, the value of the measurements are approximately correlated.

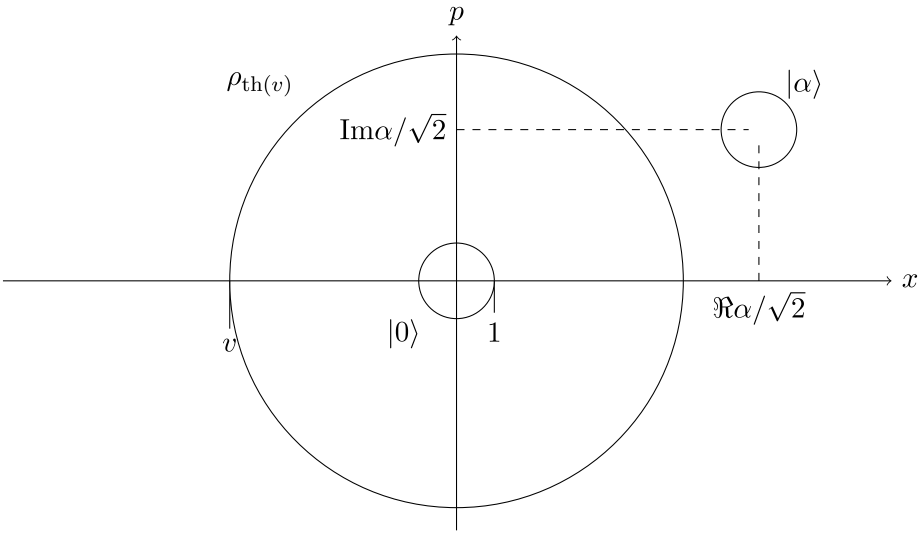


Figure A.1: Phase-space representations of the vacuum state $|0\rangle$, a coherent state centered on α and a thermal state of variance v. The diameter of the circles represent the variance of the Wigner function.

A.3 Operations

Gaussian unitary Let ρ be a n-mode Gaussian state and U be Gaussian unitary acting on n modes and characterized by a symplectic matrix S and a displacement vector d, then for all $\xi \in \mathbb{R}^{2n}$:

$$W_{U\rho U^\dagger}(\xi) = W_\rho(S^T\xi - d).$$

Homodyne measurement The homodyne measurement of one mode is the measurement of the value of one quadrature of this mode (x or p). Since these values are continuous, the outcomes of the measurement are given by a continuous probability distribution P which corresponds the marginal of the Wigner function over the other quadrature:

$$P(x) = \int_{\mathbb{R}} W(x,p)\mathrm{d}p.$$

Partial measurement When considering multimode states, the partial measurement of some of the mode is a Gaussian operation. Consider a bipartite Gaussian state with covariance matrix $\gamma_{AB} = \begin{pmatrix} \gamma_A & C \\ C^T & \gamma_B \end{pmatrix}$ and a mean vector $\mu = \mu_A \oplus \mu_B$. Denote by $\mu_m = (x_1, 0, x_2, 0, \ldots, x_{n_B}, 0)$ the values of the homodyne measurements on the "B" modes, then the resulting state on A conditionally on the outcome μ_B on B is described a covariance matrix

$$\gamma_A - C(\Delta\gamma_B\Delta)^{-1}C^T$$

where $\Delta = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}^{\oplus n_B}$ and the inverse is taken only on the range of the matrix. The mean vector reads,

$$C(\Delta\gamma_B\Delta)^{-1}C^T(\mu_m - \mu_B) + \mu_A.$$

B Additional constraint on the dual feasible points

Lemma B.1 *$P^*_A = \inf \alpha$ and $P^*_B = \inf \beta$ where the infinimum is taken over all dual feasible points.*

The difference between this lemma and Theorem 4.4, is the condition ⑤ of that the dual feasible points should obey. We will now prove that for all set of matrices $\{Z_{A,i}\}$ that satisfy the constraints ① to ④ and all $\varepsilon > 0$, there exists a set of matrices $\{Z'_{A,i}\}$ that satisfy the constraints ① to ⑤ with $\alpha = \mathrm{tr}(Z'_{A,0}\rho_0) = \mathrm{tr}(Z_{A,0}\rho_0) + \varepsilon$.

Fix $\{Z_{A,0}, \dots, Z_{A,n}\}$ a set of matrices that satisfies the constraints ① to ④ and $\varepsilon > 0$. The proof relies on the following fact: there exists $\Lambda > 0$ such that:

$$Z'_{A,0} = (\langle\psi_{A,0}|Z_{A,0}|\psi_{A,0}\rangle + \varepsilon)|\psi_{A,0}\rangle\langle\psi_{A,0}| + \Lambda(\mathbb{I} - |\psi_{A,0}\rangle\langle\psi_{A,0}|) \succeq Z_{A,0}.$$

For all $i > 0$, define $Z'_{A,i} = Z_{A,i}$. We now prove that the set of matrices $\{Z'_{A,0}, \dots, Z'_{A,n}\}$ satisfies the constraints 1) to 6). Since $|\psi_{A,0}\rangle$ is an eigenvector of $Z'_{A,0}$ of the eigenvalue $\alpha = \mathrm{tr}(Z_{A,0}\rho_0) + \varepsilon$, the constraint 6) is satisfied. Moreover, $Z'_{A,0} \succeq Z_{A,0}$ so $Z'_{A,0} \otimes \mathbb{I}_{\mathcal{M}} \succeq Z_{A,0} \otimes \mathbb{I}_{\mathcal{M}}$ so constraint 2) is also satisfied. (All the other constraints involves only matrices $Z'_{A,i}$ for $i > 0$ so they are satisfied by definition of the $Z'_{A,i}$.

The only one thing left to do is to prove the previous claim, that is for a well chosen Λ, we have $Z'_{A,0} \succeq Z_{A,0}$. Let $|\phi\rangle$ a vector in $\mathcal{A}$, then it can be decomposed as $|\phi\rangle = a|\psi_{A,0}\rangle + b|\psi^\perp\rangle$ where $\langle\psi_{A,0}|\psi^\perp\rangle = 0$. We can restrict ourselves to $b \in \mathbb{R}$ and $|a|^2 + |b|^2 = 1$, thus we have:

$$\langle\phi|Z'_{A,0} - Z_{A,0}|\phi\rangle = |a|^2\varepsilon + |b|^2(\Lambda - \langle\psi^\perp|Z_{A,0}|\psi^\perp\rangle) - 2b\Re(a\langle\psi^\perp|Z_{A,0}|\psi_{A,0}\rangle) \tag{B.1}$$

This expression is always non negative for a Λ big enough that we will explicit later on. This Λ is independent of $|\phi\rangle$, i.e. a, b and $|\psi^\perp\rangle$. We have the following cases:

- $a = 0$. We want $\Lambda \geq \langle\psi^\perp|Z_{A,0}|\psi^\perp\rangle$ for all $|\psi^\perp\rangle$. This is possible by choosing $\Lambda \geq \|Z_{A,0}\|$. Let us assume now assume that $a \neq 0$.
- $a \neq 0$. Let us see Equation (B.1) as a polynomial in b. The leading coefficient being non negative, we need to show that the discriminant is negative for Λ large enough. The discriminant reads $4\Re(a\langle\psi^\perp|Z_{A,0}|\psi_{A,0}\rangle)^2 - 4|a|^2\varepsilon(\Lambda - \langle\psi^\perp|Z_{A,0}|\psi^\perp\rangle)$. Since for any complex number x, $\Re(x) \leq |x|$, it is sufficient to prove that for Λ large enough we have, $|a|^2|\langle\psi^\perp|Z_{A,0}|\psi_{A,0}\rangle|^2 - |a|^2\varepsilon(\Lambda - \langle\psi^\perp|Z_{A,0}|\psi^\perp\rangle) \leq 0$. Since $a \neq 0$, we want $\Lambda \geq \frac{1}{\varepsilon}(|\langle\psi^\perp|Z_{A,0}|\psi_{A,0}\rangle|^2 - \langle\psi^\perp|Z_{A,0}|\psi^\perp\rangle)$. This is done by choosing $\Lambda \geq \|Z_{A,0}\|^2/\varepsilon$.

Choosing Λ such that $\Lambda \geq \|Z_{A,0}\|$ and $\Lambda \geq \|Z_{A,0}\|^2/\varepsilon$ concludes the proof.

C Time independent point game achieving bias ε

Finally in this appendix, we present Carlos Mochon's construction of a time independent point game with final point $[1/2+\varepsilon, 1/2+\varepsilon]$, but we do not give detail of the proof. They can all be found in [Moc07]. More precisely for any $k > 1$, we will construct a family of games with final points converging to $\left[\frac{k+1}{2k+1}, \frac{k+1}{2k+1}\right]$. Each of these games can be seen as a game with 3 transitions: a split, a ladder and a raise.

C.1 Overview of the game

We now proceed to the construction of a time independent point game, i.e. we simply have to place weighted points on the plane. Since we want to construct a game corresponding to a weak coin flipping protocol, all the points (except the initial ones and the final one) should have total weight 0. That is if a point in the horizontal function has some weight w, it should have weight $-w$ as seen as a point of the vertical function.

To make this simpler, we will only consider *symmetric* games, i.e. the horizontal function h and the vertical function v will satisfy:

$$v(x,y) = -h(x,y) \quad \text{and also} \quad h(x,y) = -h(y,x). \tag{C.1}$$

except for final and initial points.

To simplify the analysis even further, we also add another constraint on the points. Except the initial points $[0,1]$ and $[1,0]$ all the points are placed on a regular 2D grid of step ω i.e. every points can be written $[a\omega, b\omega]$ for some $a, b \in \mathbb{N}$.

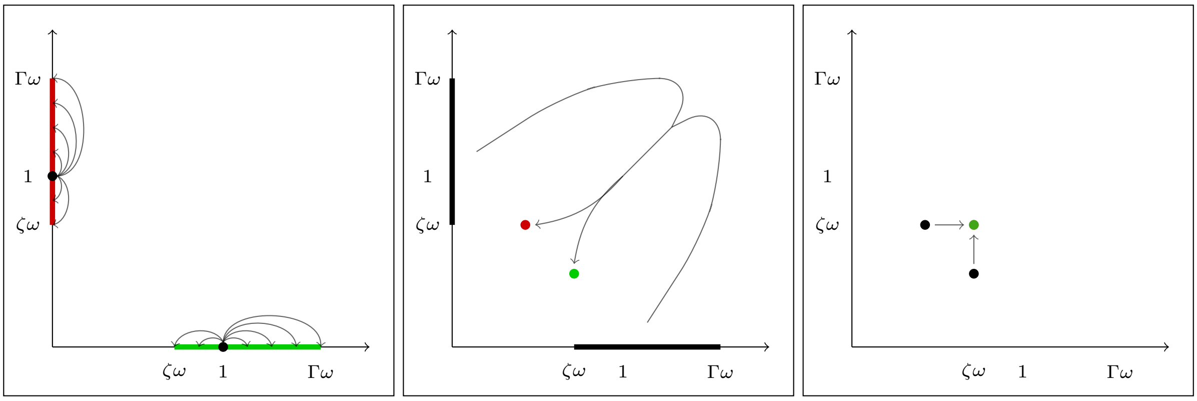


Figure C.1: Schematic representation of the game. The initial points are in black, the final points are colored in red if they are part of the horizontal ladder and in green of the vertical ladder. The arrows represents the idea of the movements of the points. a) Each point is split into many points (represented by a line) on their axes. b) The ladder combines the points on the axes into 2 points. c) The raises create the final point of the game.

We will consider a 3 step game:

Split: The point $[0,1]$ will be split into points on the vertical axis between the position $\zeta\omega$ and $\Gamma\omega$. (same treatment for $[1,0]$). See a) in Figure C.1.

Ladder of width k: This transition mixed the points on the axes and has two final points in position $[\zeta\omega - k\omega, \zeta\omega]$ and $[\zeta\omega, \zeta\omega - k\omega]$. See b) in Figure C.1.

Raises The two points are raised into a final point $[\zeta\omega, \zeta\omega]$. See c) in Figure C.1.

More formally the game will be:

$$\begin{aligned} \frac{1}{2}[0,1] + \frac{1}{2}[1,0] \quad &\overset{\text{split}}{\longrightarrow} \quad \sum_{j=\zeta}^{\Gamma} \text{split}(j)[0, j\omega] + \sum_{j=\zeta}^{\Gamma} \text{split}(j)[j\omega, 0] && \text{(C.2)} \\ &\overset{\text{ladder}}{\longrightarrow} \quad \frac{1}{2}[\zeta\omega - k\omega, \zeta\omega] + \frac{1}{2}[\zeta\omega, \zeta\omega - k\omega] && \text{(C.3)} \\ &\overset{\text{raises}}{\longrightarrow} \quad 1[\zeta\omega, \zeta\omega] \end{aligned}$$

C.2 Ladder

A *ladder of width k* is a repetitive pattern along the main diagonal for h and v, with $2k+1$ points on each level. A *rung* in the ladder, is the horizontal part of it, i.e. $\sum_x h(x,y)$ for some y. As previously discussed we will consider a symmetric ladder. Equation C.1 implies that there are no point on the main diagonal: $\forall z,\ h(z,z) = v(z,z) = 0$. If h is valid function, then v will be valid too. This is why we focus our attention on the horizontal part of the ladder.

The ladder have rungs from height $z^* = \zeta\omega$ to $\Gamma\omega$, each rung will have $2k$ points centered on the diagonal and one point on the y-axis. More formally for $\zeta < j_0 < \Gamma$, the x-axis coordinate of the points of the rung at height $j_0\omega$ are

$$\{0,\, (j_0 - k)\,\omega,\, (j_0 - k + 1)\,\omega, \ldots,\, (j_0 - 1)\omega,\, (j_0 + 1)\omega, \ldots, (j_0 + k - 1)\,\omega,\, (j_0 + k)\,\omega\}\,. \quad \text{(C.4)}$$

Some principles governing the ladder are represented in Figure C.2. First in a), we give a schematic representation of all the points defined in (C.4) that are the horizontal part of the ladder. The vertical part is constructed using the symmetry relation (C.1) we imposed. Both, the horizontal part and the vertical part of the ladder are represented in Figure b). All the points that are located on the overlap of the two parts of the ladder have total weight 0. There a then only a few remaining points: the initial points on the axes, the final points in $[\zeta\omega]$ and 4 “triangles”.

To choose the weight on the point of the ladder, we use the following lemma that is extremely useful to construct valid functions:

Lemma C.1 ([Moc07]) *Let $x_1, \ldots, x_{2k+1} \in \mathbb{R}_+$ be different points, $f \in \mathbb{R}[X]$ be a real polynomial such that:*

- *the absolute value of its leading coefficient is 1,*
- $\deg(f) \leq 2k - 1$,
- $\forall \lambda < 0,\ f(\lambda) > 0$,

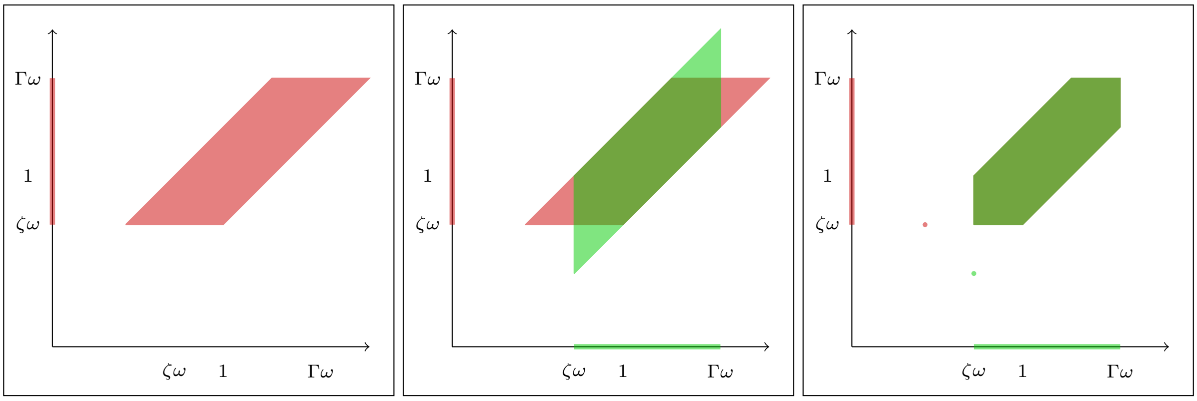


Figure C.2: Schematic construction of the ladder. a) The horizontal part of the ladder. b) Superposition of the horizontal part and the vertical part of the ladder. By symmetry, the sum of the weights of the point in the overlap is 0. Except the final points, the weights of the points in the 4 “triangle” with no overlap will be set to 0 by truncation. c) All the points actually involved in the ladder transition

then $\forall C > 0$ *the function* h_{rung} *defined by:*

$$h_{\text{rung}} = \sum_{i=1}^{2k+1} \frac{-C \cdot f(x_i)}{\prod_{j\neq i}(x_j - x_i)}\,[x_i] \tag{C.5}$$

is a valid function.

This is how we get rid of the 4 “triangles”. We use the previous lemma in order to put weights on the points in the ladder, except the one in the triangle, that is we impose the polynomial to be 0 on these points. There is then only on way (up to a constant C) to set up weights on the ladder, and the horizontal function is thus:

$$h_{\text{lad}} = \sum_{j=\zeta}^{\Gamma}\left(\frac{-C\cdot f(0,j\omega)}{\prod_{l=-k}^{k}[(j+l)\omega]}\,[0,j\omega] + \sum_{\substack{i=-k\\ i\neq 0}}^{k}\frac{C\cdot f((j+i)\,\omega,\, j\omega)}{((j+i)\omega)(j\omega)\prod_{\substack{l\neq i\\ l\neq 0}}[\omega(l-i)]}[(j+i)\omega,\ j\omega]\right), \tag{C.6}$$

where f is the polynomial defined by its zeros being on the points in the “triangles”:

$$f(x,y) = (-1)^{k+1}\prod_{i=1}^{k-1}(z^* - i\omega - x)\,(z^* - i\omega - y)\prod_{i=1}^{k}(\Gamma\omega + i\omega - x)\,(\Gamma\omega + i\omega - y)\,.$$

C.3 Splits

Notice that Equation (C.6) also defines the weight on the points of the splits:

$$\text{split}(j) = \frac{C\cdot f(0,j\omega)}{\prod_{l=-k}^{k}[(j+l)\omega]}.$$

The last remaining part is to check that the splits are valid. More precisely, we show that the ladder is high enough, and the steps ω small enough, the splits are strictly valid for all $z^* > \frac{k+1}{2k+1}$.

Lemma C.2 (The splits are strictly valid [Moc07]) *We can chose ω and Γ such that if $z^* > \frac{k+1}{2k+1}$, the functions*

$$h_{\text{split}} = \sum_{j=\zeta}^{\Gamma} \text{split}(j)[j\omega, 0] - \frac{1}{2}[1,0] \quad \text{and} \quad v_{\text{split}} = \sum_{j=\zeta}^{\Gamma} \text{split}(j)[0, j\omega] - \frac{1}{2}[0,1]$$

are strictly valid functions for

$$C = \frac{1}{2} \cdot \left(\sum_{j=\zeta}^{\Gamma} \frac{-f(0, j\omega)}{\prod\limits_{l=-k}^{k} \omega\,(j+l)} \right)^{-1}.$$

Bibliography

[Aar02] Scott Aaronson. Quantum lower bound for the collision problem. In *Proceedings of the 34th Annual ACM Symposium on Theory of Computing*, pages 635–642. ACM, 2002. arXiv:quant-ph/0111102, doi:10.1145/509907.509999. [1.4.3]

[Aar11] Scott Aaronson. A linear-optical proof that the permanent is #P-hard. In *Proceedings of the Royal Society A*. Royal Society Publishing, 2011. arXiv:1109.1674, doi:10.1098/rspa.2011.0232. [1.2.3]

[ABDR04] Andris Ambainis, Harry Buhrman, Yevgenity Dodis, and Hein Rörig. Multiparty quantum coin flipping. In *Proceedings of the 19th IEEE Annual Conference on Computational Complexity*, pages 250–259. IEEE Computer Society, 2004. arXiv:quant-ph/0304112, doi:10.1109/CCC.2004.19. [1.3.2, 4.1.2, 4.1.3]

[ACG$^+$11] Dorit Aharonov, André Chailloux, Maor Ganz, Iordanis Kerenidis, and Loïck Magnin. A simple(r) proof of existence of quantum weak coin flipping with arbitrarily small bias. In submission, 2011. [1.3.2]

[ACMT$^+$07] K. M. R. Audenaert, J. Calsamiglia, R. Muñoz-Tapia, E. Bagan, Ll. Masanes, Antonio Acín, and Frank Verstraete. Discriminating states: the quantum Chernoff bound. *Physical Review Letters*, 98(16):160501, 2007. arXiv:quant-ph/0610027, doi:10.1103/PhysRevLett.98.160501. [2.4]

[ACR$^+$10] Andris Ambainis, Andrew M. Childs, Ben W. Reichardt, Robert Špalek, and Shengyu Zhang. Any AND-OR formula of size N can be evaluated in time $N^{1/2+o(1)}$ on a quantum computer. *SIAM Journal on Computing*, 39(6):2513–2530, 2010. doi:10.1137/080712167. [1.4.2]

[Amb00] Andris Ambainis. Quantum lower bounds by quantum arguments. In *Proceedings of the 32nd Annual ACM Symposium on Theory of Computing*, pages 636–643. ACM, 2000. arXiv:quant-ph/0002066, doi:10.1145/335305.335394. [1.4.2]

[Amb04] Andris Ambainis. A new protocol and lower bounds for quantum coin flipping. *Journal of Computer and System Sciences*, 68:398–416, 2004. arXiv:quant-ph/0204022, doi:10.1016/j.jcss.2003.07.010. [1.3.2, 7.1]

[Amb05] Andris Ambainis. A new quantum lower bound method with an application to strong direct product theorem for quantum search. 2005. arXiv:quant-ph/0508200. [1.4.2, 1.4.5, 6.3]

[Amb06] Andris Ambainis. Polynomial degree vs. quantum query complexity. *Journal of Computer and System Sciences*, 72(2):220–238, 2006. arXiv:quant-ph/0305028, doi:10.1016/j.jcss.2005.06.006. [1.4.2, 1.4.3, 1.4.3, 1.2]

[Amb09] Andris Ambainis. Quantum algorithms for formula evaluation. Survey presented at the NATO Advanced Research Workshop on Quantum Cryptography and Computing: Theory and Implementation, 2009. arXiv:1006.3651. [1.1.3]

[AMRR11] Andris Ambainis, Loïck Magnin, Martin Roetteler, and Jérémie Roland. Symmetry-assisted adversaries for quantum state generation. In *Proceedings of the 26th Annual IEEE Conference on Computational Complexity*, pages 167–177, San Jose, CA, USA, 2011. IEEE Computer Society. arXiv:1012.2112, doi:10.1109/CCC.2011.24. [1.4.5]

[AS04] Scott Aaronson and Yaoyun Shi. Quantum lower bounds for the collision and the element distinctness problems. *Journal of the ACM*, 51(4):595–605, 2004. doi:10.1145/1008731.1008735. [1.4.3, 1.4.3, 1.2, 7.2]

[AŠdW07] Andris Ambainis, Robert Špalek, and Ronald de Wolf. A new quantum lower bound method with applications to direct product theorems and Time-Space tradeoffs. *Algorithmica*, 55(3):422–461, 2007. arXiv:quant-ph/0511200, doi:10.1007/s00453-007-9022-9. [1.4.2, 1.4.5, 6.2.1]

[AT03] Dorit Aharonov and Amnon Ta-Shma. Adiabatic quantum state generation and statistical zero knowledge. In *Proceedings of the 35th Annual ACM Symposium on Theory of Computing*, pages 20–29. ACM, 2003. arXiv:quant-ph/0301023, doi:10.1145/780542.780546. [1.4.4]

[ATSVY00] Dorit Aharonov, Amnon Ta-Shma, Umesh V. Vazirani, and Andrew C. Yao. Quantum bit escrow. In *Proceedings of the 32d annual ACM Symposium on Theory of Computing*, pages 705–714. ACM, 2000. arXiv:quant-ph/0004017, doi:10.1145/335305.335404. [1.3.2]

[Bai04] Rosemary Bailey. *Associations schemes: designed experiments, algebra, and combinatorics*, volume 84 of *Cambridge studies in advanced mathematics*. Cambridge University Press, 2004. [6.2.1]

[BB84] Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing*, page 175, 1984. Available from: http://www.research.ibm.com/people/b/bennetc/bennettc198469790513.pdf. [1.1.2, 1.3.1]

[BBBV97] Charles H. Bennett, Ethan Bernstein, Gilles Brassard, and Umesh Vazirani. Strengths and weaknesses of quantum computing. *SIAM Journal on Computing*, 26(5):1510–1523, 1997. arXiv:quant-ph/9701001, doi:10.1137/S0097539796300933. [1.4.2, 6.3]

[BBC$^+$01] Robert Beals, Harry Buhrman, Richard Cleve, Michele Mosca, and Ronald de Wolf. Quantum lower bounds by polynomials. *Journal of the ACM*, 48:778–797, 2001. arXiv:quant-ph/9802049, doi:10.1145/502090.502097. [1.4.3, 5.27, 5.6.4]

[BBCS92] Charles Bennett, Gilles Brassard, Claude Crépeau, and Marie-Hélène Skubiszewska. Practical quantum oblivious transfer. In *Proceedings of the 11th Annual International Cryptology Conference on Advances in Cryptology*, volume 576 of *Lecture Notes in Computer Science*, pages 351–366. Springer Berlin / Heidelberg, 1992. Available from: www.cs.mcgill.ca/~crepeau/PS/BBCS92.ps. [1.3.1]

[BCJL93] Gilles Brassard, Claude Crépeau, Richard Jozsa, and David Langlois. A quantum bit commitment scheme provably unbreakable by both parties. In *Proceeding of the 34th Annual IEEE Symphosium on Foundations of Computer Science*, pages 42–52, 1993. Available from: crypto.cs.mcgill.ca/~crepeau/COMP647/2007/TOPIC04/BCJL93.pdf, doi:10.1109/SFCS.1993.366851. [1.3.1]

[BCWdW01] Harry Buhrman, Richard Cleve, John Watrous, and Ronald de Wolf. Quantum fingerprinting. *Physical Review Letters*, 87:167902, 2001. arXiv:quant-ph/0102001, doi:10.1103/PhysRevLett.87.167902. [1.4.4]

[Bel64] John S. Bell. On the Einstein Podolsky Rosen paradox. *Physics*, 1(3):195–200, 1964. [1.1.1]

[Bha97] Rajendra Bhatia. *Matrix analysis*, volume 169 of *Graduate texts in mathematics*. Springer-Verlag, 1997. [4.22]

[BHK$^+$11] Gilles Brassard, Peter Høyer, Kassem Kalach, Marc Kaplan, Sophie Laplante, and Louis Salvail. Merkle puzzles in a quantum world. In *Proceedings of the 31st International Cryptology Conference*, volume 6841 of *Lecture Notes in Computer Science*, pages 391–410. Springer Berlin / Heidelberg, 2011. arXiv:1108.2316, doi:10.1007/978-3-642-22792-9_22. [1.4.5]

[Blu83] Manuel Blum. Coin flipping by telephone a protocol for solving impossible problems. *SIGACT News*, 15:23–27, 1983. doi:10.1145/1008908.1008911. [1.3.2]

[BR03] Alonso Botero and Benni Reznik. Modewise entanglement of Gaussian states. *Physical Review A*, 67(5):052311, 2003. arXiv:quant-ph/0209026, doi:10.1103/PhysRevA.67.052311. [2.3.3]

[Bra05] Gilles Brassard. Is information the key? *Nature Physics*, 1(1):2–4, 2005. arXiv:10.1038/nphys134. [3.3]

[BS02] Stephen D. Bartlett and Barry C. Sanders. Efficient classical simulation of optical quantum information circuits. *Physical Review Letters*, 89:207903, 2002. doi:10.1103/PhysRevLett.89.207903. [1.2.1]

[BS04] Howard Barnum and Michael Saks. A lower bound on the quantum query complexity of read-once functions. *Journal of Computer and System Sciences*, 69(2):244–258, 2004. arXiv:quant-ph/0201007, doi:10.1016/j.jcss.2004.02.002. [1.4.2]

[BSBN02] Stephen D. Bartlett, Barry C. Sanders, Samuel L. Braunstein, and Kae Nemoto. Efficient classical simulation of continuous variable quantum information processes. *Physical Review Letters*, 88(9):097904, 2002. arXiv:quant-ph/0109047, doi:10.1103/PhysRevLett.88.097904. [1.2.1]

[BV97] Ethan. Bernstein and Umesh V. Vazirani. Quantum complexity theory. *SIAM Journal on Computing*, 26(5):1411–1473, 1997. Available from: www.cs.berkeley.edu/~vazirani/pubs/bv.ps, doi:10.1137/S0097539796300921. [1.2.3]

[BvL05] Samuel L. Braunstein and Peter van Loock. Quantum information with continuous variables. *Reviews of Modern Physics*, 77:513–577, 2005. arXiv:quant-ph/0410100, doi:10.1103/RevModPhys.77.513. [1.2.1]

[Cam99] Peter James Cameron. *Permutation Groups*, volume 45 of *London Mathematical Society Student Texts*. Cambridge University Press, 1999. [6.2.1]

[CBH03] Rob Clifton, Jeffrey Bub, and Halvorson Hans. Characterizing quantum theory in terms of information-theoretic constraints. *Found. Phys*, 33(11):1561–1591, 2003. arXiv:quant-ph/0211089, doi:10.1023/A:1026056716397. [3.3]

[CEMM98] Richard Cleeve, Artur Ekert, Chiara Macchiavello, and Michele Mosca. Quantum algorithms revisited. In *Proceedings of the Royal Society A*, volume 454, pages 339–354, 1998. arXiv:quant-ph/9708016, doi:10.1098/rspa.1998.0164. [1.2.3]

[Cha87] David Chaum. Demonstrating that a public predicate can be satisfied without revealing any information about how. In *Proceedings on Advances in cryptology*, pages 195–199. Springer-Verlag, 1987. Available from: http://crypto.cs.mcgill.ca/~crepeau/COMP647/2007/TOPIC05/Chaum.pdf. [1.3.1]

[CK09] André Chailloux and Iordanis Kerenidis. Optimal quantum strong coin flipping. In *Proceeding of the 44th Annual IEEE Symposium on Foundations of Computer Science*, pages 527–533. IEEE Computer Society, 2009. arXiv:arXiv:0904.1511, doi:10.1109/FOCS.2009.71. [1.3.2, 4.2.4]

[CK11] André Chailloux and Iordanis Kerenidis. Optimal bounds for quantum bit commitment. In *Proceedings of the 52nd Annual IEEE Symposium on Foundations of Computer Science*. IEEE Computer Society, 2011. arXiv:1102.1678. [1.3.1]

[CLP07] Nicolas J. Cerf, Gerd Leuchs, and Eugene S. Polzik, editors. *Quantum information with continuous variables of atoms and light*. Imperial College Press, 2007. [1.2.1]

[CLVA01] Nicolas J. Cerf, Marc Lévy, and Gilles Van Assche. Quantum distribution of gaussian keys using squeezed states. *Physical Review A*, 63:052311, 2001. arXiv:quant-ph/0008058, doi:10.1103/PhysRevA.63.052311. [1.2.1]

[DdW11] Andrew Drucker and Ronald de Wolf. *Quantum Proofs for Classical Theorems*. Number 2 in Graduate Surveys. Theory of Computing Library, 2011. doi:10.4086/toc.gs.2011.002. [1.2.3]

[Deu85] David Deutsch. Quantum theory, the Church-Turing principle and the universal quantum computer. In *Proceedings of the Royal Society A*, volume 400, pages 97–117, 1985. Available from: http://www.cs.berkeley.edu/~christos/classics/Deutsch_quantum_theory.pdf, doi:10.1098/rspa.1985.0070. [1.2.3]

[DFSS08] Ivan B. Damgård, Serge Fehr, Louis Salvail, and Christian Schaffner. Cryptography in the bounded quantum-storage model. *SIAM J. Comput.*, 37(6):1865–1890, 2008. arXiv:quant-ph/0508222, doi:10.1109/SFCS.2005.30. [7.1]

[DJ92] David Deutsch and Richard Jozsa. Rapid solution of problems by quantum computation. In *Mathematical and Physical Sciences*, volume 439, pages 553–558. The Royal Society, 1992. doi:10.1098/rspa.1992.0167. [1.2.3]

[DKSW07] Giacomo Mauro D'Ariano, Dennis Kretschmann, Dirk Schlingemann, and Reinhard F. Werner. Reexamination of quantum bit commitment: The possible and the impossible. *Physical Review A*, 76:032328, 2007. arXiv:quant-ph/0605224, doi:10.1103/PhysRevA.76.032328. [1.3.1]

[DR09] Asen L. Dontchev and R. Tyrrell Rockafellar. *Implicit functions and solution mappings: a view from variational analysis.* Springer Monographs in Mathematics. Springer, 2009. [4.15]

[Dru11] Andrew Drucker. Improved direct product theorems for randomized query complexity. In *Proceedings of the 26th Annual IEEE Conference on Computation Complexity*, pages 1–11. IEEE Computer Society, 2011. arXiv:1005.0644, doi:10.1109/CCC.2011.29. [1.4.1]

[dW08] Ronald de Wolf. *A Brief Introduction to Fourier Analysis on the Boolean Cube.* Number 1 in Graduate Surveys. Theory of Computing Library, 2008. doi:10.4086/toc.gs.2008.001. [5.6.4, 5.6.4]

[Eke91] Artur K. Ekert. Quantum cryptography based on Bell's theorem. *Physical Review Letters*, 67:661–663, 1991. doi:10.1103/PhysRevLett.67.661. [1.1.2]

[EPR35] Albert Einstein, Boris Podolsky, and Nathan Rosen. Can quantum-mechanical description of physical reality be considered complete? *Physical Review*, 47:777–780, 1935. doi:10.1103/PhysRev.47.777. [1.1.1]

[Fey82] Richard Feynman. Simulating physics with computers. *International Journal of Theoretical Physics*, 21:467–488, 1982. doi:10.1007/BF02650179. [1.1]

[FGG08] Edward Farhi, Jeffrey Goldstone, and Sam Gutmann. A quantum algorithm for the Hamiltonian NAND tree. *Theory of Computing*, 4(1):169–190, 2008. arXiv:quant-ph/0702144, doi:10.4086/toc.2008.v004a008. [1.1.3, 1.4.2]

[FGH$^+$10] Edward Farhi, David Gosset, Avinatan Hassidim, Andrew Lutomirski, and Peter W. Shor. Quantum money from knots. Technical Report MIT-CTP-4146, Massachusetts Institute of Technology, 2010. arXiv:1004.5127. [7.2]

[Fiu01] Jaromír Fiurášek. Optical implementation of continuous-variable quantum cloning machines. *Physical Review Letters*, 86(21):4942–4945, 2001. arXiv:quant-ph/0012048, doi:10.1103/PhysRevLett.86.4942. [2.3.3]

[Fuc96] Christopher Alexander Fuchs. *Distinguishability and Accessible Information in Quantum Theory*. PhD thesis, University of New Mexico, 1996. arXiv:quant-ph/9601020. [2.4]

[Fuc01] Christopher Alexander Fuchs. Notes on a Paulian idea: Foundations, historical, anecdotal and forward-looking thoughts on the quantum. 2001. arXiv:quant-ph/0105039. [3.3]

[Fuc02] Christopher Alexander Fuchs. Quantum mechanics as quantum information (and only a little more). 2002. arXiv:quant-ph/0205039. [3.3]

[GG02] Frédéric Grosshans and Philippe Grangier. Continuous variable quantum cryptography using coherent states. *Physical Review Letters*, 88(5):057902, 2002. doi:10.1103/PhysRevLett.88.057902. [1.2.1]

[GKP01] Daniel Gottesman, Alexei Kitaev, and John Preskill. Encoding a qubit in an oscillator. *Physical Review A*, 64(012310), 2001. doi:10.1103/PhysRevA.64.012310. [2.2]

[GLLL$^+$11] Ilja Gerhardt, Qin Liu, Antia Lamas-Linares, Johannes Skaar, Christian Kurtsiefer, and Vadim Makarov. Perfect eavesdropping on a quantum cryptography system. *Nature Communication*, 2:349, 2011. arXiv:1011.0105, doi:10.1038/ncomms1348. [1.2.1]

[GPS07] Raúl García-Patrón Sanchez. *Quantum Information with Optical Continuous Variables: from Bell Tests to Key Distribution*. PhD thesis, Université Libre de Bruxelles, 2007. [1.2.1, A.1]

[Gro96] Lov K. Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the 28th Annual ACM Symposium on Theory of Computing*, pages 212–219. ACM, 1996. arXiv:quant-ph/9605043, doi:10.1145/237814.237866. [1.1.3, 6.3]

[Hil00] Mark Hillery. Quantum cryptography with squeezed states. *Physical Review A*, 61:022309, 2000. arXiv:quant-ph/9909006, doi:10.1103/PhysRevA.61.022309. [1.2.1]

[HLŠ07] Peter Høyer, Troy Lee, and Robert Špalek. Negative weights make adversaries stronger. In *Proceedings of the 39th Annual ACM Symposium on Theory of Computing*, pages 526–535. ACM, 2007. doi:10.1145/1250790.1250867. [1.4.2, 1.4.5, 1.2, 1.4.5, 5.3.1]

[HMR$^+$06] Sean Hallgren, Cristopher Moore, Martin Rötteler, Alexander Russell, and Pranab Sen. Limitations of quantum coset states for graph isomorphism. In *Proceedings of the 38th Annual ACM Symposium on Theory of Computing*, pages 604–617. ACM, 2006. arXiv:quant-ph/0511148, doi:10.1145/1132516.1132603. [1.4.4]

[HNS08] Peter Høyer, Jan Neerbek, and Yaoyun Shi. Quantum complexities of ordered searching, sorting, and element distinctness. *Algorithmica*, 34(4):429–448, 2008. arXiv:quant-ph/0102078, doi:10.1007/s00453-002-0976-3. [1.4.2]

[Joz94] Richard Jozsa. Fidelity for mixed quantum states. *Journal of Modern Optics*, 41:2315–2324, 1994. doi:10.1080/09500349414552171. [2.4, 2.4]

[Joz98] Richard Jozsa. Quantum algorithms and the Fourier transform. In *Proceedings of the Royal Society A*, volume 454, pages 323 – 337. Royal Society Publishing, 1998. arXiv:quant-ph/9707033, doi:10.1098/rspa.1998.0163. [1.2.3]

[Kai67] T. Kailath. The divergence and Bhattacharyya distance measures in signal selection. *IEEE Transactions on Communication Technology*, 15(1):52–60, 1967. doi:10.1109/TCOM.1967.1089532. [2.4]

[Ken99] Adrian Kent. Unconditional secure bit commitment. *Physical Review Letters*, 83(7):1447–1450, 1999. arXiv:quant-ph/9810068, doi:10.1103/PhysRevLett.83.1447. [1.3.1]

[Ken11] Adrian Kent. Unconditionally secure bit commitment by transmitting measurement outcomes. 2011. arXiv:1108.2879. [1.3.1]

[Kit03] Alexei Kitaev. Quantum coin-flipping. Talk at the 6th workshop on Quantum Information Processing, 2003. [1.3.2, 4.1.2, 4.1.3]

[KN04] Iordanis Kerenidis and Ashwin Nayak. Weak coin flipping with small bias. *Information Processing Letters*, 89(3):131 – 135, 2004. arXiv:quant-ph/0206121, doi:10.1016/j.ipl.2003.07.007. [1.3.2]

[KNP07] Pascal Koiran, Vincent Nesme, and Natacha Portier. The quantum query complexity of the Abelian hidden subgroup problem. *Theoretical Computer Science*, 380(1-2):115 – 126, 2007. doi:10.1016/j.tcs.2007.02.057. [1.4.3]

[KŠdW07] Hartmut Klauck, Robert Špalek, and Ronald de Wolf. Quantum and classical strong direct product theorems and optimal time-space tradeoffs. *SIAM Journal on Computing*, 36(5):1472–1493, 2007. arXiv:quant-ph/0402123, doi:10.1137/05063235X. [1.4.3]

[KW09] Robert König and Stephanie Wehner. A strong converse for classical channel coding using entangled inputs. *Physical Review Letters*, 103:070504, 2009. arXiv:0903.2838, doi:10.1103/PhysRevLett.103.070504. [7.1]

[Lan92] R. Landauer. Information is physical. In *Proceedings of the workshop on Physics and Computation*, pages 1 – 4, 1992. doi:10.1109/PHYCMP.1992.615478. [3.3]

[LB99] Seth Lloyd and Samuel L. Braunstein. Quantum computation over continuous variables. *Physical Review Letters*, 82(8):1784–1787, 1999. arXiv:quant-ph/9810082, doi:10.1103/PhysRevLett.82.1784. [7.1]

[LC97] Hoi-Kwong Lo and H. F. Chau. Is quantum bit commitment really possible? *Physical Review Letters*, 78(17):3410–3413, 1997. arXiv:quant-ph/9603004, doi:10.1103/PhysRevLett.78.3410. [1.3.1, 3.2]

[LC98] Hoi-Kwong Lo and H.F. Chau. Why quantum bit commitment and ideal quantum coin tossing are impossible. *Physica D: Nonlinear Phenomena*, 120:177 – 187, 1998. arXiv:quant-ph/9711065, doi:10.1016/S0167-2789(98)00053-0. [1.3.2]

[LM08] Sophie Laplante and Frédéric Magniez. Lower bounds for randomized and quantum query complexity using Kolmogorov arguments. *SIAM Journal on Computing*, 38(1):46–62, 2008. arXiv:quant-ph/0311189, doi:10.1137/050639090. [1.4.2]

[LMR$^+$11] Troy Lee, Rajat Mittal, Ben W. Reichardt, Robert Špalek, and Mario Szegedy. Quantum query complexity of state conversion. In *Proceedings of the 52nd Annual IEEE Symposium on Foundations of Computer Science*. IEEE Computer Society, 2011. To appear. arXiv:1011.3020. [1.4.2, 1.2, 1.4.5]

[LR11] Troy Lee and Jérémie Roland. A strong direct product theorem for quantum query complexity. 2011. arXiv:1104.4468. [1.4.1, 1.4.5, 5.24, 5.25, 5.32, 6.1, 7.2]

[Lut11] Andrew Lutomirski. Component mixers and a hardness result for counterfeiting quantum money. Technical Report MIT-CTP 4279, Massachusetts Institute of Technology, 2011. arXiv:1107.0321. [7.2]

[Mag06] Loïck Magnin. Cryptographie avec des variables continues. Master's thesis, École Normale Supérieure de Lyon, 2006. [1.2.1]

[Mag07] Loïck Magnin. Mise en gage quantique avec des variables continues. Master's thesis, École Normale Supérieure de Lyon, 2007. [1.3.1]

[May97] Dominic Mayers. Unconditionally secure quantum bit commitment is impossible. *Physical Review Letters*, 78:3414, 1997. arXiv:quant-ph/9605044v2, doi:10.1103/PhysRevLett.78.3414. [1.3.1, 3.2]

[MC11] Aikatarini Mandilara and Nicolas J. Cerf. Quantum bit commitment under Gaussian constraints. 2011. arXiv:1105.2140. [7.1]

[Mid04] Gatis Midrijānis. A polynomial quantum query lower bound for the set equality problem. In Josep Diaz, Juhani Karhumäki, Arto Lepistö, and Donald Sannella, editors, *Automata, Languages and Programming*, volume 3142 of *Lecture Notes in Computer Science*, pages 29–41. Springer Berlin / Heidelberg, 2004. arXiv:quant-ph/0401073, doi:10.1007/978-3-540-27836-8_83. [1.4.5]

[MM07] Paulina Marian and Tudor A. Marian. Optimal purifications and fidelity for displaced thermal states. *Physical Review A*, 76(5):054307, 2007. arXiv:0706.3204, doi:10.1103/PhysRevA.76.054307. [3.2.2]

[MMLC10] Loïck Magnin, Frédéric Magniez, Anthony Leverrier, and Nicolas J. Cerf. Strong no-go theorem for Gaussian quantum bit commitment. *Physical Review A*, 81:010302, 2010. arXiv:0905.3419, doi:10.1103/PhysRevA.81.010302. [1.3.1]

[Moc05] Carlos Mochon. Large family of quantum weak coin-flipping protocols. *Physical Review A*, 72:022341, 2005. arXiv:quant-ph/0502068, doi:10.1103/PhysRevA.72.022341. [1.3.2]

[Moc07] Carlos Mochon. Quantum weak coin flipping with arbitrary small bias. 2007. arXiv:quantum-ph/0711.4114. [1.3.2, 1.3.2, 4, C, C.1, C.2]

[MR11] Loïck Magnin and Jérémie Roland. Quantum adversary lower bounds by polynomials. Technical Report 2011-TR080, NEC Laboratories America, 2011. [1.4.5]

[Nao91] Moni Naor. Bit commitment using pseudorandomness. *Journal of Cryptology*, 4(2):151–158, 1991. Available from: http://crypto.cs.mcgill.ca/~crepeau/COMP647/2007/TOPIC06/Naor-bit.pdf, doi:10.1007/BF00196774. [1.3.1]

[NC04] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge Series on Information and the Natural Sciences. Cambridge University Press, 1st edition, 2004. [2.4]

[NS03] Ashwin Nayak and Peter W. Shor. Bit-commitment-based quantum coin flipping. *Physical Review A*, 67:012304, 2003. arXiv:quant-ph/0206123, doi:10.1103/PhysRevA.67.012304. [1.3.2]

[Phi03] Pierre Phillips. Bornes inférieures en calcul quantique: Méthode par adversaire vs. méthode des polynômes. Master's thesis, École Normale Supérieure de Lyon, 2003. Available from: http://www.lri.fr/~magniez/PAPIERS/philipps03.ps.gz. [1.4.3]

[PL08] Stefano Pirandola and Seth Lloyd. Computable bounds for the discrimination of Gaussian states. *Physical Review A*, 78(01):012331, 2008. arXiv:0806.1625, doi:10.1103/PhysRevA.78.012331. [2.4]

[Rab80] Michael O. Rabin. Probabilistic algorithm for testing primality. *Journal of Number Theory*, 12(1):128 – 138, 1980. doi:10.1016/0022-314X(80)90084-0. [1.1.1]

[Ral99] Tim C. Ralph. Continuous variable quantum cryptography. *Physical Review A*, 61:010303, 1999. arXiv:quant-ph/9907073, doi:10.1103/PhysRevA.61.010303. [1.2.1]

[RC09] Renato Renner and J. Ignacio Cirac. A de Finetti representation theorem for infinite dimensional quantum systems and applications to quantum cryptography. *Physical Review Letters*, 102(11):110504, 2009. arXiv:0809.2243, doi:10.1103/PhysRevLett.102.110504. [1.2.1, 3.3]

[Rei00] Margaret D. Reid. Quantum cryptography with a predetermined key, using continuous-variable Einstein-Podolsky-Rosen correlations. *Physical Review A*, 62:062308, 2000. Available from: http://link.aps.org/doi/10.1103/PhysRevA.62.062308, arXiv:quant-ph/9909030, doi:10.1103/PhysRevA.62.062308. [1.2.1]

[Rei11] Ben W. Reichardt. Reflections for quantum query algorithms. In *Proceedings of the 22nd ACM-SIAM Symposium on Discrete Algorithms*, pages 560–569, 2011. arXiv:1005.1601. [1.4.2, 1.2]

[Ren05] Renato Renner. *Security of Quantum Key Distribution*. PhD thesis, ITH Zurich, 2005. arXiv:quant-ph/0512258. [1.1.2]

[RŠ08] Ben W. Reichardt and Robert Špalek. Span-program-based quantum algorithm for evaluating formulas. In *Proceedings of the 40th Annual ACM Symposium on Theory of Computing*, pages 103–112. ACM, 2008. arXiv:0710.2630, doi:10.1145/1374376.1374394. [1.4.2]

[Sag01] Bruce E. Sagan. *The Symmetric Group Representations, Combinatorial Algorithms, and Symmetric Functions*, volume 203 of *Graduate texts in mathematics*. Springer-Verlag, 2 edition, 2001. [6.12, 6.4.2, 6.4.2]

[SBPC$^+$09] Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J. Cerf, Miloslav Dušek, Norbert Lütkenhaus, and Momtchil Peev. The security of practical quantum key distribution. *Reviews of Modern Physics*, 81:1301–1350, 2009. arXiv:0802.4155, doi:10.1103/RevModPhys.81.1301. [1.1.2]

[Sch07] Christian Schaffner. *Cryptography in the Bounded Quantum-Storage Model*. PhD thesis, University of Arhus, 2007. [1.3.1]

[SCS99] R. Simon, S. Chaturvedi, and V. Srinivassan. Congruences and canonical forms for a positive matrix: Application to the schweinler-wigner extremum principle. *J. Math. Phys*, 40:3632–3642, 1999. arXiv:math-ph/9811003, doi:10.1063/1.532913. [2.27]

[Ser77] Jean-Pierre Serre. *Linear Representations of Finite Groups*, volume 42 of *Graduate texts in mathematics*. Springer-Verlag, 1977. [6.2.2, 6.2.2]

[She11] Alexander A. Sherstov. Strong direct product theorems for quantum communication and query complexity. In *Proceedings of the 43rd Annual ACM Symposium on Theory of Computing*, pages 41–50. ACM, 2011. arXiv:1011.4935, doi:10.1145/1993636.1993643. [1.4.1, 1.4.3]

[Shi02] Yaoyun Shi. Quantum lower bounds for the collision and the element distinctness problems. In *Proceedings of the 43rd Annual IEEE Symposium on Foundations of Computer Science*, pages 513–519. IEEE Computer Society, 2002. The Index Erasure problem is introduced in the arXiv version only. arXiv:quant-ph/0112086, doi:10.1109/SFCS.2002.1181975. [1.4.3, 1.4.5, 6.4]

[Sho94] Peter W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings of the 35th Annual IEEE Symposium on Foundations of Computer Science*, pages 124 –134. IEEE Computer Society, 1994. arXiv:quant-ph/9508027, doi:10.1109/SFCS.1994.365700. [1.1.3]

[Sim97] Daniel R. Simon. On the power of quantum computation. *SIAM Journal on Computing*, 26:1474–1483, 1997. doi:10.1137/S0097539796298637. [1.2.3]

[Sim00] R. Simon. Peres-horodecki separability criterion for continuous variable systems. *Physical Review Letters*, 84:2726–2729, 2000. arXiv:quant-ph/9909044, doi:10.1103/PhysRevLett.84.2726. [3.1]

[SMGPSC07] Jimmy Sudjana, Loïck Magnin, Raúl García-Patrón Sanchez, and Nicolas J. Cerf. Tight bounds on the eavesdropping of a continuous-variable quantum cryptographic protocol with no basis switching. *Physical Review A*, 76(5):052301, 2007. arXiv:quant-ph/0706.4283, doi:10.1103/PhysRevA.76.052301. [1.2.1]

[Smo05] John A. Smolin. Can quantum cryptography imply quantum mechanics? *Journal on Quantum Information and Computation*, 05(2):161–169, 2005. arXiv:quant-ph/0310067. [3.3]

[SP00] Peter W. Shor and John Preskill. Simple proof of security of the BB84 quantum key distribution protocol. *Physical Review Letters*, 85:441–444, 2000. arXiv:quant-ph/0003004, doi:10.1103/PhysRevLett.85.441. [1.1.2]

[Špa08] Robert Špalek. The multiplicative quantum adversary. In *Proceedings of the 23rd Annual IEEE Conference on Computational Complexity*, pages 237–248. IEEE Computer Society, 2008. arXiv:quant-ph/0703237, doi:10.1109/CCC.2008.9. [1.4.2, 1.4.5, 1.4.5, 1.4.5, 5.3.2, 6.1, 6.1, 6.2.1, 6.3]

[Spe07] Robert W. Spekkens. Evidence for the epistemic view of quantum states: A toy theory. *Physical Review A*, 75(3):032110, 2007. arXiv:quant-ph/0401052, doi:10.1103/PhysRevA.75.032110. [3.3]

[SR01] R. W. Spekkens and Terry Rudolph. Degrees of concealments and bindingness in quantum bit commitment protocols. *Physical Review A*, 65(01):012310, 2001. arXiv:quant-ph/0106019, doi:10.1103/PhysRevA.65.012310. [1.3.2]

[SR02] R. W. Spekkens and Terry Rudolph. Quantum protocol for cheat-sensitive weak coin flipping. *Physical Review Letters*, 89:227901, 2002. arXiv:quant-ph/0202118, doi:10.1103/PhysRevLett.89.227901. [1.3.2]

[ŠS06] Robert Špalek and Mario Szegedy. All quantum adversary methods are equivalent. *Theory of Computing*, 2(1):1–18, 2006. Available from: http://www.theoryofcomputing.org/articles/v002a001, doi:10.4086/toc.2006.v002a001. [1.4.2, 1.2]

[SW86] Michael Saks and Avi Wigderson. Probabilistic boolean decision trees and the complexity of evaluating game trees. In *Proceedings of the 27th Annual Symposium on Foundations of Computer Science*, pages 29–38, 1986. Available from: www.math.ias.edu/~avi/PUBLICATIONS/MYPAPERS/SW86/SW86.pdf, doi:10.1109/SFCS.1986.44. [1.1.3]

[Uhl76] Armin Uhlmann. The "transition probability" in the state space of a $*$-algebra. *Reports on Mathematical Physics*, 9:273–279, 1976. Available from: http://www.physik.uni-leipzig.de/~uhlmann/PDF/Uh76a.pdf. [2.4, 2.4]

[Val79] Leslie G. Valiant. The complexity of computing the permanent. *Theoretical Computer Science*, 8(2):189 – 201, 1979. doi:10.1016/0304-3975(79)90044-6. [1.2.3]

[Wie83] Stephen Wiesner. Conjugate coding. *SIGACT News*, 15:78–88, 1983. doi:10.1145/1008908.1008920. [1.1]

[WLB$^+$04] Christian Weedbrook, Andrew M. Lance, Warwick P. Bowen, Thomas Symul, Timothy C. Ralph, and Ping Koy Lam. Quantum cryptography without switching. *Physical Review Letters*, 93:170504, 2004. doi:10.1103/PhysRevLett.93.170504. [1.2.1]

[WST08] Stephanie Wehner, Christian Schaffner, and Barbara M. Terhal. Cryptography from noisy storage. *Physical Review Letters*, 100:220502, 2008. arXiv:0711.2895, doi:10.1103/PhysRevLett.100.220502. [1.3.1, 7.1]

[WW08] Stephanie Wehner and Jürg Wullschleger. Composable security in the bounded-quantum-storage model. In *Proceedings of the 35th International Colloquium on Automata, Languages and Programming*, pages 604–615. Springer-Verlag, 2008. arXiv:0709.0492, doi:10.1007/978-3-540-70583-3_49. [7.1]

[Yao82] Andrew C. Yao. Protocols for secure computations. In *Proceedings of the 23rd Annual Symposium on Foundations of Computer Science*, pages 160–164. IEEE Computer Society, 1982. Available from: http://www.cs.wisc.edu/areas/sec/yao1982-ocr.pdf, doi:10.1109/SFCS.1982.88. [1.2.2]

[Yue00] Horace P. Yuen. Unconditionally secure quantum bit commitment is possible. 2000. arXiv:quantum-ph/0006109v7. [1.3.1]

[Zha05] Shengyu Zhang. On the power of Ambainis lower bounds. *Theoretical Computer Science*, 339(2):241–256, 2005. arXiv:quant-ph/0311060, doi:10.1016/j.tcs.2005.01.019. [1.4.2, 1.2]