ULB
Université Libre de Bruxelles

Faculté des Sciences Appliquées
Théorie de l'Information et des
Communications

Adiabatic Quantum Computation

Promoteur de thèse :
Nicolas CERF

Année Académique 2003–2004

Thèse présentée par
Jérémie ROLAND
en vue de l'obtention du grade
de Docteur en Sciences Appliquées

Résumé

Le développement de la Théorie du Calcul Quantique provient de l'idée qu'un ordinateur est avant tout un système physique, de sorte que ce sont les lois de la Nature elles-mêmes qui constituent une limite ultime sur ce qui peut être calculé ou non. L'intérêt pour cette discipline fut stimulé par la découverte par Peter Shor d'un algorithme quantique rapide pour factoriser un nombre, alors qu'actuellement un tel algorithme n'est pas connu en Théorie du Calcul Classique. Un autre résultat important fut la construction par Lov Grover d'un algorithme capable de retrouver un élément dans une base de donnée non-structurée avec un gain de complexité quadratique par rapport à tout algorithme classique.

Alors que ces algorithmes quantiques sont exprimés dans le modèle "standard" du Calcul Quantique, où le registre évolue de manière discrète dans le temps sous l'application successive de portes quantiques, un nouveau type d'algorithme a été récemment introduit, où le registre évolue continûment dans le temps sous l'action d'un Hamiltonien. Ainsi, l'idée à la base du Calcul Quantique Adiabatique, proposée par Edward Farhi et ses collaborateurs, est d'utiliser un outil traditionnel de la Mécanique Quantique, à savoir le Théorème Adiabatique, pour concevoir des algorithmes quantiques où le registre évolue sous l'influence d'un Hamiltonien variant très lentement, assurant une évolution adiabatique du système.

Dans cette thèse, nous montrons tout d'abord comment reproduire le gain quadratique de l'algorithme de Grover au moyen d'un algorithme quantique adiabatique. Ensuite, nous montrons qu'il est possible de traduire ce nouvel algorithme adiabatique, ainsi qu'un autre algorithme de recherche à évolution Hamiltonienne, dans le formalisme des circuits quantiques, de sorte que l'on obtient ainsi trois algorithmes quantiques de recherche très proches dans leur principe.

Par la suite, nous utilisons ces résultats pour construire un algorithme adiabatique pour résoudre des problèmes avec structure, utilisant une technique, dite de "nesting", développée auparavant dans le cadre d'algorithmes quantiques de type circuit.

Enfin, nous analysons la résistance au bruit de ces algorithmes adiabatiques, en introduisant un modèle de bruit utilisant la théorie des matrices aléatoires et en étudiant son effet par la théorie des perturbations.

Remerciements

Je tiens à exprimer ma profonde gratitude pour mon promoteur Nicolas Cerf, tout d'abord pour m'avoir fait découvrir ce domaine de recherche passionnant qu'est la Théorie de l'Information Quantique, mais aussi pour tous ses conseils, ses idées et son support sans lesquels cette thèse n'aurait pas été possible. Je le remercie également pour l'excellent environnement de travail qu'il a bâti au fil des années dans son service, rassemblant une équipe de chercheurs aussi sympathique que dynamique.

Je remercie également Serge Massar pour ses idées souvent fructueuses, ce fut un réel plaisir de collaborer avec lui ainsi qu'avec Stefano Pironio sur les Inégalités de Bell.

Je voudrais également remercier tous mes collègues, à commencer par Louis Lamoureux pour m'avoir changé les idées tous les jours avec son inégalable "humour canadien" et Sofyan Iblisdir avec qui j'espère encore avoir le plaisir de travailler, ne fut-ce que pour terminer cet article mis en veille depuis plus d'un an, sans oublier tous les autres, Gilles Van Assche, Jonathan Barrett, Jaromír Fiurásĕk, Raúl García-Patrón Sánchez, Anne-Cécile Muffat, Patrick Navez et Kim-Chi Nguyen.

Je tiens également à remercier tous mes amis, en particulier les courageux qui m'ont aidé en relisant cette thèse, ou du moins qui ont eu l'intention de le faire. Enfin, je remercie chaleureusement ma mère, mon père, ma soeur et Marie-Laure car, même si le sujet de cette thèse leur paraît assez obscur, ils y sont pour beaucoup dans sa réalisation.

Preface

This thesis is the result of four years of research at the Centre for Quantum Information and Communication of the Université Libre de Bruxelles, under the supervision of Nicolas Cerf. The original goal of my PhD was to study how quantum algorithms could efficiently solve NP-complete problems.

After spending a few months getting familiar with the subject, my original goal rapidly proved to be too ambitious. However, this preliminary phase to my research gave me the opportunity to read interesting literature, among which one particular article that caught my attention. In the latter, Farhi, Gutmann, Goldstone and Sipser proposed a new type of quantum algorithm to deal with NP-complete problems using an adiabatic evolution. While they could only give a numerical analysis of the running time of their algorithm when treating NP-complete problems, they were able to give an analytical result for some other problems, such as the search in an unstructured database for which Grover had discovered a remarkable quantum algorithm with a complexity of order $O(\sqrt{N})$, that is a quadratic speed-up with respect to any classical algorithm. However, the adiabatic algorithm proposed by Farhi *et al* required a running time of order $O(N)$ to solve Grover's problem, thus showing no quadratic speed-up.

My first important breakthrough was to show how to achieve the quadratic speed-up of Grover's algorithm using an adiabatic quantum algorithm. Following this first step, I continued working on Adiabatic Quantum Computation until the end of my PhD as the subject proved to be very rich. Nonetheless, I was still interested in other subjects of Quantum Information Theory, such as the test of non-locality via Bell Inequalities or the optimal estimation of quantum states. While these subjects of research are rather independent from the main theme of this thesis, I did not want to simply overlook them and I decided to enclose them as appendices. More precisely, the outline of this work will be structured as follows.

In Chapter 1, I give a brief review of Classical and Quantum Computation models. This subject is extensively covered by an excellent literature and while I do not make an exhaustive list of references all along the text, I refer the interested reader to Nielsen and Chuang's book [NC00] or John Preskill's lecture notes [Pre98], as well as to different review articles by Andrew Steane [Ste98], Peter Shor [Sho00], or Artur Ekert and Richard Jozsa [EJ96].

Chapter 2 describes the celebrated quantum algorithm for searching in a unstructured database discovered by Lov K. Grover [Gro96], and its "analog analogue", a Hamiltonian-based algorithm proposed by Edward Farhi and Sam Gutmann [FG98a].

Chapter 3 deals with the Adiabatic Theorem that lays at the heart of the Quantum Computation by Adiabatic Evolution. While this is a standard subject tackled in most books on Quantum Mechanics [Sch55, Mes59], I will nonetheless formulate it in a way that is more adapted to my purposes, that is, the design of quantum algorithms and the evaluation of their complexity.

In Chapter 4, we really enter the personal contribution of my thesis by exposing how one can achieve the quadratic speed-up of Grover's algorithm using an adiabatic algorithm. This result led to a first publication [RC02]:

- Jérémie Roland and Nicolas J. Cerf. Quantum search by local adiabatic evolution. *Phys. Rev. A*, 65:042308, 2002. e-print quant-ph/0107015.

In Chapter 5, I clarify the links between the three quantum search algorithms: Grover's algorithm, its analog analogue and the quantum search by adiabatic evolution. More precisely, I show how these last two algorithms may be translated into the quantum-circuit model of computation while keeping the quadratic speed-up of Grover's algorithm. I point out that these three quantum algorithms then take a very similar form, even though they remain three clearly distinct algorithms. The content of this chapter corresponds to a second publication [RC03b]:

- Jérémie Roland and Nicolas J. Cerf. Quantum-circuit model of Hamiltonian search algorithms. *Phys. Rev. A*, 68:062311, 2003. e-print quant-ph/0302138.

In Chapter 6, I show the possibility of using the adiabatic quantum search algorithm in a recursive manner to solve structured problems, such as the satisfiability of boolean formulas which is NP-complete. This result was published in the following article [RC03a]:

- Jérémie Roland and Nicolas J. Cerf. Adiabatic quantum search algorithm for structured problems. *Phys. Rev. A*, 68:062312, 2003. e-print quant-ph/0304039.

Chapter 7 concludes the main part of this thesis by studying the resistance to noise of a quantum algorithm based on a continuous time Hamiltonian evolution, characterized by either a time-independent Hamiltonian or an adiabatic change. This calculation combines elements of random matrix theory with perturbation theory.

Finally, Appendix A provides a few mathematical tools useful for the body of the thesis, while the two other appendices deal with independent research subjects. Appendix B studies the optimal estimation of quantum states, a work done in collaboration with Sofyan Iblisdir (still unpublished). On the other hand, Appendix C contains an article about non-locality and more precisely Bell Inequalities that follows from a collaboration with Serge Massar, Stefano Pironio, and Bernard Gisin [MPRG02]:

- Serge Massar, Stefano Pironio, Jérémie Roland, and Bernard Gisin. Bell inequalities resistant to detector inefficiency. *Phys. Rev. A*, 66:052112, 2002. e-print quant-ph/0205130.

Contents

List of Figures

Chapter 1

The advent of Quantum Computation

Introduction

Long before the first computers were built, at the dawn of mathematics, men realized that many everyday life problems could be translated into mathematical problems, and that some would be more complex to solve than others. For instance, a farmer could easily evaluate the area of his triangular field, but it was much more difficult to find the optimal way to use it, knowing that he could only cultivate particular vegetable patches in particular seasons of the year, that different seeds had different costs but could also lead to different profits, and many other parameters that should be taken into consideration. Intuitively, we understand that the first problem would take less time to solve than the latter, and therefore they should be classified in different classes of complexity.

However, one had to wait until the twentieth century to clarify this matter. Actually, the first step was taken in the middle of the nineteenth century by Charles Babbage (1791-1871), who conceived his Analytical Engine, an apparatus that would be able to perform any mathematical calculation. Nonetheless, technology lacked at that time and even when his son continued his work after he died, his theoretical model of the Analytical Engine could never been practically built and the prototypes could only solve a few problems with very frequent errors.

Another important step was performed by Kurt Gödel (1906-1978) when he gave a –rather surprising– answer to a question asked by David Hilbert (1862-1943), who realized that before trying to prove that a mathematical proposition was true or not, one should ask if such a proof was actually always achievable. He thus questioned the intuition, widely spread at the time among mathematicians, that mathematics were complete, in the sense that within a mathematical theory, any proposition could be proved to be either true or false. Surprisingly, Gödel showed that this was not the case by establishing the existence of mathematical propositions that were undecidable, meaning that they could be neither proved nor disproved. Equivalently, this refuted the idea that any properly defined mathematical function was computable or that, for every properly defined mathematical problem, it was either possible to find a solution, or to prove that none exists.

Relying on Gödel's work, it is precisely the problem of establishing the decidability of mathematical propositions, instead of their truth, that Alan Turing (1912-1954) addressed

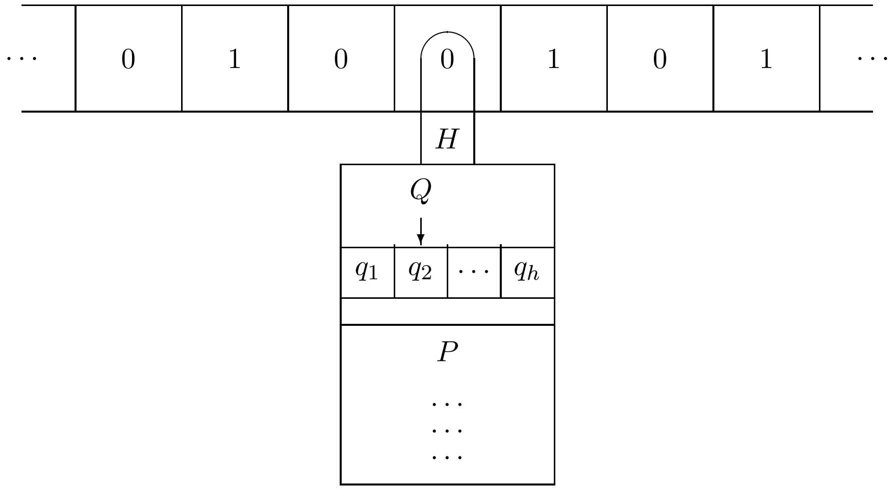

Figure 1.1: Schematic representation of a Turing Machine: The machine acts following a fixed program P, and an internal state Q that may vary during the computation, taking values in a finite set $\{q_1, q_2, \dots, q_h\}$. Thanks to a read-write tape-head H, it may interact with a tape, used like a computer memory, printed with symbols s_i. The computation consists in successive identical steps. At each step, the machine reads the symbol s_i written on the tape at the current position i of the head. Then, depending on s_i, the program P and the current internal state q, it overwrites the symbol with a new value s'_i, changes its internal state to q' then moves the head H left or right. At some point, if the machine enters the special state q_h, it halts. The computation is then finished and the output may be read on the tape.

when he proposed his model that is now widely known as the Universal Turing Machine [Tur36]. Building up on ideas developed by Babbage to devise his Analytical Engine, he defined a theoretical model of machine that was sufficiently complicated to address any mathematical problem but sufficiently simple to be analytically studied (a schematic representation of a Turing Machine is given in Fig. 1.1). Even though at that time a "computer" looked actually more like a mathematician writing equations on a piece of paper, his model proved to be sufficiently general to be "computationally" equivalent[1] to other models, such as the circuit-model we will consider later, or even to nowadays computers. In particular, considering the decidability problem, it is now widely believed that all these models permit the same functions to be computed, what Alan Turing and Alonzo Church summarized, independently and both in 1936, in a thesis that took their name [Chu36]:

> Every function "which would *naturally* be regarded as computable" can be computed by the Universal Turing Machine.

Actually, the *Church-Turing Thesis* is not a theorem, but rather an assertion about the Real World, as the set of functions being *naturally* regarded as computable is not defined rigorously. Intuitively, it corresponds to the set of functions that may be computed with any realistic physical means. Consequently, this thesis remains unproven, but the fact that no counter-example could be found in spite of numerous attempts convinces most theoreticians of its validity.

[1] The notion of computational complexity will be explained in the next section.

Following this remarkable result, we may now classify problems into two groups, whether they are solvable (if they reduce to a decidable mathematical proposition or a computable function) or not, but we have not yet defined how, among solvable problems, discriminate between easy or complex ones. An answer to this question was given by Alan Cobham and Jack Edmonds, who defined the complexity of an algorithm as the number of elementary operations it requires to be run on a Universal Turing Machine. A problem which requires a number of operations that grows exponentially with the size of the input would then be considered as complex, or *intractable* while a polynomial growth would correspond to *tractable* problems. Of course, this supposes that we know the optimal algorithm to solve a problem (for instance, there exist problems for which only exponential algorithms are known, but the existence of a polynomial algorithm is not proved to be impossible). Remarkably, it seemed that the translation of any algorithm initially formulated within another computational model into the Universal Turing Machine model could only increase the number of basics steps polynomially, so that this definition of complexity would be model-independent. However, while Church-Turing thesis survived against many attempts to find a counter-example, it was not the case for this conjecture.

The first alarm was given when it was shown that an Analog Computation model could outperform the Universal Turing Machine for some tasks. Nonetheless, this model required the use of continuous variables with arbitrary large precision, which would not be practically feasible, and it was shown that whenever errors would occur during the computation, the analog computer could not beat the Universal Turing Machine anymore. While the Analog Computation model did therefore not contradict the universality of the definition of complexity based on the Universal Turing Machine when considering realistic computations, a new crisis occurred when Robert Solovay and Volker Strassen showed that it was possible to test the primality of a given integer with a *randomized* algorithm. Their algorithm used randomness at some steps of the computation and could tell in polynomial time either that the integer was composite with certainty or prime with some large probability. Repeating the algorithm a few times, it was therefore possible to find wether an integer was prime or not with near certainty, while, at that time, no deterministic polynomial algorithm to solve this problem was known[2]. This suggested that randomized algorithms could beat deterministic ones, which inspired many other successful results. To keep an accurate definition of computation complexity, the Universal Turing Machine was generalized by allowing the use of randomness along the computation, which led to the *Strong Church-Turing Thesis*:

> Any model of computation can be simulated on a *probabilistic* Turing Machine with at most a polynomial increase in the number of elementary operations required.

The fact that the discovery of a new type of algorithms required a modification of the Strong Church-Turing Thesis suggests that we must stay cautious. Would it be possible that there exists an even more general type of Turing Machine? To answer this question, one approach would be to look for the basic principles that determine what is a possible computation... Realizing that any type of "computer", would it be a mathematician scribbling on a piece of paper, Babbage's Analytical Engine or a state-of-the art personal computer, is actually a physical system, we understand that possible computations are ultimately limited by the Laws of Nature. However, while we know from the revolution that physics lived during the last century that Nature is quantum mechanical, the concepts of Quantum Mechanics

[2] Let us note that recently, a deterministic polynomial algorithm for this problem was discovered.

are rather counter-intuitive to the human mind, which is much more used to the *classical* (as opposed to *quantum*) properties of large physical systems. Accordingly, it is within a *classical* view of Nature that Turing developed his ideas. Therefore, it is possible that a Quantum Turing Machine could be more powerful[3] than its classical equivalent. Since the dynamics of a Quantum Turing Machine would be governed, as any other quantum system, by the Schrödinger equation, it is clear that it could be simulated on a classical Turing Machine just by numerically integrating this equation, such that the introduction of this Quantum Machine would not modify the set of computable functions (that is, the Weak Church-Turing Thesis). Nonetheless, this simulation would involve the evaluation of a number of complex amplitudes that increases exponentially with the size of the input, such that it would not be efficient. It is therefore possible that there exist polynomial quantum algorithms for problems that are thought to be classically intractable. The quest for such algorithms is the main goal of the flourishing field of Quantum Computation.

In this chapter, we will first briefly summarize some notions of Classical Computation useful for this thesis, such as the ideas of algorithm, universal gates and circuit complexity. Then, after having reviewed the postulates of Quantum Mechanics, we will generalize these notions to Quantum Computation.

1.1 Classical Computation

The goal of computation is to design efficient analytical methods, called *algorithms*, to solve mathematical problems. Before considering algorithms, let us first focus on the problems. A general problem is given as a mathematical description of what is sought (the solution or *output*) depending on some unspecified variable, or *input*. The specification of this variable fixes the particular *instance* of the problem. For example, the factorization problem may be defined in the following way: “Given an integer x, find one of its factor y”. Different values of the input x will correspond to different instances of this general problem. The value of x could be written with different symbols and take the form of a number written in decimal notation or a word made of letters from the Latin alphabet. To fix a standard, we will use the binary notation, generated by the minimal set of symbols $\{0,1\}$. Each binary variable is then called a *bit*, for “binary digit”, and a sequence of ν bits allows to define 2^ν different instances. We will often refer to ν as the *size* of the problem (it is actually the size of the input written in binary notation).

1.1.1 Circuit model

An algorithm is an analytical method that, given the input x of a problem, provides an output y that satisfies the definition of the solution of the problem. Since the output y may be, exactly as the input x, written in binary notation, an algorithm corresponds to the evaluation of a function $f : \{0,1\}^\nu \to \{0,1\}^\mu : x \mapsto y = f(x)$. If this function is computable we know that the problem may be solved using a Universal Turing Machine. However, from now on we will consider another model of computation that may be proved to be equivalent, namely the *circuit model*.

Writing the μ bit output $y = (y_1, \ldots, y_\mu)$, the function f defines μ functions with one bit output $f_k : \{0,1\}^\nu \to \{0,1\} : x \mapsto y_k = f_k(x)$ $(k = 1, \ldots, \mu)$. Each of these functions

[3] From a computational complexity point of view, as explained in the following sections.

may then be rewritten as a boolean expression of the input bits $x = (x_1, \ldots, x_\nu)$ combined with the boolean operators NOT ($\neg$), AND ($\wedge$)and OR ($\vee$). These boolean expressions may be evaluated using a circuit made of wires carrying the value of bits between logical gates corresponding to the boolean operators (see Fig. 1.2).

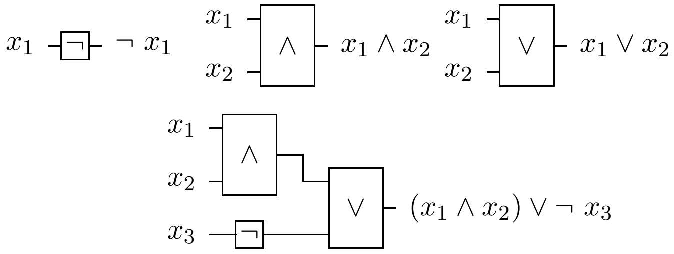

Figure 1.2: The classical gates NOT ($\neg$), AND ($\wedge$), and OR ($\vee$) and a small circuit implementing the boolean expression $(x_1 \wedge x_2) \vee \neg\, x_3$.

While each of the boolean operators cited above corresponds to a particular logical gate, we may define any logical gate as a function $g : \{0,1\}^\nu \rightarrow \{0,1\}^\mu : x \mapsto g(x)$. In particular, apart from the NOT, AND and OR gates, the practical implementation of the circuits have implicitely assumed the existence of two other gates: FANOUT, which duplicates a bit and is necessary if a bit appears more than once in the boolean expression, and CROSSOVER, which swaps two wires and is required to be able to apply a logical gate on two spatially separated bits (see Fig. 1.3).

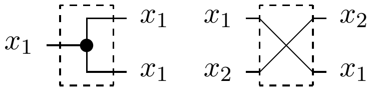

Figure 1.3: FANOUT and CROSSOVER gates, which respectively duplicates a bit and swaps two bits.

1.1.2 Universal set of gates

One important issue is to find a *universal* set of gates, meaning that, combined together, these gates are able to simulate any other logical gate. This is the case of the set {NOT, AND, OR, FANOUT, CROSSOVER} that we just described, but there exists other equivalent universal sets. One useful trick to simulate a logical gate from others is to make use of an extra bit with a known value, called an *ancilla*. For instance, as shown in Fig. 1.4, it is possible to simulate the logical gate AND with one ancilla bit with value 0 and two uses of the NAND gate ("NOT AND", which outputs 0 if and only if both input bits are 1). Actually, it is possible to show that one can simulate any logical gate using ancilla bits and the set {NAND, FANOUT, CROSSOVER}, which is therefore universal.

1.1.3 Circuit complexity

Let us now turn to the notion of complexity, which, following the Strong Church-Turing Thesis, is related to the number of elementary operations needed to solve the problem with a Turing Machine. Let us translate this idea into the picture of the circuit model of computation.

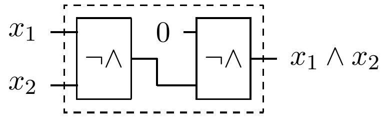

Figure 1.4: Simulation of an AND gate ($\wedge$) from two NAND gates ($\neg\wedge$) and an ancilla with value 0.

Within this model, an algorithm corresponds to a family of circuits C_ν, made of gates from a universal set, for all sizes of the input ν. To derive a proper notion of complexity, we add a *uniformity* condition, which requires that the design of the circuit C_ν may be computed efficiently (in polynomial time versus the size ν) for instance on a Turing Machine. This prevents to hide the hardness of a problem within a complex procedure to design the circuit and even more the possibility to compute uncomputable functions. For such a uniform family of circuits, the complexity will be defined as the *size* of the circuit C_ν, that is, the number of elementary gates in the circuit. Following this idea, we consider that the size of the circuit corresponds to the time it takes to run the algorithm.

Actually, we are not interested in the exact size of the quantum circuit, which for instance may vary for different universal sets of gates, but mostly on the way it scales versus the size of the input ν. Following the Strong Church-Turing Thesis, an algorithm is called *efficient* if its complexity grows polynomially with ν. To precise this notion of scaling, we will use the asymptotic notation Big-O:

$$f(\nu) = O(g(\nu)) \Leftrightarrow \exists c \geq 0, \nu_0 \geq 0 \text{ s.t. } 0 \leq f(\nu) \leq cg(\nu) \quad \forall \nu \geq \nu_0. \tag{1.1}$$

Intuitively, it means that $f(\nu)$ grows slower (or equally) with ν than $g(\nu)$. We will also use the inverse notation Big-Ω:

$$f(\nu) = \Omega(g(\nu)) \Leftrightarrow \exists c \geq 0, \nu_0 \geq 0 \text{ s.t. } 0 \leq cg(\nu) \leq f(\nu) \quad \forall \nu \geq \nu_0. \tag{1.2}$$

that means that $f(\nu)$ grows faster (or equally) with ν than $g(\nu)$.

Practically, a tractable problem admits efficient algorithms, that show a complexity scaling as $O(\nu^c)$ for some exponent c, while an intractable problem may only be solved by algorithms with a complexity that scales as $\Omega(\nu^c)$, no matter how large is c. More generally, the Big-O notation is often used to qualify the worst-case behavior of an algorithm, while the Big-Ω permits to specify lower bounds on the complexity of all algorithms able to solve a particular problem. The ideal case occurs when the worst-case behavior of the best known algorithm saturates the lower bound, in which case we know that this scaling is really optimal and we may use the Big-Θ notation

$$f(\nu) = \Theta(g(\nu)) \Leftrightarrow f(\nu) = O(g(\nu)) \text{ and } f(\nu) = \Omega(g(\nu)), \tag{1.3}$$

meaning that both functions scale similarly with ν.

Let us note that the following properties immediately follow from the definitions

$$f(\nu) = O(g(\nu)) \quad \Leftrightarrow \quad g(\nu) = \Omega(f(\nu)) \tag{1.4}$$

$$f(\nu) = \Theta(g(\nu)) \quad \Leftrightarrow \quad g(\nu) = \Theta(f(\nu)). \tag{1.5}$$

Moreover, while these definitions apply to the limit of large ν, that is, $\nu \to \infty$, we may also study a scaling in the limit of, for instance, a small error probability ε, extending the definition of the Big-O notation to the case $\varepsilon \to 0$:

$$f(\varepsilon) = O(g(\varepsilon)) \Leftrightarrow \exists c \geq 0, \varepsilon_0 \geq 0 \text{ s.t. } 0 \leq f(\varepsilon) \leq cg(\varepsilon) \quad \forall \varepsilon \leq \varepsilon_0. \tag{1.6}$$

1.1.4 Complexity classes

Now that we have defined the notions of logical circuit and complexity, we may classify mathematical problems according to the complexity of the optimal circuit that allows to solve them. This is the goal of Complexity Theory, a broad field of Information Science of which we only sketch here the basic ideas that will be helpful for the sake of this thesis.

On one hand of the complexity scale, are easy problems that may be solved in polynomial time and define the complexity class P, for *polynomial*. Unfortunately, there are of course numerous problems for which only exponential algorithms are known. Among these problems, an important sub-class is PSPACE which brings together those admitting a possibly exponentially deep circuit that works on a polynomially large register of bits, that is, they may require exponential time but only *polynomial space*.

While it is still unproven whether P≠PSPACE, it is one of the most important conjecture of Complexity Theory. Whatsoever, complexity classes that would be intermediate between P and PSPACE may be theoretically defined, such as the class of *non-deterministic polynomial* problems, or NP, which includes problems that may possibly only be solved in exponential time, but, roughly speaking, whose solution may be checked in polynomial time if some data, called a *witness* is provided. A typical example would be the factoring problem, as it may not be possible to factor a large number in polynomial time, but if a factor of the number is given as a witness, this may easily be checked just by performing a division, which takes a polynomial time.

Another example would be the problem of the satisfiability of boolean formulas, which amounts to determine if a given boolean formula involving a set of ν binary variables may be satisfied for some assignments of the variables. In this case, it is possible to check in polynomial time whether the formula is satisfiable if a satisfying assignment is given as a witness. The particularity of this problem is that it has been proved that any other problem in NP may be reduced to it with only polynomial overhead, meaning that this problem is among the most difficult problems in NP. Other problems share this property, they form the class of NP-complete problems, NP-c.

From the definition of NP-completeness, it follows that if a polynomial algorithm was found for any NP-complete problem, all other problems in NP could be solved in polynomial time and the class NP would reduce to the class P. Despite years of attempts, no polynomial algorithm for an NP-complete problem has been found so that it is now widely conjectured that none exists, although as no proof ruling out the possibility of such an algorithm was derived, the question P=NP remains open.

Another interesting open question is whether it may help to use a randomized algorithm. Such an algorithm would translate into a logical circuit which divides in different paths at some points. One would then have to flip a coin to decide which path to follow. Such a randomized circuit thus relies on a different model of computation, equivalent to the *probabilistic* Universal Turing Machine. This generalized model allows to define new classes of complexity, the most important being the class of *bounded error probabilistic polynomial* problems, or BPP. This class includes problems that may be solved by a probabilistic algorithm in polynomial time with success probability of at least 3/4. Thanks to the Chernoff Bound, which shows that, whenever the error probability is smaller than 1/2, it may be reduced exponentially fast just by repeating the algorithm a polynomial number of times, this lower bound of 3/4 is actually arbitrary. Therefore, the class BPP may really be considered as the class of problems that may be solved efficiently, that is, in polynomial time.

1.1.5 Reversible Computation

Even though Quantum Mechanics involves amplitudes instead of probabilities, quantum processes are inherently probabilistic, such that the introduction of randomness in the computational model took us one step closer to the idea of Quantum Computation. However, another peculiarity of a quantum evolution is its reversibility[4].

Considering the circuit model of computation, we see that not all gates are reversible. For instance, while the NOT gate is reversible as one may recover the input bit just by negating the output bit, this is not the case for the XOR gate, which from an input of two bits outputs the single bit corresponding to their sum modulo 2. During the application of this gate, one bit of information is actually lost or, more precisely, erased, which is the cause of irreversibility. On thermodynamical grounds, it may be shown that the erasure of information leads to a consumption of energy, as stated by *Landauer's principle* [Lan61]:

> When a computer erases a single bit of information, the amount of energy dissipated into the environment is at least $k_B T \ln 2$, where k_B is Boltzmann's constant and T is the temperature of the environment.

Even though current computers dissipate much more energy than the lower bound predicted by Landauer's principle, it turns out that this bound is the only ultimate physical limit on the reduction of power consumption, such that, theoretically, it should be possible to design a computer that consumes arbitrarily low power, as long as it behaves reversibly. The question is: is it possible to make any computation reversible? The answer is yes, it suffices to add to each irreversible gate some additional output bits containing the erased information [Ben73]. For instance, the XOR gate may be made reversible by adding a second output bit that takes the value of, say, the first input bit (see Fig. 1.5). Let us note that the reversible version of XOR then takes a particular form, as it may be viewed as a gate that performs a NOT on one bit if the other bit is set to 1, and leaves it alone otherwise. We call such a gate that performs some operation R on a *target bit* if and only if a *control bit* is set to 1 a Controlled-R. In this case the reversible XOR is equivalent to a Controlled-NOT, or "CNOT".

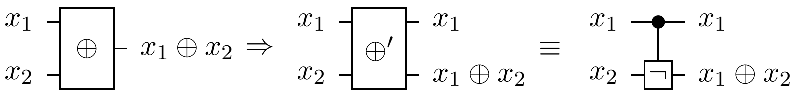

Figure 1.5: It is possible to make the XOR gate ($\oplus$) reversible by adding an extra output bit. We then obtain a CNOT gate that performs a NOT ($\neg$) on the target bit x_2 if and only if the control bit x_1 is set to 1.

Adding adequate extra output bits to each irreversible gate, one can make a whole circuit reversible, but this will introduce a lot of extra bits that are useless for the computation but necessary for preventing dissipation. Indeed, it is the erasure of these "garbage" bits that would cause irreversibility and thus energy consumption. At first view, it may seem that

[4] At least in the current, standard description of Quantum Mechanics, possibly taking apart the measurement postulate which interpretation differs among physicists and is sometimes considered as leading to a non-reversibility of the measurement operation. However, we will see that this particular interpretation of the measurement postulate does not modify the Quantum Computation model, as any measurement may be postponed to the end of the computation.

this erasure would be necessary to free some memory space in order to perform subsequent computations, otherwise garbage bits would accumulate after each computation and finally saturate the computer memory. Actually this is not true as it may be shown that it is possible to arrange the garbage bits in such a way that they all end up in a standard state, for instance all bits with value 0, ready for a new computation[5]. This means that it is theoretically really possible to perform computations with arbitrarily low energy consumption [Ben89].

Following these ideas, we may define a model of computation that involves reversible circuits only. As the translation of an irreversible circuit into a reversible one is always possible and may only increase the number of elementary gates and the work space polynomially, a crucial consequence is that this model will be computationally equivalent to its irreversible counterpart and thus the complexity classes will remain unchanged. The basic difference is that reversible circuits will be built from a different set of universal gates, all being reversible. More precisely, it may be shown that to perform Universal Reversible Computation, one needs a set that contains at least one *three-bit* gate (while it was only a *two-bit* gate for irreversible computation, for instance NAND). One example of universal set is made of only one such gate, the Fredkin gate [FT82]. This gate swaps the first two bits if the third bit is set to 1 and leaves them alone otherwise, so it may be considered as a Controlled-CROSSOVER (see Fig. 1.6). It is indeed straightforward to check that this gate alone may reproduce the NOT, AND, OR, CROSSOVER and FANOUT gates, with the help, when necessary, of extra bits prepared in a standard state, called *ancillae*, and producing garbage bits. Another interesting universal set is made of the Toffoli gate alone, also known as the "Controlled-Controlled-NOT" as it flips the third bit (the *target* bit) if the first two bits (the *control* bits) are both set to 1 and leaves it alone otherwise. This gate will play an important role in Quantum Computation, another even more physically based model of computation that we consider next.

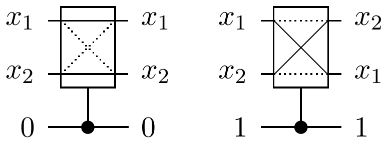

Figure 1.6: The Fredkin gate, which acts as a Controlled-CROSSOVER: it swaps the first two bits if the third bit is set to 1 and leaves them alone otherwise.

1.2 Quantum Computation

1.2.1 The postulates of Quantum Mechanics

The development of Quantum Computation relies on the simple idea that a computer is actually a physical system –and computation is therefore a physical process– such that it is the Laws of Nature themselves that ultimately limit what a computer can or cannot compute. At first view, it may seem that a computer is such a complex physical system that the study of the exact physical laws which govern its evolution would hardly lead to any useful result. Nonetheless, no matter the physical realization of the computer and the detailed physical laws that describe its evolution, all modern physical theories rely on a single mathematical model

[5] This will be even more crucial to Quantum Computation where extra bits in different states could destroy the interferences that are at the basis of most quantum algorithms.

which builds on a very few postulates only, namely Quantum Mechanics. In this section, we briefly review these postulates[6] as they will lay at the basis of the Quantum Computation model.

The first postulate defines the mathematical entity representing a particular state of some physical system:

Postulate 1 *To any isolated physical system S is associated a complex vector space with inner product, or Hilbert space, $\mathcal{H}_S$. The system state is completely determined by a unit vector $|\psi\rangle$ of this Hilbert space.*

We will use the *bracket* notation $\langle\psi_1|\psi_2\rangle$ for the inner product of two states $|\psi_1\rangle$ and $|\psi_2\rangle$ of a Hilbert space $\mathcal{H}_S$, and often refer to $\langle\psi_1|$ as a *bra* and to $|\psi_2\rangle$ as a *ket*.

Let us notice that this postulate does not specify what Hilbert space will be associated to a given physical system, that is, it does not give the basis states or even the dimension of the Hilbert space. In general, this dimension should be adequately chosen to be able to reproduce the physical properties of the system, and could be as large as infinite. However, in this thesis, we will restrict ourselves to finite-dimensional Hilbert spaces as these will suffice for our purposes.

One interesting property of vectors in a Hilbert space, and therefore of quantum states, is that if $|\psi_1\rangle$ and $|\psi_2\rangle$ are two states in $\mathcal{H}_S$, so will be any linear combination $\alpha|\psi_1\rangle + \beta|\psi_2\rangle$, where α and β are complex numbers such that $|\alpha|^2 + |\beta|^2 = 1$ to preserve normality. This property is often referred to as the *superposition principle*.

Moreover, the fact that quantum amplitudes are complex numbers also introduces the notion of *phase*, as the previous superposition may be rewritten with real numbers a and b as $e^{i\phi_1}(a|\psi_1\rangle + e^{i\phi_2}b|\psi_2\rangle)$, where ϕ_1 will be called a *global* phase and ϕ_2 a *relative* phase. Actually, in Quantum Mechanics, it so happens that global phases have no physical meaning, such that for instance the superpositions $a|\psi_1\rangle + b|\psi_2\rangle$ and $e^{i\phi_1}(a|\psi_1\rangle + b|\psi_2\rangle)$ represent exactly the same physical state. Indeed, the postulates of Quantum Mechanics imply that a change of global phase has no influence on the evolution (postulate 2) and the measurement (postulate 3) of a quantum state. Such global phases are thus irrelevant and will often be neglected subsequently.

However, this is not the case for relative phases, and the states represented by $a|\psi_1\rangle + b|\psi_2\rangle$ and $a|\psi_1\rangle + e^{i\phi_2}b|\psi_2\rangle$ will be different for a non-zero relative phase ϕ_1, and may even be orthogonal. Relative phases actually play an important role as they may lead to constructive or destructive interferences, a quantum effect that will be a useful tool for Quantum Computation.

While the first postulate deals with states at a particular fixed time, it is of course essential to precise how these states will evolve in time. This is the purpose of the second postulate:

Postulate 2 *The time evolution of a state $|\psi(t)\rangle$ of an isolated quantum system is described by the* Schrödinger equation*:*

$$i\hbar\frac{d}{dt}|\psi(t)\rangle = H|\psi(t)\rangle, \tag{1.7}$$

where $\hbar$ is a physical constant known as Planck's constant *and H is a Hermitian operator called the* Hamiltonian *of the system.*

[6] We will only consider the standard, non-relativistic Quantum Mechanics, since it will be sufficient for our purposes.

Similarly to the first postulate, this does not specify the exact form of the Hamiltonian H, which practically will vary with the system that is considered. While it is in general time-dependent, an important particular case occurs when the Hamiltonian is time-independent. In this case, the Schrödinger equation may be integrated analytically, allowing to evaluate the state $|\psi(t_1)\rangle$ at time t_1 from the state $|\psi(t_0)\rangle$ at time t_0:

$$\begin{aligned} |\psi(t_1)\rangle &= e^{-\frac{iH}{\hbar}(t_1-t_0)}|\psi(t_0)\rangle && (1.8) \\ &= U(t_0,t_1)|\psi(t_0)\rangle, && (1.9) \end{aligned}$$

where we have introduced the evolution operator $U(t_0,t_1)$ that maps the state at time t_0 to the state at time t_1. This operator is unitary $[U(t_0,t_1)]^\dagger = [U(t_0,t_1)]^{-1}$, and it may be shown that in the general case of a time-dependent Hamiltonian, such a unitary evolution operator may always be defined. From the unitarity of the evolution operator, it immediately follows the reversibility of quantum processes as unitary operators are always invertible, allowing the definition of a *reversed* evolution operator $U'(t_1,t_0) = [U(t_0,t_1)]^{-1}$, unitary as well.

Until now, we have only considered isolated systems. However, it is clear that it is necessary to interact with the system that we study at some point in order to retrieve some information from it. The description of measurement is the purpose of the following postulate:

Postulate 3 *A quantum measurement on a system S is described by a collection $\{M_m\}$ of* measurement operators*, defined as operators acting in the Hilbert space $\mathcal{H}_S$ associated with S and satisfying the* completeness relation

$$\sum_m M_m^\dagger M_m = I_S, \tag{1.10}$$

where I_S is the identity operator on $\mathcal{H}_S$. The index m refers to the measurement outcomes that may occur in an experiment. The probability $p(m)$ to obtain the outcome m if the system was in the state $|\psi\rangle$ immediately before the measurement is given by

$$p(m) = \langle\psi|M_m^\dagger M_m|\psi\rangle, \tag{1.11}$$

and the state just after the measurement becomes

$$\frac{M_m|\psi\rangle}{\sqrt{p(m)}}. \tag{1.12}$$

Practically, it often happens that one is only interested in the different probabilities to get each outcome and not in the state of the system after the measurement (this occurs when the only measurement coincides with the end of the experiment and will for instance be the case for Quantum Computation). In this case, we see from the measurement postulate that the only relevant mathematical entities are the operators $\mathcal{O}_m = M_m^\dagger M_m$. We will therefore define a *positive operator-valued measure*, or POVM, as a set of positive operators $\{\mathcal{O}_m\}$, called *POVM elements*, satisfying a completeness relation:

$$\sum_m \mathcal{O}_m = I_S. \tag{1.13}$$

The positivity of the POVM operators $\{\mathcal{O}_m\}$, often written as $\mathcal{O}_m \geq 0$, follows from the fact that they originally derive from an operator M_m as $\mathcal{O}_m = M_m^\dagger M_m$, and is equivalent to imposing that their spectrum only involves positive eigenvalues.

Physicists may not be used to this form of the measurement postulate, as they are generally more familiar with a particular type of measurement, namely *projective measurements*[7], which correspond to the special case where the measurement operators M_m are orthogonal projectors P_m, with $P_m P_{m'} = \delta_{mm'} P_m$. In Quantum Physics, each physical property that may be measured corresponds to a hermitian operator M, called *observable*, that has a spectral decomposition $M = \sum_m m P_m$, where m's are the eigenvalues of M and P_m's are the projectors on the corresponding eigenspaces. Within this formalism, we recover the measurement postulate as stated in most books on Quantum Mechanics, which says that the possible outcomes are the eigenvalues m of the observable M that is measured and that the state after the measurement lays within the eigenspace of M corresponding to the actual outcome m.

Now this generalized statement of the measurement postulate raises two questions. First, why do we state this postulate in this form? The answer lays in the developments of the Quantum Information Theory, that showed in different contexts that it is often possible to retrieve more information from a quantum system when we do not restrict ourselves to projective measurements[8]. Perhaps more fundamental is the second question, why are we allowed to state the measurement postulate in this form? Actually, it may be shown that these two formulations are strictly equivalent, as long as we add this last postulate:

Postulate 4 *The Hilbert space associated with a composite physical system AB made of two sub-systems A and B is the tensor product $\mathcal{H}_A \otimes \mathcal{H}_B$ of the Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$ associated with the sub-systems. If the sub-system A is prepared in the state $|\psi_A\rangle$ and the sub-system B is prepared in the state $|\psi_B\rangle$, then the joint state of the composite system AB will be the tensor product state $|\psi_A\rangle \otimes |\psi_B\rangle$.*

Now this postulate allows us to realize a generalized measurement $\{M_m\}$ on a system S by extending it with an additional system A prepared in some known state and performing a projective measurement on the composite system SA (see also Neumark's theorem [Per95]). Indeed, choosing an extra system A whose dimension coincides with the number of measurement operators M_m, and associating each M_m with a basis state $|m\rangle$ of A, it is always possible to define a unitary operator U such that $U|\psi\rangle|0\rangle = \sum_m M_m|\psi\rangle|m\rangle$, where $|\psi\rangle$ is the unknown state of S we want to measure and $|0\rangle$ is some arbitrary fixed state in which we prepare the system A. It is then straightforward to check that the generalized measurement $\{M_m\}$ on S may be realized by a projective measurement on SA with projectors $P_m = U^\dagger(I_S \otimes |m\rangle\langle m|)U$, where I_S is the identity on $\mathcal{H}_S$ and $|m\rangle\langle m|$ is the projector on state $|m\rangle$ of $\mathcal{H}_A$. The use of such kind of extra system prepared in a standard state, usually referred to as an *ancilla*, will actually be a common tool in Quantum Computation[9].

This last postulate leads to another interesting feature of Quantum Mechanics. Suppose that $|\psi_A\rangle$ and $|\psi'_A\rangle$ are two possible states of A, and similarly for B. Due to the superposition principle, the states of the composite system AB may take not only a product form such as $|\psi_A\rangle \otimes |\psi_B\rangle$ but also a non-separable form as $\alpha|\psi_A\rangle \otimes |\psi_B\rangle + \beta|\psi'_A\rangle \otimes |\psi'_B\rangle$. These last states may not be considered as separate states on A and B as they are only defined in the joint

[7] Projective measurements are sometimes also called *Von Neumann measurements.*

[8] See for instance the Appendix B which deals with the optimal estimation of quantum states.

[9] We have already met the idea of using an ancilla, but within a classical context, to define reversible gates in Section 1.1.5.

Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$ and therefore involve some kind of quantum correlation, which we will call *entanglement*, between systems A and B. We will therefore qualify these states as *entangled*. Entanglement is an essential resource used in Quantum Information Theory and in Quantum Computation in particular[10].

1.2.2 The qubit

We are now ready to enter the core of this thesis: Quantum Computation. As for Classical Computation, the goal of Quantum Computation is to design efficient methods to solve mathematical problems. These problems will be exactly the same as for Classical Computation and it may therefore be possible to state the instance of a problem –the input– and its solution –the output– in the same manner, that is, using a string of bits. The difference will be the method –the algorithm– used to derive the output from the input, that we will now call a *quantum algorithm* as it will deal with quantum states instead of classical information.

How can we encode a string of bits in a quantum state in order to use it as an input for a quantum algorithm? Let us first consider the smallest possible case, a single bit, that may take value 0 or 1. It then seems natural to associate each of these values to a different quantum state $|0\rangle$ and $|1\rangle$. It would of course be preferable to be able to distinguish perfectly between these states, for instance to be able to read the output of the algorithm without error. It follows from the measurement postulate 3 that this is only possible if these states are orthogonal: $\langle 0|1\rangle = 0$. These states will span a two-dimensional Hilbert space $\mathcal{H}_2$, representing the state of a system that we will call a *qubit*, for "quantum bit". It follows that a qubit may be in one of the basis states $|0\rangle$ or $|1\rangle$, corresponding to the classical bit values 0 and 1, but also, due to the superposition principle (see postulate 1), in any linear combination $\alpha|0\rangle + \beta|1\rangle$ that has no classical equivalent.

Let us now consider a string x of ν classical bits $(x_1, x_2, \ldots, x_\nu)$, each bit x_k taking value 0 or 1. We may associate to each bit x_k a qubit described by a two-dimensional Hilbert space $\mathcal{H}_{2,k}$, and then to the string x a composite quantum state

$$|x\rangle = |x_1\rangle \otimes |x_2\rangle \otimes \ldots \otimes |x_\nu\rangle \tag{1.14}$$

which lays in the Hilbert space $\mathcal{H}_N = \mathcal{H}_{2,1} \otimes \mathcal{H}_{2,2} \otimes \ldots \otimes \mathcal{H}_{2,\nu}$. The $N = 2^\nu$ possible classical bit strings x therefore defines an orthonormal basis of this N-dimensional Hilbert space, which will be called the *computational basis*. While each state $|x\rangle$ of the computational basis directly corresponds to a classical bit string x, the superposition principle implies that an arbitrary state of $\mathcal{H}_N$ takes the form

$$|\psi\rangle = \sum_{x=0}^{N-1} \alpha_x |x\rangle, \tag{1.15}$$

where x is written in binary notation, involving $N = 2^\nu$ complex amplitudes α_x satisfying the normality condition $\sum_x |\alpha_x|^2 = 1$. Except for the particular case of the computational basis states, these states are entangled and therefore do not have any classical equivalent. According to the measurement postulate 3, a projective measurement of state $|\psi\rangle$ in the computational basis will yield result x with probability $|\alpha_x|^2$. This is exactly the measurement that will practically be used in quantum algorithms.

[10] Let us mention that a particular witness of the entanglement of a quantum system follows from the use of so-called *Bell Inequalities*, which is the subject of Appendix C.

1.2.3 Quantum circuits

Following the lines of the definition of the circuit model of *Classical* Computation, we may now introduce the circuit model of *Quantum* Computation[11]. While a classical circuit is made of wires carrying the value of bits between logical gates, a quantum circuit consists of wires carrying qubit states between quantum gates. We have already defined the notion of qubit, but what is a quantum gate? Intuitively, it should be an application that maps input qubits to output qubits. As it follows from the evolution postulate 2 that any physical transformation is reversible, the number of output qubits must match the number of input qubits, and therefore a gate will just act as a reversible transformation on a fixed number of qubits. For instance, it is clear that any reversible classical gate may be generalized to a quantum gate, for instance the NOT gate:

$$U_\neg : \mathcal{H}_2 \to \mathcal{H}_2 : |x_1\rangle \mapsto |\neg x_1\rangle, \tag{1.16}$$

or the (reversible) XOR gate:

$$U_\oplus : \mathcal{H}_2 \otimes \mathcal{H}_2 \to \mathcal{H}_2 \otimes \mathcal{H}_2 : |x_1\rangle \otimes |x_2\rangle \mapsto |x_1\rangle \otimes |x_1 \oplus x_2\rangle. \tag{1.17}$$

This shows that Reversible Classical Computation is a special case of Quantum Computation. However, Quantum Computation is more general as there are quantum gates that have no classical equivalent. Indeed, this will be the case for any quantum gate that produces superposition of computational basis states or introduces relative phases. More specifically, the evolution postulate only imposes that every physical evolution is unitary, such that a general quantum gate on ν qubits will be described by a unitary operator on a Hilbert space of dimension $N = 2^\nu$. All these unitary operators form a compact Lie group generally noted $U(N)$. To perform universal Quantum Computation, we should therefore be able to simulate any element of $U(N)$ from a finite set of basic gates.

To better understand the implications of this requirement, let us first consider one-qubit gates, corresponding to the group $U(2)$. In the computational basis $(|0\rangle, |1\rangle)$, each gate U may be written as a unitary operator

$$U : \mathcal{H}_2 \to \mathcal{H}_2 : \left\{ \begin{array}{ccc} |0\rangle & \mapsto & u_{00}|0\rangle + u_{10}|1\rangle \\ |1\rangle & \mapsto & u_{01}|0\rangle + u_{11}|1\rangle, \end{array} \right. \tag{1.18}$$

or equivalently as a unitary matrix

$$U = \begin{pmatrix} u_{00} & u_{01} \\ u_{10} & u_{11} \end{pmatrix}, \tag{1.19}$$

where $u_{kl} = \langle k|U|l\rangle$ are complex numbers satisfying the unitarity conditions $\sum_{k=0,1} u_{kl}^* u_{km} = \delta_{lm}$, that is, $U^\dagger U = I$. It follows that up to an irrelevant global phase[12], each one-qubit gate may be represented by a matrix of the following form

$$U_{(\theta,\phi)} = \begin{pmatrix} \cos\frac{\theta}{2} & -e^{i\phi}\sin\frac{\theta}{2} \\ e^{-i\phi}\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix}, \tag{1.20}$$

[11] Let us recall that we have already mentionned in the introduction another model of Quantum Computation, the Quantum Turing Machine. As it is the case for their classical counterparts, these two quantum models are equivalent, but we prefer to focus on the circuit model that is more appropriate to design algorithms.

[12] We have seen in Section 1.2.1 that the postulates of Quantum Mechanics imply that global phases are irrelevant.

While classically there exist only two reversible one-bit gates, NOT ($\neg$) and Identity, which can be generalized to the quantum gates $U_\neg$ and I as

$$U_\neg = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = iU_{(\pi,\pi/2)} \qquad I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = U_{(0,0)}, \tag{1.21}$$

we see that there exists a whole continuum of one-qubit quantum gates, for all values of the angles θ and ϕ. At first view, it may seem that it will not be possible to simulate an infinite number of gates from a finite set of basic gates. However, we may show that this is not the case and that the notion of universal set of gates may be generalized to the quantum case.

1.2.4 Universal set of quantum gates

Remember that a universal set for Reversible Classical Computation consists in the Toffoli gate alone. A remarkable result is that it is possible to simulate any unitary operator on ν qubits using Toffoli gates and the set of all one-qubit gates. This means that using the continuum of unitary operators in $U(2)$ together with Toffoli gates, we may achieve the whole continuum of unitary operators in $U(N)$ (where $N = 2^\nu$).

However, it seems obvious that with a finite set it will not be possible to simulate the whole continuum of one-qubit gates exactly, though maybe it is possible to do it approximately. Suppose we take an arbitrary one-qubit gate $R = U_{(\theta,\phi)}$, with angles θ and ϕ being irrational multiples of π. Suppose now we apply this gate successively k times, simulating the gate R^k. As θ and ϕ are irrational in π, all these gates will differ for different values of k, and will ultimately fill the whole space of $U(2)$ if we let k tend to infinity. More precisely, the set of all powers of R is dense in $U(2)$, such that any element of $U(2)$ may be approached arbitrarily well by an adequate power R^k. This means that the set $\{\text{Toffoli}, R\}$ is universal for Quantum Computation. Furthermore, it is possible to reduce this set to a single gate just by combining the Toffoli and the R gate to make a Deutsch gate [Deu89], that is, a Controlled-Controlled-R (remember that the Toffoli gate was a Controlled-Controlled-NOT, as shown in Fig. 1.7). From a conceptual point of view, it is interesting to note that these universal sets of gates for Quantum Computation may simply be obtained by introducing "quantumness" in the universal set for Reversible Classical Computation, either by adding a generic one-qubit quantum gate or by modifying the universal classical gate to make it quantum.

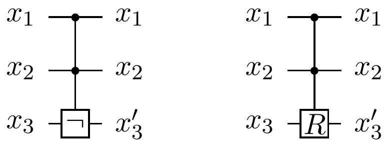

Figure 1.7: The Toffoli and Deutsch gates, which taken alone are universal respectively for Reversible Classical Computation and Quantum Computation.

While all these universal sets involve three-bit (or three-qubit) gates, and it is indeed possible to show that Universal Reversible Classical Computation requires such gates, it is actually not necessary for Quantum Computation. For instance, the set $\{\text{CNOT}, R\}$, where the two-qubit gate CNOT has replaced the Toffoli gate, is also universal [DiV98]. Remarkably, it may be shown that almost any two-qubit gate may replace the Toffoli, which is an excellent news for Quantum Computation as it means that as soon as we are able to apply a generic operator on a single qubit and a generic interaction between two qubits, we are ready for Universal Quantum Computation [DBE95, Llo95].

Before introducing quantum algorithms, let us point out another peculiar consequence of the postulates of Quantum Mechanics. Suppose we would like to define a quantum equivalent to the FANOUT classical gate. To ensure unitarity, it should be a two qubit gate, that copies an unknown qubit onto a *blank* qubit, that is a second qubit prepared in a standard state, for instance $|0\rangle$. The quantum FANOUT U_{FO} would therefore map the computational basis states as

$$U_{\mathrm{FO}}|0\rangle \otimes |0\rangle = |0\rangle \otimes |0\rangle \tag{1.22}$$

$$U_{\mathrm{FO}}|1\rangle \otimes |0\rangle = |1\rangle \otimes |1\rangle, \tag{1.23}$$

effectively copying the first qubit onto the second (blank) one. However, due to the linearity of Quantum Mechanics, this gate would map the superposition state $\alpha|0\rangle + \beta|1\rangle$ as

$$U_{\mathrm{FO}}(\alpha|0\rangle + \beta|1\rangle) \otimes |0\rangle = \alpha|0\rangle \otimes |0\rangle + \beta|1\rangle \otimes |1\rangle \tag{1.24}$$

instead of

$$(\alpha|0\rangle + \beta|1\rangle) \otimes (\alpha|0\rangle + \beta|1\rangle), \tag{1.25}$$

and would therefore not copy such a superposition state reliably. More precisely, the no-cloning theorem of Quantum Mechanics implies that it is impossible to copy an unknown quantum state with arbitrarily high fidelity. Nonetheless, even though the FANOUT gate is an essential tool for Classical Computation, we will see that it is possible to design efficient quantum algorithms without the need to effectively copy qubits.

1.2.5 Quantum algorithms and quantum complexity

We may now explicitly define the notions of quantum algorithm and complexity. A quantum algorithm consists in

1. the preparation of the register in a quantum state of ν qubits taken from the computational basis,

2. a quantum circuit C_ν made of quantum gates taken from a universal set for Quantum Computation,

3. a projective measurement of the output register in the computational basis.

Practically, the circuit C_ν will depend on the size of the particular instance of the problem it is supposed to solve through the number of needed qubits ν in the quantum register. A quantum algorithm then actually corresponds to a family of circuits C_ν for all values ν. As in the classical case, we must add a *uniformity condition* to derive a proper notion of complexity, meaning that the design of circuit C_ν may be built in time at most polynomial in ν. The complexity of an algorithm is then defined as the size of the circuit C_ν (as for classical circuits, the size of C_ν is the number of gates in C_ν).

These definitions deserve a few further comments. First of all, one could think that this definition of quantum algorithms is rather restrictive and that it could be interesting to make use of quantum processes that do not fit in this definition.

For instance, it could be possible to prepare the quantum register in a state that does not belong to the computational basis, or similarly measure this register in another basis. However, such generalized algorithms could easily be translated into our more restrictive definition just by adding some gates at the beginning and the end of the quantum circuit which rotate the generalized basis into the computational one or vice-versa. Similarly, the use of a *projective* measurement does not induce a loss of generality as we have seen that any measurement, including the most general POVM-type, may be reduced to a projective measurement with the help of ancillae.

Furthermore, one could design quantum algorithms with intermediate measurements instead of only one final measurement. Nonetheless, it is possible to show that this kind of algorithm could also be translated into our model, just by postponing any measurement to the end of the algorithm. This is true even when the subsequent computation depends on the outcome of the intermediate measurements, although in such a case ancillae are needed. The trick is simply to perform the subsequent computation conditionally to these ancillae that will only be measured at the end of the algorithm.

Finally, a peculiarity of Quantum Computation is that a universal set of quantum gates may only simulate an arbitrary quantum gate up to some error. Since these errors could accumulate as the size of the circuit C_ν increases with ν, one could wonder if all universal sets will yield an equivalent notion of complexity when errors are taken into account. Fortunately, it is indeed the case because we are only interested in the overall scaling of the complexity. More precisely, we will consider an algorithm efficient if it can solve a problem with a probability higher that $2/3$ and a complexity that grows at most polynomially in ν. Similarly to the classical class BPP, we then define the quantum class BQP, for *bounded error quantum polynomial*, that includes any problem that may be solved by such an efficient algorithm. It may be shown that the error introduced when simulating any quantum gate by a universal set may be reduced to ϵ using a circuit of elementary gates whose size grows poly-logarithmically in $O(1/\epsilon)$ only[13]. It implies that compensating the accumulation of errors along a circuit only introduces a poly-logarithmic overhead and therefore does not affect the definition of the class BQP.

A central question for Quantum Computation is whether BPP=BQP, that is, whether there exist problems that may be solved efficiently by a quantum computer but not by a classical one. Even though this question remains open, there exist problems which are known to belong to the class BQP but for which no efficient classical algorithm is known. The first remarkable achievement was the discovery by Peter Shor of an efficient quantum algorithm for the factorization of large numbers [Sho94]. Indeed, it is sill unknown whether this problem belongs to the class BPP, but as for now it has not been possible to prove that no efficient classical algorithm exists for this problem. As it is unnecessary for our purposes, we will not expose Shor's algorithm in this thesis, but in the next chapter we give some other examples, beginning with Deutsch's algorithm, a rather simple algorithm that nevertheless shows the basic principles of Quantum Computation lying at the core of Shor's algorithm.

[13] The notion of error on unitary operators will be defined more precisely later.

Chapter 2

Grover's algorithm

Introduction

As soon as the idea of Quantum Computation was proposed, the quest for quantum algorithms that could beat classical ones was launched. Following this, different algorithms paved the way to Shor's factoring algorithm, one of the earliest being Deutsch's algorithm in 1985 [Deu85], which we describe in this chapter. This algorithm is able to tell whether a 1-bit to 1-bit function is constant or balanced with only one call to the function, while classically two calls are necessary. Later, Deutsch and Jozsa [DJ92] generalized this algorithm to the case of a ν-bits to 1-bit function, showing that a quantum algorithm could find if such a function was constant or balanced with only one function call, while any classical algorithm needed $\nu/2+1$ calls to solve this problem with certainty. However, this comparison was not very fair as actually the problem is not classically hard if we do not require absolute certainty but only exponentially low error probability.

Building on the ideas developed for these algorithms, Bernstein and Vazirani [BV93], and later Simon [Sim94], did define related problems that could be solved with a quantum algorithm with exponentially less function calls than any –even probabilistic– classical algorithm. Nonetheless, this only proved that BPP≠BPQ *relatively to an oracle*. Indeed, the problems addressed by all these algorithms are expressed in the so-called oracle model of computation, where the complexity of an algorithm is defined as the number of calls to a particular function, usually called the *oracle*.

Later on, inspired by these algorithms, Shor discovered his famous polynomial algorithm for factoring [Sho94], proving that this problem is in BQP, while no efficient classical algorithm for factoring has been found so that it is not known whether this problem is in BPP or not. Shor's algorithm generated a large family of quantum algorithms, but we will not describe it here as actually, all the algorithms developed in this thesis belong to another family of quantum algorithms, which have as common parent an oracle-based algorithm, devised by Grover [Gro96]. Therefore, after a description of Deutsch's algorithm and the introduction of the oracle model of computation, this chapter will directly focus on Grover's algorithm.

2.1 Deutsch's algorithm

Let us consider a very simple problem. Suppose we have a 1-bit to 1-bit function f:

$$f : \{0,1\} \to \{0,1\} : x \mapsto f(x). \tag{2.1}$$

Such a function may be either *constant* if $f(0) = f(1)$ or *balanced* if $f(0) \neq f(1)$. The problem is to find if f is constant or balanced by calling the function a minimum number of times.

Classically, it is clear that two calls are required, one to evaluate $f(0)$ and another to evaluate $f(1)$, in order to finally compare these values and conclude on the type of function. Amazingly, David Deutsch proposed a quantum algorithm that performs the same task with only one call to the function.

Let us describe Deutsch's algorithm. As the function f, that we will call the oracle, is generally irreversible, it has to be slightly modified for the sake of Quantum Computation, in order to make it reversible. We thus have to add a second output register that keeps the value of the input, redefining the oracle as[1]

$$\tilde{f} : \{0,1\} \to \{0,1\}^2 : x \mapsto (x, f(x)). \tag{2.2}$$

As quantum gates are unitary operators, that preserve the number of qubits, the corresponding quantum oracle also requires an extra qubit register at the input, and thus takes the form

$$O_f : \mathcal{H}_2 \otimes \mathcal{H}_2 \to \mathcal{H}_2 \otimes \mathcal{H}_2 : |x_1\rangle \otimes |x_2\rangle \mapsto |x_1\rangle \otimes |f(x_1) \oplus x_2\rangle, \tag{2.3}$$

where $\oplus$ stands for the addition modulo 2. We see that if we prepare this extra register in the blank state $|0\rangle$, this quantum oracle effectively maps an input state $|x\rangle \otimes |0\rangle$ (where x takes value 0 or 1) to

$$O_f|x\rangle \otimes |0\rangle = |x\rangle \otimes |f(x)\rangle, \tag{2.4}$$

similarly to the reversible classical oracle $\tilde{f}$.

Now suppose instead that we prepare the extra register in the superposition state $(|0\rangle - |1\rangle)/\sqrt{2}$, which may be obtained from the state $|0\rangle$ by successive applications of the NOT gate $U_\neg$, that we already know, and the Hadamard gate W, that takes in the computational basis the matrix form[2]

$$W = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \tag{2.5}$$

that is, it maps $|0\rangle$ to $(|0\rangle + |1\rangle)/\sqrt{2}$ and $|1\rangle$ to $(|0\rangle - |1\rangle)/\sqrt{2}$, so that

$$WU_\neg|0\rangle = W|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \tag{2.6}$$

The oracle O_f then acts as

$$\begin{aligned} O_f|x\rangle \otimes \frac{1}{\sqrt{2}}[|0\rangle - |1\rangle] &= |x\rangle \otimes \frac{1}{\sqrt{2}}[|f(x)\rangle - |f(x) \oplus 1\rangle] && (2.7) \\ &= (-1)^{f(x)}|x\rangle \otimes \frac{1}{\sqrt{2}}[|0\rangle - |1\rangle], && (2.8) \end{aligned}$$

[1] It is straightforward to check that making the function reversible does not give any advantage in the classical case.

[2] This gate is sometimes called the Walsh-Hadamard gate, and even though the notation H is more widely used, we will use the notation W to avoid confusion with a Hamiltonian.

effectively inverting the sign of states $|x\rangle$ for which $f(x) = 1$. In this case, the second register keeps its original state during the application of O_f and therefore may be put away, so that we may practically implement a new operator

$$U_f : \mathcal{H}_2 \to \mathcal{H}_2 : |x\rangle \mapsto (-1)^{f(x)}|x\rangle, \tag{2.9}$$

using the quantum circuit illustrated in Fig. 2.1.

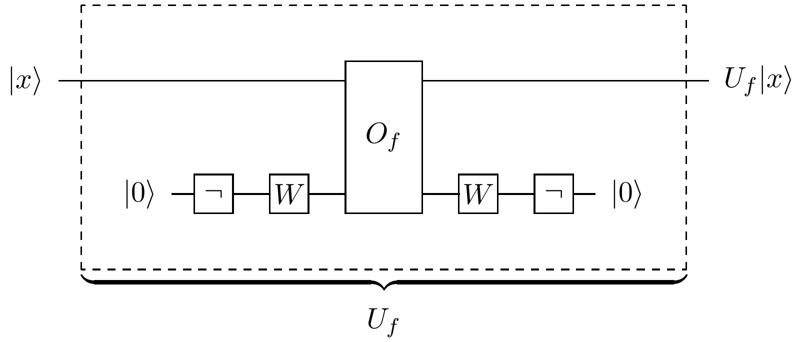

Figure 2.1: Circuit used to implement the operator U_f from the oracle O_f using one ancilla prepared in state $|0\rangle$, Hadamard (W) and NOT ($\neg$) gates.

Now suppose that instead of preparing the input register in one of the computational basis states $|0\rangle$ or $|1\rangle$, we prepare it in a superposition of both $(|0\rangle + |1\rangle)/\sqrt{2}$, a state that may once again be easily obtained with the help of the Hadamard gate W. The circuit U_f then acts as

$$\begin{aligned} U_f \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) &= \frac{1}{\sqrt{2}} \Big((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle \Big) && (2.10) \\ &= \frac{(-1)^{f(0)}}{\sqrt{2}} \Big(|0\rangle + (-1)^{f(0)\oplus f(1)}|1\rangle \Big) && (2.11) \\ &= (-1)^{f(0)} \begin{cases} W|0\rangle & \text{if } f(0) = f(1), \\ W|1\rangle & \text{if } f(0) \neq f(1). \end{cases} && (2.12) \end{aligned}$$

We see that the output states corresponding to constant or balanced functions are different, and –even better– orthogonal, such that a quantum measurement may discriminate between these two cases with success probability one. As we assumed in our computational model that the final measurement is made in the computational basis, we still have to rotate these states to this basis by applying once more the Hadamard gate W. As[3] $W^2 = I_2$ (where I_2 is the identity on $\mathcal{H}_2$), a measurement of the state in the computational basis will at this point yield $|0\rangle$ if the function f is constant and $|1\rangle$ if it is balanced. What happens is that in the case of a constant function, the quantum interferences are constructive for $|0\rangle$ and destructive for $|1\rangle$, while it is exactly the contrary for a balanced function.

Putting back things together, the whole circuit of Deutsch's algorithm is illustrated on Fig. 2.2. We see that it allows to tell whether a given function is either constant or balanced

[3] It immediately follows from the definition of the Hadamard operator W that it is both unitary and Hermitian, so that $W = W^\dagger = W^{-1}$.

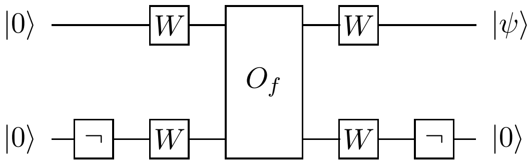

Figure 2.2: Quantum circuit for Deutsch's algorithm. Up to an irrelevant global phase, the output register $|\psi\rangle$ ends up in state $|0\rangle$ if the function f is constant or $|1\rangle$ if it is balanced.

with only one call to the function. The trick is that instead of evaluating $f(x)$ successively for $x = 0$ and for $x = 1$ as in the classical case, we have accessed the function only once with x being in a quantum superposition of both. Doing this, we have not completely identified the function as we still do not know the values of $f(0)$ and $f(1)$, but we have been able to compare these values, by measuring $f(0) \oplus f(1)$, using quantum interferences. It is precisely building on such ideas that more complex quantum algorithms were developed, such as Shor's algorithm for factoring or Grover's algorithm for database search.

2.2 The oracle model

In Deutsch's algorithm, we were not interested in the complexity as defined in Chapter 1, that is the depth of the quantum circuit, but only in the number of times a particular gate, namely O_f, was applied. This issue actually defines another model of complexity, where all the gates may be used for free except a particular gate called the oracle. The oracle acts as a *black-box*, meaning that we are allowed to use it in a logical circuit but we do not know what it exactly computes. In the *oracle model* of computation, a problem is then expressed as finding some property about the function computed by the oracle, and its complexity is defined as the minimal number of times the oracle has to be consulted in order to do so.

Besides the –rather academic– problem of distinguishing constant from balanced functions, another typical problem expressed in the oracle model, that will be intensively studied in this thesis, is the search in an unstructured database. In this case, one oracle query corresponds to one look at some element in the database, and the problem is to find a particular marked element. This is the problem addressed by Grover's algorithm, which will be described in the next section and on which most of the work in this thesis will build.

2.3 Grover's algorithm

2.3.1 Search in an unstructured database

Suppose we have a database of N items among which some are marked, through a function $f(n)$ such that

$$f : \mathcal{N} \to \{0,1\} : n \mapsto \left\{ \begin{array}{ll} 0 & n \notin \mathcal{M} \\ 1 & n \in \mathcal{M}, \end{array} \right. \tag{2.13}$$

where $\mathcal{N}$ denote the set of N items and $\mathcal{M} \subset \mathcal{N}$ is the set of marked ones, that we will consider as the solutions of the problem (see Table 2.3.1). This function is supposed unknown ($\mathcal{M}$ is not known) but may be queried as a black-box.

n	0	1	2	3	4	5	6	...	$N-1$
$f(n)$	0	0	1	0	1	0	0	...	0

Table 2.1: The problem oracle: a function $f(n)$ that maps N elements to a value 0 or 1. The elements mapped to 1 define the set of solutions $\mathcal{M}$. Each oracle call consists in the evaluation of one value $f(n)$.

The problem we study is to find a solution accessing the database a minimum number of times, that is, with a minimum number of queries to the oracle. This problem is therefore expressed in the oracle model, and its complexity will be defined as the number of queries to the oracle required by an algorithm to solve it. Classically, the very naïve algorithm consisting in successive calls to the oracle with random entries until finding a solution will require an average number of queries of order $O(N/M)$, where $M = \sharp\mathcal{M}$ is the number of marked items. If the database has no known structure (the case of a structured database will be studied in Chapter 6), this naïve algorithm is optimal and therefore the classical complexity is $\Theta(N/M)$. We will now show that its quantum complexity is $\Theta(\sqrt{N/M})$.

2.3.2 The quantum oracle

As for Deutsch's problem, the oracle has to be made reversible in the quantum case and therefore takes the form

$$O_f : \mathcal{H}_N \otimes \mathcal{H}_2 \to \mathcal{H}_N \otimes \mathcal{H}_2 : |n\rangle \otimes |q\rangle \mapsto |n\rangle \otimes |f(n) \oplus q\rangle, \tag{2.14}$$

where the basis states $|n\rangle$ of the N-dimensional Hilbert space $\mathcal{H}_N$ correspond to the N candidate solutions $n \in \mathcal{N}$. This quantum oracle acts on two registers, one N-dimensional Hilbert space $\mathcal{H}_N$ which contains the input of the oracle call and one 2-dimensional Hilbert space $\mathcal{H}_2$ (that is a qubit) which will contain its output. By preparing this second register in the superposition $\frac{1}{\sqrt{2}}[|0\rangle - |1\rangle]$, we have

$$\begin{aligned} O_f|n\rangle \otimes \frac{1}{\sqrt{2}}[|0\rangle - |1\rangle] &= |n\rangle \otimes \frac{1}{\sqrt{2}}[|f(n)\rangle - |f(n) \oplus 1\rangle] && (2.15)\\ &= (-1)^{f(n)}|n\rangle \otimes \frac{1}{\sqrt{2}}[|0\rangle - |1\rangle], && (2.16) \end{aligned}$$

exactly as for Deutsch's algorithm, so that we may implement an operator

$$U_f : \mathcal{H}_N \to \mathcal{H}_N : |n\rangle \mapsto (-1)^{f(n)}|n\rangle \tag{2.17}$$

that inverts the sign of the solution states, using a circuit similar to that of Fig. 2.1. As this is the operator that we will actually need in Grover's algorithm, we will now directly consider U_f as the oracle. Let us note that it may be rewritten in the simple form

$$U_f = I_N - 2 \sum_{m \in \mathcal{M}} |m\rangle\langle m|, \tag{2.18}$$

where I_N is the identity on $\mathcal{H}_N$.

2.3.3 The algorithm

Initially, we have no idea of what the solutions are, so we prepare the system in a uniform superposition of all possible solutions

$$|\mathcal{N}\rangle = \frac{1}{\sqrt{N}} \sum_{n\in\mathcal{N}} |n\rangle. \tag{2.19}$$

This state may easily be obtained by applying a Hadamard gate W on each of the $\nu = \log_2 N$ qubits[4] realizing the quantum register $\mathcal{H}_N$, initially prepared in state $|0\rangle$:

$$\begin{aligned}(W|0\rangle)^{\otimes\nu} &= \left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)^{\otimes\nu} && (2.20)\\ &= \frac{1}{\sqrt{2^\nu}} \sum_{n_1,\ldots,n_\nu=0,1} |n_1\rangle\otimes\ldots\otimes|n_\nu\rangle && (2.21)\\ &= \frac{1}{\sqrt{N}}\sum_{n\in\mathcal{N}}|n\rangle && (2.22)\\ &= |\mathcal{N}\rangle, && (2.23)\end{aligned}$$

where n is written as a binary string of length ν, $n = (n_1, \ldots, n_\nu)$. The algorithm also requires the operation

$$U_0 = W^{\otimes\nu}(I_N - 2|0\rangle\langle 0|)W^{\otimes\nu} = I_N - 2|\mathcal{N}\rangle\langle\mathcal{N}|, \tag{2.24}$$

which is simply the oracle operation when there is a single solution $m = 0$, rotated in the Hadamard basis.

Defining the state $|\mathcal{M}\rangle$ as the uniform superposition of solution states

$$|\mathcal{M}\rangle = \frac{1}{\sqrt{M}} \sum_{m\in\mathcal{M}} |m\rangle, \tag{2.25}$$

we see that both U_0 and U_f leave the sub-space spanned by $|\mathcal{N}\rangle$ and $|\mathcal{M}\rangle$ invariant:

$$\begin{array}{rclcrcl} U_0|\mathcal{N}\rangle &=& -|\mathcal{N}\rangle & & U_f|\mathcal{N}\rangle &=& |\mathcal{N}\rangle - 2x|\mathcal{M}\rangle \\ U_0|\mathcal{M}\rangle &=& |\mathcal{M}\rangle - 2x|\mathcal{N}\rangle & & U_f|\mathcal{M}\rangle &=& -|\mathcal{M}\rangle, \end{array} \tag{2.26}$$

where[5]

$$x = \langle\mathcal{M}|\mathcal{N}\rangle = \sqrt{\frac{M}{N}}. \tag{2.27}$$

Let us now define the operator $G = -U_0U_f$ as the Grover iteration. Grover's algorithm simply consists in successive applications of G (see Fig. 2.3). Just like U_0 and U_f, G leaves the

[4] We assume that N is an integer power of 2, such that we may implement the register $\mathcal{H}_N$ using ν qubits, associating each element $n \in \mathcal{N}$ with a binary string of length ν. If this is not the case, we may pad $\mathcal{N}$ with additional elements and define an extension of the oracle function $f(n)$ that takes value 0 for these additional elements. This will not affect the algorithm complexity for $N/M \to \infty$.

[5] We will use the notation $x = \sqrt{M/N}$, here and in following chapters related to search problems, on one hand because it will lighten mathematical expressions, but also because we will derive complexities in the limit $N \gg M$, that is $x \ll 1$.

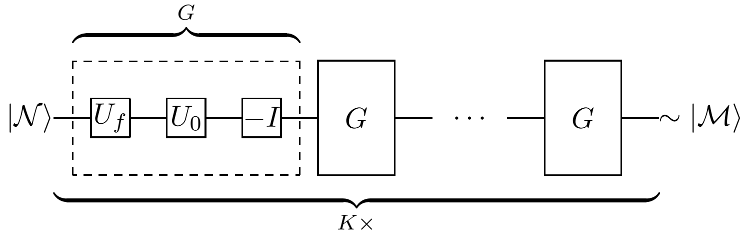

Figure 2.3: Grover's algorithm, consisting in $K = O(\sqrt{N/M})$ successive applications of the Grover iteration G.

sub-space spanned by $|\mathcal{N}\rangle$ and $|\mathcal{M}\rangle$ invariant and thus the system will stay in this sub-space. In the orthonormal basis $(|\mathcal{M}\rangle, |\mathcal{M}^C\rangle)$ of this sub-space, where

$$\begin{aligned} |\mathcal{M}^C\rangle &= \frac{1}{\sqrt{N-M}} \sum_{n\in\mathcal{N}\setminus\mathcal{M}} |n\rangle && (2.28) \\ &= \sqrt{\frac{N}{N-M}}|\mathcal{N}\rangle - \sqrt{\frac{M}{N-M}}|\mathcal{M}\rangle && (2.29) \end{aligned}$$

is the uniform superposition over the set of unmarked states $\mathcal{M}^C = \mathcal{N}\setminus\mathcal{M}$, G takes in matrix notation the form

$$\begin{aligned} G &= \begin{pmatrix} 1-2x^2 & 2x\sqrt{1-x^2} \\ -2x\sqrt{1-x^2} & 1-2x^2 \end{pmatrix} && (2.30) \\ &= \begin{pmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{pmatrix}, && (2.31) \end{aligned}$$

where

$$\alpha = \arcsin 2x\sqrt{1-x^2}. \tag{2.32}$$

We see that G is a rotation of angle α in this sub-space and therefore G^k is a rotation of angle $k\alpha$

$$G^k = \begin{pmatrix} \cos k\alpha & \sin k\alpha \\ -\sin k\alpha & \cos k\alpha \end{pmatrix} \tag{2.33}$$

As the system is initially in the state

$$\begin{aligned} |\psi_0\rangle &= |\mathcal{N}\rangle && (2.34) \\ &= x|\mathcal{M}\rangle + \sqrt{1-x^2}|\mathcal{M}^C\rangle, && (2.35) \end{aligned}$$

we get after k iterations

$$\begin{aligned} |\psi_k\rangle &= G^k|\mathcal{N}\rangle && (2.36) \\ &= \left(\sqrt{1-x^2}\sin k\alpha + x\cos k\alpha\right)|\mathcal{M}\rangle \\ &\quad + \left(\sqrt{1-x^2}\cos k\alpha - x\sin k\alpha\right)|\mathcal{M}^{\mathcal{C}}\rangle, && (2.37) \end{aligned}$$

i.e. the amplitude of marked states is progressively amplified as $\sin k\alpha$ approaches 1 (more precisely, we would have $|\psi_k\rangle = |\mathcal{M}\rangle$ for $\sin k\alpha = \sqrt{1-x^2}$). At this point, a measure of the register will yield a marked state with high probability.

To identify the number of iterations k for which $|\psi_k\rangle$ is as close as possible to $|\mathcal{M}\rangle$, let us consider the limit of a large database $x \ll 1$. In this limit, the initial state $|\mathcal{N}\rangle$ is approximately orthogonal to the solution state $|\mathcal{M}\rangle$ ($\langle\mathcal{M}|\mathcal{N}\rangle = x \approx 0$), such that we have to rotate it by a total angle of order $\pi/2$. As the angle of rotation of one iteration becomes

$$\alpha = 2x\left(1 + O(x^2)\right), \tag{2.38}$$

this will approximatively be achieved after

$$\begin{aligned} K &= \left\lfloor \frac{\pi}{4x} \right\rfloor & (2.39)\\ &= \frac{\pi}{4x}\left(1 + O(x)\right) & (2.40)\end{aligned}$$

iterations, where $\lfloor n \rfloor$ is the closest integer lower than n (K has to be integer so that we have to round $\pi/(4x)$). Indeed, Eq. (2.37) gives in the limit of large problems ($x \to 0$)

$$|\psi_k\rangle = \left(\sin k\alpha|\mathcal{M}\rangle + \cos k\alpha|\mathcal{M}^{\mathcal{C}}\rangle\right)\left(1 + O(x)\right) \tag{2.41}$$

and more precisely for $k = K$

$$\langle\mathcal{M}|\psi_K\rangle = 1 - O(x^2). \tag{2.42}$$

Thus, by measuring the register after

$$K = \frac{\pi}{4}\sqrt{\frac{N}{M}}\left(1 + O\left(\sqrt{\frac{M}{N}}\right)\right) \tag{2.43}$$

iterations, we obtain a marked item $m \in \mathcal{M}$ with a probability close to 1 (it must be checked with one more query that we actually found a marked item, if this is not the case, we just start the algorithm again from the beginning). As each Grover iteration requires one call to the oracle, this is a quadratic speed-up with respect to an optimal classical search, which requires a number of calls of order $\Theta(N/M)$. It may be shown that this algorithm is optimal, in the sense that there is no other quantum algorithm solving this problem with less than $\Theta(\sqrt{N/M})$ queries [BBBV97, Zal99].

2.3.4 Case of an unknown number of solutions

In the last section, we have implicitly supposed that the number of solutions M was known, as it was required to evaluate the number of iterations K of the algorithm. However, it is possible to slightly modify the algorithm to deal with the case of an unknown number of marked items M. In that case, M could be any number between N and 1, and therefore the actual number of Grover iterations needed K varies between 0 and $K_{\max} = (\pi/4)\sqrt{N}$. The modified algorithm simply consists in choosing a random value $\tilde{K}$ such that $0 \le \tilde{K} \le K_{\max}$ and then run Grover's algorithm as if $\tilde{K}$ was the actual number of iterations needed K. It may be shown that this algorithm will output a solution with a probability close to 1/2. This success probability may then be amplified to $1 - 1/2^t$ by repeating the algorithm t times.

2.4 Analog quantum search

2.4.1 Hamiltonian-based algorithms

While Grover's algorithm stays within the standard paradigm of Quantum Computation, that is a sequence of quantum gates (i. e., unitary operators) successively applied on a quantum register, recent developments have introduced a new type of quantum algorithms based on a continuous-time Hamiltonian evolution, including, for instance, continuous-time quantum walks [CCD$^+$03] or quantum algorithms by adiabatic evolution[FGGS00, vDMV01]. In Chapter 5, we will justify that these are genuine quantum algorithms as they may be simulated on a traditional quantum circuit by discretization.

In this section, we expose a time-independent Hamiltonian evolution, proposed by Farhi *et al* [FG98a], that is able to perform a quantum search in a time of order $\Theta(\sqrt{N/M})$, similarly to Grover's algorithm. In contrast to the discrete time evolution of Grover's algorithm, and following the authors, we will use the term "analog" to qualify this continuous-time algorithm.

2.4.2 The problem and the Hamiltonian oracle

The problem we will study is exactly the same as for Grover's algorithm, that is, the search of unknown marked items in an unstructured database. However, the oracle is formulated differently: while it was given as a unitary operator U_f inverting the sign of the states corresponding to marked items $m \in \mathcal{M}$ (see Eq. (2.17)), it now takes the form of a Hamiltonian H_f acting as

$$H_f : \mathcal{H}_N \to \mathcal{H}_N : |n\rangle \mapsto \bar{E}(1 - f(n))|n\rangle, \tag{2.44}$$

where $f(n)$ is, as in the last chapter, a function taking the value 1 for marked items $m \in \mathcal{M}$ and 0 elsewhere, while $\bar{E}$ is some energy fixing the strength of the Hamiltonian. The application of H_f during a time t induces the unitary evolution operator

$$e^{-\frac{iH_f t}{\hbar}} : \mathcal{H}_N \to \mathcal{H}_N : |n\rangle \mapsto e^{-i(1-f(n))\frac{\bar{E}t}{\hbar}}|n\rangle. \tag{2.45}$$

We immediately see that for $\bar{E}t/\hbar = \pi$, we recover the unitary oracle $-U_f$, which is a first argument for considering H_f as the Hamiltonian oracle equivalent to U_f. In Chapter 5, we will also show that the unitary evolution operator induced by H_f during an arbitrary time may be simulated by a quantum circuit using two calls to the unitary oracle O_f, which completes this justification.

While the complexity of the discrete algorithm was defined, according to the oracle model, as the number of calls to the unitary oracle, the complexity of its analog analogue will be defined as the total time of the evolution under the influence of the Hamiltonian oracle (for a fixed energy $\bar{E}$). Finally, let us also note that the Hamiltonian H_f may be rewritten as

$$H_f = \bar{E}(I_N - \sum_{m \in \mathcal{M}} |m\rangle\langle m|). \tag{2.46}$$

2.4.3 The algorithm

In addition to the oracle Hamiltonian H_f, we will need a second Hamiltonian

$$H_0 = W^{\otimes\nu}\bar{E}(I_N - |0\rangle\langle 0|)W^{\otimes\nu} = \bar{E}(I_N - |\mathcal{N}\rangle\langle\mathcal{N}|), \tag{2.47}$$

which is related to U_0 as defined in Eq. (2.24) in the same way as H_f is related to U_f. The algorithm consists in preparing the system in the uniform superposition $|\psi(t=0)\rangle = |\mathcal{N}\rangle$, exactly as for Grover's circuit-based algorithm, and then having it evolve under the time-independent Hamiltonian $H = H_0 + H_f$. Solving the Schrödinger equation (1.7), a simple calculation shows that[6]

$$\begin{aligned} |\psi(t)\rangle &= e^{-\frac{iHt}{\hbar}}|\mathcal{N}\rangle \\ &= e^{-\frac{i\bar{E}t}{\hbar}}\left(i\sin\frac{\bar{E}xt}{\hbar} + x\cos\frac{\bar{E}xt}{\hbar}\right)|\mathcal{M}\rangle \\ &\quad + e^{-\frac{i\bar{E}t}{\hbar}}\sqrt{1-x^2}\cos\frac{\bar{E}xt}{\hbar}|\mathcal{M}^C\rangle. \end{aligned} \tag{2.48}$$

Thus, the quantum search simply works via a rotation from $|\mathcal{N}\rangle$ to $|\mathcal{M}\rangle$, just as Grover's traditional algorithm. The solution state $|\mathcal{M}\rangle$ is thus obtained with probability 1 if we apply H during a time

$$T = \frac{\pi}{2}\sqrt{\frac{N}{M}}\frac{\hbar}{\bar{E}}, \tag{2.49}$$

which is comparable to the total number of iterations in Grover's algorithm. We also see that the computation may be sped up by increasing the energy $\bar{E}$. However, the energy available for the computation is practically limited so that we should consider it fixed to a constant value. Let us also note that this issue becomes particularly important if we are to fairly compare the running time of different Hamiltonian-based algorithms, as will be pointed out in the proof of optimality given in Chapter 4.

[6] As in the previous section, we use the notation $x = \sqrt{M/N}$.

Chapter 3

The Adiabatic Theorem

Introduction

The adiabatic approximation is a standard method of Quantum Mechanics used to derive approximate solutions of the Schrödinger equation in the case of a slowly varying Hamiltonian. Its basic principle is quite simple: if a quantum system is prepared in its ground state and its Hamiltonian varies slowly enough, it will stay in a state close to the instantaneous ground state of this Hamiltonian as time goes on.

Actually, this approximation was initially introduced as a means to study approximatively complex quantum systems such as molecules, and the derivation found in the literature is often somewhat intuitive at some points, and therefore leads to a rather qualitative statement of the Adiabatic Theorem that is at the basis of this approximation. While a rigorous proof of the theorem is well known (see for instance [Mes59]), it is generally formulated in a way that is not directly applicable to our purposes, that is, to design new quantum algorithms and to evaluate their complexity rigorously.

For this reason, after summarizing a quite classical version of the adiabatic approximation as derived in most standard books of Quantum Mechanics [Sch55], we give in this chapter a new formulation of the proof of the Adiabatic Theorem, and state it in a way that is specifically adapted to our purposes. Finally, we use this theorem to define the so-called quantum algorithms by adiabatic evolution (as proposed by Farhi *et al* in [FGGS00]) and then we derive a method to evaluate their complexity.

3.1 The standard adiabatic approximation

3.1.1 The Schrödinger equation

Let us solve the Schrödinger equation in the case of a time-dependent Hamiltonian (see [Sch55] for details):

$$i\hbar\frac{d}{dt}|\psi(t)\rangle = H(t)|\psi(t)\rangle, \tag{3.1}$$

with the initial condition that $|\psi(0)\rangle$ is the ground state of $H(0)$. First of all, we need to define the instantaneous eigenstates $|\varphi_k(t)\rangle$ of the Hamiltonian $H(t)$

$$H(t)|\varphi_k(t)\rangle = E_k(t)|\varphi_k(t)\rangle, \tag{3.2}$$

where $E_0(t) < E_1(t) < \ldots < E_{N-1}(t)$ are the corresponding eigenenergies[1]. Together with the normalization condition

$$\langle\varphi_k(t)|\varphi_k(t)\rangle = 1, \tag{3.3}$$

this defines the eigenstates $|\varphi_k(t)\rangle$ only up to an arbitrary phase. To suppress this ambiguity, we will use an additional condition.

3.1.2 Phase choice

Let us impose the phase condition[2]

$$\langle\varphi_k(t)|\frac{d}{dt}|\varphi_k(t)\rangle = 0 \quad \forall k. \tag{3.4}$$

This is always possible, as from an arbitrary set of normalized eigenstates $|\tilde{\varphi}_k(t)\rangle$, we may consider the eigenstates with modified phases

$$|\varphi_k(t)\rangle = e^{i\phi_k(t)}|\tilde{\varphi}_k(t)\rangle, \tag{3.5}$$

where $\phi_k(t)$ is a phase defined by some real function. The condition (3.4) then gives

$$\frac{d}{dt}\phi_k(t) = i\langle\tilde{\varphi}_k(t)|\frac{d}{dt}|\tilde{\varphi}_k(t)\rangle. \tag{3.6}$$

and integrating this expression yields the adequate real phase-function $\phi_k(t)$, as the differentiation of the normalization condition (3.3) ensures that this function is real.

$$\begin{aligned} \left(\frac{d}{dt}\langle\tilde{\varphi}_k(t)|\right)|\tilde{\varphi}_k(t)\rangle + \langle\tilde{\varphi}_k(t)|\left(\frac{d}{dt}|\tilde{\varphi}_k(t)\rangle\right) &= 0 \qquad (3.7)\\ \Rightarrow \left(\langle\tilde{\varphi}_k(t)|\frac{d}{dt}|\tilde{\varphi}_k(t)\rangle\right)^\dagger + \langle\tilde{\varphi}_k(t)|\frac{d}{dt}|\tilde{\varphi}_k(t)\rangle &= 0 \qquad (3.8)\end{aligned}$$

3.1.3 Implicit solution

To solve the Schrödinger equation, we develop its solution $|\psi(t)\rangle$ in the basis formed by the eigenstates $|\varphi_k(t)\rangle$:

$$|\psi(t)\rangle = \sum_k b_k(t)e^{-i\int_0^t \frac{E_k(t_1)}{\hbar}dt_1}|\varphi_k(t)\rangle. \tag{3.9}$$

Inserting this development into the Schrödinger equation (3.1) and projecting onto $\langle\varphi_l(t)|$, we get the following system for the amplitudes $b_k(t)$:

$$\dot{b}_k(t) = -\sum_l b_l(t)e^{i\int_0^t \omega_{kl}(t_1)dt_1}\langle\varphi_k(t)|\frac{d}{dt}|\varphi_l(t)\rangle, \tag{3.10}$$

where we have introduced the frequencies

$$\omega_{kl} = \frac{E_k - E_l}{\hbar}. \tag{3.11}$$

[1] We suppose that $E_k(t) \neq E_l(t)$ $(\forall k \neq l)$, that is, we exclude the cases of degeneracy ($E_k(t) = E_l(t)$ $\forall t$) or level-crossing ($E_k(t_1) = E_l(t_1)$ for some $t = t_1$). However, this development could be adapted to these cases with suitable modifications.

[2] Let us note that this choice corresponds to the cancellation of Berry's phase, which is irrelevant in this case.

To evaluate the matrix elements $\langle\varphi_k(t)|\frac{d}{dt}|\varphi_l(t)\rangle$ for $k \neq l$ (they cancel out for $k = l$ with our phase choice), we differentiate Eq. (3.2) with respect to time t and project onto $\langle\varphi_l(t)|$:

$$\langle\varphi_k(t)|\frac{d}{dt}|\varphi_l(t)\rangle = -\frac{\langle\varphi_k(t)|\frac{dH}{dt}|\varphi_l(t)\rangle}{E_k(t) - E_l(t)} \quad \forall k \neq l \tag{3.12}$$

and therefore our system may be rewritten

$$\dot{b}_k(t) = \sum_{l \neq k} b_l(t) e^{i\int_0^t \omega_{kl}(t_1)dt_1} \frac{\langle\varphi_k(t)|\frac{dH}{dt}|\varphi_l(t)\rangle}{E_k(t) - E_l(t)}. \tag{3.13}$$

If the system is initially in its ground state $|\psi(0)\rangle = |\varphi_0(0)\rangle$, the initial conditions are $b_k(0) = \delta_{0k}$ and we get after integration

$$b_k(t) = \delta_{0k} + \sum_{l \neq k} \int_0^t dt_1 b_l(t_1) e^{i\int_0^{t_1} \omega_{kl}(t_1')dt_1'} \omega_{kl}(t_1) A_{kl}(t_1), \tag{3.14}$$

where the elements $A_{kl}(t)$ are dimensionless and defined as

$$A_{kl}(t) = \hbar \frac{\langle\varphi_k(t)|\frac{dH}{dt}|\varphi_l(t)\rangle}{(E_k(t) - E_l(t))^2}. \tag{3.15}$$

This expression gives the exact solution to the Schrödinger equation, but only implicitly as the amplitudes $b_l(t)$ also appear in the right member.

3.1.4 Intuitive approximation

The adiabatic approximation, as stated for instance in [Sch55], follows from the intuition that if $H(t)$ varies very slowly, so will all other time-dependent quantities of the problem, such as $\omega_{kl}(t)$, $A_{kl}(t)$ and $b_k(t)$. Therefore, we may in first approximation replace $b_k(t)$ in the right member of the implicit solution by its initial value, $b_k(0) = \delta_{k0}$, which yields the approached solution:

$$b_k(t) \approx \int_0^t dt_1 e^{i\int_0^{t_1} \omega_{k0}(t_1')dt_1'} \omega_{k0}(t_1) A_{k0}(t_1) \qquad \forall k \neq 0. \tag{3.16}$$

Moreover, we may get an order of magnitude for the amplitude of the excited states $b_k(t)$ $(k \neq 0)$ by considering $A_{k0}(t)$ constant and factoring it out of the integral:

$$b_k(t) \approx -i\left[A_{k0}(t) e^{i\int_0^t \omega_{k0}(t')dt'} - A_{k0}(0)\right] \qquad \forall k \neq 0. \tag{3.17}$$

For this so-called "adiabatic approximation" to be valid, the probability to be away from the ground state $p(t) = \sum_{k\neq 0} |b_k(t)|^2$ has to remain small since we have used $b_0(t) = 1$, $\forall\ t$. This yields the "adiabatic condition"

$$\sum_{k \neq 0} |A_{k0}(t)|^2 \ll 1 \qquad \forall t \tag{3.18}$$

However, this derivation is clearly not a rigorous proof for this condition, and this will be the goal of the next section.

3.2 The adiabatic approximation revisited

3.2.1 Solution in terms of an expansion in successive orders of a slowness parameter

Let us rewrite the time-dependent Hamiltonian $H(t)$ as $\tilde{H}(s(t))$, where $\tilde{H}(s)$ is a parameterization of the path followed by $H(t)$ in the space of Hermitian operators, and write the speed ds/dt at which $H(t)$ travels through this path as

$$\frac{ds}{dt}(t) = \delta \; v(s(t)). \tag{3.19}$$

δ may be considered as a slowness parameter fixing the overall speed, while $v(s)$ contains the local speed variations along the path. Integrating this expression, we also define the function $s = s(t)$ and its inverse $t = t(s)$. We see that the evolution will be as close to adiabaticity as δ is close to 0, such that it seems natural to solve the problem for non-zero –but yet small– δ by expanding in successive orders of δ. We now have

$$A_{kl}(t) = \delta \; a_{kl}(s(t)) \tag{3.20}$$

where

$$a_{kl}(s) = \hbar \frac{\langle\tilde{\varphi}_k(s)|\frac{d\tilde{H}}{ds}|\tilde{\varphi}_l(s)\rangle}{(\tilde{E}_k(s) - \tilde{E}_l(s))^2} v(s), \tag{3.21}$$

$|\tilde{\varphi}_k(s)\rangle$ and $\tilde{E}_k(s)$ are the eigenstates and eigenenergies of $\tilde{H}(s)$

$$\begin{aligned} |\varphi_k(t)\rangle &= |\tilde{\varphi}_k(s(t))\rangle & (3.22)\\ E_k(t) &= \tilde{E}_k(s(t)). & (3.23) \end{aligned}$$

We may evaluate successive approximations $b_k^{(i)}(t)$ by recursive uses of the implicit expression for $b_k(t)$:

$$\begin{aligned} b_k^{(0)}(t) &= \delta_{0k} \\ b_k^{(1)}(t) &= \delta_{0k} + \delta \sum_{l\neq k} \delta_{0l} \int_0^t dt_1 e^{i\int_0^{t_1}\omega_{kl}(t_1')dt_1'}\omega_{kl}(t_1)a_{kl}(s(t_1)) & (3.24)\\ &\vdots \\ b_k^{(i+1)}(t) &= \delta_{0k} + \delta \sum_{l\neq k} \int_0^t dt_1 b_l^{(i)}(t_1) e^{i\int_0^{t_1}\omega_{kl}(t_1')dt_1'}\omega_{kl}(t_1)a_{kl}(s(t_1)). \end{aligned}$$

At first order, we simply have:

$$\begin{aligned} b_0^{(1)}(t) &= 1 & (3.25)\\ b_k^{(1)}(t) &= \delta \int_0^t dt_1 e^{i\int_0^{t_1}\omega_{k0}(t_1')dt_1'}\omega_{k0}(t_1)a_{k0}(s(t_1)) \qquad \forall\; k \neq 0, & (3.26) \end{aligned}$$

which coincides with Eq. (3.16). It is straightforward to check that this approximation satisfies the exact system (3.13) up to order δ.

3.2.2 The Adiabatic Theorem

From this first-order approximation, we now derive the Adiabatic Theorem. If A_{k0} and $(1/\omega_{k0})dA_{k0}/dt$ are differentiable, then the amplitudes $b_k^{(1)}(t)$ may be evaluated by two successive integrations by parts

$$b_k^{(1)}(t) = \delta \int_0^t dt_1 e^{i\int_0^{t_1}\omega_{k0}(t_1')dt_1'} \omega_{k0}(t_1) a_{k0}(s(t_1)) \tag{3.27}$$

$$\begin{aligned} &= -i\delta \left[a_{k0}(s(t_1)) e^{i\int_0^{t_1}\omega_{k0}(t_1')dt_1'}\right]_0^t + i\delta \int_0^t dt_1 e^{i\int_0^{t_1}\omega_{k0}(t_1')dt_1'} \frac{da_{k0}}{dt_1}(s(t_1)) \\ &= -i\delta \left[a_{k0}(s(t_1)) e^{i\int_0^{t_1}\omega_{k0}(t_1')dt_1'}\right]_0^t + \delta \left[\frac{1}{\omega_{k0}(t_1)} \frac{da_{k0}}{dt_1}(s(t_1)) e^{i\int_0^{t_1}\omega_{k0}(t_1')dt_1'}\right]_0^t \\ &+\delta \int_0^t dt_1 e^{i\int_0^{t_1}\omega_{k0}(t_1')dt_1'} \frac{d}{dt_1}\left(\frac{1}{\omega_{k0}(t_1)} \frac{da_{k0}}{dt_1}(s(t_1))\right) \end{aligned} \tag{3.28}$$

Using the functions $s(t)$ and $t(s)$, we may rewrite this expression as follows

$$\begin{aligned} b_k^{(1)}(t) &= -i\delta \left[a_{k0}(s_1) e^{i\int_0^{t(s_1)}\omega_{k0}(t_1')dt_1'}\right]_0^{s(t)} + \delta^2 \left[\frac{v(s_1)}{\tilde{\omega}_{k0}(s_1)} \frac{da_{k0}}{ds_1}(s_1) e^{i\int_0^{t(s_1)}\omega_{k0}(t_1')dt_1'}\right]_0^{s(t)} \\ &+\delta^2 \int_0^{s(t)} ds_1 e^{i\int_0^{t(s_1)}\omega_{k0}(t_1')dt_1'} \frac{d}{ds_1}\left(\frac{v(s_1)}{\tilde{\omega}_{k0}(s_1)} \frac{da_{k0}}{ds_1}(s_1)\right). \end{aligned} \tag{3.29}$$

Actually, the expressions behind δ and δ^2 do depend on δ, so that if we want to prove that the terms in δ^2 are negligible compared to the term in δ when $\delta \to 0$, we have to derive an upper bound for these expressions that is δ-independent. However, we see that they only depend on δ through the argument of the imaginary exponentials, which has modulus 1, so that we immediately have

$$\left| \left[\frac{v(s_1)}{\tilde{\omega}_{k0}(s_1)} \frac{da_{k0}}{ds_1}(s_1) e^{i\int_0^{t(s_1)}\omega_{k0}(t_1')dt_1'}\right]_0^{s(t)} \right| \tag{3.30}$$

$$\leq 2 \max_{s_1\in[0,1]} \left| \frac{v(s_1)}{\tilde{\omega}_{k0}(s_1)} \frac{da_{k0}}{ds_1}(s_1) \right| \tag{3.31}$$

and

$$\left| \int_0^{s(t)} ds_1 e^{i\int_0^{t(s_1)}\omega_{k0}(t_1')dt_1'} \frac{d}{ds_1}\left(\frac{v(s_1)}{\tilde{\omega}_{k0}(s_1)} \frac{da_{k0}}{ds_1}(s_1)\right) \right| \tag{3.32}$$

$$\leq \int_0^1 ds_1 \left| \frac{d}{ds_1}\left(\frac{v(s_1)}{\tilde{\omega}_{k0}(s_1)} \frac{da_{k0}}{ds_1}(s_1)\right) \right| \tag{3.33}$$

and that the amplitude $b_k(t)$ reduces at first order in δ to

$$b_k(t) = -i\delta \left[a_{k0}(s_1) e^{i\int_0^{t(s_1)}\omega_{k0}(t_1')dt_1'}\right]_0^{s(t)} + O(\delta^2). \tag{3.34}$$

We have recovered the adiabatic approximation (3.17) but within a more rigorous approach, and may now give a precise statement for the Adiabatic Theorem:

Theorem 1 (Adiabatic Theorem) *If*

1. *$\tilde{H}(s)$ is a continuous path in the space of Hermitian operators on a N-dimensional Hilbert space $\mathcal{H}_N$,*

2. *the quantum state $|\psi(t)\rangle$ belongs to $\mathcal{H}_N$, and is prepared at time $t = 0$ in the ground state of $\tilde{H}(s = 0)$,*

3. *it evolves under the influence of $H(t) = \tilde{H}(s(t))$ where $s(0) = 0$ and $ds/dt(t) = \delta\ v(s(t))$*

4. *$v(s)$ is a differentiable strictly positive real function,*

5. *the normalized instantaneous eigenstates $|\tilde{\varphi}_k(s)\rangle$ ($k = 0, \ldots, N-1$) of $\tilde{H}(s)$ are defined with a phase such that $\langle\tilde{\varphi}_k(s)|\frac{d}{ds}|\tilde{\varphi}_k(s)\rangle = 0 \quad \forall k$,*

6. *the corresponding instantaneous eigenvalues $\tilde{E}_0(s) < \tilde{E}_1(s) < \ldots < \tilde{E}_{N-1}(s)$ of $\tilde{H}(s)$, are non-degenerated,*

7. *the elements $a_{k0}(s)$, defined as*

$$a_{k0}(s) = \hbar \frac{\langle\tilde{\varphi}_k(s)|\frac{d\tilde{H}}{ds}|\tilde{\varphi}_0(s)\rangle}{(\tilde{E}_k(s) - \tilde{E}_0(s))^2} v(s) \qquad \forall\ k \neq 0, \tag{3.35}$$

their first derivative da_{k0}/ds, and the frequencies

$$\omega_{k0}(t) = \frac{\tilde{E}_k(s(t)) - \tilde{E}_0(s(t))}{\hbar} \tag{3.36}$$

are differentiable functions,

8. *the amplitudes $b_k(t)$ of $|\psi(t)\rangle$ in $|\tilde{\varphi}_k(s(t))\rangle$ are defined with a phase such that*

$$|\psi(t)\rangle = \sum_k b_k(t) e^{-i\int_0^t \frac{E_k(t_1)}{\hbar} dt_1} |\tilde{\varphi}_k(s(t))\rangle, \tag{3.37}$$

then the amplitudes of the excited states $b_k(t)$ are given for $\delta \to 0$ by

$$b_k(t) = -i\delta \left[a_{k0}(s_1) e^{i\int_0^{t(s_1)} \omega_{k0}(t_1')dt_1'} \right]_0^{s(t)} + O(\delta^2) \qquad \forall\ k \neq 0, \tag{3.38}$$

and the probability $p(t)$ to be away from the ground state is bounded in the same limit by

$$p(t) \leq 4 \sum_{k\neq 0} \max_{s' \in [0,s(t)]} |a_{k0}(s')|^2 \delta^2 + O(\delta^3). \tag{3.39}$$

The proof follows from above. We may now use this result to define a new type of computation, exploiting this adiabatic evolution.

3.3 Quantum computation by adiabatic evolution

3.3.1 Adiabatic evolution as an algorithm

Suppose we have to solve a problem that may be reformulated as preparing a quantum system in the ground state of a Hamiltonian H_f. The Adiabatic Theorem then provides a straightforward method to solve this problem:

- Prepare the quantum system in the (known and easy-to-prepare) ground state of another Hamiltonian H_0.
- Apply H_0 on the system and slowly modify it to H_f.

The Adiabatic Theorem ensures that if this has been done slowly enough, the system will end up in a state close to the ground state of H_f. It is then enough to measure the system in order to get the solution.

From now on, we will call this process an algorithm, even if this may seem abusive at first view. However, we will justify the use of this term in Chapter 5 by showing that, under some conditions on the initial and final Hamiltonians, this adiabatic evolution may be discretized in order to be implemented on a quantum circuit. We will also show that the complexity of the quantum algorithm designed with this method is directly deduced from the running time of the adiabatic evolution.

3.3.2 Running time of an adiabatic algorithm

Let us now focus on the running time T_δ, defined as the time necessary to switch adiabatically from H_0 to H_f while keeping the probability to excite the system away from the ground state $p(t)$ (that may be viewed as an error probability) less than δ^2. To make use of the Adiabatic Theorem, we will of course study this running time in the limit $\delta \to 0$. The path followed by the instantaneous Hamiltonian is defined as an interpolation between H_0 and H_f:

$$\tilde{H}(s) = (1-s)H_0 + sH_f, \tag{3.40}$$

where $s = s(t)$ is a monotonously increasing function with $s(0) = 0$ and $s(T_\delta) = 1$, chosen as to satisfy $p(t) \leq \delta^2$. The Adiabatic Theorem (3.39) states that it will be the case if

$$4 \sum_{k \neq 0} |a_{k0}(s(t))|^2 \leq 1 \quad \forall t, \tag{3.41}$$

or equivalently if

$$a(s)v(s) \leq 1 \quad \forall s, \tag{3.42}$$

where $a(s)$ is defined as

$$a(s) = 2\hbar \sqrt{\sum_{k \neq 0} \frac{|\langle \tilde{\varphi}_k(s)|H_f - H_0|\tilde{\varphi}_0(s)\rangle|^2}{(\tilde{E}_k(s) - \tilde{E}_0(s))^4}}. \tag{3.43}$$

We see that $a(s)$ only depends on the Hamiltonians H_0 and H_f, while $v(s)$ fixes the time-evolution of the algorithm, and may be optimized arbitrarily such as to satisfy the adiabatic condition (3.42) while reducing the running time

$$T_\delta = \frac{1}{\delta} \int_0^1 \frac{ds}{v(s)}. \tag{3.44}$$

To complete the description of our algorithm, we still need to choose an optimal $v(s)$ satisfying the condition (3.42), and therefore we have to evaluate $a(s)$.

3.3.3 Bounds for the adiabatic condition

In general, $a(s)$ is not known exactly, but it is possible to estimate a crude bound, as

$$\begin{aligned}
\sum_{k\neq 0} \frac{|\langle\tilde{\varphi}_k(s)|H_f - H_0|\tilde{\varphi}_0(s)\rangle|^2}{(\tilde{E}_k(s)-\tilde{E}_0(s))^4} &\leq \frac{\sum_{k\neq 0} |\langle\tilde{\varphi}_k(s)|H_f - H_0|\tilde{\varphi}_0(s)\rangle|^2}{(\tilde{E}_1(s)-\tilde{E}_0(s))^4} && (3.45)\\
&\leq \frac{\sum_{k} |\langle\tilde{\varphi}_k(s)|H_f - H_0|\tilde{\varphi}_0(s)\rangle|^2}{(\tilde{E}_1(s)-\tilde{E}_0(s))^4} && (3.46)\\
&= \frac{\|(H_f - H_0)|\tilde{\varphi}_0(s)\rangle\|^2}{(\tilde{E}_1(s)-\tilde{E}_0(s))^4} && (3.47)\\
&\leq \frac{\|\!|H_f - H_0|\!\|^2}{(\tilde{E}_1(s)-\tilde{E}_0(s))^4}, && (3.48)
\end{aligned}$$

where $\|\!|A|\!\| = \max_{|x\rangle:\||x\rangle\|=1} \|A|x\rangle\|$ is the operator norm of A. Finally, we simply have

$$\begin{aligned}
a(s) &\leq 2\hbar\frac{\|\!|H_f - H_0|\!\|}{g(s)^2} && (3.49)\\
&\leq 2\hbar\frac{\|\!|H_f - H_0|\!\|}{g_{\min}^2}, && (3.50)
\end{aligned}$$

where we have introduced the gap

$$g(s) = \tilde{E}_1(s) - \tilde{E}_0(s) \qquad (3.51)$$

between the ground state and the first excited state and its minimum value

$$g_{\min} = \min_{0\leq s\leq 1} g(s). \qquad (3.52)$$

Usually, the eigenvalues of the initial and final Hamiltonians H_0 and H_f are well known and it is therefore straightforward to derive an upper bound for $\|\!|H_f - H_0|\!\|$, such that the problem is to evaluate the minimum gap $g_{\min}$. The next section will shed more light on the importance of evaluating this minimum as we will see its scaling will directly fix the scaling of the running time.

3.4 Global versus local adiabatic evolution

The upper bound derived in the last section ensures that the adiabatic condition (3.42) is satisfied if we choose an evolution rate

$$v(s) = \frac{1}{2\hbar}\frac{g_{\min}^2}{\|\!|H_f - H_0|\!\|} \qquad (3.53)$$

that leads to a running time

$$T_\delta = \frac{2\hbar}{\delta}\frac{\|\!|H_f - H_0|\!\|}{g_{\min}^2}. \qquad (3.54)$$

As already stated, we see here that the scaling of the running time depends directly on the scaling of the minimum gap, and this explains why the minimum gap is the key quantity studied in papers considering adiabatic algorithms as a way to solve complex problems such as satisfiability problems [FGGS00, FGG$^+$01].

In that case, the evolution rate is limited *globally* on the whole evolution by the minimum value of the gap that only occurs at one moment in the evolution. Therefore, it seems clear that we could improve the running time by optimizing the evolution $v(s)$ constantly during the process. Actually, this is possible only when $a(s)$ may be evaluated exactly, even if the solution of the problem is unknown (otherwise we would have to solve the problem first to derive $a(s)$, which would require another algorithm). This may happen when the problem has a permutation symmetry such that $a(s)$ is independent of the particular instance considered (this will be the case of Grover's problem, see Chapter 4). In such a case, the adiabatic condition (3.42) may be saturated by choosing

$$v(s) = \frac{1}{a(s)} \tag{3.55}$$

and the running time will scale as

$$T_\delta = \frac{1}{\delta} \int_0^1 a(s) ds. \tag{3.56}$$

As the evolution rate $v(s)$ is now optimized *locally* at each time, we will use in this case the term *local* adiabatic evolution. Interestingly, we will show that this procedure makes it possible, in some cases such as Grover's problem, to improve the scaling of T_δ as a function of the problem size ν.

Chapter 4

Quantum search by adiabatic evolution

Introduction

The idea to use the Adiabatic Theorem as a way to design quantum algorithms was first proposed by Farhi *et al.* In their paper [FGGS00], they considered, among other problems, the search in an unstructured database of N items, that is Grover's problem. Unfortunately, their method was based on a "global" version of the Adiabatic Theorem, and therefore resulted in a running-time of order N, which is no better than a classical algorithm that simply tries random solutions.

In this chapter, we show that one can achieve the quadratic speed-up of Grover's original algorithm by continuously adjusting the rate with which the initial Hamiltonian is switched to the final Hamiltonian, so as to fulfill the adiabatic condition *locally*, i. e. at each time. Interestingly, this local adiabatic evolution approach makes it possible to improve the scaling law of the complexity of the quantum search algorithm simply by varying the speed of this adiabatic sweep. Let us note that this result has been independently discovered by van Dam *et al* [vDMV01].

4.1 The Hamiltonian and its spectrum

The problem considered in this chapter is the traditional Grover problem as exposed in Section 2.3: in an unstructured database of N items, find one out of the M items that are marked. More specifically, the problem is stated exactly as for the analog quantum search (Section 2.4): the marked items correspond to the eigenstates of lowest eigenvalue of an oracle Hamiltonian

$$H_f = \bar{E}(I_N - \sum_{m \in \mathcal{M}} |m\rangle\langle m|), \tag{4.1}$$

that we are able to apply as a black-box on the system, and the complexity of the algorithm is defined as the total running time of the evolution.

As the marked items m correspond precisely to the (degenerate) ground state of H_f, the Adiabatic Theorem gives a straightforward method to solve this problem. Similarly to both other search algorithms considered so far (Grover and analog), one starts by initializing the system in the uniform superposition $|\psi(t=0)\rangle = |\mathcal{N}\rangle$. As this is the ground state of the Hamiltonian

$$H_0 = \bar{E}(I_N - |\mathcal{N}\rangle\langle\mathcal{N}|), \tag{4.2}$$

it suffices to apply H_0 on the system and then to progressively change the instantaneous Hamiltonian into H_f to prepare a ground state of H_f. Let us write the instantaneous Hamiltonian $H(t) = \tilde{H}(s(t))$, where

$$\tilde{H}(s) = (1-s)H_0 + sH_f, \tag{4.3}$$

and study the spectrum of $\tilde{H}(s)$. Solving the eigenproblem

$$\tilde{H}(s)|\tilde{\varphi}_k(s)\rangle = \tilde{E}_k(s)|\tilde{\varphi}_k(s)\rangle, \tag{4.4}$$

we see that $\tilde{H}(s)$ admits four different eigenvalues

$$\begin{aligned}
\tilde{E}_0(s) &= \frac{\bar{E}}{2}\left[1-\sqrt{1-4(1-x^2)s(1-s)}\right] && (4.5)\\
\tilde{E}_1(s) &= \bar{E}(1-s) && (4.6)\\
\tilde{E}_2(s) &= \frac{\bar{E}}{2}\left[1+\sqrt{1-4(1-x^2)s(1-s)}\right] && (4.7)\\
\tilde{E}_3(s) &= \bar{E}, && (4.8)
\end{aligned}$$

where, as usually, $x = \sqrt{M/N}$. This spectrum is illustrated on Fig. 4.1. While $\tilde{E}_0$ and $\tilde{E}_2$ are the only eigenvalues that are non-degenerate (at least for $s \neq 0, 1$), $\tilde{E}_1$ is $M-1$ times degenerate and $\tilde{E}_3$ is $N-M-1$ times degenerate. At first view, it may seem that this degeneracy prevents us from using the Adiabatic Theorem as stated in the last chapter as it required the eigenvalues to be non-degenerate. Actually, this is not the case because of the symmetry of the problem.

4.2 Permutation symmetry

Since the initial state

$$|\mathcal{N}\rangle = x|\mathcal{M}\rangle + \sqrt{1-x^2}|\mathcal{M}^C\rangle, \tag{4.9}$$

as well as both Hamiltonians H_0 and H_f, are all invariant under the permutation of any two solution states $|m\rangle$ ($m \in \mathcal{M}$), or any two non-solution states $|n\rangle$ ($n \in \mathcal{M}^C$), so will be the whole problem and therefore the instantaneous state $|\psi(t)\rangle$. In other words, $|\psi(t)\rangle$ will stay in a subspace that is symmetric under these permutations, that is within the two-dimensional Hilbert space spanned by the uniform superposition of solution states $|\mathcal{M}\rangle$ and the uniform superposition of non-solution states $|\mathcal{M}^C\rangle$. As it corresponds exactly to the space spanned by the two non-degenerate eigenstates

$$\begin{aligned}
|\tilde{\varphi}_0(s)\rangle &= \frac{\tilde{E}_2(s)x|\mathcal{M}\rangle + \sqrt{1-x^2}(\tilde{E}_2(s)-\bar{E}s)|\mathcal{M}^C\rangle}{\sqrt{\tilde{E}_2(s)^2x^2 + (1-x^2)(\tilde{E}_2(s)-\bar{E}s)^2}} && (4.10)\\
|\tilde{\varphi}_2(s)\rangle &= \frac{\tilde{E}_0(s)x|\mathcal{M}\rangle + \sqrt{1-x^2}(\tilde{E}_0(s)-\bar{E}s)|\mathcal{M}^C\rangle}{\sqrt{\tilde{E}_0(s)^2x^2 + (1-x^2)(\tilde{E}_0(s)-\bar{E}s)^2}}, && (4.11)
\end{aligned}$$

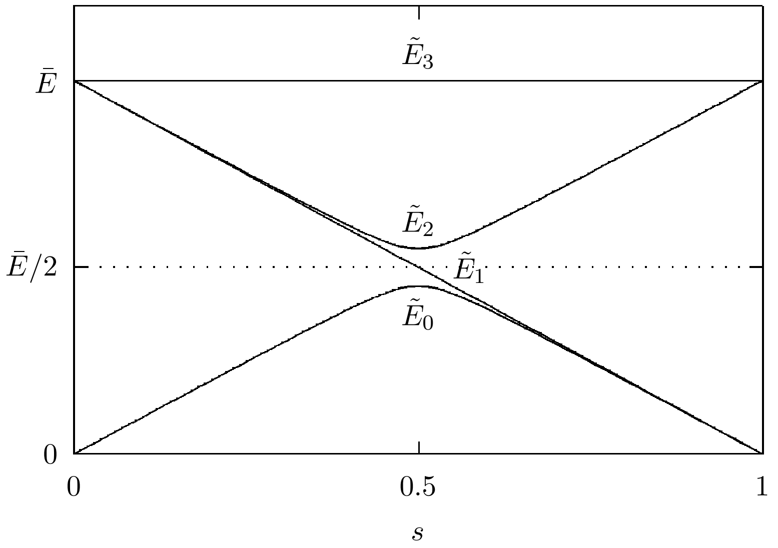

Figure 4.1: Eigenvalues of the Hamiltonian $\tilde{H}(s)$ as a function of s for $N/M = 100$. The eigenvalues $\tilde{E}_0(s)$ and $\tilde{E}_2(s)$ are non-degenerate while $\tilde{E}_1(s)$ and $\tilde{E}_3(s)$ are respectively $M - 1$ and $N - M - 1$ times degenerate.

we conclude that the other (degenerate) eigenstates, which do not satisfy the permutation symmetries, will be totally decoupled and that we may study our problem in a two-dimensional Hilbert space as it was the case for both other search algorithms. In this two-dimensional subspace, $\tilde{H}(s)$ only admits two non-degenerate eigenstates, such that the assumptions of the Adiabatic Theorem as stated in the last chapter are satisfied.

4.3 The Adiabatic Theorem

Let us now apply the Adiabatic Theorem to our problem. It states that if the adiabatic condition (3.42) is satisfied

$$a(s)v(s) \leq 1 \quad \forall s, \tag{4.12}$$

where the element

$$a(s) = 2\hbar \frac{|\langle \tilde{\varphi}_2(s)|H_f - H_0|\tilde{\varphi}_0(s)\rangle|}{(\tilde{E}_2(s) - \tilde{E}_0(s))^2} \tag{4.13}$$

depends on the Hamiltonian $\tilde{H}(s)$ and $v(s)$ defines the rate $ds/dt = \delta v(s(t))$ at which it is evolving, then, in the limit $\delta \rightarrow 0$, the system will stay in its instantaneous ground state with an error less than δ^2

$$|\langle \psi(t)|\tilde{\varphi}_0(s(t))\rangle|^2 \geq 1 - \delta^2. \tag{4.14}$$

We now have to define an evolution rate $v(s)$ such that the adiabatic condition (4.12) is satisfied, that is,

$$v(s) \leq \frac{1}{2\hbar} \frac{g(s)^2}{|\langle \tilde{\varphi}_2(s)|H_f - H_0|\tilde{\varphi}_0(s)\rangle|}, \tag{4.15}$$

where

$$g(s)=\tilde{E}_2(s)-\tilde{E}_0(s)=\bar{E}\sqrt{1-4(1-x^2)s(1-s)} \tag{4.16}$$

is the gap between the ground state and the only excited state to which it is coupled, as plotted in Fig. 4.2. As

$$|\langle\tilde{\varphi}_2(s)|H_f-H_0|\tilde{\varphi}_0(s)\rangle|\leq \|H_f-H_0\|=(1-x^2)\bar{E}, \tag{4.17}$$

this condition will necessarily be satisfied as long as

$$v(s)\leq\frac{g(s)^2}{2\hbar\bar{E}}. \tag{4.18}$$

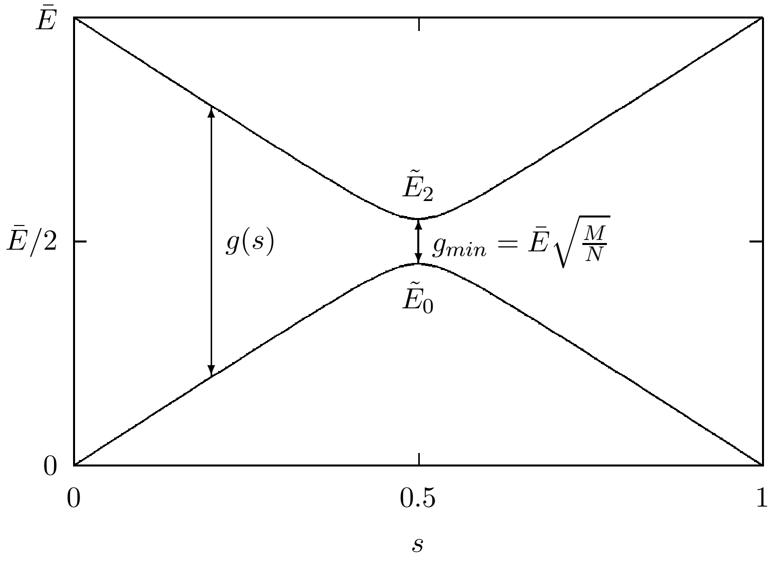

Figure 4.2: The non-degenerate eigenvalues $\tilde{E}_0(s)$ and $\tilde{E}_2(s)$ of the Hamiltonian $\tilde{H}(s)$ and the gap $g(s)$ between them for $N/M=100$.

4.3.1 Global adiabatic evolution

The simplest choice for $v(s)$ is to fix it *globally* to a constant value v_0, using a linear interpolation path between H_0 and H_f

$$\frac{ds}{dt}=\delta v_0\Rightarrow s(t)=\delta v_0 t. \tag{4.19}$$

As the adiabatic condition becomes critical when the gap $g(s)$ is minimal, that is half-way in the evolution where

$$g_{\min}=g(s=1/2)=\sqrt{\frac{M}{N}}\bar{E}, \tag{4.20}$$

the maximal allowed value for a constant $v(s) = v_0$ is

$$\begin{aligned} v_0 &= \frac{g_{\min}^2}{2\hbar\bar{E}} && (4.21) \\ &= \frac{\bar{E}}{2\hbar}\frac{M}{N}. && (4.22) \end{aligned}$$

The running time is then readily integrated

$$\begin{aligned} T_\delta &= \frac{1}{\delta}\int_0^1 \frac{ds}{v_0} && (4.23) \\ &= \frac{2\hbar}{\delta\bar{E}}\frac{N}{M}. && (4.24) \end{aligned}$$

Therefore, the quantum search by global adiabatic evolution has the same complexity $\Theta(N/M)$ as a classical search, failing to provide the quadratic speed-up of Grover's algorithm.

4.3.2 Local adiabatic evolution

Now, let us show how to improve on this adiabatic evolution method. In the global adiabatic method, we imposed a limit on the evolution rate during the whole computation while this limit was only severe around $s = 1/2$, where the gap $g(s)$ is minimum. Therefore, it seems plausible that we could reduce the running time by adapting the evolution rate $v(s)$ constantly during the computation, following the variations of the gap $g(s)$. This idea leads to an evolution rate

$$\begin{aligned} v(s) &= \frac{g(s)^2}{2\hbar\bar{E}} && (4.25) \\ &= \frac{\bar{E}}{2\hbar}\left[1 - 4(1-x^2)s(1-s)\right]. && (4.26) \end{aligned}$$

As $ds/dt = \delta v(s(t))$, we get the time t as a function of the evolution parameter s by integration

$$\begin{aligned} t(s) &= \frac{1}{\delta}\int_0^s \frac{ds'}{v(s')} && (4.27) \\ &= \frac{2\hbar}{\delta\bar{E}}\int_0^s \frac{ds'}{1-4(1-x^2)s'(1-s')} && (4.28) \\ &= \frac{\hbar}{\delta\bar{E}}\frac{1}{x\sqrt{1-x^2}}\left[\arctan\frac{\sqrt{1-x^2}}{x}(2s-1)\right. \\ &\qquad\qquad \left. + \arctan\frac{\sqrt{1-x^2}}{x}\right]. && (4.29) \end{aligned}$$

Inverting this expression, we get the evolution function

$$s(t) = \frac{1}{2}\frac{\tan x\sqrt{1-x^2}\frac{\delta\bar{E}t}{\hbar}}{x\sqrt{1-x^2} + (1-x^2)\tan x\sqrt{1-x^2}\frac{\delta\bar{E}t}{\hbar}}, \qquad (4.30)$$

plotted in Fig. 4.3, which shows the gradual change in the switching between H_0 and H_f. As expected, we see that $H(t)$ is changing faster when the gap $g(s)$ is large while it evolves

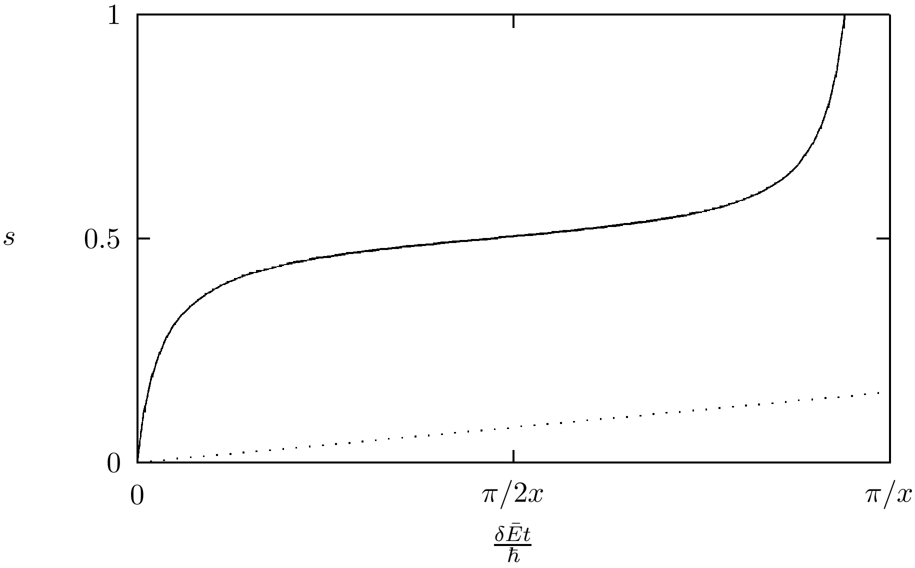

Figure 4.3: Solid line: Evolution function $s(t)$ for the local adiabatic evolution ($N/M = 100$). The global adiabatic evolution would correspond to the straight dotted line with a slope equal to the minimal slope of the local adiabatic evolution curve, taking therefore a much longer time to reach $s = 1$.

slower when s is close to 1/2, that is, where the gap is minimum. We may now evaluate the running time of our new algorithm by taking $s = 1$ in the function $t(s)$, which gives

$$\begin{aligned} T_\delta &= \frac{2\hbar}{\delta\bar{E}} \frac{1}{x\sqrt{1-x^2}} \arctan \frac{\sqrt{1-x^2}}{x} && (4.31) \\ &= \frac{\pi\hbar}{\delta\bar{E}} \frac{1}{x} \left(1 + O(x)\right). && (4.32) \end{aligned}$$

We thus have recovered the quadratic speed-up of Grover's algorithm with respect to a classical search

$$T_\delta = \frac{\pi\hbar}{\delta\bar{E}} \sqrt{\frac{N}{M}} \left(1 + O\left(\sqrt{\frac{M}{N}}\right)\right). \tag{4.33}$$

4.4 Saturation of the adiabatic condition

Actually, it would be possible to reduce the running time even more since we have not saturated the adiabatic condition (4.12) yet: instead of bounding the matrix element of $H_f - H_0$ by $\|H_f - H_0\|$ (see Eq. (4.17)), we could use its actual value, which is straightforward to derive from the eigenstates (4.10–4.11) of $\tilde{H}(s)$

$$\langle \tilde{\varphi}_2(s)|H_f - H_0|\tilde{\varphi}_0(s)\rangle = -\frac{x\sqrt{1-x^2}\bar{E}}{\sqrt{1-4(1-x^2)s(1-s)}}. \tag{4.34}$$

As this yields the actual value of

$$a(s) = 2\hbar \frac{|\langle\tilde{\varphi}_2(s)|H_f - H_0|\tilde{\varphi}_0(s)\rangle|}{(\tilde{E}_2(s) - \tilde{E}_0(s))^2} \tag{4.35}$$

$$= \frac{2\hbar}{\bar{E}} \frac{x\sqrt{1-x^2}}{[1-4(1-x^2)s(1-s)]^{3/2}}, \tag{4.36}$$

we may now saturate the adiabatic condition by choosing $v(s)$ such that $a(s)v(s) = 1$:

$$v(s) = \frac{\bar{E}}{2\hbar} \frac{[1-4(1-x^2)s(1-s)]^{3/2}}{x\sqrt{1-x^2}}. \tag{4.37}$$

Note that the evolution rate $v(s)$ now grows as $x^{-1} = \sqrt{N/M}$ for s close to 0 and 1, so that this ideal algorithm may reveal hard to implement practically. Nevertheless, it allows to reduce the running time to

$$T_\delta = \frac{2\hbar}{\delta\bar{E}} x\sqrt{1-x^2} \int_0^1 \frac{ds}{[1-4(1-x^2)s(1-s)]^{3/2}} \tag{4.38}$$

$$= \frac{2\hbar}{\delta\bar{E}} \frac{\sqrt{1-x^2}}{x} \tag{4.39}$$

$$= \frac{2\hbar}{\delta\bar{E}} \sqrt{\frac{N}{M}} \left(1 + O\left(\frac{M}{N}\right)\right). \tag{4.40}$$

This represents only a gain by a constant factor $\pi/2$ with respect to the evolution rate $v(s)$ proposed in the previous section, so that we will not consider this algorithm any further (in the next chapter, we will show that the previous section also provides an algorithm that is more closely related to the other quantum search algorithms). Moreover, we conclude from this that the scaling of the running time depends mostly on the scaling of the gap $g(s)$ and not on the exact value of the matrix element of $d\tilde{H}/ds$.

4.5 Case of an unknown number of solutions

Let us now point out an interesting advantage of the quantum search by adiabatic evolution over its cousins, Grover's algorithm and the analog quantum search. Remember that these algorithms can be used when the number of solutions is unknown by taking a random trial number of iterations (or running time for the analog version), which yields a solution with a probability close to 1/2. Should the algorithm fail at first try, it has to be run again with a new trial value, on and again until finding a solution. While this method was sufficient to solve an unstructured search problem keeping the quadratic speed-up provided by Quantum Mechanics, it could lead to a problem when trying to use Grover's algorithm as a subroutine in a larger quantum algorithm (see Chapter 6), where it would therefore not be possible to check that the subroutine was successful without performing a measurement that would make the quantum superposition collapse.

However, the quantum search by local adiabatic evolution does not suffer from this limitation. Indeed, if, following a similar idea, we run the algorithm using a trial value M' supposed to be close to the actual number of solutions M, we see that the assumptions of the Adiabatic

Theorem will still be satisfied just by replacing the target success probability $1-\delta^2$ by $1-\delta'^2$ with

$$\delta' = \frac{M'}{M}\delta. \tag{4.41}$$

Therefore, as long as the ratio M'/M stays of order 1, the algorithm will still produce a uniform superposition of all solutions with a probability close to 1. Furthermore, by taking the most pessimistic trial value $M' = 1$, the success probability may only increase for $M \neq M'$. In contrast, the success probability of Grover's algorithm may only decrease for a wrong number of iterations, and could even go down to essentially 0 just by multiplying the number of iterations by a factor of 2.

This result will be helpful to use the quantum search by adiabatic evolution as a subroutine in quantum algorithms for structured problems, as will be shown in Chapter 6.

4.6 Proof of optimality

Finally, we show that our algorithm is optimal, in the sense that the running time of any Hamiltonian evolution that solves the search problem using an oracle Hamiltonian similar to H_f scales as $\Omega(\sqrt{N})$[1]. More precisely we prove the following theorem

Theorem 2 *If $|m\rangle$ is an unknown quantum state taken from the orthonormal basis $\{|n\rangle, n = 0,\ldots,N-1\}$ of an N-dimensional Hilbert-space $\mathcal{H}_N$ and H_m is the Hamiltonian $\bar{E}(I_N - |m\rangle\langle m|)$ acting on $\mathcal{H}_N$, then any algorithm of the type*

1. *Prepare an m-independent state $|\psi(0)\rangle$ of the NL-dimensional Hilbert-space $\mathcal{H}_N \otimes \mathcal{H}_L$, where $\mathcal{H}_L$ is an extra-register of arbitrary dimension $L \geq 0$.*

2. *Let the state $|\psi(t)\rangle$ evolve under the Hamiltonian $H(t) = H_D(t) + C(t)H_m \otimes I_L$, where $H_D(t)$ is an arbitrary m-independent Hamiltonian on $\mathcal{H}_N \otimes \mathcal{H}_L$, I_L is the identity on $\mathcal{H}_L$ and $C(t) \leq 1$.*

3. *Perform a measurement on the state $|\psi(T)\rangle$ after time T.*

that finds the value of m with success probability greater than p requires a running time T such that

$$\frac{\bar{E}T}{\hbar} \geq \sqrt{N} - \sqrt{p} - \sqrt{(N-1)(1-p)}. \tag{4.42}$$

Let us note that these assumptions are very general as they include not only the quantum search by adiabatic evolution but also the analog quantum search. Furthermore, they also include quantum algorithms with intermediate measurements during the computation since all these measurements may be postponed to the end of the computation[2]. Finally, let us mention that this theorem also includes the case of a classical algorithm consisting in making a random guess for m (which does not require any Hamiltonian evolution, that is, $T = 0$), as $p = 1/N$ yields $T \geq 0$.

[1] We consider the single-solution case $M = 1$ as the proof will appear clearer, but it could be generalized to the case $M \geq 1$.

[2] As explained in Chapter 1 in the context of circuit-based algorithms, this is true even if the computation depends on the outcome of the intermediate measurements since we may apply different Hamiltonians conditionally on an additional quantum register that is only measured at the end of the computation, and since the theorem assumes no restriction on the dimension L of the extra-register (see [Zal99]).

One could wonder why we assume that $C(t) \leq 1$. Actually, if we suppress this assumption, the algorithm may become as fast as desired just by increasing the factor of the Hamiltonian: it is clear that if we multiply a Hamiltonian by a factor of, say, 2, the evolution it induces will remain the same, except that it will be twice faster. Physically, this corresponds to working at a higher energy, and therefore this assumption comes from the fact that the energy available for the quantum computer must be practically limited. Nonetheless, let us point out that we have not imposed any restriction on the part H_D of the Hamiltonian that does not depend on m, meaning that increasing the energy of this term may not be useful for the computation.

To prove this theorem, we will use results from the optimality proof for Grover's traditional algorithm derived by Zalka [Zal99] and roughly follow the lines of the optimality proof [FG98a] for the analog quantum search algorithm exposed in Section 2.4, but with more general assumptions.

Let $|\psi_m(t)\rangle$ be the state of our quantum register during the computation when the solution is m. This state will evolve under the action of the Hamiltonian $H_m^{\text{tot}}(t) = H_D(t)+C(t)H_m\otimes I_L$ according to the Schrödinger equation

$$i\hbar\frac{d}{dt}|\psi_m(t)\rangle = H_m^{\text{tot}}(t)|\psi_m(t)\rangle \tag{4.43}$$

with $|\psi_m(0)\rangle = |\psi(0)\rangle$ as initial condition. Moreover, let us define the "empty-oracle" state $|\psi_\phi(t)\rangle$ that derives from the evolution of $|\psi(0)\rangle$ when H_m has been replaced by the "empty-oracle" Hamiltonian $\bar{E}I_N$. It will evolve according to the same Schrödinger equation except that $H_m^{\text{tot}}(t)$ will be replaced by $H_\phi^{\text{tot}}(t) = [H_D(t) + C(t)\bar{E}I_N \otimes I_L]$. Intuitively, it is clear that in order to derive the value of m from a measurement of the state $|\psi_m(T)\rangle$ obtained at the end of the computation, the different states $|\psi_m(T)\rangle$ for different values of m must be sufficiently different from the m-independent state $|\psi_\phi(T)\rangle$.

More precisely, Zalka has proved [Zal99] that for a measurement to be able to discriminate between different states $|\psi_m\rangle$ with success probability p, a necessary condition is that these states sufficiently differ from any m-independent state $|\psi\rangle$ such that

$$\sum_{m=0}^{N-1} \||\psi_m\rangle - |\psi\rangle\|^2 \geq 2N - 2\sqrt{Np} - 2\sqrt{N(N-1)(1-p)}. \tag{4.44}$$

Let us now evaluate how well the Hamiltonian evolution defined by our algorithm may push $|\psi_m(t)\rangle$ away from $|\psi_\phi(t)\rangle$. As these states obey the above Schrödinger equation, we have[3]

$$\begin{aligned} \frac{d}{dt}\||\psi_m\rangle - |\psi_\phi\rangle\|^2 &= \frac{2}{\hbar}\text{Im}\left[\langle\psi_m|H_m^{\text{tot}} - H_\phi^{\text{tot}}|\psi_\phi\rangle\right] && (4.45)\\ &= \frac{2C\bar{E}}{\hbar}\text{Im}\left[\langle\psi_m|(|m\rangle\langle m|\otimes I_L)|\psi_\phi\rangle\right]. && (4.46)\end{aligned}$$

This derivative will be bounded by

$$\begin{aligned} \frac{d}{dt}\||\psi_m\rangle - |\psi_\phi\rangle\|^2 &\leq \frac{2C\bar{E}}{\hbar}\left|\langle\psi_m|(|m\rangle\langle m|\otimes I_L)|\psi_\phi\rangle\right| && (4.47)\\ &\leq \frac{2C\bar{E}}{\hbar}\|\langle m|\psi_m\rangle\|\|\langle m|\psi_\phi\rangle\| && (4.48)\\ &\leq \frac{2C\bar{E}}{\hbar}\|\langle m|\psi_\phi\rangle\|, && (4.49)\end{aligned}$$

[3] We omit the arguments "(t)" to lighten the expressions.

where we have used the Cauchy-Schwartz inequality along with the fact that $\|\langle m|\psi_m\rangle\| \leq 1$ as both states are normalized[4]. Summing over m and using the property

$$\sum_{m=0}^{N-1} \|\langle m|\psi_\phi\rangle\|^2 = 1 \Rightarrow \sum_{m=0}^{N-1} \|\langle m|\psi_\phi\rangle\| \leq \sqrt{N}, \tag{4.50}$$

we get

$$\sum_{m=0}^{N-1} \frac{d}{dt}\||\psi_m\rangle - |\psi_\phi\rangle\|^2 \leq \frac{2C\bar{E}}{\hbar}\sqrt{N} \tag{4.51}$$

We may now integrate this inequality using the initial conditions $|\psi_\phi(0)\rangle = |\psi_m(0)\rangle$:

$$\begin{aligned} \sum_{m=0}^{N-1} \||\psi_m(t)\rangle - |\psi_\phi(t)\rangle\|^2 &\leq \frac{2\bar{E}}{\hbar}\sqrt{N}\int_0^T C(t)dt &(4.52)\\ &\leq \frac{2\bar{E}}{\hbar}\sqrt{N}T, &(4.53)\end{aligned}$$

as $C(t) \leq 1$. Finally, together with Zalka's condition (4.44), this bound concludes the proof

$$\frac{\bar{E}T}{\hbar} \geq \sqrt{N} - \sqrt{p} - \sqrt{(N-1)(1-p)}. \tag{4.54}$$

Summary

In this chapter, we have applied the adiabatic evolution technique, first introduced by Farhi *et al* [FGGS00] and exposed in Chapter 3, to design a quantum algorithm for solving Grover's problem, i. e., the search for a marked item in an unstructured database. We have shown that applying the Adiabatic Theorem globally (as in [FGGS00]) imposes a running time of order N/M, where N is the number of items in the database and M is the number of marked items, whereas adjusting the evolution rate of the Hamiltonian continuously in time so as to fulfill the adiabaticity condition locally results in a time of order $\sqrt{N/M}$. We therefore recover the quadratic speed-up of Grover's usual algorithm compared to a classical search [Gro96]. Actually, this may be considered as a sign that adiabatic algorithms are purely quantum in nature (in contrast with other physically motivated, but nonetheless classical, algorithmic techniques such as simulated annealing). We have also proved that this algorithm is optimal in the sense that no other Hamiltonian evolution could solve the same problem with a running time that scales better.

We should notice that this quadratic speed-up was achieved by switching the Hamiltonian at a rate that is constantly optimized during the evolution, which is only possible because the gap $g(s)$ can be derived analytically, and does not depend on the solution of the problem. As long as these conditions are satisfied, such a local adiabatic evolution method could be applied

[4] As a value of $\|\langle m|\psi_m\rangle\|$ close to 1 allows to find m with high probability just by measuring the first register $\mathcal{H}_N$ in the computational basis, it is clear that this bound is not tight, at least before the end of the computation. Actually, a closer analysis would lead to an upper bound for $\|\langle m|\psi_m(t)\rangle\|$ that is close to $\sin^2 \bar{E}t/\hbar\sqrt{N}$ (for $\bar{E}t/\hbar \leq \pi\sqrt{N}/2$). While this will only change the final bound on T for $p = 1$ by a prefactor close to $\pi/2$, which will not modify the overall complexity $\Omega(\sqrt{N})$, it is possible to show that after this change, all the bounds are saturated by the analog quantum search, which proves that this algorithm is strictly optimal, not only through the scaling of the running time but also because of its exact value.

to more complicated problems, as we will see in Chapter 6 where an adiabatic quantum search algorithm exploiting the problem structure is proposed, following a nested version of Grover's algorithm introduced by Cerf *et al* [CGW00].

Chapter 5

Quantum circuit model

Introduction

In the last chapters, we have introduced Hamiltonian-based quantum algorithms, where the state of the quantum register evolves continuously in time under the action of some Hamiltonian, in contrast to the standard paradigm of quantum computation based on quantum gates (i. e., unitary operators) applied sequentially on a quantum register. The purpose of this chapter is to clarify the link between these two types of algorithms and, more specifically, to exhibit a general discretization method for implementing the Hamiltonian-based algorithms on a traditional quantum circuit. This method will be applied to both the analog and adiabatic quantum search algorithms.

This issue is particularly important for the adiabatic algorithm because it was never shown how to implement it on a quantum circuit while keeping the quadratic speed-up of Grover's algorithm. This possibility may be considered as an indication of the fact that the algorithms by adiabatic evolution are truly quantum. It will also be very useful in the next chapter, when we will consider nested adiabatic search algorithms.

When implemented on a quantum circuit, the analog and adiabatic quantum search algorithms define two new circuit-based algorithms that may be compared to their cousin, Grover's algorithm. It appears that all these algorithms, while remaining three clearly distinct algorithms, take nonetheless a very similar form in the high dimensional limit, a fact which is particularly unexpected for the case of the adiabatic search algorithm. Specifically, we see that the evolution parameter (which measures the covered distance along the path between the initial and final Hamiltonians in the adiabatic search algorithm) has to evolve in such a way that the instantaneous ground state rotates at a constant rate from the initial to the final ground state. This makes the link fully explicit with Grover's original algorithm.

5.1 Conversion from Hamiltonian-based to circuit-based algorithms

5.1.1 First stage: discretization

Suppose we have to implement a Hamiltonian-based algorithm, defined by the Hamiltonian $H(t)$, on a quantum-circuit, i. e. a sequence of unitary operators or quantum gates. The basic idea is quite simple, it consists in cutting the running time of the algorithm T in K

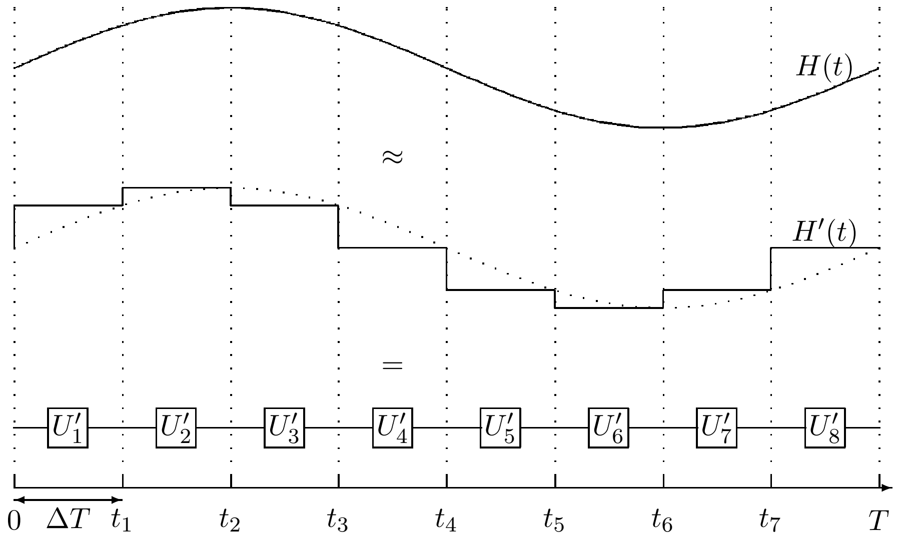

Figure 5.1: Schematic representation of the discretization of a Hamiltonian-based algorithm using a time-dependent Hamiltonian $H(t)$ (schematically represented as a one-dimensional function of t) discretized in $K = 8$ steps.

small time-intervals $[t_{k-1}, t_k]$ of size $\Delta T = T/K$, where $t_k = k\Delta T$. If the Hamiltonian is time-independent, its application during a time ΔT exactly induces the unitary operator $e^{-iH\Delta T/\hbar}$. Now if $H(t)$ is time-dependent but does not vary much in the interval $[t_{k-1}, t_k]$, it may be approximated within this interval by $H'(t) = H(t_k)$, and therefore the unitary operator U_k it induces during this time-interval may be approximated by $U'_k = e^{-iH(t_k)\Delta T/\hbar}$. This discretization stage is schematically represented in Fig. 5.1. Approximating the unitary operator $U(T)$ induced by the evolution under $H(T)$ by successive unitary operators U'_k will of course introduce an error, which may be quantified using Lemma 1 proved in Appendix A:

$$\| U(T) - \prod_{k=1}^{K} U'_k \| \leq \sqrt{\frac{2}{\hbar} \int_0^T e(t) dt}. \tag{5.1}$$

where $\| H(t) - H'(t) \| \leq e(t)$ is the error on the Hamiltonian[1].

5.1.2 Second stage: approaching a sum of Hamiltonians by sequential Hamiltonians

In the first stage, we have reduced our Hamiltonian-based algorithm to a sequence of unitary operators $U'_k = e^{-iH(t_k)\Delta T/\hbar}$. If the unitary operator U'_k induced by the Hamiltonian $H(t_k)$ during time ΔT is directly simulatable by a quantum circuit, our task is over. However this will typically not be the case. For instance, in the cases of the analog or adiabatic quantum

[1] This is a generalization of the lemma introduced by van Dam *et al* in the context of quantum algorithms by global adiabatic evolution [vDMV01]. The difference is that here the error $e(t)$ on the Hamiltonian is allowed to be time-dependent, which will be crucial in order to implement our quantum search by local adiabatic evolution while keeping the quadratic speed-up of Grover's algorithm.

search algorithms which we will consider next, the Hamiltonian $H(t_k)$ takes the form of a sum of two Hamiltonians H_0 and H_f, $H(t_k) = \alpha_{0,k}H_0 + \alpha_{f,k}H_f$, each of which is simulatable if applied alone. We may then approach the application of the two Hamiltonians H_0 and H_f in parallel

$$U'_k = e^{-\frac{i}{\hbar}(\alpha_{0,k}H_0+\alpha_{f,k}H_f)\Delta T} \tag{5.2}$$

by a successive application of H_0 and H_f

$$U''_k = e^{-\frac{iH_0\delta t_{0,k}}{\hbar}} e^{-\frac{iH_f\delta t_{f,k}}{\hbar}} \tag{5.3}$$

during times $\delta t_{0,k} = \alpha_{0,k}\Delta T$ and $\delta t_{f,k} = \alpha_{f,k}\Delta T$ respectively. The Campbell-Baker-Hausdorff approximation, consisting in replacing e^{A+B} by e^Ae^B, shows that this approximation will introduce an error

$$|||U'_k - U''_k||| = \frac{2\alpha_{0,k}\alpha_{f,k}}{\hbar^2}|||[H_0, H_f]|||\Delta T^2 \left(1 + \frac{|||H_0||| + |||H_f|||}{2\hbar}O(\Delta T)\right). \tag{5.4}$$

The errors introduced in the second stage will accumulate after each step k. To evaluate the overall error, we use Lemma 2 from Appendix A, showing that:

$$|||\prod_{k=1}^{K} U_k - \prod_{k=1}^{K} U'_k||| \leq \sum_{k=1}^{K} |||U_k - U'_k|||. \tag{5.5}$$

While we have expressed errors as differences of unitary operators, it is clear that only inner products of quantum states are physically relevant. However, these quantities are related, as shown by the Lemma 3 in Appendix A, which states that if $|\psi\rangle = U|\psi_0\rangle$ and $|\psi'\rangle = U'|\psi_0\rangle$, then

$$1 - |\langle\psi'|\psi\rangle|^2 \leq |||U - U'|||^2. \tag{5.6}$$

5.2 Grover's algorithm within a Hamiltonian-based approach

Before applying this conversion method to the Hamiltonian-based search algorithms, let us briefly recall the principle of Grover's algorithm as described in Section 2.3[2]:

- Input: Prepare the initial state $|\psi_0^{\text{dis}}\rangle = |\mathcal{N}\rangle = (1/\sqrt{N})\sum_{n\in\mathcal{N}}|n\rangle$.
- Steps $k = 1$ to $K^{\text{dis}} = \lfloor\frac{\pi}{4x}\rfloor$: Apply the Grover iteration $G = -U_0U_f$, where $U_f = I_N - 2\sum_{m\in\mathcal{M}}|m\rangle\langle m|$ and $U_0 = I_N - 2|\mathcal{N}\rangle\langle\mathcal{N}|$,

$$|\psi_k^{\text{dis}}\rangle = -U_0U_f|\psi_{k-1}^{\text{dis}}\rangle. \tag{5.7}$$

- Output: Measure the final state $|\psi_{K^{\text{dis}}}^{\text{dis}}\rangle$ in the computational basis.

In the limit $x \to 0$ (where $x = \sqrt{M/N}$), this algorithm will yield a solution state $|m\rangle$ ($m \in \mathcal{M}$) with error probability $p_{\text{err}}^{\text{dis}}$ of order $O(x^2)$. More precisely, the successive steps will rotate the quantum register following

$$|\psi_k^{\text{dis}}\rangle = \left(\sin\alpha_k^{\text{dis}}|\mathcal{M}\rangle + \cos\alpha_k^{\text{dis}}|\mathcal{M}^{\mathcal{C}}\rangle\right)(1 + O(x)), \tag{5.8}$$

[2] The superscript "$\cdot^{\text{dis}}$" stands for "discrete" Grover's algorithm and will be useful to compare the different search algorithms.

where

$$\alpha_k^{\mathrm{dis}} = 2kx\left(1 + O(x^2)\right), \tag{5.9}$$

is the angle of rotation after k steps.

Introducing the Hamiltonian oracle $H_f = \bar{E}(I_N - \sum_{m\in\mathcal{M}} |m\rangle\langle m|)$, defined in Section 2.4, we have seen that the unitary oracle U_f is equivalent (up to a phase) to the application of H_f during a time $\delta t = \pi\hbar/\bar{E}$:

$$U_f = -e^{-\frac{iH_f\delta t}{\hbar}}. \tag{5.10}$$

Moreover, the unitary operator U_0 and the Hamiltonian H_0 are similarly related

$$U_0 = -e^{-\frac{iH_0\delta t}{\hbar}}. \tag{5.11}$$

Defining the times $\delta t_{f,k}^{\mathrm{dis}} = \delta t$ and $\delta t_{0,k}^{\mathrm{dis}} = \delta t$, and the phases $\phi_k^{\mathrm{dis}} = k\pi$ and $\theta^{\mathrm{dis}} = 0$, we see that Grover's algorithm may be restated in the following generic form:

- Input: Prepare the initial state $|\psi_0^{\mathrm{dis}}\rangle = |\mathcal{N}\rangle$.

- Steps $k = 1$ to K^{dis}: Apply successively H_f during time $\delta t_{f,k}^{\mathrm{dis}}$ and H_0 during time $\delta t_{0,k}^{\mathrm{dis}}$, to get[3]

  $$|\psi_k^{\mathrm{dis}}\rangle = e^{-i\phi_k^{\mathrm{dis}}}\left(e^{i\theta^{\mathrm{dis}}}\sin\alpha_k^{\mathrm{dis}}|\mathcal{M}\rangle + \cos\alpha_k^{\mathrm{dis}}|\mathcal{M}^{\mathcal{C}}\rangle\right)(1 + O(x) + O(\delta)), \tag{5.12}$$

  where $\alpha_k^{\mathrm{dis}} = k\alpha_1^{\mathrm{dis}}$.

- Output: Measure the final state $|\psi_{K^{\mathrm{dis}}}^{\mathrm{dis}}\rangle$ in the computational basis to get a solution state $|m\rangle$ ($m \in \mathcal{M}$) with error probability $p_{\mathrm{err}}^{\mathrm{dis}} = O(x^2) + O(\delta^2)$.

We will see in the next section that both Hamiltonian-based search algorithms take the same generic form after discretization, such that the quantum circuit implementing these three algorithms only differ by a finite set of parameters, namely the number of steps K, the times $\delta t_{f,k}$ and $\delta t_{0,k}$, the angles α_k, and the phases ϕ_k and θ.

5.3 Hamiltonian version of the oracle

We have seen that the application of H_f during time $\pi\hbar/\bar{E}$ may simulate one application of the unitary operator U_f, that is one call to the quantum oracle O_f (see Fig. 2.1 in Chapter 2). To provide one more argument to the equivalence between the oracle Hamiltonian H_f and the unitary oracle O_f, we now show that the application of H_f during any time δt may be simulated by a quantum circuit using a one-qubit ancilla prepared in state $|0\rangle$, two calls to the oracle O_f, and an additional phase gate

$$U_t = e^{-\frac{i\bar{E}t}{\hbar}}|0\rangle\langle 0| + |1\rangle\langle 1|. \tag{5.13}$$

[3] In the case of Grover's algorithm, the phase $\phi_k^{\mathrm{dis}} = k\pi$ comes from the fact that $e^{-\frac{iH_0\delta t}{\hbar}}e^{-\frac{iH_f\delta t}{\hbar}} = U_0U_f = -G$, such that the sign of the state is inverted at each step.

Considering the circuit represented in Fig. 5.2, we have

$$\begin{aligned} O_f\left[|n\rangle\otimes|0\rangle\right] &= |n\rangle\otimes|f(n)\rangle \\ I\otimes U_t\left[|n\rangle\otimes|f(n)\rangle\right] &= e^{-i(1-f(n))\frac{\bar{E}t}{\hbar}}|n\rangle\otimes|f(n)\rangle \\ O_f\left[e^{-i(1-f(n))\frac{\bar{E}t}{\hbar}}|n\rangle\otimes|f(n)\rangle\right] &= e^{-i(1-f(n))\frac{\bar{E}t}{\hbar}}|n\rangle\otimes|0\rangle \\ &= e^{-\frac{iH_f t}{\hbar}}|n\rangle\otimes|0\rangle. \end{aligned} \tag{5.14}$$

which indeed coincides with the result of evolving $|n\rangle$ with H_f during time t (see Eq. (2.45)). This circuit will be helpful to implement the Hamiltonian-based search algorithms on a quantum circuit.

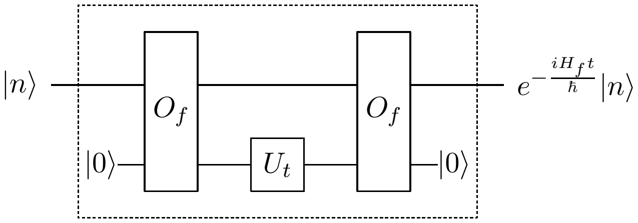

Figure 5.2: Circuit used to simulate the evolution of a Hamiltonian H_f during a time t by using twice the corresponding oracle O_f, a one-qubit phase gate U_t and an ancilla prepared in state $|0\rangle$.

5.4 Analog quantum search

Let us now use our discretization method to implement the analog algorithm exposed in Section 2.4 on a quantum circuit. Remember that it simply consists in the application of the time-independent Hamiltonian $H^{\text{an}} = H_0 + H_f$ on the initial state $|\mathcal{N}\rangle$ during time

$$T^{\text{an}} = \frac{\pi}{2x}\frac{\hbar}{\bar{E}}, \tag{5.15}$$

resulting in an evolution (2.48)

$$|\psi^{\text{an}}(t)\rangle = e^{-\frac{i\bar{E}t}{\hbar}}\left(i\sin\alpha^{\text{an}}(t)|\mathcal{M}\rangle + \cos\alpha^{\text{an}}(t)|\mathcal{M}^C\rangle\right)(1+O(x)), \tag{5.16}$$

where

$$\alpha^{\text{an}}(t) = \frac{\bar{E}xt}{\hbar}. \tag{5.17}$$

Thus, this Hamiltonian evolution rotates the state at constant rate, similarly to Grover's algorithm. More precisely, let us notice that

$$\alpha_k^{\text{dis}} = k\ \alpha^{\text{an}}\left(\frac{2\hbar}{\bar{E}}\right)\left(1+O(x^2)\right) \tag{5.18}$$

which shows that the application of H^{an} during a time $2\hbar/\bar{E}$ corresponds roughly to one Grover iteration. However, the rotation follows a different path because of the presence of i in the first term of Eq. (5.16).

Suppose now we want to implement this analog algorithm on a quantum circuit. We showed in the previous section how to simulate H_f with a quantum circuit based on two oracle calls, but this does not allow us to directly simulate $H^{\mathrm{an}} = H_0 + H_f$. However, the Campbell-Baker-Hausdorff approximation tells us that for ΔT sufficiently small, we may approach the parallel application of H_f and H_0 during time ΔT by successive applications of H_f and H_0. Following our discretization technique, this approximation will be valid if we cut the evolution time T^{an} into K^{an} sufficiently small intervals

$$\begin{aligned}\Delta T &= \frac{T^{\mathrm{an}}}{K^{\mathrm{an}}} &(5.19)\\ &= \frac{\pi\hbar}{2xK^{\mathrm{an}}\bar{E}}. &(5.20)\end{aligned}$$

Let us now study the error introduced by this discretization method in order to derive how the number of steps K^{an} should scale for this error to stay bounded. Using the quantum circuit of Section 5.3 to simulate H_f, we see that each of these steps will require two calls to the oracle O_f, such that the number of calls to the oracle will exactly scale as the number of steps.

The first stage of the conversion process, consisting in replacing the continuously varying Hamiltonian $H(t)$ by a step-wise varying Hamiltonian $H'(t)$ will not introduce any error in this case as the Hamiltonian H^{an} is time-independent. The analog algorithm is thus strictly equivalent to K^{an} successive applications of

$$U'_k = e^{-\frac{i}{\hbar}(H_0+H_f)\Delta T}. \tag{5.21}$$

However, following Eq. (5.4), the second stage, consisting in replacing U'_k by

$$U''_k = e^{-\frac{iH_0\Delta T}{\hbar}} e^{-\frac{iH_f\Delta T}{\hbar}}, \tag{5.22}$$

introduces at each step an error

$$\begin{aligned}\|U'_k - U''_k\| &= \frac{1}{2\hbar^2}\|[H_0, H_f]\|\Delta T^2\left(1 + \frac{\|H_0\| + \|H_f\|}{2\hbar}O(\Delta T)\right) &(5.23)\\ &\leq \frac{\bar{E}^2}{2\hbar^2}x\Delta T^2\left(1 + O\left(\frac{\bar{E}\Delta T}{\hbar}\right)\right), &(5.24)\end{aligned}$$

as $\|[H_0, H_f]\| = \bar{E}^2 x\sqrt{1-x^2}$. These errors add up progressively when k grows, such that the total error is bounded by

$$\|\prod_{k=1}^{K} U_k - \prod_{k=1}^{K} U'_k\| \leq \frac{\pi^2}{8xK^{\mathrm{an}}}\left(1 + O\left(\frac{\bar{E}\Delta T}{\hbar}\right)\right), \tag{5.25}$$

where we have used Eq. (5.5) along with the fact that $T^{\mathrm{an}} = K^{\mathrm{an}}\Delta T = (\pi/2x)(\hbar/\bar{E})$. For this error to stay bounded when $x \to 0$, we have to perform a number of steps K^{an} of order

$O(x^{-1})$ (just as Grover's discrete algorithm), for instance[4]

$$K^{\mathrm{an}} = \left\lfloor \frac{\pi}{4\delta x} \right\rfloor, \tag{5.26}$$

where δ is sufficiently small such that the total error is bounded by

$$\left\Vert \prod_{k=1}^{K} U_k - \prod_{k=1}^{K} U'_k \right\Vert \leq \frac{\pi\delta}{2}(1 + O(\delta)). \tag{5.27}$$

Using Eq. (5.6), which details the translation from unitary operator errors to error probabilities, this tells us that a measure of the state obtained after K^{an} steps will give a solution with error probability

$$p_{\mathrm{err}}^{\mathrm{an}} = O(\delta^2). \tag{5.28}$$

Finally, let us note that it follows from Eqs (5.20) and (5.26) that each step requires the application of H_f and H_0 during a time

$$\Delta T = \delta t_{f,k}^{\mathrm{an}} = \delta t_{0,k}^{\mathrm{an}} = \frac{2\hbar\delta}{\bar{E}} \tag{5.29}$$

and will rotate the state by an angle

$$\alpha_1^{\mathrm{an}} = \alpha^{\mathrm{an}}(\Delta t) = 2\delta x. \tag{5.30}$$

The link between the analog quantum search, translated into a circuit-based algorithm, and Grover's discrete algorithm appears now clearer as they both take the same generic form exposed at the end of Section 5.2. Among other things, this means that when translated into a circuit-based algorithm, the analog quantum search becomes a discrete algorithm that shows the same quadratic speed-up as Grover's algorithm versus a classical algorithm that would need of order $O(1/x^2)$ calls to the oracle. Nonetheless, we see that the number of steps of the analog algorithm has increased by a factor of δ^{-1} with respect to Grover's algorithm, and this may be related to the continuous-time origin of this algorithm.

5.5 Quantum search by local adiabatic evolution

For this third algorithm, exposed in Chapter 4, we once again prepare our system in the initial state $|\mathcal{N}\rangle$ and use the Hamiltonians H_0 and H_f. This time, however, we apply a time-dependent Hamiltonian $H^{\mathrm{ad}}(t) = \tilde{H}(s(t))$,

$$\tilde{H}(s) = (1 - s)H_0 + sH_f \tag{5.31}$$

where the evolution parameter $s = s(t)$ is a monotonic function with $s(0) = 0$ and $s(T^{\mathrm{ad}}) = 1$. As $|\mathcal{N}\rangle$ is the ground state of $\tilde{H}(0) = H_0$, the Adiabatic Theorem (see Section 3.2.2) tells us that the system will stay in a state $|\psi^{\mathrm{ad}}(t)\rangle$ near the instantaneous ground state $|\tilde{\varphi}_0(s(t))\rangle$ of $\tilde{H}(s)$ as long as the evolution of $\tilde{H}(s)$ imposed by $s(t)$ is "slow enough". More precisely, if the adiabatic condition (4.12) is satisfied, then

$$1 - |\langle\psi^{\mathrm{ad}}(t)|\tilde{\varphi}_0(s(t))\rangle|^2 \leq \delta^2. \tag{5.32}$$

[4] The prefactor is actually arbitrary, it has been chosen equal to $\pi/4$ to make the comparison with Grover's algorithm easier.

As the ground state of $\tilde{H}(1) = H_f$ is the superposition of solution states $|\mathcal{M}\rangle$, a measure of the system at the end of the evolution $t = T^{\text{ad}}$ will yield a solution with error probability $p_{\text{err}}^{\text{ad}}$ of order $O(\delta^2)$. More precisely, the instantaneous ground state of $\tilde{H}(s)$ (4.10–4.11) may be rewritten

$$|\tilde{\varphi}_0(s)\rangle = \sin\tilde{\alpha}^{\text{ad}}(s)|\mathcal{M}\rangle + \cos\tilde{\alpha}^{\text{ad}}(s))|\mathcal{M}^C\rangle \tag{5.33}$$

where the angle $\tilde{\alpha}^{\text{ad}}(s)$ is defined as[5]

$$\tilde{\alpha}^{\text{ad}}(s) = \frac{1}{2}\arctan' \frac{2x\sqrt{1-x^2}s}{1-2(1-x^2)s} \tag{5.34}$$

and is plotted in Fig. 5.3. We see that the evolution is once again a rotation in the $(|\mathcal{M}\rangle, |\mathcal{M}^C\rangle)$ plane. Furthermore, at discrete values such that $s(t) = \alpha_k^{\text{dis}}$, the continuous path $|\psi^{\text{ad}}(s)\rangle$ coincides (up to an error of order $O(\delta^2)$) with the states $|\psi_k^{\text{dis}}\rangle$ of Grover's traditional algorithm (in contrast to the analog algorithm where the amplitude of $|\mathcal{M}\rangle$ became imaginary). However, Fig. 5.3 shows that the rotation would *not* be performed at a constant angular velocity if $s(t)$ was chosen to be linear in t, which corresponds to the quantum search by *global* adiabatic evolution. The angular velocity would indeed be greater for s close to 1/2 and smaller at the beginning and the end of the evolution. Thus, in the global adiabatic search algorithm, the system exactly follows the path of Grover's algorithm, but at a varying rate. This suggests that this algorithm is not the correct adiabatic equivalent to Grover's algorithm, and we already know that indeed it does not reproduce the quadratic speed-up of Grover's algorithm (see Chapter 4).

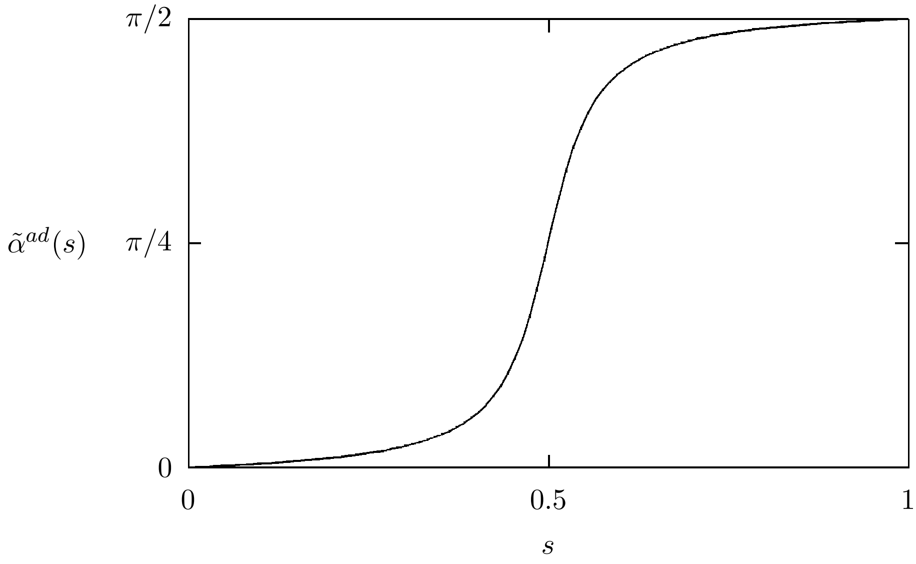

Figure 5.3: Rotation angle $\tilde{\alpha}^{\text{ad}}(s)$ for the adiabatic quantum search algorithm with $N = 100$.

In order to circumvent this problem, we must perform a *local* adiabatic evolution, optimizing $s(t)$ constantly during the evolution according to the variations of the gap $g(s)$. This

[5] We define the modified inverse tangent function arctan′ as $y = \arctan' x \Leftrightarrow \{x = \tan y \wedge 0 \leq y < \pi\}$ (instead of $-\pi/2 < y < \pi/2$ for the usual arctan).

leads to a non-linear function $s(t)$ whose inverse may be written (4.29) as

$$t(s) = \frac{\hbar}{\delta\bar{E}} \frac{1}{x\sqrt{1-x^2}} \arctan' \frac{2x\sqrt{1-x^2}s}{1-2(1-x^2)s}. \tag{5.35}$$

Remarkably, we see that the variations in the evolution rate ds/dt will exactly compensate the variations in the angular velocity, such that this angular velocity is now constant during the whole evolution:

$$\begin{aligned} \alpha^{\mathrm{ad}}(t) &= \tilde{\alpha}^{\mathrm{ad}}(s(t)) & (5.36)\\ &= \delta x\sqrt{1-x^2}\frac{\bar{E}t}{2\hbar} & (5.37)\\ &= \delta x\frac{\bar{E}t}{2\hbar}(1+O(x^2)). & (5.38) \end{aligned}$$

Note that at $t = T^{\mathrm{ad}} = \pi\hbar/(\delta\bar{E}x)\,(1+O(x))$, we have $\alpha^{\mathrm{ad}}(T^{\mathrm{ad}}) \approx \pi/2$ as expected. The fact that the state is rotated at a constant rate for this particular evolution $s(t)$ is one more argument that this is the right adiabatic equivalent to Grover' algorithm (together with the fact that it reproduces its quadratic speed-up).

Let us now use the conversion method exposed in Section 5.1 to implement this algorithm on a quantum circuit. As for the analog quantum search, the first stage consists in the discretization of the evolution by cutting the time T^{ad} into K^{ad} intervals $\Delta T = T^{\mathrm{ad}}/K^{\mathrm{ad}}$. During each interval $[t_{k-1}, t_k]$ $\quad(t_k = k\Delta T)$, we approximate the time-dependent Hamiltonian $\tilde{H}(s(t))$ by the time-independent one $H_k = (1-s_k)H_0 + s_k H_f$ $(s_k = s(t_k))$. Actually, this is equivalent to replacing the actual Hamiltonian $H(t) = \tilde{H}(s(t))$ by $H'(t) = \tilde{H}(s'(t))$ where $s'(t)$ is a step-wise function approaching $s(t)$ but varying at times t_k only (see Fig. 5.4).

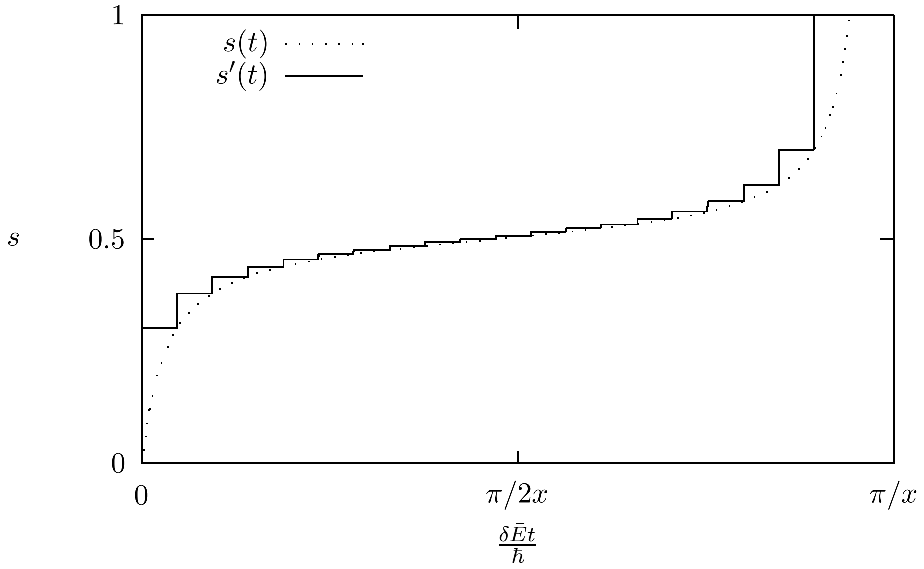

Figure 5.4: $s(t)$ and its step-wise approximation $s'(t)$ (using $K^{\mathrm{ad}} = 20$ steps) for the local adiabatic algorithm with $N/M = 100$.

A bound on the error introduced by this approximation may be derived from the error on the Hamiltonian, that is

$$\begin{aligned}
\|H(t)-H'(t)\| &= \|\tilde{H}(s(t))-\tilde{H}(s'(t))\| \\
&= |s'(t)-s(t)|\,\|H_0-H_f\| \\
&\le |s(t+\Delta T)-s(t)|\,\|H_0-H_f\| \\
&\le |s(t+\Delta T)-s(t)|\bar{E}, \qquad (5.39)
\end{aligned}$$

where we have assumed that $s(t)=1$ for $t>T^{\mathrm{ad}}$ and used the fact that

$$\|H_0-H_f\| = \||\mathcal{M}\rangle\langle\mathcal{M}|-|\mathcal{N}\rangle\langle\mathcal{N}|\| = \bar{E}\sqrt{1-x^2} \le \bar{E}. \qquad (5.40)$$

We may now use Lemma 1 of Appendix A with $e(t)=(s(t+\Delta T)-s(t))\bar{E}$, which gives

$$\begin{aligned}
\int_0^{T^{\mathrm{ad}}} e(t)dt &= \bar{E}\int_0^{T^{\mathrm{ad}}} (s(t+\Delta T)-s(t))\,dt \\
&= \bar{E}\Delta T - \bar{E}\int_0^{\Delta T} s(t)dt \\
&\le \bar{E}\Delta T. \qquad (5.41)
\end{aligned}$$

Finally, we get

$$\|U(T^{\mathrm{ad}})-U'(T^{\mathrm{ad}})\| \le \sqrt{\frac{2\bar{E}\Delta T}{\hbar}} = \sqrt{\frac{2\bar{E}T^{\mathrm{ad}}}{\hbar K^{\mathrm{ad}}}} \qquad (5.42)$$

so that in order to keep an error of constant order δ for $x\to 0$, we must choose a number of steps proportional to T^{ad}/δ^2 (T^{ad} being itself proportional to δ^{-1}), for instance[6]

$$K^{\mathrm{ad}} = \lfloor \frac{\pi}{4\delta^3 x} \rfloor. \qquad (5.43)$$

For each step, we have to apply H_k during a time $\Delta T = T^{\mathrm{ad}}/K^{\mathrm{ad}}$, that is the unitary operation:

$$U'_k = e^{-iH_k\Delta T} = e^{-i\frac{H_0(1-s_k)\Delta T + H_f s_k \Delta T}{\hbar}}. \qquad (5.44)$$

Following the second stage of the conversion method, we replace U'_k by

$$U''_k = e^{-\frac{iH_0(1-s_k)\Delta T}{\hbar}} e^{-i\frac{H_f s_k \Delta T}{\hbar}}. \qquad (5.45)$$

The error introduced at each step by this approximation will be

$$\begin{aligned}
\|U'_k - U''_k\| &= O\left(s_k(1-s_k)\frac{\|[H_0,H_f]\|\Delta T^2}{\hbar^2}\right) \qquad (5.46) \\
&= O\left(s_k(1-s_k)\delta^4 x\right). \qquad (5.47)
\end{aligned}$$

For the K^{ad} steps, we have $U'(T)=\prod_k U'_k$, so that using Lemma 2 gives the total error

$$\|U'(T) - \prod_{k=1}^{K^{\mathrm{ad}}} U''_k\| = O(\delta). \qquad (5.48)$$

[6] As it was the case for the analog quantum search, the prefactor is arbitrarily chosen in order to simplify the comparison with the other algorithms.

Consequently, the number of steps K^{ad} required in the first stage (i.e., replacing $H(t)$ by $H'(t)$) also results in an error of order δ for the second stage. We may thus conclude that to get a solution with an error probability of order $O(\delta^2)$, it suffices to discretize the evolution in a number of steps of order $O(\delta^{-3}x^{-1})$. We see that the number of steps has been further increased by a factor of order δ^{-2} with respect to the analog quantum search. The comparison between the three search algorithms is summarized in Table 5.1.

Summary

We have shown that, in spite of their different original formulations, the three quantum search algorithms are very closely related. They all perform a rotation from the uniform superposition of all states to the uniform superposition of solution states at a constant angular velocity, even though a slightly different path is followed by the analog quantum search algorithm.

Actually, the fact that imposing a local adiabatic condition, optimizing the evolution rate according to the variations of the gap between the lowest two eigenvalues, exactly comes down to rotating the state at a constant angular velocity is quite remarkable. It could be worth investigating whether such a link between the gap and the rate at which the ground state is modified could be made for other problems solved by adiabatic evolution, such as the satisfiability problem as studied by Farhi *et al* in [FGGS00, FGG$^+$01].

The similarities between these algorithms become even more obvious when they are implemented on a quantum circuit as they all take the same generic form: a number of steps of order $\sqrt{N/M}$, each step having the same form $e^{-iH_0\delta t_0/\hbar}e^{-iH_f\delta t_f/\hbar}$. Note that the time ratio $\delta t_f/(\delta t_0+\delta t_f)$ during which H_f and H_0 are applied varies along the evolution according to a specific law in the case of the local adiabatic search algorithm, while it is 50% for Grover's algorithm as well as its Hamiltonian analogue.

In the next Chapter, we show that the quantum-circuit implementation of the adiabatic search algorithm will be helpful to use it as a building block to solve more advanced search problems.

	All 3 quantum search algorithms		
$\lvert\psi_0\rangle$	$\lvert\mathcal{N}\rangle$		
$\lvert\psi_k\rangle$	$e^{-iH_0\delta t_{0,k}/\hbar}e^{-iH_f\delta t_{f,k}/\hbar}\lvert\psi_{k-1}\rangle$		
	$= e^{-i\phi_k}\left(e^{i\theta}\sin\alpha_k\lvert\mathcal{M}\rangle + \cos\alpha_k\lvert\mathcal{M}^{\mathcal{C}}\rangle\right)$		
p_{err}	$1-\lvert\langle\mathcal{M}\lvert\psi_K\rangle\rvert^2$		
	Grover	Analog	Adiabatic
K	$\lfloor\pi/4x\rfloor$	$\lfloor\pi/4\delta x\rfloor$	$\lfloor\pi/4\delta^3x\rfloor$
$\bar{E}\delta t_{f,k}/\hbar$	π	2δ	$4s_k\delta^2$
$\bar{E}\delta t_{0,k}/\hbar$	π	2δ	$4(1-s_k)\delta^2$
ϕ_k	$k\pi$	$\bar{E}t_k/\hbar$	$\int_0^{t_k}E_0(t')dt'/\hbar$
θ	0	π	0
α_k	$2kx$	$2k\delta x$	$2k\delta^3x$
p_{err}	$O(x^2)$	$O(\delta^2)$	$O(\delta^2)$

Table 5.1: Summary of the properties of the three quantum search algorithms (all given at first non-zero order in x and δ).

Chapter 6

Structured search

Introduction

The quantum algorithms we have described in the previous chapters aim at solving unstructured search problems. More specifically, Grover's algorithm and its Hamiltonian-based cousins improve on a classical search as they are able to find a marked item in an unstructured database with a number of queries of order $\sqrt{N}$ instead of N (where N is the number of items in the database). Naturally, these quantum algorithms can also be used to solve a structured search problem with a quadratic speed-up over a naïve classical search that would exhaustively check every possible solution. However, exploiting the structure of the problem is well known to lead to better classical search algorithms. It is therefore tempting to imagine that better quantum search algorithms may be devised similarly by exploiting the problem structure. Following this, Cerf, Grover and Williams showed that this could be done by partitioning the unknown variables into two (or more) sets and then nesting a quantum search over one set into another search over two (or more) sets, yielding an average complexity of order $\sqrt{N^\alpha}$, with $\alpha < 1$ [CGW00].

While this algorithm, as well as Grover's original algorithm, stay within the standard paradigm of quantum computation based on quantum circuits, we have shown in the previous chapters that it was possible to devise quantum search algorithms of a different kind, based on continuous-time Hamiltonian evolution. In particular, we have introduced in Chapter 4 a quantum adiabatic search algorithm, which works as its discrete analogue Grover's algorithm for unstructured search problems. Actually, quantum adiabatic algorithms had initially been introduced by Farhi *et al* for solving structured problems such as satisfiability problems (k-SAT), but in such a way that until now only a numerical study has been possible [FGG$^+$01].

In this chapter, we bring the ideas of nested quantum search and quantum adiabatic computation together in order to devise a new quantum adiabatic algorithm adapted to structured problems. More specifically, we will show that an adiabatic search over a subset of the variables can be used to build a better initial Hamiltonian for the global adiabatic search. With this adiabatic algorithm, we recover the same complexity as the nested discrete algorithm of Ref. [CGW00], but we will see that it is more general in that it does not require the exact number of solutions (and partial solutions) to be known a priori. In order to nest an adiabatic quantum search, used as a sub-routine, into another, we will have to discretize it, making use of the results of the last chapter.

6.1 Structured problems

In this chapter, we consider a class of problems in which one has to find an assignment for a set of variables. For each additional variable considered, new constraints appear and reduce the set of satisfying assignments. This corresponds to most problems encountered in practice (k-SAT, graph coloring, planning, combinatorial optimization, ...).

For instance, let us consider the class 3-SAT which is NP-complete. In general, an instance of SAT is expressed as a boolean formula in *conjunctive normal form*, that is a conjunction ($\wedge$) of disjunctions ($\vee$) of *literals* (a literal being an elementary boolean expression made of one binary variable that may be negated or not). For 3-SAT, each disjunction involves exactly three literals, such that a possible instance for 3-SAT would be

$$(n_1 \vee n_2 \vee \neg n_4) \wedge (n_1 \vee \neg n_3 \vee n_5) \wedge (\neg n_2 \vee n_5 \vee \neg n_6). \tag{6.1}$$

The problem is to find assignments for the binary variables $(n_1, \ldots, n_6)$ satisfying the boolean formula. Since the disjunctions are related by the conjunction $\wedge$ ("AND"), they must all be satisfied simultaneously, such that 3-SAT finally boils down to the problem of finding assignments for a set of binary variables satisfying a set of constraints, each constraint involving three variables.

Let us now generalize these concepts to a broader class of structured problems. In these problems, for a set of ν_A (not necessarily binary) variables denoted as A, there is a corresponding set of constraints C_A. We may define a function f_A that tells if an assignment of the variables in A satisfies the constraints in C_A.

$$\begin{aligned} f_A &: \mathcal{N}_A \to \{0,1\} \\ &: n_A \to \begin{cases} 0 & \text{if } n_A \text{ does not satisfy } C_A \\ 1 & \text{if } n_A \text{ satisfies } C_A, \end{cases} \end{aligned} \tag{6.2}$$

where $\mathcal{N}_A = (\mathbb{Z}_d)^{\nu_A}$ is the set of all possible assignments for the ν_A variables, d being the number of possible assignments for each variable ($d = 2$ for bits). As quantum gates have to be reversible, the quantum equivalent of this function will be an oracle:

$$O_A : \mathcal{H}_{N_A} \otimes \mathcal{H}_2 \to \mathcal{H}_{N_A} \otimes \mathcal{H}_2 : |n_A\rangle \otimes |q\rangle \to |n_A\rangle \otimes |f_A(n_A) \oplus q\rangle, \tag{6.3}$$

where $N_A = d^{\nu_A}$ is the number of possible assignments for the ν_A variables. It has been shown in previous chapters that this oracle is closely related to a Hamiltonian whose ground states, of energy 0, are the basis states encoding a satisfying assignment and whose excited states, of energy $\bar{E}$, are all other basis states:

$$H_A|n_A\rangle = \begin{cases} \bar{E}|n_A\rangle & \text{if } n_A \text{ does not satisfy } C_A \\ 0 & \text{if } n_A \text{ satisfies } C_A \end{cases} \tag{6.4}$$

or

$$H_A = \bar{E}(I_A - \sum_{m_A \in \mathcal{M}_A} |m_A\rangle\langle m_A|) \tag{6.5}$$

where $\mathcal{M}_A$ is the set of satisfying assignments for the variables in A. It is possible to efficiently simulate the time evolution according to this Hamiltonian, that is, the unitary operator $e^{-iH_A t}$ can be realized using a sequence of one- and two-qubit gates and two oracle calls (see Chapter 5 for details).

Now suppose we consider a larger set of variables $\nu_{AB} = \nu_A + \nu_B$ that have to satisfy a set of constraints $C_{AB} \supset C_A$. To discriminate between assignments satisfying C_{AB} or not, we will use an oracle O_{AB} or a corresponding Hamiltonian H_{AB} defined as in Eqs. (6.3) and (6.4). The basic idea of our structured search will be to find the solutions of C_{AB} by first building the assignments of the ν_A primary variables satisfying C_A, then by completing them with all possible assignments of the ν_B secondary variables, and finally by searching among these could-be solutions those satisfying the constraints C_{AB}.

6.2 Structured search with two levels of nesting

This problem is of the same type as the one considered in [CGW00], where the technique of nesting was introduced in the context of Grover's traditional algorithm. Here, we apply this technique to the adiabatic quantum search algorithm.

Suppose we divide the variables of our problem into two subsets A (ν_A elements) and B (ν_B elements). First, we will perform a search on the variables in A using the Hamiltonian H_A that encodes the constraints in C_A:

$$H_A = \bar{E}(I_A - \sum_{m_A \in \mathcal{M}_A} |m_A\rangle\langle m_A|). \tag{6.6}$$

Then we will use the Hamiltonian H_{AB} acting on all variables in $A \cup B$ and encoding the whole set of constraints C_{AB}

$$H_{AB} \quad = \quad \bar{E}(I_{AB} - \sum_{(m_A, m_B) \in \mathcal{M}_{AB}} |m_A\rangle\langle m_A| \otimes |m_B\rangle\langle m_B|) \tag{6.7}$$

to construct a superposition of the solutions of the full problem $\mathcal{M}_{AB}$. A final measurement of the quantum register will then give one of the global solutions at random.

6.2.1 Adiabatic search on the primary variables

The preliminary search on the variables in A is a simple unstructured search as explained in Chapter 4. As there are ν_A variables in A, the corresponding Hilbert space is of dimension $N_A = d^{\nu_A}$. Let M_A be the number of solutions in $\mathcal{M}_A$. Performing an adiabatic quantum search, we may thus transform the initial state

$$|\mathcal{N}_A\rangle = \frac{1}{\sqrt{N_A}} \sum_{n_A \in \mathcal{N}_A} |n_A\rangle \tag{6.8}$$

into a state close to the uniform superposition of all solutions in $\mathcal{M}_A$

$$|\mathcal{M}_A\rangle = \frac{1}{\sqrt{M_A}} \sum_{m_A \in \mathcal{M}_A} |m_A\rangle \tag{6.9}$$

in a time of order[1]

$$T_A = \Theta\left(\sqrt{\frac{N_A}{M_A}}\right). \tag{6.10}$$

[1] In this chapter, we will concentrate on the scaling of the running time versus the number of possible assignments N and the number of solutions M, and not on its prefactor, which is why we use the "big-Θ" and "big-O" notations.

Let us point out that here and throughout the rest of this chapter, it seems that the number of solutions M_A (and later M_{B/m_A} and M_A^S) must be known to derive the minimal time T_A (and later T_B and T_C) needed to perform the computation with a bounded error probability. Actually, as already explained in the case of the unstructured search in Chapter 4, an approximate value M' of the order of the actual M is sufficient as it will only affect the error probability by a factor of $(M'/M)^2$. In real problems, this issue may thus be addressed by using approximate methods to evaluate the number of solutions (such as Eq. (6.45) of Section 6.4 for k-SAT).

6.2.2 Adiabatic search on the secondary variables

We will now perform a preliminary search in the Hilbert space of dimension $N_B = d^{\nu_B}$ of the secondary variables in B by extending the partial solutions $|m_A\rangle$. We prepare the variables in B in a state that is the uniform superposition

$$|\mathcal{N}_B\rangle = \frac{1}{\sqrt{N_B}} \sum_{n_B \in \mathcal{N}_B} |n_B\rangle. \tag{6.11}$$

Globally, the system is thus in the superposition:

$$|\mathcal{M}_A\rangle \otimes |\mathcal{N}_B\rangle = \frac{1}{\sqrt{M_A N_B}} \sum_{\substack{m_A \in \mathcal{M}_A \\ n_B \in \mathcal{N}_B}} |m_A\rangle \otimes |n_B\rangle, \tag{6.12}$$

where some terms correspond to a global solution of the problem [$(m_A, m_B) \in \mathcal{M}_{AB}$ satisfying all constraints in C_{AB}] while the others correspond to a partial solution only [$m_A \in \mathcal{M}_A$ satisfies C_A but $(m_A, m_B) \notin \mathcal{M}_{AB}$ does not satisfy C_{AB}]. We now divide the set $\mathcal{M}_A$ of solutions of C_A into two subsets: $\mathcal{M}_A^S$ will be the set of m_A's for which there exists at least one solution (m_A, m_B) of C_{AB} and $\mathcal{M}_A^{NS}$ the set of m_A's for which there is no such solution.

$$\mathcal{M}_A^S = \{m_A \in \mathcal{M}_A \,|\, \exists\, m_B, (m_A, m_B) \in \mathcal{M}_{AB}\} \tag{6.13}$$

$$\mathcal{M}_A^{NS} = \{m_A \in \mathcal{M}_A \,|\, \forall\, n_B, (m_A, n_B) \notin \mathcal{M}_{AB}\} \tag{6.14}$$

Of course, we thus have $\mathcal{M}_A = \mathcal{M}_A^S \cup \mathcal{M}_A^{NS}$. We may now rewrite our initial state (6.12) as

$$\begin{aligned} |\mathcal{M}_A\rangle \otimes |\mathcal{N}_B\rangle = & \frac{1}{\sqrt{M_A N_B}} \sum_{\substack{m_A \in \mathcal{M}_A^{NS} \\ n_B \in \mathcal{N}_B}} |m_A\rangle \otimes |n_B\rangle \\ & + \frac{1}{\sqrt{M_A N_B}} \sum_{\substack{m_A \in \mathcal{M}_A^{S} \\ n_B \in \mathcal{N}_B}} |m_A\rangle \otimes |n_B\rangle. \end{aligned} \tag{6.15}$$

In the first part of this expression, no term correspond to a solution of the full problem, whereas in the second part, some terms do and others do not. The goal of this stage of the computation will be to increase the amplitude of the solution terms in this last part. To achieve this, we perform an adiabatic evolution using the initial Hamiltonian

$$H_i = \bar{E} I_A \otimes (I_B - |\mathcal{N}_B\rangle\langle\mathcal{N}_B|), \tag{6.16}$$

which has $|\mathcal{M}_A\rangle \otimes |\mathcal{N}_B\rangle$ as a ground state. The final Hamiltonian will be

$$H_f = H_{AB} - H_A \otimes I_B. \tag{6.17}$$

We see that these Hamiltonians share the following properties:

1. They do not induce evolution of states $|n_A\rangle \otimes |\mathcal{N}_B\rangle$ corresponding to assignments n_A of $\mathcal{N}_A$ that do not satisfy C_A:
$$H_{i,f}|n_A\rangle \otimes |\mathcal{N}_B\rangle = 0 \quad \forall\, n_A \notin \mathcal{M}_A. \tag{6.18}$$

2. They do not couple states corresponding to different m_A's:
$$\langle m_A|H_{i,f}|m'_A\rangle = 0 \quad \forall\, m_A \neq m'_A \in \mathcal{M}_A. \tag{6.19}$$

It follows that the instantaneous Hamiltonian of the adiabatic evolution $H(t)$ satisfies the same properties. Using property 2, it may easily be shown that the effect of the adiabatic evolution will be to perform independent (and parallel) adiabatic searches for each $m_A \in \mathcal{M}_A$. More precisely, each term in $|\mathcal{M}_A\rangle \otimes |\mathcal{N}_B\rangle$ corresponding to a partial solution $m_A \in \mathcal{M}_A^S$

$$|m_A\rangle \otimes |\mathcal{N}_B\rangle = \frac{1}{\sqrt{N_B}} \sum_{n_B \in \mathcal{N}_B} |m_A\rangle \otimes |n_B\rangle \tag{6.20}$$

will evolve into

$$|m_A\rangle \otimes |\mathcal{M}_{B/m_A}\rangle = \frac{1}{\sqrt{M_{B/m_A}}} \sum_{m_B \in \mathcal{M}_{B/m_A}} |m_A\rangle \otimes |m_B\rangle, \tag{6.21}$$

as long as

$$T_B = \Omega\left(\sqrt{\frac{N_B}{M_{B/m_A}}}\right), \tag{6.22}$$

where $\mathcal{M}_{B/m_A}$ is the set of m_B's such that $(m_A, m_B) \in \mathcal{M}_{AB}$ and M_{B/m_A} is the number of these elements. For this condition to be satisfied for all m_A's simultaneously, we may take

$$T_B = \Theta\left(\max_{m_A} \sqrt{\frac{N_B}{M_{B/m_A}}}\right) = \Theta\left(\sqrt{\frac{N_B}{\min_{m_A} M_{B/m_A}}}\right). \tag{6.23}$$

Here is the major advantage of this adiabatic algorithm over its discrete counter-part [CGW00] where all M_{B/m_A}'s had to be supposed equal to 1, as here it is sufficient that they are of the same order of magnitude to ensure an error probability of the same order for each term.

At the end of this second stage, we thus have constructed a state close to

$$\begin{aligned} |\psi_{AB}\rangle &= \frac{1}{\sqrt{M_A N_B}} \sum_{\substack{m_A \in \mathcal{M}_A^{NS} \\ n_B \in \mathcal{N}_B}} |m_A\rangle \otimes |n_B\rangle \\ &\quad + \frac{1}{\sqrt{M_A}} \sum_{m_A \in \mathcal{M}_A^S} e^{i\phi_{m_A}} |m_A\rangle \otimes \frac{1}{\sqrt{M_{B/m_A}}} \sum_{m_B \in \mathcal{M}_{B/m_A}} |m_B\rangle \\ &= \sqrt{\frac{M_A^{NS}}{M_A}} |\mathcal{M}_A^{NS}\rangle \otimes |\mathcal{N}_B\rangle + \sqrt{\frac{M_A^S}{M_A}} |\mathcal{M}_{AB}\rangle, \end{aligned} \tag{6.24}$$

where ϕ_{m_A}'s are phases appearing during the evolution, the non-solution state $|\mathcal{M}_A^{NS}\rangle$ is defined as

$$|\mathcal{M}_A^{NS}\rangle = \frac{1}{\sqrt{M_A^{NS}}} \sum_{m_A \in \mathcal{M}_A^{NS}} |m_A\rangle, \tag{6.25}$$

the superposition of solution states $|\mathcal{M}_{AB}\rangle$ as[2]

$$\begin{aligned} |\mathcal{M}_{AB}\rangle &= \frac{1}{\sqrt{M_A^S}} \sum_{m_A \in \mathcal{M}_A^S} e^{i\phi_{m_A}} |m_A\rangle \\ &\otimes \frac{1}{\sqrt{M_{B/m_A}}} \sum_{m_B \in \mathcal{M}_{B/m_A}} |m_B\rangle \end{aligned} \tag{6.26}$$

and M_A^{NS} (respectively M_A^S) is the number of elements in set $\mathcal{M}_A^{NS}$ (respectively $\mathcal{M}_A^S$). We thus have a superposition of all the non-solution in $\mathcal{M}_A^{NS} \otimes \mathcal{N}_B$ and all the solutions $\mathcal{M}_{AB}$.

6.2.3 Global adiabatic search

Stages A and B define a unitary evolution U that applies the initial state $|\mathcal{N}_A\rangle \otimes |\mathcal{N}_B\rangle$ onto $|\psi_{AB}\rangle$:

$$\begin{aligned} U|\mathcal{N}_A\rangle \otimes |\mathcal{N}_B\rangle &\approx |\psi_{AB}\rangle & (6.27)\\ &= \sqrt{\frac{M_A^{NS}}{M_A}} |\mathcal{M}_A^{NS}\rangle \otimes |\mathcal{N}_B\rangle + \sqrt{\frac{M_A^S}{M_A}} |\mathcal{M}_{AB}\rangle. & (6.28) \end{aligned}$$

In this state, we now need to decrease the amplitude of the first term, corresponding to partial solutions only, and increase the amplitude of the second term, corresponding to global solutions. This could be realized efficiently by performing an adiabatic search (stage C) using as initial Hamiltonian:

$$\begin{aligned} H_i &= \bar{E}(I_{AB} - |\psi_{AB}\rangle\langle\psi_{AB}|) & (6.29)\\ &\approx \bar{E}U(I_{AB} - |\mathcal{N}_A\rangle\langle\mathcal{N}_A| \otimes |\mathcal{N}_B\rangle\langle\mathcal{N}_B|)U^\dagger & (6.30)\\ &\approx U\, H_0\, U^\dagger, & (6.31) \end{aligned}$$

where $H_0 = \bar{E}(I_{AB} - |\mathcal{N}_A\rangle\langle\mathcal{N}_A| \otimes |\mathcal{N}_B\rangle\langle\mathcal{N}_B|)$, and as final Hamiltonian

$$\begin{aligned} H_f &= H_{AB} & (6.32)\\ &= \bar{E}(I_{AB} - \sum_{(m_A, m_B) \in \mathcal{M}_{AB}} |m_A\rangle\langle m_A| \otimes |m_B\rangle\langle m_B|) \end{aligned}$$

during a time

$$T_C = \Theta\left(\sqrt{\frac{M_A}{M_A^S}}\right). \tag{6.33}$$

Unfortunately, we do not have access to H_i, so that the interpolating Hamiltonian $\tilde{H}(s) = (1-s)H_i + sH_f$ cannot be applied directly. However, we know from the last chapter that the

[2] Let us note that this is generally not a uniform superposition of all solution states since, in addition to the phases ϕ_{m_A}, the amplitude of a solution state $|m_A\rangle \otimes |m_B\rangle$ will depend on the number M_{B/m_A} of other solutions sharing the same partial solution m_A.

basic steps of the quantum-circuit implementation of this adiabatic algorithm only require the application of H_i during a particular time t, that is,

$$e^{-\frac{iH_i t}{\hbar}} \approx e^{-\frac{iUH_0 U^\dagger t}{\hbar}} = Ue^{-\frac{iH_0 t}{\hbar}} U^\dagger. \tag{6.34}$$

Hence, each application of H_i during a time t will be equivalent to sequentially applying $U^\dagger$, $e^{-iH_0 t/\hbar}$, and U, which means performing the adiabatic evolution U (stages A and B) backwards, then applying H_0 for a time t, and finally rerun the adiabatic evolution U forwards (stages A and B).

We know that to discretize the adiabatic evolution with a bounded error, we must take a number of steps K_C of order T_C. We may now evaluate the complexity of this algorithm. As it consists of K_C steps, each involving two applications of U or $U^\dagger$, each taking a time of order $T_A + T_B$, the algorithm finally takes a time of order:

$$\begin{aligned} T &= (T_A + T_B)K_C \qquad (6.35)\\ &= \Theta\left(\left(\sqrt{\frac{N_A}{M_A}} + \sqrt{\frac{N_B}{\min_{m_A} M_{B/m_A}}}\right)\sqrt{\frac{M_A}{M_A^S}}\right)\\ &= \Theta\left(\sqrt{\frac{N_A}{M_A^S}} + \sqrt{\frac{M_A N_B}{M_A^S \min_{m_A} M_{B/m_A}}}\right). \qquad (6.36)\end{aligned}$$

Let us note that since $M_{B/m_A} \geq 1$ ($\forall\, m_A$), this complexity scales as

$$T = O\left(\frac{\sqrt{N_A} + \sqrt{M_A N_B}}{\sqrt{M_A^S}}\right). \tag{6.37}$$

For the particular case where there is at most one solution (m_A, m_B) per partial solution m_A

$$M_{B/m_A} = 1 \quad \forall\, m_A \in \mathcal{M}_A^S, \tag{6.38}$$

we have $M_A^S = M_{AB}$ and we recover the complexity of the equivalent discrete algorithm exposed in Ref. [CGW00]. However, it should be stressed that we do not need this last assumption here, which is the main difference between these two algorithms. A more detailed analysis of this complexity will be performed in Section 6.4.

6.3 Discretizing the adiabatic evolution

Let us now apply the discretization method developed in the last chapter to this adiabatic structured quantum search algorithm. We could of course discretize all three stages (A, B, C) of our algorithm in order to implement it on a quantum circuit, but we will concentrate on stage C which is the only one that absolutely requires discretization. Nonetheless, following the lines of the application of the discretization method to the unstructured search (see Section 5.5), it is easy to show that stage A (respectively B) would require a number of steps K_A (respectively K_B) of the same order as the computation time T_A (respectively T_B).

For the final stage, the global adiabatic search, the initial and final Hamiltonians H_i and H_f are defined in Eq. (6.29)-(6.32). Except from the fact that these Hamiltonians differ from those we treated in the case of the unstructured adiabatic quantum search, the evaluation of the errors introduced by the two stages of the discretization is totally similar and, as

$$\begin{aligned} \|H_i - H_f\| &< \bar{E}, & (6.39)\\ \|[H_i, H_f]\| &< \sqrt{\frac{M_A^S}{M_A}}\bar{E}^2 & (6.40)\end{aligned}$$

and $T_C = \Theta\left(\sqrt{\frac{M_A}{M_A^S}}\right)$, it leads to

$$\begin{aligned} \|U(T) - U'(T)\| &= O\left(\sqrt{2\frac{\sqrt{\frac{M_A}{M_A^S}}}{K_C}}\right) & (6.41)\\ \|U'(T) - \prod_{k=1} K_C U''_k\| &= O\left(\frac{\sqrt{\frac{M_A}{M_A^S}}}{K_C}\right). & (6.42)\end{aligned}$$

Therefore, as announced in Section 6.2, we have to cut our evolution in a number of steps $K_C = \Theta\left(\sqrt{\frac{M_A}{M_A^S}}\right)$ of the same order as T_C. Each step k will take the form:

$$\begin{aligned} U''_k &= e^{-\frac{i(1-s_k)H_i\Delta T}{\hbar}}e^{-\frac{is_kH_f\Delta T}{\hbar}} & (6.43)\\ &\approx Ue^{-\frac{i(1-s_k)H_0\Delta T}{\hbar}}U^\dagger e^{-\frac{is_kH_f\Delta T}{\hbar}}, & (6.44)\end{aligned}$$

where the applications of Hamiltonians H_0 during a time $(1 - s_k)\Delta T$ and H_f during a time $s_k\Delta T$ may be realized by the procedure exposed in Chapter 5.

6.4 Complexity analysis

To estimate the efficiency of this algorithm, we will follow the same development as in [CGW00]: as we have seen in Section 6.2, under the assumption (6.38) that we will consider here, the complexity of this adiabatic algorithm has exactly the same form as its circuit-based counterpart.

First of all let us define a few concepts (for details here and throughout this section, we refer the reader to Ref. [CGW00]). The structured search problem is to find an assignment of $\nu_{AB} = \nu_A + \nu_B$ variables among d possibilities for each variable and satisfying e constraints, each involving at most k of these variables. We define as a *ground instance* an assignment of all the variables involved in a particular constraint. A ground instance will be said to be *no-good* if it violates the constraint. Let ξ be the number of those no-good ground instances.

Empirical studies show that the difficulty of solving a structured problem essentially depends on four parameters: the number of variables ν_{AB}, the number of possible assignment per variable d, the number of variables per constraint k, and the number of no-good ground instances ξ. Intuitively, we understand that if ξ is small, there are many assignments satisfying the constraints so the problem is easy to solve. On the contrary, if ξ is large, the problem is over-constrained and it is easy to show that there is no solution. More precisely, it may be shown that for fixed ν_{AB} and d, the average difficulty may be evaluated by the parameter $\beta = \xi/\nu_{AB}$. The hard problems will be concentrated around a critical value β_c.

Let us now estimate the complexity (6.37). Let $p(\nu)$ be the probability that a randomly generated assignment of the ν first variables satisfies all the constraints involving these variables. We then have $M_A = p(\nu_A)d^{\nu_A}$ and $M_{AB} = p(\nu_{AB})d^{\nu_{AB}}$ while it is shown in [CGW00] that:

$$p(\nu) \approx d^{-\nu_{AB}(\beta/\beta_c)(\nu/\nu_{AB})^k}. \tag{6.45}$$

Eq. (6.37) becomes

$$T = O\left(\frac{\sqrt{d^{\nu_A}} + \sqrt{d^{\nu_{AB}[1-(\beta/\beta_c)(\nu_A/\nu_{AB})^k]}}}{\sqrt{d^{\nu_{AB}}(1-\beta/\beta_c)}}\right) \tag{6.46}$$

or equivalently, with $a = \sqrt{d^{\nu_{AB}}}$ and $y = \nu_A/\nu_{AB}$:

$$T = O\left(\frac{a^y + a^{1-\frac{\beta}{\beta_c}y^k}}{a^{1-\frac{\beta}{\beta_c}}}\right). \tag{6.47}$$

We now optimize y, the fraction of variables for which we perform a partial search, to minimize the computation time. We have to solve the equation

$$\frac{\beta}{\beta_c}ky^{k-1} = a^{\frac{\beta}{\beta_c}y^k+y-1} \tag{6.48}$$

which, for large a (that is large ν_{AB}) approximately reduces to

$$\frac{\beta}{\beta_c}y^k + y - 1 = 0. \tag{6.49}$$

The solution of this equation α ($0 \leq \alpha \leq 1$) corresponds to the optimal partial search we may perform such that the complexity grows with the smallest power in d for $\nu_{AB} \to \infty$. This optimal computation time may then be written as

$$T = O\left(\frac{2a^\alpha}{a^{1-\frac{\beta}{\beta_c}}}\right) = O\left(\frac{\sqrt{d^{\alpha\nu_{AB}}}}{\sqrt{d^{\nu_{AB}(1-\frac{\beta}{\beta_c})}}}\right). \tag{6.50}$$

Let us now consider the hardest problems for which $\beta \approx \beta_c$. For these problems, the complexity reads

$$T = O\left(\sqrt{d^{\alpha\nu_{AB}}}\right), \tag{6.51}$$

which we may immediately compare to the complexity of an unstructured quantum search, i. e. $O\left(\sqrt{d^{\nu_{AB}}}\right)$. The gain in the exponent α depends on k through Eq. (6.49) For instance, we find $\alpha = 0.62$ for $k = 2$, $\alpha = 0.68$ for $k = 3$ and $\alpha \to 1$ when $k \to \infty$.

As already pointed out, we recover exactly the same complexity as with the discrete structured search algorithm exposed in [CGW00], but with fewer hypotheses as, due to the particular form of the required running time for an adiabatic algorithm (4.33), the number of solutions derived from Eq. (6.45) must only give an order of magnitude while it must be a good approximation for its discrete analogue. Moreover, as seen in Section 6.2, the numbers of solutions M_{B/m_A} do not have to be equal for all m_A's, but only of the same order.

To compare these results with a classical algorithm, let us consider a specific problem, namely the satisfiability of boolean formulas in conjunctive normal form, or k-SAT. For 3-SAT, which is known to be NP-complete, some of the best classical algorithms have a worst-case running time that scales as $O\left(2^{0.4\nu_{AB}}\right)$ [Sch99, HSSW02], while, as $\alpha = 0.68$ for $k =$

3, our quantum adiabatic algorithm has a computation time of order $O\left(2^{0.34\nu_{AB}}\right)$, which is a slight improvement. Nonetheless, let us recall that there is a distinction between the worst-case complexity often used for characterizing classical algorithms and the average-case complexity for hardest problems ($\beta = \beta_c$) used here for characterizing our quantum algorithm. However, let us also notice that this scaling could be further improved by using several levels of nesting, i.e. by replacing the preliminary search over the primary variables by a another nested structured search (see the analysis of the discrete counterpart of this technique in the Appendix of [CGW00]).

Summary

In this chapter, we have introduced a new quantum search algorithm combining the approach based on local adiabatic evolution exposed in Chapter 4 and the nesting technique introduced in [CGW00]. It allows one to adiabatically solve structured search problems with an improved complexity over a naïve adiabatic search that would not exploit the structure of the problem.

The basic idea is to perform a preliminary adiabatic search over a reduced number of variables of the problem in order to keep only a superposition of the assignments that respect the constraints of this partial problem, and then to complete these partial solutions by finding satisfying assignments for the remaining variables. We have seen that to implement this algorithm, the global adiabatic evolution (stage C) has to be discretized, which makes it possible to *nest* the preliminary search (stages A and B) into the global one. Each step of the algorithm requires to alternate partial adiabatic searches backwards and forwards with global search operations.

A complexity analysis shows that the average computation time of this adiabatic algorithm, although still exponential, grows with a reduced exponent in the problem size compared to quantum unstructured search algorithms. We illustrated this speed-up for a NP-complete problem such as 3-SAT.

Chapter 7

Robustness to noise

Introduction

Recently, there has been a growing interest in the study of Hamiltonian-based quantum algorithms, as opposed to the standard circuit-based paradigm of quantum computing. In addition to the analog and adiabatic quantum search exposed in previous chapters, this includes many other algorithms such as the algorithms by quantum adiabatic evolution for satisfiability problems [FGGS00, FGG$^+$01] or the search algorithms by continuous quantum walks [FG98b, CCD$^+$03]. While, as shown in Chapter 5, these algorithms may be translated into circuit-based algorithms so that they can be implemented on a "standard" quantum computer, another approach is to consider a "continuous" quantum computer specifically designed to run this type of algorithm. As such a computer could be subject to noise, it seems important to study how well it behaves in the presence of noise. Until now, this has only been done for some specific algorithms subject to some very particular noise. For instance, Childs *et al* have considered the case of the quantum adiabatic algorithm for satisfiability problems [FGG$^+$01] in the presence of an error on the ideal Hamiltonian defined by an extra term with random parameters but which deterministically evolves in time [CFP02]. While this was a numerical analysis, Shenvi *et al* analytically studied the effect of a Markovian stochastic variable perturbing the amplitude of the oracle Hamiltonian [SBW03] in the specific case of the analog analogue of Grover's algorithm [FG98a]. The purpose of this chapter is to derive analytical results for any Hamiltonian-based algorithm perturbed by a general Hamiltonian error described by a stationary gaussian random process.

7.1 Noise model

First of all, let us properly define the problem we will study. Suppose we have an ideal Hamiltonian-based algorithm:

$$i\hbar\frac{d}{dt}|\bar{\psi}(t)\rangle = \bar{H}(t)|\bar{\psi}(t)\rangle. \tag{7.1}$$

At the end of the computation, $t = T$, we should obtain the state $|\bar{\psi}(T)\rangle$ that after some measurement defines the output of the algorithm. Now suppose a perturbation $\varepsilon h(t)$ adds to the ideal Hamiltonian[1]:

$$H(t) = \bar{H}(t) + \varepsilon h(t). \tag{7.2}$$

Instead of $|\bar{\psi}(T)\rangle$ we will get at the end of the computation a different state $|\psi(T)\rangle$. The problem is to evaluate the error probability

$$p_{\mathrm{err}} = 1 - |\langle\bar{\psi}(T)|\psi(T)\rangle|^2 \tag{7.3}$$

introduced by the perturbation.

In order to derive analytical results, we will have to make a few assumptions about the noise $\varepsilon h(t)$. First of all, we limit ourselves to a small amplitude noise with $\varepsilon \ll 1$ such that we may use perturbation theory.

We also assume that in any basis $|\varphi_k\rangle (k = 0, \ldots, N-1)$ of the N-dimensional Hilbert space where the computation takes place, the matrix elements of $h(t)$ are normal random variables:

$$h_{kl}(t) = \langle\varphi_k|h(t)|\varphi_l\rangle \in \mathcal{N}(0, \sigma_{kl}). \tag{7.4}$$

This implies that the matrix $h(t)$ is drawn from a Gaussian Orthogonal Ensemble (GOE), and that the standard deviation σ_{kl} of its different elements depend on an overall standard deviation σ such that $\sigma_{kl}^2 = (1+\delta_{kl})\sigma^2$ (see [Stö99] for details about random matrix ensembles). Moreover, two different elements of a GOE matrix are independent:

$$\begin{array}{ccc} \langle h_{kl}(t)h_{k'l'}(t)\rangle & = & 0 \\ & \Longleftrightarrow & \\ (k,l) \neq (k',l') & \text{and} & (k,l) \neq (l',k'). \end{array} \tag{7.5}$$

Even if this hypothesis does not seem to be based on any physical source of error, it could be justified by considering that the noise is caused by many different sources of error which, combined together and due to the central-limit theorem, would finally result in a random Hamiltonian drawn from a GOE.

Furthermore, we assume that the random matrix elements $h_{kl}(t)$ are distributed in time as a stationary random process with an autocorrelation function

$$R(\tau) = \langle h_{kl}(t+\tau)h_{kl}(t)\rangle\,. \tag{7.6}$$

For instance, a very typical noise model is a white noise with a high-frequency cut-off ω_0 (see for instance [Agr92]) which yields

$$R(\tau) = \sigma_{kl}^2 \frac{\sin\omega_0\tau}{\omega_0\tau}. \tag{7.7}$$

However, to be slightly more general, we will only assume that the autocorrelation function is of the type

$$R(\tau) = \sigma_{kl}^2 f(\omega_0\tau), \tag{7.8}$$

where $f(x)$ verifies $f(-x) = f(x)$, $f(x) \leq f(0) = 1$, and some other regularity conditions (see next sections).

[1] Throughout this chapter, ideal quantities will be overlined, while noisy quantities not.

Finally, we would like to keep a constant signal-to-noise ratio as N increases, that is, the eigenvalues of $h(t)$ should scale as the ones of $\bar{H}(t)$. Since Wigner's semi-circular law implies that the density of eigenvalues of GOE matrices for $N \gg 1$ is given by

$$\rho(E) \underset{N\to\infty}{\longrightarrow} \begin{cases} \frac{1}{4\sigma^2\pi}\sqrt{4\sigma^2 N - E^2} & \text{if } |E| \leq \sqrt{4\sigma^2 N} \\ 0 & \text{otherwise,} \end{cases} \tag{7.9}$$

as plotted in Fig. 7.1, this will be the case if we suppose that $\sigma^2 = \bar{E}^2/4N$ where $\bar{E}$ is of the order of the eigenvalues of $\bar{H}(t)$.

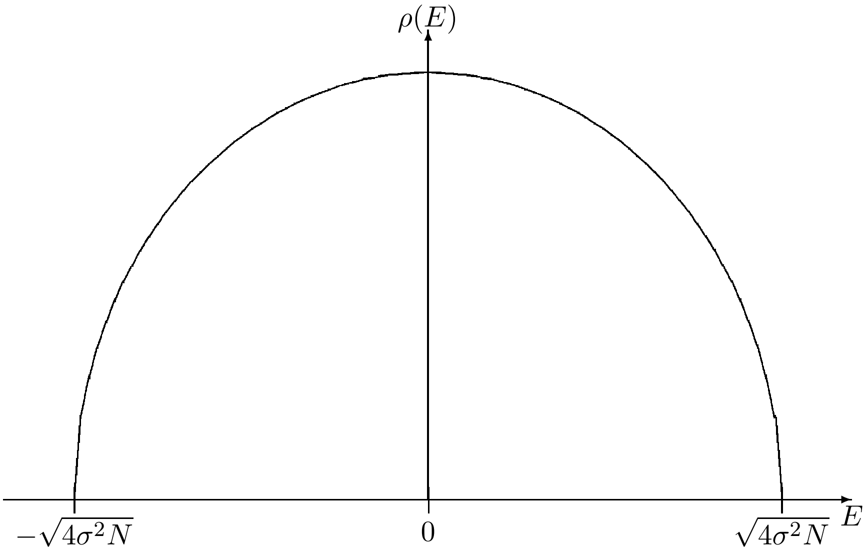

Figure 7.1: Wigner's semi-circular law: density of eigenvalues of the matrices in the Gaussian Orthogonal Ensemble (in the limit $N \to \infty$).

7.2 Noisy time-independent Hamiltonian evolution

7.2.1 Perturbation theory

Let us study the simplest case of a time-independent Hamiltonian evolution. The solution of the ideal Schrödinger equation will be

$$|\bar{\psi}(t)\rangle = \sum_k \bar{b}_k e^{-i\frac{E_k t}{\hbar}} |\varphi_k\rangle, \tag{7.10}$$

where $|\varphi_k\rangle$ and E_k are the eigenstates and eigenvalues of the ideal Hamiltonian and the $\bar{b}_k$'s follow from the initial conditions.

By use of perturbation theory, we now study the effect of a small time-dependent perturbation $\varepsilon h(t)$ on the ideal Hamiltonian $\bar{H}$. Developing the solution of the perturbed equation in the basis formed by the solutions of the ideal equation,

$$|\psi(t)\rangle = \sum_k b_k(t) e^{-i\frac{E_k t}{\hbar}} |\varphi_k\rangle, \tag{7.11}$$

and introducing into the Schrödinger equation, we get

$$\dot{b}_k = -i\frac{\varepsilon}{\hbar}\sum_l b_l e^{i\omega_{kl}t} h_{kl}(t), \tag{7.12}$$

where $\omega_{kl} = (E_k - E_l)/\hbar$. Using the same initial state as for the ideal evolution, $b_k(0) = \bar{b}_k$, we have

$$b_k(t) = \bar{b}_k - i\frac{\varepsilon}{\hbar}\sum_l \int_0^t b_l(t_1) e^{i\omega_{kl}t_1} h_{kl}(t_1) dt_1. \tag{7.13}$$

As $b_l(t_1)$ appears in the right member, this is only an implicit solution. However, similarly to the adiabatic approximation considered in Chapter 3.2.2, we may solve the system by using this implicit solution recursively, building step by step an expansion of $b_k(t)$ in terms of increasing order in ε. This is standard perturbation theory, which we now apply to our problem in order to evaluate the error probability p_{err} introduced by the perturbation. As the matrix elements of $h(t)$ are random variables, so will be p_{err}, such that we may only derive statistics about its value. Let us consider its mean $\langle p_{\text{err}}\rangle$. Using our assumption that $h(t)$ is a random matrix drawn from a GOE ensemble, we see that

$$\begin{aligned}
\langle p_{\text{err}}\rangle &= 1 - \left\langle |\langle\bar{\psi}(T)|\psi(T)\rangle|^2\right\rangle = 1 - \left\langle \left|\sum_k \bar{b}_k^* b_k(t)\right|^2 \right\rangle \\
&= \frac{\varepsilon^2}{\hbar^2}\left\{ \sum_{k,l,m} \bar{b}_k^*\bar{b}_m \iint_0^T dt_1 dt_2 e^{i(\omega_{kl}t_1+\omega_{lm}t_2)} \langle h_{kl}(t_1)h_{lm}(t_2)\rangle \right. \\
&\quad \left. - \sum_{k,l,k',l'} \bar{b}_k^*\bar{b}_l\bar{b}_{k'}^*\bar{b}_{l'} \iint_0^T dt_1 dt_2 e^{i(\omega_{kl}t_1+\omega_{k'l'}t_2)} \langle h_{kl}(t_1)h_{k'l'}(t_2)\rangle \right\} + O(\varepsilon^3) \\
&= \varepsilon^2\left\{ \sum_{k,l} |\bar{b}_k|^2(1-|\bar{b}_l|^2) I_{kl}^- - \sum_{k\neq l} (\bar{b}_k^*\bar{b}_l)^2 I_{kl}^+ \right\} + O(\varepsilon^3),
\end{aligned} \tag{7.14}$$

where we have introduced the integrals

$$I_{kl}^{\pm} = \frac{\sigma_{kl}^2}{\hbar^2}\iint_0^T dt_1 dt_2 e^{i\omega_{kl}(t_1\pm t_2)} f\left(\omega_0(t_1-t_2)\right) \tag{7.15}$$

that characterize the coupling between states $|\varphi_k\rangle$ and $|\varphi_l\rangle$ induced by the perturbation. The problem now is to evaluate these integrals. We see that apart from the noise model defined by the autocorrelation function $f(x)$ and the high-frequency cut-off ω_0, they will depend on the computation time T and the spectrum of the ideal Hamiltonian through the frequencies ω_{kl}. These will vary for different problems but we may derive some general bounds.

First of all, as these are integrals over a domain of size T^2 and as the amplitude of their integrand is bounded by 1, we immediately see that whatever the values of ω_{kl} and ω_0 will be, the coupling strength will be bounded as

$$|I_{kl}^{\pm}| \leq \frac{\sigma_{kl}^2 T^2}{\hbar^2}. \tag{7.16}$$

Furthermore, let us note that the I_{kl}^+ couplings only appear between the eigenstates that are initially populated, and may therefore be considered as the interferences caused by the noise between these states. As there are in general a small fixed number of eigenstates $|\varphi_k\rangle$ that are populated in the algorithm ($\bar{b}_k \neq 0$), Eq. (7.14) shows that there will be a fixed number of I^+_{kl} terms in $\langle p_{\text{err}}\rangle$ while the number of I^-_{kl}, representing the coupling of initially populated states to all others, will in general grow as the dimension N of the Hilbert space. So, the average error probability $\langle p_{\text{err}}\rangle$ will mostly depend on the I^-_{kl} integrals and that is why we now focus on these. Changing the integration variables to $u = t_1 - t_2$ and $v = t_1 + t_2$, we get

$$I^-_{kl} = 2\frac{\sigma^2_{kl}}{\hbar^2}\int_0^T dv \int_0^v du \cos(\omega_{kl}u) f(\omega_0 u), \tag{7.17}$$

that is the integral of a modulated oscillation. For a white noise (7.7), we get by direct integration

$$\begin{aligned} I^-_{kl} &= \frac{\sigma^2_{kl}}{\hbar^2\omega_0}\left[\frac{1-\cos(\omega_{kl}-\omega_0)T}{\omega_{kl}-\omega_0} + T\ \mathrm{Si}(\omega_{kl}-\omega_0)T \right. \\ &\left. -\frac{1-\cos(\omega_{kl}+\omega_0)T}{\omega_{kl}+\omega_0} + T\ \mathrm{Si}(\omega_{kl}+\omega_0)T\right], \end{aligned} \tag{7.18}$$

where Si(x) is the sine integral function

$$\mathrm{Si}(x) = \int_0^x \frac{\sin x' dx'}{x'}. \tag{7.19}$$

Depending on the value of ω_0, we may consider two limiting regimes: for a high cut-off frequency ω_0, we get

$$I^-_{kl} = \frac{\sigma^2_{kl}}{\hbar^2\omega_0^2} O\left(\left(1+\frac{\omega_{kl}}{\omega_0}\right)\omega_0 T\right), \tag{7.20}$$

while for a low cut-off frequency ω_0, we have

$$I^-_{kl} = \frac{\sigma^2_{kl}}{\hbar^2\omega_{kl}^2} O\left(1+\frac{\omega_0}{\omega_{kl}}\right). \tag{7.21}$$

More generally, we obtain similar results for a general function $f(x)$. In the first regime, as usually the autocorrelation function $R(\tau)$ tends to zero as τ increases ($h_{kl}(t+\tau)$ becomes less and less correlated with $h_{kl}(t)$), Eq. (7.20) follows from the approximation $\cos\omega_{kl}u = 1 + O(\omega_{kl}/\omega_0)$ whenever $f(\omega_0 u)$ is not negligible. In the second regime, we must integrate a rapidly oscillating function, as exposed in Appendix A.4. Under very general regularity conditions[2] for $f(x)$, we may use Lemma 5 twice, and finally recover Eq. (7.21). It is interesting to note that in the low frequency case, the coupling integral does not depend on the computation time T. We will see that, at least for the algorithms considered here, this causes a very different behavior for these two regimes, that is, it will determine whether the algorithm is scalable or not.

[2] Let us note that in order to satisfy the hypotheses of Lemma 5, $f(x)$ has to be infinitely differentiable. While this is generally the case for typical noise models such as white noise, $f(x)$ may not be continuous in $x = 0$ for some specific models, such as $f(x) = \exp(-|x|)$ that could follow from a Poissonian process. This discontinuity in the first derivative of $f(x)$ is actually linked to the fact that the spectral density of the noise does not rapidly converge to zero for very high frequencies and therefore that the noise has some probability to vary arbitrarily fast. We will not consider this case in details but only mention that this will yield a drastically different behavior in the regime of low ω_0, i.e. a noise that varies slowly, at least on average.

7.2.2 Analog quantum search

Let us apply this noise theory to Farhi and Gutmann's analog quantum search (exposed in Section 2.4), consisting in the application of the time-independent ideal Hamiltonian $\bar{H}^{\text{an}} = H_0 + H_f$, where[3]

$$\begin{aligned} H_0 &= \bar{E}(I_N - |\psi_0\rangle\langle\psi_0|) && (7.22)\\ H_f &= \bar{E}(I_N - |m\rangle\langle m|), && (7.23)\end{aligned}$$

during a time

$$T^{\text{an}} = \frac{\pi\hbar}{2\bar{E}}\sqrt{N} \tag{7.24}$$

on the initial state

$$|\mathcal{N}\rangle = \frac{1}{\sqrt{N}}\sum_{k=0}^{N-1}|k\rangle. \tag{7.25}$$

In order to study the robustness of this quantum algorithm versus a noise of the type defined in Sec. 7.1, let us first consider the spectrum of the ideal Hamiltonian $\bar{H}^{\text{an}} = H_0 + H_f$ (see Fig. 7.2). Its first two eigenvalues $E_0 = (1-x)\bar{E}$ and $E_1 = (1+x)\bar{E}$, where $x = 1/\sqrt{N}$, are non-degenerate and correspond to the ground and first-excited states,

$$\begin{aligned} |\varphi_0\rangle &= \sqrt{\frac{1+x}{2}}|m\rangle + \frac{x}{\sqrt{2(1+x)}}\sum_{k\neq m}|k\rangle && (7.26)\\ |\varphi_1\rangle &= \sqrt{\frac{1-x}{2}}|m\rangle - \frac{x}{\sqrt{2(1-x)}}\sum_{k\neq m}|k\rangle, && (7.27)\end{aligned}$$

whereas its third eigenvalue $E_k = 2\bar{E}$ is $N-2$ times degenerate.

Developing $|\psi(t=0)\rangle = |\mathcal{N}\rangle$ in the eigenstates $|\varphi_k\rangle$ of the ideal Hamiltonian $\bar{H}$, we get

$$|\psi(0)\rangle = \sqrt{\frac{1+x}{2}}|\varphi_0\rangle - \sqrt{\frac{1-x}{2}}|\varphi_1\rangle \tag{7.28}$$

and thus the instantaneous state of the ideal algorithm $|\bar{\psi}(t)\rangle$ is given by Eq. (7.10) with

$$\begin{aligned} \bar{b}_0 &= \sqrt{\frac{1+x}{2}} && (7.29)\\ \bar{b}_1 &= -\sqrt{\frac{1-x}{2}} && (7.30)\\ \bar{b}_k &= 0 \qquad\qquad k\neq 0,1. && (7.31)\end{aligned}$$

Only two states are populated during the ideal algorithm and as $I^-_{kl} = I^-_{2l} (\forall\ k \neq 0,1)$, the average error probability (7.14) becomes

$$\begin{aligned} \langle p_{\text{err}}\rangle = \varepsilon^2 \{ &(N-2)\left[|\bar{b}_0|^2 I^-_{20} + |\bar{b}_1|^2 I^-_{21}\right]\\ &+|\bar{b}_0|^2|\bar{b}_1|^2(I^-_{00} + I^-_{11}) + (|\bar{b}_0|^4 + |\bar{b}_1|^4)I^-_{01}\\ &-2\text{Re}\left[(\bar{b}^*_0\bar{b}_1)^2 I^+_{01}\right]\}. && (7.32)\end{aligned}$$

[3] We consider the single solution case ($M = 1$).

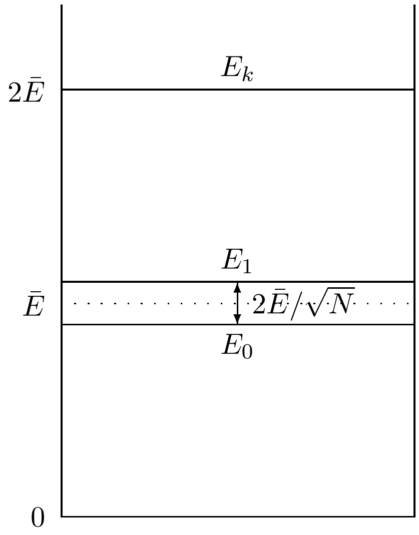

Figure 7.2: Spectrum of the ideal Hamiltonian $\bar{H}^{\text{an}} = H_0 + H_f$ for $N = 100$.

In this case, the bound (7.16) gives $|I^{\pm}_{kl}(t)| \leq \pi^2/8$. Therefore, only the first term of Eq. (7.32) representing the coupling of the ground and first excited states (the only ones initially populated) to the $N-2$ others, could grow with N. Let us focus on this term in the two limiting regimes considered above.

For a high cut-off frequency ω_0, Eq. (7.20) yields

$$I^{-}_{2l} = \frac{\bar{E}}{\hbar\omega_0} O\left(\frac{1}{\sqrt{N}}\left(1 + \frac{\bar{E}}{\hbar\omega_0}\right)\right) \qquad (l = 0, 1) \tag{7.33}$$

which should be of order $1/N$ for $\langle p_{\text{err}} \rangle$ not to grow with N. This imposes the condition $\hbar\omega_0 = \bar{E}\ \Omega(\sqrt{N})$. Therefore, in this regime, the cut-off frequency of the noise must increase as the square root of the size of the database in order to keep an error of constant order, that is $\hbar\omega_0 \gg \bar{E}\sqrt{N}$

In the case of a noise with a low cut-off frequency ω_0, Eq. (7.21) yields

$$I^{-}_{2l} = \frac{1}{N} O\left(1 + \frac{\hbar\omega_0}{\bar{E}}\right) \qquad (l = 0, 1), \tag{7.34}$$

and we conclude that $\langle p_{\text{err}} \rangle$ will not grow with N as long as $\hbar\omega_0 \ll \bar{E}$.

We see that the influence of noise is negligible if it varies either very slowly or very rapidly with respect to $\bar{E}/\hbar$, where $\bar{E}$ is the energy scale of the problem. For the typical case of a white noise, the exact integration (7.18) shows that for intermediate values of the cut-off frequency, $\omega_0 \approx \bar{E}/\hbar$, the noise may grow as $\sqrt{N}$, as displayed in Fig. 7.3. This means that there is a forbidden band for the cut-off frequency if we want to keep our algorithm robust to noise. Moreover, let us mention the possibility to recover the results of Shenvi *et al* [SBW03], even if their noise model was different as they only considered an error in the magnitude of the oracle Hamiltonian modelized as a Markovian stochastic variable with Gaussian distribution. Effectively, we have shown that for a cut-off frequency ω_0 of order $\bar{E}/\hbar$, the error probability

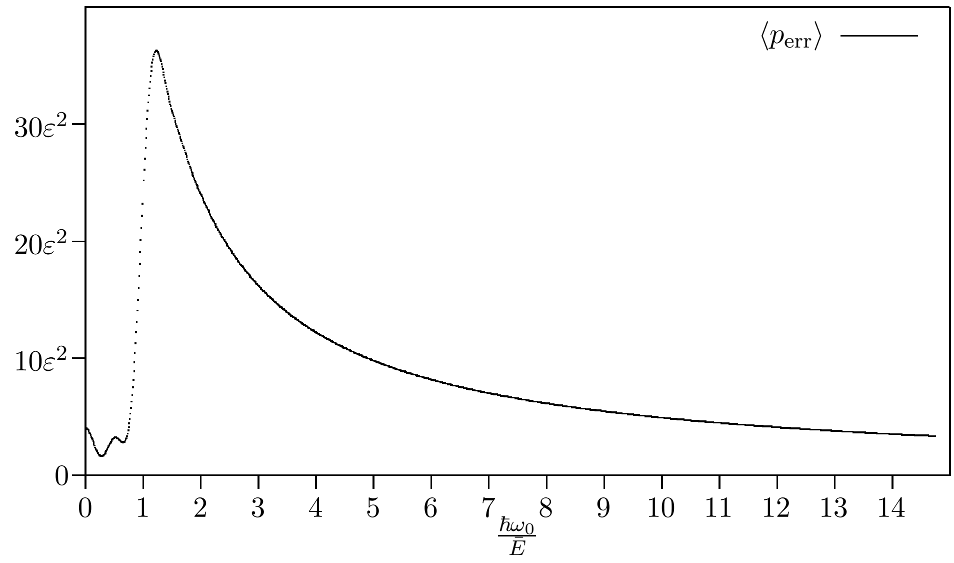

Figure 7.3: Average error probability (to second order) introduced by the noise modelized as in Sec. 7.1 with autocorrelation function $f(x) = \sin x/x$ for the analog search among $N = 100$ elements. We see that the error probability stays low as long as $\hbar\omega_0/\bar{E} \lesssim 1$ where it shows a sudden increase. Afterwards, when $\hbar\omega_0/\bar{E} \gtrsim \sqrt{N}$, it tends progressively back to a low value.

would scale as $\varepsilon^2\sqrt{N}$ for a given signal-to-noise ratio ε. Therefore, in order to keep this error probability constant, ε should scale as $N^{-1/4}$, which coincides with the results of [SBW03].

7.3 Noisy adiabatic evolution

7.3.1 Adiabatic approximation

Let us now study the effect of an additional noisy term $\varepsilon h(t)$ on the slowly time-dependent Hamiltonian $\bar{H}(t)$ of an adiabatic evolution. In Chapter 3, we had shown that by developing the quantum state in the basis formed by the instantaneous eigenstates of the ideal Hamiltonian $\bar{H}(t)$

$$|\bar{\psi}(t)\rangle = \sum_k \bar{b}_k(t) e^{-i\int_0^t \frac{E_k(t_1)}{\hbar}dt_1} |\varphi_k(t)\rangle, \tag{7.35}$$

the ideal Schrödinger evolution led to an implicit solution (3.14):

$$\bar{b}_k(t) = \delta_{0k} + \sum_{l\neq k} \int_0^t dt_1 \bar{b}_l(t_1) e^{i\int_0^{t_1}\omega_{kl}(t_1')dt_1'} \delta\omega_{kl}(t_1) a_{kl}(s(t_1)), \tag{7.36}$$

where the elements $a_{kl}(s)$ are defined in Eq. (3.21) and δ is a “slowness” parameter (see Chapter 3 for details). In the case of a noisy adiabatic evolution, we may still develop the solution of the perturbed Schrödinger equation in the basis formed by the instantaneous eigenstates of $\bar{H}(t)$,

$$|\psi(t)\rangle = \sum_k b_k(t) e^{-i\int_0^t \frac{E_k(t_1)}{\hbar}dt_1} |\varphi_k(t)\rangle \tag{7.37}$$

and, following the lines of the development that led to Eq. (7.36), we find the implicit solution[4]

$$\begin{aligned} b_k(t) &= \delta_{0k} \\ &+\frac{1}{\hbar}\sum_l \int_0^t dt_1 b_l(t_1) e^{i\int_0^{t_1}\omega_{kl}(t_1')dt_1'} \left[\delta\hbar\omega_{kl}(t_1)a_{kl}(s(t_1)) - i\varepsilon h_{kl}(t_1)\right], \end{aligned} \tag{7.38}$$

which is the analogue of Eq. (7.13) for an adiabatic evolution. As for the perturbed time-independent Hamiltonian evolution, we may build a solution as an expansion in successive orders of δ and ε by recursive uses of this implicit solution. At first order, it becomes for $k \neq 0$:

$$\begin{aligned} b_k(t) &= \frac{1}{\hbar}\int_0^t dt_1 e^{i\int_0^{t_1}\omega_{k0}(t_1')dt_1'} \left[\delta\ \hbar\omega_{k0}(t_1)a_{k0}(s(t_1)) - i\varepsilon h_{k0}(t_1)\right] \\ &+O\left((\delta+\varepsilon)^2\right). \end{aligned} \tag{7.39}$$

As before, this first order approximation will be valid if the probability $p(t) = \sum_{k\neq 0}|b_k(t)|^2$ of hopping to an excited state remains small. Let us evaluate the mean of this error probability at the end of the evolution $t = T$ using the same model as above for the perturbation $h(t)$. We have

$$\begin{aligned} \langle p_{\mathrm{err}}\rangle &= \bar{p}_{err} + \frac{\varepsilon^2}{\hbar^2}\sum_{k\neq 0}\iint_0^T dt_1 dt_2 e^{i\int_{t_2}^{t_1}\omega_{k0}(t')dt'} \langle h_{k0}(t_1)h_{k0}(t_2)\rangle \\ &+O\left((\delta+\varepsilon)^3\right), \end{aligned} \tag{7.40}$$

where $\bar{p}_{err} = O(\delta^2)$ is the error probability of the ideal adiabatic evolution. Let us note that $|\varphi_k(t_1)\rangle \neq |\varphi_k(t_2)\rangle$ in general, such that we do not immediately recover the autocorrelation function. However, as the different matrix elements of $h(t)$ are independent in a particular basis, we have:

$$\begin{aligned} \langle h_{k0}(t_1)h_{k0}(t_2)\rangle &= \langle\langle\varphi_k(t_1)|h(t_1)|\varphi_0(t_1)\rangle\langle\varphi_k(t_2)|h(t_2)|\varphi_0(t_2)\rangle\rangle \\ &= (\langle\varphi_k(t_2)|\varphi_k(t_1)\rangle\langle\varphi_0(t_1)|\varphi_0(t_2)\rangle \\ &\quad +\langle\varphi_k(t_2)|\varphi_0(t_1)\rangle\langle\varphi_k(t_1)|\varphi_0(t_2)\rangle) \\ &\quad \sigma_{k0}^2 f(\omega_0(t_1-t_2)). \end{aligned} \tag{7.41}$$

If $|\varphi_k(t)\rangle$ varies sufficiently smoothly for $0 \leq t \leq T$, then the first factor is of order $1 - O((t_1-t_2)^2/T^2)$ such that we may approximate it by 1 as long as $\omega_0 T \gg 1$, that is, the noise varies quickly compared to the adiabatic evolution. In that case, we get for the average error probability

$$\langle p_{\mathrm{err}}\rangle = \bar{p}_{err} + \varepsilon^2\sum_{k\neq 0} I_{k0} + O\left((\delta+\varepsilon)^3\right), \tag{7.42}$$

where the integrals

$$I_{k0} = \frac{\sigma_{k0}^2}{\hbar^2}\iint_0^T dt_1 dt_2 e^{i\int_{t_2}^{t_1}\omega_{k0}(t')dt'} f(\omega_0(t_1-t_2)), \tag{7.43}$$

[4] In that expression, we assume that $a_{kl}(s) = 0$ for $k = l$, as the original definition only applied to $k \neq l$.

represent the coupling of the ground state to the excited states induced by the perturbation. Similarly to the noisy time-independent Hamiltonian evolution, the effect of the perturbation depends on the coupling integrals I_{k0} bounded as

$$|I_{k0}| \leq \frac{\sigma_{k0}^2 T^2}{\hbar^2} \tag{7.44}$$

and that behave as

$$I_{k0} = \frac{\sigma_{k0}^2}{\hbar^2 \omega_0^2} O\left(\left(1 + \frac{\omega_{k0}^{\max}}{\omega_0}\right) \omega_0 T\right) \tag{7.45}$$

and

$$I_{k0} = \frac{\sigma_{k0}^2}{\hbar^2 {\omega_{k0}^{\min}}^2} O\left(1 + \frac{\omega_0}{\omega_{k0}^{\min}}\right) \tag{7.46}$$

in the limiting regimes of very high or very low cut-off frequency ω_0, respectively, where $\omega_{k0}^{\min} \leq \omega_{k0}(t) \leq \omega_{k0}^{\max}$.

7.3.2 Adiabatic quantum search

The quantum search by local adiabatic evolution was exposed in Chapter 4. Its basic principle is to apply the Hamiltonian $H_0 = \bar{E}(I_N - |\psi_0\rangle\langle\psi_0|)$ to a system prepared in its ground state $|\mathcal{N}\rangle$ and then to progressively switch to the Hamiltonian[5] $H_f = \bar{E}(I_N - |m\rangle\langle m|)$ where m is the solution of the search problem in a time of order

$$T^{\mathrm{ad}} = \frac{\pi\hbar}{4\delta\bar{E}}\sqrt{N}. \tag{7.47}$$

The spectrum of the instantaneous Hamiltonian $H^{\mathrm{ad}}(t) = \tilde{H}(s(t))$, where $\tilde{H}(s) = (1-s)H_0 + sH_f$ and $s = s(t)$ is an evolution function that has been optimized such as to reduce the computation time, has been described in the general case of multiple solutions in Chapter 4. For a single solution, this boils down to

$$\tilde{E}_0(s) = \frac{\bar{E}}{2}\left[1 - \sqrt{1 - 4\frac{N-1}{N}s(1-s)}\right] \tag{7.48}$$

$$\tilde{E}_1(s) = \frac{\bar{E}}{2}\left[1 + \sqrt{1 - 4\frac{N-1}{N}s(1-s)}\right] \tag{7.49}$$

$$\tilde{E}_k(s) = \bar{E} \quad k \neq 0, 1 \tag{7.50}$$

as plotted in Fig. 7.4.

Let us now consider that some noise, modelized as described in Section 7.1, perturbs the evolution. Eq. (7.42) then reads

$$\langle p_{\mathrm{err}}\rangle \leq \bar{p}_{err} + \varepsilon^2\left[I_{10} + (N-2)I_{20}\right] + O\left((\delta+\varepsilon)^3\right), \tag{7.51}$$

where $I_{k0} \leq \pi^2/64\delta^2$ as a result of Eq. (7.44). Let us stress that while it was the excitation probability to the first excited state only that was critical for the ideal algorithm according to the adiabatic condition, in this case it is the coupling of the ground state to all excited states

[5] We also consider the single solution case ($M = 1$).

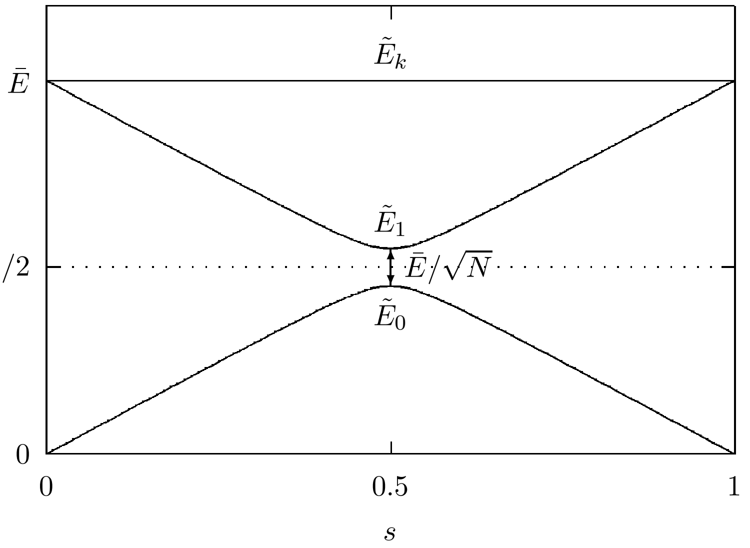

Figure 7.4: Instantaneous eigenvalues of $\tilde{H}(s)$ for $N = 100$.

that could make the algorithm fail, since their number grows as the size of the database N. Moreover, this general bound already suggests that the coupling integrals I_{k0} and therefore the error probability could increase when the evolution slows down (δ decreases), which means there must be a compromise between a slower evolution closer to adiabaticity and a faster evolution more robust to noise.

As before, let us consider the two limiting regimes of a very high or a very low cut-off frequency. In the first case, Eq. (7.45) yields

$$I_{k0} = \frac{\bar{E}}{\hbar\omega_0} O\left(\frac{1}{\delta\sqrt{N}}\left(1 + \frac{\bar{E}}{\hbar\omega_0}\right)\right) \quad (\forall\ k \neq 0), \tag{7.52}$$

exactly as for the analog quantum search, except for the presence of a factor $1/\delta$, which shows that in order to keep the algorithm robust to noise as the size of the database N grows, the cut-off frequency has to increase not only as $\sqrt{N}$ grows, but also as the evolution slows down. Indeed, we see that the average error probability (7.42) will stay of order $O(\delta^2)$ as long as $NI_{20}\varepsilon^2 = O(\delta^2)$, so that

$$\hbar\omega_0 = \bar{E}\ \Omega\left(\frac{\varepsilon^2}{\delta^3}\sqrt{N}\right). \tag{7.53}$$

When the cut-off frequency becomes very low ($\hbar\omega_0 \ll \bar{E}$), Eq. (7.46) implies that the coupling integrals behave as

$$I_{k0} = \frac{1}{N} O\left(1 + \frac{\hbar\omega_0}{\bar{E}}\right) \tag{7.54}$$

for all excited states except the first one (i. e. $k \geq 2$). For the first excited state ($k = 1$), we have $\hbar\omega_{10}^{\min} \sim \bar{E}/\sqrt{N}$ so Eq. (7.46) does not yield a useful result. Instead, we simply use the general bound $I_{k0}^{-} \leq \pi^2/(64\delta^2)$. Therefore, the error probability will remain low as long as $\hbar\omega_0 \ll \bar{E}$ but also at the condition that $\varepsilon = o(\delta)$.

Basically, we recover the same effects as for the analog quantum search, i.e. the influence of noise becomes negligible only in the case of a very high or a very low cut-off frequency, apart from the influence of the slowness parameter δ. Indeed, while decreasing δ gets the ideal evolution closer to adiabaticity and therefore reduces the intrinsic error probability, in the presence of noise it imposes either that the noise amplitude ε is lower (in both regimes of a high or low cut-off frequency) or that the cut-off frequency ω_0 is even larger in that specific regime.

Summary

We have studied the robustness of Hamiltonian-based algorithms to a noise modelized as a Hamiltonian whose elements are stationary Gaussian random processes. We have shown that, apart from the influence of the slowness parameter δ in the case of the adiabatic computation, this robustness is essentially similar for adiabatic and time-independent Hamiltonian algorithms. These algorithms are resistant to noise as long as the cut-off frequency of the noise is either very high or very low, which is in agreement with the numerical study performed by Childs *et al* in [CFP02]. Moreover, even if the noise model is rather different, it also agrees with the results of Shenvi *et al* [SBW03]. The fact that the forbidden band for the cut-off frequency increases towards higher frequencies when N raises causes these algorithms not to be scalable in the regime of a high cut-off frequency. Therefore, in that case, some kind of error correction would be needed when the size of the problem becomes too large.

However, in the case of a low cut-off frequency, the situation is quite different as the error probability stays small as soon as the cut-off frequency is low enough with respect to the energy scale of the problem, even when the size of the problem increases, at least for the case of the Grover search. This fault tolerance may be explained by the fact that the spectral density of noise will not include frequencies close to resonances and thus will not efficiently couple different eigenstates of the ideal Hamiltonian. We have shown that it is not the possible excitation from the ground state to one particular state that can make the algorithm fail but the fact that the dimension of the Hilbert space increases with the size of the problem and therefore the number of states that could be accidentally populated as well. This means, in the case of Adiabatic Computation, that even if the gap between the ground and first excited states decreases, the algorithm will remain robust to a noise with a low cut-off frequency even if this frequency remains constant, as long as the gap between the ground states and the other excited states remain lower bounded. Therefore, the algorithm would be scalable in the case of a low cut-off frequency as long as the amplitude of the ideal Hamiltonian is large enough compared to the frequencies involved in the noise. Of course, here we make the assumption that the signal-to-noise ratio remains essentially constant when the size of the Hilbert space where the computation takes place becomes large, which practically may not be the case. Therefore, even in this regime, it would be interesting to devise error correction techniques for this particular type of algorithm. This is a possible direction for further investigation of Hamiltonian-based quantum algorithms.

Chapter 8

Conclusion

Ten years after the discovery by Peter Shor of an efficient quantum algorithm for factorization, Quantum Computation is still in its infancy. However, it is evolving fast and, regularly, new ideas are found, which may ultimately lead to the realm of quantum computers.

One of these ideas, introduced by Farhi *et al* in 2000 [FGGS00], is to use adiabatic evolution to solve search problems . The basic concept is to prepare the system in the known ground state of a Hamiltonian, and then slowly modify this Hamiltonian to another one whose unknown ground state encodes the solution of the problem that has to be solved. If this switch is performed slowly enough, the Adiabatic Theorem then ensures that the system will end up in a state close to this solution state. More precisely, the evolution rate is essentially limited by the minimal gap between the ground and first excited state, in that the evolution has to slow down when the gap becomes smaller.

While this approach was originally developed aiming at solving NP-complete problems such as the satisfiability of boolean formulas, it may also be adapted to other problems, such as the search in an unstructured database, for which Grover devised a quantum algorithm exhibiting a quadratic speed-up with respect to any classical algorithm. Unfortunately, the adiabatic quantum algorithm as proposed by Farhi *et al* was unable to reproduce this quadratic speed-up. In this thesis, we have demonstrated the possibility to achieve this quadratic speed-up by optimizing the evolution rate of the Hamiltonian constantly over time, following the local variations of the gap and therefore defining a non-linear evolution between the initial and final Hamiltonian.

While Grover's algorithm is expressed in the –more standard– quantum circuit model of computation, this quantum search by adiabatic evolution belongs to a different type of quantum algorithms, where the state of the quantum register evolves continuously over time under the influence of a Hamiltonian. As a matter of fact, Farhi *et al* have introduced another Hamiltonian-based algorithm for Grover's problem, which they called the "analog analogue" of Grover's algorithm. In this thesis, we have shown how to translate these Hamiltonian-based algorithms into circuit-based algorithms, keeping the quadratic speed-up of Grover's algorithm. This is an important result as it proves that viewing these methods as quantum algorithms and their running time as a measure of their complexity was legitimate. This also suggests that the adiabatic approach could be useful even to design new *circuit-based* quantum algorithms. Moreover, we have shown that in the quantum circuit model, these three algorithms become very similar, but nonetheless remain three distinct algorithms. More precisely, the optimization of the evolution rate following the gap turns out to make the state rotate from the uniform superposition to the solution state at a constant angular velocity. It would be worth investigating if such a link between the gap and the rotation of the state in the Hilbert space could be generalized to other problems, such as satisfiability problems for which only a numerical study of the complexity was until now possible as very few analytical results are known.

The optimization of the evolution rate leading to the quadratic speed-up that we obtained here was possible because the evolution of the gap was independent of the solution of the problem. As long as this symmetry property is satisfied, the same idea could be applied to other problems. In particular, we showed that using the adiabatic quantum search as a "subroutine", we could solve structured problems defined in the very generic form of finding an assignment for a set of variables that satisfies a set of constraints. The idea, originally developed by Cerf, Grover and Williams in the context of the standard circuit-based version of Grover's algorithm, consists in nesting partial searches over a limited set of variables into a global search over the whole set of variables. In order to do so, the adiabatic evolution realizing the global search has to be discretized, and the algorithm finally results in a series of steps that alternate partial adiabatic searches backwards and forwards with global search operations. The complexity of this algorithm, although still exponential, then grows with a reduced exponent compared to quantum unstructured search algorithms. An advantage of the adiabatic approach over its circuit-based counterpart is that it does not require some hypotheses on the distribution of the number of solutions and is therefore more general. It could be interesting to study if this property of adiabatic search could be useful for algorithms with multiple levels of nesting.

While we have seen that the quantum algorithms by adiabatic evolution may be translated by discretization to the quantum circuit model and therefore be implemented on a "standard" quantum computer, another approach would be to build another type of quantum computer, that would be specifically designed for such a type of quantum algorithms and therefore would evolve continuously in time, under the influence of a Hamiltonian that depends on the computation. Practically, such a computer would be subject to errors, for instance in the form of perturbations of the ideal Hamiltonian. It seems therefore necessary to study the influence of such a noise on the computation. To our knowledge, this study had only been done to date for some specific algorithms and for some very particular types of noise, and it mostly involved numerical analysis. In this thesis, we have defined a perturbation model based on white noise with high frequency cut-off, following models widely used in various domains of science. This made it possible to derive analytical results, using first order perturbation theory. Our conclusions is that the algorithm will be robust if the cut-off frequency is either very high or very low.

This latter case may easily be understood intuitively as it means that the spectral density of the noise does not include resonating frequencies with the computer Hamiltonian, and therefore will not couple the ground state to excited states. In that regime, the algorithm will therefore be scalable, at least within our hypotheses, the most restrictive being the assumption that the signal-to-noise ratio stays constant when the size of the system increases. Practically, this would probably not be the case and therefore it would be necessary to derive an error correction method.

In the other regime, corresponding to a very large cut-off frequency, the algorithm is not robust anymore as the cut-off frequency has to be larger as the size of the system increases. The main reason is that the algorithm does not fail because of the excitation to the first excited state only, as was the case for an ideal adiabatic evolution, but because of the possible excitation to the exponentially large number of excited states. Even more in this regime, we see that error correction techniques are required to practically use quantum computers based on an adiabatic evolution, as otherwise they would not be scalable. Moreover, it would be interesting to study if our results agree with another typical model of error for quantum computers, namely decoherence.

To conclude, let us emphasize that the Adiabatic Quantum Computation is a young and promising alternative to circuit-based Quantum Computation, and that in parallel with our works, other important results have been developed over the last years, probably the most significant one being the proof that the Adiabatic Quantum Computation is computationally equivalent to the circuit-based Quantum Computation [AvDK+04]. This is of course another, very strong, motivation to try to derive efficient quantum algorithms from an adiabatic approach.

Appendix A

A few useful lemmas

A.1 Error on the unitary operator induced by an erroneous Hamiltonian

In this thesis, we sometimes need to approximate a Hamiltonian $H(t)$ by another close Hamiltonian $H'(t)$. The unitary operator $U'(T)$ induced by the evolution under $H'(T)$ will thus of course exhibit an error with respect to the original unitary operator $U(T)$ induced by $H(T)$. The purpose of the following lemma is to derive an upper bound on this error.

Lemma 1 *Let $H(t)$ and $H'(t)$ be two time-dependent Hamiltonians for $0 \leq t \leq 1$ and let $U(T)$ and $U'(T)$ be the respective unitary operators that they induce. If the difference between the Hamiltonians is limited by $\|H(t) - H'(t)\| \leq e(t)$, then the distance between the induced operators is bounded by*

$$\|U(T) - U'(T)\| \leq \sqrt{\frac{2}{\hbar}\int_0^T e(t)dt}. \tag{A.1}$$

To prove this lemma, let us consider the trajectories $|\psi(t)\rangle$ and $|\psi'(t)\rangle$ induced by $H(t)$ and $H'(t)$ starting from a common initial state $|\psi(0)\rangle = |\psi'(0)\rangle = |\psi_0\rangle$. We have

$$\begin{aligned} \frac{d}{dt}\||\psi(t)\rangle - |\psi'(t)\rangle\|^2 &= \frac{2}{\hbar}\mathrm{Im}\left[\langle\psi(t)|H(t) - H'(t)|\psi'(t)\rangle\right] & \text{(A.2)} \\ &\leq \frac{2}{\hbar}e(t) & \text{(A.3)} \end{aligned}$$

which gives after integration from $t = 0$ to $t = T$, with the initial condition $|\psi(0)\rangle = |\psi'(0)\rangle$,

$$\||\psi(T)\rangle - |\psi'(T)\rangle\|^2 \leq \frac{2}{\hbar}\int_0^T e(t)dt \tag{A.4}$$

or equivalently

$$\|U(T)|\psi_0\rangle - U'(T)|\psi_0\rangle\| \leq \sqrt{\frac{2}{\hbar}\int_0^T e(t)dt}. \tag{A.5}$$

The fact that $|\psi_0\rangle$ is arbitrary concludes the proof.

A.2 Error introduced by successive erroneous unitary operators

The error introduced by the application of a sequence of unitary operators U'_k as an approximation of another sequence U_k may be evaluated by the following lemma:

Lemma 2 *If U_k and U'_k $(k = 1, \ldots, K)$ are unitary operators on some Hilbert space $\mathcal{H}$, then*

$$\left\Vert \prod_{k=1}^{K} U_k - \prod_{k=1}^{K} U'_k \right\Vert \leq \sum_{k=1}^{K} \Vert U_k - U'_k \Vert \tag{A.6}$$

where $\prod_{k=1}^{K} U_k = U_K U_{K-1} \ldots U_2 U_1$.

We prove this lemma by recurrence using at each step the inequality

$$\Vert U_a U_b - U'_a U'_b \Vert \leq \Vert U_a - U'_a \Vert + \Vert U_b - U'_b \Vert \tag{A.7}$$

that is readily derived from

$$U_a U_b - U'_a U'_b = (U_a - U'_a)\frac{U_b + U'_b}{2} + \frac{U_a + U'_a}{2}(U_b - U'_b). \tag{A.8}$$

This inequality immediately shows that the lemma is true for $K = 2$, and that if it is true for $K - 1$, so will it be for K:

$$\begin{aligned} \left\Vert \prod_{k=1}^{K} U_k - \prod_{k=1}^{K} U'_k \right\Vert &\leq \Vert U_K - U'_K \Vert + \left\Vert \prod_{k=1}^{K-1} U_k - \prod_{k=1}^{K-1} U'_k \right\Vert & \text{(A.9)} \\ &\leq \sum_{k=1}^{K} \Vert U_k - U'_k \Vert. & \text{(A.10)} \end{aligned}$$

A.3 Unitary operator differences and error probabilities

In this thesis, we often consider errors in the computation as differences of states or unitary operators, as these are generally easier to evaluate. However, it is clear that physically only the state inner products are relevant. The following lemma allows us to derive a bound on the inner products from the unitary operator differences.

Lemma 3 *Let U and U' be two unitary operators acting on a Hilbert space $\mathcal{H}$ and $|\psi_0\rangle$ be a state in $\mathcal{H}$. If $|\psi\rangle = U|\psi_0\rangle$ and $|\psi'\rangle = U'|\psi_0\rangle$, then*

$$1 - |\langle\psi'|\psi\rangle|^2 \leq \Vert U - U' \Vert^2 \tag{A.11}$$

The proof of this lemma is rather straightforward. As

$$\begin{aligned} \Vert |\psi\rangle - |\psi'\rangle \Vert^2 &= 2(1 - \mathrm{Re}(\langle\psi'|\psi\rangle)) & \text{(A.12)} \\ &\geq 2(1 - |\langle\psi'|\psi\rangle|), & \text{(A.13)} \end{aligned}$$

we have

$$\begin{aligned}1-|\langle\psi'|\psi\rangle|^2 &\le 1-\left(1-\frac{1}{2}\|\!|\,|\psi\rangle-|\psi'\rangle\,\|\!|\right)^2 && \text{(A.14)}\\ &\le \|\!|\,|\psi\rangle-|\psi'\rangle\,\|\!|^2 && \text{(A.15)}\\ &= \|\!|(U-U')|\psi_0\rangle\|\!|^2 && \text{(A.16)}\\ &\le \|\!|U-U'\|\!|^2. && \text{(A.17)}\end{aligned}$$

A.4 Integration of an oscillating function

In this appendix, we give a useful tool to evaluate integrals of an oscillating function such as

$$\int_a^b dxF(x)e^{i\omega x}. \qquad \text{(A.18)}$$

The basic idea relies on Riemann-Lebesgue's lemma:

Lemma 4 (Riemann-Lebesgue) *If $F(x)$ is an integrable function on $[a,b]$, then*

$$\lim_{\omega\to\infty}\int_a^b dxF(x)e^{i\omega x}=0.$$

This lemma suggests that the integral (A.18) will be *relatively small* if ω is *sufficiently large*. The purpose of this appendix is to quantify this idea.

First of all, as long as $F(x)$ is differentiable on $[a,b]$, we may integrate (A.18) by parts:

$$\int_a^b dxF(x)e^{i\omega x}=-\frac{i}{\omega}\left[F(x)e^{i\omega x}\right]_a^b+\frac{i}{\omega}\int_a^b dx\frac{dF}{dx}(x)e^{i\omega x},$$

where $[f(x)]_a^b=f(b)-f(a)$, and, using this last equation iteratively, we show that for an N-time differentiable function $F(x)$ on $[a,b]$,

$$\begin{aligned}\int_a^b dxF(x)e^{i\omega x} &= -\sum_{n=0}^{N-1}\left(\frac{i}{\omega}\right)^{n+1}\left[\frac{d^nF}{dx^n}(x)e^{i\omega x}\right]_a^b\\ &\quad+\left(\frac{i}{\omega}\right)^N\int_a^b dx\frac{d^NF}{dx^N}(x)e^{i\omega x}. && \text{(A.19)}\end{aligned}$$

The order of the error introduced by neglecting the last term may be evaluated as follows:

$$\left|\left(\frac{i}{\omega}\right)^N\int_a^b dx\frac{d^NF}{dx^N}(x)e^{i\omega x}\right|\le\frac{1}{\omega^N}\int_a^b dx\left|\frac{d^NF}{dx^N}(x)\right|. \qquad \text{(A.20)}$$

We see that the accuracy of this approximation increases with the oscillation frequency ω. Moreover, if $(1/\omega^N)d^NF/dx^N\to 0$ for $N\to\infty$, this error approaches zero as N increases and we prove the following lemma:

Lemma 5 *Let the function $F(x)$ be infinitely differentiable on $[a,b]$. If*

$$\frac{1}{\omega^N}\frac{d^N F}{dx^N}(x) \underset{N\to\infty}{\longrightarrow} 0 \quad \forall\ x$$

for some real ω, then

$$\int_a^b dx F(x) e^{i\omega x} = -\sum_{n=0}^{\infty}\left(\frac{i}{\omega}\right)^{n+1}\left[\frac{d^n F}{dx^n}(x)e^{i\omega x}\right]_a^b .$$

While this result is helpful to study a time-independent Hamiltonian evolution, in the case of an adiabatic evolution the typical frequencies become time-dependent. However, using the same method, we easily generalize this lemma to the case of a varying frequency $\omega(x)$.

Lemma 6 *Let the function $F(x)$ be infinitely differentiable on $[a,b]$. If*

$$\frac{1}{\omega(x)^N}\frac{d^N F}{dx^N}(x) \underset{N\to\infty}{\longrightarrow} 0 \quad \forall\ x$$

for some real differentiable function $\omega(x)$ on $[a,b]$, then

$$\begin{aligned}
&\int_a^b dx F(x) e^{i\int_0^x \omega(x')dx'} \\
= &\sum_{n=0}^{\infty}\left\{-\left[\left(\frac{i}{\omega(x)}\right)^{n+1}\frac{d^n F}{dx^n}(x)e^{i\int_0^x \omega(x')dx'}\right]_a^b \right.\\
&\left. + \int_a^b dx \frac{d}{dx}\left(\frac{i}{\omega(x)}\right)^{n+1}\frac{d^n F}{dx^n}(x)e^{i\int_0^x \omega(x')dx'}\right\}.
\end{aligned}$$

Appendix B

Optimal estimation of quantum states from finite ensembles

Introduction

The emerging field of Quantum Information Theory essentially aims at providing a quantitative meaning to the fact that information is physical. In particular, two central questions of this discipline are: "How much information can be encoded in a finite quantum ensemble?" and "What measurements should one use in order to retrieve this information?".

In the context of measurement, a fundamental question, raised by Peres and Wooters [PW91], is whether more can be learned about an ensemble of identically prepared particles by performing a measurement on all the particles together, rather than by performing separate measurements on each particle.

One of the simplest ways to address this question was proposed by Massar and Popescu [MP95], in the form of a game between two players, Alice and Bob. Alice secretly prepares N copies of a quantum state (here a qubit, that is a spin 1/2 particle state) and sends them to Bob. With the only clue that all copies are in the same state, Bob may then perform some measurement to guess this state. The simplest strategy would be to separately measure each copy in some basis. It is then clear that in the limit $N \to \infty$, Bob may estimate the state with arbitrary large precision. However, Massar and Popescu showed that in the case of a finite ensemble, the optimal strategy was a collective measurement on all the copies, in the form of a continuous positive-operator-valued measure (POVM). While this measurement is theoretically optimal, it is unfortunately not physically realizable (it yields an infinite number of possible results). Nevertheless, it was also shown that finite POVM's achieving the same fidelity should exist. Following this, Derka *et al* devised a universal algorithm to build such a finite POVM for all values of N [DBE98]. However, the POVM's they derived were not minimal in the sense that they did not yield a minimal number of outcomes. On the other hand, Latorre *et al* proposed mathematical tools to derive minimal POVM's, but could only achieve it up to $N = 7$ [LPT98].

In this chapter, we show that the problem of finding finite optimal POVM's is actually equivalent to a simply-stated mathematical problem, namely the definition of a Gauss quadrature on the sphere. It allows us to easily derive optimal finite, though not minimal, POVM's for all N. Furthermore, with the help of mathematics literature dealing with the problem of the Gauss quadrature on the sphere, we can give a (close to) minimal solution up to $N = 131$.

B.1 Problem

Let us state the problem more precisely. Alice prepares N copies of a spin 1/2 particle state (or qubit)

$$|\Omega\rangle = \cos\frac{\theta}{2}|\uparrow\rangle + e^{i\phi}\sin\frac{\theta}{2}|\downarrow\rangle, \tag{B.1}$$

pointing in a direction $\Omega = (\theta, \phi)$ she chooses at random with a uniform distribution on the Bloch sphere. She then sends the collective state $|\psi\rangle = |\Omega\rangle^{\otimes N}$ to Bob who has to estimate Ω. If the state he guesses is $|\Omega_g\rangle$, he achieves a score $|\langle\Omega_g|\Omega\rangle|^2$. Bob aims at achieving the best average score

$$S = \frac{1}{4\pi}\int d\Omega \sum_g p(\Omega_g|\Omega)|\langle\Omega_g|\Omega\rangle|^2 \tag{B.2}$$

where $p(\Omega_g|\Omega)$ denotes the conditional probability of Bob to get a measurement outcome Ω_g when Alice sends the state $|\Omega\rangle^{\otimes N}$.

B.2 Continuous POVM

The smallest Hilbert space describing the states $|\Omega\rangle^{\otimes N}$ is the symmetric subspace of the Hilbert space of N qubits, $\mathcal{H}_+^{\otimes N}$ (that is the subspace of maximal total spin $\mathcal{S} = N/2$). As any measurement on $\mathcal{H}_+^{\otimes N}$, the measurement used by Bob is a POVM describable by a set of operators $\{\mathcal{O}_g\}$ satisfying

$$\mathcal{O}_g \geq 0, \tag{B.3}$$

$$\sum_g \mathcal{O}_g = I_+^{\otimes N}, \tag{B.4}$$

where $I_+^{\otimes N}$ denotes the identity on $\mathcal{H}_+^{\otimes N}$.

Now, Massar and Popescu demonstrated that the optimal score that Bob could achieve for a given number of copies N was [MP95]

$$S_N^{\mathrm{opt}} = \frac{N+1}{N+2}. \tag{B.5}$$

Furthermore, they showed that this score was attained by the continuous POVM

$$\mathcal{O}_g = c_{N,g}^2\,[|\Omega_g\rangle\langle\Omega_g|]^{\otimes N} \tag{B.6}$$

where Ω_g takes all possible values on the Bloch sphere and the weights $c_{N,g}^2$ are defined as

$$c_{N,g}^2 = \frac{N+1}{4\pi}d\Omega_g. \tag{B.7}$$

Indeed, as dim $\mathcal{H}_+^{\otimes N} = N+1$, Shur's lemma ensures that the POVM condition (B.4) is satisfied

$$\frac{N+1}{4\pi}\int d\Omega_g\,[|\Omega_g\rangle\langle\Omega_g|]^{\otimes N} = I_+^{\otimes N}, \tag{B.8}$$

and that, in particular,

$$\frac{N+1}{4\pi}\int d\Omega_g|\langle\Omega_g|\Omega\rangle|^{2N} = 1 \tag{B.9}$$

for all Ω. Therefore, using Eq. (B.2), we see that the average score reads

$$\begin{aligned} S &= \frac{1}{4\pi}\int d\Omega \frac{N+1}{4\pi}\int d\Omega_g |\langle\Omega_g|\Omega\rangle|^{2N+2} && \text{(B.10)} \\ &= \frac{1}{4\pi}\int d\Omega \frac{N+1}{N+2} && \text{(B.11)} \\ &= \frac{N+1}{N+2}, && \text{(B.12)} \end{aligned}$$

where we have used Eq. (B.9) with $N' = N+1$ along with the fact that the conditional probability density is given by

$$p(\Omega_g|\Omega) = \frac{N+1}{4\pi}|\langle\Omega_g|\Omega\rangle|^{2N}. \qquad \text{(B.13)}$$

As already stated, such a POVM requires an infinite number of outcomes and is therefore not realizable. It is thus desirable to provide POVM's achieving the score $S_N^{\rm opt}$ and whose number of outcomes is finite.

B.3 Finite POVM

Now observe that any set of n operators $\mathcal{O}_g = c_{N,g}^2 \left[|\Omega_g\rangle\langle\Omega_g|\right]^{\otimes N}$ satisfying the POVM condition (B.4) is optimal. Indeed this condition is equivalent to the equation

$$\sum_{g=1}^{n} c_{N,g}^2 |\langle\Omega_g|\Omega\rangle|^{2N} = 1 \quad \forall\Omega, \qquad \text{(B.14)}$$

or, expanding $\langle\Omega_g|\Omega\rangle$ in terms of spherical harmonics $Y_l^m(\Omega)$ up to $l = N$ (higher-order terms vanish), to the following system

$$\sum_{g=1}^{n} c_{N,g}^2 = N+1 \qquad \text{(B.15a)}$$

$$\sum_{g=1}^{n} c_{N,g}^2 Y_l^m(\Omega_g) = 0, \quad (l = 1,\dots,N; m = -l,\dots,l). \qquad \text{(B.15b)}$$

Thus, that the optimal average score $S_N^{\rm opt}$ is achieved by this finite POVM

$$\begin{aligned} S &= \frac{1}{4\pi}\int d\Omega \sum_{g=1}^{n} c_{N,g}^2 |\langle\Omega_g|\Omega\rangle|^{2N+2} && \text{(B.16)} \\ &= \frac{1}{N+2}\sum_{g=1}^{n} c_{N,g}^2 && \text{(B.17)} \\ &= \frac{N+1}{N+2}. && \text{(B.18)} \end{aligned}$$

The problem now is to construct such a POVM, that is to find n directions Ω_g with weights $c_{N,g}$ satisfying the set of equations (B.15). Ideally, we would like a minimal POVM, that is a solution with a minimal number of elements n. However, trying to solve system (B.15) directly leads to complex non-linear equations, such that Latorre *et al* could only deal with low numbers of copies, up to $N = 7$ [LPT98]. While their solutions were (at least conjectured) minimal, Derka *et al* could devise a –rather complex– algorithm that yields an optimal POVM for arbitrary high N values, but with a non-minimal number of elements $n = (N+1)^2$. In the next section, we show that this problem may actually be restated in a very simple form, that allows to derive quite easily a non-minimal POVM with $n = (N+1)\lceil (N+1)/2 \rceil$ for arbitrary N, as well as minimal solutions for some large N values.

B.4 Gauss quadrature

A Gauss quadrature is a rule designed to approach an integral by a sum and defined by a mesh of points x_r with weights λ_r,

$$\int dx f(x) \approx \sum_r \lambda_r f(x_r). \tag{B.19}$$

If these parameters are chosen so that the quadrature is exact for a set of functions $f_k(x)$

$$\int dx f_k(x) = \sum_r \lambda_r f_k(x_r) \tag{B.20}$$

then the linearity of the integral implies that it will also be exact for every linear combination $f(x) = \sum_k \alpha_k f_k(x)$.

Using the properties of spherical harmonics:

$$\begin{aligned} Y_0^0(\Omega) &= 1/\sqrt{4\pi} && \text{(B.21)} \\ \int d\Omega Y_l^m(\Omega)^\dagger Y_{l'}^{m'}(\Omega) &= \delta_{ll'}\delta_{mm'}, && \text{(B.22)} \end{aligned}$$

the set of equations (B.15) may be rewritten

$$\int d\Omega Y_l^m(\Omega) = \sum_{g=1}^{n} \lambda_g Y_l^m(\Omega_g), \quad (l = 0, \ldots, N; m = -l, \ldots, l) \tag{B.23}$$

with $\lambda_g = 4\pi c_{N,g}^2/(N+1)$, and thus our problem reduces to finding an exact Gauss quadrature on the sphere for the spherical harmonics up to order $l = N$, which is a well-known mathematical problem.

B.4.1 Separation of variables: Gauss-Legendre quadrature

Let us now show that we may easily build such a Gauss quadrature on the sphere. We know that the spherical harmonics may be written:

$$Y_l^m(\Omega) = (-1)^{\frac{1}{2}(m+|m|)} \sqrt{\frac{2l+1}{4\pi}} \sqrt{\frac{(l-|m|)!}{(l+|m|)!}} P_l^{|m|}(\cos\theta) e^{im\phi} \tag{B.24}$$

where

$$P_l^m(u) = (1-u^2)^{\frac{m}{2}} \frac{d^m}{du^m} P_l(u) \tag{B.25}$$

are the associated Legendre functions and

$$P_l(u) = \frac{1}{2^l l!}\frac{d^l}{du^l}(u^2-1)^l \tag{B.26}$$

are the Legendre polynomials. We see that the spherical harmonics are either a product of $e^{im\phi}$ and a polynomial of degree l in $\cos\theta$ (when m is even), or a product of $e^{im\phi}$, $\sin\theta$ and a polynomial of degree $l-1$ in $\cos\theta$ (when m is odd).

Integrating in spherical coordinates, we must find a Gauss quadrature that is exact for:

$$\int d(\cos\theta)d\phi \cos^n\theta e^{im\phi} \tag{B.27}$$

$\forall$ m even ($0 \leq m \leq N$) and n ($0 \leq n \leq N$), and for

$$\int d(\cos\theta)d\phi \sin\theta\cos^n\theta e^{im\phi} \tag{B.28}$$

$\forall$ m odd ($0 \leq m \leq N$) and n ($0 \leq n \leq N-1$).

The simplest (non-minimal) solution is obtained by separating integrations over θ and ϕ and defining an independent Gauss quadrature for each. Let us first consider the integral in ϕ. As m is integer, we have:

$$\int_0^{2\pi} d\phi\ e^{im\phi} = 0\ \forall m \neq 0 \tag{B.29}$$

and

$$\int_0^{2\pi} d\phi\ e^{im\phi} = 2\pi \text{ for } m = 0. \tag{B.30}$$

As m can take integer values up to N, it is easy to see that the minimal Gauss quadrature that will be exact for these $N+1$ integrals will require $n_1 = N+1$ equidistant points, for instance the $(N+1)^{\text{th}}$ roots of unity $\phi_k = k\frac{2\pi}{N+1}$ $(0 \leq k \leq N)$, each with same weight $\frac{2\pi}{N+1}$.

Let us now consider the integral in θ. Equation (B.29) shows that integrals for $m \neq 0$ will cancel out if the quadrature for ϕ is exact such that we must find a quadrature for θ that is only exact for $m = 0$, that is,

$$\int_{-1}^{1} d(\cos\theta)\cos^n\theta = \int_{-1}^{1} dx x^n\ \forall\ 0 \leq n \leq N. \tag{B.31}$$

Now building a Gauss quadrature that is exact for polynomials up to degree N is a well-known and quite simple problem. Indeed, we prove the following theorem [Sze95]:

Theorem 3 *Let $[a,b] \subset \mathbb{R}$, and let $\{p_n\}$ denote a complete set of orthogonal polynomials on $L^2([a,b])$. If $x_1 < \ldots < x_n$ denote the zeros of $\{p_n(x)\}$, there exist real numbers $\lambda_1, \ldots, \lambda_n$ such that*

$$\int_a^b d\alpha(x)\rho(x) = \sum_{i=1}^{n} \lambda_i \rho(x_i), \tag{B.32}$$

whenever $\rho(x)$ is an arbitrary polynomial of degree at most $2n-1$. Moreover, the distribution $d\alpha(x)$ and the integer n uniquely determine these numbers λ_i.

Following this theorem, it is indeed straightforward to build a Gauss quadrature for $\cos\theta$ on $[-1,1]$ using $n_2 = \lceil (N+1)/2 \rceil$ points, that is exact for any polynomial up to degree N. Thus, we finally obtain with this method a POVM with

$$n = n_1 n_2 = (N+1) \left\lceil \frac{N+1}{2} \right\rceil \tag{B.33}$$

elements. As the θ-part of the quadrature is based on Legendre polynomials, this separated variable Gauss quadrature is generally known as Gauss-Legendre quadrature. The corresponding number of POVM elements is shown in Table B.1 as a function of the number of qubits N.

B.4.2 Lebedev quadrature and spherical designs

The method we have described is generic but we have no guarantee that it provides us with a *minimal* optimal POVM. Actually, this is not the case, since we already know that Latorre *et al* have been able to construct optimal finite POVM's with less elements than ours, at least for $N \leq 7$.

One could have expected that the Gauss quadrature we have presented above is not minimal. Heuristically, finding a minimal Gauss quadrature is equivalent to finding n points on a sphere so as to optimally cover it. Intuitively, it is clear that minimality cannot be achieved by considering the two variables θ and ϕ separately, as we did. Actually, defining better quadrature rules proves to be a quite complex mathematical problem as it involves the solving of large non-linear systems. However, this problem has been studied for years such that results that go further than $N = 7$ may be found in the mathematical literature.

More precisely, Lebedev has published a series of articles dealing with this problem [LS92, Leb94, LL99], and could give a quadrature rule on the sphere for all odd values up to $N = 31$, as well as for higher values in the form $N = 6a + 5$ up to $N = 131$ (or $a = 21$). This last sequence requires a number of points

$$n = \frac{(N+1)^2}{3} + 2, \tag{B.34}$$

improving on the Gauss-Legendre (separated variables) quadrature. Moreover, this number of points is believed to be minimal for sufficiently high N. These quadrature rules are used in various fields such as quantum chemistry to evaluate energy levels of molecules [Lai97]. As may be seen on Fig. B.1, Lebedev quadrature rules do not define uniform distributions of points on the sphere, as all the points are not equivalent by symmetry (in particular, the weights are not all equal). Such a uniform distribution on the sphere is actually achievable for some number of points n, and is called a spherical N-design if the Gauss quadrature it defines is exact for all spherical harmonics up to order N:

$$\int d\Omega Y_l^m(\Omega) = \frac{4\pi}{n} \sum_{g=1}^{n} Y_l^m(\Omega_g), \quad (l = 0, \ldots, N; m = -l, \ldots, l). \tag{B.35}$$

Spherical N-designs are known up to $N = 13$ (see Fig. B.2), but unfortunately they require a larger number of points than Lebedev quadrature [HS96]. All these results are summarized in Table B.1.

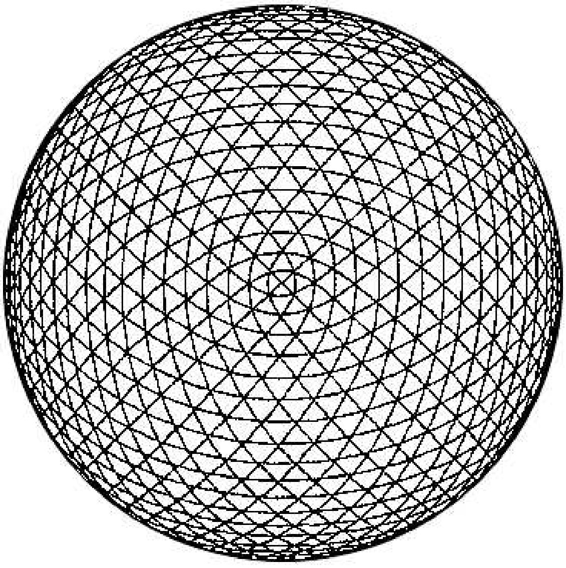

Figure B.1: Distribution of 1800 points for Lebedev quadrature of order $N = 59$ (taken from [Leb94]).

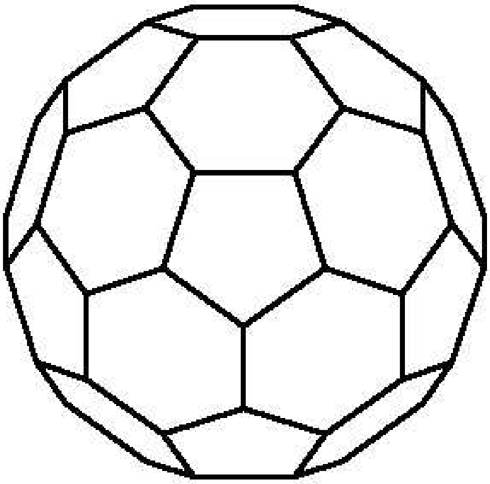

Figure B.2: Spherical design with $n = 60$ points defining a Gauss quadrature on the sphere of order $N = 10$ (the corresponding polyhedron is generally called "Buckminster" or "Bucky" ball, after the architect Buckminster Fuller who used this structure to design domes, and represents the shape of a C_{60} fullerene molecule).

N	Latorre *et al*	Legendre	Lebedev	spherical design
1	2	2		2
2	4	6		4
3	6	8	6	6
4	10	15		12
5	12	18	14	12
6	18	28		24
7	22	32	26	24
8		45		36
9		50	38	48
10		66		60
11		72	50	70
12		91		84
13		98	74	94
14		120		
15		128	86	
⋮		⋮	⋮	
29		450	302	
⋮		⋮		
35		648	434	
⋮		⋮	⋮	
131		8712	5810	
⋮		⋮		

Table B.1: Comparison of the number of elements n of optimal POVM's built using different methods as a function of the number of copies N of the estimated state. The first column corresponds to the minimal solution proposed by Latorre *et al* in [LPT98] up to $N = 7$. In the second column, we see that the separated variable Gauss-Legendre quadrature provides an optimal POVM for arbitrary large N, although the number of elements $N \approx (N+1)^2/2$ is not minimal. The third column corresponds to Lebedev quadrature that reduces the number of elements to $N \approx (N+1)^2/3$ but only exists for some odd values up to $N = 131$. Finally, the spherical designs, that define POVM's with equally weighted elements and are known up to $N = 13$, are given in the last column

B.5 Conclusion

In this Appendix, we have introduced a standard problem of Quantum Information Theory, namely the optimal estimation of an unknown quantum state by a finite measurement of a set of N copies of the state. Although the problem is quite simple to state, it proves to be very complex to solve, even in the simplest case of qubits, and a minimal solution was until now only known for a very small number of copies $N \leq 7$ [LPT98]. However, we showed that this problem may be restated in terms of a well-known mathematical problem, namely the definition of a Gauss quadrature on the sphere. Following this idea, we easily derive a solution for arbitrary large N, that while not minimal, already improves on the best known solution [DBE98]. Moreover, with the help of mathematical literature on Lebedev quadrature [LS92, Leb94, LL99] or spherical designs [HS96], we are able to give better solutions for some large values up to $N = 131$.

Finally, let us mention that as the method we used to recast our problem into a Gauss quadrature is quite generic, we could be able to generalize it to other closely related problems, the most obvious being the estimation of a state in Hilbert spaces of higher dimensions. For instance, the optimal POVM for the estimation of a qutrit (in a 3-dimensional Hilbert space), would reduce to the definition of a Gauss quadrature on a 4-dimensional hypersphere and could therefore probably be solved using the same method. Furthermore, while we have until now only considered the estimation of pure states, the problem could also be generalized to the case of mixed states. In this context, it would be interesting to study if the particular symmetry of spherical designs with respect to other quadrature rules could be of some help.

Appendix C

Bell inequalities resistant to detector inefficiency

Serge Massar, Stefano Pironio, Jérémie Roland and Bernard Gisin

Physical Review A **66**, 05112 (2002)

Introduction

A striking feature of quantum entanglement is non-locality. Indeed, as first shown by Bell in 1964 [Bel64] classical local theories cannot reproduce all the correlations exhibited by entangled quantum systems. This non-local character of entangled states is demonstrated in EPR experiments through the violation of Bell inequalities. However due to experimental imperfections and technological limitations, Bell tests suffer from loopholes which allow, in principle, the experimental data to be reproduced by a local realistic description. The most famous of these loopholes are the locality loophole and the detection loophole. Experiments carried on photons have closed the locality loophole [WJS$^+$98] and recently Rowe et al closed the detection loophole using trapped ions [RKM$^+$01]. But so far, 30 years since the first experiments, both loopholes have not been closed in a *single* experiment.

The purpose of this paper is to study how one can devise new tests of non-locality able to lower the detector efficiency necessary to reject any local realistic hypothesis. This could be a way towards a loophole-free test of Bell inequalities and is important for several reasons. First, as quantum entanglement is the basic ingredient of quantum information processing, it is highly desirable to possess undisputable tests of its properties such as non-locality. Even if one is convinced (as we almost all are) that nature is quantum mechanical, we can imagine practical situations where it would be necessary to perform loophole-free tests of Bell inequalities. For example, suppose you buy a quantum cryptographic device based on Ekert protocol. The security of your cryptographic apparatus relies on the fact that you can violate Bell inequalities with it. But if the detectors efficiencies aren't sufficiently high, the salesman can exploit it and sell to you a classical device that will mimic a quantum device but which will enable him to read all your correspondence [Lar02]. Other reasons to study the resistance of quantum tests to detector inefficiencies are connected to the classification of entanglement. Indeed an important classification of entanglement is related to quantum non-locality. One proposed criterion to gauge how much non-locality is exhibited by the quantum correlations is the resistance to noise. This is what motivated the series of works [KGZ$^+$00, DKZ01] that led to the generalization of the CHSH inequality to higher dimensional systems [CGL$^+$02]. The resistance to inefficient detectors is a second and different criterion that we analyse in this paper. It is closely related to the amount of classical communication required to simulate the quantum correlations [Mas02].

The idea behind the detection loophole is that in the presence of unperfect detectors, local hidden variables can "mask" results in contradiction with quantum mechanics by telling the detectors not to fire. This is at the origin of several local hidden variable models able to reproduce particular quantum correlations if the detector efficiencies are below some threshold value η_* (see [GG99, San92, MP03] for example). In this paper, we introduce two parameters that determine whether a detector will fire or not: η, the efficiency of the detector and λ, the probability that the pair of particles is produced by the source of entangled systems. This last parameter may be important for instance for sources involving parametric down conversion where λ is typically less than 10%. So far, discussions on the detection loophole where concentrating on η, overlooking λ. However we will show below that both quantities play a role in the detection loophole and clarify the relation between these two parameters. In particular we will introduce two different detector thresholds: η_*^λ, the value above which quantum correlations exhibit non-locality for given λ, and $\eta_*^{\forall\lambda}$, the value above which quantum correlations exhibit non-locality for any λ.

We have written a numerical algorithm to determine these two thresholds for given quantum state and quantum measurements. We then searched for optimal measurements such that $\eta_*^{\lambda=1}$ and $\eta_*^{\forall\lambda}$ acquire the lowest possible value. In the case of bipartite two dimensional systems the most important test of non-locality is the CHSH inequality [CHSH69]. Quantum mechanics violates it if the detector efficiency η is above $= 2/(\sqrt{2}+1) \approx 0.8284$ for the maximally entangled state of two qubits. In the limit of large dimensional systems and large number of settings, it is shown in [Mas02] that the efficiency threshold can be arbitrarily lowered. This suggests that the way to devise optimal tests with respect to the resistance to detector inefficiencies is to increase the dimension of the quantum systems and the number of different measurements performed by each party on these systems. (This argument will be presented in more details in [MP03]). We have thus performed numerical searches for increasing dimensions and number of settings starting from the two qubit, two settings situation of the CHSH inequality. Our results concern "multiport beam splitters measurements" [ZZH97] performed on maximally entangled states. They are summarized in Table C.1. Part of these results are accounted for by existing Bell inequalities, the other part led us to introduce new Bell inequalities.

The main conclusions that can be drawn from this work are:

1. Even in dimension 2, one can improve the resistance to inefficient detectors by increasing the number of settings.

2. One can further increase the resistance to detection inefficiencies by increasing the dimension.

3. There are different optimal measurements settings and Bell inequalities for a source that produces entangled particles with high probability ($\lambda \approx 1$) and one that produces them extremely rarely ($\lambda \to 0$). Bell inequalities associated with this last situation provide a detection threshold that doesn't depend on the value of the pair production probability.

d	$N_a \times N_b$	$\eta_*^{\lambda=1}$	$\eta_*^{\forall\lambda}$	p	Bell inequality
2	2×2	0.8284	0.8284	0.2929	CHSH
2	3×3	0.8165		0.2000	Present paper (see also ref [Bel64, Wig70])
2	3×3		0.8217	0.2859	Present paper
2	3×4		0.8216	0.2862	Present paper
2	4×4		0.8214	0.2863	Present paper
3	2×2	0.8209	0.8209	0.3038	Based on Ref.[CGL+02]
3	2×3	0.8182	0.8182	0.2500	Present paper (related to Ref [BPG02])
3	3×3	0.8079		0.2101	Present paper
3	3×3		0.8146	0.2971	Present paper
4	2×2	0.8170	0.8170	0.3095	Based on Ref.[CGL+02]
4	2×3		0.8093	0.2756	Present paper
4	3×3		0.7939	0.2625	Present paper
5	2×2	0.8146	0.8146	0.3128	Based on Ref.[CGL+02]
6	2×2	0.8130	0.8130	0.3151	Based on ref.[CGL+02]
7	2×2	0.8119	0.8119	0.3167	Based on ref.[CGL+02]
∞	2×2	0.8049	0.8049	0.3266	Based on Ref.[CGL+02]

Table C.1: Optimal threshold detector efficiency for varying dimension d and number of settings ($N_a \times N_b$) for the detectors. $\eta_*^{\lambda=1}$ is the threshold efficiency for a source such that the pair production probability $\lambda = 1$ while $\eta_*^{\forall\lambda}$ is the threshold efficiency independent of λ. The column p gives the amount of white noise p that can be added to the entangled state so that it still violates locality (we use for p the same definition as that given in Refs. [KGZ+00, DKZ01]). The last column refers to the Bell inequality that reproduce the detection threshold. Except for the case $d = \infty$, these thresholds are the result of a numerical optimization carried over the et of multiport beam-splitter measurements.

4. For the measurement scenarios numerically accessible, only small improvements in threshold detector efficiency are achieved. For instance the maximum change in threshold detector efficiency we found is approximatively 4%

The paper is organized as follows: First, we review briefly the principle of an EPR experiment in section C.1.1 and under which condition such an experiment admits a local-realistic description in section C.1.2. In section C.1.3 we clarify the role played by η and λ in the detection loophole. We then present the technique we used to perform the numerical searches in C.1.4 and to construct the new Bell inequalities presented in this paper in C.1.5. Section C.2 contains our results. In particular in C.2.1 we generalize the family of inequalities introduced in [CGL$^+$02] to take into account detection inefficiencies and in C.2.3 we present the two different Bell inequalities associated to the two-dimensional three by three settings measurement scenario. In the Appendix, we collect all the measurement settings and Bell inequalities we have obtained.

C.1 General Formalism

C.1.1 Quantum correlations

Let us review the principle of an a EPR experiment: two parties, Alice and Bob, share an entangled state ρ_{AB}. We take each particle to belong to a d dimensional Hilbert space. The parties carry out measurements on their particles. Alice can choose between N_a different von Neumann measurements A_i $(i = 1, \dots, N_a)$ and Bob can choose between N_b von Neumann measurements B_j $(j = 1, \dots, N_b)$. Let k and l be Alice's and Bob's outcomes. We suppose that the number of possible outcomes is the same for each party and that the values of k and l belong to $\{0, \dots, d-1\}$. To each measurement A_i is thus associated a complete set of d orthogonal projectors $A_i^k = |A_i^k\rangle\langle A_i^k|$ and similarly for B_j. Quantum mechanics predicts the following probabilities for the outcomes

$$\begin{aligned} P_{kl}^{QM}(A_i, B_j) &= \mathrm{Tr}((A_i^k \otimes B_j^l)\rho_{ab}) \ , \\ P_l^{QM}(B_j) &= \mathrm{Tr}((\mathbb{1}_A \otimes B_j^l)\rho_{ab}) \ , \\ P_k^{QM}(A_i) &= \mathrm{Tr}((A_i^k \otimes \mathbb{1}_B)\rho_{ab}) \ . \end{aligned} \tag{C.1}$$

In a real experiment, it can happen that the measurement gives no outcome, due to detector inefficiencies, losses or because the pair of entangled states has not been produced. To take into account these cases in the most general way, we enlarge the space of possible outcomes and add a new outcome, the "no-result outcome", which we label $\emptyset$. Quantum mechanics now predicts a modified set of correlations:

$$\begin{aligned} P_{\lambda\eta}^{QM}(A_i = k, B_j = l) &= \lambda\eta^2 P_{kl}^{QM}(A_i, B_j) \quad k, l \neq \emptyset \ , \\ P_{\lambda\eta}^{QM}(A_i = \emptyset, B_j = l) &= \lambda\eta(1-\eta) P_l^{QM}(B_j) \quad l \neq \emptyset \ , \\ P_{\lambda\eta}^{QM}(A_i = k, B_j = \emptyset) &= \lambda\eta(1-\eta) P_k^{QM}(A_i) \quad k \neq \emptyset \ , \\ P_{\lambda\eta}^{QM}(A_i = \emptyset, B_j = \emptyset) &= 1 - \lambda + \lambda(1-\eta)^2 \ . \end{aligned} \tag{C.2}$$

where η is the detector efficiency, and λ is the probability that a pair of particles is produced by the source of entangled systems. By detection efficiency η we mean the probability that the detector gives a result if a particle was produced, i.e. η includes not only the "true" efficiency of the detector but also all possible losses of the particle on the path from the source to the detectors.

C.1.2 Local Hidden Variable Theories & Bell Inequalities

Let us now define when the results (C.2) of an EPR experiment can be explained by a local hidden variable (lhv) theory. In a lhv theory, the outcome of Alice's measurement is determined by the setting A_i of Alice's measurement apparatus and by a random variable shared by both particles. This result should not depend on the setting of Bob's measurement apparatus if the measurements are carried out at spatially separated locations. The situation is similar for Bob's outcome. We can describe without loss of generality such a local variable theory by a set of $(d{+}1)^{N_a+N_b}$ probabilities $p_{K_1\ldots K_{N_a}L_1\ldots L_{N_b}}$ where Alice's local variables $K_i \in \{0,\ldots,d{-}1,\emptyset\}$ specifies the result of measurement A_i and Bob's variables $L_j \in \{0,\ldots,d{-}1,\emptyset\}$ specify the result of measurement B_j. The correlations $P(A_i = K, B_k = L)$ are obtained from these joint probabilities as marginals. The quantum predictions can then be reproduced by a lhv theory if and only if the following $N_aN_b(d+1)^2$ equations are obeyed:

$$\sum_{\mathbf{KL}} p_{\mathbf{KL}}\delta_{K_i,K}\delta_{L_j,L} \;=\; P^{QM}_{\lambda\eta}(A_i = K, B_j = L) \tag{C.3}$$

with the conditions:

$$\sum_{\mathbf{KL}} p_{\mathbf{KL}} \;=\; 1\ , \tag{C.4}$$

$$p_{\mathbf{KL}} \;\geq\; 0\ , \tag{C.5}$$

where we have introduced the notation $\mathbf{K} = K_1\ldots K_{N_a}$ and $\mathbf{L} = L_1\ldots L_{N_b}$. Note that the equations (C.3) are not all independent since quantum and classical probabilities share additional constraints such as the normalization conditions:

$$\sum_{K,L} P(A_i = K, B_j = L) = 1 \tag{C.6}$$

or the no-signaling conditions:

$$P(A_i = K) = \sum_{L} P(A_i = K, B_j = L) \quad \forall\ j \tag{C.7}$$

and similarly for B_j.

An essential result is that the necessary and sufficient conditions for a given probability distribution P^{QM} to be reproducible by a lhv theory can be expressed, alternatively to the equations (C.3), as a set of linear inequalities for P^{QM}, the Bell inequalities. They can be written as

$$I = I_{rr} + I_{\emptyset r} + I_{r\emptyset} + I_{\emptyset\emptyset} \leq c \tag{C.8}$$

where

$$\begin{aligned}
I_{rr} &= \sum_{i,j}\sum_{k,l\neq\emptyset} c_{ij}^{kl} P(A_i = k, B_j = l) \\
I_{\emptyset r} &= \sum_{i,j}\sum_{l\neq\emptyset} c_{ij}^{\emptyset l} P(A_i = \emptyset, B_j = l) \\
I_{r\emptyset} &= \sum_{i,j}\sum_{k\neq\emptyset} c_{ij}^{k\emptyset} P(A_i = k, B_j = \emptyset) \\
I_{\emptyset\emptyset} &= \sum_{i,j} c_{ij}^{\emptyset\emptyset} P(A_i = \emptyset, B_j = \emptyset).
\end{aligned} \tag{C.9}$$

For certain values of η and λ, quantum mechanics can violate one of the Bell inequalities (C.8) of the set. Such a violation is the signal for experimental demonstration of quantum non-locality.

C.1.3 Detector efficiency & pair production probability

For a given quantum mechanical probability distribution P^{QM} and given pair production probability λ, the maximum value of the detector efficiency η for which there exists a lhv variable model will be denoted $\eta_*^{\lambda}(P^{QM})$. It has been argued [GG99, Gis] that η_* should not depend on λ. The idea behind this argument is that the outcomes $(\emptyset, \emptyset)$ obtained when the pair of particles is not created are trivial and hence it seems safe to discard them. A more practical reason, is that the pair production rate is rarely measurable in experiments. Whatever, the logical possibility exists that the lhv theory can exploit the pair production rate. Indeed, we will show below that this is the case when the number of settings of the measurement apparatus is larger than 2. This motivates our definition of threshold detection efficiency valid for all values of λ

$$\eta_*^{\forall\lambda} = \max_{\lambda\neq 0}(\eta_*^{\lambda}) = \lim_{\lambda\to 0} \eta_*^{\lambda} \tag{C.10}$$

The second equality follows from the fact that if a lhv model exists for a given value of λ it also exists for a lower value of λ.

Let us study now the structure of the Bell expression $I(QM)$ given by quantum mechanics. This will allow us to derive an expression for $\eta_*^{\forall\lambda}$. Inserting the quantum probabilities (C.2) into the Bell expression of Eq. (C.8) we obtain

$$\begin{aligned}
I(QM) = \lambda\eta^2 I_{rr}(QM) + \lambda\eta(1-\eta) I_{\emptyset r}(QM) \\
+ \lambda\eta(1-\eta) I_{r\emptyset}(QM) + (1 + \lambda(\eta^2 - 2\eta)) \sum_{i,j} c_{ij}^{\emptyset\emptyset}
\end{aligned} \tag{C.11}$$

where I_{rr}^{QM} is obtained by replacing $P(A_i = k, B_j = l)$ with $P_{kl}^{QM}(A_i, B_j)$ in I_{rr} and $I_{\emptyset r}^{QM}$ by replacing $P(A_i = \emptyset, B_j = l)$ with $P_l^{QM}(B_j)$ in $I_{\emptyset r}$ and similarly for $I_{r\emptyset}^{QM}$.

For $\eta = 0$, we know there exists a trivial lhv model and so the Bell inequalities cannot be violated. Replacing η by 0 in (C.11) we therefore deduce that

$$\sum_{i,j} c_{ij}^{\emptyset\emptyset} \leq c. \tag{C.12}$$

This divides the set of Bell inequalities into two groups: those such that $\sum_{i,j} c_{ij}^{\emptyset\emptyset} < c$ and those for which $\sum_{i,j} c_{ij}^{\emptyset\emptyset} = c$. Let us consider the first group. For small λ, these inequalities will cease to be violated. Indeed, take $\eta = 1$ (which is the maximum possible value of the detector efficiency), then (C.11) reads

$$I(QM) = \lambda I_{rr}^{QM} + (1-\lambda)\sum_{i,j} c_{ij}^{\emptyset\emptyset}. \tag{C.13}$$

The condition for violation of the Bell inequality is $I(QM) > c$. But since $\sum_{i,j} c_{ij}^{\emptyset\emptyset} < c$, for sufficiently small λ we will have $I(QM) < c$ and the inequality will not be violated. These inequalities can therefore not be used to derive threshold $\eta_*^{\forall\lambda}$ that do not depend on λ, but they are still interesting and will provide a threshold η_*^{λ} depending on λ. Let us now consider the inequalities such that $\sum_{i,j} c_{ij}^{\emptyset\emptyset} = c$. Then λ cancels in (C.11) and the condition for violation of the Bell inequality is that η must be greater than

$$\eta_*^{\forall\lambda}(P^{QM}) = \frac{2c - I_{\emptyset r}^{QM} - I_{r\emptyset}^{QM}}{c + I_{rr}^{QM} - I_{\emptyset r}^{QM} - I_{r\emptyset}^{QM}}. \tag{C.14}$$

It is interesting to note that if quantum mechanics violates a Bell inequality for perfect sources $\lambda = 1$ and perfect detectors $\eta = 1$, then there exists a Bell inequality that will be violated for $\eta < 1$ and $\lambda \to 0$. That is there necessarily exists a Bell inequality that is insensitive to the pair production probability. Indeed the violation of a Bell inequality in the case $\lambda = 1$, $\eta = 1$ implies that there exists a Bell expression I_{rr} such that $I_{rr}(QM) > c$ with c the maximum value of I_{rr} allowed by lhv theories. Then let us build the following inequality

$$I = I_{rr} + I_{r\emptyset} + I_{\emptyset r} + \sum_{i,j} c_{ij}^{\emptyset\emptyset} P(A_i = \emptyset, B_j = \emptyset) \leq c \tag{C.15}$$

where $\sum_{i,j} c_{ij}^{\emptyset\emptyset} = c$ and we take in $I_{r\emptyset}$ and $I_{\emptyset r}$ sufficiently negative terms to insure that $I \leq c$. For this inequality, $\eta_*^{\forall\lambda} = (2c - I_{\emptyset r}^{QM} - I_{r\emptyset}^{QM})/(c + I_{rr}^{QM} - I_{\emptyset r}^{QM} - I_{r\emptyset}^{QM}) < 1$, which shows that Bell inequalities valid $\forall\lambda$ always exist. One can, in principle, optimize this inequality by taking $I_{r\emptyset}$ and $I_{\emptyset r}$ as large as possible while ensuring that (C.15) is obeyed.

From the experimentalist's point of view, Bell tests involving inequalities that depend on λ need all events to be taken into account, including $(\emptyset, \emptyset)$ outcomes, while in tests involving inequalities insensitive to the pair production probability, it is sufficient to take into account events where at least one of the parties produces a result, i.e. double non-detection events $(\emptyset, \emptyset)$ can be discarded. Indeed, first note that one can always use the normalization conditions (C.6) to rewrite a Bell inequality such as (C.8) in a form where the term $I_{\emptyset\emptyset}$ does not appear. Second, if the events $(\emptyset, \emptyset)$ are not recorded in an experiment, the measured probabilities are relative frequencies computed on the set of all events involving at least one result on one side. The probabilities measured in such experiments can be obtained from the probabilities (C.2) by replacing λ with $\lambda' = \lambda/(1-(1-\eta)^2)$. While this rescaling of λ is legitimate for inequalities that do not depend on the value of λ, it is however incorrect to perform it for inequalities depending of λ, in particular this will affect the detection threshold.

C.1.4 Numerical search

We have carried numerical searches to find measurements such that the thresholds $\eta_*^{\lambda=1}$ and $\eta_*^{\forall\lambda}$ acquire the lowest possible value. This search is carried out in two steps. First of all, for given quantum mechanical probabilities, we have determined the maximum value of η for which there exists a local hidden variable theory. Second we have searched over the possible measurements to find the minimum values of η_*.

In order to carry out the first step, we have used the fact that the question of whether there are classical joint probabilities that satisfy (C.3) with the conditions (C.4,C.5) is a typical linear optimization problem for which there exist efficient algorithms [ZKBL99]. We have written a program which, given λ, η and a set of quantum measurements, determines whether (C.3) admits a solution or not. η_*^λ is then determined by performing a dichotomic search on the maximal value of η so that the set of constraints is satisfied.

However when searching for $\eta_*^{\forall\lambda}$ it is possible to dispense with the dichotomic search by using the following trick. First of all because all the equations in Eq. (C.3) are not independent, we can remove the constraints which involve on the right hand side the probabilities $P(A_i = \emptyset, B_j = \emptyset)$. Second we define rescaled variables $\lambda(1-(1-\eta)^2)\tilde{p}_{\mathbf{KL}} = p_{\mathbf{KL}}$. Inserting the quantum probabilities Eq. (C.2) we obtain the set of equations

$$\begin{aligned}
\sum_{\mathbf{KL}} \tilde{p}_{\mathbf{KL}} \delta_{K_i,k}\delta_{L_j,l} &= \alpha P^{QM}_{kl}(A_i, B_j) \quad k,l \neq \emptyset \\
\sum_{\mathbf{KL}} \tilde{p}_{\mathbf{KL}} \delta_{K_i,\emptyset}\delta_{L_j,l} &= (1-\frac{\alpha}{2}) P^{QM}_{l}(B_j) \quad l \neq \emptyset \\
\sum_{\mathbf{KL}} \tilde{p}_{\mathbf{KL}} \delta_{K_i,k}\delta_{L_j,\emptyset} &= (1-\frac{\alpha}{2}) P^{QM}_{k}(A_i) \quad k \neq \emptyset
\end{aligned} \tag{C.16}$$

with the normalization

$$\sum_{\mathbf{KL}} \tilde{p}_{\mathbf{KL}} = \frac{1}{\lambda}\frac{1}{1-(1-\eta)^2} \tag{C.17}$$

where $\alpha = \eta^2/(1-(1-\eta)^2)$. Note that λ only appears in the last equation. We want to find the maximum α such that these equations are obeyed for all λ. Since $0 < \lambda \leq 1$ [1], we can replace the last equation by the condition

$$\sum_{\mathbf{KL}} \tilde{p}_{\mathbf{KL}} \geq 1. \tag{C.18}$$

We thus are led to search for the maximum α such that Eqs. (C.16) are satisfied and that the $\tilde{p}_{\mathbf{KL}}$ are positive and obey condition (C.18). In this form the search for $\eta_*^{\forall\lambda}$ has become a linear optimization problem and can be efficiently solved numerically.

Given the two algorithms that compute $\eta_*^{\lambda=1}$ and $\eta_*^{\forall\lambda}$ for given settings, the last part of the program is to find the optimal measurements. In our search over the space of quantum strategies we first considered the maximally entangled state $\Psi = \sum_{m=0}^{d-1} |m\rangle_a |m\rangle_b$ in dimension d. The possible measurements A_i and B_j we considered are the "multiport beam splitters" measurements described in [ZZH97] and which have in previous numerical searches yielded highly non local quantum correlations [KGZ$^+$00, DKZ01]. These measurements are parameterized by d phases $(\phi^1_{A_i}, \dots \phi^d_{A_i})$ and $(\phi^1_{B_j}, \dots \phi^d_{B_j})$ and involve the following steps:

[1] Actually (C.18) corresponds to $0 < \lambda \leq \frac{1}{1-(1-\eta)^2}$ so that λ can be greater than 1. But as stated earlier, if a lhv model exists for a given value of λ it is trivial to extend it to a lhv model for a lower value of λ. The maximum of η_*^λ over the set $\lambda \in]0, 1/(1-(1-\eta)^2)]$ will thus be equal to the maximum over the set $\lambda \in]0,1]$.

first each party acts with the phase $\phi_{A_i}(m)$ or $\phi_{B_j}(m)$ on the state $|m\rangle$, they then both carry out a discrete Fourier transform. This brings the state Ψ to:

$$\Psi = \frac{1}{d^{3/2}} \sum_{k,l,m=0}^{d-1} \exp\left[i\Big(\phi_{A_i}(m) - \phi_{B_j}(m) + \frac{2\pi}{d} m(k-l) \Big) \right] |k\rangle_a |l\rangle_b \tag{C.19}$$

Alice then measures $|k\rangle_a$ and Bob $|l\rangle_b$. The quantum probabilities (C.1) thus take the form

$$\begin{aligned} P_{kl}^{QM}(A_i, B_j) &= \frac{1}{d^3} | \sum_{m=0}^{d-1} \exp\Big[i\Big(\phi_{A_i}(m) - \phi_{B_j}(m) + \frac{2\pi m}{d}(k-l) \Big) \Big] |^2 \\ P_k^{QM}(A_i) &= 1/d \\ P_l^{QM}(B_j) &= 1/d \end{aligned} \tag{C.20}$$

The search for minimal $\eta_*^{\lambda=1}$ and $\eta_*^{\forall\lambda}$ then reduces to a non-linear optimization problem over Alice's and Bob's phases. For this, we used the "amoeba" search procedure with its starting point fixed by the result of a randomized search algorithm. The amoeba procedure [NM65] finds the extremum of a non-linear function F of N variables by constructing a simplex of $N+1$ vertices. At each iteration, the method evaluates F at one or more trial point. The purpose of each iteration is to create a new simplex in which the previous worst vertex has been replaced. The simplex is altered by reflection, expansion or contraction, depending on whether F is improving. This is repeated until the diameter of the simplex is less than the specified tolerance.

Note that these searches are time-consuming. Indeed, the first part of the computation, the solution to the linear problem, involves the optimization of $(d+1)^{N_a+N_b}$ parameters, the classical probabilities $p_{\mathbf{KL}}$ (the situation is even worse for η_*^{λ}, since the linear problem has to be solved several times while performing a dichotomic search for η_*^{λ}). Then when searching for the optimal measurements, the first part of the algorithm has to be performed for each phase settings. This results in a rapid exponential growth of the time needed to solve the entire problem with the dimension and the number of settings involved. A second factor that complicates the search for optimal measurements is that, due to the relatively large number of parameters that the algorithm has to optimize, it can fail to find the global minimum and converge to a local minimum. This is one of the reasons why we restricted our searches to multiport beam-splitter measurements, since the number of parameters needed to describe them is much lesser than that for general Von Neumann measurements.

Our results for setups our computers could handle in reasonable time are summarized in Table C.1. In dimension 2, we also performed more general searches using von Neumann measurements but the results we obtained where the same as for the multiport beam-splitters described above

C.1.5 Optimal Bell inequalities

Upon finding the optimal quantum measurements and the corresponding values of η_*, we have tried to find the Bell inequalities which yield these threshold detector efficiencies. This is essential to confirm analytically these numerical results but also in order for them to have practical significance, ie. to be possible to implement them in an experiment.

To find these inequalities, we have used the approach developed in [CGL$^+$02]. The first idea of this approach is to make use of the symmetries of the quantum probabilities and to search for Bell inequalities which have the same symmetry. Thus for instance if $P(A_i = k, B_j = l) = P(A_i = k+m \mod d, B_j = l+m \mod d)$ for all $m \in \{0,\dots,d-1\}$, then it is useful to introduce the probabilities

$$\begin{aligned} P(A_i = B_j + n) &= \sum_{m=0}^{d-1} P(A_i = m, B_j = n+m \mod d) \\ P(A_i \neq B_j + n) &= \sum_{\substack{m=0 \\ l\neq n}}^{d-1} P(A_i = m, B_j = l+m \mod d) \end{aligned} \tag{C.21}$$

and to search for Bell inequalities written as linear combinations of the $P(A_i = B_j + n)$. This reduces considerably the number of Bell inequalities among which one must search in order to find the optimal one. The second idea is to search for the logical contradictions which force the Bell inequality to take a small value in the case of lhv theories. Thus the Bell inequality will contain terms with different weights, positive and negative, but the lhv theory cannot satisfy all the relations with the large positive weights. Once we had identified a candidate Bell inequality, we ran a computer program that enumerated all the deterministic classical strategies and computed the maximum value of the Bell inequality. The deterministic classical strategies are those for which the probabilities $p_{K_1\dots K_{N_a}L_1\dots L_{N_b}}$ are equal either to 0 or to 1. In order to find the maximum classical value of a Bell expression, it suffices to consider them since the other strategies are obtained as convex combinations of the deterministic ones.

However when the number of settings, N_a and N_b, and the dimensionality d increase, it becomes more and more difficult to find the optimal Bell inequalities using the above analytical approach. We therefore developed an alternative method based on the numerical algorithm which is used to find the threshold detection efficiency.

The idea of this numerical approach is based on the fact that the probabilities for which there exists a solution $p_{\mathbf{KL}}$ to Eqs. (C.3,C.4,C.5) form a convex polytope whose vertices are the deterministic strategies. The facets of this polytope are hyperplanes of dimension $D-1$ where D is the dimension of the space in which lies the polytope (D is lower than the dimension $(d+1)^{N_a+N_b}$ of the total space of probabilities due to constraints such as the normalizations conditions (C.4) and the no-signaling conditions (C.7)). These hyperplanes of dimension $D-1$ correspond to Bell inequalities.

At the threshold η_*, the quantum probability $P^{QM}_{\lambda\eta_*}$ belongs to the boundary, i.e to one of the faces, of the polytope determined by Eqs (C.3,C.4,C.5). The solution $p^*_{\mathbf{KL}}$ to these equations at the threshold is computed by our algorithm and it corresponds to the convex combinations of deterministic strategies that reproduce the quantum correlations. From this solution it is then possible to construct a Bell inequality. Indeed, the face F to which $P^{QM}_{\lambda\eta_*}$ belongs is the plane passing through the deterministic strategies involved in the convex combination $p^*_{\mathbf{KL}}$. Either, this face F is a facet, i.e. an hyperplane of dimension $D-1$, or F is of dimension lower than $D-1$. In the first case, the hyperplane F correspond to the Bell inequality we are looking. In the second case, there is an infinity of hyperplanes of dimension $D-1$ passing by F, indeed every vector $\vec{v}$ belonging to the space orthogonal to the face F determines such an hyperplane. To select one of these hyperplanes lying outside the polytope, and thus corresponding effectively to a Bell inequality, we took as vector $\vec{v}$ the component normal to F of the vector which connects the center of the polytope and the quantum probabilities when $\eta = 1$: $P^{QM}_{\lambda\eta=1}$. Though this choice of $\vec{v}$ is arbitrary, it yields Bell inequalities which preserve the symmetry of the probabilities P^{QM}.

As in the analytical method given above, we have verified by enumeration of the deterministic strategies that this hyperplane is indeed a Bell inequality (ie. that it lies on one side of the polytope) and that it yields the threshold detection efficiency η_*.

C.2 Results

Our results are summarized in Table C.1. We now describe them in more detail.

C.2.1 Arbitrary dimension, two settings on each side ($N_a = N_b = 2$).

For dimensions up to 7, we found numerically that $\eta_*^{\lambda=1} = \eta_*^{\forall\lambda}$. The optimal measurements we found are identical to those maximizing the generalization of the CHSH inequality to higher dimensional systems [CGL$^+$02], thus confirming their optimality not only for the resistance to noise but also for the resistance to inefficient detectors. Our values of η_* are identical to those given in [DKZ01] where $\eta_*^{\lambda=1}$ has been calculated for these particular settings for $2 \leq d \leq 16$.

We now derive a Bell inequality that reproduces analytically these numerical results (which has also been derived by N. Gisin [Gis]). Our Bell inequality is based on the generalization of the CHSH inequality obtained in [CGL$^+$02]. We recall the form of the Bell expression used in this inequality:

$$\begin{aligned} I_{rr}^{d,2\times 2} = \sum_{k=0}^{[d/2]-1} \left(1 - \frac{2k}{d-1}\right) \Big(& [P(A_1 = B_1 + k) \\ & + P(B_1 = A_2 + k + 1) + P(A_2 = B_2 + k) \\ & + P(B_2 = A_1 + k)] - [P(A_1 = B_1 - k - 1) \\ & + P(B_1 = A_2 - k) + P(A_2 = B_2 - k - 1) \\ & + P(B_2 = A_1 - k - 1)]\Big). \end{aligned} \tag{C.22}$$

For local theories, $I_{rr}^{d,2\times 2} \leq 2$ as shown in [CGL$^+$02] where the value of $I_{rr}^{d,2\times 2}(QM)$ given by the optimal quantum measurements is also described. In order to take into account "no-result" outcomes we introduce the following inequalities:

$$I^{d,2\times 2} = I_{rr}^{d,2\times 2} + \frac{1}{2} \sum_{i,j} P(A_i = \emptyset, B_j = \emptyset) \leq 2 \tag{C.23}$$

Let us prove that the maximal allowed value of $I^{d,2\times 2}$ for local theories is 2. To this end it suffices to enumerate all the deterministic strategies. First, if all the local variables correspond to a "result" outcome then $I_{rr}^{d,2\times 2} \leq 2$ and $I_{\emptyset\emptyset}^{d,2\times 2} = \frac{1}{2}\sum_{i,j} P(A_i = \emptyset, B_j = \emptyset) = 0$ so that $I^{d,2\times 2} \leq 2$; if one of the local variables is equal to $\emptyset$ then again $I_{rr}^{d,2\times 2} \leq 2$ (since the maximal weight of a probability in $I_{rr}^{d,2\times 2}$ is one and they are only two such probabilities different from zero) and $I_{\emptyset\emptyset}^{d,2\times 2} = 0$; if there are two $\emptyset$ outcomes, then $I_{rr}^{d,2\times 2} \leq 1$ and $I_{\emptyset\emptyset}^{d,2\times 2} \leq 1$; while if there are three or four $\emptyset$ then $I_{rr}^{d,2\times 2} = 0$ and $I_{\emptyset\emptyset}^{d,2\times 2} \leq 2$.

Note that the inequality (C.23) obeys the condition $\sum_{i,j} c_{ij}^{\emptyset\emptyset} = c$, hence it will provide a bound on $\eta_*^{\forall\lambda}$. Using Eq. (C.14), we obtain the value of $\eta_*^{\forall\lambda}$:

$$\eta_*^{\forall\lambda} = \frac{4}{I_{rr}^{d,2\times2}(QM)+2} \tag{C.24}$$

Inserting the optimal values of $I_{rr}^{d,2\times2}(QM)$ given in [CGL$^+$02] this reproduces our numerical results and those of [DKZ01]. As an example, for dimension 3, $I_{rr}^{3,2\times2}(QM) = 2.873$ so that $\eta_*^{\forall\lambda} = 0.8209$. When $d \to \infty$, (C.24) gives the limit $\eta_*^{\forall\lambda} = 0.8049$.

C.2.2 Three dimensions, 2×3 settings

For three-dimensional systems, we found that adding one setting to one of the party decreases both $\eta_*^{\lambda=1}$ and $\eta_*^{\forall\lambda}$ from 0.8209 to 0.8182 (In the case of $d = 2$, it is necessary to take three settings on each side to get an improvement). The optimal settings involved are $\phi_{A_1} = (0,0,0)$, $\phi_{A_2} = (0, 2\pi/3, 0)$, $\phi_{B_1} = (0, \pi/3, 0)$, $\phi_{B_2} = (0, 2\pi/3, -\pi/3)$, $\phi_{B_3} = (0, -\pi/3, -\pi/3)$.

We have derived a Bell expression associated to these measurements:

$$\begin{aligned} I_{rr}^{3,2\times3} = \; & +[P(A_1 = B_1) + P(A_1 = B_2) + P(A_1 = B_3) \\ & +P(A_2 = B_1 + 1) + P(A_2 = B_2 + 2) + P(A_2 = B_3)] \\ & -[P(A_1 \neq B_1) + P(A_1 \neq B_2) + P(A_1 \neq B_3) \\ & +P(A_2 \neq B_1 + 1) + P(A_2 \neq B_2 + 2) + P(A_2 \neq B_3)] \end{aligned} \tag{C.25}$$

The maximal value of $I_{rr}^{3,2\times3}$ for classical theories is 2 since for any choice of local variables 4 relations with a + can be satisfied but then two with a - are also satisfied. For example we can satisfy the first four relations but this implies $A_2 = B_2 + 1$ and $A_2 = B_3 + 1$ which gives 2 minus terms. The maximal value of $I_{rr}^{3,2\times3}$ for quantum mechanics is given for the settings described above and is equal to $I_{rr}^{3,2\times3}(QM) = 10/3$. To take into account detection inefficiencies consider the following inequality:

$$I^{3,2\times3} = I_{rr}^{3,2\times3} + I_{\emptyset r}^{3,2\times3} + I_{\emptyset\emptyset}^{3,2\times3} \leq 2 \tag{C.26}$$

where

$$I_{\emptyset r}^{3,2\times3} = -\frac{1}{3}\sum_{i,j} P(A_i = \emptyset, B_j \neq \emptyset) \tag{C.27}$$

and

$$I_{\emptyset\emptyset}^{3,2\times3} = \frac{1}{3}\sum_{i,j} P(A_i = \emptyset, B_j = \emptyset). \tag{C.28}$$

($I_{r\emptyset}$ is taken equal to zero). The principle used to show that $I^{3,2\times3} \leq 2$, is the same as the one used to prove that $I^{d,2\times2} \leq 2$. For example if $A_1 = \emptyset$ then $I_{rr}^{3,2\times3} \leq 3$, $I_{\emptyset r}^{3,2\times3} = -1$ and $I_{\emptyset\emptyset}^{3,2\times3} = 0$ so that $I^{3,2\times3} \leq 3 - 1 = 2$. From (C.26) and the joint probabilities (C.20) for the optimal quantum measurements we deduce:

$$\eta_*^{\forall\lambda} = \frac{6}{\frac{10}{3}+4} = \frac{9}{11} \simeq 0.8182 \tag{C.29}$$

in agreement with our numerical result.

Note that in [BPG02], an inequality formally identical to (C.25) has been introduced. However, the measurement scenario involve two measurements on Alice's side and nine binary measurements on Bob's side. By grouping appropriately the outcomes, this measurements scenario can be associated to an inequality formally identical to (C.25) for which the violation reaches $2\sqrt{3}$. According to (C.29), this result in a detection efficiency threshold $\eta_*^{\forall\lambda}$ of $6/(2\sqrt{3}+4) \approx 0.8038$.

C.2.3 Three settings for both parties

For 3 settings per party, things become more surprising. We have found measurements that lower $\eta_*^{\lambda=1}$ and $\eta_*^{\forall\lambda}$ with respect to 2×2 or 2×3 settings. But contrary to the previous situations, $\eta_*^{\lambda=1}$ is not equal to $\eta_*^{\forall\lambda}$, and the two optimal values are obtained for two different sets of measurements. We present in this section the two Bell inequalities associated to each of these situations for the qubit case. Let us first begin with the inequality for $\eta_*^{\lambda=1}$:

$$\begin{aligned} I_{rr}^{2,3\times3,\lambda} &= E(A_1,B_2)+E(A_1,B_3)+E(A_2,B_1)+E(A_3,B_1) \\ &\quad -E(A_2,B_3)-E(A_3,B_2)-\frac{4}{3}P(A_1\neq B_1) \\ &\quad -\frac{4}{3}P(A_2\neq B_2)-\frac{4}{3}P(A_3\neq B_3)\leq 2, \end{aligned} \tag{C.30}$$

where $E(A_i,B_j) = P(A_i = B_j) - P(A_i \neq B_j)$. As usually, the fact that $I_{rr}^{2,3\times3} \leq 2$ follows from considering all deterministic classical strategies. The maximal quantum mechanical violation for this inequality is 3 and is obtained by performing the same measurements on both sides $A_1 = B_1$, $A_2 = B_2$, $A_3 = B_3$ defined by the following phases: $\phi_{A_1} = (0,0)$, $\phi_{A_2} = (0,\pi/3)$, $\phi_{A_3} = (0,-\pi/3)$. It is interesting to note that this inequality and these settings are related to those considered by Bell [Bel64] and Wigner [Wig70] in the first works on quantum non-locality. But whereas in these works it was necessary to suppose that A_i and B_j are perfectly (anti-)correlated when $i = j$ in order to derive a contradiction with lhv theories, here imperfect correlations $P(A_i \neq B_i) > 0$ can also lead to a contradiction since they are included in the Bell inequality.

If we now consider "no-result" outcomes, we can use $I_{rr}^{2,3\times3,\lambda}$ without adding extra terms and the quantum correlations obtained from the optimal measurements violate the inequality if

$$\lambda\eta^2 > \frac{2}{I_{rr}^{2,3\times3,\lambda}(QM)} = \frac{2}{3} \tag{C.31}$$

Taking $\lambda = 1$, we obtain $\eta_*^{\lambda=1} = \sqrt{2/3} \simeq 0.8165$. For smaller value of λ, η_*^{λ} increase until $\eta_*^{\lambda} = 16/19$ is reached for $\lambda \simeq 0.9401$. At that point the contradiction with local theories ceases to depend on the production rate λ. It is then advantageous to use the following inequality

$$\begin{aligned} I_{rr}^{2,3\times3,\forall\lambda} &= \frac{2}{3}E(A_1,B_2)+\frac{4}{3}E(A_1,B_3)+\frac{4}{3}E(A_2,B_1) \\ &\quad +\frac{2}{3}E(A_3,B_1)-\frac{4}{3}E(A_2,B_3)-\frac{2}{3}E(A_3,B_2) \\ &\quad -\frac{4}{3}P(A_1\neq B_1)-\frac{4}{3}P(A_2\neq B_2)-\frac{4}{3}P(A_3\neq B_3) \\ &\leq 2 \end{aligned} \tag{C.32}$$

This inequality is similar to the former one (C.30) but the symmetry between the $E(A_i, B_j)$ terms has been broken: half of the terms have an additional weight of 1/3 and the others of $-1/3$. The total inequality involving "no-result" outcomes is

$$I^{2,3\times3,\forall\lambda} = I_{rr}^{2,3\times3,\forall\lambda} + I_{\emptyset r}^{2,3\times3,\forall\lambda} + I_{r\emptyset}^{2,3\times3,\forall\lambda} + I_{\emptyset\emptyset}^{2,3\times3,\forall\lambda} \leq 2 \tag{C.33}$$

The particular form of the terms $I_{\emptyset r}^{2,3\times3,\forall\lambda}$, $I_{r\emptyset}^{2,3\times3,\forall\lambda}$ and $I_{\emptyset\emptyset}^{2,3\times3,\forall\lambda}$ is given in the Appendix. The important point is that $\sum_{i,j,k}(c_{ij}^{k\emptyset} + c_{i,j}^{\emptyset k}) = -8/3$ and $\sum_{i,j} c_{ij}^{\emptyset\emptyset} = 2$. From (C.14), (C.9) and (C.20), we thus deduce

$$\eta_*^{\forall\lambda} = \frac{4 + \frac{4}{3}}{I_{rr}^{2,3\times3,\forall\lambda}(QM) + 2 + \frac{4}{3}} \tag{C.34}$$

The measurements that optimize the former inequality (C.30) give the threshold $\eta_*^{\forall\lambda} = 16/19$. However these measurements are not the optimal ones for (C.32). The optimal phase settings are given in the Appendix. Using these settings it follows that $I_{rr}^{2,3\times3,\forall\lambda}(QM) = 3.157$ and $\eta_*^{\forall\lambda} \simeq 0.8217$.

One may argue that the situation we have presented here is artificial and results from the fact that we failed to find the optimal inequality valid for all lambda which would otherwise have given a threshold $\eta_*^{\forall\lambda} = 0.8165$ identical to the threshold $\eta_*^{\lambda=1}$. However, this cannot be the case since for $\lambda > 1$ and $\eta > \eta_*^{\lambda=1}$ there exists a lhv model that reproduces the quantum correlations. This lhv model is simply given by the result of the first part of our algorithm described in C.1.4.

C.2.4 More settings and more dimensions

Our numerical algorithm has also yielded further improvements when the number of settings increases or the dimension increases. These results are summarized in Table C.1. For more details, see the Appendix.

C.3 Conclusion

In summary we have obtained using both numerical and analytical techniques a large number of Bell inequalities and optimal quantum measurements that exhibit an enhanced resistance to detector inefficiency. This should be contrasted with the work (reported in [KGZ$^+$00, DKZ01]) devoted to searching for Bell inequalities and measurements with increased resistance to noise. In this case only a single family has been found involving two settings on each side despite extensive numerical searches (mainly unpublished, but see Ref. [ZKBL99]). Thus the structure of Bell inequalities resistant to inefficient detectors seems much richer. It would be interesting to understand the reason for such additional structure and clarify the origin of these inequalities.

It should be noted that for the Bell inequalities we have found, the amount by which the threshold detector efficiency η_* decreases is very small, of the order of 4%. This is tantalizing because we know that for sufficiently large dimension and sufficiently large number of settings, the detector efficiency threshold decreases exponentially. To increase further the resistance to inefficient detector, it would perhaps be necessary to consider more general measurements than the one we considered in this work or use non-maximally entangled states (for instance, Eberhard has shown that for two-dimensional systems, the efficiency threshold η_* can be lowered to 2/3 using non-maximally entangled states [Ebe93]). There may thus be a Bell inequality of real practical importance for closing the detection loophole just behind the corner.

Appendix

For completeness, we present here in details all the Bell inequalities and optimal phase settings we have found. This includes also the results of Table C.1 which have not been discussed in the text.

- $\boldsymbol{N_A = 2,\ N_B = 2,\ \forall\lambda}$

  Bell inequality:

$$\begin{aligned} I^{d,2\times 2} = & \sum_{k=0}^{[d/2]-1} \left(1 - \frac{2k}{d-1}\right) \\ & \Big(+[P(A_1 = B_1 + k) + P(B_1 = A_2 + k + 1) \\ & + P(A_2 = B_2 + k) + P(B_2 = A_1 + k)] \\ & - [P(A_1 = B_1 - k - 1) + P(B_1 = A_2 - k) \\ & + P(A_2 = B_2 - k - 1) + P(B_2 = A_1 - k - 1)] \Big) \\ & + \frac{1}{2} \sum_{i,j=1}^{2} P(A_i = \emptyset, B_j = \emptyset) \leq 2 \end{aligned}$$

  Optimal phase settings:

$$\begin{array}{ll} \phi_{A_1}(j) = 0 & \phi_{A_2}(j) = \frac{\pi}{d} j \\ \phi_{B_1}(j) = \frac{\pi}{2d} j & \phi_{B_2}(j) = -\frac{\pi}{2d} j \end{array}$$

  Maximal violation:

$$I^{d,2\times 2}(QM) = 4d \sum_{k=0}^{[d/2]-1} \left(1 - \frac{2k}{d-1}\right) (q_k - q_{-k-1})$$

  where $q_k = 1/\left(2d^3 \sin^2[\pi(k + 1/4)/d]\right)$.

  Detection threshold: $\eta_*^{\forall\lambda} = \frac{4}{I^{d,2\times 2}(QM)+2}$

- $\boldsymbol{d = 2,\ N_A = 3,\ N_B = 3,\ \lambda}$

  Bell inequality:

$$\begin{aligned} I^{2,3\times 3,\lambda} = & E(A_1, B_2) + E(A_1, B_3) \\ & + E(A_2, B_1) + E(A_3, B_1) - E(A_2, B_3) \\ & - E(A_3, B_2) - \frac{4}{3} P(A_1 \neq B_1) \\ & - \frac{4}{3} P(A_2 \neq B_2) - \frac{4}{3} P(A_3 \neq B_3) \leq 2 \end{aligned}$$

where $E(A_i, B_j) = P(A_i = B_j) - P(A_i \neq B_j)$.

Optimal phase settings:

$$\begin{array}{lll} \phi_{A_1} = (0,0) & \phi_{A_2} = (0,\pi/3) & \phi_{A_3} = (0,-\pi/3) \\ \phi_{B_1} = (0,0) & \phi_{B_2} = (0,\pi/3) & \phi_{B_3} = (0,-\pi/3) \end{array}$$

Maximal violation: $I^{2,3\times 3,\lambda}(QM) = 3$

Detection threshold: $\eta_*^\lambda = \sqrt{\frac{2}{3\lambda}}$

- $\boldsymbol{d = 2,\ N_A = 3,\ N_B = 3,\ \forall\lambda}$

Bell inequality:

$$\begin{aligned} I^{2,3\times3,\forall\lambda} &= \frac{2}{3}E(A_1,B_2) + \frac{4}{3}E(A_1,B_3) \\ &+ \frac{4}{3}E(A_2,B_1) + \frac{2}{3}E(A_3,B_1) - \frac{4}{3}E(A_2,B_3) \\ &- \frac{2}{3}E(A_3,B_2) - \frac{4}{3}P(A_1 \neq B_1) \\ &- \frac{4}{3}P(A_2 \neq B_2) - \frac{4}{3}P(A_3 \neq B_3) \\ &- \frac{2}{3}F_\emptyset(A_1,B_2) - \frac{4}{3}F_\emptyset(A_2,B_3) - \frac{2}{3}F_\emptyset(A_3,B_1) \\ &+ \frac{2}{3}F_\emptyset(A_3,B_2) + \frac{4}{3}P(A_2 = \emptyset, B_1 \neq \emptyset) \\ &+ \frac{4}{3}P(A_1 \neq \emptyset, B_3 = \emptyset) + \frac{4}{3}P(A_1 = \emptyset, B_1 = \emptyset) \\ &+ \frac{4}{3}P(A_2 = \emptyset, B_1 = \emptyset) + \frac{4}{3}P(A_1 = \emptyset, B_3 = \emptyset) \leq 2 \end{aligned}$$

where $E(A_i, B_j) = P(A_i = B_j) - P(A_i \neq B_j)$ and $F_\emptyset(A_i, B_j) = P(A_i = \emptyset, B_j \neq \emptyset) + P(A_i \neq \emptyset, B_j = \emptyset) + P(A_i = \emptyset, B_j = \emptyset)$.

Optimal phase settings:

$$\begin{array}{ll} \phi_{A_1} = (0,0) & \phi_{A_2} = (0,1.3934) \\ \phi_{A_3} = (0,-0.7558) & \\ \phi_{B_1} = (0,0.5525) & \phi_{B_2} = (0,1.3083) \\ \phi_{B_3} = (0,-0.8410) & \end{array}$$

Maximal violation: $I^{2,3\times3,\forall\lambda}(QM) = 3.157$

Detection threshold: $\eta_*^{\forall\lambda} = 0.8217$

- $\boldsymbol{d = 2,\ N_A = 3,\ N_B = 4,\ \forall\lambda}$

  Bell inequality:

$$\begin{aligned} I^{2,3\times 4,\forall\lambda} = &-P(A_1 \neq B_2) - P(A_1 \neq B_3) - P(A_1 \neq B_4) \\ &+ P(A_2 = B_1) + P(A_2 = B_2) - P(A_2 \neq B_3) \\ &+ P(A_2 \neq B_4) - P(A_3 = B_1) + P(A_3 = B_2) \\ &- P(A_3 \neq B_2) + P(A_3 \neq B_3) - P(A_3 = B_4) \\ &+ P(A_1 \neq \emptyset, B_1 = \emptyset) + P(A_2 = \emptyset, B_1 \neq \emptyset) \\ &- P(A_3 \neq \emptyset, B_1 = \emptyset) - P(A_1 = \emptyset, B_2 \neq \emptyset) \\ &+ P(A_1 = \emptyset, B_1 = \emptyset) + P(A_2 = \emptyset, B_2 = \emptyset) \leq 2 \end{aligned}$$

  Optimal phase settings:

$$\begin{array}{ll} \phi_{A_1} = (0,0) & \phi_{A_2} = (0,0.7388) \\ \phi_{A_3} = (0,2.1334) & \\ \phi_{B_1} = (0,-0.1347) & \phi_{B_2} = (0,1.2938) \\ \phi_{B_3} = (0,-0.0757) & \phi_{B_4} = (0,-1.0891) \end{array}$$

  Maximal violation: $I^{2,3\times 4}(QM) = 2.8683$

  Detection threshold: $\eta*^{\forall\lambda} = 0.8216$

- $\boldsymbol{d = 2,\ N_A = 4,\ N_B = 4,\ \forall\lambda}$

  Bell inequality:

$$\begin{aligned} I^{2,4\times 4,\forall\lambda} = &-P(A_1 = B_1) + P(A_1 \neq B_3) - P(A_2 = B_1) \\ &- P(A_2 = B_2) + P(A_2 \neq B_4) + P(A_3 \neq B_1) \\ &- P(A_3 \neq B_2) - P(A_3 \neq B_3) - P(A_4 \neq B_1) \\ &- P(A_4 = B_2) - P(A_4 = B_3) + P(A_4 \neq B_4) \\ &+ P(A_1 \neq \emptyset, B_4 = \emptyset) - P(A_4 \neq \emptyset, B_1 = \emptyset) \\ &+ P(A_1 = \emptyset, B_1 = \emptyset) + P(A_1 = \emptyset, B_4 = \emptyset) \leq 2 \end{aligned}$$

  Optimal phase settings:

$$\begin{array}{ll} \phi_{A_1} = (0,0) & \phi_{A_2} = (0,0.0958) \\ \phi_{A_3} = (0,2.1856) & \phi_{A_4} = (0,4.5944) \\ \phi_{B_1} = (0,4.0339) & \phi_{B_2} = (0,3.3011) \\ \phi_{B_3} = (0,2.2493) & \phi_{B_4} = (0,2.3454) \end{array}$$

  Maximal violation: $I^{2,4\times 4}(QM) = 2.8697$

  Detection threshold: $\eta_*^{\forall\lambda} = 0.8214$

- $\boldsymbol{d=3,\ N_A=2,\ N_B=3,\ \forall\lambda}$

  Bell inequality:

$$\begin{aligned} I^{3,2\times 3,\lambda} &= +[P(A_1=B_1)+P(A_1=B_2)+P(A_1=B_3) \\ &+P(A_2=B_1+1)+P(A_2=B_2+2)+P(A_2=B_3)] \\ &-[P(A_1\neq B_1)+P(A_1\neq B_2)+P(A_1\neq B_3) \\ &+P(A_2\neq B_1+1)+P(A_2\neq B_2+2)+P(A_2\neq B_3)] \\ &-\frac{1}{3}\sum_{i,j}P(A_i=\emptyset,B_j\neq\emptyset) \\ &+\frac{1}{3}\sum_{i,j}P(A_i=\emptyset,B_j=\emptyset)\leq 2 \end{aligned}$$

  Optimal phase settings:

$$\begin{array}{ll} \phi_{A_1}=(0,0,0) & \phi_{A_2}=(0,2\pi/3,0) \\ \phi_{B_1}=(0,\pi/3,0) & \phi_{B_2}=(0,2\pi/3,-\pi/3) \\ \phi_{B_3}=(0,-\pi/3,-\pi/3) & \end{array}$$

  Maximal violation: $I^{3,2\times 3}(QM)=\frac{10}{3}$

  Detection threshold: $\eta_*^{\forall\lambda}=\frac{9}{11}\simeq 0.8182$

- $\boldsymbol{d=3,\ N_A=3,\ N_B=3,\ \lambda}$

  Bell inequality:

$$\begin{aligned} I^{3,3\times 3,\lambda} &= E_1(A_1,B_2)+E_2(A_1,B_3) \\ &+E_2(A_2,B_1)-E_2(A2,B_3)+E_1(A_3,B_1) \\ &-E_1(A_3,B_2)-P(A_1\neq B_1) \\ &-P(A_2\neq B_2)-P(A_3\neq B_3)\leq 2 \end{aligned}$$

  Optimal phase settings:

$$\begin{array}{ll} \phi_{A_1}=(0,0,0) & \phi_{A_2}=(0,2\pi/9,4\pi/9) \\ \phi_{A_3}=(0,-2\pi/9,-4\pi/9) & \\ \phi_{B_1}=(0,0,0) & \phi_{B_2}=(0,2\pi/9,4\pi/9) \\ \phi_{B_3}=(0,-2\pi/9,-4\pi/9) & \end{array}$$

  Maximal violation: $I^{3,3\times 3}(QM)=3.0642$

  Detection threshold: $\eta_*^{\lambda}=\frac{2}{3.0642\lambda}$

- $\boldsymbol{d = 3,\ N_A = 3,\ N_B = 3,\ \forall\lambda}$

Bell inequality:

$$\begin{aligned}
I^{3,3\times 3,\forall\lambda} &= -\frac{5}{3}P(A_1 = B_1) - \frac{4}{3}P(A_1 = B_1 + 2)\\
&+ P(A_1 = B_2) + \frac{5}{3}P(A_1 = B_2 + 1) - \frac{5}{3}P(A_1 = B_3)\\
&- P(A_1 = B_3 + 2) + \frac{5}{3}P(A_2 = B_1) - 2P(A_2 = B_1 + 1)\\
&- \frac{5}{3}P(A_2 = B_2) + 2P(A_2 = B_2 + 1) - P(A_2 = B_3 + 1)\\
&- \frac{5}{3}P(A_2 = B_3 + 2) - \frac{11}{3}P(A_3 = B_1) - 2P(A_3 = B_1 + 2)\\
&+ \frac{2}{3}P(A_3 = B_2) + 2P(A_3 = B_2 + 1) + \frac{5}{3}P(A_3 = B_3)\\
&+ P(A_3 = B_3 + 2) + \frac{5}{3}P(A_1 \neq \emptyset, B_1 = \emptyset)\\
&- \frac{5}{3}P(A_2 \neq \emptyset, B_1 = \emptyset) - 2P(A_3 \neq \emptyset, B_1 = \emptyset)\\
&+ 2P(A_1 \neq \emptyset, B_2 = \emptyset) + \frac{5}{3}P(A_1 = \emptyset, B_1 = \emptyset)\\
&+ 2P(A_1 = \emptyset, B_2 = \emptyset) \leq 11/3
\end{aligned}$$

Optimal phase settings:

$$\begin{array}{ll}
\phi_{A_1} = (0, 0, 0) & \phi_{A_2} = (0, 1.4376, 2.8753)\\
\phi_{A_3} = (0, 0.5063, 1.0125) & \\
\phi_{B_1} = (0, 2.0452, 4.0904) & \phi_{B_2} = (0, 2.9758, -0.3315)\\
\phi_{B_3} = (0, 1.3839, 2.7678) &
\end{array}$$

Maximal violation: $I^{3,3\times 3}(QM) = 5.3358$

Detection threshold: $\eta_*^{\forall\lambda} = 0.8146$

- $\boldsymbol{d = 4,\ N_A = 2,\ N_B = 3,\ \forall\lambda}$

Bell inequality:

$$\begin{aligned}
I^{4,2\times 3,\forall\lambda} &= P(A_1 = B_1 + 1) + 2P(A_1 = B_1 + 2) \\
&+ 2P(A_1 = B_2) + P(A_1 = B_2 + 1) + 2P(A_1 = B_3) \\
&+ 2P(A_2 = B_1 + 1) + P(A_2 = B_1 + 2) + P(A_2 = B_2) \\
&+ 2P(A_2 = B_2 + 1) + 2P(A_2 = B_3 + 2) \\
&+ \frac{4}{3}\sum_i P(A_i = \emptyset, B_1 \neq \emptyset) + \frac{1}{3}\sum_i P(A_i = \emptyset, B_2 \neq \emptyset) \\
&+ \frac{1}{3}\sum_i P(A_i = \emptyset, B_3 \neq \emptyset) + \frac{5}{3}\sum_i P(A_1 \neq \emptyset, B_1 = \emptyset) \\
&+ \frac{1}{3}\sum_i P(A_2 \neq \emptyset, B_1 = \emptyset) + \frac{8}{3}P(A_1 = \emptyset, B_1 = \emptyset) \\
&+ \frac{5}{3}P(A_1 = \emptyset, B_2 = \emptyset) + \frac{5}{3}P(A_1 = \emptyset, B_3 = \emptyset) \\
&+ \frac{4}{3}P(A_2 = \emptyset, B_1 = \emptyset) + \frac{1}{3}P(A_2 = \emptyset, B_2 = \emptyset) \\
&+ \frac{1}{3}P(A_2 = \emptyset, B_3 = \emptyset) \leq 8
\end{aligned}$$

Optimal phase settings:

$$\begin{aligned}
\phi_{A_1} &= (0, 0, 0, 0) \\
\phi_{A_2} &= (0, -1.1397, 2.0019, 3.1416) \\
\phi_{B_1} &= (0, 1.7863, -0.5698, 2.3562) \\
\phi_{B_2} &= (0, 0.2155, 5.7133, 0.7854) \\
\phi_{B_3} &= (0, 1.0009, 1.0009, 0)
\end{aligned}$$

Maximal violation: $I^{4,2\times 3}(QM) = 9.4142$

Detection threshold: $\eta_*^{\forall\lambda} = 0.8093$

- $\boldsymbol{d = 4,\ N_A = 3,\ N_B = 3,\ \forall\lambda}$

  Bell inequality:

$$\begin{aligned}
I^{4,3\times3,\forall\lambda} &= -P(A_1 = B_1 + 2) + P(A_1 = B_1 + 3) \\
&+ 2P(A_1 = B_2 + 1) - P(A_1 = B_2 + 2) - P(A_1 = B_3) \\
&- 3P(A_1 = B_3 + 1) - 2P(A_1 = B_3 + 2) - P(A_2 = B_1) \\
&+ P(A_2 = B_1 + 1) - P(A_2 = B_2 + 1) + P(A_2 = B_2 + 2) \\
&+ 2P(A_2 = B_3 + 3) + 2P(A_3 = B_1 + 1) + P(A_3 = B_2) \\
&- 2P(A_3 = B_2 + 2) - P(A_3 = B_2 + 3) + 2P(A_3 = B_3) \\
&+ P(A_3 = B_3 + 2) + \sum_i P(A_i = \emptyset, B_1 \neq \emptyset) \\
&+ P(A_1 \neq \emptyset, B_1 = \emptyset) + P(A_1 \neq \emptyset, B_2 = \emptyset) \\
&- P(A_1 = \emptyset, B_3 \neq \emptyset) + P(A_3 = \emptyset, B_3 \neq \emptyset) \\
&+ P(A_3 \neq \emptyset, B_3 = \emptyset) + 2P(A_1 = \emptyset, B_1 = \emptyset) \\
&+ P(A_1 = \emptyset, B_2 = \emptyset) + P(A_2 = \emptyset, B_1 = \emptyset) \\
&+ P(A_3 = \emptyset, B_1 = \emptyset) + P(A_3 = \emptyset, B_3 = \emptyset) \leq 6
\end{aligned}$$

  Optimal phase settings:

$$\begin{aligned}
\phi_{A_1} &= (0, 0, 0, 0) \\
\phi_{A_2} &= (0, -1.2238, -1.1546, 3.9048) \\
\phi_{A_3} &= (0, 3.1572, 3.8330, 0.7070) \\
\phi_{B_1} &= (0, -0.9042, 1.7066, 0.8025) \\
\phi_{B_2} &= (0, 2.5844, 3.6937, -0.0051) \\
\phi_{B_3} &= (0, 4.1396, 3.0022, 7.1419)
\end{aligned}$$

  Maximal violation: $I^{4,3\times3}(QM) = 7.5576$

  Detection threshold: $\eta_*^{\forall\lambda} = 0.7939$

Bibliography

[Agr92] Govind P. Agrawal. *Fiber-optic communication systems*. Wiley, New York, 1992.

[AvDK$^+$04] Dorit Aharonov, Wim van Dam, Julia Kempe, Zeph Landau, and Seth Lloyd. Adiabatic quantum computation is equivalent to standard quantum computation. 2004. e-print quant-ph/0405098.

[BBBV97] Charles H. Bennett, Ethan Bernstein, Gilles Brassard, and Umesh Vazirani. Strengths and weaknesses of quantum computing. *SIAM J. Comput.*, 26(5):1510–1523, October 1997.

[Bel64] Jonh S. Bell. On the Einstein Podolsky Rosen paradox. *Physics*, 1:195, 1964.

[Ben73] Charles H. Bennett. Logical reversibility of computation. *IBM J. Res. Dev.*, 17(6):525–532, 1973.

[Ben89] Charles H. Bennett. Time-space trade-offs for reversible computation. *SIAM J. Comput.*, 18:766–776, 1989.

[BPG02] Helle Bechmann-Pasquinucci and Nicolas Gisin. Bell inequality for quNits with binary measurements. 2002. e-print quant-ph/0204122.

[BV93] Ethan Bernstein and Umesh Vazirani. Quantum complexity theory. In *Proceedings of the 25th Annual Symposium on the Theory of Computing*, pages 11–20, New York, 1993. ACM Press.

[CCD$^+$03] Andrew M. Childs, Richard Cleve, Enrico Deotto, Edward Farhi, Sam Gutmann, and Daniel A. Spielman. Exponential algorithmic speedup by quantum walk. In *Proceedings of the 35th Annual ACM Symposium on Theory of Computing*, pages 59–68, New York, 2003. ACM Press. e-print quant-ph/0209131.

[CFP02] Andrew M. Childs, Edward Farhi, and John Preskill. Robustness of adiabatic quantum computation. *Phys. Rev. A*, 65:012322, 2002. e-print quant-ph/0108048.

[CGL$^+$02] Daniel Collins, Nicolas Gisin, Noah Linden, Serge Massar, and Sandu Popescu. Bell inequalities for arbitrarily high-dimensional systems. *Phys. Rev. Lett.*, 88:040404, 2002.

[CGW00] Nicolas J. Cerf, Lov K. Grover, and Colin P. Williams. Nested quantum search and structured problems. *Phys. Rev. A*, 61:032303, 2000. e-print quant-ph/9806078.

[CHSH69] John F. Clauser, Michael A. Horne, Abner Shimony, and Richard A. Holt. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.*, 23:880–884, 1969.

[Chu36] Alonzo Church. An unsolvable problem of elementary number theory. *Am. J. Math.*, 58:345, 1936.

[DBE95] David Deutsch, Adriano Barenco, and Artur Ekert. Universality in quantum computation. *Proc. R. Soc. London A*, 449:669–677, 1995.

[DBE98] Radoslav Derka, Vladimir Buzek, and Artur K. Ekert. Universal algorithm for optimal estimation of quantum states from finite ensembles via realizable generalized measurement. *Phys. Rev. Lett.*, 80:1571–1575, 1998.

[Deu85] David Deutsch. Quantum theory, the Church-Turing principle and the universal quantum computer. *Proc. R. Soc. London A*, 400:97–117, 1985.

[Deu89] David Deutsch. Quantum computational networks. *Proc. R. Soc. London A*, 425:73, 1989.

[DiV98] David P. DiVincenzo. Quantum gates and circuits. *Proc. R. Soc. London A*, 454:261–276, 1998.

[DJ92] David Deutsch and Richard Jozsa. Rapid solution of problems by quantum computation. *Proc. R. Soc. London A*, 439:553, 1992.

[DKZ01] Thomas Durt, Dagomir Kaszlikowski, and Marek Żukowski. Violations of local realism with quantum systems described by N-dimensional Hilbert spaces up to N = 16. *Phys. Rev. A*, 64:024101, 2001.

[Ebe93] Philippe H. Eberhard. Background level and counter efficiencies required for a loophole-free Einstein-Podolsky-Rosen experiment. *Phys. Rev. A*, 47:R747–R750, 1993.

[EJ96] Artur Ekert and Richard Josza. Quantum computation and shor's factoring algorithm. *Rev. Mod. Phys.*, 68:733–753, 1996.

[FG98a] Edward Farhi and Sam Gutmann. An analog analogue of a digital quantum computation. *Phys. Rev. A*, 57:2403–2406, 1998. e-print quant-ph/9612026.

[FG98b] Edward Farhi and Sam Gutmann. Quantum computation and decision trees. *Phys. Rev. A*, 58:915–928, 1998. e-print quant-ph/9706062.

[FGG$^+$01] Edward Farhi, Jeffrey Goldstone, Sam Gutmann, Joshua Lapan, Andrew Lundgren, and Daniel Preda. A quantum adiabatic evolution algorithm applied to random instances of an NP-complete problem. *Science*, 292:472–475, 2001. e-print quant-ph/0104129.

[FGGS00] Edward Farhi, Jeffrey Goldstone, Sam Gutmann, and Michael Sipser. Quantum computation by adiabatic evolution. 2000. e-print quant-ph/0001106.

[FT82] Edward Fredkin and Tommaso Toffoli. Conservative logic. *Int. J. Theor. Phys.*, 21(3/4):219–253, 1982.

[GG99] Nicolas Gisin and Bernard Gisin. A local hidden variable model of quantum correlation exploiting the detection loophole. *Phys. Lett. A*, 260:323–327, 1999.

[Gis] Nicolas Gisin. private communication.

[Gro96] Lov K. Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the 28th Annual Symposium on the Theory of Computing*, pages 212–219, New York, 1996. ACM Press.

[HS96] R. H. Hardin and N. J. A. Sloane. McLaren's improved snub cube and other new spherical designs in three dimensions. *Discrete and Computational Geometry*, 15:429–441, 1996.

[HSSW02] Thomas Hofmeister, Uwe Schöning, Rainer Schuler, and Osamu Watanabe. A probabilistic 3-SAT algorithm further improved. In Helmut Alt and Alfonso Ferreira, editors, *Proceedings of the 19th Annual Symposium on Theoretical Aspects of Computer Science*, volume 2285 of *Lecture Notes in Computer Science*, pages 192–202. Springer, 2002.

[KGZ$^+$00] Dagomir Kaszlikowski, Piotr Gnaciński, Marek Żukowski, Wieslaw Miklaszewski, and Anton Zeilinger. Violations of local realism by two entangled N-dimensional systems are stronger than for two qubits. *Phys. Rev. Lett.*, 85:4418–4421, 2000.

[Lai97] D. N. Laikov. Fast evaluation of density functional exchange-correlation terms using the expansion of the electron density in auxiliary basis sets. *Chem. Phys. Lett.*, 281(2):151–156, 1997.

[Lan61] Rolf Landauer. Irreversibility and heat generation in the computing process. *IBM J. Res. Dev.*, 5:183, 1961.

[Lar02] Jan-Ake Larsson. A practical trojan horse for Bell-inequality-based quantum cryptography. *Quantum Inf. Comput.*, 2:434, 2002.

[Leb94] V. I. Lebedev. A quadrature formula for the sphere of the 59th algebraic order of accuracy. *Dokl. Akad. Nauk.*, 338(4):454–456, 1994.

[LL99] V. I. Lebedev and D. N. Laikov. A quadrature formula for the sphere of the 131st algebraic order of accuracy. *Dokl. Akad. Nauk.*, 366(6):741–745, 1999.

[Llo95] Seth Lloyd. Almost any quantum logic gate is universal. *Phys. Rev. Lett.*, 75(2):346, 1995.

[LPT98] José I. Latorre, Pere Pascual, and Rolf Tarrach. Minimal optimal generalized quantum measurements. *Phys. Rev. Lett.*, 81:1351–1354, 1998. e-print quant-ph/9803066.

[LS92] V. I. Lebedev and A. L. Skorokhodov. Quadrature-rules for a sphere of 41-order, 47-order and 53-order of accuracy. *Dokl. Akad. Nauk.*, 324(3):519–524, 1992.

[Mas02] Serge Massar. Nonlocality, closing the detection loophole, and communication complexity. *Phys. Rev. A*, 65:032121, 2002.

[Mes59] Albert Messiah. *Mécanique Quantique.* Dunod, Paris, 1959.

[MP95] Serge Massar and Sandu Popescu. Optimal extraction of information from finite quantum ensembles. *Phys. Rev. Lett.*, 74:1259–1263, 1995.

[MP03] Serge Massar and Stefano Pironio. Violation of local realism versus detection efficiency. *Phys. Rev. A*, 68:062109, 2003.

[MPRG02] Serge Massar, Stefano Pironio, Jérémie Roland, and Bernard Gisin. Bell inequalities resistant to detector inefficiency. *Phys. Rev. A*, 66:052112, 2002. e-print quant-ph/0205130.

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

[NM65] J. A. Nelder and R. Mead. A simplex method for function minimization. *Comput. J.*, 7:308, 1965.

[Per95] Asher Peres. *Quantum Theory: Concepts and Methods.* Kluwer, Boston, 1995.

[Pre98] John Preskill. 1998. Lecture Notes for Physics 229: Quantum Information and Computation.

[PW91] Asher Peres and William K. Wootters. Optimal detection of quantum information. *Phys. Rev. Lett.*, 66:1119—-1122, 1991.

[RC02] Jérémie Roland and Nicolas J. Cerf. Quantum search by local adiabatic evolution. *Phys. Rev. A*, 65:042308, 2002. e-print quant-ph/0107015.

[RC03a] Jérémie Roland and Nicolas J. Cerf. Adiabatic quantum search algorithm for structured problems. *Phys. Rev. A*, 68:062312, 2003. e-print quant-ph/0304039.

[RC03b] Jérémie Roland and Nicolas J. Cerf. Quantum-circuit model of Hamiltonian search algorithms. *Phys. Rev. A*, 68:062311, 2003. e-print quant-ph/0302138.

[RKM$^+$01] M. A. Rowe, D. Kielpinski, V. Meyer, C. A. Sackett, W. M. Itano, C. Monroe, and D. J. Wineland. Experimental violation of a Bell's inequality with efficient detection. *Nature*, 409:791–194, 2001.

[San92] Emilio Santos. Critical analysis of the empirical tests of local hidden-variable theories. *Phys. Rev. A*, 46:3646–3656, 1992.

[SBW03] Neil Shenvi, Kenneth R. Brown, and K. Birgitta Whaley. Effects of a random noisy oracle on search algorithm complexity. *Phys. Rev. A*, 68:052313, 2003. e-print quant-ph/0304138.

[Sch55] Leonard I. Schiff. *Quantum Mechanics.* Mc Graw-Hill, Singapore, 1955.

[Sch99] Uwe Schöning. A probabilistic algorithm for k-SAT and constraint satisfaction problems. In *Proceedings of the 40th Annual Symposium on the Foundations of Computer Science*, pages 410–414, New York, 1999. IEEE Computer Society Press.

[Sho94] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. In S. Goldwasser, editor, *Proceedings of the 35th Annual Symposium on the Foundations of Computer Science*, pages 124–134, New York, 1994. IEEE Computer Society Press. e-print quant-ph/9508027.

[Sho00] Peter W. Shor. Introduction to quantum algorithms. 2000. e-print quant-ph/0005003.

[Sim94] Daniel R. Simon. On the power of quantum computation. In S. Goldwasser, editor, *Proceedings of the 35th Annual Symposium on the Foundations of Computer Science*, pages 116–123, New York, 1994. IEEE Computer Society Press.

[Ste98] Andrew Steane. Quantum computing. *Rept. Prog. Phys.*, 61:117–173, 1998. e-print quant-ph/9708022.

[Stö99] Hans-Jürgen Stöckmann. *Quantum chaos : an introduction.* Cambridge University Press, Cambridge, 1999.

[Sze95] Gàbor Szegö. *Orthogonal polynomials.* American Mathematical Society, New York, 1895.

[Tur36] Alan M. Turing. On computable numbers, with an application to the Eintscheidungsproblem. *Proc. Lond. Math. Soc. 2*, 42:230, 1936.

[vDMV01] Wim van Dam, Michele Mosca, and Umesh Vazirani. How powerful is adiabatic quantum computation? In *Proceedings of the 42nd Annual Symposium on the Foundations of Computer Science*, pages 279–287, New York, 2001. IEEE Computer Society Press.

[Wig70] Eugene P. Wigner. On hidden variables and quantum mechanical probabilities. *Am. J. Phys.*, 38:1005, 1970.

[WJS$^+$98] Gregor Weihs, Thomas Jennewein, Christoph Simon, Harald Weinfurter, and Anton Zeilinger. Violation of Bell's inequality under strict Einstein locality conditions. *Phys. Rev. Lett.*, 81:5039–5043, 1998.

[Zal99] Christof Zalka. Grover's quantum searching algorithm is optimal. *Phys. Rev. A*, 60:2746–2751, 1999. e-print quant-ph/9711070.

[ZKBL99] Marek Żukowski, Dagomir Kaszlikowski, Adam Baturo, and Jan-Ake Larsson. Strengthening the Bell theorem: conditions to falsify local realism in an experiment. 1999. e-print quant-ph/9910058.

[ZZH97] Marek Żukowski, Anton Zeilinger, and Michael A. Horne. Realizable higher-dimensional two-particle entanglements via multiport beam splitters. *Phys. Rev. A*, 55:2564–2579, 1997.