UNIVERSITAT DE BARCELONA

Entanglement, quantum phase transitions and quantum algorithms

Román Óscar Orús Lacort

Entanglement, quantum phase transitions and quantum algorithms

Román Óscar Orús Lacort

Barcelona, July, 2006

Universitat de Barcelona

Departament d'Estructura i Constituents de la Matèria

UNIVERSITAT DE BARCELONA

Entanglement, quantum phase transitions and quantum algorithms

Memoria de la tesis presentada
por Román Óscar Orús Lacort para optar
al grado de Doctor en Ciencias Físicas

Director de la tesis: Dr. José Ignacio Latorre Sentís

Departament d'Estructura i Constituents de la Matèria
Programa de doctorado de *"Física avanzada"*
Bienio 2002-2004
Universitat de Barcelona

A los que se fueron, y
a los que se quedaron,
en especial a Mariano, Nati,
María Mercedes y Ondiz

Saber y saberlo demostrar es valer dos veces
– Baltasar Gracián

Las cuentas claras y el chocolate espeso
– Refranero popular español

Agradecimientos

He necesitado escribir más de 150 páginas llenas de ecuaciones raras y letras feas para poder saborear el delicioso momento de escribir los agradecimientos de mi tesis. Y es que dicen que de bien nacido es el ser agradecido, y tengo cuerda para rato, así que allá vamos.

La primera persona a quien le he de agradecer muchas cosas es a José Ignacio Latorre, quien se ofreció a dirigirme una tesis doctoral en el mundillo este de la información cuántica, de la cual yo no tenía ni idea hace cuatro años y pico cuando entré en su despacho cual pollito recién licenciado y él me dijo aquello de "hacer una tesis es como casarse, y si te casas, *te casas*". Memorables sentencias al margen, le agradezco la total y absoluta confianza que siempre ha depositado en mí a lo largo de este tiempo, además de lo muchísimo que he aprendido con él beneficiándome de su conocimiento multidisciplinar. Tampoco me olvido de alguna que otra cena (aquella sopa de cebolla me hizo llorar de alegría...), alguna que otra cata de vinos de la casa, y algún que otro partidazo de basket o fútbol. Seguiremos en contacto.

A Guifré Vidal he de agradecerle su confianza en mí casi desde el minuto cero. Ha sido un placer discutir de física contigo y he aprendido y disfrutado mucho. Seguiremos en Brisbane.

Gracias a todas las personas con las que he discutido sobre lo divertida que es la mecánica cuántica. En la UB, los "quantum boys" Enric Jané, Lluís Masanes, Enrique Rico (compañero de batalla tantos años, qué grandes partidos de basket, qué grandes sopas de cebolla), Joakim Bergli, Sofyan Iblisdir (Seigneur, prévenez-moi à l'avance afin que j'y pré-dispose mon système digestif...), y los recién llegados al campo Arnau Riera, José María Escartín y Pere Talavera. También a Pere Pascual por sus siempre buenos consejos e interés por mi trabajo, a Rolf Tarrach y David Mateos por meterme entre ceja y ceja cuando hacía la carrera que lo de la cuántica era interesante, a Núria Barberán, Josep Tarón, y a los profesores visitantes Andy Lütken y Krzystof Pilch. En la UAB, a Emili Bagan, Mariano Baig, Albert Bramon, John Casamiglia, Ramón Muñoz-Tapia, Anna Sanpera, y también a Álex Monrás y Sergio Boixo (que pesadito estuve con QMA, ¿eh?). En el ICFO, a Toni Acín le debo sabios consejos aquí y en algún que otro pueblo perdido del pirineo. Gracias también a Maciej Lewenstein, Joonwoo Bae, Miguel Navascués (¿cómo hiciste el truco aquél de la rata?), y Mafalda.

Durante este tiempo he colaborado con gente en mis artículos a los que también les agradezco lo mucho que he aprendido de ellos. Gracias a – thanks to – José Ignacio Latorre, Jens Eisert, Marcus Cramer, MariCarmen Bañuls, Armando Pérez (tenemos una paella pendiente), Pedro Ruíz Femenía, Enrique Rico, Julien Vidal, Rolf Tarrach, Cameron Wellard, y Miguel Ángel Martín-Delgado.

Al margen de la mecánica cuántica pura y dura, agradezco dentro de la UB y por diversos

motivos a Doménech Espriu, Joaquim Gomis, Joan Soto, Josep María Pons, Lluís Garrido, Roberto Emparan, Artur Polls, Manel Barranco, Aurora Hernández, y Marcel Porta, así como a toda la gente de la secretaría del departamento.

Y llegó la hora de volar.

I want to thank Edward Farhi for inviting me to visit MIT. Thanks also to Jeffrey Goldstone, Sam Gutmann, Andrew Childs, Andrew Landahl, and Enrico Deotto: I had a really good time in Boston. Thanks to Julien Vidal for inviting Enrique and me to collaborate with him in Paris. A Ignacio Cirac he de agradecerle entre otras cosas sus buenos consejos y su confianza, así como el invitarme a visitar el grupo de Garching. Gracias a – thanks to – María, Diego, Juanjo, Belén, David (qué gran disfraz el de aquél día), Géza, Susana, Michael, Christine, mi spanglish friend Elva, Stefan, Toby, Enrique Solano, Renate... hicisteis que Bavaria fuera como mi casa, y aprendí mucho con vosotros. Thanks to Daniel Gottesman and Debbie Leung for inviting me to visit Perimeter Institute and the University of Waterloo, and also to Mike Mosca, Lucien Hardy, Carlos Mochon, Mary Beth Ruskai and Frank Wilhem for their hospitality and for sharing interesting discussions about physics with me. I am grateful as well to David P. DiVincenzo for inviting me to visit the IBM Watson Research Center, and thanks to Charles Bennett, John Smolin, Barbara Terhal, and Roberto Oliveira: it was wonderful in New York as well. De nuevo, gracias a Guifré Vidal por invitarme a visitar las antípodas y a comer carne de canguro, and thanks to all the people that I met at the quantum information group and the physics' department of the University of Queensland for their hospitality and interesting discussions: Michael Nielsen, David Poulin, Alexei Gilchrist, Andrew Doherty, Kenny, Norma, Robert Spalek, Rolando Somma, Álvaro, Juliet, Aggie, Huan-Qiang Zhou, John Fjaerestad... I think we are going to meet again.

También he conocido a muchísima gente y he hecho amigos en congresos y escuelas, a quien en mayor o menor medida debo agradecerles lo bien que me lo he pasado haciendo física durante los últimos cuatro años y pico. El primer TAE en Peñíscola alcanzó la categoría de genial: Olga, Ester, Carmen, Pedro... estuvo bien, ¿eh? The time at the Les Houches summer school was memorable: thanks to all of you Les Houches guys, Elva, Carlos, Fabio, Derek, Alex, Silvia, Sara, Cameron, John, Neill, André, Alessio, Luca, The-Russian-Guy, Toby, David, Maggie, Chris, Philippe, Ru-Fen, Augusto... the french national day will never be the same for me. Thanks also to Fabio Anselmi, Yasser Omar, Roberta Rodríguez, Jeremie Roland, Verónica Cerletti (era "posho", ¿no?), Marcos Curty, Philipp Hyllus, Jiannis Pachos, Angelo Carollo, Almut Beige, Jonathan Oppenheim, Ivette Fuentes-Schuller, David Salgado, Adán Cabello, Marcus Cramer, Shashank Virmani... and so many people that I met and who I can not remember right now, but to whom I am grateful too.

Y aterrizamos en Barcelona.

Una mención especial se la merecen mis compañeros de departamento, hermanos de batalla científica en el arduo vía crucis del doctorado: Aleix, Álex, Toni Mateos, Toni Ramírez, Jan, Otger, Ernest (desgraciaaaaaaaaaaat!), Míriam y su infinita paciencia, Xavi y sus pesas de buzo, Diego y sus acordes, Dani, Carlos y sus cómics, el ínclito y maravilloso Luca, Jordi Garra, Joan Rojo, Jaume, Majo, Arnau Rios, Chumi alias Cristian, Jordi Mur, Sandro el revolucionario, Ignazio, Enrique, Lluís... sin vosotros me habría aburrido como una ostra. Otra mención especial a mis coleguillas de la carrera: sois tantos que no cabéis todos ni en 500 páginas, pero ya sabéis

quienes sois, así que daros por agradecidos. De todas formas, gracias en especial a Encarni (o actual señora Pleguezuelos) por soportarme estoicamente a lo largo de innumerables cafés y crepes de queso de los menjadors, y también a Alberto por aguantarme tantas paranoias. Qué grandes partidos de basket con la gente de electrónica: gracias también a vosotros. E igualmente gracias a la gente que he conocido por el IRC-Hispano, ya sabréis quienes sois si os dais por aludidos al leer esto: me lo he pasado muy bien con vosotros también. También he de dar gracias a Pablo, por comprender mi visión del mundo y estar ahí cuando hacía falta, entre Silvios y patxaranes.

Gracias también a Apple por inventar el PowerBook de 12”, a Google por encontrarme cada vez que me pierdo, a Donald Knuth por inventar el TeX, al café, al chocolate, a Haruko, a Guu, al Dr. Fleishman, y a Samantha Carter por enseñarme a hacer explotar una estrella usando un stargate. Habéis hecho mis últimos cuatro años y medio mucho más agradables y llevaderos.

Finalmente, gracias a mi familia extensa, el clan Orús Lacort y todas sus ramificaciones posibles en todos sus grados de consanguinidad y generación. Primos, sois de verdad mucho primo. Gracias a mis padres y a mi hermana por tantas cosas y tantísimo apoyo incondicional. Gracias a Lidia por aguantarme en su casa de vez en cuando. Y gracias a mi pequeño y particular desastre fraggel de ojos azules llamado Ondiz por estar siempre ahí cuando le necesito.

Research papers

This thesis is the conclusion of four and a half years of work at the *Departament d'Estructura i Constituents de la Matèria* of the *University of Barcelona*. All along this time I have contributed in several research papers, most of them being the basis of the results that I present here.

The papers on which this thesis is based, sorted in chronological order, are:

- R. Orús, J. I. Latorre, J. Eisert, and M. Cramer. Half the entanglement in critical systems is distillable from a single specimen, 2005. quant-ph/0509023 (to appear in *Phys. Rev. A*).
- M. C. Bañuls, R. Orús, J. I. Latorre, A. Pérez, and P. Ruiz-Femenía. Simulation of many-qubit quantum computation with matrix product states. *Phys. Rev. A*, 73:022344, 2006.
- R. Orús. Entanglement and majorization in (1+1)-dimensional quantum systems. *Phys. Rev. A*, 71:052327, 2005. Erratum-ibid 73:019904, 2006.
- J. I. Latorre, R. Orús, E. Rico and J. Vidal. Entanglement entropy in the Lipkin-Meshkov-Glick model. *Phys. Rev. A*, 71:064101, 2005.
- R. Orús and J. I. Latorre. Universality of entanglement and quantum computation complexity. *Phys. Rev. A*, 69:052308, 2004.
- J. I. Latorre and R. Orús. Adiabatic quantum computation and quantum phase transitions. *Phys. Rev. A*, 69:062302, 2004.
- R. Orús, J. I. Latorre, and M. A. Martín-Delgado. Systematic analysis of majorization in quantum algorithms. *Eur. Phys. J. D*, 29:119, 2004.
- R. Orús, J. I. Latorre, and M. A. Martín-Delgado. Natural majorization of the quantum Fourier transformation in phase-estimation algorithms. *Quant. Inf. Proc.*, 4:283, 2003.

Other papers in which I was involved, sorted in chronological order, are:

- R. Orús. Two slightly-entangled NP-complete problems. *Quant. Inf. and Comp.*, 5:449, 2005.

- R. Orús and R. Tarrach. Weakly-entangled states are dense and robust. *Phys. Rev. A*, 70:050101, 2004.
- C. Wellard and R. Orús. Quantum phase transitions in anti-ferromagnetic planar cubic lattices. *Phys. Rev. A*, 70:062318, 2004.

Contents

Chapter 0

Introduction

From the seminal ideas of Feynman [1] and until now, quantum information and computation [2] has been a rapidly evolving field. While at the beginning, physicists looked at quantum mechanics as a theoretical framework to describe the fundamental processes that take place in Nature, it was during the 80's and 90's that people began to think about the intrinsic quantum behavior of our world as a tool to eventually develop powerful information technologies. As Landauer pointed out [3], *information is physical*, so it should not look strange to try to bring together quantum mechanics and information theory. Indeed, it was soon realized that it is possible to use the laws of quantum physics to perform tasks which are unconceivable within the framework of classical physics. For instance, the discovery of quantum teleportation [4], superdense coding [5], quantum cryptography [6, 7], Shor's factorization algorithm [8] or Grover's searching algorithm [9], are some of the remarkable achievements that have attracted the attention of many people, both scientists and non-scientists. This settles down quantum information as a genuine interdisciplinary field, bringing together researchers from different branches of physics, mathematics and engineering.

While until recently it was mostly quantum information science that benefited from other fields, today the tools developed within its framework can be used to study problems of different areas, like quantum many-body physics or quantum field theory. The basic reason behind that is the fact that quantum information develops a detailed study of quantum correlations, or quantum *entanglement*. Any physical system described by the laws of quantum mechanics can then be considered from the perspective of quantum information by means of entanglement theory.

It is the purpose of this introduction to give some elementary background about basic concepts of quantum information and computation, together with its possible relation to other fields of physics, like quantum many-body physics. We begin by considering the definition of a *qubit*, and move then towards the definition of *entanglement* and the convertibility properties of pure states by introducing *majorization* and the *von Neumann entropy*. Then, we consider the notions of *quantum circuit* and *quantum adiabatic algorithm*, and move towards what is typically understood by a *quantum phase transition*, briefly sketching how this relates to *renormalization* and *conformal field theory*. We also comment briefly on some possible *experimental implementations* of quantum computers.

What is a "qubit"?

A *qubit* is a quantum two-level system, that is, a physical system described in terms of a Hilbert space $\mathbb{C}^2$. You can think of it as a spin-$\frac{1}{2}$ particle, an atom in which we only consider two energy levels, a photon with two possible orthogonal polarizations, or a "dead or alive" Schrödinger's cat. Mathematically, a possible orthonormal basis for this Hilbert space is denoted by the two orthonormal vectors $|0\rangle$ and $|1\rangle$. This notation is analogous to the one used for a classical bit, which can be in the two "states" 0 or 1. Notice, however, that the laws of quantum mechanics allow a qubit to physically exist in *any* linear combination of the states $|0\rangle$ and $|1\rangle$. That is, the generic state $|\psi\rangle$ of a qubit is given by

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

where α and β are complex numbers such that $|\alpha|^2 + |\beta|^2 = 1$. Given this normalization condition, the above state can always be written as

$$|\psi\rangle = e^{i\gamma}\left(\cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi}\sin\left(\frac{\theta}{2}\right)|1\rangle\right) \,, \tag{2}$$

where γ, θ and ϕ are some real parameters. Since the global phase $e^{i\gamma}$ has no observable effects, the physical state of a qubit is always parameterized in terms of two real numbers θ and ϕ, that is,

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi}\sin\left(\frac{\theta}{2}\right)|1\rangle \,. \tag{3}$$

The angles θ and ϕ define a point on a sphere that is usually referred to as the *Bloch sphere*. Generally speaking, it is possible to extend the definition of qubits and define the so-called *qudits*, by means of quantum d-level systems.

What is "entanglement"?

The definition of entanglement varies depending on whether we consider only pure states or the general set of mixed states. Only for pure states, we say that a given state $|\psi\rangle$ of n parties is *entangled* if it is not a tensor product of individual states for each one of the parties, that is,

$$|\psi\rangle \neq |v_1\rangle_1 \otimes |v_2\rangle_2 \otimes \cdots \otimes |v_n\rangle_n \,. \tag{4}$$

For instance, in the case of 2 qubits A and B (sometimes called "Alice" and "Bob") the quantum state

$$|\psi^+\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |1\rangle_B\right) \tag{5}$$

is entangled since $|\psi^+\rangle \neq |v_A\rangle_A \otimes |v_B\rangle_B$. On the contrary, the state

$$|\phi\rangle = \frac{1}{2}\left(|0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |0\rangle_B + |0\rangle_A \otimes |1\rangle_B + |1\rangle_A \otimes |1\rangle_B\right) \tag{6}$$

is not entangled, since

$$|\phi\rangle = \left(\frac{1}{\sqrt{2}}\left(|0\rangle_A + |1\rangle_A\right)\right) \otimes \left(\frac{1}{\sqrt{2}}\left(|0\rangle_B + |1\rangle_B\right)\right) \,. \tag{7}$$

A pure state like the one from Eq.5 is called a *maximally entangled state of two qubits*, or a *Bell pair*, whereas a pure state like the one from Eq.7 is called *separable*.

In the general case of mixed states, we say that a given state ρ of n parties is *entangled* if it is not a probabilistic sum of tensor products of individual states for each one of the parties, that is,

$$\rho \neq \sum_k p_k \, \rho_1^k \otimes \rho_2^k \otimes \cdots \otimes \rho_n^k \, , \tag{8}$$

with $\{p_k\}$ being some probability distribution. Otherwise, the mixed state is called *separable*.

The essence of the above definition of entanglement relies on the fact that entangled states of n parties cannot be prepared by acting locally on each one of the parties, together with classical communication (telephone calls, e-mails, postcards...) among them. This set of operations is often referred to as "local operations and classical communication", or LOCC. If the actions performed on each party are probabilistic, as is for instance the case in which one of the parties draws a random variable according to some probability distribution, the set of operations is called "stochastic local operations and classical communication", or SLOCC. Entanglement is, therefore, a genuine quantum-mechanical feature which does not exist in the classical world. It carries non-local correlations between the different parties in such a way that they cannot be described classically, hence, these correlations are *quantum correlations*.

The study of the structure and properties of entangled states constitutes what is known as *entanglement theory*. In this thesis, we shall always restrict ourselves to the entanglement that appears in pure states. We also wish to remark that the notation for the tensor product of pure states can be different depending on the textbook, in such a way that $|v_A\rangle_A \otimes |v_B\rangle_B = |v_A\rangle_A |v_B\rangle_B = |v_A, v_B\rangle$. An introduction to entanglement theory, both for pure and mixed states, can be found for instance in [10].

Majorization and the von Neumann entropy

Majorization theory is a part of statistics that studies the notion of order in probability distributions [11–14]. Namely, majorization states that given two probability vectors $\vec{x}$ and $\vec{y}$, the probability distribution $\vec{y}$ majorizes $\vec{x}$, written as $\vec{x} \prec \vec{y}$, if and only if

$$\vec{x} = \sum_k p_k P_k \vec{y} \, , \tag{9}$$

where $\{p_k\}$ is a set of probabilities and $\{P_k\}$ is a set of permutation matrices. The above definition implies that the probability distribution $\vec{x}$ is more disordered than the probability distribution $\vec{y}$, since it can be obtained by a probabilistic sum of permutations of $\vec{y}$. More details on majorization theory, which is often used in this thesis, are given in Appendix A.

Majorization theory has important applications in quantum information science. One of them is that it provides a criteria for the interconvertibility of bipartite pure states under LOCC. More concretely, given two bipartite states $|\psi_{AB}\rangle$ and $|\phi_{AB}\rangle$ for parties A and B, and given the spectrums $\vec{\rho}_\psi$ and $\vec{\rho}_\phi$ of their respective reduced density matrices describing any of the two parties, the state $|\psi_{AB}\rangle$ may be transformed to $|\phi_{AB}\rangle$ by LOCC if and only if [15]

$$\vec{\rho}_\psi \prec \vec{\rho}_\phi \, . \tag{10}$$

An important theorem from classical information theory that plays a role in the study of entanglement is the so-called *theorem of typical sequences*. In order to introduce it, let us previously sketch some definitions. Consider a source of letters x which are produced with some probability $p(x)$. The *Shannon entropy* associated to this source is defined as $H = -\sum_x p(x)\log_2 p(x)$. Given a set of n independent sources, we say that a string of symbols $(x_1, x_2, \ldots, x_n)$ is ϵ-typical if

$$2^{-n(H-\epsilon)} \leq p(x_1, x_2, \ldots, x_n) \leq 2^{-n(H+\epsilon)} , \tag{11}$$

where $p(x_1, x_2, \ldots, x_n) \equiv p(x_1)p(x_2)\cdots p(x_n)$ is the probability of the string. The set of the ϵ-typical sequences of length n is denoted as $T(n, \epsilon)$. We are now in position of considering the theorem of typical sequences, which is composed of three parts:

Theorem 0.1 (of typical sequences):

- *Given $\epsilon > 0$, for any $\delta > 0$ and sufficiently large n, the probability that a sequence is ϵ-typical is at least $1 - \delta$.*
- *For any fixed $\epsilon > 0$ and $\delta > 0$, and sufficiently large n, the number $|T(n, \epsilon)|$ of ϵ-typical sequences satisfies*
$$(1 - \delta)2^{n(H-\epsilon)} \leq |T(n, \epsilon)| \leq 2^{n(H+\epsilon)} . \tag{12}$$
- *Let $S(n)$ be a collection of size at most 2^{nR}, of length n sequences from the source, where $R < H$ is fixed. Then, for any $\delta > 0$ and for sufficiently large n,*
$$\sum_{(x_1,x_2,\ldots,x_n) \in S(n)} p(x_1, x_2, \ldots, x_n) \leq \delta . \tag{13}$$

It is not our purpose here to provide a detailed proof of this theorem (the interested reader is addressed for instance to [2]). We shall, however, make use of it in what follows.

Let us introduce at this point a quantity which is to play a major role all along this thesis. Given a bipartite pure quantum state $|\psi_{AB}\rangle$, with reduced density matrices $\rho_A = \mathrm{tr}_B(|\psi_{AB}\rangle\langle\psi_{AB}|)$ and $\rho_B = \mathrm{tr}_A(|\psi_{AB}\rangle\langle\psi_{AB}|)$, the *von Neumann entropy* of this bipartition is defined as

$$S \equiv S(\rho_A) = -\mathrm{tr}(\rho_A \log_2 \rho_A) = S(\rho_B) = -\mathrm{tr}(\rho_B \log_2 \rho_B) , \tag{14}$$

where the equality follows from the fact that ρ_A and ρ_B share the same spectrum. This entropy is also called *entanglement entropy*, since it provides a measure of the bipartite entanglement present in pure states. To be precise, the entanglement entropy measures the optimal rate at which it is possible to distill Bell pairs by LOCC in the limit of having an infinite number of copies of the bipartite system.

Let us explain how the above consideration works. Given the bipartite pure state $|\psi_{AB}\rangle$, we write it in terms of the so-called *Schmidt decomposition*:

$$|\psi_{AB}\rangle = \sum_x \sqrt{p(x)}|x_A\rangle_A|x_B\rangle_B , \tag{15}$$

where the square $p(x)$ of the Schmidt coefficients define the probability distribution that appears as the spectrum of the reduced density matrices for the two parties. The n-fold tensor product $|\psi_{AB}\rangle^{\otimes n}$ can be written as

$$|\psi_{AB}\rangle^{\otimes n} = \sum_{(x_1,x_2,\ldots,x_n)} \sqrt{p(x_1)p(x_2)\cdots p(x_n)}|x_{1A}, x_{2A}, \ldots, x_{nA}\rangle_A |x_{1B}, x_{2B}, \ldots, x_{nB}\rangle_B \,. \tag{16}$$

Let us now define a quantum state $|\phi_n\rangle$ obtained by omitting in Eq.16 those strings $(x_1, x_2, \ldots, x_n)$ which are not ϵ-typical:

$$|\phi_n\rangle = \sum_{(x_1,x_2,\ldots,x_n)\,\in\, T(n,\epsilon)} \sqrt{p(x_1)p(x_2)\cdots p(x_n)}|x_{1A}, x_{2A}, \ldots, x_{nA}\rangle_A |x_{1B}, x_{2B}, \ldots, x_{nB}\rangle_B \,. \tag{17}$$

Since the previous state is not properly-normalized, we define the state $|\phi'_n\rangle \equiv |\phi_n\rangle / \sqrt{\langle\phi_n|\phi_n\rangle}$. Because of the first part of the theorem of typical sequences, the overlap between $|\psi_{AB}\rangle^{\otimes n}$ and $|\phi'_n\rangle$ tends to 1 as $n \to \infty$. Furthermore, by the second part of the theorem we have that $|T(n,\epsilon)| \leq 2^{n(H+\epsilon)} = 2^{n(S+\epsilon)}$. Given these properties, a possible protocol to transform copies of the state $|\psi_{AB}\rangle$ into Bell pairs by means of LOCC reads as follows: party A may convert the state $|\psi_{AB}\rangle^{\otimes n}$ into the state $|\phi'_n\rangle$ with high probability by performing a local measurement into its ϵ-typical subspace. The largest Schmidt coefficient of $|\phi_n\rangle$ is $2^{-n(S-\epsilon)/2}$ by definition of typical sequence, and since the theorem of typical sequences also tells us that $1-\delta$ is a lower bound on the probability for a sequence to be ϵ-typical, the largest Schmidt coefficient of $|\phi'_n\rangle$ is at most $2^{-n(S-\epsilon)/2}/\sqrt{1-\delta}$. Let us now choose an m such that

$$\frac{2^{-n(S-\epsilon)}}{1-\delta} \leq 2^{-m} \,. \tag{18}$$

Then, the spectrum of the reduced density matrices for A and B are majorized by the probability vector $(2^{-m}, 2^{-m}, \ldots, 2^{-m})^T$, and therefore the state $|\phi'_n\rangle$ can be transformed into m copies of a Bell state by means of local operations and classical communication. More specifically, in the limit $n \to \infty$ the ratio m/n between the number of distilled Bell pairs and the original number of states exactly coincides with the entanglement entropy S.

It is possible to see that the above distillation protocol is optimal, that is, it is not possible to distill more than nS Bell pairs from a total of n copies of a bipartite pure state in the limit $n \to \infty$. Because of this property, the von Neumann entropy is also called the *distillable entanglement* of a pure bipartite system. Furthermore, it is possible to see that the entropy S coincides as well with the *entanglement of formation* of bipartite pure states, which is the optimal ratio m/n describing the number m of Bell pairs that are required to create n copies of a given bipartite pure state by means of LOCC, in the limit $n \to \infty$. The von Neumann entropy constitutes then a genuine measure of the bipartite entanglement that is present in a given pure quantum state.

Quantum circuits and adiabatic quantum algorithms

Much in analogy to the situation in classical computation, where it is possible to define a computation by means of logic gates applied to bits, a quantum computation may be defined in terms of a set of *unitary gates* applied to qubits. These unitary gates may either be local, acting on a

Figure 1: Quantum circuits representing the action of a Hadamard gate on a single qubit and a controlled-not gate on two qubits. The controlling qubit is denoted by a black dot, and the controlled qubit is denoted by the symbol $\oplus$.

single qubit, or non-local, acting on several qubits at a time. An important example of a local gate is given by the so-called Hadamard gate:

$$U_H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} , \tag{19}$$

which acts on the two-dimensional Hilbert space of a single qubit such that

$$\begin{aligned} U_H|0\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ U_H|1\rangle &= \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) . \end{aligned} \tag{20}$$

Also, an important example of a non-local gate is the controlled-not gate U_{CNOT}:

$$U_{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} , \tag{21}$$

acting on the four-dimensional Hilbert space of two qubits such that

$$\begin{aligned} U_{CNOT}|0,0\rangle &= |0,0\rangle \\ U_{CNOT}|0,1\rangle &= |0,1\rangle \\ U_{CNOT}|1,0\rangle &= |1,1\rangle \\ U_{CNOT}|1,1\rangle &= |1,0\rangle . \end{aligned} \tag{22}$$

In the example of the controlled-not gate, the first and second qubits are respectively called the *controlling qubit* and the *controlled qubit*, since the action of the gate on the second qubit depends on the value of the first one. It is possible to define more general *controlled gates* similarly to the controlled-not gate, namely, if the controlling qubit is in the state $|0\rangle$ nothing is done on the second one, whereas if the controlling qubit is in the state $|1\rangle$ then some local unitary gate acts on the second qubit. The application of the different unitary gates that define a quantum computation on a system of qubits can be represented in terms of *quantum circuits*, such as the ones from Fig.1 and Fig.2. In a quantum circuit each wire represents a qubit, and the time flows from left to right.

Independently of quantum circuits, it is possible to define alternative models to perform quantum computations, such as the adiabatic model of quantum optimization [16]. The adiabatic

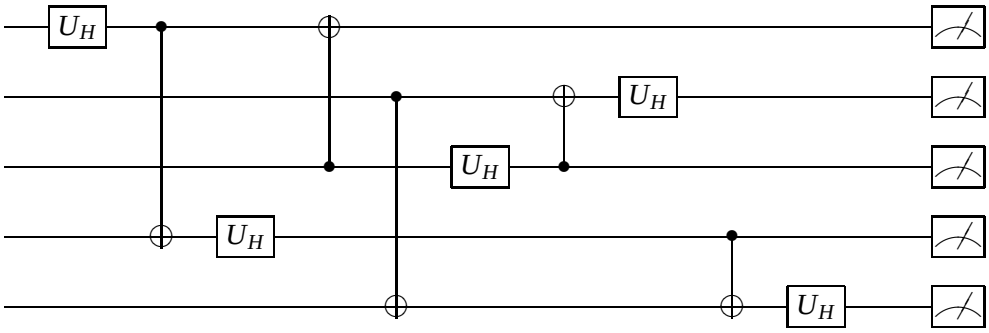

Figure 2: A possible quantum circuit of 5 qubits composed of Hadamard and controlled-not gates. Some measurements are performed on the qubits at the end of the quantum computation.

quantum algorithm deals with the problem of finding the ground state of a physical system represented by its Hamiltonian H_P. The basic idea is to perform an interpolation in time between some easy-to-build Hamiltonian H_0 and H_P, such that if the initial state of our system is a ground state of H_0, we may end up in a ground state of H_P with high probability after evolving for a certain amount of time, as long as some adiabaticity conditions are fulfilled. For example, we could consider the time-dependent Hamiltonian

$$H(t) = \left(1 - \frac{t}{T}\right) H_0 + \frac{t}{T} H_P \,, \tag{23}$$

where $t \in [0, T]$ is the time parameter, T being some computational interpolation time. If g_{min} represents the global minimum along the evolution of the energy gap between the ground state and the first excited state of the system, the adiabatic theorem implies that, if at $t = 0$ the system is at ground state of H_0, in order to be at the ground state of H_P at time T with high probability it is required that $T \sim 1/g_{min}^2$. The scaling properties with the size of the system of the minimum energy gap controls then the computational time of the quantum algorithm. Actually, the fact that the system evolves through a point of minimum gap implies that it approaches a quantum critical point, to be defined in what follows. A more detailed explanation of adiabatic quantum algorithms is given in Chapter 4.

Quantum criticality in quantum many-body systems

A *quantum phase transition* is a phase transition between different phases of matter at zero temperature. Contrary to classical (also called "thermal") phase transitions, quantum phase transitions are driven by the variation of some physical parameter, like a magnetic field. The transition describes an abrupt change in the properties of the ground state of the quantum system due to the effect of quantum fluctuations. The point in the space of parameters at which a quantum phase transition takes place is called the *critical point*, and separates quantum phases of different symmetry.

Some properties of the system may display a characteristic behavior at a quantum critical point. For instance, the correlators in a quantum many-body system may decay to zero

as a power-law at criticality, which implies a divergent correlation length and therefore scale-invariance, while decaying exponentially at off-critical regimes. Since quantum correlations are typically maximum at the critical point, some entanglement measures may have a divergence. The ground-state energy may display non-analyticities when approaching criticality, and the energy gap between the ground state and the first excited state of the system may close to zero. Our definition of quantum phase transition is very generic and does not necessarily involve all of the above behaviors. In fact, it is indeed possible to find quantum systems in which there is an abrupt change of the inner structure of the ground state that can be detected by some properties but not by others [17].

Let us give a simple example of a quantum critical point: consider the $(1+1)$-dimensional[a] ferromagnetic quantum Ising spin chain, as defined by the Hamiltonian

$$H = -J \sum_{i=1}^{N} \sigma_i^x \sigma_{i+1}^x - \sum_{i=1}^{N} \sigma_i^z \,, \tag{24}$$

where σ_i^α is the Pauli matrix α at site i of the chain, $J \geq 0$ is a coupling parameter, and N is the number of spins. At $J = \infty$ the ground state of the system is two-fold degenerate and consists of all the spins aligned ferromagnetically in the x-direction, being its subspace spanned by the two vectors $|+,+,\ldots,+\rangle$ and $|-,-,\ldots,-\rangle$, where $|+\rangle$ and $|-\rangle$ denote the two possible eigenstates of the pauli matrix σ^x. On the other hand, at $J = 0$ the ground state of the system consists of all the spins aligned along the z-direction, $|0,0,\ldots,0\rangle$, where $|0\rangle = \frac{1}{\sqrt{2}}(|+\rangle + |-\rangle)$. We now consider the behavior of the magnetization per particle of the ground state in the z-direction, as defined by the expected value $M \equiv \frac{<\sum_{i=1}^{N} \sigma_i^z>}{N}$. In the thermodynamic limit $N \to \infty$ this quantity tends to one when $J \to 0$, and tends to zero when $J \to \infty$. A detailed analysis of this model in this limit shows that there is a specific point at which the magnetization per particle has a sudden change, as is represented in Fig.3. This behavior implies that the model undergoes a second-order quantum phase transition at the critical point $J = J^* = 1$ in the thermodynamic limit.

One may wonder what is the symmetry that we are breaking in this simple example of a quantum phase transition: it is the symmetry $\mathbb{Z}_2$ that the Hamiltonian from Eq.24 has at high values of the coupling parameter. In fact, this symmetry could even be further broken when $J \to \infty$ if some extremely small magnetic field in the x-direction were present in our system, selecting one of the two possible ground states within this phase. In such a case, it is said that the symmetry of the Hamiltonian is *spontaneously broken*.

A useful tool in the study of quantum critical systems is the *renormalization group* [18, 19], which describes the way in which a theory gets modified under scale transformations. Given some Hamiltonian depending on a set of parameters, the transformations of the renormalization group define a flow in the parameter space, and in particular the fixed points of those transformations correspond to theories which are invariant under changes of scale. Indeed, the essence of the renormalization procedure is the elimination of degrees of freedom in the description of a system. This point of view is one of the basis for the development of different numerical tech-

[a] We use the field-theoretical notation $(1+1)$ to denote one spatial and one temporal dimension. Time is always to be kept fixed.

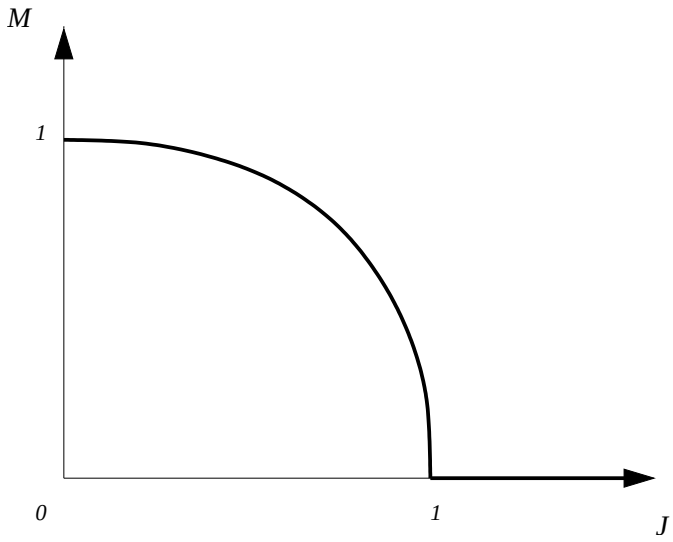

Figure 3: Magnetization per particle in the ferromagnetic quantum Ising spin chain as a function of the coupling parameter, in the thermodynamic limit. The point $J = J^* = 1$ corresponds to a second-order quantum phase transition point.

niques that allow to compute basic properties of quantum many-body systems, as is the case of the so-called *density matrix renormalization group* algorithm [20].

The behavior of many quantum critical models can also be explained by using tools from *conformal field theory* [21]. There are quantum many-body systems which can be understood as a regularization on a lattice of a quantum field theory, as is the case of the previously-discussed Ising quantum spin chain, which can be represented by the quantum field of a (1+1)-dimensional spinless fermion [22]. When those quantum many-body systems become critical, their description in terms of a quantum field theory allows to see that the symmetry group is not composed of only scale transformations, but of the full group of *conformal transformations*. In fact, conformal symmetry is particularly powerful when applied to (1 + 1)-dimensional quantum systems, allowing to determine almost all the basic properties of the model in consideration just by means of symmetry arguments. We perform some conformal field theory calculations in this thesis, and some basic technical background is given in Appendix B.

Experimental quantum computers

There will exist some day a quantum computer? This apparently simple question is by no means easy to answer. Actually, it is the opinion of some scientists that it is eventually impossible to build a quantum computer because of the unavoidable problem of the *decoherence* that any quantum system undergoes when it interacts with its environment. Nevertheless, other physicists think that these experimental drawbacks can be eventually in part ameliorated if the appropriate conditions are given. The main requirements that any experimental proposal must match if its purpose is to faithfully represent a quantum computer are known as the *DiVincenzo criteria* [23],

and so far there have been many different ideas to perform experimental quantum computation that try to fulfill as much as possible these conditions. Important proposals are those based on quantum optical devices, such as the *optical photon quantum computer*, *cavity quantum electrodynamics devices*, *optical lattices*, or *ion traps* [24]. The idea of performing quantum computation by means of *nuclear magnetic resonance* (NMR) has been considered as well [25–27]. Furthermore, proposals based on *superconductor devices*, *quantum dots* [28], and *doped semiconductors* [29, 30] have also been considered by different people. The future development of these and other experimental techniques, and to what extent they can implement a many-qubit quantum computer, remains yet uncertain. A detailed discussion about experimental quantum computation can be found for instance in [2].

What is this thesis about?

We focus here on the fields of quantum information science, condensed-matter physics, and quantum field theory. While these three branches of physics can be regarded as independent by themselves, there are clear overlaps among them, such that knowledge from one field benefits the others. As we said, conformal field theory [21] has helped to understand the universality classes of many critical (1 + 1)-dimensional quantum many-body systems. Also, the study of the entanglement present in the ground state of quantum Hamiltonians at a quantum phase transition shows direct analogies with those coming from the study of entropies in quantum field theory [31–44]. These results in turn connect with the performance of numerical techniques like the density matrix renormalization group [20], that allow to compute basic properties of some quantum many-body systems [45–60]. Indeed, quantum phase transitions are very much related to the model of adiabatic quantum computation [16, 61–71], which poses today challenges within the field of computational complexity [72].

The work that we present in this thesis tries to be at the crossover of quantum information science, quantum many-body physics, and quantum field theory. We use tools from these three fields to analyze problems that arise in the interdisciplinary intersection. More concretely, in Chapter 1 we consider the irreversibility of renormalization group flows from a quantum information perspective by using majorization theory and conformal field theory. In Chapter 2 we compute the entanglement of a single copy of a bipartite quantum system for a variety of models by using techniques from conformal field theory and Toeplitz matrices. The entanglement entropy of the so-called Lipkin-Meshkov-Glick model is computed in Chapter 3, showing analogies with that of (1+1)-dimensional quantum systems. In Chapter 4 we apply the ideas of scaling of quantum correlations in quantum phase transitions to the study of quantum algorithms, focusing on Shor's factorization algorithm and quantum algorithms by adiabatic evolution solving an NP-complete and the searching problems. Also, in Chapter 5 we use techniques originally inspired by condensed-matter physics to develop classical simulations, using the so-called matrix product states, of an adiabatic quantum algorithm. Finally, in Chapter 6 we consider the behavior of some families of quantum algorithms from the perspective of majorization theory.

The structure within each Chapter is such that the last section always summarizes the basic results. Some general conclusions and possible future directions are briefly discussed in Chapter 7. Appendix A, Appendix B and Appendix C respectively deal with some basic notions on majorization theory, conformal field theory, and classical complexity theory.

Chapter 1

Majorization along parameter and renormalization group flows

Is it possible to somehow relate physical theories that describe Nature at different scales? Say, given a theory describing Nature at high energies, we should demand that the effective low-energy behavior should be obtained by integrating out the high-energy degrees of freedom, thus getting a new theory correctly describing the low-energy sector of the original theory. This should be much in the same way as Maxwell's electromagnetism correctly describes the low-energy behavior of quantum electrodynamics.

This non-perturbative approach to the fundamental theories governing Nature was essentially developed by Wilson and is the key ingredient of the so-called renormalization group [18, 19, 73]: effective low-energy theories can be obtained from high-energy theories by conveniently eliminating the high-energy degrees of freedom. To be more precise, the renormalization group is the mechanism that controls the modification of a physical theory through a change of scale. Renormalization group transformations then define a flow in the space of theories from high energies (ultraviolet theories) to low energies (infrared theories). Actually, it is possible to extend this idea, and the renormalization procedure can be more generically understood as the *elimination of some given degrees of freedom* which we are not interested in because of some reason. The name "renormalization group" is used due to historical reasons, since the set of transformations does not constitute a formal group from a mathematical point of view.

Since the single process of integrating out modes seems to apparently be an irreversible operation by itself, one is naturally led to ask whether renormalization group flows are themselves irreversible. This question is in fact equivalent to asking whether there is a fundamental obstruction to recover microscopic physics from macroscopic physics, or more generally, whether there is a net information loss along renormalization group trajectories. While some theories may exhibit limit cycles in these flows, the question is under which conditions irreversibility remains. Efforts in this direction were originally carried by Wallace and Zia [74], while a key theorem was later proven by Zamolodchikov [75] in the context of (1+1)-dimensional quantum field theories: for every unitary, renormalizable, Poincaré invariant quantum field theory, there exists a universal c-function which decreases along renormalization group flows, while it is only stationary at (conformal) fixed points, where it reduces to the central charge c of the conformal

theory. This result sets an arrow on renormalization group flows, since it implies that a given theory can be the infrared (IR) realization of another ultraviolet (UV) theory only if their central charges satisfy the inequality $c_{IR} < c_{UV}$.

The following question then arises: "under which conditions irreversibility of renormalization group flows holds in higher dimensions?". This has been addressed from different perspectives [76–94]. It is our purpose here to provide a new point of view about this problem based on the accumulated knowledge from the field of quantum information science, by focusing first on the case of (1 + 1) dimensions.

An important application of quantum information to quantum many-body physics has been the use of majorization theory [11–14] in order to analyze the structure present in the ground state – also called vacuum – of some models along renormalization group flows. Following this idea, in [95] it was originally proposed that irreversibility along the flows may be rooted in properties concerning only the vacuum, without necessity of accessing the whole Hamiltonian of the system and its full tower of eigenstates. Such an irreversibility was casted into the idea of an *entanglement loss* along renormalization group flows, which proceeded in three constructive steps for (1+1)-dimensional quantum systems: first, due to the fact that the central charge of a (1+1)-dimensional conformal field theory is in fact a genuine measure of the bipartite entanglement present in the ground state of the system [36–44], there is a global loss of entanglement due to the *c*-theorem of Zamolodchikov [75]; second, given a splitting of the system into two contiguous pieces, there is a monotonic loss of entanglement due to the numerically observed monotonicity for the entanglement entropy between the two subsystems along the flow, decreasing when going away from the critical fixed – ultraviolet – point; third, this loss of entanglement is seen to be fine-grained, since it follows from a strict set of majorization ordering relations, numerically obeyed by the eigenvalues of the reduced density matrix of the subsystems. This last step motivated the authors of [95] to conjecture that there was a *fine-grained entanglement loss* along renormalization group flows rooted *only in properties of the vacuum*, at least for (1+1)-dimensional quantum systems. In fact, a similar fine-grained entanglement loss had already been numerically observed in [37, 38], for changes in the size of the bipartition described by the corresponding ground-state density operators, at conformally-invariant critical points.

The aim of this Chapter is to analytically prove relations between conformal field theory, renormalization group and entanglement. We develop, in the bipartite scenario, a detailed and analytical study of the majorization properties of the eigenvalue spectrum obtained from the reduced density matrices of the ground state for a variety of (1+1)-dimensional quantum models. Our approach is based on infinitesimal variations of the parameters defining the model – magnetic fields, anisotropies – or deformations in the size of the block L for one of the subsystems. We prove in these situations that there are strict majorization relations underlying the structure of the eigenvalues of the considered reduced density matrices or, in other words, that there is a fine-grained entanglement loss. The result of our study is presented in terms of two theorems. On the one hand, we are able to prove continuous majorization relations as a function of the parameters defining the model under study. Some of these flows in parameter space may indeed be understood as renormalization group flows for a particular class of integrable theories, like the Ising quantum spin chain. On the other hand, using the machinery of conformal field theory in the bulk we are able to prove exact continuous majorization relations in terms of deformations

of the size of the block L that is considered. We also provide explicit analytical examples for models with a boundary based on previous work of Peschel, Kaulke and Legeza [96–98].

1.1 Global, monotonous and fine-grained entanglement loss

Consider the pure ground state $|\Omega\rangle$ of a given regularized physical system which depends on a particular set of parameters, and let us perform a bipartition of the system into two pieces A and B. The density matrix for A, describing all the physical observables accessible to A, is given by $\rho_A = \mathrm{tr}_B(|\Omega\rangle\langle\Omega|)$ – and analogously for B –. Here we will focus our discussion on the density matrix for the subsystem A, so we will drop the subindex A from our notation. Let us consider a change in one of the parameters on which the resultant density matrix depends, say, parameter "t", which can be an original parameter of the system, or be related to the size of the region A. To be precise, we perform a change in the parameter space from t_1 to t_2, with $t_2 > t_1$. This involves a flow in the space of reduced density matrices from $\rho(t_1)$ to $\rho(t_2)$, as represented in Fig.1.1.

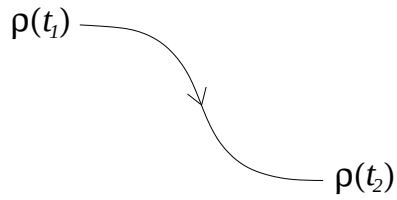

Figure 1.1: A flow in the space of density matrices, driven by parameter t.

We wish to understand how this variation of the parameter alters the inner structure of the ground state and, in particular, how it modifies the entanglement between the two partys, A and B. Because we are considering entanglement at two different points t_2 and t_1, let us assume that the entanglement between A and B is larger at the point t_1 than at the point t_2, so we have an entanglement loss when going from t_1 to t_2.

Our characterization of this entanglement loss will progress through three stages, refining at every step the underlying ordering of quantum correlations. These three stages will be respectively called *global*, *monotonous* and *fine-grained* entanglement loss.

Global entanglement loss.- A possible way to quantify the loss of entanglement between A and B when going from t_1 to t_2 is by means of the entanglement entropy $S(\rho(t)) = -\mathrm{tr}(\rho(t)\log_2\rho(t))$. Since at t_2 the two partys are less entangled than at t_1, we have that

$$S(\rho(t_1)) > S(\rho(t_2))\,, \tag{1.1}$$

which is a global assessment between points t_2 and t_1. This is what we shall call *global* entanglement loss.

Monotonous entanglement loss.- A more refined condition of entanglement loss can be obtained by imposing the monotonicity of the derivative of the entanglement entropy when varying the parameter "t". That is, the infinitesimal condition

$$S(\rho(t)) > S(\rho(t+dt)) \tag{1.2}$$

implies a stronger condition on the structure of the ground state under deformations of the parameter along the flow in t. This monotonic behavior of the entanglement entropy is what we shall call *monotonous* entanglement loss.

Fine-grained entanglement loss.- When monotonous entanglement loss holds, we can wonder whether the spectrum of $\rho(t)$ becomes more and more ordered as we change the value of the parameter. It is then plausible to ask if it is possible to make stronger claims than the inequalities given by Eq.1.1 and Eq.1.2 and unveil some richer structure. The finest notion of reordering when changing the parameter is then given by the monotonic majorization of the eigenvalue distribution along the flow. If we call $\vec{\rho}(t)$ the vector corresponding to the probability distribution of the spectrum arising from the density operator $\rho(t)$, then the infinitesimal condition

$$\vec{\rho}(t) \prec \vec{\rho}(t+dt) \tag{1.3}$$

along the flow in t reflects a strong ordering of the ground state along the flow. This is what we call *fine-grained* entanglement loss, because this condition involves a whole tower of inequalities to be simultaneously satisfied. This Chapter is devoted to this precise majorization condition in different circumstances when considering $(1+1)$-dimensional quantum systems. For background on majorization, see Appendix A.

1.2 Majorization along parameter flows in $(1+1)$-dimensional quantum systems

Our aim in this section is to study strict continuous majorization relations along parameter flows, under the conditions of monotonicity of the eigenvalues of the reduced density matrix of the vacuum in parameter space. Some of these flows indeed coincide with renormalization group flows for some integrable theories, as is the case of the Ising quantum spin chain.

Before entering into the main theorem of this section, let us perform a small calculation which will turn to be very useful: we want to compute the reduced density matrix for an interval of length L of the vacuum of a conformal field theory in $(1+1)$ dimensions – see Appendix B for background on conformal field theory –. With this purpose, let $Z_L(q) = q^{-c/12}\mathrm{tr}\left(q^{(L_0+\bar{L}_0)}\right)$ denote the partition function of a subsystem of size L [21, 36], where $q = e^{2\pi i\tau}$, $\tau = (i\pi)/(\ln(L/\eta))$, η being an ultraviolet cut-off, and L_0 and $\bar{L}_0$ the 0th Virasoro operators. Let $b \equiv c/12$ be a parameter that depends on the central charge and therefore on the universality class of the model. The unnormalized density matrix can then be written as $q^{-b}q^{(L_0+\bar{L}_0)}$, since it can be understood

as a propagator and $(L_0 + \bar{L}_0)$ is proportional to the generator of translations in time – which corresponds to dilatations in the conformal plane – [21]. Furthermore, we have that

$$\mathrm{tr}(q^{(L_0+\bar{L}_0)}) = 1 + n_1 q^{\alpha_1} + n_2 q^{\alpha_2} + \cdots , \tag{1.4}$$

due to the fact that the operator $(L_0 + \bar{L}_0)$ is diagonalized in terms of highest-weight states $|h, \bar{h}\rangle$: $(L_0+\bar{L}_0)|h, \bar{h}\rangle = (h+\bar{h})|h, \bar{h}\rangle$, with $h \geq 0$ and $\bar{h} \geq 0$; the coefficients $\alpha_1, \alpha_2, \ldots > 0$, $\alpha_i \neq \alpha_j \; \forall i \neq j$ are related to the eigenvalues of $(L_0 + \bar{L}_0)$, and $n_1, n_2, \ldots$ correspond to degeneracies. The normalized distinct eigenvalues of $\rho_L = \frac{1}{Z_L(q)} q^{-b} q^{(L_0+\bar{L}_0)}$ are then given by

$$\begin{aligned}
\lambda_1 &= \frac{1}{(1 + n_1 q^{\alpha_1} + n_2 q^{\alpha_2} + \cdots)} \\
\lambda_2 &= \frac{q^{\alpha_1}}{(1 + n_1 q^{\alpha_1} + n_2 q^{\alpha_2} + \cdots)} \\
&\vdots \\
\lambda_l &= \frac{q^{\alpha_{(l-1)}}}{(1 + n_1 q^{\alpha_1} + n_2 q^{\alpha_2} + \cdots)}.
\end{aligned} \tag{1.5}$$

We are now in conditions of introducing the main result of this section, which can be casted into the following theorem:

Theorem 1.1: *Consider a* (1 + 1)*-dimensional physical theory which depends on a set of real parameters* $\vec{g} = (g_1, g_2, \ldots)$*, such that*

- *there is a non-trivial conformal point* $\vec{g}^*$*, for which the model is conformally invariant in the bulk,*
- *the deformations from* $\vec{g}^*$ *in parameter space in the positive direction of a given unity vector* $\hat{e}$ *preserve part of the conformal structure of the model, that is, the eigenvalues of the generic reduced density matrices of the vacuum* $\rho(\vec{g})$ *are still of the form given by Eq.1.5 with some parameter-dependent factors* $q(\vec{g})$*, for values of the parameters* $\vec{g} = \vec{g}^* + a\hat{e}$*, and*
- *the factor* $q(\vec{g})$ *is a monotonic decreasing function along the direction of* $\hat{e}$*, that is, we demand that*

$$\hat{e} \cdot \left(\vec{\nabla}_{\vec{g}} q(\vec{g})\right) = \frac{\mathrm{d}q(\vec{g})}{\mathrm{d}a} \leq 0 \tag{1.6}$$

along the flow.

Then, away from the conformal point there is continuous majorization of the eigenvalues of the reduced density matrices of the ground state along the flow in the parameters $\vec{g}$ *in the positive direction of* $\hat{e}$ *(see Fig.1.2), that is,*

$$\begin{gathered}
\rho(\vec{g}_1) \prec \rho(\vec{g}_2) , \\
\vec{g}_1 = \vec{g}^* + a\hat{e},\; \vec{g}_2 = \vec{g}^* + a'\hat{e},\; a' \geq a .
\end{gathered} \tag{1.7}$$

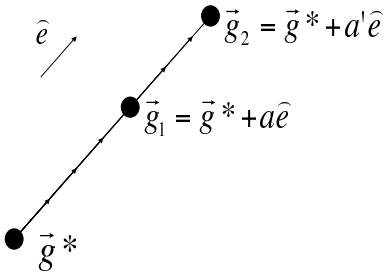

Figure 1.2: A possible flow in the space of parameters in the direction of $\hat{e}$.

Proof: Let us define the quantity $\tilde{Z}(q) \equiv (1 + n_1 q^{\alpha_1} + n_2 q^{\alpha_2} + \cdots)$, where it is assumed that $q = q(\vec{g})$, for values of $\vec{g}$ along the flow in a. Notice that at conformal points $\tilde{Z}(q(\vec{g}^*))$ is *not* invariant under modular transformations, as opposed to the partition function $Z(q(\vec{g}^*))$. The behavior of the eigenvalues in terms of deformations with respect to the parameter a follows from

$$\frac{\mathrm{d}\tilde{Z}(q)}{\mathrm{d}a} = \frac{\tilde{Z}(q) - 1}{q}\frac{\mathrm{d}q}{\mathrm{d}a} \leq 0 \,, \tag{1.8}$$

and therefore

$$\frac{\mathrm{d}\lambda_1}{\mathrm{d}a} = \frac{\mathrm{d}}{\mathrm{d}a}\left(\frac{1}{\tilde{Z}(q)}\right) \geq 0 \,. \tag{1.9}$$

Because λ_1 is always the largest eigenvalue $\forall a$, the first cumulant automatically satisfies continuous majorization along the considered flow. The variation of the other eigenvalues λ_l ($l > 1$) with respect to a reads as follows:

$$\begin{aligned} \frac{\mathrm{d}\lambda_l}{\mathrm{d}a} &= \frac{\mathrm{d}}{\mathrm{d}a}\left(\frac{q^{\alpha_{(l-1)}}}{\tilde{Z}(q)}\right) \\ &= \frac{q^{\alpha_{(l-1)}-1}}{\tilde{Z}(q)}\left(\alpha_{(l-1)} - \frac{\tilde{Z}(q) - 1}{\tilde{Z}(q)}\right)\frac{\mathrm{d}q}{\mathrm{d}a} \,. \end{aligned} \tag{1.10}$$

Let us concentrate on the behavior of the second eigenvalue λ_2. We observe that two different situations can happen:

- if

$$\left(\alpha_1 - \frac{\tilde{Z}(q) - 1}{\tilde{Z}(q)}\right) \geq 0 \,, \tag{1.11}$$

then since $\alpha_{(l-1)} > \alpha_1 \; \forall l > 2$, we have that

$$\left(\alpha_{(l-1)} - \frac{\tilde{Z}(q) - 1}{\tilde{Z}(q)}\right) > 0 \; \forall l > 2 \,, \tag{1.12}$$

which in turn implies that

$$\frac{\mathrm{d}\lambda_l}{\mathrm{d}a} \leq 0 \; \forall l \geq 2 \,. \tag{1.13}$$

From this we have that the second cumulant satisfies

$$\frac{\mathrm{d}(\lambda_1+\lambda_2)}{\mathrm{d}a} = -\frac{\mathrm{d}}{\mathrm{d}a}\left(\sum_{l>2}\lambda_l\right) \geq 0\,, \tag{1.14}$$

thus fulfilling majorization. The same conclusion extends easily in this case to all the remaining cumulants, and therefore majorization is satisfied by the whole probability distribution.

- if

$$\left(\alpha_1 - \frac{\tilde{Z}(q)-1}{\tilde{Z}(q)}\right) < 0\,, \tag{1.15}$$

then

$$\frac{\mathrm{d}\lambda_2}{\mathrm{d}a} > 0\,, \tag{1.16}$$

and therefore

$$\frac{\mathrm{d}(\lambda_1+\lambda_2)}{\mathrm{d}a} > 0\,, \tag{1.17}$$

so the second cumulant satisfies majorization, but nothing can be said from the previous three equations about the remaining cumulants.

Proceeding with this analysis for each one of the eigenvalues we see that, if these are monotonically decreasing functions of a then majorization is fulfilled for the particular cumulant under study, but since $\alpha_{i+1} > \alpha_i\ \forall i$ we notice that once the first monotonically increasing eigenvalue is found, majorization is directly satisfied by the whole distribution of eigenvalues, therefore $\rho(\vec{g}_1) \prec \rho(\vec{g}_2)$ if $\vec{g}_1 = \vec{g}^* + a\hat{e}$, $\vec{g}_2 = \vec{g}^* + a'\hat{e}$, and $a' \geq a$, as claimed. □

An interesting application of Theorem 1.1 comes whenever a can be related to the scale of a renormalization group transformation. Then it can be understood as a proof of fine-grained entanglement loss along a renormalization group flow for a particular set of integrable theories, namely, those theories which fulfill the hypothesis of our theorem. We stress that, while it would probably be possible to obtain results based on perturbation theory in the neighborhood of the conformal point for non-integrable theories, our theorem is based on the alternative approach of completely non-perturbative results under the assumption of integrability of the theory along the flow. This assumption is naturally fulfilled by many interesting models: we wish to illustrate this point with the analytical examples of similar situations for the Heisenberg and XY quantum spin chains with a boundary. At this point we wish to remark as well that, for those theories depending only on one parameter g, the monotonicity in the change of the parameter along a renormalization group flow between two fixed points is trivial, since between two zeros the β-function $\beta = -\frac{\mathrm{d}g}{\mathrm{d}\ln l}$, l being the scale of the renormalization group transformation, can only be either positive or negative, thus implying the monotonicity of the parameter when flowing from one fixed point to the other. Notice that our claim, which is majorization of the reduced density matrices of the vacuum, is stronger.

A majorization lemma

As a previous step in our derivations, let us state a useful lemma about majorization theory which we shall constantly use in the forthcoming sections. We refer the reader to Appendix A for mathematical definitions and more background on majorization theory. The lemma reads as follows:

Lemma 1.1 [95]: *If $\vec{p}_1 \prec \vec{p}_2$ and $\vec{q}_1 \prec \vec{q}_2$, then $(\vec{p}_1 \otimes \vec{q}_1) \prec (\vec{p}_2 \otimes \vec{q}_2)$. This means that majorization is preserved under the direct product operation.*

Proof: If $\vec{p}_1 \prec \vec{p}_2$ and $\vec{q}_1 \prec \vec{q}_2$ then $\vec{p}_1 = D_p \vec{p}_2$ and $\vec{q}_1 = D_q \vec{q}_2$ where D_p, D_q are both doubly stochastic matrices. Therefore $(\vec{p}_1 \otimes \vec{q}_1) = (D_p \otimes D_q)(\vec{p}_2 \otimes \vec{q}_2)$, where $(D_p \otimes D_q)$ is a doubly stochastic matrix in the direct product space, and so $(\vec{p}_1 \otimes \vec{q}_1) \prec (\vec{p}_2 \otimes \vec{q}_2)$. □

1.2.1 Quantum Heisenberg spin chain with a boundary

Consider the Hamiltonian of the Heisenberg quantum spin chain with a boundary

$$H = \sum_{i=1}^{\infty} \left(\sigma_i^x \sigma_{i+1}^x + \sigma_i^y \sigma_{i+1}^y + \Delta \sigma_i^z \sigma_{i+1}^z \right) , \tag{1.18}$$

where $\Delta \geq 1$ is the anisotropy parameter. This model is non-critical in the region defined by $\Delta > 1$ and critical at $\Delta = 1$. Notice that, since this is a uniparametric theory which can be mapped to a Gaussian free theory, any renormalization group transformation must be reflected in a change of the only existing parameter. Thus, the flow in Δ must necessarily coincide with a renormalization group flow.

From the pure ground state of the system, we trace out the $N/2$ contiguous spins $i = 1, 2, \ldots, N/2$, getting an infinite-dimensional density matrix ρ_Δ in the limit $N \to \infty$ which describes half of the system, and such that it can be written as a thermal density matrix of free fermions [96–98]. Its eigenvalues are given by

$$\begin{aligned} \rho_\Delta(n_0, n_1, \ldots, n_\infty) &= \frac{1}{Z_\Delta} e^{-\sum_{k=0}^{\infty} n_k \epsilon_k} \\ &= \rho_\Delta(n_0) \rho_\Delta(n_1) \cdots \rho_\Delta(n_\infty) , \end{aligned} \tag{1.19}$$

with $\rho_\Delta(n_k) = \frac{1}{Z_\Delta^k} e^{-n_k \epsilon_k}$, where $Z_\Delta^k = (1 + e^{-\epsilon_k})$ is the partition function for the mode k, $n_k = 0, 1$, for $k = 0, 1, \ldots, \infty$ and with dispersion relation

$$\epsilon_k = 2k \, \mathrm{arcosh}(\Delta) . \tag{1.20}$$

The physical branch of the function $\mathrm{arcosh}(\Delta)$ is defined for $\Delta \geq 1$ and is a monotonic increasing function of Δ. On top, the whole partition function Z_Δ can be decomposed as an infinite direct product of the different free fermionic modes:

$$Z_\Delta = \prod_{k=0}^{\infty} (1 + e^{-\epsilon_k}) . \tag{1.21}$$

From the last equations, it is not difficult to see that $\rho_\Delta \prec \rho_{\Delta'}$ if $\Delta \leq \Delta'$. Fixing the attention on a particular mode k, we evaluate the derivative of the largest probability for this mode, $P^k_\Delta = (1+e^{-\epsilon_k})^{-1}$. This derivative is seen to be

$$\frac{\mathrm{d}P^k_\Delta}{\mathrm{d}\Delta} = \frac{2k}{(1+e^{-\epsilon_k})^2\sqrt{\Delta^2-1}} > 0\,, \tag{1.22}$$

for $k = 1, 2, \ldots \infty$ and 0 for $k = 0$. It follows from this fact that all the modes independently majorize their respective probability distributions as Δ increases, with the peculiarity that the 0th mode remains unchanged along the flow, since its probability distribution is always $(\frac{1}{2}, \frac{1}{2})^T$. The particular behavior of this mode is responsible for the appearance of the "cat" state that is the ground state for large values of Δ – notice that in that limit the model corresponds to the quantum Ising model without magnetic field –. These results, together with the Lemma 1.1, make this example obey majorization along the flow in the parameter, which can indeed be understood as a renormalization group flow because of the reasons mentioned at the beginning of the example.

1.2.2 Quantum XY spin chain with a boundary

Similar results to the one obtained for the Heisenberg model can be obtained for a different model. Let us consider the quantum XY-model with a boundary, as described by the Hamiltonian

$$H = -\sum_{i=1}^{\infty}\left(\frac{(1+\gamma)}{2}\sigma_i^x\sigma_{i+1}^x + \frac{(1-\gamma)}{2}\sigma_i^y\sigma_{i+1}^y + \lambda\sigma_i^z\right)\,, \tag{1.23}$$

where γ can be regarded as the anisotropy parameter and λ as the magnetic field. The phase diagram of this model is shown in Fig.1.3, where one can see that there exist different critical regions depending on the values of the parameters, corresponding to different universality classes [37–40, 99]. Similarly to the previous example, this model is integrable and can be mapped to a Gaussian free theory with a mass parameter depending on a particular combination of both λ and γ once the kinetic term has been properly normalized (see [22]). A renormalization group flow can then be understood as a set of flows in the plane of λ and γ.

Consider the ground state of Eq.1.23, and trace out the contiguous spins $i = 1, 2, \ldots, N/2$ in the limit $N \to \infty$. The resulting density matrix $\rho_{(\lambda,\gamma)}$ can be written as a thermal state of free fermions, and its eigenvalues are given by [96–98]:

$$\rho_{(\lambda,\gamma)}(n_0, n_1, \ldots, n_\infty) = \frac{1}{Z_{(\lambda,\gamma)}}e^{-\sum_{k=0}^{\infty} n_k\epsilon_k}\,, \tag{1.24}$$

where $n_k = 0, 1$, and the single-mode energies ϵ_k are given by

$$\epsilon_k = \begin{cases} 2k\epsilon\,, & \text{if } \lambda < 1 \\ (2k+1)\epsilon\,, & \text{if } \lambda > 1\,, \end{cases} \tag{1.25}$$

with $k = 0, 1, \ldots, \infty$. The parameter ϵ is defined by the relation

$$\epsilon = \pi\frac{I(\sqrt{1-x^2})}{I(x)}\,, \tag{1.26}$$

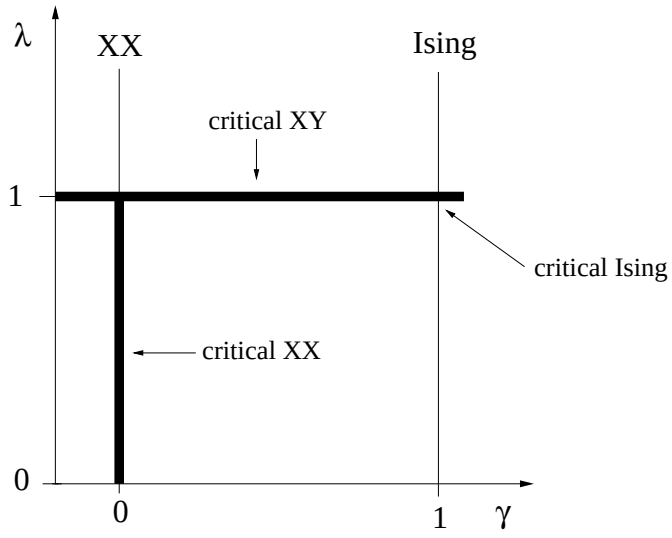

Figure 1.3: Phase diagram of the quantum XY-model.

$I(x)$ being the complete elliptic integral of the first kind

$$I(x) = \int_0^{\pi/2} \frac{d\theta}{\sqrt{1 - x^2 \sin^2(\theta)}} \tag{1.27}$$

and x being given by

$$x = \begin{cases} (\sqrt{\lambda^2 + \gamma^2 - 1})/\gamma \,, & \text{if } \lambda < 1 \\ \gamma/(\sqrt{\lambda^2 + \gamma^2 - 1}) \,, & \text{if } \lambda > 1 \,, \end{cases} \tag{1.28}$$

where the condition $\lambda^2 + \gamma^2 > 1$ is assumed for a correct behavior of the above expressions (external region of the Baruoch-McCoy circle [99]).

We observe that the probability distribution defined by the eigenvalues of $\rho_{(\lambda,\gamma)}$ is again the direct product of distributions for each one of the separate modes. Therefore, in order to study majorization we can focus separately on each one of these modes, in the same way as we already did in the previous example. We wish now to consider our analysis in terms of the flows with respect to the magnetic field λ and with respect to the anisotropy γ in a separate way. Other trajectories in the parameter space may induce different behaviors, and a trajectory-dependent analysis should then be considered for each particular case.

Flow along the magnetic field λ

We consider in this subsection a fixed value of γ while the value of λ changes, always fulfilling the condition $\lambda^2 + \gamma^2 > 1$. Therefore, at this point we can drop γ from our notation. We separate the analysis of majorization for the regions $1 < \lambda < \infty$ and $+\sqrt{1 - \gamma^2} < \lambda < 1$ for reasons that will become clearer during the study example but that already can be realized just by looking at the phase space structure in Fig.1.3.

Region $1 < \lambda < \infty$**.-** We show that $\rho_\lambda \prec \rho_{\lambda'}$ if $\lambda \leq \lambda'$. In this region of parameter space, the largest probability for the mode k is $P^k_\lambda = (1+e^{-\epsilon_k})^{-1}$. The variation of P^k_λ with respect to λ is

$$\frac{\mathrm{d}P^k_\lambda}{\mathrm{d}\lambda} = \frac{(2k+1)e^{-(2k+1)\epsilon}}{\left(1+e^{-(2k+1)\epsilon}\right)^2}\frac{\mathrm{d}\epsilon}{\mathrm{d}\lambda}\,. \tag{1.29}$$

A direct computation using Eq.1.26, Eq.1.27 and Eq.2.43 shows that $\frac{\mathrm{d}\epsilon}{\mathrm{d}\lambda} > 0$. Therefore, $\frac{\mathrm{d}P^k_\lambda}{\mathrm{d}\lambda} > 0$ for $k = 0, 1, \ldots, \infty$. This derivation shows mode-by-mode majorization when λ increases. Combining this result with the Lemma 1.1, we see that this example obeys majorization.

Region $+\sqrt{1-\gamma^2} < \lambda < 1$**.-** For this case, we show that $\rho_\lambda \prec \rho_{\lambda'}$ if $\lambda \geq \lambda'$. In particular, the probability distribution for the 0th fermionic mode remains constant and equal to $(\frac{1}{2}, \frac{1}{2})^T$, which brings again a "cat" state for low values of λ. Similarly to the latter case, the largest probability for mode k is $P^k_\lambda = (1+e^{-\epsilon_k})^{-1}$, with

$$\epsilon_k = 2k\pi\frac{I(\sqrt{1-x^2})}{I(x)} = 2k\epsilon\,, \tag{1.30}$$

and $x = (\sqrt{\lambda^2+\gamma^2-1})/\gamma$. Its derivative with respect to λ is

$$\frac{\mathrm{d}P^k_\lambda}{\mathrm{d}\lambda} = \frac{2ke^{-2k\epsilon}}{\left(1+e^{-2k\epsilon}\right)^2}\frac{\mathrm{d}\epsilon}{\mathrm{d}\lambda}\,. \tag{1.31}$$

It is easy to see that this time $\frac{\mathrm{d}\epsilon}{\mathrm{d}\lambda} < 0$, and therefore $\frac{\mathrm{d}P^k_\lambda}{\mathrm{d}\lambda} < 0$ for $k = 1, 2, \ldots, \infty$, which brings majorization individually for each one of these modes when λ decreases. The mode $k = 0$ calls for special attention. From Eq.1.31 it is seen that $\frac{\mathrm{d}P^{k=0}_\lambda}{\mathrm{d}\lambda} = 0$, therefore the probability distribution for this mode remains equal to $(\frac{1}{2}, \frac{1}{2})^T$ all along the flow. This is a marginal mode that brings the system to a "cat" state that appears as ground state of the system for low values of λ. Notice that this peculiarity is rooted on the particular form of the dispersion relation given in Eq.1.25, which is proportional to $2k$ instead of $2k+1$ for this region in parameter space. These results, together with the Lemma 1.1, prove that this example also fulfills majorization.

Flow along the anisotropy γ

In this subsection, the magnetic field λ is fixed and the anisotropy γ is the only free parameter of the model, still fulfilling $\lambda^2+\gamma^2 > 1$. Thus, at this point we can drop λ from our notation. We will see that $\rho_\gamma \prec \rho_{\gamma'}$ if $\gamma \geq \gamma'$, in the two regions $1 < \lambda < \infty$ and $+\sqrt{1-\gamma^2} < \lambda < 1$. In particular, in the region $+\sqrt{1-\gamma^2} < \lambda < 1$, the probability distribution for the 0th fermionic mode remains constant and equal to $(\frac{1}{2}, \frac{1}{2})^T$. Let us consider the biggest probability for the mode k, $P^k_\gamma = (1+e^{-\epsilon_k})^{-1}$, with $\epsilon_k = \omega\epsilon$, where

$$\omega = \begin{cases} 2k\,, & \text{if } \lambda < 1 \\ (2k+1)\,, & \text{if } \lambda > 1\,, \end{cases} \tag{1.32}$$

and ϵ as defined in the preceding sections. It is easy to verify that

$$\frac{\mathrm{d}P_\gamma^k}{\mathrm{d}\gamma} = \frac{\omega e^{-\omega\epsilon_k}}{(1+e^{-\omega\epsilon_k})^2}\frac{\mathrm{d}\epsilon}{\mathrm{d}x}\frac{\mathrm{d}x}{\mathrm{d}\gamma} < 0 \tag{1.33}$$

for $k = 0, 1, \ldots, \infty$ if $\lambda > 1$ and for $k = 1, 2, \ldots, \infty$ if $\lambda < 1$. The mode $k = 0$ for $\lambda < 1$ needs of special attention, since $\frac{\mathrm{d}P_\lambda^{k=0}}{\mathrm{d}\lambda} = 0$, and therefore the probability distribution for this mode remains constant and equal to $(\frac{1}{2}, \frac{1}{2})^T$ all along the flow. These results, together with the Lemma 1.1, show that this case obeys again majorization along the flow in the parameter.

1.3 Majorization with L in $(1+1)$-dimensional conformal field theories

A similar study to the one presented in the previous section about majorization along flows in parameter space can be now performed exclusively at the conformal point for flows in the size of the block under consideration. Here we present an analytical derivation of majorization relations for any $(1+1)$-dimensional conformal field theory without boundaries – or in the bulk[a] – in the bipartite scenario when the size of the considered subsystems changes, that is to say, under deformations in the interval of the accessible region for one of the two partys. This size will be represented by the length L of the space interval for which we consider the reduced density matrix ρ_L after tracing out all the degrees of freedom corresponding to the rest of the universe. Our main result in this section can be casted into the following theorem:

Theorem 1.2: *$\rho_L \prec \rho_{L'}$ if $L \geq L'$ for all possible $(1+1)$-dimensional conformal field theories in the bulk.*

Proof: Since the factors q are now monotonic functions of the size of the interval L, the proof of this theorem is analogous to the proof of Theorem 1.1, with the only exception that now the cumulants are monotonically decreasing (instead of increasing) functions along the flow in L. Taking this into account, it immediately follows that $\rho_L \prec \rho_{L'}$ if $L \geq L'$. This proof is valid for all possible $(1+1)$-dimensional conformal field theories in the bulk, since it only relies on completely general assumptions. □

1.3.1 Critical quantum XX spin chain with a boundary

Let us give an example of a similar situation to the one presented in Theorem 1.2 for the particular case of the quantum XX-model with a boundary, for which the exact spectrum of ρ_L can be explicitly computed. The Hamiltonian of the model without magnetic field is given by

$$H = \sum_{i=1}^{\infty}(\sigma_i^x\sigma_{i+1}^x + \sigma_i^y\sigma_{i+1}^y). \tag{1.34}$$

[a]The case in which boundaries are present in the system must be properly considered from the point of view of the so-called *boundary* conformal field theory. This has been done by H.Q. Zhou et *al.* in [100]. For technical background on conformal field theory without boundaries, see Appendix B.

The system as described by this model is critical since it is gapless. Notice that the ultraviolet cut-off coincides with the lattice spacing and the theory is naturally regularized, hence $\eta = 1$. Taking the ground state and tracing out all but a block of $1, 2, \ldots, L$ contiguous spins, the density matrix ρ_L describing this block can be written, in the large-L limit, as a thermal state of free fermions [96–98]:

$$\rho_L = \frac{e^{-H'}}{Z_L}, \tag{1.35}$$

Z_L being the partition function for a given L, $H' = \sum_{k=0}^{L-1} \epsilon_k d_k^\dagger d_k$, with fermionic creation and annihilation operators $d_k^\dagger$, d_k and dispersion relation

$$\epsilon_k = \frac{\pi^2}{2\ln L}(2k+1) \quad k = 0, 1, \ldots, L-1 \, . \tag{1.36}$$

The eigenvalues of the density matrix ρ_L can then be written in terms of non-interactive fermionic modes

$$\begin{aligned} \rho_L(n_0, n_1, \ldots, n_{L-1}) &= \frac{1}{Z_L} e^{-\sum_{k=0}^{L-1} n_k \epsilon_k} \\ &= \rho_L(n_0) \cdots \rho_L(n_{L-1}) \, , \end{aligned} \tag{1.37}$$

with $\rho(n_k) = \frac{1}{Z_L^k} e^{-n_k \epsilon_k}$, where $Z_L^k = (1 + e^{-\epsilon_k})$ is the partition function for the mode k, and $n_k = 0, 1$, $\forall k$. It is worth noticing that the partition function of the whole block Z_L factorizes as a product over the L modes:

$$Z_L = \prod_{k=0}^{L-1} (1 + e^{-\epsilon_k}) \, . \tag{1.38}$$

Once the density matrix of the subsystem is well characterized with respect to its size L, it is not difficult to prove that $\rho_L \prec \rho_{L'}$ if $L \geq L'$. In order to see this, we will fix our attention on the majorization within each mode and then we will apply Lemma 1.1 for the whole subsystem. We initially have to observe the behavior in L of the largest probability defined by each individual distribution for each one of the modes, that is, $P_L^k = 1/Z_L^k = (1 + e^{-\epsilon_k})^{-1}$, for $k = 0, 1, \ldots, L-1$. It is straightforward to see that

$$\frac{\mathrm{d}P_L^k}{\mathrm{d}L} = \frac{e^{-\epsilon_k}}{(1 + e^{-\epsilon_k})^2} \frac{\mathrm{d}\epsilon_k}{\mathrm{d}L} < 0 \, , \tag{1.39}$$

which implies that P_L^k decreases if L increases $\forall k$. This involves majorization within each mode $k = 0, 1, \ldots, L-2$ when decreasing L by one unit. In addition, we need to see what happens with the last mode $k = L-1$ when the size of the system is reduced from L to $L-1$. Because this mode disappears for the system of size $L-1$, its probability distribution turns out to be represented by the probability vector $(1, 0)^T$, which majorizes any probability distribution of two components. Combining these results with Lemma 1.1, we see that this example for the quantum XX-model provides a similar situation for a model with a boundary to the one presented in Theorem 1.2.

1.4 Conclusions of Chapter 1

In this Chapter we have analyzed majorization relations along parameter and renormalization group flows for a variety of models in (1 + 1) dimensions. We have also provided in a rigorous way explicit and detailed proofs for all the majorization conjectures raised in some papers on quantum spin chains [37, 38, 95]. In order to be more specific:

- We have proven the existence of a fine-grained entanglement loss for (1 + 1)-dimensional quantum systems along uniparametric flows, when perturbations in parameter space preserve part of the conformal structure of the partition function, and some monotonicity conditions hold as well. These flows may coincide with renormalization group flows in some cases. We also considered similar situations which can be treated analytically, arising in the Heisenberg and XY models with a boundary.

- We have also developed a completely general proof of majorization relations underlying the structure of the vacuum with respect to the size of the block L for all possible (1 + 1)-dimensional conformal field theories in the bulk. An example of a similar situation has been considered for the particular case of the XX-model with a boundary.

These results provide solid mathematical grounds for the existence of majorization relations along renormalization group flows underlying the structure of the vacuum of (1+1)-dimensional quantum spin chains. It would be interesting to relate the results of this Chapter to possible extensions of the c-theorem [75] to systems with more than (1 + 1) dimensions. While other approaches are also possible [76–88], majorization may be a unique tool in order to assess irreversibility of renormalization group flows in terms of properties of the vacuum only, and some numerical results in this direction have already been observed in systems of different dimensionality for flows in the parameter space [101, 102]. The analytical derivation and the consideration of the consequences for higher-dimensional systems of the properties presented here for (1 + 1) dimensions remains an open problem.

Chapter 2

Single-copy entanglement in (1 + 1)-dimensional quantum systems

How much entanglement is contained in a given quantum many-body system? This simple but fundamental question has been considered for systems close to and at quantum phase transitions by means of analyzing very different entanglement measures [17, 31, 36–44, 56, 103–118]. All these different ways of measuring entanglement lead to results which complement each other and which help us to understand the precise way in which the ground state of critical models is organized. While the concurrence measures the pairwise entanglement that is present in the system between two of its specific constituents [119], the entanglement entropy measures the entanglement that appears between two different blocks in a bipartition, in turn showing very interesting connections to the entropic area law found for systems such as black holes [31–35]. A detailed analysis of the entanglement entropy in critical quantum spin chains unveils a universal logarithmic scaling law with the size of the block under consideration, which admits an explanation in terms of the underlying conformal field theory in (1 + 1) dimensions [36–44]. Furthermore, it is now well understood that the good performance of density matrix renormalization group algorithms in (1 + 1) dimensions relies very much on this property[a] [56].

Our aim in this Chapter is to study an entanglement measure which, very much like the entanglement entropy, is proven to have intriguing scaling properties for (1 + 1)-dimensional quantum systems. We call this measure *single-copy entanglement* [113, 120], and its operational definition comes naturally motivated by a practical reason: while the entanglement entropy measures the average amount of entanglement possible to be distilled from a bipartite system in the limit of having an infinite number of copies of the system [121], the single-copy entanglement measures the amount of entanglement present in the more realistic case of having just *one* copy of the system, in a way to be precisely defined later. As we shall see, we are able to *analytically* compute the asymptotic leading scaling behavior of the single-copy entanglement for all (1 + 1)-dimensional conformal field theories in the bulk, together with its first-order correction. At that point in our derivations a surprise will appear: the entanglement contained in a single specimen of a critical (1 + 1)-dimensional system is seen to be, asymptotically, *half* the entanglement that

[a] The relation between scaling of entanglement and the performance of classical numerical simulations for different quantum systems will be addressed in detail in Chapters 4 and 5.

is available in the ideal case of having an infinite number of copies. This result is reinforced by an analysis from the point of view of quasi-free fermionic systems in $(1+1)$ dimensions which leads again to similar conclusions: whenever the entanglement entropy scales logarithmically in the size of the system, the single-copy entanglement scales asymptotically as half of the entanglement entropy. Furthermore, and in order to make our study more complete, we also analyze the behavior of single-copy entanglement away from criticality for the specific example of the XY quantum spin chain. Let us then begin our study by formally defining what the single-copy entanglement is.

2.1 Operational definition of the single-copy entanglement

Let us ask ourselves the following question: how much entanglement is contained in an infinite number of copies of a pure bipartite system $|\psi_{AB}\rangle$? Let us be more specific with the term "how much", by posing the question differently: what is the maximal rate at which EPR-pairs $\frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B)$ can be distilled from an infinite number of copies of a pure bipartite system $|\psi_{AB}\rangle$, just by invoking local operations and classical communication (LOCC) between the two parties? The answer to this question was originally found by Bennett et *al.* in [121]: if we are able to distill M EPR-pairs from N copies of a pure bipartite system $|\psi_{AB}\rangle$, the rate M/N coincides, in the infinite-copy limit, with the entanglement entropy between the two partys, namely

$$\lim_{N\to\infty} \frac{M}{N} = S(\rho_A) = -\mathrm{tr}(\rho_A \log_2 \rho_A) = S(\rho_B) = -\mathrm{tr}(\rho_B \log_2 \rho_B)\,, \tag{2.1}$$

ρ_A and ρ_B respectively being the reduced density matrices of the two partys A (Alice) and B (Bob). This situation corresponds to the one represented in Fig.2.1.

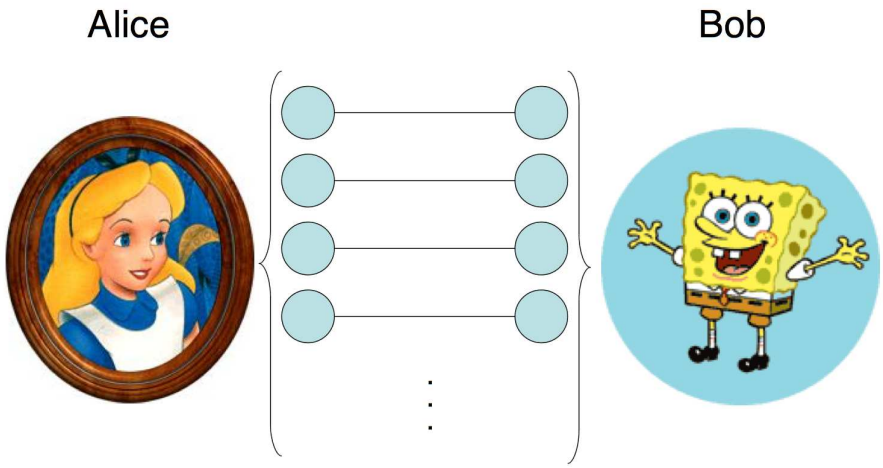

Figure 2.1: Scenario defining the entanglement entropy. Alice and Bob share an infinite number of copies of the bipartite system, and wish to distill EPR-pairs by performing LOCC.

While the above definition of entanglement entropy obviously makes sense, having an infinite number of copies of the system at hand is an unrealistic situation from the experimental point of view. Thus, let us now ask ourselves this variant of the above original question: how much entanglement is contained in a single specimen of a pure bipartite system $|\psi_{AB}\rangle$? Or, equivalently, what is the largest entanglement content that any apparatus could potentially distill by LOCC from just one bipartite entangled system at hand? This scenario is represented in Fig.2.2.

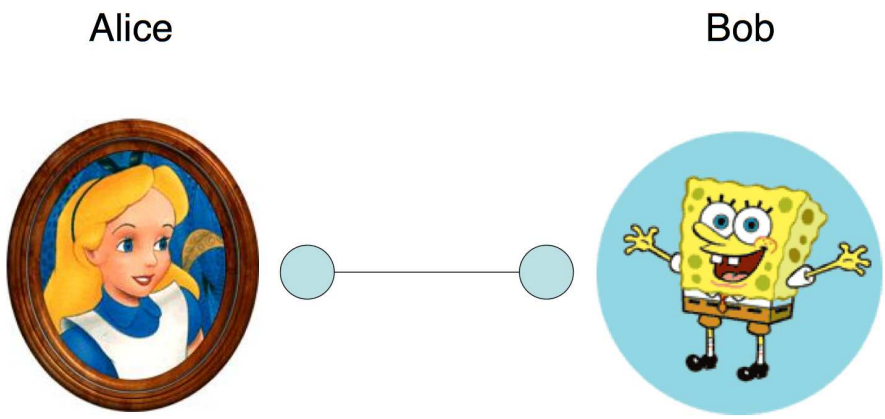

Figure 2.2: Scenario defining the single-copy entanglement. Alice and Bob share only one copy of the bipartite system, and wish to distill a maximally entangled state of the largest possible dimension by performing LOCC.

The maximum entanglement that it is possible to obtain by distillation with LOCC in the single-copy case can be measured by the largest dimension of a maximally entangled state that can be distilled with certainty from the single specimen. That is, for a pure bipartite state $|\psi_{AB}\rangle$ with reduced density matrices ρ_A and ρ_B, we write for the single-copy entanglement

$$E_1(\rho_A) = E_1(\rho_B) = \log_2(M) \tag{2.2}$$

if

$$|\psi_{AB}\rangle \longmapsto |\psi_M\rangle \text{ under LOCC}\,, \tag{2.3}$$

where

$$|\psi_M\rangle \equiv \frac{1}{\sqrt{M}} \sum_{q=1}^{M} |q\rangle_A |q\rangle_B \tag{2.4}$$

is a maximally entangled state of dimension M. Now, we recall the result that the interconversion of bipartite pure states under LOCC in the single-copy case is governed by the following majorization relation for the reduced density matrices [15]:

$$|\psi_{AB}\rangle \longrightarrow |\widetilde{\psi}_{AB}\rangle \text{ under LOCC} \iff \rho_A \prec \widetilde{\rho}_A\,, \tag{2.5}$$

where $\widetilde{\rho}_A$ is the reduced density matrix of the converted state $|\widetilde{\psi}_{AB}\rangle$ for the party A[b]. Replacing in the above condition $|\widetilde{\psi}_{AB}\rangle = |\psi_M\rangle$ and $\widetilde{\rho}_A = \frac{1}{M}\mathbb{I}_M$, $\mathbb{I}_M$ being the $M \times M$ identity matrix, and considering the definition of majorization between probability distributions in terms of a set of inequalities to be satisfied by partial sums of its components – see Appendix A –, we find the inequality

$$\lambda_1 \leq \frac{1}{M} \Rightarrow M \leq \frac{1}{\lambda_1} , \tag{2.6}$$

λ_1 being the largest eigenvalue of ρ_A. Given the above upper bound for M, one finds that

$$E_1(\rho_A) = -\log_2 \lambda_1 = E_1(\rho_B) . \tag{2.7}$$

Therefore, the single-copy entanglement can be directly computed by looking only at the *largest eigenvalue* of the reduced density matrix of the system under consideration. This situation is very different from that of the entanglement entropy, where all the eigenvalues of the reduced density matrix contribute to the final quantity.

2.2 Exact conformal field theoretical computation

Now we wish to show the exact and analytical computation of the single-copy entanglement in the case of (1 + 1)-dimensional conformal field theories in the bulk. We remind that the systems described by these theories correspond to the continuum limit of a variety of regularized quantum critical theories defined on a chain. For technical background, see Appendix B.

As we saw in the previous Chapter, the reduced density matrix for a block of size L describing the vacuum of a (1 + 1)-dimensional conformal field theory can be written as [21, 36, 112]

$$\rho_L = \frac{1}{Z_L(q)} q^{-c/12} q^{(L_0+\bar{L}_0)} , \tag{2.8}$$

where c is the central charge of the theory, L_0 and $\bar{L}_0$ are the 0th holomorphic and antiholomorphic Virasoro operators, $Z_L(q)$ is the partition function, $q = e^{2\pi i\tau}$, and $\tau = (i\pi)/(\ln(L/\eta))$, η being a regularization ultraviolet cut-off. For critical quantum chains we have that $\eta = 1$, which corresponds to the lattice spacing, and which is to be understood in our forthcoming calculations.

The largest eigenvalue of the density matrix ρ_L corresponds to the zero mode of $(L_0 + \bar{L}_0)$, that is,

$$\lambda_1 = \frac{1}{Z_L(q)} q^{-c/12} , \tag{2.9}$$

since for this mode $|0\rangle$ we have that $(L_0 + \bar{L}_0)|0\rangle = 0$. We then get a first expression for the single-copy entanglement:

$$E_1(\rho_L) = -\log_2 \lambda_1 = \log_2 \left(Z_L(q) q^{c/12} \right) . \tag{2.10}$$

[b] Of course the same relation holds as well for the party B.

The leading behavior for the partition function can be computed when L is large by taking advantage of its invariance under modular transformations. The needed transformation corresponds to $\tau \to -1/\tau$, which amounts to $Z_L(q) = Z_L(\tilde{q})$, $q = e^{-2\pi^2/\ln L}$, $\tilde{q} = e^{-2\ln L} = 2^{-2\log_2 L}$. It is now possible to expand the partition function in powers of $\tilde{q}$, since all the eigenvalues of the operator $(L_0 + \bar{L}_0)$ are positive, and find that the leading contribution originates from the central charge:

$$\log_2 Z_L(\tilde{q}) = -\frac{c}{12}\log_2 \tilde{q} + O\left(\frac{1}{L}\right) = \frac{c}{6}\log_2 L + O\left(\frac{1}{L}\right) . \tag{2.11}$$

This result translates into an explicit expression for the single-copy entanglement

$$E_1(\rho_L) = \frac{c}{6}\log_2 L - \frac{c}{6}\frac{(\pi \log_2 e)^2}{\log_2 L} + O\left(\frac{1}{L}\right) . \tag{2.12}$$

We wish to point out that the above result is exact up to polynomial corrections in $1/L$ since no further powers of $1/\log_2 L$ appear in the expansion when L is large.

Similar conformal field theory manipulations were used to prove that the von Neumann entropy for the same reduced density matrix ρ_L is given by [36]

$$S(\rho_L) = -\frac{c}{6}\log_2 \tilde{q} + O\left(\frac{1}{L}\right) , \tag{2.13}$$

which implies the following direct relation between entropy and single-copy entanglement:

$$E_1(\rho_L) = \frac{1}{2}S(\rho_L) - \frac{c}{6}\frac{(\pi \log_2 e)^2}{\log_2 L} + O\left(\frac{\log_2 L}{L}\right) , \tag{2.14}$$

where the last subleading correction is easily calculated by comparing the results from [36] and our expression given in Eq.2.12. It should be noted here that the above result completely fixes the leading eigenvalue of the reduced density matrix of the block of size L to be dictated by its entropy within the large-L limit, that is,

$$\lim_{L\to\infty}\left(\frac{\lambda_1}{2^{S(\rho_L)/2}}\right) = 1 . \tag{2.15}$$

Corrections to this limit can be obtained from Eq.2.14. Quite remarkably, we also notice that all the eigenvalues will inherit the same leading behavior and differ by their subleading corrections controlled by the conformal weights corresponding to the universality class of the particular model in consideration.

2.3 Exact computation in quasi-free fermionic quantum spin chains

We aim now to reinforce the previously achieved result by investigating the same question from an alternative point of view, namely, we investigate all translationally invariant quantum spin models which can, under a Jordan-Wigner transformation, be written as an isotropic quadratic Hamiltonian in fermionic operators.

The Jordan-Wigner transformation relates the Pauli operators in the quantum spin system to spinless fermionic operators $\{c_j\}$ obeying the fermionic anticommutation relations

$$\begin{aligned} \{c_j, c_k\} &= 0 \\ \{c_j^\dagger, c_k^\dagger\} &= 0 \\ \{c_j^\dagger, c_k\} &= \delta_{jk} \,, \end{aligned} \tag{2.16}$$

according to

$$\begin{aligned} \sigma_l^x &= \frac{1}{2}\prod_{n=1}^{l-1}(1-2c_n^\dagger c_n)(c_l^\dagger + c_l) \\ \sigma_l^y &= \frac{1}{2i}\prod_{n=1}^{l-1}(c_l^\dagger - c_l)(1-2c_n^\dagger c_n) \\ \sigma_l^z &= c_l^\dagger c_l - \frac{1}{2} \,. \end{aligned} \tag{2.17}$$

Consider now an infinite quantum spin system in $(1+1)$ dimensions that corresponds to a general translationally invariant isotropic quasi-free fermionic model. These correspond to chain systems whose Hamiltonian can be cast into the form

$$H = \sum_{l,k} c_l^\dagger A_{l-k} c_k \tag{2.18}$$

with $A_l = A_{-l} \in \mathbb{R}$. The ground state of H is a quasi-free fermionic state, that is, a state that is completely characterized by the second moments of the fermionic operators. Notice that, while some of the spin chains described by this setting can be considered as well within the framework of conformal field theory in $(1+1)$ dimensions, there may also be models that do not correspond to any such conformal field theory.

Our claim is the following: if the entropy of entanglement satisfies

$$S(\rho_L) = \xi \log_2(L) + O(1) \,, \tag{2.19}$$

for some $\xi > 0$, then the single-copy entanglement satisfies

$$E_1(\rho_L) = \frac{1}{2} S(\rho_L) + O(1) \,. \tag{2.20}$$

That is, if we find that the entropy of entanglement scales asymptotically as the logarithm of L – as typically observed for this class of systems at criticality – then we can infer that the leading behavior of the single-copy entanglement will asymptotically be exactly one half of it. Notice that this does not fix such a relationship in the case that, for example, the system is gapped and the entropy of entanglement saturates (we shall consider an example of non-critical behavior within the next section). Let us now show how we arrive to the previous statement.

The reduced state of a block of length L is entirely specified by the eigenvalues of the real symmetric $L\times L$ Toeplitz matrix T_L, with l-th row being given by $(t_{-l+1}, t_{-l+2}, ..., t_0, ..., t_{L-l})$. The latter numbers are for an infinite quasi-free fermionic quantum chain found to be

$$t_l = \frac{1}{2\pi}\int_0^{2\pi} g(k)e^{-ilk}dk\,, \tag{2.21}$$

where $g : \mathbb{C} \to \mathbb{C}$ is the so-called symbol [99, 122, 123], which essentially characterizes the fermionic model. The fact that T_L is a Toeplitz matrix reflects the translational invariance of the model. The real eigenvalues of T_L will be labeled as $\mu_1, ...\mu_L \in [-1, 1]$. They can be found from the zeroes of the characteristic polynomial $F : \mathbb{C} \to \mathbb{C}$,

$$F(z) = \det\left(z\mathbb{I}_L - T_L\right)\,. \tag{2.22}$$

The entropy of entanglement can then be obtained as [39, 40, 108, 115]

$$S(\rho_L) = \sum_{l=1}^{L} f_S(1, \mu_l)\,, \tag{2.23}$$

where $f_S : \mathbb{R}^+ \times \mathbb{C} \to \mathbb{C}$ is defined as

$$f_S(x, y) = -\left(\frac{x+y}{2}\right)\log_2\left(\frac{x+y}{2}\right) - \left(\frac{x-y}{2}\right)\log_2\left(\frac{x-y}{2}\right). \tag{2.24}$$

In fact, we can write [39, 40, 108, 115]

$$S(\rho_L) = \lim_{\varepsilon\to 0}\lim_{\delta\to 0}\frac{1}{2\pi i}\int f_S(1+\varepsilon, z)\frac{F'(z)}{F(z)}dz\,. \tag{2.25}$$

The contour of the integration in the complex plane is shown in Fig.2.3. In turn, we may also write for the single-copy entanglement [113]

$$E_1(\rho_L) = \sum_{l=1}^{L} f_1(0, \mu_l)\,, \tag{2.26}$$

in terms of the above $\mu_1, ..., \mu_L$, where now $f_1 : \mathbb{R}^+ \times \mathbb{C} \to \mathbb{C}$ is to be defined as

$$f_1(\varepsilon, z) = -\log_2\left(\frac{1 + (z^2+\varepsilon^2)^{1/2}}{2}\right)\,. \tag{2.27}$$

Respecting the cuts of the logarithm (see [113]), we may now cast $E_1(\rho_L)$ into the form

$$E_1(\rho_L) = \lim_{\varepsilon\to 0}\lim_{\delta\to 0}\frac{1}{2\pi i}\int f_1(\varepsilon, z)\frac{F'(z)}{F(z)}dz\,. \tag{2.28}$$

Now we take advantage of the fact that T_L is a real symmetric Toeplitz matrix, which means that we can assess the asymptotic behavior of their determinants using proven instances of the Fisher-Hartwig conjecture [39, 40, 99, 108, 115, 122, 123]. We wish to remark at this point that

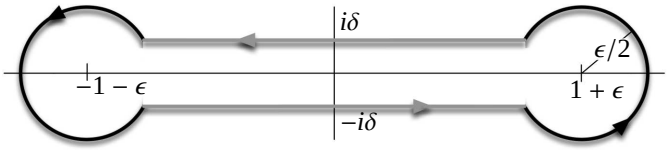

Figure 2.3: Contour of integration to be taken in case of both the entropy of entanglement and the single-copy entanglement.

the observation that we only refer to proven instances of the Fisher-Hartwig conjecture derives from the fact that we are only considering isotropic models [108]. Concerning the function $F : \mathbb{C} \to \mathbb{C}$, the Fisher-Hartwig conjecture allows us to write

$$\frac{F'(z)}{F(z)} = a(z)L - b(z)\log_2 L + O(1) \tag{2.29}$$

in the large-L limit, where

$$b(z) = -2\sum_{r=1}^{R}\beta(z)\beta'(z)\,, \tag{2.30}$$

with $\beta : \mathbb{C} \to \mathbb{C}$ such that [108]

$$z \to \frac{1}{2\pi i}\log_2\left(\frac{z+1}{z-1}\right)\,. \tag{2.31}$$

The number R, in turn corresponds to half the number of discontinuities of the above symbol $g(k)$ in the interval $[0, 2\pi)$. Now, if we assume the validity of the logarithmic scaling of the entropy given in the expression of Eq.2.19, we know that, necessarily,

$$\lim_{\varepsilon\to 0}\lim_{\delta\to 0}\int f_S(1+\varepsilon, z)a(z)dz = 0\,, \tag{2.32}$$

since no linear dependence in L must appear. Moreover, we know that $S(\rho_L) \geq E_1(\rho_L)$, which can easily be proven from their respective mathematical definitions – apart from the intuition that many copies of a system may help in entanglement distillation –. Therefore, in the large-L limit we must also necessarily have

$$\lim_{\varepsilon\to 0}\lim_{\delta\to 0}\int f_1(\varepsilon, z)a(z)dz = 0\,. \tag{2.33}$$

Consequently, we only have to consider the logarithmically divergent term. For the entropy of entanglement the only relevant contour integral reads

$$I_S = \lim_{\varepsilon\to 0}\lim_{\delta\to 0}\frac{1}{2\pi i}\int f_S(1+\varepsilon, z)b(z)dz\,. \tag{2.34}$$

In turn, for the single-copy entanglement the relevant contour integral becomes

$$I_1 = \lim_{\varepsilon\to 0}\lim_{\delta\to 0}\frac{1}{2\pi i}\int f_1(\varepsilon, z)b(z)dz\,. \tag{2.35}$$

Taking into account that $b(z)$ is analytic outside the interval $[-1,1]$, the contributions of the circle pieces vanish in the two cases. Hence, we finally arrive at

$$\begin{aligned} S(\rho_L) &= \frac{R}{\pi^2}\int_{-1}^{1} dx \frac{f_S(1,x)}{1-x^2}\log_2(L) + O(1) \\ E_1(\rho_L) &= \frac{R}{\pi^2}\int_{-1}^{1} dx \frac{f_1(0,x)}{1-x^2}\log_2(L) + O(1)\,. \end{aligned} \tag{2.36}$$

Since $f_1(0,x) = -\log_2((1+|x|)/2)$ for $x \in [-1,1]$, we have that within the large-L limit,

$$\begin{aligned} S(\rho_L) &= \frac{R}{3}\log_2 L + O(1) \\ E_1(\rho_L) &= \frac{R}{6}\log_2 L + O(1)\,, \end{aligned} \tag{2.37}$$

which in turn implies the validity of the expression that we anticipated in Eq.2.20. We have therefore proven that, in this class of models, whenever the system has a logarithmic asymptotical scaling of the entanglement entropy, the single-copy entanglement is exactly half the asymptotically available in the infinite-copy case in its leading contribution. We wish to remark as well that, from Eq.2.37, the number R precisely corresponds to the central charge c for those models that are governed by an underlying conformal symmetry. For instance, for the quantum XX spin chain, we have that $R = c = 1$, corresponding to the universality class of a free boson.

2.4 Single-copy entanglement away from criticality

In this section we exhibit an explicit example for which the relation between single-copy entanglement and entanglement entropy can be demonstrated near but off the critical region. We consider the XY quantum spin chain with a boundary, with Hamiltonian

$$H = -\sum_{i=1}^{\infty}\left(\frac{(1+\gamma)}{2}\sigma_i^x\sigma_{i+1}^x + \frac{(1-\gamma)}{2}\sigma_i^y\sigma_{i+1}^y + \lambda\sigma_i^z\right)\,, \tag{2.38}$$

studied in Chapter 1. Again, we consider the chain of semi-infinite length with a boundary, where the spins $i = 1,2,\ldots,N/2$ with $N \to \infty$ have been traced out from the ground state of the system. The resultant density matrix $\rho_{(\lambda,\gamma)}$ can be written as a thermal density operator of a system of spinless fermions with creation and annihilation operators $d_k^\dagger$ and d_k in the following way [98]:

$$\rho_{(\lambda,\gamma)} = \frac{e^{-H}}{\mathrm{tr}\,(e^{-H})} \qquad H = \sum_k \epsilon_k d_k^\dagger d_k\,, \tag{2.39}$$

where

$$\epsilon_k = \begin{cases} 2k\epsilon\,, & \text{if } \lambda < 1 \\ (2k+1)\epsilon\,, & \text{if } \lambda > 1\,, \end{cases} \tag{2.40}$$

$k \in \mathbb{N}$, and $\lambda \in \mathbb{R}$ is the parameter controlling the external magnetic field, $\lambda^* = 1$ corresponding to the quantum phase transition point. We also have that

$$\epsilon = \pi \frac{I(\sqrt{1-x^2})}{I(x)} , \tag{2.41}$$

$I(x)$ being the complete elliptic integral of the first kind,

$$I(x) = \int_0^{\pi/2} \frac{d\theta}{\left(1 - x^2 \sin^2(\theta)\right)^{1/2}} . \tag{2.42}$$

Furthermore, x is related to the parameters λ and γ defining the model as follows:

$$x = \begin{cases} (\sqrt{\lambda^2+\gamma^2-1})/\gamma , & \text{if } \lambda < 1, \\ \gamma/(\sqrt{\lambda^2+\gamma^2-1}) , & \text{if } \lambda > 1 , \end{cases} \tag{2.43}$$

with the condition $\lambda^2 + \gamma^2 > 1$ (external region of the Baruoch-McCoy circle [99]). A computation of the single-copy entanglement with respect to this partitioning can be performed in terms of ϵ, transforming sums into integrals by means of the Euler-McLaurin expansion, and finding

$$E_1(\rho_{L\to\infty,\epsilon}) = \frac{\pi^2 \log_2 e}{24\epsilon} - \frac{\epsilon \log_2 e}{24} + O(e^{-\epsilon}) \tag{2.44}$$

if $\lambda < 1$ and

$$E_1(\rho_{L\to\infty,\epsilon}) = \frac{\pi^2 \log_2 e}{24\epsilon} + \frac{1}{2} + \frac{\epsilon \log_2 e}{12} + O(e^{-\epsilon}) \tag{2.45}$$

if $\lambda > 1$. No subleading corrections in powers of ϵ do appear in the expansion. On the other hand it is easy to see by explicit evaluation that the entropy of entanglement can be related to the single copy-entanglement by

$$S(\rho_{L\to\infty,\epsilon}) = \left(1 - \epsilon \frac{\partial}{\partial\epsilon}\right) E_1(\rho_{L\to\infty,\epsilon}) , \tag{2.46}$$

which shows that

$$\lim_{\epsilon\to 0} \left(E(\rho_{L\to\infty,\epsilon}) - \frac{1}{2} S(\rho_{L\to\infty,\epsilon}) \right) = 0 . \tag{2.47}$$

We notice that the limit $\epsilon \to 0$ is precisely the limit where the theory becomes critical, that is when $\lambda \to \lambda^* = 1$. The above expression for finite ϵ gives us corrections away from criticality to the $1/2$ factor between the entanglement entropy and the single copy entanglement that has been discussed in the preceding sections. These corrections vanish as the system approaches criticality, as we have explicitly seen in this example.

2.5 Conclusions of Chapter 2

In this Chapter we have analyzed the single-copy entanglement, that is, the entanglement that it is possible to deterministically distill by using local operations and classical communication when only one copy of a bipartite system is at hand, in quantum systems in $(1 + 1)$ dimensions. We have carried our analysis mainly from the point of view of conformal field theory in $(1 + 1)$ dimensions in the bulk and quasi-free fermionic models in order to analyze critical systems, and also studied the behavior close to but away from criticality for the integrable example of the XY quantum spin chain. To be more precise:

- For $(1 + 1)$-dimensional conformal field theories we have proven that the leading scaling behavior of the single-copy entanglement is exactly *half* the asymptotic behavior of the entanglement entropy. The first-order correction to the leading term has also been explicitly computed.

- For quasi-free fermionic quantum systems we have proven that if the asymptotic scaling of the entanglement entropy is logarithmic, then the asymptotic scaling of the single-copy entanglement is also logarithmic, with a prefactor that is exactly *half* the one of the entanglement entropy.

- For the example of the semi-infinite XY quantum spin chain, we have computed the single-copy entanglement away from criticality and have observed that the factor $1/2$ between the entropy and the single-copy entanglement is *only* recovered when the system approaches the quantum phase transition point.

The main conclusion is, therefore, that for $(1+1)$-dimensional quantum systems at criticality the single-copy entanglement and the entanglement entropy for a system described by a reduced density matrix ρ_L typically obey the law

$$\lim_{L\to\infty}\left(\frac{S(\rho_L)}{E_1(\rho_L)} = 2\right) . \tag{2.48}$$

For systems obeying the above relation we can say that in a *single run*, with a single invocation of a physical device acting on only one physical system, it is possible to obtain half the entanglement per specimen that is asymptotically available in the infinite-copy limit. Furthermore, all these results also show relationships between the largest eigenvalue of the reduced vacuum ρ_L and its full spectrum for a very large class of quantum systems.

Chapter 3

Entanglement entropy in the Lipkin-Meshkov-Glick model

Most of the analytical studies of the entanglement properties of quantum many-body systems close to criticality have been focused on the particular case of (1 + 1)-dimensional systems, like the ones that we considered in the previous Chapters. Few models have been discussed so far in higher dimensions [31, 34, 35, 58–60, 101, 109–111, 124–131] either due to the absence of an exact diagonalization of the system or to a difficult numerical treatment. We can in part understand this difficulty because of the existing link between the connectivity of a system and its entanglement entropy: one should naively think that, the bigger the connectivity of the system is, the bigger the amount of quantum correlations present in the ground state of the model should be, especially when the system is close to a quantum critical point. A classical numerical treatment of the model can become then very inefficient, as we shall in detail explain in the forthcoming Chapters 4 and 5. The idea in favor of this is rather simple: the more connected a system is, the more interactions it has, therefore the more entangled its ground state should be and the more difficult it should be to get its fundamental properties – like the ground-state energy or the correlation functions – by means of a classical numerical treatment.

Actually, with some insight it is possible to make a non-accurate quantitative statement about the previous idea: given a system of N particles in $(d+1)$ dimensions, d being the number of spatial dimensions of the underlying lattice, if we believe that at criticality the entropy of entanglement S is to scale proportionally to the area of the boundary of the region that separates the two subsystems under consideration, as is the case of bosonic systems [31, 105, 131], then it is not difficult to check that the entropy of a bipartition of the system between $N/2$ contiguous particles and the rest has to roughly scale like

$$S \sim N^{\frac{d-1}{d}} . \tag{3.1}$$

Critical fermionic systems may differ from the above law by means of an $O(\log_2 N)$ multiplicative factor [109–111]. From the above reasoning we can see that the bigger the dimensionality d is – which is directly related to the connectivity of the system –, the stronger the scaling of the entanglement entropy should be. The case of a conformally-invariant critical system with $d = 1$ has to be treated separately since the entropy has a *logarithmic* divergence, as we already

remarked in previous Chapters. This intuitive relation between entanglement and connectivity will be considered again in Chapter 4, when studying the scaling of entanglement in quantum algorithms.

In this context, the Lipkin-Meshkov-Glick model [132–134] has drawn much attention since it allows for a very efficient numerical treatment as well as analytical calculations. Furthermore, it provides a useful counter-example of the previous intuitive relation between entanglement and connectivity: in a system defined on a simplex – totally connected network –, and contrary to the intuition that we have specified before, the entanglement in the system behaves *as if* the system were $(1+1)$-dimensional. This is a consequence of the role played by the symmetries within the description of the model, as we shall see. Entanglement can be increased by the connectivity, but can also be "killed" by the symmetries in some cases.

First introduced by Lipkin, Meshkov and Glick in nuclear physics, this model has been the subject of intensive studies during the last two decades. It is of interest in order to describe in particular the Josephson effect in two-mode Bose-Einstein condensates [135, 136]. Its entanglement properties have been already discussed through the concurrence, which exhibits a cusp-like behavior at the critical point [137–139] as well as interesting dynamical properties [140]. Similar results have also been obtained in the Dicke model [141–143] which can be mapped onto the Lipkin-Meshkov-Glick model in some cases [144], or in the reduced BCS model [145]. Let us mention as well that the entanglement entropy has also been calculated for the anti-ferromagnetic Lipkin-Meshkov-Glick model [146] for which the ground state is known exactly [138, 147]. Here we analyze the von Neumann entropy computed from the ground state of the Lipkin-Meshkov-Glick model. We show that, at criticality, it behaves logarithmically with the size of the blocks L used in the bipartite decomposition of the density matrix with a prefactor that depends on the anisotropy parameter tuning the underlying universality class. We also discuss the dependence of the entropy with the magnetic field and stress the close analogy of the found results with those of $(1+1)$-dimensional quantum systems.

3.1 The Lipkin-Meshkov-Glick model

The Lipkin-Meshkov-Glick model is defined by the Hamiltonian

$$H = -\frac{\lambda}{N}\sum_{i<j}\left(\sigma_i^x\sigma_j^x + \gamma\sigma_i^y\sigma_j^y\right) - h\sum_{i=1}^{N}\sigma_i^z\,, \tag{3.2}$$

where σ_k^α is the Pauli matrix at position k in the direction α, and N the total number of spins. This Hamiltonian describes a set of spins one-half located at the vertices of a N-dimensional simplex – complete graph, as shown in Fig.3.1 – interacting via a ferromagnetic coupling $\lambda > 0$ in the xy-spin plane, γ being an anisotropy parameter and h an external magnetic field applied along the z direction.

Given that the model is defined on a simplex, the symmetry under permutations of particles allows us to rewrite the Hamiltonian from Eq.3.2 in terms of the total spin operators J^α =

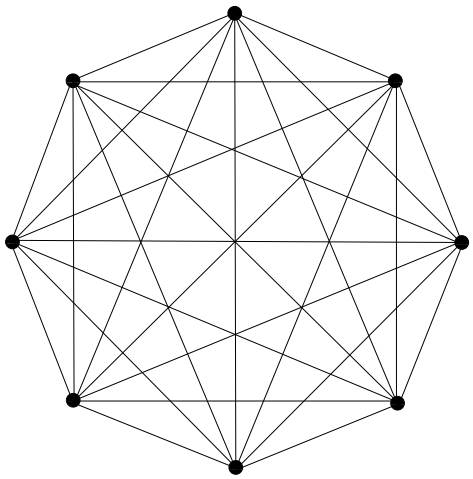

Figure 3.1: Complete graph – or simplex – of 8 vertices.

$\sum_{i=1}^{N} \sigma_i^\alpha/2$. The previous Hamiltonian can then be expressed as

$$\begin{aligned} H &= -\frac{\lambda}{N}(1+\gamma)\left(\mathbf{J}^2 - J^z J^z - N/2\right) - 2hJ^z \\ &\quad -\frac{\lambda}{2N}(1-\gamma)\left(J^+ J^+ + J^- J^-\right) , \end{aligned} \tag{3.3}$$

where $\mathbf{J}^2$ is the representation of spin $N/2$ of the Casimir operator and $J^\pm \equiv J^x \pm iJ^y$. In the following, we set for simplicity $\lambda = 1$ and since the spectrum of H is even under the transformation $h \leftrightarrow -h$ [140], we restrict our analysis to the region $h \geq 0$. Furthermore, we only consider the maximum spin sector $J = N/2$ to which the full spectrum of the Hamiltonian from Eq.4.18 belongs. A convenient basis of this subspace is spanned by the so-called Dicke states $|N/2, M\rangle$ which are invariant under the permutation of spins and are eigenstates of $\mathbf{J}^2$ and J^z with eigenvalues $N(N+2)/4$ and $M = -N/2, -N/2+1, \ldots, N/2-1, N/2$, respectively.

3.2 Entanglement within different regimes

We consider the von Neumann entropy associated with the ground state reduced density matrix $\rho_{L,N}$ of a block of size L out of the total N spins, $S_{L,N} \equiv S(\rho_{L,N}) = -\mathrm{tr}\,(\rho_{L,N} \log_2 \rho_{L,N})$ and analyze its behavior as L is changed, both keeping N finite or sending it to infinity. Notice that since the ground state reduced density matrix is spanned by the set of $(L+1)$ Dicke states, the entropy of entanglement obeys the constraint $S_{L,N} \leq \log_2(L+1)$ for all L and N, where the upper bound corresponds to the entropy of the maximally mixed state $\rho_{L,N} = \mathbb{I}/(L+1)$ in the Dicke basis. This argument implies that entanglement, as measured by the von Neumann entropy, cannot grow faster than the typical logarithmic scaling law observed in $(1+1)$-dimensional quantum spin chains at conformally-invariant critical points [36–38]. Entanglement has thus been drastically reduced by the symmetry under permutations of the model, as we hinted at the

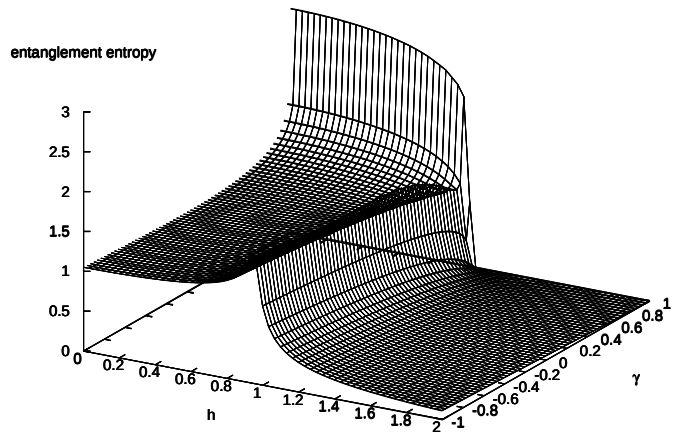

Figure 3.2: Entanglement entropy for $N = 500$ and $L = 125$ as a function of h and γ.

beginning of the Chapter[a].

3.2.1 The $\gamma - h$ plane

In order to study the different entanglement regimes, we compute the entropy in the plane spanned by γ and h. The numerical computation can be done by taking advantage of the Hamiltonian symmetries to reduce the complexity of the task to a polynomial growth in N. Results are displayed in Fig.3.2 for $N = 500$ and $L = 125$. For $\gamma \neq 1$, one clearly observes a peak at the critical point $h = 1$ whereas the entropy goes to zero at large h since the ground state is then a fully polarized state in the field direction. In the zero field limit, the entropy saturates when the size of the system increases and goes to $S_{L,N} = 1$ for $\gamma = 0$ where the ground state approaches a GHZ-like "cat" state as in the Ising quantum spin chain [37, 38, 95, 112]. By contrast, for $\gamma = 1$, the entropy increases with the size of the system in the region $0 \leq h < 1$ and jumps directly to zero at $h = 1$ as we shall now discuss.

3.2.2 Analytical study of the isotropic case

In the isotropic case ($\gamma = 1$), it is possible to analytically compute the entropy of entanglement since, at this point, the Hamiltonian is diagonal in the Dicke basis. The ground-state energy is given by $E_0(h, \gamma = 1) = -\frac{N}{2} + \frac{2}{N}M^2 - 2hM$, with

$$M = \begin{cases} I(hN/2)\,, & \text{if} \quad 0 \leq h < 1 \\ N/2\,, & \text{if} \quad h \geq 1 \end{cases}, \tag{3.4}$$

[a]One should take care with this statement, since there are other models which are symmetric under permutations of particles and such that the entropy of entanglement is very large, as are for instance those systems described by the Laughlin wavefunction [148].

and the corresponding eigenvector is simply $|N/2, M\rangle$. Here, $I(x)$ denotes the round value of x.

To calculate the entropy, it is convenient to introduce the number n of spins "up" so that $M = n - N/2$, and to write this state in a bipartite form. Indeed, since Dicke states are completely symmetric under any permutation of sites, it is straightforward to see that the ground state can be written as a sum of byproducts of Dicke states

$$\begin{aligned} |N/2, n - N/2\rangle \quad = \quad & \sum_{l=0}^{L} p_l^{1/2} |L/2, l - L/2\rangle \otimes \\ & |(N-L)/2, n - l - (N-L)/2\rangle \,, \end{aligned} \tag{3.5}$$

where the partition is made between two blocks of size L and $(N - L)$ and

$$p_l = \frac{\left(\begin{array}{c} L \\ l \end{array}\right)\left(\begin{array}{c} N-L \\ n-l \end{array}\right)}{\left(\begin{array}{c} N \\ n \end{array}\right)} \,, \tag{3.6}$$

defining an hypergeometric probability distribution. The expression given in Eq.3.6 corresponds to the Schmidt decomposition of the ground state of the system. The entropy of this state for this bipartition is then simply given by $S_{L,N}(h, \gamma = 1) = -\sum_{l=0}^{L} p_l \log_2 p_l$. In the limit $N, L \gg 1$, the hypergeometric distribution of the p_l can be recast into a Gaussian distribution

$$p_l \simeq p_l^g = \frac{1}{\sqrt{2\pi}\sigma} e^{-\left(\frac{(l-\bar{l})^2}{2\sigma^2}\right)} \,, \tag{3.7}$$

of mean value $\bar{l} = n\frac{L}{N}$ and variance

$$\sigma^2 = n(N-n)\frac{(N-L)L}{N^3} \,, \tag{3.8}$$

where we have retained the sub-leading term in $(N - L)$ to explicitly preserve the symmetry $S_{L,N} = S_{N-L,N}$. The entropy then reads

$$-\int_{-\infty}^{\infty} \mathrm{d}l \; p_l^g \log_2 p_l^g = \frac{1}{2}\left(\log_2 e + \log_2 2\pi + \log_2 \sigma^2\right) \,, \tag{3.9}$$

and only depends on its variance as expected for a Gaussian distribution[b]. Of course, for $h \geq 1$, the entanglement entropy is exactly zero since the ground state is, in this case, fully polarized in the magnetic field direction ($n = N$). For $h \in [0, 1)$ and in the limit $N, L \gg 1$, Eq.3.4, Eq.3.8 and Eq.3.9 lead to

$$S_{L,N}(h, \gamma = 1) \sim \frac{1}{2} \log_2 \left(\frac{L(N-L)}{N}\right) \,. \tag{3.10}$$

Moreover, the dependence of the entropy on the magnetic field is given by

$$S_{L,N}(h, \gamma = 1) - S_{L,N}(h = 0, \gamma = 1) \sim \frac{1}{2} \log_2 \left(1 - h^2\right) \,, \tag{3.11}$$

and thus diverges, at fixed L and N, in the limit $h \to 1^-$.

[b]This result has also been obtained in the context of the ferromagnetic Heisenberg chain [149].

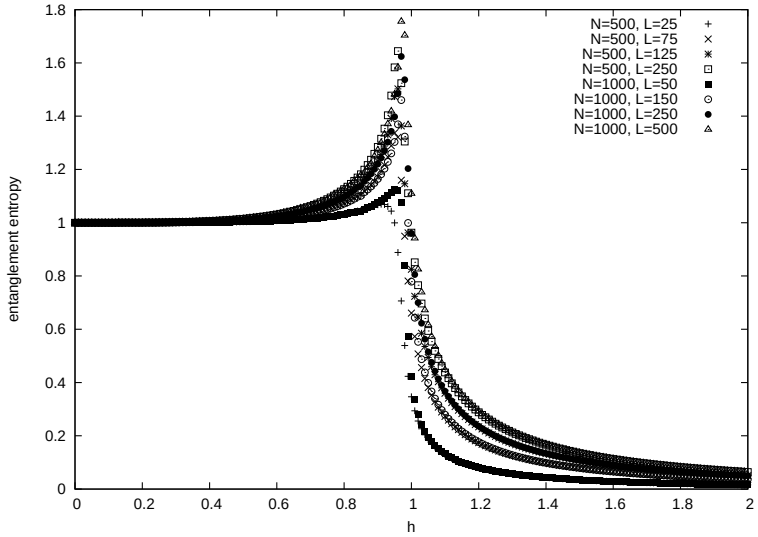

Figure 3.3: Entanglement entropy at $\gamma = 0$ as a function of h for different values of N and L. Outside of the critical region, the entropy only depends on the ratio L/N.

3.2.3 Numerical study of the anisotropic case

Let us now discuss the more general situation $\gamma \neq 1$ for which no simple analytical solution exists. In this case, the ground state is a superposition of Dicke states with coefficients that can be easily determined by exact numerical diagonalizations. Upon tracing out $(N - L)$ spins, each Dicke state decomposes as in Eq.3.5. It is then easy to build the $(L + 1) \times (L + 1)$ ground state reduced density matrix and to compute its associated entropy.

We have displayed in Fig.3.3, the behavior of the entropy as a function of h, for different values of the ratio L/N and for $\gamma = 0$. For $h \neq 1$, the entropy only depends on the ratio L/N. For any γ, at fixed L/N and in the limit $h \to \infty$, the entropy goes to zero since the ground state becomes then fully polarized in the field direction. Notice that the entropy also vanishes, at $h > 1$, in the limit $L/N \to 0$ where the entanglement properties become trivial. In the zero field limit, the entropy goes to a constant which depends on γ and equals 1 at $\gamma = 0$ since the ground state is then a GHZ-like state made up of spins pointing in $\pm x$ directions. Close to criticality, the entropy displays a logarithmic divergence, which we numerically find to obey the law

$$S_{L,N}(h, \gamma) \sim -a \log_2 |1 - h| \,, \tag{3.12}$$

where a is close to 1/6 for $N, L \gg 1$ as can be seen in Fig.3.4.

At the critical point, the entropy has a nontrivial behavior that we have studied focusing on the point $\gamma = 0$ which is representative of the class $\gamma \neq 1$. There, the entropy also scales logarithmically with L as in the isotropic case, but with a different prefactor. More precisely, we find

$$S_{L,N}(h = 1, \gamma \neq 1) \sim b \log_2 \left(\frac{L(N - L)}{N} \right) . \tag{3.13}$$

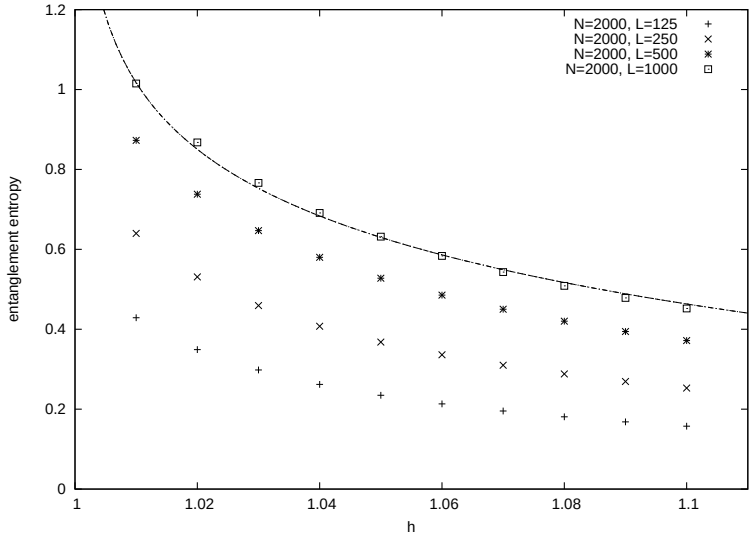

Figure 3.4: Entanglement entropy as a function of h near the critical point for $\gamma = 0$. The full line corresponds to the fitting law from Eq.3.12 with $a = 1/6$.

For the finite-size systems investigated here, the prefactor varies when either the ratio L/N or γ is changed, as can be seen in Fig.3.5. However, in the thermodynamic limit $N, L \gg 1$ (and finite L/N), $b = 1/3$ fits well our numerical results.

In addition, at fixed L and N, the entropy also depends on the anisotropy parameter logarithmically as

$$S_{L,N}(h = 1, \gamma) - S_{L,N}(h = 1, \gamma = 0) \sim f \log_2(1 - \gamma) , \tag{3.14}$$

for all $-1 \leq \gamma < 1$ as can be seen in Fig.3.6. Here again, it is likely that, in the thermodynamic limit, f has a simple (rational) value which, from our data, seems to be $1/6$. It is important to keep in mind that the limit $\gamma \to 1$ and the thermodynamic limit do not commute so that Eq.3.14 is only valid for $\gamma \neq 1$.

Actually, the logarithmic behavior of the laws given in Eq.3.12, Eq.3.13 and Eq.3.14 has been very recently confirmed by yet unpublished analytical computations [150], but with values of a and b that differ from those obtained in simulations. More precisely, it has been proven that the exact coefficients a and b governing the logarithmic behaviors of Eq.3.12 and Eq.**??** are $1/4$ and $1/2$ respectively, instead of the values $1/6$ and $1/3$ obtained from the numerical computations. The same analytical study confirms the value of $1/6$ for coefficient f in Eq.3.14.

3.3 Comparison to quantum spin chains

Let us now compare the previous results with those found in the (1+1)-dimensional quantum XY model. As for the Lipkin-Meshkov-Glick model, the XY quantum spin chain has two different universality classes depending on the anisotropy parameter. At the critical point, the entropy has

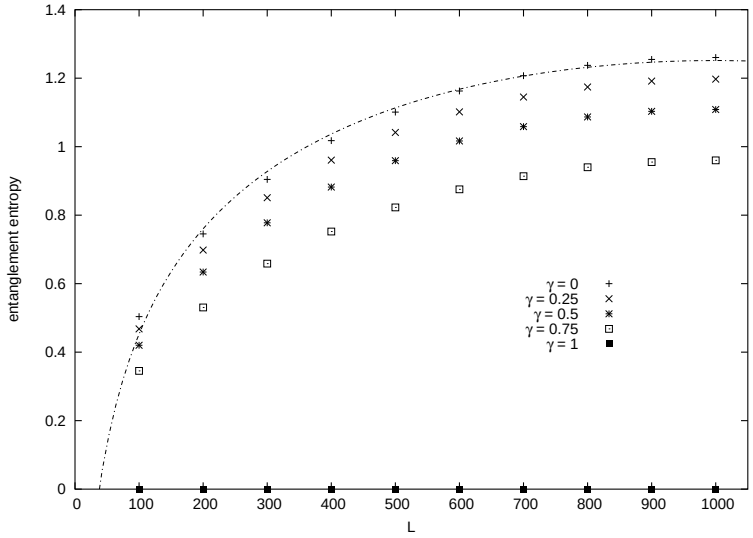

Figure 3.5: Entanglement entropy as a function of L at the critical point for different γ and $N = 2000$. The full line corresponds to the fitting law from Eq.3.13 with $b = 1/3$.

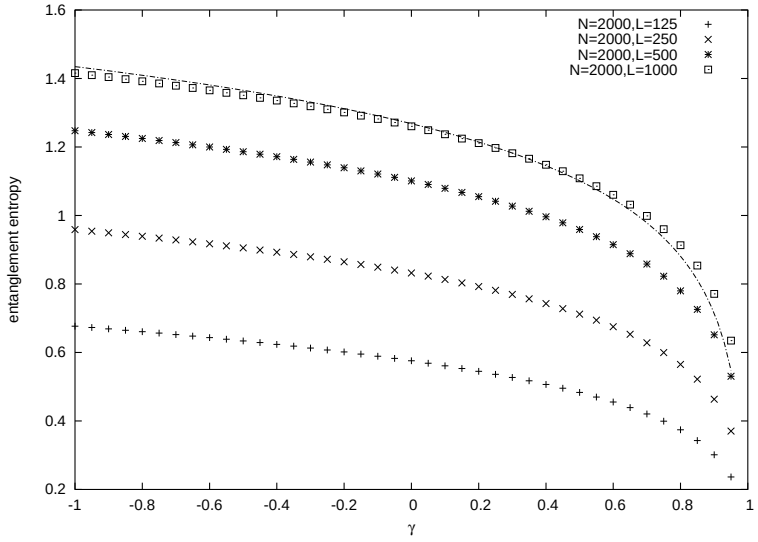

Figure 3.6: Entanglement entropy at the critical point $h = 1$ as a function of γ. The full line corresponds to the fitting law from Eq.3.14 with $f = 1/6$.

XY quantum spin chain	Lipkin-Meshkov-Glick model
$H = -\sum_{i=1}^{N}\left(\frac{(1+\gamma)}{2}\sigma_i^x\sigma_{i+1}^x + \frac{(1-\gamma)}{2}\sigma_i^y\sigma_{i+1}^y + \lambda\sigma_i^z\right)$	$H = -\frac{1}{N}\sum_{i<j}\left(\sigma_i^x\sigma_j^x + \gamma\sigma_i^y\sigma_j^y\right) - h\sum_{i=1}^{N}\sigma_i^z$
$S_L(\lambda, \gamma = 0) \sim \frac{1}{3}\log_2(L)$	$S_L(h, \gamma = 1) \sim \frac{1}{2}\log_2(L)$
$S_L(\lambda, \gamma = 0) - S_L(\lambda = 0, \gamma = 0) \sim \frac{1}{6}\log_2\left(1-\lambda^2\right)$	$S_L(h, \gamma = 1) - S_L(h = 0, \gamma = 1) \sim \frac{1}{2}\log_2\left(1-h^2\right)$
$S_L(\lambda = 1, \gamma = 1) \sim \frac{1}{6}\log_2(L)$	$S_L(h = 1, \gamma = 0) \sim \frac{1}{3}\log_2(L)$
$S_L(\lambda, \gamma = 1) \sim -\frac{1}{6}\log_2(m)$	$S_L(h, \gamma = 0) \sim -\frac{1}{4}\log_2\lvert 1-h\rvert$
$S_L(\lambda = 1, \gamma) - S_L(\lambda = 1, \gamma = 1) \sim \frac{1}{6}\log_2(\gamma)$	$S_L(h = 1, \gamma) - S_L(h = 1, \gamma = 0) \sim \frac{1}{6}\log_2(1-\gamma)$

Table 3.1: Comparison of results between the XY quantum spin chain and the Lipkin-Meshkov-Glick model, when $N \gg L \gg 1$.

been found to behave as [37, 38, 115]

$$S_{L,N} \sim \frac{c}{3}\log_2\left(\frac{L(N-L)}{N}\right), \tag{3.15}$$

where c is the central charge of the corresponding $(1+1)$-dimensional conformal field theory [36] (see Appendix B). For the isotropic case, the critical model is indeed described by a free boson theory with $c = 1$ whereas the anisotropic case corresponds to a free fermion theory with $c = 1/2$. It is striking to see that the entropy in the Lipkin-Meshkov-Glick model has the same logarithmic dependence with some prefactor which, as in the $(1+1)$-dimensional case, only seems to depend on the universality class – see Eq.3.10 and Eq.3.13 –. Concerning the dependence with the magnetic field and with the anisotropy parameter, it is also worth noting that logarithmic behaviors of Eq.3.11, Eq.3.12, and Eq.3.14 are similar to those found in the XY quantum spin chain [37, 38] except that the prefactors in the Lipkin-Meshkov-Glick model are different. A list of analogies between the results of the Lipkin-Meshkov-Glick model and the XY quantum spin chain in the limit $N \gg L \gg 1$ is given in Table 3.1. Also, and just as a remark, it is possible to numerically check that the behavior of this model with respect to majorization (see Appendix A) for $\gamma \neq 1$ and as h departs from its critical value is completely analogue to the case of the quantum XY model [95, 112], which was analytically studied in Chapter 1. Namely, the whole set of eigenvalues of the reduced density matrices of the ground state obey strict majorization relations as h grows, while for decreasing h one of the eigenvalues of the reduced density matrix in consideration drives the system towards a GHZ-like state in such a way that majorization is only strictly obeyed in the thermodynamic limit. This behavior implies a very strong sense of order of the correlations present in the ground state, in complete analogy to the behavior of the XY quantum spin chain.

3.4 Conclusions of Chapter 3

In this Chapter we have studied the entanglement properties of a quantum spin model defined on a simplex. We have seen that:

- Contrary to the intuitive idea that the quantum correlations present in the system increase together with the connectivity of the model, here the symmetries force the entropy to scale *as if* the system were defined on a chain.
- Also, the Lipkin-Meshkov-Glick model presents striking similarities with the XY quantum spin chain: not only their phase diagrams are almost identical, but the scaling properties of the entanglement of the ground state seem to obey the same laws but with appropriate proportionality coefficients.

The observed similarity in the behavior of this model to $(1+1)$-dimensional quantum systems is indeed very pleasant, since quantum spin chains have been heavily studied and their properties are very well-known. Some of their properties seem to be directly translated into systems which, a priori, are not defined in $(1+1)$ dimension, like the Lipkin-Meshkov-Glick model. Nevertheless, most of the situations that one finds when considering models which are not defined on a chain turn out to be much more intrincated, as we will see in the next two Chapters. Perhaps, a perturbative analysis around the Lipkin-Meshkov-Glick model – for instance removing a few number of links in the simplex and thus slightly breaking the symmetry present in the problem – could allow to analytically study non-trivial properties of quantum many-body systems of high dimensionality.

Chapter 4

Entanglement entropy in quantum algorithms

The previous Chapters were focused on the properties of quantum many-body systems, basically from a condensed matter and field theoretical point of view. In particular, we saw that it is possible to apply tools from quantum information science – such as majorization and entanglement theory – to obtain a better understanding of the properties of these systems. We will now see that these tools can also be used to understand better problems arising in the area of quantum information and quantum computation.

In this and the forthcoming Chapters our aim is to study a physical system which is very close to the spirit of quantum many-body physics: we wish to understand the properties and behavior of *quantum computers and quantum algorithms*. Indeed, a quantum computer is nothing but a physical system which is governed by the laws of quantum mechanics and on which we can perform physical actions – algorithms – such that the device is able deliver solutions to specific problems. Of course, the kind of problems that we can solve by using a quantum computer is necessarily limited by quantum physics itself, being this properly formalized by the area of quantum complexity theory [151]. Furthermore, it is plausible to think of a quantum computer as a device made of qubits which interact among themselves in some way. Therefore, *a quantum computer can be understood as an interacting quantum many-body system*. The full machinery from quantum many-body physics can then in principle be applied to analyze the performance of quantum algorithms. In particular, there is a very strong connection between quantum algorithms and quantum phase transitions, as we shall see.

From the point of view of quantum computation, the design of new quantum algorithms is a great theoretical challenge. The most relevant property in order to understand these algorithms is clearly the role entanglement plays in quantum computational speedup, while some other properties seem to play a role as well, as we shall see in Chapter 6 with majorization [152–154]. Regarding entanglement, several results have been found [49, 50, 155–159] which suggest that entanglement is at the heart of the power of quantum computers. An important and remarkable result was obtained by Vidal [49], who proved that large entanglement between the qubits of a quantum register is a *necessary* condition for exponential speed-up in quantum computation. To be precise, a quantum register such that the maximum Schmidt number of any bipartition is

bounded at most by a polynomial in the size of the system can be simulated efficiently by classical means. The classical simulation scheme proposed in [49] was, indeed, a time-dependent version of the density matrix renormalization group algorithm, based on the efficient updates in time of the quantum register defined in terms of a matrix product state [45, 46]. Those methods are, indeed, tools for the classical simulation of the dynamics of a quantum many-body system which are also useful in the simulation of a quantum computation, since any quantum algorithm can be understood as the time evolution of a quantum many-body system [71]. Here we just sketch the basic idea of Vidal's algorithm, and leave all the specific details of this and other classical simulation protocols for the next Chapter.

The figure of merit χ proposed in [49] is the maximum Schmidt number of any bipartitioning of the quantum state or, in other words, the maximum rank of the reduced density matrices for any possible splitting. It can be proven that $\chi \geq 2^{S(\rho)}$, where the von Neumann entropy $S(\rho)$ refers to the reduced density matrix of any of the two partitions. From now on, in this and also in all the forthcoming Chapters we shall use the following computer-science notation: the number of qubits in the quantum register will be denoted by n, and $N = 2^n$ denotes the dimensionality of the computational Hilbert space, as opposed to the condensed matter notation of the previous Chapters, were N was the number of particles present in the system. Using this notation, Vidal proved that if $\chi = O(\text{poly}(n))$ at every step of the computation in a quantum algorithm, then it can be efficiently classically simulated. Exponential speed-up over classical computation is only possible if at some step along the computation $\chi \sim \exp(n^a)$, or $S(\rho) \sim n^b$, a and b being positive constants. In order to exponentially accelerate the performance of classical computers any quantum algorithm must necessarily create an exponentially large amount of χ at some point.

As we saw in the previous Chapters, a topic of intense research concerns the behavior of entanglement in systems undergoing a quantum phase transition [160]. More generally, when a splitting of a $(d+1)$-dimensional spin system is made, the von Neumann entropy of the ground state for the reduced density matrix of one of the subsystems $S(\rho) = -\text{tr}(\rho \log_2 \rho)$ at the critical point should typically display a universal leading scaling behavior determined by the *area* of the region partitioning the whole system [31, 105, 131], with at most logarithmic corrections if the system is fermionic [109–111]. As hinted in the previous Chapter, this result depends on the connectivity of the Hamiltonian. Using a naive reasoning, we saw there that the leading universal scaling behavior for the entropy of an exact bipartition of the system should typically be written in terms of the number of particles n as

$$S(\rho) \sim n^{\frac{d-1}{d}} \tag{4.1}$$

for a $(d+1)$-dimensional critical non-fermionic system with sufficiently local interactions, which reduces to a logarithmic law for $d = 1$. This explicit dependence of entanglement on dimensionality turns out to shed new light into some well established results from quantum computation.

A similar situation is present in quantum adiabatic algorithms, originally introduced by Farhi et *al.* in [16], where the Hamiltonian of the system depends on a control parameter s which in turn has a given time dependence. The Hamiltonians related to adiabatic quantum computation for solving some NP-complete problems (such as 3-SAT or Exact Cover) can be directly mapped to interacting non-local spin systems, and therefore we can extend the study of

entanglement to include this kind of Hamiltonians. This point of view has the additional interest of being directly connected to the possibility of efficient classical simulations of the quantum algorithm, by means of the protocol proposed in [49].

Here we analyze the scaling of the entropy of entanglement in several quantum algorithms. More concretely, we focus on Shor's quantum factoring algorithm [8] and on a quantum algorithm by adiabatic evolution solving the Exact Cover NP-complete problem [16, 61–68], finding for both of them evidence (either analytical or numerical) of a quantum exponential speedup with linear scaling of quantum correlations – as measured by the entropy –, which seems to prohibit the possibility of an efficient classical simulation. We furthermore make an analytical study of the adiabatic implementation of Grover's quantum search algorithm [9, 69, 70], in which entanglement is a bounded quantity between calls to the quantum oracle even at the critical point, regardless of the size of the system. Let us begin, then, by considering the behavior of the factoring quantum algorithm.

4.1 Entanglement in Shor's factoring quantum algorithm

It is believed that the reason why Shor's quantum algorithm for factorization [8] beats so clearly its classical rivals is rooted in the clever use it makes of quantum entanglement. Several attempts have been made in order to understand the behavior of the quantum correlations present along the computation [157–159]. In our case, we will concentrate in the study of the scaling behavior for the entanglement entropy of the system. We shall first remember both Shor's original [8] and phase-estimation [161] proposals of the factoring algorithm and afterwards we shall move to the analytical study of their quantum correlations.

4.1.1 The factoring quantum algorithm

The interested reader is addressed to [2, 8, 161, 162] for precise details. Given an odd integer N to factorize, we pick up a random number $a \in [1, N]$. We make the assumption that a and N are co-primes – otherwise the greatest common divisor of a and N would already be a non-trivial factor of N –. There exists a smaller integer $r \in [1, N]$, called the *order* of the modular exponentiation $a^x \bmod N$, such that $a^r \bmod N = 1$. Let us assume that the a we have chosen is such that r is even and $a^{r/2} \bmod N \neq -1$, which happens with very high probability, bigger than or equal to $1/(2\log_2 N)$. This is the case of interest because then the greatest common divisor of N and $a^{r/2} \pm 1$ is a non-trivial factor of N. Therefore, the original factorization problem has been reduced to the order-finding problem of the modular exponentiation function $a^x \bmod N$, and it is at this point where quantum mechanics comes at work. The procedure can be casted in two different (but equivalent) ways:

Shor's proposal for order-finding

We make use of two quantum registers: a source register of k qubits such that $2^k \in [N^2, 2N^2]$, and a target register of $n = \lceil \log_2 N \rceil$ qubits. The quantum circuit of the quantum algorithm is shown in Fig.4.1, where we are making use of the Hadamard gate initially acting over the k

qubits of the source, the unitary implementation of the modular exponentiation function

$$U_f|q\rangle|x\rangle = |q\rangle|(x + a^q) \bmod N\rangle \,, \tag{4.2}$$

where $|q\rangle$ and $|x\rangle$ respectively belong to the source and target registers, and the quantum Fourier transform operator

$$QFT|q\rangle = \frac{1}{2^{k/2}} \sum_{m=0}^{2^k-1} e^{2\pi i q m/2^k} |m\rangle \,. \tag{4.3}$$

All these operations can be efficiently implemented by means of one and two-qubit gates. Finally, a suitable classical treatment of the final measurement of this quantum algorithm provides us with r in few steps, and therefore the prime factorization of N in a time $O((\log_2 N)^3)$.

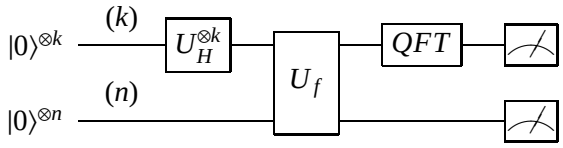

Figure 4.1: Quantum circuit for the order-finding algorithm for the modular exponentiation function. The source and target registers have k and n qubits respectively.

Phase-estimation proposal for order-finding

We shall address the specific details of the generic quantum phase-estimation algorithm in Chapter 6 and refer the interested reader to [161] for more information. For order-finding purposes, the quantum circuit is similar to the one shown in the previous section but slightly modified, as is shown in Fig.4.2. The unitary operator V_f to which the phase-estimation procedure is applied is defined as

$$V_f|x\rangle = |(a\ x) \bmod N\rangle \tag{4.4}$$

(notice the difference between Eq.4.4 and Eq.4.2), being diagonalized by eigenvectors

$$|v_s\rangle = \frac{1}{r^{1/2}} \sum_{p=0}^{r-1} e^{-2\pi i s p/r} |a^p \bmod N\rangle \tag{4.5}$$

such that

$$V_f|v_s\rangle = e^{2\pi i s/r}|v_s\rangle \,, \tag{4.6}$$

and satisfying the relation $\frac{1}{r^{1/2}} \sum_{s=0}^{r-1} |v_s\rangle = |1\rangle$. The operator is applied over the target register being controlled on the qubits of the source in such a way that

$$\Lambda(V_f)|j\rangle|x\rangle = |j\rangle V_f^j|x\rangle \,, \tag{4.7}$$

where by $\Lambda(V_f)$ we understand the full controlled operation acting over the whole system, which can be efficiently implemented in terms of one and two-qubit gates. As in the previous case, the information provided by a final measurement of the quantum computer enables us to get the factors of N in a time $O((\log_2 N)^3)$.

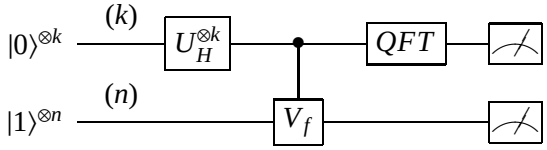

Figure 4.2: Phase-estimation version of the quantum circuit for the order-finding algorithm. The controlled operation is $\Lambda(V_f)$. The source and target registers have k and n qubits respectively.

4.1.2 Analytical results

We choose to study the amount of entanglement between the source and the target register in the two proposed quantum circuits, right after the modular exponentiation operation U_f from Fig.4.1 or the controlled V_f operation from Fig.4.2, and before the quantum Fourier transform in both cases. At this step of the computation, the pure quantum state of the quantum computer is easily seen to be exactly the same for both quantum circuits, and is given by

$$|\psi\rangle = \frac{1}{2^{k/2}} \sum_{q=0}^{2^k-1} |q\rangle |a^q \bmod N\rangle \,, \tag{4.8}$$

and therefore the density matrix of the whole system is

$$|\psi\rangle\langle\psi| = \frac{1}{2^k} \sum_{q,q'=0}^{2^k-1} (|q\rangle\langle q'|) \left(|a^q \bmod N\rangle\langle a^{q'} \bmod N|\right) \,. \tag{4.9}$$

Tracing out the quantum bits corresponding to the source, we get the density matrix of the target register, which reads

$$\rho_{\text{target}} = \text{tr}_{\text{source}}(|\psi\rangle\langle\psi|) = \frac{1}{2^k} \sum_{p,q,q'=0}^{2^k-1} (\langle p|q\rangle\langle q'|p\rangle) \left(|a^q \bmod N\rangle\langle a^{q'} \bmod N|\right) \,, \tag{4.10}$$

that is,

$$\rho_{\text{target}} = \frac{1}{2^k} \sum_{p=0}^{2^k-1} |a^p \bmod N\rangle\langle a^p \bmod N| \sim \frac{1}{r} \sum_{p=0}^{r-1} |a^p \bmod N\rangle\langle a^p \bmod N| \,. \tag{4.11}$$

The last step comes from the fact that $a^r \bmod N = 1$, where $r \in [1, N]$ denotes the order of the modular exponentiation. If 2^k were a multiple of r there would not be any approximation

and the last equation would be exact. This is not necessarily the case, but the corrections to this expression are $O(1/2^k)$, thus being exponentially small in the size of the system.

It follows from Eq.4.11 that the rank of the reduced density matrix of the target register at this point of the computation is

$$\text{rank}(\rho_{\text{target}}) \sim r \, . \tag{4.12}$$

Because $r \in [1, N]$, this rank is usually $O(N)$. If this were not the case, for example if r were $O(\log_2 N)$, then the order-finding problem could be efficiently solved by a classical naive algorithm and it would not be considered as classically hard. Because N is exponentially big in the number of qubits, we have found a particular bipartition of the system (namely, the bipartition between the source register and the target register) and a step in the quantum algorithm in which the entanglement, as measured by the rank of the reduced density matrix of one of the subsystems, is exponentially big. This implies in turn that Shor's quantum factoring algorithm can not be efficiently classically simulated by any protocol in [49] owing to the fact that at this step $\chi = O(N)$, therefore constituting an inherent exponential quantum speed-up based on an exponentially big amount of entanglement. It is worth noticing that the purpose of the entanglement between the two registers consists on leaving the source in the right periodic state to be processed by the quantum Fourier transform. Measuring the register right after the entangling gate disentangles the two registers while leaving the source in a periodic state, and this effect can only be accomplished by previously entangling source and target. These conclusions apply both to Shor's original proposal (circuit of Fig.4.1) and to the phase-estimation version (circuit of Fig.4.2).

The behavior of the rank of the system involves that the entropy of entanglement of the reduced density matrix at this point will essentially scale linearly with the number of qubits, $S(\rho_{\text{target}}) = \log_2 r \sim \log_2 N \sim n$, which is the hardest of all the possible scaling laws. We will find again this strong behavior for the entropy in the following section, when considering an adiabatic quantum algorithm solving an optimization NP-complete problem.

4.2 Entanglement in an adiabatic NP-complete optimization algorithm

We now turn to analyze how entanglement scales for a quantum algorithm based on adiabatic evolution [16], designed to solve the Exact Cover NP-complete problem [63]. Basic background on NP-completeness and classical complexity theory can be found in Appendix C. We first briefly review the proposal and, then, we consider the study of the properties of the system, in particular the behavior of the entanglement entropy for a given bipartition of the ground state.

4.2.1 The adiabatic quantum algorithm

The adiabatic model of quantum optimization algorithm deals with the problem of finding the ground state of a given system represented by its Hamiltonian. Many relevant computational problems, such as 3-SAT [72], can be mapped to this situation. The method is briefly summa-

rized as follows: we start from a time dependent Hamiltonian of the form

$$H(s(t)) = (1 - s(t))H_0 + s(t)H_P \,, \tag{4.13}$$

where H_0 and H_P are the initial and problem Hamiltonian respectively, and $s(t)$ is a time-dependent function satisfying the boundary conditions $s(0) = 0$ and $s(T) = 1$ for a given T. The desired solution to a certain problem is encoded in the ground state of H_P. The gap between the ground and the first excited state of the instantaneous Hamiltonian at time t will be called $g(t)$. Let us define g_{min} as the global minimum of $g(t)$ for t in the interval $[0, T]$. If at time T the ground state is given by the state $|E_0; T\rangle$, the adiabatic theorem states that if we prepare the system in its ground state at $t = 0$, which is assumed to be easy to prepare, and let it evolve under this Hamiltonian, then

$$|\langle E_0; T|\psi(T)\rangle|^2 \geq 1 - \epsilon^2 \tag{4.14}$$

provided that

$$\frac{\max|\frac{dH_{1,0}}{dt}|}{g_{min}^2} \leq \epsilon \tag{4.15}$$

where $H_{1,0}$ is the Hamiltonian matrix element between the ground and first excited state, $\epsilon << 1$, and the maximization is taken over the whole time interval $[0, T]$. Because the problem Hamiltonian encodes the solution of the problem in its ground state, we get the desired solution with high probability after a time T. A closer look at the adiabatic theorem tells us that T dramatically depends on the scaling of the inverse of g_{min}^2 with the size of the system. More concretely, if the gap is only polynomially small in the number of qubits (that is to say, it scales as $O(1/\text{poly}(n))$, the computational time is $O(\text{poly}(n))$, whereas if the gap is exponentially small ($O(2^{-n})$) the algorithm makes use of an exponentially big time to reach the solution.

The explicit functional dependence of the parameter $s(t)$ on time can be very diverse. The point of view we adopt in this Chapter is such that this time dependence is not taken into account, as we study the properties of the system as a function of s, which will be understood as the Hamiltonian parameter. We will in particular analyze the entanglement properties of the ground state of $H(s)$, as adiabatic quantum computation assumes that the quantum state remains always close to the instantaneous ground state of the Hamiltonian all along the computation. Notice that we are dealing with a system which is suitable to undergo a quantum phase transition at some critical value of the Hamiltonian parameter in the thermodynamic limit, and therefore we expect to achieve the largest quantum correlations when evolving close to this point. The question is how these large quantum correlations scale with the size of the system when dealing with interesting problems. This is the starting point for the next two sections.

4.2.2 Exact Cover

The Exact Cover NP-complete problem is a particular case of the 3-SAT problem, and is defined as follows: given the n boolean variables $\{x_i\}_{i=1,...n}$, $x_i = 0, 1 \; \forall \; i$, where i is regarded as the bit index, we define a *clause* of Exact Cover involving the three qubits i, j and k (say, clause "C")

by the equation $x_i + x_j + x_k = 1$. There are only three assignments of the set of variables $\{x_i, x_j, x_k\}$ that satisfy this equation, namely, $\{1,0,0\}$, $\{0,1,0\}$ and $\{0,0,1\}$. The clause can be more specifically expressed in terms of a boolean function in Conjunctive Normal Form (CNF) as

$$\begin{aligned}\phi_C(x_i, x_j, x_k) \quad &= (x_i \vee x_j \vee x_k) \wedge (\neg x_i \vee \neg x_j \vee \neg x_k) \wedge (\neg x_i \vee \neg x_j \vee x_k) \\ &\wedge(\neg x_i \vee x_j \vee \neg x_k) \wedge (x_i \vee \neg x_j \vee \neg x_k)\,, \end{aligned} \tag{4.16}$$

so $\phi_C(x_i, x_j, x_k) = 1$ as long as the clause is properly satisfied. An *instance* of Exact Cover is a collection of clauses which involves different groups of three bits. The problem is to find a string of bits $\{x_1, x_2 \ldots, x_n\}$ which satisfies all the clauses.

This problem can be mapped into finding the ground state of the Hamiltonian H_P of a spin-1/2 system in the following way: given a clause C define the Hamiltonian associated to this clause as

$$\begin{aligned} H_C \;=\; & \frac{1}{2}(1+\sigma_i^z)\frac{1}{2}(1+\sigma_j^z)\frac{1}{2}(1+\sigma_k^z) \\ + \; & \frac{1}{2}(1-\sigma_i^z)\frac{1}{2}(1-\sigma_j^z)\frac{1}{2}(1-\sigma_k^z) \\ + \; & \frac{1}{2}(1-\sigma_i^z)\frac{1}{2}(1-\sigma_j^z)\frac{1}{2}(1+\sigma_k^z) \\ + \; & \frac{1}{2}(1-\sigma_i^z)\frac{1}{2}(1+\sigma_j^z)\frac{1}{2}(1-\sigma_k^z) \\ + \; & \frac{1}{2}(1+\sigma_i^z)\frac{1}{2}(1-\sigma_j^z)\frac{1}{2}(1-\sigma_k^z)\,, \end{aligned} \tag{4.17}$$

where we have defined $\sigma^z|0\rangle = |0\rangle$, $\sigma^z|1\rangle = -|1\rangle$. Note the analogy between Eq.4.16 and Eq.4.17. The quantum states of the computational basis that are eigenstates of H_C with zero eigenvalue (ground states) are the ones that correspond to the bit string which satisfies C, whereas the rest of the computational states are penalized with an energy equal to one[a]. Now, we construct the problem Hamiltonian as the sum of all the Hamiltonians corresponding to all the clauses in our particular instance, that is to say,

$$H_P = \sum_{C \,\in\, \text{instance}} H_C\,, \tag{4.18}$$

so the ground state of this Hamiltonian corresponds to the quantum state whose bit string satisfies *the maximum number* of clauses (all of them if the clauses are mutually compatible). We have reduced the original problem stated in terms of boolean logic to the hard task of finding the ground state of a two and three-body interactive spin Hamiltonian with local magnetic fields. Observe that the couplings depend on the particular instance we are dealing with, and that the spin system has not an a priori well defined dimensionality neither a well defined lattice topology, in contrast with some usual simple spin models.

[a] In the next Chapter we shall consider a different implementation of H_C.

We now define our s-dependent Hamiltonian $H(s)$ as a linear interpolation between an initial Hamiltonian H_0 and H_P:

$$H(s) = (1 - s)H_0 + sH_P \tag{4.19}$$

where we take the initial Hamiltonian H_0 to be that resulting from the interaction with a magnetic field in the x direction:

$$H_0 = \sum_{i=1}^{n} \frac{d_i}{2}(1 - \sigma_i^x) \,, \tag{4.20}$$

where d_i is the number of clauses in which qubit i appears, and $\sigma^x|+\rangle = |+\rangle$, with $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, so the ground state of H_0 is an equal superposition of all the possible computational states. Observe that $H(s)$ is, apart from a constant factor, a sum of terms involving local magnetic fields in the x and z direction, together with two and three-body interaction coupling terms in the z component. We can thus expect this system to undergo a quantum phase transition (in the limit of infinite n) as s is shifted from 0 to 1. The numerical study of this phenomena is the aim of the next section.

4.2.3 Numerical results up to 20 qubits

We have randomly generated instances for Exact Cover with only one possible satisfying assignment and have constructed the corresponding problem Hamiltonians. Instances are produced by adding clauses randomly until there is exactly one satisfying assignment, starting over if we end up with no satisfying assignments. According to [63], these are believed to be the most difficult instances for the adiabatic algorithm. Our analysis proceeds as follows:

Appearance of a quantum phase transition

We have generated 300 Exact Cover instances – 300 random Hamiltonians with a non-degenerated ground state – and have calculated the ground state for 10, 12 and 14 qubits for different values of the parameter s in steps of 0.01. We then consider a particular bipartition of the system into two blocks of $n/2$ qubits, namely, the first $n/2$ qubits versus the rest, and have calculated the entanglement entropy between the two blocks. For each of the randomly generated Hamiltonians we observe a peak in the entanglement entropy around a critical value of the parameter $s_c \sim 0.7$. We have averaged the obtained curves over the 300 instances and have obtained the plot from Fig.4.3.

The point at which the entropy of entanglement reaches its maximum value is identified as the one corresponding to the critical point of a quantum phase transition in the system (in the limit of infinite size). This interpretation is reinforced by the observation of the typical energy eigenvalues of the system. For a typical instance of 10 qubits we observe that the energy gap between the ground state and the first excited state reaches a minimum precisely for a value of the parameter $s_c \sim 0.7$ (see Fig.4.4).

We observe from Fig.4.3 that the peak in the entropy is highly asymmetric with respect to the parameter s. A study of the way this peak seems to diverge near the critical region seems

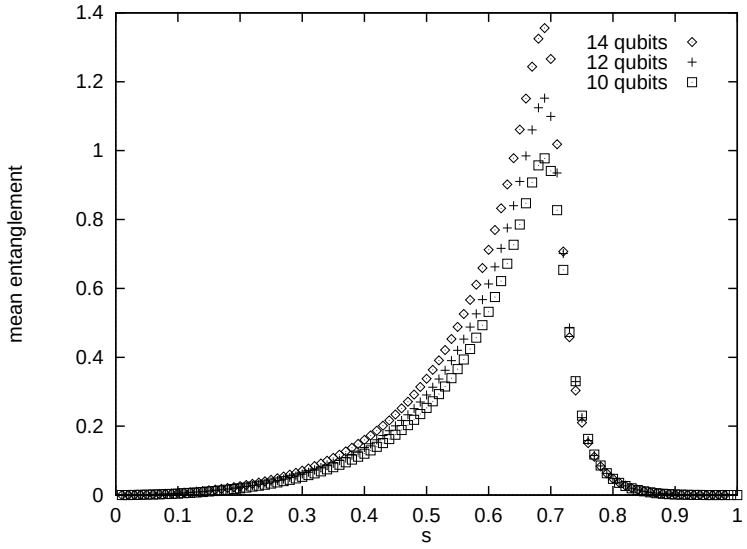

Figure 4.3: Evolution of the entanglement entropy between the two blocks of size $n/2$ when a bipartition of the system is made, on average over 300 different instances with one satisfying assignment. A peak in the correlations appears for $s_c \sim 0.7$ in the three cases.

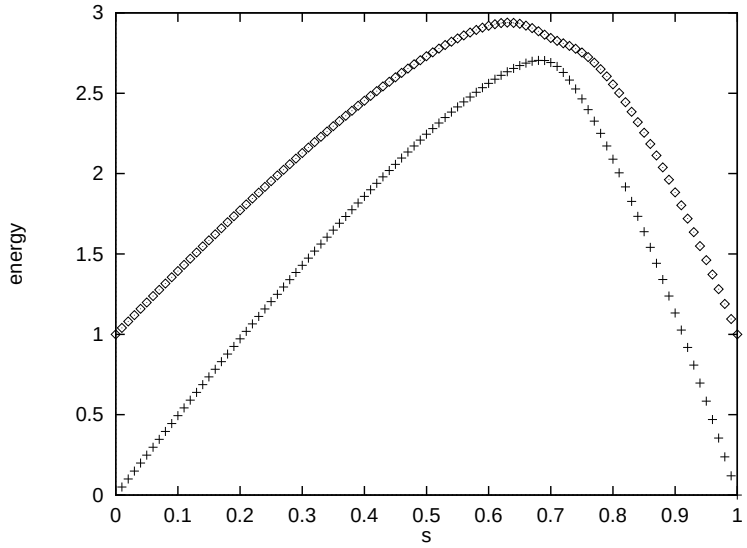

Figure 4.4: Energies of the ground state and first excited state for a typical instance with one satisfying assignment of Exact Cover in the case of 10 qubits (in dimensionless units). The energy gap approaches its minimum at $s_c \sim 0.7$.

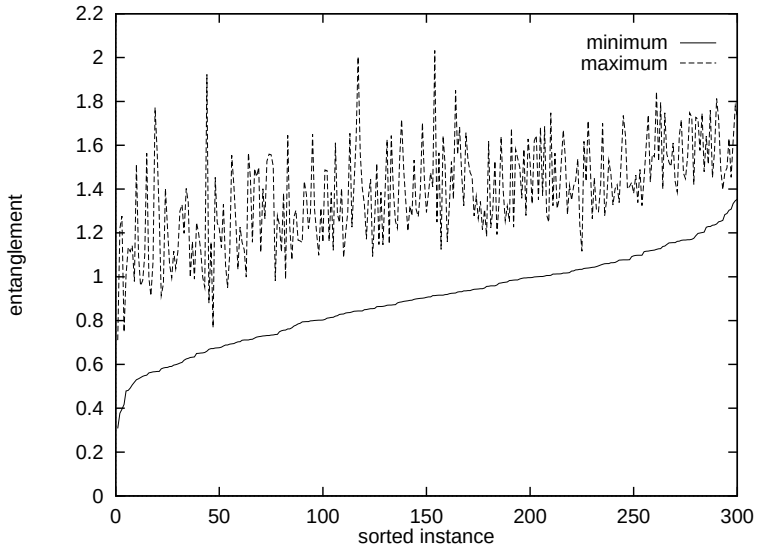

Figure 4.5: Minimum and maximum entropy over all possible bipartitions of a 10-qubit system for each of the 300 randomly generated instances of Exact Cover. Instances are sorted such that the minimum entanglement monotonically increases.

to indicate that the growth of entanglement is slower at the beginning of the evolution and fits remarkably well a curve of the type $S \sim \log_2 |\log_2 (s - s_c)|$, whereas the falling down of the peak is better parameterized by a power law $S \sim |s - s_c|^{-\alpha}$ with $\alpha \sim 2.3$, α being a certain critical exponent. These laws governing the critical region fit better and better the data as the number of qubits is increased.

Analysis of different bipartitions of the system

An explicit numerical analysis for 10 qubits tells us that all possible bipartitions for each one of the instances produce entropies at the critical point of the same order of magnitude – as expected from the non-locality of the interactions –. This is represented in Fig.4.5, where we plot the minimum and maximum entanglement obtained from all the possible bipartitions of the system for each one of the generated instances (points are sorted such that the minimum entropy monotonically increases).

Similar conclusions follow from the data plotted in Fig.4.6, where we have considered again the same quantities but looking at 64 randomly-chosen bipartitions of the ground state for 10 different instances of 16 qubits. According to these results we restrict ourselves in what follows to the analysis of a particular bipartition of the system, namely the first $n/2$ qubits versus the rest.

Scaling laws for the minimum energy gap and the entanglement entropy

To characterize the finite-size behavior of the quantum phase transition, we have generated 300 random instances of Exact Cover with only one satisfying assignment from 6 to 20 qubits,

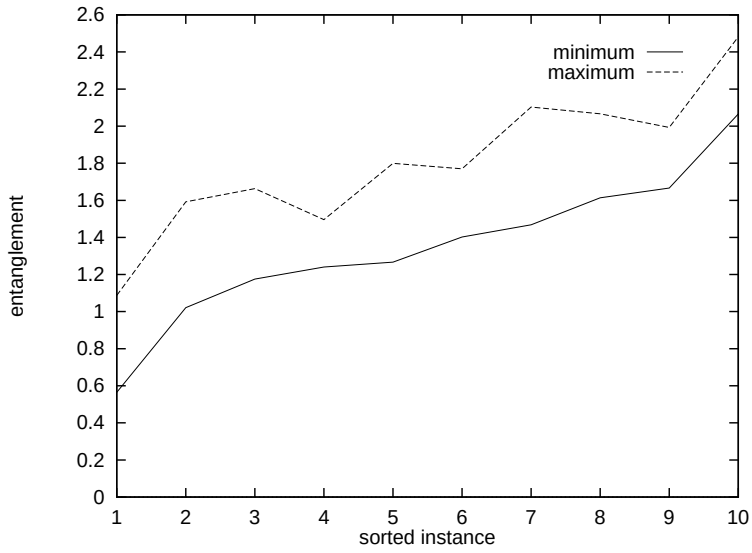

Figure 4.6: Minimum and maximum entropy over 64 bipartitions of a 16-qubit system for 10 randomly generated instances of Exact Cover. Instances are sorted such that the minimum entanglement monotonically increases.

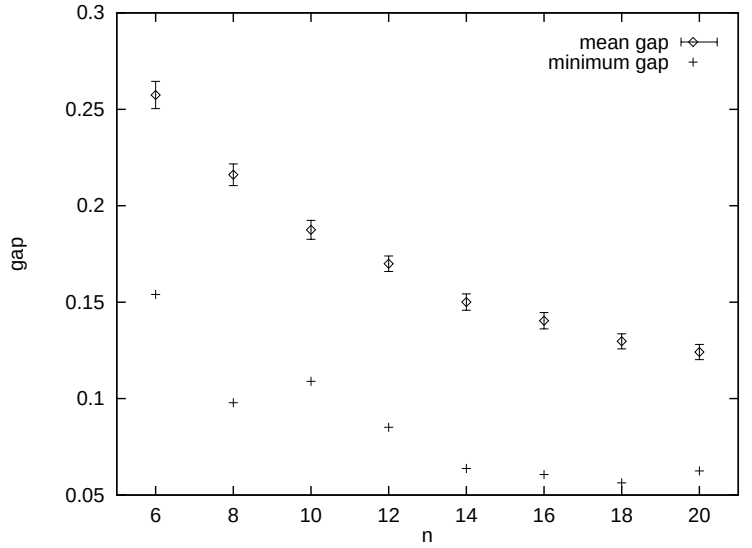

Figure 4.7: Scaling of the minimum energy gap (in dimensionless units) with the size of the system, both in the worst case and in the mean case over all the randomly generated instances. Error bars give 95 per cent of confidence level for the mean.

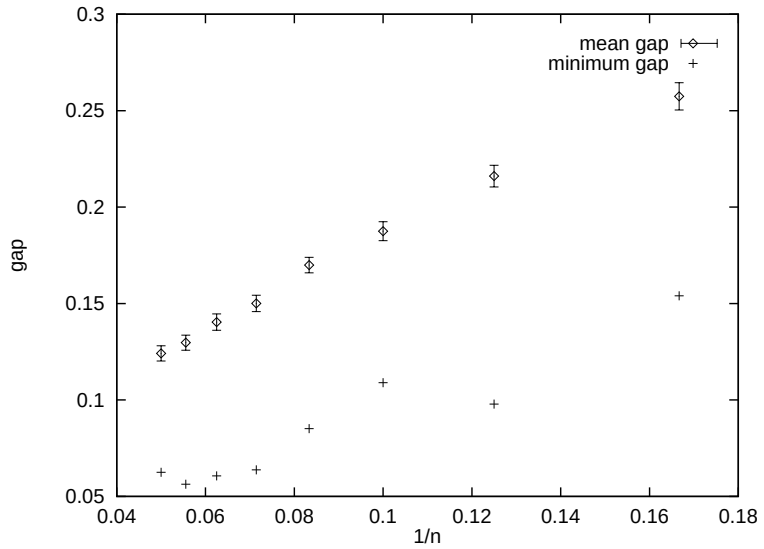

Figure 4.8: Minimum energy gap (in dimensionless units) versus the inverse size of the system, both in the worst case and in the mean case over all the randomly generated instances. Error bars give 95 per cent of confidence level for the mean. The behavior of the mean is apparently linear.

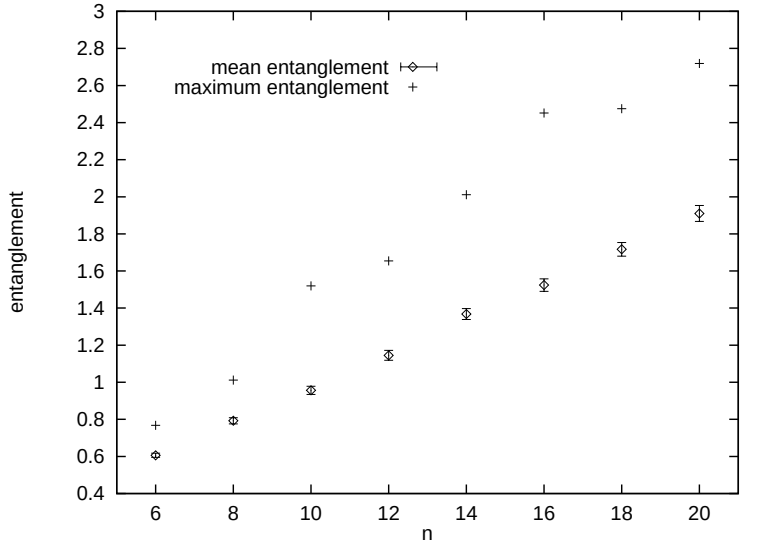

Figure 4.9: Scaling of the entanglement entropy for an equally sized bipartition of the system, both in the worst case and in the mean case over all the randomly generated instances. Error bars give 95 per cent of confidence level for the mean. The data are consistent with a linear scaling.

and studied the maximum von Neumann entropy for a bipartition of the system as well as the minimum gap, both in the worst case and in the mean case over all the randomly generated instances. We must point out that the scaling laws found in this section are limited to the small systems we can handle with our computers in an exact way. Increasing the number of qubits may lead to corrections in the numerical results, which should be of particular importance for a more precise time-complexity analysis of the adiabatic algorithm. Fig.4.7 represents the behavior of the gap in the worst and mean cases. From Fig.4.8 we observe that the gap seems to obey a scaling law of the type $O(1/n)$, n denoting the number of qubits, which would guarantee a polynomial-time quantum computation. This law is in agreement with the results in [63], and are in concordance with the idea that the energy gap typically vanishes as the inverse of the volume in condensed matter systems (here the volume is the number of qubits). Error bars in the two plots give 95 per cent of confidence level in the numerically calculated mean.

We have also considered the scaling behavior of the entanglement entropy for an equally sized bipartition of the system, again both in the worst and in the mean case. The obtained data from our simulations are plotted in Fig.4.9 – where error bars give 95 per cent of confidence level in the mean – and seem to be in agreement with a linear scaling of entanglement as a function of the size of the number of qubits. More concretely, a numerical linear fit for the mean entanglement entropy gives us the law $S \sim 0.1n$. Observe that the entropy of entanglement does not saturate at its maximum allowed value (which would be $S_{\max} = n/2$ for n qubits), so we can say that only twenty percent of all the possible potential available entanglement appears in the quantum algorithm. Linearity in the scaling law would imply that this quantum computation by adiabatic evolution, after a suitable discretization of the continuous time dependence, could not be classically simulated by the protocol of [49]. Given that the scaling of the gap seems to indicate that the quantum computation runs in a polynomial time in the size of the system, our conclusion is that apparently we are in front of an exponentially fast quantum computation that seems extremely difficult (if not impossible) to be efficiently simulated by classical means. This could be an inherent quantum mechanical exponential speedup that can be understood in terms of the linear scaling of the entropy of entanglement. Note also the parallelism with the behavior of the entanglement found in Shor's algorithm in the previous section. As a remark, our numerical analysis shows that the quantum algorithm is difficult to simulate classically in an efficient way, which does not necessarily imply that the quantum computer runs exponentially faster than the classical one, as our time-complexity analysis is limited to 20 qubits.

The linear behavior for the entropy with respect to the size of the system could in principle be expected according to the following qualitative reasoning. Naively, the entropy was expected to scale roughly as the area of the boundary of the splitting. This area-law is in some sense natural: since the entropy value is the same for both density matrices arising from the two subsystems, it can only be a function of their shared properties, and these are geometrically encoded in the area of the common boundary. For a system of n qubits, we observe again that this implies a scaling law for the entropy of an exact bipartition like $S \sim n^{\frac{d-1}{d}}$ (which reduces to a logarithm for $d = 1$). Our system does not have a well defined dimensionality, but owing to the fact that there are many random two and three-body interactions, the effective dimensionality of the system should be very large. Therefore, we expect a linear (or almost linear) scaling, which is what we numerically obtained. While this reasoning is not valid for critical fermionic

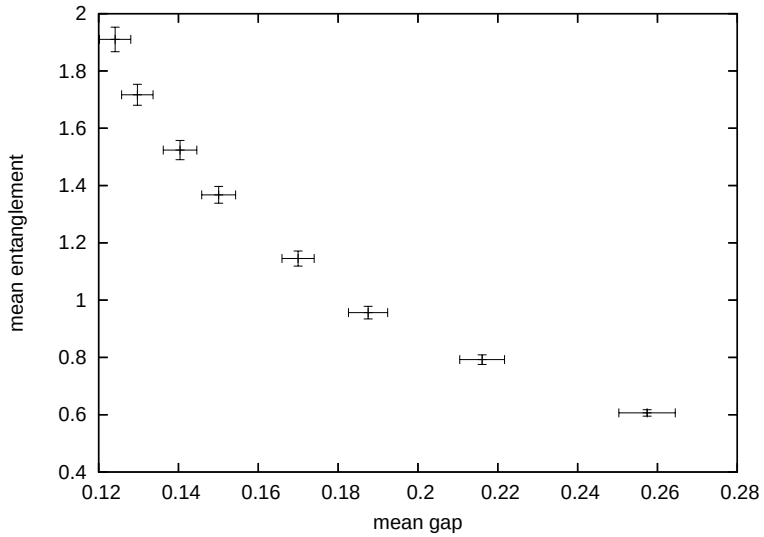

Figure 4.10: Mean entropy of entanglement versus mean size of the energy gap (in dimensionless units). Error bars give 95 per cent of confidence level for the means. Each point corresponds to a fixed number of qubits.

systems, it differs only by at most a logarithmic multiplicative correction which we did not see in our computations. The data seems to indicate that such an effective dimensionality is around $d \sim n$, thus diverging as n goes to infinity.

It is possible to compare our seemingly linear scaling of the mean entropy of entanglement with the known results obtained by averaging this quantity over the entire manifold of n-qubit pure states, with respect to the natural Fubini-Study measure. According to the results conjectured in [163] and later proved in [164], the average entropy for an equally-sized bipartition of a random n-qubit pure state in the large n limit can be approximated by $S \sim (n/2) - 1/(2 \ln 2)$ (in our notation), therefore displaying as well a linear scaling law (but different from ours). In fact, this is an indicator that most of the n-qubit pure states are highly entangled, and that adiabatic quantum computation naturally brings the system close to these highly entangled regions of the pure state manifold.

The entanglement-gap plane

The plots in Fig.4.10 and Fig.4.11 show the behavior of the peak in the entanglement versus the gap, both again in the average and the worst case for all the generated instances. Clearly, as the gap becomes smaller the production of entanglement in the algorithm increases. A compression of the energy levels correlates with high quantum correlations in the system.

Convergence of the critical points

The critical point s_c seems to be bounded by the values of s associated with the minimum gap and the maximum entropy. Actually, the value of the critical point corresponding to the

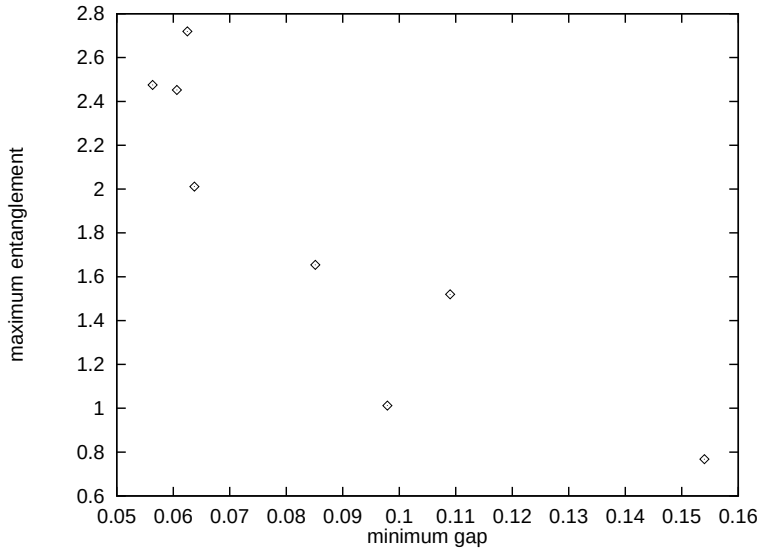

Figure 4.11: Maximum entropy of entanglement versus minimum size of the energy gap (in dimensionless units). Each point corresponds to a fixed number of qubits.

minimum size of the energy gap is systematically slightly bigger than the value of the critical point corresponding to the peak in the entropy. By increasing the size of the system these two points converge towards the same value, which would correspond to the true critical point of a system of infinite size. This effect is neatly observed in Fig.4.12, which displays the values of s associated with the mean critical points both for the gap and for the entropy as a function of n.

Universality

The above results suggest that the system comes close to a quantum phase transition. The characterization we have presented based on the study of averages over instances reconstructs its universal behavior. Results do not depend on particular microscopic details of the Hamiltonian, such as the interactions shared by the spins or the strength of local magnetic fields. Any adiabatic algorithm solving a k-sat problem and built in the same way we have done for Exact Cover should display on average exactly the same properties we have found *regardless of the value of* k, which follows from universality ($k = 1$ is a particular case, as its Hamiltonian is non-interacting). Linear scaling of entanglement should therefore be a universal law for this kind of quantum algorithms. The specific coefficients of the scaling law for the entropy should be a function only of the connectivity of the system, that is on the type of clauses defining the instances.

We have explicitly checked this assertion by numerical simulations for clauses of Exact Cover but involving 4 qubits ($x_i + x_j + x_k + x_l = 1$), which is a particular case of 4-SAT. In Fig.4.13 we plot the behavior of the entropy of entanglement for a 10-qubit system for these type of clauses and compare it to the same quantity calculated previously for the clauses involving 3 qubits (the common Exact Cover Hamiltonian). We observe again the appearance of a peak in the entropy, which means that the system is evolving close to a quantum phase transition.

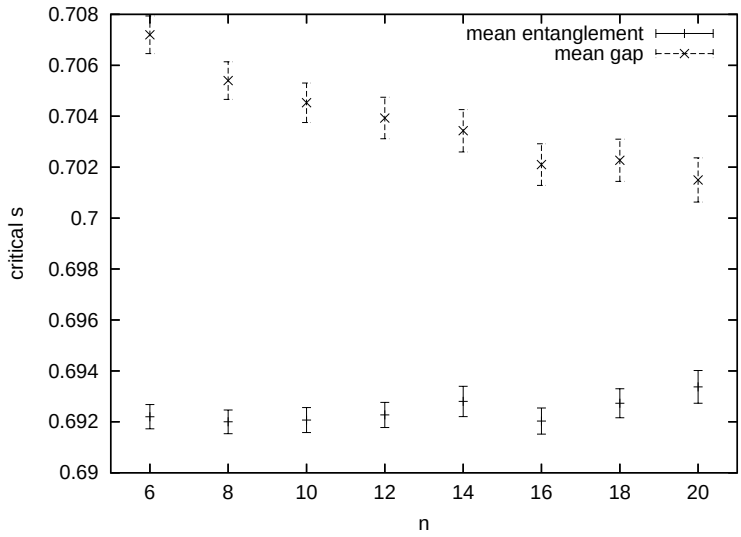

Figure 4.12: Mean critical point for the energy gap and for the entropy. Error bars give 95 per cent of confidence level for the means. Note that they tend to approach as the size of the system is increased.

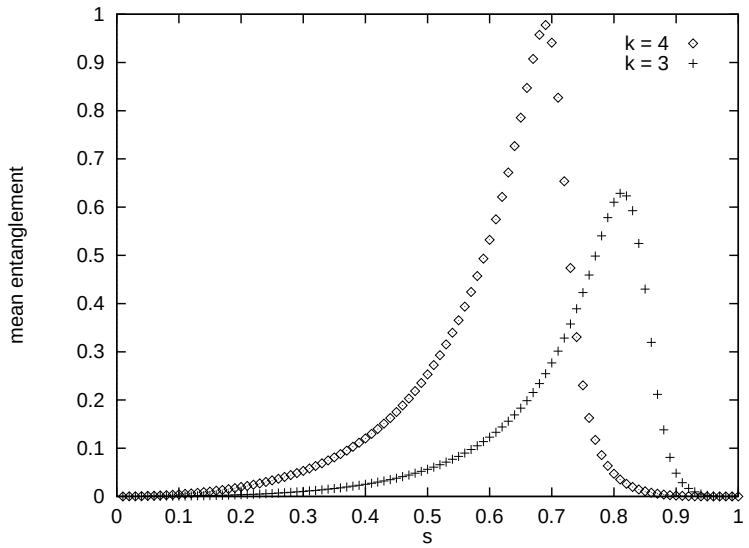

Figure 4.13: Entanglement as a function of the Hamiltonian parameter for clauses of Exact Cover involving 3 ($k = 3$) and 4 ($k = 4$) qubits, for a 10-qubit system, averaged over all the randomly generated instances.

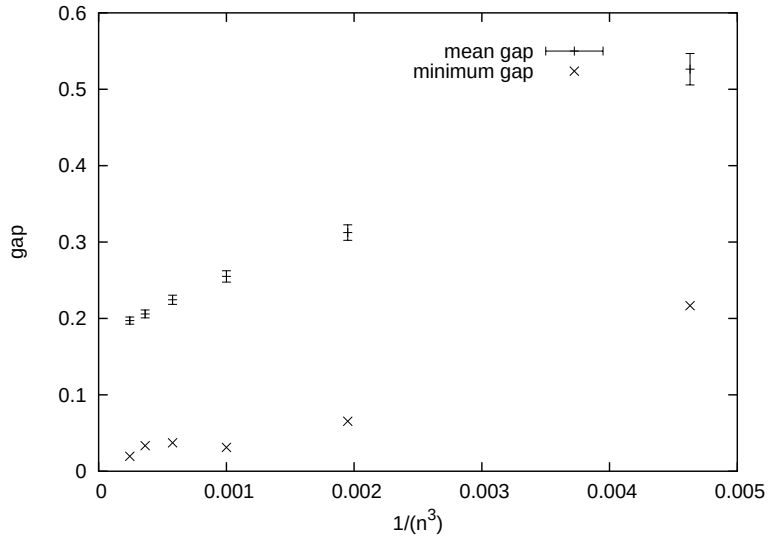

Figure 4.14: Minimum energy gap (in dimensionless units) versus $1/(n^3)$, both in the worst and in the mean cases over all the randomly generated instances of clauses involving 4 qubits, up to $n = 16$. Error bars give 95 per cent of confidence level for the mean. The behavior seems to be linear.

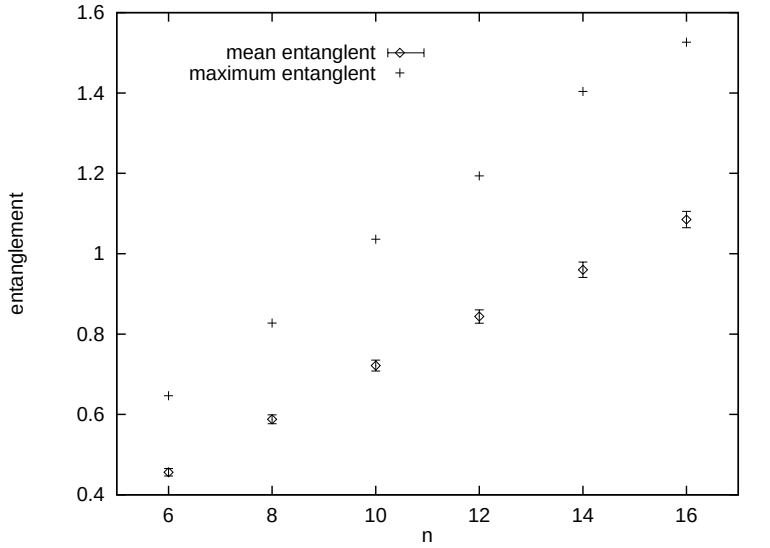

Figure 4.15: Scaling of the entanglement entropy for an equally sized bipartition of the system, both in the worst and in the mean cases over all the randomly generated instances of clauses involving 4 qubits, up to $n = 16$. Error bars give 95 per cent of confidence level for the mean. The data are consistent with a linear scaling.

Fig.4.14 and Fig.4.15 respectively show the scaling of the energy gap in the mean and worst case and the scaling of the peak in the entropy in the mean and worst case as well, up to 16 qubits. Error bars give again 95 per cent of confidence level for the means. The behavior is similar to the one already found for the instances of Exact Cover involving 3 qubits (Fig.4.8 and Fig.4.9), which supports the idea of the universality of the results. The minimum energy gap seems to scale in this case as $\sim \frac{1}{n^3}$ (n being the number of qubits), which would guarantee again a polynomial-time quantum adiabatic evolution.

4.3 Entanglement in adiabatic quantum searching algorithms

Grover's quantum algorithm solves the problem of finding a "needle in a haystack", which is mathematically defined as finding a specific element of an unsorted database by means of calls to an oracular function. If the database is composed of 2^n elements, n being the number of bits, then the best classical algorithm for solving this problem takes $O(2^n)$ time as measured in calls to the oracle, whereas Grover's quantum algorithm takes only $O(2^{n/2})$ calls to the quantum implementation of the oracular function [9]. Optimality of Grover's quantum algorithm has been proven as well [165].

Let us now consider the adiabatic implementation of Grover's quantum searching algorithm in terms of a Hamiltonian evolution [9, 69, 70] and study its properties as a function of the number of qubits and the parameter s. For this problem, it is possible to compute all the results analytically, so we shall get a closed expression for the scaling of entanglement. As a side remark, it is worth noting that the treatment made in [49] is not valid for the oracular model of quantum computation, as it is assumed that all quantum gates are known in advanced. Independently of this issue, we shall see that the system remains weakly entangled between calls to the oracle.

4.3.1 Adiabatic quantum search

Grover's searching algorithm [9] can be implemented in adiabatic quantum computation by means of the s-dependent Hamiltonian

$$H(s) = (1-s)(I - |\psi\rangle\langle\psi|) + s(I - |x_0\rangle\langle x_0|)\,, \tag{4.21}$$

where $|\psi\rangle \equiv \frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} |x\rangle$, n is the number of qubits, and $|x_0\rangle$ is the marked state. The computation takes the quantum state from an equal superposition of all computational states directly to the state $|x_0\rangle$, as long as the evolution remains adiabatic. The time the algorithm takes to succeed depends on how we choose the parameterization of s in terms of time. Our aim here is to compute the amount of entanglement present in the register and need not deal with the explicit dependence of the parameter s on time and its consequences (see [69, 70] for further information about this topic).

It is straightforward to check that the Hamiltonian from Eq.4.21 has its minimum gap between the ground and first excited states at $s = 0.5$, which goes to zero exponentially fast as the number of qubits in the system is increased. Therefore, this Hamiltonian apparently seems to

undergo a quantum phase transition in the limit of infinite size at $s = 0.5$. Quantum correlations approach their maximum for this value of s.

4.3.2 Analytical results

It can be seen (see for example [166]) that the ground state energy of the Hamiltonian given in Eq.4.21 corresponds to the expression

$$E_-(s) = \frac{1}{2}\left(1 - \sqrt{(1-2s)^2 + \frac{4}{2^n}s(1-s)}\right) , \tag{4.22}$$

s denoting the Hamiltonian parameter. The corresponding normalized ground state eigenvector is given by

$$|E_-(s)\rangle = a|x_0\rangle + b\sum_{x\neq x_0}|x\rangle , \tag{4.23}$$

where we have defined the quantities

$$\begin{aligned} a &\equiv \alpha\, b \\ b^2 &\equiv \frac{1}{2^n - 1 + \alpha^2} \\ \alpha &\equiv \frac{2^n - 1}{2^n - 1 - \left(\frac{2^n}{1-s}\right)E_-(s)} . \end{aligned} \tag{4.24}$$

In all the forthcoming analysis we will assume that the marked state corresponds to $|x_0\rangle = |0\rangle$, which will not alter our results. The corresponding density matrix for the ground state of the whole system of n qubits is then given by

$$\rho_n = b^2(\alpha^2 - 2\alpha + 1)|0\rangle\langle 0| + b^2|\phi\rangle\langle\phi| + b^2(\alpha - 1)(|\phi\rangle\langle 0| + |0\rangle\langle\phi|) , \tag{4.25}$$

where we have defined $|\phi\rangle$ as the the unnormalized sum of all the computational quantum states (including the marked one), $|\phi\rangle \equiv \sum_{x=0}^{2^n-1}|x\rangle$. Taking the partial trace over half of the qubits, regardless of what $n/2$ qubits we choose, we find the reduced density matrix

$$\rho_{n/2} = b^2(\alpha^2 - 2\alpha + 1)|0'\rangle\langle 0'| + 2^{n/2}b^2|\phi'\rangle\langle\phi'| + b^2(\alpha - 1)(|\phi'\rangle\langle 0'| + |0'\rangle\langle\phi'|) , \tag{4.26}$$

where we understand that $|0'\rangle$ is the remaining marked state for the subsystem of $n/2$ qubits and $|\phi'\rangle \equiv \sum_{x=0}^{2^{n/2}-1}|x\rangle$ is the remaining unnormalized equally superposition of all the possible computational states for the subsystem. Defining the quantities

$$\begin{aligned} A &\equiv \frac{\alpha^2 + 2^{n/2} - 1}{\alpha^2 + 2^n - 1} \\ B &\equiv \frac{\alpha + 2^{n/2} - 1}{\alpha^2 + 2^n - 1} \\ C &\equiv \frac{2^{n/2}}{\alpha^2 + 2^n - 1} \end{aligned} \tag{4.27}$$

(note that $A + (2^{n/2} - 1)C = 1$), the density operator for the reduced system of $n/2$ qubits can be expressed in matrix notation as

$$\rho_{n/2} = \begin{pmatrix} A & B & \cdots & B \\ B & C & \cdots & C \\ \vdots & \vdots & \ddots & \vdots \\ B & C & \cdots & C \end{pmatrix} \tag{4.28}$$

in the computational basis, where its dimensions are $2^{n/2} \times 2^{n/2}$. We clearly see that the density matrix has a rank equal to 2. Therefore, because $\text{rank}(\rho) \geq 2^{S(\rho)}\ \forall\rho$ (where $S(\rho)$ is the von Neumann entropy of the density matrix ρ) we conclude that $S(\rho_{n/2})$, which corresponds to our entanglement measure between the two blocks of qubits, is always ≤ 1. This holds true even for non symmetric bipartitions of the complete system. Regardless of the number of qubits, entanglement in Grover's adiabatic algorithm is always a *bounded* quantity for any s, in contrast with the results obtained in the previous sections for Shor's factoring algorithm and for the Exact Cover problem. Grover's adiabatic quantum algorithm essentially makes use of very little entanglement between calls to the quantum oracle, but even this bounded quantity of quantum correlations is enough to give a square-root speedup.

We have explicitly calculated the von Neumann entropy for $\rho_{n/2}$. Because the rank of the reduced density matrix is two, there are only two non-vanishing eigenvalues that contribute in the calculation which are

$$\lambda_{\pm} = \frac{1}{2}\left(1 \pm \sqrt{1 - 4(2^{n/2} - 1)(AC - B^2)}\right) . \tag{4.29}$$

We analyze the limit $n \to \infty$ for $s \neq 0.5$ and $s = 0.5$ separately.

Entropy at $s \neq 0.5$

In the limit of very high n we can approximate the ground state energy given in Eq.4.22 by

$$E_{-}(s) \sim \frac{1}{2}\left(1 - \sqrt{1 - 4s(1-s)}\right) . \tag{4.30}$$

Therefore, the quantity

$$\alpha \sim \frac{1}{1 - \left(\frac{E_{-}(s)}{1-s}\right)} \tag{4.31}$$

diverges at $s = 0.5$, which implies that this limit can not be correct for that value of the parameter. The closer we are to $s = 0.5$, the bigger is α. In this limit we find that

$$A \sim \frac{\alpha^2 + 2^{n/2}}{\alpha^2 + 2^n} \tag{4.32}$$

$$B \sim \frac{\alpha + 2^{n/2}}{\alpha^2 + 2^n} \tag{4.33}$$

$$C \sim \frac{2^{n/2}}{\alpha^2 + 2^n} , \tag{4.34}$$

where all these quantities tend to zero as $n \to \infty$. It is important to note that the convergence of the limit depends on the value of α or, in other words, how close to $s = 0.5$ we are. The closer we are to $s = 0.5$, the slower is the convergence, and therefore any quantity depending on these parameters (such as the entropy) will converge slower to its asymptotical value. For the eigenvalues of the reduced density matrix we then find that when $n \to \infty$

$$\lambda_\pm \to \frac{1}{2}(1 \pm 1) , \tag{4.35}$$

so $\lambda_+ \sim 1$ and $\lambda_- \sim 0$, and therefore the asymptotical entropy is

$$S(s \neq 0.5, n \to \infty) = -\lambda_+ \log_2 \lambda_+ - \lambda_- \log_2 \lambda_- = 0 . \tag{4.36}$$

The convergence of this quantity is slower as we move towards $s = 0.5$.

Entropy at $s = 0.5$

We begin our analysis by evaluating the quantities at $s = 0.5$ and then taking the limit of big size of the system. We have that $\alpha(s = 0.5) = \frac{2^n - 1}{2^{n/2} - 1} \sim 2^{n/2}$. From here it is easy to get the approximations

$$A \sim \frac{1}{2}$$

$$B \sim \frac{1}{2^{n/2}}$$

$$C \sim \frac{1}{2^{n/2+1}} , \tag{4.37}$$

and therefore

$$\lambda_\pm \sim \frac{1}{2}\left(1 \pm \sqrt{1 - 4\, 2^{n/2}\left(\frac{1}{4}\frac{1}{2^{n/2}} - \frac{1}{2^n}\right)}\right) = \frac{1}{2} \pm \frac{1}{2^{n/4}} , \tag{4.38}$$

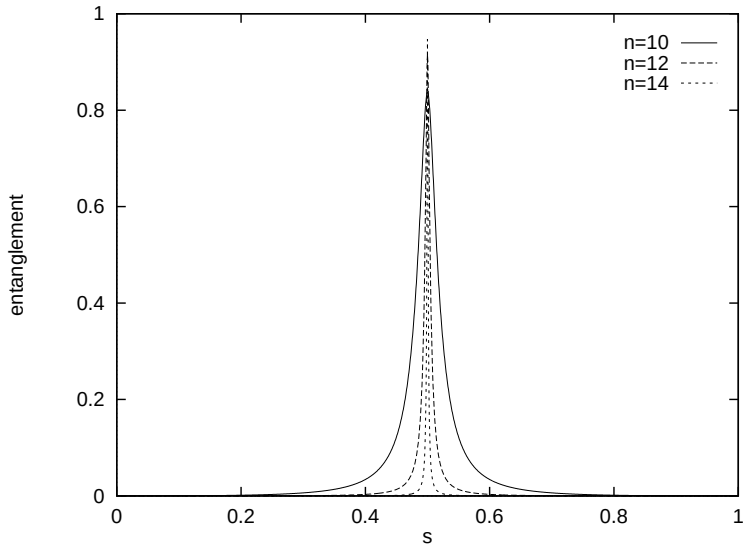

Figure 4.16: Von Neumann entropy for the reduced system as a function of s for 10, 12 and 14 qubits. As the size of the system increases the entropy tends to zero at all points, except at $s = 0.5$ in which tends to 1.

so $\lambda_{\pm} \to \frac{1}{2}$ and $S(s = 0.5, n \to \infty) = 1$. According to Eq.4.38 we can evaluate the finite size corrections to this behavior and find the scaling of the entropy with the size of the system for very large n. The final result for the entropy at the critical point reads

$$S(s = 0.5, n \gg 1) \sim 1 - \frac{4}{\ln 2} 2^{-n/2} \, . \tag{4.39}$$

Note that the entropy remains bounded and tends to 1 for $s = 0.5$ as a square root in the exponential of the size of the system, which is the typical factor in Grover's quantum algorithm.

We have represented the evolution of the entanglement entropy as a function of s for different sizes of the system in Fig.4.16 and have plotted in Fig.4.17 the maximum value of the entropy along the computation as a function of the size of the system according to the expression given in Eq.4.39. We can now compare the two plots with Fig.4.3 and Fig.4.9 in the previous section. The behavior for the entropy in Grover's adiabatic algorithm is dramatically different to the one observed in the NP-complete problem. Entanglement gets saturated in Grover's adiabatic algorithm *even at the point at which the gap vanishes*, which reminds us of short ranged quantum correlations in non-critical quantum spin chains[b].

Let us note that, in the limit of infinite size, the quantum state in Grover's algorithm is separable with respect to any bipartition of the system (and therefore not entangled, as it is a pure state) for any s except for $s = 0.5$. All the entanglement along the algorithm is concentrated at this point, but this entanglement is still a bounded quantity and actually equal to 1. Consequently, a small amount of entanglement appears essentially only at one point when the size

[b] A somehow similar situation is present in (1 + 1)-dimensional quantum spin chains outside of the critical region, where the entanglement entropy also reaches a saturation when increasing the size of the system [22, 37, 38]. Saturation does not appear in higher dimensional systems.

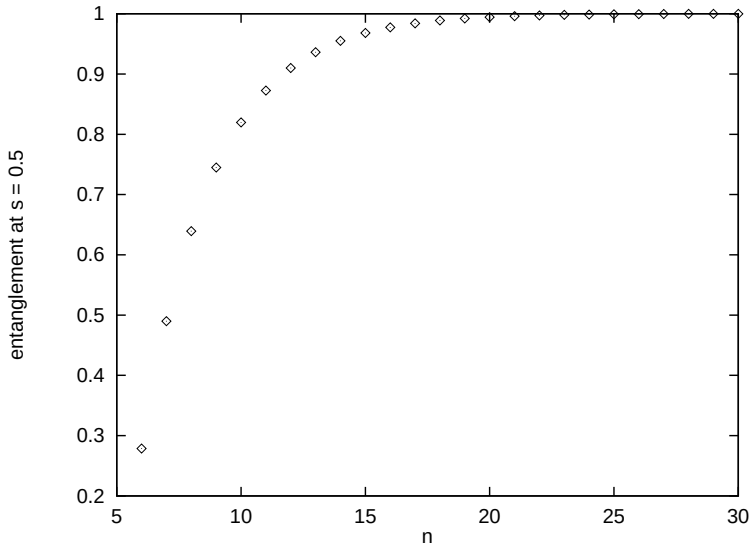

Figure 4.17: Von Neumann entropy for the reduced system at $s = 0.5$ as a function of n. For infinite size of the system there is a saturation at 1.

of the system is big, whereas the rest of the algorithm needs to handle just separable states. We point out that these results apply as well to the traditional discrete-time implementation of Grover's searching algorithm, as the states between iterations are the same as in the adiabatic version for discrete s values.

4.4 Conclusions of Chapter 4

In this Chapter we have studied the scaling of the entanglement entropy in several quantum algorithms. In order to be precise:

- We have analytically proven that Shor's factoring quantum algorithm makes use of an exponentially large amount of entanglement in the size of the system between the target register and the source register after the modular exponentiation operation, which in turn implies the impossibility of an efficient classical simulation by means of the protocol of Vidal in [49].

- We have provided numerical evidence for a universal linear scaling of the entropy with the size of the system together with a polynomially small gap in a quantum algorithm by adiabatic evolution devised to solve the NP-complete Exact Cover problem, therefore obtaining a polynomial-time quantum algorithm which would involve exponential resources if simulated classically, in analogy to Shor's algorithm. Universality of this result follows from the fact that the quantum adiabatic algorithm evolves close to a quantum phase transition and the properties at the critical region do not depend on particular details of the microscopic Hamiltonian (instance) such as interactions among the spins or local magnetic fields.

- We have also proven that the von Neumann entropy remains bounded by 1 between calls to the quantum oracle in Grover's adiabatic algorithm regardless of the size of the system and even at the critical point. More concretely, the maximum entropy approaches one as a square root in the size of the system, which is the typical Grover's scaling factor.

Our results show that studying the scaling of the entropy is a useful way of analyzing entanglement production in quantum computers. Results from the study of quantum many-body systems can be directly applied to bring further insight into the analysis of the quantum correlations present in a quantum computer. Different entanglement scaling laws follow from different situations according to the amount of correlations involved, as can be seen in Table 4.1. A quantum algorithm can be understood as the simulation of a system evolving close to a quantum phase transition. The amount of entanglement involved depends on the effective dimensionality of the system, which in turn governs the possibilities of certain efficient classical simulation protocols.

⟵ less entanglement	Problem	Scaling of the entanglement entropy
	Adiabatic Exact Cover's quantum algorithm	$S = O(n)$
	Shor's quantum factoring algorithm	$S = O(\log_2 r) \sim O(n)$
	Critical $(d+1)$-dimensional fermionic lattices	$S = O(n^{\frac{d-1}{d}} \log_2 n)$
	Critical $(d+1)$-dimensional bosonic lattices	$S = O(n^{\frac{d-1}{d}})$
	Critical $(1+1)$-dimensional spin chains	$S = O(\log_2 n)$
	Non-critical $(1+1)$-dimensional spin chains	$S = O(1)$
	Adiabatic Grover's quantum algorithm	$S = O(1)$

Table 4.1: Entanglement scaling laws in different problems, in decreasing complexity order.

These scaling laws provide also a new way of understanding some aspects from one-way quantum computation. It is known that the so-called cluster state of the one-way quantum computer can be generated by using Ising-like interactions on a planar $(2+1)$-dimensional lattice [167–169]. This fact can be related to the at least linear (in the size of a box) behavior of the entropy for spin systems in $(2+1)$ dimensions. $(1+1)$-dimensional models seem not to be able to efficiently create the highly-entangled cluster state. Again, this fact can be traced to the logarithmic scaling law of the entropy in spin chains which is insufficient to handle the

large amount of entanglement to carry out for instance Shor's algorithm. Note also that $(d+1)$-dimensional systems with $d \geq 3$ bring unnecessarily large entanglement.

Quantum phase transitions stand as demanding systems in terms of entanglement. They are very hard to simulate classically. It is then reasonable to try to bring NP-complete problems to a quantum phase transition setup, which quantum mechanics handles naturally.

Chapter 5

Classical simulation of quantum algorithms using matrix product states

In Chapter 4 we saw that understanding the detailed behavior and properties of quantum many-body systems plays a role in different areas of physics. Those systems whose properties can be analytically found are typically called *integrable* systems and offer a way to study, for instance, the low-energy sector of different models. It is a pity, though, that many of the models that we know are not integrable, in the sense that it is not even known whether it is possible or not to study in an exact way their fundamental properties. The realistic alternative is, then, to use different techniques based on numerical simulations by means of computer programs, so that we can get a detailed understanding of the system.

While it is possible to numerically study the low-energy properties of any model by means of an exact diagonalization of the quantum Hamiltonian or related techniques, such a possibility is always limited to a relatively small number of particles due to the exponential growth in the size of the Hilbert space. Indeed, this is at the heart of the motivation to build a quantum computer, as originally proposed by Feynman [1]. Using standard present technology, a faithful numerical study of the ground-state properties of a general quantum Hamiltonian can be achieved for systems up to the order of 20 spins, as we did in the previous Chapter. Luckily enough, other numerical techniques are possible. For instance, quantum Montecarlo algorithms have provided good results for some systems while they fail for some others due to the presence of the so-called sign problem [170]. Another example of successful numerical technique has been the density matrix renormalization group (DMRG) algorithm, as introduced by White in [20]. While it was soon realized that DMRG produced extremely accurate results when computing the ground-state energy of quantum systems in one spatial dimension, it was also realized that the method did not work so well when applied to higher dimensional systems [171, 172]. Even in the $(1 + 1)$-dimensional case, there was a difference in the performance of the algorithm between open and periodic boundary conditions, and between non-critical and critical systems, the former being the more successful in both cases. Nevertheless, DMRG has been the algorithm of reference for computing the low-energy properties of quantum models with one spatial dimension during the last decade.

After the appearance of DMRG, a notorious result was found by Ostlund and Rommer

in [47], where they showed that the original DMRG algorithm can be completely understood in terms of the so-called matrix product states. Originally introduced in the valence-bond model of Affleck, Kennedy, Lieb and Tasaki [45, 46], generalized by Fannes, Nachtergaele and Werner [48], and rediscovered in the field of quantum information science by Vidal [49], matrix product states have been proved to be an extremely useful tool in order to develop numerical techniques for computing the low-energy properties together with the dynamics of sufficiently local Hamiltonians in one spatial dimension [50–57], and have inspired as well several numerical techniques to study higher-dimensional systems [58–60].

The natural question arises of whether matrix product states can be applied to simulate the dynamics of a quantum computer. The content of this Chapter is aimed to show that this is indeed possible and that we can handle relatively large simulations with controlled accuracy. We call the parameter controlling the size of the matrices χ, which was already introduced in Chapter 4, and which can in turn be related to the entanglement entropy S of a considered bipartition of the system like $\chi \geq 2^{S(\rho)}$. As we shall see, the total time cost of the simulation scales polynomially in parameter χ. Thus, we expect this approximation scheme to fail whenever the inherently needed χ is $O(2^n)$, n being the number of qubits of the quantum register. Nevertheless, it may be possible in some of these cases that by keeping only $\chi = O(\text{poly}(n))$ in the simulation we already get a reasonable approximation to the exact computation. This is indeed the case of the quantum algorithm that we consider here. We study the numerical performance of the classical simulation scheme for quantum computations originally proposed by Vidal in [49] based on matrix product states, when applied to the simulation of an adiabatic quantum algorithm solving the Exact Cover NP-complete problem. The performance of this quantum algorithm was already addressed in Chapter 4, where we saw that the typical entanglement entropy of the system for a given bipartition tends to scale roughly as $S \sim 0.1n$, which makes the parameter χ exponentially big in the number of qubits and thus forbids the possibility of an *exact* classical simulation. Nevertheless, the fact that the coefficient in front of the scaling law of the entropy is small inspires us to think that, perhaps, it should still be possible to perform a relatively good *approximated* classical simulation of the quantum algorithm by keeping a small amount of χ along the evolution. Notice that this is a necessary, while not sufficient condition to have a good approximation of the evolution of the quantum algorithm. Let us then proceed in what follows with an explanation of what matrix product states are and how do they inspire numerical simulation algorithms for time evolution, moving then to our explicit results on the numerical simulation of a quantum computer.

5.1 The matrix product state ansatz

A matrix product state is a parameterization of a pure quantum state of n local systems (like, for instance, qubits) in terms of the amount of bipartite entanglement present in the state. Here we derive this ansatz from two different perspectives: on the one hand, we show how matrix product states appear from the point of view inspired by Affleck, Kennedy, Lieb and Tasaki in [45, 46] based on projectors on some ancillary unphysical particles; on the other hand, we show how it is possible to obtain a matrix product state by means of a series of Schmidt decompositions of the quantum state at hand, in the way done by Vidal in [49]. These two perspectives complement

each other, and give different insights about the significance of the different parameters and quantities that appear in the ansatz.

Derivation by means of projectors

Let us consider a set of n physical local d-level systems, described by (pure) quantum state given by

$$|\psi\rangle = \sum_{i_1=1}^{d} \sum_{i_2=1}^{d} \cdots \sum_{i_n=1}^{d} c_{i_1,i_2,\ldots,i_n} |i_1, i_2, \ldots, i_n\rangle \,, \tag{5.1}$$

where the states $|i_l\rangle$, $l = 1, 2, \ldots, n$ denote a local d-level basis, and $c_{i_1,i_2,\ldots,i_n}$ are the corresponding d^n coefficients specifying the state. We now consider the following picture. First, imagine that the local systems are placed on a linear chain. Second, let us represent the physical local d-level systems by means of two ancillary unphysical particles, each one of them being described by a Hilbert space of dimension χ, together with a projector from the joint ancillary Hilbert space of dimension χ^2 to the physical Hilbert space of dimension d. We also assume that the state of the ancillary particles (without the projectors) is in a dimerized state of maximally entangled pairs of dimension χ. The projector on the local Hilbert space at site l is represented by the three-index tensor

$$A^{(l)i_l}_{\alpha_{l-1}\alpha_l} \,, \tag{5.2}$$

where the index $i_l = 1, 2, \ldots, d$ corresponds to the physical local Hilbert space, while the indexes $\alpha_{l-1} = 1, 2, \ldots, \chi$ and $\alpha_l = 1, 2, \ldots, \chi$ correspond to the two ancillary Hilbert spaces. This is represented in Fig.5.1.

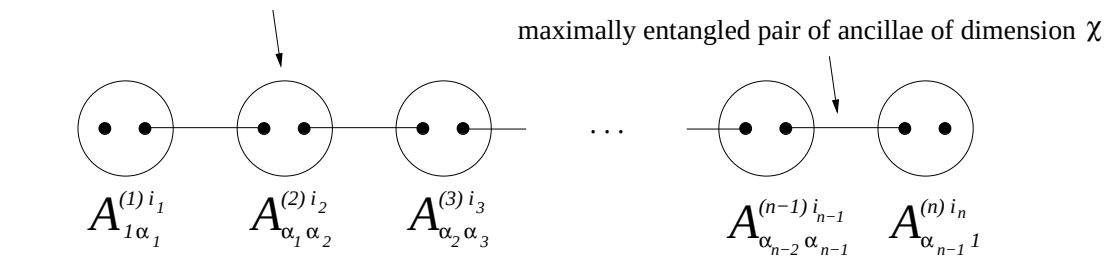

Figure 5.1: Graphical representation of a matrix product state in terms of projections. The projectors act on a dimerized state of maximally entangled pairs of dimension χ.

At every site, and for each value of the physical index, we have then a matrix. Because the ancillary particles are in a dimerized state of maximally entangled pairs, the coefficients $c_{i_1,i_2,\ldots,i_n}$

of the system are decomposed as products of matrices, hence the name of matrix product state. The explicit form of the state is

$$|\psi\rangle = \sum_{\{i\}} \sum_{\{\alpha\}} A^{(1)i_1}_{1\alpha_1} A^{(2)i_2}_{\alpha_1\alpha_2} \dots A^{(n)i_n}_{\alpha_{n-1}1} |i_1, i_2, \dots, i_n\rangle \,, \tag{5.3}$$

where the sums are to be understood from now on over the complete range of the set of physical indices $\{i\}$ and ancillary indices $\{\alpha\}$.

Derivation by means of Schmidt decompositions

Consider again the same set of n physical local d-level systems described by the pure state of Eq.5.1, where we assume as before that the local systems are sorted from 1 to n in such a way that they can be thought as placed on a linear chain. Following Vidal [49], if we perform the Schmidt decomposition between the local system 1 and the remaining $n-1$ we can write the state as

$$|\psi\rangle = \sum_{\alpha_1} \lambda^{(1)}_{\alpha_1} |\phi^{(1)}_{\alpha_1}\rangle |\phi^{(2\cdots n)}_{\alpha_1}\rangle \,, \tag{5.4}$$

where $\lambda^{(1)}_{\alpha_1}$ are the Schmidt coefficients, $|\phi^{(1)}_{\alpha_1}\rangle$ and $|\phi^{(2\cdots n)}_{\alpha_1}\rangle$ are the corresponding left and right Schmidt vectors, and $\alpha_1 = 1, 2, \dots, d$. By expressing the left Schmidt vector in terms of the original local basis for system 1 the state can then be written as

$$|\psi\rangle = \sum_{i_1,\alpha_1} \Gamma^{(1)i_1}_{1\alpha_1} \lambda^{(1)}_{\alpha_1} |i_1\rangle |\phi^{(2\cdots n)}_{\alpha_1}\rangle \,, \tag{5.5}$$

$\Gamma^{(1)i_1}_{1\alpha_1}$ being the appropriate coefficients of the change of basis, that is, $|\phi^{(1)}_{\alpha_1}\rangle = \sum_{i_1} \Gamma^{(1)i_1}_{1\alpha_1} |i_1\rangle$. At this point, we expand each Schmidt vector $|\phi^{(2\cdots n)}_{\alpha_1}\rangle$ in the original local basis for system 2, that is,

$$|\phi^{(2\cdots n)}_{\alpha_1}\rangle = \sum_{i_2} |i_2\rangle |\omega^{(3\cdots n)}_{\alpha_1 i_2}\rangle \,. \tag{5.6}$$

We now write the unnormalized quantum state $|\omega^{(3\cdots n)}_{\alpha_1 i_2}\rangle$ in terms of the at most d^2 eigenvectors of the joint reduced density matrix for systems $(3, 4, \dots, n)$, that is, in terms of the right Schmidt vectors $|\phi^{(3\cdots n)}_{\alpha_2}\rangle$ of the particular bipartition between the first two local systems and the rest, together with the corresponding Schmidt coefficients $\lambda^{(2)}_{\alpha_2}$:

$$|\omega^{(3\cdots n)}_{\alpha_1 i_2}\rangle = \sum_{\alpha_2} \Gamma^{(2)i_2}_{\alpha_1\alpha_2} \lambda^{(2)}_{\alpha_2} |\phi^{(3\cdots n)}_{\alpha_2}\rangle \,. \tag{5.7}$$

Replacing the last two expressions into Eq.5.5 we obtain

$$|\psi\rangle = \sum_{i_1,\alpha_1,i_2,\alpha_2} \Gamma^{(1)i_1}_{1\alpha_1} \lambda^{(1)}_{\alpha_1} \Gamma^{(2)i_2}_{\alpha_1\alpha_2} \lambda^{(2)}_{\alpha_2} |i_1 i_2\rangle |\phi^{(3\cdots n)}_{\alpha_2}\rangle \,. \tag{5.8}$$

By iterating the above procedure we finally get a representation of the quantum state in terms of some tensors Γ and some vectors λ:

$$|\psi\rangle = \sum_{\{i\}} \sum_{\{\alpha\}} \Gamma^{(1)i_1}_{1\alpha_1} \lambda^{(1)}_{\alpha_1} \Gamma^{(2)i_2}_{\alpha_1\alpha_2} \lambda^{(2)}_{\alpha_2} \ldots \lambda^{(n-1)}_{\alpha_{n-1}} \Gamma^{(n)i_n}_{\alpha_{n-1}1} |i_1, i_2, \ldots, i_n\rangle \, . \tag{5.9}$$

Several remarks are to be considered at this point. First, notice that the above decomposition immediately provides the Schmidt vectors λ of all the possible contiguous bipartitions of the system. Second, the state from Eq.5.9 is indeed a reparametrization of a matrix product state of the form given in Eq.5.3 if we define the matrices at site l in the following way:

$$A^{(l)i_l}_{\alpha_{l-1}\alpha_l} \equiv \Gamma^{(l)i_l}_{\alpha_{l-1}\alpha_l} \lambda^{(l)}_{\alpha_l} \, . \tag{5.10}$$

Third, we see that the maximum allowed rank of the different indices α_l, $l = 1, 2, \ldots, n-1$, is site-dependent, since the size of the Hilbert spaces considered when performing the consecutive Schmidt decompositions depends on the site. In particular, we have that, at most, $\alpha_l = 1, 2, \ldots, d^l$ for $l = 1, 2, \ldots, \lfloor n/2 \rfloor$, and $\alpha_l = 1, 2, \ldots, d^{(n-l)}$ for $l = \lfloor n/2 \rfloor + 1, \lfloor n/2 \rfloor + 2, \ldots, n-1$. Actually, the fact that the maximum allowed range of the matrix indices is site-dependent can also be seen from Eq.5.3 by performing an appropriate set of concatenated singular value decompositions of the matrices defining the state. In practice, however, many of the Schmidt coefficients for the different contiguous bipartitions of the system shall be equal to (or almost equal to) zero depending on the particular state being considered. Let us then call $\chi(l, \mathcal{P})$ the local Schmidt rank for the bipartition between the l and the $l+1$ sides for a given permutation $\mathcal{P}$ of the particles. We shall now define χ as the maximum Schmidt rank over all the possible bipartitions of the system, that is

$$\chi \equiv \max_{l,\mathcal{P}} \chi(l, \mathcal{P}) \, . \tag{5.11}$$

We immediately see from this definition that the parameter χ controlling the maximum possible size of the matrices in a matrix product state of n particles is, indeed, a measure of the maximum bipartite entanglement that is present in the system. This representation is very appealing, since quantum states with low (bipartite) entanglement can then be represented by small matrices, while highly-entangled states must necessarily be described by matrices of large size, corresponding to the idea that the more entangled a system is, the harder it is to perform an exact classical description of it.

The above picture can be made specific by noticing that $\chi \geq d^S$, where S is the entanglement entropy (measured in e-dits) corresponding to any possible bipartition of the system. The study of the scaling of the entanglement entropy can thus be translated into the study of the possibility or not of an efficient representation of the quantum state in terms of a matrix product state. To be more precise, matrix product states allow a representation of the state in terms of $O(nd\chi^2)$ parameters instead of the original d^n coefficients. Therefore, those quantum states with $\chi = O(\text{poly}(n))$ can be efficiently classically represented by a matrix product state, while those where $\chi = O(2^n)$ cannot. In fact, the computation of the expected values of local observables can be done in $O(\chi^3)$ time, thus being efficient for systems with small enough χ. This is an important property, since it means that the matrix product state representation is not only nice, but useful

as well, in the sense that it allows to compute important physical quantities, like correlators, in an efficient way. Any possible parameterization of a quantum state which does not allow to efficiently compute physical properties is not a useful parameterization for computational purposes. How to efficiently compute correlators with matrix product states can be found for instance in [57].

The matrix product state parameterization has been very useful in computing low-energy properties of some sufficiently local Hamiltonians, and also the dynamics of quantum states. We shall not explain here the details of some optimization algorithms like DMRG, and the interested reader is addressed to the huge amount of existing literature about this (see for example [57, 173]). We do sketch, however, the basic ideas on how to proceed for computing dynamical evolutions with matrix product states. In fact, some optimization algorithms, like euclidean time evolution, can also be understood in terms of the dynamical procedures that we explain in what follows.

5.1.1 Computing dynamics

In this section we explain how to compute the dynamics of a matrix product state. Our model for dynamical evolution is based on the application of a set of unitary gates acting either on one or two local d-level systems, which could perfectly correspond to a discretization of the continuous time evolution driven by a generic one and two-body Hamiltonian.

Let us begin this explanation by considering the effect of a unitary gate $U^{(l)}$ acting over a single d-level system l. The consequence of this operation involves an updating of the matrices $A^{(l)}$ at site l that goes as follows:

$$A'^{(l)i'_l}_{\alpha_{l-1}\alpha_l} = \sum_{i_l} U^{(l)}_{i_l i'_l} A^{(l)i_l}_{\alpha_{l-1}\alpha_l} \, . \tag{5.12}$$

Notice that this type of local gates does not affect the ancillary indices. Entanglement is thus unaffected, which is a necessary condition since we are just performing a local operation.

The effect of non-local unitary gates acting on different local systems is less obvious. We initially consider the case of a non-local gate $U^{(l,l+1)}$ involving contiguous local systems l and $l+1$. Let us define

$$\sum_{i_l, i_{l+1}} U^{(l,l+1)}_{i'_l i'_{l+1}, i_l i_{l+1}} A^{(l)i_l}_{\alpha_{l-1}\alpha_l} A^{(l+1)i_{l+1}}_{\alpha_l \alpha_{l+1}} \equiv \Theta^{i'_l i'_{l+1}}_{\alpha_{l-1}\alpha_{l+1}} \, . \tag{5.13}$$

Unlike with local gates, the action of an interacting gate does not preserve the product form of the tensors A. To reestablish the matrix product state structure we need to rewrite Θ using a Schmidt decomposition. The procedure to follow is to compute the reduced density matrix from the bipartition of the system between the l and $l+1$ sides, which for the $l+1$ side reads

$$\rho^{ij}_{\alpha_{l+1}\beta_{l+1}} = \sum_{k, \alpha_{l-1}} |\lambda^{(l-1)}_{\alpha_{l-1}}|^2 \Theta^{ki}_{\alpha_{l-1}\alpha_{l+1}} \Theta^{*kj}_{\alpha_{l-1}\beta_{l+1}} \, , \tag{5.14}$$

where we have made use of the at most χ known Schmidt coefficients $\lambda^{(l-1)}_{\alpha_{l-1}}$ for the cut between the $l-1$ and the l sides. After diagonalizing ρ using (i, α_{l+1}) and (j, β_{l+1}) as composed indices, we

directly read from the eigenvalues the at most $d\chi$ updated Schmidt coefficients $\lambda'^{(l)}_{\alpha_l}$ for this bipartition, together with the updated matrices $A'^{(l+1)i_{l+1}}_{\alpha_l\alpha_{l+1}}$ from the coefficients of the eigenvectors. Finally, the new tensors for system l are easily calculated as $A'^{(l)i_l}_{\alpha_{l-1}\alpha_l} = \sum_{i_l,\alpha_{l+1}} A'^{(l+1)i_{l+1}}_{\alpha_l\alpha_{l+1}} \Theta^{i_l i_{l+1}}_{\alpha_{l-1}\alpha_{l+1}}$. Non-local gates between non-contiguous systems can be reduced to the previous case by using SWAP gates, producing a typical overhead of $O(n)$ operations. Notice that all our manipulations can be done in a time that grows like $O(\chi^3)$.

As we have seen, non-local gates entangle the system by increasing the size of the matrices that must be kept in the classical simulation scheme. Each time an entangling gate is operated on two neighboring systems, the index of the connected ancillae is multiplied by d. To keep the numerical simulation under control, a (non-unique) truncation scheme is needed to stop the exponential growth of ancillary dimensions. The ability in this truncation is the key element for the success of the time-evolution algorithm. Here we explain two possible truncation schemes, the first one based on the original proposal of Vidal [49] of an optimal local truncation, and the second one inspired on the methods of Verstraete and Cirac [53–55, 58] based on an optimal non-local truncation procedure.

Before entering into the details of the possible truncation schemes, let us introduce a graphical representation of the quantum state that shall be useful in what follows. We represent the tensor $A^{(l)i_l}_{\alpha_{l-1}\alpha_l}$ at site l by the following diagram:

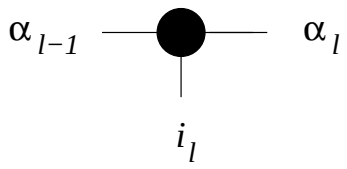

Figure 5.2: Diagrammatic representation of the tensor $A^{(l)i_l}_{\alpha_{l-1}\alpha_l}$ at site l.

With this notation, a matrix product state like the one from Eq.5.3 is represented by means of the following tensor network:

Figure 5.3: Diagrammatic representation of a matrix product state in terms of a tensor network.

In the above figure we have decided to drop off the name of the indices of the matrices since they do not bring any extra information. Each one of the dots represents a specific particle. Vertical lines correspond to the indices of the physical Hilbert spaces and run up to d, while horizontal links between the dots correspond to the ancillary indices and run at most up to χ. Now, we are in a position to discuss the different truncation procedures.

Local truncation scheme

After the application of a non-local gate on the adjacent systems l and $l+1$, the obtained matrix product state is identical to the original one with the only exception that matrices for sites l and $l+1$ have been updated, and the rank of the link connecting these two matrices has been multiplied by d. A possible truncation procedure is to *only* change the matrices at sites l and $l+1$, computing two new matrices with ancillary indices up to χ, in such a way that the difference with the original state is minimum (or analogously, the overlap with the original state is maximum). This is a local scheme, since it only affects the two very specific matrices of the whole matrix product state that were touched by the action of the unitary gate. It is easy to see that optimality in this truncation is achieved by keeping the χ terms in the range of the common index that correspond to the largest eigenvalues $|\lambda'^{(l)}_{\alpha_l}|^2$ of the reduced density matrices of the bipartition of the system between the sites l and $l+1$. The diagrammatic representation of this truncation is shown in Fig.5.4.

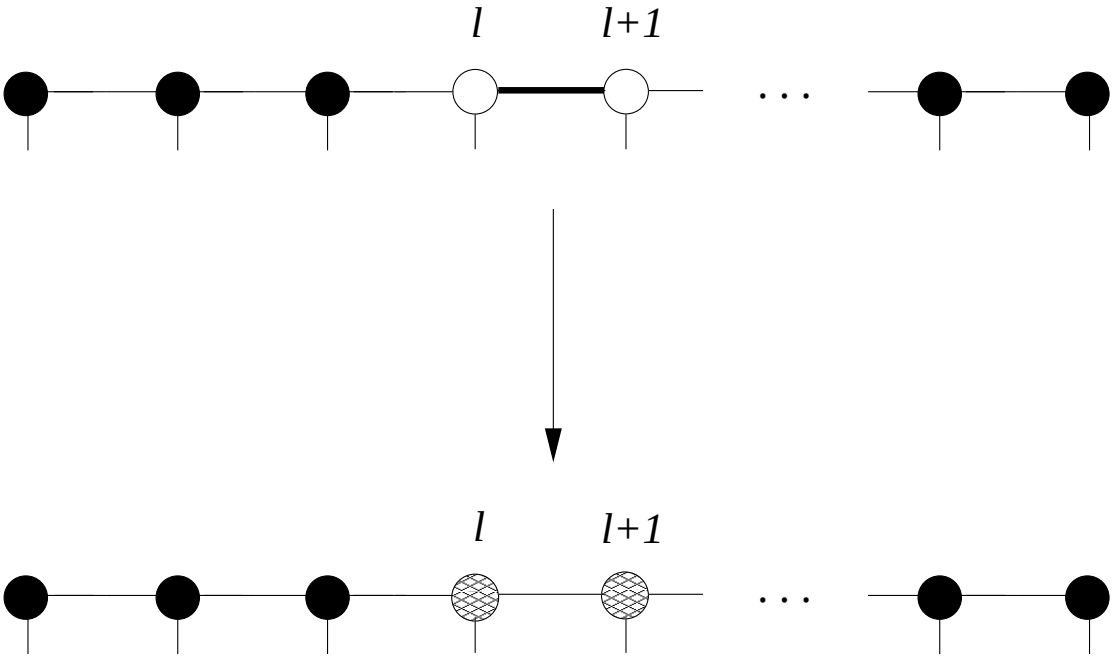

Figure 5.4: Local truncation scheme. Black dots correspond to old matrices, white dots correspond to updated matrices after the unitary evolution, and the thick link line has a rank at most $d\chi$. Only matrices at sites l and $l+1$ are truncated (indicated by dashed dots), and this is done by keeping only the most relevant χ terms of the corresponding Schmidt decomposition.

Notice that given the locality of the procedure, this scheme seems to be a good way to implement a truncation in order to eventually parallelize the code of the classical simulation algorithm. More precisely, one could think of different nodes of a computer network, each one of them storing one matrix (or a finite set of them). This truncation scheme would only involve

communication between the two nodes on which the non-local gate operates, leaving the rest $n-2$ nodes untouched, and therefore involving a small amount of information to be sent between different nodes.

Non-local truncation scheme

Given the above local procedure, we can see that there exists the possibility to improve the precision in the truncation by means of a non-local updating of the matrices that define the matrix product state. The main idea is as follows: instead of performing an optimal truncation only in matrices at sites l and $l+1$, perform an optimal truncation in *all* the matrices defining the matrix product state, that is, find a new state with new matrices for all the sites with ancillary indices up to χ such that the distance to the original state is minimum. This is represented in Fig.5.5.

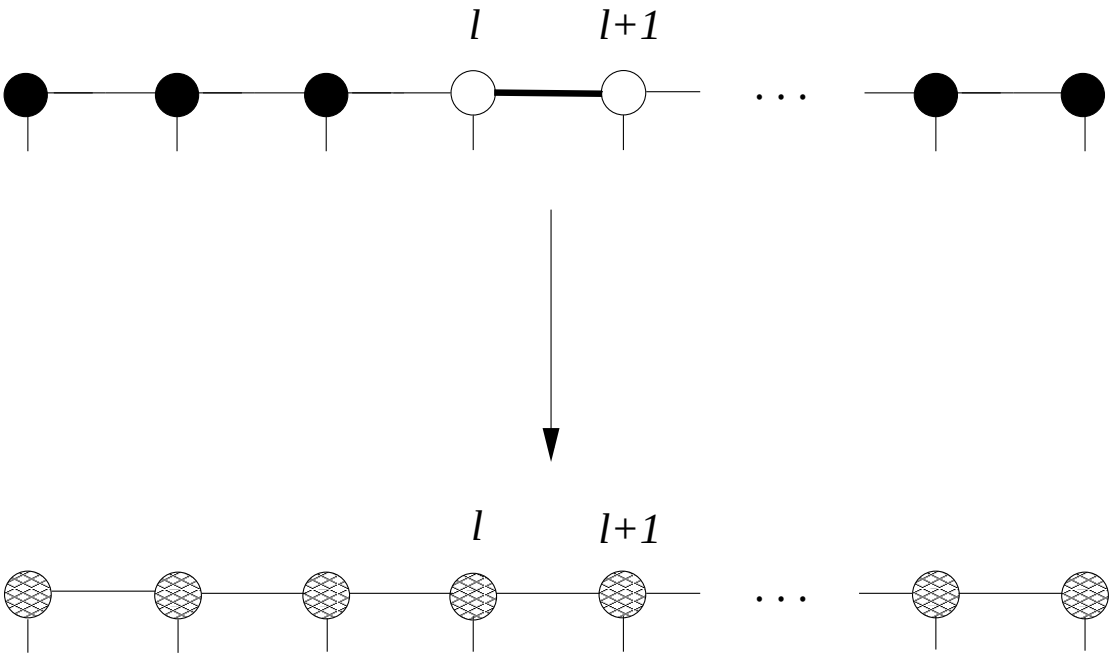

Figure 5.5: Non-local truncation scheme. Black dots correspond to old matrices, white dots correspond to updated matrices after the unitary evolution, and the thick link line has a range $d\chi$. We find new matrices at every site (indicated by dashed dots) with ancillary indices up to χ such that the distance to the original state is minimized.

In order to find the new optimal matrices it is possible to proceed in the following way. Let us call $|\psi'\rangle$ the exact state after the non-local unitary evolution, and $|\tilde{\psi}\rangle$ the new matrix product state that we use to approximate $|\psi'\rangle$. We wish to maximize the quantity $\left|\langle\psi'|\tilde{\psi}\rangle\right|^2$ over all possible matrix product states $|\tilde{\psi}\rangle$ with ancillary indices up to χ with the normalization constraint $|\langle\tilde{\psi}|\tilde{\psi}\rangle|^2 = 1$. In order to perform this minimization, we fix all the matrices of $|\tilde{\psi}\rangle$ to a

fixed value except the first one, and maximize the overlap with respect to the first matrix with the appropriate normalization constraint, which can be done in $O(\chi^3)$ time[a]. Once the values of the first matrix are found, we repeat the procedure maximizing with respect to the second matrix and finding a better approximation to the original exact state. The complete maximization is then performed by repeating this procedure sequentially for every site, and sweeping back and forth along the system until some desired convergence is achieved.

Indeed, this truncation scheme does not require the non-local gate to be necessarily applied on adjacent systems. Imagine that we wish to apply a non-local gate $U^{(l,m)}$ between distant systems l and m. It is possible to see that any such unitary matrix $U^{(l,m)} \in \mathrm{U}(d^2)$ can always be written as $U^{(l,m)} = \sum_{a,b} C_{ab} O_a^{(l)} \otimes O_b^{(m)}$, where $O_a^{(l)}$ and $O_b^{(m)}$ are $2d^2$ local operators acting respectively on sites l and m (d^2 operators per site), and C_{ab} are d^4 coefficients[b]. Performing a singular value decomposition of the coefficient C_{ab}, this can be written as $C_{ab} = \sum_\mu U_{a\mu} D_\mu V_{\mu b}$, and therefore the original unitary matrix can be expressed as $U^{(l,m)} = \sum_\mu \tilde{O}_\mu^{(l)} \otimes \tilde{O}_\mu^{(m)}$, where we have defined the operators $\tilde{O}_\mu^{(l)} \equiv \sum_a U_{a\mu} O_a^{(l)} D_\mu^{1/2}$ and $\tilde{O}_\mu^{(m)} \equiv \sum_b V_{\mu b} O_b^{(m)} D_\mu^{1/2}$. Applying these operators on the original matrix product state is equivalent to redefine the tensors at sites l and m in such a way that we add a new index μ of rank d^2:

$$
\begin{aligned}
A'^{(l)i'_l}_{\mu\ ;\ \alpha_{l-1}\alpha_l} &\equiv \sum_{i_l} A^{(l)i_l}_{\alpha_{l-1}\alpha_l} \tilde{O}^{(l)}_{\mu\ ;\ i'_l i_l} \\
A'^{(m)i'_m}_{\mu\ ;\ \alpha_{m-1}\alpha_m} &\equiv \sum_{i_m} A^{(m)i_m}_{\alpha_{m-1}\alpha_m} \tilde{O}^{(m)}_{\mu\ ;\ i'_m i_m} \ .
\end{aligned}
\tag{5.15}
$$

Given the above equation, we see that after the application of the unitary gate, the sites l and m get linked by a common index μ. This is another way of understanding how non-local gates entangle the system, namely, by creating new bonds between the sites on which they act. Now, it is possible to perform again a non-local truncation much in the same way as before, by finding new matrices for all the sites with only two ancillary indices up to χ and also in $O(\chi^3)$ time as well. This is represented in Fig.5.6.

We shall expect better accuracies for this non-local truncation scheme than for the local truncation procedure, basically because we optimize over a larger set of parameters, and because we do not have to necessarily implement SWAP operations in order to perform non-local gates between distant systems, thus reducing the number of truncations to be applied in the simulation. Nevertheless, this scheme has the drawback that the number of operations to be done at each truncation step is bigger than in the local case. Also, the fact that the truncation is non-local makes it a bad candidate for a possible parallelization of the numerical code, since all the nodes of the computer network should communicate among themselves at each truncation step in order to perform the approximation of the exact state by a new matrix product state.

[a] This is valid for the case of open boundary conditions that we analyze here. Periodic boundary conditions may involve a larger computational time than our case.

[b] It is possible to see this property by expressing the unitary operator as the exponential of a local basis for the algebra $\mathrm{u}(d^2)$ and performing a Taylor expansion.

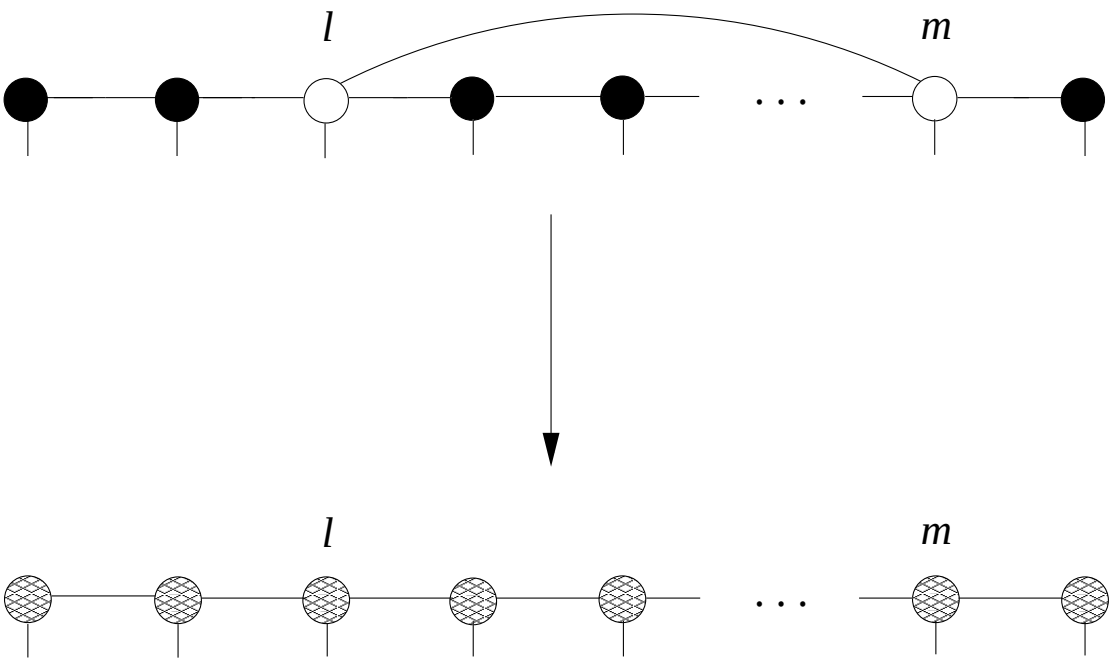

Figure 5.6: Non-local truncation scheme. Black dots correspond to old matrices, and white dots correspond to updated tensors after the unitary evolution. The action of a non-local gate has created a new link of rank d^2 between sites l and m. We find new matrices at every site (indicated by dashed dots) with ancillary indices up to χ such that the distance to the original state is minimized.

5.2 Classical simulation of an adiabatic quantum algorithm solving Exact Cover

In this section we show the results of a simulation of a quantum algorithm using matrix product states. More precisely, we have implemented the local truncation scheme explained in the previous section to the simulation of a quantum adiabatic algorithm solving hard instances of the Exact Cover NP-complete problem. The performance of this algorithm was already analyzed in detail in the previous Chapter by means of an exact numerical computation of its properties up to 20 qubits. There we saw that the entanglement entropy of a typical bipartition of the system seems to scale as $S \sim 0.1n$, n being the number of qubits. We also found that the linear scaling of the entanglement entropy forbids the possibility of an efficient numerical simulation with the methods of [49]. The reason becomes clear now, since a linear scaling of the entanglement entropy involves an exponentially big χ in the number of qubits, and therefore any algorithm based on matrix product states must necessarily handle matrices of exponential size in order to get a result sufficiently close to the exact one. In any case, the possibility of a numerical simulation of this quantum algorithm by using matrix product states is motivated in part by the fact that the coefficient of the scaling law for the entanglement entropy seems to be rather small (only

0.1). Thus, even though we should need an exponentially big χ to perform a very accurate simulation of the adiabatic quantum algorithm, it could be possible that already good simulations can be performed by keeping a relatively small χ. Furthermore, the performance of a classical simulation of a quantum algorithm by using the matrix product state ansatz may bring further insight on the way entanglement is used along the quantum evolution. As we shall see, the basic features of the quantum algorithm can still be observed even in the case of a highly-truncated simulation with very small χ.

Let us sketch the basic features of our simulation. First, let us remind that classically hard instances of Exact Cover seem to appear at the so-called easy-hard-easy transition around $m \sim 0.8n$ [174], m being the number of clauses and n being the number of qubits. We have generated such hard instances, with the additional property of having only a unique satisfying assignment. The generation of hard instances is in itself a hard problem for which we have developed specific algorithms, essentially based on the iterative addition of random and non-redundant clauses until the number of solutions of the instance is one. The quantum algorithm for a given Exact Cover instance follows the adiabatic evolution of the ground state of a Hamiltonian defined by $H(s) = (1-s)H_0 + sH_P$, where the adiabatic parameter is $s = t/T$ and t runs up to a total predetermined time T. We take the initial Hamiltonian to be $H_0 = \sum_{i=1}^{n} \frac{d_i}{2}(1-\sigma_i^x)$ where d_i stands for the number of clauses where qubit i enters. The non-local problem Hamiltonian corresponds to the sum of clauses defined as

$$H_P = \sum_{C \in \text{instance}} (z_i + z_j + z_k - 1)^2 \,, \tag{5.16}$$

where $z_i = (1-\sigma_i^z)/2$ has eigenvalues 0 and 1, and C stands for a clause involving bits i, j and k in the specific instance. Notice the difference between the problem Hamiltonians from Eq.5.16 and from Eq.4.18. Both Hamiltonians describe correctly the solution to an Exact Cover instance in its ground state. The essential difference between them is that while the Hamiltonian of Eq.4.18 has three-body interactions, the Hamiltonian of Eq.5.16 has not. The problem Hamiltonian that we use in this Chapter is built only from one and two-body terms, together with local magnetic fields, and its evolution can therefore be classically simulated by the algorithms based on matrix product states that we have already discussed, based on the efficient updatings of the register after performing one and two-body unitary gates. At the level of eigenvalues, notice that the only difference between the two Hamiltonians comes on the eigenvalues of the excited states, thus keeping the properties of the low-energy sector untouched. In fact, it is easy to see by means of direct simulations that an adiabatic quantum algorithm based on this problem Hamiltonian shows the same important features as the ones already described in Chapter 4, in particular the appearance of a quantum phase transition at $s_c \sim 0.69$ in the thermodynamic limit, together with a linear scaling of the entanglement entropy with the number of qubits with a small scaling coefficient of the order of 0.1.

Exact simulations of quantum algorithms by adiabatic evolution solving hard instances of satisfiability problems were carried so far up to 30 qubits [175]. Here we present the possibility of performing *approximated* simulations of this quantum algorithm beyond that number.

5.2.1 Discretization of the continuous time evolution in unitary gates

Let us now turn to discuss the detailed way matrix product states can handle the simulation of the adiabatic evolution of Exact Cover. The simulation needs to follow a time evolution controlled by the s-dependent Hamiltonian. This continuous unitary time evolution from time 0 to time T can be discretized as follows:

$$U(T,0) = U(T,T-\Delta)\dots U(2\Delta,\Delta)U(\Delta,0)\,, \tag{5.17}$$

where the increment $\Delta \equiv \frac{T}{M}$ defines the discretization, M being a positive integer. Our simulations indicate that we can take the value $\Delta = 0.125$ while keeping sufficient accuracy – as compared to smaller Δ – in all of them. After l steps $s = \frac{t}{T} = \frac{l\Delta}{T} = \frac{l}{M}$, that is $l = 0,\dots M$.

At any point l along the evolution the unitary operator $U((l+1)\Delta, l\Delta)$ needs further subdivision into elementary one and two-qubit gates. This requires the use of Trotter's formula to second order [176–178]:

$$U((l+1)\Delta, l\Delta) = e^{i\Delta H(s)} \sim \left(e^{i\frac{\delta}{2}(1-s)H_0} e^{i\delta s H_P} e^{i\frac{\delta}{2}(1-s)H_0}\right)^{\frac{\Delta}{\delta}}\,, \tag{5.18}$$

where the partition in $H_0 : H_P : H_0$ minimizes the number of two-qubit gates as compared to the alternative partition $H_P : H_0 : H_P$. We have verified as well that we can maintain a faithful classical simulation by choosing $\delta = \Delta$. Notice that the split of exponentials in the Trotter's expansion of Eq.5.18 is chosen so that H_0 is explicitly separated from H_P, so that this brings the advantage that both pieces of the Hamiltonian can be decomposed in mutually commuting one and two-qubit gates:

$$e^{i\frac{\delta}{2}(1-s)H_0} = \prod_{i=1}^{n} e^{i\frac{\delta}{4}(1-s)d_i(1-\sigma_i^x)}\,, \tag{5.19}$$

and

$$\begin{aligned} e^{i\delta s H_P} &= \prod_{C\,\in\,\text{instance}} e^{i\delta s(z_i+z_j+z_k-1)^2} \\ &= \prod_{C\,\in\,\text{instance}} e^{i\delta s(z_i^2-2z_i)} e^{i\delta s(z_j^2-2z_j)} e^{i\delta s(z_k^2-2z_k)} e^{i\delta s} \\ &\quad e^{i2\delta s z_i z_j} e^{i2\delta s z_i z_k} e^{i2\delta s z_j z_k}\,. \end{aligned} \tag{5.20}$$

The complete adiabatic evolution is thus finally discretized in terms of the sequential action of the above one and two-qubit gates.

5.2.2 Numerical results of a simulation with matrix product states

The exact simulation of a quantum computer using matrix product states is then completely defined. As we said before, we have chosen the local truncation scheme in order to implement our algorithm. It is possible to see that the total running time of the simulation algorithm scales as $O(Tnm\chi^3)$. This reasonable truncation carries, though, an inherent – but always under control – loss of norm of the quantum state, since the sum of the retained squared eigenvalues will not reach 1. As we shall see, larger χ's allow for more faithful simulations, as expected.

We have implemented a number of optimizations upon the above basic scheme which are worth mentioning. For any non-local gate there is an overhead of SWAP operations that damage the precision of the computation. To minimize this effect, every three-qubit clause is operated as follows: we bring together the three qubits with SWAPs of the left and right qubits keeping the central one fixed and, then, we operate the two-qubit gates. Before returning the qubits to their original positions we check if any of them is needed in the next gate. If so, we save whatever SWAP may be compensated between the two gates. Ordering of gates is also used to produce a saving of $\sim 2/3$ of the naive SWAPs. Diagonalization of the relevant reduced density matrices in the allowed Hilbert space of minimum dimension is used as well. A further improvement is to keep a both dynamical and local χ, so that ancillary indices at the different partitions are allowed to take independent values and grow up to site-dependent and time-dependent limits. This last procedure, though, has shown essentially no big improvement upon a naive fixed χ strategy. Let us now explain in what follows the different results of our simulations.

Instantaneous expected energy

We first simulate the adiabatic algorithm with the requirement that the right solution is found for a typical instance of $n = 30$ qubits with $m = 24$ clauses and $T = 100$. Along the evolution we compute the expected value of the Hamiltonian of the system, which can be calculated in $O(\chi^3)$ time. Our numerical data are shown in Fig.5.7. The system remains remarkably close to the instantaneous ground-state all along the approximated evolution and, as we can see, the maximum absolute error with respect to our best classical simulation ($\chi = 40$) comes when evolving close to the quantum phase transition point. We also see convergence in the error while the system approaches the critical point. This minimum absolute error in the ground-state energy is, when close to criticality, of the order of $10^{-2} - 10^{-3}$, smaller than the typical value of the energy gap for 30 qubits – as hinted by extrapolating the data from Fig.4.7 in Chapter 4 –. A bigger χ may bring a better precision by using a larger, but eventually affordable, time cost in the simulation.

The error in the expected energy is minimized as χ increases. It is noteworthy to observe how the error in the simulation of the adiabatic algorithm increases at the phase transition point. We have also numerically checked in our simulations that it is precisely at this point where each qubit makes a decision towards its final value in the solution. Physically, the algorithm builds entanglement up to the critical point where the solution is singled out and, thereon, the evolution seems to drop the superposition of wrong states in the register.

Loss of norm

We plot in Fig.5.8 the norm of the quantum state at the end of the simulation as a function of χ in logarithmic scale, for typical instances of 14, 18, 22 and 30 qubits. The remarkable fact is that some observables, like the energy, appear to be very robust against this inaccuracy, while the behavior of this norm was already expected not to be good, since this is precisely the parameter in which we are truncating with respect to the exact evolution, and furthermore its accumulation is multiplicative as time evolves.

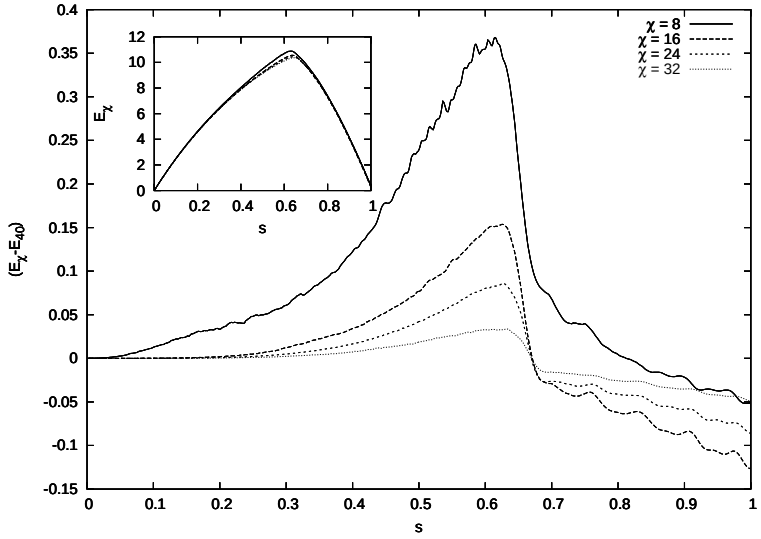

Figure 5.7: Computation of the absolute error, as compared to the $\chi = 40$ case, of the expected value of the Hamiltonian (in dimensionless units) along the adiabatic evolution for a typical instance with 30 qubits and 24 clauses for $T = 100$ as χ increases. Note the increasing precision with larger χ as s approaches the phase transition from the left-hand-side. In the inset, the instantaneous expected energy is plotted (in dimensionless units). A similar behavior is also obtained for other instances, getting *perfect* solution at the end of the computation (zero energy).

Decay of the Schmidt coefficients

Our simulations also allow to compute the decay of the χ Schmidt coefficients $\lambda_\alpha^{(l)}$, $\alpha = 1, 2, \ldots, \chi$, at any site l and at any step of the computation. At the closest point to criticality, and for the central bipartition of the system, these can be approximately fitted by the law $\log_2(\lambda_\alpha^{(n/2)}) = a + \frac{b}{\sqrt{\alpha}} + c\sqrt{\alpha}$, with appropriate instance-dependent coefficients a, b and c. The behavior for a typical instance of 30 qubits is shown in Fig.5.9.

100-qubit instance

The ultimate goal of finding the correct solution appears also to be very robust in the simulations we have performed. The exact probability of success can be calculated in $O(\chi^2)$ time as well. As a symbolic example, our program has solved an instance with $n = 100$ bits, that is, the adiabatic evolution algorithm has found the correct product state out of $2^{100} \sim 10^{30}$ possibilities for a hard instance with $m = 84$ clauses and $T = 2000$. The simulation was done with a remarkably small value of $\chi = 14 \ll 2^{50} = \chi_{max}$ and is presented in Fig.5.10. Notice that while the entanglement entropy shows fluctuations because it is directly related to the truncation parameter of the simulation, the probability of success follows a smooth behavior, being almost zero at the beginning of the evolution, and jumping directly to one precisely when close to the quantum critical point.

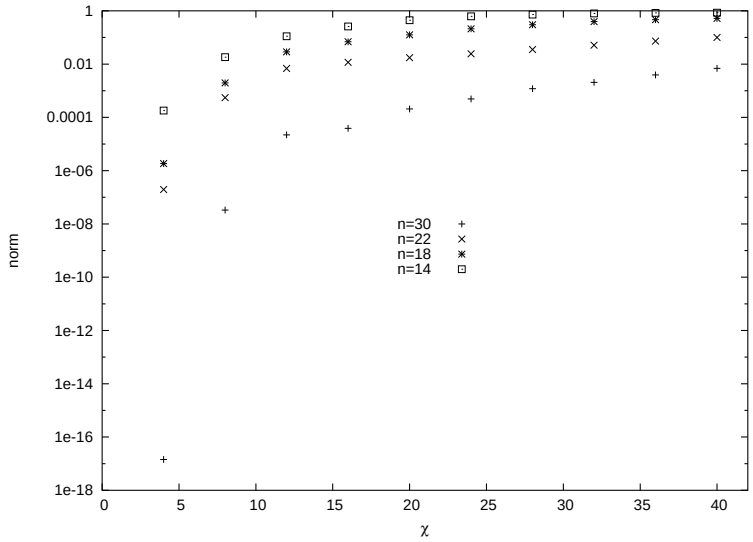

Figure 5.8: Final norm in the register as a function of χ in logarithmic scale, for instances of $14, 18, 22$ and 30 qubits.

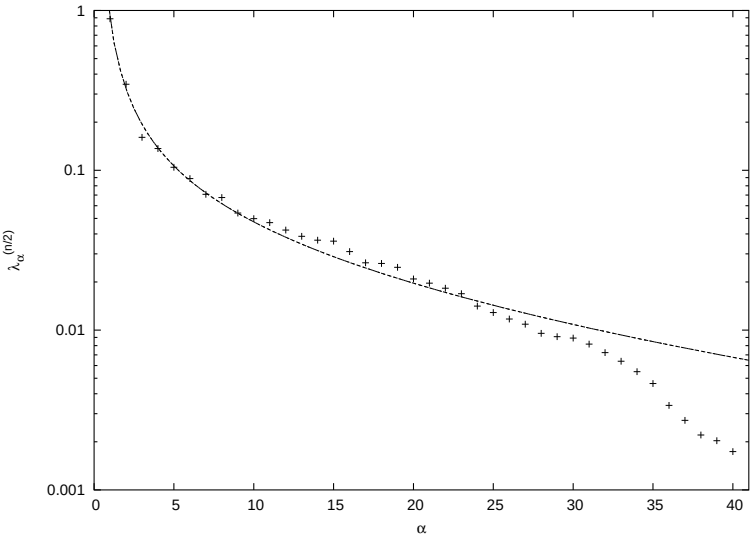

Figure 5.9: Decay of the Schmidt coefficients for a typical instance of 30 qubits in logarithmic scale, with $\chi = 40$. The behavior seems to be approximately described by a law of the kind $\log_2(\lambda_\alpha^{(n/2)}) = a + \frac{b}{\sqrt{\alpha}} + c\sqrt{\alpha}$, for appropriate coefficients a, b and c (solid line).

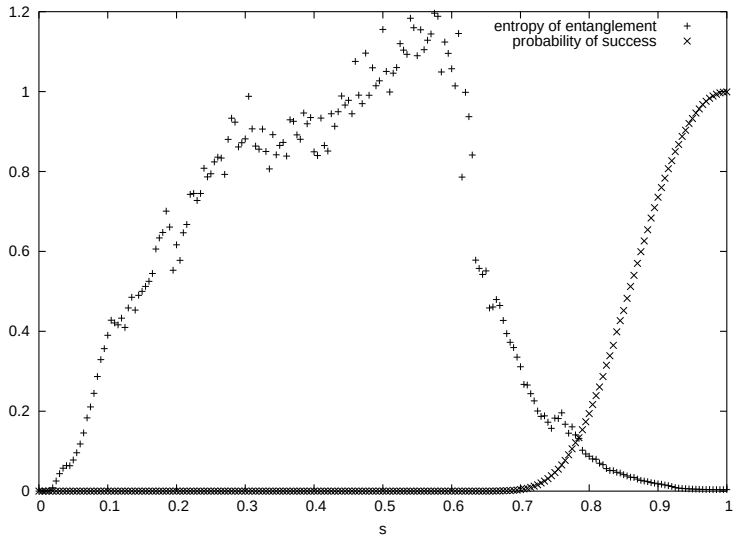

Figure 5.10: Entanglement entropy of a bipartition and probability of being at the correct solution as a function of s for a simulation with $\chi = 14$ of adiabatic evolution solving a hard instance of $n = 100$ bits and $m = 84$ clauses.

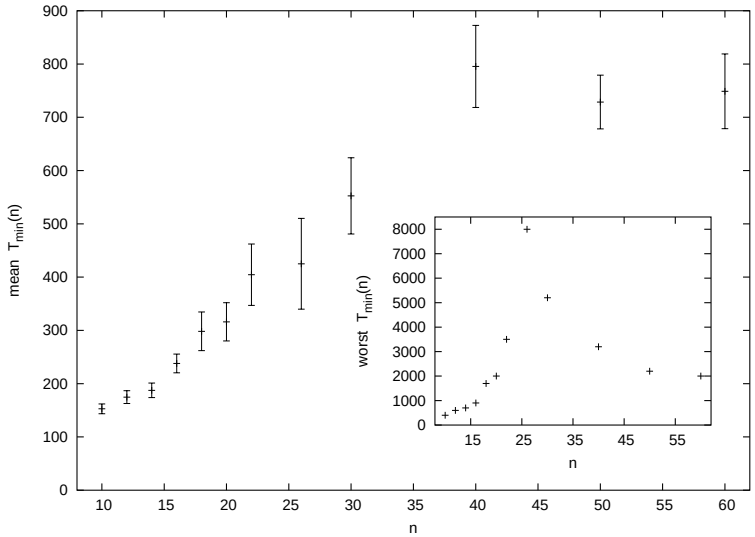

Figure 5.11: Mean and worst cases of the accumulated statistics up to $n = 60$ for $T_{min}(n)$ (in dimensionless units) such that an instance is solved. Averages are performed over 200 instances for each n, except for $n = 50, 60$ with respectively $199, 117$ instances. Error bars give 95 per cent of confidence level in the mean.

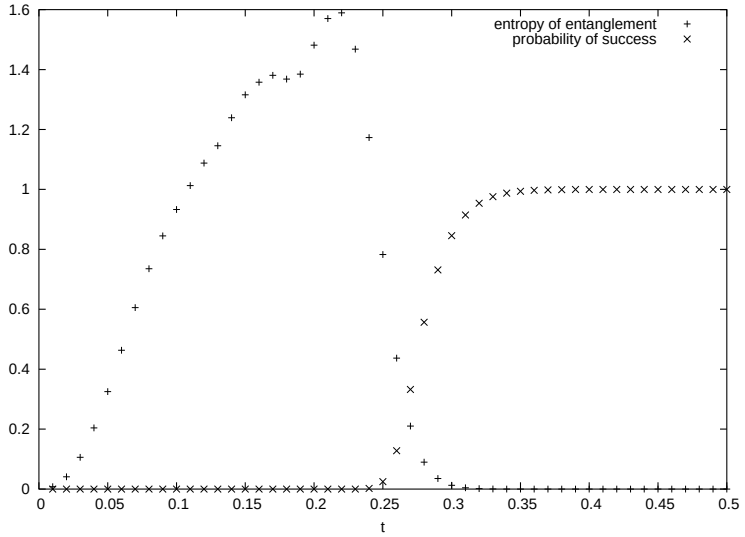

Figure 5.12: Euclidean time evolution solving a typical instance of 26 qubits with $\chi = 6$. The algorithm finds the correct solution much faster than the simulations of adiabatic quantum computation. The sudden jump in the probability of success comes again at the maximal point for the entanglement entropy.

Time statistics

The robustness of evolving towards the correct solution is found for any number of qubits and small χ. To analyze further the performance of this classical simulation, we have launched a search for the minimal $T_{min}(n)$ that solves samples of n-qubit hard instances in the following way: for a set of small values of χ, we try a random instance with an initial T, for instance $T = 100$. If the solution is found, we proceed to a new instance, and if not, we restart with a slower adiabatic evolution with, for instance, $T = 200$. This slowing down of the algorithm is performed until a correct solution is found and the minimum successful T_{min} is stored. Our results are shown in Fig.5.11. The average over n-qubit instances of $T_{min}(n)$ appears to grow very slowly with n, though the extreme cases need increasingly larger times up to $n = 25$. The slowing-down in the plots for a large number of qubits is a side-effect of the inherent difficulty to generate hard instances of Exact Cover for large n. We want to remind as well that finding an instance that needs a very large T_{min} is no counterproof for the validity of the adiabatic algorithm, as alternative interpolating paths may solve the instance efficiently [66].

Solving hard classical instances by euclidean time evolution

Independently of the fact that our simulation describes in an approximate way the behavior of an adiabatic quantum algorithm, we can think of it as a plausible classical algorithm for solving hard instances of an NP-complete problem. In fact, if our aim is to solve instances of Exact Cover, all that is required is a classical algorithm to find the ground-state of the problem Hamiltonian H_P from Eq.5.16. A possibility is to perform an evolution in euclidean time, that

is, to simulate the evolution driven by the non-unitary operator

$$e^{-H_P t} . \tag{5.21}$$

The above evolution is not physical, since it is not unitary and therefore does not correctly preserve the probabilities as the parameter t (the euclidean time) flows. In any case, it is easy to see that if we have a (possibly not normalized) quantum state such that it has a non-zero overlap with the ground state of H_P, the action of the operator from Eq.5.21 over the state will eventually drive the original state towards the only fixed point of the map at $t \to \infty$, which is the ground state of H_P. In practice, the action of the above operator over an equally-weighted superposition of all possible computational states will drive the original state towards the ground state of H_P with very high probability at times bigger than the inverse of the first gap of the system. This optimization algorithm can be easily implemented by using the same time-evolution procedures described before in terms of matrix product states. Evolution in euclidean time shall not be unitary, though, but this particularity does not affect any of the essential features of the updating and truncation schemes previously explained.

The performance of the evolution in euclidean time for solving hard instances of Exact Cover is remarkably good, as compared to the performance of the simulation of the adiabatic quantum algorithm. This new classical algorithm finds the correct solution to the instances much faster than our previous simulations of adiabatic evolution. As an example, we show in Fig.5.12 the result of a simulation for a typical instance of 26 qubits with $\chi = 6$. The behavior of the euclidean time evolution algorithm resembles very much the one of the adiabatic evolution, in the sense that the probability of success remains very close to zero, until some specific point in the evolution is reached, where it jumps to one very quickly. It is also interesting to notice that this point corresponds, once more, to the point of maximum entanglement in the evolution, as measured by the entanglement entropy. Since the ground state of H_P is non-degenerate and separable, and since we begin with an equal superposition of all the possible states of the computational basis, the entropy must begin at zero and eventually die in zero, so it must necessarily reach a maximum at some point along the evolution. Remarkably, the point of maximum entropy coincides again with the jump in the probability of success. Note that even though the system is not evolving close to any quantum phase transition (like the one of the adiabatic quantum algorithm), the behavior along the evolution is very analogous to the one observed in those cases (compare Fig.5.12 and Fig.5.10). Again, maximum entanglement brings the correct solution to the problem, although our algorithm is entirely classical.

5.3 Conclusions of Chapter 5

In this Chapter we have shown that it is possible to implement approximated classical simulations of quantum algorithms by the use of matrix product states with controlled accuracy. More specifically:

- We have implemented a simulation based on matrix product states of an adiabatic quantum algorithm solving the NP-complete Exact Cover problem. This simulation is made precise by means of an optimal local truncation scheme, and provides robust results for

quantities like the expected energy or the probability of success, with a relatively small size of the involved matrices.

- We have solved a hard 100-qubit instance of Exact Cover by means of a highly-truncated simulation of the adiabatic evolution algorithm. This classical simulation finds the correct product state out of $2^{100} \sim 10^{30}$ possibilities by using matrices whose indices range up to $\chi = 14$, much smaller than the necessary 2^{50} for an exact simulation.

- We have seen that the mean time that our approximated classical simulations take to succeed increases slowly with the number of qubits, though not a definite scaling law can be inferred given the inherent difficulty to generate very hard instances of Exact Cover for a large number of qubits.

- Matrix product states algorithms for dynamical evolution can also be applied for simulating the non-unitary evolution in euclidean time, which we have shown to be a classical optimization algorithm that solves hard instances of Exact Cover much more efficiently than the classical simulations of the adiabatic algorithm.

The results presented here could be extended in several directions. For instance, it should be possible to study the performance of the optimal non-local truncation scheme and to compare it with the one we have considered here. Also, the performance of a parallelization of the numerical code that we have considered here could be analyzed. More generically, it should also be plausible to extend the rigid structure of a matrix product state to other tensor networks specifically adapted to the particular problem or instance in consideration, much in the same way as PEPS do in $(2 + 1)$-dimensional systems [58]. Finally, the study of the performance of all the ideas exposed here but with other quantum algorithms is a direction to be considered as well. For instance, it should be possible to see the behavior of a classical simulation of Shor's factoring algorithm by using matrix product states or related techniques. As we saw in Chapter 4, Shor's algorithm is yet another quantum algorithm which inherently makes use of an exponentially big amount of χ in the number of qubits. The effect of truncations in that algorithm are, though, not evident. Perhaps, a classical simulation of Shor's quantum algorithm using the ideas of this Chapter could be a good candidate for a new classical factorization algorithm.

Chapter 6

Majorization arrow in quantum algorithm design

Finding underlying mathematical structures in efficient quantum algorithms is one of the problems that quantum computation deals with. The fact that there is only a short list of ideas behind quantum algorithm design hints how difficult it is to come up with new quantum techniques and strategies to efficiently solve important problems. Grover's quantum searching algorithm [9] exploits calls to an oracle by enhancing a particular state, actually implementing a rotation in the relevant Hilbert space associated to the problem. Shor's factoring quantum algorithm [8] exploits the periodicity of an initial quantum state using a minimum of Hadamard and controlled-phase gates at the core of the quantum Fourier transform. Based on more general quantum mechanical principles, the idea of using adiabatic evolution to carry quantum computation [16] has proven suitable for performing Grover's algorithm and has been numerically studied as a candidate for attacking NP-complete problems, as we saw in Chapters 4 and 5. Also, the so-called quantum walks in continuous time have proven to efficiently solve a classically hard problem [179], whereas quantum random walks in discrete-time have proven to bring also Grover's square-root speed-up in a problem of quantum search [180]. Many other quantum algorithms can be mapped to the above families, being then based on the same basic principles.

Some attempts to uncover the properties of quantum algorithms have already been explored. One relevant instance is undoubtedly the role of entanglement [49, 50, 155–159], which was already considered in detail in the preceding two Chapters. In fact, although entanglement is a natural resource to be exploited in quantum algorithm design, there are known examples of faster-than-classical oracle-based quantum algorithms where the quantum register remains in a product state between calls to the quantum oracle all along the computation, though the speed-up is only by a factor of two [161, 181, 182]. In this Chapter we will concentrate on quite a different proposal. The basic idea is that there is an underlying strong majorization behavior in some quantum algorithms that seems to play a role as well.

More concretely, we study the evolution in different quantum algorithms, with respect to majorization, of the probability distribution arising in the evolving quantum state from the probabilities of the final outcomes, as introduced in [152]. We consider several families of quantum algorithms based on distinct properties. As a first step, we analyze the majorization behavior

of the family of quantum phase-estimation algorithms, comparing their performance with respect to majorization to that of Grover's algorithm [152], and giving also the explicit example of a slightly different quantum algorithm solving a hidden affine function problem by means of calls to an oracle [161,181,182]. We also consider here the class of adiabatic algorithms [16] by studying the behavior of the adiabatic algorithm implementing a quantum search [9,69,70]. Efficiency is seen to depend on the interpolating time path taken along the evolution [66,69,70], and we observe that optimality in adiabatic quantum searching appears when step-by-step majorization is present. Finally, quantum walks provide exponential speed-up over classical oracle-based random walks [179], and again a manifest strong majorization behavior is detected. Let us begin, then, by considering the way in which we understand majorization theory as applied to the study of quantum algorithms.

6.1 Applying majorization theory to quantum algorithms

The way we relate majorization theory – as defined in Appendix A – to quantum algorithms is as follows: let $|\psi^{(m)}\rangle$ be the pure state representing the register of a quantum computer at an operating stage labeled by $m = 1 \dots M$, where M is the total number of steps in the algorithm, and let N be the dimension of the Hilbert space. If we denote as $\{|i\rangle\}_{i=1}^{N}$ the basis in which the final measurement is to be performed, we can naturally associate a set of sorted probabilities p_i, $i = 1 \dots N$, to this quantum state in the following way: decompose the register state in the measurement basis such that

$$|\psi^{(m)}\rangle = \sum_{i=1}^{N} a_i^{(m)} |i\rangle \, . \tag{6.1}$$

The probability distribution associated to this state is

$$\vec{p}^{(m)} = \{p_i^{(m)}\} \qquad p_i^{(m)} \equiv |a_i^{(m)}|^2 = |\langle i|\psi^{(m)}\rangle|^2 \, , \tag{6.2}$$

where $i = 1 \dots N$. This corresponds to the probabilities of all the possible outcomes if the computation were to be stopped at stage m and a measurement were performed. A quantum algorithm will be said to majorize this probability distribution between steps m and $m+1$ if and only if [152–154]

$$\vec{p}^{(m)} \prec \vec{p}^{(m+1)} \, . \tag{6.3}$$

Similarly, a quantum algorithm will be said to reversely majorize this probability distribution between steps m and $m+1$ if and only if

$$\vec{p}^{(m+1)} \prec \vec{p}^{(m)} \, . \tag{6.4}$$

If Eq.6.3 is step-by-step verified, then there is a net flow of probability towards the value of highest weight, in such a way that the probability distribution will be steeper and steeper as time flows in the algorithm. In physical terms, this can be stated as a very particular constructive interference behavior, namely, a constructive interference that has to step-by-step satisfy a set of

$N-1$ constraints – see Appendix A – at each time step. The quantum algorithm monotonically builds up the solution by means of this very precise reordering of the probability distribution.

It is important to note that majorization is checked on a particular basis. Step-by-step majorization is, then, a basis-dependent concept. Nevertheless there is a preferred basis, namely, the basis defined by the final measurement of the quantum register. This typically (though not necessarily always) corresponds to the computational basis of the quantum computer. The principle we analyze is rooted in the physical and practical possibility to arbitrarily stop the computation at any time and perform a measurement. Generically speaking, we analyze the majorization properties of the probability distribution of the possible outcomes of our measurement apparatus along the time-flow in the algorithm.

Natural majorization

Let us now define the concept of natural majorization for quantum algorithms. Working with the probability amplitudes in the basis $\{|i\rangle\}_{i=1}^{N}$ as defined in Eq.6.1, the action of a generic unitary gate at step m makes the amplitudes evolve to step $m+1$ in the following way:

$$a_i^{(m+1)} = \sum_{j=1}^{N} U_{ij} a_j^{(m)} \,, \tag{6.5}$$

where U_{ij} are the matrix elements in the chosen basis of the unitary evolution operator. By inverting this evolution, we can write

$$a_i^{(m)} = \sum_{j=1}^{N} C_{ij} a_j^{(m+1)} \,, \tag{6.6}$$

where C_{ij} are the matrix elements of the inverse unitary evolution, which is of course unitary as well. Taking the square-modulus we find

$$|a_i^{(m)}|^2 = \sum_{j=1}^{N} |C_{ij}|^2 |a_j^{(m+1)}|^2 + \text{interference terms} \,. \tag{6.7}$$

Should the interference terms disappear, majorization would be verified in a "natural" way between steps m and $m+1$ since the initial probability distribution could be obtained from the final one just by the action of a doubly stochastic matrix with entries $|C_{ij}|^2$. We shall refer to this property as "natural majorization": majorization which naturally emerges from the unitary evolution due to the lack of interference terms when making the square-modulus of the probability amplitudes. Similarly, we can define the concept of "natural reverse majorization", which follows in a straightforward way: there will be "natural reverse majorization" between steps m and $m+1$ if and only if there is "natural majorization" between steps $m+1$ and m. As we shall see, this very specific kind of majorization shall appear in some of our forthcoming calculations.

6.2 Majorization in quantum phase-estimation algorithms

Quantum phase-estimation algorithms [2, 8, 161, 181–183] are a good example of a wide class of quantum algorithms to begin our study. Their key ingredients are the use of the quantum Fourier transform operator and the promise of a specific structure of the initial state. In [152], it has been numerically checked that the canonical form of the quantum Fourier transform majorizes step-by-step the probability distribution attached to the computational basis. Here we analytically address this problem and provide a proof of how the notion of majorization formulated in [152] explicitly operates in the special case of quantum phase-estimation algorithms. To be more specific, our purpose now is to present a detailed proof of the following proposition: majorization works step-by-step in the quantum Fourier transform of quantum phase-estimation algorithms. The whole property is based on the idea that Hadamard operators act by majorizing the probability distribution given the symmetry of the quantum state, and such a symmetry is partially preserved under the action of both Hadamard and controlled-phase gates [152].

6.2.1 The quantum phase-estimation algorithm

Quantum phase-estimation algorithms were originally introduced by Kitaev in [183], and the basic problem that they aim to solve can be stated as follows. Given a unitary operator U and one of its eigenvectors $|\phi\rangle$, estimate the phase of the corresponding eigenvalue $U|\phi\rangle = e^{-2\pi i\phi}|\phi\rangle$, $\phi \in [0, 1)$ up to n bits of accuracy. An efficient solution was found in [161] and can be summarized in the following steps, as represented by the quantum circuit of Fig.6.1:

(i) Prepare the pure state $|\psi^{(i)}\rangle = |0, 0, \ldots, 0\rangle|\phi\rangle$, where $|0, 0, \ldots, 0\rangle$ is called the source register state of n qubits and $|\phi\rangle$ is the target state where we have stored the given eigenvector of the unitary operator U.

(ii) Apply Hadamard operators

$$U_H^{(i)} = \frac{1}{\sqrt{2}}\left(\sigma_i^x + \sigma_i^z\right) \tag{6.8}$$

over all the qubits i in the source state, $i = 1, 2, \ldots, n$.

(iii) Apply bit-wise controlled U^j gates over the target state as shown in the Fig.6.1, where each U^j gate corresponds to the application of j times the proposed U-gate with $j = 0, 1 \ldots n-1$.

(iv) Apply the quantum Fourier transform operator

$$QFT|q\rangle = \frac{1}{2^{n/2}} \sum_{q'=0}^{2^n-1} e^{2\pi i q q'/2^n}|q'\rangle \tag{6.9}$$

over the source register state.

(v) Make a measurement of the source state of the system. This provides with high probability the corresponding eigenvalue of U with the required precision.

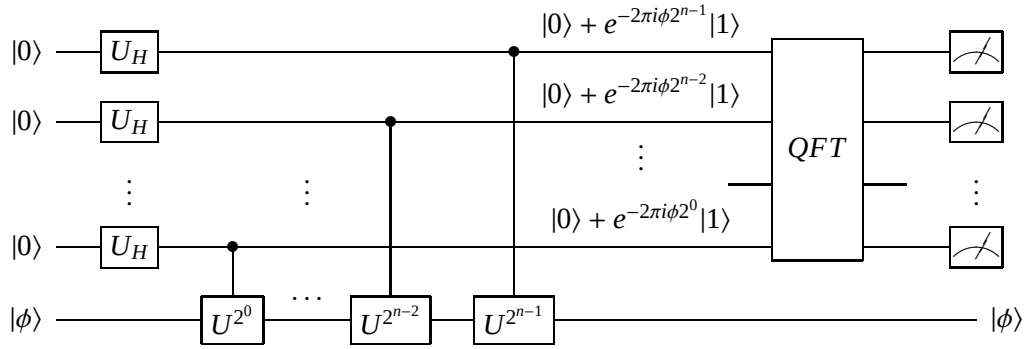

Figure 6.1: Quantum circuit for the quantum phase-estimation algorithm.

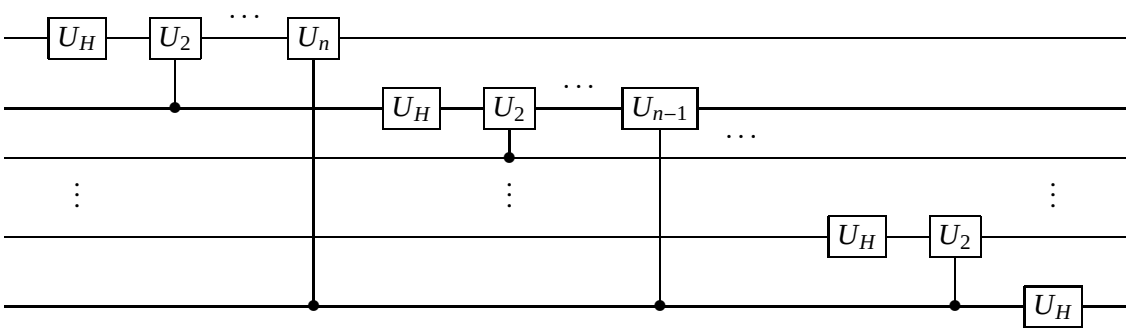

Figure 6.2: Canonical decomposition of the quantum Fourier transform operator. By U_j we denote the unitary gate $|0\rangle\langle 0| + e^{2\pi i/2^j}|1\rangle\langle 1|$, to be controlled $j-1$ qubits below.

6.2.2 Analytical results

Let us now go through the steps of the algorithm focusing on how the majorization of the considered set of probabilities of the computational states evolve. The application of the Hadamard gates in step (ii) to the initial state produces a lowest element of majorization by means of step-by-step reverse majorization,

$$|\psi^{(ii)}\rangle = 2^{-n/2} \sum_{x=0}^{2^n-1} |x\rangle|\phi\rangle \,, \tag{6.10}$$

yielding the probability distribution $p_x^{(ii)} = 2^{-n}\ \forall x$. The outcome of the controlled U^j gates in step (iii) is the *product* state

$$\begin{aligned} |\psi^{(iii)}\rangle &= 2^{-n/2} \left(|0\rangle + e^{-2\pi i 2^{n-1}\phi}|1\rangle\right) \cdots \left(|0\rangle + e^{-2\pi i 2^{0}\phi}|1\rangle\right) |\phi\rangle \\ &= 2^{-n/2} \textstyle\sum_{x=0}^{2^n-1} e^{-2\pi i x\phi}|x\rangle|\phi\rangle \,. \end{aligned} \tag{6.11}$$

Since the action of these gates adds only local phases in the computational basis, the uniform distribution for the probabilities is maintained ($p_x^{(iii)} = 2^{-n}\ \forall x$).

Verifying majorization for the global action of the quantum Fourier transform is simple. After step (iv) the quantum state becomes

$$|\psi^{(iv)}\rangle = 2^{-n} \sum_{x,y=0}^{2^n-1} e^{-2\pi i x(\phi - y/2^n)} |y\rangle|\phi\rangle \; . \tag{6.12}$$

We then have the probability distribution

$$p_y^{(iv)} = \left| 2^{-n} \sum_{x=0}^{2^n-1} e^{-2\pi i x(\phi - y/2^n)} \right|^2 \qquad \forall y \; . \tag{6.13}$$

Global majorization between steps (ii) and (iv) holds [152]. The remaining step (v) corresponds to a measurement whose output is controlled with the probability distribution $p_y^{(iv)}$.

While global majorization of the probability distribution is somehow straightforward to see, step-by-step majorization is less obvious. To this aim, the mathematical result that we shall prove reads as follows: the quantum Fourier transform majorizes step-by-step the probability distribution calculated in the computational basis as used in the quantum phase-estimation algorithm. This fact is seen to emerge from two important properties. It is, first, essential that the initial state entering the quantum Fourier transform has a certain symmetry to be discussed. Second, the order of the action of Hadamard and controlled-phase gates maintains as much of this symmetry as to be used by the rest of the algorithm. To be precise, Hadamard gates take the role of majorizing the probability distribution as long as some relative phases are properly protected. Controlled-phase transformations do preserve such a symmetry, as we shall see.

The above property arises in three steps: the first one consists on a majorization lemma, the second one is a lemma concerning the preservation of phases, and finally the third one is the analysis of the controlled-phase operators in the quantum Fourier transform. As hinted above, we shall observe that the only relevant operators for the majorization procedure are the Hadamard gates acting over the different qubits, while controlled-phase operators, though providing entanglement, turn out to be immaterial for majorization purposes.

A majorization lemma

Let us first introduce the concept of "H(j)-pair", central to this discussion. Consider a Hadamard gate $U_H^{(j)}$ acting on qubit j of the quantum register. In general, the quantum register would correspond to a superposition of states. This superposition can be organized in pairs, each pair being characterized by the fact that the Hadamard operation on qubit j will mix the two states in the pair. Let us illustrate this concept with the example of a general quantum state of two qubits:

$$\begin{aligned} |\psi\rangle \quad &= \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle \\ &= \underbrace{(\alpha|00\rangle + \gamma|10\rangle)}_{\text{H(0)}-\text{pair}} + \underbrace{(\beta|01\rangle + \delta|11\rangle)}_{\text{H(0)}-\text{pair}} \\ &= \underbrace{(\alpha|00\rangle + \beta|01\rangle)}_{\text{H(1)}-\text{pair}} + \underbrace{(\gamma|10\rangle + \delta|11\rangle)}_{\text{H(1)}-\text{pair}} \; . \end{aligned} \tag{6.14}$$

The second line corresponds to organizing the state as $H(0)$-pairs, because each pair differs only on the 0th qubit value. The third line, instead, organizes the state on $H(1)$-pairs, since each pair differs only on the first qubit value. We now formulate the following lemma:

Lemma 6.1: *Let $|\psi\rangle$ denote a pure quantum state of n qubits, with the property that the probability amplitudes of the computational H(j)-pairs differ only by a phase for a given qubit j. Then, the probability distribution resulting from $U_H^{(j)}|\psi\rangle$ in the computational basis majorizes the one resulting from $|\psi\rangle$.*

Proof: The state $|\psi\rangle$ can always be written as:

$$\begin{aligned}|\psi\rangle = a_1|0,0,\ldots,0^j,\ldots,0\rangle + a_1 e^{i\delta_1}|0,0,\ldots,1^j,\ldots,0\rangle \\ +\cdots + a_{2^{n-1}}|1,1,\ldots,0^j,\ldots,1\rangle + a_{2^{n-1}}e^{i\delta_{2^{n-1}}}|1,1,\ldots,1^j,\ldots 1\rangle\,.\end{aligned} \tag{6.15}$$

The above expression makes it explicit that the amplitudes for every pair of states that can be mixed by a Hadamard transformation on the qubit j only differ by a phase. The Hadamard gate $U_H^{(j)}$ will mix all these pairs. The two states in every pair are equal in all their qubits except for the jth one. After the application of the $U_H^{(j)}$ we have

$$\begin{aligned}U_H^{(j)}|\psi\rangle = 2^{-1/2}\Big(a_1\left(1+e^{i\delta_1}\right)|0,0,\ldots,0^j,\ldots,0\rangle + a_1\left(1-e^{i\delta_1}\right)|0,0,\ldots,1^j,\ldots,0\rangle \\ +\cdots + a_{2^{n-1}}\left(1+e^{i\delta_{2^{n-1}}}\right)|1,1,\ldots,0^j,\ldots,1\rangle + a_{2^{n-1}}\left(1-e^{i\delta_{2^{n-1}}}\right)|1,1,\ldots,1^j,\ldots,1\rangle\Big)\,.\end{aligned} \tag{6.16}$$

We have to find a set of probabilities p_k and permutation matrices P_k such that

$$\begin{pmatrix}|a_1|^2\\|a_1|^2\\\vdots\\|a_{2^n-1}|^2\\|a_{2^n-1}|^2\end{pmatrix} = \sum_k p_k P_k \begin{pmatrix}|a_1|^2(1+\cos(\delta_1))\\|a_1|^2(1-\cos(\delta_1))\\\vdots\\|a_{2^n-1}|^2(1+\cos(\delta_{2^n-1}))\\|a_{2^n-1}|^2(1-\cos(\delta_{2^n-1}))\end{pmatrix}, \tag{6.17}$$

and the unique solution to this probabilistic mixture is

$$p_1 = p_2 = \tfrac{1}{2}$$

$$P_1 = \begin{pmatrix}1&&&&\\&1&&&\\&&\ddots&&\\&&&1&\\&&&&1\end{pmatrix};\quad P_2 = \begin{pmatrix}0&1&&&\\1&0&&&\\&&\ddots&&\\&&&0&1\\&&&1&0\end{pmatrix}. \tag{6.18}$$

The permutation matrix P_1 is nothing but the identity matrix and P_2 is a permutation of the probabilities of each pair which has undergone Hadamard mixing. This completes the proof of the lemma. □

The lemma we have just presented states that Hadamard transformations do order the probability distribution when the input state has a special structure, namely, those amplitudes to be mixed only differ by phases. This is the key element pervading in the quantum phase-estimation algorithm: Hadamard transformations and controlled-phase transformations carefully preserve such a structure when needed, as we shall now see.

A phase-preservation lemma

Let us now prove the following lemma:

Lemma 6.2: *Consider the Hadamard gate $U_H^{(j)}$ acting on qubit j, and the quantum state $|\psi^{(iii)}\rangle$ from Eq.6.11 with the property that the probability amplitudes of the computational H(i)-pairs differ only by a phase which only depends on i, $\forall i$. Then, the quantum state $U_H^{(j)}|\psi^{(iii)}\rangle$ is such that the H(i)-pairs differ only by a phase $\forall i \neq j$.*

This lemma implies that the quantum Fourier transform works in such a way that states to be mixed by Hadamard transformations only differ by a phase all along the computation, until the very moment when the Hadamard operator acts. In other words, the structure of gates respects the relative weights of the H(i)-pairs.

Before proving the Lemma 6.2 let us build some intuition by considering first an example. We start by introducing a new notation for the phases appearing in the source quantum state of Eq.6.11 to be operated by the quantum Fourier transform operator by defining $\beta_x \equiv -2\pi x\phi$. Then

$$|\psi^{(iii)}\rangle = 2^{-n/2} \sum_{x=0}^{2^n-1} e^{i\beta_x}|x\rangle \ . \tag{6.19}$$

Notice that since $x = \sum_{i=0}^{n-1} x_i 2^i$, we can write

$$\beta_x = \sum_{i=0}^{n-1} -2\pi x_i 2^i \phi \equiv \sum_{i=0}^{n-1} x_i \alpha_i \ , \tag{6.20}$$

where $\alpha_i \equiv -2\pi 2^i \phi$. As an example of this notation, let us write the state $|\psi^{(iii)}\rangle$ in the case of three qubits:

$$\begin{aligned} |\psi^{(iii)}\rangle = & \quad \frac{1}{2^{3/2}}\Big(|000\rangle + e^{i\alpha_2}|100\rangle + e^{i\alpha_1}|010\rangle + e^{i(\alpha_2+\alpha_1)}|110\rangle\Big) \\ + & \quad \frac{1}{2^{3/2}}\Big(|001\rangle + e^{i\alpha_2}|101\rangle + e^{i\alpha_1}|011\rangle + e^{i(\alpha_2+\alpha_1)}|111\rangle\Big)e^{i\alpha_0} \ . \end{aligned} \tag{6.21}$$

We have factorized the α_0 phase in the second line of the above equation. Alternatively, we can choose to factorize α_1,

$$\begin{aligned} |\psi^{(iii)}\rangle = & \quad \frac{1}{2^{3/2}}\Big(|000\rangle + e^{i\alpha_2}|100\rangle + e^{i\alpha_0}|001\rangle + e^{i(\alpha_2+\alpha_0)}|101\rangle\Big) \\ + & \quad \frac{1}{2^{3/2}}\Big(|010\rangle + e^{i\alpha_2}|110\rangle + e^{i\alpha_0}|011\rangle + e^{i(\alpha_2+\alpha_0)}|111\rangle\Big)e^{i\alpha_1} \ , \end{aligned} \tag{6.22}$$

or α_2,

$$|\psi^{(iii)}\rangle = \frac{1}{2^{3/2}}\left(|000\rangle + e^{i\alpha_1}|010\rangle + e^{i\alpha_0}|001\rangle + e^{i(\alpha_1+\alpha_0)}|011\rangle\right) + \frac{1}{2^{3/2}}\left(|100\rangle + e^{i\alpha_1}|110\rangle + e^{i\alpha_0}|101\rangle + e^{i(\alpha_1+\alpha_0)}|111\rangle\right)e^{i\alpha_2} . \quad (6.23)$$

On the whole, the initial state for three qubits can be factorized in these three different ways. This example shows that there are three different possibilities to write the quantum state by focusing on a particular qubit. The above property is easily extrapolated to the general case of n qubits: we can always write the quantum state $|\psi^{(iii)}\rangle$ in n different ways by factorizing a particular phase in the second line.

Proof: In the general case we can factorize the α_j phase so that the pure state is written as

$$|\psi^{(iii)}\rangle = \frac{1}{2^{n/2}}\left(|0,0,\ldots,0^j,\ldots,0\rangle + \cdots + e^{i\sum_{k\neq j}\alpha_k}|1,1,\ldots,0^j,\ldots,1\rangle\right) + \frac{1}{2^{n/2}}\left(|0,0,\ldots,1^j,\ldots,0\rangle + \cdots + e^{i\sum_{k\neq j}\alpha_k}|1,1,\ldots,1^j,\ldots,1\rangle\right)e^{i\alpha_j} . \quad (6.24)$$

Then, the action of $U_H^{(j)}$ transforms the state as follows:

$$U_H^{(j)}|\psi^{(iii)}\rangle = \frac{(1+e^{i\alpha_j})}{2^{(n+1)/2}}\left(|0,0,\ldots,0^j,\ldots,0\rangle + \cdots + e^{i\sum_{k\neq j}\alpha_k}|1,1,\ldots,0^j,\ldots,1\rangle\right) + \frac{(1-e^{i\alpha_j})}{2^{(n+1)/2}}\left(|0,0,\ldots,1^j,\ldots,0\rangle + \cdots + e^{i\sum_{k\neq j}\alpha_k}|1,1,\ldots,1^j,\ldots,1\rangle\right) . \quad (6.25)$$

The resulting state still preserves the necessary symmetry property to apply Lemma 6.2 to the rest of qubits $i \neq j$. The reason is that the effect of the operator has been to split the quantum state in two pieces which individually retain the property that all the H(i)-pairs differ only by a phase for $i \neq j$. If we now apply another Hadamard operator over a different qubit, for instance qubit $j-1$, each of these two quantum states splits in turn in two pieces

$$\begin{aligned} & U_H^{(j-1)}U_H^{(j)}|\psi^{(iii)}\rangle = \\ & \frac{(1+e^{i\alpha_j})(1+e^{i\alpha_{j-1}})}{2^{(n+2)/2}}\left(|0,0,\ldots,0^{j-1},0^j,\ldots,0\rangle + \cdots + e^{i\beta_{\tilde{x}}}|1,1,\ldots,0^{j-1},0^j,\ldots,1\rangle\right) \\ + & \frac{(1+e^{i\alpha_j})(1-e^{i\alpha_{j-1}})}{2^{(n+2)/2}}\left(|0,0,\ldots,1^{j-1},0^j,\ldots,0\rangle + \cdots + e^{i\beta_{\tilde{x}}}|1,1,\ldots,1^{j-1},0^j,\ldots,1\rangle\right) \\ + & \frac{(1-e^{i\alpha_j})(1+e^{i\alpha_{j-1}})}{2^{(n+2)/2}}\left(|0,0,\ldots,0^{j-1},1^j,\ldots,0\rangle + \cdots + e^{i\beta_{\tilde{x}}}|1,1,\ldots,0^{j-1},1^j,\ldots,1\rangle\right) \\ + & \frac{(1-e^{i\alpha_j})(1-e^{i\alpha_{j-1}})}{2^{(n+2)/2}}\left(|0,0,\ldots,1^{j-1},1^j,\ldots,0\rangle + \cdots + e^{i\beta_{\tilde{x}}}|1,1,\ldots,1^{j-1},1^j,\ldots,1\rangle\right) , \end{aligned} \quad (6.26)$$

where $\beta_{\tilde{x}}$ is the phase defined in Eq.6.20 for the n-bit string $\tilde{x} = (1,1,\ldots,0^{j-1},0^j,\ldots,1)$. The register now consists of a superposition of four quantum states, each one made of amplitudes

that only differ by a phase. Further application of a Hadamard gate over yet a different qubit would split each of the four states again in two pieces in a way that the symmetry would again be preserved within each piece. This splitting takes place each time a particular Hadamard acts. Thus, all Hadamard gates operate in turn producing majorization while not spoiling the symmetry property needed for the next step. This completes the proof of the phase-preserving Lemma 6.2. □

Analysis of the controlled-phase operators

It is still necessary to verify that the action of controlled-phase gates does not interfere with the majorization action carried by the Hadamard gates. Let us concentrate on the action of $U_H^{(n-1)}$, which is the first Hadamard operator applied in the canonical decomposition of the quantum Fourier transform. Originally we had

$$\begin{aligned} |\psi^{(iii)}\rangle = & \quad \frac{1}{2^{n/2}}\left(|0,0,\ldots,0\rangle + \cdots + e^{i\sum_{k\neq n-1}\alpha_k}|0,1,\ldots,1\rangle\right) \\ + & \quad \frac{1}{2^{n/2}}\left(|1,0,\ldots,0\rangle + \cdots + e^{i\sum_{k\neq n-1}\alpha_k}|1,1,\ldots,1\rangle\right)e^{i\alpha_{n-1}}\,, \end{aligned} \tag{6.27}$$

where we have taken the α_{n-1} phase-factor out. After the action of $U_H^{(n-1)}$ we get

$$\begin{aligned} U_H^{(n-1)}|\psi^{(iii)}\rangle = & \quad \frac{(1+e^{i\alpha_{n-1}})}{2^{(n+1)/2}}\left(|0,0,\ldots,0\rangle + \cdots + e^{i\sum_{k\neq n-1}\alpha_k}|0,1,\ldots,1\rangle\right) \\ + & \quad \frac{(1-e^{i\alpha_{n-1}})}{2^{(n+1)/2}}\left(|1,0,\ldots,0\rangle + \cdots + e^{i\sum_{k\neq n-1}\alpha_k}|1,1,\ldots,1\rangle\right) \equiv |a\rangle + |b\rangle\,. \end{aligned} \tag{6.28}$$

We repeat our previous observation that the state resulting from the action of $U_H^{(n-1)}$ can be considered as the sum of two states, which we have called $|a\rangle$ and $|b\rangle$. For each of these two states the amplitudes of the $H(i)$-pairs $\forall i \neq n-1$ still differ only by a phase.

We can now analyze the effect of the controlled-phase operators. Following the structure of the quantum Fourier transform operator (see Fig.6.2) we focus on what happens after applying a general controlled-phase operator on the $(n-1)$th qubit of the quantum state $U_H^{(n-1)}|\psi^{(iii)}\rangle$ (the following procedure is easily extrapolated to the controlled-phase operators acting over the rest of the qubits). If the control qubit is the lth one, $l \neq n-1$, then the operator will only add phases over those computational states from Eq.6.28 such that both the $(n-1)$th and the lth qubits are equal to 1, so we see that it will only act on the $|b\rangle$ state. Let us write $|b\rangle$ by factorizing the lth phase as follows:

$$\begin{aligned} |b\rangle = & \quad \frac{(1-e^{i\alpha_{n-1}})}{2^{(n+1)/2}}\left(|1,0,\ldots,0^l,\ldots,0\rangle + \cdots + e^{i\sum_{k\neq l,n-1}\alpha_k}|1,1,\ldots,0^l,\ldots,1\rangle\right) \\ + & \quad \frac{(1-e^{i\alpha_{n-1}})}{2^{(n+1)/2}}\left(|1,0,\ldots,1^l,\ldots,0\rangle + \cdots + e^{i\sum_{k\neq l,n-1}\alpha_k}|1,1,\ldots,1^l,\ldots,1\rangle\right)e^{i\alpha_l}\,. \end{aligned} \tag{6.29}$$

It is now clear that the action of the controlled-phase gate only adds a global phase in the second piece of $|b\rangle$, which can always be absorbed by means of a convenient redefinition of the phase

α_l. Hence we see that no relevant change is made in the quantum state concerning majorization, because the amplitudes of the computational $H(i)$-pairs $\forall i \neq n-1$ still differ only by a single phase which only depends on i. The action of controlled-phase operators only amounts to a redefinition of phases, which does not affect the necessary property for the Lemma 6.1 to hold. We see that the needed phase redefinition can be easily made each time one of these operators acts over a particular qubit.

From all the above considerations and lemmas, it immediately follows that the quantum Fourier transform operator majorizes step-by-step the probability distribution in phase-estimation algorithms, as we wished to show. We wish to emphasize the fact that controlled-phase operators play no role on majorization, though they provide entanglement. On the contrary, local Hadamard operators act exactly in the complementary way, providing majorization without providing entanglement. We also note that the majorization arrow in the quantum algorithm is based on two ingredients. On the one hand we have the special properties of the quantum state, and on the other hand we have the structure of the quantum Fourier transform. A quantum Fourier transform acting on an arbitrary state would fail to obey majorization.

One may be tempted to say at this point that Shor's quantum factoring algorithm [8] obeys a majorization arrow, since it can be completely understood in terms of a certain quantum-phase estimation algorithm, as we already saw in Chapter 4 (see Fig.4.2). Notice, though, that there is a subtle but key difference between the quantum phase-estimation procedure explained here and the one being used in Shor's algorithm, namely, the target register in Shor's algorithm is not in a particular eigenstate of the unitary operator of Eq.4.4, but in a given superposition of all of them. This difference makes step-by-step majorization in Shor's quantum factoring algorithm fail. To see how this actually happens, let us remind that in Shor's quantum factoring algorithm the source state to be processed by the QFT operator is not the one from Eq.6.11, but the state

$$\sqrt{\frac{r}{2^n}} \sum_{i=0}^{2^n/r-1} |ir + l\rangle \,, \tag{6.30}$$

for a particular $l = 0, 1, \ldots, r-1$ (or a superposition of all of them according to Eq.4.8), where r is the period of the modular exponentiation function $f(x) = a^x \bmod N$, with a randomly chosen $a \in [1, N]$, N being the number to be factorized. The number of qubits n of the source register is chosen such that $2^n \in [N^2, 2N^2]$. The non-trivial instances of Shor's algorithm come whenever r is both even and $O(N)$, as we saw in Chapter 4. We notice that whenever r is even, then $ir + l$ is either even if l is even, or odd if l is odd, $\forall i$. Therefore, the single bit that determines the parity of $ir + l$ will always be either 0 or 1, which implies that the corresponding qubit will always be either $|0\rangle$ or $|1\rangle$ in all the states of the superposition from Eq.6.30. It is clear, then, that the action of a Hadamard gate on that specific qubit does not majorize the probability distribution of the final outcomes. Even in the case of removing that qubit from the register, there typically are other qubits in the quantum state from Eq.6.30 that have the same value in all the states of the superposition, as happens already in the simple case $r = 4$, and about which we can not have any a priori information. The whole computation must be then carried without the possibility of removing these qubits, whose evolution breaks step-by-step majorization. Nevertheless, majorization seems to be working locally in the neighborhood of the final peaks of the distribution rather than globally on the whole set of probabilities. As a

matter of fact, it is also true that our derivations rely very much on the specific decomposition of the quantum Fourier transform in terms of individual gates. The underlying quantum circuit is not unique and majorization may not be present if alternative decompositions are considered.

6.2.3 Natural majorization and comparison with quantum searching

We now turn to investigate further the way majorization has emerged in the quantum phase-estimation algorithm as compared to majorization in other quantum algorithms, such as Grover's searching algorithm [9, 152].

For a search in an unstructured database of a particular item, the best known classical algorithm takes asymptotically $O(2^n)$ steps in succeeding (where $2^n \equiv N$ is the number of entries). However, and as we already said in Chapter 4, Grover was able to discover a quantum mechanical algorithm that implements a quadratic speed-up as compared to the best classical one, that is, Grover's quantum algorithm makes use of $O(2^{n/2})$ steps. We do not enter here into precise details about the construction of this quantum algorithm, and will only make a few comments on the way it proceeds. The interested reader is addressed to [9].

The analysis of Grover's algorithm can be reduced to a two-dimensional Hilbert space spanned by the state we are searching $|x_0\rangle$ and some orthogonal state $|x_0^{\perp}\rangle$ [2]. The unitary evolution of the quantum state is given by the repeated application of a given kernel K which amounts to a rotation

$$K = \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}, \tag{6.31}$$

where $\cos(\theta) = 1 - 2/2^n$. Other choices of kernels are possible but the one from the above equation is optimal [162, 184]. The initial state of the computation is an equal superposition of all the computational states, written as $|\psi\rangle = 2^{-n/2}|x_0\rangle + (1-2^{-n})^{1/2}\,|x_0^{\perp}\rangle$ in this two-dimensional notation. For a given intermediate computation step the state $(\alpha,\beta)^T$ will be transformed to $(\alpha',\beta')^T$. If we wish to express the initial amplitudes in terms of the final ones, we have:

$$\begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \alpha' \cos(\theta) + \beta' \sin(\theta) \\ -\alpha' \sin(\theta) + \beta' \cos(\theta) \end{pmatrix}. \tag{6.32}$$

We now take the square-modulus of the amplitudes, obtaining:

$$\begin{aligned} |\alpha|^2 &= \cos^2(\theta)\,|\alpha'|^2 + \sin^2(\theta)\,|\beta'|^2 + 2\cos(\theta)\sin(\theta)\,\mathcal{R}e(\alpha'^{*}\beta') \\ |\beta|^2 &= \sin^2(\theta)\,|\alpha'|^2 + \cos^2(\theta)\,|\beta'|^2 - 2\cos(\theta)\sin(\theta)\,\mathcal{R}e(\alpha'^{*}\beta')\,. \end{aligned} \tag{6.33}$$

If the interference terms were to vanish then majorization would follow in a straightforward way from the above relations. But it is not the case. Yet it has been proven that step-by-step majorization in Grover's algorithm exists [152], although the way it arises is not so directly related to the unitary evolution in the way suggested here.

Let us turn back to majorization in the quantum phase-estimation algorithm and its relation to unitary evolution. We write a generic n-qubit state $|\psi\rangle$ to be operated by a Hadamard gate acting on the jth qubit as

$$|\psi\rangle = c_0|0,0,\ldots,0^j,\ldots,0\rangle + c_j|0,0,\ldots,1^j,\ldots,0\rangle$$
$$+\cdots + c_{2^n-1-j}|1,1,\ldots,0^j,\ldots,1\rangle + c_{2^n-1}|1,1,\ldots,1^j,\ldots,1\rangle\,, \tag{6.34}$$

where we are focusing on the coefficients of the different $H(j)$-pairs. Applying the Hadamard gate over the jth qubit we get

$$U_H^{(j)}|\psi\rangle = 2^{-1/2}(c_0 + c_j)|0,0,\ldots,0^j,\ldots,0\rangle + 2^{-1/2}(c_0 - c_j)|0,0,\ldots,1^j,\ldots,0\rangle$$
$$+\cdots + 2^{-1/2}(c_{2^n-1-j} + c_{2^n-1})|1,1,\ldots,0^j,\ldots,1\rangle$$
$$+2^{-1/2}(c_{2^n-1-j} - c_{2^n-1})|1,1,\ldots,1^j,\ldots,1\rangle\,. \tag{6.35}$$

For a given pair of original amplitudes c_{m-j} and c_m we now find final amplitudes c'_{m-j} and c'_m to be related to the initial ones as follows:

$$\begin{pmatrix} c_{m-j} \\ c_m \end{pmatrix} = \tfrac{1}{2^{1/2}} \begin{pmatrix} c'_{m-j} + c'_m \\ c'_{m-j} - c'_m \end{pmatrix}\,. \tag{6.36}$$

Taking the square-modulus of the amplitudes in the above expression we have

$$\begin{aligned} |c_{m-j}|^2 &= \frac{1}{2}|c'_{m-j}|^2 + \frac{1}{2}|c'_m|^2 + \mathcal{R}e(c'^*_{m-j}c'_m) \\ |c_m|^2 &= \frac{1}{2}|c'_{m-j}|^2 + \frac{1}{2}|c'_m|^2 - \mathcal{R}e(c'^*_{m-j}c'_m)\,. \end{aligned} \tag{6.37}$$

As in the Grover's previous example, we observe that if interference terms disappeared majorization would arise from this set of relations. In such a case, we would only have to choose the set of probabilities and permutation matrices given in Eq.6.18 to prove majorization. For those terms to vanish, very specific properties for the coefficients c_{m-j} and c_m must hold. It can be checked that the interference terms vanish if and only if

$$\begin{aligned} c_{m-j} &= a_{m-j} \\ c_m &= a_{m-j}e^{i\delta_{m-j}}\,, \end{aligned} \tag{6.38}$$

where a_{m-j} is real.

The above case is indeed the case of quantum phase-estimation algorithms. Recalling our previous lemmas, it is possible to see that the interference terms vanish also step-by-step, and therefore step-by-step majorization arises as a natural consequence of the unitary evolution of the algorithm. Notice that the quantum state from Eq.6.11 has a very specific structure so that natural majorization is verified step-by-step along the evolution through the quantum Fourier transform circuit. In a way we can say that previous steps in the algorithm prepare the source state in this particular and unique form, in order to be processed by the QFT operator.

6.2.4 The quantum hidden affine function determination algorithm

We now wish to see how all the above properties work in a specific example of quantum algorithm, namely, we study majorization in a quantum algorithm solving a particular hidden affine function problem [181] as a generalization of Deutsch's problem [185]. Further studies have provided a range of fast quantum algorithms for solving different generalizations [161, 182]. The case that we present here is one of the multiple variations that appear in [182], but our main results are also valid for the whole set of quantum algorithms that solve similar situations. As we shall see, this algorithm can indeed be understood in terms of a slight variation of the general quantum phase-estimation algorithm previously discussed.

Let us consider the following problem [182]: given an integer-N function $f : \mathbb{Z}_N \to \mathbb{Z}_N$, $f(x) = mx + b$, where $x, m, b \in \mathbb{Z}_N$, find out the value of m. A classical analysis reveals that no information about m can be obtained with only one evaluation of the function f. Conversely, given the unitary operator U_f acting in a reversible way such that

$$U_f|x\rangle|y\rangle = |x\rangle|y + f(x)\rangle\,, \tag{6.39}$$

– where the sum is to be interpreted as modulus N – there is a quantum algorithm solving this problem with only one single query to U_f. The requested quantum algorithm proceeds as follows: let us take $N = 2^n$, n being the number of qubits. Perform then the following steps:

(i) Prepare two n-qubit registers (source and target) in the state $|0, 0, \ldots, 0\rangle|\psi_1\rangle$, where $|\psi_1\rangle = QFT^{-1}|1, 1, \ldots, 1\rangle$, and QFT^{-1} denotes the inverse quantum Fourier transform in a Hilbert space of dimension N.

(ii) Apply the operator QFT over the source register.

(iii) Apply the operator U_f over the whole quantum state (source and target registers).

(iv) Apply the operator QFT^{-1} over the source register.

(v) Measure the source register and output the measured value.

The different steps concerning this process are summarized in Fig.6.3.

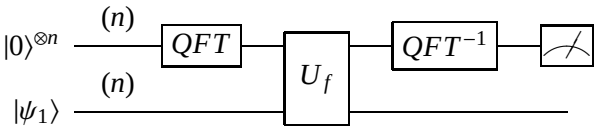

Figure 6.3: Quantum circuit solving the hidden affine function problem. Both source and target registers are assumed to be respectively composed of n qubits.

We now show how the proposed quantum algorithm leads to the solution of the problem. Our analysis raises observations concerning the way both entanglement and majorization behave along the evolution.

In step (i) of the algorithm the quantum state is not entangled, since that the quantum Fourier transform – and its inverse – applied on a well defined state in the computational basis leads to a separable state (see, for example, [2]). That is, the quantum state $|0,0,\ldots,0\rangle|\psi_1\rangle$ is completely separable. In step (ii) the algorithm evolves through a quantum Fourier transform in the source register. This action leads to a step-by-step reverse majorization of the probability distribution of the possible outcomes while it does not use neither create any entanglement. Moreover, natural reverse majorization is at work due to the absence of interference terms.

Next, it is easy to verify that the quantum state

$$|\psi_1\rangle = \frac{1}{2^{n/2}} \sum_{y=0}^{2^n-1} e^{-2\pi i y/2^n} |y\rangle \tag{6.40}$$

is an eigenstate of the operation $|y\rangle \rightarrow |y + f(x)\rangle$ with eigenvalue $e^{2\pi i f(x)/2^n}$. Thus, after the third step, the quantum state reads

$$\frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} e^{2\pi i f(x)/2^n} |x\rangle|\psi_1\rangle = \frac{e^{2\pi i b/2^n}}{2^{n/2}} \left(\sum_{x=0}^{2^n-1} e^{2\pi i m x/2^n} |x\rangle \right) |\psi_1\rangle \, . \tag{6.41}$$

The probability distribution of possible outcomes has not been modified, thus not affecting majorization. Furthermore, the pure quantum state of the first register can be written as $QFT|m\rangle$ (up to a phase factor), so this step has not eventually created any entanglement among the qubits of the system right after the application of the quantum oracle.

In step (iv) of the algorithm, the action of the operator QFT^{-1} over the first register leads to the state $e^{2\pi i b/2^n}|m\rangle|\psi_1\rangle$. A subsequent measurement in the computational basis over the first register provides the desired solution. Recalling our previous results, we see that the inverse quantum Fourier transform naturally majorizes step-by-step the probability distribution attached to the different outputs. Notice also that the separability of the quantum state still holds step-by-step. This observation completes our analysis of this example.

6.3 Majorization in adiabatic quantum searching algorithms

Our aim now is to study the majorization behavior of quantum adiabatic algorithms, which were already considered in the two previous Chapters. Here, we choose to analyze a very specific instance of the quantum adiabatic algorithm, namely, we consider the quantum adiabatic algorithm that solves the problem of searching in an unstructured database. As we shall see, the effects of a change of path between the initial and the problem Hamiltonian imply also a change of behavior in the algorithm from the majorization's perspective. More concretely, those paths leading to optimality in the quantum algorithm do lead as well to step-by-step majorization, while the converse is not necessarily true. We do not repeat here the details of how do adiabatic quantum algorithms work, since they were already explained in Chapter 4. We do, however, sketch a couple of its basic properties.

The quantum adiabatic evolution method has been successfully applied to the searching problem [69, 70, 166]. Let the initial state be $|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{x=1}^{N} |x\rangle$, N being the number of entries

of the database, and let the initial and problem Hamiltonian respectively be $H_0 = I - |\psi\rangle\langle\psi|$ and $H_P = I - |x_0\rangle\langle x_0|$, $|x_0\rangle$ being the marked state. The interpolating Hamiltonian $H(s(t)) = (1 - s(t))H_0 + s(t)H_P$ depends on a time-dependent parameter $s(t)$ satisfying the boundary conditions $s(0) = 0$ and $s(T) = 1$, T being the computational time of the adiabatic algorithm. This scheme leads to different results depending on whether we apply the adiabatic condition globally (that is, in the whole time interval $[0, T]$) or locally (at each time t). In what follows, we consider these two situations without entering into precise details of the involved calculations. For further information, we refer the reader to [69, 70] and references therein.

6.3.1 Numerical results

We have performed a numerical analysis of the way in which majorization appears in the quantum adiabatic searching algorithm. Our study can be divided into two parts, regarding whether we demand the adiabatic condition to be fulfilled either globally or locally along the evolution.

Analysis of the fastest global adiabatic evolution

Let us suppose that we demand the usual adiabatic condition given in Eq.4.15 of Chapter 4 to be satisfied globally in the whole interval $[0, T]$. This does not involve any particular restriction on the t-dependence of $s(t)$, so we can choose $s(t) = t/T$, leading to a linear evolution of the Hamiltonian. Under these circumstances, it can be proven [69, 70] that the global adiabatic condition is verified provided that

$$T \geq \frac{N}{\epsilon}\,, \tag{6.42}$$

ϵ being the probability amplitude of not being at the ground-state of H_P at time T. Hence, this quantum algorithm needs a computational time of $O(N)$ to hit the right solution with high probability, so the global adiabatic searching does not lead to an increasing efficiency with respect to a classical searching.

In what follows we call $P_+(t)$ the probability of being at the marked state at time t and similarly $P_-(t)$ the probability of being at one of the remaining $N - 1$ basis states different from the desired one at time t. Notice that, given the symmetry of the problem, $P_-(t)$ will exactly be the same for all those basis states different from the marked one all along the evolution. In order to analyze majorization, we recall the set of inequalities given in Eq.A.3 of Appendix A to be satisfied at each majorizing time step. Let us make the observation that the maximum probability at all times is indeed $P_+(t)$, while the other probabilities will remain smaller than this quantity all along the computation and equal to $P_-(t)$. It is possible to see that the whole set of N cumulants that arise from the probability distribution follows the same basic behavior as time flows. Because of that, we present here the behavior of the first two non-trivial cumulants $P_+(t)$ and $P_+(t) + P_-(t)$, as the rest of them do not lead to different conclusions.

We have performed exact numerical simulations of the quantum algorithm in the fastest allowed case saturating the bound from Eq.6.42 ($T = \frac{N}{\epsilon}$) and have found the time evolution for the two cumulants. The results for $\epsilon = 0.2$ and $N = 32$ are shown in Fig.6.4. From our numerical analysis we conclude that a naive adiabatic quantum searching process does not produce an optimal algorithm neither verifies step-by-step majorization. This property is observed as the

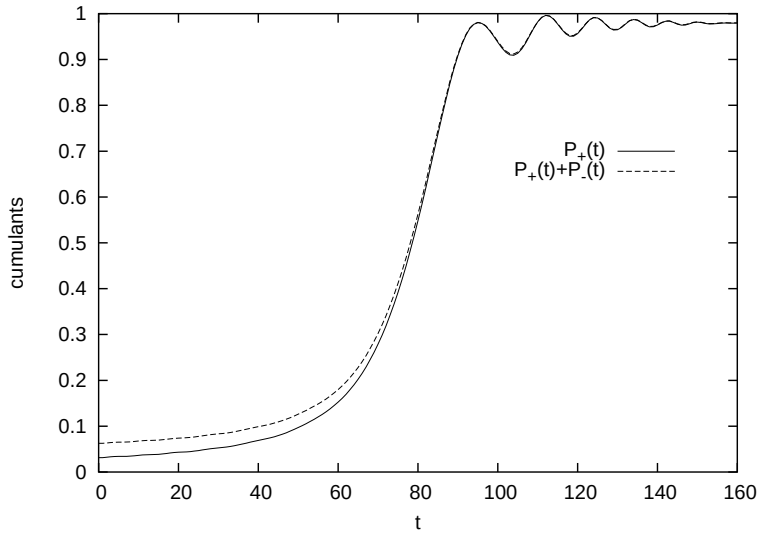

Figure 6.4: Quantum searching using global adiabatic evolution with parameters $\epsilon = 0.2$, $N = 32$ and $T = 160$.

two cumulants decrease in time for some time steps, since there are wiggles which indicate that the system is evolving too fast to remain close enough to the ground state, and thus not verifying step-by-step majorization along the flow in time.

Analysis of the local adiabatic evolution

The preceding global adiabatic method can be improved if we apply the adiabatic condition given in Eq.4.15 of Chapter 4 locally. That is, let us divide the interval $[0, T]$ into many small subintervals and let us apply Eq.4.15 to each one of these subintervals individually. Taking the limit of the size of the subintervals going to zero, we find that the adiabatic restriction has to be fulfilled locally at each time t:

$$\frac{|\frac{dH_{1,0}}{dt}|}{g^2(t)} \leq \epsilon \qquad \forall t \,, \tag{6.43}$$

where $H_{1,0}$ is the Hamiltonian matrix element between the ground state and the first excited state and $g(t)$ is the energy gap between these two states, everything given at t. This is a less demanding condition than Eq.4.15, and means that the adiabaticity condition must be satisfied at each infinitesimal time interval. It can be shown (see, for example, [69]) that proceeding in this way the function $s(t)$ must have a precise form which is given by the relation

$$t = \frac{1}{2\epsilon}\frac{N}{\sqrt{N-1}}\left(\arctan(\sqrt{N-1}(2s-1)) + \arctan(\sqrt{N-1})\right) . \tag{6.44}$$

We can observe this dependence in Fig.6.5, in the case of $\epsilon = 0.2$ and $N = 32$. The local adiabatic process implies that the smaller the energy gap between the ground and first excited

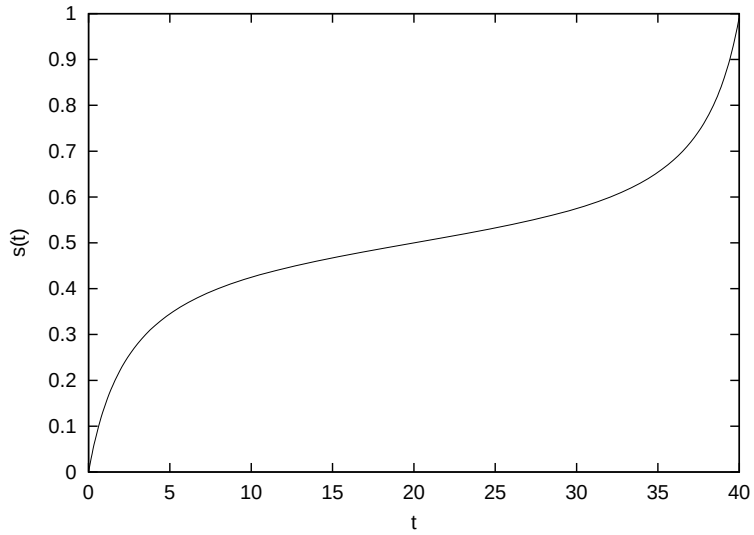

Figure 6.5: Interpolating parameter $s(t)$ for quantum searching using local adiabatic evolution.

states is, the slower the rate at which the Hamiltonian changes. With this information it can be proven [69, 70] that the evolution time for the algorithm to succeed with sufficiently high probability is, in the limit $N \gg 1$,

$$T = \frac{\pi}{2\epsilon}\sqrt{N}\,. \tag{6.45}$$

Hence, in the case of local adiabatic evolution the computational process takes $O(\sqrt{N})$ time, just as in Grover's quantum searching algorithm, obtaining an square-root speed-up with respect to the best classical searching.

Defining $P_+(t)$ and $P_-(t)$ as before, we can again restrict ourselves to the study of the two non-trivial cumulants $P_+(t)$ and $P_+(t) + P_-(t)$ in order to observe the evolution of majorization. We have numerically solved the dynamical equations for $\epsilon = 0.2$ and $N = 32$, and have found the evolution of the two quantities, which is given in Fig.6.6. From the numerical analysis, it follows that a local adiabatic searching algorithm is not only optimal in time, but also verifies step-by-step majorization.

Analysis of slower global adiabatic evolutions

Let us now consider global adiabatic evolutions which are not necessarily tight in time, that is, extremely slow time variations of the Hamiltonian, much slower than the minimum necessary for the adiabatic theorem to hold. In the case we are dealing with, this implies the consideration of the case in which $T > \frac{N}{\epsilon}$, that is, the adiabatic inequality from Eq.6.42 is not saturated.

We have again performed a numerical analysis for the time evolution of the two non-trivial cumulants $P_+(t)$ and $P_+(t) + P_-(t)$, for $\epsilon = 0.2$, $N = 32$, and $T = 320$ and 480 (both cases bigger than $\frac{N}{\epsilon} = 160$). The results are plotted in Fig.6.7 and Fig.6.8. From these two plots, we observe that a step-by-step majorization tends to appear as long as the evolution of the Hamiltonian becomes slower and slower. From a physical point of view, this means that the

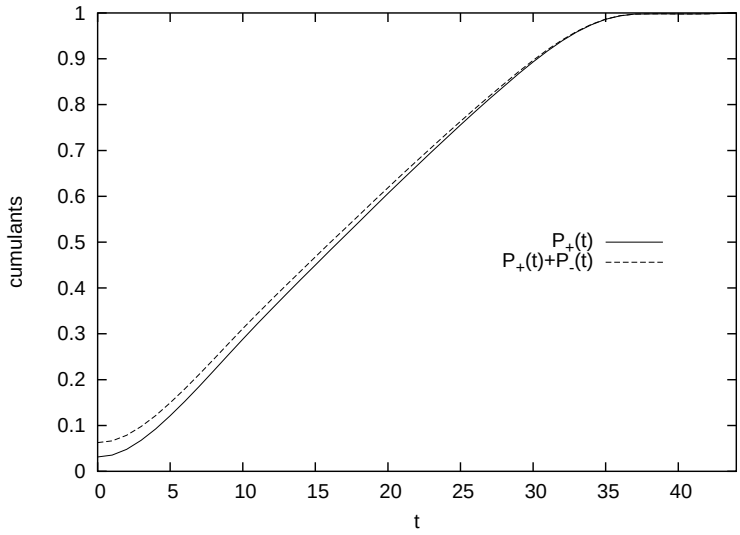

Figure 6.6: Quantum searching using local adiabatic evolution with parameters $\epsilon = 0.2$, $N = 32$ and $T = 44$.

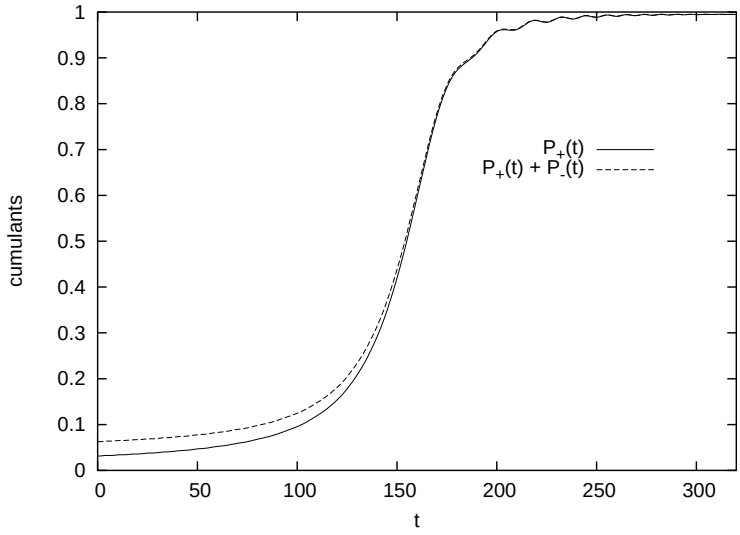

Figure 6.7: Quantum searching using global adiabatic evolution with parameters $\epsilon = 0.2$, $N = 32$, and $T = 320$.

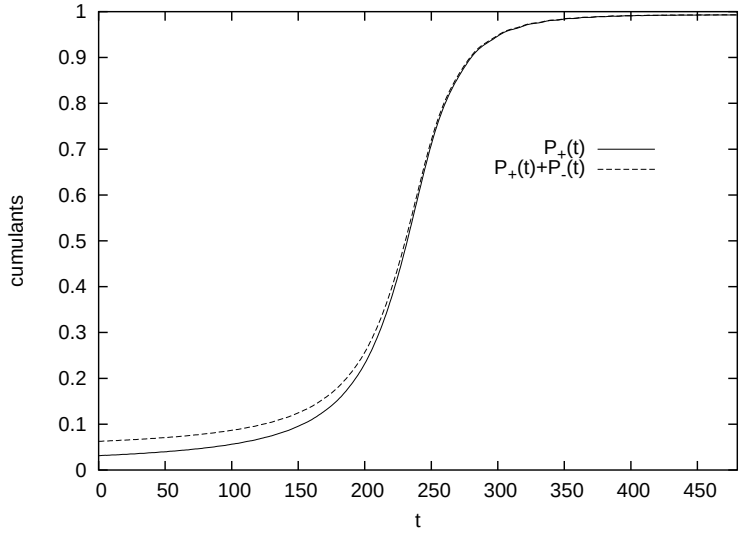

Figure 6.8: Quantum searching using global adiabatic evolution with parameters $\epsilon = 0.2$, $N = 32$, and $T = 480$.

probability of "jumping" to the first excited state decreases as long as the evolution is performed at slower changing rates, thus satisfying better the assumptions of the adiabatic theorem. Step-by-step majorization may thus appear in global adiabatic searching processes for a slow enough evolution rate.

6.4 Majorization in a quantum walk algorithm with exponential speed-up

The extension of classical random walks to the quantum world has been widely studied, yielding two different models of quantum random walks, namely, those which operate in discrete time by means of a "coin operator" [186–188] and those based on a Hamiltonian evolution in continuous time [179, 189, 190]. Regarding the discrete-time model of quantum random walk, two indicative algorithmic results have been found, namely, an exponentially fast time when crossing the hypercube with respect to the classical random walk [191] and a quantum searching algorithm achieving Grover's quadratic speed-up [180]. As a matter of fact, the first one of these two results does not provide any algorithmic speed-up, as there exists a classical algorithm that solves the hitting problem in the hypercube exponentially faster than the naive classical random walk, that is, in a time $O(\text{poly}(\log_2 N))$ where N is the number of nodes of the graph (see [191, 192]). Nevertheless, the second of these examples shows algorithmic advantage with respect to any possible classical strategy. The analysis of the quantum random walk searching algorithm shows that the quantum evolution can be understood as an (approximate) rotation of the quantum state in a two-dimensional Hilbert space which is exact in the limit of a very large database (see [180] for details), resembling the original proposal of Grover's searching algorithm which can be decomposed exactly in a two-dimensional Hilbert space (see Eq.6.32). This

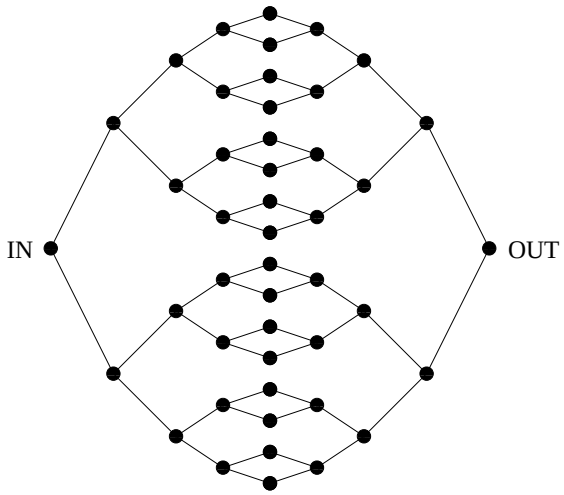

Figure 6.9: A possible graph constructed from two binary trees with $n = 4$.

rotational structure of the evolution implies again step-by-step majorization when approaching the marked state, exactly in the same way as the usual Grover's searching algorithm [9, 152].

Here we wish to restrict ourselves to the continuous-time model of quantum walk and analyze a proposed quantum algorithm based on a quantum walk on continuous time solving a classically hard problem [179]. We sketch the main ingredients of the problem setting and its efficient solution in terms of a quantum evolution (the interested reader is addressed to [179] for specific details). For a more generic review on quantum walks both in discrete and continuous time, see [192].

6.4.1 The exponentially fast quantum walk algorithm

The problem we wish to solve is defined by means of a graph built in the following way (see [179]): suppose we are given two balanced binary trees of height n with the 2^n leaves of the left tree identified with the 2^n leaves of the right tree in a simple way, as shown in Fig.6.9. A way of modifying such a graph is to connect the leaves by a random cycle that alternates between the leaves of the two trees, instead of identifying them directly. An example of such a graph is shown in Fig.6.10.

Suppose that the edges of such a graph are assigned a consistent coloring (that is, not two edges incident in the same vertex have the same color), and that the vertices are each one given a different name (with a $2n$-bit string, so there are more possible names than the ones assigned). We now define a black-box that takes two inputs, a name a given as a $2n$-bit string and a color c, and acts in the following way: if the input name a corresponds to a vertex that is incident with an edge of color c, then the output corresponds to the name of the vertex joined by that edge; if a is not the name of a vertex or a is the name of a vertex but there is no incident edge of color c, the output is the special $2n$-bit string $(1, 1, \ldots, 1)$, which is not the name of any vertex.

Now, the problem we wish to solve reads as follows: given a black-box for a graph such as the one previously described, and given the name of the IN vertex, find out the name of the

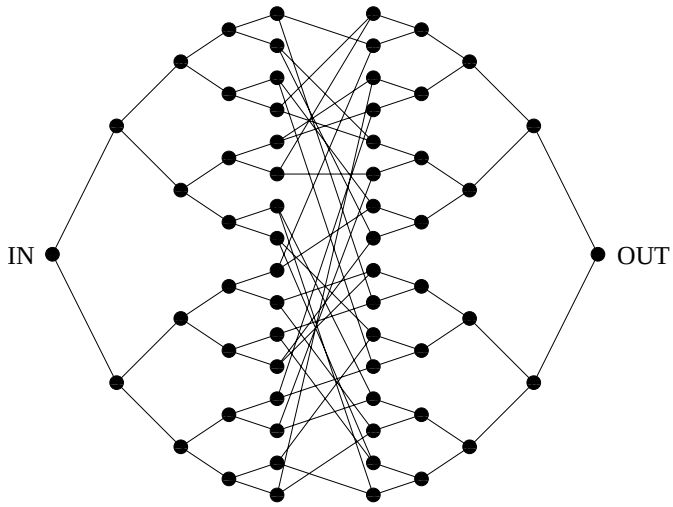

Figure 6.10: An alternative graph constructed from two binary trees with $n = 4$. Connection between the leaves is made through a random cycle.

OUT vertex.

In [179] it was proven that no classical algorithm can transverse a graph such as the one in Fig.6.10 in polynomial time, given such a black-box. Furthermore, an explicit construction of a quantum algorithm based on a continuous-time quantum walk on the graph that succeeds in finding the solution for this oracular problem in polynomial time was given. The quantum algorithm of [179] for this problem can be briefly summarized as follows: consider the $(2n+2)$-dimensional subspace spanned by the states

$$|\text{col } j\rangle = \frac{1}{\sqrt{N_j}} \sum_{a \,\in\, \text{column } j} |a\rangle \,, \tag{6.46}$$

where $N_j = 2^j$ if $0 \leq j \leq n$ and $N_j = 2^{2n+1-j}$ if $n+1 \leq j \leq 2n+1$. We call this subspace the "column subspace", and each state of the basis is an equally weighted sum of the states corresponding to the vertices lying on each column of the graph. We now define a Hamiltonian acting on this subspace by the following non-zero matrix elements:

$$\langle \text{col } (j+1)|H|\text{col } j\rangle = \langle \text{col } j|H|\text{col } (j+1)\rangle = \begin{cases} 1 \,, & \text{if } 0 \leq j \leq n-1 \,,\ n+1 \leq j \leq 2n \\ 2^{1/2} \,, & \text{if } j = n \,. \end{cases} \tag{6.47}$$

The action of this Hamiltonian on the graph is nothing but promoting transitions between adjoint vertices, so a quantum walk on the graph (on the whole Hilbert space) generated by this Hamiltonian is equivalent to a quantum walk on the line (on the column subspace). Because of that, from now on we only focus our attention on the quantum walk on the line generated by the Hamiltonian from Eq.6.47. Moreover, it can be proven that given the structure of the graph in the form of a black-box such as the one already described, our Hamiltonian can be efficiently simulated by means of a quantum circuit [179].

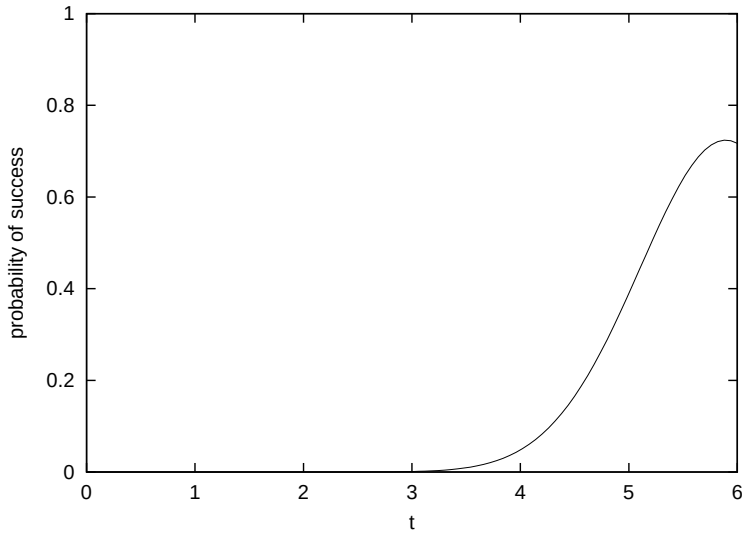

Figure 6.11: Probability of finding the OUT node in the quantum walk algorithm, for $n = 4$.

The quantum walk works as follows: at first the "wave packet" will be precisely localized at the IN vertex (the initial state will be $|\text{col } 0\rangle$). Due to the unitary time evolution driven by the Hamiltonian, it will initially spread out through the different vertices at the left hand side of the graph (those belonging to the left binary tree), but after a short time (once half the graph has been transversed) it will begin to spread through the vertices on the right hand side, interfering constructively in the OUT vertex as the time goes on. Physically, this is nothing but a wave propagation. Should we wait longer, the wave packet would come back to be localized at IN vertex and the process would similarly be repeated again. Actually, due to the "defect" of the Hamiltonian in the central vertices, it can be shown that the transmission through the central columns is not perfect, but high enough for the OUT node to be achieved with a very high probability in small computational time. In [179] the authors prove that the succeeding time is polynomial in n.

6.4.2 Numerical results

We have numerically simulated this quantum walk for the particular case of $n = 4$, and have plotted the time evolution of the probability of success in Fig.6.11. We observe that the numerical result is in agreement with the prediction that the time the algorithm takes in hitting the OUT node with high probability seems to be, at first sight, linear with the size of the system.

In order to analyze majorization, for the case $n = 4$ there are 62 cumulants that can be computed from a set of 10 non-trivial probabilities. This is so due to the fact that all the states of the whole Hilbert space belonging to the same column always share the same probability amplitude. The quantities to be considered are then the probabilities of being at each column state normalized by the number of nodes belonging to that column, that is, the probability of being in one node of each column. In general, there are then $2n + 2$ different probabilities to be considered at each time step. Given only these 10 quantities, we were able to compute all of the

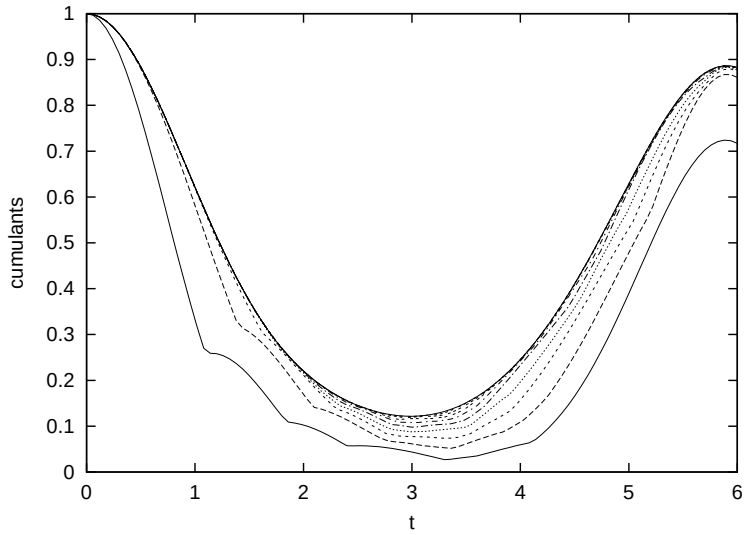

Figure 6.12: Time evolution of the ten cumulants in the quantum walk algorithm when one node per column is considered, for $n = 4$. The evolution follows a majorization cycle

62 cumulants corresponding to all the partial sums of sorted probabilities, according to Eq.A.3 in Appendix A. In order to make the figures as clear as possible we have only plotted 10 of these quantities in Fig.6.12, which correspond to the cumulants arising from the sorted probabilities when only one node per column is considered. Our numerical simulations indicate that the rest of the cumulants exhibit a behavior similar to that of the ones appearing in Fig.6.12 and thus bring no further insight. We have also numerically simulated the algorithm in the case of a bigger graph, namely, in the case $n = 10$. In this case there are $2n+2 = 22$ different probabilities to be considered at each time step. Proceeding in the same way than in the case $n = 4$ (that is, not plotting all the cumulants, but the only the sorted sum of these 22 probabilities), we obtain a similar behavior as in the case for $n = 4$, as is shown in Fig.6.13.

Looking at the two plots, we conclude that the continuous time quantum walk follows a step-by-step majorization cycle all along the computation until it reaches the OUT node. It is worth remarking as well that the time the algorithm spends reversely majorizing the probability distribution is about half of the time of the whole computation. The physical reason for this behavior is clear, as this is the time the "wave packet" spends spreading over the binary tree on the left hand side, thus leading to a destructive interference part. Note that such a destructive interference indeed strictly follows a step-by-step reverse majorization of probabilities. Furthermore, by combining Fig.6.11 and Fig.6.12 we see that the raising of the probability of success is linked to a step-by-step majorization. Physically, this is the part in which the algorithm constructively interferes into the OUT node once the wave packet is approximately in the right-hand-side binary tree. We see that this constructive interference follows a majorization arrow. Actually, the observed majorization cycle is very similar to the one that we already found in the quantum phase-estimation algorithm, but in this case we have numerically checked that the present cycle does not seem to follow the rules of natural majorization. Complementarily,

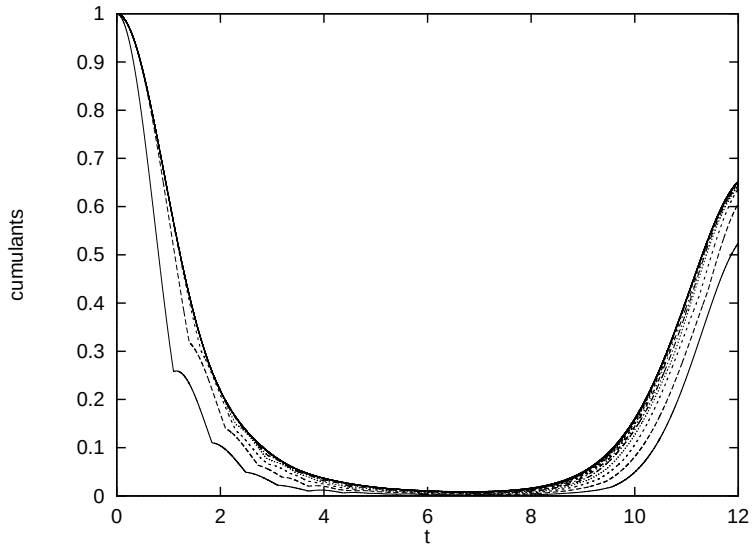

Figure 6.13: Time evolution of the 22 cumulants in the quantum walk algorithm when one node per column is considered, for $n = 10$. The cumulants tend to collapse in the plot given the size of the graph. The evolution follows a majorization cycle.

we have also observed that the probability amplitudes follow the rule that those belonging to even columns are real, while those belonging to odd columns are imaginary.

The quantum random walk heavily exploits the column structure of the problem. The register works on a superposition of columns, that is of states belonging to the same column with equal weight. It is then natural to ask whether a step-by-step majorization cycle operates also at the level of columns. The idea behind this analysis corresponds to accept that the final measurement will filter each one of the columns as a whole. The result of the measurement would correspond to determining a particular column. The point here is to find to what extent the success of finding the OUT state is related to the column structure of the algorithm. We have numerically considered the column amplitudes for $n = 4$ and $n = 10$ with a total of 9 and 21 cumulants to be calculated respectively from the sorted probabilities at each time step of being *at each column* of the graph. In Fig.6.14 and Fig.6.15 we plot our results, which show that there does not exist a majorization cycle when the final measurement is carried on columns. The conclusion is that deterministic quantum walks cleverly exploit the column subspace structure of the problem to achieve step-by-step majorization on the individual states, but not on the individual columns.

6.5 Conclusions of Chapter 6

We have seen in this Chapter that majorization seems to appear in the fauna of quantum algorithms in a very specific way, namely, in such a way that some instances of efficient quantum algorithms seem to step-by-step majorize the probability distribution of the final outcomes all along the flow in time. In order to be precise:

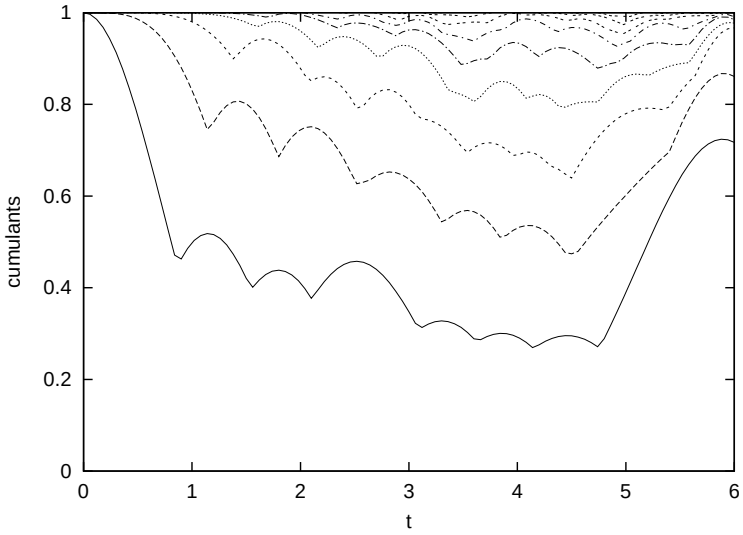

Figure 6.14: Time evolution of the nine cumulants in the quantum walk algorithm when the column-measurement is considered, for $n = 4$. No majorization cycle is present.

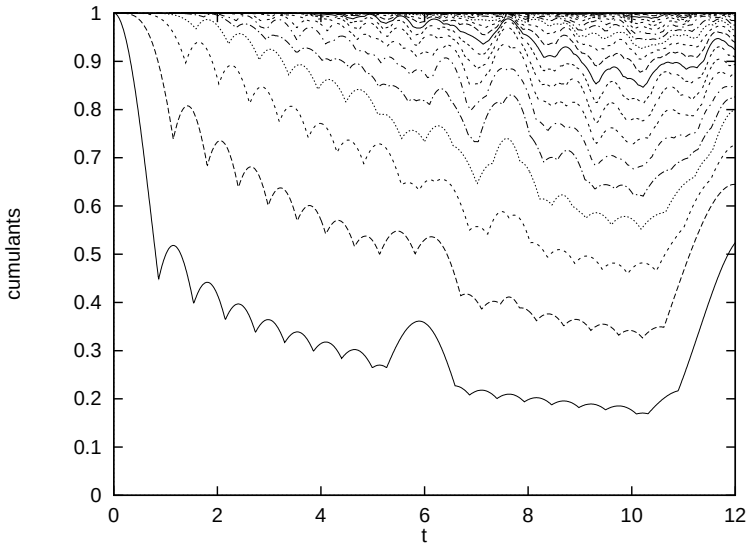

Figure 6.15: Time evolution of the 21 cumulants in the quantum walk algorithm when the column measurement is considered, for $n = 10$. No majorization cycle is present.

- We have proven that the quantum Fourier transform in quantum phase-estimation algorithms majorizes step-by-step the probability distribution of the final outcomes. This step-by-step majorization is seen to appear in a natural way from the absence of some interference terms in the unitary evolution, in contrast with what is found for Grover's quantum searching algorithm. The example of a quantum algorithm solving a hidden affine function problem also shows the same basic features than the quantum-phase estimation algorithm, which can be understood in terms of a majorization cycle along the complete time-evolution. However, Shor's quantum factoring algorithm, though being based on a variant of the quantum phase-estimation algorithm, does not globally obey step-by-step majorization on the whole set of relevant probabilities.

- We have seen that step-by-step majorization in adiabatic quantum searching algorithms is heavily attached to the optimality of the interpolating path. Those paths which do not produce an optimal quantum search are seen to step-by-step majorize the probability of the final outcomes only if the change rate of the Hamiltonian is extremely slow. On the contrary, the optimal path producing a square-root speed-up directly obeys step-by-step majorization.

- We have observed that there is a majorization cycle of the probabilities of the final outcomes in an exponentially fast quantum walk algorithm solving a classically hard problem defined in terms of a non-trivial graph. This majorization cycle does not appear if alternative collective measurements are considered.

Our conclusion is that some broad families of quantum algorithms seem to have an underlying majorization structure in the way they proceed in order to get the desired solution to the problem that they deal with. This behavior is somehow similar to the one of greedy algorithms in classical computation, which always evolve such that the probability of the "winner" increases at each time step. Majorization is, though, a far more severe condition, since it not only involves constraints on one single and specific probability, but on the complete probability distribution. In some sense, majorization seems to be a plausible candidate to look at in order to have a good understanding of the performance of a quantum algorithm, together with entanglement. How these two quantities behave along the computational evolution of a given quantum algorithm may already provide a lot of information about its performance.

Chapter 7

General conclusions and outlook

The work presented in this thesis tries to bring together different fields of physics. We used tools from quantum information science to analyze problems in quantum field theory and condensed-matter physics in Chapters 1 and 3. Conformal field theory can in turn be useful to analyze problems in quantum information science, as we saw in Chapters 1 and 2. Moreover, quantum phase transitions and quantum algorithms are seen to be very much related, as we have seen in Chapters 4 and 5. Furthermore, ideas related to the performance of some quantum algorithms were shown in Chapter 6 by using majorization theory. All in all, we have seen that the fields of quantum information science, condensed-matter physics, and quantum field theory have very much in common, and that their multidisciplinary intersection is useful.

Let us consider several future directions. First, the use of majorization theory and conformal field theory together with related techniques applied to a comprehension of both the irreversibility of renormalization group flows and the behavior of the single-copy entanglement in more than $(1 + 1)$ dimensions is something that remains to be done. Also, it is still a theoretical challenge to know whether adiabatic quantum algorithms can solve NP-complete problems in polynomial time or not, which in the end amounts to ask about the possibilities of quantum computation to solve the celebrated P$\neq$NP conjecture. Further analysis of adiabatic quantum algorithms could be done, for instance, by means of a parallelization of the local truncation scheme that we used in Chapter 5, or by means of non-local truncation schemes, adapted valence-bond ansatzs for the ground state wavefunction, or other related techniques. Indeed, classical numerical simulations using the ideas from Chapter 5 of some other quantum algorithms, like Shor's factoring quantum algorithm, could bring further insight both for the quantum algorithm and for the classical simulation technique itself. The big problem in quantum computation remains to be, yet, the design of new, useful and efficient quantum algorithms. Furthermore, from the many-body physics point of view, the challenge now is to perform reliable and accurate classical simulations of the properties of $(2 + 1)$-dimensional quantum many-body systems, for which new numerical techniques are beginning to be discovered. However, the tools developed so far do not apply to the study of critical fermionic systems in more than one spatial dimension, since some of these systems break the entropic area-law scaling [109–111]. A better understanding of these models, both from a theoretical and numerical point of view, together with a plausible numerical ansatz for their ground state wave function, remains as an open problem.

Appendix A

Majorization

Majorization theory deals with the notion of relative order of probability distributions. It was originally introduced within the fields of mathematical statistics and economics [11–14], and its basic idea relies on the comparison of two given probability distributions by means of a set of order relations to be satisfied by their components.

We now precisely define the notion of majorization [14]. Let $\vec{x}, \vec{y} \in \mathbb{R}^{+N}$ be two normalized probability vectors, $\sum_{i=1}^{N} x_i = \sum_{i=1}^{N} y_i = 1$. We say that distribution $\vec{y}$ majorizes distribution $\vec{x}$, written $\vec{x} \prec \vec{y}$, if and only if there exist a set of permutation matrices P_k and probabilities $p_k \geq 0$, $\sum_k p_k = 1$, such that

$$\vec{x} = \sum_k p_k P_k \vec{y} \,. \tag{A.1}$$

Since, from the previous definition, $\vec{x}$ can be obtained by means of a probabilistic combination of permutations of $\vec{y}$, we get the intuitive notion that probability distribution $\vec{x}$ is more disordered than probability distribution $\vec{y}$. This defines a partial order in the space of probability distributions.

There are two alternative equivalent definitions of majorization which turn out to be useful. The first one reads as follows. We say that a given $N \times N$ matrix D is doubly stochastic if it has non-negative entries and each row and column adds up to 1. Then, $\vec{y}$ majorizes $\vec{x}$ if and only if there is a doubly stochastic matrix D such that

$$\vec{x} = D\vec{y} \,. \tag{A.2}$$

Notice that in Eq.A.1, $\sum_k p_k P_k \equiv D$ defines a doubly stochastic matrix, that is, D has nonnegative entries and each row and column adds up to unity, thus satisfying Eq.A.2.

The third equivalent definition of majorization can be stated in terms of a set of inequalities between partial sums of the two distributions. Consider the components of the two probability vectors sorted in decreasing order. Then, $\vec{x} \prec \vec{y}$ if and only if

$$\sum_{i=1}^{k} x_i \leq \sum_{i=1}^{k} y_i \qquad k = 1, 2, \ldots, N-1 \,. \tag{A.3}$$

All along this thesis, we refer to these partial sums of sorted probabilities as *cumulants*.

A powerful relation between majorization and any convex function f over the set of probability vectors states that

$$\vec{x} \prec \vec{y} \Rightarrow f(\vec{x}) \leq f(\vec{y}) \ . \tag{A.4}$$

From this relation it follows that the Shannon entropy $H(\vec{z}) \equiv -\sum_{i=1}^{N} z_i \log_2 z_i$ of a probability distribution $\vec{z} \in \mathbb{R}^N$ satisfies $H(\vec{x}) \geq H(\vec{y})$ whenever $\vec{x} \prec \vec{y}$. Majorization is, therefore, a stronger notion of order for probability distributions that the one imposed by the entropy $H(\vec{z})$.

The connection between majorization and quantum mechanics can be established whenever a probability distribution appears. For instance, one could be interested in the majorization properties of the probability distribution arising from the spectrum of some given reduced density matrix, as happens often in the field of quantum information science. For two reduced density operators ρ and σ with spectrums $\vec{\rho}$ and $\vec{\sigma}$, we say that $\rho \prec \sigma$ if and only if $\vec{\rho} \prec \vec{\sigma}$. This extends the notion of majorization to positive semi-definite operators by considering their normalized spectrum.

Appendix B

Some notions about conformal field theory

The aim of this Appendix is to give a brief, non-technical and non-exhaustive idea about some of the basic concepts of conformal field theory. The interested reader is referred to the specific literature in the field for further details and developments (see for example [21] and references therein).

Consider a metric $g_{\mu\nu}(x)$ of signature (p, q) in a space of total dimension D, where x stands for a given point of this space in some given coordinate system. Under a change of coordinates $x \to x'$, the metric transforms as $g'_{\mu\nu}(x') = \frac{\partial x^\alpha}{\partial x'^\mu}\frac{\partial x^\beta}{\partial x'^\nu} g_{\alpha\beta}(x)$, where sums are to be understood on repeated indices from now on. The conformal group in D dimensions is, by definition, the subgroup of coordinate transformations that leave the metric invariant up to a local change of scale,

$$g_{\mu\nu}(x) \to g'_{\mu\nu}(x') = \Omega(x) g_{\mu\nu}(x) \,, \tag{B.1}$$

where $\Omega(x)$ is a local dilatation factor. It is possible to exactly characterize the form of these transformations, which are given by the Poincaré group

$$\begin{aligned} x &\to x' = x + a \\ x &\to x' = \Lambda x \qquad (\Lambda \in \mathrm{SO}(p, q)) \end{aligned} \tag{B.2}$$

with $\Omega(x) = 1$, the dilatations

$$x \to x' = \lambda x \tag{B.3}$$

with $\Omega = \lambda^{-2}$, and the so-called special conformal transformations

$$x \to x' = \frac{x + bx^2}{1 + 2b \cdot x + b^2 x^2} \tag{B.4}$$

with $\Omega(x) = (1 + 2b \cdot x + b^2 x^2)^2$. Conformal symmetry can then be understood as some generalization of scale symmetry. Those field theories defined in the continuum that are invariant under conformal transformations constitute the so-called *conformal field theories*.

Conformal symmetry is especially powerful in the case of 2 dimensions, typically denoted as $(1 + 1)$, in the case of having one temporal and one spatial dimension. Given the coordinates

of the plane x^1 and x^2, and defining new complex coordinates $z = x^1 + ix^2$ and $\bar{z} = x^1 - ix^2$ (respectively called holomorphic and antiholomorphic coordinates), conformal transformations in 2 dimensions coincide with the set of analytic coordinate transformations in the plane

$$\begin{aligned} z &\rightarrow f(z) \\ \bar{z} &\rightarrow \bar{f}(\bar{z}) \,, \end{aligned} \tag{B.5}$$

f and $\bar{f}$ being analytic complex functions. Typically, it is useful to work with z and $\bar{z}$ treated as independent variables, so that the physical condition $\bar{z} = z^*$ is left to be imposed at our convenience. The fact that conformal transformations in the plane precisely coincide with the group of analytic coordinate transformations is very notorious, since the number of generators of the conformal group in 2 dimensions is then *infinite*, which only happens for this number of dimensions. The behavior of conformally-invariant field theories in 2 dimensions is, then, heavily constrained by the symmetry.

In order to be more specific, assume that we are given a conformally-invariant quantum field theory in $D = 2$. Those operator fields $\Phi(z, \bar{z})$ that transform under conformal transformations like

$$\Phi(z, \bar{z}) \rightarrow \left(\frac{\partial f}{\partial z}\right)^h \left(\frac{\partial \bar{f}}{\partial \bar{z}}\right)^{\bar{h}} \Phi(f(z), \bar{f}(\bar{z})) \,, \tag{B.6}$$

with positive real h and $\bar{h}$, are called primary fields of conformal weight $(h, \bar{h})$. Conformal symmetry imposes that the two-point correlation function of two primary fields $\langle \Phi_1(z_1, \bar{z}_1) \Phi_2(z_2, \bar{z}_2) \rangle$ must be

$$\langle \Phi_1(z_1, \bar{z}_1) \Phi_2(z_2, \bar{z}_2) \rangle = \frac{1}{z_{12}^{2h} \bar{z}_{12}^{2\bar{h}}} \tag{B.7}$$

if $(h_1, \bar{h}_1) = (h_2, \bar{h}_2)$ and zero otherwise, where $z_{12} = z_1 - z_2$, $\bar{z}_{12} = \bar{z}_1 - \bar{z}_2$. Note that the decay of the correlation function in Eq.B.7 is algebraic, as is the typical situation of critical condensed-matter systems. This is not strange, since many critical quantum many-body systems can be understood at criticality as the regularization on a lattice of some given conformal field theory, as is the case, for example, of the critical Ising quantum spin chain [21, 22]. Indeed, conformal symmetry imposes similar decaying laws for the two-point correlators in any number of dimensions.

An important quantity which is to play a role is the *stress-energy tensor* $T_{\mu\nu}(x)$, which can be always defined for any field theory. For instance, for a free-bosonic quantum field theory defined in terms of a Lagrangian $\mathcal{L}$, the stress-energy tensor reads

$$T_{\mu\nu}(x) = \frac{\partial \mathcal{L}}{\partial(\partial^\mu \phi)} \partial_\nu \phi - \mathcal{L} g_{\mu\nu} \,, \tag{B.8}$$

where ϕ stands for the quantum field of the free boson. It can be seen that in two dimensions, the stress-energy tensor of a conformally-invariant quantum field theory has only two non-vanishing components, which are called $T(z)$ and $\bar{T}(\bar{z})$. An important property of a primary field $\Phi(w, \bar{w})$

is that its operator product expansion with the stress-energy tensor reads

$$\begin{aligned} T(z)\Phi(w,\bar{w}) &= \frac{h}{(z-w)^2}\Phi(w,\bar{w}) + \frac{1}{(z-w)}\partial_w\Phi(w,\bar{w}) + \cdots \\ \bar{T}(\bar{z})\Phi(w,\bar{w}) &= \frac{\bar{h}}{(\bar{z}-\bar{w})^2}\Phi(w,\bar{w}) + \frac{1}{(\bar{z}-\bar{w})}\partial_{\bar{w}}\Phi(w,\bar{w}) + \cdots , \end{aligned} \tag{B.9}$$

which can be understood as an alternative definition of a primary field of conformal weight $(h,\bar{h})$.

The stress-energy tensor is an example of a quantum field that is not primary. Computing its operator product expansion with itself, one gets

$$\begin{aligned} T(z)T(w) &= \frac{c/2}{(z-w)^4} + \frac{2}{(z-w)^2}T(w) + \frac{1}{(z-w)}\partial_w T(w) \\ \bar{T}(\bar{z})\bar{T}(\bar{w}) &= \frac{\bar{c}/2}{(\bar{z}-\bar{w})^4} + \frac{2}{(\bar{z}-\bar{w})^2}\bar{T}(\bar{w}) + \frac{1}{(\bar{z}-\bar{w})}\partial_{\bar{w}}\bar{T}(\bar{w}) , \end{aligned} \tag{B.10}$$

which clearly differs from Eq.B.9. The above equations define the so-called holomorphic and antiholomorphic central charges c and $\bar{c}$, which depend on the particular theory under consideration, much in the same way as the conformal weights $(h,\bar{h})$ do. For example, for a free bosonic quantum field theory $c = \bar{c} = 1$, whereas for a free fermionic quantum field theory $c = \bar{c} = 1/2$. Yet, another property of the stress-energy tensor for conformally-invariant quantum field theories in 2 dimensions is that it is possible to expand it in terms of modes as follows:

$$\begin{aligned} T(z) &= \sum_{n\in\mathbb{Z}} z^{-n-2}L_n \\ \bar{T}(\bar{z}) &= \sum_{n\in\mathbb{Z}} \bar{z}^{-n-2}\bar{L}_n , \end{aligned} \tag{B.11}$$

where the operators L_n and $\bar{L}_n$ satisfy the commutation relations

$$[L_n, L_m] = (n-m)L_{n+m} + \frac{c}{12}(n^3-n)\delta_{n+m,0}$$

$$[\bar{L}_n, \bar{L}_m] = (n-m)\bar{L}_{n+m} + \frac{\bar{c}}{12}(n^3-n)\delta_{n+m,0}$$

$$[L_n, \bar{L}_m] = 0 . \tag{B.12}$$

The above equations define two copies of an algebra which is called the Virasoro algebra. Every conformally-invariant quantum field theory determines a representation of this algebra, with some c and $\bar{c}$.

The construction of the Hilbert space for a conformal field theory in 2 dimensions is very much related to the above operator algebra. Given a vacuum $|\Omega\rangle$ which is assumed to exist by hypothesis, the state

$$|h,\bar{h}\rangle \equiv \Phi(0,0)|\Omega\rangle \tag{B.13}$$

created by a primary field $\Phi(z,\bar{z})$ of conformal weight $(h,\bar{h})$ satisfies

$$\begin{aligned} L_0|h,\bar{h}\rangle &= h|h,\bar{h}\rangle \\ \bar{L}_0|h,\bar{h}\rangle &= \bar{h}|h,\bar{h}\rangle \\ L_n|h,\bar{h}\rangle &= \bar{L}_m|h,\bar{h}\rangle = 0 \ \ \forall n,m>0\ . \end{aligned} \tag{B.14}$$

Any state satisfying the above relations is called a highest-weight state. States of the form

$$L_{-n_1}L_{-n_2}\cdots L_{-n_j}\bar{L}_{-m_1}\bar{L}_{-m_2}\cdots\bar{L}_{-m_k}|h,\bar{h}\rangle \tag{B.15}$$

are called descendant states, and are also eigenstates of L_0 and $\bar{L}_0$ with eigenvalues $h+n_1+n_2+\cdots+n_j$ and $\bar{h}+m_1+m_2+\cdots+m_k$ respectively. The full tower of eigenstates of L_0 and $\bar{L}_0$ constructed in this way is known as the Verma module. Therefore, the Hilbert space of a conformally-invariant quantum field theory in 2 dimensions decomposes as the direct sum of Verma modules, the number of which depends only on the number of primary fields appearing in the theory.

Appendix C

Some notions about classical complexity theory

In this Appendix our aim is to give some very basic notions and non-technical background on classical complexity theory. Excellent textbooks on this topic are those of Garey and Johnson [193] and Papadimitriou [194]. A review on complexity theory, with extensions to quantum complexity theory, is given by Aharonov and Naveh in [151].

Let us begin with the following definition:

Definition C.1: *An alphabet* Σ *is a set of symbols.*

We did not define the concept of *symbol* since we believe its meaning to be clear from the context. Examples of alphabets are $\Sigma_1 \equiv \{a, b, \ldots, z\}$, $\Sigma_2 \equiv \{\alpha, \beta, \ldots, \omega\}$, and $\Sigma_3 \equiv \{0, 1\}$. The alphabet Σ_3, with only two symbols, is usually referred to as the *binary alphabet*.

Definition C.2: *A language* L *over an alphabet* Σ *is a set of strings of symbols from* Σ.

For instance, $L_1 \equiv \{jack, sam, daniel, tealc\}$ is a language over the alphabet Σ_1, and $L_2 \equiv \{010, 00010, 1001\}$ is a language over the binary alphabet Σ_3.

Definition C.3: *A decision problem is a problem for which the answer belongs to a binary alphabet.*

This is the kind of "yes" or "no" problems. That is, questions of the type "will the universe expand forever?", or "do I prefer chocolate or lemon ice-creams?", but also questions like "is the number 1761935875391 the product of two or more primes?". An important part of the theory of computational complexity is built in terms of decision problems. More concretely, one has to decide whether a given string of symbols from an alphabet, called *instance*, belongs to a certain language or not. From now on we shall always restrict ourselves to the binary alphabet, whose symbols are called *bits*.

Languages are classified in terms of *complexity classes*, according to different criteria. We now define a complexity class that plays a major role in complexity theory:

Definition C.4: P *is the class of languages L for which a deterministic Turing machine can decide in a time O*(poly(|*x*|) *if an instance x belongs to L or not,* |*x*| *being the number of bits of x.*

In the above definition, we understand that a *deterministic Turing machine* is our classical model of computation. Usually, it is said that languages $L \in$ P can be *decided* in polynomial time by a deterministic Turing machine. Intuitively, we understand that a language L belongs to the complexity class P if there is an *efficient* classical algorithm that allows to deterministically decide whether a given instance x belongs to L or not, where by the term "efficient" we mean "polynomial in the size of the instance". Let us now define another important complexity class:

Definition C.5: NP *is the class of languages L for which there exists a deterministic polynomial-time verifier V such that*

- $\forall x \in L$*, there is a y such that* $|y| = \text{poly}(|x|)$ *and* $V(x, y) = 1$*, and*
- $\forall x \notin L$ *and* $\forall y$ *such that* $|y| = \text{poly}(|x|)$*,* $V(x, y) = 0$*.*

Usually y is referred to as the *witness* or *certificate*. Both the witness y and the verifier V help in deciding whether the instance x belongs to L or not. Let us clarify Definition C.5 by means of an example: let $L =$ COMPOSITE be the language of numbers that can be decomposed as a product of two or more primes. Let $x = 161$ be an instance of the decision problem "does x belong to COMPOSITE?". A possible witness y can be given by the two prime numbers 7 and 23, and the verifier V can be a classical deterministic algorithm that performs the following check: $7 \times 23 = 161$. Notice then that if the instance 161 belongs to COMPOSITE there is a witness 7, 23 such that the verifier can check that the instance belongs to the language. On the contrary, if we are given an instance that does not belong to COMPOSITE (for instance, $x = 17$), then there is no witness y such that our verifier can check that 17 is a product of two or more primes. In a way, the witness has to be thought of as the "proposal of solution", and the verifier has to be considered as a classical algorithm that allows to deterministically and efficiently check whether the proposed solution to the specific instance is correct or not. This example shows that COMPOSITE $\in NP$, which in less mathematical words is commonly referred to as "the problem of deciding whether a given number is the product of two or more primes is NP".

Given the Definition C.5 of the NP complexity class, we can now define the following:

Definition C.6: NP-hard *is the class of languages L such that the problem of deciding whether an instance* x' *belongs or not to a language* $L' \in NP$ *can be efficiently reduced to the problem of deciding whether an instance x belongs or not to L,* $\forall x'$ *and* $L' \in NP$*.*

In plain words, a problem is said to be NP-hard if *all* the instances of *all* the NP problems can be efficiently mapped to specific instances of the NP-hard problem. Therefore, if a language $L \in$ NP-hard can be decided by some deterministic classical algorithm, the same procedure can essentially be applied to decide all the languages in the complexity class NP, and "solve all the NP problems".

Let us now define the important concept of NP-complete:

Definition C.7: NP-complete *is the class of languages* L *such that* $L \in$ NP-hard *and* $L \in$ NP.

According to Definition C.7, NP-complete languages are those languages in NP such that being able to decide about one of them implies being able to decide about *the whole* complexity class NP. An important example of an NP-complete language is 3-SAT. A possible instance of the 3-SAT decision problem is a boolean formula in conjunctive normal form over n bits $\phi(x_1, x_2, \ldots, x_n) = C_1 \wedge C_2 \wedge \cdots \wedge C_m$, where x_i, $i = 1, 2, \ldots, n$, denotes the value of the bits, and C_j, $j = 1, 2, \ldots, m$, are the so-called *clauses*. Each clause C_j is built in the way $C_j = (\tilde{x}_{j,1} \vee \tilde{x}_{j,2} \vee \tilde{x}_{j,3})$, where $\tilde{x}_{j,\alpha}$ is a *literal* for bit α of clause j, which can be any of the n bit variables or its negation. The decision problem is properly defined by the following question: "given an instance ϕ is there a string of n bits $(y_1, y_2, \ldots, y_n)$ such that $\phi(y_1, y_2, \ldots, y_n) = 1$?", or equivalently, "is there a string of n bits $(y_1, y_2, \ldots, y_n)$ such that all the m clauses are satisfied?".

The proof of the NP-completeness of 3-SAT is one of the most relevant results in the field of complexity theory, and is due to the original work of Cook [72]. That proof opened the door to the discovery of many other NP-complete languages and, today, NP-complete languages (or problems) appear in many different fields of mathematics, physics, and science in general. Their relevance comes in part from the fact that they are at the heart of one of the most celebrated open questions in mathematics, which reads as follows:

Problem C.1: *Is* P $\neq$ NP *?*

To determine the answer to the above question, it would be sufficient to prove that it is possible to deterministically decide some NP-complete language efficiently, and then P = NP, or on the contrary to prove that it is impossible to efficiently and deterministically decide an NP-complete language, and therefore P $\neq$ NP. While the most accepted opinion is that P $\neq$ NP, it has been so far impossible to produce a precise and mathematical proof of this, neither of the opposite statement P = NP. Indeed, Problem C.1 remains today as probably the most challenging open problem in computer science [194].

Let us mention as well that the deterministic complexity classes P, NP, NP-hard and NP-complete can be further generalized if we consider classical probabilistic models of computation, the equivalent *probabilistic* complexity classes being called BPP, MA, MA-hard and MA-complete. Furthermore, if the underlying computational model is a quantum computer, the corresponding generalized *quantum* complexity classes are called BQP, QMA, QMA-hard and QMA-complete. The study of these classes is beyond the scope of this Appendix, and we refer the reader to [151] and references therein for further details on quantum complexity theory and its consequences for quantum computation.

Apéndice D

Resumen en español

D.1 Introducción

Desde las pioneras ideas de Feynman [1] hasta el día de hoy, la información y computación cuánticas han evolucionado de forma veloz. Siendo la mecánica cuántica en sus orígenes considerada esencialmente como un marco teórico en el que poder explicar ciertos procesos fundamentales que acontecían en la Naturaleza, fue durante los años 80 y 90 cuando se empezó a pensar sobre el comportamiento intrínsecamente cuántico del mundo en el que vivimos como una herramienta con la que poder desarrollar tecnologías de la información más potentes, basadas en los mismos principios de la física cuántica. Tal y como Landauer dijo, *la información es física* [3], por lo que no debe en absoluto extrañarnos el que se intentara comulgar la mecánica cuántica con la teoría de la información. Y nada más lejos de la realidad, pues pronto se vio que era posible utilizar las leyes de la física cuántica para realizar tareas inconcebibles desde un punto de vista clásico. Por ejemplo, el descubrimiento de la teleportación [4], la codificación superdensa [5], la criptografía cuántica [6, 7], el algoritmo de factorización de Shor [8] o el algoritmo de búsqueda de Grover [9], constituyen algunos de los logros remarcables que han atraído la atención de mucha gente, dentro y fuera de la ciencia. Queda la información cuántica, pues, constituida como un campo genuinamente pluridisciplinar, en el que se concentran investigadores provenientes de diferentes ramas de la física, las matemáticas y la ingeniería.

Mientras en sus orígenes era la información cuántica quien se beneficiaba del conocimiento de otros campos, a día de hoy las herramientas desarrolladas en el marco de la teoría cuántica de la información pueden ser asimismo usadas en el estudio de problemas de diferentes áreas, como la física de muchos cuerpos o la teoría cuántica de campos. Ello es debido al estudio detallado que la información cuántica desarrolla de las correlaciones cuánticas, o *entrelazamiento* cuántico. Cualquier sistema físico descrito por las leyes de la mecánica cuántica se puede por lo tanto considerar bajo la perspectiva de la teoría cuántica de la información a través de la teoría del entrelazamiento.

Para ser más concretos, concentrémonos aquí en los campos de la información cuántica, la física de la materia condensada, y la teoría cuántica de campos. Pese a que estas tres ramas de la física se pueden considerar en sí mismas como independientes, hay claro solapamiento entre ellas, de forma que el conocimiento en una beneficia al resto. Por ejemplo, la teoría de campos

conforme [21] ha ayudado a entender las diferentes clases de universalidad que aparecen en los sistemas de muchos cuerpos en $(1 + 1)$ dimensiones. El estudio del entrelazamiento que aparece en el estado fundamental de algunos Hamiltonianos cuánticos en una transición de fase cuántica muestra analogías directas con el estudio de entropías en teoría cuántica de campos [31–44]. Tales resultados conectan también con el funcionamiento de técnicas numéricas, como el grupo de renormalización de la matriz densidad [20], el cual permite calcular propiedades básicas de algunos sistemas cuánticos de muchos cuerpos [45–60]. Por otra parte, existe una relación intrínseca entre las transiciones de fase cuánticas y el modelo universal de computación cuántica adiabática [16, 61–71], el cual plantea hoy retos dentro del campo de la teoría de la complejidad [72].

El trabajo que presentamos en esta tesis, y del que tratamos de destilar algunos de los aspectos más importantes en este resumen, se encuentra en la interfase entre la información y computación cuánticas, la teoría cuántica de muchos cuerpos, y la teoría cuántica de campos. Usamos herramientas de estas tres disciplinas para analizar problemas que aparecen en su intersección. Concretamente, en la sección 2 de este resumen consideramos la irreversibilidad del grupo de renormalización desde el punto de vista de la teoría cuántica de la información mediante el uso de la teoría de mayorización y la teoría de campos conforme. En la sección 3 calculamos el entrelazamiento de una copia de un sistema bipartito para una gran variedad de modelos con la ayuda de técnicas de teoría de campos conforme y matrices de Toeplitz. La entropía de entrelazamiento del modelo de Lipkin, Meshkov y Glick se considera en la sección 4, mostrando muchas analogías con la que aparece en sistemas cuánticos en $(1 + 1)$ dimensiones. En la sección 5 aplicamos las ideas de las leyes de escala de las correlaciones cuánticas en las transiciones de fase cuánticas al estudio de los algoritmos cuánticos, en especial el algoritmo de factorización de Shor y los algoritmos cuánticos de evolución adiabática que solucionan un problema NP-completo y el problema de búsqueda en una base de datos desordenada, respectivamente. De igual manera, utilizamos técnicas inspiradas originariamente en la física de la materia condensada para realizar simulaciones clásicas, por medio de estados producto de matriz, de un algoritmo cuántico adiabático en la sección 6. Finalmente, la sección 7 considera el comportamiento de algunas familias de algoritmos cuánticos bajo el punto de vista de la teoría de mayorización, y la sección 8 recoge algunas posibles direcciones futuras a partir de este trabajo.

D.2 Mayorización a lo largo de flujos paramétricos y de renormalización

Desde la introducción del grupo de renormalización por Wilson [18, 19, 73], y dado que el proceso de integración de modos parece ser una operación irreversible en sí misma, es natural el hecho de preguntarse si los flujos del grupo de renormalización son irreversibles. Tal pregunta es en cierta medida equivalente a preguntarse si existe una obstrucción fundamental para recuperar la física microscópica a partir de la macroscópica, o más genéricamente, si existe una pérdida neta de información a lo largo de las trayectorias del grupo de renormalización. Esfuerzos en esta dirección fueron originariamente debidos a Wallace y Zia [74], pero el teorema clave fue posteriormente demostrado por Zamolodchikov [75], dentro del contexto de las teorías de cam-

pos en (1 + 1) dimensiones: para cada teoría de campos unitaria, renormalizable, e invariante Poincaré, existe una función c universal que decrece a lo largo de los flujos de renormalización, siendo únicamente estacionaria en los puntos fijos conformes, donde se reduce a la carga central c de la teoría. Tal resultado establece una flecha en los flujos del grupo de renormalización, dado que implica que una teoría puede ser la realización infrarroja (IR) de otra ultravioleta (UV) sólo si sus respectivas cargas centrales satisfacen la desigualdad $c_{IR} < c_{UV}$.

Se da entonces la siguiente pregunta: ¿bajo qué condiciones se verifica la irreversibilidad del grupo de renormalización en dimensiones mayores? Tal cuestión ha sido analizada desde diferentes puntos de vista [76–94]. Nuestro propósito aquí es más humilde: tratamos de entender la irreversibilidad del grupo de renormalización en (1 + 1) dimensiones desde la perspectiva de la información cuántica, por medio de la teoría de mayorización.

En particular, demostramos el siguiente teorema[a]:

Teorema 1.1: *Dada una teoría física en* $(1+1)$ *dimensiones que depende de un conjunto de parámetros reales* $\vec{g} = (g_1, g_2, \ldots)$*, tal que*

- *hay un punto conforme no trivial* $\vec{g}^*$*, para el que el modelo es invariante conforme y sin fronteras,*
- *las deformaciones desde* $\vec{g}^*$ *en el espacio de parámetros en la dirección positiva de cierto vector unitario* $\hat{e}$ *preservan parte de la estructura conforme del modelo, de tal forma que los autovalores de la matriz densidad del vacío* $\rho(\vec{g})$ *son de la forma*

$$\begin{aligned} \lambda_1 &= \frac{1}{(1 + n_1 q^{\alpha_1} + n_2 q^{\alpha_2} + \cdots)} \\ \lambda_2 &= \frac{q^{\alpha_1}}{(1 + n_1 q^{\alpha_1} + n_2 q^{\alpha_2} + \cdots)} \\ &\vdots \\ \lambda_l &= \frac{q^{\alpha_{(l-1)}}}{(1 + n_1 q^{\alpha_1} + n_2 q^{\alpha_2} + \cdots)} \,, \end{aligned} \tag{D.1}$$

  con degeneraciones n_i*, exponentes* $\alpha_1 > 0 \; \forall i$*, y factores* $q(\vec{g})$ *dependientes de los parámetros, para valores* $\vec{g} = \vec{g}^* + a\hat{e}$*,* $a > 0$*, y*

- *los factores* $q(\vec{g})$ *son funciones monótonas decrecientes en la dirección de* $\hat{e}$*, es decir,*

$$\hat{e} \cdot \left(\vec{\nabla}_{\vec{g}} q(\vec{g}) \right) = \frac{\mathrm{d}q(\vec{g})}{\mathrm{d}a} \leq 0 \tag{D.2}$$

  a lo largo del flujo.

Entonces, fuera del punto conforme hay mayorización continua de los autovalores de la matriz densidad reducida del estado fundamental a lo largo del flujo en los parámetros $\vec{g}$ *en la dirección positiva de* $\hat{e}$*, es decir,*

$$\begin{gathered} \rho(\vec{g}_1) \prec \rho(\vec{g}_2) \,, \\ \vec{g}_1 = \vec{g}^* + a\hat{e}, \; \vec{g}_2 = \vec{g}^* + a'\hat{e}, \; a' \geq a \,. \end{gathered} \tag{D.3}$$

[a]Utilizamos aqui la misma numeración para los teoremas y lemas que se ha usado a lo largo de la tesis

Ejemplos analíticos de situaciones similares a la descrita por el anterior teorema pueden ser obtenidos para las cadenas cuánticas de espín de Heisenberg y XY, para las que algunos flujos paramétricos coinciden con flujos del grupo de renormalización. Un estudio parecido se puede también realizar exclusivamente en el punto conforme para flujos en el tamaño del bloque en consideración. En particular, derivamos relaciones de mayorización analíticas para cualquier teoría conforme en $(1+1)$ dimensiones y sin fronteras en el escenario bipartito cuando el tamaño del subsistema considerado cambia, es decir, bajo deformaciones del tamaño L de la región accesible a una de las partes. Nuestro resultado principal aquí se puede expresar mediante el siguiente teorema:

Teorema 1.2: *$\rho_L \prec \rho_{L'}$ si $L \geq L'$ para todas las posibles teorías conformes en* $(1+1)$ *dimensiones sin fronteras.*

Un ejemplo de situación similar a la descrita por este teorema viene dada por el modelo cuántico de cadena de espín XX. Todos estos resultados proporcionan fundamentos matemáticos sólidos para la existencia de relaciones de mayorización a lo largo de flujos de renormalización para el estado fundamental de teorías definidas en $(1+1)$ dimensiones, en particular muchas cadenas cuánticas de espín.

D.3 Entrelazamiento de una copia en sistemas cuánticos en $(1+1)$ dimensiones

El objetivo de los resultados resumidos en esta sección es el estudiar una medida de entrelazamiento que, como la entropía de entrelazamiento, se puede demostrar que presenta leyes de escala para sistemas cuánticos críticos en $(1+1)$ dimensiones. Llamamos a esta medida *entrelazamiento de una copia* [113,120], y su definición operacional viene esencialmente motivada por razones prácticas: mientras que la entropía mide la cantidad promedio de entrelazamiento que es posible destilar de un sistema bipartito en el límite de tener un número infinito de copias del sistema [121], el entrelazamiento de una copia mide la cantidad de entrelazamiento que existe en el caso más realista de disponer únicamente de *una* única copia del sistema. Dado un sistema bipartito de partes A y B, esta medida viene dada por la expresión

$$E_1(\rho_A) = -\log_2 \lambda_1 = E_1(\rho_B)\,, \tag{D.4}$$

donde ρ_A y ρ_B son las matrices densidad reducidas para A y B, y λ_1 es el máximo autovalor de éstas.

El resultado que demostramos es que, para cualquier teoría de campos conforme en $(1+1)$ dimensiones, el entrelazamiento de una copia del estado fundamental para un subsistema de longitud L está relacionado con la entropía de entrelazamiento mediante la expresión

$$E_1(\rho_L) = \frac{1}{2}S(\rho_L) - \frac{c}{6}\frac{(\pi \log_2 e)^2}{\log_2 L} + O\left(\frac{\log_2 L}{L}\right)\,, \tag{D.5}$$

donde $S(\rho_L)$ es la correspondiente entropía de entrelazamiento. Este resultado se ve reforzado por cálculos analíticos para sistemas fermiónicos cuasi-libres, donde demostramos que siempre que la entropía de entrelazamiento del estado fundamental de un subsistema de longitud L escala logarítmicamente para $L \gg 1$, así lo hace también el entrelazamiento de una copia, con un prefactor que es exactamente *la mitad* del prefactor de la entropía. Ello involucra que la mitad del entrelazamiento cuántico disponible en un numero infinito de copias de un sistema bipartito está ya disponible en el caso de una copia, en el límite $L \gg 1$. Tal relación parece estar íntimamente relacionada con los sistemas críticos en $(1+1)$ dimensiones, pues fuera de la región crítica tal afirmación deja de ser cierta, y el entrelazamiento de una copia deja de ser, asintóticamente, la mitad de la entropía de entrelazamiento, como se puede demostrar para el modelo de cadena cuántica de espín XY.

D.4 Entropía de entrelazamiento en el modelo de Lipkin, Meshkov y Glick

El modelo de Lipkin, Meshkov y Glick [132–134] ha atraído la atención en mayor o menor grado dado que se trata de un modelo que permite un tratamiento numérico muy eficiente, así como cálculos analíticos. Además, proporciona un ejemplo antiintuitivo de la relación existente entre el entrelazamiento y la conectividad de un sistema definido en una red: en un modelo definido en un grafo completamente conectado, el entrelazamiento del estado fundamental del sistema se comporta *como si* éste estuviera definido en $(1+1)$ dimensiones. Ello es consecuencia del papel jugado por las simetrías en la descripción del modelo. En esta tesis, analizamos la entropía de von Neumann calculada para el estado fundamental del modelo de Lipkin, Meshkov y Glick, y mostramos que en las diferentes regiones críticas del sistema ésta escala logarítmicamente con el tamaño del bloque en consideración, con un prefactor que depende del parámetro de anisotropía del modelo.

Más específicamente, el modelo de Lipkin, Meshkov y Glick viene descrito por el Hamiltoniano

$$H = -\frac{\lambda}{N}\sum_{i<j}\left(\sigma_i^x\sigma_j^x + \gamma\sigma_i^y\sigma_j^y\right) - h\sum_{i=1}^{N}\sigma_i^z\,, \tag{D.6}$$

donde σ_k^α es la matriz de Pauli correspondiente a la posición k y en la dirección α, N al número total de espines, y λ, γ y h son ciertos parámetros. Para $\lambda = 1$ el anterior Hamiltoniano se puede escribir también en términos del espín total como

$$\begin{aligned} H &= -\frac{\lambda}{N}(1+\gamma)\left(\mathbf{J}^2 - J^zJ^z - N/2\right) - 2hJ^z \\ &\quad -\frac{\lambda}{2N}(1-\gamma)\left(J^+J^+ + J^-J^-\right)\,, \end{aligned} \tag{D.7}$$

donde $\mathbf{J}^2$ es la representación de espín $N/2$ del operador de Casimir, y $J^\pm \equiv J^x \pm iJ^y$. Este modelo presenta diferentes clases de universalidad, como se muestra en la Fig.D.1 mediante el cálculo numérico de la entropía de entrelazamiento para un bloque de $L = 125$ espines en un sistema con $N = 500$. El estudio de las leyes de escala de la entropía en las diferentes regiones

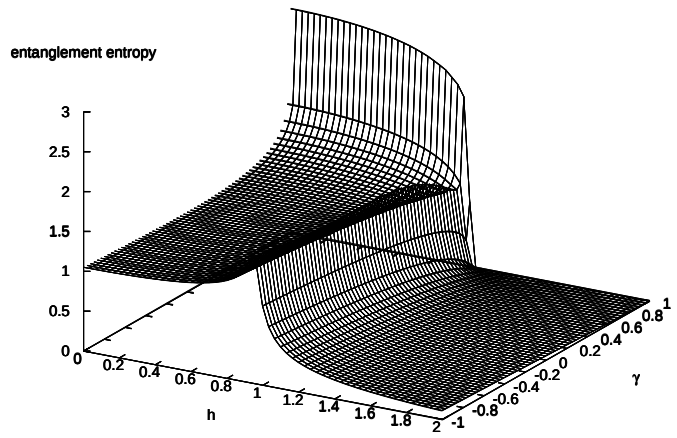

Figura D.1: Entropía de entrelazamiento para $N = 500$ y $L = 125$ como función de h y γ.

del anterior diagrama de fases muestra grandes similitudes con el que aparece en el modelo de cadena cuántica de espín XY, con proliferación de leyes logarítmicas. Una comparación de las leyes obtenidas en los dos modelos se presenta en la Tabla D.1. La similitud observada en el comportamiento del entrelazamiento de este modelo y los modelos cuánticos en $(1 + 1)$ dimensiones es notoria.

D.5 Entropía de entrelazamiento en algoritmos cuánticos

Los resultados mencionados en las secciones anteriores se centraban en las propiedades de entrelazamiento de sistemas cuánticos de muchos cuerpos, básicamente desde la perspectiva de la materia condensada y de la teoría de campos. También hemos visto que es posible aplicar algunas de las herramientas de la teoría cuántica de la información, como la mayorización, de cara a una mejor comprensión de estos sistemas. No es de extrañar, pues, que se puedan usar técnicas de materia condensada y teoría de campos para entender mejor problemas dentro de la información y computación cuánticas.

Nos centramos ahora en el análisis de escala del entrelazamiento presente en los algoritmos cuánticos. La figura de mérito χ propuesta en [49] es el número de Schmidt máximo sobre todas las posibles biparticiones de un sistema de n qubits o, en otras palabras, el máximo de los rangos de las matrices densidad reducidas de cualquier bipartición posible. Se puede demostrar que $\chi \geq 2^{S(\rho)}$, donde la entropía de von Neumann $S(\rho)$ se refiere a la matriz densidad reducida de cualquiera de los dos subsistemas de la partición. Vidal demostró que, dada una computación cuántica, si $\chi = O(\text{poly}(n))$ en cada paso del algoritmo cuántico, entonces ésta puede ser simulada por medio de métodos clásicos de manera eficiente. En otras palabras, una aceleración exponencial en un algoritmo cuántico es sólo posible si $\chi \sim \exp(n^a)$, o $S(\rho) \sim n^b$, siendo a y b constantes positivas.

Cadena de espín cuántica XY	Modelo de Lipkin, Meshkov y Glick
$H = -\sum_{i=1}^{N}\left(\frac{(1+\gamma)}{2}\sigma_i^x\sigma_{i+1}^x + \frac{(1-\gamma)}{2}\sigma_i^y\sigma_{i+1}^y + \lambda\sigma_i^z\right)$	$H = -\frac{1}{N}\sum_{i<j}\left(\sigma_i^x\sigma_j^x + \gamma\sigma_i^y\sigma_j^y\right) - h\sum_{i=1}^{N}\sigma_i^z$
$S_L(\lambda, \gamma = 0) \sim \frac{1}{3}\log_2(L)$	$S_L(h, \gamma = 1) \sim \frac{1}{2}\log_2(L)$
$S_L(\lambda, \gamma = 0) - S_L(\lambda = 0, \gamma = 0) \sim \frac{1}{6}\log_2\left(1-\lambda^2\right)$	$S_L(h, \gamma = 1) - S_L(h = 0, \gamma = 1) \sim \frac{1}{2}\log_2\left(1-h^2\right)$
$S_L(\lambda = 1, \gamma = 1) \sim \frac{1}{6}\log_2(L)$	$S_L(h = 1, \gamma = 0) \sim \frac{1}{3}\log_2(L)$
$S_L(\lambda, \gamma = 1) \sim -\frac{1}{6}\log_2(m)$	$S_L(h, \gamma = 0) \sim -\frac{1}{4}\log_2\lvert 1-h\rvert$
$S_L(\lambda = 1, \gamma) - S_L(\lambda = 1, \gamma = 1) \sim \frac{1}{6}\log_2(\gamma)$	$S_L(h = 1, \gamma) - S_L(h = 1, \gamma = 0) \sim \frac{1}{6}\log_2(1-\gamma)$

Cuadro D.1: Comparación de resultados entre la cadena de espín cuántica XY y el modelo de Lipkin, Meshkov y Glick, cuando $N \gg L \gg 1$.

En esta tesis analizamos las leyes de escala de la entropía de entrelazamiento en diversos algoritmos cuánticos. En primer lugar, un estudio analítico del algoritmo cuántico de factorización de Shor [8] muestra que las correlaciones escalan de la manera más fuerte posible. Concretamente, demostramos que hay un paso en el algoritmo en el que

$$\text{rango}(\rho) \sim r\ , \tag{D.8}$$

donde ρ es cierta matriz densidad reducida del sistema, y $r = O(N)$, siendo $N = O(2^n)$ el número a factorizar, con n el número total de qubits usados en el algoritmo.

Posteriormente, realizamos un análisis numérico de un algoritmo cuántico adiabático solucionando el problema NP-completo conocido como Cobertura Exacta [16,61–68]. Mediante una generación de instancias duras de solución única, calculamos las leyes de escala con el tamaño del sistema para la diferencia energética entre el estado fundamental del sistema y el primer estado excitado, y también para la entropía de entrelazamiento de una bipartición exacta, cerca del punto crítico y hasta 20 qubits. Los resultados, mostrados en la Fig.D.2 y en la Fig.D.3 son compatibles con una ley de escala inversa con el tamaño del sistema para la diferencia energética, y con una ley de escala proporcional al tamaño del sistema para la entropía, similar a la observada previamente en el algoritmo de Shor.

Finalmente, realizamos un análisis de la entropía de entrelazamiento presente en la implementación adiabática del algoritmo de búsqueda de Grover [9, 69, 70]. Un estudio analítico nos permite demostrar que lejos del punto de mínima diferencia energética la entropía de cualquier bipartición tiende a cero a medida que se incrementa el tamaño $N = 2^n$ de la base de datos, mientras que en el punto de mínima diferencia energética ésta tiende a saturarse en 1 mediante

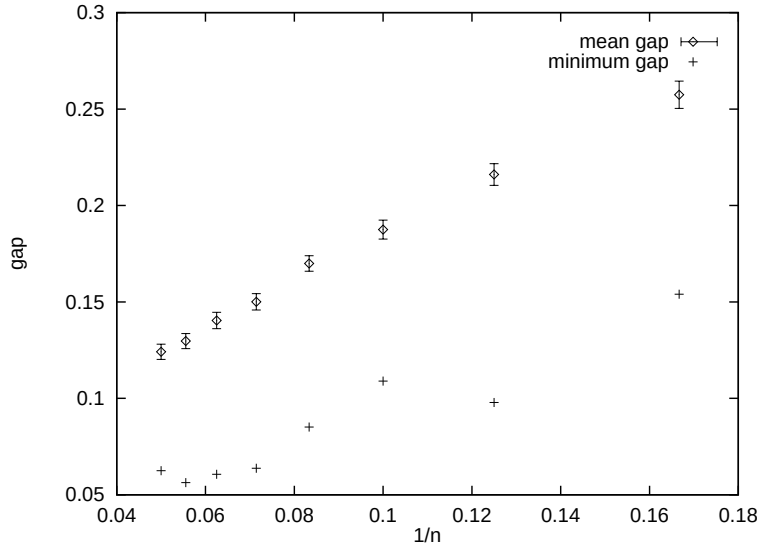

Figura D.2: Mínima diferencia energética (en unidades adimensionales) en función del tamaño inverso del sistema, en promedio y para el peor caso sobre todas las instancias generadas aleatoriamente. Las barras de error dan un 95 por ciento de nivel de confianza para la media. El comportamiento es aparentemente lineal para el promedio.

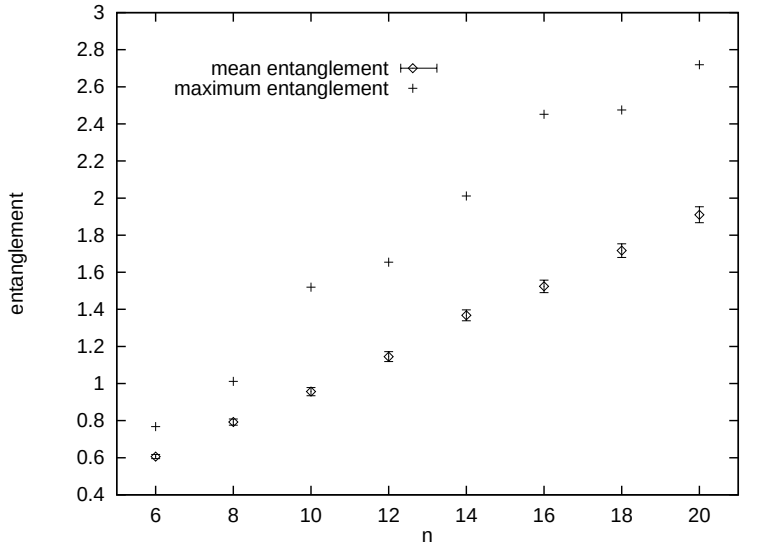

Figura D.3: Ley de escala de la entropía de entrelazamiento para una bipartición del sistema de igual tamaño de las partes, en promedio y para el peor caso sobre todas las instancias generadas aleatoriamente. Las barras de error dan un 95 por ciento de nivel de confianza para la media. Los datos son consistentes con una ley de escala lineal.

la ley

$$S(n \gg 1) \sim 1 - \frac{4}{\ln 2} 2^{-n/2} \, . \tag{D.9}$$

Las anteriores consideraciones involucran que el entrelazamiento en este algoritmo permanece siempre *acotado* entre las distintas llamadas al oráculo cuántico. Tal conclusión también es válida para la implementación del algoritmo de Grover en términos de un circuito cuántico, y recuerdan a la saturación del entrelazamiento en cadenas cuánticas de espín no críticas [22, 37, 38].

En la Tabla D.2 mostramos una recopilación de las diferentes leyes de escala para el entrelazamiento observadas en diferentes situaciones. La dureza de la ley de escala depende de la dureza del problema a tratar.

Problema	Entropía de entrelazamiento
Algoritmo para Cobertura Exacta	$S = O(n)$
Algoritmo de Shor	$S = O(\log_2 r) \sim O(n)$
Fermiones críticos en $(d+1)$ dimensiones	$S = O(n^{\frac{d-1}{d}} \log_2 n)$
Bosones críticos en $(d+1)$ dimensiones	$S = O(n^{\frac{d-1}{d}})$
Cadenas de espín críticas	$S = O(\log_2 n)$
Cadenas de espín no críticas	$S = O(1)$
Algoritmo de Grover	$S = O(1)$

← menos entropía

Cuadro D.2: Leyes de escala del entrelazamiento para diferentes problemas, en orden decreciente en complejidad.

D.6 Simulación clásica de algoritmos cuánticos usando estados producto de matriz

Pese a que es posible estudiar numéricamente las propiedades de baja energía de cualquier modelo mediante una diagonalización exacta de su Hamiltoniano o técnicas similares, tal posibilidad se limita siempre a un número de partículas relativamente pequeño debido al crecimiento exponencial del tamaño del espacio de Hilbert. Ciertamente, esta es una de las motivaciones

básicas para construir un ordenador cuántico [1]. Usando la tecnología actual convencional, un estudio numérico fiable de las propiedades del estado fundamental de un Hamiltoniano cuántico genérico sólo se puede realizar para sistemas del orden de 20 espines. Afortunadamente, tenemos a nuestra disposición otras técnicas numéricas. Un ejemplo de ellas es el grupo de renormalización de la matriz densidad (GRMD), introducido por White en [20]. A pesar de que pronto se vio que el GRMD proporcionaba resultados precisos para la energía del estado fundamental de sistemas cuánticos en una dimensión espacial, también se observó que el método no funcionaba tan bien al ser aplicado a sistemas de mayor dimensionalidad [171, 172]. Incluso en el caso de (1 + 1) dimensiones había una diferencia en los resultados obtenidos a partir del método para sistemas con condiciones de contorno abiertas y periódicas, siendo la primera la más precisa. No obstante, el GRMD ha sido el algoritmo de referencia a lo largo de la última década para calcular las propiedades de baja energía de modelos cuánticos en una dimensión espacial.

Tras la aparición del GRMD, Ostlund y Rommer obtuvieron un resultado notable [47], al mostrar que el algoritmo original del GRMD se podía entender completamente en términos de los llamados estados producto de matriz. Originariamente introducidos en el modelo de ligaduras de valencia de Affleck, Kennedy, Lieb y Tasaki [45, 46], generalizados por Fannes, Nachtergaele y Werner [48], y redescubiertos en el ámbito de la información cuántica por Vidal [49], los estados producto de matriz han demostrado ser especialmente útiles de cara a desarrollar técnicas numéricas para el cálculo de las propiedades de baja energía junto con la dinámica de Hamiltonianos suficientemente locales en una dimensión espacial [50–57], y han servido también de inspiración para diversas técnicas numéricas de cara al estudio de sistemas con mayor dimensionalidad [58–60].

La pregunta natural es, pues, si los estados producto de matriz pueden ser empleados de cara a simular la dinámica de un ordenador cuántico. En esta tesis hemos mostrado que ello es ciertamente posible, y que se pueden realizar simulaciones para tamaños relativamente grandes del sistema con una precisión controlada. El parámetro que controla la precisión de nuestras simulaciones es el tamaño χ de las matrices que parametrizan el estado, y del que ya hablamos en la sección anterior. Esperamos por lo tanto que nuestras aproximaciones clásicas fallen para aquellos sistemas en los que el χ necesario sea inherentemente exponencial en el tamaño del sistema. No obstante, en ciertos casos es posible reproducir una buena simulación clásica manteniendo $\chi = O(\text{poly}(n))$ a lo largo del proceso, siendo n es el número de qubits.

Concretamente, hemos realizado un análisis de diversas simulaciones clásicas del algoritmo adiabático descrito en la sección anterior solucionando el problema NP-completo de Cobertura Exacta. El hecho de que la entropía de entrelazamiento obedezca en ese algoritmo la ley de escala $S \sim 0{,}1n$ nos induce a pensar que tal vez sea posible reproducir con fidelidad y de manera aproximada algunas de las propiedades esenciales del algoritmo cuántico mediante una simulación clásica con estados producto de matriz, dado que el prefactor de la ley de escala es relativamente pequeño.

Nuestros datos numéricos para la evolución del valor esperado de la energía de sistema se muestran en la Fig.D.4. El sistema prevalece notoriamente cerca del estado fundamental instantáneo a lo largo de la evolución aproximada y, como podemos ver, el error absoluto máximo respecto a nuestra mejor simulación clásica ($\chi = 40$) aparece cuando la evolución se acerca a

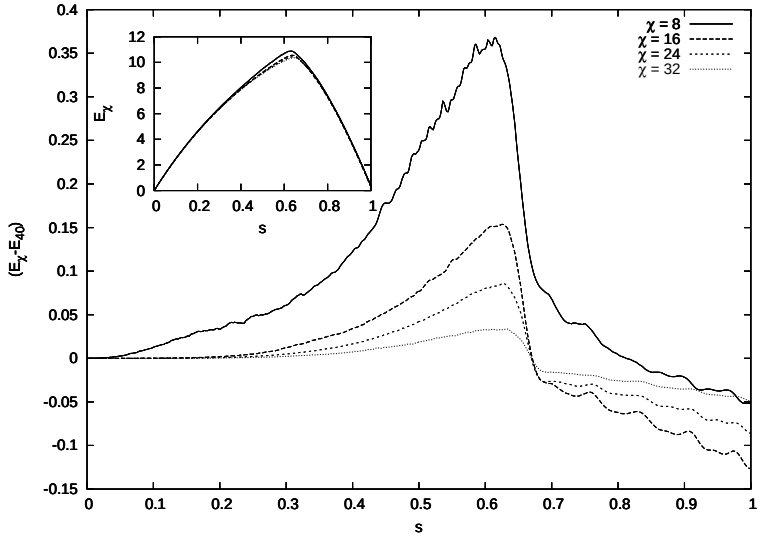

Figura D.4: Cálculo del error absoluto, comparado con el caso $\chi = 40$, del valor esperado de la energía (en unidades adimensionales) en función del parámetro de interpolación s para una instancia típica de 30 bits y 24 cláusulas, para $T = 100$, y χ creciente. En pequeño, mostramos el valor esperado instantáneo de la energía (en unidades adimensionales). Otras instancias muestran un comportamiento similar.

un punto crítico. Cerca de este punto de transición de fase, el error absoluto en la energía es del orden de $10^{-2} - 10^{-3}$, menor que la típica diferencia energética entre el estado fundamental y el primer estado excitado para este tipo de sistemas.

Como ejemplo simbólico, nuestro programa ha solucionado una instancia con $n = 100$ bits, es decir, el algoritmo adiabático aproximado ha encontrado el estado producto correcto entre $2^{100} \sim 10^{30}$ posibilidades para una instancia dura con $m = 84$ cláusulas y $T = 2000$. La simulación se realizó con un especialmente pequeño $\chi = 14 \ll 2^{50} = \chi_{max}$, y se presenta en la Fig.D.5.

De cara a un análisis más profundo de la simulación clásica, hemos lanzado una búsqueda del mínimo $T_{min}(n)$ que soluciona muestras de instancias duras de n bits. Nuestros resultados aparecen en la Fig.D.6. El promedio sobre instancias de n bits de $T_{min}(n)$ parece crecer lentamente con n, a pesar de que los casos extremos necesitan mayores tiempos hasta $n = 25$. El relajamiento del crecimiento con n en los gráficos es debido a la dificultad en la generación de instancias duras para n grande.

D.7 Flecha de mayorización en el diseño de algoritmos cuánticos

Algunos intentos de desenmascarar las propiedades básicas de los algoritmos cuánticos ya han sido explorado. Un rol esencial es indudablemente el que juega el entrelazamiento [49, 50, 155–159]. De hecho, pese a que éste es un recurso natural a ser explotado en el diseño de algoritmos cuánticos, existen ejemplos conocidos de algoritmos basados en oráculos, más rápidos que

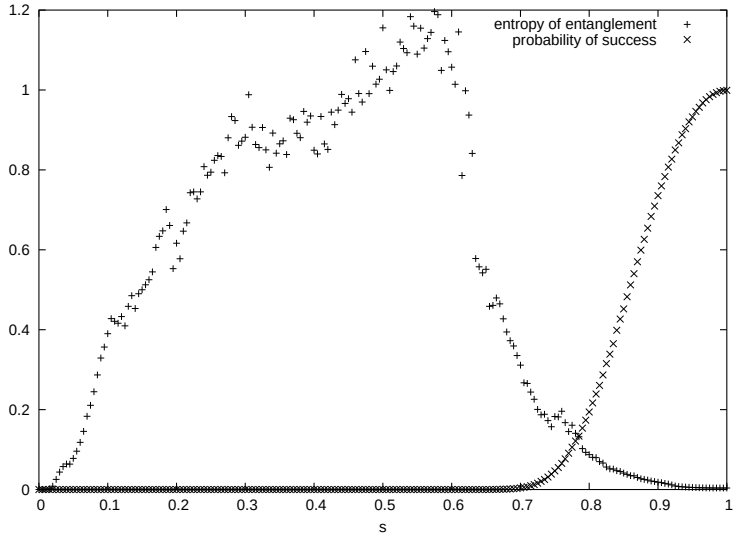

Figura D.5: Entropía de entrelazamiento de una bipartición y probabilidad de la solución como función del parámetro de interpolación s, para una simulación con $\chi = 14$ de la evolución adiabática solucionando una instancia dura de $n = 100$ bits y $m = 84$ cláusulas.

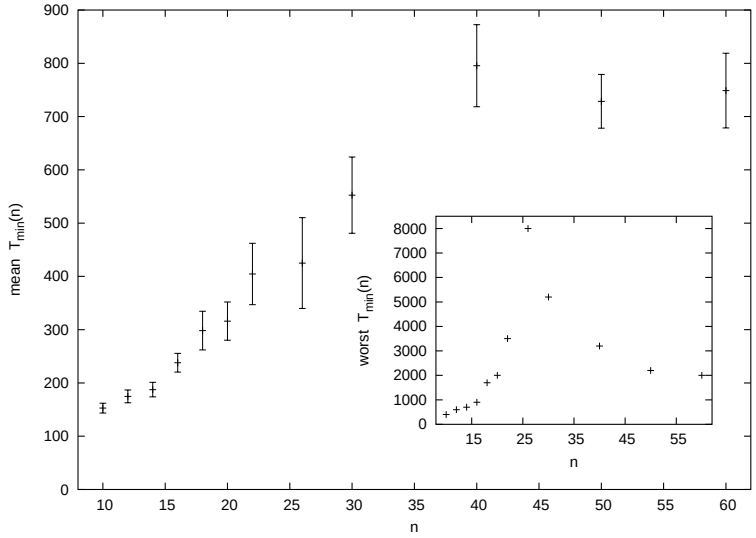

Figura D.6: Casos promedio y peor de la estadística acumulada hasta $n = 60$ para $T_{min}(n)$ (en unidades adimensionales). Los promedios se realizan sobre 200 instancias para cada n, excepto para $n = 50, 60$, con $199, 117$ instancias respectivamente. Las barras de error dan un 95 por ciento de nivel de confianza en la media.

cualquier posible algoritmo clásico, y en los que el registro cuántico permanece siempre en un estado producto entre las diversas llamadas al oráculo. Pese a todo, la aceleración respecto al caso clásico es sólo por un factor dos en estos ejemplos [161, 181, 182]. En esta tesis presentamos una alternativa al estudio de los algoritmos cuánticos. La idea básica es que existe un fuerte comportamiento subyacente respecto a mayorización en algunas familias de algoritmos cuánticos que parece jugar también algún papel en su eficiencia. Concretamente, estudiamos la evolución en el tiempo, respecto a mayorización, de la distribución de probabilidad de los posibles resultados de nuestro aparato de medida, para diversos algoritmos cuánticos, tal y como fue introducido en [152].

En primer lugar, estudiamos la amplia familia de algoritmos cuánticos de estimación de fase [2, 8, 161, 181–183]. El elemento clave en estos algoritmos es el uso de la transformada de Fourier cuántica sobre un estado previamente preparado, tal y como se muestra en los circuitos cuánticos representados en la Fig.D.7 y la Fig.D.8.

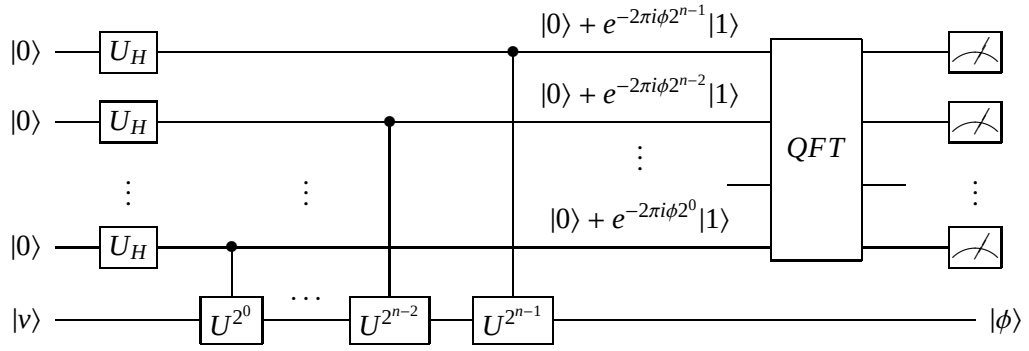

Figura D.7: Circuito cuántico para el algoritmo de estimación de fase. El operador U y el vector $|\phi\rangle$ son tal que $U|\phi\rangle = e^{-2\pi i\phi}|\phi\rangle$, siendo $\phi \in [0, 1)$ el parámetro a estimar con n bits de precisión.

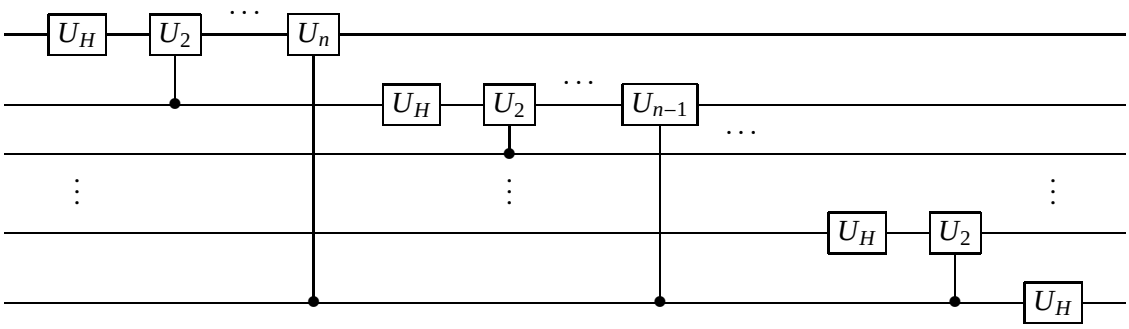

Figura D.8: Descomposición canónica del operador transformada de Fourier cuántica. Por U_j nos referimos a la puerta unitaria $|0\rangle\langle 0| + e^{2\pi i/2^j}|1\rangle\langle 1|$, controlada $j-1$ qubits por debajo.

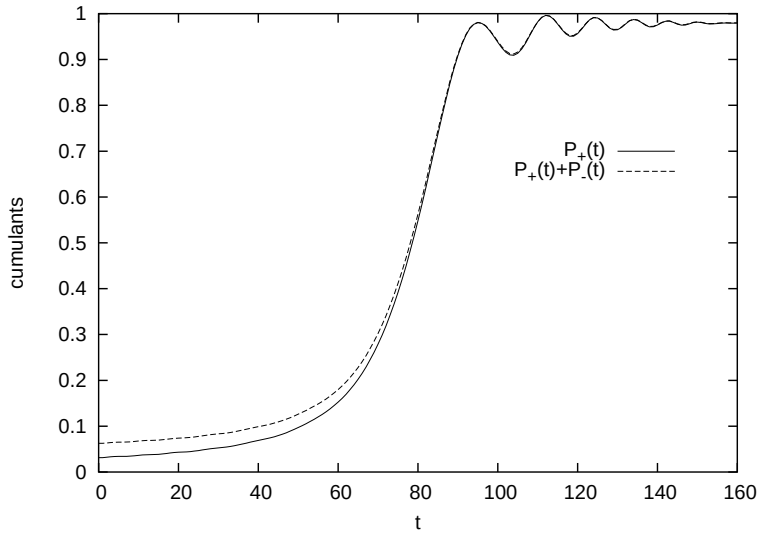

Figura D.9: Búsqueda cuántica adiabática para el camino no óptimo con $N = 32$ elementos y tiempo $T = 160$. No hay mayorización paso a paso

Demostramos que el operador transformada de Fourier cuántica mayoriza paso a paso la distribución de probabilidad resultante de las medidas en la base computacional, en el algoritmo cuántico de estimación de fase. La distribución de probabilidad resultante sigue, por lo tanto, un ciclo de mayorización a lo largo de la totalidad del algoritmo.

Posteriormente, consideramos el análisis respecto a mayorización de diferentes algoritmos cuánticos adiabáticos solucionando el problema de Grover. Tal y como se muestra en la Fig.D.9 y la Fig.D.10, donde $P_+(t)$ y $P_+(t) + P_-(t)$ representan los dos primeros cumulantes de mayorización en el instante t, la flecha de mayorización aparece en la evolución correspondiente a un parámetro de interpolación óptimo, dando aceleración cuadrática respecto al caso clásico junto con mayorización paso a paso a lo largo de toda la evolución.

Finalmente, estudiamos la aparición de mayorización en un algoritmo de camino cuántico solucionando un problema clásico definido en un grafo no trivial con aceleración exponencial [179]. Para tal algoritmo, la evolución de los cumulantes de mayorización obedece un ciclo tal y como se muestra en la Fig.D.11. Este comportamiento recuerda al ya observado en los algoritmos cuánticos de estimación de fase.

D.8 Direcciones futuras

Hay diversas direcciones futuras que pueden ser consideradas a partir del trabajo presentado en esta tesis. En primer lugar, podría hacerse un estudio analítico detallado de mayorización e irreversibilidad a lo largo de los flujos del grupo de renormalización para teorías en mas de (1 + 1) dimensiones. El comportamiento del entrelazamiento de una copia para tales teorías también es otra posible extensión. Desde el punto de vista de complejidad computacional, es aún un reto el saber si los algoritmos cuánticos adiabáticos serán o no capaces de solucionar los problemas

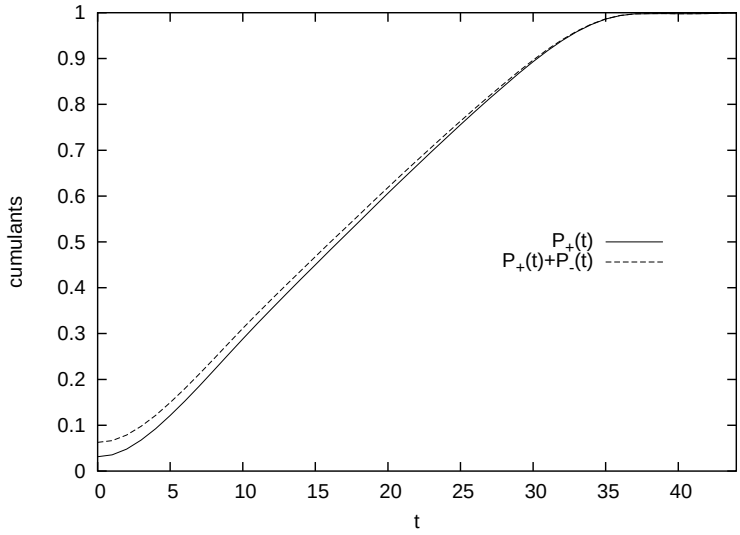

Figura D.10: Búsqueda cuántica adiabática para el camino óptimo con $N = 32$ elementos y tiempo $T = 44$. Se verifica mayorización paso a paso.

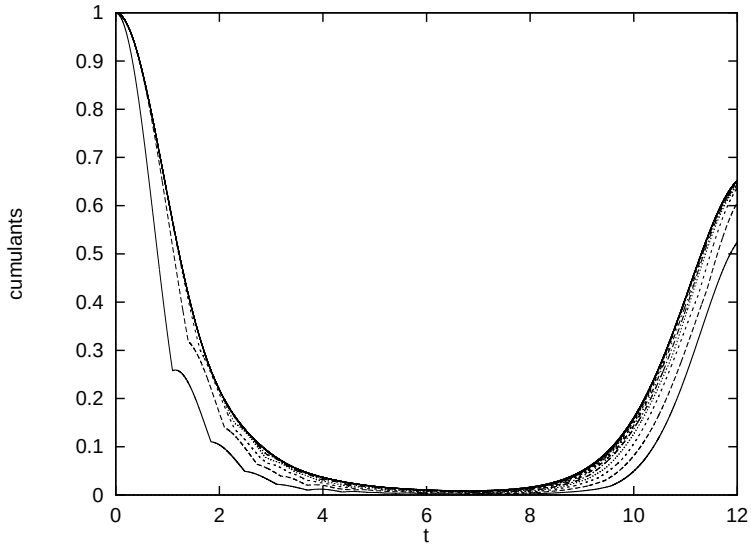

Figura D.11: Evolución temporal de 22 cumulantes en el algoritmo de camino cuántico, para $n = 10$ qubits. El proceso obedece a un ciclo de mayorización.

NP-completos de manera eficiente. Análisis numéricos de estos algoritmos se podrían realizar mediante extensiones de las técnicas basadas en los estados producto de matriz que nosotros hemos considerado. Asimismo, sería plausible realizar simulaciones clásicas mediante los mismos métodos de otros algoritmos cuánticos, tales como el algoritmo de factorización de Shor. No obstante, el gran problema en computación cuántica continúa siendo el diseño de nuevos algoritmos cuánticos útiles y eficientes. Por otra parte, desde la perspectiva de la teoría cuántica de muchos cuerpos, el reto es el desarrollo de nuevas de técnicas numéricas para el estudio de sistemas cuánticos en $(2+1)$ dimensiones, y en especial para sistemas fermiónicos, para los que se sabe que la ley de escala de área para la entropía de entrelazamiento falla. Un mejor entendimiento de estos sistemas, tanto desde un punto de vista teórico como numérico, junto con un ensayo de la función de onda de su estado fundamental que sea práctico desde el punto de vista computacional y que reproduzca fidedignamente sus propiedades de entrelazamiento, prevalece a día de hoy como un problema abierto.

Bibliography

[1] R. P. Feynman. Simulating physics with computers. *Int. J. Theor. Phys.*, 21:467, 1982.

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

[3] R. Landauer. Irreversibility and heat generation in the computing process. *IBM J. Res. Dev.*, 5:183, 1961.

[4] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. Wootters. Teleporting an unknown quantum state via dual classical and EPR channels. *Phys. Rev. Lett.*, 70:1895, 1993.

[5] C. H. Bennett and S. J. Wiesner. Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states. *Phys. Rev. Lett.*, 69:2881, 1992.

[6] C. H. Bennett and G. Brassard. Quantum cryptography: public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, page 175, 1984.

[7] A. K. Ekert. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.*, 67:661, 1991.

[8] P. W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings of the 35th Annual Symposium on Fundations of Computer Science*, 1994.

[9] L. K. Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the 28th Annual ACM Symposium on the Theory of Computing*, page 212, 1996.

[10] M. Lewenstein, D. Bruss, J. I. Cirac, B. Kraus, M. Kus, J. Samsonowicz, A. Sanpera, and R. Tarrach. Separability and distillability in composite quantum systems – a primer –. *J. Mod. Opt.*, 47:2841, 2000.

[11] R. F. Muirhead. Some methods applicable to identities and inequalities of symmetric algebraic functions of *n* letters. In *Proceedings of the Edinburg Mathematical Society*, volume 21, page 144, 1903.

[12] G. H. Hardy, J. E. Littlewood, and G. Pólya. *Inequalities*. Cambridge University Press, Cambridge, 1978.

[13] A. W. Marshall and I. Olkin. *Inequalities: Theory of Majorization and its Applications*. Acad. Press Inc., 1979.

[14] R. Bhatia. *Matrix Analysis*. Springer-Verlag, New York, 1997.

[15] M. A. Nielsen. Conditions for a class of entanglement transformations. *Phys. Rev. Lett.*, 83:436, 1999.

[16] E. Farhi, J. Goldstone, S. Gutmann, and M. Sipser. Quantum computation by adiabatic evolution, 2000. quant-ph/0001106.

[17] F. Verstraete, M. A. Martín-Delgado, and J. I. Cirac. Diverging entanglement length in gapped quantum spin systems. *Phys. Rev. Lett.*, 92:087201, 2004.

[18] K. Wilson. Renormalization group and critical phenomena. I. Renormalization group and the Kadanoff scaling picture. *Phys. Rev. B*, 4:3174, 1971.

[19] K. Wilson. Renormalization group and critical phenomena. II. Phase-space cell analysis of critical behavior. *Phys. Rev. B*, 4:3184, 1971.

[20] S. R. White. Density matrix formulation for quantum renormalization groups. *Phys. Rev. Lett.*, 69:2863, 1992.

[21] P. Ginsparg. *Applied Conformal Field Theory*. Les Houches Summer School, France, 1988.

[22] E. Rico. *Quantum Correlations in* (1 + 1)*-Dimensional Systems*. PhD thesis, Universitat de Barcelona, 2005.

[23] D. P. DiVincenzo. Quantum computation. *Science*, 270:255, 1995.

[24] J. I. Cirac and P. Zoller. Quantum computations with cold trapped ions. *Phys. Rev. Lett.*, 74:4091, 1995.

[25] D. P. DiVincenzo. Two-bit gates are universal for quantum computation. *Phys. Rev. A*, 51:1015, 1995.

[26] D. G. Cory, A. F. Fahmy, and T. F. Havel. Ensemble quantum computing by NMR spectroscopy. In *Proceedings of the National Academy of Science USA*, volume 94, page 1634, 1997.

[27] N. Gershenfeld and I. L. Chuang. Bulk spin resonance quantum computation. *Science*, 275:350, 1997.

[28] D. Loss and D. P. DiVincenzo. Quantum computation with quantum dots. *Phys. Rev. A*, 57:120, 1998.

[29] B. Kane. A silicon-based nuclear spin quantum computer. *Nature*, 393:133, 1998.

[30] R. Vrijen, E. Yablonovitch, K. Wang, H. W. Jiang, A. Balandin, V. Roychowdhury, T. Mor, and D. P. DiVincenzo. Electron spin resonance transistors for quantum computing in silicon-germanium heterostructures, 1999. quant-ph/9905096.

[31] M. Srednicki. Entropy and area. *Phys. Rev. Lett.*, 71:666, 1993.

[32] C. G. Callan and F. Wilczek. On geometric entropy. *Phys. Lett. B*, 333:55, 1994.

[33] T. M. Fiola, J. Preskill, A. Strominger, and S. P. Trivedi. Black hole thermodynamics and information loss in two-dimensions. *Phys. Rev. D*, 50:3987, 1994.

[34] D. Kabat and M. J. Strassler. A comment on entropy and area. *Phys. Lett. B*, 329:46, 1994.

[35] D. Kabat. Black hole entropy and entropy of entanglement. *Nucl. Phys. B*, 453:281, 1995.

[36] C. Holzhey, F. Larsen, and F. Wilczek. Geometric and renormalized entropy in conformal field theory. *Nucl. Phys. B*, 424:443, 1994.

[37] G. Vidal, J. I. Latorre, E. Rico, and A. Kitaev. Entanglement in quantum critical phenomena. *Phys. Rev. Lett.*, 90:227902, 2003.

[38] J. I. Latorre, E. Rico, and G. Vidal. Ground state entanglement in quantum spin chains. *Quant. Inf. and Comp.*, 4:48, 2004.

[39] V. E. Korepin. Universality of entropy scaling in 1d gap-less models. *Phys. Rev. Lett.*, 92:096402, 2004.

[40] A. R. Its, B. Q. Jin, and V. E. Korepin. Entanglement in XY spin chain. *J. Phys. A*, 38:2975, 2005.

[41] P. Calabrese and J. Cardy. Entanglement entropy and quantum field theory. *J. Stat. Mech.*, 0406:002, 2004.

[42] P. Calabrese and J. Cardy. Evolution of entanglement entropy in one-dimensional systems. *J. Stat. Mech.*, 0504:010, 2005.

[43] H. Casini, C. D. Fosco, and M. Huerta. Entanglement and alpha entropies for a massive Dirac field in two dimensions. *J. Stat. Mech.*, 0507:007, 2005.

[44] H. Casini and M. Huerta. Entanglement and alpha entropies for a massive scalar field in two dimensions. *J. Stat. Mech.*, 0512:012, 2005.

[45] I. Affleck, T. Kennedy, E. H. Lieb, and H. Tasaki. Rigorous results on valence-bond ground states in antiferromagnets. *Phys. Rev. Lett.*, 59:799, 1987.

[46] I. Affleck, T. Kennedy, E. H. Lieb, and H. Tasaki. Valence bond ground states in isotropic quantum antiferromagnets. *Commun. Math. Phys.*, 115:477, 1988.

[47] S. Ostlund and S. Rommer. Themodynamic limit of density matrix renormalization. *Phys. Rev. Lett.*, 75:3537, 1995.

[48] M. Fannes, B. Nachtergaele, and R. F. Werner. Finitely correlated states on quantum spin chains. *Commun. Math. Phys.*, 144:443, 1992.

[49] G. Vidal. Efficient classical simulation of slightly entangled quantum computations. *Phys. Rev. Lett.*, 91:147902, 2003.

[50] G. Vidal. Efficient simulation of one-dimensional quantum many-body systems. *Phys. Rev. Lett.*, 93:040502, 2004.

[51] M. Zwolak and G. Vidal. Mixed-state dynamics in one-dimensional quantum lattice systems: a time-dependent superoperator renormalization algorithm. *Phys. Rev. Lett.*, 93:207205, 2004.

[52] U. Schollwöck. Time-dependent density-matrix renormalization-group methods. *J. Phys. Soc. Jpn*, 74:246, 2005.

[53] F. Verstraete, D. Porras, and J. I. Cirac. Density matrix renormalization group and periodic boundary conditions: a quantum information perspective. *Phys. Rev. Lett.*, 93:227205, 2004.

[54] F. Verstraete, J. J. García-Ripoll, and J. I. Cirac. Matrix product density operators: simulation of finite-temperature and dissipative systems. *Phys. Rev. Lett.*, 93:207204, 2004.

[55] F. Verstraete, A. Weichselbaum, U. Schollwöck, J. I. Cirac, and J. von Delft. Variational matrix product state approach to quantum impurity models, 2005. cond-mat/0504305.

[56] F. Verstraete and J. I. Cirac. Matrix product states represent grund states faithfully. *Phys. Rev. B*, 73:094423, 2006.

[57] U. Schollwöck. The density-matrix renormalization group. *Rev. Mod. Phys.*, 77:259, 2005.

[58] F. Verstraete and J. I. Cirac. Renormalization algorithms for quantum-many body systems in two and higher dimensions, 2004. cond-mat/0407066.

[59] G. Vidal. Entanglement renormalization, 2005. cond-mat/0512165.

[60] S. Anders, M. B. Plenio, W. Dür, F. Verstraete, and H.-J. Briegel. Ground state approximation for strongly interacting systems in arbitrary dimension, 2006. quant-ph/0602230.

[61] E. Farhi, J. Goldstone, and S. Gutmann. A numerical study of the performance of a quantum adiabatic evolution algorithm for satisfiability, 2000. quant-ph/0007071.

[62] A. M. Childs, E. Farhi, J. Goldstone, and S. Gutmann. Finding cliques by quantum adiabatic evolution. *Quant. Inf. and Comp.*, 2:181, 2002.

[63] E. Farhi, J. Goldstone, S. Gutmann, J. Lapan, A. Lundgren, and D. Preda. A quantum adiabatic evolution algorithm applied to random instances of an NP-complete problem. *Science*, 292:472, 2001.

[64] A. M. Childs, E. Farhi, J. Goldstone, and J. Preskill. Robustness of adiabatic quantum computation. *Phys. Rev. A*, 65:012322, 2002.

[65] E. Farhi, J. Goldstone, and S. Gutmann. Quantum adiabatic evolution algorithms versus simulated annealing, 2002. quant-ph/0201031.

[66] E. Farhi, J. Goldstone, and S. Gutmann. Quantum adiabatic evolution algorithms with different paths, 2002. quant-ph/0208135.

[67] E. Farhi, J. Goldstone, S. Gutmann, and D. Nagaj. How to make the quantum adiabatic algorithm fail, 2005. quant-ph/0512159.

[68] S. P. Jordan, E. Farhi, and P. W. Shor. Error corrrecting codes for adiabatic quantum computation, 2005. quant-ph/0512170.

[69] J. Roland and N. J. Cerf. Quantum search by local adiabatic evolution. *Phys. Rev. A*, 65:042308, 2002.

[70] W. van Dam, M. Mosca, and U. Vazirani. How powerful is adiabatic quantum computation? In *Proceedings of the 42nd Symposium on Foundations of Computer Science*, page 279, 2001.

[71] D. Aharonov, W. van Dam, J. Kempe, Z. Landau, S. Lloyd, and O. Regev. Adiabatic quantum computation is equivalent to standard quantum computation, 2004. quant-ph/0405098.

[72] S. A. Cook. The complexity of theorem-proving procedures. In *Proceedings of the 3rd Annual ACM Symposium on the Theory of Computing*, page 151, 1971.

[73] K. Wilson and J. Kogut. The renormalization group and the ϵ expansion. *Phys. Rep.*, 12:75, 1974.

[74] D. J. Wallace and R. K. P. Zia. Gradient properties of the renormalization group equations in multicomponent systems. *Ann. Phys.*, 92:142, 1975.

[75] A. B. Zamolodchikov. 'Irreversibility' of the flux of the renormalization group in a 2-d field theory. *JETP Lett.*, 43:730, 1986.

[76] A. Capelli, J. I. Latorre, and X. Vilasís-Cardona. Renormalization group patterns and *c*-theorem in more than two dimensions. *Nucl. Phys. B*, 376:510, 1992.

[77] G. Zumbach. The renormalization group in the local potential approximation and its applications to the O(n) model. *Nucl. Phys. B*, 413:754, 1994.

[78] G. Zumbach. The local potential approximation of the renormalization group and its applications. *Phys. Lett. A*, 190:225, 1994.

[79] J. Generowicz, C. Harvey-Fros, and T. R. Morris. *c* function representation of the local potential approximation. *Phys. Lett. B*, 407:27, 1997.

[80] P. E. Haagensen, Y. Kubyshin, J. I. Latorre, and E. Moreno. Gradient flows from an approximation to the exact renormalization group. *Phys. Lett. B*, 323:330, 1994.

[81] F. Bastianelli. Tests for *c*-theorems in 4d. *Phys. Lett. B*, 369:249, 1996.

[82] D. Anselmi, J. Erlich, D. Z. Freedman, and A. Johansen. Positivity constraints on anomalies in supersymmetric gauge theories. *Phys. Rev. D*, 57:7570, 1998.

[83] D. Anselmi, D. Z. Freedman, M. T. Grisaru, and A. A. Johansen. Non-perturbative formulas for central functions of supersymmetric gauge theories. *Nucl. Phys. B*, 526:543, 1998.

[84] J. L. Cardy. Is there a *c*-theorem in four dimensions? *Phys. Lett. B*, 215:749, 1988.

[85] H. Osborn. Derivation of a four dimensional *c*-theorem for renormalisable quantum field theories. *Phys. Lett. B*, 222:97, 1989.

[86] I. Jack and H. Osborn. Analogs of the *c*-theorem for four-dimensional renormalisable field theories. *Nucl. Phys. B*, 343:647, 1990.

[87] A. Capelli, D. Friedan, and J. I. Latorre. *c*-theorem and spectral representation. *Nucl. Phys. B*, 352:616, 1991.

[88] S. Forte and J. I. Latorre. A proof of the irreversibility of renormalization group flows in four dimensions. *Nucl. Phys. B*, 535:709, 1998.

[89] S. Forte and J. I. Latorre. Realization of symmetries and the *c*-theorem. In *Proceedings of the I Workshop on Exact Renormalization Group*, 1998.

[90] H. Osborn and G. M. Shore. Correlation functions of the energy momentum tensor on spaces of constant curvature. *Nucl. Phys. B*, 571:287, 2000.

[91] A. Capelli, G. D'Appollonio, R. Guida, and N. Magnoli. On the *c*-theorem in more than two dimensions. In *Proceedings of the TMR Conference "Non-perturbative quantum effects 2000"*, 2000.

[92] A. Capelli and G. D'Appollonio. On the trace anomaly as a measure of degrees of freedom. *Phys. Lett. B*, 487:87, 2000.

[93] E. Barnes, K. Intriligator, B. Wecht, and J. Wright. Evidence for the strongest version of the 4d a-theorem, via a-maximization along RG flows. *Nucl. Phys. B*, 702:131, 2004.

[94] D. Anselmi. Inequalities for trace anomalies, length of the RG flow, distance between the fixed points and irreversibility. *Class. Quant. Grav.*, 21:29, 2004.

[95] J. I. Latorre, C. A. Lütken, E. Rico, and G. Vidal. Fine-grained entanglement loss along renormalization group flows. *Phys. Rev. A*, 71:034301, 2005.

[96] I. Peschel, M. Kaulke, and Ö. Legeza. Density-matrix spectra for integrable models. *Ann. Physik (Leipzig)*, 8:153, 1999.

[97] I. Peschel. On the reduced density matrix for a chain of free electrons. *J. Stat. Mech.*, 0406:004, 2004.

[98] I. Peschel. On the entanglement entropy for a *XY* spin chain. *J. Stat. Mech.*, 0412:005, 2004.

[99] E. Baruoch and B. M. McCoy. Statistichal mechanics of the *XY* model. II. Spin-correlation functions. *Phys. Rev. A*, page 786, 1971.

[100] H. Q. Zhou, T. Barthel, J. O. Fjaerestad, and U. Schollwöck. Entanglement and boundary critical phenomena, 2005. cond-mat/0511732.

[101] C. Wellard and R. Orús. Quantum phase transitions in anti-ferromagnetic planar cubic lattices. *Phys. Rev. A*, 70:0409611, 2004.

[102] J. I. Latorre, R. Orús, E. Rico, and J. Vidal. Entanglement entropy in the Lipkin-Meshkov-Glick model. *Phys. Rev. A*, 71:064101, 2005.

[103] A. Osterloh, L. Amico, G. Falci, and R. Fazio. Scaling of entanglement close to a quantum phase transition. *Nature*, 416:608, 2002.

[104] T. J. Osborne and M. A. Nielsen. Entanglement in a simple quantum phase transition. *Phys. Rev. A*, 66:032110, 2002.

[105] K. Audenaert, J. Eisert, M. B. Plenio, and R. F. Werner. Entanglement properties of the harmonic chain. *Phys. Rev. A*, 66:042327, 2002.

[106] A. Botero and B. Reznik. Spatial structures and localization of vacuum entanglement in the linear harmonic chain. *Phys. Rev. A*, 70:052329, 2004.

[107] M. Hein, J. Eisert, and H. J. Briegel. Multiparty entanglement in graph states. *Phys. Rev. A*, 69:062311, 2004.

[108] J. P. Keating and F. Mezzadri. Entanglement in quantum spin chains, symmetry classes of random matrices, and conformal field theory. *Phys. Rev. Lett.*, 94:050501, 2005.

[109] M. M. Wolf. Violation of the entropic area law for fermions. *Phys. Rev. Lett.*, 96:010404, 2006.

[110] D. Gioev and I. Klich. Entanglement entropy of fermions in any dimension and the Widom conjecture. *Phys. Rev. Lett.*, 96:100503, 2006.

[111] T. Barthel, M.-C. Chung, and U. Schollwöck. Entanglement scaling in critical two-dimensional fermionic and bosonic systems, 2006. cond-mat/0602077.

[112] R. Orús. Entanglement and majorization in (1 + 1)-dimensional quantum systems. *Phys. Rev. A*, 71:052327, 2005.

[113] J. Eisert and M. Cramer. Single-copy entanglement in critical quantum spin chains. *Phys. Rev. A*, 72:042112, 2005.

[114] M. Popp, F. Verstraete, and M. A. Martín-Delgado. Localizable entanglement. *Phys. Rev. A*, 71:042306, 2005.

[115] B. Q. Jin and V. E. Korepin. Quantum spin chain, Toeplitz determinants and Fisher-Hartwig conjecture. *J. Stat. Phys.*, 116:79, 2003.

[116] B. Q. Jin and V. E. Korepin. Correlation functions in spin chains and information theory. *Phys. Rev. A*, 69:062314, 2004.

[117] H. Fan, V. Korepin, and V. Roychowdhury. Entanglement in a valence-bond-solid state. *Phys. Rev. Lett.*, 93:227203, 2004.

[118] J. Eisert and T. J. Osborne. General entanglement scaling laws from time evolution, 2006. quant-ph/0603114.

[119] W. K. Wootters. Entanglement of formation of an arbitrary state of two qubits. *Phys. Rev. Lett.*, 80:2245, 1998.

[120] I. Peschel and J. Zhao. On single-copy entanglement. *J. Stat. Mech.*, 0511:002, 2005.

[121] C. H. Bennett, H. J. Bernstein, S. Popescu, and B. Schumacher. Concentrating partial entanglement by local operations. *Phys. Rev. A*, 53:2046, 1996.

[122] E. Lieb, T. Schultz, and D. Mattis. Two soluble models of an antiferromagnetic chain. *Ann. Phys.*, 16:407, 1961.

[123] T. Ehrhardt and B. Silbermann. Toeplitz determinants with one Fisher-Hartwig singularity. *J. Funct. Anal.*, 148:229, 1997.

[124] O. F. Syljuasen. Concurrence in the two dimensional XXZ- and transverse field Ising-models, 2003. quant-ph/0312101.

[125] A. Hamma and P. Zanardi. Quantum entangling power of adiabatically connected Hamiltonians. *Phys. Rev. A*, 69:062319, 2004.

[126] A. Hamma, R. Ionicioiu, and P. Zanardi. Ground state entanglement and geometric entropy in the Kitaev's model. *Phys. Lett. A*, 337:22, 2005.

[127] A. Hamma, R. Ionicioiu, and P. Zanardi. Bipartite entanlement and entropic boundary law in lattice spin systems. *Phys. Rev. A*, 71:022315, 2005.

[128] A. Hamma, P. Zanardi, and X. G. Wen. String and membrane condensation on 3d lattices. *Phys. Rev. B*, 72:035307, 2005.

[129] J. I. Latorre and R. Orús. Adiabatic quantum computation and quantum phase transitions. *Phys. Rev. A*, 69:062302, 2004.

[130] R. Orús and J. I. Latorre. Universality of entanglement and quantum computation complexity. *Phys. Rev. A*, 69:052308, 2004.

[131] M. Cramer, J. Eisert, M. B. Plenio, and J. Dreissig. Entanglement-area law for general bosonic harmonic lattice systems. *Phys. Rev. A*, 73:012309, 2006.

[132] H. J. Lipkin, N. Meshkov, and A. J. Glick. Validity of many-body approximation methods for a solvable model. I. Exact solutions and perturbation theory. *Nucl. Phys.*, 62:188, 1965.

[133] N. Meshkov, A. J. Glick, and H. J. Lipkin. Validity of many-body approximation methods for a solvable model. II. Linearization procedures. *Nucl. Phys.*, 62:199, 1965.

[134] A. J. Glick, H. J. Lipkin, and N. Meshkov. Validity of many-body approximation methods for a solvable model. III. Diagram summations. *Nucl. Phys.*, 62:211, 1965.

[135] G. J. Milburn, J. Corney, E. M. Wright, and D. F. Walls. Quantum dynamics of an atomic Bose-Einstein condensate in a double-well potential. *Phys. Rev. A*, 55:4318, 1997.

[136] J. I. Cirac, M. Lewenstein, K. Mølmer, and P. Zoller. Quantum superposition states of Bose-Einstein condensates. *Phys. Rev. A*, 57:1208, 1998.

[137] J. Vidal, G. Palacios, and R. Mosseri. Entanglement in a second-order quantum phase transition. *Phys. Rev. A*, 69:022107, 2004.

[138] J. Vidal, R. Mosseri, and J. Dukelsky. Entanglement in a first-order quantum phase transition. *Phys. Rev. A*, 69:054101, 2004.

[139] S. Dusuel and J. Vidal. Continuous unitary transformations and finite-size scaling exponents in the Lipkin-Meshkov-Glick model. *Phys. Rev. B*, 71:224420, 2005.

[140] J. Vidal, G. Palacios, and C. Aslangul. Entanglement dynamics in the Lipkin-Meshkov-Glick model. *Phys. Rev. A*, 70:062304, 2004.

[141] R. H. Dicke. Coherence in spontaneous radiation processes. *Phys. Rev.*, 93:99, 1954.

[142] N. Lambert, C. Emary, and T. Brandes. Entanglement and the phase transition in single-mode superradiance. *Phys. Rev. Lett.*, 92:073602, 2004.

[143] N. Lambert, C. Emary, and T. Brandes. Entanglement and entropy in a spin-boson quantum phase transition, 2004. quant-ph/0405109.

[144] J. Reslen, L. Quiroga, and N. F. Johnson. Direct equivalence between quantum phase transition phenomena in radiation-matter and magnetic systems: scaling of entanglement. *Europhys. Lett.*, 69:8, 2005.

[145] S. Dusuel and J. Vidal. Finite-size scaling exponents and entanglement in the two-level BCS model. *Phys. Rev. A*, 71:060304, 2005.

[146] R. G. Unayan, C. Ionescu, and M. Fleischhauer. Bi-partite and global entanglement in a many-particle system with collective spin coupling, 2004. quant-ph/0412164.

[147] R. G. Unayan and M. Fleischhauer. Decoherence-free generation of many-particle entanglement by adiabatic ground-state transitions. *Phys. Rev. Lett.*, 90:133601, 2003.

[148] R. B. Laughlin. Anomalous quantum Hall effect: an incompressible quantum fluid with fractionally charged excitations. *Phys. Rev. Lett.*, 50:1395, 1983.

[149] V. Popkov and M. Salerno. Logarithmic divergence of the block entanglement entropy for the ferromagnetic Heisenberg model. *Phys. Rev. A*, 71:012301, 2005.

[150] S. Dusuel and J. Vidal, 2006. In preparation.

[151] D. Aharonov and T. Naveh. Quantum NP – a survey, 2002. quant-ph/0210077.

[152] J. I. Latorre and M. A. Martín-Delgado. The majorization arrow in quantum algorithm design. *Phys. Rev. A*, 66:022305, 2002.

[153] R. Orús, J. I. Latorre, and M. A. Martín-Delgado. Natural majorization of the quantum Fourier transform in phase-estimation algorithms. *Quant. Inf. Proc.*, 4:283, 2003.

[154] R. Orús, J. I. Latorre, and M. A. Martín-Delgado. Systematic analysis of majorization in quantum algorithms. *Eur. Phys. J. D*, 29:119, 2004.

[155] J. Ahn, T. C. Weinacht, and P. H. Bucksbaum. Information storage and retrieval through quantum phase. *Science*, 287:463, 2000.

[156] P. Knight. Quantum information processing without entanglement. *Science*, 287:441, 2000.

[157] R. Jozsa and N. Linden. On the role of entanglement in quantum computational speed-up, 2002. quant-ph/0201143.

[158] S. Parker and M. B. Plenio. Entanglement simulations of Shor's algorithm. *J. Mod. Opt.*, 49:1325, 2002.

[159] V. M. Kendon and W. J. Munro. Entanglement and its role in Shor's algorithm, 2004. quant-ph/0412140.

[160] S. Sachdev. *Quantum Phase Transitions*. Cambridge University Press, Cambridge, 1999.

[161] R. Cleve, A. Ekert, C. Macchiavelo, and M. Mosca. Quantum algorithms revisited. In *Proceedings of the Royal Society of London, Ser. A*, volume 454, page 339, 1998.

[162] A. Galindo and M. A. Martín-Delgado. Information and computation: classical and quantum aspects. *Rev. Mod. Phys.*, 74:347, 2002.

[163] D. N. Page. Average entropy of a subsystem. *Phys. Rev. Lett.*, 71:1291, 1993.

[164] S. Sen. Average entropy of a quantum subsystem. *Phys. Rev. Lett.*, 77:1, 1996.

[165] C. H. Bennett, E. Bernstein, G. Brassard, and U. Vazirani. The strengths and weaknesses of quantum computation. *SIAM J. on Comp.*, 26:1510, 1997.

[166] S. Das, R. Kobes, and G. Kunstatter. Energy and efficiency of adiabatic quantum search algorithms. *J. Phys. A*, 36:1, 2003.

[167] R. Raussendorf and H.-J Briegel. A one-way quantum computer. *Phys. Rev. Lett.*, 86:5188, 2001.

[168] H.-J. Briegel and R. Raussendorf. Persistent entanglement in arrays of interacting particles. *Phys. Rev. Lett.*, 86:910, 2001.

[169] R. Raussendorf and H.-J. Briegel. Computational model for the one-way quantum computer: concepts and summary, 2002. quant-ph/0207183.

[170] J. E. Hirsch. Two-dimensional Hubbard model: numerical simulation study. *Phys. Rev. B*, 31:4403, 1985.

[171] R. M. Noack, S. R. White, and D. J. Scalapino. Correlations in a two-chain Hubbard model. *Phys. Rev. Lett.*, 73:882, 1994.

[172] S. Liang and H. Pang. Approximate diagonalization using the density matrix renormalization-group method: a two-dimensional-systems perspective. *Phys. Rev. B*, 49:9214, 1994.

[173] G. De Chiara, M. Rizzi, D. Rossini, and S. Montangero. Density matrix renormalization group for dummies, 2006. cond-mat/0603842.

[174] J. M. Crawford and L. D. Auton. Experimental results on the crossover point in random 3SAT. *Art. Intel.*, 81:31, 1996.

[175] T. Hogg. Adiabatic quantum computing for random satisfiability problems. *Phys. Rev. A*, 67:022314, 2003.

[176] M. Suzuki. Fractal decomposition of exponential operators with applications to many-body theories and Monte Carlo simulations. *Phys. Lett. A*, 146:319, 1990.

[177] M. Suzuki. General theory of fractal path integrals with applications to many-body theories and statistical physics. *J. Math. Phys.*, 32:400, 1991.

[178] A. T. Sornborger and E. D. Stewart. Higher-order methods for quantum simulations. *Phys. Rev. A*, 60:156, 1999.

[179] A. M. Childs, R. Cleve, E. Deotto, E. Farhi, S. Gutmann, and D. A. Spielman. Exponential algorithmic speedup by quantum walk. In *Proceedings of the 35th ACM Symposium on Theory of Computing (STOC)*, page 59, 2003.

[180] N. Shenvi, J. Kempe, and K B. Whaley. A quantum random walk search algorithm. *Phys. Rev. A*, 67:052307, 2003.

[181] E. Bernstein and U. Vazirani. Quantum complexity theory. *SIAM J. on Comp.*, 26:1411, 1997.

[182] M. Mosca. *Quantum Computer Algorithms*. PhD thesis, University of Oxford, 1999.

[183] A. Y. Kitaev. Quantum measurements and the abelian stabilizer problem, 1995. quant-ph/9511026.

[184] A. Galindo and M. A. Martín-Delgado. A family of Grover's quantum searching algorithms. *Phys. Rev. A*, 62:62303, 2001.

[185] D. Deutsch. Quantum theory, the Church-Turing principle and the universal quantum computer. In *Proceedings of the Royal Society of London, Ser. A*, volume 400, page 97, 1985.

[186] Y. Aharonov, L. Davidovich, and N. Zagury. Quantum random walks. *Phys. Rev. A*, 48:1687, 1993.

[187] D. Aharonov, A. Ambainis, J. Kempe, and U. Vazirani. Quantum walks on graphs. In *Proceedings of the 33rd ACM Symposium on the Theory of Computing*, page 50, 2001.

[188] A. Ambainis, E. Bach, A. Nayak, A. Vishwanath, and J. Watrous. One-dimensional quantum walks. In *Proceedings of the 33rd ACM Symposium on the Theory of Computing*, page 37, 2001.

[189] E. Farhi and S. Gutmann. Quantum computation and decision trees. *Phys. Rev. A*, 58:915, 1998.

[190] A. M. Childs, E. Farhi, and S. Gutmann. An example of the difference between quantum and classical random walks. *Quant. Inf. Proc.*, 1:35, 2002.

[191] J. Kempe. Quantum random walks hit exponentially faster. *Prob. Theor. and Related Fields*, 133:215, 2005.

[192] J. Kempe. Quantum random walks – an introductory overview. *Contemp. Phys.*, 44:307, 2003.

[193] M. R. Garey and D. S. Johnson. *Computers and Intractability. A Guide to the Theory of NP-Completeness*. W. H. Freeman and Company, New York, 1979.

[194] C. H. Papadimitriou. *Computational Complexity*. Addison-Wesley, New York, 1994.