Instituto Potosino de Investigación Científica y Tecnológica

Posgrado en Ciencias Aplicadas

Enhancement of Entanglement using a Tight-Binding Hamiltonian

Tesis que presenta

Jorge Carlos Navarro Muñoz

Para obtener el grado de

Maestro en Ciencias Aplicadas

En la opción de

Nanociencias y Nanotecnología

Codirectores de Tesis

Dr. Román López-Sandoval
Dr. Haret-Codratian Rosu Barbus

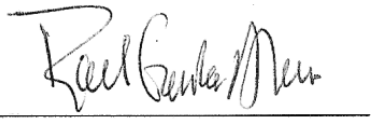
San Luis Potosí, S.L.P., Febrero 2006

La tesis "**Enhancement of Entanglement using a Tight-Binding Hamiltonian**" presentada para obtener el Grado de Maestro en Ciencias Aplicadas en la opción de Nanociencias y Nanotecnología fue elaborada por **Jorge Carlos Navarro Muñoz** y aprobada el **22 de Febrero de 2006** por los suscritos, designados por el Colegio de Profesores de la División de Materiales Avanzados para la Tecnología Moderna del Instituto Potosino de Investigación Científica y Tecnológica, A.C.

Dr. Román López Sandoval
Codirector de la tesis

Dr. Haret C. Rosu Barbus
Codirector de la tesis

Dr. Florentino López Urías
Asesor



Dr. Raúl Garibay Alonso
Asesor externo

IPICYT

Instituto Potosino de Investigación Científica y Tecnológica, A.C.

Acta de Examen de Grado

COPIA CERTIFICADA

El Secretario Académico del Instituto Potosino de Investigación Científica y Tecnológica, A.C., certifica que en el Acta 015 del Libro Primero de Actas de Exámenes de Grado del Programa de Maestría en Ciencias Aplicadas en la opción de Nanociencias y Nanotecnología está asentado lo siguiente:

En la ciudad de San Luis Potosí a los 22 días del mes de febrero del año 2006, se reunió a las 17:00 horas en las instalaciones del Instituto Potosino de Investigación Científica y Tecnológica, A.C., el Jurado integrado por:

Dr. Haret-Codratian Rosu Barbus	**Presidente**	**IPICYT**
Dr. Raúl Garibay Alonso	**Secretario**	**UASLP**
Dr. Florentino López Urías	**Sinodal**	**IPICYT**
Dr. Román López Sandoval	**Sinodal**	**IPICYT**

a fin de efectuar el examen, que para obtener el Grado de:

MAESTRO EN CIENCIAS APLICADAS
EN LA OPCIÓN DE NANOCIENCIAS Y NANOTECNOLOGÍA

sustentó el C.

Jorge Carlos Navarro Muñoz

sobre la Tesis intitulada:

Enhancement of Entanglement using a Tight-Binding Hamiltonian

que se desarrolló bajo la dirección de

Dr. Haret-Codratian Rosu Barbus
Dr. Román López Sandoval

El Jurado, después de deliberar, determinó

APROBARLO

Dándose por terminado el acto a las 18:30 horas, procediendo a la firma del Acta los integrantes del Jurado. Dando fé el Secretario Académico del Instituto.

A petición del interesado y para los fines que al mismo convengan se extiende el presente documento en la ciudad de San Luis Potosí, S.L.P., México, a los 22 días del mes febrero de 2006.

Dr. Marcial Bonilla Marín
Secretario Académico

INSTITUTO POTOSINO DE INVESTIGACIÓN CIENTÍFICA Y TECNOLÓGICA, A.C.
IPICYT
SECRETARIA ACADEMICA

L.C.C. Ivonne Lizette Cuevas Velez
Jefa del Departamento de Asuntos Escolares

Esta tesis fue elaborada en la División de Materiales Avanzados del Instituto Potosino de Investigación Científica y Tecnológica, A.C., bajo la codirección de los doctores Román López Sandoval y Haret C. Rosu Barbus.

Durante la realización del trabajo el autor recibió una beca académica del Consejo Nacional de Ciencia y Tecnología (182532) y del Instituto Potosino de Investigación Científica y Tecnológica, A. C.

To my parents

Acknowledgements

Although this is by no means a complete list, I would like to thank the following which have –in some way or another– contributed to this work:

- My advisors, Drs. Román López Sandoval and Haret C. Rosu Barbus, without whom this work would have not been completed.
- For continuous support during this time: My parents, Pily, University people (IATL, JMSZ, VHCJ, BEHC), older fellows (JMW, BGM) and classmates from the Advanced Materials department in IPICyT.
- My teachers, past and present, good and bad. For I owe you much.
- CONACYT, for economic support via the scholarship 182532.

Contents

Resumen

Debido a la disminución del tamaño en los procesos de fabricación de microchips de computadora, se está llegando a límites físicos donde efectos cuánticos pueden interferir en el desempeño de tales dispositivos. Por otra parte, aun con el poder de cómputo actual el cálculo de sistemas microscópicos es ineficiente.

Para tratar de resolver estos inconvenientes, se ha desarrollado un nuevo modelo computacional que aproveche efectos cuánticos: la *computadora cuántica*. Esto ha dado lugar a nuevos recursos como el *entanglement*, que se define como una correlación especial entre dos sistemas microscópicos. Esta propiedad resulta ser crítica en los procesos involucrados en computación cuántica.

En este trabajo, se utilizó un hamiltoniano tipo *Tight Binding* para estudiar el entanglement en sistemas unidimensionales con y sin desorden, así como la aplicación de un método computacional para optimizar dicha propiedad en sistemas unidimensionales y en redes cuadrada y triangular.

Palabras Clave: Computación Cuántica, Entanglement, Concurrencia, Algoritmos Genéticos.

Abstract

The shrinking processes employed by microchips manufacturers are begining to reach physical limits where quantum effects can seriously impact performance of such devices. On the other hand, even with present-day computing capabilities, exact calculation of microscopic systems is heavily limited.

To try to cope with this issues, a new computational model that takes advantage of quantum effects was developed: the *quantum computer*. This has led to the study of new resources such as *entanglement*, which is defined as a special kind of correlation between microscopic systems. It turns out that this is a key resource in quantum computation processes.

In the present work, a Tight-Binding hamiltonian was used in order to study entanglement on one dimensional systems with and without disorder, as well as the application of a computational method to optimize such property on one dimensional systems and square and triangular lattices.

Key Words: Quantum Computation, Entanglement, Concurrence, Genetic Algorithms.

Chapter 1

Basic Concepts on Quantum Computation

Contents

Have a friend, calls me up
Says hello, then hangs up
He must have read my mind
These are the days of a different paradigm
Maybe once, even twice
He said "God does not play dice "
Yet if he's everywhere
He's in casinos with aces to spare.
Tears For Fears

1.1 Foreword

Quantum Computation and Quantum Information are relatively new fields which make use of quantum mechanical processes to accomplish information processing tasks. It is believed that this fields will eventually allow certain problems to be solved in times that are currently prohibitive on classical computers.

One of the key concepts in these disciplines –and this work– is the so-called *entanglement*, which is a set of states where special correlations arise. This correlations allow entangled systems to affect each other without the presence of a physical link (a phenomena that Prof. Albert Einstein would famously describe as "spooky action at a distance").

The present work deals with disordered systems and their capacity to display this behavior.

1.2 Computer Science

The modern incarnation of computer science was announced by the great mathematician Alan Turing [2] in a remarkable 1936 paper. Turing showed that there is such a thing as a 'Universal Turing Machine' that can be used to simulate any other Turing machine (see the "*Notes*" Appendix). Moreover, he claimed that, if an algorithm can be performed on any piece of hardware (say, a modern personal computer), then there is an equivalent algorithm of a Universal Turing Machine which performs exactly the same task as the algorithm running on the personal computer. This assertion, known as the Church-Turing thesis, asserts the equivalence between the physical concept of what class of algorithms can be performed on some physical device with the rigorous mathematical concept of a Universal Turing Machine.

In the late 1960s and early 1970s, it seemed as though the Turing Machine was at least as powerful as any other model of computation. This observation was codified into a strengthened version of the Church-Turing thesis:

> "Any algorithmic process can be simulated efficiently using a Turing Machine"

The first major challenge to the strong Church-Turing thesis arose in the mid 1970s. Robert Solovay and Volker Strassen showed that it is possible to test whether an integer is prime or composite using a randomized algorithm (i.e. randomness is an essential part of the algorithm). This algorithm can determine that a number was *probably* prime or else composite, and by repeating the test a few times it is possible to reach a conclusion with near certainty.

The Strong Church-Turing thesis, lacking randomness, was promptly fixed making a slight modification:

> "Any algorithmic process can be simulated efficiently using a *probabilistic* Turing Machine"

Yet, uncertainty arose of whether it could exist another set of problems not efficiently solved by the Turing Machine. Even more importantly, could it be that there is some another model of computation that efficiently solves such kind of problems?

On the other hand, since the development of the transistor in 1947 computer hardware has grown in power at an amazing speed. However, quantum effects are beginning to interfere in the functioning of electronic devices as they are made smaller and smaller (At the time of writing this document, actual computer processors are manufactured using 90 nm and even 65nm technology, with recent claims stating the beginning of a new process to develop 45 nm chips tentatively in 2007).

Motivated by this issues, in 1985 David Deutsch wondered whether the laws of physics could be used to derive an even stronger version of the Church-Turing thesis [3]. Deutsch looked to physical theory to provide a foundation for the Church-Turing thesis that would be as secure as the status of that physical theory. In particular, Deutsch attempted to define a computational device that would be capable of efficiently simulate an arbitrary physical system. Because the laws of physics are ultimately quantum mechanical, he was naturally led to consider computing devices based on the principles of quantum mechanics.

In 1994 Peter Shor demonstrated that two enormously important problems —finding the prime factors of an integer, and the so-called 'discrete

logarithm' problem— could be solved efficiently if performed on a quantum computer [4]. Other evidence for the power of quantum computers came in 1996 when Lov Grover showed that another important problem —conducting a search through some unstructured search space— could also be sped up by a quantum computer [5].

Following an idea of Richard Feynman, it is likely that one of the major applications of quantum computers in the future will be performing simulations of quantum mechanical systems too difficult to simulate on a classical computer [6].

At this point, though, we do not know what other problems can be solved on a quantum computation as it is not easy to come up with good quantum algorithms. One of the reasons for this is that, to design good quantum algorithms one must turn off the 'classical' intuition for at least part of the design process, using truly quantum effects to achieve the desired algorithmic end. Moreover, it is not enough to design an algorithm that is merely quantum mechanical: the algorithm must be *better* that any existing classical algorithm.

1.3 Quantum Qubits

The bit is the fundamental concept of classical computation. Quantum computation and quantum information are built upon an analogous concept, the **quantum bit**, or **qubit**. For the most part qubits are treated as abstract mathematical objects although they can be realized as actual physical systems (including quantum dots [7], nuclear magnetic resonance [8], photons [9] and trapped ions [10]).

Just as a classical bit has a *state* —either 0 or 1— a qubit also has a state. Two possible states for a qubit are the states $|0\rangle$ and $|1\rangle$. Notation like '$|\ \rangle$' is called the Dirac notation and it is the standard notation for states in quantum mechanics. The difference between bits and qubits is that a qubit can be in a state other than $|0\rangle$ or $|1\rangle$, that is, it is also possible to form linear combinations of states, often called *superpositions*:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle. \tag{1.1}$$

The numbers α and β are complex numbers. The special states $|0\rangle$ and $|1\rangle$ are known as *computational basis* states, and form an orthonormal basis for this vector space. We cannot examine a qubit to determine its quantum state, that is, the values of α and β. Instead, when we measure a qubit we get *either* the result 0, with probability $|\alpha|^2$, or the result 1 with probability $|\beta|^2$. Naturally, $|\alpha|^2 + |\beta|^2 = 1$, since the probabilities must sum

to one. Thus, in general a qubit's state is a unit vector in a two-dimensional complex vector space.

Contrary to the classical world where discrete states are accessible (think about a light bulb), a qubit can exist in a continuum of states between $|0\rangle$ and $|1\rangle$ *until* it is observed, when it becomes either one. Furthermore, *measurements change the state of a qubit, collapsing it from its superposition of* $|0\rangle$ *and* $|1\rangle$. In other words, if measurement gives $|0\rangle$, then post-measurements will always yield $|0\rangle$.

1.4 Multiple Qubits

If we had two classical bits, then there could be four possible states: 00, 01, 10 and 11. In the same fashion, a two qubit system has four computational basis states denoted $|00\rangle$, $|01\rangle$, $|10\rangle$ and $|11\rangle$. A pair of qubits can also exist in superpositions of these four states, so the quantum state of two qubits involves a complex coefficient —sometimes called an *amplitude*—, such that the vector describing the two qubits is

$$|\psi_{\text{two qubits}}\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle \tag{1.2}$$

or, in matrix representation:

$$\alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle = \begin{pmatrix} \alpha_{00} \\ \alpha_{01} \\ \alpha_{10} \\ \alpha_{11} \end{pmatrix}. \tag{1.3}$$

As before, measurement result x (i.e. result 00, 01, 10 or 11) occurs with probability $|\alpha_x|^2$, with the state of the qubits after the measurement being $|x\rangle$. The condition that probabilities must sum to one remains. These *normalization* condition is expressed as $\sum_x |\alpha_x|^2 = 1$.

In a system such as this (with only two qubits), we could measure just a subset of the qubits. Measuring only the first qubit gives 0 with probability $|\alpha_{00}|^2 + |\alpha_{01}|^2$ leaving the state as

$$|\psi'\rangle = \frac{\alpha_{00}|00\rangle + \alpha_{01}|01\rangle}{\sqrt{(|\alpha_{00}|^2 + |\alpha_{01}|^2)}}. \tag{1.4}$$

Note that in order to fulfill the normalization condition, the denominator must be introduced for this post-measurement state.

One important two qubit state is the *Bell State* or *Einstein-Podolsky-Rosen* (EPR) *Pair*

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}}. \tag{1.5}$$

Suppose that, upon measurement of the first qubit, we obtained the 0 result out of the Bell State. The post-measurement state would then become $|00\rangle$. In this case, *we already know that measuring the second qubit will yield* 0 *again*, that is, the measurement results are *correlated*. It was John Bell that proved [11] that measurement correlations in the Bell state are stronger than it could ever exist between classical systems.

Three extra special states considered Bell States also exist. They are briefly discussed in the *Dense Coding* section and the "Quantum Circuits Overview" Appendix.

1.5 Quantum Mechanics Postulates

As it has already been mentioned, Quantum Mechanics does not tell what laws a physical system must obey, but it does provide a mathematical and conceptual framework for the development of such laws. What follows is a basic overview of the Postulates of Quantum Mechanics (for a quick introduction to linear algebra concepts used, please go to the "Linear Algebra" Appendix).

1.5.1 The First Postulate: The State Space

The first Postulate states that there is a complex vector space with an inner product associated to any isolated physical system (or equivalently, a Hilbert space known as the *state space* of the system). The system is completely described by its *state vector*, which is a unit vector in the system's state space.

The simplest quantum mechanical system is the qubit. A qubit has a two-dimensional state space. Suppose $|0\rangle$ and $|1\rangle$ form an orthonormal basis for that state space. Then an arbitrary state vector in the state space can be written in the same way as (1.1), that is:

$$|\psi\rangle = a|0\rangle + b|1\rangle, \tag{1.6}$$

where a and b are complex numbers. The condition that $|\psi\rangle$ be a unitary vector, $\langle\psi|\psi\rangle = 1$, is therefore equivalent to the *normalization condition* already defined for state vectors.

There is an alternate and useful formulation of the state vectors. In this formulation the system is completely described by its **density operator** or **density matrix**.

Suppose a quantum system is in one of a number of states $|\psi_i\rangle$ where i is an index, with respective probabilities p_i. The density operator for the system is defined by the equation

$$\rho \equiv \sum_i p_i |\psi_i\rangle\langle\psi_i| \equiv \sum_i p_i \rho_i. \tag{1.7}$$

It is said that a system is in a *pure state* if it satisfies tr$(\rho^2) = 1$ where tr( ) is the trace operator. A *mixed state* satisfies tr$(\rho^2) < 1$.

This formulation can be applied to the remaining Postulates.

1.5.2 The Second Postulate: Evolution

The second postulate states that the evolution of a *closed* (that is, an isolated) quantum system is described by a *unitary transformation*. This means that a state $|\psi\rangle$ of a system at time t_1 is related to the state $|\psi'\rangle$ of the system at time t_2 by a unitary operator U which depends only on the times t_1 and t_2.

$$|\psi'\rangle = U|\psi\rangle. \tag{1.8}$$

In the case of qubits, any unitary operator can be realized in realistic systems.

In a more refined version of this postulate, the evolution of a quantum system is described in *continuous time* by the Schrödinger equation:

$$i\hbar \frac{d|\psi\rangle}{dt} = H|\psi\rangle. \tag{1.9}$$

In this equation, $\hbar$ is a physical constant known as the *Planck's constant* and H is a fixed Hermitian operator known as the *Hamiltonian* of the closed system.

If the Hamiltonian of the system becomes known, then it is possible to understand the dynamics of this system completely. In general, this is a very difficult problem.

Because the Hamiltonian is a Hermitian operator it has a spectral decomposition given by

$$H = \sum_E E|E\rangle\langle E|, \tag{1.10}$$

with eigenvalues E and corresponding normalized eigenvectors $|E\rangle$. The states $|E\rangle$ are conventionally referred to as *energy eigenstates*, and E is

the *energy* of the state $|E\rangle$. The lowest energy is known as the *ground state energy* for the system, and the corresponding energy eigenstate is known as the *ground state*.

1.5.3 The Third Postulate: Quantum measurement

The third postulate states that quantum measurements are described by a collection $\{M_m\}$ of *measurement operators*. These are operators acting on the state space of the system being measured. The index m refers to the measurement outcomes that may occur in the experiment. If the state of the quantum system is $|\psi\rangle$ immediately before the measurement, then the probability that result m occurs is given by

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

and the state of the system after the measurement is

$$\frac{M_m|\psi\rangle}{\sqrt{\langle\psi|M_m^\dagger M_m|\psi\rangle}}, \tag{1.12}$$

where the denominator is introduced to satisfy the normalization condition.

The measurement operators satisfy the *completeness equation*,

$$\sum_m M_m^\dagger M_m = I. \tag{1.13}$$

The completeness equation expresses the fact that probabilities sum to one:

$$\begin{array}{rcl} \sum_m M_m^\dagger M_m & = & I \\ \langle\psi|\left(\sum_m M_m^\dagger M_m\right)|\psi\rangle & = & \langle\psi|I|\psi\rangle \\ \sum_m \langle\psi|M_m^\dagger M_m|\psi\rangle & = & \langle\psi|\psi\rangle \\ \sum_m p(m) & = & 1. \end{array} \tag{1.14}$$

1.5.4 The Fourth Postulate: Composite Systems

The fourth Postulate states that the state space of a composite physical system is the tensor product of the state spaces of the component physical systems. Moreover, if we have systems numbered 1 through n, and any system i is prepared in a state $|\psi_i\rangle$, then the joint state of the total system is $|\psi_1\rangle \otimes |\psi_2 \otimes, \ldots, \otimes |\psi_n\rangle$.

Postulate 4 also enables us to define one of the most interesting and puzzling ideas associated with composite quantum systems- **entanglement**. A detailed definition of this concept –as well as its importance and various examples– will be discussed thoroughly in further sections.

1.6 Entanglement

1.6.1 Definition of Entanglement

Consider the two qubit state

$$|\psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}. \tag{1.15}$$

This state has the remarkable property that there are not single qubit states $|a\rangle$ and $|b\rangle$ such that $|\psi\rangle = |a\rangle|b\rangle$. As a proof, consider that such states exist. Then

$$|a\rangle|b\rangle = (\alpha|a_1\rangle + \beta|a_2\rangle)(\gamma|b_1\rangle + \delta|b_2\rangle) = \frac{|00\rangle + |11\rangle}{\sqrt{2}} \tag{1.16}$$

$$= \alpha\beta|a_1b_1\rangle + \alpha\delta|a_1b_2\rangle + \beta\gamma|a_2b_1\rangle + \beta\delta|a_2b_2\rangle. \tag{1.17}$$

One of these states must be $|00\rangle$. Suppose that $|a_1\rangle = |b_1\rangle = |0\rangle$:

$$\alpha\gamma|00\rangle + \alpha\delta|0b_2\rangle + \beta\gamma|a_20\rangle + \beta\delta|a_2b_2\rangle. \tag{1.18}$$

The middle states cannot be $|11\rangle$, so $|a_2\rangle = |b_2\rangle = 0$. In that case

$$|a\rangle|b\rangle = \alpha\gamma|00\rangle \neq \frac{|00\rangle + |11\rangle}{\sqrt{2}}. \tag{1.19}$$

Composite systems that cannot be written as a product of states of its component systems are called *entangled* states, as seen in the example above.

A pure state of a pair of quantum systems is called entangled if it is unfactorizable, as in the case of the Bell States. A mixed state is entangled if it cannot be factorizable into pure states.

Entanglement is also regarded as the potential of quantum states to exhibit correlations that cannot be accounted for classically [12].

A very important tool that helps us to clarify the idea of Entanglement is the Schmidt Decomposition. It is presented as the following theorem:

The Schmidt Decomposition 1.6.1 *Suppose $|\psi\rangle$ is a pure state of a composite system, AB. Then there exist orthonormal states $|i_A\rangle$ for system A and orthonormal states $|i_B\rangle$ for system B such that*

$$|\psi\rangle = \sum_i \lambda_i |i_A\rangle|i_B\rangle \tag{1.20}$$

where λ_i are non-negative real numbers satisfying $\sum_i \lambda_i^2 = 1$ known as the Schmidt coefficients or Schmidt numbers.

This is a very important result as many interesting properties of quantum-mechanical systems are completely determined by the eigenvalues of the reduced density operator (in this case, the Schmidt coefficients). The Schmidt numbers can be used to identify entangled states and quantify the degree of entanglement using the formula for the *Entropy of Entanglement* between two systems A and B.

This formula states that for each pure state, the Entropy of Entanglement E is defined as the entropy of one of the subsystems A or B [14]:

$$E(|\Psi\rangle) = -\mathrm{tr}(\rho_A \log_2 \rho_A) = -\mathrm{tr}(\rho_B \log_2 \rho_B) \tag{1.21}$$

where ρ_x is the partial trace of $|\Psi\rangle\langle\Psi|$ over subsystem x. Using the Schmidt decomposition:

$$\rho_A = \mathrm{tr}_B(\sum_i \lambda_i^2 |i_A\rangle|i_B\rangle\langle i_A|\langle i_B|) \tag{1.22}$$

$$= \sum_i \lambda_i^2 |i_A\rangle\langle i_A|. \tag{1.23}$$

It is remarkable that this formula requires both the Schmidt Decomposition and the complete knowledge of the wave function $|\Psi\rangle$. This makes it a complicated calculation of entanglement.

However, there is an alternative way to calculate entanglement [15]. This explicit formula makes use of a quantity called *Concurrence*, which shall be discussed in the “Measuring Entanglement” section.

A couple of strange effects of entanglement are superdense coding and the violation of Bell’s inequality. It also makes it possible to “teleport” quantum states. Details in the following section.

1.6.2 Importance of Entanglement

Entanglement has been seen in recent years as a potentially useful resource. The predicted capabilities of a quantum computer, for example, rely crucially on said resource [16], and a proposed quantum cryptographic scheme converts shared entanglement into a shared secret key [17].

One of the most important application for entanglement between two systems is the transmission of quantum information between them. In particular, a remarkable phenomena called *Quantum Teleportation* will be discussed shortly.

Another example of the use of entanglement between two systems include *Superdense Codification*, which consists of sending two classical

bits manipulating a single qubit. This effect will also be discussed afterwards.

One could be led to believe that the importance of entanglement is limited to quantum computation and quantum information schemes. However, another point of view about unfactorizable or entangled states is that they cannot be represented as a single Slater determinant under any unitary transformation. This naturally relates entanglement with strongly correlated systems. Moreover, the fact that entanglement is a purely quantum-mechanical property makes it ideal for the study of many-body fermionic systems under the influence of quantum fluctuations –that is, close to a quantum phase transition– [18]. That is why a great amount of work is being directed towards using entanglement to characterize quantum phase transitions [19, 20, 21, 22].

Cryptography

In the field of cryptography (that is, doing communication or computation involving two or more parties who may not trust each other) there are two main kinds of cryptosystems, *private key cryptosystems* and *public key cryptosystems*.

The way a private key cryptosystem works is that two parties (enter 'Alice' and 'Bob') wish to communicate by sharing a private key, which only they know. This key is used to encrypt the information to be sent. To recover this information, the same key must be used. However, the key distribution problem is in many cases just as difficult as the original problem of communicating in private.

One of the earliest discoveries in quantum computation and quantum information was that quantum mechanics can be used to do key distribution in such a way that Alice and Bob's security cannot be compromised [23]. This is known as quantum cryptography or quantum key distribution. In this way, the presence of an undesired listener will be discovered by Alice and Bob, who can then stop communicating.

The second major type of cryptosystem is the public key cryptosystem. In this kind of system, a public key is available to the general public. One of the parties can make use of this public key to encrypt a message. What is important is that nobody else can make use of the public key to decrypt the message. In order to decrypt the message, it is necessary to own a *secret* key. Theoretically one could use the public key to decipher the message, but the encryption transformation is chosen in such a very clever and non-trivial way that it is extremely difficult to invert the encryption using only the public key.

Nowadays the most widely deployed public key cryptosystem is the RSA cryptosystem, which is believed to offer a fine balance of security and practical usability. It turns out that inverting the encryption stage of RSA is a problem closely related to factoring so that Shor's fast algorithm for factoring on a quantum computer could be used to easily break RSA. Although we are years before a large scale quantum computer is built, quantum algorithms have become a serious issue due to the level of compromise it has posed to security systems.

Dense Coding

In 1992 Charles Bennett and Stephen Wiesner explained how to transmit two classical bits of information, while only transmitting one quantum bit from sender to receiver, a result called dense coding [24].

Let us review a quick example that clarifies the concept of dense coding.

Suppose that Alice has to send Bob some information stored in binary form. This means that a string of ones and zeroes has to be sent, for example 01110010 (which represents the decimal number 114 or the ASCII character 'r'). Previously Bob or some other third party has prepared the Bell State (1.5),

$$\mathrm{B}_{00} = \frac{(|00\rangle + |11\rangle)}{\sqrt{2}} \tag{1.24}$$

and the first qubit has been sent to Alice. Then Alice is able to turn the original (1.24) state into one of a four–element set catalogued as **Bell States Set** through Pauli Operators (Pauli Operators are defined in the "General Mathematical Concepts" Appendix. Explicit construction of the Bell States can be found in the "Quantum Circuits Overview" Appendix):

$$I \otimes I\left(\mathrm{B}_{00}\right) = \frac{(|00\rangle + |11\rangle)}{\sqrt{2}} = \mathrm{B}_{00} \tag{1.25}$$

$$Z \otimes I\left(\mathrm{B}_{00}\right) = \frac{(|00\rangle - |11\rangle)}{\sqrt{2}} = \mathrm{B}_{01} \tag{1.26}$$

$$X \otimes I\left(\mathrm{B}_{00}\right) = \frac{(|01\rangle + |10\rangle)}{\sqrt{2}} = \mathrm{B}_{10} \tag{1.27}$$

$$\imath Y \otimes I\left(\mathrm{B}_{00}\right) = \frac{(|01\rangle - |10\rangle)}{\sqrt{2}} = \mathrm{B}_{11}. \tag{1.28}$$

Therefore, in our early example, Alice could apply the Z, $\imath Y$, I and X operator on her four qubits and then send them to Bob. As it can be easily

seen, the Bell Set forms a basis (the set is linearly independent and spans the $\mathbf{C}^4$ space) so it can be measured by operators with the form $|B_{xy}\rangle\langle B_{xy}|$. In principle, Bob could distinguish that Alice has just send him the B_{01}, B_{11}, B_{00} and B_{10} Bell States corresponding to the information strings 01, 11, 00 and 10, respectively. In the end, this pieces can be concatenated to form the original 01110010 string.

Experimental evidence of this technique has already been demonstrated [25] although only partial identification of the Bell States was possible, rendering a 1.58 codification instead of the expected 2 ratio.

Quantum Teleportation

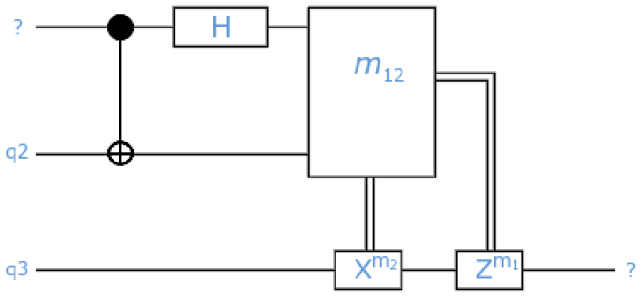


Figure 1.1: Schematic Quantum Circuit for teleporting an unknown qubit (top) using two entangled qubits in the possesion of Alice (qubit q_2) and Bob (qubit q_3). The box labeled "m_{12}" is a measurement over the first two qubits. The X Pauli Operator is applied if the second qubit yields 1 and then the Z Operator is applied if the first qubit yields 1.

This is an example that shows how entanglement plays a critical role in a potential application on quantum computation: Quantum Teleportation. Quantum teleportation is a technique for moving quantum states around, even in the absence of a quantum communications channel [26].

It is recommended to check the "Quantum Circuits Overview" Appendix for information about the different Quantum Gates which will be used in this section.

Here's how it works. Suppose Alice and Bob generated an EPR pair and took one qubit of the pair. Alice has to deliver some unknown state $|\psi\rangle$ to Bob but they live far apart now. Alice must make use of quantum teleportation to solve the problem. The steps of the solution are as follows: Alice interacts the qubit $|\psi\rangle$ with her half of the EPR pair, and then measures the two qubits in her possession, obtaining one of four possible classical results, 00, 01, 10 and 11. She sends this information to Bob. Depending on Alice's classical message, Bob performs one of four operations

on his half of the EPR pair. By doing this he can recover the original state $|\psi\rangle$. The quantum circuit for quantum teleportation is shown in figure 1.1. The state to be teleported is $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, where α and β are unknown amplitudes. The state input into the circuit $|\psi_0\rangle$ is

$$|\psi_0\rangle = |\psi\rangle|\beta_{00}\rangle = \frac{1}{\sqrt{2}}[\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|00\rangle + |11\rangle)] \tag{1.29}$$

where we use the convention that the first two qubits (on the left) belong to Alice (the first from the unknown input and the second from the first part of the EPR pair), and the third qubit to Bob. Alice sends her qubits through a CNOT gate, obtaining

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}[\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|10\rangle + |01\rangle)] \tag{1.30}$$

She then sends the first qubit through a Hadamard gate, obtaining

$$|\psi_2\rangle = \frac{1}{2}[\alpha(|0\rangle + |1\rangle)(|00\rangle + |11\rangle) + \beta(|0\rangle - |1\rangle)(|10\rangle + |01\rangle)] \tag{1.31}$$

This state may be re-written in the following way

$$\begin{aligned}
|\psi_2\rangle =& \frac{1}{2}[\alpha(|0\rangle + |1\rangle)(|00\rangle + |11\rangle) + \beta(|0\rangle - |1\rangle)(|10\rangle + |01\rangle)] && (1.32)\\
=& \frac{1}{2}[\alpha(|000\rangle + |011\rangle + |100\rangle + |111\rangle) + \beta(|010\rangle + |001\rangle \\
& - |110\rangle - |101\rangle)] && (1.33)\\
=& \frac{1}{2}[\alpha|000\rangle + \beta|001\rangle + \alpha|100\rangle - \beta|101\rangle + \alpha|111\rangle - \beta|110\rangle \\
& + \alpha|011\rangle + \beta|010\rangle] && (1.34)\\
=& \frac{1}{2}[|00\rangle(\alpha|0\rangle + \beta|1\rangle) + |10\rangle(\alpha|0\rangle - \beta|1\rangle) + |11\rangle(\alpha|1\rangle - \beta|0\rangle) \\
& + |01\rangle(\alpha|1\rangle + \beta|0\rangle)]. && (1.35)
\end{aligned}$$

This expression naturally breaks down into four terms. The first term has Alice's qubits in the state $|00\rangle$, and Bob's qubit in the state $\alpha|0\rangle + \beta|1\rangle$ —which is the original state $|\psi\rangle$. If Alice performs a measurement and obtains the result 00 then Bob's system will be in the state $|\psi\rangle$. In the same manner, from the other results of Alice's measurement, we are able to know what the state of Bob's system is:

$$\begin{aligned}
00 &\rightarrow |\psi_3(00)\rangle \equiv [\alpha|0\rangle + \beta|1\rangle] && (1.36)\\
01 &\rightarrow |\psi_3(01)\rangle \equiv [\alpha|1\rangle + \beta|0\rangle] && (1.37)\\
10 &\rightarrow |\psi_3(10)\rangle \equiv [\alpha|0\rangle - \beta|1\rangle] && (1.38)\\
11 &\rightarrow |\psi_3(11)\rangle \equiv [\alpha|1\rangle - \beta|0\rangle]. && (1.39)
\end{aligned}$$

Depending on the outcome of Alice's measurement, Bob's qubit will end up in one of these four possible states. Of course, to know which state it is in, Bob must be told the result of Alice's measurement (notice that this fact prevents teleportation from being used to transmit information faster than light). Once Bob has learned the measurement outcome, Bob can 'fix up' his state, recovering $|\psi\rangle$, by applying the appropriate quantum gate. For example, if the measurement yields 00, Bob doesn't need to do anything. If the measurement is 01 then Bob has to apply the X gate; if it is 10 then he must apply the Z gate and finally if it is 11 he has to apply the Z gate and then the X gate.

It may be argued that teleportation appears to create a copy of the quantum state being teleported. This is not the case, as only the target qubit is left in the state $|\psi\rangle$, and the original data qubit ends up in one of the computational basis $|0\rangle$ or $|1\rangle$.

Summarizing, sending quantum information using only a classical channel is impossible. This issue is tackled simply by using the help of an entangled state.

1.6.3 Measuring Entanglement

Due to its importance, entanglement is a resource that must be carefully quantified.

In the last few years a lot of work has been devoted to finding quantative measures of entanglement, particularly for mixed states of a bipartite system [27]. Perhaps the most basic of these measures is the *entanglement of formation*, which is intended to quantify the resources needed to create a given entangled state .

The formula for the entanglement of formation of a mixed state ρ of two qubits for a general density matrix is [15]:

$$E(\rho) = \mathrm{E}(C(\rho)) \tag{1.40}$$

where function $\mathrm{E}(C(\rho))$ is defined as:

$$\begin{array}{rcl} \mathrm{E}(C) & = & h(\frac{1+\sqrt{1-C^2}}{2}); \\ h(x) & = & -x\log_2 x - (1-x)\log_2(1-x) \end{array} \tag{1.41}$$

and C is the quantity known as **Concurrence**. Concurrence is an *Entanglement Monotone* in its own right (i.e. positive or zero for any density matrix ρ; 0 for factorizable states and 1 for the Bell States):

$$C(\rho) = \max\{0, \lambda_1 - \lambda_2 - \lambda_3 - \lambda_4\}. \tag{1.42}$$

In this last formula the λ coefficients are the square roots of the eigenvalues of the non-Hermitian matrix $\rho_A\tilde{\rho_A}$, in decreasing order. The formula applies over the density matrix of the subsystem with the pair of qubits (ρ_A =tr$_B(\rho)$).

To construct the density matrix $\tilde{\rho}$ it is necessary to make use of the *spin flip* transformation defined as

$$\tilde{\rho_A} = \big(\sigma_y \otimes \sigma_y\big)\rho_A^*\big(\sigma_y \otimes \sigma_y\big). \tag{1.43}$$

In this case σ_y is the Pauli Operator Y.

Chapter 2

Genetic Algorithms

Contents

2.1 Genetic Algorithms Overview

The advent of electronic computers has undoubtly been one of the most revolutionary developments in the history of science and technology. This revolution is profoundly increasing our ability to predict and understand nature in ways that were barely conceived even half a century ago.

The earliest computer scientists (Alan Turing, John von Neumann and Norbert Wiener, among others) were motivated in large part by visions of imbuing computer programs with intelligence, with the life-like ability to self-replicate, and with the adaptive capability to learn and to control their environments. These early pioneers of computer science were as much interested in biology and psychology as in electronics, and they looked to natural systems as a guidance for how to achieve their visions. It should be no surprise, then, that from the earliest days computers were applied to model the brain, trying to mimic human learning and simulating biological evolution. A couple of those biologically motivated computing activities have recently undergone an important resurgence: the field of neural networks, and what is now called “evolutionary computation”, of which genetic algorithms are the most prominent example.

2.2 A (very) brief history of genetic algorithms

In the 1950s and the 1960s several computer scientists independently studied evolutionary systems with the idea that evolution could be used as an optimization tool for engineering problems. The main idea in all these systems was to evolve a population of candidate solutions to a given problem, using operators inspired by natural genetic variation and natural selection.

Genetic Algorithms (GAs) were invented by John Henry Holland in the 1960s and were developed by Holland and his students and colleagues at the University of Michigan in the 1960s and the 1970s. Holland’s goal was not to design algorithms to solve specific problems, but rather to formally study the phenomenon of adaptation as it occurs in nature and to develop ways in which the mechanisms of natural adaptation might be imported into computer systems. Holland’s 1975 book *Adaptation in Natural and Artificial Systems* presented the genetic algorithm as an abstraction of biological evolution and gave a theoretical framework for adaptation under the GA.

Much alike nature, Holland’s GA is a method for moving from one population of “chromosomes” (e.g. strings of characters or numbers) to a new

population by using a kind of “natural selection” together with the genetics-inspired operators of crossover, mutation and inversion (this last operator is rarely used nowadays).

2.3 Genetic Pseudo-Algorithm

Given a clearly defined problem to be solved and a representation for candidate solutions, a simple GA works as follows:

1. Start with a randomly generated population of *n* chromosomes (called **Encoded Candidate Solutions**).

2. Repeat the following steps until a **Terminating Condition** is met:

    - Calculate the **Fitness** of each of the n chromosomes in the population
    - Until *n* offsprings have been created:
        - Select a pair of chromosomes from the present population using some **Selection Method**.
        - Apply the **Crossover Operator** to the pair of chromosomes with probability p_c.
        - Apply the **Mutation Operator** to the pair of chromosomes with probability p_m.
    - Replace the present population with the newly created offsprings.

Each iteration of this process is called a generation.

2.4 Genetic Terms and Operators in Detail

2.4.1 Encoded Candidate Selection

The way in which candidate solutions are encoded is a crucial point in the success of a Genetic Algorithm.

Most GA applications use fixed-length chromosomes although this is not a condition.

Binary Encodings

The most common encoding of solutions are the *Binary Encodings*. One of the reason for this is historical as the early work by Holland concentrated in such encoding. Holland gave theoretical justification for using Binary Encodings although this justification is only valid if *Schema* Analysis is taken into account (*Schemas* are common pieces of chromosomes that appear in individuals with high fitness). This analysis, however has been questioned [29, 30, 31] and for some problems, Binary Encodings are unnatural and not very effective (for example, when encoding real-valued parameters).

Many-Character and Real-Valued Encodings

For many applications, it is more natural to use an alphabet of many characters or real numbers to form chromosomes. Holland's schema argument seems to imply that GAs should exhibit worse performance on multiple-character encodings than on binary encodings. However, in the end, the performance depends very much on the problem and the details of the GA being used, and at present there are no rigorous guidelines for predicting which encoding will work best.

Later on, it will be clear that the present work is better represented encoding solutions as collections of real numbers.

2.4.2 Fitness

The fitness function evaluates each chromosome and gives a relative value of how good a solution it is. The fitness value can be used to maximize some value (for example, finding maxima of a given function) or to minimize some value (for example, finding the minimum potential energy for some molecule configuration).

In order to evaluate the fitness value of each individual, a decoding function will be necessary to translate the values stored in the chromosome to usable information (for example, translating from a binary base to a decimal one).

2.4.3 Terminating Conditions

Terminating Conditions include: running time, number of generations, desired fitness and relative change of fitness between generations. Find-

ing an appropriate Termination Condition is no easy task and several tries may be necessary.

2.4.4 Selection Method

Different Selection Methods have been proposed, each one claiming different advantages.

Fitness-Proportionate Selection

Holland's original approach was to select individuals with probability proportionate to its fitness value. The so-called "Roulette Wheel" consisted in spinning an imaginary roulette, divided in as many pieces as the number of the population. The fitter individuals received a bigger piece of the roulette, so there would be more chance in selecting them. A random number between 0 and the total sum of the generation's fitness is picked and the 'wheel' is spun. Fitness of individuals is then summed iteratively until such sum exceeds the random number, returning the index of the selected chromosome.

Sigma Scaling

In the beginning of the search it is probable that there are some individuals *much* fitter than the rest of the population. Under fitness-proportionate selection, this individuals and their descendents will multiply quickly not allowing the potential exploration of initially less fitting roads. This is known as "premature convergence". Later in the search, when all individuals are very similar, there are no great fitness differences for selection to exploit, and the evolution grinds to a near halt.

To address such problems, GA researches have experimented with several "scaling" methods. Under sigma scaling, the expected value of an individual is a function of its fitness ($f(i)$), the population mean ($\overline{f}(t)$), and the population standard deviation ($\sigma(t) = \sqrt{\langle \overline{f}(t)^2 \rangle - \langle \overline{f}(t) \rangle^2}$).

$$\text{Expected Value}(i,t) = \begin{cases} 1 + \frac{f(i) - \overline{f}(t)}{2\sigma(t)} & \text{if } \sigma(t) \neq 0 \\ 1.0 & \text{if } \sigma(t) = 0 \end{cases} \tag{2.1}$$

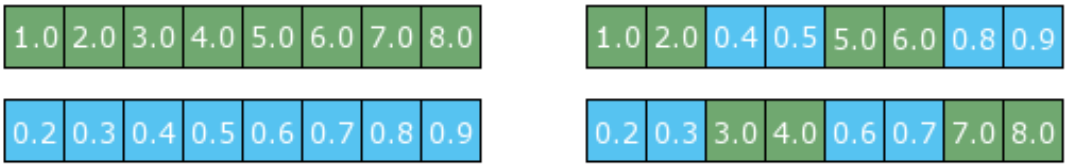


Figure 2.1: Example of 3 point crossover

2.4.5 Crossover Operator

This operator usually takes two chromosomes and creates two offsprings. This is achieved by combining information from the parent chromosomes. Most often there is only one *crossover point*, but various crossover points can be selected too. The parents are crossed with certain probability p_c. A typical value for this parameter is 0.7. In the present work, two types of Crossover Operator were used. The first had only one crossover point, but it was placed randomly along the chromosome. The second had a fixed number of crossover points distributed uniformly.

2.4.6 Mutation Operator

If only the **Crossover Operator** was used, the population would eventually stagnate because only the same pieces of information are exchanged. The **Mutation Operator** is designed to change one specific piece of a chromosome (in biology this piece is called *allele*) with another value. In this way the population is ensured to explore other roads to the solution. A typical value for the mutation probability p_m is 0.001. If this probability raises to high values, there would be no time to explore possible solutions as populations had the tendency to change very fast. Another approach is to dynamically change the value of the mutation probability if differences in individuals become negligible with time.

Figure 2.2: Example of mutation

It's important to note that the Mutation Operator is applied to *every* piece of the chromosome.

Chapter 3

Enhancement of Entanglement

Contents

3.1 Introduction

In earlier sections, entanglement has been described as an important characteristic for quantum information and quantum computation.

In this chapter concurrence, an alternative measure of entanglement, will be studied in various kinds of systems and optimized entangled states will be calculated using genetic algorithms.

3.2 Theory

In this section, the specific formulas for entanglement calculation using concurrence will be deduced.

In the systems about to be studied, qubits are represented by sites in a lattice or a chain. The two computational basis $|0\rangle$ and $|1\rangle$ are represented by occupied and empty sites, respectively.

Using this representation, entanglement can be calculated for different fillings. This approach might be useful for physical experiments involving electron control (e.g. quantum dots [32]).

The electronic system will be described by a tight binding Hamiltonian of the form

$$\hat{H} = \sum_i \varepsilon_i \hat{n}_i + \sum_{\langle ij \rangle} t_{ij} \hat{c}_i^\dagger \hat{c}_j \tag{3.1}$$

where, for simplicity, we will consider spinless electrons. In (3.1) $\hat{c}_i^\dagger$ ($\hat{c}_j$) is the usual creation (annihilation) operator of a spinless electron at site i, whereas $\hat{n}_i = \hat{c}_i^\dagger \hat{c}_i$ is the number operator, and t_{ij} is the hopping integral between nearest-neighbors (NN) and next-nearest-neighbors (NNN) sites i and j. ε_i is the on-site energy for atom i. In general, it is considered that we are working with the same kind of atoms and we take $\varepsilon_i = 0$.

In the first chapter the general formula (1.42) for calculation the concurrence was introduced. First, we have to obtain the density matrix ρ_A for qubits i, j.

3.2.1 The density matrix

The density matrix ρ_A is the trace over system B of all the possible states $|\psi_{AB}\rangle\langle\psi_{AB}|$. The general state function for this system is

$$|\psi_{AB}\rangle = \sum_n \alpha_n |\psi_A\rangle |\psi_B\rangle \tag{3.2}$$

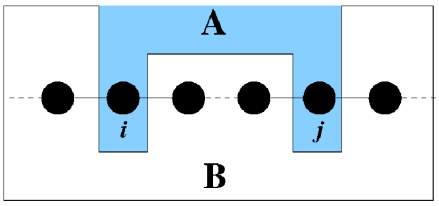


Figure 3.1: Schematic illustration of the partition of the system of interest into two subsystems for the calculation of the concurrence between sites i and j.

where, for a system comprised of N sites, n goes through all the 2^N possible combinations in the computational basis (e.g. $|00\ldots00\rangle \rightarrow |11\ldots11\rangle$). Subsystem A is comprised of the two qubits of interest in the sites i, j (i.e. $|\psi_i\rangle \otimes |\psi_j\rangle$, see also figure 3.1. For a specific system of N sites, there are N_1 occupied and $N - N_1$ not occupied sites. Our two qubit subsystem A has, naturally, four possible states –namely $|00\rangle, |01\rangle, |10\rangle$ and $|11\rangle$– therefore Eq. (3.2) can be decomposed in the following manner

$$|\psi_{AB}\rangle = \sum_m a_m |00\rangle \otimes |\psi_B^m\rangle + \sum_o b_o |01\rangle \otimes |\psi_B^o\rangle + \sum_p c_p |10\rangle \otimes |\psi_B^p\rangle + \sum_q d_q |11\rangle \otimes |\psi_B^q\rangle. \tag{3.3}$$

In this equation, the sums run for all the possible combinations in the $|\psi_B\rangle$ space such that the number N_1 of occupied sites is preserved. For example if $|\psi_A\rangle = |01\rangle$, system B is left with $N_1 - 1$ occupied sites.

To obtain the reduced density matrix it is necessary to perform the trace over system B:

$$\rho_A = \sum_{l=1}^{2^{N-2}} \left(\langle I| \otimes \langle\psi_B^l|\right) |\psi_{AB}\rangle\langle\psi_{AB}| \left(|I\rangle \otimes |\psi_B^l\rangle\right). \tag{3.4}$$

It is clear that applying this operation will not eliminate those terms whose elements in the B subsystem in $|\psi_{AB}\rangle\langle\psi_{AB}|$ have the same number of occupied sites. The terms in system A that are left after the trace operation are of the kind $|00\rangle\langle 00|$, $|01\rangle\langle 01|$, $|01\rangle\langle 10|$, $|10\rangle\langle 01|$, $|10\rangle\langle 10|$ and $|11\rangle\langle 11|$.

The $|00\rangle\langle 00|$ element is spared after the trace operator because its $|\psi_B^m\rangle$ elements contain the same quantity of occupied sites (i.e. N_1 sites). This is a similar case with the $|11\rangle\langle 11|$ elements where the $|\psi_B^q\rangle$ wave functions contain $N_1 - 2$ occupied sites.

In the case of the $|01\rangle\langle 01|$, $|01\rangle\langle 10|$, $|10\rangle\langle 01|$ and $|10\rangle\langle 10|$ elements, notice how their $|\psi_B^{o,p}\rangle$ wave functions have the same number of occupied sites ($N_1 - 1$).

Finally, the elements in the reduced density matrix are

$$\rho_A = \begin{pmatrix} \rho_{11} & 0 & 0 & 0 \\ 0 & \rho_{22} & \rho_{23} & 0 \\ 0 & \rho_{32} & \rho_{33} & 0 \\ 0 & 0 & 0 & \rho_{44} \end{pmatrix} \tag{3.5}$$

For ρ_A to be a valid density matrix, it has to be Hermitic ($\rho_A = \rho_A^{\dagger *}$) and its trace be equal to 1. This means that $\rho_{32} = \rho_{23}^*$ and $\rho_{11}+\rho_{22}+\rho_{33}+\rho_{44} = 1$ so it is necessary to calculate only four elements of the matrix.

3.2.2 The density matrix elements

In order to calculate each of the reduced density matrix elements, the second quantization approach will be used.

The first element of the matrix, ρ_{11} can be realized as follows

$$\rho_{11} = \langle\psi_{AB}|\big(1-\hat{n}_i\big)\big(1-\hat{n}_j\big)|\psi_{AB}\rangle \tag{3.6}$$

where the operator $\hat{n}_j$ finds all the elements of the type $|x1\rangle \otimes |\psi_B\rangle$ and after applying $(1-\hat{n}_j)$ we end up with all the elements that do *not* occupy the site j (i.e. $|x0\rangle \otimes |\psi_B\rangle$). A similar approach follows $(1-\hat{n}_i)$ and after applying the bra operation we are left only with the coefficients of all the $|00\rangle \otimes |\psi_B\rangle$ states.

Likely, the other elements are obtained with the following operators:

$$\rho_{22} = \langle\psi_{AB}|\big(1-\hat{n}_i\big)\hat{n}_j|\psi_{AB}\rangle \tag{3.7}$$
$$\rho_{33} = \langle\psi_{AB}|\hat{n}_i\big(1-\hat{n}_j\big)|\psi_{AB}\rangle \tag{3.8}$$
$$\rho_{44} = \langle\psi_{AB}|\hat{n}_i\hat{n}_j|\psi_{AB}\rangle \tag{3.9}$$
$$\rho_{23} = \langle\psi_{AB}|c_j c_i^\dagger|\psi_{AB}\rangle. \tag{3.10}$$

In the last equation, $c_i^\dagger$ leaves only those states with the form $|0x\rangle \otimes |\psi_B\rangle$ and transforms them into $|1x\rangle \otimes |\psi_B\rangle$. Out of this set of states, c_j deletes all states of the type $|x0\rangle \otimes |\psi_B\rangle$ and we end up with states $|10\rangle \otimes |\psi_B\rangle$.

It is very easy to show that the ρ_A elements can be calculated as average quantities of the complete ground-state wave function. For example,

$$\begin{aligned} \rho_{11} =& \langle\psi_{AB}|\psi_{AB}\rangle - \langle\psi_{AB}|\hat{n}_i|\psi_{AB}\rangle - \langle\psi_{AB}|\hat{n}_j|\psi_{AB}\rangle \\ &+ \langle\psi_{AB}|\hat{n}_i\hat{n}_j|\psi_{AB}\rangle \\ =& 1 - \langle\hat{n}_i\rangle - \langle\hat{n}_j\rangle + \langle\hat{n}_i\hat{n}_j\rangle. \end{aligned} \tag{3.11}$$

The other elements are obtained similarly:

$$\begin{array}{ll} \rho_{22} = \langle \hat{n}_j \rangle - \langle \hat{n}_i \hat{n}_j \rangle & \rho_{33} = \langle \hat{n}_i \rangle - \langle \hat{n}_i \hat{n}_j \rangle \\ \rho_{44} = \langle \hat{n}_i \hat{n}_j \rangle & \rho_{23} = \langle c_j c_i^{\dagger} \rangle \end{array} \tag{3.12}$$

3.2.3 Concurrence

In order to use the Concurrence formula (1.42), the non-Hermitian matrix $\rho_A \tilde{\rho_A}$ must be calculated. The matrix $\tilde{\rho_A}$ is constructed using (1.43):

$$\tilde{\rho_a} = \begin{pmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} \rho_{11}^* & 0 & 0 & 0 \\ 0 & \rho_{22}^* & \rho_{23}^* & 0 \\ 0 & \rho_{32}^* & \rho_{33}^* & 0 \\ 0 & 0 & 0 & \rho_{44}^* \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{pmatrix} \tag{3.13}$$

$$= \begin{pmatrix} 0 & 0 & 0 & -\rho_{44}^* \\ 0 & \rho_{32}^* & \rho_{33}^* & 0 \\ 0 & \rho_{22}^* & \rho_{23}^* & 0 \\ -\rho_{11}^* & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{pmatrix} \tag{3.14}$$

$$= \begin{pmatrix} \rho_{44}^* & 0 & 0 & 0 \\ 0 & \rho_{33}^* & \rho_{32}^* & 0 \\ 0 & \rho_{23}^* & \rho_{22}^* & 0 \\ 0 & 0 & 0 & \rho_{11}^* \end{pmatrix} \tag{3.15}$$

Now we are able to construct the non-Hermitian matrix $\rho_A \tilde{\rho_A}$:

$$\rho_A \tilde{\rho_A} = \begin{pmatrix} \rho_{11} & 0 & 0 & 0 \\ 0 & \rho_{22} & \rho_{23} & 0 \\ 0 & \rho_{32} & \rho_{33} & 0 \\ 0 & 0 & 0 & \rho_{44} \end{pmatrix} \begin{pmatrix} \rho_{44}^* & 0 & 0 & 0 \\ 0 & \rho_{33}^* & \rho_{32}^* & 0 \\ 0 & \rho_{23}^* & \rho_{22}^* & 0 \\ 0 & 0 & 0 & \rho_{11}^* \end{pmatrix} \tag{3.16}$$

$$= \begin{pmatrix} \rho_{11}\rho_{44}^* & 0 & 0 & 0 \\ 0 & \rho_{22}\rho_{33}^* + \rho_{23}\rho_{23}^* & \rho_{22}\rho_{32}^* + \rho_{23}\rho_{22}^* & 0 \\ 0 & \rho_{32}\rho_{33}^* + \rho_{33}\rho_{23}^* & \rho_{32}\rho_{32}^* + \rho_{33}\rho_{22}^* & 0 \\ 0 & 0 & 0 & \rho_{11}^*\rho_{44} \end{pmatrix} \tag{3.17}$$

but ρ_A is indeed Hermitian so the following relationships are taken into account: $\rho_{11} = \rho_{11}^*$, $\rho_{22} = \rho_{22}^*$, $\rho_{32} = \rho_{23}^*$, $\rho_{33} = \rho_{33}^*$ y $\rho_{44} = \rho_{44}^*$. The matrix

$\rho_A\tilde{\rho_A}$ now has the form

$$\rho_A\tilde{\rho_A} = \begin{pmatrix} \rho_{11}\rho_{44} & 0 & 0 & 0 \\ 0 & \rho_{22}\rho_{33} + \rho_{23}\rho_{23}^* & \rho_{22}\rho_{23} + \rho_{23}\rho_{22} & 0 \\ 0 & \rho_{23}^*\rho_{33} + \rho_{33}\rho_{23}^* & \rho_{22}\rho_{33} + \rho_{23}\rho_{23}^* & 0 \\ 0 & 0 & 0 & \rho_{11}\rho_{44} \end{pmatrix} \tag{3.18}$$

$$= \begin{pmatrix} \rho_{11}\rho_{44} & 0 & 0 & 0 \\ 0 & \rho_{22}\rho_{33} + \rho_{23}\rho_{23}^* & 2\rho_{22}\rho_{23} & 0 \\ 0 & 2\rho_{33}\rho_{23}^* & \rho_{22}\rho_{33} + \rho_{23}\rho_{23}^* & 0 \\ 0 & 0 & 0 & \rho_{11}\rho_{44} \end{pmatrix} \tag{3.19}$$

$$= \begin{pmatrix} \rho_{11}\rho_{44} & 0 & 0 & 0 \\ 0 & \rho_{22}\rho_{33} + |\rho_{23}|^2 & 2\rho_{22}\rho_{23} & 0 \\ 0 & 2\rho_{33}\rho_{23}^* & \rho_{22}\rho_{33} + |\rho_{23}|^2 & 0 \\ 0 & 0 & 0 & \rho_{11}\rho_{44} \end{pmatrix}. \tag{3.20}$$

In a block diagonal matrix, eigenvalues are simply the eigenvalues of individual blocks so two eigenvalues are readily available. The other two are obtained calculating the determinant of:

$$\begin{pmatrix} \rho_{22}\rho_{33} + |\rho_{23}|^2 - \lambda & 2\rho_{22}\rho_{23} \\ 2\rho_{33}\rho_{23}^* & \rho_{22}\rho_{33} + |\rho_{23}|^2 - \lambda \end{pmatrix}. \tag{3.21}$$

which simply is

$$(\rho_{22}\rho_{33} + |\rho_{23}|^2 - \lambda)^2 - 4\rho_{22}\rho_{33}|\rho_{23}|^2 = 0. \tag{3.22}$$

And now we simply find the value of λ

$$(\rho_{22}\rho_{33} + |\rho_{23}|^2 - \lambda)^2 = 4\rho_{22}\rho_{33}|\rho_{23}|^2 \tag{3.23}$$
$$\rho_{22}\rho_{33} + |\rho_{23}|^2 - \lambda = \pm 2\sqrt{\rho_{22}\rho_{33}}|\rho_{23}| \tag{3.24}$$
$$\lambda = \rho_{22}\rho_{33} + |\rho_{23}|^2 \mp 2\sqrt{\rho_{22}\rho_{33}}|\rho_{23}| \tag{3.25}$$

which yields the values for the λ coefficients:

$$\lambda_a = \rho_{22}\rho_{33} - 2\sqrt{\rho_{22}\rho_{33}}|\rho_{23}| + |\rho_{23}|^2 = (\sqrt{\rho_{22}\rho_{33}} - |\rho_{23}|)^2 \tag{3.26}$$
$$\lambda_b = \rho_{22}\rho_{33} + 2\sqrt{\rho_{22}\rho_{33}}|\rho_{23}| + |\rho_{23}|^2 = (\sqrt{\rho_{22}\rho_{33}} + |\rho_{23}|)^2 \tag{3.27}$$
$$\lambda_c = \rho_{11}\rho_{44} \tag{3.28}$$
$$\lambda_d = \rho_{11}\rho_{44}. \tag{3.29}$$

Finally, to be able to use equation (1.42) we use the square roots of the

lambda coefficients:

$$\sqrt{\lambda_a} = \sqrt{\rho_{22}\rho_{33}} - |\rho_{23}| \tag{3.30}$$

$$\sqrt{\lambda_b} = \sqrt{\rho_{22}\rho_{33}} + |\rho_{23}| \tag{3.31}$$

$$\sqrt{\lambda_c} = \sqrt{\rho_{11}\rho_{44}} \tag{3.32}$$

$$\sqrt{\lambda_d} = \sqrt{\rho_{11}\rho_{44}} \tag{3.33}$$

Notice that λ_b is the largest eigenvalue. Thus, the final formula becomes

$$C = \max\{0, \sqrt{\rho_{22}\rho_{33}} + |\rho_{23}| - \sqrt{\rho_{22}\rho_{33}} + |\rho_{23}| - \sqrt{\rho_{11}\rho_{44}} - \sqrt{\rho_{11}\rho_{44}}\} \tag{3.34}$$

$$C = \max\{0, 2|\rho_{23}| - 2\sqrt{\rho_{11}\rho_{44}}\} \tag{3.35}$$

$$C = 2\max\{0, |\rho_{23}| - \sqrt{\rho_{11}\rho_{44}}\} \tag{3.36}$$

3.3 One dimensional ordered and disordered systems

To begin our study of entanglement we present results for ordered and disordered rings. Concurrence is calculated between all nearest neighbor sites.

3.3.1 Ordered rings

The concurrence between nearest neighbors as a function of system size for a perfectly ordered, periodic ring can be easily computed, using the theory presented in the previous section. We have calculated nearest neighbors concurrence for different ring sizes n. Results are shown in figure 3.2. We observe in figure 3.2(a) that for smaller ring sizes ($n = 4, 8$ and 12 sites) it is very difficult to perceive which is the band filling x where $\overline{C}_{NN}$ will have a maximum.

When we begin to increase the ring size, we notice that the finite size effect begins to disappear (figure 3.2(b)). Moreover, $\overline{C}_{NN}$ starts to show monotonous behavior and we find that the maximum value of nearest neighbor concurrence occurs at half band filling. For $n = 64$ sites the thermodynamic limit has been reached already and the values of $\overline{C}_{NN}$ have almost converged.

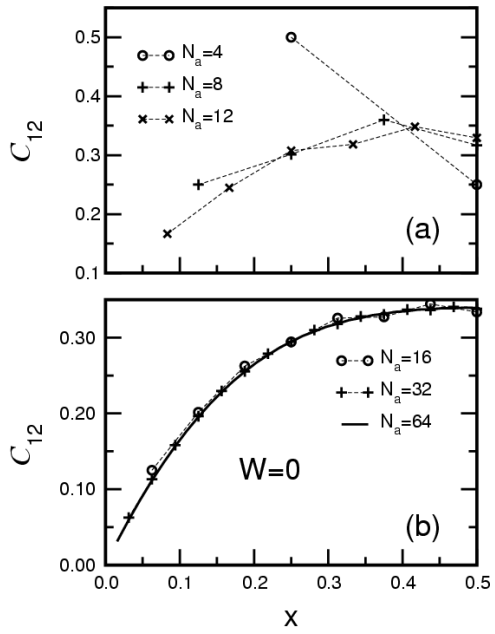


Figure 3.2: Nearest neighbor concurrence for different ring sizes as function of filling

3.3.2 Disordered rings

Off diagonal disorder

Although for one dimensional systems with diagonal or off-diagonal disorder the wave function is localized for all disorder strengths, it is known that the physical properties are strongly dependent on the type of disorder. In this subsection we study how off-diagonal disorder affects the concurrence.

In figures 3.3(a) and 3.3(b) we present results for $\overline{C}_{NN}$ for a ring with $n = 200$ sites and with off-diagonal disorder $t_{NN} \in [1, W + 1]$. In figure 3.3(a) $\overline{C}_{NN}$ is showed as a function of band filling for some representative disorder strengths W whereas in figure 3.3(b) $\overline{C}_{NN}$ is presented as a function of disorder strength W for some representative values of band filling. From the figures, we observe that $\overline{C}_{NN}$ can increase for some band fillings when the disorder strength is increased, contrary to the not disordered case ($W = 0$). In particular, we observe that this occurs for band fillings larger than 0.25 and for off-diagonal disorder strength $W \geq 4$. Notice that the maximum value of the concurrence is found for band filling values in the range $(0.4, 0.45)$ and for $W = 20$. Moreover, the overall form of the concurrence curves does not change significantly for $W > 20$.

It is rather counter intuitive that off-diagonal disorder is able to actually increase $\overline{C}_{NN}$ with respect to the non disordered case. This behavior could

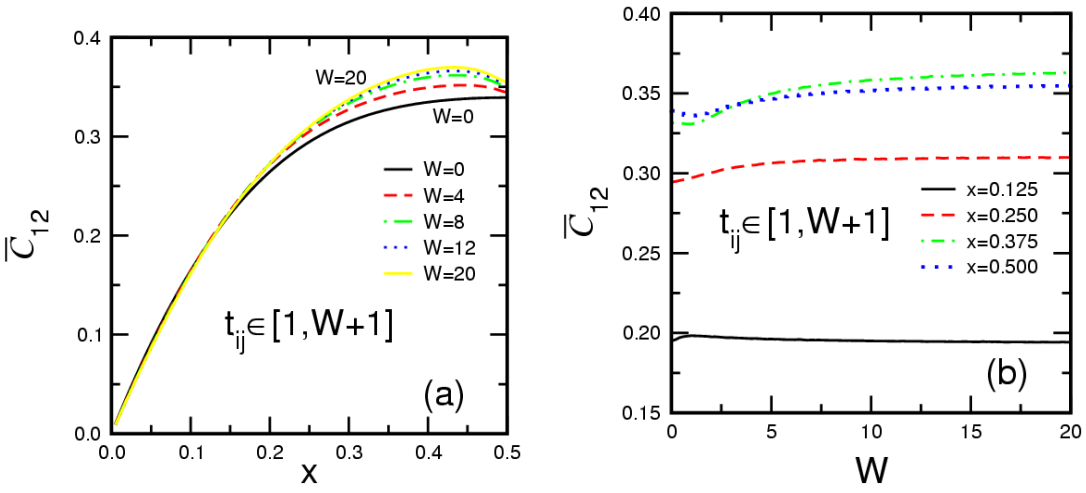


Figure 3.3: Nearest neighbor average concurrence $\overline{C}_{NN}$ of a ring with $n = 200$ sites as a function of band filling for several representative values of the off-diagonal disorder strength W.

be related to the anomaly in the density of states found in these kind of systems. To inquire about it, we have calculated $\overline{C}_{NN}$ as a function of the band filling for a small system with $n = 16$ sites with only one hopping element different with respect to the others. Results are shown in figure 3.4, where concurrence between sites 1 and 2, 2 and 3, 3 and 4 and 4 and 5 is shown. To depict the impurity, $t_{12} = -2$ and $t_{NN} = -1$ for the other pairs of nearest neighbors.

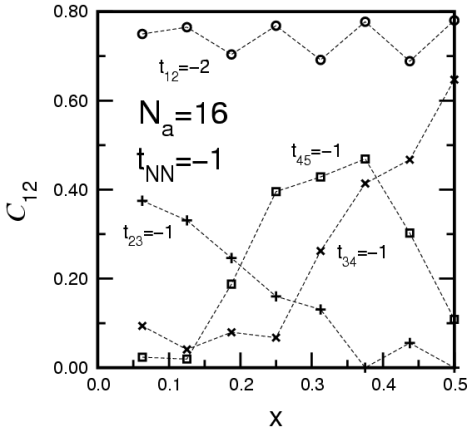


Figure 3.4: Nearest neighbor concurrence for a ring with 16 sites and one impurity localized between sites 1 and 2. Concurrence for close pairs of nearest neighbors (sites 2 and 3, 3 and 4 and 4 and 5) are also shown.

Concurrence between sites where the impurity is located is almost independent to the band filling and oscillates around 0.72. These high values are related to the fact that the impurity localizes the eigenfunction $|\psi_0\rangle$

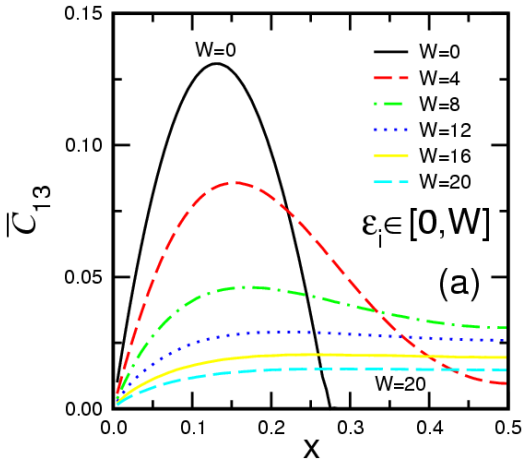


Figure 3.5: $\overline{C}_{NNN}$ in the presence of off diagonal disorder in a chain with 200 sites.

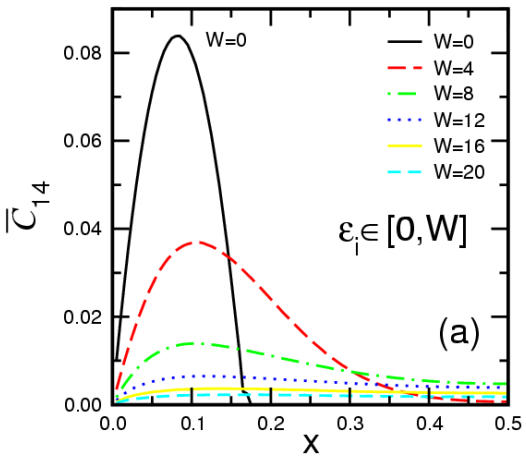


Figure 3.6: $\overline{C}_{NNNN}$ in the presence of off diagonal disorder in a chain with 200 sites.

with the lowest eigenvalue E_0 between the sites where the impurity was placed, whereas the other eigenfunctions are almost delocalized. Thus $z = \langle\psi_0|c_2 c_1^\dagger|\psi_0\rangle$ has very large contribution to the concurrence for all the band fillings. It is necessary to remark that the localization effect due to one impurity only strongly modifies concurrence between sites very close to it.

Finally, we also studied concurrence as a function of distance in the context of off-diagonal disorder. Results are shown in figures 3.5 and 3.6. We can observe that increasing the disorder strength W decreases concurrence for both cases. This confirms that the effect of the increase in the maxima of the nearest neighbor concurrence is due to strong localization on the bonds. Even in the least disordered case, concurrence is significantly smaller in comparison to its nearest neighbor counterpart in both cases.

3.4 Optimizing Entanglement using Genetic Algorithms

There have been recent studies about maximum nearest-neighbor entanglement [33, 34]. In these cases, a N qubit ring in a translationally invariant quantum state has been considered. Under certain conditions, O'Connor and Wootters have found formulas to obtain the maximum possible nearest-neighbor entanglement. Moreover, they have compared this quantity with the entanglement produced by an antiferromagnetic state of

a ring with an even number of spin $1/2$ particles.

Also, there have been studies of concurrence for nearest-neighbors in finite clusters to see the trend in two dimensions. In particular, this was carried on for square, triangular and Kagomé lattices [35].

Further studies focus on systems with higher order of entanglement, that is, when subsystem A is bigger than two qubits.

In this section maximization of entanglement using genetic algorithms will be discussed. Specifically, we will consider the fundamental state of a spinless system modelled by a tight binding Hamiltonian as presented in Eq. (3.1).

The concurrence calculations in the following sections are a sum over all the pairs of sites, divided over the total number of sites. This is not to be confused with the previous section's sum over all the pairs of nearest neighbors.

The pseudo-algorithm goes as follows:

1. Read input parameters including type of lattice, sites in the system, number of generations, crossover probability, mutation probability etc.

2. Build a table with indices of the nearest neighbors of each site. A table including also next nearest neighbors can be built as well.

3. Using the Neighbor Table, identify the specific places in the Hamiltonian Matrix where "bonds" occur. This places represent valid t_{ij} entries and will be stored in a special array. This array will be considered hereafter as a **chromosome**.

4. Allocate two arrays, "generation0" and "generation1" composed of chromosomes.

5. Construct an additional chromosome "best" with initial random numbers between $(0, 5)$.

6. For a given range of filling repeat

    - Initialize "generation0" with random values in the range $(0, 5)$.
    - Make the first chromosome of "generation0" equal to "best".
    - For a given number of generations repeat
        - Decode each chromosome in "generation0" into a Hamiltonian Matrix, diagonalize it and calculate the total concurrence between all nearest neighbors of the system. In other words, calculate fitness for each individual in "generation0".

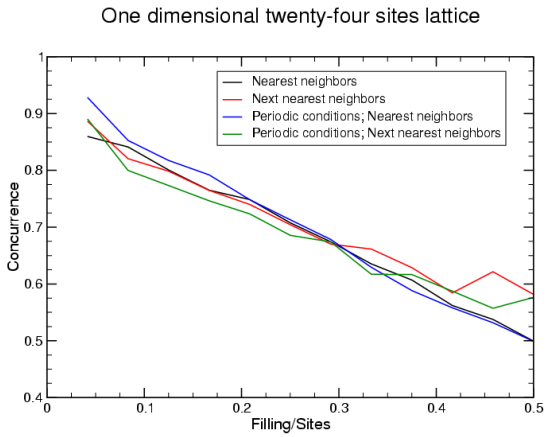


Figure 3.7: Linear chain with 24 sites. 250 generations; population $= 400$; $p_c = 0.70$; $p_m = 0.002$

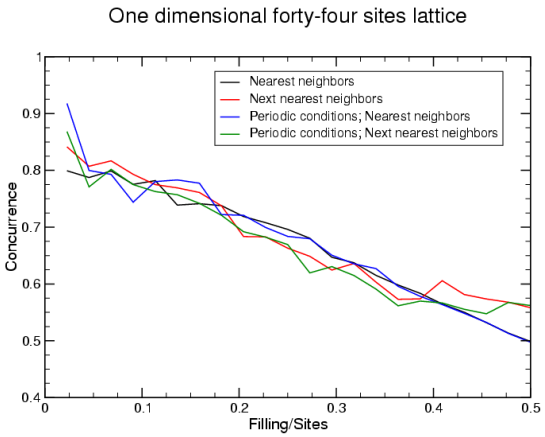


Figure 3.8: Linear chain with 44 sites. 250 generations; population $= 400$; $p_c = 0.70$; $p_m = 0.002$

  - Make “best” equal to the chromosome with highest value of fitness in “generation0”
  - Print the value of the average fitness of the population of “generation0” and fitness of “best” in output files.
  - Apply selection operator: Use crossover and mutation operators on chromosomes in “generation0” to create new chromosomes into “generation1”.
  - Make “generation0” equal to “generation1”.
  - Make the first chromosome in “generation0” equal to “best”.
- Find the chromosome with the maximum fitness. Print its fitness value in an output file.

3.4.1 One-dimensional chains

Analysis of entanglement maximization using genetic algorithms begins with the study of small lineal chains with and without periodic boundary conditions. In figures 3.7 and 3.8 we present results of concurrence as a function of percentage filling for two chains with 24 and 44 sites, respectively. Probability of crossover was $p_c = 0.70$ and probability of mutation was $p_m = 0.002$. Besides nearest neighbors interactions, we have also considered interactions with both nearest neighbors and next nearest neighbors in the Hamiltonian. The population size remained at 400 individuals and the generations were kept at 250. Later on, the role of the number of generations will become apparent.

From the figures, it can be observed that in the case of nearest neighbors interactions with and without periodic boundary conditions, concur-

rence as function of filling is smoother than in the cases where next nearest neighbors are also considered. This can be due to a larger size in the chromosomes in the latter case and a greater number of generations are necessary to obtain a similar behavior than its only-nearest neighbors counterpart. We can only conclude that a larger number of generations and possibly a greater size in the population is necessary to overcome these oscillations.

Also, notice that cases including next nearest neighbors cannot yield lower results than the only nearest neighbors case. This is because the chromosomes from the former case contain the chromosomes of the latter (i.e. the NN case is a subset of the NNN case), which gives the possibility to explore a wider spectrum of solutions. In the case where this extra space yielded only lower results, the best chromosomes would be those of the NN space.

This phenomenon could be most clearly noticed near half filling. Once again, this behavior is a direct consequence of the number of generations.

At this point, it is important to remember that there are various parameters responsible for a larger chromosome in this kind of system. These parameters are the size of the system, the periodic boundary conditions and bringing next nearest neighbors interactions into play. A larger chromosome would allow an exploration of a wider solution space but on the other hand it is expected to decrease convergence time.

We have already mentioned the possibility of a greater number of generations affecting directly the smoothness of the concurrence. We addressed this question by running two cases depicted in figures 3.9 and 3.10, where the former does not consider periodic boundary conditions while the latter does. In both cases we have set a 44-sites chain with a population size of 400. Only the interactions between nearest neighbors were taken into account.

Both figures confirm our early supposition about increasing the number of generations since the correlation curves look increasingly smoother. Notice, however, that certain roughness still remains. Some possible solutions consist of increasing the size of the population, dynamically change the mutation probability (when variation between individuals begins to narrow) and raising further more the number of generations. Different selection methods could also be considered, because an inefficient parent selection could lead to slow evolution of the system. Even though it is clear that individuals with better fitness are obtained, notice how in figure 3.9 the best chromosome near 0.05 filling was obtained with 600 generations despite having cases with up to three times more generations. This gives further evidence about the necessity to investigate the methods discussed

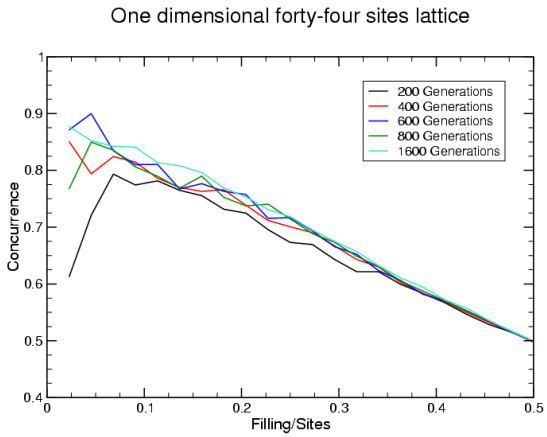


Figure 3.9: Comparison with different number of generations not using periodic conditions. Only nearest neighbors interactions are considered. Population size $= 400$; $p_c = 0.70$; $p_m = 0.002$

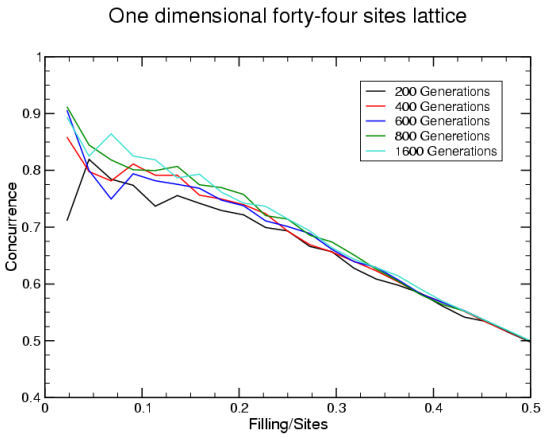


Figure 3.10: Comparison with different number of generations using periodic conditions. Only nearest neighbors interactions are considered. Population size $= 400$; $p_c = 0.70$; $p_m = 0.002$

above.

In figure 3.11, we follow the evolution (optimization) of concurrence for each filling in a 44 site chain with periodic boundary conditions and interactions only between nearest neighbors. The population size remained at 350 and generations were 500 per filling. Black dots represent average fitness per population while red spots represent fitness from the best chromosome in the population. Notice how the population always follows closely the evolution of the best chromosome. Transitions between different fillings are readily noticeable through a drop in average fitness. A very remarkable feature is that the best chromosome for a certain filling ranks high for the next filling but is *not* the highest. In other words, there are different best chromosomes for different band fillings. Further studies are needed to determine exactly the degree of differences and their exact nature.

We also notice that the bottom dots correspond to the average concurrence for randomly disordered populations and that the average concurrences for the subsequent optimized GA populations are always better than the disordered cases.

Another remarkable characteristic about figure 3.11 is its symmetry around half band filling. This property is due to the fact that this is a bipartite lattice and consequently its physical properties are symmetric because of an electron-hole transformation. Remember that a lattice is considered bipartite if it can be divided into two independent lattices. The fact that the results presented show this property reassures the validity of our calculations.

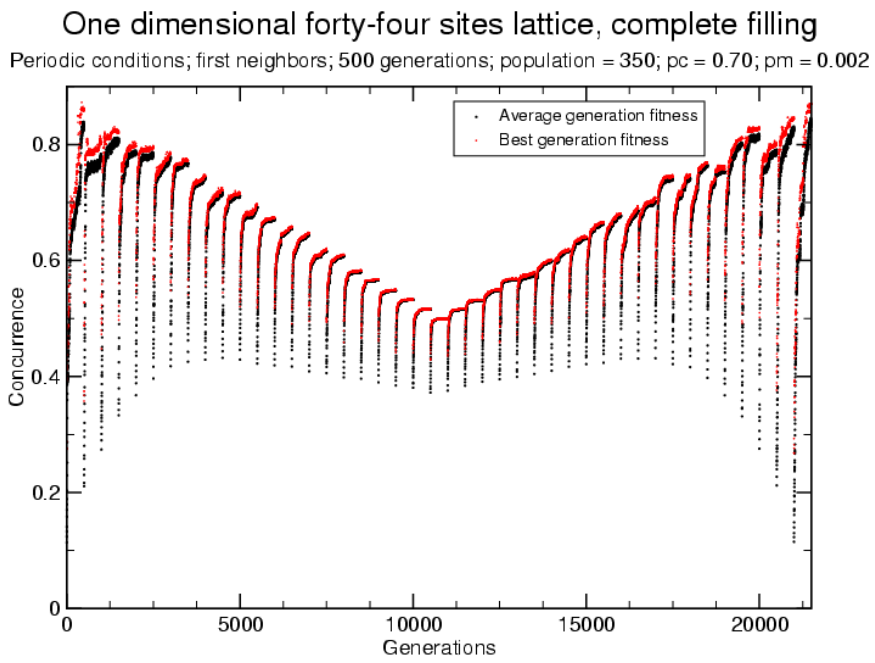


Figure 3.11: Best and average fitness for each generation

3.4.2 Two dimensional systems

Recently, the effect of the dimensionality on concurrence has begun to be studied in square, triangular and Kagomé lattices [35]. In this section we will study the optimization of concurrence in two dimensional systems modelled by means of a tight binding Hamiltonian.

Square lattices

In figures 3.12, 3.13 and 3.14 we display concurrence as a function of band filling for a square lattice of 7x7 sites. In all cases the crossover probability p_c and the mutation probability p_m have been 0.70 and 0.002, respectively.

In figure 3.12, we present a comparison between systems using nearest neighbor and next nearest neighbor interactions as well as periodic and open boundary conditions. The number of generations for these cases remained at 350 and the population size 350. It is worth mentioning that, in general, the cases with interactions only between nearest neighbors rank slightly higher in its concurrence value. Possible reasons for this behavior were addressed in the previous section. In figure 3.13 the number of generations for the exact same cases as figure 3.12 were increased to 600. It can be seen that this parameter is responsible for a slight increase in

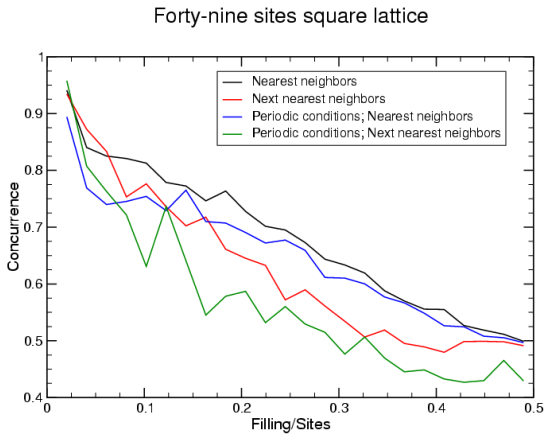


Figure 3.12: Square lattice comparing nearest neighbor interactions, next nearest neighbor interactions and boundary conditions. 350 generations; Population size $= 350$; $p_c = 0.70$; $p_m = 0.002$

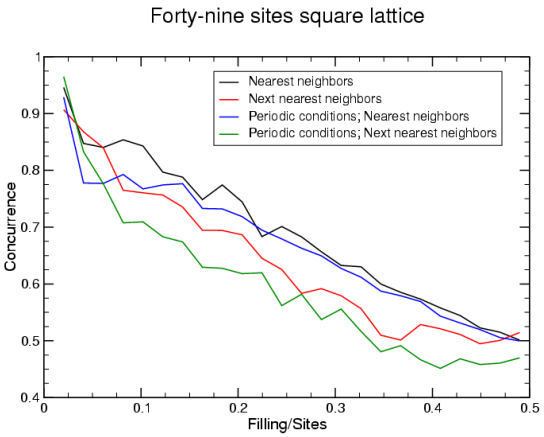


Figure 3.13: This picture depicts the same conditions as those in figure 3.12 except for an increase of generations, which were raised to 600.

concurrence and greatly reduces roughness of the curves.

To study the effect of the number of generations on the optimized value of concurrence and the smoothness of the curve, we present calculations for four different cases in figure 3.14. In this cases, the population size was kept at 400. It is clear that by raising this number we are able to obtain better optimized solutions and the concurrence curve tends to be smoother.

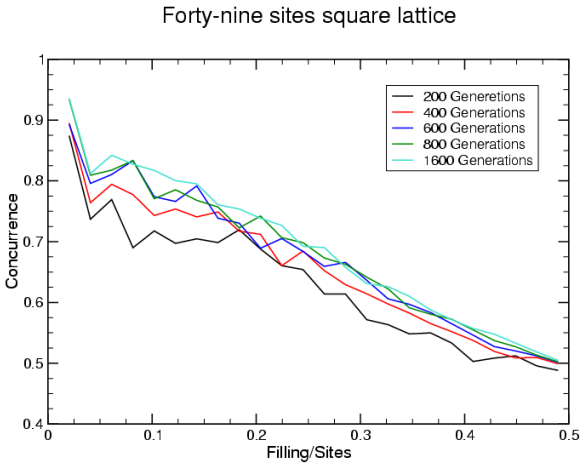


Figure 3.14: Square lattice comparing number of generations. Nearest neighbor interactions; periodic boundary conditions; Population size $= 400$; $p_c = 0.70$; $p_m = 0.002$

We believe it is necessary to make further investigations on the effect of the population size, as well as different selection methods.

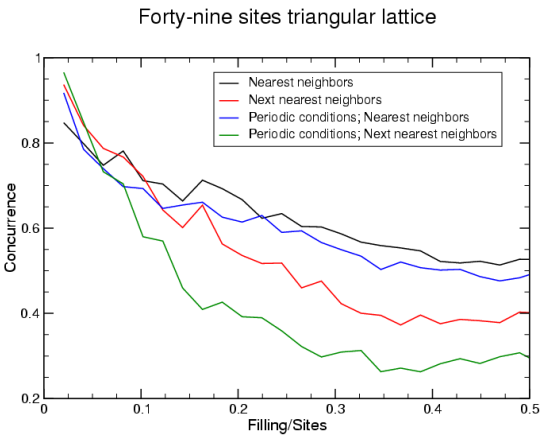


Figure 3.15: Triangular lattice comparing nearest neighbor interactions, next nearest neighbor interactions and boundary conditions. 350 generations; Population size $= 350$; $p_c = 0.70$; $p_m = 0.002$

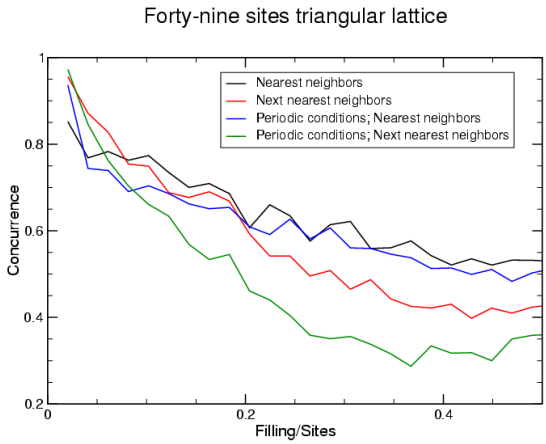


Figure 3.16: Triangular lattice with the same cases as figure 3.15. Generations were increased to 600.

Triangular lattices

Finally, we have made calculations for non bipartite lattices in order to study the effect of frustration on concurrence. It has already been mentioned that this kind of lattices are not symmetric under an electron-hole transformation. This is the reason why their physical properties differ completely between lower and upper sections of band filling.

As a particular case of a not bipartite lattice, we have considered a triangular lattice with 49 sites. In all cases a crossover probability of 0.70 and a mutation probability of 0.002 have been used. Results of our calculations are shown in figures 3.15, 3.16 and 3.17.

In figure 3.15 a population size of 350 has been used and the system has been allowed to go up to 350 generations. As in previous sections, this case includes the interaction between nearest and next nearest neighbors, as well as open and periodic boundary conditions. Once again, we find better optimizations for nearest neighbor interactions. It is important to remember that we are dealing with a more complex chromosome, as sites in this kind of lattice have a greater number of neighbors than one dimensional systems. This is also a cause for a lower time in convergence as the solution space increases considerably. Evidence for this behavior is demonstrated in figure 3.16 where, with almost twice the number of generations, concurrence was only slightly increased. Notice that concurrence behavior is very similar to the square lattice case.

The effect of the number of generations is depicted in figure 3.17. These results demonstrate the slow convergence when calculating this

kind of systems. Notice that, although oscillations decrease and better individuals are found, efficiency narrows between the cases with 600, 800 and even 1600 generations.

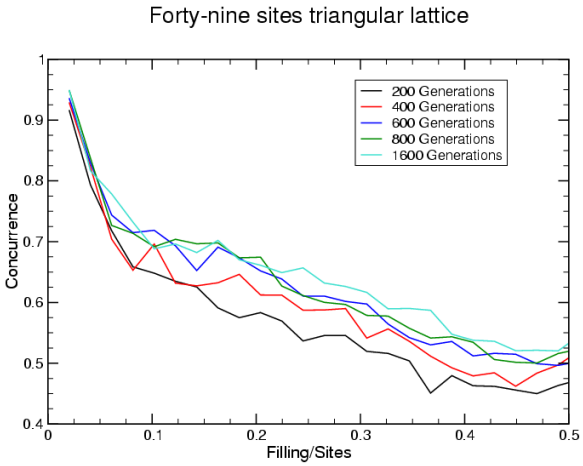


Figure 3.17: Triangular lattice comparing number of generations. nearest neighbor interactions; periodic boundary conditions; Population size $= 400$; $p_c = 0.70$; $p_m = 0.002$

3.5 Conclusions

In this work, we present the necessary formulation to measure entanglement through concurrence for a pair of sites. By doing this, we have been able to calculate the behavior of concurrence and the effect of off-diagonal disorder in rings. We have also implemented computational techniques –more specifically genetic algorithms– to optimize entanglement in systems modeled after a Tight Binding hamiltonian. The qubits in all these studies have been described as sites in the system and the computational basis as occupied or empty sites.

Our novel application of genetic algorithms has proved to be valuable, since we obtained configurations which yield better results for concurrence in randomly disordered systems (for instance, see figure 3.11). Moreover, the GA optimization privided better results even with respect to the ordered cases as can be noticed in figures 3.18, 3.19 and 3.20.

Quantum computation and quantum information are still a long way to go. Nevertheless, these areas represent a logical and necessary step in tomorrow's technological world. In this scenario, quantum entanglement will play a critical role, and our work attempts to be another step towards better understanding it. We hope that this effort will also bring us closer to being able to take advantage of this fascinating quantum property.

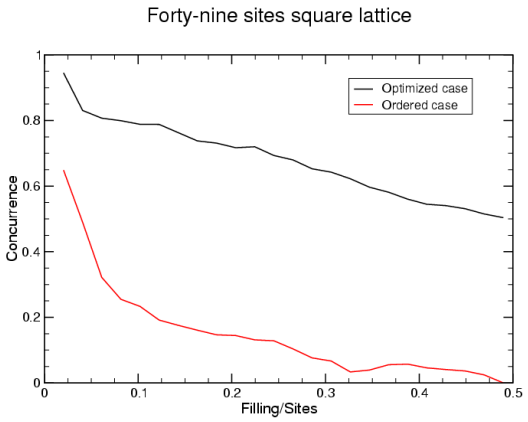


Figure 3.18: Concurrence for an optimized and ordered case in a square lattice of 49 sites. 800 generations; Population size $= 400$. Only nearest neighbors interactions were allowed. Periodic boundary conditions were used. $p_c = 0.70$; $p_m = 0.002$. Ordered case was calculated with off diagonal values of $t_{NN} = 1$

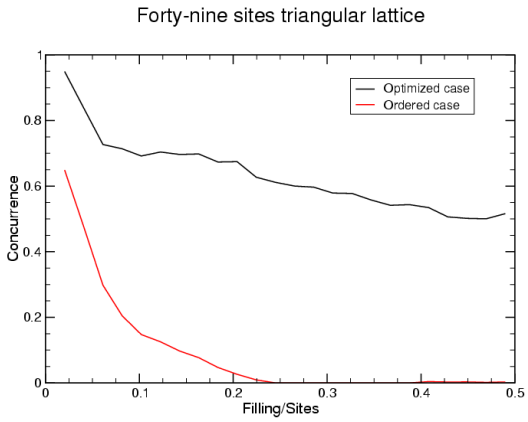


Figure 3.19: Concurrence for an optimized and ordered case in a triangular lattice of 49 sites. 800 generations; Population size $= 400$. Only nearest neighbors interactions were allowed. Periodic boundary conditions were used. $p_c = 0.70$; $p_m = 0.002$. Ordered case was calculated with off diagonal values of $t_{NN} = 1$

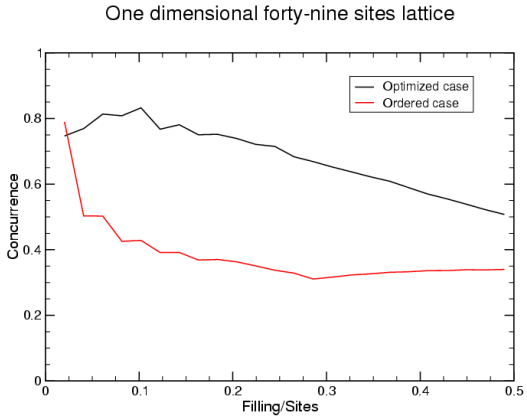


Figure 3.20: Concurrence for an optimized and ordered case in a one dimensional system of 49 sites. 800 generations; Population size $= 400$. Only nearest neighbors interactions were allowed. Periodic boundary conditions were used. $p_c = 0.70$; $p_m = 0.002$. Ordered case was calculated with off diagonal values of $t_{NN} = 1$

Appendix A

Notes

Biographies and definitions were taken from Wikipedia, the free encyclopedia that anyone can edit.

Alice and Bob. Alice and Bob are conventional placeholder terms referring to common archetypal characters used in explanations in fields such as cryptography and physics. Generally Alice wants to send a message to Bob. The names were invented by Ron Rivest for the 1978 Communications of the ACM article presenting the RSA cryptosystem. Other commonly used names include Carol, a third participant in the communication and Eve, and *eavesdropper* who tries to spy the communication but cannot modify it.

Alan M. Turing (1912-1954). Born in the United Kingdom, Turing is often considered father of modern computer science. He provided an influential formalization of the concept of algorithm and computation with the concept of Turing machine. During World War II, Turing was a pivotal player in breaking German cyphers (the Enigma machine). After the war, he designed one of the earliest electronic programmable digital computers at the National Physical Laboratory. In 1950 he proposed an experiment now known as the Turing test, an attempt to define a standard for a machine to be called “sentient”. Turing worked from 1952 until his death in 1954 on mathematical biology, specifically morphogenesis. His central interest in the field was understanding Fibonacci phyllotaxis, the existence of Fibonacci numbers in plant structures.

He died in 1954, from eating an apple with cyanide.

Appendix B

General Mathematical Concepts

B.1 Linear Algebra

Linear algebra is the study of vector spaces and of linear operations on those vector spaces. A good understanding of quantum mechanics is based upon a solid grasp of elementary linear algebra.

The basic objects of linear algebra are *vector spaces*. The vector space of most interest to us is C^n, the space of all n-tuples of complex numbers, $(z_1, \ldots, z_n)$. The elements of a vector space are called *vectors*, and the column matrix representation is often used:

$$\begin{pmatrix} z_1 \\ \vdots \\ z_n \end{pmatrix} \tag{B.1}$$

There is an addition operation defined which takes pairs of vectors to other vectors. In C^n the addition operation for vectors is defined by:

$$\begin{pmatrix} z_1 \\ \vdots \\ z_n \end{pmatrix} + \begin{pmatrix} z'_1 \\ \vdots \\ z'_n \end{pmatrix} \equiv \begin{pmatrix} z_1 + z'_1 \\ \vdots \\ z_n + z'_n \end{pmatrix} \tag{B.2}$$

where the addition operations on the right are just ordinary additions of complex numbers.

In a vector space there is a multiplication by a scalar operation. This operation is defined by

$$z \begin{pmatrix} z_1 \\ \vdots \\ z_n \end{pmatrix} \equiv \begin{pmatrix} z z_1 \\ \vdots \\ z z_n \end{pmatrix} \tag{B.3}$$

where the multiplications on the right are ordinary multiplications of complex numbers.

The standard quantum mechanical notation for a vector in a vector space is:

$$|\psi\rangle \tag{B.4}$$

In this representation, ψ is a label and the entire object is often called a *ket*.

A vector space also contains a special *zero vector*, which is denoted by 0 (NOT to be confused with the vector *labeled* zero: $|0\rangle$). It satisfies the property that for any other vector $|v\rangle$, $|v\rangle + 0 = |v\rangle$ and $0|v\rangle = 0$. In $\mathbf{C}^n$ the zero element is $(0, 0, \ldots, 0)$.

A *vector subspace* of a vector space V is a subset W of V such that W is also a vector space (i.e. the earlier definitions of addition and scalar multiplication also work in W).

B.1.1 Bases and linear independence

A *spanning set* for a vector space is a set of vectors $|v_1\rangle, \ldots, |v_i\rangle$ such that any vector $|v\rangle$ in the vector space can be written as a linear combination $|v\rangle = \sum_i a_i|v_i\rangle$. For example, a spanning set for the vector space $\mathbf{C}^2$ is the set

$$|v_1\rangle \equiv \begin{pmatrix} 1 \\ 0 \end{pmatrix}; \qquad |v_2\rangle \equiv \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{B.5}$$

since any vector

$$|v\rangle = \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} \tag{B.6}$$

can be written as a linear combination $|v\rangle = a_1|v_1\rangle + a_2|v_2\rangle$. In this case we say that the vectors $|v_1\rangle$ and $|v_2\rangle$ *span* the vector space $\mathbf{C}^2$. Generally, a vector space may have many different spanning sets. For example, a second spanning set for $\mathbf{C}^2$ is the set

$$|v_1\rangle \equiv \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}; \qquad |v_2\rangle \equiv \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} \tag{B.7}$$

since an arbitrary vector $|v\rangle = (a_1, a_2)$ can be written as a linear combination of $|v_1\rangle$ and $|v_2\rangle$:

$$|v\rangle = \frac{a_1 + a_2}{\sqrt{2}}|v_1\rangle + \frac{a_1 - a_2}{\sqrt{2}}|v2\rangle \tag{B.8}$$

If we have a set of non-zero vectors $|v_1\rangle, \ldots, |v_n\rangle$ and somehow *find* a set of complex numbers $a_1, \ldots, a_n$ (with at least two of them non-zero) such that the following relation is satisfied:

$$a_1|v_1\rangle + a_2|v_2\rangle +, \ldots, +a_n|v_n\rangle = 0 \tag{B.9}$$

we say that that set of vectors is *linearly dependent*. If we *cannot* find such set of complex coefficients then the set of vectors is said to be *linearly independent*. For example consider the set (B.5). It can be readily seen that one cannot find complex non-zero coefficients such that $a_1|v_1\rangle + a_2|v_2\rangle = 0$. Thus this set is linearly independent. Furthermore, this is a spanning set for $\mathbf{C}^2$, in which case this set is called a *basis* for $\mathbf{C}^2$. It can be shown that any two bases for a vector space contain the same number of elements (e.g. the sets (B.5) and (B.7) both are basis and have 2 elements each). The number of elements in a basis is defined to be the *dimension* of the vector space.

B.1.2 Linear Operators and Matrices

A *linear operator* between vector spaces V and W is defined to be any function $A : V \mapsto W$ which is linear in its inputs, that is:

$$A\left(\sum_i a_i|v_i\rangle\right) = \sum_i a_i A(|v_i\rangle) \tag{B.10}$$

An important linear operator on any vector space V is the *identity operator*, I_V, defined by the equation $I_V|v\rangle \equiv |v\rangle$ for all vectors $|v\rangle$. Another important linear operator is the *zero operator*, which is denoted by 0 and maps all vectors to the zero vector, $0|v\rangle \equiv 0$.

If V, W and X are vector spaces and A, B linear operators such that $A : V \mapsto W$ and $B : W \mapsto X$, then the notation BA denotes de *composition* of B with A and $BA : V \mapsto X$.

The most convenient way to understand linear operators is in terms of their matrix representation. It helps to first understand that an m by n complex matrix A with entries A_{ij} is in fact a linear operator sending vectors in the vector space $\mathbf{C}^n$ to the vector space $\mathbf{C}^m$, under matrix multiplication of the matrix A by a vector in $\mathbf{C}^n$.

A matrix can be regarded as a linear operator and the contrary is also true (this justifies interchanging terms from matrix theory and operator theory). Suppose $A : V \in \mathbf{C}^m \mapsto W \in \mathbf{C}^n$ is a linear operator between vector spaces V and W and $|v_1\rangle, \ldots, |v_m\rangle$ and $|w_1\rangle, \ldots, |w_n\rangle$ are bases for V and

W, respectively. Then there exists complex numbers A_{ij} such that:

$$A|v_j\rangle = \sum_i A_{ij}|w_i\rangle; \qquad \begin{array}{l} 1 \leq j \leq m \\ 1 \leq i \leq n \end{array} \tag{B.11}$$

The matrix whose entries are the values A_{ij} is said to form a matrix representation of the operator A. This matrix representation of A is completely equivalent to the operator A. Note that to make the connection between matrices and linear operators we had to specify a set of input ($|v_1\rangle, \ldots, |v_m\rangle$) and output ($|w_1\rangle, \ldots, |w_n\rangle$) basis states for the input ($\mathbf{C}^m$) and output ($\mathbf{C}^n$) vector spaces of the linear operator.

B.1.3 The Pauli Matrices

The following are four extremely useful matrices, the *Pauli matrices* and their various representations:

$$\begin{array}{cc} \sigma_0 \equiv I \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} & \sigma_1 \equiv \sigma_x \equiv X \equiv \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\ \sigma_2 \equiv \sigma_y \equiv Y \equiv \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} & \sigma_3 \equiv \sigma_z \equiv Z \equiv \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \end{array} \tag{B.12}$$

B.1.4 Inner Products

An *inner product* is a function which takes as input two vectors $|v\rangle$ and $|w\rangle$ from a vector space and produces a complex number as output. A useful but not standard notation for the inner product is $(|v\rangle, |w\rangle)$. The standard quantum mechanical notation for the inner product $(|v\rangle, |w\rangle)$ is $\langle v|w\rangle$. The notation $\langle v|$ is used for the *dual vector* to the vector $|v\rangle$ and is a linear operator from the inner product space V to the complex numbers $\mathbf{C}$, defined by $\langle v|(|w\rangle) \equiv \langle v|w\rangle \equiv (|v\rangle, |w\rangle)$

An inner product satisfies the requirements that:

1. Is linear in the second argument,

$$\left(|v\rangle, \sum_i \lambda_i |w_i\rangle\right) = \sum_i \lambda_i (|v\rangle, |w_i\rangle) \tag{B.13}$$

2. $(|v\rangle, |w\rangle) = (|w\rangle, |v\rangle)^*$

3. $(|v\rangle, |v\rangle) \geq 0$ with equality if and only if $|v\rangle = 0$

$\mathbf{C}^n$ has an inner product defined by

$$((y_1, \ldots, y_n), (z_1, \ldots, z_n)) \equiv \sum_i y_i^* z_i = \left[\begin{array}{c} y_1^*, \ldots, y_n^* \end{array} \right] \left[\begin{array}{c} z_1 \\ \vdots \\ z_n \end{array} \right] \tag{B.14}$$

A vector space equipped with an inner product is called an *inner product space*.

In the finite dimensional complex vector spaces, a Hilbert space is exactly the same thing as an inner product space.

Vectors $|w\rangle$ and $|v\rangle$ are *orthogonal* if their inner product is zero. The vectors $|v\rangle \equiv (1, 0)$ and $|w\rangle \equiv (0, 1)$ are an example of orthogonal vectors.

A *norm* of a vector $|v\rangle$ is defined as:

$$\| \, |v\rangle \, \| \equiv \sqrt{\langle v|v\rangle} \tag{B.15}$$

A *unit vector* is a vector $|v\rangle$ such that $\| \, |v\rangle \, \| = 1$. A *normalized* vector is formed by dividing by its norm: $|v\rangle / \| \, |v\rangle \, \|$ for any non-zero vector. A set of vectors is *orthonormal* if each vector in the set is normalized (i.e. a unit vector) *and* different vectors in the set are orthogonal, that is, $\langle i|j\rangle = \delta_{ij}$.

Suppose $|w_1\rangle, \ldots, |w_d\rangle$ is a basis set for some inner product vector space V. The *Gram-Schmidt* procedure is a useful method that can be used to produce an orthonormal basis set $|v_1\rangle, \ldots, |v_d\rangle$ for the same vector space. Define $|v_1\rangle \equiv |w_1 / \| \, |w_1\rangle \, \|$, and for $1 \leq k \leq d-1$ define $|v_{k+1}\rangle$ inductively by:

$$|v_{k+1}\rangle \equiv \frac{|w_{k+1}\rangle - \sum_{i=1}^{k} \langle v_i|w_{k+1}\rangle |v_i\rangle}{\| \, |w_{k+1}\rangle - \sum_{i=1}^{k} \langle v_i|w_{k+1}\rangle |v_i\rangle \, \|} \tag{B.16}$$

There is a useful way of representing linear operators which makes use of the inner product, known as the *outer product* representation. Suppose $|v\rangle$ is a vector in an inner product space V, and $|w\rangle$ is a vector in an inner product space W. Define $|w\rangle\langle v|$ to be the linear operator from V to W whose action is defined by

$$(|w\rangle\langle v|)(|v'\rangle) \equiv |w\rangle\langle v|v'\rangle = \langle v|v'\rangle |w\rangle \tag{B.17}$$

Linear combinations of outer product operators are also a linear operators:

$$\left(\sum_i a_i |w_i\rangle\langle v_i| \right) |v'\rangle \equiv \sum_i a_i |w_i\rangle\langle v_i|v'\rangle \tag{B.18}$$

An important result known as the *completeness relation* for orthonormal vectors represents the usefulness of the outer product notation. Let

$|v_1\rangle$,. . . , $|v_i\rangle$, . . ., $|v_n\rangle$ be any orthonormal basis for the vector space V such that any vector $|v\rangle$ in V can be written as $|v\rangle = \sum_{j=1}^{n} a_j|v_j\rangle$ for some set of complex numbers a_j. Note that

$$(\langle v_i|)\,|v\rangle = (\langle v_i|)\sum_{j=1}^{n} a_j|v_j\rangle = \sum_{j=1}^{n} a_j\langle v_i|v_j\rangle \tag{B.19}$$

Because the states $|v_i\rangle$ and $|v_j\rangle$ are part of an orthonormal set, all terms in the summatory vanish except when $j = i$:

$$(\langle v_i|)\,|v\rangle = a_i\langle v_i|v_i\rangle = a_i \tag{B.20}$$

Therefore

$$\left(\sum_{i=1}^{n} |v_i\rangle\langle v_i|\right)|v\rangle = \sum_{i=1}^{n} |v_i\rangle\langle v_i|v\rangle = \sum_{i=1}^{n} a_i|v_i\rangle \tag{B.21}$$

If we write the label j instead of i in the last expression, we recover our later definition of $|v\rangle$, thus

$$\left(\sum_{i=1}^{n} |v_i\rangle\langle v_i|\right)|v\rangle = |v\rangle \tag{B.22}$$

Since the last is true for all $|v\rangle$ it follows that

$$\left(\sum_{i=1}^{n} |v_i\rangle\langle v_i|\right) = I \tag{B.23}$$

This equation is known as the completeness relation. It gives a means for representing any operator in the outer product notation. Suppose $A : V \mapsto W$ is a linear operator and $|v_1\rangle, \ldots, |v_i\rangle, \ldots, |v_n\rangle$, $|w_1\rangle, \ldots, |w_j\rangle, \ldots, |w_m\rangle$ orthonormal basis for V and W respectively. Using twice the completeness relation we obtain:

$$\begin{aligned} A &= I_W A I_V \\ &= \textstyle\sum_{ij} |w_j\rangle\langle w_j|A|v_i\rangle\langle v_i| \\ &= \textstyle\sum_{ij} \langle w_j|A|v_i\rangle|w_j\rangle\langle v_i| \end{aligned} \tag{B.24}$$

We see from this equation that A has matrix element $\langle w_j|A|v_i\rangle$ in the jth row and ith column, with respect to the input basis $|v_i\rangle$ and $|w_j\rangle$.

B.1.5 Eigenvectors and eigenvalues

An *eigenvector* of a linear operator A on a vector space is a non-zero vector $|v\rangle$ such that $A|v\rangle = v|v\rangle$ where v is a complex number known as the

eigenvalue of A corresponding to $|v\rangle$. The so-called *characteristic equation* is used to find them and is defined as

$$c(\lambda) \equiv \det|A - \lambda I| \tag{B.25}$$

Where 'det' is the determinant function for matrices. The solutions of the characteristic equation $c(\lambda) = 0$ are the eigenvalues of the operator A. Once the eigenvalues of the operator are known, it is possible to find the corresponding eigenvectors. Every operator A has at least one eigenvalue and a corresponding eigenvector. The set of vectors which have the same eigenvalue v is a subspace of the vector space on which A acts and is called *eigenspace*.

A *diagonal representation* for an operator A on a vector space V is a representation $A = \sum_i \lambda_i |i\rangle\langle i|$, where the vectors $|i\rangle$ form an orthonormal set of eigenvectors for A, with corresponding eigenvalues λ_i. As an example of diagonal representation, the Pauli matrix Z can be written

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = |0\rangle\langle 0| - |1\rangle\langle 1| \tag{B.26}$$

Where the matrix representation is with respect to orthonormal eigenvectors $|0\rangle$ and $|1\rangle$.

B.1.6 Adjoints and Hermitian Operators

If A is any linear operator on a Hilbert space V, there exists a unique linear operator $A^\dagger$ on V such that for all vectors $|v\rangle$, $|w\rangle \in V$

$$(|v\rangle, A|w\rangle) = \left(A^\dagger|v\rangle, |w\rangle\right) \tag{B.27}$$

this linear operator is known as the *adjoint* or *Hermitian conjugate* of the operator A. From the definition it is easy to see that $(AB)^\dagger = B^\dagger A^\dagger$:

$$\begin{aligned}(|v\rangle, AB|w\rangle) = (|v\rangle, Z|w\rangle) = \left((Z)^\dagger|v\rangle, |w\rangle\right) = \left((AB)^\dagger|v\rangle, |w\rangle\right) \\ (|v\rangle, AB|w\rangle) = (|v\rangle, A|z\rangle) = \left(A^\dagger|v\rangle, |z\rangle\right) = \left(A^\dagger|v\rangle, B|w\rangle\right) = \left(B^\dagger A^\dagger|v\rangle, |w\rangle\right)\end{aligned} \tag{B.28}$$

By convention, $|v\rangle^\dagger \equiv \langle v|$.

In a matrix representation of an operator A, the action of the Hermitian conjugation operation is to take the matrix of A to the conjugate-transpose matrix, $A^\dagger \equiv (A^*)^T$. For example

$$\begin{pmatrix} 1+3i & 2i \\ 1+i & 1-4i \end{pmatrix}^\dagger = \begin{pmatrix} 1-3i & 1-i \\ -2i & 1+4i \end{pmatrix} \tag{B.29}$$

An operator A whose adjoint is A is known as a *Hermitian* or *self-adjoint* operator.

An important class of Hermitian operators is the *projectors*. Suppose W is a k-dimensional vector subspace of the d-dimensional vector space V. Using the Gram-Schmidt procedure it is possible to construct an orthonormal basis $|1\rangle, \ldots, |d\rangle$ for V such that $|1\rangle, \ldots, |k\rangle$ is an orthonormal basis for W. By definition

$$P \equiv \sum_{i=1}^{k} |i\rangle\langle i| \tag{B.30}$$

is the projector onto the subspace W. From the definition, any vector $|v\rangle\langle v|$ is Hermitian, so P is Hermitian, $P^\dagger = P$. The *orthogonal complement* of P is the operator $Q \equiv I - P$. Q is a projector onto de vector space spanned by $|k+1\rangle, \ldots, |d\rangle$, which can be called the *orthonormal complement* of P.

An operator is said to be *normal* if $AA^\dagger = A^\dagger A$. An operator which is Hermitian is clearly also normal (for $A = A^\dagger$ and $AA^\dagger = A^\dagger A = A^2$). According to the theorem of *spectral decomposition*, an operator is normal only if it is diagonalizable.

A matrix U is said to be *unitary* if $U^\dagger U = I$. A unitary matrix (or operator) is also normal and has a spectral decomposition.

A *positive operators* are a special and important class of Hermitian operators. A posivite operator is defined to be an operator A such that for any vector $|v\rangle$, $\langle v|A|v\rangle$ is a real, non-negative number. If this product is strictly greater than zero then the operator is *positive definite*

B.1.7 Tensor Products

The *tensor product* is a way of putting vector spaces together to form larger vector spaces.

Suppose V and W are Hilbert spaces of dimension m and n respectively. Then $V \otimes W$ ('V tensor W') is an mn dimensional vector space. The elements of $V \otimes W$ are linear combinations of 'tensor products' $|v\rangle \otimes |w\rangle$ of elements. In particular, if $|i\rangle$ and $|j\rangle$ are basis for V and W respectively, then $|i\rangle \otimes |j\rangle$ is a basis for $V \otimes W$. For example, if V is a two-dimensional vector space with basis vectors $|0\rangle$ and $|1\rangle$ then $|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle$ is an element of $V \otimes V$. Abbreviated notations for the tensor product are often used: $|v\rangle|w\rangle$, $|v, w\rangle$ or even $|vw\rangle$.

The tensor product satisfies the following basic properties:

1. For an arbitrary scalar z and elements $|v\rangle \in V$ and $|w\rangle \in W$,

$$z(|v\rangle \otimes |w\rangle) = (z|v\rangle) \otimes |w\rangle = |v\rangle \otimes (z|w\rangle) \tag{B.31}$$

2. For arbitrary $|v_1\rangle$ and $|v_2\rangle$ in V and $|w\rangle$ in W,

$$(|v_1\rangle + |v_2\rangle) \otimes |w\rangle = |v_1\rangle \otimes |w\rangle + |v_2\rangle \otimes |w\rangle \tag{B.32}$$

3. For arbitrary $|v\rangle$ in V and $|w_1\rangle$ and $|v_2\rangle$ in W,

$$|v\rangle \otimes (|w_1\rangle + |w_2\rangle) = |v\rangle \otimes |w_1\rangle + |v\rangle \otimes |w_2\rangle \tag{B.33}$$

Operators which act of the new tensor spaces can be defined as $A \otimes B$ by the equation

$$(A \otimes B)(|v\rangle \otimes |w\rangle) \equiv A|v\rangle \otimes B|w\rangle \tag{B.34}$$

An arbitrary operator C mapping $V \otimes W$ to $V' \otimes W'$ can be represented as a linear combination of tensor products of operators mapping $V \mapsto V'$ and $W \mapsto W'$:

$$C = \sum_i c_i A_i \otimes B_i \tag{B.35}$$

A natural inner product on $V \otimes W$ can be defined:

$$\left(\sum_i a_i |v_i\rangle \otimes |w_i\rangle, \sum_j b_j |v'_j\rangle \otimes |w'_j\rangle \right) \equiv \sum_{ij} a_i^* b_j \langle v_i|v_j\rangle \langle w_i|w'_j\rangle \tag{B.36}$$

There is a known convenient matrix representation, the *Kronecker product*. Suppose A is an m by n matrix, and B is a p by q matrix. Then:

$$\begin{aligned} A \otimes B &\equiv \begin{pmatrix} A_{11} & \dots & A_{1n} \\ \vdots & \ddots & \vdots \\ A_{m1} & \dots & A_{mn} \end{pmatrix} \otimes \begin{pmatrix} B_{11} & \dots & B_{1q} \\ \vdots & \ddots & \vdots \\ B_{p1} & \dots & B_{pq} \end{pmatrix} \\ &\equiv \begin{pmatrix} A_{11} \begin{pmatrix} B_{11} & \dots & B_{1q} \\ \vdots & \ddots & \vdots \\ B_{p1} & \dots & B_{pq} \end{pmatrix} & \dots & A_{1n} \begin{pmatrix} B_{11} & \dots & B_{1q} \\ \vdots & \ddots & \vdots \\ B_{p1} & \dots & B_{pq} \end{pmatrix} \\ \vdots & \ddots & \vdots \\ A_{m1} \begin{pmatrix} B_{11} & \dots & B_{1q} \\ \vdots & \ddots & \vdots \\ B_{p1} & \dots & B_{pq} \end{pmatrix} & \dots & A_{mn} \begin{pmatrix} B_{11} & \dots & B_{1q} \\ \vdots & \ddots & \vdots \\ B_{p1} & \dots & B_{pq} \end{pmatrix} \end{pmatrix} \end{aligned} \tag{B.37}$$

Tensor product vectors can be represented in the same fashion.

Finally there is a final useful notation $|\psi\rangle^{\otimes k}$ which means $|\psi\rangle$ tensored with itself k times. For example $|\psi\rangle^{\otimes 2} = |\psi\rangle \otimes |\psi\rangle$.

B.1.8 Operator Functions

Given a function f from the complex numbers to the complex numbers, it is possible to define a corresponding matrix function on normal matrices by the following construction. If $A = \sum_a a|a\rangle\langle a|$ is a spectral decomposition for a normal operator A then $f(A) \equiv \sum_a f(a)|a\rangle\langle a|$. As an example, it has already been shown that $Z \equiv |0\rangle\langle 0| - |1\rangle\langle 1|$ so that

$$\exp(\theta Z) = \exp(\theta)|0\rangle\langle 0| + \exp(-\theta)|1\rangle\langle 1| \tag{B.38}$$

in matrix form this becomes

$$\begin{aligned}\exp(\theta Z) &= \begin{bmatrix} \langle 0|\left(e^{(\theta)}|0\rangle\langle 0| + e^{(-\theta)}|1\rangle\langle 1|\right)|0\rangle & \langle 0|\left(e^{(\theta)}|0\rangle\langle 0| + e^{(-\theta)}|1\rangle\langle 1|\right)|1\rangle \\ \langle 1|\left(e^{(\theta)}|0\rangle\langle 0| + e^{(-\theta)}|1\rangle\langle 1|\right)|0\rangle & \langle 1|\left(e^{(\theta)}|0\rangle\langle 0| + e^{(-\theta)}|1\rangle\langle 1|\right)|1\rangle \end{bmatrix} \\ &= \begin{bmatrix} e^{\theta} & 0 \\ 0 & e^{-\theta} \end{bmatrix}\end{aligned} \tag{B.39}$$

Another important matrix function is the *trace* of a matrix. The trace of some matrix A is defined to be the sum of its diagonal elements

$$\mathrm{tr}(A) \equiv \sum_i A_{ii} \tag{B.40}$$

The trace is said to be *cyclic*, tr(AB)=tr(BA), and *linear*, tr(A+B)=tr(A)+tr(B) From the cyclic property, the trace of a matrix is invariant under the unitary operation called *similarity transformation*, that is $A \rightarrow UAU^\dagger$, as tr($UAU^\dagger$) = tr($U^\dagger UA$)

B.1.9 The Commutator and Anti-commutator

The *commutator* between two operators A and B is defined to be

$$[A, B] \equiv AB - BA \tag{B.41}$$

If $[A, B] = 0$, that is $AB = BA$, then it's said that A *commutes* with B. The *anti-commutator* between two operators is similarly defined:

$$\{A, B\} \equiv AB + BA \tag{B.42}$$

and it's said that the operators *anti-commute* if $\{A, B\} = 0$. If a pair of Hermitian operators commute, then it is possible to *simultaneously diagonalize* them. In other words, it is possible to write $A = \sum_i a_i|i\rangle\langle i|$, $B = \sum_i b_i|i\rangle\langle i|$, where $|i\rangle$ is some common orthonormal set of eigenvectors for A and B.

This result connects the commutator of two operators, which is often easy to compute, to the property of being simultaneously diagonalizable. As an example, consider

$$\begin{aligned}[X,Y] &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} - \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\ &= 2i\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \\ &= 2iZ \end{aligned} \tag{B.43}$$

so X and Y do not commute. In fact, Pauli matrices have the commutation relationship

$$[\sigma_j, \sigma_k] = 2i\sum_{l=1}^{3}\epsilon_{jkl}\sigma_l \tag{B.44}$$

where $\sigma_{jkl} = 0$ except $\sigma_{jkl} = 1$ for $jkl = 123, 231, 312$ and $\sigma_{jkl} = -1$ for $jkl = 132, 213, 321$.

B.1.10 The Polar and Singular Value Decompostitions

The *polar* and *single value* decompositions allow us to break general linear operators up into products of unitary operators and positive operators. This is useful because unitary operators and positive operators are better understood than general linear operators.

Let A be a linear operator on a vector space V. Then there exists unitary U, and positive operators J and K such that

$$A = UJ = KU \tag{B.45}$$

where the unique positive operators J and K satisfying these equations are defined by $J \equiv \sqrt{A^\dagger A}$ and $K \equiv \sqrt{AA^\dagger}$. If A is invertible then U is unique. The expression $A = UJ$ is called the *left polar decomposition* of A and $A = KU$ the *right polar decomposition* of A.

If A is a square matrix, then there are unitary matrices U and V, and diagonal matrix D with non-negative entries such that

$$A = UDV \tag{B.46}$$

The diagonal elements of D are called the *singular values* of A.

Appendix C

Quantum Circuits Overview

C.1 Qubit Gates

Analogous to the way a classical computer is built from an electrical circuit containing wires and logic gates, a quantum computer is built from a quantum circuit containing wires and elementary quantum gates.

Consider for example the classical single bit NOT gate, whose operation is defined by its *truth table*, in which $0 \rightarrow 1$ and $1 \rightarrow 0$, that is, the 0 and 1 states are interchanged. The quantum equivalent (*quantum NOT gate*) takes the state

$$\alpha|0\rangle + \beta|1\rangle \tag{C.1}$$

to the corresponding state in which the roles of $|0\rangle$ and $|1\rangle$ have been interchanged

$$\alpha|1\rangle + \beta|0\rangle \tag{C.2}$$

There is a convenient way of representing the quantum NOT gate in matrix form. Such matrix is

$$\mathbf{X} \equiv \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{C.3}$$

If the quantum state $\alpha|0\rangle + \beta|1\rangle$ is written in a vector notation as

$$\begin{pmatrix} \alpha \\ \beta \end{pmatrix} \tag{C.4}$$

with the top entry corresponding to the amplitude for $|0\rangle$ and the botton

entry the amplitude for $|1\rangle$, then the corresponding output from the quantum NOT gate is

$$\mathbf{X}\begin{pmatrix}\alpha\\ \beta\end{pmatrix}=\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}\alpha\\ \beta\end{pmatrix}=\begin{pmatrix}\beta\\ \alpha\end{pmatrix} \tag{C.5}$$

Quantum gates on a single qubit, thus, can be effectively described by two by two matrices. For a matrix to be a valid quantum gate, the appropriate and only condition is that the matrix U be *unitary*, that is $U^\dagger U = I$ where $U^\dagger$ is the *adjoint* of U (obtained by transposing and then complex conjugating U). I is the two by two identity matrix. This unitarity constraint is the only constraint on quantum gates.

Two important matrices that shall be useful are the Z gate:

$$\mathbf{Z}\equiv\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix} \tag{C.6}$$

which flips the sign of $|1\rangle$ to $-|1\rangle$. The other is no less than the *Hadamard* gate:

$$\mathbf{H}\equiv\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix} \tag{C.7}$$

This gate turns a $|0\rangle$ into $(|0\rangle+|1\rangle)/\sqrt{2}$ and $|1\rangle$ into $(|0\rangle-|1\rangle)/\sqrt{2}$. Note that $H^2=I$ so applying H twice to a state does nothing to it.

C.2 Multiple Qubit Gates

In the classical world, any function on bits can be computed from the composition of NAND gates alone, which is thus known as a *universal* gate.

The prototypical multi-qubit quantum logic gate is the controlled-NOT or CNOT gate. This gate has two input qubits, known as the control qubit and the target qubit.

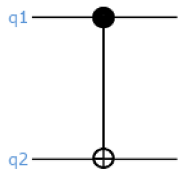


Figure C.1: Schematic diagram for the CNOT gate

If the control qubit (the one with the dark dot) is set to 0, then the target qubit is left unchanged, otherwise (control qubit $= 1$) the target qubit is flipped. For example:

$$\begin{array}{ccc} \text{control} & & \text{control} \\ \downarrow & & \downarrow \\ |00\rangle \rightarrow |00\rangle; & & |10\rangle \rightarrow |11\rangle \\ \uparrow & & \uparrow \\ \text{target} & & \text{target} \end{array} \tag{C.8}$$

Another way of describing the action of the CNOT is as a generalization of the classical XOR gate, since the action of the gate may be summarized as

$$|A, B\rangle \rightarrow |A, B \oplus A\rangle \tag{C.9}$$

where $\oplus$ is addition modulo two, which is exactly what the XOR does. Yet another way to describe the action of the CNOT is in matrix representation:

$$U_{CN} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \tag{C.10}$$

Naturally, as the CNOT gate acts over two qubits, the matrix representation is to be applied to a column vector with the amplitudes of the four possible two-qubit combinations (namely $|00\rangle$, $|01\rangle$, $|10\rangle$ and $|11\rangle$).

As it can be easily verified, the U_{CN} matrix is a unitary matrix.

The CNOT gate can be considered as a type of generalized XOR gate. Unfortunately, other classical gates such as the NAND or the regular XOR gate cannot be represented in the same way the quantum CNOT gate represents the classical NOT gate because they are irreversible or non-invertible. In other words, it's not possible, given the output of those gates, to know what the inputs were. On the other hand, unitary quantum gates are always invertible, since the inverse of a unitary matrix is also a unitary matrix. There have already been experimental implementations for this gate, including trapped ions [36] and photons [37].

C.3 Quantum Circuits

A quantum circuit is read from left to right. Each line in the circuit represents a 'wire'. However, this wire may not correspond to a physical one, but instead it may represent passage of time or perhaps some physical particle moving through space.

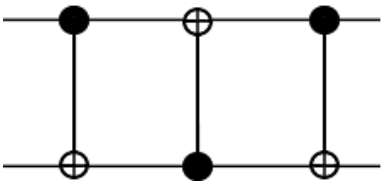


Figure C.2: Schematic Quantum Circuit for "swapping" the states of two qubits (e.g $|ab\rangle \rightarrow |ba\rangle$)

For example, a simple quantum circuit containing three quantum gates is shown if figure C.2. This circuit swaps the states of two bits in the following way:

$$\begin{aligned} |a,b\rangle &\rightarrow |a, a\oplus b\rangle \\ &\rightarrow |a\oplus(a\oplus b), a\oplus b\rangle = |b, a\oplus b\rangle \\ &\rightarrow |b, (a\oplus b)\oplus b\rangle = |b,a\rangle \end{aligned} \tag{C.11}$$

In matrix notation this is:

$$\mathrm{SWAP} = \mathrm{CNOT}_{c=1}\mathrm{CNOT}_{c=2}\mathrm{CNOT}_{c=1} \tag{C.12}$$

$$= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \tag{C.13}$$

$$= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \tag{C.14}$$

There are a few features allowed in classical circuits that are not usually present in quantum circuits. For instance, 'loops', or feedback is not allowed. Other feature not allowed is what is known as FANIN, that is, allowing wires to be joined together resulting in a single wire containing the bitwise OR of the inputs. Also, the operation known as FANOUT —using one wire to obtain several copies of a bit— is not allowed.

Another important operation is measurement. This operation converts a single qubit state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ into a probabilistic classical bit M which is 0 with probability $|\alpha|^2$, or 1 with probability $|\beta|^2$.

C.4 Bell States

The circuit depicted in figure C.3 shows a Hadamard gate followed by a CNOT. As an example of how it works, let's suppose we feed the circuit

with the state $|00\rangle$. The Hadamard gate acts on the first qubit only, turning the input into

$$|00\rangle \rightarrow \frac{(|0\rangle + |1\rangle)}{\sqrt{2}}|0\rangle = \frac{(|00\rangle + |10\rangle)}{\sqrt{2}} \tag{C.15}$$

The first qubit in each part of the state acts as a control input for the CNOT gate, and thus we have

$$\frac{|00\rangle + |10\rangle}{\sqrt{2}} \rightarrow \frac{|00\rangle + |11\rangle}{\sqrt{2}} \tag{C.16}$$

(note how the flipped qubit). The output state is one of the four states known as the *Bell States*, or sometimes the *EPR states* or *EPR pairs*, after some of the people —Bell, Einstein, Podolsky and Rosen— who pointed out the strange properties of states like these.

The explicit construction of the remaining Bell States in matrix notation goes as follows:

$$\begin{aligned} Z \otimes I\,(\mathrm{B}_{00}) &= \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ \frac{1}{\sqrt{2}} \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ \frac{1}{\sqrt{2}} \end{pmatrix} \\ &= \begin{pmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ -\frac{1}{\sqrt{2}} \end{pmatrix} = \frac{(|00\rangle - |11\rangle)}{\sqrt{2}} = \mathrm{B}_{01} \end{aligned} \tag{C.17}$$

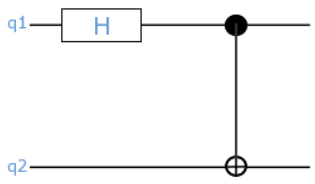


Figure C.3: Quantum Circuit to create a Bell State

$$
\begin{aligned}
X \otimes I\left(\mathrm{B}_{00}\right) &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ \frac{1}{\sqrt{2}} \end{pmatrix} \\
&= \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ \frac{1}{\sqrt{2}} \end{pmatrix} \\
&= \begin{pmatrix} 0 \\ \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \\ 0 \end{pmatrix} = \frac{(|01\rangle + |10\rangle)}{\sqrt{2}} = \mathrm{B}_{10}
\end{aligned}
\tag{C.18}
$$

$$
\begin{aligned}
{}_{i}Y \otimes I\left(\mathrm{B}_{00}\right) &= \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ \frac{1}{\sqrt{2}} \end{pmatrix} \\
&= \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ \frac{1}{\sqrt{2}} \end{pmatrix} \\
&= \begin{pmatrix} 0 \\ \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \\ 0 \end{pmatrix} = \frac{(|01\rangle - |10\rangle)}{\sqrt{2}} = \mathrm{B}_{11}.
\end{aligned}
\tag{C.19}
$$

Bibliography

[1] Michael A. Nielsen, Isaac L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, 2000). ISBN: 0521635039

[2] http://en.wikipedia.org/wiki/Alan_turing

[3] D. Deutsch, Proceedings of the Royal Society of London A, **400**, 97 (1985).

[4] P. W. Shor, Proc. 35nd Annual Symposium on Foundations of Computer Science (Shafi Goldwasser, ed.), IEEE Computer Society Press 124-134 (1994).

[5] L. K. Grover, Proc., 28th Annual ACM Symposium on the Theory of Computing (STOC), 212-219 (1996).

[6] R. Feynman, Int. J. Theor. Phys. 21, 467 (1982)

[7] D. Loss and D. P. DiVincenzo, Phys. Rev. A, 57, 120 (1998)

[8] N. A. Gershenfeld and I. L. Chuang, Science, 275, 350 (1997)

[9] Q. A. Turchette, C. J. Hood, W. Lange, H. Mabuchi and H. J. Kimble, Phys. Rev. Lett. 75, 4710 (1995)

[10] J. I. Cirac and P. Zoller, Phys. Rev. Lett. **74**, 4091 (1995)

[11] J. S. Bell, *Speakable and unspeakable in quantum mechanics*, (Cambridge University Press 1964) ISBN: 0521523389

[12] Scot Hill, William K. Wootters, Phys. Rev. Lett. **78**, 26 (1997).

[13] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996).

[14] C. H. Bennett, H. J. Bernstein, S. Popescu, B. Schumacher, Phys. Rev. A **53**, 2046 1996.

[15] William K. Wootters, Phys. Rev. Lett. **80**, 2245 (1998).

[16] D. P. DiVicenzo, Science **270**, 255 (1995).

[17] A. K. Ekert, Phys Rev. Lett. **67**, 661 (1991).

[18] J. Preskill, J. of Mod. Opt. **47**, 127 (2000).

[19] A. Osterloh, L. Amico, G. Falci, and R. Fazio, Nature **416**, 608 (2002).

[20] S. Ghosh, T. F. Rosenbaun, G. Aeppli, and N. Coppersmith, Nature **425**, 48 (2003)

[21] G. Vidal, J. I. Latorre, E. Rico, and A. Kitaev, Phys. Rev. Lett. **90**, 227902 (2003)

[22] S. J. Gu, S. S. Deng, Y. Q. Li, and H. Q. Lin, Phys. Rev. Lett. **93**, 086402 (2004)

[23] A. K. Ekert, Phys. Rev. Lett. **67**, 661663 (1991)

[24] C. H. Bennett and S. J. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992)

[25] K. Mattle, H. Weinfurter, P. G. Kwiat and A. Zeilinger, Phys. Rev. Lett. **76**, 4656 (1996)

[26] C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).

[27] C. H. Bennett, D. P. DiVincenzo, J. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996).

[28] M. Mitchell, *An Introduction to Genetic Algorithms*, Cambridge MA: MIT Press, 1996.

[29] J. J. Grefenstette, *Foundations of Genetic Algorithms 2* L. D. Whitley, ed. (Morgan Kaufmann, 1993). ISBN: 1558602631

[30] A. J. Mason, 1993. “Crossover non-linearity ratios and the Genetic Algoritm: Escaping the blinkers of schema processing and intrinsic parallelism”. Report 535b, University of Auckland School of Engineering.

[31] C. C. Peck and A. P. Dhawan, 1993. “A review and critique of genetic algorithm theories”. Technical report TR 153/6/93/ECE, College of Engineering University of Cincinnati. Department of Electrical and Computer Engineering

[32] V. Cerletti, W. A. Coish, O. Gywat and D. Loss, Nanotechnology **16** R27, (2005)

[33] K. M. O’Connor and W. K. Wootters, Phys. Rev. A **63**, 052302 (2001)

[34] W. K. Wootters, Contemporary Mathematics **305**, 299 (2002)

[35] V. Subrahmanyam, Phys. Rev. A **69**, 022311 (2004)

[36] C. Monroe, D. M. Meekhof, B. E. King, W. M. Itano and D. J. Wineland, Phys. Rev. Lett. **75**, 4714 (1995)

[37] S. Gasparoni, J. Pan, P. Walther, T. Rudolph and A. Zeilinger, Phys. Rev. Lett. **93**, 020504-1 (2004)

The last page

All code compiled using a licenced Portland Group Fortran 90 compiler under Linux enviroment. LAPACK routines were also used. Code run on a dual Opteron workstation (“genesis”) and a dual Xeon workstation (“comalli”).

Figures created with GIMP and xmgrace.

Text compiled with LaTeX.