Introduction to Quantum Computing

Simão Gonçalves Eusébio

Thesis to obtain the Master of Science Degree in

Electrical and Computer Engineering

Supervisor(s): Prof. Carlos Manuel dos Reis Paiva
Prof. Filipa Isabel Rodrigues Prudêncio

Examination Committee

Chairperson: Prof. José Eduardo Charters Ribeiro da Cunha Sanguino
Supervisor: Prof. Carlos Manuel dos Reis Paiva
Member of the Committee: Prof. Marco Alexandre dos Santos Ribeiro

December 2020
Declaration

I declare that this document is an original work of my own authorship and that it fulfills all the requirements of the Code of Conduct and Good Practices of the Universidade de Lisboa.
I would like to thank my supervisors, Prof. Carlos Manuel dos Reis Paiva and Prof. Filipa Isabel Rodrigues Prudêncio, for their support and guidance.
Abstract

Quantum computation has become very popular, even though it is still in its infancy. To understand its capability and potential, one must understand the theory of quantum computation.

In this work, an introduction to the theory of quantum computation is provided, whose essential prerequisites for understanding it are the fundamentals of linear algebra and complexity theory.

It starts by introducing the fundamental concepts of quantum computation theory, followed by the exposition of quantum gates and quantum circuits, from which a journey through quantum error correction (protection of the quantum data by encoding it) and fault-tolerant quantum computation (protection of the quantum data throughout the whole process of quantum computation; it uses quantum error-correction) is taken. Finally, quantum computation's more core subjects are presented, including reversible computation, the application of complexity theory to quantum computation, and quantum algorithms.

For the specific notation and another helpful information needed to understand the body of the work one may consult the appendices. Besides notation and some linear algebra, the appendices include some group theory, the Pauli matrices, the postulates of quantum mechanics and the fidelity, a measure of distance between quantum states.

**Keywords:** Quantum computation, quantum nonlocality, quantum entanglement, Bloch sphere, quantum fault-tolerance, quantum error correction, Hilbert spaces, parallelism
Resumo

Computação quântica tornou-se bastante popular, mesmo estando ainda na sua infância. Para perceber o seu potencial e o que se é capaz de alcançar com a mesma, é necessário perceber a teoria da computação quântica.

Neste trabalho, uma introdução à teoria da computação quântica é disposta, cujos requisitos essenciais ao seu entendimento são o fundamental de álgebra linear e da teoria da complexidade.

Começa por introduzir os conceitos fundamentais da teoria da computação quântica, seguidos por uma exposição às portas quânticas e aos circuitos quânticos, da qual uma excursão pela correção de erros quântica (proteção de dados quânticos, codificando-os) e pela computação quântica tolerante a falhas (proteção de dados quânticos ao longo de toda a computação quântica; utiliza correção de erros quântica) é feita. Finalmente, os assuntos mais centrais da computação quântica são apresentados, incluindo computação reversível, a aplicação da teoria da complexidade à computação quântica, e algoritmos quânticos.

No que diz respeito a notação específica e outra informação útil necessária ao entendimento do corpo do trabalho, os anexos podem ser consultados. Além de notação e alguma álgebra linear, os anexos incluem alguma teoria de grupos, matrizes de Pauli, os postulados da mecânica quântica e a fidelidade, uma medida de distância entre estados quânticos.

Palavras-chave: Computação quântica, não-localidade quântica, entrelaçamento quântico, esfera de Bloch, computação quântica tolerante a falhas, correção de erros quântica, espaços de Hilbert, paralelismo
Contents

Declaration .......................................................... i
Acknowledgments .................................................. ii
Abstract ............................................................. iii
Resumo ................................................................. iv
List of Tables ....................................................... vii
List of Figures ....................................................... viii
List of Acronyms ................................................... x
List of Symbols ..................................................... xi

1 Introduction ....................................................... 1
  1.1 State-of-the-Art .................................................. 1
  1.2 Objectives ...................................................... 3
  1.3 Structure ........................................................ 4
  1.4 Original contributions ........................................ 5

2 The essentials .................................................... 6
  2.1 Qubits ............................................................ 6
  2.2 Quantum Measurement ........................................ 6
  2.3 Quantum Nonlocality and Entanglement ...................... 10
    2.3.1 Quantum Nonlocality and Entanglement: Introduction ... 10
    2.3.2 Entanglement related experiments and games ........... 11
    2.3.3 A final remark ............................................ 15
  2.4 The density operator .......................................... 15
  2.5 The partial trace .............................................. 17
  2.6 Schmidt decomposition, purification and entanglement .... 18
  2.7 Bloch Sphere Representation .................................. 20

3 Quantum circuits and quantum gates ......................... 24
  3.1 Quantum gates ................................................ 24
  3.2 Measurement on quantum circuits ............................ 25
  3.3 No-cloning theorem .......................................... 27
  3.4 Quantum gate’s accuracy ..................................... 28
  3.5 Universal quantum gates ..................................... 28

4 Quantum error correction .................................... 32
  4.1 Quantum Operations and Operator-sum Representation .... 32
  4.2 Quantum error correction: Introduction ................. 35
  4.3 Distance and classical linear codes ...................... 41
  4.4 The stabilizer construction ................................ 42
    4.4.1 The stabilizer construction ........................... 42
    4.4.2 The CSS codes ........................................ 47
List of Tables

<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1</td>
<td>$3 \times 3$ grid with strategy that wins Mermin-Peres magic square game with probability $\frac{2}{3}$</td>
<td>14</td>
</tr>
<tr>
<td>2.2</td>
<td>$3 \times 3$ grid containing a winning quantum strategy for the Mermin-Peres magic square game</td>
<td>14</td>
</tr>
<tr>
<td>4.1</td>
<td>Five qubit code's generators and logical operators</td>
<td>50</td>
</tr>
<tr>
<td>4.2</td>
<td>Shor code's generators, check matrix, logical operators and Shor code's CSS construction associated generator matrices</td>
<td>51</td>
</tr>
<tr>
<td>6.1</td>
<td>List of algorithms solving the quantum linear systems problem and list of their respective runtime complexities</td>
<td>75</td>
</tr>
</tbody>
</table>
List of Figures

1.1 Schematic diagram of a general communication system. ............................................ 1

2.1 Canonical set of generators for a stabilizer group $S$ with respect to a given partition \{A, B\} of the qubits. $S_A$ and $S_B$ contain the purely local information of $|\psi\rangle$. $S_{AB}$ is generated by $p$ pairs $(g_k, \bar{g}_k)$ whose projections on $A$ (or $B$) anticommute, but commute with all other generators of $S$ including elements of other pairs. .................................................. 19

2.2 Bloch sphere representation of a qubit. .............................................................. 22

2.3 Photon polarization represented on a Riemann sphere. ..................................... 23

3.1 Name, matrix and gate symbol of the most common single qubit gates. .................. 24

3.2 Matrix and gate symbol of the CNOT gate. ....................................................... 25

3.3 CNOT gate flipping the target qubit when the control bit is set to 0. ....................... 25

3.4 Controlled-U gate. ......................................................................................... 26

3.5 Measurement gate. ......................................................................................... 26

3.6 Example of a procedure to defer a measurement. .............................................. 26

3.7 Decomposition of a two-qubit unitary transformation using controlled gates acting on a single qubit. .................................................................................. 30

3.8 Implementation of a $C^n(V)$ gate using Toffoli gates and one $C^1(V)$. ................. 30

3.9 Implementation of a Toffoli gate using CNOTs and single qubit gates. ................. 30

3.10 Implementation of a $C^1(V)$ gate using CNOTs and single qubit gates, where $ABC = I$ and $V = AXBXC$. ................................................................. 31

4.1 Encoding circuit for the Shor code. ........................................................................ 37

4.2 Explanation of the distance requirement in order for the code to correct errors on up to $t$ bits. ................................................................................................. 41

5.1 Tranversal controlled-NOT between two encoded qubits implementing the controlled-NOT operation on qubits encoded with a Steane code. .................................................. 54

5.2 Scheme for the fault-tolerant measurement of an observable $M$ that can be implemented by applying a single qubit operation to each qubit on the encoded data, $|\psi\rangle$. ............... 55

5.3 Knill's error correction method. ........................................................................... 56

5.4 Steane's error correction method. ........................................................................ 57

5.5 Four-qubit cat state fault-tolerant preparation. .................................................... 57

5.6 $\frac{\pi}{2}$ gate fault-tolerant implementation. ............................................................ 58

6.1 Quantum teleportation circuit. ............................................................................. 62

6.2 Circuit implementing the quantum Fourier transform. ........................................ 64

6.3 Reversible NAND implemented using a Toffoli gate. .......................................... 65

6.4 Reversible version of a circuit $C_f$ resetting the ancilla qubits to $|0\rangle$. ................ 65

6.5 Circuit acting like $|x\rangle \rightarrow f(x)$ for an invertible function $f$. .......................... 66

6.6 Implementation of SWAP gate using CNOTs. ..................................................... 66
6.7 Circuit implementing the phase estimation procedure. ........................................ 66
6.8 Geometric proof for the bound $|\theta|/|1 - e^{i\theta}| \leq \pi/2$ on the complex plane. .......... 67
6.9 Representation of the action of a single Grover iteration on $|\psi\rangle$, with the referred reflection axes highlighted in blue. ................................................................. 70
6.10 Circuit implementing a Grover iteration. ................................................................. 71
6.11 Circuit implementing the controlled rotation $R_y(2\theta)$. ......................................... 73
6.12 Quantum circuit (before measurement of the top ancilla) for solving the linear system $A\vec{x} = \vec{b}$. .............................................................................................................. 73
List of Acronyms

AI  Artificial Intelligence.


CNOT  Controlled-NOT.

CSS  Calderbank-Shor-Steane.

EPR  Einstein-Podolsky-Rosen.

FT  Fault-tolerant, Fourier Transform.

GHZ  Greenberger–Horne–Zeilinger.

HHL  Harrow-Hassidim-Lloyd.

PE  Phase Estimation.

POVM  Positive operator-valued measure.

QECC  Quantum error-correcting code.

QLSA  Quantum Linear System Algorithm.

VTAA-HHL  Variable time amplitude amplification HHL.
List of Symbols

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>(</td>
<td>\rangle)</td>
</tr>
<tr>
<td>(&lt;\ldots</td>
<td>\rangle )</td>
</tr>
<tr>
<td>(\otimes)</td>
<td>Tensor product</td>
</tr>
<tr>
<td>(\det(\cdot))</td>
<td>Determinant</td>
</tr>
<tr>
<td>(\text{tr}(\cdot))</td>
<td>Trace</td>
</tr>
<tr>
<td>(\text{tr}<em>{A}(\cdot</em>{AB}))</td>
<td>Partial trace of system (AB) over system (A)</td>
</tr>
<tr>
<td>(|\cdot|)</td>
<td>Norm</td>
</tr>
<tr>
<td>(\cdot_{1} \rightarrow \cdot_{2})</td>
<td>(\cdot_{1}) results in (\cdot_{2}) when acted by (\cdot)</td>
</tr>
<tr>
<td>(\cdot_{1} \rightarrow \cdot_{2})</td>
<td>(\cdot_{1}) tends to (\cdot_{2}), yields</td>
</tr>
<tr>
<td>(\prod_{i=a}^{b} i)</td>
<td>Product on (i) with left application order from (a) to (b)</td>
</tr>
<tr>
<td>(\langle \cdot</td>
<td>\rangle)</td>
</tr>
<tr>
<td>(d(\cdot_{1},\cdot_{2}))</td>
<td>Distance between codewords (\cdot_{1}) and (\cdot_{2})</td>
</tr>
<tr>
<td>(\text{wt}(\cdot))</td>
<td>Weight of codeword (\cdot)</td>
</tr>
<tr>
<td>(\mathcal{P}_{n})</td>
<td>Pauli group on (n) qubits</td>
</tr>
<tr>
<td>(\mathcal{Z}(\cdot))</td>
<td>Centralizer of (\cdot)</td>
</tr>
<tr>
<td>(\mathcal{N}(\cdot))</td>
<td>Normalizer of (\cdot)</td>
</tr>
<tr>
<td>(\delta_{1,2})</td>
<td>Kronecker delta</td>
</tr>
<tr>
<td>(\oplus)</td>
<td>Direct sum, exclusive or (XOR)</td>
</tr>
<tr>
<td>(S(\cdot))</td>
<td>Von Neumann entropy</td>
</tr>
<tr>
<td>(\cdot^{T})</td>
<td>Transpose</td>
</tr>
<tr>
<td>(H(\cdot))</td>
<td>Shannon entropy</td>
</tr>
<tr>
<td>(\mathcal{C}_{n})</td>
<td>Clifford group on (n) qubits</td>
</tr>
<tr>
<td>(SU(n))</td>
<td>Special unitary group of degree (n)</td>
</tr>
<tr>
<td>(O(\cdot))</td>
<td>Big-O</td>
</tr>
<tr>
<td>(\Theta(\cdot))</td>
<td>Big-Theta</td>
</tr>
<tr>
<td>(\Omega(\cdot))</td>
<td>Big-Omega</td>
</tr>
</tbody>
</table>
$\mathcal{O}(\cdot)$  Big-O ignoring logarithmic factors

$\epsilon_{1,2,3}$  Levi-Civita symbol

$h$  Planck's constant

$F(\cdot_1, \cdot_2)$  Fidelity

$\cdot^*$  Conjugate

$\cdot^\dagger$  Hermitian conjugate

$[\cdot_1, \cdot_2]$  Commutator of $\cdot_1$ and $\cdot_2$

$\{\cdot_1, \cdot_2\}$  Anti-commutator of $\cdot_1$ and $\cdot_2$

$\mathbb{E}[\cdot], \langle \cdot \rangle$  Expected value

$\Delta(\cdot)$  Standard deviation
Chapter 1
Introduction

1.1 State-of-the-Art

The birth of the theory of computation (1937) can be traced back to Alan Turing, the father of computation, in fact he is often considered the father of computer science and artificial intelligence. Two of his most notable works are [1] and [2]. The first article lies the foundations of the theory of computation, where Turing defines his namesake machine and answers some important questions regarding computation. The second article is a journey of thoughts spawned by the question ‘Can machines think?’, question from which artificial intelligence is born, and it is born to solve it. In that article, the Turing test is formulated, where a human evaluator asks questions in written form and receives two answers (with no knowledge of the identity of the participants), one from a machine and another from a human, being a conversation established. From this conversation the evaluator should distinguish between the human participant and the machine participant, and if the evaluator cannot reliably identify them, then the machine passes the test. The objective of the test’s questions should be to evaluate how closely the machine’s answers resemble those a human would give.

Parallely (1937), Claude Shannon finished his Master’s thesis “A Symbolic Analysis Of Relay And Switching Circuits”, also published as a paper [4], which is said to be the most important Master’s thesis of the 20th century. It showed how the logical algebra of 19th-century mathematician George Boole could be implemented using electronic circuits of relays and switches. Even though this thesis was of great significance (specially concerning the area of computation), there was a paper [3] which was considered more important, his most notable achievement, “A Mathematical Theory of Communication” (1948). It marks the birth of information theory, making of Shannon, the father of information theory. The article introduced the term bit as the basic unit of information (perhaps for the first time), and the basic blocks in a communication scheme, presented in figure 1.1. Namely, the source which produces the message, the transmitter which operates on the message in some way to produce a signal suitable for transmission over the channel, the channel which is the medium used to transmit the message from the transmitter to the receiver, the receiver which reconstructs the message from the signal, and the destination which is the person (or thing) for whom the message is intended. It also introduced the concepts of bandwidth of a channel and of information entropy.
This was how the classical theory of computation and information was born. In computation, two important aspects are computability and complexity. Complexity will be explained later in the body of this work, and the computability of a problem answers if it can be solved by a computer device, and the problem is said to be computable, if true. Hence, one can only hope to solve computable problems and because not all problems are computable, this sets some limitations. This is a consequence of Gödel's incompleteness theorems (1931, [5]) with the first stating that any consistent formal system $F$ within which a certain amount of elementary arithmetic can be carried out is incomplete, i.e. there are statements of the language of $F$ which can neither be proved nor disproved in $F$. Thus, $F$ has arithmetical truths that are not provable in $F$, requiring a formal system, $F''$, incorporating methods going beyond it to prove them, however the Gödel's first incompleteness theorem also means that such a formal system $F''$ also has arithmetical truths that are not provable in $F''$. The second theorem states that for any consistent system $F$ within which a certain amount of elementary arithmetic can be carried out, the consistency of $F$ cannot be proved in $F$ itself. This statement is stronger than the first one and implies that the consistency of $F$ cannot be proven within it (assuming that $F$ is consistent). Consistency, basically, means that the formal system does not contradict itself, i.e. no statement derivable from the system has its negation also derivable from the system. Thus, the entirety of mathematics might be inconsistent, and a contradiction might be reached at some point, rendering all mathematics invalid.

A related problem to Gödel's incompleteness theorem is the halting problem (posed by Turing) asking if there is a general algorithm that can predict whether the Turing machine will stop with a given program and a given input. There is no such algorithm.

Gödel's incompleteness theorems also raise questions regarding AI. The strong AI's view is that consciousness is reducible to computation, i.e. that it is an emergent property (such as temperature which is a macroscopic property, an average of the kinetic energy of the particles) of the complexity of the computation. All other views can be included in strong AI's opposite view, that consciousness is not reducible to computation. That implies that consciousness requires something more, something currently unknown.

Penrose and Lucas advocate this last view and provided several objections against the strong AI's view raised on the grounds of Gödel's incompleteness theorems; objections that have come to be referred to as Gödelian Arguments. Some of their arguments are based on the idea that the human mind knows the Gödelian formula (statement which the system is unable to prove) to be true, or something similar (like "the human mind can see that the formal system is consistent"), but the inference system cannot prove the formula. Of course, there are several objections against these arguments. From one of the objections (Benacerraf’s objection) , one could at most see that either the human mind could not be simulated by a formal system, or such a formal system would be so complex that a human mind could not fully understand it (so that the human mind would not grasp its Gödel formula).

The argument presented was Luca’s (1961, [6]). Penrose made a similar one (1989, refined version in [7]), which also has its own set of objections. Penrose believed that the missing piece (if any) from the human mind must come from new physics (of quantum nature, for example).

Regardless of this discussion, AI evolved: all computation, no consciousness. Hence, all AI systems known to this day are said to be weak AI.

With the theory of classical computation and information providing such a colourful landscape, it became even more colourful with the addition of quantum computation and quantum information. In 1982, Feynman publishes “Simulating Physics with Computers” [8], where he postulated that to simulate quantum systems one would need to build quantum computers. Since that time, the research and interest on quantum computers has increased, and much progress has been made.
Quantum computers are commonly believed to do every computation that a classical computer does, but faster, by the uninformed individual. This is not accurate. Theoretically, a quantum computer can do everything a classical computer can, at least at the same speed, however there are problems that can be solved much faster in a quantum computer than in a classical computer (to the extent of the current knowledge), and there are also problems that can be solved faster (but not with an "exponential" increase in speed) in a quantum computer than in a classical computer. The greatest interest is in the problems which can be solved much faster in a quantum computer than in a classical computer, obviously. The true power of a quantum computer over a classical one will be proven if quantum supremacy is achieved. Quantum supremacy is the goal of demonstrating that a quantum computer can solve a problem that no classical computer can solve in any feasible amount of time. Moreover, one would be particularly keen on this to be achieved for problems of practical interest. To the extent of the current knowledge, there are problems of particular interest that satisfy quantum supremacy’s statement, theoretically, and some of them will be presented here, such as the discrete logarithm problem, and the factorization problem (whose hardness to solve is the foundation of RSA, today’s most common encryption protocol). Some other problems which can be solved much faster in a quantum computer than in a classical computer can be found in [9], among others. Moreover, if a quantum computer is indeed more powerful than a classical one, then the Church-Turing thesis is wrong and must be revised to: "A quantum Turing machine can efficiently simulate any realistic model of computation with polynomial overhead" (instead of a probabilistic Turing machine).

The areas of quantum computation and quantum information have evolved immensely since they were first envisioned, which can be traced back to the early 80s. A theory has been developed, several possible physical implementations of a quantum computer were proposed, and some quantum computers of small computational power have been successfully implemented by Google and IBM, for example. There are several candidate quantum computer’s physical realizations, but it does not seem to exist a clear winner, all having pros and cons. However, the physical realization of quantum computers is still at its infancy, thus more and better physical realizations can be proposed, and the existing ones may still see improvement. Some recent related developments are [10] and [11].

One of the big problems that quantum computers face is quantum noise, namely decoherence (undesirable correlations between the data qubits and the environment), for which the theory of quantum error correction and quantum fault-tolerance are of use and require an increase in the number of qubits, specially to flush the noise. Hence, the noise is one of the biggest challenges in order to perform reliable quantum computation. Moreover, the current computers only work with small amounts of qubits, in the order of the 50 qubits. Most of the current efforts on the area are related with the physical implementation of quantum computers. The development of quantum algorithms is also a continued endeavour.

Regarding quantum information, several protocols were already created, and experiences have already been performed successfully, for example, quantum teleportation [12].

1.2 Objectives

The objective of this dissertation is to provide an introduction to quantum computation which should be easily understood by anyone with a firm knowledge of linear algebra and knowing the basic concepts of complexity theory. This work proposes to study some of the main concepts and algorithms of quantum computation known to this day. It also serves as an introduction to the field, providing an overview of certain phenomena from quantum mechanics which are at the core of quantum computation, postulates and models.

Quantum computation is studied here from a theoretical point of view. The theory is exposed in a
manner that is hopefully easily comprehensible with a careful reading and that permits a clear understanding of the main ideas behind and its important nuances. Another objective is to provide the reader some intuition on the topics presented and to trigger curiosity regarding the subject, since this work is far from covering all theory of quantum computation. With this work, the reader should be prepared to understand all other areas from quantum computation (besides physical realizations and quantum simulation).

1.3 Structure

The dissertation is composed of 7 chapters. The first chapter is the present one, where the scenario is portrayed, the area in which the work is inserted and the work’s outline and objectives.

The second chapter explains the most important concepts, descriptions and representations for quantum computation. First, the elementary unit of information, the qubit, and the generalization of quantum state for systems of more than one qubit are presented. Secondly, it is described in what consists a quantum measurement, mathematically. The third section comprises firstly an explanation of what is understood by quantum nonlocality and quantum entanglement, secondly a series of experiments/games that show that the correlations due to entanglement are of a different character than any common probabilistic correlation, allowing to achieve goals which are not possible for any locally realistic strategy. For the next section, a different formalism is presented, it describes a system state in terms of a density operator, which accounts for a system whose state is uncertain due to the lack of knowledge of its actual state, i.e. it can be one of many (with some probabilities associated). The following section introduces the partial trace, which is an operation that takes a subsystem from a larger system, by perceiving the rest of the larger system as measured, and therefore seeing it as independent from the rest (the correlations are not observed because only the subsystem is considered). In the sixth section, the Schmidt decomposition of a state is presented, the purification method introduced, and the Schmidt decomposition is seen from an entanglement measure perspective. An entanglement measure based on stabilizers is also presented. In the last section of this chapter, the Bloch sphere representation of one qubit is described, it is a way to represent the state of one qubit in a sphere.

The third chapter starts by introducing quantum gates which are the components for a quantum circuit (along with the measurement apparatus, whose representation on circuit is introduced right after). The no-cloning theorem is also given, which states that no quantum gate can clone non-orthogonal states, that is, generally a qubit cannot be copied. Next, one observes that the errors on quantum gates accumulate linearly, and finally the existence of universal quantum gates is proven, i.e. the existence of a set of gates which can be combined in order to obtain any possible quantum gate to an arbitrarily small accuracy.

In the fourth chapter, quantum error correction is introduced starting with quantum operations which act on a density operator, leaving as resulting density operator the sum of all operators’ action on the density operator. A quantum operation can be identified with a unitary transformation acting on the system plus the environment which is measured afterwards (the environment; and where the outcome of the measurement is unknown), which in turn can be identified with each operator acting on the system, with the uncertainty of which one actually acted on the system. From there, the formalism used is stated, the conditions for which an error correction code corrects a set of errors are presented, and a quantum error correction code is shown as example and to familiarize with the ideas behind error correction. Following is the presentation of the concept of distance for a classical code and the introduction of classical linear codes. Next, the stabilizer construction/formalism is introduced, which describe quantum error correction codes in an elegant and convenient way, and at the section’s end a particular class
of stabilizer codes is presented, the **CSS** codes. Finally, some quantum error correction codes are shown and bounds for quantum error correction codes are established, which concern its associated parameters.

In the fifth chapter, fault-tolerant computation is introduced, where methods and procedures to perform the operations involved in the computation fault-tolerantly are given. At the end, the threshold theorem confirms that error correction is capable of protecting the data from noise, given some reasonable assumptions, and also some remarks are made about fault-tolerance.

The sixth chapter presents initially the basic from complexity theory in order to evaluate the resources needed for some quantum algorithm, and to evaluate the hardness of a problem from a quantum and classical perspective, in order to be able to compare the performance of classical and quantum algorithms solving the same problem. After, an example of a simple interesting circuit is shown, the circuit for quantum teleportation, where a qubit is transmitted between two parties by sending two classical qubits, which are result of a measurement outcome. Following is the quantum Fourier transform which is followed by reversible computation, since classically, computation is done irreversibly, and in this section it is delineated how to implement reversibly a classical circuit, in order to implement it in a quantum fashion (quantum computation is performed reversibly). Finally, the quantum algorithm of phase estimation (estimates the phase of an eigenvalue of some unitary matrix $U$), from which the order-finding, factoring and discrete logarithm algorithms are built, and the Grover’s algorithm (searches for a solution, having only an oracle as problem’s information) are presented.

In the last chapter, the dissertation is concluded and considerations about future work are made.

The appendix consists mostly of important notes for understanding this work.

### 1.4 Original contributions

A lot of the work presented in this dissertation comes from the literature, being the information organized according to the design of the dissertation’s author. The greatest contribution regarding this work is the exposition of the information, the considerations and explanations.

The original contributions include the exposition for the partial trace, the quantum measurement and all the explanations in section 2.3. It includes too the deduction of the Bloch sphere representation from the state vector representation, the demonstration of the principles of implicit measurement and of deferred measurement and the end of deduction regarding existence of universal quantum gates. Other ones are the Shor code exposition in section 4.2, the stabilizer code’s exposition, the analysis of $\sum_{y \in \mathbb{C}} (-1)^{x \cdot y}$ for $x \in \mathbb{C}$ and for $x \notin \mathbb{C}$, the final remarks regarding the **CSS** code, the derivation of the asymptotic bounds on quantum error correction and much of the exposition of the fault-tolerant computation, including Knill’s error correction method and Steane’s error correction method explanation, some of the considerations regarding concatenated codes for the threshold theorem, and the final remarks of chapter 5. Part of the exposition regarding the quantum teleportation circuit is included, as is part of the exposition of the algorithms and most of the exposition on the appendix.
Chapter 2

The essentials

2.1 Qubits

Before starting and as a first suggestion, it is recommended that appendices A, C and optionally appendix D be consulted if the notation and other basic matters are not familiar.

The qubit is the elementary unit of information for quantum computation and quantum information, the same way as the bit is for classical computation and classical information. A single qubit can be represented as below

\[ |\psi\rangle = a |0\rangle + b |1\rangle, \] (2.1)

where \(|0\rangle\) and \(|1\rangle\) form an orthonormal basis of a two-dimensional complex vector space, since \(a\) and \(b\) are complex numbers. A classical bit may have either the value 0 or 1, however a quantum bit can be in a superposition of both, as it can be perceived by (2.1). Another important aspect is that one cannot examine the qubit in order to attain its state (determined by \(a\) and \(b\)), instead the measurement of a qubit collapses its state to \(|0\rangle\) or \(|1\rangle\), with probabilities \(|a|^2\) and \(|b|^2\), respectively. Of course, \(|a|^2 + |b|^2 = 1\) and therefore a qubit state is normalized to 1.

A state is considered the same if differs from other by a global phase factor; in other words \(|\psi\rangle\) and \(e^{i\alpha} |\psi\rangle\) (\(\alpha\) being a real number) represent the same state.

In general, for a system of \(N\) qubits a state may be written as

\[ |\psi\rangle = \sum_{i=0}^{2^N-1} \alpha_i |i\rangle = \alpha_0 |0\ldots0\rangle + \alpha_1 |0\ldots01\rangle + \alpha_2 |0\ldots010\rangle + \ldots + \alpha_{2^N-1} |1\ldots1\rangle \] (2.3)

2.2 Quantum Measurement

The operation of measuring in a quantum system consists in measuring something named observable, and it is how information is extracted from qubits.

An observable has several possible outcomes, and from the Born rule the observable might be described by a set of orthogonal projection operators \(\{P_i\}\). If outcome \(m\) happens then the (normalized) post-measurement state is

\[ \frac{P_m |\psi\rangle}{\sqrt{p(m)}} \] (2.4)

where \(p(m)\) is the probability of outcome \(m\), which is defined by

\[ p(m) = \langle \psi | P_m^* P_m |\psi\rangle \] (2.5)
and the following holds
\[ \sum_i p(i) = \langle \psi | (\sum_i M_i^\dagger M_i) | \psi \rangle = \langle \psi | I | \psi \rangle = 1 \] (2.6)
for measurement operators \( \{ M_i \} \), which satisfies the normalization constraint on probabilities.

Hence, an observable is defined as
\[ M = \sum_m m P_m. \] (2.7)

The expectation of an observable is defined as
\[ \mathbb{E}[M] = \sum_m m p(m) = \sum_m \langle \psi | M_m^\dagger M_m | \psi \rangle = \langle \psi | \sum_m m M_m^\dagger M_m | \psi \rangle, \] (2.8)
which for projective measurements translates into
\[ \mathbb{E}[M] = \langle \psi | \sum_m M_m^\dagger M_m | \psi \rangle = \langle \psi | \sum_m m P_m | \psi \rangle = \langle \psi | M | \psi \rangle \] (2.9)
which is usually denoted by \( \langle M \rangle \psi \) and by \( \langle M \rangle \) when the quantum state is implicit. The observable’s standard deviation is
\[ \Delta(M) \equiv \langle (M - \langle M \rangle)^2 \rangle^{1/2} = \langle (M^2) - \langle M \rangle^2 \rangle^{1/2}. \] (2.10)

An important statement of quantum mechanics is the Heisenberg uncertainty principle. An instance of such principle can be obtained for observables in the following manner,
\[ \Delta(A) \Delta(B) = \langle (\langle \psi | A_0 | \psi \rangle \langle \psi | B_0 | \psi \rangle)^2 \rangle^{1/2} \geq \langle \langle \psi | A_0 B_0 | \psi \rangle \rangle \]
\[ = \langle \psi | \frac{A_0 B_0 + B_0 A_0}{2} | \psi \rangle + i \langle \psi | \frac{A_0 B_0 - B_0 A_0}{2i} | \psi \rangle \]
\[ \geq \langle \psi | \frac{A_0 B_0 - B_0 A_0}{2i} | \psi \rangle \rangle = \frac{1}{2} \langle \psi | [A_0, B_0] | \psi \rangle \rangle = \frac{1}{2} \langle \psi | [A, B] | \psi \rangle \rangle, \] (2.11)
where \( A_0 \equiv A - \langle A \rangle \) and \( B_0 \equiv B - \langle B \rangle \) and it was applied the Cauchy-Schwarz inequality. Hence, one obtains a lower bound on the product of the standard deviations of the observables.

A generalization of quantum measurement can be achieved where the measurement operators do not need to be orthogonal projection operators, while still satisfying the completeness relation. These kind of measurements result from realizing that the system in question, denote it \( S \), is part of a larger system \( S' \) where by applying a unitary transformation in \( S' \) the augmented measurement is in fact described by a set of orthogonal projection operators, thus, actually, no violation of the first definition of measurement presented occurs. In light of this paradigm, the first definition of measurement contains the generalized one. Now, heed the following proposition which ensures that one can define the \( U \) presented next as a unitary transformation.

**Proposition 2.2.1.** \([3]\)** Suppose \( V \) is a finite dimension complex vector space (with inner product) with a subspace \( W \). Suppose \( U : W \to V \) is a linear operator which preserves inner products, that is, for any \( |w_1\rangle \) and \( |w_2\rangle \) in \( W \),
\[ \langle w_1 | U^\dagger U | w_2 \rangle = \langle w_1 | w_2 \rangle. \] (2.12)
Then, there exists a unitary operator \( U' : V \to V \) which extends \( U \). That is, \( U' |w\rangle = U |w\rangle \) for all \( |w\rangle \) in \( W \), but \( U' \) is defined on the entire space \( V \).

**Proof.** Let \( W^\perp \) be the orthogonal complement of \( W \), from which \( V = W \oplus W^\perp \). Also, let \( \{|w_i\}\}, \{|w'_j\}\) be orthonormal bases of \( W \) and \( W^\perp \), respectively. Consider also, \( |u_1\rangle = U |w_1\rangle \) with \( \{|u_i\}\) forming an orthonormal basis of a subspace of \( V \), call it \( X \), since \( U \) preserves inner products on \( W \). Let an
orthonormal basis for the complement of \( X, X^\perp \), be \( |u_i^j\rangle \), and so \( V = X \oplus X^\perp \). Write \( U' : V \to V \) as
\[
U' = \sum_{i=1}^{\dim(W)} |u_i\rangle \langle w_i| + \sum_{j=1}^{\dim(W^\perp)} |w_j^j\rangle \langle w_j^j|.
\]
It is clear that \( U'|w\rangle = U|w\rangle \) for all \( |w\rangle \in W \) since
\[
U'|w\rangle = \sum_i |u_i\rangle \langle w_i|w\rangle = \sum_i U|w_i\rangle \langle w_i|w\rangle = U \left( \sum_i |w_i\rangle \langle w_i|w\rangle \right) = U|w\rangle,
\]
where the completeness relation and the fact that \( \langle w_j^j|w\rangle = 0 \) were used. Since
\[
U'^*U' = \sum_i |w_i\rangle \langle w_i| + \sum_j |w_j^j\rangle \langle w_j^j| = I
\]
\[
U'U'^\dagger = \sum_i |u_i\rangle \langle u_i| + \sum_j |w_j^j\rangle \langle w_j^j| = I,
\]
\( U' \) is unitary.

To prove the statement previous to the proposition, an ancillary system in a fixed state \( |0\rangle \) and with an orthonormal basis \( \{|m\rangle\} \) is introduced. The measurement operators under consideration are \( \{M_m\} \), and let \( U \) be such that
\[
U|\psi\rangle|0\rangle = \sum_m M_m|\psi\rangle|m\rangle.
\]

Using the orthogonal projection operators \( P_m \equiv I_S \otimes |m\rangle \langle m| \) the normalization constraint on probabilities can be verified.
\[
\sum_m p(m) = \sum_m \langle \psi|0\rangle U^\dagger P_m U|\psi\rangle|0\rangle = \sum_m \langle \psi|0\rangle U^\dagger P_m U|\psi\rangle|0\rangle
\]
\[
= \sum_{m,m',m''} \left( \langle \psi|M_{m'}^\dagger M_{m''}|\psi\rangle \otimes \langle m'|m\rangle \langle m|m''\rangle \right) + \sum_m \langle \psi|M_{m'}^\dagger M_{m}|\psi\rangle
\]
\[
= \langle \psi| \left( \sum_m M_{m'}^\dagger M_{m} \right) |\psi\rangle = 1
\]

The post-measurement state for this measurement if outcome \( m \) occurs is
\[
\frac{P_m U|\psi\rangle|0\rangle}{\sqrt{\langle \psi|0\rangle U^\dagger P_m U|\psi\rangle|0\rangle}} = \frac{M_m|\psi\rangle|m\rangle}{\sqrt{\langle \psi|M_{m'}^\dagger M_{m}|\psi\rangle}}.
\]

Therefore, it is possible to conclude that a general measurement is completely equivalent to a unitary transformation in the augmented system using an ancillary system and projective measurements. Notice the pseudo augmented measurement operators \( \{M_m \otimes |0\rangle \langle 0| \} \) (action of \( U \) on the state \( |\psi\rangle|0\rangle \)) which are the fundamental piece on the previous construction. The unitary operation \( U \) acts as if it applies them and together with the corresponding orthogonal projection operators one obtains the equivalent procedure. Another technique (regarding unitary transformations) in quantum measurement (with no need of ancillary systems) is to perform a unitary transformation to change the basis of the state followed by a projective measurement in the canonical basis, resulting in the corresponding measurement being made in the desired basis.

An important result regarding quantum measurements is that non-orthogonal states cannot be reliably distinguished. If it is desired to distinguish the states \( \{|\psi_i\rangle\} \) or more simply one of the states from any other. Let
\[
|\psi\rangle, i = 1, \ldots, n \quad \sum_{k=1}^N M_k^\dagger M_k = I
\]
using $N \geq n$ measurement operators $\{M_k\}$. Wishing to distinguish $|\psi_1\rangle$ from any other state means $\langle \psi_1 | M_k^\dagger M_k | \psi_1 \rangle = 1$ or in order to generalize, allowing to identify with more than one operator, $\langle \psi_1 | \sum_{k} M_k^\dagger M_k | \psi_1 \rangle = 1$. Hence, using the completeness relation, one has

$$\langle \psi_1 | \sum_{k} M_k^\dagger M_k | \psi_1 \rangle = 1 \iff \sum_{k \notin \{s\}} \langle \psi_1 | M_k^\dagger M_k | \psi_1 \rangle = 0 \iff M_k | \psi_1 \rangle = 0, \; k \notin \{s\} \quad (2.19)$$

and also

$$\langle \psi_j | \sum_{k} M_k^\dagger M_k | \psi_1 \rangle = \langle \psi_j | \psi_1 \rangle \iff \langle \psi_j | \left( \sum_{k \in \{s\}} M_k^\dagger M_k \right) | \psi_1 \rangle = \langle \psi_j | \psi_1 \rangle , \quad (2.20)$$

meaning that $\sum_{s} M_k^\dagger M_k$ preserves inner products involving $|\psi_1\rangle$. Let $|\psi_2\rangle$ be an arbitrary state, and consequently can be written as a linear combination of the component parallel to $|\psi_1\rangle$ and components perpendicular to $|\psi_1\rangle$: $|\psi_2\rangle = \alpha |\psi_1\rangle + \beta |\psi_1^\perp\rangle$, $|\alpha|^2 + |\beta|^2 = 1$. Then

$$\langle \psi_3 | \sum_{k \in \{s\}} M_k^\dagger M_k | \psi_3 \rangle = |\alpha|^2 + \alpha^* \beta \langle \psi_1^\dagger | \psi_1 \rangle + \alpha \beta^* \langle \psi_1 | \psi_1^\perp \rangle + |\beta|^2 \langle \psi_1^\perp | \left( \sum_{k \in \{s\}} M_k^\dagger M_k \right) | \psi_1^\perp \rangle$$

$$= |\alpha|^2 (1 - l) + l, \; l = \langle \psi_1^\perp | \left( \sum_{k \in \{s\}} M_k^\dagger M_k \right) | \psi_1^\perp \rangle , \quad (2.21)$$

which is minimized for $|\alpha|^2 = 0$, unless $l = 1$ where it is impossible to distinguish between $|\psi_1\rangle$ and $|\psi_1^\perp\rangle$ and therefore the value of $|\alpha|^2$ is irrelevant, and it is impossible to distinguish the states. One concludes that $\langle \psi_3 | \sum_{k \in \{s\}} M_k^\dagger M_k | \psi_3 \rangle = l$ if $|\alpha|^2 = 0$, and with $l = 0$ one obtains $\langle \psi_3 | \sum_{k \in \{s\}} M_k^\dagger M_k | \psi_3 \rangle = 0$ (can be achieved using $\sum_{k \in \{s\}} M_k^\dagger M_k = |\psi_1\rangle \langle \psi_1|$). Lastly, $|\alpha|^2$ must be 0 to have

$$\langle \psi_3 | \sum_{k \in \{s\}} M_k^\dagger M_k | \psi_3 \rangle = 0 \quad (2.22)$$

which means that to distinguish a state from a distinct one, they must necessarily be orthogonal. In this spirit, let $\Phi$ be a matrix composed by all the states to be distinguished arranged in columns and with eigenvalues $\{\lambda_i\}$, and $\alpha \equiv \Phi^\dagger \Phi$ where $\alpha_{ij} = \langle \psi_i | \psi_j \rangle$ satisfying $1 \leq \max_i \lambda_i \leq n$, $tr(\alpha) = n$, $0 \leq \det(\alpha) \leq 1$. This matrix can be used to identify how far the states are from the ideal case of being all distinguishable, $\alpha = I$, more concretely using $f(\lambda_i) = \sum_j (\lambda_i - 1)^2 = \sum_j \lambda_j^2 - n$ which has a maximum value of $n^2 - n$ when all the states are the same and a minimum value of 0 when all the states are orthogonal.

This result raises a problem in how to distinct non-orthogonal states. The problem of distinguishing non-orthogonal states is connected to the problem of quantum state cloning: one can argue that by being able to identify a state and being able to prepare it, it is possible to clone it. Distinguishing between non-orthogonal states in an optimum way brings measurements that are optimal according to some criteria. The two more important are the minimum error discrimination, strategy whose solution are measurements that achieve the minimum average probability of error regarding the discrimination, and the unambiguous discrimination, an error-free discrimination method but with a finite probability of an inconclusive result. A useful formalism developed concerning unambiguous discrimination is the Povm (positive operator-valued measure) formalism. It comes forth from

$$E_m \equiv M_m^\dagger M_m, \quad p(m) = \langle \psi | M_m^\dagger M_m | \psi \rangle = \langle \psi | E_m | \psi \rangle , \quad I = \sum_m M_m^\dagger M_m = \sum_m E_m , \quad (2.23)$$

where $\{M_m\}$ are the measurement operators. Attention to the fact that to a positive operator $E_m$ can correspond several measurement operators since any of the form $M_m = U_m \sqrt{E_m}$ satisfy $E_m = M_m^\dagger M_m = \sqrt{E_m} U_m^\dagger U_m \sqrt{E_m} = E_m$, for some unitary operation $U_m$. \quad 9
Such formalism is useful if the post-measurement state is not of concern, and the outcome of the measurement is the object of interest, which is the case in unambiguous discrimination.

The unambiguous discrimination with minimum failure (inconclusive result) probability for two states is

\[
E_1 = 1 - \sqrt{\frac{p_1}{p_2}} |\langle \psi_1 | \psi_2 \rangle|^2, \quad E_2 = 1 - \sqrt{\frac{p_2}{p_1}} |\langle \psi_1 | \psi_2 \rangle|^2, \quad E_3 = I - E_1 - E_2, \tag{2.24}
\]

where \( p_1 \) and \( p_2 \) are the a priori probabilities of the states, i.e. the probability of the corresponding state being prepared; \( |\psi_j\rangle \), \( j = 1, 2 \) are states that are orthogonal to every other states \( |\psi_i\rangle \) such that \( i \neq j \) except state \( |\psi_i\rangle \) with \( i = j \). Hence, \( \langle \psi_1 | E_j | \psi_1 \rangle = P_j \delta_{ij}, \ j, i = 1, 2 \) (where \( P_j \) is a probability) and one is certain that the state measured was \( j \) if outcome \( j \) occurs (if not inconclusive, in the present case corresponds to \( j = 3 \)). One important aspect regarding unambiguous discrimination is that it is only possible if the states are linearly independent.

A bound on the probability of successfully identifying the state for unambiguous discrimination is

\[
P_{\text{success}} \leq 1 - \frac{1}{n-1} \sum_i \sum_{j \neq i} \sqrt{p_i p_j} |\langle \psi_i | \psi_j \rangle|^2 \tag{2.25}
\]

A lower bound is \( P_{\text{success}} \geq \min \lambda_i \) where \( \{ \lambda_i \} \) are the eigenvalues of the matrix \( \alpha \) introduced before. This sets an example of the importance of the superposition between the states to discriminate.

2.3 Quantum Nonlocality and Entanglement

2.3.1 Quantum Nonlocality and Entanglement: Introduction

Foremost, before diving into quantum nonlocality, quantum entanglement is explained.

A group of particles that are in quantum entanglement cannot be described independently of the state of the others. If the state of the particle could be described independently of the group then it would be possible, considering the mathematic formalism used to describe quantum mechanics, to describe the state of the whole group as a tensorial product of the individual states, however this is not possible as it is shown below for a pair of qubits.

\[
|\psi_1\rangle \otimes |\psi_2\rangle = \begin{bmatrix} \alpha_0 \\ \beta_0 \\ \alpha_1 \\ \beta_1 \end{bmatrix} = \begin{bmatrix} \alpha_0 \beta_0 \\ \alpha_0 \beta_1 \\ \alpha_1 \beta_0 \\ \alpha_1 \beta_1 \end{bmatrix} \tag{2.26}
\]

\[
|\psi\rangle = \begin{bmatrix} \gamma_0 \\ \gamma_1 \\ \gamma_2 \\ \gamma_3 \end{bmatrix} \tag{2.27}
\]

Obviously for a quantum system composed of \( N \) qubits to be decomposed in individual independent qubit states means

\[
|\psi\rangle = \otimes_{i=1}^{N} |\psi_i\rangle \tag{2.28}
\]

and in this case, it requires the necessary condition \( \gamma_0 \gamma_3 = \gamma_1 \gamma_2 \) to be satisfied. An entangled state (for this two-qubit system) is any state \( |\psi\rangle \) which cannot be written as \( |\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle \). For quantum systems composed of more qubits, the system state might be decomposable in entangled parts and
parts composed of independent qubit states. Although, for a multiqubit quantum system to be fully decomposable in individual independent qubit states as (2.28) requires meeting the necessary condition

\[ \gamma_0 \gamma_2^{N-1} = \cdots = \gamma_i \gamma_2^{N-1-i} = \cdots = \gamma_2^{i-1} \gamma_1, \quad i = 0, \ldots, 2^{N-1} - 1. \]  (2.29)

One can hence conclude that particles which are entangled effectively lose their individuality.

This entanglement phenomenon is responsible for quantum nonlocality; thus its description is rather important for the description of quantum nonlocality since they are closely related.

What is meant by quantum nonlocality? Quantum nonlocality refers to the apparent ability of objects to attain information about each other’s states instantaneously. Therefore, this phenomenon is in contravention with the principle of locality, which states that an object is directly influenced only by its immediate surroundings. From the special theory of relativity, the speed of such influences is limited to the speed of light. However, for an entangled pair of particles performing a projective measurement in one of the particles instantly collapses the state of the other, regardless of how distant they are, raising this apparent nonlocal behaviour. Therefore, entangled quantum systems however far apart are correlated and cannot be fully described independently of each other.

2.3.2 Entanglement related experiments and games

How is it possible to distinguish if an object has received a property with definite value from its creation, or if that property obtained a definite value when a measurement was made, in a random fashion? The Bell inequalities aid in this matter by evidencing the correlations associated to certain quantum systems in opposition to hidden variables’ models that might describe that system fully.

\textbf{CHSH experiment}

The following experiment is used to study the implications of the previous behaviour from quantum mechanics in the way that the world is perceived, it is named the CHSH experiment.

Such experiment is as follows. Two agents, Alice and Bob, have two particles each with two properties, for Alice’s particle these properties are \( a_0 \) and \( a_1 \), and for Bob’s particle these properties are \( b_0 \) and \( b_1 \). These properties take values \(+1\) or \(-1\). The objective of the experiment is to maximize the expected value of the following quantity:

\[ a_0 b_0 + a_1 b_0 + a_1 b_1 - a_0 b_1. \]  (2.30)

Equation (2.30) determines that the maximization is such that properties \( a_0 \) and \( b_0 \) should have the same value, \( a_1 \) and \( b_0 \) should have the same value, \( a_1 \) and \( b_1 \) should have the same value, \( a_0 \) and \( b_1 \) should have different values (in order to obtain the maximum value possible). Taking into account the possible values for the properties it follows that either \((a_1 - a_0)b_1 = 0\) or \((a_0 + a_1)b_0 = 0\) and is also easy to notice that the quantity (2.30) takes values \(+2\) or \(-2\). With the joint probability distribution of these properties as \( p(a_0, a_1, b_0, b_1) \) the expected value of (2.30) can be bounded from above.

\[
E(a_0 b_0 + a_1 b_0 + a_1 b_1 - a_0 b_1) = \sum_{a_0 a_1 b_0 b_1} p(a_0, a_1, b_0, b_1)(a_0 b_0 + a_1 b_0 + a_1 b_1 - a_0 b_1) \\
\leq \sum_{a_0 a_1 b_0 b_1} p(a_0, a_1, b_0, b_1) \times 2 \\
= 2
\]  (2.31)

Note that

\[ E(a_0 b_1 + a_1 b_0 + a_1 b_1 - a_0 b_1) = E(a_0 b_0) + E(a_1 b_0) + E(a_1 b_1) - E(a_0 b_1). \]  (2.32)
From equations (2.31) and (2.32) one obtains the Bell Inequality:

\[
E(a_0b_0) + E(a_1b_0) + E(a_1b_1) - E(a_0b_1) \leq 2
\]  

(2.33)

The analogous quantum mechanical experiment is performed on the quantum system of two qubits prepared in the state

\[
|\psi\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}} ,
\]  

(2.34)

which could be identified with the singlet state of a pair of electrons (with the $|0\rangle$ corresponding to the spin-up state and the $|1\rangle$ to the spin-down state). The following observables are to be used for the measure of the corresponding properties:

\[
A_0 = Z \quad A_1 = X
\]  

(2.35)

\[
B_0 = -Z - X \quad B_1 = Z - X \quad \sqrt{2}
\]  

(2.36)

Therefore, the expected value of (2.30) can be written noticing that for the state $|\psi\rangle$

\[
\langle A_0 \otimes B_0 \rangle = \frac{1}{\sqrt{2}} \langle A_1 \otimes B_0 \rangle = \frac{1}{\sqrt{2}} \langle A_1 \otimes B_1 \rangle = \frac{1}{\sqrt{2}} \langle A_0 \otimes B_1 \rangle = -\frac{1}{\sqrt{2}} ,
\]  

(2.37)

and thus

\[
\langle A_0 \otimes B_0 \rangle + \langle A_1 \otimes B_0 \rangle + \langle A_1 \otimes B_1 \rangle - \langle A_0 \otimes B_1 \rangle = 2\sqrt{2} > 2.
\]  

(2.38)

It is rather obvious that a contradiction was reached, and only one of (2.33) and (2.38) is correct. To infer which one is incorrect one can perform the quantum mechanical experiment physically, from which it is verified that Bell’s inequality does not hold. Hence, one or more of the assumptions made in its proof must be wrong. The demonstration of Bell’s inequality is based in the assumptions of local realism, in the EPR sense, existing a model with local hidden variables (which cannot be measured but have a definite value) that determines the statistics of the measurement results.

This local realism assumption consists in:

- The assumption that Alice’s measurements do not influence Bob’s measurements and vice versa, known as the assumption of locality.
- The assumption that the properties have definite values independent of observation (in the referred experiment the properties were $a_0$, $a_1$, $b_0$ and $b_1$), known as the assumption of realism.

The experiment’s conclusion is that the world is not locally realistic.

Another interesting test that is also educational on the understanding of quantum nonlocality is the GHZ experiment.

The GHZ test/experiment presented involves three players: Alice, Bob and Charlie. Each player has one particle each having two properties, for Alice’s particle these properties are $a_0$ and $a_1$, for Bob’s particle these properties are $b_0$ and $b_1$ and for Charlie these properties are $c_0$ and $c_1$. These properties take values $+1$ or $-1$. Starting from the quantum mechanical experiment side, the properties are measured using the corresponding observables stated in (2.39),

\[
A_0 = B_0 = C_0 = X \quad A_1 = B_1 = C_1 = Y,
\]  

(2.39)
for a quantum system of three qubits prepared in the state

\[ |\psi\rangle = \frac{|000\rangle + |111\rangle}{\sqrt{2}}. \] (2.40)

It is easily noticeable that

\[ \langle A_0 B_1 C_1 \rangle = -1 \quad \langle A_1 B_0 C_1 \rangle = -1 \]
\[ \langle A_1 B_1 C_0 \rangle = -1 \quad \langle A_0 B_0 C_0 \rangle = 1 \] (2.41)

Now from the EPR perspective, let

\[ E(a_0 b_1 c_1) = E(a_1 b_0 c_1) = E(a_1 b_1 c_0) = -1. \] (2.42)

This implies that \( a_0 b_1 c_1 = a_1 b_0 c_1 = a_1 b_1 c_0 = -1 \) since in every single trial each of these quantities \( a_0 b_1 c_1, a_1 b_0 c_1, a_1 b_1 c_0 \) had to be -1. By multiplying these quantities (and noting that \( a_1^2 = b_1^2 = c_1^2 = 1 \))

\[ (a_0 b_1 c_1)(a_1 b_0 c_1)(a_1 b_1 c_0) = (a_0 b_0 c_0)(a_1^2)(b_1^2)(c_1^2) \]
\[ \iff (-1)(-1)(-1) = (a_0 b_0 c_0)(1)(1)(1) \]
\[ \iff a_0 b_0 c_0 = -1 \] (2.43)

one obtains \( a_0 b_0 c_0 = -1 \) and therefore \( E(a_0 b_0 c_0) = -1 \). Hence an inconsistency between the EPR perspective and the quantum mechanics’ one is met.

Several other tests may be performed in this same spirit and having its physical realization performed, whose results support quantum mechanics.

An inequality for this experiment of the same fashion as (2.33) can be deduced in the form of (2.44).

\[ E(a_0 b_0 c_0) - E(a_0 b_1 c_1) - E(a_1 b_0 c_1) - E(a_1 b_1 c_0) \leq 2 \] (2.44)

Although, the following is also easily deduced,

\[ \langle A_0 B_0 C_0 \rangle - \langle A_0 B_1 C_1 \rangle - \langle A_1 B_0 C_1 \rangle - \langle A_1 B_1 C_0 \rangle = 4 > 2, \] (2.45)
evidencing again the inconsistency.

The Mermin-Peres magic square game

The Mermin-Peres magic square game is another game used to evidence that entanglement provides itself as a useful resource, by correlating systems. It involves a \( 3 \times 3 \) grid and two players, Alice and Bob, which can agree on a strategy in advance, however no communication is allowed once the game starts.

The game’s rules are as follows:

1. A row \( r \in \{1, 2, 3\} \) is picked at random and a column \( c \in \{1, 2, 3\} \) is also picked at random by the referee.
2. The referee sends \( r \) to Alice and \( c \) to Bob.
3. Alice must fill row \( r \) of the grid with an even number of -1 values in its entries \( (\prod_{c'} m_{r,c'} = 1) \), sending the values to the referee.
4. Bob must fill column \( c \) of the grid with an odd number of -1 values in its entries \( (\prod_{r} m_{r,c} = -1) \), sending the values to the referee.
5. The referee verifies Alice filled the row \( r \) with an even number of -1 values and Bob filled the column \( c \) with an odd number of -1 values.

6. The referee checks if the entry corresponding to row \( r \) and column \( c \) was assigned with the same value by Alice and Bob; if so, they win, otherwise they lose.

There is no classical strategy that wins this game with probability one, in fact

\[
\prod_i \left( \prod_j m_{i,j} \right) = 1, \quad \prod_j \left( \prod_i m_{i,j} \right) = -1, \quad \prod_i \left( \prod_j m_{i,j} \right) = \prod_j \left( \prod_i m_{i,j} \right) = 1, \quad \prod_i \left( \prod_j m_{i,j} \right),
\]

which is an obvious contradiction. Moreover, no classical strategy can win the game with probability greater than \( \frac{8}{9} \). From a quantum perspective, it translates into not existing a sure winning “classical” strategy using observables of the form \( \pm I \). An example of a failed solution (in the sense that it does not allow to win with probability 1) that only wins with probability \( \frac{8}{9} \) is presented in table 2.1.

### Table 2.1: 3 x 3 grid with strategy that wins Mermin-Peres magic square game with probability \( \frac{8}{9} \)

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>-1</td>
<td>-1</td>
</tr>
<tr>
<td>-1</td>
<td>1</td>
<td>?</td>
</tr>
</tbody>
</table>

Even though there is no classical strategy that allows the players to win the game with probability 1, there are quantum strategies that do. Reaching towards the Pauli matrices and making use of them and two pairs of quantum entangled qubits to build such a strategy by constructing observables formed by tensor products between two Pauli matrices allows to achieve a winning strategy. A quantum strategy that is a solution to this game is presented in table 2.2.

### Table 2.2: 3 x 3 grid containing a winning quantum strategy for the Mermin-Peres magic square game

| \( \sigma_z \otimes \sigma_z \) | \( I \otimes \sigma_z \) | \( \sigma_z \otimes I \) |
| \( \sigma_x \otimes \sigma_x \) | \( \sigma_x \otimes I \) | \( I \otimes \sigma_x \) |
| \( \sigma_y \otimes \sigma_y \) | \( -\sigma_x \otimes \sigma_z \) | \( -\sigma_z \otimes \sigma_x \) |

Considering the properties of the Pauli matrices it is easy to verify that the observables in a line or in a row commute with each other, so they can be jointly measured. Furthermore, each observable has as eigenvalues +1 and −1. Also easily, it can be checked that the product of the observables on a line is \( I \) and on a column is \( -I \) (this implies that \( \prod_r m_{r,c} = 1 \) and \( \prod_r m_{r,c'} = -1 \), respectively), as desired. Now notice that the eigenvectors of each Pauli matrix can be written as a combination of the eigenvectors of some other Pauli matrix, more precisely

\[
|\psi_x^\pm\rangle = \frac{|\psi_x^+\rangle \pm i |\psi_x^-\rangle}{\sqrt{2}} = \frac{1 \pm i}{\sqrt{2}} |\psi_x^+\rangle + \frac{1 \mp i}{\sqrt{2}} |\psi_x^-\rangle,
\]

\[
|\psi_y^\pm\rangle = \frac{|\psi_y^+\rangle \pm i |\psi_y^-\rangle}{\sqrt{2}} = \frac{1 \pm i}{\sqrt{2}} |\psi_y^+\rangle + \frac{1 \mp i}{\sqrt{2}} |\psi_y^-\rangle,
\]

\[
|\psi_z^\pm\rangle = \frac{|\psi_z^+\rangle \pm i |\psi_z^-\rangle}{\sqrt{2}} = i(\frac{1 \pm i}{\sqrt{2}} |\psi_z^+\rangle \pm |\psi_z^-\rangle).
\]

Hence, if the qubit is in a uniform superposition of eigenvectors of one of the Pauli matrices, then there will be equal probability of obtaining any of the eigenvalues of a Pauli matrix, and if it is measured using a same Pauli matrix as observable twice consecutively, the eigenvalue observed on the second observation will be the same as the one in the first.
The two pairs of entangled qubits that form the state to use in the game are such that

$$|\psi\rangle = \frac{1}{\sqrt{2}} ((|0\rangle_A |0\rangle_B + |1\rangle_A |1\rangle_B) \otimes |\alpha\rangle \langle \alpha| + |\beta\rangle \langle \beta|)$$

$$= \frac{1}{2} (|00\rangle_A |00\rangle_B + |01\rangle_A |01\rangle_B + |10\rangle_A |10\rangle_B + |11\rangle_A |11\rangle_B)$$

(2.48)

and notice that

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}} (|\psi^+_x \psi^+_y\rangle + |\psi^-_x \psi^-_y\rangle) = \frac{1}{\sqrt{2}} (|\psi^+_x \psi^-_y\rangle + |\psi^-_x \psi^+_y\rangle) = \frac{1}{\sqrt{2}} (|\psi^+_y \psi^+_y\rangle + |\psi^-_y \psi^-_y\rangle),$$

(2.49)

which means that the entry corresponding to row $r$ and column $c$ was assigned with the same value by Alice and Bob. To clarify, regarding the $\sigma_y \otimes \sigma_y$ observer the first pair colapses in a state of the form $|\psi^+_y \psi^+_y\rangle$ while the second pair also collapses in one of the states from the same set and note that the eigenkets of such an observable are $|\psi^+_y \psi^+_y\rangle_A |\psi^+_y \psi^+_y\rangle_B \otimes |\psi^+_y \psi^+_y\rangle_A |\psi^-_y \psi^-_y\rangle_B = |\psi^+_y \psi^+_y\rangle_A |\psi^-_y \psi^+_y\rangle_B$ and $|\psi^-_y \psi^-_y\rangle_A |\psi^-_y \psi^-_y\rangle_B \otimes |\psi^-_y \psi^-_y\rangle_A |\psi^+_y \psi^+_y\rangle_B$ for the eigenvalue 1 and in similar manner for $-1$ the corresponding eigenkets are $|\psi^+_y \psi^-_y\rangle_A |\psi^+_y \psi^-_y\rangle_B$ and $|\psi^-_y \psi^+_y\rangle_A |\psi^-_y \psi^+_y\rangle_B$, which evidences that the observer together with the state prepared satisfy the rule presented in item 6 of the list of the game’s rules, since $-1 \cdot -1 = 1 \cdot 1 = 1$ and $-1 \cdot 1 = 1 \cdot -1 = -1$. For the remaining observers, it can also be easily seen that they respect that same rule. Hence, a sure winning strategy for this game is found, which is quantum in nature. Remark that permuting columns or rows in table 2.2 also provides a sure winning strategy.

2.3.3 A final remark

As a final remark, it is pointed out that having $|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$ is different than having the state $|0\rangle$ with probability $p_0 = |\alpha|^2$ or $|1\rangle$ with probability $p_1 = |\beta|^2$. Same as for the Bertlmann’s socks example, where Bertlmann always comes with one pink sock and one not-pink sock, thus if one sees that he is wearing a pink sock on one foot, then one knows the sock on the other foot will not be pink. If one identifies $|0\rangle$ with the sock not being pink and $|1\rangle$ with the sock being pink, then considering that Bertlmann is equally likely to wear the pink sock in either foot, the corresponding state is $|01\rangle$ with probability $1/2$ and $|10\rangle$ with probability $1/2$. This is different than $|\psi\rangle = (|01\rangle + |10\rangle)/\sqrt{2}$, and the reason is the same as for the first case (with $|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$). If one measures $|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$ on the canonical basis, $\{|0\rangle, |1\rangle\}$, then the probability of obtaining each outcome is $|\alpha|^2$ and $|\beta|^2$, and likewise for the related probabilistic case. However if one measures $|\psi\rangle = \alpha (|+\rangle + |-\rangle)/\sqrt{2} + \beta (|+\rangle - |-\rangle)/\sqrt{2} = ((|+\rangle + |\alpha - \beta| |-\rangle))/\sqrt{2}$ on the $\{|+\rangle, |-\rangle\}$ basis, the probability of obtaining each outcome is $|\alpha + \beta|^2/2$ and $|\alpha - \beta|^2/2$, and for the related probabilistic case, the state is $|0\rangle = (|+\rangle + |-\rangle)/\sqrt{2}$ with probability $p_0$, and for such state the probability of obtaining each outcome is $1/2$, also the state is $|1\rangle = (|+\rangle - |-\rangle)/\sqrt{2}$ with probability $p_1$, and for such state the probability of obtaining each outcome is also $1/2$. Hence, for the probabilistic case one obtains $|+\rangle$ with probability $(p_0 + p_1)/2 = 1/2$ and $|-\rangle$ with probability $(p_0 + p_1)/2 = 1/2$, which are not necessarily equal to the corresponding probabilities on the superposition case (where $|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$). Therefore, these descriptions are not equivalent, and represent fundamentally different things.

2.4 The density operator

The density operator presents itself as representing a system in which instead of being in some specific concrete state $|\psi\rangle$, the state is unknown and the system has a certain probability $p_i$ of being in a state $|\psi_i\rangle$. Hence, a density operator is written as

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

(2.50)
In contrast to a certain exact state that a system has, denoted by pure state, which can be represented by a density operator of the form \( \rho = |\psi\rangle \langle \psi| \), a system whose state is an unknown and has a certain probability \( p_i \) of being in one of the several states \( \{ |\psi_i\rangle \} \) is said to be in a mixed state. If a measurement is made it can be imagined that the result is not observed and hence any of the possible post-measurement states could have been obtained, and so the state can be thought has being in a post-measurement state \( |\psi_i\rangle \) with some probability \( p_i \); this is an example of the usefulness of the operator and of what it actually represents. The set \( \{ p_i, |\psi_i\rangle \} \) is called an ensemble of states.

If a system was initially on a mixed state associated to the ensemble \( \{ p_i, |\psi_i\rangle \} \) and a unitary transformation \( U \) is applied then the respective density operator after the transformation is

\[
\rho' = \sum_i p_i U |\psi_i\rangle \langle \psi_i| U^\dagger = U \left( \sum_i p_i |\psi_i\rangle \langle \psi_i| \right) U^\dagger = U \rho U^\dagger, \tag{2.51}
\]

which is associated to the ensemble \( \{ p_i, U |\psi_i\rangle \} \). The density operator is positive, and its trace is 1 due to the probability normalization to 1.

\[
tr(\rho) = tr\left( \sum_i p_i |\psi_i\rangle \langle \psi_i| \right) = \sum_i p_i tr(|\psi_i\rangle \langle \psi_i|) = \sum_i p_i = 1
\]

\[
\langle \varphi | \rho | \varphi \rangle = \sum_i p_i \langle \varphi | \psi_i \rangle \langle \psi_i | \varphi \rangle = \sum_i p_i | \langle \psi_i | \varphi \rangle |^2 \geq 0
\tag{2.52}
\]

Considering any positive and unit trace operator, it has a spectral decomposition \( \rho = \sum_i \lambda_i |i\rangle \langle i| \) with \( \{ \lambda_i \} \) all non-negative, and also \( tr(\rho) = \sum_i \lambda_i = 1 \) so the ensemble of states \( \{ \lambda_i, |i\rangle \} \) forms an ensemble corresponding to the operator \( \rho \).

Let a measurement be made with measurement operators \( \{ M_m \} \) then if the system is in state \( |\psi_i\rangle \) the post-measurement state obtained if outcome \( m \) occurred is

\[
\frac{M_m |\psi_i\rangle}{\sqrt{\langle \psi_i | M_m^\dagger M_m | \psi_i \rangle}} \quad p(m|i) = \langle \psi_i | M_m^\dagger M_m | \psi_i \rangle = tr(M_m |\psi_i\rangle \langle \psi_i| M_m^\dagger) \tag{2.53}
\]

and its associated probability is \( p(m|i) \) (probability of occurrence of outcome \( m \) given that the system was in state \( |\psi_i\rangle \)); \( p(m) \) is obtained from the law of total probability. Then, the resulting density operator is

\[
\rho_m = \sum_i p(i|m) \frac{M_m |\psi_i\rangle \langle \psi_i| M_m^\dagger}{\langle \psi_i | M_m^\dagger M_m | \psi_i \rangle} = \sum_i \frac{p(m|i) p_i |\psi_i\rangle \langle \psi_i| M_m^\dagger}{p(m)} \frac{\langle \psi_i | M_m^\dagger M_m | \psi_i \rangle}{\langle \psi_i | M_m^\dagger M_m | \psi_i \rangle}
\]

\[
= \sum_i \frac{p_i}{tr(M_m^\dagger M_m)} \frac{M_m |\psi_i\rangle \langle \psi_i| M_m^\dagger}{\langle \psi_i | M_m^\dagger M_m | \psi_i \rangle} = \frac{M_m \rho M_m^\dagger}{tr(M_m^\dagger M_m)}, \tag{2.54}
\]

where the Bayes’ rule was used.

If the outcome of the measurement is not known, one has

\[
\rho' = \sum_m p(m) \rho_m = \sum_m tr(M_m^\dagger M_m) \frac{M_m \rho M_m^\dagger}{tr(M_m^\dagger M_m)} = \sum_m M_m \rho M_m^\dagger. \tag{2.55}
\]

It is important to state that a density operator is not specific to an ensemble of states.

\[
\rho = \sum_i \lambda_i |\psi_i\rangle \langle \psi_i| \quad \rho' = \sum_j \gamma_j |\varphi_j\rangle \langle \varphi_j| \quad \rho = \rho' \leftrightarrow \sum_i \langle \tilde{\psi}_i | \langle \tilde{\psi}_i| = \sum_j \langle \tilde{\varphi}_j | \langle \tilde{\varphi}_j| \quad \rho = \rho' \leftrightarrow \sum_i \langle \tilde{\psi}_i | \langle \tilde{\psi}_i| = \sum_j \langle \tilde{\varphi}_j | \langle \tilde{\varphi}_j| = \delta_{kk}, \tag{2.56}
\]

\[
\rho = \sum_i l_{ij} |\tilde{\psi}_i\rangle \langle \tilde{\psi}_i| = \sum_j \langle \tilde{\varphi}_j | \langle \tilde{\varphi}_j| = \sum_j \left( \sum_{kh} l_{jk} l_{jh}^* \langle \tilde{\psi}_k| \langle \tilde{\varphi}_h| = \sqrt{\gamma_j} |\varphi_j\rangle \right) \quad \rho' = \sum_i |\tilde{\psi}_i\rangle \langle \tilde{\psi}_i| = \sum_j \left( \sum_{kh} l_{jk} l_{jh}^* \langle \tilde{\psi}_k| \langle \tilde{\psi}_h| = \delta_{kk}, \right.
\]
where the \( \{ \lambda_i \} \) are the positive eigenvalues of the density operator and \( \{ \psi_i \} \) the respective eigenvectors. The columns of the matrix \( L \) are orthonormal and can be appended with extra columns, which are orthonormal vectors with the remaining columns of \( L \) thus forming an orthonormal basis and making of \( L \) a unitary matrix, call it \( \tilde{L} \), and so \( \{ | \tilde{\psi}_i \rangle \} \) is also extended with 0 vectors, call this extension \( \{ | \tilde{\psi}'_i \rangle \} \), from which \( | \tilde{\varphi}_k \rangle = \sum_i \tilde{L}_{ki} | \tilde{\psi}'_i \rangle = \sum_i L_{ki} | \tilde{\psi}_i \rangle \). Any other density operator equal to \( \rho = \rho'' = \sum_i \alpha_i | \epsilon_i \rangle \langle \epsilon_i | \), by a similar reasoning, can have its ensemble expressed as \( | \tilde{\epsilon}_j \rangle = \sum_i \tilde{v}_{ij} | \psi''_i \rangle \) (with the extension of appropriate size). To relate \( \{ | \tilde{\epsilon}_j \rangle \} \) with \( \{ | \tilde{\varphi}_k \rangle \} \) by a unitary matrix, the smallest set has to be extended with 0 vectors, and \( \{ | \tilde{\psi}'_i \rangle \} \) is also extended to that same size with 0 vectors. Thus, it holds that \( | \tilde{\psi}'_i \rangle = \sum_i \tilde{v}_{ij} | \epsilon_j \rangle \), and that \( | \tilde{\varphi}_k \rangle = \sum_i \sum_k \tilde{L}_{ki} \tilde{v}_{ij} | \epsilon_j \rangle \) from which it is noted that the relation between two ensembles which are represented with a same density operator is given by the unitary matrix \( U = \tilde{L} \tilde{V}^\dagger \) relating the vectors \( \{ \tilde{\varphi}_k \} \) and \( \{ \tilde{\epsilon}_j \} \). Conversely, having \( | \tilde{\varphi}_k \rangle = \sum_j u_{kj} | \epsilon_j \rangle \) then

\[
\sum_i | \tilde{\varphi}_i \rangle \langle \tilde{\varphi}_i | = \sum_i \sum_j u_{ij} u_{ij}^* | \epsilon_j \rangle \langle \epsilon_j | = \sum_j \left( \sum_i u_{ij}^* u_{ij} \right) | \epsilon_j \rangle \langle \epsilon_j | = \sum_j | \epsilon_j \rangle \langle \epsilon_j | \quad (2.57)
\]

which shows that they both have the same density operator. Hence, the ensemble associated to the sets of states \( \{ | \tilde{\varphi}_k \rangle \} \) and \( \{ | \tilde{\epsilon}_j \rangle \} \) are represented by the same density operator if and only if \( | \tilde{\varphi}_k \rangle = \sum_j u_{kj} | \epsilon_j \rangle \) where \( U \) is a unitary matrix and where the sets of vectors \( \{ | \tilde{\varphi}_k \rangle \} \) and \( \{ | \tilde{\epsilon}_j \rangle \} \) may have zero vectors included so as to make the cardinality of the sets equal and thus leaving the matrix \( U \) as a square and unitary matrix.

In section 2.7 it will be proved that for a mixed state \( tr(\rho^2) < 1 \) while for a pure state it is easily seen that \( tr(\rho^2) = 1 \).

### 2.5 The partial trace

Consider a system which is taken to be bipartite with subsystems \( A \) and \( B \) and whose density operator is \( \rho_{AB} \). It is wished to describe each subsystem by a respective density operator, implying that any correlations between \( A \) and \( B \) are discarded. One solely observes the subsystem, which is the part of the system available. Then, the measurement statistics of a measurement applied to the subsystem should be the same as the corresponding to the same measurement on the whole system (the measurement is the same), hence

\[
p(i) = \frac{tr(P_i \rho_{A} P_i^\dagger)}{f_1} = \frac{tr((P_i^\dagger \otimes I) \rho_{AB} (P_i \otimes I))}{f_2}
\]

\[
\begin{align*}
 f_1 &= \sum_{a} \langle a|_A \rho_{A} P_i^\dagger |a\rangle_A \\
 f_2 &= \sum_{a} \sum_{b} \langle a|_A \langle b|_B (P_i \otimes I) \rho_{AB} (P_i \otimes I) |a\rangle_A |b\rangle_B \rightarrow \rho_A = \sum_{b} \langle b|_B \rho_{AB} |b\rangle_B ,
\end{align*}
\]

where \( \{ |a\rangle_A \} \) is an orthonormal basis of \( A \), \( \{ |b\rangle_B \} \) is an orthonormal basis of \( B \) and \( \{ P_i \} \) are the measurement operators. \( \rho_A \) is referred to as the reduced density operator of system \( A \), and it is obtained by taking the partial trace of the overall system over system \( B \), i.e. \( tr_B(\rho_{AB}) = \sum_{b} \langle b|_B \rho_{AB} |b\rangle_B \) which can be verified to result in an operator with the properties of a density operator. It is also true that \( tr_B(\sum_{b} \langle b|_B \rho_{AB} |b\rangle_B) = tr_B(\rho_{AB}) \) and so the partial trace of \( B \) is also equivalent to measuring system \( B \) in an orthonormal basis without acquiring knowledge regarding the outcome. The following can also be seen to hold: \( tr(\rho_{AB}) = tr_A(tr_B(\rho_{AB})) = tr_B(tr_A(\rho_{AB})) \). The density operator \( \rho_{AB} \) can be written as

\[
\rho_{AB} = \sum_{ij} \sum_{kl} c_{ijkl} |i\rangle_A \langle k| \langle k| \rightarrow \rho_A = tr_B(\rho_{AB}) = \sum_{ij} \left( \sum_k c_{ijkk} \right) |i\rangle_A \langle j|_A \quad (2.59)
\]
resulting in the form for $\rho_A$ in terms of such decomposition. If $\rho_{AB} = \rho_A \otimes \rho_B$ meaning $AB$ is in a product state, then $tr_B(\rho_{AB}) = \rho_A tr_B(\rho_B) = \rho_A$, as it would be expected. An example of application of the partial trace: if system $AB$ is in the entangled pure state $\frac{|01\rangle + |10\rangle}{\sqrt{2}}$, the partial trace over $A$ or over $B$ (the system is in a symmetric state regarding both subsystems) of the system results in the reduced density operator $\rho_A = \frac{|0\rangle \langle 0| + |1\rangle \langle 1|}{2}$, which means that the subsystem is in state $|0\rangle$ or $|1\rangle$ with equal probability; note that the correlations between the subsystems are discarded in the reduced density operator of each, which is in a maximally mixed state.

2.6 Schmidt decomposition, purification and entanglement

**Theorem 2.6.1** (Schmidt decomposition [13]). Let $|\psi\rangle$ be a pure state of a composite system $AB$. Then, there exist orthonormal basis $\{k_A\}$ and $\{k_B\}$ for systems $A$ and $B$ with state space dimensions $n$ and $m \leq n$, respectively, such that

$$|\psi\rangle = \sum_{k=1}^{m} \lambda_k |k_A\rangle |k_B\rangle,$$

where $\lambda_i \geq 0$ and satisfy $\sum_i \lambda_i^2 = 1$.

**Proof.** Let $\{|i_A\rangle\}$ and $\{|j_B\rangle\}$ be any fixed orthonormal bases for systems $A$ and $B$, respectively. Then $|\psi\rangle$ can be written as

$$|\psi\rangle = \sum_{ij} a_{ij} |i_A\rangle |j_B\rangle$$

for some complex matrix $A$ of size $n \times m$. The singular value decomposition of a rectangular matrix can be expressed as

$$A = UD'V = U \begin{bmatrix} D \\ 0 \end{bmatrix} V$$

where $U$ and $V$ are unitary matrices and $D$ is an $m \times m$ diagonal matrix with non-negative elements. Hence, it follows that

$$|\psi\rangle = \sum_{k=1}^{m} \sum_{k'=1}^{m} \sum_{j=1}^{m} a_{ik} d_{k'k} v_{kj} |i_A\rangle |j_B\rangle = \sum_{k=1}^{m} \sum_{k'=1}^{m} \sum_{j=1}^{m} a_{ik} d_{k'k} v_{kj} |i_A\rangle |j_B\rangle$$

$$= \sum_{k=1}^{m} \sum_{i=1}^{n} \sum_{j=1}^{m} a_{ik} d_{k'k} v_{kj} |i_A\rangle |j_B\rangle = \sum_{k=1}^{m} d_{kk} |k_A\rangle |k_B\rangle = \sum_{k=1}^{m} \lambda_k |k_A\rangle |k_B\rangle,$$

defining $|k_A\rangle \equiv \sum_{i=1}^{n} u_{ik} |i\rangle$, $|k_B\rangle \equiv \sum_{j=1}^{m} v_{kj} |j\rangle$, and $\lambda_k \equiv d_{kk}$. The $\{k_A\}$ are part of an orthonormal basis for system $A$ and the $\{k_B\}$ form an orthonormal basis for system $B$. The property $\sum_i \lambda_i^2 = 1$ follows from the fact that $\langle \psi | \psi \rangle = 1$.

Clearly, $\rho_A = tr_B(|\psi\rangle \langle \psi|) = \sum_{k=1}^{m} \lambda_k^2 |k_A\rangle \langle k_A|$, and $\rho_B = tr_A(|\psi\rangle \langle \psi|) = \sum_{k=1}^{m} \lambda_k^2 |k_B\rangle \langle k_B|$. From the Schmidt decomposition, it can be said that the state is separable if and only if $\lambda_i = 1$ for some (unique) value of $i$ (all other $\lambda_i$s are 0), however if more than one is non-zero the state is an entangled state, and in the particular case where all $\lambda_i$s are equal and different than zero, it is said to be maximally entangled. Hence, the number of non-zero $\lambda_i$s, called the Schmidt number, quantifies to some extent the entanglement of the state $|\psi\rangle$. Generalizing to multi-partite systems, one could decompose the state analogously (according to its subsystems), and take the decomposition with minimum number of non-zero coefficients and consider that number as a quantifier of the entanglement of the state.

A particular interesting way to measure entanglement is described in [14] which uses the stabilizer formalism presented in section 4.4. It takes the $n$-qubit state and its corresponding stabilizer, that state
is then split into \( k \) partitions, and the entanglement measure is given by

\[
e_A(\ket{\psi}) = n - \left| \prod_{j=1}^{k} S_j \right| \tag{2.64}
\]

with \(|\cdot|\) denoting the size of the minimal generating set of the group, and where the \( \{S_j\} \) contain the local operations of \( S \) that act as identity on partitions \( \{A_j\} \) of the state. For a bipartite state, the entanglement measure is simple to understand. The stabilizer is split into a local part, \( S_A \cdot S_B \) (with generators of the form \( a_i \otimes I_B \) and \( I_A \otimes b_j \), respectively) and the part accounting for the correlations \( S_{AB} \) (where the system is \( AB \), and the generators of \( S_{AB} \) have the form \( g^A_m \otimes g^B_m \)). Thus, the \( S_A \) and \( S_B \) contain the local operations that act as identity on the corresponding partitions. This partitioning of the stabilizer is illustrated in figure 2.1. The entanglement measure in this case is simply \(|S_{AB}|\). Considering the state \((\ket{00} + \ket{11})/\sqrt{2}\) stabilized by \( S = \langle XX, ZZ \rangle \), one has \( S_A = S_B = \{I\} \) and \( S_{AB} = S \). For the state \((\ket{000} + \ket{111})/\sqrt{2}\) the corresponding stabilizer is \( S = \langle XXX, ZZI, IZZ \rangle \), and considering the first two qubits as the partition \( A \) and the remaining qubit as the partition \( B \), one has \( S_A = \{ZZI\}, S_B = \{I\} \) and \( S_{AB} = \{XXX, IZZ\} \). For both the states considered, \(|S_{AB}| = 2\). For bipartite states, \(2.64\) is \(|S_{AB}|\), and it becomes clear that \(2.64\) is a measure of the correlations among the partitions and is therefore a measure for multipartite entanglement. This measure provides an efficient and elegant way of measuring entanglement of stabilizer states. Other entanglement measures can be conceived, but they should all respect some properties (among others) in order to be valid measures, such as the measure being invariant to local unitary transformations (since entanglement can only be created by interacting both systems), measurements on the state can only leave constant or reduce the value of the entanglement measure, and the minimum value of the entanglement measure should be achieved for fully separable states.

Consider now a density operator that represents an ensemble of pure states, a possible abstraction (might be the case in reality or not) is that such an ensemble is obtained by considering only part of a bigger system, being that part entangled with the rest of it. If the system in question is \( A \), then one can take the system \( AR \) to be the overall system where \( R \) is a reference system which is not accessible, and the density operator obtained for \( A \) is a reduced density operator. This method of going from \( A \) to \( AR \) is called purification, since one goes from a mixed state to a pure state. Let \( \rho_A = \sum_i p_i \ket{i} \bra{i}_A \), then let

\[
S_A \left( \begin{array}{cc} a_i & \otimes I_B \\ \end{array} \right) (1 \leq i \leq |S_A|)
\]

\[
S_{AB} \left( \begin{array}{cc} g^A_k & \otimes g^B_k \\ \end{array} \right) (1 \leq k \leq p)
\]

\[
S_B \left( \begin{array}{cc} I_A & \otimes b_j \\ \end{array} \right) (1 \leq j \leq |S_B|)
\]
the state for the combined system be
\[ |\psi\rangle_{AR} = \sum_i \sqrt{P_i} |i\rangle_A |i\rangle_R, \] (2.65)
which is a pure state. Thus it should be true that \( p_A = tr_R(|\psi\rangle \langle \psi|_{AR}) \), so
\[ tr_R(|\psi\rangle \langle \psi|_{AR}) = \sum_{ij} \sqrt{P_i P_j} |i\rangle_A \langle i|_A \langle j|_R tr_R(|j\rangle_R \langle j|_R) = \sum_{ij} \sqrt{P_i P_j} |i\rangle_A \delta_{ij} = \sum_i \sqrt{P_i} |i\rangle_A = p_A \] (2.66)
holds, where \( \{ |i\rangle_R \} \) form (or are part of) an orthonormal basis for the state space of system \( R \). Therefore \( |\psi\rangle_{AR} \) is a purification of \( p_A \). It is clear that another purification \( |\psi'\rangle_{AR} \) can be obtained by a change of basis, \( |\psi'\rangle_{AR} = (I_A \otimes U_R) |\psi\rangle_{AR} \). It is also possible to use a reference system \( R' \) such that \( \dim(H_R) \leq \dim(H_{R'}) \) (with \( \dim(H_A) \leq \dim(H_{R'}) \) always holding) with \( \{ |i\rangle_{R'} \} \) part of an orthonormal basis for the state space of system \( R' \). From these considerations, \( p_A (p_B) \) is pure if and only if the global state is separable, i.e. if \( |\psi\rangle_{AB} \) is a pure state. It is clear that if the global state \( |\psi\rangle_{AB} \) is separable then \( p_A (p_B) \) is pure, now for the converse let \( |\psi\rangle_{AB} = \sum_i \lambda_i |i\rangle_A |i\rangle_B \) (using the Schmidt decomposition), then
\[ p_A = tr_B (p_{AB}) = \sum_i \lambda_i^2 |i\rangle_A \langle i|_A = |i\rangle_A \langle i|_A \] (2.67)
for some \( i \), since \( p_A \) is pure and therefore \( p_{AB} = |\psi\rangle \langle \psi|_{AB} \) with \( |\psi\rangle_{AB} = |i\rangle_A |i\rangle_B \), being \( p_{AB} \) in a pure product state.

### 2.7 Bloch Sphere Representation

The Bloch sphere representation of quantum states allows for a visual representation of the effect of an operation/transformation on them. It is particularly useful in the analysis of the effect of certain quantum channels used in quantum information.

Starting by writing the coefficients of a single qubit in polar coordinates,
\[ a |0\rangle + b |1\rangle = r_a e^{i \theta_a} |0\rangle + r_b e^{i \theta_b} |1\rangle = e^{i \theta_a} (r_a |0\rangle + r_b e^{i (\theta_b - \theta_a)} |1\rangle), \] (2.68)
and recalling that the representation of a state is unique apart from global phase factor, and renaming \( r_a \) as \( z \), and turning to cartesian coordinates, \( x + iy = r_a e^{i(\theta_b - \theta_a)} \), one obtains
\[ |\psi\rangle = z |0\rangle + (x + iy) |1\rangle \] (2.69)
and
\[ \langle \psi|\psi\rangle = 1 \iff x^2 + y^2 + z^2 = 1, \] (2.70)
which results in an equation of a sphere of radius 1. Hence, it is obtained the following 3-dimensional vector written in spherical coordinates:
\[ (x, y, z) = (r \sin \theta' \cos \phi, r \sin \theta' \sin \phi, r \cos \theta'), \quad r = 1, \quad \theta' \in [0, \pi), \quad \phi \in [0, 2\pi]. \] (2.71)

A complex global phase factor was set aside in the previous reasoning, however no actual restriction was imposed on \( r_a \) so that it would be always non-negative or non-positive, allowing the redundancy \( |\psi\rangle = -|\phi\rangle \) in the representation, not obtaining a one to one correspondence between a point \((x, y, z)\) on the sphere and a state \(|\psi\rangle\).
\[ |\psi\rangle = -|\phi\rangle \iff \cos \theta' |0\rangle + \sin \theta' (\cos \phi + \sin \phi) |1\rangle = -\cos \theta'' |0\rangle - \sin \theta'' (\cos \phi' + \sin \phi') |1\rangle \]
\[ \iff \cos \theta' |0\rangle + \sin \theta' (\cos \phi + \sin \phi) |1\rangle = \cos (\pi - \theta'') |0\rangle \]
\[ + \sin (\pi - \theta'') (\cos (\pi + \phi') + \sin (\pi + \phi')) |1\rangle \]
\[ \iff \theta' = \pi - \theta'' + 2\pi k, \quad \phi = \pi + \phi' + 2\pi l, \quad k, l \in \mathbb{Z} \] (2.72)
This result implies diagonally opposite points correspond to the same state (differing from a global phase of \(-1\)). Imposing \(r_a \geq 0\) is equivalent to

\[
\cos \theta' \geq 0 \iff 0 \leq \theta' \leq \frac{\pi}{2}.
\]

(2.73)

Therefore, by making \(\theta = \theta'\), a one to one correspondence between a point \((x, y, z)\) on a sphere and a quantum state can be achieved.

<table>
<thead>
<tr>
<th>State Vector Representation</th>
<th>Bloch Sphere Representation</th>
</tr>
</thead>
<tbody>
<tr>
<td>(\cos \frac{\theta}{2}</td>
<td>0\rangle + \sin \frac{\theta}{2} e^{i\phi}</td>
</tr>
</tbody>
</table>

Taking the inner product between two quantum states,

\[
\langle \psi | \varphi \rangle = \cos \frac{\theta_0}{2} \cos \frac{\theta_1}{2} + e^{i(\phi_1 - \phi_0)} \sin \frac{\theta_0}{2} \sin \frac{\theta_1}{2}
\]

\[
= \cos (\phi_1 - \phi_0) \sin \frac{\theta_0}{2} \sin \frac{\theta_1}{2} + \cos \theta_0 \cos \theta_1
\]

\[
+ i \sin (\phi_1 - \phi_0) \sin \frac{\theta_0}{2} \sin \frac{\theta_1}{2}
\]

(2.74)

and finding the conditions so that they are orthogonal,

\[
\langle \psi | \varphi \rangle = 0
\]

\[
\iff \begin{cases} 
0 = \cos (\phi_1 - \phi_0) \sin \frac{\theta_0}{2} \sin \frac{\theta_1}{2} + \cos \theta_0 \cos \theta_1 \\
0 = \sin (\phi_1 - \phi_0) \sin \frac{\theta_0}{2} \sin \frac{\theta_1}{2}
\end{cases}
\]

\[
\iff \begin{cases} 
0 = \cos (\phi_1 - \phi_0) \sin \frac{\theta_0}{2} \sin \frac{\theta_1}{2} + \cos \theta_0 \cos \theta_1 \\
\theta_0 = 0 \lor \theta_1 = 0 \lor \phi_1 = \phi_0 \lor \phi_1 = \pi + \phi_0 = \pi + \phi_1
\end{cases}
\]

(2.75)

\[
\phi_1 = \phi_0 \Rightarrow \theta_0 = 0 \lor \theta_1 = \pi \lor \phi_0 = \pi + \phi_1
\]

\[
\Rightarrow \theta_1 = \pi \Rightarrow \theta_0 = \pi
\]

\[
\phi_1 = \pi + \phi_0 \Rightarrow \theta_0 = 0 \lor \theta_1 = \pi \lor \phi_0 = \pi + \phi_1
\]

(2.76)

Concluding that orthogonal states are diagonally opposite in the Bloch sphere, i.e. antipodal. For \(\theta = 0\) the state \(|0\rangle\) is obtained and for \(\theta = \pi\) one obtains the state \(|1\rangle\). For the remaining axis, \(\theta = \frac{\pi}{2}\) and the values \(0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}\) for \(\phi\) yield the states \(|+\rangle, |i\rangle, |-\rangle, |-i\rangle\). The Bloch sphere is illustrated in figure 2.2.

From the Bloch sphere it is possible understand that states in the equator correspond to states with maximal superposition and the lower or upper the state is in the sphere the bigger is the weight of \(|1\rangle\) or \(|0\rangle\) (in respect to the other), respectively, on the superposition. Some other interesting properties.
are that rotations in the Bloch sphere in respect to each of the axis correspond to the rotation matrices defined as

\[ R_x(\theta) \equiv e^{-i\frac{\theta}{2}X}, \quad R_y(\theta) \equiv e^{-i\frac{\theta}{2}Y}, \quad R_z(\theta) \equiv e^{-i\frac{\theta}{2}Z}. \tag{2.77} \]

Consider now the state in terms of a density operator description, operator which has trace equal to one and is Hermitian, and that can be described by

\[ \rho = \frac{1}{2} \begin{bmatrix} 1 + r_z & r_x - i r_y & 0 \\ r_x + i r_y & 1 - r_z & 0 \\ 0 & 0 & 0 \end{bmatrix} \tag{2.78} \]

and is equivalent to

\[ \rho = \frac{I + \vec{r} \cdot \vec{\sigma}}{2}, \quad \vec{r} = (r_x, r_y, r_z), \quad \vec{\sigma} = (\sigma_x, \sigma_y, \sigma_z). \tag{2.79} \]

Expressing the density operator for a pure state one obtains

\[ \rho = |\psi\rangle \langle \psi| = \begin{bmatrix} \cos^2 \frac{\theta}{2} & \cos \frac{\theta}{2} \sin \frac{\theta}{2} e^{-i\phi} \\ \cos \frac{\theta}{2} \sin \frac{\theta}{2} e^{i\phi} & \sin^2 \frac{\theta}{2} \end{bmatrix}, \tag{2.80} \]

which corresponds to \( \vec{r} = (\sin \theta \cos \phi, \sin \theta \sin \phi, \cos \theta) \) in (2.79), which is the position of the state in the Bloch sphere.

From the definition of a pure state, it is obvious that the correspondent density matrix has a null eigenvalue and therefore its determinant is zero, which by (2.78) results in \( \| \vec{r} \| = 1 \), confirming that a pure state belongs to the Bloch sphere. For mixed states, having \( \rho \) a spectral decomposition, since it is positive, one has

\[ \rho = \sum_j \lambda_j \langle j | j \rangle, \quad \rho^2 = \sum_j \lambda_j^2 \langle j | j \rangle. \tag{2.81} \]

\( \rho^2 \) also has one where \( \{ |j\rangle \} \) are orthonormal and \( \lambda_j \) are real non-negative eigenvalues of \( \rho \). Thus the following inequalities hold

\[ tr(\rho^2) = \sum_j \lambda_j^2 \leq \lambda_{\text{max}} \sum_j \lambda_j = \lambda_{\text{max}} \cdot tr(\rho) = \lambda_{\text{max}} < 1, \tag{2.82} \]
where $\lambda_{\text{max}} = \max_j \lambda_j$ and $\lambda_{\text{max}} < 1$ due to fact that there are more than one non-null eigenvalues for a mixed state and $\sum_j \lambda_j = 1$. Hence, using (2.78):

$$\text{tr}(\rho^2) = \frac{1}{2} (1 + \| \vec{r} \|^2) < 1 \iff \| \vec{r} \| < 1.$$  

(2.83)

This leads to the conclusion that mixed states are inside the "Bloch ball", since their position satisfies $\| \vec{r} \| < 1$, while pure states are in the surface of the ball ($\| \vec{r} \| = 1$), the Bloch sphere. In fact, the maximally mixed state with $\rho = \frac{1}{2}$ corresponds to the origin (center) of the ball.

Another use of this representation: Let the state $|\psi\rangle = \alpha |+\rangle + \beta |-\rangle$ be identified with a photon’s polarization which is a linear combination of the states of positive helicity $|+\rangle$ and negative helicity $|-\rangle$. According to [16] the polarization ellipse and its correct orientation can be obtained from the state represented in a Riemann sphere. Hence, assuming the photon is travelling upwards in the direction of $|+\rangle$, by projecting orthogonally the circle (whose borders coincide with the sphere’s borders, and whose orientation is right-handed about the Stokes vector) in the diametral plane perpendicular to the Stokes vector into the equatorial plane, one obtains the referred ellipse with the correct orientation (figure 2.3).

![Figure 2.3: Photon polarization represented on a Riemann sphere. Adapted from: [16].](image-url)
Chapter 3
Quantum circuits and quantum gates

3.1 Quantum gates

In quantum mechanics, the time evolution of a closed quantum system is described by a unitary transformation ($U$ is unitary $\iff U^\dagger = U^{-1}$). Such a transformation preserves inner products and therefore probability normalization. Moreover, it is reversible by definition and therefore the computations on a quantum computer are reversible and the quantum gates represent unitary operations. This differs from classical computers which contain several irreversible gates (e.g. AND).

Quantum gates that differ from each other by a global phase factor are considered the same. The most common single qubit gates are presented in figure 3.1. A quantum circuit is comprised by a sequence of gates and possibly measurement operations applied to a set of qubits. In a quantum circuit a wire (diagrammatically represented by a single line) represents a qubit, more specifically the history of the qubit in terms of transformations applied to it, read from left to right. For operations that involve multiple qubits, the CNOT (controlled-NOT) flips the target qubit (bottom one in the gate of figure 3.2) according to the state of the control qubit, i.e. $|c\rangle |t\rangle \rightarrow |c\rangle |t \oplus c\rangle$, more concretely. In the action of the CNOT gate, the target qubit flips if the control qubit is 1, but if it is desired that it flips on 0 the flipped control bit is considered (represented by a hollow disc, a circle) as in figure 3.3. A more general version of a controlled gate is $|c_1 \ldots c_n\rangle |t\rangle \rightarrow |c_1 \ldots c_n\rangle U_{c_1 c_2 \ldots c_n} |t\rangle$ represented in the form of quantum gate in figure 3.4.

![Figure 3.1: Name, matrix and gate symbol of the most common single qubit gates. Source: [13].](image)

<table>
<thead>
<tr>
<th>Gate</th>
<th>Matrix</th>
<th>Gate Symbol</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hadamard</td>
<td>$\frac{1}{\sqrt{2}} \begin{bmatrix} 1 &amp; 1 \ 1 &amp; -1 \end{bmatrix}$</td>
<td>$H$</td>
</tr>
<tr>
<td>Pauli-X</td>
<td>$\begin{bmatrix} 0 &amp; 1 \ 1 &amp; 0 \end{bmatrix}$</td>
<td>$X$</td>
</tr>
<tr>
<td>Pauli-Y</td>
<td>$\begin{bmatrix} 0 &amp; -i \ i &amp; 0 \end{bmatrix}$</td>
<td>$Y$</td>
</tr>
<tr>
<td>Pauli-Z</td>
<td>$\begin{bmatrix} 1 &amp; 0 \ 0 &amp; -1 \end{bmatrix}$</td>
<td>$Z$</td>
</tr>
<tr>
<td>Phase</td>
<td>$\begin{bmatrix} 1 &amp; 0 \ 0 &amp; i \end{bmatrix}$</td>
<td>$S$</td>
</tr>
<tr>
<td>$\frac{\pi}{8}$</td>
<td>$\begin{bmatrix} 1 &amp; 0 \ 0 &amp; e^{\frac{i\pi}{4}} \end{bmatrix}$</td>
<td>$T$</td>
</tr>
</tbody>
</table>
3.2 Measurement on quantum circuits

Concerning the operation of measurement in quantum circuits, a projective measurement in the computational basis is represented by a meter symbol (figure 3.5). The double-line wire represents the bit associated to the outcome of the measurement, since the outcome is usually the result of interest (which might be used to condition future computations) and not the qubits in the post-measurement state (might be lost in the measurement process). If the single-line wire is used instead of the double-line one in figure 3.5, then one is referring to the post-measurement state. Two important principles about quantum circuits in what regards measurements are the principle of deferred measurement and the principle of implicit measurement.

Principle of implicit measurement: Without loss of generality, any unterminated quantum wires (qubits which are not measured) at the end of a quantum circuit may be assumed to be measured.

To verify that such a principle holds, consider the following equation:

$$
\rho = \sum c_i P_i^1 \otimes \ldots \otimes P_i^n, \quad \Pi_i^B = \bigotimes_j \Gamma_j^i, \quad \Gamma_j^i = \begin{cases} 
\Pi_{k_{i,j}} | \{ j : j = b_i \} & \text{if } j \in \{ b_i \} \\
I_{2 \times 2} & \text{if } j / \in \{ b_i \} 
\end{cases}, \quad i = \sum k_{i,j} 2^{j-1}
$$

$$
tr_B(\rho') = tr_B \left( \rho \left( \sum_i \Pi_i^B \right) \right) = \sum_i c_i P_i^{a_1} \otimes \ldots \otimes P_i^{a_N} tr \left( (P_i^{b_1} \otimes \ldots \otimes P_i^{b_N}) \left( \sum_i \Pi_i^B \right) \right) = tr_B(\rho),
$$

(3.1)

where the density matrix is written in terms of a linear combination of a tensor product of characteristic 1 matrices of dimension 2 (such a decomposition is always possible), $m$ is the number of qubits ($m = n + N$), $n$ is the number of qubits belonging to subsystem $B$, $N$ is the number of qubits belonging to subsystem $A$, $\{a_i\}$ is the set of the indices of the qubits that belong to $A$, and analogously $\{b_i\}$ is the set of the indices of the qubits that belong to $B$. $\{\Pi_i^B\}$ is the set of all projection operators in the computational basis of subsystem $B$, which are written in (3.1) in terms of projection operators on each qubit. From (3.1) it is concluded that performing a projective measurement in $B$ does not alter the statistics of $A$, since $tr_B(\rho' = \sum_i \Pi_i^B \rho \Pi_i^B) = tr_B(\rho)$. This principle can be easily seen from the considerations on the section regarding the partial trace which mentions the previous argument.

Principle of deferred measurement: Measurements can always be moved from an intermediate stage of a quantum circuit to the end of the circuit; if the measurement results are
used at any stage of the circuit then the classically controlled operations can be replaced by conditional quantum operations.

To prove this principle, figure 3.6 presents the scheme which the proof follows.

Letting the qubits from $C$ be an auxiliary measurement apparatus, $A$ the subsystem to be measured and $B$ the remaining subsystem, $CNOT$s are applied from $A$ to $C$, then following the circuit and performing a measurement to $C$ in the end allows to conclude that the resulting final state is the same as when the measurement is applied to $A$ in the middle of the circuit. From this, a proof using density
operators is easily designed.

\[ \rho' = \sum_k p_k |\psi_k\rangle \langle \psi_k | = \sum_k p_k \sum_{i,j} (a_j^k)^* a_i^k |i\rangle \langle j | \otimes |b_k^j\rangle \langle b_k^j | \otimes |i\rangle \langle j | \]

\[ \rightarrow \rho'' = (U_2 \otimes I) \rho' (U_2^\dagger \otimes I) = \sum_k p_k \sum_{i,j} (a_j^k)^* a_i^k U_2 |i\rangle \langle j | \otimes |b_k^j\rangle \langle b_k^j | U_2^\dagger \otimes |i\rangle \langle j | \]

\[ \rightarrow \sum_l (I \otimes I \otimes |l\rangle \langle l |) \rho'' (I \otimes I \otimes |l\rangle \langle l |) = \sum_k p_k \sum_l |a_l^k|^2 U_2 (|l\rangle \langle l | \otimes |b_k^l\rangle \langle b_k^l | U_2^\dagger \otimes |l\rangle \langle l |) \]

\[ tr_C(\rho'') = tr_C \left( \sum_l |l\rangle \langle l | C \rho'' |l\rangle \langle l | \right) = \sum_k p_k \sum_l |a_l^k|^2 U_2 (|l\rangle \langle l | \otimes |b_k^l\rangle \langle b_k^l | U_2^\dagger \right) \tag{3.5} \]

\[ \rho = \sum_k p_k |\phi_k\rangle \langle \phi_k | = \sum_k p_k \sum_{i,j} (a_j^k)^* a_i^k |i\rangle \langle j | \otimes |b_k^j\rangle \langle b_k^j | \]

\[ \rightarrow \sum_l (|l\rangle \langle l | \otimes I) \rho (|l\rangle \langle l | \otimes I) = \sum_k p_k \sum_l |a_l^k|^2 |l\rangle \langle l | \otimes |b_k^l\rangle \langle b_k^l | \]

\[ \rightarrow U_2 (\sum_l (|l\rangle \langle l | \otimes I) \rho (|l\rangle \langle l | \otimes I)) U_2^\dagger = \sum_k p_k \sum_l |a_l^k|^2 U_2 (|l\rangle \langle l | \otimes |b_k^l\rangle \langle b_k^l | U_2^\dagger \]

Therefore, it is proved that measurements can always be moved from an intermediate stage of a quantum circuit to the end of the circuit. In what concerns the particular case of conditional operations the proof follows directly from the fact that an operation of the form \(|c_1\ldots c_n\rangle \langle l | \rightarrow |c_1\ldots c_n\rangle U^{c_1\ldots c_n} |l\rangle \) commutes with a measurement of the states \(|c_1\ldots c_n\rangle \), i.e. if measured qubits are used only in the rest of the circuit to control operations (functioning as classical bits in practice, which is usually the case), the measurements can be moved to the end of the circuit directly (which is the actually the essence of the principle).

The writing of the state in the form \(|\psi\rangle = \sum_j a_j |j\rangle |b_j\rangle \) can always be done. Consider the state written in the canonical basis, \(|\{k\}\rangle \). This canonical basis can be split in two, \(|\{s\}\rangle \) and \(|\{r\}\rangle \), with \(|\{s\rangle \{r\} \rangle = \{\{k\}\} \). The state can therefore be split in a corresponding fashion and

\[ |\psi\rangle = \sum_{k=0}^{2^N-1} a_k |k\rangle = \sum_{s=0}^{2^N-1} \sum_{r=0}^{2^N-1} a_{k=s2^{N_B}} |s\rangle |r\rangle = \sum_{s=0}^{2^N-1} a_s |s\rangle \left( \sum_{r=0}^{2^N-1} \frac{1}{a_s} \frac{a_{k=s2^{N_B}+r}}{a_s} |r\rangle \right) \]

\[ = \sum_{s=0}^{2^N-1} a_s |s\rangle |b_s\rangle, \tag{3.6} \]

where \(a_s = \sqrt{\sum_{r=0}^{2^N-1} |a_{k=s2^{N_B}+r}|^2} \) and \(N = NA + N_B \). This form is also valid with some \(a_s = 0\) (easily seen), which just means that there is no component associated to \(|s\rangle \). It is clear that \(|b_s\rangle |b_s\rangle = 1\), that \(|\sum_s a_s |s\rangle |b_s\rangle|^2 = 1\) and \(\sum_s |a_s|^2 = 1\).

### 3.3 No-cloning theorem

Having introduced quantum gates, it is simple to answer the question: Is it possible to copy a qubit's state with no prior information about it? The answer is

\[ U |\psi\rangle \otimes |\alpha\rangle = |\psi\rangle \otimes |\psi\rangle , U |\phi\rangle \otimes |\alpha\rangle = |\phi\rangle \otimes |\phi\rangle \]

\[ \rightarrow (\phi \otimes |\alpha\rangle U U^\dagger |\psi\rangle \otimes |\alpha\rangle = (\phi |\psi\rangle , (\psi \otimes |\alpha\rangle U U^\dagger |\phi\rangle \otimes |\alpha\rangle = (\psi |\phi\rangle \]

\[ \rightarrow (\phi \otimes |\alpha\rangle U U^\dagger |\psi\rangle \otimes |\alpha\rangle = (\langle \phi \otimes \phi \rangle (|\psi\rangle \otimes |\psi\rangle) = 1 \langle \phi \otimes \phi \rangle \]

\[ \leftrightarrow \langle \phi \psi\rangle^2 = \langle \phi \psi\rangle = \langle \psi \phi\rangle \leftrightarrow \langle \phi \psi\rangle (1 - \langle \psi | \phi\rangle) = 0 \wedge \langle \psi \phi\rangle (1 - \langle \phi | \psi\rangle) = 0 \]

\[ \leftrightarrow \langle \phi \psi\rangle = 0 \lor \langle \phi \psi\rangle = 1 \]

only orthogonal states can be copied, meaning that one can construct \(U\) capable of cloning some set of orthogonal states, however that is as far as it goes for a unitary transformation. One might think
that the cloning is not possible because the transformation is limited to be unitary. However, it is a consequence of the linearity of quantum mechanics. To verify, consider the following definition of the cloning operation:

\[ |\psi\rangle \rightarrow |\psi\rangle |\psi\rangle, \quad |\phi\rangle \rightarrow |\phi\rangle |\phi\rangle, \quad |\psi\rangle + |\phi\rangle \rightarrow (|\psi\rangle + |\phi\rangle)(|\psi\rangle + |\phi\rangle). \]  (3.8)

But by linearity,

\[ |\psi\rangle + |\phi\rangle \rightarrow |\psi\rangle |\psi\rangle + |\phi\rangle |\phi\rangle, \]  (3.9)

which differs from the action on \(|\psi\rangle + |\phi\rangle\) presented in (3.8).

### 3.4 Quantum gate’s accuracy

The scenario is the following: a sequence of unitary operations is applied to a state, however those unitary operations cannot be applied exactly, thus lacking accuracy some other unitary operations that approximately implement the referred operations are applied. Setting the scenario

\[ |\psi_N\rangle = U_N \ldots U_2 U_1 |\psi_0\rangle, \quad |\tilde{\psi}_N\rangle = \tilde{U}_N \ldots \tilde{U}_2 \tilde{U}_1 |\psi_0\rangle \]  \[ U_n |\psi_{n-1}\rangle = |\psi_n\rangle, \quad \tilde{U}_n |\psi_{n-1}\rangle = |\psi_n\rangle + |\Delta_n\rangle, \]  \[ (3.10) \]

which results in

\[ |\tilde{\psi}_n\rangle = \tilde{U}_n \ldots \tilde{U}_1 |\psi_0\rangle = |\psi_n\rangle + |\Delta_n\rangle + \sum_{j=1}^{n-1} \prod_{k=j+1}^{n} \tilde{U}_k |\Delta_j\rangle, \quad |\Delta_n\rangle = (\tilde{U}_n - U_n) |\psi_{n-1}\rangle \]  \[ (3.11) \]

\[ \left\| |\tilde{\psi}_N\rangle - |\psi_N\rangle\right\| \leq \sum_{j=1}^{N} \left\| |\Delta_j\rangle\right\| = \sum_{j=1}^{N} \left\| (\tilde{U}_j - U_j) |\psi_{j-1}\rangle\right\| \leq \sum_{j=1}^{N} \left\| \tilde{U}_j - U_j\right\| \leq N\epsilon \]

where \(\epsilon = \max_j \left\| \tilde{U}_j - U_j\right\|\), one concludes that the error increases linearly with the number of non-ideal gates applied.

### 3.5 Universal quantum gates

A desired goal is to be able to perform transformations on qubits using only a limited set of quantum gates, ideally this set would be capable of generating all possible unitary transformations. In order to reach this goal, one can start by decomposing a general unitary matrix as a product of several simpler ones, and if each of the simpler ones can be implemented using a finite set of quantum gates a universal set of gates has been obtained, i.e., a set composed of gates that can be combined to realize any possible unitary transformation. Relaxing the definition allows to include under that same name any set of gates that can implement any unitary transformation to arbitrary accuracy (but possibly not exactly).

This is in fact true and this result’s importance is specially recognized considering some quantum gates might be easier to implement physically, and hence finding a set of such gates that is universal allows an easier implementation of an arbitrary unitary transformation.

Starting with the decomposition of a unitary transformation, several decompositions of a unitary matrix are possible, however here the focus will be in a special type of decomposition in two-level matrices whose adjoint’s action on the matrix \(U\) by multiplying it on the left (or right depending on the manner one desires to decompose it) is to set one of the entries (outside of the diagonal) of matrix \(U\) to zero. The end goal is to arrive to the identity matrix since if each \(V_i\) sets to zero an entry from an \(n \times n\) matrix then \(V_{n(n-1)} \ldots V_1 U = I\) and hence \(U = V_1^\dagger \ldots V_{n(n-1)}^\dagger\).

Defining the form of the matrix to be used in the decomposition:
where the entry to be set to zero is in the $i$th column and $j$th row, and it is done with the help of the entry on the $i$th row and $i$th column of matrix $U$. Using matrices of this form to nullify all elements in the first column of $U$, except the one in the diagonal leads to that same element being turned to 1 and the first row to have all the entries set to 0 except the one in the diagonal of the matrix, taking into account the resultant matrix is unitary. Following this procedure for the remaining of the columns results in the identity as a final result, as desired. For reasons to be presented and also to obtain as resultant diagonal matrix the identity, the form is specified even further setting $k = j - 1$. Considering that a column or a row of a unitary matrix as norm 1, deleting each entry $j$ on column $i$ from $n$ to $i + 1$ allows to notice that its entry $j - 1$ is the norm of the vector composed by the entries $j - 1$ to $n$ of column $i$ of the original unitary matrix $U$, hence when arriving to $j = i$ (remaining entries $j < i$ are 0 considering argument presented above) the entry is 1 (trivial to verify for $i = 1$). The $\lambda_{j,k,i}$ are values such that $|\lambda_{j,k,i}| = 1 \land \prod \lambda_{j,k,i} = det(U)$, so that $det(V_{\text{null}}\ldots V_1) det(U) = (\prod \lambda_{j,k,i}) det(U) = (det(U))^n det(U) = 1$, ensuring that the resulting diagonal matrix is the identity. If the $\lambda_{j,k,i}$s were not used (all equal to 1) the final diagonal element in row $n$ and column $n$ would be equal to $det(U)$. As a next step, let the transformation represented by the matrix presented in (3.12) be implemented using single qubit gates and $CNOT$ gates. To achieve this, the decomposition is made so that the binary strings corresponding to the coordinates involved in the transformation represented by the matrix factor (a matrix of the form $j\cdot i V$) in the decomposition differ in only one bit. For that reason, the decomposition elected is based on the Gray code. A Gray code represented by an $N$-tuple $(X_1,\ldots,X_N)$ of binary strings, each corresponding to a number from 0 to $N - 1$ corresponding $(X_1,\ldots,X_N)$ to a permutation of the numbers from 0 to $N - 1$, satisfies the following property

- $X_i$ and $X_{i+1}$ differ in only one bit, for $i = 1,\ldots,N - 1$, and $X_N$ and $X_1$ also differ in only one bit

with $N = 2^b, b \in \mathbb{N}^*$. Let $\gamma_b(i)$ be the string $i$ from the Gray code of length $b$. Constructing a Gray code recursively

$$
\gamma_1 = (0,1), \ \gamma_b = (X_1,\ldots,X_N) \rightarrow \gamma_{b+1} = (0X_1,\ldots,0X_N,1X_N,\ldots,1X_1)
$$

(3.13)

For $b = 3$, the Gray code is represented by the tuple $(000, 001, 011, 010, 110, 111, 101, 100)$. The decomposition proposed is written for each $j\cdot i V$ in the Gray code basis (where $\gamma_b(i) = 1 + \gamma_b(i)$) in (3.14) which can be implemented as a controlled gate acting on a single qubit since two adjacent coordinates differ in only one bit in the Gray code basis.

$$
\left(\prod_i^{1\rightarrow 2^b - 1} \prod_j^{i + 1 \rightarrow 2^b} P_{j\cdot i - 1} V_{\text{GCB}} P_i^\dagger \right) U_{\text{BCB}} = I \iff \left(\prod_i^{1\rightarrow 2^b - 1} \prod_j^{i + 1 \rightarrow 2^b} \gamma_b(i) \gamma_b(i + 1) V_{\text{BCB}} \right) U_{\text{BCB}} = I
$$

(3.14)
An implementation of a general two-qubit unitary transformation in terms of this decomposition is presented as example in figure 3.7 which is written (in the standard binary code basis) as

\[ U = \frac{1}{3} V_{4}^{\dagger} + \frac{1}{2} V_{2,1}^{\dagger} + \frac{1}{4} V_{3,4}^{\dagger}, \]

where the matrices \( V_{1}^{\dagger}, \ldots, V_{6}^{\dagger} \) in the figure correspond to the principal submatrices of the matrices \( V_{3,4}^{\dagger}, \ldots, V_{1,3}^{\dagger} \), respectively.

Figure 3.7: Decomposition of a two-qubit unitary transformation using controlled gates acting on a single qubit.

Hence, in general any quantum gate might be implemented using \( C_{n}(V) \) gates for some single qubit unitary matrix \( V \), which in turn can be implemented using Toffoli gates and \( C_{1}(V') \) gates (figure 3.8) for some single qubit unitary matrix \( V' \). Toffoli gates can be implemented using \( CNOT \)s and single qubit gates (figure 3.9), and \( C_{1}(V) \) gates can be implemented using \( CNOT \)s and single qubit gates (figure 3.10). Hence, an arbitrary quantum gate can be implemented using single qubit gates and \( CNOT \) gates.

Figure 3.8: Implementation of a \( C_{n}(V) \) gate using Toffoli gates and one \( C_{1}(V') \). Adapted from: [13].

Conclusion: the set composed by the \( CNOT \) gate and all possible single qubit gates is a universal set of gates. Unfortunately, this is not a finite set for there are infinitely many unitary transformations corresponding to single qubit gates. However, it is possible to approximate a single qubit gate to an arbitrary desired accuracy, as close as desired to the ideal gate. To prove the claim, take the following...
Figure 3.10: Implementation of a $C^1(V)$ gate using CNOTs and single qubit gates, where $ABC = I$ and $V = AXBXC$. Source: [13].

A form for a general unitary matrix

$$U = e^{i\frac{\theta}{2}} \begin{bmatrix} e^{i\phi} & 0 & 0 \\ 0 & e^{-i\phi} & 0 \\ e^{i\Delta} & 0 & e^{-i\Delta} \end{bmatrix}. \quad (3.15)$$

Then, take the matrices

$$\left\{ \begin{bmatrix} e^{i\delta} & 0 & 0 \\ 0 & e^{-i\delta} & 0 \\ \cos \alpha & -\sin \alpha & \sin \alpha & \cos \alpha \end{bmatrix}, \begin{bmatrix} \cos (k\alpha) & -\sin (k\alpha) \\ \sin (k\alpha) & \cos (k\alpha) \end{bmatrix} \right\} \quad (3.16)$$

with $\delta$ and $\alpha$ irrational numbers ($\in \mathbb{R}\backslash\mathbb{Q}$). This detail makes so that $k_0\delta \pi \neq k_1\delta \pi + 2\pi k$, $k_0, k_1 \in \mathbb{N}^*$, $k \in \mathbb{Z}$ for $k_0 \neq k_1$. Hence, $k, k \in \mathbb{N}^*$ generates different points $e^{ik\delta \pi}$ along the complex unit circle. The corresponding group is therefore dense, and $\forall \varepsilon > 0, \forall x \in \mathbb{R}, \exists (k, m) \in \mathbb{Z}^2, |k\theta + 2m\pi - x| < \varepsilon$. Thus, the first matrix of the set in (3.16) raised to $k$ is capable of generating approximations that are as close as possible to a matrix of the form

$$\begin{bmatrix} e^{ia\pi} & 0 \\ 0 & e^{-ia\pi} \end{bmatrix}, a \in \mathbb{R}, \|\hat{U} - U\| = \sqrt{2}\sqrt{1 - \cos(a - k\delta)}. \quad (3.17)$$

A similar reasoning follows for the second matrix of (3.16). Note that

$$\begin{bmatrix} \cos \alpha & -\sin \alpha \\ \sin \alpha & \cos \alpha \end{bmatrix}^k = \begin{bmatrix} \cos (k\alpha) & -\sin (k\alpha) \\ \sin (k\alpha) & \cos (k\alpha) \end{bmatrix} \quad (3.18)$$

and that the referred matrix raised to $k$ is capable of generating approximations that are as close as possible to a matrix of the form

$$\begin{bmatrix} \cos (a\pi) & -\sin (a\pi) \\ \sin (a\pi) & \cos (a\pi) \end{bmatrix}, a \in \mathbb{R}, \|\hat{U} - U\| = \sqrt{2}\sqrt{1 - \cos(a - k\alpha)}. \quad (3.19)$$

Hence $U$ can be approximated using CNOTs and the set of (3.16), forming a universal set of gates, considering that two gates that differ from a global phase factor represent the same quantum gate. Regarding the rate of convergence of the approximation, the Solovay-Kitaev theorem implies that a single qubit gate can be approximated to an accuracy $\varepsilon$ using $O(\log (\frac{1}{\varepsilon})^c)$ gates from a fixed finite set, where $c$ is a constant approximately equal to 2. This in turn means that the number of gates from a fixed finite set needed to approximate a circuit with $m$ CNOTs and single qubit gates to an accuracy $\varepsilon$ is $O(m \log (\frac{1}{\varepsilon})^c)$. Taking the fact that exist universal sets of gates, particular sets of that sort which can be implemented fault-tolerantly are of particular interest, since operations in quantum computation are vulnerable to errors due to quantum noise and decoherence (including the ones due to the inaccuracy of the gates). The standard set of universal gates is composed of the Hadamard, phase, CNOT and $\frac{\pi}{8}$ gates, which can be implemented fault-tolerantly.
Chapter 4
Quantum error correction

4.1 Quantum Operations and Operator-sum Representation

The scenario is the following: the bipartite system $AB$ is subjected to a unitary transformation $U$, and only the system $A$ is available or it is only wished to know what transformation system $A$ undergoes.

Let the system of interest, $A$, and the system $B$ be in a product state (unentangled) $\rho_A \otimes \rho_B$. Then, if the initial state of $B$ is $|c_0\rangle \langle c_0|$, and if the system $B$ is not in a pure state, a purified version can be obtained by means of an extra system, so there is no loss of generality there in using this extra system in intermediate calculations, it follows that

$$\mathcal{E}(\rho) = tr_B(U\rho U^\dagger) = tr_B(U\rho_A \otimes |c_0\rangle \langle c_0| U^\dagger) = \sum_k \langle e_k| U\rho_A \otimes |c_0\rangle \langle e_0| U^\dagger |e_k\rangle = \sum_k E_k\rho_A E_k^\dagger, \quad (4.1)$$

with $E_k = \langle e_k| U |c_0\rangle$. The operators $\{E_k\}$ are called Kraus operators or operation elements and this form of expressing a quantum operation is called the operator-sum representation. A more formal definition of quantum operation will be presented later. The assumption of the systems $A$ and $B$ being unentangled is somewhat reasonable, since it is common before making an experiment or some computation to undo all correlations between the system of interest $A$ and the environment, $B$. This assumption sets a limitation on the initial states of the systems involved and hence on the type of transformation it describes. The system $B$ as presented here is in most cases identified as the environment. It is easily seen that the operator-sum representation can be interpreted as the result of a measurement on the environment where is considered the associated measurement ensemble inherent to the unknown outcome of the measurement (with each $E_k$ corresponding to a possible outcome), after the transformation $U$ is applied on the overall system. Now, let a measurement be made on the overall system after $U$ is applied with corresponding projectors $\{P_m\}$. Given that measurement $m$ occurred, the final state tracing out $B$ is

$$\frac{tr_B(P_m U\rho_A \otimes \rho_B U^\dagger P_m)}{tr(P_m U\rho_A \otimes \rho_B U^\dagger P_m)} \quad (4.2)$$

and

$$\mathcal{E}_m(\rho_A) = tr_B(P_m U\rho_A \otimes \rho_B U^\dagger P_m) = tr_B(P_m U\rho_A \otimes \sum_i \lambda_i |i\rangle \langle i| U^\dagger P_m)$$

$$= \sum_i \sum_j \sqrt{\lambda_i} \langle j| P_m |i\rangle \rho_A \sqrt{\lambda_i} \langle i| U^\dagger P_m |j\rangle = \sum_i \sum_j E_{ji} \rho_A E_{ji}^\dagger, \quad (4.3)$$

generalizing the first definition with $E_{ji} = \sqrt{\lambda_i} \langle j| P_m |i\rangle$ and where $\rho_B = \lambda_i |i\rangle \langle i|$. The final state of $A$ is $\mathcal{E}_m(\rho_A)/tr(\mathcal{E}_m(\rho_A))$ where the probability of outcome $m$ occurring is $tr(\mathcal{E}_m(\rho_A))$. Note that the trace of the quantum operation $\mathcal{E}_m(\rho_A)$ is not 1 (if $P_m \neq I$), since it is not normalized and concerns only a possible outcome.

It was shown the operator-sum representation with the implicit assumption that the input space and the output space are the same, thus the $\{E_k\}$ are square, however the input space and the output space need not be the same and the $\{E_k\}$ can be rectangular. To prove such a statement, let there be systems $AB$ and $CD$ initially in the state $\rho_{AB} \otimes |c_0\rangle \langle c_0|_{CD}$ which undergo the unitary transformation $U$ and also
let systems $A$ and $D$ be discarded afterwards.

$$\mathcal{E}(\rho) = tr_{AD}(U \rho \otimes |e_0\rangle \langle e_0|_{CD} U^\dagger) = \sum_{k,j} \langle k_A | j_D | U \rho \otimes |e_0\rangle_{CD} U^\dagger | k_A \rangle | j_D \rangle$$

$$= \sum_{k,j} \langle k_A | j_D | U | e_0 \rangle_{CD} \rho \langle e_0|_{CD} U^\dagger | k_A \rangle | j_D \rangle$$

$$= \sum_{k,j} \sum_{m,i} \sum_{n,l} \langle k_A | j_D | U | m_C \rangle | i_D \rangle \alpha_{m,i} \rho \alpha_{n,l}^* \langle n_C | (l_D | U^\dagger | k_A \rangle | j_D \rangle$$

$$= \sum_{k,j} \left( \sum_{m,i} \alpha_{m,i} \langle k_A | j_D | U | m_C \rangle | i_D \rangle \right) \rho \left( \sum_{n,l} \alpha_{n,l}^* \langle n_C | (l_D | U^\dagger | k_A \rangle | j_D \rangle \right) = \sum_{k,j} E_{k,j} \rho E_{k,j}^\dagger \tag{4.4}$$

Note that $|e_0\rangle = \sum_{m,i} \alpha_{m,i} |m_C\rangle |i_D\rangle$ in (4.4). The operators $\{E_k\}$ take from the state space of $AB$ to the state space of $BC$ and satisfy the completeness relation.

$$\sum_{k,j} E_{k,j} E_{k,j} = \left( \sum_{n,l} \alpha_{n,l}^* \langle n_C | (l_D | | k_A \rangle | j_D \rangle \right) U^\dagger \left( \sum_{k,j} \langle k_A | j_D \rangle \langle k_A | j_D \rangle \right) U \left( \sum_{m,i} \alpha_{m,i} |m_C\rangle |i_D\rangle \right)$$

$$= \left( \sum_{n,l} \alpha_{n,l}^* \langle n_C | (l_D | \right) U^\dagger \left( I_{AB} \sum_{m,i} |m_C\rangle |i_D\rangle \right) = I_{AB} \sum_{n,l} |\alpha_{n,l}|^2 = I_{AB} \tag{4.5}$$

Now, consider the converse problem: if given a set of operators $\{E_k\}$, there is some reasonable system-environment model and dynamics which give rise to a quantum operation with those operation elements. By ‘reasonable’ it is meant that the dynamics must be either a unitary evolution or a projective measurement. For a quantum operation with same input space and same output space, however it also holds for the general case, it can be proved that the answer to the problem is yes, and indeed defining $U |\psi\rangle |e_0\rangle \equiv \sum_k E_k |\psi\rangle |e_k\rangle$ it is seen

$$\langle \psi | (e_0) U^\dagger U | \phi \rangle |e_0\rangle = \langle \psi | \sum_k E_k^\dagger E_k | \phi \rangle = \langle \psi | \phi \rangle$$

$$\text{tr}_B (U \rho_A \otimes |e_0\rangle \langle e_0| U^\dagger) = \sum_k E_k \rho_A E_k^\dagger$$

$$\tag{4.6}$$

where the unitary operation $U$ was created in order to generate the operators $\{E_k\}$ satisfying the completeness relation and a system-environment model was designed starting in the state $\rho_A \otimes |e_0\rangle \langle e_0|$ with the orthonormal basis of the environment $\{|e_k\rangle\}$ with cardinality equal to the number of operators, hence setting the dimension of the environment.

The more formal definition of quantum operation is presented below.

A quantum operation maps density operators to density operators and has the following properties:

- $\text{tr}[\mathcal{E}(\rho)]$ is the probability that the process represented by $\mathcal{E}$ occurs, when $\rho$ is the initial state. Thus, $0 \leq \text{tr}[\mathcal{E}(\rho)] \leq 1$ for any state $\rho$.

- $\mathcal{E}$ is a convex-linear map on the set of density matrices, that is, for probabilities $\{p_i\}$,

$$\mathcal{E} \left( \sum_i p_i \rho_i \right) = \sum_i p_i \mathcal{E}(\rho_i) \tag{4.7}$$

- $\mathcal{E}$ is a completely positive map. That is, if $\mathcal{E}$ maps density operators on Hilbert space $\mathcal{H}_A$ to density operators on Hilbert space $\mathcal{H}_A'$, then $\mathcal{E}(A)$ must be positive for any positive operator $A$. Furthermore, if the operation is extended to the input space $\mathcal{H}_B \otimes \mathcal{H}_A$ with the extended operator $I \otimes \mathcal{E}$, hence mapping $BA$ to $BA'$, $\mathcal{E}$ is said to be completely positive if any such extension of $\mathcal{E}$ is positive.
The map $\mathcal{E}$ satisfies the mentioned properties if and only if $\mathcal{E}(\rho) = \sum_k E_k \rho E_k^\dagger$ for some set of operators $\{E_k\}$ which map the input Hilbert space to the output Hilbert space and satisfy $\sum_k E_k^\dagger E_k \leq I$.

If $\mathcal{E}(\rho) = \sum_k E_k \rho E_k^\dagger$ then $\mathcal{E}$ is obviously a convex-linear map. Also, $tr[\mathcal{E}(\rho)] = tr(\rho \sum_k E_k^\dagger E_k) \leq tr(\rho) = 1$, since $\sum_k E_k^\dagger E_k \leq I$ and $tr(\rho) = 1$. Extending the operation to a higher dimension Hilbert space, identifying that space with the system $BA$, then defining $|\psi_k\rangle = (I \otimes E_k^\dagger) |\phi\rangle$ one has

$$\langle \phi | (I \otimes E_k) C (I \otimes E_k^\dagger) |\phi\rangle = \langle \psi_k | C |\psi_k\rangle \geq 0 \Rightarrow \langle \phi | (I \otimes E)(C) |\phi\rangle = \sum_k \langle \psi_k | C |\psi_k\rangle \geq 0$$

(4.8) for a positive operator $C$ on the input space of the extended operator. Conversely, suppose $\mathcal{E}$ satisfies the previously mentioned properties. $\mathcal{E}$ takes operators from Hilbert space $\mathcal{H}_A$ to $\mathcal{H}_A'$; let it be introduced an auxiliary system $R$ having the same dimension as $\mathcal{H}_A$. The not-normalized maximally entangled state $|\tilde{\phi}\rangle$ (to unclutter equations of normalization factors) of system $RA$ is defined and one has the following,

$$|\tilde{\phi}\rangle = \sum_i |i_R\rangle |i_A\rangle \rightarrow (I \otimes \mathcal{E}) \left(|\tilde{\phi}\rangle \langle \tilde{\phi}^*|_{RA}\right) = \sum_k |\tilde{\psi}_k\rangle \langle \tilde{\psi}_k|_{RA'}$$

(4.9)

where $\{|i_R\rangle\}$ and $\{|i_A\rangle\}$ are orthonormal bases associated to the systems $R$ and $A$, respectively. Taking an arbitrary pure state $|s_A\rangle$ of $A$,

$$|s_A\rangle = \sum_j s_j |j_A\rangle = \sum_j s_j \langle j_R| \tilde{\phi}\rangle = \langle s_R^* | \tilde{\phi}\rangle,$$

(4.10)

which from (4.9) means

$$\mathcal{E}(|s_A\rangle \langle s_A|) = \sum_k \langle s_R^* | \tilde{\psi}_k\rangle \langle \tilde{\psi}_k | s_R\rangle.$$  

(4.11)

Defining the following map mapping $\mathcal{H}_A$ to $\mathcal{H}_A'$, one has

$$E_k |s_A\rangle \equiv \langle s_R^* | \tilde{\psi}_k\rangle \rightarrow \sum_k E_k |s_A\rangle E_k^\dagger = \sum_k \langle s_R^* | \tilde{\psi}_k\rangle \langle \tilde{\psi}_k | s_R\rangle = \mathcal{E}(|s_A\rangle \langle s_A|)$$

(4.12)

from which it is easily seen that $\{E_k\}$ are linear and by convex-linearity

$$\mathcal{E}(\rho) = \sum_k E_k \rho E_k^\dagger$$

(4.13)

Hence, any completely positive linear map is a quantum channel.

Considering $0 \leq tr[\mathcal{E}(\rho)] \leq 1$, it is clear that by taking an orthonormal basis $\{|j\rangle\}$ of the corresponding dimension to $\rho$ and using $\rho = \sum j \langle j |j\rangle$ for each $j$ one has $tr[\mathcal{E}(\rho)] = tr(\sum_k E_k \rho E_k^\dagger) = tr(\rho(\sum_k E_k^\dagger E_k)) = \langle j |(\sum_k E_k^\dagger E_k) |j\rangle \leq 1$ which in turn is equivalent to

$$0 \leq \langle j | P - \sum_k E_k^\dagger E_k |j\rangle,$$

(4.14)

where $\langle j | P |j\rangle = 1$, and because $P$ satisfies this for each $|j\rangle$ of the orthonormal basis, $P = I$ and one concludes that $0 \leq I - \sum_k E_k^\dagger E_k \leftrightarrow \sum_k E_k^\dagger E_k \leq I$.

Remembering that two ensembles generate a same density operator if and only if the representative states of the ensemble relate through $|\tilde{\psi}_k\rangle = \sum_j u_{kj} |\tilde{\phi}_j\rangle$ and considering $(I \otimes \mathcal{E}) \left(|\tilde{\phi}\rangle \langle \tilde{\phi}|\right) = \sum_k |\tilde{\psi}_k\rangle \langle \tilde{\psi}_k| = \sum_k |\tilde{\psi}_k\rangle \langle \tilde{\psi}_k| = \sum_k |\tilde{\psi}_k\rangle \langle \tilde{\phi}_j| \langle \tilde{\psi}_k| = \sum_k |\tilde{\psi}_k\rangle \langle \tilde{\psi}_k|$, then the two corresponding sets of operators $\{E_k\}$, $\{F_j\}$ represent the same quantum operation and relate through

$$E_k |s_A\rangle = \langle s_R^* | \tilde{\psi}_k\rangle = \sum_j u_{kj} \langle s_R^* | \tilde{\phi}_j\rangle = \sum_j u_{kj} F_j |s_A\rangle$$

(4.15)
with $F_j |s_k\rangle \equiv \langle s_k'|e_j\rangle$ and are related by $E_k = \sum_j u_{kj} F_j$. Of course that if two sets of operators representing each a quantum operation are related by $E_k = \sum_j u_{kj} F_j$ then,

$$E(\rho) = \sum_k E_k \rho E_k^\dagger = \sum_k \sum_{ji} u_{kj} u_{ki}^\dagger F_j \rho F_i^\dagger = \sum_{ji} \left( \sum_k u_{kj} u_{ji}^\dagger \right) F_j \rho F_i^\dagger = \sum_j I_{ij} F_j \rho F_i^\dagger = \sum_j F_j \rho F_j^\dagger,$$ (4.16)

and consequently they represent the same quantum operation. In conclusion, if two sets of operators $\{E_k\}$ and $\{F_j\}$ giving rise to quantum operations $E$ and $F$, respectively, are related through $E_k = \sum_{ij} u_{kj} F_j$ is equivalent to saying $E = F$ where $U$ is a unitary matrix (the smallest set of operators can be padded with zero operators, so that they both have the same number of operators). A set of non-zero operators representing a quantum operation has at most size $dd'$ where $d$ is the dimension of the space associated with $A$ (input space) and $d'$ is the dimension of the space associated with $A'$ (output space), which can be easily verified by the equivalent form of channel $E$ as the density operator in $RA'$, which by the spectral decomposition theorem has a minimal decomposition in terms of orthonormal vectors corresponding to non-zero eigenvalues in number not surpassing $dd'$. Since to each eigenvector can be associated an operator, the minimum number of operators describing a quantum operation is at most $dd'$. From this it can be noted that the maximum size of an environment that would be needed to realize a unitary transformation giving rise to a given quantum operation is $dd'$.

To conclude, consider the composition of two quantum operations $E_2 \otimes E_1$. If $E_1$ has $N$ operators, $\{E_k\}$, and $E_2$ has $M$ operators, $\{F_j\}$, the referred composition has $NM$ operators, $\{F_j E_k\}$.

Regarding nomenclature, a quantum channel is a quantum operation perceived as a communication channel and is very important in quantum information theory.

### 4.2 Quantum error correction: Introduction

Although, the quantum systems in question (quantum computers) are taken to be closed systems, that is in fact an approximation. Quantum computers inevitably interact with its environment, which results in decoherence. Decoherence is the phenomenon by which the system in question becomes correlated to the environment resulting in a loss of information on the quantum system. It can be said that the system leaks information to its surroundings. Quantum noise refers to any noise process in quantum processing. This term is sometimes used interchangeably with decoherence on the field of quantum computation and quantum information theory, since a closed quantum system that does not interact with its environment and hence is isolated, its dynamic is determined only by itself, and evolving ideally in respect to the purpose associated to it, no dynamic is regarded as undesirable, meaning that none of it would be regarded as noise; in conclusion, noise comes from undesirable interactions with the environment if the desired internal behaviour of the system corresponds to the obtained. On that note, the gates in a quantum computer cannot be implemented exactly, i.e. with perfect accuracy, and the errors associated to their imperfection accumulate and must be corrected to prevent failure in the computation.

Moving on, quantum noise and errors are a very serious issue when it comes to actually implementing a quantum computer, considering its impact in computation, which if not fought generally means failure in the computation. Quantum error correction serves the purpose of protecting quantum information from quantum noise and errors, correcting the affected information. It uses redundancy in the encoding of the quantum states. Redundancy makes it harder for information to be compromised, since there is more of the same information and more information needs to be affected for it to be compromised. The encoding is done by representing the logical $|0\rangle$ and $|1\rangle$ using more than one qubit, thus representing them in a higher dimensional Hilbert space.
Taking into account the previous considerations and the study presented here concerning quantum operations, the noise occurring in a quantum system is going to be described by a quantum operation. Being a system in state $|\psi\rangle$, the quantum operation with operators $\{E_i\}$ applies $E_i$ to $|\psi\rangle$ with probability $\langle \psi | E_i^\dagger E_i | \psi \rangle$. Moreover, the quantum-error correction operation is going to be expressed as a trace-preserving quantum operation $R$. And so, it is going to be required from a quantum error-correction operation that

$$ (R \circ E)(\rho) \propto \rho. \quad (4.17) $$

The requirement of proportionality instead of equality is only due to the fact that non-trace-preserving operations for $E$ might be of interest (if $E$ were to be trace-preserving equality would hold), nonetheless the error-correction strategy $R$ should succeed with probability 1 (trace-preserving). Consider now, that noise affects one particular qubit which before the noise was in state $|\psi\rangle$ and after is in state $E_i|\psi\rangle = |\psi'\rangle$. The $E_i$ operator can be described by a complex $2 \times 2$ matrix which in turn may be expanded as a linear combination of the matrices $I$, $X$, $Z$ and $XZ = -iY$:

$$ E_i = e_{i0}I + e_{i1}X + e_{i2}Z + e_{i3}XZ. \quad (4.18) $$

This expansion is extremely relevant because as it will be proved later if the operators $\{F_j\}$ of the quantum operation $F$ are linear combinations of the operators $\{E_i\}$ of the quantum operation $E$, i.e. $F_j = \sum_i m_{ji}E_i$ for some matrix $M$ of complex numbers, then an error-correction operation $R$ which corrects $E$ over the quantum code $C$ also corrects $F$ over that same quantum code. Meaning that looking at the case where the noise affects only one particular qubit, if $R$ corrects a quantum operation with operators $I$, $X$, $Z$ and $XZ$ then it is capable of correcting the effect of any quantum operation on that qubit. The error associated with $X$ is called the bit flip error, the error associated with $Z$ is called the phase flip error and the error associated with $XZ$ is called the bit-phase flip error. Let these errors be considered and the state $|\psi\rangle$, then after the qubit passes the corresponding channel representing the error, the associated density matrix is

$$ \rho_N = (1 - p) |\psi\rangle \langle \psi| + pN |\psi\rangle \langle \psi| N^\dagger, \quad N = \{X, Z, XZ\}, \quad (4.19) $$

which applies the operation $N$ with probability $p$ and leaves the state unchanged with probability $1 - p$. The corresponding fidelity (check appendix 5 is $F_N = \langle \psi | \rho_N | \psi \rangle = (1 - p) + p |\psi| N |\psi| N^\dagger$ whose minimum value is $1 - p$ for all operations $N$. The objective of an error-correcting code and an error-correcting operation is to maintain the fidelity between the ideal state and the real one (the one affected by errors) close to 1.

The first error-correction code to be presented is

$$ |0_L\rangle \equiv \frac{(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)}{2\sqrt{2}}, $$
$$ |1_L\rangle \equiv \frac{(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)}{2\sqrt{2}}. \quad (4.20) $$

Focusing on the first three qubits, for $|0_L\rangle$ and $|1_L\rangle$ the respective parts are $\frac{|000\rangle + |111\rangle}{\sqrt{2}}$ and $\frac{|000\rangle - |111\rangle}{\sqrt{2}}$ and if one or less of the qubits flips it is easy to correct it since the other two agree. The key idea is in the sub-components $|0\rangle = |000\rangle$, $|1\rangle^\dagger = |111\rangle$ which if, for example, the first qubit flips they turn into $|100\rangle$ and $|011\rangle$, respectively, and as it is seen it is easily correctable, assuming that the probability of error on a qubit is small, by flipping the first qubit. Hence, turns out that the quantum-error correction code $|0_L\rangle = |000\rangle$, $|1_L\rangle = |111\rangle$ allows for a better protection of the state from the bit flip error. In fact, for this last quantum-error correction code if $p$ is the probability of a qubit flipping then the error-correction works
successfully with probability \((1 - p)^3 + 3p(1 - p)^2 = 1 - 3p^2 + 2p^3\) which corresponds to the probability of one or less qubits flipping (it is better than \(1 - p\), the original error probability). Now taking the same code that is in equation (4.20) and writing it in this form,

\[
\begin{align*}
|0_L\rangle &\equiv \frac{(|0'\rangle + |1'\rangle)(|0'\rangle + |1'\rangle)(|0'\rangle + |1'\rangle)}{2\sqrt{2}} \\
|1_L\rangle &\equiv \frac{(|0'\rangle - |1'\rangle)(|0'\rangle + |1'\rangle)(|0'\rangle - |1'\rangle)}{2\sqrt{2}}
\end{align*}
\]

then a three qubit analogue version with \(|0''_L\rangle = |+\rangle |+\rangle |+\rangle\) and \(|1''_L\rangle = |\rangle |\rangle |\rangle\) can be analysed. If one or less of the qubits have their phase flipped it is easy to correct it since the other two agree. This works similarly to \(|0'\rangle\) and \(|1'\rangle\) for the bit flip error, but instead \(|0''_L\rangle\) and \(|1''_L\rangle\) are used taking into account the phase-flip error. For example, if the first qubit phase-flips then \(|0''_L\rangle\) and \(|1''_L\rangle\) turn into \(|\rangle |\rangle |\rangle\) and \(|+-\rangle |+-\rangle |+-\rangle\), respectively, and as it is seen it is easily correctable, assuming that the probability of error on a qubit is small, by applying the \(Z\) gate to the first qubit. The probability of having the original state after this error-correction procedure is analogously calculated as for the previous case yielding \(1 - 3p^2 + 2p^3\). This is similar to the previous case with \(|0''_L\rangle\) and \(|1''_L\rangle\) however now the qubits’ state are a repetition of a vector from the Hadamard basis \((|+\rangle\) for \(|0''_L\rangle\) and \(|\rangle\) for \(|1''_L\rangle\)). From these considerations it can be easily seen that the code of (4.20) is also capable of correcting bit-phase flip errors for small probability of error. The code in (4.20) is the Shor code and its encoding circuit is presented in figure 4.1. The encoding takes \(|\psi\rangle = \alpha |0\rangle + \beta |1\rangle\) to \(|\bar{\psi}\rangle = \alpha |0_L\rangle + \beta |1_L\rangle\).

![Figure 4.1: Encoding circuit for the Shor code. Source: [13](#).

The error-correction process may be separated into two steps: the error-detection or syndrome diagnosis and the recovery. In the error-detection step a measurement is performed, the outcome of this measurement is the error syndrome and the post-measurement state is the same as the pre-measurement state. This measure identifies if there was an error and if there was, which error was it, so that it can be corrected in the recovery step. Also, \(\langle \bar{\psi} | M_i^\dagger M_i | \bar{\psi} \rangle = 1\) for some measurement operator \(M_i\) and for any state \(|\bar{\psi}\rangle\) generated by an accounted error on the protected state or that is the protected state. In the recovery step, the error syndrome is used to select the appropriate transformation to apply in order to recover the original state, i.e. the error-free state. However, they can be made simultaneously without measurement using unitary operations and ancilla systems prepared in standard states. In fact, let \(\{M_i\}\) be the measurement operators and the conditional unitary operations \(\{U_i\}\) responsible for the
correction of the errors, with \( M_i \) having one corresponding \( U_i \). Then, \( U \) characterized by

\[
U |\psi\rangle = \sum_i (U_i M_i |\psi\rangle) |i\rangle
\]  

(4.22)
can be extended to a unitary operator acting on the whole space since

\[
\langle \phi | 0 \rangle U^\dagger U |\psi\rangle = \sum_{ij} \langle \phi | M_i^\dagger M_j |\psi\rangle \delta_{ij} = \sum_i \langle \phi | M_i^\dagger M_i |\psi\rangle = \langle \phi | \psi \rangle.
\]  

(4.23)

The transformation \( U \) implements the quantum operation \( R(\rho) = \sum_i U_i M_i \sigma M_i^\dagger U_i^\dagger \) on the system being error-corrected, thus the error-correction process is successfully implemented by \( U \).

Going back to the code in (4.20), let it be considered the error-detection step and the recovery step starting by considering the phase-flip error. Both \(|0_L\rangle\) or \(|1_L\rangle\) can be written (not caring for normalization) as in (4.24), considering none or one of the three presented errors happened, where the \(|a_i\rangle\) are vectors

\[
\begin{align*}
\ket{a_0} &= e^{i\pi n_0} \ket{0} \\
\ket{a_1} &= e^{i\pi n_1} \ket{1} \\
\ket{a_2} &= e^{i\pi n_2} \ket{2} \\
\ket{0} &\downarrow x_1 X_2 \downarrow x_3 X_2 X_3 \\
\ket{1} &\downarrow x_4 X_5 \downarrow x_6 X_2 X_3 X_4 X_5 \\
\ket{2} &\downarrow x_7 X_8 \downarrow x_9 X_2 X_3 X_4 X_5 X_6 X_7 X_8 X_9 \\
&\text{where } n_0, n_1, n_2 \in \{0, 1\}.
\end{align*}
\]  

(4.24)

from the computational basis of a 3-qubit system, e.g. \(|000\rangle\), and the \(|\bar{a}_i\rangle\) are also vectors from that computational basis and are the negated version of \(|a_i\rangle\), e.g. \(|111\rangle\) for \(|000\rangle\). Focusing on the first block of three qubits, by performing a measurement corresponding to the observable \(X_1 X_2 X_3\) one will always get \(e^{i\pi n_0}\) (since it is \(\pm 1\), and since the outcomes are 1 or \(-1\), it takes one of the values with probability 1) which is the factor corresponding to the phase of the block and is 1 or \(-1\). The same goes for the remaining blocks, hence if one uses the observables \(X_1 X_2 X_3 X_4 X_5 X_6\) and \(X_4 X_5 X_6 X_7 X_8 X_9\), one can attain from the first if the phase of the two first blocks agree (outcome is 1) and from the second if the phase of the second and third blocks agree (outcome is 1). For instance, if the outcome from the first was \(-1\) and from the second was 1 then the second and the third block would agree in phase and because the first and second did not (outcome was \(-1 = e^{i\pi n_0} e^{i\pi n_1}\)) then the phase of the first block is wrong and must be flipped, which can be done applying \(Z_1 Z_2 Z_3\) (or just \(Z\) in one of these qubits).

Considering now the bit-flip error, and focusing on the first block of three qubits, one has

\[
\begin{align*}
\langle Z_1 Z_2 \rangle &= e^{i\pi b_1} e^{i\pi \bar{b_2}} \\
\langle Z_2 Z_3 \rangle &= e^{i\pi b_2} e^{i\pi \bar{b_3}}
\end{align*}
\]  

(4.25)

where \(b_i\) is the value of the \(i\)th bit (counting from the most significant) on \(a_0\) (of course \(b_i \in \{0, 1\}\)) and \(\bar{b}_i\) is the value of the \(i\)th bit of \(\bar{a}_0\), which is the negation of \(b_i\) and follows that \(\bar{b}_i = 1 - b_i\). As it can be seen, by the expectation of the observable \(Z_1 Z_2\) (one will always get the expected value as measurement’s outcome also for these observables for the same reasons as before) which is 1 if both bits (first and second) have the same value in the binary expansion of \(a_0\) or \(\bar{a}_0\), otherwise it is \(-1\). The same goes for the observable \(Z_2 Z_3\) but with respect to the bits 2 and 3. So, using this two observables one can detect if a bit-flip occurred, for instance, if the outcome of the measurement corresponding to the observable \(Z_1 Z_2\) was 1 and the one corresponding to the observable \(Z_2 Z_3\) was \(-1\) then the first and second most significant bits agree in value, however the third does not agree with the second, therefore the value of
the third is wrong, and the third qubit must be flipped using $X_3$. Then to recover the original qubit state it is only needed to apply $X$. For the remaining blocks of three qubits the reasoning is the same in order to find flipped qubits within those blocks, more specifically for the second block the observables would be $Z_4 Z_5$ and $Z_5 Z_6$ and for the third block they would be $Z_7 Z_8$ and $Z_9 Z_6$. For both phase and bit flip ($XZ$ applied to a qubit), it is easy to see that one just needs to correct the phase flip and the bit flip with the previously seen procedures. Therefore, the Shor code can protect against the errors generated by the operators $X$, $Z$, $ZX$ and generated by operators which are linear combinations of those and $I$.

Until now, only errors on a particular qubit were considered, however an operator $E_i$ on an $n$-qubit Hilbert space can be described by a complex $2^n \times 2^n$ matrix which in turn can be expanded in terms of

$$\{I,X,Z,ZX\} \odot \alpha$$

which in number are $4^n$ matrices. The errors a quantum error-correcting code can correct or that one intends the devised quantum error-correction code to correct are therefore a subset of (4.26). One can also subdivide the set of operators in (4.26) into operators representing errors on zero qubits (identity), on one qubit, on two qubits, and henceforth. If the effect of the noise on one qubit is fairly small, then the dominating terms are the terms representing errors on no qubits or on one qubit. In fact, if

$$\alpha U = P \beta U$$

for some Hermitian matrix $\alpha$ of complex numbers.

**Theorem 4.2.1** (Quantum error-correction conditions [13]). Let $C$ be a quantum code and let $P$ be the projector onto $C$. Suppose $E$ is a quantum operation with operation elements $\{E_i\}$. A necessary and sufficient condition for the existence of an error-correction operation $R$ correcting $E$ on $C$ is that

$$PE_i^\dagger E_i P = \alpha_{ij} P$$

for some Hermitian matrix $\alpha$ of complex numbers.

**Proof.** If $PE_i^\dagger E_i P = \alpha_{ij} P$ is true with Hermitian matrix $\alpha$, then $\alpha$ can be diagonalized, $D = U^\dagger \alpha U$ (for unitary $U$ and diagonal $D$) and defining $F_k \equiv \sum_i u_k E_i$, where $\{F_k\}$ is also a set of operators for $E$ according to the considerations made at the end of the previous section, one obtains

$$PF_k^\dagger F_k P = \sum_{ij} u_k^\dagger u_j P E_i^\dagger E_j P = \left( \sum_{ij} u_k^\dagger \alpha_{ij} u_j \right) P = d_k P,$$

from which by using the polar decomposition yields $F_k P = U_k \sqrt{PF_k^\dagger F_k P} = \sqrt{d_k} U_k P$ for some unitary $U_k$. Therefore, the effect of $F_k$ is to rotate the coding subspace into the subspace defined by the projector $P_k \equiv U_k PU_k^\dagger = F_k PU_k^\dagger / \sqrt{d_k}$. These subspaces are orthogonal since when $k \neq l$ (from (4.29))

$$P_l P_k = P_l^\dagger P_k = \frac{U_l P E_l^\dagger F_l P U_k}{\sqrt{d_l d_k}} = 0.$$  

(4.30)

Let the projectors $P_k$ form a projective measurement corresponding to the syndrome diagnosis, augmented by an additional projector if necessary to satisfy the completeness relation $\sum_k P_k = I$. The
recovery step is done by applying $U_k^\dagger$. Hence, the quantum operation describing the combined detection-recovery step is $\mathcal{R}(\sigma) = \sum_k U_k^\dagger P_k \sigma P_k U_k$. For states $\rho$ in the code (so $P \sqrt{\rho} = \sqrt{\rho}$), it follows that
\[
U_k^\dagger P_k F_l \sqrt{\rho} = U_k^\dagger F_l^\dagger F_l P_k \sqrt{\rho} = \frac{U_k^\dagger U_k F_l^\dagger F_l P_k \sqrt{\rho}}{\sqrt{d_{kk}}} = \delta_{kl} \sqrt{d_{kk}} \sqrt{\rho} = \delta_{kl} \sqrt{d_{kk}} \sqrt{\rho}
\]
and since $\mathcal{E}(\rho) = \sum_i F_i \rho F_i^\dagger$ one obtains
\[
\mathcal{R}(\mathcal{E}(\rho)) = \sum_{kl} U_k^\dagger P_k F_l \rho F_l^\dagger P_k U_k = \sum_{kl} \delta_{kl} d_{kk} \rho \propto \rho
\]
as required. Being the sufficiency of the conditions (4.28) proven, the necessity is proven next. If $\{E_i\}$ is a set of operators perfectly correctable by an error-correction operation $\mathcal{R}$ with operation elements $\{R_j\}$, defining $\mathcal{E}_C$ by $\mathcal{E}_C(\rho) = \mathcal{E}(\rho^C \rho)$ it follows that $\mathcal{R}(\mathcal{E}_C(\rho)) \propto \rho^C \rho$ for all states $\rho$. Moreover, the proportionality factor must be a constant $c$, not depending on $\rho$ if both sides of the equation are to be linear. Rewriting the last equation explicitly results in
\[
\sum_{ij} R_j E_i P \rho P E_i^\dagger R_j^\dagger = c \rho P P,
\]
thus the quantum operation with operators $\{R_jE_i\}$ is identical to the quantum operation with a single operation element $\sqrt{\alpha} P$. The considerations at the end of the previous section imply that there exist complex numbers $c_{ki}$ such that $R_k E_i P = c_{ki} P$, hence
\[
PE_i^\dagger R_k^\dagger R_k E_j P = c_{ki} c_{kj} P \rightarrow \sum_k PE_i^\dagger R_k^\dagger R_k E_j P = \sum_k c_{ki}^* c_{kj} P \Leftrightarrow PE_i^\dagger E_j P = \alpha_{ij} P
\]
given that $\sum_k R_k^\dagger R_k = I$, since $\mathcal{R}$ is trace-preserving. Then $\alpha_{ij} \equiv \sum_k c_{ki}^* c_{kj}$ is a Hermitian matrix, and the quantum error-correction conditions are reached. \hfill $\blacksquare$

The previous conditions can be rewritten in another form letting $\{|k\rangle\}$ be an orthonormal basis for the code subspace. Thus, $P = \sum_k |k\rangle \langle k|$ and $PE_i^\dagger E_j P = \alpha_{ij} P$ turns into the equivalent form $\langle l| PE_i^\dagger E_j |k\rangle = \alpha_{ij} \delta_{lk}$ considering
\[
\left( \sum_l |l\rangle \langle l| \right) E_i^\dagger E_j \left( \sum_k |k\rangle \langle k| \right) = \alpha_{ij} \sum_r |r\rangle \langle r| \Leftrightarrow \sum_{lk} \langle l| E_i^\dagger E_j |k\rangle |l\rangle \langle k| = \alpha_{ij} \sum_r |r\rangle \langle r| \Leftrightarrow \langle l| E_i^\dagger E_j |k\rangle |l\rangle \langle k| = \alpha_{ij} \delta_{lk}
\]

From this form it easily observed that the perfect distinguishability of orthogonal vectors of the code subspace is preserved under the operators corresponding to errors and thus of the orthogonal codewords. Moreover, it means that the integrity of the encoded quantum information is preserved under those operations. Another aspect evidenced by this form is that $\langle k| E_i^\dagger E_j |k\rangle$ is independent of $k$, meaning that no information from the pre-error encoded state is acquired and so the state is not disturbed. If $\alpha_{ij} = \delta_{ij}$ then the various subspaces associated to the errors are orthogonal to each other, and a code satisfying the quantum error-correction conditions and this equality is called a nondegenerate code. The particularity of degenerate codes ($\alpha_{ij} \neq \delta_{ij}$) is that it might not be possible to distinguish between certain errors, however this does not mean that they can’t be corrected; take the case of the Shor code which is degenerate, since for example $Z_1 |\psi\rangle = Z_2 |\psi\rangle$ for $|\psi\rangle$ in the code space, and nonetheless correction only requires the application of $Z$ to one of the qubits of the same block.

The following theorem proves that an error-correction operation is more general in correcting than just doing it for errors that it was set out to correct explicitly.
Theorem 4.2.2. [13]. If the operators \( \{F_j\} \) of the quantum operation \( \mathcal{F} \) are linear combinations of the operators \( \{E_i\} \) of the quantum operation \( \mathcal{E} \), i.e., \( F_j = \sum_i m_{ji} E_i \) for some matrix \( M \) of complex numbers, then an error-correction operation \( \mathcal{R} \) which corrects \( \mathcal{E} \) over the quantum code \( C \) (in the conditions of theorem 4.2.1) also corrects \( \mathcal{F} \) over that same quantum code.

Proof. As shown in the proof of theorem 4.2.1 the operation elements for \( \mathcal{E} \) can be chosen such that \( \alpha = D \) is a diagonal matrix with real entries. The error-correction operation \( \mathcal{R} \) has operators \( \{U_k^\dagger P_k\} \) satisfying \( U_k^\dagger P_k E_i \sqrt{\rho} = \delta_{ki} \sqrt{d_{kk}} \sqrt{\rho} \) for \( \rho \) in the code space. Substituting \( F_j = \sum_i m_{ji} E_i \) yields

\[
U_k^\dagger P_k F_j \sqrt{\rho} = \sum_i m_{ji} \delta_{ki} \sqrt{d_{kk}} \sqrt{\rho} = m_{jk} \sqrt{d_{kk}} \sqrt{\rho}
\]

and thus

\[
\mathcal{R}(\mathcal{F}(\rho)) = \sum_{kj} U_k^\dagger P_k F_j \rho F_j^\dagger P_k U_k = \sum_{kj} |m_{jk}|^2 d_{kk} \rho \propto \rho
\]

as required. \( \blacksquare \)

4.3 Distance and classical linear codes

The concept of distance between classical binary strings is obtained from the following definition: the distance between the words \( x \) and \( y \) of \( n \) bits, \( d(x, y) \), is the number of bits in which the corresponding value differ for the words \( x \) and \( y \). As example, \( d((101), (001)) = 1 \) (differing only on the first bit).

The weight of a word is defined as \( wt(x) \equiv d(x, 0) \), and therefore \( d(x, y) = wt(x + y) \) (sum operation is done modulo 2, as most of the following) also. The distance of a code \( C \) is the minimum distance between any two codewords, more specifically \( d(C) \equiv \min_{x, y \in C, x \neq y} d(x, y) \), and for a linear code \( d(C) = \min_{x \in C, x \neq 0} wt(x) \) if \( x \) and \( y \) are. Then, a code \( C \) with \( d \equiv d(C) \), which encodes \( k \) bits of information using \( n \) bits is said to be an \([n, k, d]\) code. If an error that might change the codeword up to \( t \) bits is to be corrected then the distance between two different codewords must be big enough so as to be able to identify the corrupted codeword \( y' \) to one of the closest possible codewords as the original one, and so \( d \geq 2t + 1 \) is needed and the original codeword \( y \) is the only codeword from all the code space that satisfies \( d(y, y') \leq t \). An illustration of the situation is presented in figure 4.2, where \( d(c_1, c_2) > 2t \wedge d(c_1, c_2) \in \mathbb{N} \Rightarrow d(c_1, c_2) \geq 2t + 1 \) for the closest codewords to the error, \( c_1 \) and \( c_2 \). Now,

\[
\begin{align*}
\text{t} & \quad \text{t} \\
\begin{array}{c}
c_1 \quad \text{y'} \quad c_2 \\
\geq d
\end{array} \\
\begin{array}{c}
c_1 \quad y_{\text{max}} \quad y_{2\text{max}} \quad c_2 \\
\geq d
\end{array}
\end{align*}
\]

Figure 4.2: Explanation of the distance requirement in order for the code to correct errors on up to \( t \) bits.

a linear \([n, k, d]\) code \( C \) can be specified either by an \( n \times k \) generator matrix \( G \) or an \( (n - k) \times n \) parity check matrix \( H \) (being \( H \) and \( G \) binary matrices and the following operations all modulo 2). If \( x \) is the unencoded \( k \) bit message, then \( Gx \) is its encoding. On the other hand, if \( x \) is an encoded \( n \) bit message \( H \) is such that \( Hx = 0 \). The kernel of \( H \) is \( k \)-dimensional and the corresponding \( k \) linearly independent vectors spanning it form a possible generator matrix \( G \) (as its columns), and analogously the kernel of
Another important concept is of dual code, a dual code of $C$ is called $C^\perp$ and is defined by having generator matrix $H^T$ and parity check matrix $G^T$ and consists of all codewords orthogonal to all the codewords in $C$ (note that codewords from $C$ might be orthogonal to all codewords in $C$, i.e. $C \subseteq C^\perp$, with each codeword in $C$ being orthogonal to itself), moreover $\dim(C) + \dim(C^\perp) = n$.

**Theorem 4.3.1.** The distance $d$ of a linear code $C$ equals the minimum number of linearly dependent columns of the parity check matrix $H$

**Proof.** Let $H_i$ be the $i$th column of $H$ then for a codeword $x$ it holds that $Hx = \sum_i x_i H_i = 0$ and the columns corresponding to $x_i \neq 0$ are associated to a linearly dependant set of columns. Therefore $d \geq c$ where $c$ is the minimum number of linearly dependant columns. However, if $L$ is the set of the indices of the columns belonging to the set of minimum size of linearly dependant columns, then choosing $x'$ such that $x'_i = 0$ for $i \notin L$ then surely $x' \in C$ since $Hx' = 0$, and so one has $Hx' = \sum_{i \in L} x_i H_i + \sum_{i \notin L} x_i H_i = \sum_{i \in L} H_i x'_i$, and hence $d \leq \wt(x')$ where $\wt(x') = c$ and because any other $x \in C$ will select at least as much linearly dependant columns as $x'$ to satisfy $Hx = 0$. Therefore, $d = c$.

A consequence of the previous theorem is that $d - 1 \leq n - k$ because any set of columns of $H$ of size $d - 1$ has to be linearly independent, otherwise from theorem 4.3.1 the distance of the code would be $d - 1$ resulting in a contradiction ($d - 1 = d$), and due to the fact that cannot be more than $n - k$ linearly independent columns ($n - k$ is the size of the columns).

### 4.4 The stabilizer construction

#### 4.4.1 The stabilizer construction

The stabilizer construction builds upon the group theory in order to provide a useful representation of a quantum code. Look into appendix B for a small introduction of group theory. Let it be defined what is considered a stabilizer.

**Definition 4.4.1.** Let $S = \{M_1, \ldots, M_n\} \subseteq \mathcal{P}_n$ be a group (with regular matrix multiplication as group operation) of operators, then the nontrivial subspace which is invariant to the operators $\{M_i\}$, i.e. $M_i P = P$ ($P$ being the projector onto that subspace), is said to be stabilized by the stabilizer $S$.

where $\mathcal{P}_n = \{\pm i, \pm 1\} \times \{I, X, Z, Y\} \otimes I^n$. Moreover, the stabilizer $S$ is going to be identified with the subspace of maximal dimension stabilized by $S$. From this definition some additional properties can be obtained regarding a stabilizer $S$. The first is that the operators in $S$ commute since for all $|\psi\rangle$ stabilized by $S$ and $M_i, M_j \in S$ it follows that $M_i M_j |\psi\rangle = M_j M_i |\psi\rangle = |\psi\rangle$ and that $M_i M_j |\psi\rangle = M_j |\psi\rangle = |\psi\rangle$ so $[M_i, M_j] |\psi\rangle = 0$, and considering any two Pauli operators either commute or anti-commute, one concludes that any two operators in $S$ commute, i.e. $[M_i, M_j] = 0$, and $S$ is an Abelian group. Another important aspect regarding a stabilizer $S$ is that $-I \notin S$ because $-I |\psi\rangle = -|\psi\rangle$, but $M_i |\psi\rangle = |\psi\rangle$ for $M_i \in S$, so if $M_i = -I$ it follows that $-I |\psi\rangle = |\psi\rangle$ which results in $|\psi\rangle = 0$ and consequently the subspace invariant to $S$ is trivial, but by definition the subspace invariant to $S$ has to be nontrivial, hence $-I \notin S$ and also $\pm iI \notin S$, since for $M \in S : MM |\psi\rangle = |\psi\rangle$ and that does not hold for $M = \pm iI$ noting that $(\pm iI)(\pm iI) |\psi\rangle = -I |\psi\rangle$ which proves it from the fact that $-I \notin S$. Other important property is that if $M \in S$, then so does $M^\dagger$, since any element of $\mathcal{P}_n$ is either Hermitian or anti-Hermitian, although
no operator in $S$ can be anti-Hermitian because $M = -M^\dagger : MM |\psi\rangle = M(-M^\dagger) |\psi\rangle = -I |\psi\rangle$ and $-I \notin S$. Hence, one concludes that for any $M$ in $S$ it holds that $MM |\psi\rangle = M^\dagger |\psi\rangle = |\psi\rangle$ which satisfies $MM |\psi\rangle = |\psi\rangle$, and that $M \in S \iff M^\dagger \in S$.

A compact way to represent a group is by its generators. A set of elements $\{g_1, \ldots, g_l\}$ in a group $G$ is said to generate the group $G$ if and only if every element in $G$ can be written as a product of elements from that set named generators, and one may write $G = \langle g_1, \ldots, g_l \rangle$ (not to confuse with the notation for expectation of an observable; should be clear from context how the notation is being used). Then, a stabilizer $S$ can be written as $S = \langle s_1, \ldots, s_l \rangle$, and it is easy to see that any two generators from $S$ commute, i.e. $[s_i, s_j] = 0$ for the generators are elements of $S$, and also the generators commuting implies that all elements in $S$ commute. Something that is needed to know is given the conditions for a set of operators in $P_n$ to generate a stabilizer group, does removing a generator leaves a stabilizer subgroup generated by the remaining generators? It is clear that if $S$ is a group then by proposition B.0.2 from appendix B, that removing a generator leaves a subgroup generated by the remaining generators, since any operator in $S$ is Hermitian and so for generators $s_1, s_2 \in S$ it holds that $s_is_j^{-1} = s_is_j = s_i, s_j \in S$, and because any operator in the group can be written as a product of generators the relation also holds for any two operators in $S$. Now, let it be seen what the constraints on the operators are to generate a valid stabilizer. First, note that a stabilizer's operators are from a subset of $\{I, X, Z, Y\} \otimes^n$, since no operator in $\pm i \times \{I, X, Z, Y\} \otimes^n$ is Hermitian. Writing differently $\pm 1 \times \{I, X, Z, Y\} \otimes^n = \pm 1 \times \{I, X, Z, iXZ\} \otimes^n = \pm i^y \times \{I, X, Z, XZ\} \otimes^n$ where $y$ is the number of $Y$s in the operator. Considering this, any operator in a stabilizer $S$ can be written as

$$f(s_1, s_2) = \pm i^{s_1T}s_2 \prod_{j=1}^n X^{s_1^{t_j}}Z^{s_2^{t_j}}, \quad (4.38)$$

where $s_1$ and $s_2$ are binary strings of length $n$ (which in $4.38$ are multiplied element by element; normal vector multiplication), that for a particular $j$ determine if $X$ and $Z$, respectively, are applied to bit $j$ (if the operator is to be applied to some $n$-qubit state), and if the bit in position $j$ is 1 for both strings, $Y$ is applied. The operators must be commutative, so noting that

$$f(s_1, s_2)f(s'_1, s'_2) = (-1)^{s_2s'_1+s_1s'_2}f(s'_1, s'_2)f(s_1, s_2), \quad (4.39)$$

one concludes that $s_2s'_1+s_1s'_2 = 0$ (modulo 2 for this and following operations) which can be written as

$$sAs'^T = 0, \quad A = \begin{bmatrix}0 & I \\ I & 0\end{bmatrix}, \quad (4.40)$$

with line vectors $s' = [s'^T s'^T]$ and $s = [s^T s^T]$ (where here, the binary strings $s_l|l=1, t=2$ and $s'_l|l=1, t=2$ are treated as column vectors). Such a statement means that vectors $s$ and $s'$ must be orthogonal with respect to the inner product defined in $4.40$. The square of the operators must be the identity since $M = M^\dagger \implies (MM^\dagger = I \iff M^2 = I)$ and so

$$f(s_1, s_2)^2 = (-1)^{s_1s_2}I, \quad (4.41)$$

which means that $y = s_1s_2 = 0$, therefore the operators must have an even number of $Y$s in their corresponding tensor product decomposition in $4.38$. Moreover, note that with respect to the inner product in $4.40$ each binary string corresponding to an operator is self-orthogonal, verify with $sAs^T = s^T s_2 + s_2^T s_1 = 2s^T s_2 = 0$. Having the generators satisfy these conditions allows for a stabilizer group to arise. Now, it is desired the set of generators to be minimal, i.e. no generator can be written in terms of
any other, otherwise one could just have a pile of redundant generators for no good reason. Hence, let there be a a set of generators of the stabilizer \( G = \{ g_i \} \), where the condition is
\[
\forall g \in G, \, \exists k_j \in \mathbb{N} \land \exists g_j \in G \setminus \{ g \} : g = \prod_j g_j^{k_j}. \tag{4.42}
\]

**Proposition 4.4.1.** Consider the stabilizer \( S = \langle g_1, \ldots, g_r \rangle \) (with generators belonging to \( \mathcal{P}_n \)) where \( r \) is the minimum number of generators generating \( S \), i.e. the generators are independent, then the dimension of the subspace which is invariant to \( S \) is \( 2^n - r \) (\( n \) being the dimension of the full space). Hence, for a stabilizer to have a space invariant to it with dimension \( k = n - r \), \( r = n - k \) linearly independent generators generate it. This holds except for \( S = \langle I \rangle \) for which the parameters stated before have values \( r = 1 \) and \( k = n \).

**Proof.** First, it should be clear that there could not be \( r + 1 \) independent generators originating \( S \), because if different of its generators are multiplied they originate different operators, since if that were not true they would not be independent, hence if \( \{ h_i \} \) was a set of \( r \) independent generators, if one were to had a new independent generator, the size of the group would double, thus the group would not be the same. This reasoning allows to prove the proposition and to notice that removing a generator from an independent set reduces its number of elements, and thus is a subgroup. Now, the stabilizer generators have eigenvalues \( \pm 1 \) and considering that the trace of Pauli matrices which are not the identity is \( 0 \) and that \( tr(A \otimes B) = tr(A)tr(B) \), one has \( tr(g_i) = 0 \) \( \forall g_i \neq I \), resulting in the conclusion that half \( (2^n - 1) \) of its eigenvalues are \( +1 \) and the other half of its eigenvalues is \( -1 \). In the case where the identity is the sole generator, the subspace invariant to \( S \) would be the full space, which is quite an uninteresting case and is only brought as a remark at the end of the proposition. Proceeding, \( g_i |\psi\rangle = |\psi\rangle \) splits the Hilbert space in half with the projector onto the \( +1 \) eigenspace of \( g_i \) being \( g_i + I \). For another generator \( g_j \) \( (g_j \neq g_i) \) one gets \( g_j g_i + I |\psi\rangle = |\psi\rangle \) and \( tr(g_j g_i + I) = 0 \) (and \( tr(g_j) = 0 \) still, and hence following the same reasoning, the Hilbert space is split again in two halves corresponding to the \( \pm 1 \) eigenvalues of \( g_j \), having now the resultant subspace dimension \( 2^{n-2} \) with the corresponding projector being \( \frac{g_j g + I}{2} \). Proceeding inductively from \( g_1 \) until \( g_r \), one obtains that the resultant final subspace which corresponds to the subspace invariant to \( S \) has dimension \( 2^{n-r} \).

**Remark.** If the identity is the sole generator then \( r = 1 \) and \( k = n \), evidently.

The condition of independence on the generators can be formulated in the binary string representation presented in [4.38] using the following relation
\[
\prod_l f(s_l)^{k_l} = f \left( \sum_l k_l s_{l,1} , \sum_l k_l s_{l,2} \right) = \alpha(s_1, \ldots, s_r, k_1, \ldots, k_r) f \left( \sum_l k_l s_l \right), \tag{4.43}
\]
where \( \alpha(\cdot) \) takes a value from \( \{ -1, 1, -i, i \} \) and ensures the operator is Hermitian. Then the condition in [4.42] means that no generator can be written in this form,
\[
f(s) = \alpha(\ldots) f \left( \sum_{j, s_j \neq s} k_j s_j \right), \tag{4.44}
\]
as a linear combination of the binary strings associated to the other generators. That means, the condition translates in the generators’ associated binary strings \( \{ s_j \} \) being linearly independent, therefore a matrix analogous to the parity check matrix can be constructed called check matrix.
\[
H = \left[ \begin{array}{c} s_1 \\ \vdots \\ s_r \end{array} \right] \tag{4.45}
\]
The matrix dimension is $r \times 2n$ or equivalently $(n-k) \times 2n$, considering the conditions of proposition 4.4.1.

On the other hand, one can construct some matrix $H$ with dimension $r' \times 2n$ with some binary strings as lines, satisfying the orthogonality properties mentioned before with respect to the inner product defined in 4.4.4, and then see if the lines are linearly independent in order to originate the matrix $H$ where the corresponding generators satisfy the conditions of proposition 4.4.1.

A stabilizer code $C(S)$ is represented by an orthonormal basis of the subspace invariant to $S$, call it $\{|\psi_i\}\}$. The stabilizer codes are an important class of quantum codes whose construction is similar to the linear codes, as it may have been noted from the previous analysis and as it will be even more evidenced next. Suppose $C(S)$ is corrupted by an error $E \in P_n$, then $E$ commutes or anti-commutes with the elements of $S$, in fact it is only necessary to consider if commutes or anti-commutes with the generators of $S$, and if it anti-commutes with at least one, $g$, then $gE|\bar{\psi}_i\rangle = -gE|\bar{\psi}_i\rangle = -E|\bar{\psi}_i\rangle$ and therefore $E|\bar{\psi}_i\rangle$ is an eigenvector of $g$ with corresponding eigenvalue $-1$ instead of $1$ and so it is only needed to measure $g$ to detect $E$. If $E$ commutes with all the generators and it doesn’t belong to $S$, then it is an actual error that is not detected; the set of $E \in P_n : E g = gE$ for all $g \in S$ is known as the centralizer of $S$, and is denoted by $Z(S)$. With this knowledge, let the error-correction conditions be applied to the stabilizer codes.

**Theorem 4.4.1.** [13]. Let $S$ be the stabilizer for a stabilizer code $C(S)$. Suppose $\{E_j\}$ is a set of operators in $P_n$ such that $E_j^\dagger E_k \notin Z(S) - S$ for all $j$ and $k$. Then $\{E_j\}$ is a correctable set of errors for the code $C(S)$.

**Proof.** Let $P$ be a projector onto the code space $C(S)$. For given $j$ and $k$ there are two possibilities: either $E_j^\dagger E_k \in S$ or $E_j^\dagger E_k \in P_n - Z(S)$. For the first case, $PE_j^\dagger E_k P = P$ since $P$ is invariant to operators in $S$, hence the conditions are satisfied in this case. Now, suppose $E_j^\dagger E_k \in P_n - Z(S)$ instead, so $E_j^\dagger E_k$ must anticommute with at least one generator of $S$, call it $g_1$. Then, let $g_1, \ldots, g_{n-k}$ be a set of generators of $S$, so that

$$P = \prod_{l=1}^{n-k} (I + g_l) \frac{2n-k}{2n-k}$$

(4.46)

is the projector onto the subspace that is invariant to $S$. Hence, using the anti-commutativity property yields

$$E_j^\dagger E_k P = (I - g_1) E_j^\dagger E_k \prod_{l=2}^{n-k} (I + g_l) \frac{2n-k}{2n-k}.$$ (4.47)

However, $P(I-g_1) = 0$ since $(I+g_1)(I-g_1) = 0$ and therefore $PE_j^\dagger E_k P = 0$ whenever $E_j^\dagger E_k \in P_n - Z(S)$. It follows that the set of errors $\{E_j\}$ satisfies the quantum error-correction conditions, and thus forms a correctable set of errors.

In these conditions, a code is non-degenerate if $E_j^\dagger E_k \in P_n - Z(S)$ for all $j$ and $k$, except for $j = k$ (where $\alpha_{j \neq j} = 1$, making $\alpha_{j = j} = 0$) because $E_j^\dagger E_j = I \in S$. One can perform the error-correction operation by measuring the generators of the stabilizer, and if the result of the measurement is $+1$ then no error was detected, otherwise the error syndrome is specified by the result of the measurements, $\beta_l$ to $\beta_{n-k}$, with each combination corresponding to at least one error. If the error $E_c$ occurred, then applying $E_c^\dagger$ corrects the error, moreover if the code is degenerate more than one error might be associated to an error syndrome, nonetheless it can be corrected with either one of the errors associated since if $E_j PE_j^\dagger = E_j' PE_j^\dagger$, then $E_j^\dagger E_j' PE_j^\dagger = P$, whence $E_j^\dagger E_j' \in S$. Therefore, if the error $E_j$ occurs, it can be corrected with $E_j^\dagger$, and if the error $E_j'$ occurs, it can be corrected with $E_j'$. Thus, each error syndrome can be associated with a single error $E_j$ and the error corrected with $E_j^\dagger$. When $E_j^\dagger E_k$ belong to $Z(S) - S$ (commuting with all operators in $S$), then both $E_j |\psi\rangle$ and $E_k |\psi\rangle$ (for $|\psi\rangle$ in the code subspace) have the
same error syndrome (which is none), and $E_j^i E_k$ acts non-trivially on the subspace invariant to $S$, hence correcting $E_j$ with $E_j^i$ or $E_k$ with $E_k^i$ can incur in an erroneous state different from the original (pre-error state), although still belonging to the subspace invariant to $S$.

Focusing now on $N(S)$ (normalizer of $S$, for which a stabilizer coincides with the centralizer of $S$), it can be easily observed that it translates, in the symplectic form (binary representation description presented before for the operators), to the space $\{x : H x = 0\}$, i.e. to the kernel of $H$ which can be denoted $S^\perp$ space and whose dimension is $2n - (n - k) = n + k$. Hence, all orthogonal vectors to the $n - k$ linearly independent generators of $S$ in symplectic form are in $S^\perp$ and theorem 4.4.2 allows to say that one can express $S^\perp$ with the $n - k$ linearly independent vectors generating $S$ and $k$ pairs of vectors that are linearly independent and orthogonal to $S$, with the vectors of each pair being orthogonal to any other belonging to other pairs, but not orthogonal to the one belonging to the same pair. More precisely

\[
S^\perp = \text{span}\{u_1, \ldots, u_{n-k}\} \oplus \text{span}\{\tilde{u}_1, v_1, \ldots, v_k\} \quad \tilde{u}_i = u_{n-k+i}, \ i = 1, \ldots, k.
\]

\[
\tilde{u}_i A v_i^T = 1 \\
\tilde{u}_i A v_j^T = 0 \quad (i \neq j) \quad \text{for} \ i, j = 1, \ldots, k \\
v_i A v_j^T = 0 \\
\tilde{u}_i A \tilde{u}_j^T = 0
\] (4.48)

Focusing on the relations on the left in (4.48) regarding the inner products and considering the commutative and anti-commutative properties taken from them, it can be seen that the vectors $\tilde{u}_i$ and $v_j$ can be made to correspond to operations $Z_i$ and $X_j$, which play a similar role to $Z_i$ and $X_j$ but on the encoded state. These operators act non-trivially on the subspace stabilized by $S$ and correspond to operators generating $N(S) - S$, the space of the troublesome errors.

**Theorem 4.4.2.** There is a basis $e_1, \ldots, e_l, f_1, \ldots, f_l, u_1, \ldots, u_t$ of $V$ such that

\[
u_i A v_i^T = 0 \quad \text{for all} \ i \ \text{and all} \ v \in V \\
e_i A f_j^T = 0 = f_j A f_i^T \quad \text{for all} \ i, j \quad (4.49)
\]

**Proof.** Let $U = \{u \in V : u A v^T = 0 \text{ for all } v \in V\}$, choose a basis $u_1, \ldots, u_t$ of $U$ and choose a complementary space $W$ to $U$ in $V$, $V = U \oplus W$. Taking any nonzero $v_1 \in W$, then there is $f_1 \in W$ such that $e_1 A f_1^T = 1$. Let

\[
W_1 = \text{span}\{e_1, f_1\}, \quad W_1^\Omega = \{w \in W : w A v^T = 0 \text{ for all } v \in W_1\},
\]

then it follows that $W_1 \cap W_1^\Omega = \{0\}$ since supposing $v = a e_1 + b f_1 \in W_1 \cap W_1^\Omega$ one obtains

\[
0 = v A e_1^T = b \\
0 = v A f_1^T = a
\] \[\implies v = 0 \]

(4.51)

\[\text{Moreover } W = W_1 \oplus W_1^\Omega, \text{ since supposing } v \in W \text{ has } v A e_1^T = c \text{ and } v A f_1^T = d \text{ results in}
\]

\[
v = \left((-c f_1 + d e_1) + (v + c f_1 - d e_1) \right) \in \bigwedge_{W_1^\Omega}
\]

(4.52)

One proceeds with a non-zero $e_2 \in W_1^\Omega$ for which there is an $f_2 \in W_1^\Omega$ such that $e_2 A f_2^T = 1$. Similarly, letting $W_2 = \{e_2, f_2\}$, and proceeding analogously and performing the referred steps until all $\{e_i, f_i\}$ have been retrieved (this process eventually stops because $\dim(V) < \infty$) yields

\[V = U \oplus W_1 \oplus W_2 \oplus \ldots \oplus W_t,
\]

(4.53)

with the properties enunciated in the theorem’s statement.
Hence, according to theorem 4.4.2 one can use a version of the Gram-Schmidt procedure to obtain the referred basis. So, choosing a basis of \( n + k \) linearly independent vectors for \( S^1 \) with \( n - k \) of those being the generators of \( S \) (which correspond to the theorem’s \( \{u_1, \ldots, u_t\} \) now with \( t = n - k \), one finds the pairs \( \{e_i, f_i\} \) (with the theorem’s \( l = k \)) corresponding to the mentioned \( \{\tilde{u}_i, v_i\} \) pairs, \( k \) in number. Indeed, having a basis of \( n + k \) linearly independent vectors for \( S^2 \) which includes the linearly independent \( n-k \) stabilizer generators (with the remaining \( 2k \) orthogonal to the all of these) and where by extending them to a maximal set of \( n \) commuting operators (all orthogonal to each other, symplectically speaking), leaves \( k \) linearly independent operators which must anti-commute (non-orthogonal to at least one, symplectically speaking) with at least one of the \( n \) operators of the maximal set of \( n \) commuting operators. By choosing for each of the \( k \) vectors a different and unique vector \( f \) (from the \( k \) used for the expansion) such that \( f \Lambda e^T = 1 \) by performing \( v' = v + (v \Lambda e^T)f - (v \Lambda f^T)e \) to all other vectors \( v \) (so that \( e \Lambda v^T = f \Lambda v^T = 0 \)) one obtains \( 4.49 \), with the theorem’s \( u_i \) corresponding to \( u_i, i = 1, \ldots, n - k \) in \( 4.48 \), \( \tilde{u}_i \) corresponding to the theorem’s \( f_i \) and \( v_i \) corresponding to the theorem’s \( e_i \).

Let it now be defined the concept of distance for a quantum code which is analogous to the distance for a classical code. The weight of an operator belonging to the bit flips on the codewords (since any classical codeword belonging to a coset of \( C \) with the bit flips on up to \( d \) \( \perp C \)) leaves \( n \) independent number. Indeed, having a basis of \( n \) independent operators. By choosing for each of the \( n \) operators of the maximal set of \( n \) commuting operators, \( \Lambda \) of the 

\[ |x_i + C_2\rangle = \frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} |x_i + y\rangle, \]  

with the \( \{|x_i + C_2\rangle\} \) spanning the code subspace whose dimension is the number of disjoint cosets of \( C_2 \) in \( C_1 \) which is \( |C_1|/|C_2| = 2^{k_1-k_2} \). Thus, \( CSS(C_1, C_2) \) is an \( [n, k_1 - k_2] \) quantum code. To correct quantum errors, the fact that the Hadamard gate switches between a code and its dual (in this case \( C_2 \) and \( C_2^+ \) will be demonstrated later) with the fact that it switches phase errors with bit flip errors \( (HZH = X, HXH = Z) \) makes it clear that the error-correcting properties of \( C_2^+ \) can be used to correct the phase flips on the codewords (which translate into correcting bit flip errors on the Hadamard basis), and hence on the protected state, and that the error-correcting properties of \( C_1 \) can be used to correct the bit flips on the codewords (since any classical codeword belonging to a coset of \( C_2 \) must be in \( C_1 \), since \( C_2 \subset C_1 \) with an error being detected in a classical codeword \( x \) if \( Hx \neq 0 \), and hence on the
protected state. Now, let some properties be demonstrated regarding \( \sum_{y \in C} (-1)^{x \cdot y} \) for some classical linear code \( C \). If \( x \in C^\perp \), then \( x \cdot y = 0 \) and hence \( \sum_{y \in C} (-1)^{x \cdot y} = |C| \). If \( x \notin C^\perp \), then exists at least one codeword \( y \in C \) such that \( x \cdot y = 1 \), and because one can always describe a codeword as a linear combination of its generators (for a linear code), then exists at least one generator \( g \) of \( C \) such that \( x \cdot g = 1 \). Focusing on the generators, let the \( g_1, \ldots, g_p \) be the generators satisfying \( x \cdot g_i = 1 \) and \( g_{p+1}, \ldots, g_m \) be the generators satisfying \( x \cdot g_i = 0 \), thereupon

\[
\sum_{y \in C} (-1)^{x \cdot y} = \sum_{y \in C} (-1)^{x \cdot (y \cdot g_i)} (-1)^{x \cdot (\sum_{i=2}^{m} y_i g_i)} \\
= \sum_{y \in C : y_1 = 0} (-1)^{x \cdot (\sum_{i=2}^{m} y_i g_i)} - \sum_{y \in C : y_1 = 1} (-1)^{x \cdot (\sum_{i=2}^{m} y_i g_i)} = 0,
\]

(4.55)

where \( y = y_1 g_1 + \ldots + y_m g_m \) and where \( y_1 \ldots y_m \) goes from 000 \ldots 0 to 111 \ldots 1 in order for the generators to generate all the codewords \( y \in C \). The fact that this sum is equal to zero is a direct consequence of the fact that the number of codewords of \( C \) that are not orthogonal to \( x \notin C^\perp \) are half. If an Hadamard transform is applied to a quantum codeword of \( CSS(C_1, C_2) \) it results in

\[
|x_1 + C_2\rangle = \frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} |x_1 + y\rangle \xrightarrow{H^{\otimes n}} \frac{1}{\sqrt{|C_2|} 2^n} \sum_{\sum z} (-1)^{z \cdot (x_1 + y)} |z\rangle = \sqrt{\frac{|C_2|}{2^n}} \sum_{z \in C_2^\perp} (-1)^{z \cdot x_1} |z\rangle,
\]

(4.56)

in light of what was derived in (4.55). Hence, an Hadamard transform turns a superposition of all the codewords of a coset of code \( C_2 \) into a superposition of all the codewords of the dual code \( C_2^\perp \). Now, let \( e_1 \) be an \( n \) bit vector with 1s where bit flips occurred, and 0s elsewhere and \( e_2 \) an \( n \) bit vector with 1s where phase flips occurred, and 0s elsewhere. Thus, a corrupted quantum codeword can be written as

\[
\frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} (-1)^{e_2 \cdot (x_1 + y)} |x_1 + y + e_1\rangle.
\]

(4.57)

Using the parity check matrix of \( C_1 \) and some ancilla qubits one can detect where the bit flips occurred and from the error syndrome \( H_1 e_1 \), correct the errors; from the error-correcting properties of \( C_1 \) the code can correct up to \( t_1 \) bit flip errors. The reversible transformation used is as follows,

\[
\frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} (-1)^{e_2 \cdot (x_1 + y)} |x_1 + y + e_1\rangle |0\rangle \rightarrow \frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} (-1)^{e_2 \cdot (x_1 + y)} |x_1 + y + e_1\rangle |H_1 e_1\rangle,
\]

(4.58)

since \( H_1 (x_1 + y) = 0 \), thus the error can be corrected from the error syndrome by applying NOT gates on the corrupted qubits and the ancilla discarded, resulting in

\[
\frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} (-1)^{e_2 \cdot (x_1 + y)} |x_1 + y\rangle |H_1 e_1\rangle.
\]

Applying Hadamard gates to each qubit yields

\[
\frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} (-1)^{e_2 \cdot (x_1 + y)} |x_1 + y\rangle \rightarrow \frac{1}{\sqrt{|C_2|} 2^n} \sum_{z} \sum_{y \in C_2} (-1)^{(z + e_2) \cdot (x_1 + y)} |z\rangle \\
= \frac{1}{\sqrt{|C_2|} 2^n} \sum_{z'} \sum_{y \in C_2} (-1)^{(z' + e_2) \cdot (x_1 + y)} |z' + e_2\rangle \\
= \sqrt{\frac{|C_2|}{2^n}} \sum_{z' \in C_2^\perp} (-1)^{z' \cdot x_1} |z' + e_2\rangle,
\]

(4.59)

with \( z' = z + e_2 \) which translates into a bit flip error described by the vector \( e_2 \). Similarly to what was done before, the parity check matrix of \( C_1^\perp \), \( H_2 \), can be used to correct the bit flip error (originally phase flip
error) described by \(e_2\); from the error-correcting properties of \(C_2^+\) the code can correct up to \(t_2\) (originally) phase flip errors. Correcting the error yields

\[
\sqrt{\frac{|C_2^+|}{2^n}} \sum_{i' \in C^+} (-1)^{x_i} |z'\rangle
\]  

(4.60)

to which can be applied the \(n\)-qubit Hadamard transformation resulting in the state

\[
\frac{1}{\sqrt{|C_2^+|}} \sum_{y \in C_2} |x_i + y\rangle ,
\]  

(4.61)

considering the Hadamard gate is self-inverse, thus leading back to the original state, and that now \(e_2 = 0\). The original state can therefore be retrieved, and from this exposition the code \(\text{CSS}(C_1, C_2)\) is an \([n, k_1 - k_2, d \geq \min(d_1, d_2')]\) quantum code (with \(d = \min(d_1, d_2')\) if the code is non-degenerate), with \(d_1\) and \(d_2\) relating to \(t_1 = \lfloor \frac{d_1 - 1}{2} \rfloor\) and \(t_2 = \lfloor \frac{d_2 - 1}{2} \rfloor\), and correcting errors occurring in at least up to \(\min(t_1, t_2)\) qubits.

From a stabilizer perspective, the check matrix associated to the \(\text{CSS}\) code is

\[
\begin{bmatrix}
H(C_2^+) & 0 \\
0 & H(C_1)
\end{bmatrix}
\]  

(4.62)

and because this matrix must satisfy the commutativity condition \(H(C_2^+)H(C_1)^T = 0\), and hence \(H(C_2^+)H(C_1)^T = [H(C_1)G(C_2)]^T = 0\) which is verified since \(C_2 \subset C_1\).

### 4.5 Some quantum error correction codes

#### 4.5.1 The Steane code

The Steane code is an example of a \(\text{CSS}\) code which uses the classical \([7, 4, 3]\) Hamming code \(C\) with \(C_1 \equiv C\) and \(C_2 \equiv C^+\), and associated matrices

\[
H(C_1) = G(C_2)^T = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}, \quad H(C_2) = G(C_1)^T = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}.
\]  

(4.63)

Verifying that \(H(C_1)G(C_2) = H(C_1)H(C_1)^T = 0\) one obtains that \(C_2 \subset C_1\). Noting \(C_2\) is a \([7, 7 - 4, d = 4 \geq 3] = [7, 3, 4]\) classical linear code, then the Steane code is a \([7, 4 - 3, 3 \geq \min(3, 4)] = [7, 1, 3]\) quantum code, calculating the code’s distance. In this case, \(C_2^+ = C = C_1\) and the check matrix of the quantum code is

\[
\begin{bmatrix}
H(C) & 0 \\
0 & H(C)
\end{bmatrix}.
\]  

(4.64)

From (4.63), one infers that the weight of the codewords generated by the trivial coset is even, and of those generated by the other coset \((C_2 + [1110000])\) is odd, obtaining the following codewords (with normalizing factors used in the denominator of the kets multiplying the projector),

\[
|0_L\rangle = \prod_{i=1}^{n-k} \left( \frac{(I + g_i)}{2^{n-k}} \right) \frac{\mid 0000000 \rangle}{\sqrt{|C_2^+|/2^{n-k}}} = \frac{1}{\sqrt{|C_2^+|}} \sum_{s \in C} |s\rangle = |0000000\rangle + |1010101\rangle + |0110011\rangle + |0001111\rangle + |1100110\rangle + |0111100\rangle + |1101001\rangle + |0110101\rangle + |1001001\rangle + |1000111\rangle + |0100101\rangle + |0111100\rangle + |0110000\rangle + |0010110\rangle + |0101010\rangle + |1001100\rangle + |0011100\rangle \]  

(4.65)

\[
|1_L\rangle = \prod_{i=1}^{n-k} \left( \frac{(I + g_i)}{2^{n-k}} \right) \frac{\mid 1111111 \rangle}{\sqrt{|C_2^+|/2^{n-k}}} = \frac{1}{\sqrt{|C_2^+|}} \sum_{s \in C} |s\rangle = |1111111\rangle + |1001001\rangle + |0100101\rangle + |1000011\rangle + |1100000\rangle + |0010110\rangle + |0101010\rangle + |0101100\rangle + |0110011\rangle + |0110101\rangle + |0011000\rangle + |0011100\rangle + |0010110\rangle + |0101010\rangle + |1001100\rangle + |0011000\rangle \]  

(4.65)
and where the encoded $Z$ and $X$ operators are $\bar{X} \equiv X_1X_2X_3X_4X_5X_6X_7$ and $\bar{Z} \equiv Z_1Z_2Z_3Z_4Z_5Z_6Z_7$.

### 4.5.2 The five qubit code

The five qubit code is the smallest code capable of protecting against a single qubit error, and its corresponding generators and logical operators are presented below. Note that the generators are obtained by a cyclic permutation of the qubits to which each single qubit operator is applied; more clearly, one can shift right the first generator a certain number of times to obtain the remaining. This code is a non-degenerate $[5, 1, 3]$ CSS quantum code; regarding its distance, it is easy to see that any Pauli operator of weight one or two anticommutes with at least one of the generators. The codewords are

$$\begin{align*}
|0_L\rangle &= \sum_{M \in S} M |00000\rangle \sqrt{2^{n-k}} = \frac{1}{4} (|00000\rangle + |10010\rangle + |01001\rangle + |01010\rangle + |01010\rangle - |00110\rangle - |11011\rangle - |11100\rangle - |10111\rangle - |00101\rangle - |01101\rangle - |10101\rangle - |01000\rangle - |11000\rangle - |01111\rangle - |10110\rangle - |01011\rangle - |10011\rangle - |00100\rangle - |11010\rangle - |00001\rangle - |00010\rangle - |00011\rangle - |00100\rangle - |00110\rangle - |01001\rangle - |10000\rangle - |11001\rangle - |11100\rangle - |11111\rangle).
\end{align*}$$

$$|1_L\rangle = \bar{X} |0_L\rangle = \frac{1}{4} (|11111\rangle + |01101\rangle + |10110\rangle + |01011\rangle + |10101\rangle - |00010\rangle - |10000\rangle - |01001\rangle - |11001\rangle - |11100\rangle - |01111\rangle - |00111\rangle - |10111\rangle - |01101\rangle - |10100\rangle + |00101\rangle + |00001\rangle + |00010\rangle - |00011\rangle) \quad (4.66)$$

<table>
<thead>
<tr>
<th>Name</th>
<th>Operator</th>
</tr>
</thead>
<tbody>
<tr>
<td>$g_1$</td>
<td>$XZZXI$</td>
</tr>
<tr>
<td>$g_2$</td>
<td>$IXZZX$</td>
</tr>
<tr>
<td>$g_3$</td>
<td>$XIXZZ$</td>
</tr>
<tr>
<td>$g_4$</td>
<td>$ZXIXZ$</td>
</tr>
<tr>
<td>$\bar{Z}$</td>
<td>$ZZZZZ$</td>
</tr>
<tr>
<td>$\bar{X}$</td>
<td>$XXXXX$</td>
</tr>
</tbody>
</table>

### 4.5.3 The Shor code

The Shor code is a $[9, 1, 3]$ degenerate CSS code. The corresponding generators and logical operators can be taken to be the ones in table 4.2.

The distance of the code is seen to be 3 and not 2, a consequence of its degeneracy, and $C_2 \subseteq C_1$ since $H(C_1)G(C_2) = H(C_1)H(C_2^\perp)^T = 0$.

### 4.6 Bounds in quantum error correction

Take an $[n, k]$ non-degenerate code which can correct errors on $t$ qubits or less. Then, if errors occur in $j$ qubits the number of subsets of the $n$ qubits in which an error occurs in $j$ qubits is $\binom{n}{j}$. Moreover, for each qubit taking the error to be one of the three Pauli matrices $X$, $Y$, and $Z$ gives a total of $3^j$ possible errors for a particular set of qubits affected by $j$ errors, therefore the number of errors that may occur on $t$ or fewer qubits is $\sum_{j=0}^{t} \binom{n}{j} 3^j$. Because the code is non-degenerate each particular error must lead the $2^k$-dimensional subspace of the codewords into an orthogonal $2^k$-dimensional subspace with respect to the remaining errors, and those must fit into the total $2^n$ dimensional space available to $n$ qubits, hence

$$\sum_{j=0}^{t} \binom{n}{j} 3^j 2^k \leq 2^n, \quad (4.67)$$
For an arbitrary quantum code (i.e. including degenerate codes) one can obtain the quantum singleton bound which is \( n - k \geq 2(d - 1) \) (for an \([n, k, d]\) quantum code). Proving it for \( k = 1 \), assume \( 2(d - 1) = n \) (first value of \( n \) violating the bound), thus having the non-corrupted original encoded state one can take \( d - 1 \) of its qubits and add \( d - 1 \) garbage qubits, e.g. \([0 \ldots 0]\), performing \( n \) qubits, similarly one can take the remaining \( d - 1 \) qubits and do the same. Now, because the code can correct up to \( d - 1 \) erasure errors (qubits affected by the errors are known, thus one distinguishes errors of weight \( w < d \) of this kind on the code) it is possible to recover from the garbage qubits of both sets and obtain two copies of the original state from itself, hence violating the no-cloning theorem and therefore \( n \geq 2(d - 1) + 1 \). For \( k \geq 1 \), let the state considered be \( |\psi\rangle = \frac{1}{\sqrt{2^n}} \sum_x |x\rangle_Q |x'\rangle_R \) with the encoded state of \( Q \) entangled with the \( k\)-qubit state of the reference system \( R \) where each \( x \) corresponds to \( x' \) encoded. Let the qubits of \( Q \) be subdivided into two sets of \( d - 1 \) qubits, \( Q_1 \) and \( Q_2 \), and one set of \( n - 2(d - 1) \) qubits, \( Q_3 \) (accounting for all \( n \) qubits). Note now that one could take \( Q_1 \) and \( Q_3 \) (\( Q_2 \) and \( Q_3 \)) and from it reconstruct the original state \( |x\rangle \) with the reconstruction being entangled with \( R \). Therefore, \( Q_2 \) and \( R \) (\( Q_1 \) and \( R \)) are uncorrelated (thus the respective density operator can be written as a tensor product of both parts) and so \( S(RQ_1) = S(R) + S(Q_1) \) and \( S(RQ_2) = S(R) + S(Q_2) \), and

\[
S(RQ_1) = \begin{cases} 
S(Q_2Q_3) & \text{from the purity of } RQ_1Q_3 \\
S(Q_1Q_3) & \text{from the purity of } RQ_1Q_3 
\end{cases}
\leq S(Q_2) + S(Q_3)
\]

\[
S(RQ_2) = \begin{cases} 
S(Q_2Q_3) & \text{from the purity of } RQ_1Q_3 \\
S(Q_1Q_3) & \text{from the purity of } RQ_1Q_3 
\end{cases}
\leq S(Q_1) + S(Q_3)
\]

where \( S(\rho) = -\text{tr}(\rho \log \rho) \) is the von Neumann entropy and some of its properties were used, obtaining \( n - k \geq 2(d - 1) \).

Another bound is the quantum Gilbert-Varshamov bound which is somewhat similar to the quan-
tum Hamming bound. Recalling the quantum error correction conditions which can be expressed as 
\[ \langle \psi | E_a^\dagger E_b | \psi \rangle = \alpha_{ab} \delta_{ij} \] . When the possible errors are all operators of weight less than or equal to \( t \), \( O = E_a^\dagger E_b \) can be any operator of weight \( \leq 2t \). Therefore, consider a code encoding a maximum number of qubits \( k \) for a given \( n \) of distance \( d \), and so \( O \) is any operator of weight less than \( d \), hence the statement 
\[ \langle \psi | E_a^\dagger E_b | \psi \rangle = \alpha_{ab} \]  
(4.69)
translates into \( N = \sum_{j=0}^{d-1} \binom{n}{j} 3^j \) constraints on the state \( |\psi\rangle \). Now, for a generic \( \alpha_{ab} \) (satisfying the appropriate algebraic constraints) one can choose a generic state \( |\psi_1\rangle \) satisfying (4.69). Now, focus on the subspace orthogonal to \( |\psi_1\rangle \) and to all \( O |\psi_1\rangle \) for operators \( O \) of weight less than \( d \), which is a subspace with dimension \( 2^n - N \) for an \( n \)-qubit Hilbert space. One can then choose a \( |\psi_2\rangle \) in that subspace satisfying (4.69). It is possible to continue choosing \( |\psi_i\rangle \) orthonormal to all \( |\psi_j\rangle \) and \( O |\psi_j\rangle \) \( (j = 1, \ldots, i - 1) \) and satisfying (4.69) as long as \( 0 < 2^n - Ni \). Since the code encodes the maximum number of qubits, then for \( i = 2^k \) is where this condition first fails, otherwise the code subspace could be augmented to \( 2^k + 1 \) codewords continuing the procedure, contradicting the maximality of \( k \). Thus,
\[ \sum_{j=0}^{d-1} \binom{n}{j} 3^j 2^k \geq 2^n, \]  
(4.70)
which is the quantum Gilbert-Varshamov bound. Both the Gilbert-Varshamov bound and the quantum singleton bound are applicable to degenerate codes.

The most famous forms of the quantum Gilbert-Varshamov bound and the quantum Hamming bound are their asymptotical versions. Regarding the Gilbert-Varshamov bound, from the Chernoff bound one obtains
\[ n - k \leq \log \left( \sum_{j=0}^{d-1} \binom{n}{j} 3^j \right) \leq \log \left( \frac{1}{p^n} \sum_{j=0}^{\bar{\mu} n} \binom{n}{j} p^{n-j} q^j \right) \leq \log \left( \frac{e^{-nH(\bar{\mu} | q)}}{p^n} \right) \leq -n(H(\bar{\mu} | q) + \log p), \]  
(4.71)
with \( H(\bar{\mu} | q) = \bar{\mu} \log (\bar{\mu} / q) + (1 - \bar{\mu}) \log ((1 - \bar{\mu}) / (1 - q)) \) and where \( p = 1 - q, \bar{\mu} n = \mu n = d - 1 \) and
\[ \sum_{j=0}^{d-1} \binom{n}{j} 3^j = \frac{1}{p^n} \sum_{j=0}^{\bar{\mu} n} \binom{n}{j} p^{n-j} q^j, \]  
(4.72)
Therefore,
\[ n - k \leq n(H(\bar{\mu}) + \bar{\mu} \log (1 - p) + (1 - \bar{\mu}) \log (p) - \log (p)) \iff k \geq \frac{1}{n} \left( 1 - H(\bar{\mu}) - \bar{\mu} \log (1 - \bar{\mu}) \right). \]  
(4.73)
where \( H(\cdot) \) is the Shannon entropy, \( H(\bar{\mu}) \equiv -\bar{\mu} \log (\bar{\mu}) - (1 - \bar{\mu}) \log (1 - \bar{\mu}) \).

For the Hamming bound one has
\[ \binom{n}{\mu n} 3^{\mu n} \leq \sum_{j=0}^{\mu n} \binom{n}{j} 3^j \leq 2^{n - \mu n}, \]  
(4.74)
where \( \mu n = t \). By applying logarithm on both sides of (4.74) and taking into account that \( \binom{n}{\mu n} = (1 + o(1)) 2^{nH(\mu / n)} \) one obtains
\[ \log (2^{nH(\mu)} + \mu n \log (3)) \leq \log (1 + o(1)) 2^{nH(\mu)} + \mu n \log (3) \leq n - k \iff \frac{k}{n} \leq 1 - \mu n \log (3) - H(\mu). \]  
(4.75)
Thus, an \([n, k, d]\) quantum code correcting \( t \) errors satisfies
\[ 1 - \frac{d - 1}{n} \log (3) - H \left( \frac{d - 1}{n} \right) \leq \frac{k}{n} \leq 1 - \frac{t}{n} \log (3) - H \left( \frac{t}{n} \right) \]  
(4.76)
in the limit \( n \to \infty \), where the upper bound only applies for non-degenerate quantum codes.
Chapter 5
Fault-tolerant quantum computation

5.1 Fault-tolerant quantum computation: Introduction

A quantum computer is affected by noise which incurs in errors in the data, thus one must protect data from the noise and minimize the propagation of errors. If one wishes to make an arbitrarily long computation in a quantum computer, then the components of the circuit must be implemented fault-tolerantly. With quantum error correction codes and fault-tolerant techniques derived from keen considerations it is possible to develop proper fault-tolerant components.

As a starting point, let the error model be defined. The first assumption regarding it is that the possible errors on a qubit are $X$, $Y$ or $Z$ (errors from Pauli group when considering all the qubits) which occur with some probability. The second assumption is that errors on different qubits occur independently except when some set of qubits is involved in some interaction (such as some multi-qubit gate), in that case that set can suffer from a correlated error (from the Pauli group) involving those qubits, hence the gate errors only affect the qubits the gate acts upon. Another aspect important for the model is what locations are vulnerable to errors; those are the gates, the state preparations, the measurements, and the wires (storage errors; it is considered that the qubit is susceptible to errors when it is waiting for some operation to be performed on it). Now, let it be stated what is understood by fault-tolerant regarding each of these locations. Define fault-tolerance of an operation to be the property that an error on a single qubit or elementary gate does not cause more than one error (affecting a single qubit) in each encoded block of qubits. Even though the QECC (quantum error-correcting code) might be able to correct $t > 1$ errors, this property is adequate to all QECCs with $t \geq 1$ and even if it is somewhat conservative, it aids in keeping the propagation of errors to a minimum. In a more specific note, it is also required for a fault tolerant measurement result to be correct with probability $1 - O(p^2)$ where $p$ is the maximum probability of failure in any of the FT measurement’s elementary components (more on this later).

In light of the definition of fault-tolerance, a particular interesting set of operations are the ones that act independently on different qubits of a same encoded block (i.e. with a tensor product of single-qubit gates) or/and interact only qubits from one block to corresponding qubits of another block (can be an ancilla block). Such operations are called transversal and clearly, any transversal operation is fault-tolerant. One of the goals of fault-tolerant quantum computation is to perform the operations on the encoded states, since if they were to be done on the unencoded versions, the data would be unprotected in those moments, which is not desirable. In order to understand how to do this let the Clifford group be introduced. The Clifford group is the set $C_n = \{ U \in U(2^n) : UPU^\dagger \in P_n, \ \forall P \in P_n \}$ and is the normalizer of $P_n$ in the unitary group $U(2^n)$. The generators of this group are the CNOT, $H$ and $S$ gates. Note that $U |\psi\rangle = UM |\psi\rangle = (UMU^\dagger)U |\psi\rangle$ for a stabilizer operator $M$ and a unitary operation $U$, thus after $U$ is applied the stabilizer is formed by the operators $\{UMU^\dagger \}$ which are the conjugate of $M$ by $U$. Conjugation is a group homomorphism, and hence $U$ takes the stabilizer $S$ to a stabilizer $S'$ of the same form. Since the implementation of an arbitrary unitary gate is desired, and not just operators from the Clifford group, then one needs more gates in order to form a universal set of gates. In fact, taking the Clifford group and a gate from $SU(2^n)$ which is not in the Clifford group originates a group which
is dense in $SU(2^n)$, thus forming a universal set of gates. Regarding the operations from the Clifford group, heed the following theorem.

**Theorem 5.1.1** (Gottesman-Knill theorem). *A quantum circuit consisting only of state preparations in the computational basis, measurements of observables in the Pauli group (which includes measurement in the computational basis as a special case), Clifford group gates and Clifford group gates conditioned on classical information can be efficiently simulated on a classical computer.*

This theorem shows how subtle is the power of a quantum computer, with a substantial portion of quantum circuits efficiently simulatable in a classical computer. The simulation on the computer is done simply by keeping track of the $n$ generators of the stabilizer, and since the elementary operators mentioned in the theorem can be simulated using $O(n^2)$ steps, it means that a circuit with $m$ operations can be simulated using $O(mn^2)$ operations on a classical computer.

Now, let the error locations be addressed starting with how to perform encoded logical operations. From the study of stabilizers, a stabilizer code has associated to $N(S) - S$ logical operators $\bar{X}_i$ and $\bar{Z}_i$ which are transversal, and hence automatically fault tolerant. Extending the view to Clifford group operators, transversal $\bar{X}$, $\bar{CNOT}$, and $\bar{S}$ would also be desirable, however this is not a given, nonetheless it is possible to find codes for which all these gates are transversal, thus the Clifford group’s gates can be implemented transversally. Still, there is no code having a universal set of transversal gates, hence at least one of the gates of the set must have a specific tailored fault-tolerant design.

For any CSS code the $\bar{CNOT}$ gate is transversal and there are CSS codes that also have transversal $\bar{H}$, $\bar{CNOT}$ and $\bar{S}$, and one such code is the Steane code which will be used here as example. For the

\[
\begin{align*}
\text{First block} & \{ \bullet \quad \vdots \quad \bullet \} \\
\text{Second block} & \{ \oplus \quad \vdots \quad \oplus \}
\end{align*}
\]

Figure 5.1: Tranversal controlled-NOT between two encoded qubits implementing the controlled-NOT operation on qubits encoded with a Steane code. Source: [13].

Steane code, $\bar{X} = X^{\otimes 7}$, $\bar{Z} = Z^{\otimes 7}$, $\bar{H} = H^{\otimes 7}$ ($\bar{X} = \bar{H} \bar{Z} \bar{H}$), $\bar{P} = P^{\otimes 7}$ and $\bar{CNOT}$ is just the bitwise $CNOT$ (figure 5.1). For the last gate needed to have a universal set it is chosen the $\frac{\pi}{8}$ gate whose fault tolerant implementation will be shown later (the Toffoli gate would also be a valid choice).

Consider now the propagation of errors on the two-qubit elementary $CNOT$ gate. Affecting two qubits, the $CNOT$ can provoke errors on both if one has already an error. For a $CNOT$ from the first qubit to the second, if the error $X \otimes I$ occurs then by composition with the $CNOT$ one obtains $X \otimes X$ and the error $X$ is propagated forward to the other qubit, if the error $I \otimes X$ occurs then after the $CNOT$ the error is still $I \otimes X$, if the error $Z \otimes I$ occurs then after the $CNOT$ the error is still $Z \otimes I$, and if the error $I \otimes Z$ occurs then after the $CNOT$ the error is $Z \otimes Z$, and therefore, the error $Z$ is propagated backwards to the first qubit (propagated to the control qubit).
5.2 Fault-tolerant measurement

Let $M = M_1 \otimes \ldots \otimes M_l$ be the observable to measure, then the circuit in figure 5.2 can be used to measure it. Regarding the cat state, its preparation will be described later. With respect to the functioning, the cat state is used to identify if $M |\bar{\psi}\rangle = |\bar{\psi}\rangle$ or $M |\bar{\psi}\rangle = -|\bar{\psi}\rangle$, hence identifying the eigenvalue corresponding to the eigenstate $|\bar{\psi}\rangle$. It does it by applying all of the $M_i$s at the same time (behaviour associated to the $|1\ldots 1\rangle$ part of the cat state) and consequently acquiring the value of the of the eigenvalue $\lambda$ as $\lambda |1\ldots 1\rangle$ while the $|0\ldots 0\rangle$ component of the cat state leaves the state be and so the resulting state until the moment is $\frac{1}{\sqrt{2}} ((0\ldots 0) + \lambda |1\ldots 1\rangle) |\psi\rangle$. Applying the Hadamard to each qubit associated with the cat state results in $\frac{1}{\sqrt{2}} ((0\ldots 0) + |1\ldots 1\rangle) \rightarrow \frac{1}{\sqrt{2^{n_{anc}-1}}} \sum_{\text{even} z} |z\rangle$ and $\frac{1}{\sqrt{2}} ((0\ldots 0) - |1\ldots 1\rangle) \rightarrow \frac{1}{\sqrt{2^{n_{anc}-1}}} \sum_{\text{odd} z} |z\rangle$. Thus, the measurement will yield a random odd (even) codeword if the correspondent eigenvalue is $-1 (+1)$. In order for the outcome to be correct with probability $1 - O(p^2)$, the measurement is repeated at least three times so one can take the majority vote as the measurement result. If the cat state is prepared fault-tolerantly then this procedure realizes a fault-tolerant measurement.

5.3 Error correction

After some operation is done, an error correcting operation is performed in order to undo damage done to the state during the operation. Considering the stabilizer formalism, one obtains the error syndrome by verifying if some error commutes or anti-commutes with each generator, which is equivalent to measuring the generators, i.e. applying the state to each generator obtaining the associated eigenvalue. The circuit of figure 5.2 where $M$ will be each of the generators does exactly that. With the error syndrome one can use a look-up table of error syndromes if the code is not to large, or if it is large a decoding algorithm in order to identify the error and correct it by applying it again to the state (or some operation with the same syndrome if the code is degenerate). Another circuit that can be used in error correction of stabilizer codes is the one in figure 5.3, which is Knill's error correction method.

Wire (1) corresponds to a procedure to obtain the $Z$ factors of the error (consider the Pauli group error tensorial-product writing) and wire (2) corresponds to a procedure to obtain the $X$ factors of the
error. Wire (3) is used to reconstruct the original state. Take the following map of events in the circuit,

\[
(\alpha |0_c\rangle + \beta |1_c\rangle)(|0\rangle + |1\rangle) / \sqrt{2} \xrightarrow{\text{CNOT}^{(1,2)}} (\alpha |0_c\rangle + \beta |1_c\rangle)(|0\rangle|0_n\rangle + |1\rangle|1_n\rangle) / \sqrt{2}
\]

\[
\bar{H} \alpha \left( \frac{|0_{cz}\rangle + |1_{cz}\rangle}{\sqrt{2}} \right) |s_1\rangle + \beta \left( \frac{|0_{cz}\rangle - |1_{cz}\rangle}{\sqrt{2}} \right) |s_2\rangle
\]

\[
= |0_{cz}\rangle \left( \frac{\alpha |s_1\rangle + \beta |s_2\rangle}{\sqrt{2}} \right) + |1_{cz}\rangle \left( \frac{\alpha |s_1\rangle - \beta |s_2\rangle}{\sqrt{2}} \right)
\]

\[
\Rightarrow |c_1\rangle (\alpha |s_1\rangle + (-1)^{m(1)} \beta |s_2\rangle) / \sqrt{2}
\]

\[
= |c_1\rangle (\alpha |0_{ne}\rangle + (-1)^{m(1)} \beta |1_{ne}\rangle) + |1_c\rangle (\alpha |1_{ne}\rangle + (-1)^{m(1)} \beta |0_{ne}\rangle) / 2
\]

where subscript c means that the state is corrupted by noise (with Z and X components), the subscript e means that the state is corrupted by the same X errors as the corrupted state with subscript c, the subscript ne emphasizes that the associated state is not corrupted (|0_ne\rangle = |0\rangle) and the ez subscript highlights that the Z errors (of the corrupted state of the data) were switched to X errors by the Hadamard, and those are the relevant ones considering the corresponding qubit is going to be measured (M(1)). In measurement M(1) the codeword obtained (|c_1\rangle) is part of |\bar{0}_{cz}\rangle (with |m(1) = 0\rangle as the correct corresponding quantum codeword) or of |1_{cz}\rangle (with |m(1) = 1\rangle as the correct corresponding quantum codeword), and m(1) ∈ {0, 1} is the variable identifying to which one the codeword is part. The same goes for m(2) ∈ {0, 1} but with respect to |\bar{0}_{c}\rangle and |\bar{1}_{c}\rangle, with the corresponding codeword being |c_2\rangle. By identifying the codeword of the code that is closest to the corrupted codewords c1 and c2, it is possible to find m(1) and m(2) (depending on the weight of the errors and the error-correcting capabilities of the code), and thus correct the final state in wire (3) to α|0\rangle + β|1\rangle by applying \( \bar{Z} \) (\((m(1), m(2)) = (1, 0)\)), \( \bar{X} \) (\((m(1), m(2)) = (0, 1)\)) or \( \bar{Z}\bar{X} \) (\((m(1), m(2)) = (1, 1)\)).

For CSS codes, the Steane's error correction method can be used and the associated circuit is presented in figure 5.4. In its wire (1) the bit-flip errors are detected, the X’s, and in its wire (2) the phase errors are detected, the Z’s. The CNOT error propagation properties are again used as an advantage in this circuit. Regarding the effect of the CNOT between the data qubit and wire (1), for an unencoded version of the circuit the state |+_s\rangle = |0\rangle |+_s\rangle / \sqrt{2} would remain the same, however for the encoded version the X errors propagate to the state changing the codewords that constitute |0\rangle and |1\rangle of |+_s\rangle, thus by measuring it one obtains a random flipped codeword, which is flipped in the places of the X errors, hence finding the codeword of C1, that is closest to the resultant codeword of the measurement allows

Figure 5.3: Knill’s error correction method. Adapted from: [18].

\[
\psi \quad (1)
\]

\[
\pm \quad (2)
\]

\[
|0\rangle \quad (3)
\]
the correction of the bit-flip errors. Regarding the effect of the CNOT between the data qubit and wire (2), the Z errors propagate to \( \ket{0} \) and by action of the Hadamard gate they are switched to bit-flip errors, also it rotates the state to the Hadamard basis (the quantum codeword is a superposition of codewords in \( C_2^\perp \) in that basis), thus performing the measurement will yield a random corrupted codeword, which by finding the codeword of \( C_2^\perp \) that is closest to it allows the correction of the phase errors.

5.4 State preparation

One of the states used previously to perform a measurement was the cat state. A circuit preparing this state is shown in figure 5.5 where the last ancilla qubit is used to verify the state; note that no single bit-flip error can pass the verification. Note also that the circuit is susceptible to phase errors in odd number (thus equivalent to just one applied; this considering the three lower qubits become corrupted after targeted by the CNOTs) on the cat state resulting in the state \( \frac{\ket{0000} - \ket{1111}}{\sqrt{2}} \), which in the circuit of figure 5.2 flips the outcome of the measurement. For a general size cat-state, more parity checks would be required, hence replicas of the one in figure 5.5 for different pairs of qubits (using more ancillas) would be necessary. If the state does not pass the verification, it is discarded, and a new state is prepared which is accepted by passing the verification. This procedure thus implements a fault-tolerant preparation of the cat state. For encoding purposes, preparing the state \( \ket{\overline{0}} \) is enough and can be done considering its stabilizer which is \( \langle S, Z \rangle \). The state \( \ket{\overline{+}} \), for example, has stabilizer \( \langle S, X \rangle \). Starting with an arbitrary state, one can measure each generator and with the resulting eigenvalues from the measurements an error syndrome is obtained, from which one can correct the state obtaining the single state stabilized by \( \langle S, Z \rangle \) which is \( \ket{0} \). Other states can be obtained directly from this one, such as \( \ket{1} = X \ket{0} \) or \( \ket{\overline{+}} = H \ket{0} \).

Figure 5.5: Four-qubit cat state fault-tolerant preparation. Adapted from [13].
5.5 The $\frac{\pi}{8}$ gate

The circuit implementing the $\frac{\pi}{8}$ fault-tolerantly is presented in figure 5.6 where $|\tilde{0}\rangle = \tilde{T}H|0\rangle = |\tilde{0}\rangle + e^{i\pi/4}|1\rangle \sqrt{2}$ and where after the $CNOT$ one has

$$|\tilde{0}\rangle \langle \tilde{0}| + \beta|\tilde{1}\rangle \langle \tilde{1}| + e^{i\pi/4}|\tilde{1}\rangle \langle \tilde{1}| + \beta|\tilde{0}\rangle \langle \tilde{0}| = \frac{1}{\sqrt{2}} \left[ (|\alpha\rangle |0\rangle + \beta e^{i\pi/4}|1\rangle) |0\rangle + (|\beta\rangle |0\rangle + \alpha e^{i\pi/4}|1\rangle) |1\rangle \right]$$

with $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. If the measurement outcome is 0, then the desired transformation ($\tilde{T}$) was applied to the state, while if it is 1, $SX$ is applied so the transformation becomes the desired one. Note that the $|\tilde{0}\rangle$ is a +1 eigenstate of $SX$, i.e. it is stabilized by it, and being $Z$ the stabilizer of the state $|0\rangle$, note that $THZHT^\dagger = TXT^\dagger = e^{-i\pi/4}SX$. Note also that the measurement outcome being 1 means that the resultant state is $TX|\psi\rangle$ and to obtain $T|\psi\rangle$ one only needs to apply $TXT^\dagger = e^{-i\pi/4}SX$ (which is $SX$, except for the global phase which is irrelevant). The state $|\tilde{0}\rangle$, to be prepared fault-tolerantly needs to be verified, and to do it the circuit in figure 5.2 is used by repeating the measurement of the observable $e^{-i\pi/4}SX$ which stabilizes the state, and taking the majority vote, if it is +1 the state is taken to be correct one, otherwise it is discarded and this procedure starts anew repeating itself until the state passes the verification. Of course, the observable $e^{-i\pi/4}SX$ has to be implemented in a transversal fashion, but since the Clifford group can all be implemented transversally this should not be a problem. For the Steane code, one can use the observable $SX$ and seven single-qubit $T$ gates applied to each of the ancilla qubits ($e^{T\pi/4} = e^{-i\pi/4}$) in the circuit of figure 5.2. Hence, the $\frac{\pi}{8}$ gate can be implemented fault-tolerantly. A last remark is although the $T$ gate used in the circuit in figure 5.6 is not a fault-tolerant implementation, it should respect the principles of fault tolerance as much as possible (in order to minimize the amount of errors).

![Figure 5.6: $\frac{\pi}{8}$ gate fault-tolerant implementation. Adapted from: [13](#)](image)

5.6 The threshold theorem

A question that should be answered from the beginning of the fault-tolerant construction (since the negative answer would turn most of the construction useless) is if quantum error correction can actually improve the data’s reliability. This is a valid question considering that using it requires more gates, more wires, more hardware overall, thus introducing also more noise and errors. The question then is if the overall noise including the inherent to using a QECC has effectively less impact on the data than when not using the QECC. The answer to the question is that quantum error correction can actually improve the data’s reliability given that some reasonable conditions are satisfied.

Consider an encoded block and that each qubit in that block is also encoded, and that each qubit from this previous block is also encoded, and so on until some level. Such a code is called a concatenated code. This type of code exploits parallelism very well. If the code used at each level is an $[n_i, 1, d_i]$ then the concatenated code is an $[n_1 \ldots n_l, 1, d_1 \ldots d_l]$ code. The error correction is made level by level starting from the deepest level, the one with $n_1 \ldots n_{l-1}$ blocks of $n_l$ qubits, and ending with the correction of the first level, the one with $n_1$ blocks of $n_2 \ldots n_l$ qubits. The correction of all the blocks in one level...
can be made in parallel. Now, let \( p \) be the probability of a component failing at the deepest level (level \( l \)), then for every block at this level the probability of failure (two or more errors, thus \( O(p^2) \)) is \( c(p^2)^2 \), in the next level the probability of two errors in a block is \( c(p^2)^2 \) for all its blocks, and so on until the first level is reached. Then the probability of failure in the first level is \( (cp)^2/l \) with the size of the simulated circuit \( d' \) times bigger the original circuit’s size, where \( d \) is a constant representing the maximum number of operations used in a fault-tolerant procedure to do an encoded gate and error-correction. Supposing that it is wished to simulate a circuit with \( p(n) \) (a polynomial function on the size \( n \) of the problem) gates achieving some final accuracy \( \epsilon \), then each gate must be accurate to \( \epsilon/p(n) \), then the concatenation level must be such that

\[
\frac{(cp)^2}{c} \leq \frac{\epsilon}{p(n)},
\]

which can be satisfied for some value of \( l \) provided that \( p < p_{th} \equiv 1/c \). The condition \( p < p_{th} \) is known as the threshold condition for quantum computation. The size of the simulated circuit is

\[
d^k = \left( \frac{\log(p(n)/\epsilon)}{\log(1/pe)} \right)^{\log d} = O(poly(\log p(n)/\epsilon)),
\]

obtained by solving for equality in (5.3), where \( poly \) indicates a polynomial of fixed degree, and thus the simulating circuit contains \( O(p(n)poly(\log p(n)/\epsilon)) \) gates. From all this reasoning the following theorem can be stated.

**Theorem 5.6.1 (Threshold theorem for quantum computation [13]).** A quantum circuit containing \( p(n) \) gates may be simulated with probability of error at most \( \epsilon \) using

\[
O(p(n)poly(\log p(n)/\epsilon))
\]

gates on hardware whose components fail with probability at most \( p \), provided \( p \) is below some constant threshold, \( p < p_{th} \), and given reasonable assumptions about the noise in the underlying hardware.

### 5.7 Some final remarks

With quantum error correction, the entropy introduced by noise and error correction is flushed to the ancillas. So, error correction requires that a supply of fresh ancilla qubits is available, however much like the Maxwell demon (see [13]) the computer does not have infinite memory and so, it does not seem sustainable producing new ancillas in arbitrary long computations, hence the ancillas must be reused, thus its previous information erased, which by Landauer’s principle means a dissipation of power, and hence the computer will heat, therefore the quantum computer will need cooling.

To minimize storage errors and the time of computation, parallelization is fundamental. The quantum computer’s hardware might be more susceptible to a certain type of errors, thus the QECC and the circuit design should be chosen so as to better protect the data against it. Something to consider is that the distance between the qubits might provide itself as an obstacle in performing computation involving them.

Some classical computation is needed in error correction, although in the exposition above it was not considered the time required to do it, it was assumed so fast that it would not affect significantly the operation of the quantum computer and that would not be so long that new errors would start to creep up.

The QECCs should be chosen considering its suitability to the type of noise that most afflicts the circuit, the transversal operations associated to it, the value of \( n/k \) and the code’s distance, among others.
Chapter 6
Quantum Computation

6.1 Computation complexity theory and quantum computation

Recall computation complexity theory which provides a solid definition that makes it possible to measure the resources (in a standard way) needed to solve some computational problem independently of the machine solving it. The referred definition sets a line in how the resources increase with the input size, this line separates the problems and algorithms which have a polynomial bounded increase of resources with the increase of the input size, from the ones that have a greater increase with the increase of the input size, which are usually denoted in complexity theory, abusively, as having an exponential increase of resources. Hence, a problem is labelled polynomial in \( n \) for some resource, with \( n \) being the input size (where \( n \) should be measured using the same unit of size when comparing different algorithms), otherwise it is labelled exponential in \( n \) for that same resource. This type of definition determines which algorithm is better asymptotically unequivocally, however for smaller values of input size this definition allows one of the algorithms to be better or worse than the other regardless of the asymptotic behaviour, hence if an algorithm is to be used for small sized inputs the algorithms’ resource variation in that domain should be analysed instead. However, usually the asymptotic behaviour of the resources with the input size is the important factor to consider in the domain of input sizes of interest and thus, the presented definition is a relevant and meaningful definition (another important aspect for this relevance is that the Strong Church-Turing thesis brings to the definition the machine independent complexity property for classical computers).

With so many different computers with different specifications, an abstract general machine is taken to be the representative, one such that anything a real computer can compute that machine can also compute, an abstract model of a machine that captures the computational power of a real classical computer, the Turing machine. Hence, it is important for the reader to identify the Turing machine model with a real computer. The probabilistic Turing machines adds a probabilistic component to it, however all the outcomes associated to its probabilistic transitions can be explored using a deterministic Turing machine, thus the deterministic Turing machine can simulate the probabilistic one, hence both models of computation are equivalent. Note that they are nonetheless different in efficiency, namely the deterministic is less efficient. For this reason and for its probabilistic nature shared also by the quantum computer, this model (probabilistic Turing machine) is the one that is chosen as the classical computer base of comparison for a quantum computer; it will be clearer computation-wise later.

The Strong Church-Turing thesis implies that any model of computation can be simulated on a probabilistic Turing machine with at most a polynomial increase in the number of elementary operations required, but this might not encompass a quantum computer, if a quantum computer cannot be simulated on a probabilistic Turing machine with at most a polynomial increase in the number of elementary operations required. In that case, the strong Church-Turing thesis does not hold for quantum computers and quantum supremacy is the reality; that a quantum computer can solve problems (useful ones, desirably) polynomial in time that a classical computer cannot in polynomial time, hence a quantum computer model would be more efficient than a classical computer one.
Going back to resources, the resources of interest are time and space/memory. The time complexity classes will be the first explored. A complexity class is a set of problems of related complexity and are defined according to the following properties: the model of computation (deterministic Turing machine, probabilistic Turing machine, quantum computer, ...), type of computational problem (decision, optimization, counting ...), and the resource of interest (time, space, ...).

The classes presented next are very famous, because of the important \( P \) versus \( NP \) problem, an open problem so far. The complexity class \( P \) contains all decision problems solvable in polynomial time (on a Turing machine), and the complexity class \( NP \) contains all decision problems for which there is a polynomial time algorithm (on a Turing machine) which can verify if a given input is a solution to that problem. Then, from the comments made previously where the model identifies algorithms/problems whose resources’ amount are bounded by a polynomial function on the input size as efficient/easy and the ones whose resources’ amount cannot be bounded by any polynomial function on the input size, that are instead bounded by a supra-polynomial function on the input size as inefficient/hard, the class \( P \) can be identified with efficiently solvable problems and the class \( NP \) can be identified with efficiently verifiable problems. The fact that \( P \subseteq NP \) is clear and well known, but the \( P \) versus \( NP \) problem focuses on the question: \( P = NP \) or \( P \neq NP \)? In other words, it focuses on answering if \( P \) is the same as \( NP \). If \( P \neq NP \) then it is possible to prove that there is a non-empty intermediate class, \( NPI \), whose problems are neither solvable with polynomial resources, nor are \( NP \)-complete (set of \( NP \) problems such that if one can solve an \( NP \)-complete problem efficiently, then one is also capable of solving all \( NP \) problems efficiently). No problems are known to be in \( NPI \), otherwise it would imply that \( P \neq NP \) and \( P \neq NP \) would be known to be true. This class might be important because if quantum computers are not able of efficiently solving all problems in \( NP \) (and hence \( NP \)-complete problems) then the \( NPI \) is the class of problems to focus on, since problems in \( P \) are already efficiently solvable on classical computers.

Now, regarding space complexity classes, the class \( PSPACE \) is presented. The \( PSPACE \) class is the class of all decision problems solvable using a polynomial amount of space on the input size (on a Turing machine). Relating with previous presented classes, \( PSPACE \) contains \( P \) since one can only fill a polynomial amount of space using a polynomial amount of time, but also contains \( NP \) for checking a possible solution takes polynomial amount of time, and hence can only fill a polynomial amount of space on the input size, and checking all guesses until a correct one is found overwriting the space used by the former incorrect guesses only fills also a polynomial amount of space on the input size.

Now, let’s introduce the class that is the classical analogue of the class that represents the problems solved efficiently on a quantum computer. The \( BPP \) is the class of decision problems solvable by a probabilistic Turing machine on polynomial time with an error probability less than \( \frac{1}{3} \). The number \( \frac{1}{3} \) is arbitrary, it suffices that the success probability is bigger than \( p \) with \( \frac{1}{2} < p \leq 1 \) (in the choice selected \( p = \frac{2}{3} \)). On the other hand, \( BQP \) is the class of decision problems solvable by a quantum computer in polynomial time with an error probability less than \( \frac{1}{2} \). Considering these remarks, the \( BPP \) may be regarded as the class of problems efficiently solvable on a classical computer and \( BQP \) as the class of problems efficiently solvable on a quantum computer. Both \( BQP \) and \( BPP \) are contained in \( PSPACE \), thus

\[
P \subseteq NP \subseteq PSPACE, \ P \subseteq BPP \subseteq PSPACE, \ P \subseteq BQP \subseteq PSPACE.
\] (6.1)

However, it is not clear what problems outside of \( P \) are also solved efficiently by quantum computers, namely which ones in \( NP \setminus P \) (if \( P \neq NP \)).

Finally, to evaluate the complexity associated to an algorithm, one considers the number of operations in it (regarding time), the longest sequential path in the circuit (more concretely), or the number of
qubits used (regarding space) and how they scale with the input, the size of the problem. One might
wonder that if an algorithm can be implemented by more than one circuit, the complexity obtained
might be different from circuit to circuit. However, if the algorithm is implemented by one circuit and it scales
polynomially in the size of the problem, all the others should also scale polynomially in the size of the
problem, otherwise the algorithm is not the same, i.e. something more is being done (if it scales at a
larger rate for some of the other circuits). The instructions on how to implement the corresponding cir-
cuit also form an algorithm, which given the problem size should return the circuit in polynomial time (on
the problem size), hence efficiently. This condition is called the uniformity condition and is important in
constructing the circuit. Thus, from a circuit implementing the algorithm, its complexity can be unequiv-
ocally determined, and such a uniform circuit is efficiently constructed. Concerning time complexity, one
looks at the length of the circuit, the longest path from the input to the output, counting the number of
elementary operations in it. These elementary operations can be taken to be two-qubit (or one-qubit)
gates, measurements and state preparations. The time to perform each operation was implicitly stated
as being the same, however regarding the time complexity this is not restrictive, since this value could
just be set to the maximum time that any of these elementary operation takes to be performed.

6.2 A simple example: Quantum teleportation

Consider the following circuit that basically passes a qubit from one wire to another. Consider also

the following scenario: Alice wishes to transmit the state of a qubit to Bob by only sending classical
information, moreover they share a resource, an EPR pair \( |00\rangle + \frac{1}{\sqrt{2}} |11\rangle \). The two bottom wires on the
circuit correspond to the EPR pair with the top one of those corresponding to Alice’s qubit and the
bottom one corresponding to Bob’s qubit. The top wire corresponds to the state to transmit. Hence, the
two top wires correspond to Alice’s system and the bottom wire corresponds to Bob’s system. Following
the history of the qubits, Alice interacts the state to transmit and the qubit which is her half of the EPR
pair and measures them. Then she sends the two classical bits resulting from the measurement’s result
to Bob, which in turn uses them to apply certain gates conditioned on the value of those bits in order to
obtain the state of interest. Let the state to be teleported be written as

\[
|\psi\rangle = \alpha |0\rangle + \beta |1\rangle,
\]

then

\[
|\psi\rangle |\beta_{00}\rangle = \frac{\alpha |00\rangle (|00\rangle + |11\rangle) + \beta |11\rangle (|00\rangle + |11\rangle)}{\sqrt{2}}.
\]

Applying

\[
H_1 \rightarrow \frac{1}{2} [\alpha (|0\rangle + |1\rangle)(|00\rangle + |11\rangle) + \beta (|0\rangle - |1\rangle)(|10\rangle + |01\rangle)]
\]

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

Clearly, by measuring the top two qubits four outcomes might happen, and it is easily seen that applying
\(Z^{m_1} X^{m_2}\) recovers the state \(|\psi\rangle\), where \(m_1\) and \(m_2\) are the outcomes of the measurement of the two

Figure 6.1: Quantum teleportation circuit. Source: [13].
top qubits (on the circuit). In fact, to show this, if the measurement were done at the end (principle of deferred measurement) one would obtain after the action of the conditioned gates used in the recovery

\[
\frac{1}{2} \left[ |00\rangle \left( \alpha |0\rangle + \beta |1\rangle \right) + |01\rangle X(\alpha |1\rangle + \beta |0\rangle) + |10\rangle Z(\alpha |0\rangle - \beta |1\rangle) + |11\rangle ZX(\alpha |1\rangle - \beta |0\rangle) \right]
\]

\[
= \frac{1}{2} \left[ |00\rangle + |01\rangle + |10\rangle + |11\rangle \right] \left( \alpha |0\rangle + \beta |1\rangle \right)
\]

so for each combination in the superposition of the two top qubits the bottom qubit is corrected becoming \(|\psi\rangle\) its state. If one was just considering the quantum circuit, and not the communication scenario, it could be said that the measurements are irrelevant since the end states become unentangled (state of interest \(|\alpha\rangle\)). Coming back to the communication scenario, it is seen that with a shared entangled pair (an e-bit) and sending two classical bits (two c-bits) a qubit can be teleported. This is an interesting circuit which can actually have practical use. Indeed, a similar design based on this one was already seen regarding Knill’s error correction.

### 6.3 Quantum Fourier transform

The quantum Fourier transform is the quantum analogue of the discrete Fourier transform. The discrete Fourier transform maps a vector representation, \(x(n)\), \(n = 0, \ldots, N-1\), into another vector representation \(y(k)\), \(k = 0, \ldots, N-1\) where \(y(k) = \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} x(n) e^{2\pi i nk/N}\). \(\omega_N = e^{2\pi i/N}\), with the corresponding change-of-basis matrix being

\[
F_N = \frac{1}{\sqrt{N}} \begin{bmatrix}
1 & 1 & 1 & 1 & \ldots & 1 \\
1 & \omega & \omega^2 & \omega^3 & \ldots & \omega^{N-1} \\
1 & \omega^2 & \omega^4 & \omega^6 & \ldots & \omega^{2(N-1)} \\
1 & \omega^3 & \omega^6 & \omega^9 & \ldots & \omega^{3(N-1)} \\
\vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\
1 & \omega^{N-1} & \omega^{2(N-1)} & \omega^{3(N-1)} & \ldots & \omega^{(N-1)(N-1)}
\end{bmatrix}, \quad \omega = \omega_N, \quad (6.4)
\]

so \(y = F_N x\). The matrix \(F_N\) is unitary. Let it be proven. The inner product between two of its columns results in

\[
\langle c_m | c_n \rangle = \frac{1}{N} \left( \sum_{l=0}^{N-1} \omega^{-lm} \omega^l \right) = \frac{1}{N} \left( \sum_{l=0}^{N-1} \left( \omega^{n-m} \right)^l \right) = \begin{cases} \frac{1}{N} & \frac{1}{N} = 1, \text{ for } n \neq m \\ \frac{1}{N} \sum_{l=0}^{N-1} \omega^{n-m} = 0, \text{ for } n = m \end{cases}. \quad (6.5)
\]

Hence, the columns form an orthonormal basis, thus the matrix is unitary and a quantum Fourier transform can be considered. The quantum Fourier transform takes the following action on the basis states: \(|j\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i jk/N} |k\rangle\). For an arbitrary state, \(\sum_{j=0}^{N-1} x_j |j\rangle \rightarrow \sum_{k=0}^{N-1} \left( \sum_{j=0}^{N-1} x_j e^{2\pi i jk/N} \right) |k\rangle = \sum_{k=0}^{N-1} y_k |k\rangle\). For \(N = 2\) the Fourier transform turns out to be the Hadamard transform. Take \(N = 2^n\) with \(n\) the number of qubits involved. Now, notice that

\[
|j\rangle \rightarrow \frac{1}{2^{n/2}} \sum_{k=0}^{2^n-1} e^{2\pi i jk/2^n} |k\rangle = \frac{1}{2^{n/2}} \sum_{k_1=0}^{1} \ldots \sum_{k_n=0}^{1} e^{2\pi i j(\sum_{i=1}^{n} k_i 2^{-i})} |k_1 \ldots k_n\rangle
\]

\[
= \frac{1}{2^{n/2}} \sum_{k_1=0}^{1} \ldots \sum_{k_n=0}^{1} e^{2\pi i jk_1 2^{-1}} |k_1\rangle = \frac{1}{2^{n/2}} \sum_{k_1=0}^{1} \ldots \sum_{k_n=0}^{1} e^{2\pi i jk_1 2^{-1}} \left( \sum_{l=1}^{n} e^{2\pi i jk_l 2^{-l}} |k_l\rangle \right)
\]

\[
= \left( |0\rangle + e^{2\pi i j_1} |1\rangle \right) \left( |0\rangle + e^{2\pi i j_2} |1\rangle \right) \ldots \left( |0\rangle + e^{2\pi i j_n} |1\rangle \right)
\]

\[
= \frac{1}{2^{n/2}} \left[ \left( |0\rangle + e^{2\pi i j_0} |1\rangle \right) \left( |0\rangle + e^{2\pi i j_1} |1\rangle \right) \ldots \left( |0\rangle + e^{2\pi i j_n} |1\rangle \right) \right]
\]
From this expansion an efficient circuit can be derived using the unitary transformation

\[ R_k \equiv \begin{bmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^k} \end{bmatrix}. \]  

(6.7)

To obtain a particular term \((0) + e^{2\pi i 0, j_{n-t+1} \ldots j_n} |1\rangle\) one applies \(R_1, R_2\) (controlled by \(j_{n-t+2}\)) and so on until \(R_t\) (controlled by \(j_n\)) to the qubit \(n-t+1\) corresponding to \(j_{n-t+1}\), since

\[ j = j_1 \ldots j_n = j_1 2^{n-1} + \ldots + j_n = \sum_{l=1}^n j_l 2^{n-l} \]

\(\rightarrow 0, j_{n-t+1} \ldots j_n = \left( \sum_{l=1}^n j_l 2^{n-l} \right) / 2^t - s = \sum_{l=n-t+1}^n j_l 2^{n-l-t} = \sum_{k=1}^t j_{n+k-t} 2^{-k}, \)

(6.8)

where \(s = \text{int}(\sum_{l=1}^n j_l 2^{n-l-t})\) and \(k = t + l - n\), making \(\angle R_k = 1/2^k = 1/2^t l - n\).

Hence, considering \(R_t \equiv H\) the circuit from figure 6.2 that implements the quantum Fourier transform is obtained. Notice that qubits are in the reverse order of the expression in (6.6), which can be fixed either by using swap operations explicitly to reach the correctly ordered state, or the following operations can be adopted so as to act in the proper manner leaving the order reversed. The circuit implementing

\[
|j_1\rangle \xrightarrow{H} |j_2\rangle \xrightarrow{R_1} \cdots \xrightarrow{R_{n-1}} |j_n\rangle \xrightarrow{R_n} |0\rangle + e^{2\pi i 0, j_{n-t+1} \ldots j_n} |1\rangle
\]

\[
|j_2\rangle \xrightarrow{H} \cdots \xrightarrow{R_{n-1}} |j_n\rangle \xrightarrow{H} |0\rangle + e^{2\pi i 0, j_{n-t} \ldots j_n} |1\rangle
\]

\[
|j_{n-1}\rangle \xrightarrow{H} \cdots \xrightarrow{R_{n-2}} |j_n\rangle \xrightarrow{H} |0\rangle + e^{2\pi i 0, j_{n-1} \ldots j_n} |1\rangle
\]

\[
|j_n\rangle \xrightarrow{H} |0\rangle + e^{2\pi i 0, j_{n} |1\rangle}
\]

Figure 6.2: Circuit implementing the quantum Fourier transform. Source: [13].

the inverse quantum Fourier transform \((F_N^\dagger)\) is the circuit obtained by reversing (applying operations in reverse order) the one implementing the quantum Fourier transform \((F_N)\), figure 6.2. With \(t\) ranging from 1 to \(n\) the number of gates necessary is \(\sum_{l=1}^n t = n(n + 1)/2\) in order to implement the circuit of figure 6.2 and if swaps are included, at most \(n/2\) of those are required, thus this algorithm to accomplish the quantum Fourier transform is \(\Theta(n^2)\). Although this is faster than the best classical algorithms computing the Fourier transform which are \(\Theta(n 2^n)\), the Fourier transform amplitudes cannot be directly accessed.

### 6.4 Reversible computation

To implement a non-invertible function \(f: \mathbb{Z}_m \to \mathbb{Z}_n\) \((\{0, 1\}^m \to \{0, 1\}^n)\) on a quantum computer, an invertible version of the function must be used. Let \(C_f\) be the classical circuit implementing \(f\), then using reversible components the same function can be implemented reversibly. Consider the Toffoli gate, with some ancilla bits/qubits, the classical/quantum reversible versions of binary gates required to implement any computation can be implemented. The NAND gate is a universal gate for classical computation, and since the Toffoli gate can be used to perform a NAND (using some ancilla bits; quantum case in figure 5.3), the Toffoli gate is a universal gate for classical computation, thus a reversible version of a non-invertible function’s circuit can be constructed using only Toffoli gates (and ancilla qubits, for the quantum Toffoli gate).

The first thing to note is that the input size and the output size of a reversible circuit must be equal. Thus, if \(f_{inv}: \mathbb{Z}_{m+a} \to \mathbb{Z}_{n+b}\) then \(m + a = n + b\) with \(a\) being the number of ancilla bits/qubits necessary to make the computation reversible and \(b\) being the number of garbage bits/qubits, the extra ones that
remain from the computation (and allow to reverse it). It is not desirable to have some garbage qubits in some irrelevant state to the desired computation. In order to "reset" them, take the inverse circuit of \( C_{f_{inv}} \), \( C_{f_{inv}}^{-1} \), by applying the Toffoli gates (which are their own inverse) on \( C_{f_{inv}} \) in reverse order. With such a circuit, a cleaner reversible circuit to obtain \( f \) is arrived at, figure 6.4. The ancilla qubits can thus be re-used and one can disregard them from the action of the computation on writing (for neatness) \( |x\rangle \langle y| \to |x\rangle \langle y \oplus f(x)| \).

To implement an invertible function \( f : \mathbb{Z}_n \to \mathbb{Z}_n \) a reversible circuit can also be constructed in these moulds acting like \( |x\rangle \langle y| \to |x\rangle \langle y \oplus f(x)| \) (by \( C_f \)) or \( |x\rangle \to |f(x)| \) (with the possible use of some ancilla qubits). The latter can be constructed from the former considering \( |x\rangle \langle 0| \to |x\rangle \langle f(x)| \) and \( |f(x)| \langle x| \to |f(x)| \langle f^{-1}(f(x))| = |f(x)| \langle 0| \) for a circuit acting like \( |x\rangle \langle y| \to |x\rangle \langle y \oplus f^{-1}(x)| \) (\( C_f^{-1} \), computing \( f^{-1} \) in the previous moulds). The overall circuit is presented in figure 6.5, where the gates with X’s at their extremities are SWAP gates (they simply swap the qubits); an implementation is presented in figure 6.6. On the referred moulds, the increase in amount of gates in comparison to the original circuit \( C \) is linear on the original amount, since every non-reversible gate can be implemented with a number of reversible gates that is constant and two circuits of the same size, \( C_{f_{inv}} \) and \( C_{f_{inv}}^{-1} \), are used, thus making the amount of gates double; also there are the CNOT’s used to copy the result, which are of the size of the output of the original circuit in number (can be regarded as a constant depending on that size).
6.5 Phase estimation

Consider a unitary operator \( U \) with eigenvector \(|u\rangle\) and associated eigenvalue \( e^{2\pi i \phi} \). The goal of phase estimation is to estimate the phase \( \phi \). For achieving this, assume that the controlled-\( U^{2^t} \) can be performed by a black box (an oracle), also assume that one is able to prepare \(|u\rangle\) (how to do this will depend on the particular \( U \); concrete examples will be shown later). To perform this take the circuit of figure 6.7. Let it be explained.

\[
|0\rangle \otimes |u\rangle \xrightarrow{H} \frac{1}{\sqrt{2^t}} \sum_{k=0}^{2^t-1} |k\rangle |u\rangle \xrightarrow{U^k} \frac{1}{\sqrt{2^t}} \sum_{k=0}^{2^t-1} |k\rangle U^k |u\rangle = \frac{1}{\sqrt{2^t}} \sum_{k=0}^{2^t-1} e^{2\pi i k \phi} |k\rangle |u\rangle \quad (6.9)
\]

After the application of the inverse Fourier transform one has \( \frac{1}{2^t} \sum_{k,l=0}^{2^t-1} \sum_{k=0}^{2^t-1} e^{2\pi i k (\phi - \frac{l}{2^t})} |l\rangle\) (disregarding \(|u\rangle\), since they are in a tensor product state). If \( \phi = \frac{l'}{2^t} \) for some integer \( l' \) then the state results in \(|l'\rangle\) and the phase is obtained with certainty. However, if that is not the case the state is written as

\[
\frac{1}{2^t} \sum_{l=0}^{2^t-1} \left( \sum_{k=0}^{2^t-1} e^{2\pi i k \left(\phi - \frac{l'}{2^t}\right)} \right) |l\rangle = \frac{1}{2^t} \sum_{l=0}^{2^t-1} \frac{1 - e^{2\pi i \left(2^t \phi - l\right)}}{1 - e^{2\pi i \left(\phi - \frac{l'}{2^t}\right)}} |l\rangle = \sum_{l=0}^{2^t-1} \alpha_l |l\rangle
\]

\[
\alpha_l = \frac{1}{2^t} \frac{1 - e^{2\pi i (l' - l + 2^t \epsilon)}}{1 - e^{2\pi i (\frac{l'}{2^t} + \epsilon)}} \quad (6.10)
\]
letting $\phi = \frac{r}{2^t} + \epsilon$ with $|\epsilon| \leq 1/2^{t+1}$ for $\frac{r}{2^t}$ is the closest fraction (of this form) to $\phi$. The probability that the measurement outcome is outside a certain distance from the best estimate is written as

$$p(|m - l'| > \epsilon) = \sum_{-2^{t-1} \leq l - l' \leq -(e+1)} |\alpha_l|^2 + \sum_{e+1 \leq l - l' \leq 2^{t-1}} |\alpha_l|^2,$$

and because $|\theta|/|1 - e^{i\theta}| \leq \pi/2$ for $-\pi \leq \theta \leq \pi$ (check figure 6.8) and $|1 - e^{i\theta}| \leq 2$, the following is obtained:

$$p(|m - l'| > \epsilon) \leq \frac{1}{4} \left[ \sum_{j=0}^{-(e+1)} \left( \frac{1}{l - 2^t \epsilon} \right)^2 + \sum_{l=0}^{2^t-1} \left( \frac{1}{l - 2^t \epsilon} \right)^2 \right] + \frac{1}{4} \left[ \sum_{j=0}^{-(e+1)} \left( \frac{1}{l + \frac{1}{2}} \right)^2 + \sum_{l=0}^{2^t-1} \left( \frac{1}{l + \frac{1}{2}} \right)^2 \right] \leq \frac{1}{2} \int_{\epsilon}^{2^{t-1}} \frac{dl}{(l + \frac{1}{2})^2} \leq \frac{1}{2(e - 1/2)} \tag{6.12}
$$

where $\tilde{l} = l' - l$ and noting that $|2^t \epsilon| \leq 1/2$. If it is desired to approximate $\phi$ to an accuracy $2^{-n}$, then making $\frac{\epsilon}{2^t} = 2^{-n}$ achieves it fixing the value $\epsilon = 2^{t-n} - 1$ for $\epsilon$. Using $t = n + p$ qubits, one sees that

$$p(|m - l'| > \epsilon) \leq \frac{1}{2} \left[ \sum_{j=0}^{-(e+1)} \left( \frac{1}{l - 2^t \epsilon} \right)^2 + \sum_{l=0}^{2^t-1} \left( \frac{1}{l - 2^t \epsilon} \right)^2 \right] \leq \frac{1}{2} \int_{\epsilon}^{2^{t-1}} \frac{dl}{(l + \frac{1}{2})^2} \leq \frac{1}{2(e - 1/2)} \tag{6.12}
$$

the probability of obtaining an approximation correct to this accuracy is at least $1 - 1/2(2^p - 3/2)$, so if one wishes a probability of success of at least $1 - \epsilon$ regarding the referred accuracy, then

$$1 - 1/2(2^p - 3/2) \geq 1 - \epsilon \Leftrightarrow p \geq \log \left( \frac{3}{2} + \frac{1}{2\epsilon} \right) \Rightarrow t = n + \left\lceil \log \left( \frac{3}{2} + \frac{1}{2\epsilon} \right) \right\rceil \tag{6.13}
$$

fixing $t$. Following this line of reasoning it is also possible to find that $p_t \geq \frac{1}{\sqrt{p}}$, which is a lower bound for the probability of getting the best estimate to $t$ qubits of precision, and from it one sees that the referred probability has an agreeable value.

### 6.6 Order-finding, factoring and discrete logarithm

The order-finding problem consists on determining the order of a positive integer $x$ modulo $N$, which is defined to be the least positive integer, $r$, satisfying $x^r = 1$ (mod $N$). A quantum algorithm for order-finding is going to be constructed from phase estimation. For this particular case, $U$ is such that $U |y⟩ = |xy(x(y) N)⟩$ for $0 \leq y \leq N - 1$ and $U |y⟩ = |y⟩$ for $N \leq y \leq 2L$, where $L \equiv \lceil \log(N) \rceil$. Concerning its eigenvectors, note that any vector of the form $|u_s⟩ \equiv \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \omega_r^{-sk} |x^k \text{mod } N⟩$ for $0 \leq s \leq r - 1$ is an eigenvector of $U$ with eigenvalue given by

$$U |u_s⟩ = \sum_{k=0}^{r-1} \omega_r^{-sk} |x^{k+1} \text{mod } N⟩ = \omega_r^s |u_s⟩ \Rightarrow \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |u_s⟩ = \frac{1}{r} \sum_{k=0}^{r-1} \left( \sum_{s=0}^{r-1} \omega_r^{-sk} \right) |x^k \text{mod } N⟩ = |1⟩ \tag{6.14}$$
and it can be seen that the superposition of this eigenstates is an easy to prepare state, not depending
on $r$. Thus, initializing $|u\rangle = |1\rangle$, the phase estimation algorithm can be performed to find the order $r$, since the controlled-$U^{2^j}$ can be efficiently performed by a procedure known as modular exponentiation, with the sequence of these operations used in the algorithm requiring $O(L^3)$ gates. From the phase estimation, it is obtained with high probability one of the closest approximations to one of the $s/r$ resulting states. To find $r$, the use of the continued fractions algorithm yields $x$ and $y$ where $x/y$ is the closest to $\phi$. If in the phase estimation one makes $t = 2L + 1 + \left\lceil \log \left( \frac{3}{2} + \frac{1}{x} \right) \right\rceil$, then the phase obtained $\phi \approx s/r$ is accurate to $2L + 1$ with probability at least $(1 - \epsilon)/r$, therefore if this accuracy is obtained $|s/r - \phi| \leq 2^{1-2L-1} = 1/2r^2$ holds, since $r \leq N \leq 2^L$. In this case, the continued fraction for $\phi$ is assured to converge to $s/r$ in $O(L^3)$ operations, and assuming $s/r$ is irreducible one obtains $s$ and $r$. If $s/r$ is reducible, then only a factor of $r$ and a factor of $s$ are obtained, and from the continued fractions algorithm one obtains $s'$ and $r'$ forming an irreducible fraction which satisfies $s'/r' = s/r$. Then by repeating it, the factors obtained can be used to infer the value of $r$, or it is possible that for some repetition $s$ is co-prime with $r$, and consequently one obtains $r$ directly. The runtime of the order-finding algorithm is $O(L^3)$ (dominated by the execution of the controlled-$U^{2^j}$'s) succeeding with probability $O(1)$. Factoring can be reduced to order-finding, thus solving efficiently order-finding implies solving efficiently factoring. Take the following theorems

**Theorem 6.6.1.** Suppose $N$ is an $L$ bit composite number, and $x$ is a non-trivial solution to the equation $x^2 = 1\pmod{N}$ in the range $1 \leq x \leq N$ ($x \neq \pm 1\pmod{N}$). Then, at least one of $\gcd(x - 1, N)$ and $\gcd(x + 1, N)$ is a non-trivial factor of $N$ that can be computed in $O(L^3)$ operations.

**Theorem 6.6.2.** Suppose $N = p_1^{a_1} \cdots p_m^{a_m}$ is the prime factorization of an odd composite positive integer. Let $x$ be an integer chosen uniformly at random, subject to the requirements that $1 \leq x \leq N - 1$ and $x$ is co-prime to $N$. Let $r$ be the order of $x$ modulo $N$. Then

$$p(r \text{ is even and } x^{r/2} \neq -1\pmod{N}) \geq 1 - \frac{1}{2^{n-1}}.$$  \hspace{1cm} (6.15)

Using these theorems a factoring algorithm can be developed:

1. If $N$ is even, return the factor 2. [Classic]
2. Determine whether $N = a^b$ for integers $a \geq 1$ and $b \geq 2$, and if so return the factor $a$. [Classic]
3. Randomly choose $x$ in the range 1 to $N - 1$. If $\gcd(x, N) > 1$ then return the factor $\gcd(x, N)$. [Classic]
4. Use the order-finding subroutine to find the order $r$ of $x$ modulo $N$. [Quantum]
5. If $r$ is even and $x^{r/2} \neq -1\pmod{N})$ then compute $\gcd(x^{r/2} - 1, N)$ and $\gcd(x^{r/2} + 1, N)$, and test to see if one of these is a non-trivial factor, returning that factor if so. Otherwise, the algorithm fails. [Classic]

This algorithm requires $O(L^3)$ operations and succeeds with probability $O(1)$, returning a non-trivial factor of $N$. Repeating the algorithm, a complete prime factorization of $N$ can be found. All the classical steps referred in the algorithm can be efficiently implemented on a classical computer, thus the real advantage is acquired in step 4, where there is no known efficient classical procedure to perform it. The algorithm achieves an exponential improvement compared to classical ones solving the factoring problem, therefore it is much more efficient.

The discrete logarithm problem consists in finding $s$ such that $b = a^s\pmod{N}$ given $a$ and $b$. This is an important problem in cryptography since public-key cryptography’s security relies on the hardness
of this problem (likewise regarding factoring). To contradict the algorithm to solve this problem consider the function \( f(x_1, x_2) = b^{x_1}a^{x_2} \) performed by the quantum black box \( U \) as \( U |x_1\rangle |x_2\rangle |y\rangle \rightarrow |x_1\rangle |x_2\rangle |y \oplus f(x_1, x_2)\rangle \). The algorithm is as follows. The registers are initialized as \(|0\rangle |0\rangle |0\rangle \), from there the superposition state \( \frac{1}{\sqrt{r}} \sum_{x_1=0}^{2^r-1} \sum_{x_2=0}^{2^l-1} |x_1\rangle |x_2\rangle |y\rangle \) is created applying Hadamard gates on the first two registers. \( U \) is then applied to that state resulting in the state \( \frac{1}{\sqrt{r}} \sum_{x_1=0}^{2^r-1} \sum_{x_2=0}^{2^l-1} |x_1\rangle |x_2\rangle |y \oplus f(x_1, x_2)\rangle \). Now, note that for a particular value of function \( f \), \( a^{x_0} \), the \( x_1 \) and \( x_2 \) associated are the ones that satisfy \( sx_1 + x_2 = x_0 ( \text{mod} \ r ) \) \( (r \text{ is the order of } a) \), then let the following states be defined.

\[
|\tilde{f}\rangle = \frac{1}{\sqrt{r}} \sum_{x_0=0}^{r-1} e^{-2\pi i x_0 / r} |a^{x_0}\rangle, \quad l = 0, \ldots, r - 1
\]  

(6.16)

It turns out that the state \(|f(x_1, x_2)\rangle\) can be written as \(|f(x_1, x_2)\rangle = a^{sx_1+x_2} \rangle = \frac{1}{\sqrt{r}} \sum_{l=0}^{r-1} e^{2\pi i (sx_1+x_2)/r} |\tilde{f}\rangle\), thus

\[
\frac{1}{2^l} \sum_{x_1=0}^{2^l-1} \sum_{x_2=0}^{2^l-1} |x_1\rangle |x_2\rangle |f(x_1, x_2)\rangle = \frac{1}{2^l} \sqrt{r} \sum_{x_1=0}^{2^l-1} \sum_{x_2=0}^{2^l-1} e^{2\pi i (sx_1+x_2)/r} |x_1\rangle |x_2\rangle |\tilde{f}\rangle
\]

\[
= \frac{1}{2^l r} \sum_{x_1=0}^{2^l-1} \left( \sum_{x_2=0}^{2^l-1} e^{2\pi i l x_1 / r} |x_1\rangle \right) \left( \sum_{x_2=0}^{2^l-1} e^{2\pi i l x_2 / r} |x_2\rangle \right) |\tilde{f}\rangle
\]  

(6.17)

Applying the inverse Fourier transform to the first two registers yields the state \( \frac{1}{\sqrt{r}} \sum_{l=0}^{r-1} \sum_{s=0}^{r-1} |ls/r\rangle |\tilde{f}\rangle |\tilde{f}\rangle\) and by measuring it one obtains the estimates for \( ls/r \) and \( l/r \) from which \( s \) is estimated. For the first two registers \( t = O(\lfloor \log r \rfloor + \log 1/\epsilon) \). Regarding runtime, the algorithm uses \( U \) once and \( O(\lfloor \log r \rfloor^2) \) operations. It succeeds with probability \( O(1) \).

All of these section’s problems are specific problems which fall into a more general problem, the finite Abelian hidden subgroup problem. Its definition is as follows:

Let \( G \) be a finite Abelian group and \( f \) a function from \( G \) to a finite set \( X \), which is constant on the cosets of a subgroup \( H < G \), and different between each coset of \( H \). Determine a generating set for \( H \).

The quantum Fourier transform exploits this characteristic of function \( f \) to aid in solving the problem efficiently for some of the instances of the general problem discussed above.

### 6.7 Quantum search: Grover’s algorithm

The purpose of Grover’s algorithm is to find an element on an unstructured search space of \( N \) elements that satisfies some condition (e.g. \( f(x) = 1 \) for some element \( x \)), doing so in \( O(\sqrt{N}) \) operations, thus introducing an improvement compared to classical algorithms for this same problem (that require \( O(N) \) operations). It is an impressive speedup, but perhaps not impressive enough, however it is the best that can be done in these terms, i.e. Grover’s algorithm is optimal for this type of problem. Formally defining the problem, an element \( x \) is a solution to the problem if it satisfies the solution condition, which will be checked by \( f : \mathbb{Z}_n \rightarrow \{0, 1\} \), being \( f(x) = 1 \) if \( x \) is a solution and being \( f(x) = 0 \) if \( x \) is not a solution. Grover’s algorithm solves this problem without any further assumptions, hence all it can exploit is in the definition of this problem. Let the quantum black box implementing \( f \) (the oracle) be \( U \) acting as \( U |x\rangle |y\rangle = |x\rangle |y \oplus f(x)\rangle \). The desired action on \( x \) by \( U \) is going to be \( |x\rangle \rightarrow (-1)^{f(x)} |x\rangle \) which can be achieved by choosing \( |y\rangle = H |1\rangle = |\rangle \). The initial state for the input is \(|0\rangle\), which will be transformed into a superposition of all \( N \) (the search space can be extended in order to be a power of 2) binary
The transformation matrix is given by

\[
\frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle = \sqrt{\frac{N-M}{N}} |\alpha\rangle + \sqrt{\frac{M}{N}} |\beta\rangle , \quad |\alpha\rangle \equiv \frac{1}{\sqrt{N-M}} \sum_{x : f(x) = 0} |x\rangle , \quad |\beta\rangle \equiv \frac{1}{\sqrt{M}} \sum_{x : f(x) = 1} |x\rangle , \quad (6.18)
\]

where \( M \) is the number of solutions. Grover’s algorithm action will be to rotate \( |\psi\rangle \) in the two-dimensional space spanned by \( |\alpha\rangle \) and \( |\beta\rangle \) until \( |\psi\rangle \approx |\beta\rangle \), and so measuring the state will yield one (if any exists) of the solutions with high probability. How this rotation is made is going to be explained. First note that

\[
|\psi\rangle \approx (2 \cos (\theta/2) - \sin (\theta/2)) |\alpha\rangle + (2 \sin (\theta/2) - \sin (\theta/2)) |\beta\rangle \quad (6.20)
\]

This translates into the matrix

\[
G = \left[ \begin{array}{cc} \frac{N-M}{N} - \frac{M}{N} & -2 \sqrt{\frac{N-M}{N}} \sqrt{\frac{M}{N}} \\ -2 \sqrt{\frac{N-M}{N}} \sqrt{\frac{M}{N}} & (2 \frac{M}{N} - 1) \end{array} \right]
\]

\[
= \left[ \begin{array}{cc} \cos^2 (\theta/2) - \sin^2 (\theta/2) & -2 \cos (\theta/2) \sin (\theta/2) \\ 2 \cos (\theta/2) \sin (\theta/2) & \cos^2 (\theta/2) - \sin^2 (\theta/2) \end{array} \right]. \quad (6.21)
\]

Thus, a Grover iteration rotates the vector by an angle \( \theta \). It is also easy to see that the reflection about

![Figure 6.9: Representation of the action of a single Grover iteration on |\psi\rangle, with the referred reflection axes highlighted in blue. Adapted from: [13.](image)](image)
$|\beta\rangle$ followed by the reflection about $|\psi\rangle$ is be equivalent to a rotation by the double of the angle between the reflection axis, since the product of two reflections is a rotation by the double of the angle between the reflection axis (figure 6.9). So, from $|\psi\rangle = \cos \theta/2 |\alpha\rangle + \sin \theta/2 |\beta\rangle$, after $k$ Grover iterations (circuit implementing one Grover iteration presented in figure 6.10) one has

$$G^k |\psi\rangle = \cos \left(\frac{2k+1}{2} \theta\right) |\alpha\rangle + \sin \left(\frac{2k+1}{2} \theta\right) |\beta\rangle$$  \hspace{1cm} (6.22)

and in order to get $|\psi\rangle \approx |\beta\rangle$, one must have $\sin \left(\frac{2k+1}{2} \theta\right) \approx 1$, and so $\frac{2k+1}{2} \theta \approx \pi/2$ which translates into $k \approx \pi/2 \theta - 1/2$ and since $\theta/2 \geq (\sin \theta/2) = \sqrt{M/N}$ one has $k \leq \left\lceil \frac{\pi}{4} \sqrt{N/M} \right\rceil$, so $O(\sqrt{N/M})$ Grover iterations must be performed in order to obtain the solution with high probability (a classic algorithm would require $O(N/M)$ calls to the oracle). For small $\theta$ (few solutions in the search space) $\theta/2 \approx \sin (\theta/2)$, thus this bound is close to the number of iterations $k$ leading to solutions with high probability, however it depends on $M$, the number of solutions to the problem, hence with a good estimate of $M$ a good estimate of $\pi/2 \theta - 1/2$ can be obtained. An estimate of $M$ can be obtained by applying phase estimation to the transformation $G$, since two of its eigenvectors are in the space spanned by $|\alpha\rangle$ and $|\beta\rangle$ and their corresponding eigenvalues are $e^{i\theta}$ and $e^{i(2\pi-\theta)}$, therefore $\theta$ can be estimated (and from it $M$).

To bound the error on the estimate consider the parameters for the phase estimation algorithm with the first register having $t \equiv m + \left\lceil \log \left(\frac{1}{2} + \frac{1}{2^n}\right) \right\rceil$ qubits and the second register $n$ qubits. From it one obtains an estimate of $\theta$ or $2\pi - \theta$, since $|\psi\rangle = \sum_x |x\rangle / \sqrt{N}$ is a superposition of its corresponding eigenvectors, accurate to within $|\Delta \theta| \leq 2^{-m}$, with probability at least $1 - \epsilon$. Let $\Delta M$ be bounded.

$$\frac{|\Delta M|}{N} = \left| \sin^2 \left(\frac{\theta + \Delta \theta}{2}\right) - \sin^2 \left(\frac{\theta}{2}\right) \right|$$

$$= \left| \sin \left(\frac{\theta + \Delta \theta}{2}\right) + \sin \left(\frac{\theta + \Delta \theta}{2}\right) \right| \sin \left(\frac{\theta + \Delta \theta}{2}\right) - \sin \left(\frac{\theta}{2}\right) \right|$$

and since $|\sin ((\theta + \Delta \theta)/2) - \sin (\theta/2)| \leq |\Delta \theta|/2$ and $|\sin ((\theta + \Delta \theta)/2)| < \sin ((\theta/2) + |\Delta \theta|/2$, it is true that

$$\frac{|\Delta M|}{N} < \left(2 \sin (\theta/2) + \frac{|\Delta \theta|}{2}\right) \frac{|\Delta \theta|}{2} \rightarrow |\Delta M| < \left(\sqrt{MN} + \frac{N}{2^{m+2}}\right) 2^{-m},$$

considering $\sin^2 \theta/2 = M/N$ and $|\Delta \theta| \leq 2^{-m}$. So, one can specify the parameters in order to have a good estimate of $M$ with high probability, $1 - \epsilon$, according to (6.24). Moreover, it can efficiently determine if $M = 0$ or $M \neq 0$, if for example it is chosen $m = \lceil n/2 \rceil$ then $|\Delta M| < 1/4$ when $M = 0$, thus with probability $1 - \epsilon$ the value estimated for $M$ is 0. Of course, one can just consider $|\Delta \theta|$ and use $k = \pi/2 \theta - 1/2$. Grover’s algorithm is useful for a problem with a search space with few solutions, since

![Figure 6.10: Circuit implementing a Grover iteration. Source: [13].](image-url)
for problems with more than a few, one can randomly pick items from the search space until a solution is found after just a few trials, on average. The search space can be expanded by doubling the search space, obtaining \( 2^N \) elements with the new \( f \) having a new input bit which if it has value 0, then the element is not a solution (corresponds to the \( N \) "fake" elements added) and if it has value 1 then it might be or not, depending on the rest of the string (which is evaluated as before by \( f \)).

### 6.8 HHL: A quantum algorithm for linear systems of equations

Consider the problem of solving a system of linear equations, and let that system be written as \( A\vec{x} = \vec{b} \) for a matrix \( A \), a vector of unknowns \( \vec{x} \), and a vector \( \vec{b} \). For an invertible matrix \( A \), the solution to this problem is \( \vec{x} = A^{-1}\vec{b} \). The problem of interest is analogous, taking \( \vec{x} \) and \( \vec{b} \) and renormalizing them results in the states \( |x\rangle = \frac{\sum_i x_i |i\rangle}{\|\sum_i x_i |i\rangle\|} \) and \( |b\rangle = \frac{\sum_i b_i |i\rangle}{\|\sum_i b_i |i\rangle\|} \). For such vectors, the system of equations represented by \( A |x\rangle = |b\rangle \), where \( A \) is a Hermitian matrix, is to be solved. For an invertible matrix \( A \), the solution to this problem is \( |x\rangle = A^{-1} |b\rangle \). Given that \( A \) is Hermitian (non-Hermitian case discussed later), it can be written as \( A = \sum_i \lambda_i |u_i\rangle \langle u_i| \) (by the spectral decomposition theorem), and its inverse as \( A^{-1} = \sum_i \lambda_i^{-1} |u_i\rangle \langle u_i| \). The first step to perform the inversion is to obtain the eigenvalues, which can be done with the phase estimation procedure. The eigenvalues are then inverted using an iterative method and applied using a rotation on an ancilla qubit.

Consider that \( |b\rangle \) can be efficiently prepared (with time complexity absorbed by the remaining of the operations on the algorithm), and let the initial state of interest be (the rest of it is in a tensor-product basis. Applying the phase estimation procedure using the matrix \( U = e^{i\lambda t} = \sum_i e^{i\lambda_i t} |u_i\rangle \langle u_i| \) (by matrix exponentiation), one obtains the state \( \sum_j \beta_j |\lambda_j\rangle |u_j\rangle \). To invert the eigenvalues, one might use an iteration method such as Newton iteration as in [20] to approximate \( v^{-1} \) (for an input \( v \)). That way the state becomes \( \sum_j \beta_j |\lambda_j^{-1}\rangle |u_j\rangle \). For the controlled rotation, it is necessary to calculate \( \arcsin C/\lambda_j \), hence the function \( \arcsin C/v \) (for an input \( v \) and a constant \( C \)) must be approximated, which can be done using iterative methods as in [21] (this can be done on a classical computer efficiently, so, using reversible computation it can also be done efficiently on a quantum computer), for example. Therefore, the angle \( \theta_j = \arcsin C/\lambda_j \) can be estimated and used to perform the following rotation,

\[
R_y(2\theta) = e^{-i\theta Y} = \begin{bmatrix} 1 - \sin^2 \theta & -\sin \theta \\ \sin \theta & 1 - \sin^2 \theta \end{bmatrix}
\]

which considering \( \theta = \sum_{k=1}^{\ell} k \theta 2^{-k}, \ k \theta \in \{0, 1\} \) leads to the decomposition

\[
R_y(2\theta) = e^{-iY \sum_{k=1}^{\ell} k \theta 2^{-k}} = \prod_{k=1}^{\ell} R_y^{(\theta)}(2^{1-k}),
\]

which can be implemented by the circuit in figure 5.11. The constant \( C \) satisfies \( C \leq \min_j |\lambda_j| = O(1/\kappa) \) (where \( \kappa \) is defined later). The probability of obtaining outcome 1 from the measurement of the ancilla qubit can be increased using amplitude amplification (generalization of the idea behind Grover’s algorithm). Before this measurement, one usually uncomputes (does the inverse of the computation, thus obtaining the initial state of the register and unentangling the register from the rest of the qubits) the registers that do not correspond to the result.

Obtained the outcome 1 from the measurement of the ancilla and uncomputing the remaining registers except the one corresponding to the input \( |b\rangle \) yields \( \sum_j \beta_j |u_j\rangle \approx |x\rangle \). In figure 6.12 the algorithm is summarized in the form of a circuit (with the redefined rotation on the figure corresponding to the one in figure 5.11), the factor of 2 was absorbed for aesthetic reasons), and where \( PE \) corresponds to

72
the phase estimation procedure, $U_\lambda$ to the subroutine computing $|\tilde{\theta}_j\rangle$ from $|\lambda_j\rangle$ and $U^\dagger$ represents the uncomputation of the registers L, C and the ancillary register (doing the inverse of all the operations before the controlled $R_y$ rotation).

Some important details that were somewhat ignored during the algorithm’s presentation must be discussed. One important factor in the performance of the matrix inversion is the condition number of matrix $A$, $\kappa$ ($\kappa = \frac{\max \sigma_j}{\min \sigma_j}$, where $\sigma_j$ is a singular value of $A$, which for normal matrices, as is a Hermitian matrix, coincides with the ratio $\frac{\max \lambda_j}{\min \lambda_j}$). Without loss of generality, one can take the singular values of $A$ to lie between $1/\kappa$ and 1 (rescaling $A$); equivalently $\kappa^{-2}I \leq A^\dagger A \leq I$. If $\kappa$ is large, then the matrix is closer to being singular (with $\kappa = \infty$ meaning it is singular). In the case of the matrix being singular there are two cases for the system of equations: or $|b\rangle$ contains components corresponding to eigenvectors of null eigenvalues, in which case there is no solution $|x\rangle$ (since if $|u_0\rangle$ is associated to a null eigenvalue and it is tried on $|x\rangle$, then that component disappears, $Ax_0 |u_0\rangle = 0 |u_0\rangle \langle u_0|u_0\rangle x_0 = 0$), or it does not, in which case there many possible solutions (and $|x\rangle$ can be expressed in terms of the eigenvectors of $A$ corresponding to non-null eigenvalues) due to the possibility of adding components corresponding to eigenvectors of the null eigenspace of $A$ to a particular solution ($A(|u_0\rangle + |x\rangle) = 0 + |b\rangle = |b\rangle$). Thus, in the second case, the algorithm presented can invert the matrix and give the unique solution that is composed only of eigenvectors of the non-null eigenspace of $A$.

A matrix $A$ with a large condition number is said to be ill-conditioned, and its inversion is more susceptible to errors (since for a small $\lambda$, small variations in it cause great variations in $1/\lambda$). In such a case, it might be of interest only to invert the well-conditioned part of the matrix. It can be considered that

---

Figure 6.11: Circuit implementing the controlled rotation $R_y(2\theta)$. Adapted from: [20].

Figure 6.12: Quantum circuit (before measurement of the top ancilla) for solving the linear system $A\vec{x} = \vec{b}$. Adapted from: [20].
the ill-conditioned part of the matrix is the subspace spanned by the eigenvectors whose corresponding eigenvalues are \( \lambda < 1/\kappa \). Thus, the inversion of \( \lambda \) could be done considering its well-conditioned and ill-conditioned part (just inverting the well-conditioned one) using filter functions \( f(\lambda) \) and \( g(\lambda) \) such that \( f^2(\lambda) + g^2(\lambda) \leq 1 \) and the controlled rotation defined as

\[
|h(\lambda)| \equiv \sqrt{1 - f^2(\lambda) - g^2(\lambda)} \, |\text{nothing}| + f(\lambda) \, |\text{well}| + g(\lambda) \, |\text{ill}| ,
\]  

(6.27)

satisfying \( f(\lambda) = 1/C_0 \lambda \) for \( \lambda \geq 1/\kappa \) and \( g(\lambda) = 1/C_0 \lambda \) for \( \lambda \leq 1/\kappa' \equiv 1/2\kappa \) (this constant \( C \) is such that \( C > 1 \)). The ‘nothing’ corresponds to no inversion taking place, the ‘well’ means it has, and the ‘ill’ indicates the part of \( |\beta| \) in the ill-conditioned subspace of \( A \). For a better numerical stability, an interpolating behaviour is of interest, thus considering \( 1/\kappa' \leq \lambda \leq 1/\kappa \) for some \( \kappa' \) (chosen here to be \( \kappa' = 2\kappa \)) as the range of eigenvalues considered in the interpolation one can choose for filter functions

\[
f(\lambda) = \begin{cases} 
\frac{1}{2\kappa'\lambda}, & \text{for } \lambda \geq 1/\kappa \\
\frac{1}{2} \sin \left( \frac{\pi - \lambda}{2} - \frac{\pi}{2\kappa} \right), & \text{for } 1/\kappa > \lambda \geq 1/\kappa' \\
0, & \text{for } 1/\kappa' > \lambda 
\end{cases},
\]

\[
g(\lambda) = \begin{cases} 
0, & \text{for } \lambda \geq 1/\kappa \\
\frac{1}{2} \cos \left( \frac{\pi - \lambda}{2} - \frac{\pi}{2\kappa' \lambda} \right), & \text{for } 1/\kappa > \lambda \geq 1/\kappa', \\
\frac{1}{2}, & \text{for } 1/\kappa' > \lambda 
\end{cases}
\]

(6.28)

for example. To improve the probability of obtaining \( |\text{well}| \), amplitude amplification can be performed with \( R_{\text{succ}} = I - 2 |\text{well}\rangle \langle \text{well}| \) and \( R_{\text{init}} = I - 2 |\text{initial}\rangle \langle \text{initial}| \) and using \( U_{\text{inv}}B R_{\text{init}}B^\dagger U_{\text{inv}}^\dagger R_{\text{succ}} \) applied in each iteration, for an initial state \( U_{\text{inv}}B |\text{initial}\rangle \) (where \( B \) produces the state \( |b\rangle \) when applied to \( |\text{initial}\rangle \)), and \( U_{\text{inv}} \) is the transformation represented by the circuit in 5.12 but with this type of controlled rotation).

Now, consider that \( A \) is an \( M \times N \) complex matrix and the cases where \( M \geq N \) and \( M \leq N \). Consider first the case \( M \leq N \). \( A \) can be written as

\[
A = \sum_{j=1}^{M} \sigma_j |u_j\rangle \langle v_j| \tag{6.29}
\]

in terms of its singular value decomposition. Define now the matrix

\[
H = \begin{bmatrix} 0 & A \\ A^\dagger & 0 \end{bmatrix},
\]

(6.30)

which is Hermitian. Its eigenvalues are \( \pm \sigma_1, \ldots, \pm \sigma_M \) (and \( N - M \) zero eigenvalues, corresponding to the orthogonal complement of \( V = \text{span}\{|u_1\}, \ldots, |u_M\rangle\} \), and the corresponding eigenvectors are \( |w_j^+\rangle \equiv (|0\rangle |u_j\rangle \pm |1\rangle |v_j\rangle)/\sqrt{2} \). Therefore, using \( |0\rangle |b\rangle \) as input and \( H \) as the matrix to invert and noting \( |0\rangle |b\rangle \) can be written as

\[
|0\rangle |b\rangle = \sum_{j=1}^{M} \beta_j \frac{1}{\sqrt{2}} (|w_j^+\rangle + |w_j^-\rangle),
\]

(6.31)

then

\[
H^{-1} |0\rangle |\beta\rangle = \sum_{j=1}^{M} \beta_j \sigma_j^{-1} \frac{1}{\sqrt{2}} (|w_j^+\rangle - |w_j^-\rangle) = \sum_{j=1}^{M} \beta_j \sigma_j^{-1} |1\rangle |v_j\rangle = |1\rangle |x\rangle.
\]

(6.32)

For the case where \( M \geq N \), consider \( U = \text{span}\{|u_1\}, \ldots, |u_N\rangle\} \). The equation \( A |x\rangle = |b\rangle \) is satisfiable only if \( |b\rangle \in U \). If \( |b\rangle \in U \), then applying \( H^{-1} \) to \( |0\rangle |b\rangle \) will return a valid solution. However if \( |b\rangle \) has some component in \( U^\perp \), then \( |0\rangle |b\rangle \) will have some component in the zero eigenspace of \( H \), which will be flagged as ill-conditioned by the algorithm, and only the part corresponding to the components in \( U \) is inverted, that is \( |x\rangle = \sum_{j=1}^{N} \beta_j \sigma_j^{-1} |u_j\rangle \) (only the projection of \( |b\rangle \) onto the non-null eigenspace of \( A, U \), is obtained from \( |x\rangle, A |x\rangle = (\sum_{j=1}^{N} |u_j\rangle \langle u_j|) |b\rangle \).
The portion of the algorithm more time consuming is the phase estimation procedure. In the original paper [22], phase estimation is performed using Hamiltonian simulation, in which the conditional Hamiltonian evolution \( \sum_{r=0}^{T-1} |\tau\rangle \langle \tau | \otimes e^{iA\tau t_0/T} \) is applied on \( |\Psi_0\rangle |b\rangle \) (where \( |\Psi_0\rangle = \sum_{r=0}^{T-1} \alpha_r |\tau\rangle \) is an initial state with \( \alpha_r \), minimizing a certain quadratic loss function, \( t_0 = O(\kappa/\epsilon) \) and the resulting \( \tilde{\lambda} \approx 2\pi k/t_0 \) with \( k \in \{0, \ldots, T - 1\} \).

Let the algorithm’s time complexity be estimated. Let the algorithm corresponding to the circuit in figure 6.12 be considered, consider also that the operations in \( U_\lambda \) are logarithmic in \( N \) and that they scale well with the accuracy \( \epsilon \) desired for the solution, and let \( 1/\kappa \leq \lambda \leq 1 \). Consider the following theorem:

**Theorem 6.8.1** (Simulation of sparse Hamiltonians [23]). For an \( s \)-sparse (for an \( s \ll N \) and efficientlyrow computable (meaning it has at most \( s \) nonzero entries per row and given a row index these entries can be computed in time \( O(s) \)) Hermitian matrix \( A \), \( e^{iAt} \) can be simulated in time \( \tilde{O}(\log(N)s^2t) \).

A great source of error is the phase estimation procedure, which errors by \( \lambda^{\epsilon} \) if \( \lambda \geq 1/\kappa \). If \( \lambda \geq 1/\kappa \) taking \( t_0 = O(\kappa/\epsilon) \) induces a final error of \( \epsilon \). Considering the success probability of the post-selection process is

\[
\tilde{p} = \sum_j \frac{\beta_j^2 C}{\lambda_j^2} \geq C^2/\lambda_{\text{max}}^2 = C^2 = O(1/\kappa^2),
\]

since \( \lambda \leq 1 \) (for the rescaled \( A \) and \( C = O(1/\kappa) \). Using amplitude amplification [24] this probability can be increased to \( O(1/\kappa) \), sufficing \( O(1/\kappa) \) repetitions on average to succeed. Taking into account the time necessary to perform the phase estimation, considering theorem 6.8.1 \( t_0 = O(\kappa/\epsilon) \) and the conditional Hamiltonian evolution used on the phase estimation, \( \sum_{r=0}^{T-1} |\tau\rangle \langle \tau | \otimes e^{iA\tau t_0/T} \), an upper-bound of the runtime of the HHL is given by \( \tilde{O}(s^2\kappa^2 \log(N)/\epsilon) \). The same result can be reached for the case where 6.27 is used instead.

Several improvements on the original algorithm were already accomplished, and a list is presented on table 6.1.

**Table 6.1**: List of algorithms solving the quantum linear systems problem and list of their respective runtime complexities

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Runtime Complexity</th>
</tr>
</thead>
<tbody>
<tr>
<td>HHL [22]</td>
<td>( O(\log(N)s^2\kappa^2/\epsilon) )</td>
</tr>
<tr>
<td>VTAA-HHL [25]</td>
<td>( O(\log(N)s^2\kappa/\epsilon) )</td>
</tr>
<tr>
<td>Childs et al. [26]</td>
<td>( O(s\kappa \text{polylog}(s\kappa/\epsilon)) )</td>
</tr>
<tr>
<td>QLSA [27]</td>
<td>( O(\kappa^2 \text{polylog}(N)</td>
</tr>
</tbody>
</table>

In particular, QLSA achieves a sparsity-independent runtime scaling, thus being suitable for dense matrices, and Childs et al. exponentially improve the dependence of the runtime complexity on precision while keeping essentially the same dependence on other parameters (in comparison to HHL by bypassing the quantum phase estimation algorithm, whose dependence on \( \epsilon \) is prohibitive.

The best general-purpose classical matrix inversion algorithm is the conjugate gradient method [28], which, when \( A \) is positive definite has a total runtime of \( O(Ns\sqrt{k}\log (1/\epsilon)) \) (if \( A \) is not positive definite, a total time of \( O(Ns\kappa \log (1/\epsilon)) \) is required). Even though HHL presents a runtime which is an exponential improvement over the best classical algorithm, one only has the solution available in the form of a quantum state \( |\tilde{x}\rangle \), requiring the procedure to be repeated at least \( N \) times to retrieve all the entries of \( \tilde{x} \) through measurement of the output. This would render the algorithm useless in comparison to the
general-purpose classical matrix inversion algorithm. However, the advantage is not lost if \( |x \rangle \)'s purpose is to be further used in quantum computation, or if one is interested in some global property of the solution, not all of it, which can be determined by performing measurements on \( |x \rangle \). In fact, one can compute some expectation value \( \langle x | M | x \rangle \) (\( M \) is some linear operator) corresponding to a feature of \( |x \rangle \) desired to be estimated. In particular, one can efficiently determine whether the solutions of two sets of linear equations are close to one another using the HHL algorithm and the SWAP test [29].

Also, notice that the register that relates to the vectors \( |b \rangle \) and \( |x \rangle \) is a \( O(\log N) \)-qubit register, thus instead of having registers of size \( N \) one has a more compact representation for the vectors (at a cost), with the weights of the components as amplitudes of the components of the quantum state. Thus, space-wise it is in part more efficient, exponentially so.

Regarding the preparation of \( |b \rangle \), there are ways to prepare certain states efficiently, one of which is [30], doing so in time polylogarithmic in \( N \) (polynomial in the number of particles; time complexity also dependent on other parameters).

For an instance of the problem stated before (involving obtaining \( \langle x | M | x \rangle \)), HHL is seen as optimal, being the problem BQP-complete [31]. Let the mentioned problem be defined concretely:

**Definition 6.8.1 ((Quantum) Matrix Inversion).** An algorithm solves a matrix inversion if it has:

- **Input:** An \( O(1) \)-sparse matrix \( A \) specified using an oracle or via a \( \text{poly}(\log N) \)-time algorithm that returns the non-zero elements of a row.

- **Output:** A bit that equals one with probability \( \langle x | M | x \rangle \pm \epsilon \), where \( M = |0\rangle \langle 0| \otimes I_{N/2} \) corresponds to measuring the first qubit and \( |x \rangle \) is a normalized state proportional to \( A^{-1} |b \rangle \) for \( |b \rangle = 0 \).

It is also demanded that \( A \) is Hermitian and that \( \kappa^{-1} I \leq A \leq I \).

Despite this very weak definition for matrix inversion, this task is still classically hard, however it is efficiently performed on a quantum computer using the HHL algorithm.
Chapter 7
Conclusions and future work

7.1 Conclusions

Several areas of quantum computation were presented and discussed here, namely the quantum gates, quantum circuits, quantum error correction, fault-tolerant quantum computation and quantum algorithms. The fundamental concepts to understand them were also introduced.

Regarding algorithms, some of the most basic and important ones were presented along with their application in solving some problems of interest. A more elaborate algorithm was also presented, the HHL algorithm, which served as an example of an algorithm using some of the basic procedures introduced.

Regarding quantum error correction, the identification of errors with the operators of a quantum operation was made and the possible interpretation of the error being the result of some unitary transformation involving the system in question and the environment was given. With this perspective, the continuum of quantum errors was characterized in a way in which it was clear that they could be corrected by only considering the correction of a discrete subset of these errors. The quantum error correction conditions were obtained and allowed to identify if a set of errors was correctable by a certain code. Classical linear codes were introduced, since quantum error correction codes can be constructed from them and are used in the stabilizer construction. The concept of distance of a code was also introduced, which is one plus the maximum number of bits/qubits (qubits for the distance of a quantum code) that an error can have so that when applied on a valid codeword it does not result in another valid codeword (otherwise one might not be able to identify that an error occurred). The distance of a classical code is defined as the minimum distance between two codewords of the code, from which one can understand how the previous statement came to be. Analogously, for a quantum code, if $d$ is its distance then it can detect errors on up to $d - 1$ qubits, and its definition is closely related to this statement. With these elements presented, the stabilizer formalism is given and the particular case of the interesting stabilizer CSS codes was shown. Some examples of quantum error correction codes were also shown and bounds concerning the parameters of the quantum codes were unfolded.

Regarding fault-tolerant computation, it was discussed the requirements a fault-tolerant implementation of the components of a quantum circuit should satisfy, how a non-identifiable error can be used as a useful operation on the encoded qubits and how the stabilizer construction is useful for quantum fault tolerance. The transversal design for implementing components fault-tolerantly was also considered, allowing errors from a qubit of an encoded block to affect only a qubit of the other encoded block interacting with it, granting a small error propagation. It was also pointed that after performing an operation on the qubits, error correction should be performed. Certain operations were also shown how to be implemented fault-tolerantly, such as gates, measurements and state preparations. The threshold theorem was also given, stating that under reasonable assumptions it is possible to improve the reliability of the computation using error correction, thus making of fault-tolerant quantum computation something to follow. Some final remarks were also made for a better understanding and also to present some eventual situations that might present themselves in the fault-tolerant implementation of a quantum computer.
Regarding quantum circuits and quantum gates, some of the basic quantum gates were introduced, and the quantum measurement on a circuit was also discussed, with the principle of deferred measurement being stated and proved, which states that any measurement made in the middle of the circuit can be made instead at the end of it, and with the principle of implicit measurement also being stated and proved, which states that any qubits that were not measured at the end of the circuit may be assumed to be measured, since measuring them would not alter the statistics of the measured ones. The no-cloning theorem was presented, from which it is concluded that one cannot clone non-orthogonal states using a unitary transformation. It was also seen that errors on gates accumulate linearly, that is, if there is an error less than $\epsilon_1$ in a gate and that gate is followed by a gate with an error less than $\epsilon_2$, then the overall error of the two gates is less than $\epsilon_1 + \epsilon_2$. These errors come from the fact that one cannot represent the gate exactly, which given the continuum of gates possible it does not come as a shock. It is also true that some gates might be more easily implementable than others, and so the fact that there exist universal sets of gates is very agreeable; a universal set of gates is a set made of a finite number of gates from which all possible gates can be obtained to an arbitrary accuracy. The existence of such a set was proven and an upper bound on how many gates would be needed to approximate a specific gate to a specified accuracy was presented.

Regarding the fundamental concepts, the elementary unit of information for quantum computation and quantum information was introduced, the qubit. Alongside, the state representation of a system of an arbitrary number of qubits was introduced. The quantum measurement was also introduced, and the phenomena of quantum nonlocality and quantum entanglement were discussed, with some games into the mixture so as to familiarize with the behaviours associated to those same phenomena. The description of a system’s state as a density operator was introduced. With it, the system could be said to be in one of several possible states with some probabilities associated. Such a valuable description can be used to describe the statistics associated to subsystems of a larger system by means of the partial trace operator, which when applied to the density operator of the larger system returns the density operator of the subsystem of interest. The Schmidt decomposition of a state and its relation with measuring entanglement was presented. The purification method was also introduced by which a mixed state of a system could be identified with the mixed state of a subsystem whose larger system’s state is a pure state. Besides that, the Bloch sphere representation was introduced. This is a representation of a single qubit state in a sphere, which is interesting in its own right, and which has several properties, applications and is quite useful for describing transformations on a qubit.

Given this summary, it is considered that the objectives were accomplished, being the introduction to quantum computation filled with relevant content and providing an adequate perspective of the theory from an introductory point of view. Some of the most important areas of quantum computation were presented and discussed, providing a starting point from which to explore quantum computation theory even further, to more advanced topics.

The power of a quantum computer is something subtle, solving some apparently hard classical problems efficiently. However, this increased power of a quantum computer over a classical one is not a proven fact, and it is related to the $P$ vs. $NP$ problem. Although it is believed that $P \neq NP$, with some of the problems efficiently solvable on quantum computer believed to belong to the intermediate complexity class $NP\overline{P}$ (existing if $N \neq NP$), that is still not proven. Moreover, exploiting the power of a quantum computer can be a challenging task. Since a quantum computer is much more susceptible to noise than a classical computer, quantum computation should be done fault-tolerantly. This is one of the applications of quantum error-correction.

It is clear that a quantum computer can do all that a classical computer can, however unlike a classical
computer a quantum computer performs only reversible transformations (besides measurement), thus any classical circuit which is desired to be implemented on a quantum computer must be done so reversibly.

Furthermore, there are things that a quantum computer can do which do not seem to be efficiently simulatable on a classical computer. Such traits can be used to efficiently perform tasks that a classical computer does not seem to be able to perform. In that spirit, quantum algorithms’ design is somewhat different than the classical algorithms’ one. One characteristic aspect is quantum parallelism, which is the effect associated to the application of a transformation to a state which is a superposition of the base states, thus the transformation being applied to each of the base states, by linearity. Thus, if the state is a superposition of an exponential number of base states, a transformation applied to that state acts on those base states which are exponential in number, something that would require (classically) the transformation to be applied to each of those exponential number of base states to obtain the resulting transformation output for each of the base states involved. Thus, an exponential number of those transformations would be needed to be performed instead of just one! This quantum parallelism property associated to the superposition nature of a quantum state is very valuable in quantum algorithms and its application was observed on the algorithms studied here. Another such property is quantum entanglement. Quantum entanglement in algorithms is especially useful to associate values, identifying them as a related block of information. For example, having some register in a superposition of the states \( \{ |u_j \rangle \} \), it can be useful in order to perform some computation to make those states related to some other states \( \{ |v_j \rangle \} \), and therefore one can entangle two registers into a state \( \sum_{j} |u_j \rangle |v_j \rangle \) (apart from the normalization constant), where the states \( \{ |u_j \rangle |v_j \rangle \} \) are seen as blocks of related information. Information from these registers became correlated. The application of the quantum entanglement property was also observed on the algorithms studied here. These are all nice features, however there is the caveat that one cannot obtain the full description of the quantum state, indeed one can only get one component associated to that state. For example, if one is measuring a state in a basis \( \{ |u_j \rangle \} \), and that state is written in that basis as \( \sum_j \alpha_j |u_j \rangle \), then one can only obtain one of the \( |u_j \rangle \). This is a limitation which makes the design of efficient quantum algorithms (more efficient than classical ones solving the same problem) a substantially harder task, and asks for a more thoughtful approach in developing efficient quantum algorithms, since a quantum measurement of the projective kind is a destructive measurement, thus acquiring information of the state in this way is not a reversible procedure and therefore the original state is lost.

Some simple but important points in what regards designing a quantum algorithm are outlining the steps required to solve the problem and finding how those steps could be implemented more efficiently or with the same efficiency (some step must be implemented more efficiently in order for the algorithm to perform better than the classical alternative) on a quantum computer than on a classical one. There are problems which might not see significant improvement on a quantum computer than on a classical one. Hence, one should consider carefully the problem wished to be solved with the quantum algorithm.

Quantum computation (fully exploiting the resources available) is therefore radically different from classical computation, and one can hardly expect a somewhat modified version of a classical algorithm into a quantum algorithm to be adequate. Therefore, quantum algorithms usually have to be created from scratch.

Quantum computing is advancing slowly with some of the most important objectives regarding hardware being a much lower cost for the full system and operation at room temperature. Besides that, hardware should be able to handle a much greater number of qubits and their manipulation than it.
currently does.

One particular issue for classical computers which a quantum computer can solve easily is the generation of random numbers. It seems that quantum computers will aid classical computers on solving some hard-classical problems that a quantum computer can solve efficiently. Thus, a quantum computer can definitely work as a support for the classical computer, and on that note, one has an hybrid machine. This also inspires the development of hybrid algorithms.

7.2 Future work

Quantum computation revolves mostly around Hilbert spaces of finite dimension, tensor products and linear algebra. It exploits the quantum mechanical interpretation of those to develop a different computational paradigm, unlike the classical one. This paradigm seems to provide improvement on performing certain tasks, which are of practical interest.

Instead of Hilbert spaces of finite dimension, I pretend to explore other types of spaces. On my future work, I am inclined on studying different types of spaces, such as for example curved spaces and their associated geometry, more specifically the area of differential geometry, where linearity is also exploited. Also, spaces of infinite dimension such as infinite-dimensional Banach spaces (from which Hilbert spaces are a special case), more specifically the areas of functional analysis, dynamical systems and differential equations. For general differential equations, for example, linearity is not a given property, hence for non-linear differential equations this property whose usefulness on quantum computation was observed is of no help. Even though the spaces studied in this work were of finite dimension, infinite dimension is not such a strange concept to at least one of the studied transformations, the Fourier transform. The Fourier transform can represent a periodic function as a linear combination of basis functions, namely \{1, \cos \omega x, \sin \omega x, \cos 2\omega x, \sin 2\omega x, \ldots\} (\omega = 2\pi/T where T is the period of the function), which is an orthogonal basis (with respect to the inner product $f \cdot g = \int_{-T/2}^{T/2} f(x)g(x)dx$) of infinite size.

Some of the referred areas might benefit of quantum computation (in what regards computation related to those areas). Therefore, an eye should be kept open for possible applications of quantum computation in solving computational problems associated with the referred areas.
References

Main reference

Introduction

The essentials
Quantum circuits and quantum gates


Fault-tolerant quantum computation


Quantum computation


Bibliography

The essentials


Quantum circuits and quantum gates


Quantum error correction


Appendix A


Appendix B

Appendix A

Notation and linear algebra for quantum computing

A.1 Bra-ket notation

The notation used in this thesis is the bra-ket notation, also known as the Dirac notation, and is in essence a linear algebra notation to represent and manipulate vectors and matrices. This \langle \cdot | \rangle is denoted a bra and this | \cdot \rangle a ket. It follows:

\[ |\psi\rangle = \begin{bmatrix} \psi_1 \\ \psi_2 \\ \vdots \\ \psi_n \end{bmatrix}, \quad \langle \psi | = \langle \psi \rangle^\dagger = (|\psi\rangle^*)^T = \begin{bmatrix} \psi_1^* & \psi_2^* & \cdots & \psi_n^* \end{bmatrix}. \quad (A.1) \]

Hence,

\[ \langle \psi | \psi \rangle = \sum_j |\psi_j|^2, \quad |\psi\rangle \langle \psi | = \begin{bmatrix} \psi_1 \psi_1^* & \psi_1 \psi_2^* & \cdots & \psi_1 \psi_n^* \\ \psi_2 \psi_1^* & \psi_2 \psi_2^* & \cdots & \psi_2 \psi_n^* \\ \vdots & \vdots & \cdots & \vdots \\ \psi_n \psi_1^* & \psi_n \psi_2^* & \cdots & \psi_n \psi_n^* \end{bmatrix}. \quad (A.2) \]

Also, the following is included in the notation

\[ |vs\rangle = |v\rangle \otimes |s\rangle = \begin{bmatrix} v_1 s_1 \\ v_1 s_2 \\ \vdots \\ v_1 s_n \\ v_2 s_1 \\ \vdots \\ v_2 s_n \\ \vdots \\ v_n s_1 \\ \vdots \\ v_n s_n \end{bmatrix}^T, \quad (A.3) \]

where \( \otimes \) denotes the tensor product, which translates, for matrices, in

\[ A \otimes B = \begin{bmatrix} A_{11}B & A_{12}B & \cdots & A_{1n}B \\ A_{21}B & A_{22}B & \cdots & A_{2n}B \\ \vdots & \vdots & \cdots & \vdots \\ A_{m1}B & A_{m2}B & \cdots & A_{mn}B \end{bmatrix}. \quad (A.4) \]

An example of the usefulness of (A.3):

\[ |0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \quad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \]

\[ |00\rangle = |0\rangle \otimes |0\rangle = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, \quad |01\rangle = |0\rangle \otimes |1\rangle = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}, \quad |10\rangle = |1\rangle \otimes |0\rangle = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} \]

\[ |11\rangle = |1\rangle \otimes |1\rangle = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}. \quad (A.5) \]

Just like that, an orthonormal basis in two dimensions creates an orthonormal basis in four dimensions, representing each base vector one of the possible classical two-bit strings.
The outer product of two vectors of dimensions \( m \) and \( n \) is

\[
|\phi\rangle \langle \psi| = |\phi\rangle \otimes |\psi\rangle = \begin{bmatrix}
\phi_1 \psi_1^* & \phi_1 \psi_2^* & \ldots & \phi_1 \psi_n^* \\
\phi_2 \psi_1^* & \phi_2 \psi_2^* & \ldots & \phi_2 \psi_n^* \\
\vdots & \vdots & \ddots & \vdots \\
\phi_m \psi_1^* & \phi_m \psi_2^* & \ldots & \phi_m \psi_n^*
\end{bmatrix}.
\]

(A.6)

Another useful property is

\[
(A \otimes B)(C \otimes D) = (AC \otimes BD),
\]

where \( A, B, C, \) and \( D \) are matrices of appropriate sizes, more specifically are such that \( AC \) and \( BD \) are valid matrices’ products.

Consider now the space \( \mathcal{H}_1 \otimes \mathcal{H}_2 \), the operator \( X \otimes Y \) (for matrices \( X \) and \( Y \) acting on the spaces \( \mathcal{H}_1 \) and \( \mathcal{H}_2 \), respectively) is usually denoted by \( X_1Y_2 \) or by \( XY \) (when it is clear from context that it is not matrix multiplication).

### A.2 The projection operators and the completeness relation

An interesting property can be obtained whose deduction shows the convenience of the notation used. Let \(|i\rangle\) be an orthonormal basis, then \(|\psi\rangle = \sum_i m_i |i\rangle\) and

\[
|\psi\rangle = \sum_i m_i |i\rangle : \left( \sum_i |i\rangle \langle i| \right) |\psi\rangle = \sum_{i,j} m_j |i\rangle \langle i|j\rangle = \sum_{i,j} m_j \delta_{ij} |i\rangle = \sum_i m_i |i\rangle = |\psi\rangle
\]

(A.8)

for an arbitrary \(|\psi\rangle\), which leads to the following conclusion,

\[
\sum_i |i\rangle \langle i| = I,
\]

(A.9)

since there is only one identity \((|\psi\rangle\text{ is arbitrary})\). (A.9) is denoted the completeness relation.

A Hermitian operator \( P \) is said to be a projection or a projection operator if \( P^2 = P \). A set of projectors \( \{P_i\} \) are said to be orthogonal projectors if

\[
P_iP_j = \begin{cases} P_i & \text{if } i = j \\ 0 & \text{if } i \neq j \end{cases}
\]

(A.10)

and it follows that \( \sum_i P_i \) is also a projector. In fact, if \( \langle \psi|\psi\rangle = 1 \) then \( P = |\psi\rangle \langle \psi| \) is a projector so that \( P^* = (|\psi\rangle \langle \psi|)^\dagger = (\langle \psi|\psi\rangle)^\dagger = |\psi\rangle \langle \psi| \) and \( P^2 = (|\psi\rangle \langle \psi|)(|\psi\rangle \langle \psi|) = |\psi\rangle \langle \psi| \langle \psi| |\psi\rangle = |\psi\rangle \langle \psi| \). Hence, the completeness relation holds for a set of orthogonal projectors where \( \{|i\rangle\} \) is an orthonormal basis and the correspondent projectors are \( \{|i\rangle \langle i|\} \). Another property associated to projectors, which is very expected, is that its eigenvalues are either 1 or 0 for \( Pv = \lambda v, v \neq 0 \Rightarrow \lambda(\lambda - 1)v = 0, v \neq 0 \Rightarrow \lambda = 1 \lor \lambda = 0 \).

### A.3 Hermitian and unitary operators

A linear operator \( A \) is said to be Hermitian if \( A = A^\dagger \). A Hermitian operator’s eigenvalues are real and its eigenvectors are orthogonal.

An operator \( A \) on an inner product space is said to be positive, \( A \geq 0 \), if \( \langle \psi|A|\psi\rangle \geq 0 \), and such an operator is Hermitian.

An operator is said to be unitary if \( U^{-1} = U^\dagger \), that is, if \( UU^\dagger = U^\dagger U = I \). The unitary operator’s eigenvalues have absolute value 1. \( U \) being unitary is equivalent to \( U^\dagger \) being unitary. Moreover, from
$U^\dagger U = I$ one concludes that the columns of $U$ form an orthonormal basis with respect to the usual inner product, and from $UU^\dagger = I$ one concludes that the rows of $U$ form an orthonormal basis with respect to the usual inner product.

The commutator and anti-commutator of the matrices $A$ and $B$ are respectively defined as

$$[A, B] = AB - BA, \quad \{A, B\} = AB + BA.$$  \hfill (A.11)

An operator is said to be normal if

$$[A, A^\dagger] = 0.$$  \hfill (A.12)

### A.4 The Trace

The trace of a matrix is defined as $\text{tr}(A) = \sum_i A_{ii} = \sum_i \langle i | A | i \rangle$, and two important properties associated to the trace are demonstrated below.

$$\text{tr}(AB) = \sum_i (AB)_{ii} = \sum_i \sum_j A_{ij} B_{ji} = \sum_j \left( \sum_i B_{ji} A_{ij} \right) = \sum_j (BA)_{jj} = \text{tr}(BA)$$  \hfill (A.13)

The property in (A.13) is the cyclic property of the trace.

$$\text{tr}(ab^T) = \sum_i (ab^T)_{ii} = \sum_i \sum_j a_{ij} b_{ji} = \sum_j \left( \sum_i a^T_{ji} b_{ij} \right)$$

$$= \sum_i a^T_{i1} b_{1} = \sum_i a_i b_i = a^T b = b^T a, \quad \text{for column vectors } a \text{ and } b.$$  \hfill (A.14)

It is seen that, for any orthonormal basis $\{j\}$, the trace can be written in terms of its elements as $\text{tr}(A) = \sum_j \langle j | A | j \rangle$.

Also, considering eigenvalues and eigenvectors of a tensor product of matrices, and its trace and determinant:

$$(A \otimes B)(v \otimes x) = (Av \otimes Bx) = (\lambda v \otimes \mu x) = \lambda \mu (v \otimes x),$$  \hfill (A.16)

$$\text{tr}(A \otimes B) = \sum_j \sum_i \lambda_j \mu_i = \sum_j \lambda_j \sum_i \mu_i = \left( \sum_j \lambda_j \right) \left( \sum_i \mu_i \right) = \text{tr}(A)\text{tr}(B),$$  \hfill (A.17)

$$\text{det}(A \otimes B) = \prod_{j=1}^n \prod_{i=1}^m \lambda_j \mu_i = \prod_{j=1}^n \lambda_j^m \left( \prod_{i=1}^m \mu_i \right) = \left( \prod_{j=1}^n \lambda_j^m \right) \left( \prod_{i=1}^m \mu_i \right),$$

$$= \left( \prod_{j=1}^n \lambda_j^m \right) \left( \prod_{i=1}^m \mu_i \right) = \text{det}(A)^m \text{det}(B)^n,$$  \hfill (A.18)

where $\lambda$ corresponds to an eigenvalue of $A$ (with $A$ having $n$ eigenvalues) and $v$ to the respective eigenvector; $\mu$ corresponds to an eigenvalue of $B$ (with $B$ having $m$ eigenvalues) and $x$ to the respective eigenvector.

Remark. Eigenvectors of norm 1 are sometimes called eigenkets.
A.5 The Spectral Decomposition Theorem

Theorem A.5.1 (Spectral Decomposition). Let \( H \) be a normal operator, its eigenvalues be \( \{\lambda_i\} \) and its orthonormal eigenvectors \( \{|v_i\}\) then \( H \) can be written as

\[
H = \sum_i \lambda_i |v_i\rangle \langle v_i| = \sum_i \check{\lambda}_i P_i,
\]

where \( \{\check{\lambda}_i\} \) are all its distinct eigenvalues and \( \{P_i\} \) are the projectors in each of the eigenspaces of the distinct eigenvalues.

Let \( M \) be an operator on a vector space \( W \). \( M \) is diagonalized by a unitary transformation if and only if \( M \) is a normal matrix. Saying this is the same as saying that \( M \) being a normal matrix means that \( M \) is diagonal with respect to some orthonormal basis for \( W \) (the columns and rows of a unitary matrix form an orthonormal basis).

Proof. Every matrix has at least one non-null eigenvector, hence let \( v_1 \) be an eigenvector of \( A \) with eigenvalue \( \lambda_1 \) and completing a set \( v_1, \ldots, v_n \) of orthonormal vectors spanning the \( n \)-dimensional space \( W \), which serve as columns of the unitary matrix \( V \). Then, applying it as a similarity transformation,

\[
V^\dagger AV = \begin{bmatrix} v_1^\dagger & v_2^\dagger & \cdots & v_n^\dagger \end{bmatrix} A \begin{bmatrix} v_1 & v_2 & \cdots & v_n \end{bmatrix} = \begin{bmatrix} v_1^\dagger Av_1 & v_1^\dagger Av_2 & \cdots & v_1^\dagger Av_n \\ v_2^\dagger Av_1 & v_2^\dagger Av_2 & \cdots & v_2^\dagger Av_n \\ \vdots & \vdots & \ddots & \vdots \\ v_n^\dagger Av_1 & v_n^\dagger Av_2 & \cdots & v_n^\dagger Av_n \end{bmatrix} = \begin{bmatrix} \lambda_1 & b^\dagger \\ 0 & C \end{bmatrix},
\]

since \( v_i^\dagger Av_1 = \lambda_1 v_i^\dagger v_1 = \lambda_1 \delta_{i1} \), and where \( b^\dagger \) is a \( 1 \times (n-1) \) row vector, \( 0 \) is an \( (n-1) \times 1 \) column vector (of zeroes) and \( C \) is an \( (n-1) \times (n-1) \) matrix. Note that normal matrices remain normal under unitary similarity transformations since

\[
[U^\dagger AU, (U^\dagger AU)^\dagger] = U^\dagger A U U^\dagger A^\dagger U = U^\dagger (AA^\dagger - A^\dagger A) U = U^\dagger [A, A^\dagger] U = 0,
\]

for any unitary matrix \( U \).

Thus,

\[
[V^\dagger AV, (V^\dagger AV)^\dagger] = \begin{bmatrix} \lambda_1 & b^\dagger \\ 0 & C \end{bmatrix} \begin{bmatrix} \lambda_1 & 0 \\ b^\dagger & C^\dagger \end{bmatrix} - \begin{bmatrix} \lambda_1^\dagger & 0 \\ b^\dagger & C^\dagger \end{bmatrix} \begin{bmatrix} \lambda_1 & b^\dagger \\ 0 & C \end{bmatrix} = \begin{bmatrix} b^\dagger b & b^\dagger C^\dagger - \lambda_1 b^\dagger \\ C b & C C^\dagger \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix},
\]

and because \( b^\dagger b = \|b\|^2 \) and \( b^\dagger b = 0 \), then \( b = 0 \) from which it can be concluded that \( [C, C^\dagger] = 0 \), thus \( C \) is normal and

\[
V^\dagger AV = \begin{bmatrix} \lambda_1 & 0 \\ 0 & C \end{bmatrix}.
\]

Since the eigenvalues of a matrix are invariant under similarity transformations, \( V^\dagger AV \) has the same eigenvalues as \( A \) and the characteristic equation results in
\[
\det \left( \begin{bmatrix} \lambda_1 & 0 \\ 0 & C \end{bmatrix} - \lambda I_n \right) = (\lambda_1 - \lambda) \det (C - \lambda I_{n-1}),
\] (A.24)

meaning that the eigenvalues of \( C \) are the same as those of \( A \), with the exception of \( \lambda_1 \).

Continuing the procedure by choosing an eigenvector \( y_1 \) of \( C \) with eigenvalue \( \lambda_2 \) and completing a set \( y_1, \ldots, y_n \) of orthonormal vectors spanning this \( (n-1) \)-dimensional space, which serve as columns of the unitary matrix \( Y \), leads to

\[
X = \begin{bmatrix} 1 & 0 \\ 0 & Y \end{bmatrix}
\] (A.25)

\[
X^\dagger V^\dagger A V X = (V X)^\dagger A (V X) = \begin{bmatrix} 1 & 0 \\ 0 & X^\dagger \end{bmatrix} \begin{bmatrix} \lambda_1 & 0 \\ 0 & C \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & X \end{bmatrix} = \begin{bmatrix} \lambda_1 & 0 \\ 0 & X^\dagger C X \end{bmatrix}
\]

Using the same arguments as above,

\[
X^\dagger C X = \begin{bmatrix} \lambda_2 & 0 \\ 0 & D \end{bmatrix},
\] (A.26)

where \( D \) is normal and has the same eigenvalues as \( A \) except \( \lambda_1 \) and \( \lambda_2 \). Hence,

\[
(V X)^\dagger A (V X) = \begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix}.
\] (A.27)

Clearly, this process can be continued. Since the product \( U \) of unitary matrices is unitary, after \( n-1 \) steps \( U^\dagger A U = \Lambda \) where \( \Lambda \) is a diagonal matrix whose first \( n-1 \) diagonal elements are \( \lambda_1, \ldots, \lambda_{n-1} \), and because the eigenvalues of \( \Lambda \) are the same as those of \( A \), the \( n \)th diagonal element is \( \lambda_n \) and hence every \( n \times n \) normal matrix may be diagonalized by a unitary matrix.

Conversely, suppose a matrix \( A \) can be diagonalized by a unitary matrix \( U \). Then,

\[
D = U^\dagger A U, \quad D^\dagger = U^\dagger A^\dagger U \quad [D, D^\dagger] = U^\dagger A U U^\dagger A^\dagger U - U^\dagger A^\dagger U U^\dagger A U = U^\dagger [A, A^\dagger] U.
\] (A.28)

Thus,

\[
[A, A^\dagger] = U [D, D^\dagger] U^\dagger = 0,
\] (A.29)

since \( D \) and \( D^\dagger \) are diagonal matrices and diagonal matrices commute. Therefore, \([A, A^\dagger] = 0\), meaning that \( A \) is normal.

Now, according to what has been shown

\[
U^\dagger A U = \Lambda \iff A U = U \Lambda \iff \begin{bmatrix} A u_1 & A u_2 & \cdots & A u_n \end{bmatrix} = \begin{bmatrix} \lambda_1 u_1 & \lambda_2 u_2 & \cdots & \lambda_n u_n \end{bmatrix},
\] (A.30)

meaning that each column of the unitary matrix \( U \) corresponds to a matrix with columns \( \{u_i\} \) which are orthonormal eigenvectors of \( A \), each corresponding to one of the eigenvalues \( \{\lambda_i\} \).

So, finally, \( A \) can be written as

\[
A = \sum_i \lambda_i |u_i \rangle \langle u_i|.
\] (A.31)

If the dimension of an eigenspace is bigger than one, then its corresponding eigenvectors in the decomposition can be selected needing only to be orthonormal and spanning the corresponding eigenspace.

In fact, in general, for the distinct eigenvalues \( \{\tilde{\lambda}_i\} \),

\[
A = \sum_i \tilde{\lambda}_i P_i,
\] (A.32)

where \( P_i \) is a projection operator that projects onto the eigenspace of the eigenvalue \( \tilde{\lambda}_i \).
### A.6 The Polar and Singular Value Decompositions

**Theorem A.6.1** (Polar Decomposition [13]). Let $A$ be a linear operator on a vector space $W$. Then, there exist unitary $U$ and positive operators $J$ and $K$ such that

$$
A = UJ = KU,
$$
(A.33)

where the unique positive operators $J$ and $K$ satisfying these equations are defined by $J = \sqrt{AA^\dagger}$ and $K = \sqrt{A^\dagger A}$. Moreover, if $A$ is invertible then $U$ is unique.

**Proof.** Starting with the characterization of $AA^\dagger$ and $A^\dagger A$,

$$
[A^\dagger A, (A^\dagger A)^\dagger] = A^\dagger AA^\dagger A - A^\dagger A A^\dagger = 0
$$

$$
\text{Im} \left\{ A^\dagger A \right\} = \frac{A^\dagger(A^\dagger A)^\dagger}{2} = 0
$$

it can be deduced that both are normal matrices, symmetric (since they are real and equal to its conjugate transposed) and thus having a spectral decomposition, and from

$$
\langle \psi | A^\dagger A | \psi \rangle = \| A | \psi \|_2^2 \geq 0
$$

$$
\langle \psi | AA^\dagger | \psi \rangle = \| A^\dagger | \psi \|_2^2 \geq 0,
$$
(A.35)

$A^\dagger A$ can be decomposed as $A^\dagger A = \sum_i \lambda_i | \psi_i \rangle \langle \psi_i |$, $\lambda_i \geq 0$ and similarly for $AA^\dagger$. Now, focusing on $A^\dagger A$ it is clear that $J$ can be written as $J = \sum_i \sqrt{\lambda_i} | \psi_i \rangle \langle \psi_i |$. Defining $| \psi_i \rangle \equiv A | i \rangle$ and noting $\langle \psi_i | \psi_i \rangle = \lambda_i$, the following normalized versions are defined as $| e_i \rangle = | \psi_i \rangle / \sqrt{\lambda_i}$ for all $i$ whose $\lambda_i$ is different from zero. The vectors $\{ | e_i \rangle \}$ are clearly orthonormal, and since the set is formed for elements such that $\lambda_i \neq 0$, the set can be extended in order to form an orthonormal basis, and $\{ | e_i \rangle \}$ can be redefined to denote this extended set. Defining the unitary operator $U \equiv \sum_i | e_i \rangle \langle i |$, then for $\lambda_i \neq 0$ $U | i \rangle = \sqrt{\lambda_i} | e_i \rangle = | \psi_i \rangle = A | i \rangle$ and for $\lambda_i = 0$ one has $UJ | i \rangle = 0 = | \psi_i \rangle$. $A$ and $UJ$ agree on the basis $\{ | i \rangle \}$ which forms an orthonormal basis, and any vector can be written in terms of it. Since each vector of the basis when applied to $A$ and $UJ$ originates the same vector, then $A = UJ$. Now, from $A^\dagger A = (UJ)^\dagger (UJ) = J^2$ it is seen that $J = \sqrt{A^\dagger A}$, hence $J$ is uniquely defined. $J$ is invertible iff $A$ is invertible, since if $A$ is invertible it holds that $| \text{det}(A) | \neq 0 \Rightarrow | \text{det}(J) | \neq 0 \Rightarrow | \text{det}(J) | \neq 0 \Rightarrow \text{det}(J) \neq 0$ and if $J$ has inverse, $A^{-1} U^\dagger = UJ J^{-1} U^\dagger = I \Rightarrow A = UJ = J^{-1} U^\dagger$. Considering this, $U$ is uniquely determined as $U = A J^{-1}$ if $A$ is invertible. The proof of the right polar decomposition follows, since $A = UJ = U J U^\dagger U = K U$ where $K \equiv U J U^\dagger$ is a positive operator uniquely defined and which satisfies $AA^\dagger = K U U^\dagger K = K^2$ and so $K = \sqrt{A^\dagger A}$. 

Now that the polar decomposition (which is the analogue of the polar representation of a complex number) was obtained, from it the singular value decomposition can also be obtained.

Let $A$ be a square matrix. Then, there exist unitary matrices $U$ and $V$ and a diagonal matrix $D$ with non-negative entries such that $A = U D V$. The diagonal elements of $D$ are called the singular values of $A$.

This result can be seen as a consequence of the polar decomposition, in fact, by the polar decomposition $A = RJ$, for unitary $R$ and positive $J$. By the spectral decomposition theorem $J = T D T^\dagger$, for unitary $T$ and diagonal $D$ with non-negative entries. Then $A = RT D T^\dagger = U D V$ with $U \equiv RT$ and $V = T^\dagger$. 

89
Appendix B

Group theory

A group \((G, \cdot)\) is a non-empty set \(G\) of elements that together with a binary operation (name it a multiplication operation) satisfy the following properties

- **Closure**: If \(g_1, g_2 \in G\) then \(g_1 \cdot g_2 \in G\), also.

- **Associativity**: The group’s multiplication is associative, i.e., for all \(g_1, g_2, g_3 \in G\), \(g_1 \cdot (g_2 \cdot g_3) = (g_1 \cdot g_2) \cdot g_3\).

- **Identity**: There exists \(e \in G\) such that for all \(g \in G\) it is true that \(e \cdot g = g \cdot e = g\).

- **Inverse**: For all \(g \in G\) there exists \(g^{-1} \in G\) such that \(g \cdot g^{-1} = g^{-1} \cdot g = e\).

The multiplication \(g_1 \cdot g_2\) is usually just written by juxtaposition as \(g_1 g_2\). The order of a group \(G\), \(|G|\), is the number of elements it contains. The generators of a group are a subset of its elements, with the property that all elements in \(G\) can be written as a product of these generators. These generators are said to be independent if none of them can be written as product of the remaining generators.

**Proposition B.0.1.** \([43]\). If \(G\) is a group (with identity \(e\)), it follows that:

1. If \(g, g', h \in G\) and \(gh = g'h\) or \(hg = hg'\), then \(g = g'\).
2. In particular, if \(gg = g\) then \(g = e\).
3. The equation \(gx = h\) (respectively, \(xg = h\)) has as unique solution \(x = g^{-1}h\) (respectively, \(x = hg^{-1}\)).

**Proof.** It follows that

\[
gh = g'h \implies (gh)h^{-1} = (g'h)h^{-1} \implies g(hh^{-1}) = g'(hh^{-1}) \implies ge = g'e \implies g = g'
\]

(B.1)

The proof for \(hg = hg'\) is analogous, thus (1) is verified. Using (1),

\[
 gg = g \implies gg = ge \implies g = e
\]

(B.2)

therefore (2) is true. For \(xg = h\), one has \(x = hg^{-1}\), from (1). It is easy to see that this solution is unique, since also from (1) it is true that \(xg = x'g \implies x = x'\) meaning that any other \(x'\) equals \(hg^{-1}\) also. For \(gx = h\) the proof of the existence and uniqueness of the solution \(x = g^{-1}h\) is analogous, thus (3) is verified.

**Proposition B.0.2.** \([43]\) If \(G\) is a group (with identity \(e\)), and \(H \subset G\) is non-empty, then \(H\) is a subgroup of \(G\) if and only if \(hh^{-1} \in H\), for any \(h, h' \in H\).

**Proof.** Suppose first that \(H\) is a group. If \(H\) is a group, then it has an identity \(\tilde{e}\), which satisfies \(\tilde{e}\tilde{e} = \tilde{e}\). From proposition B.0.1 (2), one concludes that \(\tilde{e} = e\), and therefore \(H\) contains the identity of \(G\). Let \(h \in H\) and consider the equation \(hx = e\), which from proposition B.0.1 (3) has a unique solution in \(H\), that is also the solution of the same equation in \(G\), and therefore can only be \(x = h^{-1}\) (the inverse of \(h\)
in the original group $G$). Thus, if $h \in H$, then $h^{-1} \in H$. Finally, if $h, h' \in H$, one has $hh'^{-1} \in H$ and since $H$ is closed under its multiplication, $hh'^{-1} \in H$.

Suppose now that $hh'^{-1} \in H$ for any $h, h' \in H$. Since $H$ is non-empty, taking $h \in H$ it is true that $hh^{-1} = e \in H$, and therefore $H$ contains the identity of $G$. Analogously, if $h \in H$ one has $eh^{-1} = h^{-1} \in H$, and thus $H$ contains all the inverses (in $G$) of its elements. Finally, and to prove that $H$ is closed under its multiplication, one observes that if $h, h' \in H$, one has $h'^{-1} \in H$ from which $h(h'^{-1})^{-1} = hh' \in H$. ■

Theorem B.0.1. Cosets of $H$ partition the entire group $G$ into equal-size, non-overlapping sets.

Proof. Let the following properties be proven

\begin{align}
(1) & \quad a \in aH \\
(2) & \quad aH = bH \text{ or } aH \cap bH = \emptyset \\
(3) & \quad |aH| = |bH| \\
(4) & \quad aH = bH \iff a^{-1}b \in H
\end{align}

For (1) take $e \in H \implies a = ae \in aH$ to prove it. To prove (2), suppose $aH \cap bH \neq \emptyset$, then $\exists h_1, h_2 : x = ah_1 = bh_2 (x \in aH \cap bH)$. Hence, $a = xh_1^{-1} = bh_2h_1^{-1}$, so $aH = bh_1h_2^{-1}H = b(2h_1^{-1}H) = bH$.

To prove (3), let the following map $f : aH \to bH$ be defined as $f(aH) = bH$, then if $f(ah_1) = f(ah_2)$, one has $bh_1 = bh_2 \iff h_1 = h_2$ from which $ah_1 = ah_2$ also, so $f$ is bijective. Therefore, one concludes $|aH| = |bH|$ from the one-to-one correspondence between the two sets. Regarding (4), suppose $aH = bH$, consequently $b = ah$ (since $b \in bH$) for some $h \in H$ from which $a^{-1}b \in H$. Conversely, if $a^{-1}b \in H$ then $H = (a^{-1}b)H$ from which $aH = bH$, thus proving (4).

Now, let $x_1 \in G$ and take $x_2 \in G \setminus x_1$ where $x_1^{-1}x_2 \notin H$ and therefore $x_1H \neq x_2H$, then $x_1H \cup x_2H$ is a disjoint union of the sets. Proceeding analogously, one obtains $G = \bigcup_i x_iH$, $x_iH \cap x_jH = \emptyset$ if $x_i \neq x_j$, and because $|x_iH| = |H|$ it results that $|G| = n|H|$ for some $n \in \mathbb{N}$.

Considering theorem B.0.1 if a subgroup $H$ of a group $G$ is created with only some of its (independent) generators, then the subgroup $T$ formed by the remaining generators verifies $h^{-1}t = h't \notin H$, $t \in T \setminus \{e\}$, $h \in H$ and so each operator in $T$ originates a new disjoint coset with the identity originating $H$.  

91
Appendix C

The Pauli matrices

The Pauli matrices are defined as follows

\[ X = \sigma_1 = \sigma_x \equiv \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Y = \sigma_2 = \sigma_y \equiv \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad Z = \sigma_3 = \sigma_z \equiv \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \] (C.1)

These matrices have properties that make them matrices of interest.

\[ \sigma_i^2 = I, \quad \sigma_i \sigma_j = I \delta_{ij} + i \epsilon_{ijk} (\delta_{ij} - \delta_{ik} \delta_{ij}), \quad [\sigma_i, \sigma_j] = 2i \epsilon_{ijk} \epsilon_{(6-\delta_{ij})} \delta_{ij}, \quad \{\sigma_i, \sigma_j\} = 2I \delta_{ij} \] (C.2)

where

\[ \epsilon_{ijk} = \begin{cases} 0 & \text{for } i = j, j = k \text{ or } k = i \\ +1 & \text{for } (i, j, k) \in \{(1, 2, 3), (2, 3, 1), (3, 1, 2)\} \\ -1 & \text{for } (i, j, k) \in \{(1, 3, 2), (1, 3, 2), (2, 1, 3)\} \end{cases} \] (C.3)

is the permutation symbol, also called the Levi-Civita symbol and \( \delta \) is the Kronecker delta. Thus, distinct Pauli matrices commute. Because the square of a Pauli matrix is the identity and because each Pauli matrix is Hermitian, they are also unitary. Another interesting property is that \(-i \sigma_1 \sigma_2 \sigma_3 = I\), from which it is clear that a Pauli matrix can be written as the product of the two remaining Pauli matrices times \( \pm i \). It is also true that \( det(\sigma_i) = -1 \) and \( tr(\sigma_i) = 0 \), from which one deduces that the eigenvalues of each Pauli matrix are \( \pm 1 \). The eigenvectors of the Pauli matrices are

\[ |\psi_{x+}\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \quad |\psi_{y+}\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ i \end{pmatrix}, \quad |\psi_{z+}\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |\psi_{x-}\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}, \quad |\psi_{y-}\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -i \end{pmatrix}, \quad |\psi_{z-}\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \] (C.4)

The Pauli matrices together with the identity form a basis for the space of complex \( 2 \times 2 \) matrices, i.e. any \( 2 \times 2 \) complex matrix can be written as \( A = a_0 I + a_1 X + a_2 Y + a_3 Z \) with the \( a_i \)s being complex numbers. Moreover, one can make tensorial products of \( I, X, Y, Z \), and write any \( 2^m \times 2^n \) complex matrix as a linear combination of those matrices

\[ A = \sum_{i=0}^{4^m-1} a_i \left( \bigotimes_{j=0}^{m-1} \sigma_{(i/4^j) \mod 4} \right) \] (C.5)

being the division in (C.5) the integer division, \( \sigma_0 = I \) and the \( a_i \)s complex numbers. If one describes a \( 2 \times 2 \) complex matrix in terms of the coordinates associated with \( I, X, Y, Z \), then the product of two
matrices can be written as
\[
\vec{q} = \begin{bmatrix} q_0 \\ q_1 \\ q_2 \\ q_3 \end{bmatrix}, \quad \vec{p} = \begin{bmatrix} p_0 \\ p_1 \\ p_2 \\ p_3 \end{bmatrix}
\]

\[
\vec{q} \vec{p} = \sum_i \sum_j q_i p_j \sigma_i \sigma_j = \sum_i \sum_j p_i q_j \delta_{ij} I + i \sum_{i=1}^3 \sum_{j=1}^3 q_i p_j \epsilon_{ij}(6-i-j) \sigma_{6-i-j} + \sum_j q_0 p_j \sigma_j + \sum_i q_i p_0 \sigma_i
\]

\[
= (\vec{p} \cdot \vec{q}) I + i \begin{bmatrix} 0 \\ (\vec{q} \times \vec{p}) \end{bmatrix} + q_0 \vec{p} + p_0 \vec{q} = \begin{bmatrix} (\vec{p} \cdot \vec{q}) \\ (\vec{q} \times \vec{p}) \end{bmatrix} + q_0 \vec{p} + p_0 \vec{q}
\]

using the vectors of coordinates \(\vec{p}\) and \(\vec{q}\) associated to the matrices involved in the product.

The exponential of a matrix which is the linear combination of Pauli matrices is
\[
\vec{n} = |n| \hat{n}, \quad e^{i \vec{n} \cdot \vec{\sigma}} = e^{i |n| \hat{n} \cdot \vec{\sigma}} = I \cos (|n|) + i (\hat{n} \cdot \vec{\sigma}) \sin (|n|) = I \cos (|n|) + i \sin (|n|)(n_1 X + n_2 Y + n_3 Z) \quad (C.7)
\]

with \(|\vec{n}| = |n|\), with \(\vec{q} = \vec{p} = [0 \ \hat{n}^T]^T\).

The Pauli matrices (together with the identity) can be related to the quaternions, existing an isomorphism between the quaternions and \(I, iX, iY, iZ\), hence one can represent a quaternion in terms of a \(2 \times 2\) complex matrix using these ones.

\[
1 \cong I, \quad i \cong iX, \quad j \cong iY, \quad k \cong iZ \rightarrow q_0 + q_1 i + q_2 j + q_3 k \cong q_0 I + (q_1 X + q_2 Y + q_3 Z)i \quad (C.8)
\]

In \(C.8\) the coordinates \(q_0, q_1, q_2, q_3 \in \mathbb{R}\).
The postulates of quantum mechanics

The postulates of quantum mechanics are the mathematical foundation for the mathematical description of quantum mechanics and translate the conclusions obtained from experiments' results. They provide the connection between the physical word and the mathematical formalism of quantum mechanics. From all the postulates, four of those axioms are presented here. These are the important ones in what concerns this work.

The postulates will be stated here in terms of the state space representation, however they can be easily and analogously stated in terms of the density operator representation.

Postulate 1: Associated to any isolated physical system is a complex vector space with inner product (that is, 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.

Postulate 2: The time evolution of the state of a closed quantum system is described by the Schrödinger equation,

\[ i\hbar \frac{d}{dt} |\psi\rangle = H |\psi\rangle. \]  

(D.1)

In this equation, \( \hbar \) is a physical constant known as Planck's constant. In practice, it is common to absorb the factor \( \hbar \) into \( H \), effectively setting \( \hbar = 1 \). \( H \) is a fixed Hermitian operator known as the Hamiltonian of the closed system.

Now, let \( |\psi_1\rangle = |\psi(t_1)\rangle \) and \( |\psi_2\rangle = |\psi(t_2)\rangle \). From the solution of the Shrödinger equation, which represents the time evolution of the state, one has

\[ |\psi(t_2)\rangle = e^{-iH(t_2-t_1)/\hbar} |\psi(t_1)\rangle = U(t_1,t_2) |\psi(t_1)\rangle \leftrightarrow |\psi_2\rangle = U(t_1,t_2) |\psi_1\rangle \]  

(D.2)

where

\[ U(t_1,t_2) \equiv e^{-iH(t_2-t_1)/\hbar}. \]  

(D.3)

\( U(t_1,t_2) \) is a unitary operator. To prove it consider that \( e^A e^B = e^{A+B} \) if \( A \) and \( B \) commute. Since \( H \) and \(-H\) commute, making \( A = iH(t_2-t_1)/\hbar \) and \( B = -iH(t_2-t_1)/\hbar \) (which also commute) results in

\[ U(t_2-t_1)U(t_2-t_1) = e^{iH(t_2-t_1)/\hbar} e^{-iH(t_2-t_1)/\hbar} = e^{iH(t_2-t_1)/\hbar} e^{-iH(t_2-t_1)/\hbar} = e^0 = I. \]  

(D.4)

Similarly, it can be seen that \( U(t_2-t_1)U^\dagger(t_2-t_1) = I \), thus \( U(t_2-t_1) \) is unitary. Hence, the evolution of a closed quantum system is described by a unitary transformation.

Postulate 3: 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
The state of the quantum system is $|\psi\rangle$ immediately before the measurement then the probability that result $m$ occurs is given by

$$p(m) = \langle \psi | M_m^\dagger M_m | \psi \rangle$$  \hspace{1cm} (D.5)

and the state of the system after the measurement is

$$\frac{M_m | \psi \rangle}{\sqrt{\langle \psi | M_m^\dagger M_m | \psi \rangle}}.$$  \hspace{1cm} (D.6)

The measurement operators satisfy the completeness equation,

$$\sum_m M_m^\dagger M_m = I,$$  \hspace{1cm} (D.7)

where the completeness relation expresses the fact that probabilities sum to one.

**Postulate 4**: The state space of a composite physical system is the tensor product of the state spaces of the component physical systems. Moreover, if the systems are numbered 1 through $n$, and system number $i$ is prepared in the state $|\psi_i\rangle$, then the joint state of the total system is $|\psi_1\rangle \otimes |\psi_2\rangle \otimes \ldots \otimes |\psi_n\rangle$. 
Appendix E

Fidelity: A distance measure between two quantum states

Fidelity is a measure of distance between density operators and is defined as

\[ F(\rho, \sigma) \equiv \left( \text{tr} \sqrt{\rho \sigma \rho} \right)^2. \]  
(E.1)

with \( \sqrt{F} \) denoted as the square root fidelity. In some of the literature, an alternative version of fidelity is considered, where \( F' \equiv \sqrt{F} \) is identified as the fidelity.

Some of its properties are:

1. \( 0 \leq F(\rho, \sigma) \leq 1 \)
2. \( F(\rho, \sigma) = 1 \iff \rho = \sigma \)
3. \( F(\rho, \sigma) = 0 \) if and only if \( \rho \) and \( \sigma \) have support on orthogonal subspaces
4. \( F(\rho, \sigma) = F(\sigma, \rho) \)
5. \( F(\rho, p\sigma_1 + (1-p)\sigma_2) \geq pF(\rho, \sigma_1) + (1-p)F(\rho, \sigma_2) \), \( p \in [0, 1] \)
6. \( F(\rho, \sigma) \geq \text{tr}(\rho\sigma) \)
7. \( F(\rho, \sigma) = \text{tr}(\rho\sigma) \) if either \( \rho \) or \( \sigma \) is a pure state
8. \( F(U\rho U^\dagger, U\sigma U^\dagger) = F(\rho, \sigma) \) for unitary \( U \)
9. \( F(\rho_1 \otimes \rho_2, \sigma_1 \otimes \sigma_2) = F(\rho_1, \sigma_1)F(\rho_2, \sigma_2) \)
10. If any measurement is made on the states, transforming \( \rho_1, \rho_2 \) into \( \rho'_1, \rho'_2 \) then \( F(\rho'_1, \rho'_2) \geq F(\rho_1, \rho_2) \)

The more distinguishable two states are, the more fidelity decreases, and the less distinguishable two states are, the more fidelity increases. Hence, for example, if \( \sigma \) was to be close to \( \rho \), that is, \( \sigma = \rho \) ideally, then \( F(\rho, \sigma) \) should be close to 1.

Moreover, let \( |\psi\rangle \) and \( |\phi\rangle \) be purifications of \( \rho \) and \( \sigma \), respectively, then

\[ F(\rho, \sigma) = \max_{|\psi\rangle, |\phi\rangle} |\langle \psi | \phi \rangle|^2, \]  
(E.2)

where the maximization is over all the purifications. Let it be proved.

For states \( \rho \) and \( \sigma \) of a quantum system \( Q \), let the reference system \( R \) of the same dimension be introduced. Consider now the Schmidt decomposition of the purifications.

\[ |\psi\rangle = \sum_i \sqrt{\lambda_i} |s_i\rangle |u_i\rangle = (\sqrt{\rho} U_\rho \otimes U_R) |m\rangle \quad |\phi\rangle = \sum_j \sqrt{\mu_j} |t_j\rangle |v_j\rangle = (\sqrt{\sigma} U_\sigma \otimes V_R) |m\rangle, \]  
(E.3)
Therefore, using the Cauchy-Schwarz inequality for the Hilbert-Schmidt inner product \( \langle \rho \mid \sigma \rangle = \text{tr}(\sqrt{\rho} \sqrt{\sigma}) \), the fidelity establishes that two states can only remain as distinguishable or become more undistinguishable after the application of a quantum operation.

To prove \( \text{tr}(AU) \leq \text{tr}(|A|) \), consider the polar decomposition of \( A = |A|V \), and notice that \( \text{tr}(AU) = \text{tr}(|A|U) \) for \( U = V^\dagger \). Now, note that

\[
|\langle \psi | \phi \rangle| = |\text{tr}(\sqrt{\rho} \sqrt{\sigma})| \leq \text{tr}(\sqrt{|\rho| |\sigma|}) = \text{tr}(\sqrt{|\rho|^2 |\sigma|^2}).
\]

Therefore, using the Cauchy-Schwarz inequality for the Hilbert-Schmidt inner product \( \langle A, B \rangle = \text{tr}(AB^\dagger) \),

\[
|\text{tr}(AB^\dagger)| \leq \sqrt{\text{tr}(|A||B^\dagger|)} \sqrt{\text{tr}(B^\dagger B)},
\]

yields

\[
|\text{tr}(AU)| \leq \sqrt{\text{tr}(|A|) \text{tr}(U^\dagger V |A| V U)} = \text{tr}(|A|).
\]

Thus, \( E^2 \) means that the fidelity is equal to the square of the absolute value of the inner product of the less distinguishable pure states.

It is also true that if a trace-preserving quantum operation is applied to \( \rho \) and \( \sigma \), then the fidelity of the resulting density operators is bigger than the fidelity of \( \rho \) and \( \sigma \), \( F(\mathcal{E}(\rho), \mathcal{E}(\sigma)) \geq F(\rho, \sigma) \). Therefore, fidelity establishes that two states can only remain as distinguishable or become more undistinguishable after the application of a quantum operation.

If a quantum operation \( \mathcal{E} \) is applied to a pure state \( |\psi\rangle \), then its fidelity is \( \sum_i |\langle \psi | E_i |\psi \rangle|^2 \) where \( \{E_i\} \) are the operation elements.

For the classical case, fidelity is defined as

\[
F(p_i, q_i) = \left( \sum_i \sqrt{p_i q_i} \right)^2
\]

for probability distributions \( \{p_i\} \) and \( \{q_i\} \) and can be interpreted as the square of the inner product between two vectors with components \( \{\sqrt{p_i}\} \) and \( \{\sqrt{q_i}\} \). This can be retrieved in the quantum case for \( \rho \) and \( \sigma \) that commute, that is, when they are diagonal in the same basis. Hence, for \( \rho = \sum_i p_i |i\rangle \langle i| \) and \( \sigma = \sum_i q_i |i\rangle \langle i| \) it holds that

\[
F(\rho, \sigma) = \left( \text{tr} \left( \sum_i \sqrt{p_i q_i} |i\rangle \langle i| \right) \right)^2 = \left( \sum_i \sqrt{p_i q_i} \right)^2 = F(p_i, q_i).
\]

The fidelity between a pure state \( |\psi\rangle \langle \psi| \) and an arbitrary state \( \rho \) also has a simplified form,

\[
F(|\psi\rangle \langle \psi|, \rho) = \left( \text{tr}(\sqrt{\rho} |\psi\rangle \langle \psi| \sqrt{\rho}) \right)^2 = \langle \psi | \rho |\psi\rangle.
\]

Thus, the fidelity is equal to the overlap between \( |\psi\rangle \) and \( \rho \).
The fidelity is also equal to
\[ F(\rho, \sigma) = \min_{\{E_i\}} F(p_i, q_i), \tag{E.11} \]
where the minimum is over all POVMs \( \{E_i\} \), and \( p_i \equiv \text{tr}(\rho E_i) \), \( q_i \equiv \text{tr}(\sigma E_i) \) are the probability distributions for \( \rho \) and \( \sigma \) corresponding to the POVM \( \{E_i\} \).

Let it be proved. Consider the polar decomposition \( \sqrt{\rho \sigma} = \sqrt{\rho} \sqrt{\sigma} U \). Since \( \sqrt{F(\rho, \sigma)} = \text{tr}(\sqrt{\rho} \sqrt{\sigma} U) \leq \sum_i \sqrt{\text{tr}(\rho E_i) \text{tr}(\sigma E_i)} = \sqrt{F(p_i, q_i)} \), \( \sqrt{E_i} (I - \alpha_i M) = 0 \),\( \tag{E.14} \)
from the completeness relation and the Cauchy-Schwarz inequality, \( |\text{tr}(A^\dagger B)|^2 \leq \text{tr}(A^\dagger A) \text{tr}(BB^\dagger) \), one has that
\[ F(\rho, \sigma) \leq \min_{\{E_i\}} F(p_i, q_i). \tag{E.13} \]

For the Cauchy-Schwarz inequality to be satisfied for equality, \( \sqrt{E_i} \sqrt{\rho} = \alpha_i \sqrt{E_i} \sqrt{\sigma} U \) must hold for some set of complex numbers \( \alpha_i \). For invertible \( \rho \), \( \sqrt{\sigma U} = \rho^{-1/2} \sqrt{\rho^{1/2} \sigma \rho^{1/2}} \), since \( \sqrt{\rho} \sqrt{\sigma U} = \sqrt{\rho^{1/2} \sigma \rho^{1/2}} \).

Substituting in the equality that must be satisfied yields
\[ \sqrt{E_i} (I - \alpha_i M) = 0, \tag{E.14} \]
where \( M \equiv \rho^{-1/2} \sqrt{\rho^{1/2} \sigma \rho^{1/2}} \). If \( M = \sum_i \beta_i |i\rangle \langle i| \) is a spectral decomposition for \( M \) then one chooses \( E_i = |i\rangle \langle i| \) and \( \alpha_i = 1/\beta_i \). The case of non-invertible \( \rho \) follows from continuity.

Equation (E.11) thus shows that having states \( \rho \) and \( \sigma \), the POVM achieving the maximum distinguishability (with respect to the classical fidelity) between the distributions associated to \( \rho \) and \( \sigma \) allows to calculate the fidelity by computing the classical fidelity between the corresponding distributions, i.e. \( \{\sqrt{p_i}\} \) and \( \{\sqrt{q_i}\} \) minimize the classical fidelity, and therefore achieve the maximum distinguishability for a POVM on \( \rho \) and \( \sigma \). Intuitively, this means that according to the fidelity minimization criterion on equation (E.11), if one was to perform a POVM in order to distinguish the states \( \rho \) and \( \sigma \), then the POVM corresponding to (E.11) is the one achieving maximum distinguishability (with respect to fidelity), with the inner product of the vectors \( \sqrt{p_i} \) and \( \sqrt{q_i} \) being minimal for that POVM.