

Quantum Entanglement, Bell's Inequalities and Quantum Computation

Dharmine Jitendra Jamnadas

Thesis to obtain the Master of Science Degree in

Electrical and Computer Engineering

Supervisors: Prof. Carlos Manuel dos Reis Paiva

Prof. Filipa Isabel Rodrigues Prudêncio

Examination Committee

Chairperson: Prof. José Eduardo Charters Ribeiro da Cunha Sanguino

Supervisors: Prof. Carlos Manuel dos Reis Paiva

Members of the Committee: Prof. Marco Alexandre dos Santos Ribeiro

November 2021

Declaration

I declare that this document is an original work of my authorship and that it fulfills all the requirements of the Code of Conduct and Good Practices of the Universidade de Lisboa.

Abstract

The main objective of this thesis is to provide an overview of some quantum computation concepts.

An important concept is the Quantum Nonlocality concept, which was introduced by an intriguing EPR (Einstein-Podolsky-Rosen) theoretical experiment. This concept was also explored in form of games like the PR (Popescu-Rohrlich) box, and GHZ (Greenberger-Horne-Zeilinger) game to emphasize the power of quantum mechanics. Bell's contribution was fundamental to comprehend that the hidden value argument couldn't be the explanation for the obtained results. This thesis will explore those experiments and games assuring that quantum superposition and quantum entanglement are real by explaining them mathematically.

After presenting the experiments in a form of a card game or show, other concepts of quantum computation, such as linear algebra, quantum bits, quantum measurement, density operator, Bloch sphere representation, quantum gates, quantum parallelism, and the Deutsch algorithm will be clarified.

More complex quantum algorithms only make sense if it solves problems that classical computation algorithms cannot solve. And this is exactly what happens with the large number factorization problem, which today cannot be solved by classical computers and theoretically can be solved by quantum computers. Although this seems to be good, there are some inherent security risks, because today this difficulty is explored to make classical encryption code such as RSA (Rivest-Shamir-Adleman). This thesis will also explain how Shor's Algorithm (which solves the large factoring problem) could be used to break RSA encryption code.

Keywords: Quantum Nonlocality, EPR Experiment, PR Boxes, GHZ Game, Quantum Computation, Shor's Algorithm

Resumo

O principal objetivo desta tese é dar uma visão geral de alguns conceitos de computação quântica.

Um conceito importante é o conceito de não localidade quântica, que foi introduzido pela intrigante experiência teórica EPR (Einstein-Podolsky-Rosen). Este conceito também foi explorado na forma de jogos como as caixas PR (Popescu-Rohrlich) e jogo GHZ (Greenberger-Horne-Zeilinger) para enfatizar o poder da mecânica quântica. A contribuição de Bell foi fundamental para compreender que o argumento do valor oculto não poderia ser a explicação para os resultados obtidos. Esta tese irá explorar essas experiências e jogos provando que a superposição quântica e o entrelaçamento quântico são reais, explicando-os matematicamente.

Após a apresentação das experiências, outros conceitos de computação quântica, como álgebra linear, bits quânticos, medição quântica, operador de densidade, representação da esfera de Bloch, portas quânticas, paralelismo quântico e o algoritmo de Deutsch, são apresentados.

O desenvolvimento de algoritmos quânticos mais complexos só fazem sentido se resolverem problemas que os algoritmos de computação clássica não consigam resolver. E é exatamente isso que acontece com o problema da fatorização de grandes números, que hoje não pode ser resolvido por computadores clássicos e teoricamente pode ser resolvido por computadores quânticos. Embora isso pareça ser bom, existem alguns riscos de segurança inerentes, porque hoje essa dificuldade é explorada para fazer criptografia clássica, como RSA (Rivest-Shamir-Adleman). Esta tese também irá explicar como o Algoritmo de Shor (que resolve o problema da fatoração anteriormente referido) pode ser usado para quebrar o código de criptografia RSA.

Palavras-chave: Não Localidade Quântica, Experiência EPR, Caixas PR, Jogo GHZ, Computação Quântica, Algoritmo de Shor

Acknowledgments

Firstly, I want to thank my supervisor Prof. Carlos Manuel dos Reis Paiva and co-supervisor Prof. Filipa Isabel Rodrigues Prudencio, for their guidance, availability, and all the support provided during this journey.

Additionally, I want to thank my family (especially my parents, my sisters, and my brother-in-law), my friends and my colleagues for their unconditional support.

Without all of them, it wouldn't be possible to achieve this important milestone.

Contents

Declaration	ii
Abstract	iii
Resumo	iv
Acknowledgments	v
Contents	vi
List of figures	viii
List of Tables	x
List of Acronyms	xii
1. Introduction	1
1.1. State of the Art	1
1.2. Objectives/Motivation	3
1.3. Structure	4
1.4. Original contribution.....	5
2. Quantum Nonlocality	6
2.1. Einstein-Podolsky-Rosen thought experiment	6
2.1.1. Concept Definition – Alice and Bob Card Show	6
2.1.2. EPR’s Device	8
2.1.3. Hidden Value Argument.....	9
2.1.4. Quantum Mechanics (QM) Argument.....	11
2.1.5. Quantum Superposition	12
2.1.6. Quantum Entanglement.....	12
2.2. Popescu-Rohrlich (PR) Box.....	15
2.2.1. Concept Definition – Alice and Bob Card Game	15
2.2.2. PR Device	18
2.2.3. Hidden Value Argument.....	18
2.2.4. Quantum Mechanics (QM) Argument.....	21
2.3. Greenberger–Horne–Zeilinger (GHZ) Game.....	23
2.3.1. Concept Definition – Alice, Bob and Charles Card Game.....	23
2.3.2. GHZ Device	24

2.3.3. Hidden Value Argument.....	25
2.3.4. Quantum Mechanics (QM) Approach	28
3. Quantum Computation	31
3.1. Linear Algebra	31
3.2. Qubit	34
3.3. Quantum measurement.....	35
3.4. Density Operator	37
3.5. Bloch Sphere Representation	38
3.6. Quantum Gates Representation.....	40
3.7. Quantum Parallelism	48
3.8. Deutsch's Algorithm	49
4. Shor's Algorithm	53
4.1. Quantum Fourier Transform (QFT)	53
4.2. Quantum Phase Estimation (QPE).....	58
4.3. RSA Protocol	61
4.4. Breaking RSA Protocol	62
4.4.1. Quantum circuit to find period r	63
5. Conclusions and Future Work.....	66
5.1. Conclusions	66
5.2. Future work.....	67
6. References.....	68
Appendix A Malus Law (Quantum interpretation).....	70
A.1 Single-photon.....	70
A.2 Entangled photons	72
Appendix B Pauli Matrices and GHZ state	76

List of figures

Figure 1: Turing Tape with an input value $\{0, 1, 1, 0\}$, with tape head starting at point (q0 state)	1
Figure 2: Turing State diagram to write $fx = x + 1$ on tape	2
Figure 3: Turing Tape with an output value $\{0, 1, 1, 1\}$	2
Figure 4: Von Neumann Architecture	2
Figure 5: Cards $\{1,2,3\}$ given to Alice and Bob	6
Figure 6: Answers that could be written down by Alice or Bob.....	7
Figure 7: A schematic representation of the EPR device and its two detectors.....	9
Figure 8: Settings numbers 1,2 and 3 and respective angles of polarization	14
Figure 9: Cards $\{0,1\}$	15
Figure 10: Answers that could be written down by Alice or Bob.....	15
Figure 11: A schematic representation of the PR device and its two detectors	18
Figure 12: Axes of detector A (x_0 and x_1 with an angle of 45° between them) and B (y_0 and y_1 with an angle of 45° between them).....	21
Figure 13: Polarization filter directions and angles between 4 different values of x and y	22
Figure 14: Cards $\{X,Y\}$	23
Figure 15: Answers that could be written down by Alice, Bob and Charles	23
Figure 16: A schematic representation of the GHZ device and its three detectors	25
Figure 17: Representation of vector ψ	35
Figure 18: Bloch sphere representation of a qubit	40
Figure 19: Circuit and matrix representation of NOT gate (Pauli-X)	41
Figure 20: Circuit and matrix representation of Pauli-Y Gate.....	42
Figure 21: Circuit and matrix representation of Pauli-Z Gate.....	42
Figure 22: Circuit and matrix representation of Hadamard Gate	43
Figure 23: Circuit and matrix representation of Phase Gate	44
Figure 24: Circuit and matrix representation of T Gate	45
Figure 25: Circuit and matrix representation of CNOT Gate	46
Figure 26: Oracle U_f transforming x, y into $ x, y \oplus fx\rangle$	48
Figure 27: Deutsch's circuit	50

Figure 28: UQFT4 represented by an oracle (2 qubits)	55
Figure 29: Decomposing UQFT4 Oracle components → Hadamard Gates	56
Figure 30: Decomposing UQFT4 Oracle components → Hadamard Gates + S Gate	58
Figure 31: Decomposing UQFTN Oracle components → Hadamard Gates + R Gates.....	58
Figure 32: Unitary Control-U Gate.....	59
Figure 33: Hadamard $H \otimes n$ Gate	59
Figure 34: QPE circuit	60
Figure 35: Shor circuit to find period r using oracle $U_{f_a, M}$	63
Figure 36: Shor circuit to find period r	64
Figure 37: The transmitted light's intensity according to the Malus law	70

List of Tables

Table 1: Combination of hidden answer YYY for Cards 123	7
Table 2: Combination of hidden answer YYN for Cards 123.....	7
Table 3: All possible combinations for the hidden values of cards 123	8
Table 4: Individual outcomes and respective combination according to the configuration of settings 1, 2 and 3.....	9
Table 5: Combination of hidden answer GGG for Settings 123	10
Table 6: Combination of hidden answer RRR for Settings 123	10
Table 7: Combination of hidden answer GGR for Settings 123.....	11
Table 8: Rules to score one point in Alice and Bob PR Card Game	16
Table 9: Table of results according to the strategy chosen	17
Table 10: Table of probabilities of scoring according to combination chosen	19
Table 11: Score Combination according to the input of Detector A (x_0, x_1) and B(y_0, y_1).....	20
Table 12: Rules to score one point in Alice and Bob GHZ Card Game.....	24
Table 13: Measurement for the combined value of possible outcomes to succeed.....	25
Table 14: Combined Result ($mabc$) for combination of settings $\{XXX\}$ in Detectors ABC	26
Table 15: Combined Result ($mabc$) for combination of settings $\{XYY\}$ in Detectors ABC	27
Table 16: Combined Result ($mabc$) for combination of settings $\{YXY\}$ in Detectors ABC	27
Table 17: Combined Result ($mabc$) for combination of settings $\{YYX\}$ in Detectors ABC	27
Table 18: Combined Result ($mabc$) for combination of settings $\{XXX; XYY; YXY; YYX\}$ in Detectors ABC	30
Table 19: Representation of Pauli-X outputs in Bloch Sphere according to their inputs $ 0\rangle$ and $ 1\rangle$	41
Table 20: Representation of Pauli-Y outputs in Bloch Sphere according to their inputs $ 0\rangle$ and $ 1\rangle$	42
Table 21: Representation of Pauli-Z outputs in Bloch Sphere according to their inputs $ 0\rangle$ and $ 1\rangle$	43
Table 22: Representation of Hadamard gate outputs in Bloch Sphere according to their inputs $ 0\rangle$ and $ 1\rangle$	44
Table 23: Representation of Phase Gate outputs in Bloch Sphere according to their inputs $ 0\rangle$ and $ 1\rangle$	45
Table 24: Representation of T Gate outputs in Bloch Sphere according to their inputs $ 0\rangle$ and $ 1\rangle$	46

Table 25:Representation of CNOT Gate outputs in Bloch Sphere according to their inputs $|00\rangle$, $|01\rangle$, $|10\rangle$ and $|11\rangle$ 47

Table 26: Four types of function $f(x)$ 49

List of Acronyms

CNOT	Controlled NOT
DFT	Discrete Fourier Transform
EPR	Einstein-Podolsky-Rosen
GHZ	Greenberger–Horne–Zeilinger
POVM	Positive Operator Valued Measure
PR	Popescu-Rohrlich
QFT	Quantum Fourier Transform
QPE	Quantum Phase Estimation
RSA	Rivest–Shamir–Adleman

1.Introduction

1.1.State of the Art

To understand quantum computation it is necessary to go back to the origin of the computer field. It all started with classical computation.

The computer science field started with the theoretical study of algorithms (sequence of computational steps that transform a set of values which can be called input into other sets of values that are called output [1]). The classical computer science field was born in 1936 when Alan Turing [2] attempted to prove that mathematician David Hilbert's decision problem (Entscheidungsproblem) solution was true. In this problem, David Hilbert believed that there was an algorithm that could tell if a proposition was universally valid, given all the axioms of math. Turing developed a model for computation (now known as the Turing machine) that proved Hilbert's decision problem was surprisingly not true. Later, Church–Turing thesis corroborated that any algorithm can be run in a Turing machine. Until this day, if an algorithm cannot be run in the Turing machine, then it's not computable. In fact, even a Turing machine can be simulated in a (Universal) Turing machine.

So, how was an algorithm run in the first version of the Turing machine? The first version of the Turing machine used tapes, divided into squares, to read and write symbols 0 and 1 (which today are called bits). To demonstrate how a simple task is performed in this machine, let's start with an input tape with the following information: {0, 1, 1, 0}, meaning $x = 2$.

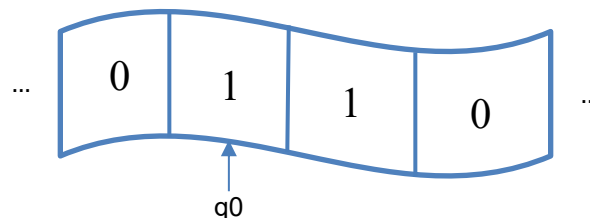


Figure 1: Turing Tape with an input value {0, 1, 1, 0}, with tape head starting at point (q0 state)

The task could be done manually or performed by a tape head that ran throughout the tape and made some operations.

The possible tape head operations from start to the end are:

- Read/Scan symbol below tape head(0/1,_,_)
- Update/Write symbol below tape head(,0/1,_)
- Move the tape head one step right (,_, R)
- Move the tape head one step left (,_, L)

The task could be to receive an input x and calculate a mathematical operation of that input and transform that into an output $f(x)$.

Being the input x (number of 1's) and the output $f(x) = x + 1$, the tape head instructions are as follows:

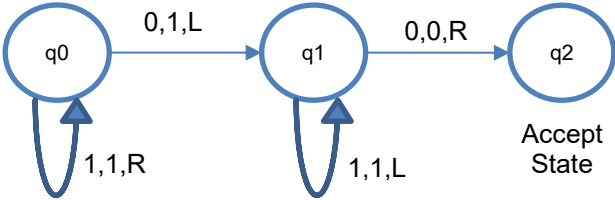


Figure 2: Turing State diagram to write $f(x) = x + 1$ on tape

With these instructions, the originated value on this slice of Tape is the output $f(2) = 3$

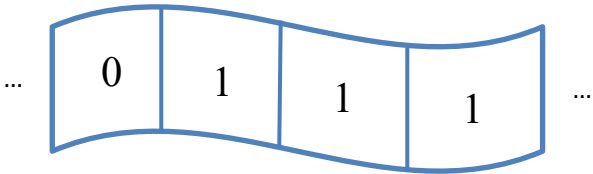


Figure 3: Turing Tape with an output value {0, 1, 1, 1}

Turing Machine is an abstract representation that defines the mathematical model of a computer and this was the first software representation of the computer field.

In 1945, von Neumann proposed a complementary theoretical architecture that would be the baseline to construct a classical computer. The innovation consisted in saving a program and its data in memory before writing the output [3]. The architecture proposed by Von Neumann is now used in all classical computers.

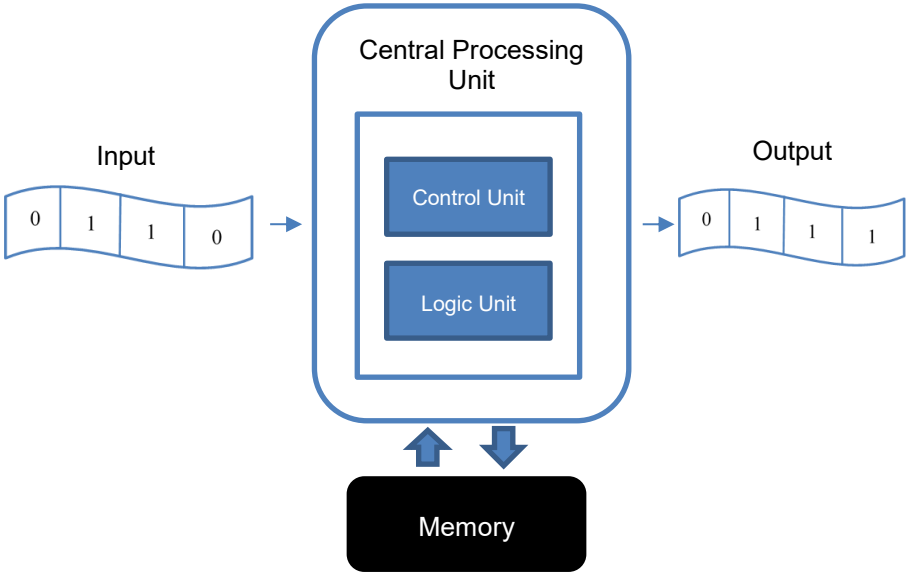


Figure 4: Von Neumann Architecture

Von Neumann architecture contains the following components: a CPU (Central Processing Unit), a memory unit, an input and output devices.

In 1947, John Bardeen, Walter Brattain, and Will Shockley developed the transistor that helped computer hardware to grow rapidly [4]. The growth was so fast that in 1965, Gordon Moore stated that the computer power would increase once every two years, keeping the cost constant (Moore's law) [5]. To increase power one needs to increase the number of transistors in a dense integrated circuit which leads to an increase in the number of components on a single silicon chip. However, this increase is not indefinitely sustainable. As the size of the chip approximates into atomic sizes, the laws of classical physics are challenged making it impossible to make more powerful computers. To overcome these challenges Richard Feynmann initiated a revolutionary thought. He stated that to simulate physical phenomenon's it would be necessary to build quantum computers [6]. Before looking at the definition and specificities of quantum machines, it is relevant to notice that in 1985, David Deutsch introduced an important principle, the Church-Turing-Deutsch principle [7]. He showcased that all physical processes can be simulated through a Quantum Turing machine which consists in a generalization of the previously explained Universal Turing Machine.

Nowadays it is also known that quantum computers can be used beyond the simulation of physical phenomena. Quantum computers can do very specific tasks such as searching in large datasets, assisting in drug development, and supporting traffic route optimization in a significantly shorter time when compared to classical computing. Even though it is true that quantum computers can perform all the tasks of classical computers, it is not true they should be used as a replacement. On one hand, quantum machines are extremely expensive and therefore industry scalability is not viable. On the other hand, using such machines to perform relatively simple (or not overly complex) tasks would not bring relevant gains or benefits for the user (the trade-off between the time saved and the resources/energy allocated to use the computer is not justified).

1.2.Objectives/Motivation

According to the theory, all classical computers are Turing machines and use symbols that can be either 0 or 1, but what about quantum computers? Quantum machines can have symbols that are 0,1 or a superposition of 0 and 1. What exactly is a superposition (atomically represented by particles like photons or electrons)? It is a property that allows the computer to execute many computations at once, giving a big advantage over classical computers. This thesis will explain exactly what it is and how it can be used when constructing an algorithm.

Another property used by quantum computers is known as quantum entanglement. This property provides the abilities described below:

→The ability of subatomic particles to "influence each other", making values collapse in values that could be related between them;

→The ability to know a value by looking into the value of another subatomic particle.

Quantum entanglement differentiates classical and quantum computation and the reason for that to happen is going to be explored in this thesis.

Nowadays, quantum computation solves some problems that were not possible to be solved before, such as the factorization of large prime numbers.

The big problem that emerges is that some cryptographic algorithms such as RSA (Rivest–Shamir–Adleman) take the advantage of the complexity of the factorization of large prime numbers to encrypt information, i.e. the RSA is extremely useful for decoding and encoding secret information over the internet.

The emergence of quantum computation jeopardizes RSA, as it will allow performing complex and challenging tasks such as factorization large prime numbers. As a consequence, the ability to keep information secret or protected is threatened.

1.3.Structure

This thesis is an introduction to a growing field of quantum computation.

The first chapter is a brief initiation to the topic of quantum computation, and the main goal is to be familiarized with the subjects that will be covered in the next chapters.

In the second chapter, Quantum Nonlocality will be explained using the EPR (Einstein-Podolsky-Rosen), PR (Popescu-Rohrlich), and GHZ (Greenberger–Horne–Zeilinger) thought experiments. This chapter is very important to understand the two main concepts used in quantum computation: quantum superposition and quantum entanglement.

The third chapter covers the basic concepts of quantum computation, such as linear algebra, quantum bits, quantum measurement, density operator, Bloch sphere representation, quantum gates, quantum parallelism, and the Deutsch algorithm.

The following chapter, explains how the large number factorization problem could be solved using quantum computation and how this could be used to break RSA (Rivest–Shamir–Adleman) encryption code.

The last chapter is for conclusions and has some considerations about future work that can be developed to better understand the subject of quantum computation.

Lastly, the appendix provides additional information to explore in more depth some of the topics that were presented throughout the chapters.

1.4.Original contribution

With this research, I want to explain comprehensively the topics of quantum nonlocality, as well as quantum computation.

The original contribution is the demonstration and how the topics are organized and explained.

For instance, in chapter two, concepts are introduced through a card show or game. Afterwards, they are explained considering a subatomic experiment. Additionally, both classic and quantum approaches are explained mathematically (with some notes in the appendix).

Further ahead the original contribution is the Bloch Sphere representation of what happens to a qubit 0 or 1 when the quantum gate is applied.

As a final note, in the fourth chapter, the original contribution is the way the topic is mathematically explained.

2. Quantum Nonlocality

Quantum Nonlocality was a very controversial principle when discovered. The topic is counterintuitive being Einstein the first person to find this intriguing.

2.1. Einstein-Podolsky-Rosen thought experiment

Quantum Nonlocality was and still is a counterintuitive principle because it indicates that one particle property can be influenced by a different particle in a faraway distance and this is made instantaneously (meaning in a velocity greater than the velocity of light).

This was so controversial, that Einstein claimed that properties of a particle in region B cannot be affected by properties of another particle on faraway region A, rejecting the so-called spooky actions at a distance [8]. Einstein advocated that each particle should have hidden values and these hidden values would explain the correlation between two separated particles in each region.

This hidden value argument started in a thought experiment made in 1935 by Einstein, Podolsky, and Rosen [9], but it was rejected mathematically by John Bell in 1964 [10] and later on (in the early 1980s) proved wrong experimentally by Alain Aspect [11].

2.1.1. Concept Definition – Alice and Bob Card Show

To better understand Einsteins' hypothesis, a theatrical example will be presented. Two performers called Alice and Bob (example of GianCarlo Ghirardi used in his book [12]) will gather a show where each one receives one of the 3 numbered cards: {1,2,3}, from an audience member.

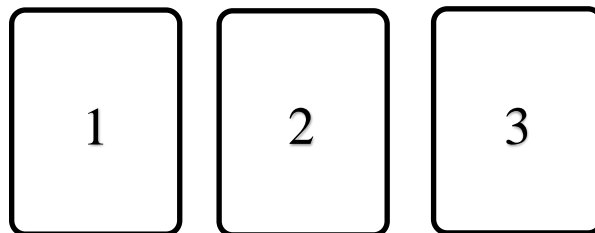


Figure 5: Cards {1,2,3} given to Alice and Bob

After receiving one of the three cards randomly, Alice and Bob have to write one of two possible answers: {Yes, No} on a post-it:



Figure 6: Answers that could be written down by Alice or Bob

It is important to notice they are seated apart from each other and receive the cards randomly from the audience members. Despite that, what happens empirically is that every time they receive the same number, the answers they write are always equal {yes, yes or no, no}.

And this happens every time they perform.

They don't have any type of communication device and as performers, both answer simultaneously.

So, what is happening? The audience could think that this is happening because they know what to answer every time they receive a card to get coordinated responses. Would that be the case?

Considering the hidden value proposition, each card number {1,2,3} has its unique hidden value {yes; no} and this value will help Alice and Bob have coordinated responses.

In the first performance they could have the following combination of hidden values:

Table 1: Combination of hidden answer YYY for Cards 123

1	2	3
Yes	Yes	Yes

Meaning they will always give the same answer (Yes) regardless of the number received (1,2 or 3) by the audience member.

And in the second performance, they could change the combination. The combination used could be:

Table 2: Combination of hidden answer YYN for Cards 123

1	2	3
Yes	Yes	No

Meaning, Alice and Bob will always give the same answer according to the number received 1, 2 or 3:

- If they both receive 1 they will both answer Yes
- If they both receive 2 they will both answer Yes

- If they both receive 3 they will both answer No

In fact, all the combinations that can be used across their performances are described in Table 3:

Table 3: All possible combinations for the hidden values of cards 123

1	2	3
Yes	Yes	Yes
Yes	Yes	No
Yes	No	Yes
Yes	No	No
No	Yes	Yes
No	Yes	No
No	No	Yes
No	No	No

The below subchapters main goal is to understand if the hidden value is true for the subatomic world, through Einstein, Podolsky and Rosen (EPR) thought experiment.

2.1.2.EPR's Device

In this experiment, we have one device that produces two independent particles that go to opposite sides in each run. One goes to region A (Detector A) and the other to region B (Detector B). In each run, both particles collapse in different detectors with 3 different settings (1, 2 and 3) and the outcome will be one of the following light colors: Green or Red (G or R).

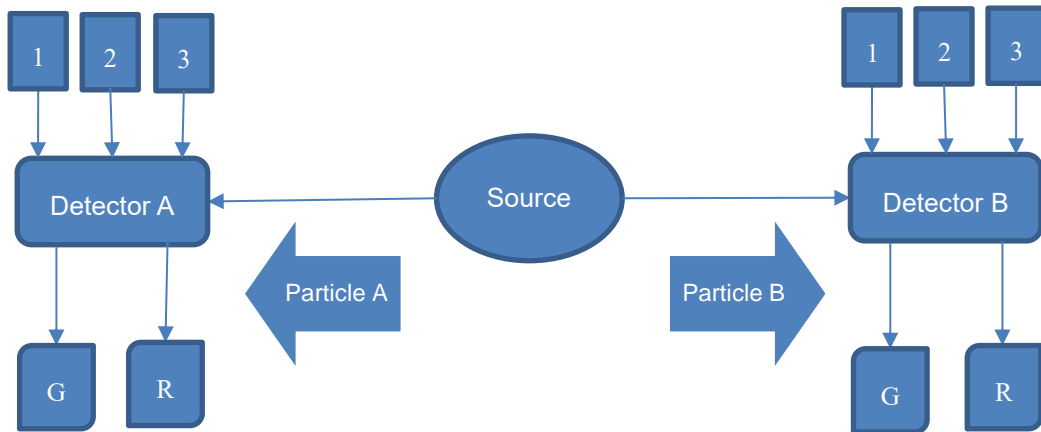


Figure 7: A schematic representation of the EPR device and its two detectors

After millions of runs, the two main conclusions were:

1. When both switches have the same setting, the outcome is always the same color;
2. The likelihood of the outcome being the same colors or different colors is equal

Linking Alice and Bob Show to this subatomic device, it's possible to deduce that the card numbers represent the settings on the detectors A (Alice) and B (Bob) and the output green and red represent the answers written by Alice and Bob (Yes and No).

2.1.3. Hidden Value Argument

The hypothesis for explaining the correlation between colors of different regions is the hidden value proposition which stated that the particles have values before they leave the device. There are no links or communication between two particles after they leave the device (source). The detectors are also independent. Table 4 presents the possible outcomes (outputs) according to the inputs (settings) for each particle, once they collapse on each of their detectors.

Table 4: Individual outcomes and respective combination according to the configuration of settings 1, 2 and 3

	1	2	3
G	G	G	G
G	G	G	R
G	G	R	G
G	G	R	R

R	G	G
R	G	R
R	R	G
R	R	R

The assumption is: the outcome for one particle has a hidden value associated to the combination of detector settings and the collapse of the particle. To check if there is any type of correlation between the setting and the light color, it is necessary to check the combination of settings of both detectors: {11; 12; 13; 21; 22; 23; 31; 32; 33} and their individual outcomes {G; R}. By performing this analysis, conclusion 2. 'The likelihood of the outcome being the same colors or different colors is equal' will be tested.

Each run can be represented by {12GR} and this means that the setting in detector A is 1 and the outcome color is Green and the setting in detector B is 2 and the outcome color is Red.

In the first row of Table 4 (row represented again in Table 5), we have (GGG) for any kind of setting (123), which means that the two particles (A and B) will flash the same color G in each run.

Table 5: Combination of hidden answer GGG for Settings 123

1	2	3
G	G	G

$$\{11GG; 12GG; 13GG; 21GG; 22GG; 23GG; 31GG; 32GG; 33GG\} \rightarrow P_{\text{hiddenvalue}}(\text{same color} \mid GGG) = \frac{9}{9} = 1$$

Where $P_{\text{hiddenvalue}}(\text{same color} \mid GGG)$ can be read as the probability of flashing the same color knowing that the hidden value in setting 123 is GGG.

Probability of 1 means that all runs have the same color output.

In the last row of Table 4 (row represented again in Table 6), we have (RRR) for any kind of setting (123), which means that the two particles (A and B) will flash the same color R in each run.

Table 6: Combination of hidden answer RRR for Settings 123

1	2	3
R	R	R

$$\{11RR; 12RR; 13RR; 21RR; 22RR; 23RR; 31RR; 32RR; 33RR\} \rightarrow P_{\text{hiddenvalue}}(\text{same color} | RRR) = \frac{9}{9} = 1$$

(Probability of 1 means that all runs have the same color output).

For the second row we have (GGR) for setting (123), which means that the two particles (A and B) will flash the same color in some of the runs.

Table 7: Combination of hidden answer GGR for Settings 123

1	2	3
G	G	R

$$\{11GG; 12GG; 21GG; 22GG; 33RR\} \rightarrow P_{\text{hiddenvalue}}(\text{same color} | GGR) = \frac{5}{9}.$$

Applying the same logic for the remaining rows of Table 4 one conclusion stands out:

$$P_{\text{hiddenvalue}}(\text{Same color}) \geq \left(\frac{5}{9}\right) \quad (2.1)$$

This contradicts the conclusion from earlier subchapter: 2. 'The likelihood of the outcome being the same colors or different colors is equal.'

Because If

$$P_{\text{hiddenvalue}}(\text{Same color}) + P_{\text{hiddenvalue}}(\text{Different color}) = 1 \quad (2.2)$$

And

$$P_{\text{hiddenvalue}}(\text{Same color}) \geq \frac{5}{9} \quad (2.3)$$

Then

$$P_{\text{hiddenvalue}}(\text{Same color}) \neq P_{\text{hiddenvalue}}(\text{Different color}) \quad (2.4)$$

For this reason, Bell concludes that the hidden value proposition cannot be true, meaning that there is no hidden value in each particle once they leave the source.

2.1.4. Quantum Mechanics (QM) Argument

If there is no hidden value in each particle before it leaves the source, a new hypothesis arises - both particles should be influenced by each other somehow and the particle does not have value until it collapses. This means that the particle is in superposition form before it collapses.

2.1.5. Quantum Superposition

To represent a particle, Dirac notation will be used (also known as bracket notation).

In this form, one particle is represented by ket $|\psi\rangle$:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \quad \alpha, \beta \in \mathbb{C} \quad (2.5)$$

Where α and β are the amplitudes with probabilities of $|\alpha|^2$ and $|\beta|^2$ being $|\alpha|^2 + |\beta|^2 = 1$.

In this particular example, $|0\rangle$ represents horizontally (\rightarrow) polarized amplitude and $|1\rangle$ represents vertically (\uparrow) polarized amplitude. If a particle is only represented by one amplitude then the particle is vertically or horizontally polarized being the other amplitude 0.

2.1.6. Quantum Entanglement

Each particle has its properties. So particle A is represented with $|\psi\rangle_A$ and Particle B with $|\psi\rangle_B$

$$|\psi\rangle_A = \alpha_A|0\rangle_A + \beta_A|1\rangle_A, \quad \alpha, \beta \in \mathbb{C} \quad (2.6)$$

$$|\psi\rangle_B = \alpha_B|0\rangle_B + \beta_B|1\rangle_B, \quad \alpha, \beta \in \mathbb{C} \quad (2.7)$$

But when particles are entangled both states are inseparable, hence cannot be studied as separate states.

Which leads to a combined state represented by $|\Psi\rangle_{AB}$:

$$|\Psi\rangle_{AB} = C_{00}(|0\rangle_A \otimes |0\rangle_B) + C_{01}(|0\rangle_A \otimes |1\rangle_B) + C_{10}(|1\rangle_A \otimes |0\rangle_B) + C_{11}(|1\rangle_A \otimes |1\rangle_B) \quad (2.8)$$

And the new state can simply be represented as:

$$|\Psi\rangle_{AB} = C_{00}|00\rangle_{AB} + C_{01}|01\rangle_{AB} + C_{10}|10\rangle_{AB} + C_{11}|11\rangle_{AB}, \quad C_{00}, C_{01}, C_{10}, C_{11} \in \mathbb{C} \quad (2.9)$$

And in this case, particles generated are entangled photons.

For entangled photons:

$$|C_{01}|^2 = |C_{10}|^2 = 0 \quad (2.10)$$

And

$$|C_{00}|^2 + |C_{11}|^2 = 1 \quad (2.11)$$

Hence

$$|C_{00}|^2 + |C_{01}|^2 + |C_{10}|^2 + |C_{11}|^2 = 1 \quad (2.12)$$

If $|C_{00}|^2 = |C_{11}|^2$ (meaning that probability of both particles A and B having same polarization $|00\rangle$ or $|11\rangle$ are equal) then:

$$|C_{00}|^2 + |C_{11}|^2 = 1 \quad (2.13)$$

$$|C_{11}|^2 + |C_{11}|^2 = 1 \quad (2.14)$$

$$2|C_{11}|^2 = 1 \quad (2.15)$$

$$C_{11} = \frac{1}{\sqrt{2}} \quad (2.16)$$

The final state is then, simply represented by:

$$|\Psi\rangle_{AB} = \frac{1}{\sqrt{2}} [|00\rangle_{AB} + |11\rangle_{AB}] \quad (2.17)$$

This example also proves that $C_{00} \neq \alpha_A \cdot \alpha_B$, $C_{01} \neq \alpha_A \cdot \beta_B$, $C_{10} \neq \beta_A \cdot \alpha_B$ and $C_{11} \neq \beta_A \cdot \beta_B$ because if

$$C_{01} = 0 \rightarrow \alpha_A \cdot \beta_B = 0 \text{ (means that either } \alpha_A \text{ or } \beta_B \text{ are equal 0)} \quad (2.18)$$

$$C_{10} = 0 \rightarrow \beta_A \cdot \alpha_B = 0 \text{ (means that either } \beta_A \text{ or } \alpha_B \text{ are equal 0)} \quad (2.19)$$

Then we cannot have $C_{00} = \alpha_A \cdot \alpha_B \neq 0$ and $C_{11} = \beta_A \cdot \beta_B \neq 0$

$$C_{00} \neq 0 \rightarrow \alpha_A \cdot \alpha_B \neq 0 \text{ (means that neither } \alpha_A \text{ or } \alpha_B \text{ could be equal 0)} \quad (2.20)$$

$$C_{11} \neq 0 \rightarrow \beta_A \cdot \beta_B \neq 0 \text{ (means that neither } \beta_A \text{ or } \beta_B \text{ could be equal 0)} \quad (2.21)$$

As there are three settings, this means that there are three types of polarization filters. Each filter is polarized at a very specific angle. If the angle of polarization of the particle is the same as the polarization filter the particle goes through the filter (the outcome is Green), otherwise it's blocked (the outcome is Red). The particle only defines its orientation once it collapses on the filter.

The three settings number are represented in Figure 8 by their respective angles of polarization. Each of the settings (1, 2 or 3) has two angles representation because they could have one of the two directions represented.

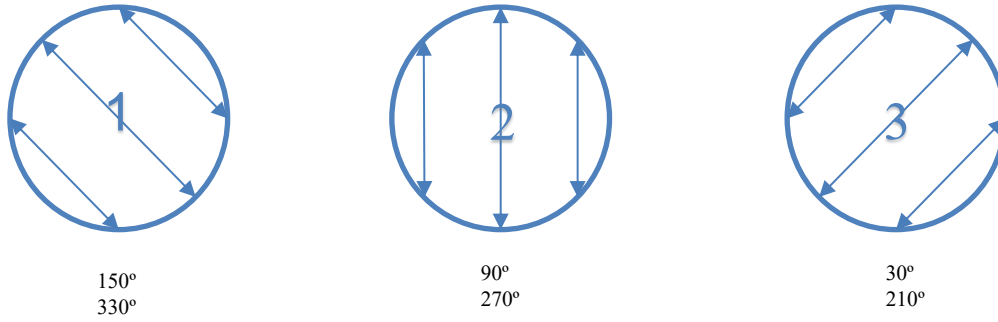


Figure 8: Settings numbers 1,2 and 3 and respective angles of polarization

According to the Malus Law, the probability of having the same outcome is given by (details in Appendix A.1/A.2):

$$P(\theta) = \cos^2(\theta) \quad (2.22)$$

$$\theta = \theta_B - \theta_A \quad (2.23)$$

Where θ is the difference between the angle of particle B and particle A once they collapse the filter.

If the settings are the same {11;22;33} they will flash the same color because $P(0^\circ) = \cos^2(0^\circ) = 1$.

If the settings are different {12;13;21;23;31;32} the particles have the probability of flashing the same according to $P(\pm 300^\circ) = P(\pm 240^\circ) = P(\pm 120^\circ) = P(\pm 60^\circ) = \cos^2(60^\circ) = \frac{1}{4}$.

Which leads to

$$P_{QM}(\text{Same color}) \quad (2.24)$$

$$= P(\text{Same Setting}).P(\text{flashing same color} | \text{same setting}) \\ + P(\text{Different Setting}).P(\text{flashing same color} | \text{Different Setting})$$

$$P_{QM}(\text{Same color}) = \frac{3}{9} \cdot 1 + \frac{6}{9} \cdot \frac{1}{4} = \frac{1}{3} + \frac{1}{6} = \frac{1}{2} \quad (2.25)$$

Therefore, according to the quantum mechanics hypothesis, the outcome same colors in both detectors is as likely as different colors, not contradicting the EPR experiment.

$$P_{QM}(\text{Same color}) + P_{QM}(\text{Different color}) = 1 \quad (2.26)$$

$$P_{QM}(\text{Same color}) = P_{QM}(\text{Different color}) = \frac{1}{2} \quad (2.27)$$

2.2. Popescu-Rohrlich (PR) Box

Popescu and Rohrlich invented a theoretical device [13] that today is also known as PR boxes. These boxes are presented as game boxes to demonstrate one more time that the hidden value argument proposed by Einstein does not explain the results obtained in a subatomic world.

In the next subchapter, the experiment is presented in the form of a card game to get familiarized with the concepts. The results of the hidden values argument will be compared with the quantum mechanics values argument (in a subatomic world). The main objective is to see which strategy is better to win the game.

2.2.1. Concept Definition – Alice and Bob Card Game

Starting with the rules of the game, two players (Alice and Bob) will each receive one of 2 numbered cards: $\{0,1\}$ randomly.

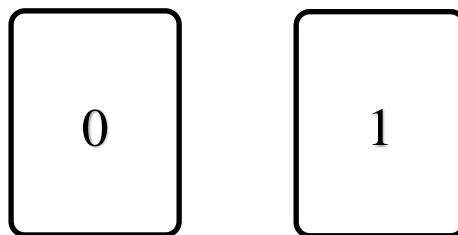


Figure 9: Cards $\{0,1\}$

After receiving one of two options randomly Alice and Bob should write one of two answers: $\{\text{zero}, \text{one}\}$ on a post-it:

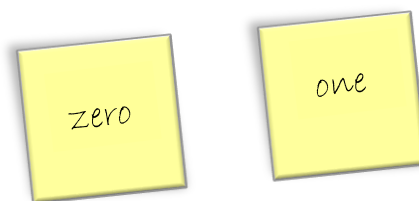


Figure 10: Answers that could be written down by Alice or Bob

They are seated apart from each other, receive the cards randomly in each run, and respectively write an answer. The main objective is to get a maximum score without communicating with each other. Each one gets 1 point in each run if the conditions in Table 8 are satisfied:

Table 8: Rules to score one point in Alice and Bob PR Card Game

	Alice Receive Card 0	Alice Receive Card 1
Bob Receive Card 0	Alice and Bob write the same answer	Alice and Bob write the same answer
Bob Receive Card 1	Alice and Bob write the same answer	Alice and Bob write different answers

What is the best strategy to win the game? For this purpose one of the following strategies could be used:

- A. Write always the answer zero;
- B. Write always the answer one;
- C. Write always the same number as the card received:
 - If the card number is 0 it's written zero;
 - If the card number is 1 it's written one;
- D. Write always the opposite number as the card received:
 - If the card number is 0 it's written one;
 - If the card number is 1 it's written zero;

Both Alice and Bob could use different strategies in each run {A, B, C, D}.

There are 16 possible combinations, as shown in Table 9.

Additionally, each card received (input) by Alice, is represented with values $x \{0 \text{ or } 1\}$ and each card received (input) by Bob with values $y \{0 \text{ or } 1\}$. Each answer (output) given by Alice is represented by values $a \{0 \text{ or } 1\}$ and each answer given by Bob is represented by values $b \{0 \text{ or } 1\}$.

Table 9: Table of results according to the strategy chosen

Alice Strategy	Bob Strategy	Results for x=0 and y=0	Results for x=0 and y=1	Results for x=1 and y=0	Results for x=1 and y=1	Maximum score possible
A	A	a = 0;b = 0	a = 0;b = 0	a = 0;b = 0	a = 0;b = 0	3
A	B	a = 0;b = 1	a = 0;b = 1	a = 0;b = 1	a = 0;b = 1	1
A	C	a = 0;b = 0	a = 0;b = 1	a = 0;b = 0	a = 0;b = 1	3
A	D	a = 0;b = 1	a = 0;b = 0	a = 0;b = 1	a = 0;b = 0	1
B	A	a = 1;b = 0	a = 1;b = 0	a = 1;b = 0	a = 1;b = 0	1
B	B	a = 1;b = 1	a = 1;b = 1	a = 1;b = 1	a = 1;b = 1	3
B	C	a = 1;b = 0	a = 1;b = 1	a = 1;b = 0	a = 1;b = 1	1
B	D	a = 1;b = 1	a = 1;b = 0	a = 1;b = 1	a = 1;b = 0	3
C	A	a = 0;b = 0	a = 0;b = 0	a = 1;b = 0	a = 1;b = 0	3
C	B	a = 0;b = 1	a = 0;b = 1	a = 1;b = 1	a = 1;b = 1	1
C	C	a = 0;b = 0	a = 0;b = 1	a = 1;b = 0	a = 1;b = 1	1
C	D	a = 0;b = 1	a = 0;b = 0	a = 1;b = 1	a = 1;b = 0	3
D	A	a = 1;b = 0	a = 1;b = 0	a = 0;b = 0	a = 0;b = 0	1
D	B	a = 1;b = 1	a = 1;b = 1	a = 0;b = 1	a = 0;b = 1	1
D	C	a = 1;b = 0	a = 1;b = 1	a = 0;b = 0	a = 0;b = 1	3
D	D	a = 1;b = 1	a = 1;b = 0	a = 0;b = 1	a = 0;b = 0	1

In the next subchapters, through a thought experiment using a device that produces two photons, the probabilities of succeeding in this game will be calculated. Two arguments are applied: the hidden values argument and the quantum mechanics argument. The main goal is to evaluate the best approach to win the game.

2.2.2. PR Device

In this thought experiment, we have one device very similar to the EPRs device. The PR device produces two independent photons in each run that goes to opposite sides. One goes to region A (Detector A) and the other goes to region B (Detector B). In each run, both photons collapse in different detectors with 2 different polarization filters (0, 1) and the outcome will be one of the following values: (0, 1).

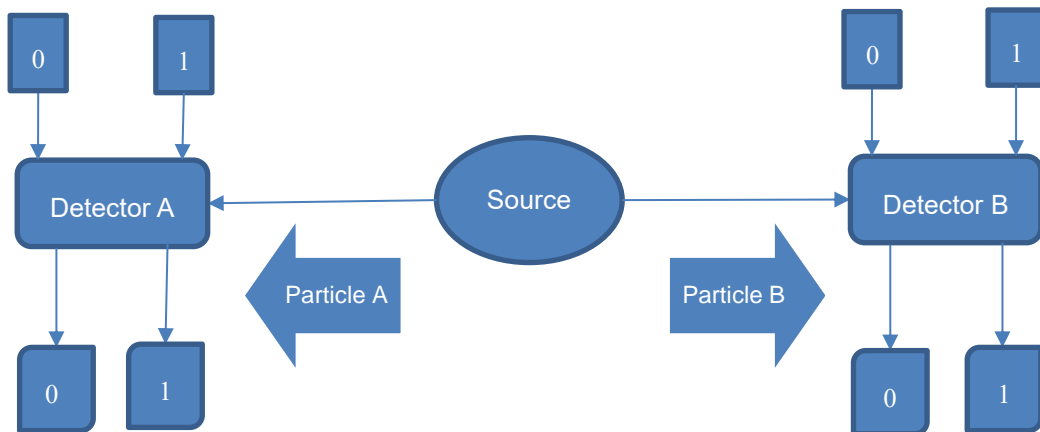


Figure 11: A schematic representation of the PR device and its two detectors

2.2.3. Hidden Value Argument

Table 10 shows the possible outcomes (outputs) according to the inputs (settings), for each particle, once they collapse on each of their detectors if a hidden values argument is used.

In the first two columns, the assumption is that both photons have a hidden polarization defined, once they leave the source and that this will define if the photon goes through or if it is blocked once it collapses on the polarization filter:

- A. The Photon is always blocked by the polarization filter (independently of its value) meaning that the outcome value on the detector is always 0;
- B. The Photon always passes by polarization filter (independently of its value) meaning that the outcome value on the detector is always 1;
- C. The Photon is blocked or passes by a polarization filter according to the value of the polarization filter:
 - If the polarizer has a value of 0 the photon is blocked meaning that the outcome value on the detector is always 0;
 - If the polarizer has a value of 1 the photon passes, meaning that the outcome value on the detector is always 1;
- D. The Photon is blocked or passes by a polarization filter according to the opposite value of the polarization filter:
 - If the polarizer has a value of 0 the photon passes, meaning that the outcome value on the detector is always 1;

- If the polarizer has a value of 1 the photon is blocked, meaning that the outcome value on the detector is always 0.

The value x represents the value of the setting of detector A and y the value of the setting of detector B. Value a is the value of the outcome in detector A and b is the outcome value in detector B.

Table 10: Table of probabilities of scoring according to combination chosen

Photon hidden's value	A	Photon hidden's value	B	Results for $x=0$ and $y=0$	Results for $x=0$ and $y=1$	Results for $x=1$ and $y=0$	Results for $x=1$ and $y=1$	Probability of Scoring
A		A		$a = 0; b = 0$	$a = 0; b = 0$	$a = 0; b = 0$	$a = 0; b = 0$	$P_{hv}(\text{Score}) = \frac{3}{4}$
A		B		$a = 0; b = 1$	$a = 0; b = 1$	$a = 0; b = 1$	$a = 0; b = 1$	$P_{hv}(\text{Score}) = \frac{1}{4}$
A		C		$a = 0; b = 0$	$a = 0; b = 1$	$a = 0; b = 0$	$a = 0; b = 1$	$P_{hv}(\text{Score}) = \frac{3}{4}$
A		D		$a = 0; b = 1$	$a = 0; b = 0$	$a = 0; b = 1$	$a = 0; b = 0$	$P_{hv}(\text{Score}) = \frac{1}{4}$
B		A		$a = 1; b = 0$	$a = 1; b = 0$	$a = 1; b = 0$	$a = 1; b = 0$	$P_{hv}(\text{Score}) = \frac{1}{4}$
B		B		$a = 1; b = 1$	$a = 1; b = 1$	$a = 1; b = 1$	$a = 1; b = 1$	$P_{hv}(\text{Score}) = \frac{3}{4}$
B		C		$a = 1; b = 0$	$a = 1; b = 1$	$a = 1; b = 0$	$a = 1; b = 1$	$P_{hv}(\text{Score}) = \frac{1}{4}$
B		D		$a = 1; b = 1$	$a = 1; b = 0$	$a = 1; b = 1$	$a = 1; b = 0$	$P_{hv}(\text{Score}) = \frac{3}{4}$
C		A		$a = 0; b = 0$	$a = 0; b = 0$	$a = 1; b = 0$	$a = 1; b = 0$	$P_{hv}(\text{Score}) = \frac{3}{4}$
C		B		$a = 0; b = 1$	$a = 0; b = 1$	$a = 1; b = 1$	$a = 1; b = 1$	$P_{hv}(\text{Score}) = \frac{1}{4}$

C	C	a = 0;b = 0	a = 0;b = 1	a = 1;b = 0	a = 1;b = 1	$P_{hv}(Score)$ $= \frac{1}{4}$
C	D	a = 0;b = 1	a = 0;b = 0	a = 1;b = 1	a = 1;b = 0	$P_{hv}(Score)$ $= \frac{3}{4}$
D	A	a = 1;b = 0	a = 1;b = 0	a = 0;b = 0	a = 0;b = 0	$P_{hv}(Score)$ $= \frac{1}{4}$
D	B	a = 1;b = 1	a = 1;b = 1	a = 0;b = 1	a = 0;b = 1	$P_{hv}(Score)$ $= \frac{3}{4}$
D	C	a = 1;b = 0	a = 1;b = 1	a = 0;b = 0	a = 0;b = 1	$P_{hv}(Score)$ $= \frac{3}{4}$
D	D	a = 1;b = 1	a = 1;b = 0	a = 0;b = 1	a = 0;b = 0	$P_{hv}(Score)$ $= \frac{1}{4}$

In this table the $P_{hv}(Score|line_combination)$ is calculated, similarly, in each line.

Bellow the example, where $line_combination = AA$ (first line of the table)

$$P_{hv}(Score|AA) = \frac{Score_{AA_Total}}{N_{AA_Total}} \quad (2.28)$$

$$= \frac{Score_{AA}(x = 0; y = 0) + Score_{AA}(x = 0; y = 1) + Score_{AA}(x = 1; y = 0) + Score_{AA}(x = 1; y = 1)}{N_{AA_Total}}$$

N_{AA_Total} is the number total of possible choices and $Score_{AA_Total}$ is the sum of each score: $Score_{AA}(x = 0; y = 0)$, $Score_{AA}(x = 0; y = 1)$, $Score_{AA}(x = 1; y = 0)$ and $Score_{AA}(x = 1; y = 1)$. Each score value is calculated accordingly to Table 11.

Table 11: Score Combination according to the input of Detector A (x_0, x_1) and B (y_0, y_1)

	x=0 (x_0)	x=1 (x_1)
y=0 (y_0)	If a=b, then score = 1 else score = 0	If a=b, then score = 1 else score = 0
y=1 (y_1)	If a=b, then score = 1 else score = 0	If a≠ b, then score = 1 else score = 0

In the remaining rows ($line_combination \in \{AB, AC, AD, BA, BB, BC, BD, CA, CB, CC, CD, DA, DB, DC, DD\}$), the same logic of the first row is used ($line_combination = AA$).

In conclusion :

$$P_{\text{hiddenvalue}}(\text{Score}) \leq \left(\frac{3}{4}\right) \quad (2.29)$$

$$P_{\text{hiddenvalue}}(\text{Score}) \leq 75\% \quad (2.30)$$

This means that in the best case scenario it is possible to win the game 3 out of 4 times (75%) using the hidden value proposition.

2.2.4. Quantum Mechanics (QM) Argument

In the previous subchapter was demonstrated that the maximum probability of scoring (running a successful simulation) using the hidden value proposition was $\frac{3}{4}$. In this subchapter, the same probability will be calculated using the quantum mechanics proposition.

As seen in the EPRs subchapter, both photons are entangled and cannot be studied individually. They will leave the source in the following state.

$$|\Psi\rangle_{AB} = \frac{1}{\sqrt{2}} [|00\rangle_{AB} + |11\rangle_{AB}] \quad (2.31)$$

They are in a superposition state and the only thing that is possible to conclude before their collapse in their respective detectors is that they both have $\frac{1}{2}$ chances of collapsing as 0 (blocked) and $\frac{1}{2}$ chances of collapsing as 1 (passing through the polarizer). Both photons, A and B, will have the same polarization once they collapse on detectors. The outcome will be 0 or 1 according to the polarization of the filters settings on Detector A and Detector B.

In this example, polarization filters (represented by the settings) have different axes in both detectors. Detector A is represented by either $x = 0$ or $x = 1$ (with an angle of 45° between them). Detector B is represented by either $y = 0$ or $y = 1$ (with an angle of 45° between them).

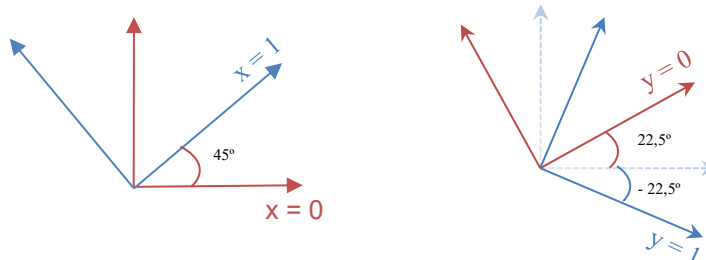


Figure 12: Axes of detector A (x_0 and x_1 with an angle of 45° between them) and B (y_0 and y_1 with an angle of 45° between them)

Figure 13 demonstrates the angle between axes of Detector A and B altogether.

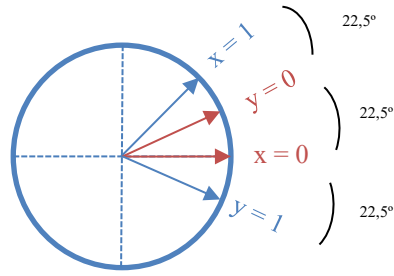


Figure 13: Polarization filter directions and angles between 4 different values of x and y

According to the Malus Law, the probability of having the same outcome is given by (details in Appendix A.1/A.2):

$$P_s = \cos^2(\theta) \quad (2.32)$$

$$\theta = \theta_B - \theta_A \quad (2.33)$$

Where θ is the difference between the angle of particle B and particle A once they collapse the filter.

Following the same law, the probability of having a different outcome is given by (details in Appendix A.1/A.2):

$$P_d = \sin^2(\theta) \quad (2.34)$$

$$\theta = \theta_B - \theta_A \quad (2.35)$$

Referring back to Figure 13, if the combination of the settings in detector A and B are $\{00;01;10\}$ then the probability of having the same outcome is given by $P_s(22,5^\circ) = \cos^2(22,5^\circ)$.

If the settings are $\{11\}$ the probability of having the different outcome is $P_d(67,5^\circ) = \sin^2(67,5^\circ) = \cos^2(22,5^\circ)$.

This leads to:

$$P_{QM}(Score) = P(x_0; y_0).P(a = b | x_0; y_0) + P(x_0; y_1).P(a = b | x_0; y_1) + P(x_1; y_0).P(a = b | x_1; y_0) + P(x_1; y_1).P(a \neq b | x_1; y_1) \quad (2.36)$$

$$P_{QM}(Score) = \frac{1}{4} \cdot \cos^2(22,5^\circ) + \frac{1}{4} \cdot \cos^2(22,5^\circ) + \frac{1}{4} \cdot \cos^2(22,5^\circ) + \frac{1}{4} \cdot \sin^2(67,5^\circ) \quad (2.37)$$

$$P_{QM}(Score) = \cos^2(22,5^\circ) = \frac{1}{4}(2 + \sqrt{2}) \approx 85\% \quad (2.38)$$

In conclusion, we have a better probability of scoring using quantum mechanics preposition than using hidden values preposition.

$$P_{\text{hiddenvalue}}(\text{Score}) < P_{QM}(\text{Score}) \quad (2.39)$$

2.3.Greenberger–Horne–Zeilinger (GHZ) Game

The Greenberger–Horne–Zeilinger (GHZ) experiment is another important experiment that explains nonlocality with an entanglement involving three particles. This leads to a new state (state of three entangled particles) proposed in 1989, by the article Bell's theorem without inequalities [14], in which statistical analysis is not required to contradict hidden variables theory, showing the accuracy of quantum mechanics argument.

2.3.1.Concept Definition – Alice, Bob and Charles Card Game

Starting with the rules of the game, three players (Alice, Bob and Charles) receive one of the 2 cards {X, Y} randomly.

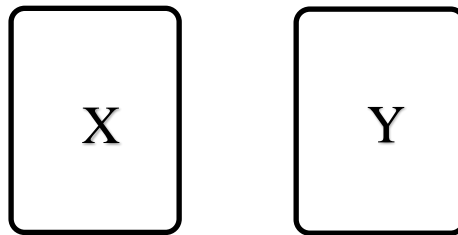


Figure 14: Cards {X,Y}

After receiving one of the two options randomly, each player (Alice, Bob and Charles) should write one of two possible answers: {-1, +1} on a post-it:



Figure 15: Answers that could be written down by Alice, Bob and Charles

They are seated apart from each other and receive the cards randomly, in each run. After that, they write an answer separately in a post-it. The main objective is to get a maximum score without communicating with each other. Each gets one point in every run if the conditions below are satisfied:

1. Alice, Bob, and Charles, all receive card X and an odd number of +1 is written as their answers (either one player writes +1 and others writes -1 or all write +1).

- Two out of three players (Alice, Bob, or Charles) receives card Y and the remaining one receives the card X and an even number of +1 is written in the answers (either two players write +1 and the other writes -1 or no one writes +1).

Table 12 summarizes the conditions to get one point.

In the table a is the output value of Alice, b is the output value of Bob, and c is the output value of Charles. Also, r is the input value for Alice, s is the input value for Bob and t the input value for Charles.

Table 12: Rules to score one point in Alice and Bob GHZ Card Game

Alice Input	Bob Input	Charles Input	Condition to win 1 point	Possible outputs to gain one point (a, b, c)
$r = X$	$s = X$	$t = X$	ODD number of +1's as output	$(+1, +1, +1)$ $(+1, -1, -1)$ $(-1, +1, -1)$ $(-1, -1, +1)$
$r = X$	$s = Y$	$t = Y$	EVEN number of +1's as output	$(+1, +1, -1)$ $(+1, -1, +1)$ $(-1, +1, +1)$ $(-1, -1, -1)$
$r = Y$	$s = X$	$t = Y$	EVEN number of +1's as output	$(+1, +1, -1)$ $(+1, -1, +1)$ $(-1, +1, +1)$ $(-1, -1, -1)$
$r = Y$	$s = Y$	$t = X$	EVEN number of +1's as output	$(+1, +1, -1)$ $(+1, -1, +1)$ $(-1, +1, +1)$ $(-1, -1, -1)$

Is there any way to always win the game using a hidden value argument? And what happens if the quantum mechanics argument is used?

In the next subchapters, through a thought experiment using a device that produces photons, these 2 questions will be answered.

2.3.2.GHZ Device

This device has a source that produces three photons, one goes to region A (Detector A), the second goes to region B (Detector B) and the third goes to region C (Detector C). In each run, three photons collapse in different detectors with 2 different polarization filters (X, Y) and the outcome will be one of the following values: (+1, -1).

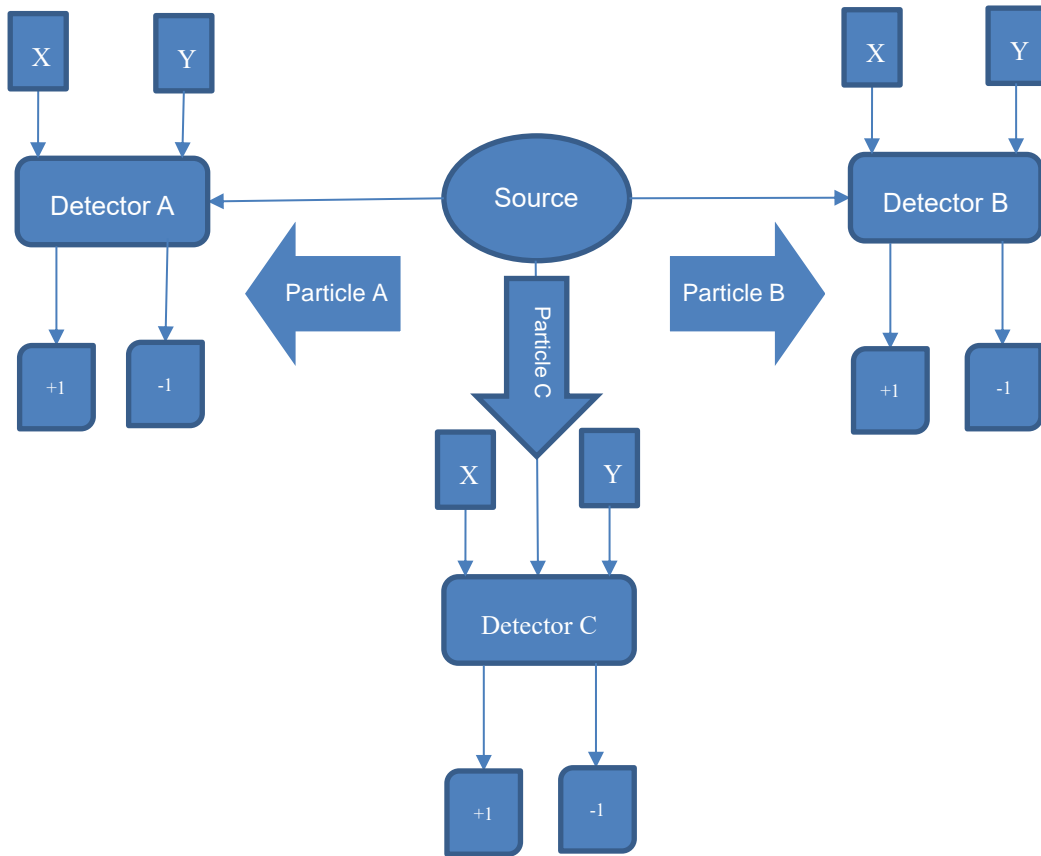


Figure 16: A schematic representation of the GHZ device and its three detectors

2.3.3. Hidden Value Argument

Table 13 shows the combined outcomes (outputs), according to the inputs (settings) for each particle once they collapse on each of their detectors if a hidden values argument is used.

Table 13: Measurement for the combined value of possible outcomes to succeed

Setting (r) in detector A	Setting (s) in detector B	Setting (t) in detector C	Condition to succeed	Measurement for the combined value of possible outcomes to succeed $m_{abc} = (a \times b \times c)$
$r = X$	$s = X$	$t = X$	ODD number of +1's as output	$+1 \times +1 \times +1 = +1$ $+1 \times -1 \times -1 = +1$ $-1 \times +1 \times -1 = +1$ $-1 \times -1 \times +1 = +1$
$r = X$	$s = Y$	$t = Y$	EVEN number of	$+1 \times +1 \times -1 = -1$ $+1 \times -1 \times +1 = -1$ $-1 \times +1 \times +1 = -1$ $-1 \times -1 \times -1 = -1$

			+1's as output	
$r = Y$	$s = X$	$t = Y$	EVEN number of +1's as output	$+1 \times +1 \times -1 = -1$ $+1 \times -1 \times +1 = -1$ $-1 \times +1 \times +1 = -1$ $-1 \times -1 \times -1 = -1$
$r = Y$	$s = Y$	$t = X$	EVEN number of +1's as output	$+1 \times +1 \times -1 = -1$ $+1 \times -1 \times +1 = -1$ $-1 \times +1 \times +1 = -1$ $-1 \times -1 \times -1 = -1$

The detectors could have settings X or Y (polarized filters in x or y-direction).

The individual values of measurement (a, b or c) could be either +1 (photon passes through the polarizer) or -1 (photon is blocked).

The combined value of the outcome m_{abc} is a multiplication of their values a, b and c .

In summary, although there are 8 possible arrangements $\{XXX; XYY; YXY; YYX; YXX; XYX; XXY; YYY\}$, there are only 4 arrangements of settings with relevant useful information in the context under study $\{XXX; XYY; YXY; YYX\}$.

Choosing the value for X in detectors A, B and C of +1, it is easy to conclude that the combined measurement is +1.

Table 14: Combined Result (m_{abc}) for combination of settings $\{XXX\}$ in Detectors ABC

Detector A Input	Detector B Input	Detector C Input	Detector A Output	Detector B Output	Detector C Output	Result $m_{abc} = (a \times b \times c)$
X	X	X	+1	+1	+1	+1

This means that, to continue to have a successful simulation the output of detectors B and C, knowing that Y is the input for both, should have opposite values of output (one should have +1 and the other should have value -1), because the combined value should be -1 ($m_{abc} = a \times b \times c = -1$). It is possible to make again an arbitrary choice (because there are two possible choices) of having an output of -1 for detector B, if Y is the input and +1 for detector C, if Y is input.

Table 15: Combined Result (m_{abc}) for combination of settings {XYY} in Detectors ABC

Detector A Input	Detector B Input	Detector C Input	Detector A Output	Detector B Output	Detector C Output	Result $m_{abc} = (a \times b \times c)$
X	Y	Y	+1	-1	+1	-1

To continue to have successful simulation, the value output value in detector A, knowing that the input is Y should be -1, otherwise, it's impossible to get $m_{abc} = a \times b \times c = -1$, because in earlier tables were already defined that if detector B has X as input then output is +1 and if detector C has Y as input then output is +1.

Table 16: Combined Result (m_{abc}) for combination of settings {YXY} in Detectors ABC

Detector A Input	Detector B Input	Detector C Input	Detector A Output	Detector B Output	Detector C Output	Result $m_{abc} = (a \times b \times c)$
Y	X	Y	-1	+1	+1	-1

Finally, with earlier choices we have all hidden values defined:

- If Detector A has X as input, then the output is +1;
- If Detector A has Y as input, then the output is -1;
- If Detector B has X as input, then the output is +1;
- If Detector B has Y as input, then the output is +1;
- If Detector C has X as input, then the output is +1;
- If Detector C has Y as input, then the output is -1.

And with these hidden values defined it's impossible to have a successful simulation for the arrangement {YYX} because the combined value $m_{abc} = a \times b \times c = +1$, instead of -1.

Table 17: Combined Result (m_{abc}) for combination of settings {YYX} in Detectors ABC

Detector A Input	Detector B Input	Detector C Input	Detector A Output	Detector B Output	Detector C Output	Result $m_{abc} = (a \times b \times c)$
Y	Y	X	-1	-1	+1	+1 (instead of -1)

Hence, it's only possible to win $\frac{3}{4}$ of times using these hidden values. If the same exercise is done for all hidden values and arrangements, the conclusion will always be the same: it's impossible to always win the game using a hidden value approach.

2.3.4. Quantum Mechanics (QM) Approach

In the previous subchapter, it was shown that it's impossible to always win the game using the hidden value approach. In this subchapter, we will see if it's possible to always win the game with the quantum mechanics approach.

Each particle has its properties. So particle A is represented with $|\psi\rangle_A$, Particle B with $|\psi\rangle_B$ and Particle C with $|\psi\rangle_C$

$$|\psi\rangle_A = \alpha_A |0\rangle_A + \beta_A |1\rangle_A, \quad \alpha, \beta \in \mathbb{C} \quad (2.40)$$

$$|\psi\rangle_B = \alpha_B |0\rangle_B + \beta_B |1\rangle_B, \quad \alpha, \beta \in \mathbb{C} \quad (2.41)$$

$$|\psi\rangle_C = \alpha_C |0\rangle_C + \beta_C |1\rangle_C, \quad \alpha, \beta \in \mathbb{C} \quad (2.42)$$

But when particles are entangled states are inseparable, hence cannot be studied as separate states.

Which leads to

$$\begin{aligned} |\Psi\rangle_{ABC} = & C_{000}(|0\rangle_A \otimes |0\rangle_B \otimes |0\rangle_C) + C_{001}(|0\rangle_A \otimes |1\rangle_B \otimes |0\rangle_C) + C_{010}(|0\rangle_A \\ & \otimes |1\rangle_B \otimes |0\rangle_C) + C_{011}(|0\rangle_A \otimes |1\rangle_B \otimes |1\rangle_C) + C_{100}(|1\rangle_A \otimes |0\rangle_B \\ & \otimes |0\rangle_C) + C_{110}(|1\rangle_A \otimes |1\rangle_B \otimes |0\rangle_C) + C_{111}(|1\rangle_A \otimes |1\rangle_B \otimes |1\rangle_C) \end{aligned} \quad (2.43)$$

The equation (2.43) can simply be represented as

$$\begin{aligned} |\Psi\rangle_{ABC} = & C_{000}|000\rangle_{ABC} + C_{001}|001\rangle_{ABC} + C_{010}|010\rangle_{ABC} + C_{011}|011\rangle_{ABC} \\ & + C_{100}|100\rangle_{ABC} + C_{101}|101\rangle_{ABC} + C_{110}|110\rangle_{ABC} + C_{111}|111\rangle_{ABC}, \\ & C_{000}, C_{001}, C_{010}, C_{011}, C_{100}, C_{101}, C_{110}, C_{111} \in \mathbb{C} \end{aligned} \quad (2.44)$$

And in this case, particles generated are entangled photons.

For that case of entanglement between photons, we find a special case of $|C_{001}|^2 = |C_{010}|^2 = |C_{011}|^2 = |C_{100}|^2 = |C_{101}|^2 = |C_{110}|^2 = 0$, and $|C_{000}|^2 + |C_{111}|^2 = 1$ hence $|C_{000}|^2 + |C_{001}|^2 + |C_{010}|^2 + |C_{011}|^2 + |C_{100}|^2 + |C_{101}|^2 + |C_{110}|^2 + |C_{111}|^2 = 1$

Since $|C_{000}|^2 = |C_{111}|^2$ (polarization of particle A is equal to particle B and to particle C) then $2|C_{111}|^2 = 1 \rightarrow C_{111} = \frac{1}{\sqrt{2}}$

This means that the result of entangled photons are always equal when they collapse on their respective detector, as a result they flash the same output with the same setting.

$$|\Psi\rangle_{ABC} = \frac{1}{\sqrt{2}} [|000\rangle_{ABC} + |111\rangle_{ABC}] \quad (2.45)$$

This example also proves that $C_{000} \neq \alpha_A \cdot \alpha_B \cdot \alpha_C$, $C_{001} \neq \alpha_A \cdot \alpha_B \cdot \beta_C$, $C_{010} \neq \alpha_A \cdot \beta_B \cdot \alpha_C$, $C_{011} \neq \alpha_A \cdot \beta_B \cdot \beta_C$, $C_{100} \neq \beta_A \cdot \alpha_B \cdot \alpha_C$, $C_{101} \neq \beta_A \cdot \alpha_B \cdot \beta_C$, $C_{110} \neq \beta_A \cdot \beta_B \cdot \alpha_C$ and $C_{111} \neq \beta_A \cdot \beta_B \cdot \beta_C$ because if

$$C_{000} \neq 0 \rightarrow \alpha_A \cdot \alpha_B \cdot \alpha_C \neq 0 \text{ (means that neither } \alpha_A, \alpha_B \text{ or } \alpha_C \text{ are equal 0)} \quad (2.46)$$

$$C_{111} \neq 0 \rightarrow \beta_A \cdot \beta_B \cdot \beta_C \neq 0 \text{ (means that neither } \beta_A, \beta_B \text{ or } \beta_C \text{ are equal 0)} \quad (2.47)$$

Then we cannot have $C_{001} = \alpha_A \cdot \alpha_B \cdot \beta_C = 0$

$$C_{001} = 0 \rightarrow \alpha_A \cdot \alpha_B \cdot \beta_C = 0 \text{ (means that } \alpha_A, \alpha_B \text{ or } \beta_C \text{ should be equal 0)} \quad (2.48)$$

Not considering the entanglement factor, each measurement could be done in the x-axis (X) or y-axis (Y), meaning that in the original state a linear transformation is applied, in order to get measurement in the desired axis.

To get a measurement in the x-axis, the Pauli matrix σ_x should be applied to the original state:

$$(\sigma_x)|0\rangle = |1\rangle \quad (2.49)$$

$$(\sigma_x)|1\rangle = |0\rangle \quad (2.50)$$

To get a measurement in the y-axis, the Pauli matrix σ_y is applied should be applied to the original state:

$$(\sigma_y)|0\rangle = i|1\rangle \quad (2.51)$$

$$(\sigma_y)|1\rangle = -i|0\rangle \quad (2.52)$$

More details about Pauli matrices are available in Appendix B.

There are 4 arrangements of settings with useful information in the context that is being studied $\{XXX; XYY; YXY; YYX\}$, it is also possible to have 4 combined measurements.

The measurements for each arrangement to the state $|\Psi\rangle_{ABC}$ are given by the eigenvalues m_{abc} of the following transformations (detailed demonstration in Appendix B):

$$(\sigma_x \otimes \sigma_x \otimes \sigma_x)|\Psi\rangle_{ABC} = +|\Psi\rangle_{ABC}, \quad m_{abc} = +1 \quad (2.53)$$

$$(\sigma_x \otimes \sigma_y \otimes \sigma_y)|\Psi\rangle_{ABC} = -|\Psi\rangle_{ABC}, \quad m_{abc} = -1 \quad (2.54)$$

$$(\sigma_y \otimes \sigma_x \otimes \sigma_y)|\Psi\rangle_{ABC} = -|\Psi\rangle_{ABC}, \quad m_{abc} = -1 \quad (2.55)$$

$$(\sigma_x \otimes \sigma_y \otimes \sigma_y)|\Psi\rangle_{ABC} = -|\Psi\rangle_{ABC}, \quad m_{abc} = -1 \quad (2.56)$$

Table 18: Combined Result (m_{abc}) for combination of settings $\{XXX; XYY; YXY; YYY\}$ in Detectors ABC

Detector A Input	Detector B Input	Detector C Input	Result m_{abc}
X (σ_x)	X (σ_x)	X (σ_x)	+1
X (σ_x)	Y (σ_y)	Y (σ_y)	-1
Y (σ_y)	X (σ_x)	Y (σ_y)	-1
Y (σ_y)	Y (σ_y)	X (σ_x)	-1

In conclusion, we have a probability of scoring equal to 100% using quantum mechanics, therefore there's an incentive to continue to explore further the field.

3. Quantum Computation

3.1. Linear Algebra

To better understand quantum computation it is important to understand some essential notions about vector spaces and vectors:

- A vector space consists of an isolated physical system with a group of objects called vectors. In quantum mechanics, the vector space is a complex vector space with an inner product (also known as Hilbert space). An n-dimensional complex vector (represented as column matrix) is a unit vector in the system's state space (with an ordered list of n complex numbers).
- The vector $|u\rangle$ is represented by:

$$|u\rangle = \begin{bmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{bmatrix}, \quad u_1, \dots, u_n \in \mathbb{C} \quad (3.1)$$

The sum of two vectors $|u\rangle$ and $|v\rangle$ results in another vector with component values equal to the sum of each component of the vectors $|u\rangle$ and $|v\rangle$

$$|u\rangle + |v\rangle = \begin{bmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{bmatrix} + \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{bmatrix} = \begin{bmatrix} u_1 + v_1 \\ u_2 + v_2 \\ \vdots \\ u_n + v_n \end{bmatrix} \quad (3.2)$$

Multiplication of $|u\rangle$ by a scalar number λ , also results in another vector (with scalar number multiplied by each component of the original vector)

$$\lambda|u\rangle = \lambda \begin{bmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{bmatrix} = \begin{bmatrix} \lambda u_1 \\ \lambda u_2 \\ \vdots \\ \lambda u_n \end{bmatrix} \quad (3.3)$$

The dual vector is represented by bra $\langle u|$ and represents the conjugate transposed vector of $|u\rangle$:

$$\langle u| = |u\rangle^\dagger = (|u\rangle^*)^T = [u_1^* \quad u_2^* \quad \dots \quad u_n^*], \quad \text{if } u_n = (a + ib) \text{ then } u_n^* = (a - ib) \quad (3.4)$$

The inner product of two vectors is represented by $\langle u|v\rangle$:

$$\langle u|v\rangle = |u\rangle^\dagger |v\rangle = [u_1^* \quad u_2^* \quad \dots \quad u_n^*] \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{bmatrix} = u_1^* v_1 + u_2^* v_2 + \dots + u_n^* v_n \quad (3.5)$$

If $\langle u|v\rangle = 0$ then vectors $|u\rangle$ and $|v\rangle$ are orthogonal.

The norm of vector $|u\rangle$ is $\|u\|$

$$\|u\| = \sqrt{\langle uu\rangle} \quad (3.6)$$

Vector $|u\rangle$ is normalized if $\|u\| = 1$.

Both vectors $|u\rangle$ and $|v\rangle$ are orthonormal if $\langle u|v\rangle = 0$, $\|u\| = 1$ and $\|v\| = 1$.

The outer product of two vectors is represented by $|u\rangle\langle v|$:

$$|u\rangle\langle v| = |u\rangle |v\rangle^\dagger = \begin{bmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{bmatrix} [v_1^* \quad v_2^* \quad \dots \quad v_n^*] = \begin{bmatrix} u_1 v_1^* & u_1 v_2^* & \dots & u_1 v_n^* \\ u_2 v_1^* & u_2 v_2^* & \dots & u_2 v_n^* \\ \vdots & \vdots & \ddots & \vdots \\ u_n v_1^* & u_n v_2^* & \dots & u_n v_n^* \end{bmatrix} \quad (3.7)$$

The tensor product of two vectors is represented by $|u\rangle \otimes |v\rangle$:

$$|u\rangle \otimes |v\rangle = \begin{bmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{bmatrix} \otimes \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{bmatrix} = \begin{bmatrix} u_1 \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{bmatrix} \\ u_2 \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{bmatrix} \\ \vdots \\ u_n \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{bmatrix} \end{bmatrix} = \begin{bmatrix} u_1 v_1 \\ u_1 v_2 \\ \vdots \\ u_1 v_n \\ u_2 v_1 \\ u_2 v_2 \\ \vdots \\ u_2 v_n \\ \vdots \\ u_n v_1 \\ u_n v_2 \\ \vdots \\ u_n v_n \end{bmatrix} \quad (3.8)$$

The tensor product $|u\rangle \otimes |v\rangle$ could be also represented by $|uv\rangle$ or $|u\rangle|v\rangle$

$$|u\rangle \otimes |v\rangle = |uv\rangle = |u\rangle|v\rangle \quad (3.9)$$

Linear transformations represent a modification on vectors and usually are represented by matrices

$$T = \begin{bmatrix} T_{11} & T_{12} & \dots & T_{1n} \\ T_{21} & T_{22} & \dots & T_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ T_{n1} & T_{n2} & \dots & T_{nn} \end{bmatrix}, \quad T_{ij} \in \mathbb{C} \quad (3.10)$$

A trace of a matrix represents the sum of all diagonal components. Hence, the trace of this matrix T is $tr(T) = T_{11} + T_{22} + \dots + T_{nn}$

A linear transformation on vector $|u\rangle$ is written as $T|u\rangle$

$$T|u\rangle = \begin{bmatrix} T_{11} & T_{12} & \dots & T_{1n} \\ T_{21} & T_{22} & \dots & T_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ T_{n1} & T_{n2} & \dots & T_{nn} \end{bmatrix} \begin{bmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{bmatrix} = \begin{bmatrix} T_{11}u_1 + T_{12}u_2 + \dots + T_{1n}u_n \\ T_{21}u_1 + T_{22}u_2 + \dots + T_{2n}u_n \\ \vdots \\ T_{n1}u_1 + T_{n2}u_2 + \dots + T_{nn}u_n \end{bmatrix} \quad (3.11)$$

If the following condition is true:

$$T|u\rangle = \lambda|u\rangle \quad (3.12)$$

Then $|u\rangle$ is an eigenvector and λ (scalar number) its eigenvalue.

It's also possible to apply the linear transformation T on dual vector $\langle u|$, which is represented by $\langle u|T$

$$\langle u|T = [u_1^* \quad u_2^* \quad \dots \quad u_n^*] \begin{bmatrix} T_{11} & T_{12} & \dots & T_{1n} \\ T_{21} & T_{22} & \dots & T_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ T_{n1} & T_{n2} & \dots & T_{nn} \end{bmatrix} \quad (3.13)$$

The adjoint of a matrix T is equal to the transposed complex conjugated matrix.

$$T^\dagger = (T^*)^T = \begin{bmatrix} T_{11}^* & T_{21}^* & \dots & T_{n1}^* \\ T_{12}^* & T_{22}^* & \dots & T_{n2}^* \\ \vdots & \vdots & \ddots & \vdots \\ T_{1n}^* & T_{2n}^* & \dots & T_{nn}^* \end{bmatrix} \quad (3.14)$$

If $T = T^\dagger$ then the matrix is called Hermitian

Special matrix \mathbb{I} is called the identity matrix

$$\mathbb{I} = \begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{bmatrix} \quad (3.15)$$

If identity transformation \mathbb{I} is applied to a vector $|u\rangle$ it does not change the vector.

$$\mathbb{I}|u\rangle = \begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{bmatrix} \begin{bmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{bmatrix} = \begin{bmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{bmatrix} \quad (3.16)$$

Matrix U is called a unitary matrix when the below condition is true.

$$UU^\dagger = \mathbb{I} \Leftrightarrow U^{-1} = U^\dagger \quad (3.17)$$

The result of two different linear transformations S and T could be applied to a vector

$$ST = \begin{bmatrix} S_{11} & S_{12} & \dots & S_{1n} \\ S_{21} & S_{22} & \dots & S_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ S_{n1} & S_{n2} & \dots & S_{nn} \end{bmatrix} \begin{bmatrix} T_{11} & T_{12} & \dots & T_{1n} \\ T_{21} & T_{22} & \dots & T_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ T_{n1} & T_{n2} & \dots & T_{nn} \end{bmatrix} = \begin{bmatrix} S_{11}T_{11} + S_{12}T_{21} + \dots + S_{1n}T_{n1} & S_{11}T_{12} + S_{12}T_{22} + \dots + S_{1n}T_{n2} & \dots & S_{11}T_{1n} + S_{12}T_{2n} + \dots + S_{1n}T_{nn} \\ S_{21}T_{11} + S_{22}T_{21} + \dots + S_{2n}T_{n1} & S_{21}T_{12} + S_{22}T_{22} + \dots + S_{2n}T_{n2} & \dots & S_{21}T_{1n} + S_{22}T_{2n} + \dots + S_{2n}T_{nn} \\ \vdots & \vdots & \ddots & \vdots \\ S_{n1}T_{11} + S_{n2}T_{21} + \dots + S_{nn}T_{n1} & S_{n1}T_{12} + S_{n2}T_{22} + \dots + S_{nn}T_{n2} & \dots & S_{n1}T_{1n} + S_{n2}T_{2n} + \dots + S_{nn}T_{nn} \end{bmatrix} \quad (3.18)$$

Projection Operator of $|u\rangle$ is written as P_u in bellow equation

$$P_u = |u\rangle\langle u| \quad (3.19)$$

To be a projection an operation must obey the following conditions

$$P_u^2 = P_u \quad (3.20)$$

$$P_u = P_u^\dagger \quad (3.21)$$

3.2.Qubit

Qubit (also known as Quantum Bit) is the fundamental unit of quantum computation. It is essential to make operations and to create algorithms to solve logic problems. In classical computation, the essential units are called bits and have values of 0 and 1. Qubits are usually represented with kets $|0\rangle$ and $|1\rangle$. In mathematical terms the units could be represented as vectors:

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad (3.22)$$

$$|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \quad (3.23)$$

In classical computation, the unit should be in one of the states 0 or 1, however, quantum computation allows the superposition between the two states $|0\rangle$ and $|1\rangle$.

So one qubit could be represented by ket $|\psi\rangle$

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \quad \alpha, \beta \in \mathbb{C} \quad (3.24)$$

Where α and β are the amplitudes with probabilities of $|\alpha|^2$, $|\beta|^2$ and $|\alpha|^2 + |\beta|^2 = 1$

Qubits could be represented with $|\psi\rangle$ in a cartesian axis with $|0\rangle$ and $|1\rangle$ as the basis. In the below figure, the vector $|\psi\rangle$ is represented in this cartesian axis

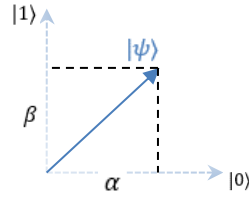


Figure 17: Representation of vector $|\psi\rangle$

3.3. Quantum measurement

As seen before quantum computation allows superposition between states. Bellow, it will be demonstrated what will happen if a measurement is performed on the state $|\psi\rangle$.

Measurement operator M_m acts on the state space of the system being measured. The index m refers to the measurement outcomes that may occur. Collection $\{M_m\}$ describes quantum measurements satisfying completeness equation:

$$\sum_m (M_m^\dagger M_m) = \mathbb{I} \quad (3.25)$$

Knowing that the state of the quantum system is $|\psi\rangle$ before the measurement, then the probability that result m occurs is specified by:

$$p(m) = \langle \psi | M_m^\dagger M_m | \psi \rangle \quad (3.26)$$

And the post-measurement state is

$$|\phi_m\rangle = \frac{1}{\sqrt{p(m)}} M_m |\psi\rangle = \frac{M_m |\psi\rangle}{\sqrt{\langle \psi | M_m^\dagger M_m | \psi \rangle}} \quad (3.27)$$

If $|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$, we have M_0 given by

$$M_0 = |0\rangle\langle 0| \quad (3.28)$$

And $p(0)$ is

$$p(0) = \langle \psi | M_0^\dagger M_0 | \psi \rangle = \langle \psi | (|0\rangle\langle 0|)^\dagger (|0\rangle\langle 0|) | \psi \rangle \quad (3.29)$$

$$p(0) = \langle \psi | (|0\rangle\langle 0|)^\dagger (|0\rangle\langle 0|) | \psi \rangle = \langle \psi | (|0\rangle\langle 0|) (|0\rangle\langle 0|) | \psi \rangle \quad (3.30)$$

$$p(0) = \langle \psi | 0 \rangle \underbrace{\langle 0 | 0 \rangle}_1 \langle 0 | \psi \rangle = \langle \psi | 0 \rangle \langle 0 | \psi \rangle \quad (3.31)$$

$$p(0) = \langle \psi | 0 \rangle \langle 0 | (\alpha |0\rangle + \beta |1\rangle) = \langle \psi | 0 \rangle \left(\alpha \underbrace{\langle 0 | 0 \rangle}_1 + \beta \underbrace{\langle 0 | 1 \rangle}_0 \right) \quad (3.32)$$

We also have $\langle \psi | = \alpha^* \langle 0 | + \beta^* \langle 1 |$, where α^* and β^* are the complex conjugate of α and β

$$p(0) = (\alpha^* \cdot \langle 0 | + \beta^* \cdot \langle 1 |) |0\rangle \cdot \alpha \quad (3.33)$$

$$p(0) = \left(\alpha^* \cdot \underbrace{\langle 0 | 0 \rangle}_1 + \beta^* \cdot \underbrace{\langle 1 | 0 \rangle}_0 \right) \cdot \alpha \quad (3.34)$$

$$p(0) = (\alpha^*) \cdot \alpha = |\alpha|^2 \quad (3.35)$$

Note that the post-measurement state is

$$|\phi_0\rangle = \frac{1}{\sqrt{p(0)}} M_0 |\psi\rangle = \frac{(|0\rangle\langle 0|) |\psi\rangle}{\sqrt{|\alpha|^2}} = \frac{(|0\rangle) \cdot \alpha}{|\alpha|} = |0\rangle \quad (3.36)$$

Similarly, we have

$$M_1 = |1\rangle\langle 1| \quad (3.37)$$

With $p(1)$

$$p(1) = (\beta^*) \cdot \beta = |\beta|^2 \quad (3.38)$$

And post-measurement state

$$|\phi_1\rangle = \frac{1}{\sqrt{p(1)}} M_1 |\psi\rangle = \frac{(|1\rangle\langle 1|) |\psi\rangle}{\sqrt{|\beta|^2}} = \frac{(|1\rangle) \cdot \beta}{|\beta|} = |1\rangle \quad (3.39)$$

In this case each measurement operator M_m is Hermitian ($M_m = M_m^\dagger$), and $M_0^2 = M_0$, $M_1^2 = M_1$. Therefore the completeness equation is satisfied:

$$M_0^\dagger M_0 + M_1^\dagger M_1 = M_0^2 + M_1^2 = M_0 + M_1 = |0\rangle\langle 0| + |1\rangle\langle 1| = \mathbb{I} \quad (3.40)$$

An important special case of measurement is known as projective measurements (performed in unitary transformations). This projective measurement is described by an observable, O :

$$O = \sum_m m P_m \quad (3.41)$$

Observable O is a Hermitian operator defined by the projector P_m (onto the eigenspace of M) and eigenvalue m . Knowing that the state of the quantum system is $|\psi\rangle$ before the measurement then the probability that result m occurs is specified by:

$$p(m) = \langle \psi | P_m | \psi \rangle \quad (3.42)$$

And the post-measurement state is

$$|\phi_m\rangle = \frac{P_m |\psi\rangle}{\sqrt{p(m)}} \quad (3.43)$$

The post-measurement state of the system is not always important and for that cases, there is a formalism called Positive Operator Valued Measure (POVM). This formalism is the result of the general description of measurements defined by E_m

$$E_m \equiv M_m^\dagger M_m \quad (3.44)$$

The collection $\{E_m\}$ describes POVM

If Measurement operators M_m is performed on the state $|\psi\rangle$, we have the probability that result m occurs specified by:

$$p(m) = \langle \psi | M_m^\dagger M_m | \psi \rangle = \langle \psi | E_m | \psi \rangle \quad (3.45)$$

To make this assumption the operators E_m should satisfy non-negativity and completeness condition:

$$\sum_m (M_m^\dagger M_m) = \sum_m (E_m) = \mathbb{I} \quad (3.46)$$

$$\forall m: E_m \geq 0 \quad (3.47)$$

3.4. Density Operator

Quantum mechanics uses the language of state vectors, but there is an alternate formulation that uses a density operator or density matrix.

Quantum systems whose states are not completely known could be described by a density operator:

$$\rho \equiv \sum_i p_i |\psi_i\rangle \langle \psi_i| \quad (3.48)$$

Where p_i is a probability of being in one of the states $|\psi_i\rangle$

The density operator ρ' when unitary operator U is applied is described by the equation

$$\rho' = \sum_i p_i U |\psi_i\rangle\langle\psi_i| U^\dagger = U \rho U^\dagger \quad (3.49)$$

It is also possible to perform measurements described by measurement operators M_m and calculate the probability of getting result m , with the initial state $|\psi_i\rangle$:

$$p(m|i) = \langle\psi_i| M_m^\dagger M_m |\psi_i\rangle = \text{tr}(M_m^\dagger M_m |\psi_i\rangle\langle\psi_i|) \quad (3.50)$$

And this leads to the probability of obtaining result m :

$$p(m) = \sum_i p(m|i) \cdot p_i = \sum_i \text{tr}(M_m^\dagger M_m |\psi_i\rangle\langle\psi_i|) \cdot p_i \quad (3.51)$$

$$p(m) = \text{tr}(M_m^\dagger M_m \rho) \quad (3.52)$$

The state after obtaining the result m is given by $|\psi_i^m\rangle$

$$|\psi_i^m\rangle = \frac{M_m |\psi_i\rangle}{\sqrt{\langle\psi_i| M_m^\dagger M_m |\psi_i\rangle}} \quad (3.53)$$

And the post-measurement state is:

$$\rho_m = \frac{M_m^\dagger M_m \rho}{\text{tr}(M_m^\dagger M_m \rho)} \quad (3.54)$$

To make this assumption completeness condition should satisfied:

$$\sum_m (M_m^\dagger M_m) = \mathbb{I} \quad (3.55)$$

Additionally, it defined that a pure state have $\text{tr}(\rho^2) = 1$, while a mixed state (can only be represented with density operator) has $\text{tr}(\rho^2) < 1$

3.5. Bloch Sphere Representation

Qubit could be transformed from one state to another allowing to make logical operations. To understand transformations and operations geometrically, equation (3.56) could be written in another form.

$$|\psi\rangle = \alpha |0\rangle + \beta |1\rangle, \quad \alpha, \beta \in \mathbb{C} \quad (3.56)$$

α and β being complex numbers could also be written as:

$$\alpha = r_0 e^{i\Phi_0} \text{ and } \beta = r_1 e^{i\Phi_1}, \quad \alpha, \beta \in \mathbb{C} \quad (3.57)$$

So $|\psi\rangle$ becomes:

$$|\psi\rangle = r_0 e^{i\Phi_0} |0\rangle + r_1 e^{i\Phi_1} |1\rangle \quad (3.58)$$

Simplifying, the equation it turns into

$$|\psi\rangle = e^{i\Phi_0} (r_0 |0\rangle + r_1 e^{i(\Phi_1 - \Phi_0)} |1\rangle) \quad (3.59)$$

As $e^{i\Phi_0}$ is an overall phase affecting both terms, it has no physical relevance

$$|\psi\rangle \equiv r_0 |0\rangle + r_1 e^{i(\Phi_1 - \Phi_0)} |1\rangle \quad (3.60)$$

Knowing that $|r_0|^2 + |r_1|^2 = 1$ and $\cos^2(\phi) + \sin^2(\phi) = 1$ the equation could be written as:

$$|\psi\rangle \equiv \cos(\phi) |0\rangle + \sin(\phi) e^{i\varphi} |1\rangle \quad (3.61)$$

This will allow geometric representation using Bloch Sphere [4]. Rewriting $|\psi\rangle$ in terms of θ and φ obtaining the equation:

$$|\psi\rangle = \cos\frac{\theta}{2} |0\rangle + e^{i\varphi} \sin\frac{\theta}{2} |1\rangle, \quad 0 \leq \theta \leq \pi; \quad 0 \leq \varphi \leq 2\pi \quad (3.62)$$

Equation (3.61) becomes (3.62) with the condition:

$$\phi = \frac{\theta}{2} \quad (3.63)$$

To guarantee that $|0\rangle$ and $|1\rangle$ are antipodal points in geometric representation (opposite points the sphere representation).

In Figure 18, $|\psi\rangle$ is represented inside the Bloch sphere geometrically:

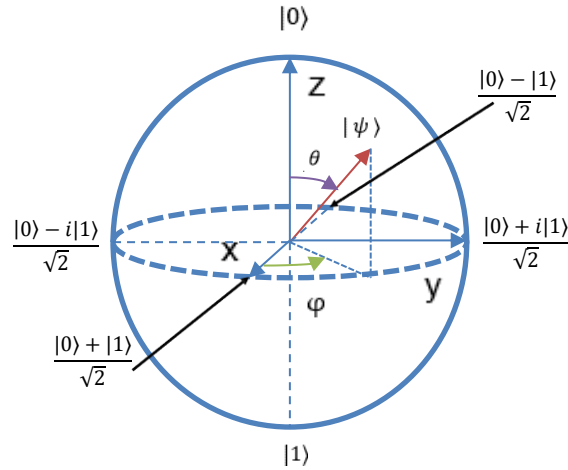


Figure 18: Bloch sphere representation of a qubit

The equation (3.62) gives state representation as a pure state (because it is on the surface of the Bloch sphere), a mixed state is represented within the Bloch sphere.

Bloch vector is defined as follows:

$$\hat{n} = (x, y, z)^T = (\cos \varphi \sin \theta, \sin \varphi \sin \theta, \cos \theta)^T \quad (3.64)$$

Where

$$\hat{n}_x = \cos \varphi \sin \theta \quad (3.65)$$

$$\hat{n}_y = \sin \varphi \sin \theta \quad (3.66)$$

$$\hat{n}_z = \cos \theta \quad (3.67)$$

3.6. Quantum Gates Representation

Quantum gates represent the transformation of Qubit from one state to another. They are necessary to make logical operations. There are 2 types of quantum gates: single-qubit gates and multiple qubit gates. With single-qubit gates, there is a logical transformation of the unit that performs negation of the initial state. This Unitary and Hermitian gate is called NOT gate (also known as Pauli-X Gate) and could be represented with the following circuit diagram and as Pauli X matrix.

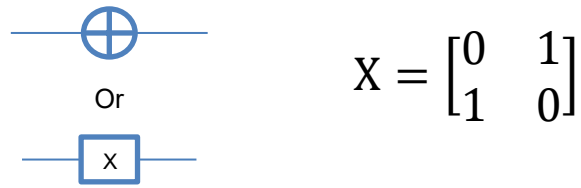


Figure 19: Circuit and matrix representation of NOT gate (Pauli-X)

Using $|\psi\rangle$ from equation (2.3) as input for the gate, it is possible to understand why the output is a negation:

$$X|\psi\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \beta \\ \alpha \end{bmatrix} \quad (3.68)$$

This represents a rotation around the x-axis of the Bloch sphere by 180° .

Considering two different input states $|0\rangle$ ($\alpha = 1; \beta = 0$) and $|1\rangle$ ($\alpha = 0; \beta = 1$), the transformation results are described in Table 19.

Table 19: Representation of Pauli-X outputs in Bloch Sphere according to their inputs $|0\rangle$ and $|1\rangle$

Input	Input (Bloch Sphere)	Gate	Output (Bloch Sphere)	Output
$ 0\rangle$				$ 1\rangle$
$ 1\rangle$				$ 0\rangle$

Considering that the Pauli X gate represents the rotation around the x-axis in the Bloch sphere, it is possible to have rotation around the other two axes (Y or Z). Having said this, Pauli-Y Gate is represented by:

$$\text{---} \boxed{Y} \text{---} \quad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

Figure 20: Circuit and matrix representation of Pauli-Y Gate

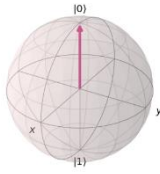

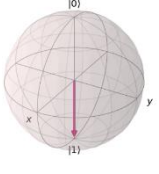
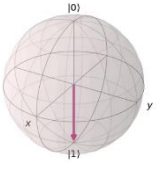

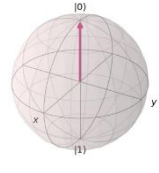
Using $|\psi\rangle$ from equation (2.3) as input of the gate, we have:

$$Y|\psi\rangle = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} i\beta \\ -i\alpha \end{bmatrix} \quad (3.69)$$

And this represents a rotation around the y-axis of the Bloch sphere by 180° .

Considering two different states $|0\rangle$ ($\alpha = 1; \beta = 0$) and $|1\rangle$ ($\alpha = 0; \beta = 1$) as input, the output results are described in Table 20.

Table 20: Representation of Pauli-Y outputs in Bloch Sphere according to their inputs $|0\rangle$ and $|1\rangle$

Input	Input (Bloch Sphere)	Gate	Output (Bloch Sphere)	Output
$ 0\rangle$				$i 1\rangle$
$ 1\rangle$				$-i 0\rangle$

Pauli-Z Gate is represented by:

$$\text{---} \boxed{Z} \text{---} \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

Figure 21: Circuit and matrix representation of Pauli-Z Gate

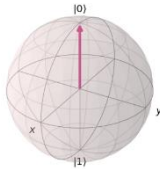

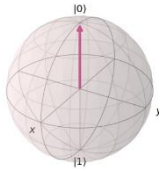
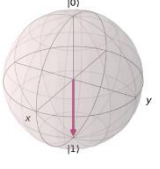

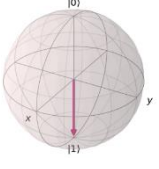
Using $|\psi\rangle$ from equation (2.3) as input of the gate, we have:

$$Z|\psi\rangle = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \alpha \\ -\beta \end{bmatrix} \quad (3.70)$$

And this represents a rotation around the z-axis of the Bloch sphere by 180°.

Considering two different states $|0\rangle$ ($\alpha = 1; \beta = 0$) and $|1\rangle$ ($\alpha = 0; \beta = 1$) as input we have the results described in Table 21, as output.

Table 21: Representation of Pauli-Z outputs in Bloch Sphere according to their inputs $|0\rangle$ and $|1\rangle$

Input	Input (Bloch Sphere)	Gate	Output (Bloch Sphere)	Output
$ 0\rangle$				$ 0\rangle$
$ 1\rangle$				$- 1\rangle$

Besides Pauli gates, there are several other one-bit gates. The Hadamard gate is very important because it can introduce a superposition into a well-defined input state $|0\rangle$ or $|1\rangle$.

The Hadamard gate is represented by:

$$\text{---} \boxed{\text{H}} \text{---} \quad H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

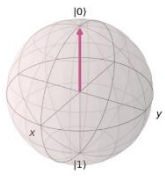
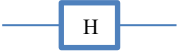
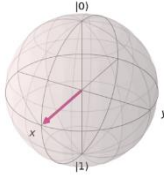
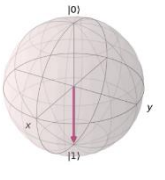
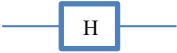
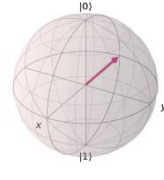
Figure 22: Circuit and matrix representation of Hadamard Gate

Using $|\psi\rangle$ from equation (2.3) as input of the gate, we have:

$$H|\psi\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} \alpha + \beta \\ \alpha - \beta \end{bmatrix} \quad (3.71)$$

Considering two different states $|0\rangle$ ($\alpha = 1; \beta = 0$) and $|1\rangle$ ($\alpha = 0; \beta = 1$) as input we have the results described in Table 22, as output:

Table 22: Representation of Hadamard gate outputs in Bloch Sphere according to their inputs $|0\rangle$ and $|1\rangle$

Input	Input (Bloch Sphere)	Gate	Output (Bloch Sphere)	Output
$ 0\rangle$				$\frac{1}{\sqrt{2}}(0\rangle + 1\rangle)$
$ 1\rangle$				$\frac{1}{\sqrt{2}}(0\rangle - 1\rangle)$

Another possible gate is Phase Gate, represented in Figure 23:



$$S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$$

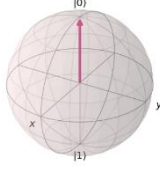

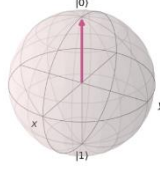
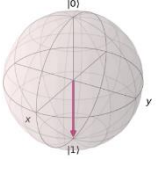
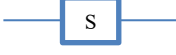
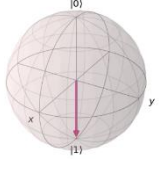
Figure 23: Circuit and matrix representation of Phase Gate

Using $|\psi\rangle$ from equation (2.3) as input of the gate, we have:

$$S|\psi\rangle = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \alpha \\ i\beta \end{bmatrix} \quad (3.72)$$

Considering two different states $|0\rangle$ ($\alpha = 1; \beta = 0$) and $|1\rangle$ ($\alpha = 0; \beta = 1$) as input we have the results described in Table 23, as output:

Table 23: Representation of Phase Gate outputs in Bloch Sphere according to their inputs $|0\rangle$ and $|1\rangle$

Input	Input (Bloch Sphere)	Gate	Output (Bloch Sphere)	Output
$ 0\rangle$				$ 1\rangle$
$ 1\rangle$				$ 0\rangle$

$\pi/8$ gate (also denoted as T Gate) is represented by:

$$\text{---} \boxed{\text{T}} \text{---} \quad \text{T} = \begin{bmatrix} 1 & 0 \\ 0 & e^{\frac{i\pi}{4}} \end{bmatrix}$$

Figure 24: Circuit and matrix representation of T Gate

Using $|\psi\rangle$ from equation (2.3) as input of the gate, we have:

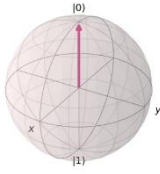

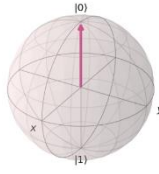
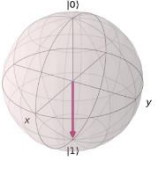

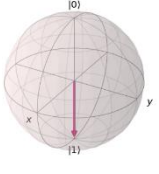
$$\text{T}|\psi\rangle = \begin{bmatrix} 1 & 0 \\ 0 & e^{\frac{i\pi}{4}} \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \alpha \\ e^{\frac{i\pi}{4}}\beta \end{bmatrix} \quad (3.73)$$

Also

$$e^{\frac{i\pi}{4}} = \cos\left(\frac{\pi}{4}\right) + i\sin\left(\frac{\pi}{4}\right) = \frac{\sqrt{2}}{2} + i \cdot \frac{\sqrt{2}}{2} \quad (3.74)$$

Considering two different states $|0\rangle$ ($\alpha = 1; \beta = 0$) and $|1\rangle$ ($\alpha = 0; \beta = 1$) as input the output results are described in Table 24:

Table 24: Representation of T Gate outputs in Bloch Sphere according to their inputs $|0\rangle$ and $|1\rangle$

Input	Input (Bloch Sphere)	Gate	Output (Bloch Sphere)	Output
$ 0\rangle$				$ 0\rangle$
$ 1\rangle$				$\left(\frac{\sqrt{2}}{2} + i \cdot \frac{\sqrt{2}}{2}\right) 1\rangle$

It is also possible to make operations with multiple qubits. Quantum computation requires that all operations and gates are reversible, meaning that all outputs should have a unique input.

The gate to make multiple bit operations is called the CNOT gate and it is represented as it follows (two qubit representation):



Figure 25: Circuit and matrix representation of CNOT Gate

Having two qubits requires an understanding of how they interact. To do it, it is necessary to understand mathematically what happens. In mathematical terms, the two qubits units could be represented as vectors:

$$|00\rangle = |0\rangle \otimes |0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \begin{bmatrix} 1 \\ 0 \end{bmatrix} \\ 0 \begin{bmatrix} 1 \\ 0 \end{bmatrix} \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} \quad (3.75)$$

$$|01\rangle = |0\rangle \otimes |1\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \begin{bmatrix} 0 \\ 1 \end{bmatrix} \\ 0 \begin{bmatrix} 0 \\ 1 \end{bmatrix} \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} \quad (3.76)$$

$$|10\rangle = |1\rangle \otimes |0\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \begin{bmatrix} 1 \\ 0 \end{bmatrix} \\ 1 \begin{bmatrix} 1 \\ 0 \end{bmatrix} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} \quad (3.77)$$

$$|11\rangle = |1\rangle \otimes |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \begin{bmatrix} 0 \\ 1 \end{bmatrix} \\ 1 \begin{bmatrix} 0 \\ 1 \end{bmatrix} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} \quad (3.78)$$

So two-qubit system could be represented by ket $|\Psi\rangle$

$$|\Psi\rangle = C_{00}|00\rangle + C_{01}|01\rangle + C_{10}|10\rangle + C_{11}|11\rangle, \quad C_{00}, C_{01}, C_{10}, C_{11} \in \mathbb{C} \quad (3.79)$$

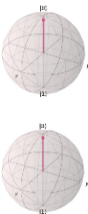

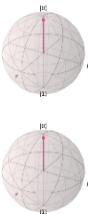
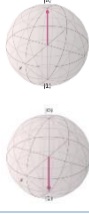

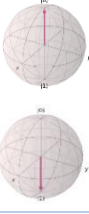
Where C_{00}, C_{01}, C_{10} and C_{11} are the amplitudes with probabilities of $|C_{00}|^2 + |C_{01}|^2 + |C_{10}|^2 + |C_{11}|^2 = 1$

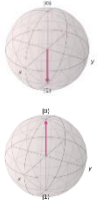

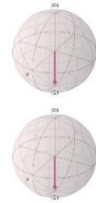
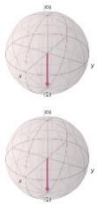

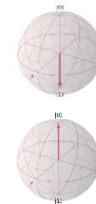
Using $|\Psi\rangle$ from equation (3.79) as input of the gate, we have:

$$\text{CNOT} |\Psi\rangle = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} C_{00} \\ C_{01} \\ C_{10} \\ C_{11} \end{bmatrix} = \begin{bmatrix} C_{00} \\ C_{01} \\ C_{11} \\ C_{10} \end{bmatrix} \quad (3.80)$$

Considering four different states $|00\rangle, |01\rangle, |10\rangle$ and $|11\rangle$ as input the output results are described in Table 25.

Table 25: Representation of CNOT Gate outputs in Bloch Sphere according to their inputs $|00\rangle, |01\rangle, |10\rangle$ and $|11\rangle$

Input	Input (Bloch Sphere)	Gate	Output (Bloch Sphere)	Output
$ 00\rangle$				$ 00\rangle$
$ 01\rangle$				$ 01\rangle$

10⟩				11⟩
11⟩				10⟩

3.7. Quantum Parallelism

In the earlier chapter, it was seen that quantum gates are essential to make logical operations. Although one gate is important, sometimes complex problems cannot be solved using a single gate, it's necessary to have a quantum circuit with several gates. One big advantage used in quantum circuits is quantum parallelism. Quantum parallelism allows having several values of output simultaneously in a single run. Bellow, it is shown mathematically how that is possible.

Considering a binary function f :

$$f: \{0,1\} \rightarrow \{0,1\} \tag{3.81}$$

And an oracle U_f that making the following transformation:

$$U_f: |x, y\rangle \rightarrow |x, y \oplus f(x)\rangle \tag{3.82}$$

An oracle is usually used in computation to represent a black box containing a circuit. To explain the problem and the solution it's not necessary to define the content of the black box, it's only important to know the behavior. Being said that, the circuit representation of (3.82) is:

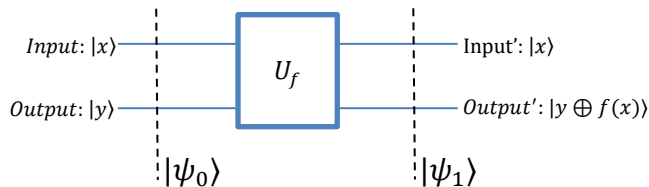


Figure 26: Oracle U_f transforming $|x, y\rangle$ into $|x, y \oplus f(x)\rangle$

If $|x\rangle$ is equal to $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$ (state in sobreposition) and $|y\rangle$ is equal to $|0\rangle$, then $|\psi_0\rangle$ is:

$$|\psi_0\rangle = |x\rangle \otimes |y\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes |0\rangle \quad (3.83)$$

$$|\psi_0\rangle = \frac{|00\rangle + |10\rangle}{\sqrt{2}} \quad (3.84)$$

Which leads to a $|\psi_1\rangle$:

$$|\psi_1\rangle = U_f |\psi_0\rangle \quad (3.85)$$

$$|\psi_1\rangle = |x, y \oplus f(x)\rangle \quad (3.86)$$

$$|\psi_1\rangle = \frac{(|0,0 \oplus f(0)\rangle + |1,0 \oplus f(1)\rangle)}{\sqrt{2}} = \frac{(|0, f(0)\rangle + |1, f(1)\rangle)}{\sqrt{2}} \quad (3.87)$$

And this concludes that state $|\psi_1\rangle$ contains information about $f(0)$ and $f(1)$, simultaneously, in a single run.

3.8. Deutsch's Algorithm

Mathematically, quantum circuits that solve problems are called algorithms. One of the first algorithm to show the power of quantum computation is the Deutsch Algorithm. This algorithm demonstrates that if quantum computing is used it's possible to know, in a single run if one function is balanced or constant in contrast to classical computation that only allows knowing this information in two runs.

Considering only binary functions f :

$$f: \{0,1\} \rightarrow \{0,1\} \quad (3.88)$$

It's possible to have four different functions, as shown in Table 26:

Table 26: Four types of function $f(x)$

Function	Graph	Type of function
$f(x) = 0$		Constant $f(1) = f(0) = 0$

$f(x) = 1$		<p>Constant</p> $f(1) = f(0) = 1$
$f(x) = x$		<p>Balanced</p> $f(1) \neq f(0)$ $f(1) = 1 - f(0)$ $f(1) = \bar{f}(0)$
$f(x) = 1 - x$		<p>Balanced</p> $f(1) \neq f(0)$ $f(1) = 1 - f(0)$ $f(1) = \bar{f}(0)$

In classical computation, it's necessary to calculate $f(0)$ and $f(1)$ and with these two results, it will be possible to conclude if the function was balanced or constant.

Using oracle (3.82), the Deutsch circuit could be defined as described in Figure 27.

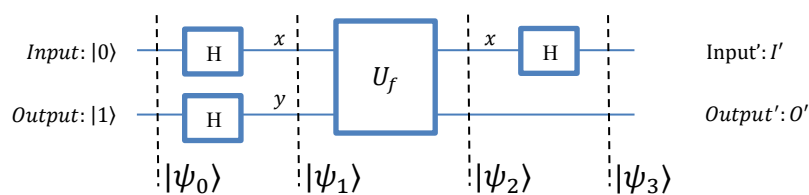


Figure 27: Deutsch's circuit

If Input is $|0\rangle$ and output $|1\rangle$, then $|\psi_0\rangle$ is:

$$|\psi_0\rangle = |0\rangle \otimes |1\rangle \quad (3.89)$$

Which leads to a $|\psi_1\rangle$:

$$|\psi_1\rangle = (H \otimes H)(|0\rangle \otimes |1\rangle) \quad (3.90)$$

$$|\psi_1\rangle = H|0\rangle \otimes H|1\rangle \quad (3.91)$$

$$|\psi_1\rangle = \frac{1}{\sqrt{2}} \cdot (|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) = \frac{1}{2} \cdot [(|0\rangle + |1\rangle) \otimes (|0\rangle - |1\rangle)] \quad (3.92)$$

$$|\psi_1\rangle = \frac{1}{2} \cdot [|0\rangle \otimes |0\rangle - |0\rangle \otimes |1\rangle + |1\rangle \otimes |0\rangle - |1\rangle \otimes |1\rangle] \quad (3.93)$$

And $|\psi_2\rangle$:

$$|\psi_2\rangle = U_f |\psi_1\rangle \quad (3.94)$$

$$|\psi_2\rangle = \frac{1}{2} \cdot [|0\rangle \otimes f(0) - |0\rangle \otimes \bar{f}(0) + |1\rangle \otimes f(1) - |1\rangle \otimes \bar{f}(1)] \quad (3.95)$$

Where $\bar{f}(0) = 1 \oplus f(0) = 1 - f(0)$ and $\bar{f}(1) = 1 \oplus f(1) = 1 - f(1)$

For two types of function there two types of results:

$$|\psi_2\rangle = \begin{cases} \frac{1}{2} \cdot [|0\rangle \otimes f(0) - |0\rangle \otimes \bar{f}(0) + |1\rangle \otimes f(0) - |1\rangle \otimes \bar{f}(0)], & f(1) = f(0) \\ \frac{1}{2} \cdot [|0\rangle \otimes f(0) - |0\rangle \otimes \bar{f}(0) + |1\rangle \otimes \bar{f}(0) - |1\rangle \otimes f(0)], & f(1) = \bar{f}(0) \end{cases} \quad (3.96)$$

$$|\psi_2\rangle = \begin{cases} \frac{1}{2} \cdot [(|0\rangle + |1\rangle) \otimes f(0) - (|0\rangle + |1\rangle) \otimes \bar{f}(0)], & f(1) = f(0) \\ \frac{1}{2} \cdot [(|0\rangle - |1\rangle) \otimes f(0) - (|0\rangle - |1\rangle) \otimes \bar{f}(0)], & f(1) = \bar{f}(0) \end{cases} \quad (3.97)$$

$$|\psi_2\rangle = \begin{cases} \frac{1}{2} \cdot (|0\rangle + |1\rangle) \otimes [f(0) - \bar{f}(0)], & f(1) = f(0) \\ \frac{1}{2} \cdot (|0\rangle - |1\rangle) \otimes [f(0) - \bar{f}(0)], & f(1) = \bar{f}(0) \end{cases} \quad (3.98)$$

And applying $(H \otimes I)$ to the $|\psi_2\rangle$ we finally have $|\psi_3\rangle$:

$$|\psi_3\rangle = (H \otimes I) |\psi_2\rangle \quad (3.99)$$

$$|\psi_3\rangle = \begin{cases} |0\rangle \otimes \frac{[f(0) - \bar{f}(0)]}{\sqrt{2}}, & f(1) = f(0) \\ |1\rangle \otimes \frac{[f(0) - \bar{f}(0)]}{\sqrt{2}}, & f(1) = \bar{f}(0) \end{cases} \quad (3.100)$$

With this, it's possible to conclude in a single run that if $I' = |0\rangle$ the function $f(x)$ is constant and if $I' = |1\rangle$ the function $f(x)$ is balanced. The disadvantage of this algorithm is that it's not possible to know

the information about the function of $f(x)$, it's only possible to know if the function is balanced or constant.

4. Shor's Algorithm

In this chapter, the goal is to find a period of a function using a quantum computation algorithm and give it a practical utility. The period of a function $f(x)$ is a repetition of values at regular intervals of multiples k of x . Finding the period (of a periodic) function is the key to factoring products of large prime numbers. This is not an easy task, and that is why the most common security protocol to encrypt information nowadays RSA (Rivest–Shamir–Adleman) protocol exploits this difficulty. Shor's factoring algorithm will make breaking RSA protocol easier. In the next subchapters, it will be explained how.

4.1. Quantum Fourier Transform (QFT)

It's needed to introduce one important module, the Fourier Transform, and its meaning when used in quantum computation.

In quantum computation, the quantum Fourier transform performs a change of bases from a computational basis ($|0\rangle, |1\rangle$) to a Fourier basis $\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}, \frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)$. This transform is essential to find a period in Shor's factoring algorithm, as it will be shown in further subchapters.

To better understand the quantum transform is important to comprehend the Discrete Fourier transform (DFT). DFT is a type of transform that is performed in discrete sets of units. Mathematically, this transform is represented by:

$$b_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} a_j e^{\frac{2\pi i j k}{N}}, \quad e^{\frac{2\pi i j k}{N}} = \cos\left(\frac{2\pi j k}{N}\right) + i \sin\left(\frac{2\pi j k}{N}\right) \quad (4.1)$$

Considering the state $|\psi\rangle$ represented by:

$$|\psi\rangle = a_0|0\rangle + a_1|1\rangle = \begin{bmatrix} a_0 \\ a_1 \end{bmatrix} \quad (4.2)$$

Applying U_{QFT_N} to the state $|\psi\rangle$, the result could be calculated as follow:

$$U_{QFT_N}|\psi\rangle = \sum_{k=0}^{N-1} b_k |k\rangle \quad (4.3)$$

Leading to:

$$b_0|0\rangle = \frac{1}{\sqrt{2}} \cdot \left[a_0 \underbrace{e^{\frac{2\pi \cdot i \cdot 0 \cdot 0}{1}}_1} + a_1 \underbrace{e^{\frac{2\pi \cdot i \cdot 1 \cdot 0}{1}}_1} \right], \quad N = 1; k = 0 \quad (4.4)$$

$$b_0|0\rangle = \frac{1}{\sqrt{2}} \cdot [a_0 + a_1] = \frac{1}{\sqrt{2}} \cdot \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \end{bmatrix} \quad (4.5)$$

$$b_1|1\rangle = \frac{1}{\sqrt{2}} \left[a_0 e^{\frac{2\pi i \cdot 0 \cdot 1}{1}} + a_1 e^{\frac{2\pi i \cdot 1 \cdot 1}{-1}} \right], \quad N = 1; k = 1 \quad (4.6)$$

$$b_1|1\rangle = \frac{1}{\sqrt{2}} \cdot [a_0 - a_1] = \frac{1}{\sqrt{2}} \cdot \begin{bmatrix} 1 & -1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \end{bmatrix} \quad (4.7)$$

Concluding formula (4.3), the result becomes:

$$U_{QFT_2}|\psi\rangle = \frac{1}{\sqrt{2}} \cdot \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \cdot \begin{bmatrix} a_0 \\ a_1 \end{bmatrix} \quad (4.8)$$

Considering a $|\psi\rangle$ represented by :

$$|\psi\rangle = a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle = \begin{bmatrix} a_{00} \\ a_{01} \\ a_{10} \\ a_{11} \end{bmatrix} \quad (4.9)$$

And $b_{00}, b_{01}, b_{10}, b_{11}$ as:

$$b_{00}|00\rangle = \frac{1}{\sqrt{4}} \cdot \left[a_{00} e^{\frac{2\pi i \cdot 0 \cdot 0}{1}} + a_{01} e^{\frac{2\pi i \cdot 1 \cdot 0}{1}} + a_{10} e^{\frac{2\pi i \cdot 2 \cdot 0}{1}} + a_{11} e^{\frac{2\pi i \cdot 3 \cdot 0}{1}} \right], \quad (4.10)$$

$N = 4; k = 0(\text{decimal})$

$$b_{01}|01\rangle = \frac{1}{\sqrt{4}} \cdot \left[a_{00} e^{\frac{2\pi i \cdot 0 \cdot 1}{1}} + a_{01} e^{\frac{2\pi i \cdot 1 \cdot 1}{\frac{\pi i}{e^2}}} + a_{10} e^{\frac{2\pi i \cdot 2 \cdot 1}{e^{\pi i}}} + a_{11} e^{\frac{2\pi i \cdot 3 \cdot 1}{\frac{3\pi i}{e^2}}} \right], \quad (4.11)$$

$N = 4; k = 1(\text{decimal})$

$$b_{10}|10\rangle = \frac{1}{\sqrt{4}} \cdot \left[a_{00} e^{\frac{2\pi i \cdot 0 \cdot 2}{1}} + a_{01} e^{\frac{2\pi i \cdot 1 \cdot 2}{e^{\pi i}}} + a_{10} e^{\frac{2\pi i \cdot 2 \cdot 2}{e^{2\pi i}}} + a_{11} e^{\frac{2\pi i \cdot 3 \cdot 2}{e^{3\pi i}}} \right], \quad (4.12)$$

$N = 4; k = 2(\text{decimal})$

$$b_{11}|11\rangle = \frac{1}{\sqrt{4}} \cdot \left[a_{00} e^{\frac{2\pi i \cdot 0 \cdot 3}{1}} + a_{01} e^{\frac{2\pi i \cdot 1 \cdot 3}{\frac{3\pi i}{e^2}}} + a_{10} e^{\frac{2\pi i \cdot 2 \cdot 3}{e^{3\pi i}}} + a_{11} e^{\frac{2\pi i \cdot 3 \cdot 3}{\frac{9\pi i}{e^2}}} \right], \quad (4.13)$$

$N = 4; k = 3(\text{decimal})$

This results in:

$$U_{QFT_4}|\psi\rangle = \frac{1}{\sqrt{4}} \cdot \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & e^{\frac{\pi i}{2}} & e^{\pi i} & e^{\frac{3\pi i}{2}} \\ 1 & e^{\pi i} & e^{2\pi i} & e^{3\pi i} \\ 1 & e^{\frac{3\pi i}{2}} & e^{3\pi i} & e^{\frac{9\pi i}{2}} \end{bmatrix} \cdot \begin{bmatrix} a_{00} \\ a_{01} \\ a_{10} \\ a_{11} \end{bmatrix} \quad (4.14)$$

Writing $\omega^k = e^{\frac{2\pi i}{N} \cdot k} = e^{\frac{2\pi i}{4} \cdot k} = e^{\frac{\pi i}{2} \cdot k}$, the result becomes:

$$U_{QFT_4}|\psi\rangle = \frac{1}{\sqrt{4}} \cdot \begin{bmatrix} \omega^0 & \omega^0 & \omega^0 & \omega^0 \\ \omega^0 & \omega^1 & \omega^2 & \omega^3 \\ \omega^0 & \omega^2 & \omega^4 & \omega^6 \\ \omega^0 & \omega^3 & \omega^6 & \omega^9 \end{bmatrix} \cdot \begin{bmatrix} a_{00} \\ a_{01} \\ a_{10} \\ a_{11} \end{bmatrix} \quad (4.15)$$

Reformulating the (4.15) as a linear operator of N components, the unitary quantum transform becomes:

$$U_{QFT_N} = \frac{1}{\sqrt{N}} \cdot \begin{bmatrix} \omega^0 & \omega^0 & \omega^0 & \omega^0 & \dots & \omega^0 \\ \omega^0 & \omega^1 & \omega^2 & \omega^3 & \dots & \omega^{N-1} \\ \omega^0 & \omega^2 & \omega^4 & \omega^6 & \dots & \omega^{2(N-1)} \\ \omega^0 & \omega^3 & \omega^6 & \omega^9 & \dots & \omega^{3(N-1)} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ \omega^0 & \omega^{N-1} & \omega^{2(N-1)} & \omega^{3(N-1)} & \dots & \omega^{(N-1)(N-1)} \end{bmatrix} \quad (4.16)$$

Knowing that U_{QFT_N} for N components are already defined, it's also important to define the circuit represented.

Regarding a two-qubit system ($N = 2^n, n = 2$) the oracle U_{QFT} is represented by:

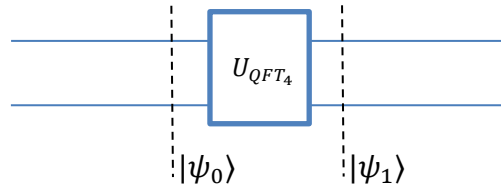


Figure 28: U_{QFT_4} represented by an oracle (2 qubits)

Decomposing the oracle, it's possible to determine that:

$$U_{QFT_4}|\psi_0\rangle = |\psi_1\rangle \quad (4.17)$$

$$\frac{1}{\sqrt{2^2}} \cdot \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & e^{\frac{2\pi i}{2^2} \cdot 1} & e^{\frac{2\pi i}{2^2} \cdot 2} & e^{\frac{2\pi i}{2^2} \cdot 3} \\ 1 & e^{\frac{2\pi i}{2^2} \cdot 2} & e^{\frac{2\pi i}{2^2} \cdot 4} & e^{\frac{2\pi i}{2^2} \cdot 6} \\ 1 & e^{\frac{2\pi i}{2^2} \cdot 3} & e^{\frac{2\pi i}{2^2} \cdot 6} & e^{\frac{2\pi i}{2^2} \cdot 9} \end{bmatrix} \cdot \begin{bmatrix} a_{00} \\ a_{01} \\ a_{10} \\ a_{11} \end{bmatrix} = \frac{1}{\sqrt{2^2}} \cdot \begin{bmatrix} a_{00} + a_{01} + a_{10} + a_{11} \\ a_{00} + e^{\frac{2\pi i}{2^2} \cdot 1} a_{01} + e^{\frac{2\pi i}{2^2} \cdot 2} a_{10} + e^{\frac{2\pi i}{2^2} \cdot 3} a_{11} \\ a_{00} + e^{\frac{2\pi i}{2^2} \cdot 2} a_{01} + e^{\frac{2\pi i}{2^2} \cdot 4} a_{10} + e^{\frac{2\pi i}{2^2} \cdot 6} a_{11} \\ a_{00} + e^{\frac{2\pi i}{2^2} \cdot 3} a_{01} + e^{\frac{2\pi i}{2^2} \cdot 6} a_{10} + e^{\frac{2\pi i}{2^2} \cdot 9} a_{11} \end{bmatrix} \quad (4.18)$$

So if $|\psi_0\rangle = |00\rangle = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$, the result of $|\psi_1\rangle$ becomes:

$$\frac{1}{\sqrt{2^2}} \cdot \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & e^{\frac{2\pi i}{2^2 \cdot 1}} & e^{\frac{2\pi i}{2^2 \cdot 2}} & e^{\frac{2\pi i}{2^2 \cdot 3}} \\ 1 & e^{\frac{2\pi i}{2^2 \cdot 2}} & e^{\frac{2\pi i}{2^2 \cdot 4}} & e^{\frac{2\pi i}{2^2 \cdot 6}} \\ 1 & e^{\frac{2\pi i}{2^2 \cdot 3}} & e^{\frac{2\pi i}{2^2 \cdot 6}} & e^{\frac{2\pi i}{2^2 \cdot 9}} \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2^2}} \cdot \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} \quad (4.19)$$

$$|\psi_1\rangle = \frac{1}{\sqrt{2^2}} \cdot \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} = \frac{1}{2} \cdot [|00\rangle + |01\rangle + |10\rangle + |11\rangle] \quad (4.20)$$

So it's possible to conclude that the oracle has 2 Hadamard Gates because the input $|00\rangle$ becomes $\frac{1}{2} \cdot [|00\rangle + |01\rangle + |10\rangle + |11\rangle]$:

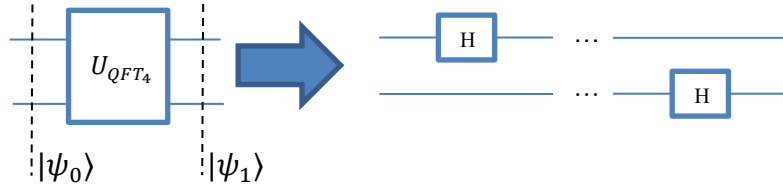


Figure 29: Decomposing U_{QFT_4} Oracle components \rightarrow Hadamard Gates

If $|\psi_0\rangle = |01\rangle = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}$, the result of $|\psi_1\rangle$ becomes:

$$\frac{1}{\sqrt{2^2}} \cdot \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & e^{\frac{2\pi i}{2^2 \cdot 1}} & e^{\frac{2\pi i}{2^2 \cdot 2}} & e^{\frac{2\pi i}{2^2 \cdot 3}} \\ 1 & e^{\frac{2\pi i}{2^2 \cdot 2}} & e^{\frac{2\pi i}{2^2 \cdot 4}} & e^{\frac{2\pi i}{2^2 \cdot 6}} \\ 1 & e^{\frac{2\pi i}{2^2 \cdot 3}} & e^{\frac{2\pi i}{2^2 \cdot 6}} & e^{\frac{2\pi i}{2^2 \cdot 9}} \end{bmatrix} \cdot \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2^2}} \cdot \begin{bmatrix} 1 \\ e^{\frac{2\pi i}{2^2 \cdot 1}} \\ e^{\frac{2\pi i}{2^2 \cdot 2}} \\ e^{\frac{2\pi i}{2^2 \cdot 3}} \end{bmatrix} \quad (4.21)$$

$$|\psi_1\rangle = \frac{1}{\sqrt{2^2}} \cdot \begin{bmatrix} 1 \\ e^{\frac{2\pi i}{2^2 \cdot 1}} \\ e^{\frac{2\pi i}{2^2 \cdot 2}} \\ e^{\frac{2\pi i}{2^2 \cdot 3}} \end{bmatrix} = \frac{1}{2} \cdot \begin{bmatrix} 1 \\ e^{\frac{\pi i}{2}} \\ e^{\pi i} \\ e^{\frac{3\pi i}{2}} \end{bmatrix} = \frac{1}{2} \cdot [|00\rangle + e^{\frac{\pi i}{2}}|01\rangle + e^{\pi i}|10\rangle + e^{\frac{3\pi i}{2}}|11\rangle] \quad (4.22)$$

$$|\psi_1\rangle = \frac{1}{\sqrt{2^2}} \cdot \begin{bmatrix} 1 \\ e^{\frac{2\pi i}{2^2 \cdot 1}} \\ e^{\frac{2\pi i}{2^2 \cdot 2}} \\ e^{\frac{2\pi i}{2^2 \cdot 3}} \end{bmatrix} = \frac{1}{2} \cdot \begin{bmatrix} 1 \\ i \\ -1 \\ -i \end{bmatrix} = \frac{1}{2} \cdot [|00\rangle + i|01\rangle - |10\rangle - i|11\rangle] \quad (4.23)$$

If $|\psi_0\rangle = |10\rangle = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}$, the result of $|\psi_1\rangle$ becomes:

$$\frac{1}{\sqrt{2^2}} \cdot \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & e^{\frac{2\pi i}{2^2 \cdot 1}} & e^{\frac{2\pi i}{2^2 \cdot 2}} & e^{\frac{2\pi i}{2^2 \cdot 3}} \\ 1 & e^{\frac{2\pi i}{2^2 \cdot 2}} & e^{\frac{2\pi i}{2^2 \cdot 4}} & e^{\frac{2\pi i}{2^2 \cdot 6}} \\ 1 & e^{\frac{2\pi i}{2^2 \cdot 3}} & e^{\frac{2\pi i}{2^2 \cdot 6}} & e^{\frac{2\pi i}{2^2 \cdot 9}} \end{bmatrix} \cdot \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2^2}} \cdot \begin{bmatrix} 1 \\ e^{\frac{2\pi i}{2^2 \cdot 2}} \\ e^{\frac{2\pi i}{2^2 \cdot 4}} \\ e^{\frac{2\pi i}{2^2 \cdot 6}} \end{bmatrix} \quad (4.24)$$

$$|\psi_1\rangle = \frac{1}{\sqrt{2^2}} \cdot \begin{bmatrix} 1 \\ e^{\frac{2\pi i}{2^2 \cdot 2}} \\ e^{\frac{2\pi i}{2^2 \cdot 4}} \\ e^{\frac{2\pi i}{2^2 \cdot 6}} \end{bmatrix} = \frac{1}{2} \cdot \begin{bmatrix} 1 \\ e^{\pi i} \\ e^{2\pi i} \\ e^{3\pi i} \end{bmatrix} = \frac{1}{2} \cdot [|00\rangle + e^{\pi i}|01\rangle + e^{2\pi i}|10\rangle + e^{3\pi i}|11\rangle] \quad (4.25)$$

$$|\psi_1\rangle = \frac{1}{\sqrt{2^2}} \cdot \begin{bmatrix} 1 \\ e^{\frac{2\pi i}{2^2 \cdot 2}} \\ e^{\frac{2\pi i}{2^2 \cdot 4}} \\ e^{\frac{2\pi i}{2^2 \cdot 6}} \end{bmatrix} = \frac{1}{2} \cdot \begin{bmatrix} 1 \\ -1 \\ 1 \\ -1 \end{bmatrix} = \frac{1}{2} \cdot [|00\rangle - |01\rangle + |10\rangle - |11\rangle] \quad (4.26)$$

If $|\psi_0\rangle = |11\rangle = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}$, the result of $|\psi_1\rangle$ becomes:

$$\frac{1}{\sqrt{2^2}} \cdot \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & e^{\frac{2\pi i}{2^2 \cdot 1}} & e^{\frac{2\pi i}{2^2 \cdot 2}} & e^{\frac{2\pi i}{2^2 \cdot 3}} \\ 1 & e^{\frac{2\pi i}{2^2 \cdot 2}} & e^{\frac{2\pi i}{2^2 \cdot 4}} & e^{\frac{2\pi i}{2^2 \cdot 6}} \\ 1 & e^{\frac{2\pi i}{2^2 \cdot 3}} & e^{\frac{2\pi i}{2^2 \cdot 6}} & e^{\frac{2\pi i}{2^2 \cdot 9}} \end{bmatrix} \cdot \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2^2}} \cdot \begin{bmatrix} 1 \\ e^{\frac{2\pi i}{2^2 \cdot 3}} \\ e^{\frac{2\pi i}{2^2 \cdot 6}} \\ e^{\frac{2\pi i}{2^2 \cdot 9}} \end{bmatrix} \quad (4.27)$$

$$|\psi_1\rangle = \frac{1}{\sqrt{2^2}} \cdot \begin{bmatrix} 1 \\ e^{\frac{2\pi i}{2^2 \cdot 3}} \\ e^{\frac{2\pi i}{2^2 \cdot 6}} \\ e^{\frac{2\pi i}{2^2 \cdot 9}} \end{bmatrix} = \frac{1}{2} \cdot \begin{bmatrix} 1 \\ e^{\frac{3\pi i}{2}} \\ e^{3\pi i} \\ e^{\frac{9\pi i}{2}} \end{bmatrix} = \frac{1}{2} \cdot [|00\rangle + e^{\frac{3\pi i}{2}}|01\rangle + e^{3\pi i}|10\rangle + e^{\frac{9\pi i}{2}}|11\rangle] \quad (4.28)$$

$$|\psi_1\rangle = \frac{1}{\sqrt{2^2}} \cdot \begin{bmatrix} 1 \\ e^{\frac{2\pi i}{2^2 \cdot 3}} \\ e^{\frac{2\pi i}{2^2 \cdot 6}} \\ e^{\frac{2\pi i}{2^2 \cdot 9}} \end{bmatrix} = \frac{1}{2} \cdot \begin{bmatrix} 1 \\ -i \\ -1 \\ 1 \end{bmatrix} = \frac{1}{2} \cdot [|00\rangle - i|01\rangle - |10\rangle + |11\rangle] \quad (4.29)$$

To get this result the circuit should be as described in Figure 30:

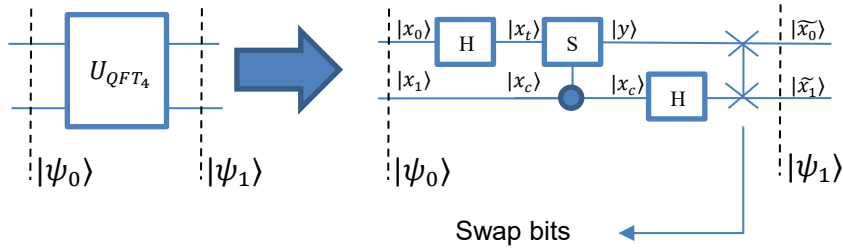


Figure 30: Decomposing U_{QFT_4} Oracle components \rightarrow Hadamard Gates + S Gate

Because

$$|y\rangle = \begin{cases} |x_t\rangle, & x_c = 0 \\ S|x_t\rangle, & x_c = 1 \end{cases} \quad (4.30)$$

And it is important to implement the Swap of bits in the end as the result bits are in the reverse order.

For N components it's fundamental to define R_n :

$$R_n \equiv \begin{bmatrix} 1 & 0 \\ 0 & e^{\frac{2\pi i}{2^n}} \end{bmatrix} \quad (4.31)$$

The first Gate R_2 was already defined:

$$R_2 \equiv \begin{bmatrix} 1 & 0 \\ 0 & e^{\frac{2\pi i}{2^2}} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} = S \quad (4.32)$$

Having said that, the generalization of the circuit U_{QFT_N} is as described in Figure 31.

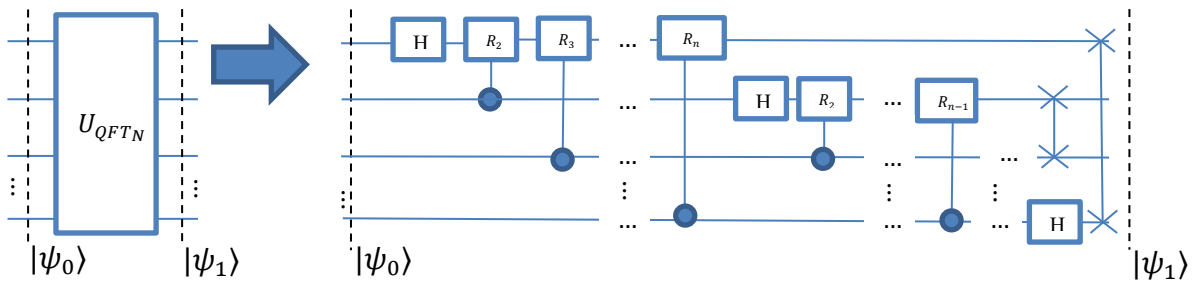


Figure 31: Decomposing U_{QFT_N} Oracle components \rightarrow Hadamard Gates + R Gates

4.2. Quantum Phase Estimation (QPE)

Another important concept is quantum phase estimation (QPE). As seen in the subchapter above the QFT performs a change of basis from a computational basis to a Fourier basis but does not solve a real problem. QPE solves a real problem in the sense that it finds a phase θ from a unitary Matrix U with eigenvector $|u\rangle$ and eigenvalue λ .

$$U|u\rangle = \lambda|u\rangle \tag{4.33}$$

Where λ could be represented as $\lambda = e^{2\pi i\theta}$

$$U|u\rangle = e^{2\pi i\theta}|u\rangle, \quad 0 \leq \theta < 1 \tag{4.34}$$

To start it's important to define a control U gate. Considering that Control U Gate is represented by:

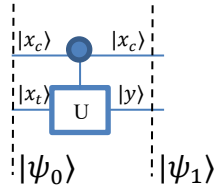


Figure 32: Unitary Control-U Gate

Where $|y\rangle$ equals to

$$|y\rangle = \begin{cases} |x_t\rangle, & x_c = 0 \\ U|x_t\rangle, & x_c = 1 \end{cases} \tag{4.35}$$

And applying Hadamard on an n qubits state is represented by $H^{\otimes n}$:

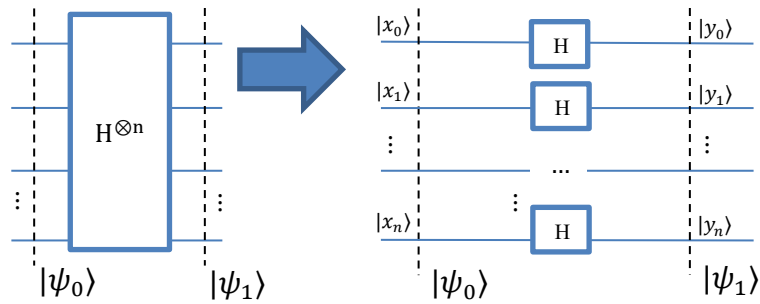


Figure 33: Hadamard $H^{\otimes n}$ Gate

$$H^{\otimes n}|\psi_0\rangle = |\psi_1\rangle \tag{4.36}$$

$$H^{\otimes n}|x_0x_1 \dots x_n\rangle = |y_0y_1 \dots y_n\rangle \tag{4.37}$$

$$H|x_0\rangle \otimes H|x_1\rangle \otimes \dots \otimes H|x_n\rangle = |y_0\rangle \otimes |y_1\rangle \otimes \dots \otimes |y_n\rangle \tag{4.38}$$

Now gathering these pieces, the QPE algorithm circuit for n qubits is defined by:

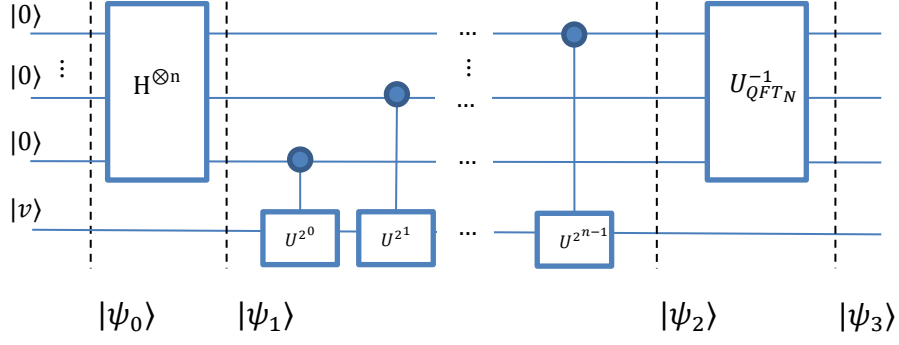


Figure 34: QPE circuit

And the result is calculated as follows:

$$|\psi_0\rangle = |0\rangle^{\otimes n} \otimes |v\rangle \quad (4.39)$$

$$|\psi_1\rangle = \left(\frac{1}{\sqrt{2}}\right)^n [(|0\rangle + |1\rangle)^{\otimes n}] \otimes |v\rangle \quad (4.40)$$

$$|\psi_2\rangle = \left(\frac{1}{\sqrt{2}}\right)^n [(|0\rangle + U^{2^{n-1}}|1\rangle) \otimes \dots \otimes (|0\rangle + U^{2^1}|1\rangle) \otimes (|0\rangle + U^{2^0}|1\rangle)] \otimes |v\rangle \quad (4.41)$$

$$|\psi_2\rangle = \left(\frac{1}{\sqrt{2^n}}\right) [(|0\rangle + e^{2\pi i \theta 2^{n-1}}|1\rangle) \otimes \dots \otimes (|0\rangle + e^{2\pi i \theta 2^0}|1\rangle)] \otimes |v\rangle \quad (4.42)$$

$$|\psi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{2\pi i k \theta} |k\rangle \otimes |v\rangle \quad (4.43)$$

The inverse QFT is given by:

$$U_{QFT}^{-1} = \left[\frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} \sum_{j=0}^{2^n-1} e^{\frac{2\pi i k j}{2^n}} |k\rangle \right]^{-1} \quad (4.44)$$

So the relation between θ and k is:

$$\theta = \frac{k}{2^n} \quad (4.45)$$

$$2^n \theta = k \quad (4.46)$$

Concluding the result becomes:

$$|\psi_3\rangle = |2^n \theta\rangle \otimes |v\rangle \quad (4.47)$$

4.3.RSA Protocol

Before trying to break the RSA protocol, it is important to understand how it works.

RSA protocol is a secure encryption protocol that encrypts a message in a way that it's almost impossible to decrypt by knowing only the encrypted message and the encryption rule (key). Four steps are involved:

1. Key Generation;
2. Key Distribution;
3. Message encryption;
4. Message decryption;

In the key generation phase two keys (K_s and K_p) are generated

- K_s is the secret key (also known as private key) with components (d and M).
- K_p is the public key with components (e and M).

To generate the keys the following rules should be followed:

- Choose two prime numbers (meaning that the numbers should have only 2 factors: 1 and themselves): p and q
- Compute $M = pq$ (M equals to p times q)
- Choose e in the way that $1 < e < \phi(M)$, where
 - $\phi(M) = (p - 1)(q - 1)$
 - Being $\phi(M)$ the Euler's totient function (a function that gives the number of integers that are coprime to M) with the following property:
 - $\phi(p) = (p - 1)$
 - A specific case of $\phi(M) = \prod_{M|p} M \left(1 - \frac{1}{p}\right)$, for prime $p > 1$
 - $\phi(q) = (q - 1)$
 - A specific case of $\phi(M) = \prod_{M|q} M \left(1 - \frac{1}{q}\right)$, for prime $q > 1$
 - $\phi(M) = \phi(p) \phi(q) = (p - 1)(q - 1)$
 - Moreover the greatest common divisor between e and $\phi(M)$ (the largest positive integer that divides each of the integers) are equal to 1: $\gcd(e, \phi(M)) = 1$
 - Compute d in the way that $1 < d < \phi(M)$, where
 - $\phi(M) = (p - 1)(q - 1)$
 - And $\underbrace{ed}_{a} \equiv \underbrace{1}_{b} \pmod{\left(\frac{\phi(M)}{s}\right)}$
 - These two integers (a and b) are said to be congruent $\text{mod } S$, if $S > 1 \in \mathbb{Z}$ is a divisor of their difference ($a - b = kS$): The congruence relation could be written as $a = kS + b$

The encryption process is described by the below example:

- Alice sends a message to Bob
 1. Alice receives from Bob the public key $K_p \rightarrow (M, e)$
 2. Alice transforms the message (Text) into an integer (using for example the ASCII Code) T
 3. Alice sends to Bob ciphertext C :
 - $C \equiv T^e \pmod{M}$
- Bob receives the message and understands the content
 1. Bob receives the ciphertext C
 - $C \equiv T^e \pmod{M}$
 2. Having the secret key $K_s \rightarrow (M, d)$, bob applies d on C
 - $C^d \equiv (T^e \pmod{M})^d$

Since $ed \equiv 1 \pmod{\phi(M)}$, the result becomes:

 - $C^d \equiv T^{ed} \pmod{M}$
 - $C^d \equiv T^{ed} \pmod{M} = T^{k\phi(M)+1} \pmod{M}$
 - $C^d \equiv T^{\phi(M)k} \cdot T^1 \pmod{M}$

Applying Euler's Theorem the result becomes

 - $C^d \equiv T^{M-1k} \cdot T^1 \pmod{M}$
 - Applying Fermat's Little Theorem the result becomes
 - $C^d \equiv 1^k \cdot T^1 \pmod{M} = T$
 3. Convert T to letters (using for example ASCII Code)

4.4. Breaking RSA Protocol

One of the practical utilities that the Shor algorithm has is breaking the RSA protocol. The Shor Algorithm has several steps that can be computed by classical computers. One of the steps should be performed by a quantum computer. The step performed by quantum computation is finding the period of modular arithmetic.

Steps to break RSA protocol

- 1) Firstly, to find factors (p and q) of the number M (seen in the earlier subchapter), it's necessary to find a coprime number a with M (meaning a don't share any common divisor with M).

Choose an a , with the condition:

$$\gcd(a, M) = 1 \tag{4.48}$$

- 2) Using quantum computation find the smallest r of the function that makes the statement $a^r \pmod{M} \equiv 1 \pmod{M}$ true.

Being r a period representation of the modular arithmetic of M , r can be repeated k times. This means that the function $f(x)$ is equal to $f(x + kr)$

$$f(x) = f(x + kr) \equiv a^x \pmod{M} = a^{x+kr} \pmod{M}, \quad k \text{ and } r \in \mathbb{N} \quad (4.49)$$

- 3) Having calculated the value of r , it's necessary to validate if r is even or if it is odd.
 - a) If the value of r is odd:
 - i) It's necessary to choose a new value of a and run step 1) again.
 - b) If the value of r is even:
 - i) It's necessary to calculate b :

$$b \equiv a^{\frac{r}{2}} \pmod{M} \quad (4.50)$$

(1) If $b + 1 \not\equiv 0 \pmod{M}$ then

$$\{p, q\} = \{\gcd(b + 1, M), \gcd(b - 1, M)\} \quad (4.51)$$

(2) Else It's necessary to choose a new value of a and do step 1) again.

Having p and q , it's possible to find e and d using the steps of the subchapter containing steps to compute RSA protocol.

4.4.1. Quantum circuit to find period r

To find period r using quantum computation, it's necessary to define the quantum circuit.

Starting with the oracle $U_{f_{a,M}}$, the circuit is defined in Figure 35.

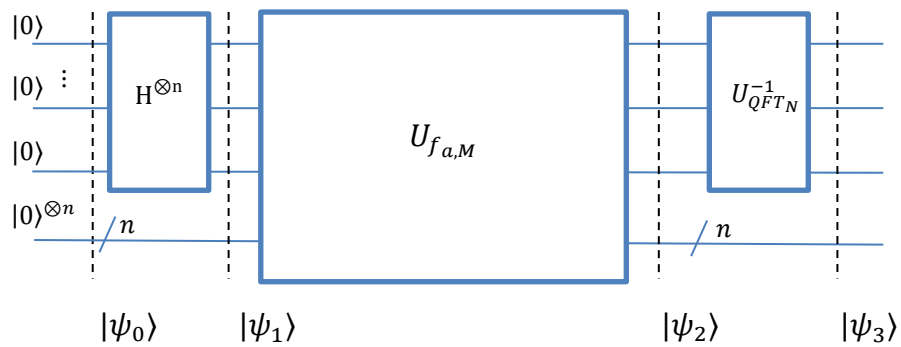


Figure 35: Shor circuit to find period r using oracle $U_{f_{a,M}}$

Where:

$$f_{a,M}(x) \equiv a^x \pmod{M} \quad (4.52)$$

Being $x = [x_1 x_2 x_3 \dots x_n]$, the result becomes:

$$f_{a,M}(x) \equiv a^x \text{ mod}(M) \quad (4.53)$$

$$f_{a,M}(x) \equiv a^{2^{n-1}x_1 + \dots + 2^1x_{n-1} + 2^0x_n} \text{ mod}(M) \quad (4.54)$$

$$f_{a,M}(x) \equiv a^{2^{n-1}x_1} \dots a^{2^1x_{n-1}} a^{2^0x_n} \text{ mod}(M) \quad (4.55)$$

And the circuit is defined in Figure 36.

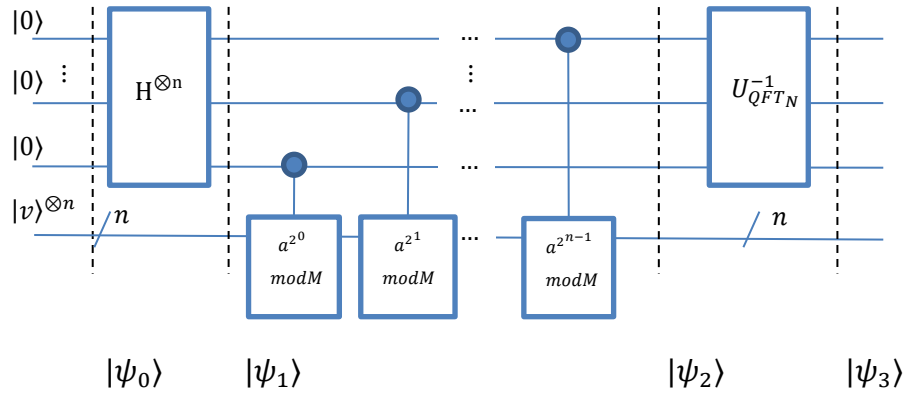


Figure 36: Shor circuit to find period r

Now it's possible to use quantum phase estimation on the unitary operator:

$$U|y\rangle \equiv |ay \text{ mod } M\rangle \quad (4.56)$$

It's possible to find the period r (first integer different than zero that turns $a^r \text{ mod } M = 1$) from a unitary Matrix U with eigenvector $|u\rangle$ and eigenvalue λ :

$$U|u\rangle = \lambda|u\rangle \quad (4.57)$$

Where λ could be represented as $\lambda = e^{2\pi i\theta}$ as seen QPE subchapter (because this problem is in the fact a QPE disguised)

$$U|u\rangle = e^{2\pi i\theta}|u\rangle \quad (4.58)$$

Where the eigenvector is:

$$|u\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-\frac{2\pi ik}{r}} |a^k \text{ mod } M\rangle \quad (4.59)$$

And the result is calculated as follows:

$$|\psi_0\rangle = |0\rangle^{\otimes n} \otimes |v\rangle^{\otimes n} \quad (4.60)$$

$$|\psi_1\rangle = \left(\frac{1}{\sqrt{2}}\right)^n [(|0\rangle + |1\rangle)^{\otimes n}] \otimes |v\rangle^{\otimes n} \quad (4.61)$$

$$|\psi_2\rangle = \left(\frac{1}{\sqrt{2}}\right)^n [(|0\rangle + U^{2^{n-1}}|1\rangle) \otimes \dots \otimes (|0\rangle + U^{2^1}|1\rangle) \otimes (|0\rangle + U^{2^0}|1\rangle)] \otimes |v\rangle \quad (4.62)$$

$$|\psi_2\rangle = \left(\frac{1}{\sqrt{2^n}}\right) [(|0\rangle + e^{2\pi i\theta^{2^{n-1}}}|1\rangle) \otimes \dots \otimes (|0\rangle + e^{2\pi i\theta^{2^0}}|1\rangle)] \otimes |v\rangle \quad (4.63)$$

$$|\psi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{2\pi i k \theta} |k\rangle \otimes |v\rangle \quad (4.64)$$

The inverse QFT is given by:

$$U_{QFT_N}^{-1} = \left[\frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} \sum_{j=0}^{2^n-1} e^{\frac{2\pi i k j}{2^n}} |k\rangle \right]^{-1} \quad (4.65)$$

And the relation between phase θ and k is given by is:

$$\theta = \frac{k}{2^n} \quad (4.66)$$

$$2^n \theta = k \quad (4.67)$$

And r is given by

$$k = 2^n \cdot \frac{s}{r} \quad (4.68)$$

With s being a random integer between 0 and $r - 1$.

Concluding the result becomes:

$$|\psi_3\rangle = |2^n \cdot \frac{s}{r}\rangle \otimes |v\rangle \quad (4.69)$$

5. Conclusions and Future Work

5.1. Conclusions

As stated in the introduction, the computer field started with Alan Turing in 1936 [2], and the study of the quantum computing field started in 1982 with Richard Feynman [6]. In the beginning, it was a theoretical study. Then, theoretical concepts started to become more known and more solid. Concepts such as quantum parallelism allowed algorithms like Deutsch's Algorithm to demonstrate the power of quantum computation over classical computation.

More complex algorithms such as Shor's Algorithm (originally designed to solve the problem of large number factorization) appeared, exposing some vulnerabilities of encryption codes such as RSA encryption code. The first RSA number generated was the RSA-100 (100 decimal digits which are equivalent to 330 classical bits). The latest version is the RSA-2048 (which consists of a number with 617 decimal digits, equivalent to 2048 bits, which are commonly used to exchange encrypted messages between two parties).

In 2016, a real five-qubit computer was introduced to the world by IBM [15]. Although this was 5 years ago, today it is still not possible to have a fully functional computer with more than 200 qubits.

Building a quantum computer is only useful if it can solve problems that no classical computer can solve in a feasible amount of time (such as factoring products of large prime numbers). When a quantum computer can do this it means that Quantum Supremacy was reached [16].

The main reason for not having reached yet this great era is Quantum Decoherence. Quantum Decoherence is the opposite of coherence, meaning that the result could be faulty, being impossible to know a result without errors and that affects the output result. In classical computation, the problem is solved mainly by adding redundancy. In quantum computation, the same is not possible because of the no-cloning theorem, which affirms that it is impossible to make a copy of a unitary state (qubit state) out of another unitary state [17]. There are two ways to solve this issue: by creating a quantum computer with more stable qubits or by improving quantum error correction techniques. Both solutions are complicated to implement, but there is still hope and every year small improvements that allow this field to grow are seen.

According to the latest state of art Google's Craig Gidney and KTH's Martin Ekera quantum journal paper, it will be necessary to build a quantum computer with 20 million qubits to break the RSA-2048 encryption code using an improved version of Shor's algorithm [18].

Although there seems to be a long way to go, history has taught us that change will happen and perhaps, sooner than we expect.

5.2.Future work

As quantum computation emerged, some known encryption codes are becoming more threatened. With the increase of power, there comes also a great responsibility. Being said that, it's necessary to prepare for the future and try to mitigate the risks that come along with quantum computation. So the risk should be approached and a plan of mitigation should be prepared.

There are two ways to mitigate the problem:

1. Study, improvement, and implementation of quantum-resistant cryptography.
2. Study, improvement, and implementation of quantum-based cryptography

The first approach could start now even using classical computers. These quantum-resistant algorithms do not guarantee to be 100% resistant but are much more secure. These are known as symmetric algorithms and the strongest one is known as AES-256 (Advanced Encryption Standard with 256 bits). Grover's algorithm could be used to weaken these encryption algorithms, but it only can weaken them being still impossible to break it in a feasible time.

The second approach relies on the fact that this type of cryptography cannot be made by classical computers, but only by quantum devices using quantum properties. Although they are made for quantum computation they should also be resistant not only from quantum computation attacks but also from classical computation attacks. This new type of quantum encryption explores the already discussed concepts like superposition, entanglement, the observer effect that makes the collapse of the result, and the no-cloning theorem.

Future work includes the exploration of these two types of cryptography to better prepare the upcoming transition to the world with quantum computers.

6. References

- [1] T. Corman, C. Leiserson, R. Rivest and C. Stein, Introduction to Algorithms, 2nd ed., McGraw-Hill, 2002.
- [2] A. M. Turing, "On computable numbers, with an application to the Entscheidungsproblem," *Proceedings of the London Mathematical Society*, vol. 42, pp. 230-265, 1937.
- [3] J. v. Neumann, "First Draft of a Report on the EDVAC," *IEEE Annals of the History of Computing*, vol. 15, pp. 27-75, 1993.
- [4] M. Nielsen and I. Chuang, Quantum Computation and Quantum Information, Cambridge University Press, 2000.
- [5] G. E. Moore, "Cramming more components onto integrated circuits," *Electronics*, vol. 38, 1965.
- [6] R. P. Feynman, "Simulating physics with computers," *International Journal of Theoretical Physics*, vol. 21, pp. 467-488, 1982.
- [7] D. Deutsch, "Quantum theory, the Church-Turing principle and the universal quantum computer," *Proceedings of the Royal Society of London*, pp. 97-117, 1985.
- [8] N. D. Mermin, "BOOJUMS ALL THE WAY THROUGH: Communicating Science in a Prosaic Age," New York, Cambridge University Press, 1990.
- [9] A. Einstein, B. Podolsky and N. Rosen, "Can quantum-mechanical description of physical reality be considered complete?," *Physical Review*, p. 777-780, 1935.
- [10] J. S. Bell, "On the Einstein Podolsky Rosen Paradox," *Physics, Physique, Fizika*, p. 777-780, 1964.
- [11] A. Aspect, P. Grangier and G. Roger, "Experimental Realization of Einstein-Podolsky-Rosen-Bohm Gedanken experiment: A New Violation of Bell's Inequalities," *Phys. Rev. Lett.*, vol. 49, pp. 91-94, 1982.
- [12] G. Ghirardi, "Sneaking a Look at God's Cards - Unraveling the Mysteries of Quantum Mechanics," Princeton University Press, 2007.

- [13] S. Popescu and D. Rohrlich , "Quantum Nonlocality as an Axiom," *Foundations of Physics*, vol. 24, p. 379, 1994.
- [14] D. Greenberger, M. Horne, A. Shimony and A. Zeilinger, "Bell's theorem without inequalities," *American Journal of Physics*, no. 58 (12), pp. 1131-1143, 1990.
- [15] C. Bernhardt, *Quantum Computing for Everyone*, The MIT Press, 2019, p. 183.
- [16] J. Preskill, "Quantum computing and the entanglement frontier," in *The Theory of the Quantum World*, Brussels, 2011.
- [17] W. Wootters and W. Zurek, "A Single Quantum Cannot be Cloned," *Nature*, vol. 299, pp. 802-803, 1982.
- [18] C. Gidney and M. Ekerå, "How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits," *Quantum*, vol. 5, p. 433, 2021.

Appendix A

Malus Law (Quantum interpretation)

In classical physic, the malus law equation is given by:

$$I_2 = I_1 \cos^2(\theta) \quad (\text{A.1})$$

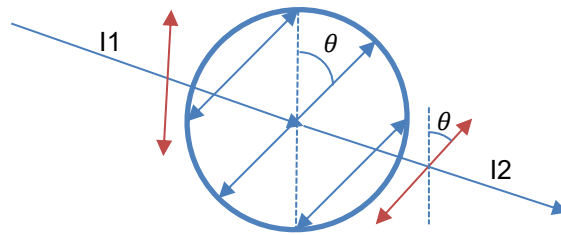


Figure 37: The transmitted light's intensity according to the Malus law

Where I_1 is the linearly polarized light intensity input and I_2 is the transmitted linearly polarized light intensity.

In this equation the result will always depend on θ (angle between the light's initial polarization direction and the axis of the polarizer), therefore the intensity will be diminished. The maximum value is when $I_2 = I_1$ and occurs when $\cos^2(0^\circ) = 1$

For quantum physic, the concept of intensity is not completely accurate, because the light does not behave as a wave but rather as a particle (photon).

Being said that, the photon either passes through the polarizer or not.

A.1 Single-photon

The only explanation possible is that fewer photons exit the polarizer because after passing a linear polarizer each photon has the same energy as before.

For the case of photon prepared in the horizontal polarization (x-axis) we have:

$$|\Psi\rangle = |0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad (\text{A.1.2})$$

And eigenvectors associated with a linear polarizer are:

$$|v\rangle = \cos(\theta) |0\rangle + \sin(\theta) |1\rangle \quad (\text{A.1.3})$$

$$|v^\perp\rangle = -\sin(\theta)|0\rangle + \cos(\theta) |1\rangle \quad (\text{A.1.4})$$

Where θ is the angle between the polarizer and the x-axis.

Observable is

$$O = |v\rangle\langle v| \quad (\text{A.1.5})$$

And $\langle v|$ given by:

$$\langle v| = \cos(\theta)\langle 0| + \sin(\theta)\langle 1| \quad (\text{A.1.6})$$

Then

$$O|\Psi\rangle = O \cdot |0\rangle \quad (\text{A.1.7})$$

$$O|\Psi\rangle = |v\rangle\langle v| \cdot |0\rangle \quad (\text{A.1.8})$$

$$O|\Psi\rangle = |v\rangle \cdot (\cos(\theta)\langle 0| + \sin(\theta)\langle 1|) \cdot |0\rangle \quad (\text{A.1.9})$$

The inner product that results in 1 is $\langle 0|0\rangle$:

$$O|\Psi\rangle = |v\rangle \cdot \cos(\theta)\langle 0|0\rangle + \sin(\theta)\langle 1|0\rangle \quad (\text{A.1.10})$$

$$O|\Psi\rangle = |v\rangle \cdot \cos(\theta) \cdot 1 + \sin(\theta) \cdot 0 \quad (\text{A.1.11})$$

$$O|\Psi\rangle = |v\rangle \cdot \cos(\theta) \quad (\text{A.1.12})$$

And the probability that photon goes through the polarizer is given by:

$$p = \langle \Psi|O|\Psi\rangle \quad (\text{A.1.13})$$

$$p = \langle \Psi|v\rangle \cdot \cos(\theta) \quad (\text{A.1.14})$$

$$p_{\text{photon passes}} = \langle 0|(\cos(\theta) |0\rangle + \sin(\theta) |1\rangle) \cdot \cos(\theta) \quad (\text{A.1.15})$$

$$p_{\text{photon passes}} = \cos(\theta) \langle 0|0\rangle + \sin(\theta) \langle 0|1\rangle \cdot \cos(\theta) \quad (\text{A.1.16})$$

The inner product that results in 1 is $\langle 0|0\rangle$:

$$p_{\text{photon passes}} = \cos(\theta) \cdot \cos(\theta) \quad (\text{A.1.17})$$

$$p_{\text{photon passes}} = \cos^2(\theta) \quad (\text{A.1.18})$$

And the probability that photon is blocked polarizer is given by:

$$p_{\text{photon blocked}} + p_{\text{photon passes}} = 1 \quad (\text{A.1.19})$$

Knowing that

$$\cos^2(\theta) + \sin^2(\theta) = 1 \quad (\text{A.1.20})$$

$$\sin^2(\theta) = 1 - \cos^2(\theta) \quad (\text{A.1.21})$$

We have

$$p_{\text{photon blocked}} = 1 - \cos^2(\theta) = \sin^2(\theta) \quad (\text{A.1.22})$$

A.2 Entangled photons

Both v_1 and v_2 $\lambda = +1$ eigenvector

$$O_{\theta_1} = |v_1\rangle\langle v_1|$$

$$O_{\theta_2} = |v_2\rangle\langle v_2|$$

$$O = O_{\theta_1} \otimes O_{\theta_2}$$

$$O = |v_1\rangle\langle v_1| \otimes |v_2\rangle\langle v_2| = |v_1\rangle|v_2\rangle\langle v_1|\langle v_2|$$

We know that

$$\langle v_1| = \cos(\theta_1)\langle 0| + \sin(\theta_1)\langle 1|$$

$$\langle v_2| = \cos(\theta_2)\langle 0| + \sin(\theta_2)\langle 1|$$

Then

$$O|\Psi\rangle = O \cdot \left(\frac{1}{\sqrt{2}} \cdot (|00\rangle + |11\rangle)\right)$$

$$O|\Psi\rangle = |v_1\rangle|v_2\rangle\langle v_1|\langle v_2| \cdot \left(\frac{1}{\sqrt{2}} \cdot (|00\rangle + |11\rangle)\right)$$

$$O|\Psi\rangle = |v_1\rangle|v_2\rangle \cdot (\cos(\theta_1)\cos(\theta_2)\langle 00| + \cos(\theta_1)\sin(\theta_2)\langle 01| \\ + \sin(\theta_1)\cos(\theta_2)\langle 10| + \sin(\theta_1)\sin(\theta_2)\langle 11|) \cdot \left(\frac{1}{\sqrt{2}} \cdot (|00\rangle + |11\rangle)\right)$$

The inner products that result in 1 are $\langle 00|00\rangle$ and $\langle 11|11\rangle$

$$O|\Psi\rangle = \frac{1}{\sqrt{2}} |v_1\rangle|v_2\rangle \cdot (\cos(\theta_1)\cos(\theta_2) \underbrace{\langle 00|00\rangle}_1 + \sin(\theta_1)\sin(\theta_2) \underbrace{\langle 11|11\rangle}_1)$$

And

$$\cos(\theta_1 - \theta_2) = \cos(\theta_1)\cos(\theta_2) + \sin(\theta_1)\sin(\theta_2)$$

Then

$$O|\Psi\rangle = \frac{1}{\sqrt{2}} |v_1\rangle|v_2\rangle \cdot \cos(\theta_1 - \theta_2)$$

We know that

$$|v_1\rangle = \cos(\theta_1)|0\rangle + \sin(\theta_1)|1\rangle$$

$$|v_2\rangle = \cos(\theta_2)|0\rangle + \sin(\theta_2)|1\rangle$$

And the probability is given by:

$$p = \langle \Psi|O|\Psi\rangle$$

$$\langle \Psi|O|\Psi\rangle = \left(\frac{1}{\sqrt{2}} \cdot \langle 00| + \langle 11|\right) \cdot \frac{1}{\sqrt{2}} \cdot |v_1\rangle|v_2\rangle \cdot \cos(\theta_1 - \theta_2)$$

$$|v_1\rangle|v_2\rangle = (\cos(\theta_1)\cos(\theta_2)|00\rangle + \cos(\theta_1)\sin(\theta_2)|01\rangle + \sin(\theta_1)\cos(\theta_2)|10\rangle + \sin(\theta_1)\sin(\theta_2)|11\rangle)$$

The inner products that result in 1 are $\langle 00|00\rangle$ and $\langle 11|11\rangle$

$$\langle \Psi|O|\Psi\rangle = \frac{1}{2} (\cos(\theta_1)\cos(\theta_2) \underbrace{\langle 00|00\rangle}_1 + \sin(\theta_1)\sin(\theta_2) \underbrace{\langle 11|11\rangle}_1) \cdot \cos(\theta_1 - \theta_2)$$

$$\langle \Psi|O|\Psi\rangle = \frac{1}{2} \cdot \cos(\theta_1 - \theta_2) \cdot \cos(\theta_1 - \theta_2)$$

$$p_{v_1 \text{ and } v_2 \lambda=1} = \langle \Psi|O|\Psi\rangle = \frac{1}{2} \cdot \cos^2(\theta_1 - \theta_2)$$

Both v_1 and v_2 $\lambda = -1$ eigenvector

$$O_{\theta_1}^\perp = |v_1^\perp\rangle\langle v_1^\perp|$$

$$O_{\theta_2}^\perp = |v_2^\perp\rangle\langle v_2^\perp|$$

$$O^\perp = O_{\theta_1}^\perp \otimes O_{\theta_2}^\perp$$

$$O^\perp = |v_1^\perp\rangle\langle v_1^\perp| \otimes |v_2^\perp\rangle\langle v_2^\perp| = |v_1^\perp\rangle|v_2^\perp\rangle\langle v_1^\perp|\langle v_2^\perp|$$

We know that

$$\langle v_1^\perp | = -\sin(\theta_1)\langle 0 | + \cos(\theta_1)\langle 1 |$$

$$\langle v_2^\perp | = -\sin(\theta_2)\langle 0 | + \cos(\theta_2)\langle 1 |$$

Then

$$O^\perp |\Psi\rangle = O \cdot \left(\frac{1}{\sqrt{2}} \cdot (|00\rangle + |11\rangle) \right)$$

$$O^\perp |\Psi\rangle = |v_1^\perp\rangle |v_2^\perp\rangle \langle v_1^\perp | \langle v_2^\perp | \cdot \left(\frac{1}{\sqrt{2}} \cdot (|00\rangle + |11\rangle) \right)$$

$$O^\perp |\Psi\rangle = |v_1^\perp\rangle |v_2^\perp\rangle \cdot (\sin(\theta_1) \sin(\theta_2) \langle 00 | - \sin(\theta_1) \cos(\theta_2) \langle 01 | \\ - \cos(\theta_1) \sin(\theta_2) \langle 10 | + \cos(\theta_1) \cos(\theta_2) \langle 11 |) \cdot \left(\frac{1}{\sqrt{2}} \cdot (|00\rangle + |11\rangle) \right)$$

The inner products that result in 1 are $\langle 00|00\rangle$ and $\langle 11|11\rangle$

$$O^\perp |\Psi\rangle = \frac{1}{\sqrt{2}} |v_1^\perp\rangle |v_2^\perp\rangle \cdot (\sin(\theta_1) \sin(\theta_2) \underbrace{\langle 00|00\rangle}_1 + \cos(\theta_1) \cos(\theta_2) \underbrace{\langle 11|11\rangle}_1)$$

And

$$\cos(\theta_1 - \theta_2) = \cos(\theta_1) \cos(\theta_2) + \sin(\theta_1) \sin(\theta_2)$$

Then

$$O^\perp |\Psi\rangle = \frac{1}{\sqrt{2}} |v_1^\perp\rangle |v_2^\perp\rangle \cdot \cos(\theta_1 - \theta_2)$$

We know that

$$|v_1^\perp\rangle = -\sin(\theta_1)|0\rangle + \cos(\theta_1)|1\rangle$$

$$|v_2^\perp\rangle = -\sin(\theta_2)|0\rangle + \cos(\theta_2)|1\rangle$$

And the probability is given by:

$$p^\perp = \langle \Psi | O^\perp | \Psi \rangle$$

$$\langle \Psi | O^\perp | \Psi \rangle = \left(\frac{1}{\sqrt{2}} \cdot \langle 00 | + \langle 11 | \right) \cdot \frac{1}{\sqrt{2}} \cdot |v_1^\perp\rangle |v_2^\perp\rangle \cdot \cos(\theta_1 - \theta_2)$$

$$|v_1^\perp\rangle |v_2^\perp\rangle = (\sin(\theta_1) \sin(\theta_2) |00\rangle - \sin(\theta_1) \cos(\theta_2) |01\rangle - \cos(\theta_1) \sin(\theta_2) |10\rangle + \cos(\theta_1) \cos(\theta_2) |11\rangle)$$

The inner products that result in 1 are $\langle 00|00\rangle$ and $\langle 11|11\rangle$

$$\langle \Psi | O^\perp | \Psi \rangle = \frac{1}{2} (\sin(\theta_1) \sin(\theta_2) \underbrace{\langle 00|00\rangle}_1 + \cos(\theta_1) \cos(\theta_2) \underbrace{\langle 11|11\rangle}_1) \cdot \cos(\theta_1 - \theta_2)$$

$$\langle \Psi | O^\perp | \Psi \rangle = \frac{1}{2} \cdot \cos(\theta_1 - \theta_2) \cdot \cos(\theta_1 - \theta_2)$$

$$p_{v_1 \text{ and } v_2 \lambda = -1} = \langle \Psi | O^\perp | \Psi \rangle = \frac{1}{2} \cdot \cos^2(\theta_1 - \theta_2)$$

So we have

$$p_{\text{Agree}} = p_{v_1 \text{ and } v_2 \lambda = 1} + p_{v_1 \text{ and } v_2 \lambda = -1} = \frac{1}{2} \cdot \cos^2(\theta_1 - \theta_2) + \frac{1}{2} \cdot \cos^2(\theta_1 - \theta_2) = \cos^2(\theta_1 - \theta_2)$$

Then

$$p_{\text{disagree}} + p_{\text{Agree}} = 1$$

$$p_{\text{disagree}} = 1 - p_{\text{Agree}}$$

$$p_{\text{disagree}} = 1 - \cos^2(\theta_1 - \theta_2)$$

Knowing that

$$\cos^2(\theta) + \sin^2(\theta) = 1$$

$$\sin^2(\theta) = 1 - \cos^2(\theta)$$

We have

$$\theta = \theta_1 - \theta_2$$

$$p_{\text{disagree}} = \sin^2(\theta_1 - \theta_2)$$

Appendix B

Pauli Matrices and GHZ state

Pauli Matrices are defined by:

$$\mathbb{I} = |0\rangle\langle 0| + |1\rangle\langle 1| = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad (\text{B.1})$$

$$\sigma_x = |0\rangle\langle 1| + |1\rangle\langle 0| = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad (\text{B.2})$$

$$\sigma_y = i(|1\rangle\langle 0| - |0\rangle\langle 1|) = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \quad (\text{B.3})$$

$$\sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1| = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \quad (\text{B.4})$$

Having the GHZ state:

$$|\Psi\rangle_{ABC} = \frac{1}{\sqrt{2}} [|000\rangle_{ABC} + |111\rangle_{ABC}] \quad (\text{B.5})$$

The value $(\sigma_x \otimes \sigma_x \otimes \sigma_x)|000\rangle_{ABC}$ is:

$$(\sigma_x \otimes \sigma_x \otimes \sigma_x)|000\rangle_{ABC} = \sigma_x|0\rangle \otimes \sigma_x|0\rangle \otimes \sigma_x|0\rangle \quad (\text{B.6})$$

$$(\sigma_x \otimes \sigma_x \otimes \sigma_x)|000\rangle_{ABC} = (|0\rangle\langle 1| + |1\rangle\langle 0|)|0\rangle(|0\rangle\langle 1| + |1\rangle\langle 0|)|0\rangle(|0\rangle\langle 1| + |1\rangle\langle 0|)|0\rangle \quad (\text{B.7})$$

$$(\sigma_x \otimes \sigma_x \otimes \sigma_x)|000\rangle_{ABC} \quad (\text{B.8})$$

$$= \left(|0\rangle \underbrace{\langle 1|0\rangle}_0 + |1\rangle \underbrace{\langle 1|1\rangle}_1 \right) \left(|0\rangle \underbrace{\langle 1|0\rangle}_0 + |1\rangle \underbrace{\langle 1|1\rangle}_1 \right) \left(|0\rangle \underbrace{\langle 1|0\rangle}_0 + |1\rangle \underbrace{\langle 1|1\rangle}_1 \right)$$

$$(\sigma_x \otimes \sigma_x \otimes \sigma_x)|000\rangle_{ABC} = |1\rangle|1\rangle|1\rangle = |111\rangle \quad (\text{B.9})$$

The value $(\sigma_x \otimes \sigma_x \otimes \sigma_x)|111\rangle_{ABC}$ is:

$$(\sigma_x \otimes \sigma_x \otimes \sigma_x)|111\rangle_{ABC} = \sigma_x|1\rangle \otimes \sigma_x|1\rangle \otimes \sigma_x|1\rangle \quad (\text{B.10})$$

$$(\sigma_x \otimes \sigma_x \otimes \sigma_x)|111\rangle_{ABC} = (|0\rangle\langle 1| + |1\rangle\langle 0|)|1\rangle(|0\rangle\langle 1| + |1\rangle\langle 0|)|1\rangle(|0\rangle\langle 1| + |1\rangle\langle 0|)|1\rangle \quad (\text{B.11})$$

$$(\sigma_x \otimes \sigma_x \otimes \sigma_x)|111\rangle_{ABC} \quad (B.12)$$

$$= \left(|0\rangle \underbrace{\langle 1|1\rangle}_1 + |1\rangle \underbrace{\langle 1|0\rangle}_0 \right) \left(|0\rangle \underbrace{\langle 1|1\rangle}_1 + |1\rangle \underbrace{\langle 1|0\rangle}_0 \right) \left(|0\rangle \underbrace{\langle 1|1\rangle}_1 + |1\rangle \underbrace{\langle 1|0\rangle}_0 \right)$$

$$(\sigma_x \otimes \sigma_x \otimes \sigma_x)|111\rangle_{ABC} = |0\rangle|0\rangle|0\rangle = |000\rangle \quad (B.13)$$

Therefore

$$(\sigma_x \otimes \sigma_x \otimes \sigma_x)|\Psi\rangle_{ABC} = (\sigma_x \otimes \sigma_x \otimes \sigma_x) \frac{1}{\sqrt{2}} [|000\rangle_{ABC} + |111\rangle_{ABC}] \quad (B.14)$$

$$(\sigma_x \otimes \sigma_x \otimes \sigma_x)|\Psi\rangle_{ABC} = \frac{1}{\sqrt{2}} \cdot [(\sigma_x \otimes \sigma_x \otimes \sigma_x)|000\rangle_{ABC} + (\sigma_x \otimes \sigma_x \otimes \sigma_x)|111\rangle_{ABC}] \quad (B.15)$$

$$(\sigma_x \otimes \sigma_x \otimes \sigma_x)|\Psi\rangle_{ABC} = \frac{1}{\sqrt{2}} \cdot [|111\rangle_{ABC} + |000\rangle_{ABC}] \quad (B.16)$$

$$(\sigma_x \otimes \sigma_x \otimes \sigma_x)|\Psi\rangle_{ABC} = |\Psi\rangle_{ABC} \quad (B.17)$$

The value $(\sigma_x \otimes \sigma_y \otimes \sigma_y)|000\rangle_{ABC}$ is:

$$(\sigma_x \otimes \sigma_y \otimes \sigma_y)|000\rangle_{ABC} = \sigma_x|0\rangle \otimes \sigma_y|0\rangle \otimes \sigma_y|0\rangle \quad (B.18)$$

$$(\sigma_x \otimes \sigma_y \otimes \sigma_y)|000\rangle_{ABC} = (|0\rangle\langle 1| + |1\rangle\langle 0|)|0\rangle \cdot i(|1\rangle\langle 0| - |0\rangle\langle 1|)|0\rangle \cdot i(|1\rangle\langle 0| - |0\rangle\langle 1|)|0\rangle \quad (B.19)$$

$$(\sigma_x \otimes \sigma_y \otimes \sigma_y)|000\rangle_{ABC} \quad (B.20)$$

$$= \left(|0\rangle \underbrace{\langle 1|0\rangle}_0 + |1\rangle \underbrace{\langle 1|1\rangle}_1 \right) \cdot i \left(|1\rangle \underbrace{\langle 0|0\rangle}_1 - |0\rangle \underbrace{\langle 1|0\rangle}_0 \right) \cdot i \left(|1\rangle \underbrace{\langle 0|0\rangle}_1 - |0\rangle \underbrace{\langle 1|0\rangle}_0 \right)$$

$$(\sigma_x \otimes \sigma_x \otimes \sigma_x)|000\rangle_{ABC} = i^2 \cdot |1\rangle|1\rangle|1\rangle = (-1)|111\rangle = -|111\rangle \quad (B.21)$$

The value $(\sigma_x \otimes \sigma_y \otimes \sigma_y)|111\rangle_{ABC}$ is:

$$(\sigma_x \otimes \sigma_y \otimes \sigma_y)|111\rangle_{ABC} = \sigma_x|1\rangle \otimes \sigma_y|1\rangle \otimes \sigma_y|1\rangle \quad (B.22)$$

$$(\sigma_x \otimes \sigma_y \otimes \sigma_y)|111\rangle_{ABC} = (|0\rangle\langle 1| + |1\rangle\langle 0|)|1\rangle \cdot i(|1\rangle\langle 0| - |0\rangle\langle 1|)|1\rangle \cdot i(|1\rangle\langle 0| - |0\rangle\langle 1|)|1\rangle \quad (B.23)$$

$$(\sigma_x \otimes \sigma_y \otimes \sigma_y)|111\rangle_{ABC} \quad (B.24)$$

$$= \left(|0\rangle \underbrace{\langle 1|1\rangle}_1 + |1\rangle \underbrace{\langle 1|0\rangle}_0 \right) \cdot i \left(|1\rangle \underbrace{\langle 0|1\rangle}_0 - |0\rangle \underbrace{\langle 1|1\rangle}_1 \right) \cdot i \left(|1\rangle \underbrace{\langle 0|1\rangle}_0 - |0\rangle \underbrace{\langle 1|1\rangle}_1 \right)$$

$$(\sigma_x \otimes \sigma_x \otimes \sigma_x)|111\rangle_{ABC} = i^2 \cdot |0\rangle(-1)|0\rangle(-1)|0\rangle = -|000\rangle \quad (B.25)$$

Therefore

$$(\sigma_x \otimes \sigma_y \otimes \sigma_y)|\Psi\rangle_{ABC} = (\sigma_x \otimes \sigma_y \otimes \sigma_y) \frac{1}{\sqrt{2}} [|000\rangle_{ABC} + |111\rangle_{ABC}] \quad (\text{B.26})$$

$$(\sigma_x \otimes \sigma_y \otimes \sigma_y)|\Psi\rangle_{ABC} = \frac{1}{\sqrt{2}} \cdot [(\sigma_x \otimes \sigma_y \otimes \sigma_y)|000\rangle_{ABC} + (\sigma_x \otimes \sigma_y \otimes \sigma_y)|111\rangle_{ABC}] \quad (\text{B.27})$$

$$(\sigma_x \otimes \sigma_y \otimes \sigma_y)|\Psi\rangle_{ABC} = \frac{1}{\sqrt{2}} \cdot [-|111\rangle_{ABC} - |000\rangle_{ABC}] = -\frac{1}{\sqrt{2}} \cdot [|000\rangle_{ABC} + |111\rangle_{ABC}] \quad (\text{B.28})$$

$$(\sigma_x \otimes \sigma_y \otimes \sigma_y)|\Psi\rangle_{ABC} = -|\Psi\rangle_{ABC} \quad (\text{B.29})$$

And if $(\sigma_x \otimes \sigma_y \otimes \sigma_y)|\Psi\rangle_{ABC} = -|\Psi\rangle_{ABC}$, then making the same calculation it's possible to conclude that:

$$(\sigma_y \otimes \sigma_x \otimes \sigma_y)|\Psi\rangle_{ABC} = -|\Psi\rangle_{ABC} \quad (\text{B.30})$$

$$(\sigma_x \otimes \sigma_y \otimes \sigma_y)|\Psi\rangle_{ABC} = -|\Psi\rangle_{ABC} \quad (\text{6.23})$$