



Democratic People's Republic of Algeria
Ministry of Higher Education and Scientific Research
University of Kasdi Merbah Ouargla
Faculty of Mathematics and Sciences of Mater
Department of Physics



Memory

Academic Master

Domain: Science of Mater

Option: Theoretical Physics

Prepared by: Barkat Seyf Eddin & Beggse Youssra

Quantum Computing

Application: Shor's Algorithm

Discussed at the day: 2018/06/05

Before the jury:

Doctor: P. M.A. Benbitour	UKM Ouargla	MC – A –	Framer / reporter
Doctor: P. Bentouila Omar	UKM Ouargla	MC – A –	President
Doctor: P. Garbouza yasin	UKM Ouargla	MC – A –	Examiner

university Year: 2017/2018



Democratic People's Republic of Algeria
Ministry of Higher Education and Scientific Research
University of Kasdi Merbah Ouargla
Faculty of Mathematics and Sciences of Mater
Department of Physics



Memory to accomplished conditions Academic Master

Quantum Computing



Written by:

Barkat Seyf Eddin

E-Mail: seyfoamin2013gmail.com

Beggas Yousra

E-Mail: yousra166@gmail.com

Under Supervising:

P. Benbitour M.A

E-Mail : mohamedbenbitour@gmail.com



Dedication.

To my mother and father

To my family and my friends

To my teachers

To my colleagues and colleagues

To candles that burn to light up for others

To everyone who taught me characters

I dedicate this humble research to the Lord

Almighty to find acceptance and success





Thanks.

Thanks and gratitude

We must take our last steps in university life from a stand back to years
We spent it in the university with our distinguished professors who gave us a lot of
humiliation

... there is a great effort in building the future generation to re-emit the nation

And before we go forward, my name is the signs of thanksgiving, gratitude,
appreciation, and love to those

... They carried the most sacred message in life

... to those who paved our way to knowledge and knowledge

... to all our illustrious professors

Thanks and appreciation

the professor / Ben Bitour Mohamed Aabd El Wahab, and the professor Bentouila
Omar I don't forget the Examiner P. Garbouza yasin.

Which we say to him with the words of the Messenger of Allah peace be upon him

"The whale in the sea and the bird in the sky to guard the teacher of the people"

We thank all those who helped to complete this research, gave us help and provided
us with a helping hand

The information needed for this research is particularly noteworthy

the professor /

Be a scientist ... If you can not be educated ... If you can not love scientists ... if not

You can not hate them.



Table of Maters:

Continent:	Page Numbe r
I. Dedication.....	iv
II. Thanks.....	v
III. Abstract.....	vi
IV. List of contents.....	vii
V. List of Table.....	ix
VI. List of Figures.....	x
VII. List of Index.....	xi
VIII. Introduction.....	xii
<u>Chapter i:</u>	
1. The Classical Algorithm.....	2
2. Boole Algebra.....	3
A. Abstract.....	3
B. Axioms for a Boolean Algebra.....	4
C. Som baisic laws for Boolean algebra.....	5
3. Bit {0.1}.....	6
4. Classical gates:(bitwise operation) Or, Not, Not.....	6
5. Postulates of Quantum mechanics.....	7
A. Postulate1.....	7
B. Postulate2.....	7
C. Postulate3.....	8
D. Postulate4.....	9
6. Two Quantum State (up. Down).....	9
7. Quantum Bit (qubit).....	11
8. Quantum Memory (quantum register).....	12
9. Summary.....	12
<u>Chapter ii:</u>	
1. Notation.....	14
2. Quantum gates.....	16
Examples.....	21
3. Entanglement.....	
4. Teleportation.....	23
5. Non-Cloning Theorem.....	26
6. Simon’s Problem.....	27
7. Deutsch-Jozsa Problem.	29
8. Summary	31
<u>Chapter iii:</u>	
1. Shore algorithm.....	33
a. Proposition of the Problem.....	
b. QFT, DFT and Their relation to factorization.....	33
c. Application in Quantum Computing (Shor algorithm step).....	33

	d. Application.....	34
	e. Summary.....	35
IX.	Conclusion.....	38
X.	Reference's.....	39
XI.	Table of Maters.....	40
XII.	Appendix's.....	42
	Appendix A.....	
	Appendix B.....	
	Appendix C.....	xiv
		xvii
		xx

Abstract:

This research aims to demonstrating the effectiveness of quantum algorithms in the treatment of some of the most difficult problems for classical algorithms. As an example of known problem, we have the factorization of number composed by tow prime factors. There are several algorithms that solve this problem, but it takes more steps, while by the quantum Shor's algorithm it can be solved in a few steps and so less time.

As an illustration of how quantum computing is capable and expected, we have included two examples of the Simon algorithm and the Deutch-Jozsa algorithm.

Key Words:

Q-bit, Algorithm, Quantum gate, Hadamerd, QFT, Shor's Algorithm.

Cette recherche vise à démontrer l'efficacité des algorithmes quantiques dans le traitement de certains des problèmes les plus difficiles pour les algorithmes classiques. A titre d'exemple de problèmes connus, nous avons une factorisation du nombre en deux facteurs premiers. Il existe plusieurs algorithmes qui résolvent ce problème, mais par l'algorithme quantique Shor peut être résolu en quelques étapes et moins de temps.

Pour illustrer comment l'informatique quantique est capable de résoudre les problèmes nous avons inclus deux exemples : l'algorithme de Simon et l'algorithme de Deutch-Jozsa.

Les mots clé :

Q-bit, algorithme, porte quantique, Hadamerd, QFT, algorithme de Shor.

يهدف بحثنا هذا إلى إظهار مدى فعالية و نجاعة الخوارزميات الكمومية في معالجة بعض المشاكل العسيرة بالنسبة للخوارزميات الكلاسيكية، و أخذنا كمثال على المشاكل المعروفة، مشكل تحليل عدد إلى جداء عوامل أولية، صحيح أنه توجد عدة خوارزميات تقوم بحل هذا المشكل، إلا أنها تأخذ وقتا و خطوات أكثر، بينما بواسطة خوارزمية Shor الكمومية يمكن حلها في خطوات معدودة.

وكتوضيح لمدى القدرة اللتي يتيحها الحاسوب الكمومي والافاق المنتظر تحقيقها منه، أدرجنا مثالين خوارزمية Simon و خوارزمية Deutch-Jozsa.

الكلمات المفتاحية:

كيوبيت، خوارزمية، بوابات كمومية، هادامار، تحويل فوري الكمومي، خوارزمية شور.

I. List of contents:

II.	<u>Dedication</u>	iv
III.	<u>Thanks</u>	v
IV.	<u>Table of Maters:</u>	vi
V.	<u>Abstract:</u>	viii
I.	<u>List of contents</u>	ix
II.	<u>List of Table:</u>	xi
III.	<u>List of Figures:</u>	xii
IV.	<u>List of Appendix:</u>	xiii
V.	<u>List of index:</u>	xiv
VI.	<u>Introduction:</u>	xv
VII.	<u>Chapter: I</u>	
	1. The Classical Algorithm.	
	2. Boole Algebra.	
	A. Abstract.	
	B. Axioms for a Boolean Algebra.	
	C. Some basic laws for Boolean algebra	
	3. Bit {0,1}.	
	4. Classical gates:(bitwise operation) Or, Not, Not.	
	5. Postulates of Quantum mechanics.	
	Postulate1.	
	Postulate2.	
	Postulate3	
	Postulate4.	
	6. Two Quantum State (up. Down).	
	7. Quantum Bit (qubit).	
	8. n-qubit(quantum registr).	
	9. Summary.	
VIII.	<u>Chapter II:</u>	
	1. Notation.	
	2. Quantum gates.	

Examples.

3. Entanglement.
4. Teleportation.
5. Non-Cloning Theorem.
6. Simon's Problem.
7. Dutch-Jozsa Problem.
8. Summary

IX. Chapter III:

1. Shor algorithm.
 - 1.1. Proposition of the problem.
 - 1.2. QFT, DFT and Their relation to factorization.
 - 1.3. Application in Quantum Computing (Shor algorithm step).
 - 1.4. Summary.

X. Conclusion:

XI. Reference's

XII. Appendix's:

Appendix A:

Appendix B:

Appendix C:

VI. List of Table:

Table 1: Logical Gates and their graphics representation.

Table 2: the notation used in the quantum computing.

VII. List of Figures:

Graph -1- : Schematic illustrates the algorithm structure

Figure 1: Stern-Gerlach Experiment.

Figure2: Bloch Sphere TLS

Figure 3: Showing the X-gate protocol

Figure 4: The C-NOT gate notion

Figure 5: How the Controlled-Not gate work.

Figure 6: The Entanglement Phenomena with photons.

Figure 7: The teleportation scenario between Alice and Bob.

Figure 8: operation process to create a copy

Figure 9 : Simon's Algorithm circuit's.

Figure 10 : Deutsch-Jozsa quantum algorithm

Figure 11: Quantum Shor factorisation circuit.

Figure 12: the step of Shor algorithm

VIII. List of Appendix:

Appendix a: QFT

Appendix b: Classical Factorization method.

Appendix c: Q-bit realization.

IX. List of index:

Q-bit	Quantum bit
DFT	Discret Fourier transformation
QFT	Quantum Fourier transformation
$ ket\rangle$	Ket notation
$\langle bra $	Bra notation
\otimes	Tensoriel Product state
\oplus	Direct sommation
\dagger	Daguer notation (transposition*complexe conjugue)
$ \uparrow\rangle$	Up state
$ \downarrow\rangle$	Down state

Introduction:

The world's biggest jump in computing since the first computer with air valves and light bulbs was to detect integrated circuits on silicon chips, through the transistor revolution.

All this progress has been an important role in physics, and researchers around the world are still exploiting the development and progress of applications of modern physics in various fields, and the field of computing. the field of computing can not take advantage of this progress, and the idea of exploiting quantum phenomena to build what is now known as the "quantum computer" originated with Richard Feynman and David Dutch...

Under the law of a provider under which the number of transistors multiplies in a microprocessor, it is logical for the world to set up quantum computers.

Quantum computers have the ability to perform multiple calculations at the same time, with fewer steps, allowing us to accelerate many difficult applications, in quantum computing, basic computing rules change, so quantum phenomena are exploited for the construction of algorithms and quantum gates, the bit in classic can be 0 or 1, the qubit is 0 and 1 in the same time.

When we store information in classical circuit, we must read it again, this we'll be different with qubit, because you need to measure a qubit to determinate it state.

The Q-C used the **quantum parallelism**, and **entanglement** and **Superposition** phenomenon.

But the realization of a quantum computer is how to save coherence propriety of qubit, because it's very Sensitive to the outer center, researcher's try with different method's, as example

- Ion traps.
- Optical traps.
- Quantum dots.
- Semiconductor impurities.

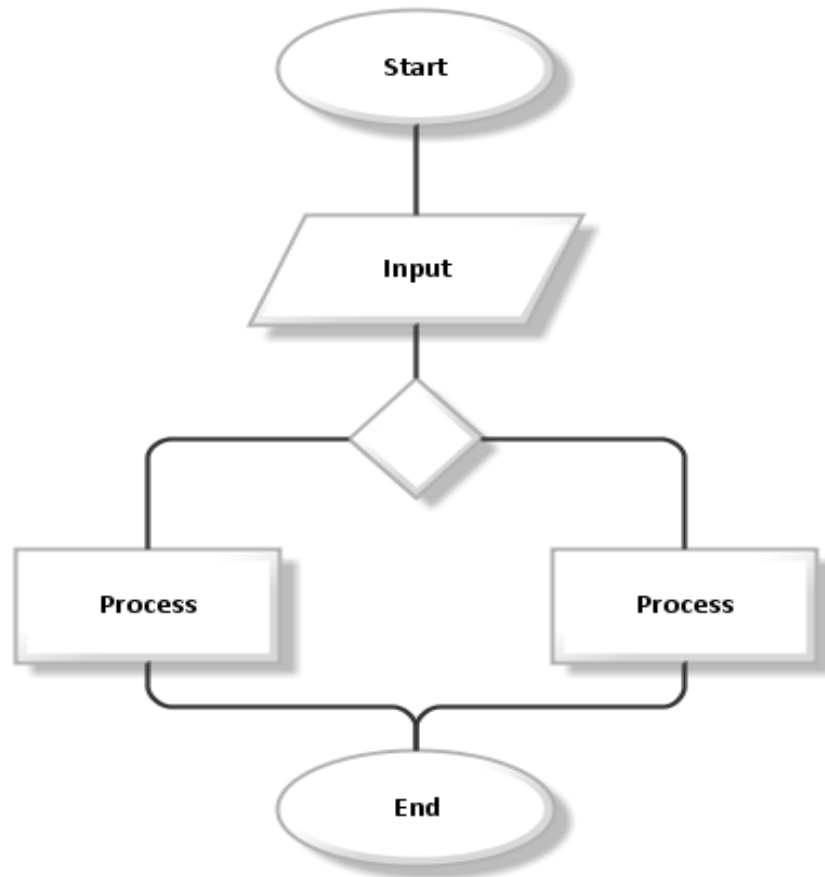
Chapter: I

1. The Classical Algorithm.
2. Boole Algebra.
 - A. Abstract.
 - B. Axioms for a Boolean Algebra.
 - C. Some basic laws for Boolean algebra
3. Bit {0,1}
4. Classical gates:(bitwise operation) Or, Not, Not.
5. Postulates of Quantum mechanics.
 - A. Postulate1.
 - B. Postulate2.
 - C. Postulate3
 - D. Postulate4.
6. Two Quantum State (up. Down).
7. Quantum Bit (qubit).
8. N qubit (quantum register).
9. Summary.

1. The Classical Algorithm :

➤ Algorithm :

It's a collection of logical steps to solve an problem in Mathematics “Algorithm” means:



Graph -1- : Schematic illustration of the algorithm's structure

And The Name Algorithm originated from to the muslim scientist “ABOU DJAFARE MOUHAMED IBN MOUSSA ALKHAWARZMI”, that who invented in the ninth century AD

Digital Logic:

All the machines (here we talked about the digital machines), are based at a simple principle, it's a representation of the information with two numbers {0 and 1}, in which every machine consists of a set of electronic circuits.

Each circuit provides a well-defined logical function (addition, comparison ...).

CHAPTER 1

Example:

$$f : \{0,1\}^m \rightarrow \{0,1\}^p \quad (1.1)$$

Example: Algorithm for Finding the roots of a quadratic equation

- 1) Start
- 2) Read the coefficient a,b,c
- 3) Calculate $z = b^2 - 4ac$
- 4) If $z < 0$ display a message roots are imaginary go to ---- Else proceed to next step
- 5) If $z = 0$ display a message roots are real and unequal and go to---Else proceed to next step----
- 6) Display a message roots are real and un equal and go to---
- 7) Calculate $r1 = r2 = \frac{-b}{2a}$, and go to step---
- 8) Calculate r1 and r2 and go to step---

$$r1 = \frac{-b + \sqrt{b^2 - 4ac}}{2a}, r2 = \frac{-b - \sqrt{b^2 - 4ac}}{2a}$$

- 9) Display roots r1 and r2
- 10) Stop

2. Booléen Algèbre :

A. Abstract :

To design and realize electronic circuits we must have a mathematical model of the function realized by this circuit, this model must take into consideration the binary system.

The mathematical model used is that of" Boolean Algebra “.

George Boole is an English mathematician (1815-1864), he has done works whose functions (expressions) are constituted by variables that can take the values 'YES' or 'NO'.

These works have been used to study systems that have two states mutually exclusive:

The system can only be in two states E1 and E2 such that E1 is the opposite of E2.

CHAPTER 1

The system can not be in state E1 and E2 at the same time, these works are well adapted to the binary system (0 and 1).

We denote a bit (0.1)

Boolean algebra is a different kind of algebra or rather can be said a new kind of algebra which was invented by world famous mathematician George Boole in the year of 1854. He published it in his book “An Investigation of the Laws of Thought”. Later using this technique Claude Shannon introduced a new type of algebras which is termed as Switching Algebras. In digital electronics there are several methods of simplifying the design of logic circuits. This algebra is one of these methods. According to George Boole symbols can be used to represent the structure of logical thoughts. This type of algebra deals with the rules or laws, which are known as laws of Boolean algebra by which the logical operations are carried out.

There are also few theorems of Boolean algebra, that are needed to be noticed carefully because these make calculation fastest and easier. Boolean logic deals with only two variables, 1 and 0 by which all the mathematical operations are to be performed.

There only three basis binary operations, AND, OR and NOT by which all simple as well as complex binary mathematical operations are to be done. There are many rules in Boolean algebra by which those mathematical operations are done. In Boolean algebra, English Capital Letter like A, B, C etc, represents the variables and the value of each variable can be either 1 or 0, nothing else. In Boolean algebra an expression given can also be converted into a logic diagram using different logic gates like AND gate, OR gate and NOT gate, NOR gates, NAND gates, XOR gates, XNOR gates etc.

Some basic logical Boolean operations, AND Operation OR Operation Not Operation
Some basic laws for Boolean Algebra.

B. Axioms for a Boolean Algebra:

1. Cumulative Law for Boolean algebra:

$$\begin{aligned} A + B + C &= A + C + B = B + A + C = B + C + A = C + A + B = C + B + A \\ A.B.C &= A.C.B = B.A.C = B.C.A = C.A.B = C.B.A \end{aligned} \quad (1.2)$$

CHAPTER 1

According to Cumulative Law, the order of **OR** operations and **AND** operations conducted on the variables makes no differences.

2. Associative Laws for Boolean algebra:

$$\begin{aligned}(A + B) + C &= A + (B + C) \\ (A \cdot B) \cdot C &= A \cdot (B \cdot C)\end{aligned}\tag{1.3}$$

This law is for several variables, where the OR operation of the variables result is same though the grouping of the variables. This law is quite same in case of AND operators.

3. Distributive Laws for Boolean algebra:

$$A \cdot (B + C) = A \cdot B + A \cdot C\tag{1.4}$$

This law is composed of two operators, **AND** and **OR**.

C. Some basic laws for Boolean algebra

$$\bar{0} = 1, \bar{1} = 0, \text{ if } A=1 \text{ then } \bar{A} = 0, \text{ and if } A=0, \text{ then } \bar{A} = 1.$$

$A \cdot 0 = 0$ where A can be either 0 or 1.

$A \cdot 1 = A$ where A can be either 0 or 1.

$A \cdot A = A$ where A can be either 0 or 1.

$A \cdot \bar{A} = 0$ where A can be either 0 or 1.

$A + 0 = A$ where A can be either 0 or 1.

$A + 1 = 1$ where A can be either 0 or 1.

$A + \bar{A} = 1$

$A + A = A$

$A + B = B + A$ where A and B can be either 0 or 1.

$A \cdot B = B \cdot A$ where A and B can be either 0 or 1.

The laws of Boolean algebra are also true for more than two variables like.

3. Bit :

Definition: We denote bit as a measurement unit of information, it is used in information computing and digital communication, while 1 bit consisted for 0 and 1, also it can represent by **true** or **false** value.

Confusion often arises because the words bit and binary digit are used interchangeably. But, within information theory, a bit and a binary digit are fundamentally different types of entities. A binary digit is a number that can adopt one of two possible values (0 or 1), whereas a bit is the maximum amount of information that can be conveyed by a binary digit. By analogy, a binary digit is like a container, whereas information is the amount of matter in the container [1].

Physical representation:

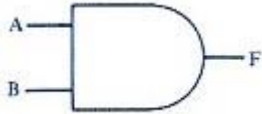
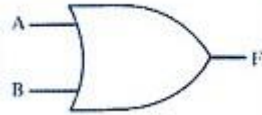
in classical machines we manipulated the bit as an electrical current, where.

0: means there is no electric signal.

1: existence of electric signal.

Between 1950 and 1960, the representation of a bit developed by magnetic polarisation of certain area of a ferromagnetic film. The bit is a base of all computing process.

4. Classical Operations (Bitwise Operations) :

Name	Graphic symbol	Algebraic Function
AND		$F = A + B$ <i>or</i> $F = AB$
OR		$F = A \div B$

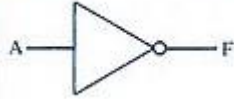
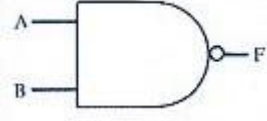
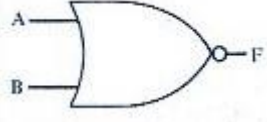
NOT		$F = \bar{A}$ or $F = A'$
NAND		$F = (\overline{AB})$
NOR		$F = (\overline{A + B})$

Table -1- Logical Gates and their graphics representation

Where \bar{x} is the complement of x .

5. Postulats of Quantum Mechanics :

I. Postulate 1: A quantum bit:

- **Postulate 1: Associated to any isolated physical system is a complex vector space with inner product (that is, a Hilbert space) known as the *state space* of the system. The system is completely described by its *state vector*, which is a unit vector in the system's state space.**

II. Postulate 2: Evolution of quantum systems:

The evolution of a closed quantum system is described by a unitary transformation.

That is, the state $|\psi\rangle$ of the system at time t_1 is related to the state $|\psi'\rangle$ of the system at time t_2 by a unitary operator U which depends only on the times t_1 and t_2 . [2]

$$|\psi'\rangle = U |\psi\rangle \quad (1.6)$$

Example:

let us take the Pauli matrices as an evolution operator and apply it on a single qubit:

1. $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$.

$$U = \sigma_x = X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$|\psi'\rangle = U|\psi\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}(\alpha|0\rangle + \beta|1\rangle) = \begin{pmatrix} \beta \\ \alpha \end{pmatrix} = \beta|0\rangle + \alpha|1\rangle$$

2. $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$.

$$U = \sigma_z = Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$|\psi'\rangle = U|\psi\rangle = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}(\alpha|0\rangle + \beta|1\rangle) = \alpha|0\rangle - \beta|1\rangle$$

3. $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$.

$$U = T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$$

$$|\psi'\rangle = U|\psi\rangle = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}(\alpha|0\rangle + \beta|1\rangle) = \alpha|0\rangle + e^{i\pi/4}\beta|1\rangle$$

III. Measurement:

- All the developments that occur within the isolated quantum system, is a unitary evolution, but once the measurement on the system of the universe is a non-unitary transformation, and to describe this development we offer the third postulate of the quantum mechanics.
- **“Postulate 3: Quantum measurements are described by a collection $\{M_m\}$ of measurement operators. These are operators acting on the state space of the system being measured. The index m refers to the measurement outcomes that may occur in the experiment. If the state of the quantum system is $|\psi\rangle$ immediately before the measurement, then the probability that result m occurs is given by”:**

$$p(m) = \langle \psi | M_m^\dagger M_m | \psi \rangle \tag{1.7}$$

The measurement operator satisfy the

$$\sum_m M_m^\dagger M_m = I \text{ condition:} \tag{1.8}$$

IV. Postulate 4: Multi-qubit systems:

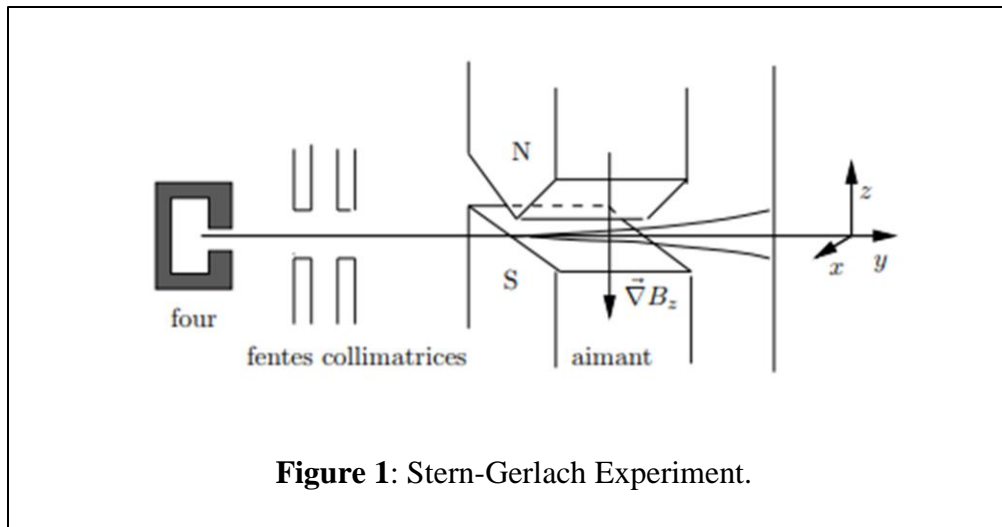


Figure 1: Stern-Gerlach Experiment.

Postulate 4: "The state space of a composite physical system is the tensor product of the state spaces of the component physical systems. Moreover, if we have systems numbered 1 through n , and system number i is prepared in the state, $|\psi_i\rangle$ then the joint state of the total system is $|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle \otimes \dots \otimes |\psi_n\rangle$ "[3]

6. Two Quantum State (up, down):

When we deal with systems in quantum level, as example **Stern-Gerlach experiment** Is give a proof that all particle has just two possible state, which described by a superposition of two state.

Mathematically this stat written as next:

$$|\xi\rangle = \alpha|+\rangle + \beta|-\rangle \tag{1.9}$$

In measurement can to have tow value: positive value with probability $|\alpha|^2$, or negative value with $|\beta|^2$.

7. Quantum Bit (qubit):

After first we should note: "Classical bit is 0 or 1, but the **qu-bit** is a superposition of 0 and 1"

- we use the Dirac notation ($|bra\rangle\langle Ket|$), and the superposition state of a physics system, Specifically systems who have tow possible state like polarisation system, Systems with spin ...

A state of those system can have represented by the state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, where $\alpha, \beta \in \mathbb{C}$ and since we require this to be a normalized state, we require that

$$|\alpha|^2 + |\beta|^2 = 1 \quad (1.5)$$

this Bit can be representing as a vector where:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \text{ and } |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \rightarrow |\psi\rangle = \alpha \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \beta \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

Also we can represent two qubits as follows

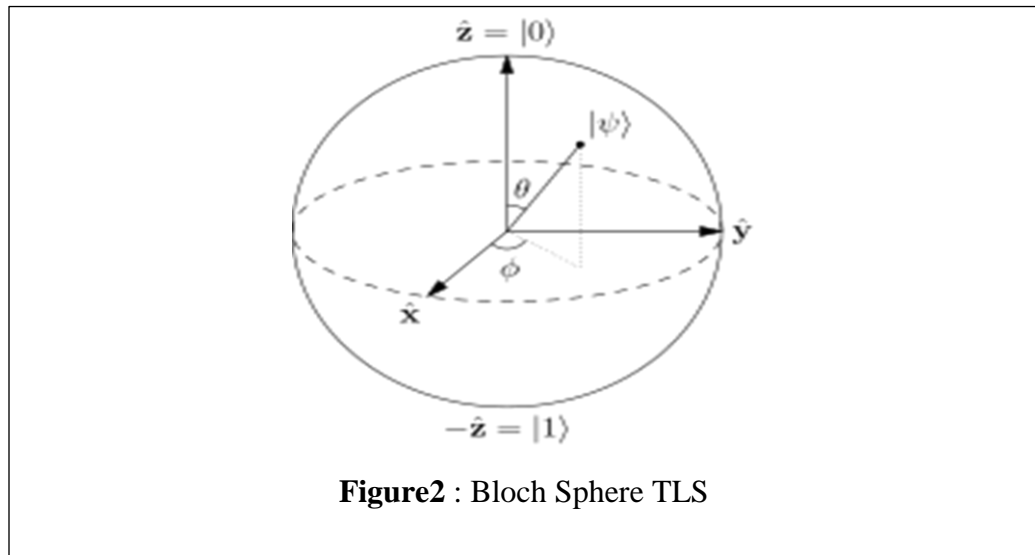
$$\alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle \rightarrow \begin{bmatrix} \alpha_{00} \\ \alpha_{01} \\ \alpha_{10} \\ \alpha_{11} \end{bmatrix} \quad (1.10)$$

where $|ab\rangle$ is the basis vector representing a state where the first qubit is in the state $|a\rangle$ and the second qubit in the state $|b\rangle$ and so on .

Each basis state represents a vector in Bloch sphere (Bloch sphere, a geometrical representation of a two-level quantum system.), such that the coefficient of the $|0\rangle$ ket is real an non-negative. Using this and the normalization constraint, it is useful to not use α and β , but instead to use:

$\alpha = \cos\left(\frac{\theta}{2}\right)$ and $\beta = e^{i\phi} \sin\left(\frac{\theta}{2}\right)$, where $0 < \theta < \pi$ and $0 < \phi < 2\pi$, you can see that when we use this notation, it give us a possibility to represent all basis vector (single qubit) in a sphere that called **Bloch Sphere**.^[4]

In classical computation, the smallest unit of DATA is the bit, element of tow element set



$\{0,1\}$, in quantum computation the smallest unit of DATA is a quantum bit, or qubit, defined as a ray in Hilbert Spaces or Bloch Sphere. [5]

8. n-qubit (Quantum Registre) :

Suppose a system of n-qubit, the state of This system described by the tonsorial product of the component of the system as follows:

$$|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle \otimes \dots \otimes |\psi_n\rangle \quad (1.11)$$

$$|\psi\rangle = \sum_{x \in \{0,1\}^n} \alpha_x |x\rangle \in \mathbb{C}^2 \quad (1.12)$$

With the condition of normalization of this system written as:

$$\sum_{x \in \{0,1\}^n} |\alpha_x|^2 = 1 \quad (1.13)$$

This formula called a quantum register described by:

$$|\varphi\rangle = \sum_{i=0}^{2^n-1} p_i |i\rangle \quad (1.14)$$

9. Summary:

The difficulties stand in front of the researchers is how to building a quantum computer is that conserve a coherence propriety.

It can build a qubit from different methods, as example:



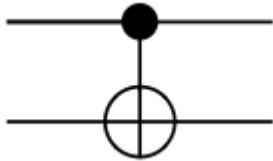



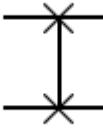
- Trapped ion.
- Entangled Photons.
- Quantum Dots.
- Nuclei of atoms.
- Superconductor.

Chapter II:

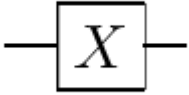
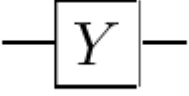
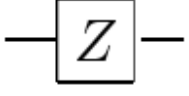
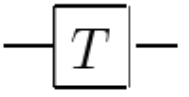
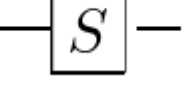
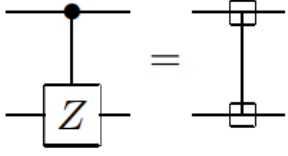
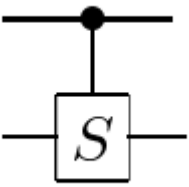
1. Notation.
2. Quantum gates.
Examples.
3. Entanglement.
4. Teleportation.
5. Non-Cloning Theorem.
6. Simon's Problem.
7. Dutch-Jozsa Problem.
8. Summary

CHAPTER 2 :

1. Notation:

Symbol of the circuit	Name of circuit	Operation
	Not= X gate	this operation applied for one qubit: $ \psi\rangle = \bar{\psi}\rangle$ $ \bar{\psi}\rangle = \psi\rangle$
	Hadamerd	$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$
	controlled-Not	$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, a, f(x)\rangle \rightarrow a, a \oplus f(x)\rangle$
	Measurement	Project on to $ 0\rangle$ or $ 1\rangle$
	Tonsorial Product	$\begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$ $\begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$
	Tonsorial summation	
	swap	$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$

CHAPTER 2 :

	Pauli-X	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
	Pauli-Y	$\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$
	Pauli-Z	$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$
	$\pi/8$	$\begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$
	Phase	$\begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$
	Controlled-Z	$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$
	Controlled-Phase	$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & i \end{pmatrix}$


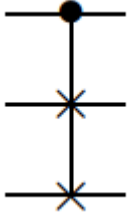


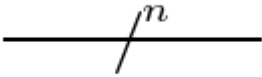
	<p>Toffoli</p>	$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$
	<p>Fredkin (Controlled-Swap)</p>	$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$
	<p>Qubit</p>	<p>Wire carrying a single qubit</p>
	<p>Classical Bit</p>	<p>Wire carrying a classical bit</p>
	<p>n qubit</p>	<p>Wire carrying n qubit</p>

Table 2 : the notation used in the quantum computing.

2. Quantum gates : [6]

The quantum gates are the operation that can be applied for a qubit, this quantum gates are the operator satisfied the next condition: Unitary and Hermitian

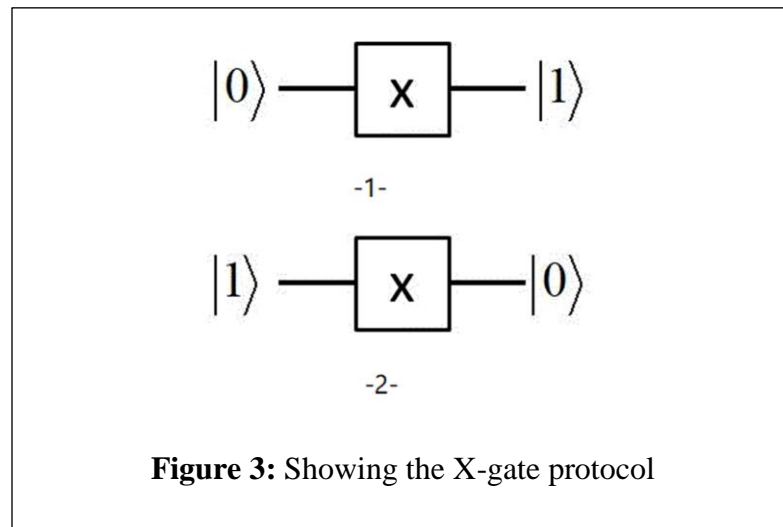
Can we say that this operation, simply is the Pauli matrix:

CHAPTER 2 :

a. **Gate for one qubit:** we have four gate con applied on a single qubit, are the Pauli matrix:

a) **Not Gate:**

$$NOT = X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad (2.1)$$



$$X |0\rangle = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle, \text{ and } X |1\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle$$

$$XX = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0+1 & 0 \times 0 \\ 0 \times 0 & 0+1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I$$

b) **Z Gate:**

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad (2.2)$$

Example: application of the Z-Gate for a qubit in the state $|0\rangle$ and $|1\rangle$.

CHAPTER 2 :

$$Z |0\rangle = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle$$

$$Z |1\rangle = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ -1 \end{pmatrix} = -|1\rangle$$

c) **T Gate:**

$$\begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix} \tag{2.3}$$

Example: application of the T-Gate for a qubit in the state $|0\rangle$ and $|1\rangle$.

$$T |0\rangle = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle$$

$$T |1\rangle = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = e^{i\pi/4} |1\rangle$$

d) **S Gate:**

$$\begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \tag{2.4}$$

Example: application of the S-Gate for a qubit in the state $|0\rangle$ and $|1\rangle$.

$$S |0\rangle = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle$$

$$S |1\rangle = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = i |1\rangle$$

e) **Y Gate:**

$$\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \tag{2.5}$$

Example: application of the Y-Gate for a qubit in the state $|0\rangle$ and $|1\rangle$.

$$Y |0\rangle = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = i |0\rangle$$

$$Y |1\rangle = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = -i |1\rangle$$

f) Hadamard Gate:

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad (2.6)$$

Example: application of the Y-Gate for a qubit in the state $|0\rangle$ and $|1\rangle$.

$$H |0\rangle = \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) ; H |1\rangle = \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)$$

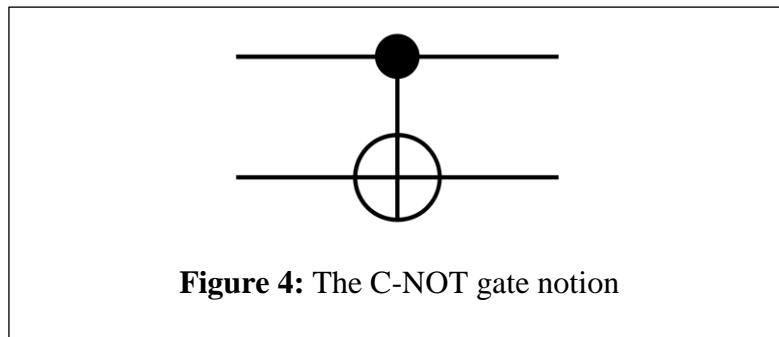
but:

$$\begin{aligned} H \left[\frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \right] &= \frac{1}{\sqrt{2}} H |0\rangle + \frac{1}{\sqrt{2}} H |1\rangle \\ &= \frac{1}{\sqrt{2}} \left[\frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \right] + \frac{1}{\sqrt{2}} \left[\frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \right] = \frac{1}{2} (|0\rangle + |1\rangle + |0\rangle - |1\rangle) = |0\rangle \end{aligned}$$

$$\begin{aligned} H \left[\frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \right] &= \frac{1}{\sqrt{2}} H |0\rangle - \frac{1}{\sqrt{2}} H |1\rangle \\ &= \frac{1}{\sqrt{2}} \left[\frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \right] - \frac{1}{\sqrt{2}} \left[\frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \right] = \frac{1}{2} (|0\rangle + |1\rangle - |0\rangle + |1\rangle) = |1\rangle \end{aligned}$$

b. Gate for two qubit:

The operation available for two qubit is the **C-NOT** gate.

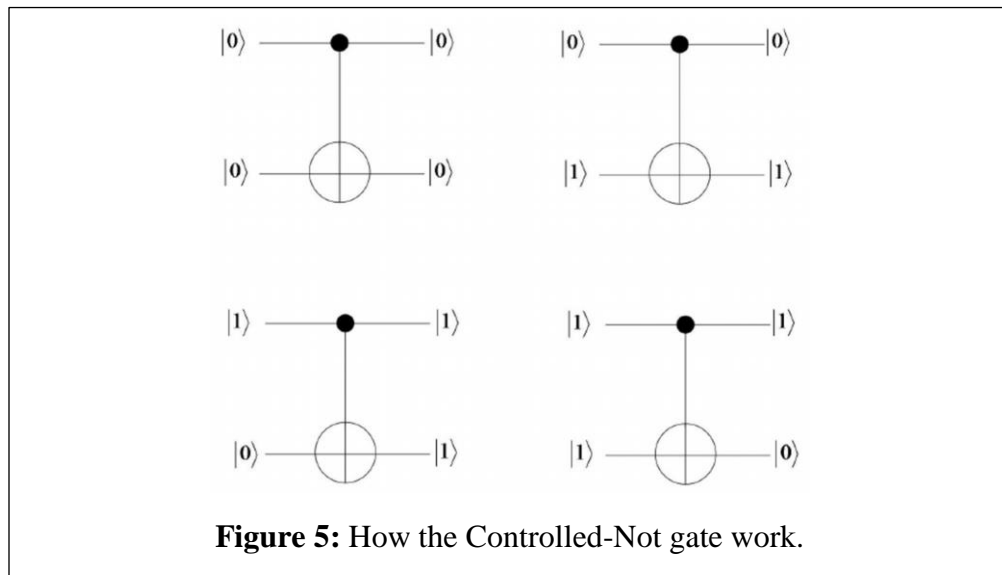


We can define C-NOT gate with two different methods, as matrix or with analytical formula.

$$C - NOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, |a,b\rangle \rightarrow |a, a \oplus b\rangle \quad (2.7)$$

All the qubit in the base n=2 written in terms of: $|00\rangle, |10\rangle, |01\rangle, |11\rangle$ basis vectors.

Applications:



c. Gate for n qubit:

The operation available for n qubit is the generalization of C-NOT.

$$U_f = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle |f(x)\rangle \quad (2.8)$$

And also the 'QFT' Quantum Fourier Transformation [7][8] : $|j\rangle \rightarrow |\chi_j\rangle$

$$|\chi_j\rangle = \frac{1}{\sqrt{q}} \sum_{k=0}^{q-1} e^{\frac{2\pi ijk}{q}} |k\rangle \quad (2.9)$$

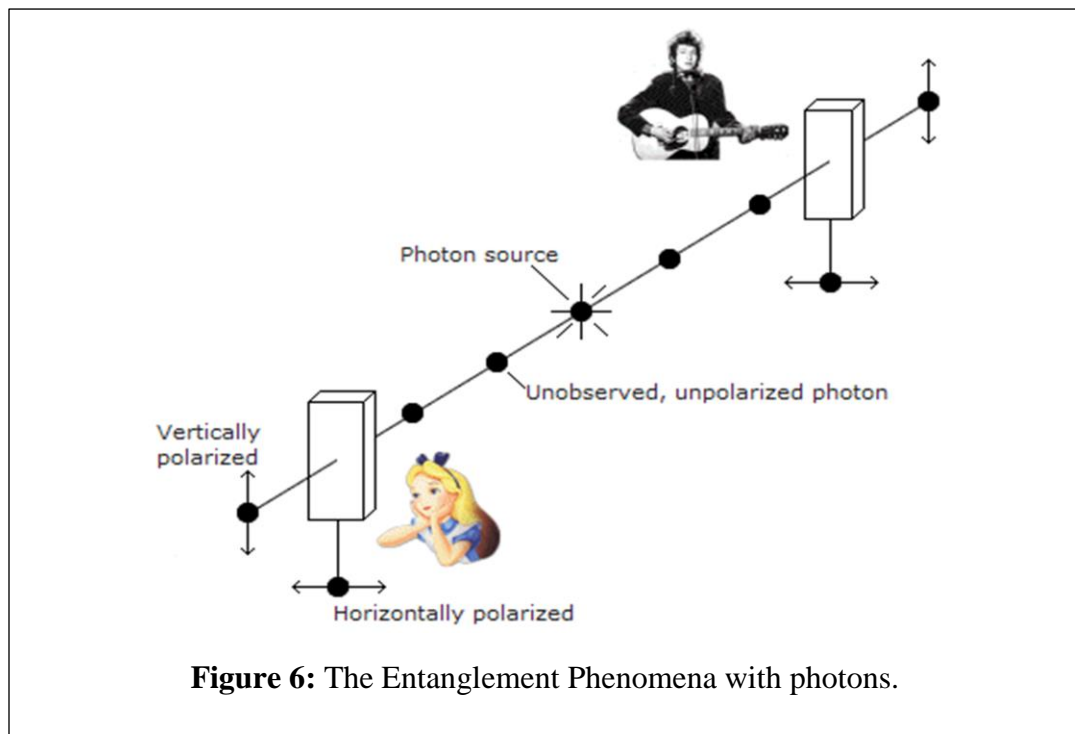
The Quantum Fourier Transformation are the generalization of HADAMER gate, we'll talk about it in a special clause.

3. Entanglement :

a. Physical meaning:

is a physical phenomenon which occurs when pairs or groups of particles are generated or interact in ways such that the quantum state of each particle cannot be described independently of the state of the other(s), even when the particles are separated by a large distance—instead, a quantum state must be described for the system as a whole. [4][5]

Here we can ask what can be done by entanglement? save this question until the Teleportation.



Suppose that the source of photon create photons in the state: $|\psi\rangle = \frac{1}{\sqrt{2}}(|1_A 1_B\rangle + |0_A 0_B\rangle)$

So when Bob measured and found her photon in the state $|1_B\rangle$, the photon of Alice take the state $|1_A\rangle$, simultaneously when Bob find her photon in the state $|0_B\rangle$, the state of

CHAPTER 2 :

Alice photon turned to $|0_A\rangle$, in more generally in the case of EPR pair, described by:

$$|\phi\rangle = \sum_{\lambda_i} \lambda_i |A_i B_i\rangle \quad , \quad \sum |\lambda_i|^2 = 1$$

when the measure detected one of them, we get an information about the other instantaneously.

Mathematical Formalism:

At first consider a state system of two Q-bit, described by the next formula:

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|10\rangle + |01\rangle) \quad (2.10)$$

When a measurement effect on a system and we find the first Q-bit in the state $|1\rangle$,

instantaneously we can said that the second Q-bit is at the state $|0\rangle$, with a probability $\frac{1}{2}$,

as well as that when we find the first qubit in the state $|0\rangle$ we found the second qubit in the state $|1\rangle$.

So more generally the state of n qubit described as next:

$$|\xi\rangle = \sum_{i=0} p_i |\psi_1 \otimes \psi_2 \otimes \dots \otimes \psi_i\rangle \quad (2.11)$$

Where:

P_i : is the probability to found the system in the state $|\psi_i\rangle$, this probability can counted by the formula:

$$P_i = |\psi_i\rangle \langle \psi_i| \quad (2.12)$$

4. Téléportation : [7]

a. Physical meaning:

Teleportation process by which quantum information can be transmitted from one location to another, the help of classical communication and previously shared quantum entanglement between the sending and receiving location.

b. Teleportation protocol:

The setup for the teleportation experiment is as follows: we start with a spin in an unknown state $\alpha|\uparrow\rangle + \beta|\downarrow\rangle$ which we are trying to teleport. This spin begins in lab A. we

also start with an entangled state «single state" with state $\frac{1}{\sqrt{2}}|\uparrow, \downarrow\rangle - \frac{1}{\sqrt{2}}|\downarrow, \uparrow\rangle$

This state consists of two spins the first of which is in lab A and the second is in lab B.

The states of all spins can be written as $\frac{\alpha}{\sqrt{2}}|\uparrow, \uparrow, \downarrow\rangle - \frac{\beta}{\sqrt{2}}|\downarrow, \uparrow, \downarrow\rangle - \frac{\alpha}{\sqrt{2}}|\uparrow, \downarrow, \uparrow\rangle + \frac{\beta}{\sqrt{2}}|\downarrow, \downarrow, \uparrow\rangle$

So we start with three spins:

- 1- Spin1 Is the unknown spin that we are trying to teleport and is located in lab A
- 2- Spin2 is the first spin of the entangled pair and is located in lab A
- 3- Spin 3 is the second spin of the entangled pair and is located in lab B

Teleportation is accomplished by the following steps:

Step1: apply the C-X operation to spin 1 and 2.

Step2: apply the Hadamerd.

Step3: Measure spin 2 in the z basis.

Step4: Measure spin 1 in the x basis.

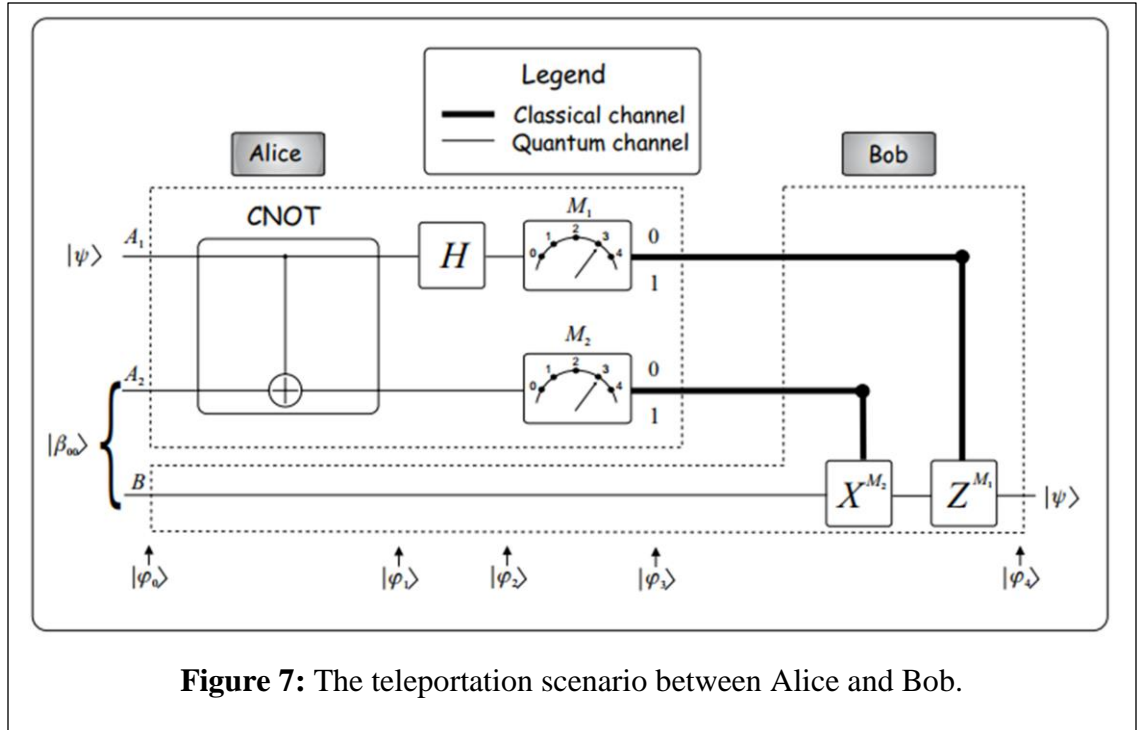
Step5: Lab A calls lab B and informs them of the outcome of the two measurements.

Step6: In lab B they do the following:

- If the measurement outcomes were \downarrow for spin 2 and \rightarrow for spin1: do nothing
- If the measurement outcomes were \downarrow for spin 2 and \leftarrow for spin 1: apply the Z gate to spin3

CHAPTER 2 :

- If the measurement outcomes were \uparrow for spin 2 and \rightarrow for spin 1: apply the X gate to spin3
- If the measurement outcomes were \uparrow for spin 2 and \leftarrow for spin 1: apply the Z gate to spin 3 and then apply the X gate to spin 3.



The state of our register is $|\psi\rangle \otimes |\beta_{00}\rangle = |\varphi_0\rangle$, let us consider that $|\psi\rangle = a|0\rangle + b|1\rangle$ and the state $|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.

So:

$$|\varphi_0\rangle = |\psi\rangle \otimes |\beta_{00}\rangle = \frac{1}{\sqrt{2}} [a|0\rangle(|00\rangle + |11\rangle) + b|1\rangle(|00\rangle + |11\rangle)] \quad (2.13)$$

Respect that: first and second qubit into Alice hand, and the last qubit are in Bob's hand.

$$|A_1\rangle|A_2B\rangle, |\varphi_0\rangle = \frac{1}{\sqrt{2}} \left[a|0\rangle \begin{pmatrix} A_2 B \\ |00\rangle + |11\rangle \end{pmatrix} + b|1\rangle \begin{pmatrix} A_2 B \\ |00\rangle + |11\rangle \end{pmatrix} \right]$$

CHAPTER 2 :

next we apply a C-NOT gate onto Alice qubit A_1 A_2 , the state of the whole system becomes: $|\varphi_0\rangle \rightarrow |\varphi_1\rangle$

$$\begin{aligned} |\varphi_1\rangle &= \frac{1}{\sqrt{2}} \left[a |0\rangle^{A_1} \left(|00\rangle^{A_2 B} + |11\rangle^{A_2 B} \right) + b |1\rangle^{A_1} \left(|00\rangle^{A_2 B} + |11\rangle^{A_2 B} \right) \right] \\ &= \frac{a}{\sqrt{2}} \left(|0\rangle^{A_1} |00\rangle^{A_2 B} + |0\rangle^{A_1} |11\rangle^{A_2 B} \right) + \frac{b}{\sqrt{2}} \left(|1\rangle^{A_1} |00\rangle^{A_2 B} + |1\rangle^{A_1} |11\rangle^{A_2 B} \right) \rightarrow C - NOT \\ &= \frac{a}{\sqrt{2}} \left(|0\rangle^{A_1} |00\rangle^{A_2 B} + |0\rangle^{A_1} |11\rangle^{A_2 B} \right) + \frac{b}{\sqrt{2}} \left(|1\rangle^{A_1} |10\rangle^{A_2 B} + |1\rangle^{A_1} |01\rangle^{A_2 B} \right) \end{aligned}$$

After this step, applies the Hadamerd on A_1 qubit, the Hadamerd rule as next:

$$H |0\rangle = \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle)$$

$$H |1\rangle = \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)$$

So the last formula becomes:

$$\begin{aligned} |\varphi_2\rangle &= \frac{a}{\sqrt{2}} \left(\frac{1}{\sqrt{2}} \left(|0\rangle^{A_1} + |1\rangle^{A_1} \right) |00\rangle^{A_2 B} + \frac{1}{\sqrt{2}} \left(|0\rangle^{A_1} + |1\rangle^{A_1} \right) |01\rangle^{A_2 B} \right) + \frac{b}{\sqrt{2}} \left(\frac{1}{\sqrt{2}} \left(|0\rangle^{A_1} - |1\rangle^{A_1} \right) |10\rangle^{A_2 B} + \frac{1}{\sqrt{2}} \left(|0\rangle^{A_1} - |1\rangle^{A_1} \right) |01\rangle^{A_2 B} \right) \\ |\varphi_2\rangle &= \frac{1}{\sqrt{2}} \frac{1}{\sqrt{2}} \left(a \left(|0\rangle^{A_1} + |1\rangle^{A_1} \right) |00\rangle^{A_2 B} + a \left(|0\rangle^{A_1} + |1\rangle^{A_1} \right) |01\rangle^{A_2 B} \right) + \frac{1}{\sqrt{2}} \frac{1}{\sqrt{2}} \left(b \left(|0\rangle^{A_1} - |1\rangle^{A_1} \right) |10\rangle^{A_2 B} + b \left(|0\rangle^{A_1} - |1\rangle^{A_1} \right) |01\rangle^{A_2 B} \right) \\ &= \frac{1}{\sqrt{2}} \frac{1}{\sqrt{2}} \left[\left(a \left(|0\rangle^{A_1} + |1\rangle^{A_1} \right) |00\rangle^{A_2 B} + a \left(|0\rangle^{A_1} + |1\rangle^{A_1} \right) |01\rangle^{A_2 B} \right) + \left(b \left(|0\rangle^{A_1} - |1\rangle^{A_1} \right) |10\rangle^{A_2 B} + b \left(|0\rangle^{A_1} - |1\rangle^{A_1} \right) |01\rangle^{A_2 B} \right) \right] \\ &= \frac{1}{\sqrt{2}} \frac{1}{\sqrt{2}} \left[a |0\rangle^{A_1} |00\rangle^{A_2 B} + a |1\rangle^{A_1} |00\rangle^{A_2 B} + a |0\rangle^{A_1} |01\rangle^{A_2 B} + a |1\rangle^{A_1} |01\rangle^{A_2 B} + b |0\rangle^{A_1} |10\rangle^{A_2 B} - b |1\rangle^{A_1} |10\rangle^{A_2 B} + b |0\rangle^{A_1} |01\rangle^{A_2 B} - b |1\rangle^{A_1} |01\rangle^{A_2 B} \right] \end{aligned}$$

Now reorder this result and obtain:

$$|\varphi_0\rangle = \frac{1}{2} \left[|00\rangle (a|0\rangle + b|1\rangle) + |01\rangle (a|1\rangle + b|0\rangle) + |10\rangle (a|0\rangle - b|1\rangle) + |11\rangle (a|1\rangle - b|0\rangle) \right] \quad (2.14)$$

From the last step we remark that the stat of the qubit A_1 transmitted to a qubit B in Bob's hand.

5. Non-Cloning Theorem :

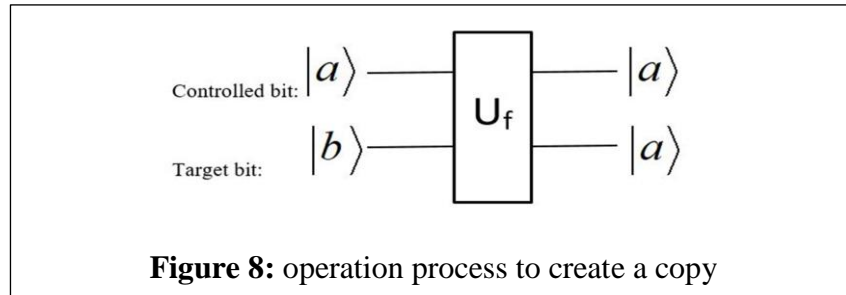
a. Physical meaning:

The Engineers in Classical machines make circuit which can do a copy of a bit, but in quantum machines this operation is unavailable, because when you try to build a copy you will mangle the origin, or you need to create a special printer for any qubit (this operation is impossible for realization), the third option is an operator non unitary.

From the above we conclude that there is no quantum process able to create a copy from the original qubit.

b. Mathematical Formalism: [7]

The quantum circuit for copying a qubit is simulated as:



The previous operation described as:

$$|\chi_1 \otimes \varphi\rangle U_f \rightarrow |\chi_1 \otimes \chi_1\rangle \tag{2.13}$$

This operator should satisfy the next properties:

$$U_f^\dagger U_f = 1 .$$

Independent from the controlled bit.

Now evaluate the dot product: $|\chi_1 \otimes \varphi\rangle U_f = |\chi_1 \otimes \chi_1\rangle$ so

$$\begin{aligned} &= \langle \chi_1 \otimes \varphi | U_f^\dagger U_f | \chi_1 \otimes \varphi \rangle \\ &= \langle \varphi | \varphi \rangle \langle \chi_1 | \chi_1 \rangle = \langle \chi_1 | \chi_1 \rangle \langle \chi_1 | \chi_1 \rangle \end{aligned} \tag{2.14}$$

The last formulation, can conclude that does not exist any operator **Unitary** and **independent** from the controlled bit can do the cloning, because:

CHAPTER 2 :

- either: the operator U_f are non unitary.
- or the operator U_f depended the controlled bit.

In the two cases the information transferred by this qubit it can non cloning, this is the meaning of the **non-cloning theorem**.

6. Simon's Problem :^[8]

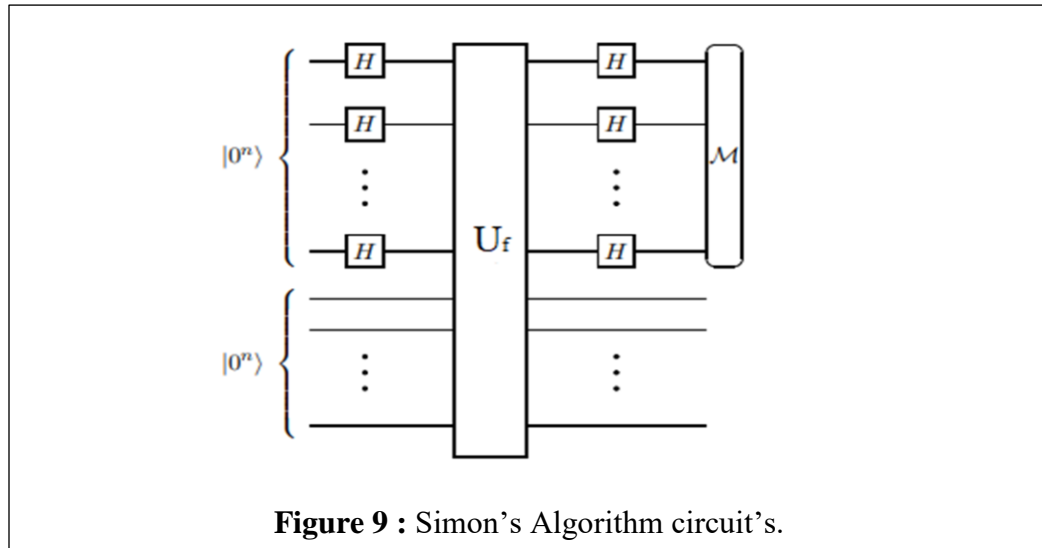


Figure 9 : Simon's Algorithm circuit's.

a. Proposition of the problem:

Let the function f , where $f : \{0,1\}^n \rightarrow \{0,1\}^n$ which is guaranteed to satisfy $f(x) = f(y)$, if and only if $x = y \oplus s$, Simon's problem is then, by querying

$f(x)$ to determine whether the function belongs to $s = 0^n \wedge s \neq 0^n$, Actually sometimes

Simon's problem is stated as the problem of being

given a function which satisfies the promise and then to identify s . We will continue with the tradition of blurring

the distinction between these two problems and call both of the Simon's problem.^[9]

b. Solving Simon's problem Step's with quantum algorithm:

Give a function for n qubit string.

CHAPTER 2 :

Step 1:

Create a Q-register of $2n$ qubit, in the state $|\phi_0\rangle = |x\rangle \otimes |y\rangle$, respectively $|x\rangle$ for the first register and $|y\rangle$ for the second register, in our case the first and second register are $|0^n\rangle$ so:

$$|\phi_0\rangle = |0^{\otimes n}\rangle |0^{\otimes n}\rangle \quad (2.15)$$

Step 2:

Applies the Hadamerd gate into the first register, the outcome of all the string after the first Hadamerd is:

$$|\phi_1\rangle = H^{\otimes n} |\phi_0\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^m} |x\rangle |0^{\otimes n}\rangle \text{ where } m=2n \quad (2.16)$$

Step 3:

Input the last outcomes (2.16) into U_f operation:

$$U_f = \sum_{x,y \in \{0,1\}^m} |x\rangle \langle x| \otimes |y \oplus f(x)\rangle \langle y| \quad (2.17)$$

So when we apply the B_f onto $|\phi_1\rangle$ we obtain:

$$|\phi_2\rangle = U_f |\phi_1\rangle = U_f \frac{1}{\sqrt{2}} \sum_{x \in \{0,1\}^m} |x\rangle |0^{\otimes n}\rangle = \frac{1}{\sqrt{2}} \sum_{x \in \{0,1\}^m} |x\rangle |f(x)\rangle \quad (2.18)$$

Step 4:

Apply the Hadamerd for the second time on (2.18), we get:

Remarque:

$$H^{\otimes n} |x\rangle = \frac{1}{\sqrt{2^n}} \sum_{y \in \{0,1\}^n} (-1)^{x \cdot y} |y\rangle$$

$$\begin{aligned} |\phi_3\rangle &= H^{\otimes n} |\phi_2\rangle = H^{\otimes n} \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle |f(x)\rangle \\ &= \frac{1}{2^n} \sum_{x \in \{0,1\}^n} \sum_{y \in \{0,1\}} (-1)^{x \cdot y} |y\rangle |f(x)\rangle \end{aligned} \quad (2.19)$$

Step 5:

In this step we measure the outcomes of the first register, now we calculate the probability:

$$P0(y) = \left\| \frac{1}{2^n} \sum_x (-1)^{x \cdot y} |f(x)\rangle \right\|^2 = \begin{cases} \frac{1}{2^n}, & \text{if } s \neq 0 \\ 0, & \text{if } s=0 \end{cases} \quad (2.20)$$

7. Deutsch-Jozsa Problem :

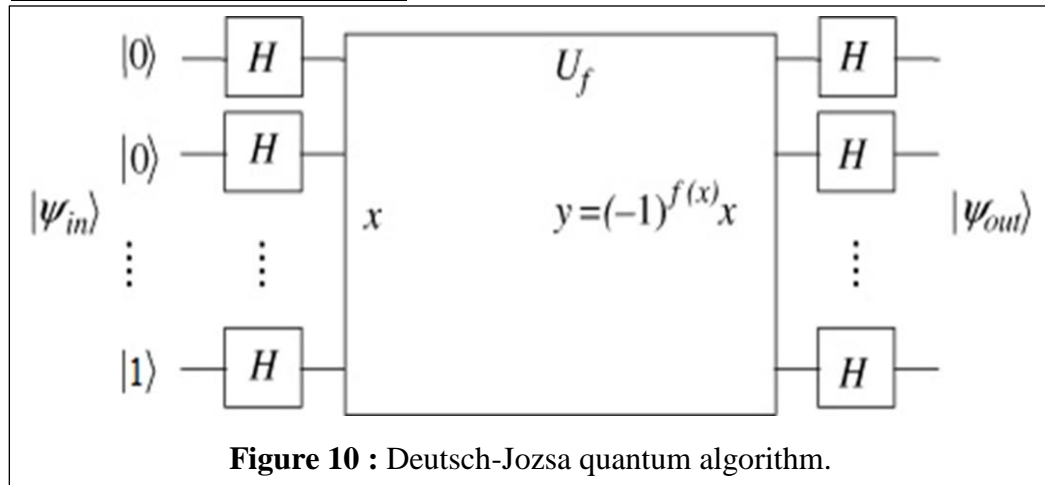


Figure 10 : Deutsch-Jozsa quantum algorithm.

a. Position of the problem:

Deutsch-Jozsa problem is another example that shows the efficiency of quantum algorithm.

This algorithm answers questions of the type that is likely to answer yes or no, the question is a vector of N-bit in which $N = 2^n$, the answer come $\in \{0,1\}$, so we know that:

$$f(x) : \{0,1\}^n \rightarrow \{0,1\}^1 \quad (2.21)$$

b. Solving Deutsch-Jozsa problem Step's with quantum algorithm:

Step 1:

Create a quantum register, and split it into two parts, a first register in a state $|\zeta\rangle = |\psi^{\otimes n}\rangle$, the second register contain just one qubit in the state $|1\rangle$.

The whole string state described by:

$$|\zeta_0\rangle = |00\dots 0\rangle|1\rangle \quad (2.22)$$

Step 2:

Apply n-qubit Hadamerd and get:

$$|\zeta_1\rangle = H^{\otimes n} |\zeta_0\rangle = \frac{1}{\sqrt{2^{n+1}}} \sum_{x=0}^{2^n} |x\rangle (|0\rangle - |1\rangle) \quad (2.23)$$

Step 3:

Input the (2.23) outcomes onto U_f oracle, this operation affects as:

$$f : |x\rangle|y\rangle \rightarrow |x\rangle|y \oplus f(x)\rangle \quad (2.24)$$

The result of this step is:

$$|\zeta_2\rangle = \frac{1}{\sqrt{2^{n+1}}} \sum_{x=0}^{2^n-1} |x\rangle (|f(x)\rangle - |1 \oplus f(x)\rangle) \quad (2.25)$$

We should consider that: $\forall x, f(x) = \begin{cases} 0 \\ or \\ 1 \end{cases}$ so the formula (2.25) becomes:

$$|\zeta_2\rangle = \frac{1}{\sqrt{2^{n+1}}} \sum_{x=0}^{2^n-1} (-1)^{f(x)} |x\rangle (|0\rangle - |1\rangle) \quad (2.26)$$

Step 4:

Apply the second Hadamerd

$$\begin{aligned} |\zeta_3\rangle &= \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{f(x)} |x\rangle \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \\ &= \frac{1}{2^n} \sum_{x=0}^{2^n-1} (-1)^{f(x)} \sum_{y=0}^{2^n-1} (-1)^{x \cdot y} |y\rangle \\ &= \frac{1}{2^n} \sum_{\substack{x=0 \\ y=0}}^{2^n-1} (-1)^{f(x)} (-1)^{x \cdot y} |y\rangle \end{aligned} \quad (2.27)$$

CHAPTER 2 :

$$x \cdot y = x_0 y_0 \oplus x_1 y_1 \oplus \dots \oplus x_n y_n$$

Step 5:

Measure the final state:

If the probability equal 1 to finding $|0^{\otimes n}\rangle$, then we have a constructive Interference, which means a constant function.

If the probability is 0, so we have a destructive interference, which means a balanced function.

8. Summary:

Quantum algorithms can speed up many difficult processes on classical algorithms, and as an example we have previously seen algorithms of Simon's, and Deutsch-Jozsa.

The quantum algorithm is more exponentially speed up and take a few steps than the classical algorithm.

Chapter III:

1. Shor's algorithm.
2. Position of the problem.
3. QFT, DFT and Their relation to factorization.
4. Application in Quantum Computing (Shor algorithm step).
5. Summary.

CHAPTER 3 :

1. Shore algorithm :

a. Proposition of the problem:

One of the famous common problems in mathematics, is how to factorize number N into two prime numbers.

$$N = p \times q, p, q \in \mathbb{N} \quad (3.1)$$

This operation is a basis for all the cryptography in informatics world, to affect this operation we need to find a period of this number or this function.

Suppose a periodic number or a periodic function, Shor's algorithm for factoring a large integer is a quantum method for computing the period of the functions written as:

$$f_{x,n} = x^a \bmod(N) \equiv x^a [N] \quad (3.2)$$

That method is exponentially more efficient than any classical method, Shor's Algorithm just tells us that once we know the period "r", we can obtain the factor of "N" from the **GCD** (Greatest Common Divisor) of the next formula.

$$\left(x^{\frac{r}{2}} - 1, N \right) \text{ and } \left(x^{\frac{r}{2}} + 1, N \right) \quad (3.3)$$

In our case n , is the period depended respectively a number P and function f , assuming there is no analytic technique to determine the period of f , Classically we'll compute at least $N/2$ value of the possible value of the function.

b. QFT, DFT and Their relation to factorization: [1]

Fourier transformation is a utility which extracts the period of a function, we will exploit this property to build Shor's algorithm.

Classically FT, for example:

$$\text{Given } x_j = \{0, 1\} \text{ calculate the } y_k = \frac{1}{\sqrt{2}} \sum_{j=0}^1 x_j e^{2\pi ijk/2}$$

$$\text{So } y_0 = \frac{1}{\sqrt{2}}, y_1 = \frac{-1}{\sqrt{2}}.$$

CHAPTER 3 :

Now define the Discrete Fourier Transformation, abbreviation DFT:

$$y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j e^{2\pi ijk/N} \quad (3.4)$$

We can apply the DFT for a quantum state $|\psi\rangle$, which called QFT, and define it as next:

$$QFT |\psi\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} x_j e^{2\pi ijk/N} |K\rangle \quad (3.5)$$

c. Application in Quantum Computing (Shor's algorithm step):

In quantum computing this operation take just 4 steps:

Step 1: create a single quantum memory register that we partition into two parts called Register1 and Register 2.

$$\begin{cases} \text{Re gister 1} \equiv a \\ \text{Re gister 2} \equiv b \end{cases} \text{ that we can denote it as flows: } |a, b\rangle.$$

And apply Quantum Fourier Transformation gate for all controlled bit.

Step 2: input all qubit in the oracle O_f (controlled and target bits).

Step 3: apply the second QFT.

Step 4: measure the output from the second QFT.

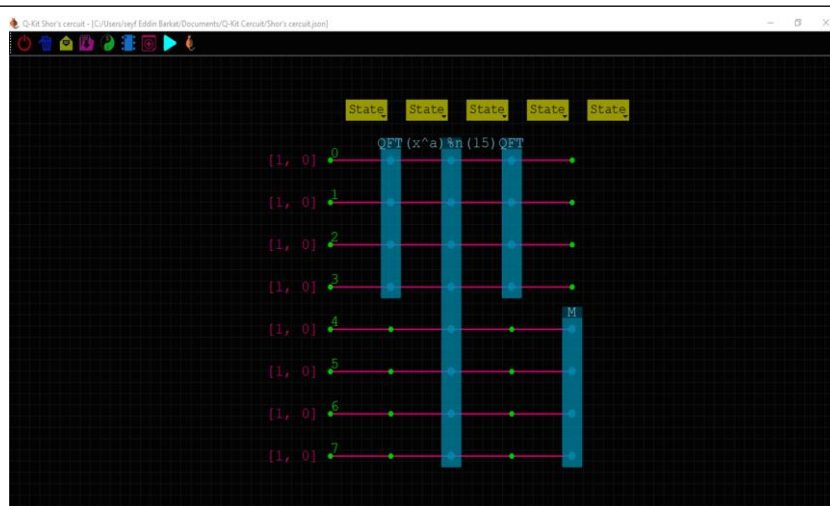


Figure 11 : Quantum Shor factorisation circuit.

CHAPTER 3 :

d. Application:

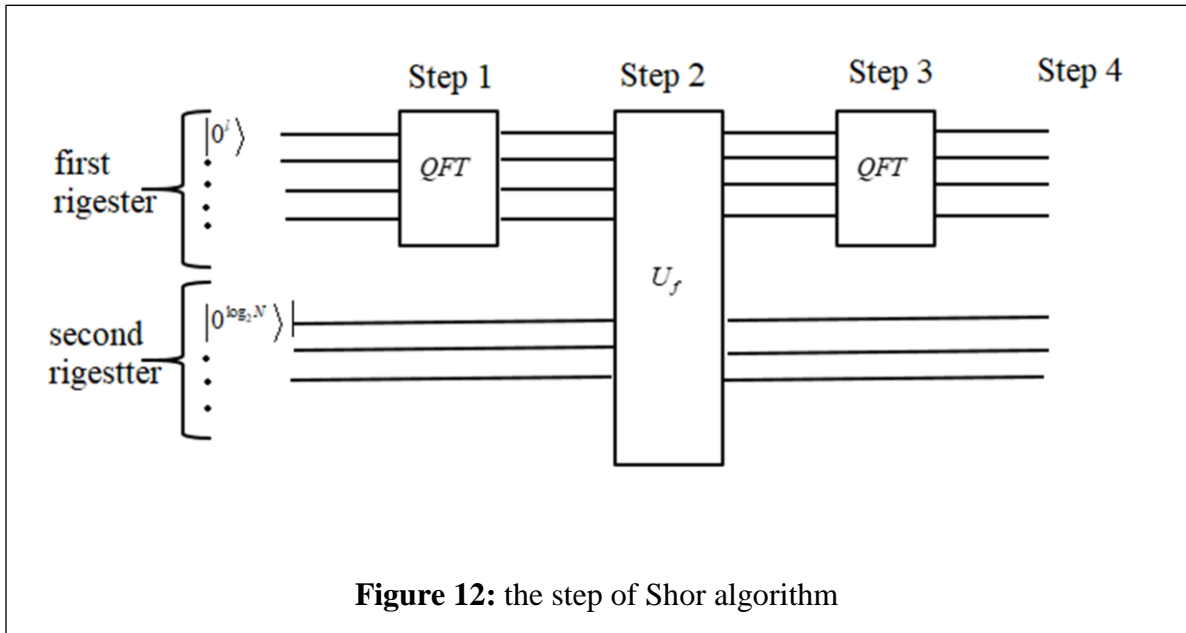


Figure 12: the step of Shor algorithm

We'll explain the mathematical steps of Shor's algorithm:

Step 1:

We input N qubit, and apply the **QFT** for first l qubit, the other qubit arrive to U_f without any transformation which means:

$$|0\rangle^l \rightarrow QFT \rightarrow \frac{1}{\sqrt{2^l}} \sum_{a=0}^{2^l-1} |a\rangle |0\rangle \quad (3.3)$$

We should be careful because the QFT in the term (3.3) Available just for the qubit $|0\rangle$.

Step 2:

All the qubit in register 1 and register 2 a cross to U_f , in this step we deal with the second register:

$$QFT \rightarrow \frac{1}{\sqrt{2^l}} \sum_{a=0}^{2^l-1} |a\rangle |0\rangle \rightarrow U_f \rightarrow \frac{1}{\sqrt{2^l}} \sum_{a=0}^{2^l-1} |a\rangle |x^a [N]\rangle \quad (3.4)$$

Expend the last sum, we found:

CHAPTER 3 :

$$\begin{aligned}
 & \frac{1}{\sqrt{2^L}} \sum_{a=0}^{2^l-1} |a\rangle |x^a [N]\rangle \\
 &= \frac{1}{\sqrt{2^L}} \{ |0\rangle |1[N]\rangle + |1\rangle |x [N]\rangle + |2\rangle |x^2 [N]\rangle + \dots + |r\rangle |1[N]\rangle \\
 &+ |r+1\rangle |x [N]\rangle + |r+2\rangle |x^2 [N]\rangle + \dots + |r\alpha + \beta\rangle |x^\beta [N]\rangle \} \\
 &= \{ |0\rangle + |r\rangle + |2r\rangle + \dots + |\alpha r\rangle \} |1[N]\rangle \\
 &+ \{ |1\rangle + |r+1\rangle + |2r+1\rangle + \dots + |\alpha r + 1\rangle \} |x [N]\rangle \\
 \text{M} \\
 &+ \{ |n\rangle + |r+n\rangle + |2r+n\rangle + \dots + |\alpha r + n\rangle \} |x^n [N]\rangle
 \end{aligned}$$

It is clear that the last sum can be written as:

$$\sum_{s=0}^{r-1} \sum_{j=0}^{2^l-1} |jr + s\rangle |x^j [N]\rangle \quad (3.5)$$

Step 3:

In this step we apply the second **QFT** for the first register in the term (3.5), so we obtain the next result:

$$\begin{aligned}
 |x\rangle &\rightarrow_{QFT} \rightarrow \frac{1}{\sqrt{q}} \sum_{y=0}^{q-1} e^{\frac{2\pi i}{q} x \cdot y} |y\rangle \\
 |jr + s\rangle &\rightarrow_{QFT} \rightarrow \frac{1}{\sqrt{q}} \sum_{y=0}^{q-1} e^{\frac{2\pi i}{q} (jr+s) \cdot y} |y\rangle
 \end{aligned} \quad q = 2^l \quad (3.6)$$

Total result is:

$$\frac{1}{\sqrt{q}} \sum_{y=0}^{q-1} \exp\left(\frac{i\theta_{j,s}}{q} y\right) |y\rangle \quad (3.7)$$

Where: $\theta_{j,s} = 2\pi(jr + s)$, r : is the period, and the qubit after the second QFT described by:

CHAPTER 3 :

$$\frac{1}{2^l} \sum_{s=0}^{r-1} \sum_{j=0}^{\frac{2^l}{r}-1} \sum_{y=0}^{2^l-1} e^{\frac{i\theta_{j,s}y}{q}} |y\rangle |x^s [N]\rangle \quad (3.8)$$

Step 4:

At last step we affect a measure on the second register:

$$\frac{1}{2^l} \sum_{y=0}^{2^l-1} \sum_{j=0}^{\frac{2^l}{r}-1} e^{\frac{i\theta_{j,s}y}{q}} |y\rangle |x^s [N]\rangle \quad (3.9)$$

We well try to calculate this sum, writ it as:

$$\begin{aligned} \frac{1}{2^l} \sum_{y=0}^{2^l-1} \sum_{j=0}^{\frac{2^l}{r}-1} e^{\frac{2\pi i(jr+s)y}{q}} |y\rangle &= \frac{1}{2^l} \sum_{y=0}^{2^l-1} \sum_{j=0}^{\frac{2^l}{r}-1} e^{i\frac{2\pi jr}{q}y} e^{i\frac{2\pi s}{q}y} |y\rangle \\ &= \frac{1}{2^l} \sum_{y=0}^{2^l-1} e^{i\frac{2\pi s}{q}y} \sum_{j=0}^{\frac{2^l}{r}-1} e^{i\frac{2\pi jr}{q}y} |y\rangle = \frac{1}{2^l} \sum_{y=0}^{2^l-1} e^{i\frac{2\pi s}{q}y} \left(\sum_{j=0}^{\frac{2^l}{r}-1} Q^j \right) |y\rangle \end{aligned} \quad (3.10)$$

We deal with it as a geometric series: $\sum_{j=0}^{\frac{2^l}{r}-1} Q^j = \sum_{j=0}^{\frac{2^l}{r}-1} e^{\left(\frac{i}{q}2\pi ry\right)j} = \frac{1-Q^{\frac{2^l}{r}}}{1-Q}$ (A)

The rest from the formula (3.10) call it (B), $\frac{1}{2^l} \sum_{y=0}^{2^l-1} e^{i\frac{2\pi s}{q}y} |y\rangle$ (B)

$$\begin{aligned} (3.10) &= \frac{1}{2^l} \sum_{y=0}^{2^l-1} e^{i\frac{2\pi s}{q}y} \left(\sum_{j=0}^{\frac{2^l}{r}-1} Q^j \right) |y\rangle = \frac{1}{2^l} \frac{1 - \left(e^{\frac{i2\pi s \cdot y}{q}}\right)^{\frac{2^l}{r}}}{1 - \left(e^{\frac{i2\pi s \cdot y}{q}}\right)} \frac{1 - \left(e^{\frac{i2\pi r \cdot y}{q}}\right)^{\frac{2^l}{r}}}{1 - \left(e^{\frac{i2\pi r \cdot y}{q}}\right)} |y\rangle \\ &= \frac{1}{2^l} \frac{1 - \left(e^{\frac{i2\pi y}{q}(r+s)}\right)^{\frac{2^l}{r}}}{1 - \left(e^{\frac{i2\pi y}{q}(r+s)}\right)} |y\rangle \end{aligned} \quad (3.11)$$

the probability is the square of the factor of $|y\rangle$, so:

CHAPTER 3 :

$$P(y) = \left| \frac{1}{2^l} \frac{1 - \left(e^{\frac{i2\pi y}{q}(r+s)} \right)^{2^l}}{1 - \left(e^{\frac{i2\pi y}{q}(r+s)} \right)} \right|^2 \quad (3.12)$$

we use the propriety of the complex number: $|Z| = \sqrt{ZZ^*}$, the outcome is:

$$P(y) = \frac{\sin(\pi y)}{\sin\left(\frac{r}{2^l} \pi y\right)} \quad (3.13)$$

This result has two possible cases:

First case: $\frac{r}{q} = \frac{r}{2^l} = n \in \mathbb{Y}$ so $P(y) \neq 0$, $n = 1 \Rightarrow r = 2^l$, if $n \neq 1 \Rightarrow \frac{2^l}{r} = \frac{y}{k} \Rightarrow r = \frac{k \cdot 2^l}{y}$

Second case: $\frac{r}{q} = \frac{r}{2^l} = n \notin \mathbb{Y}$, so $\frac{r}{2^l} \approx \frac{k}{y}$ in this case the period r can't determinant exactly.

Our original problem is how to factor a number N to p and q :

$$\begin{aligned} \gcd\left[N, x^{\frac{x}{2}} + 1\right] &= p \\ \gcd\left[N, x^{\frac{x}{2}} - 1\right] &= q \end{aligned} \quad (3.14)$$

e. summary

Shor's algorithm is most powerful tool, but it also sometimes fails to determine the period.

X. Conclusion:

Quantum algorithms can open up promising horizons in computing, and as we have seen earlier, that latter have properties that enable them to work on many operations at one time, and with fewer steps than their performance on classical algorithms.

But there are still some obstacles to achieving these algorithms, including maintaining how saving coherence of qubit.

As we see before the quantum Shor's algorithm some times fail, but it is also more efficient and so fast.

In our study we use a Q-Kit program to simulate the quantum circuit's.

XI. Recommendation:

Through the study we have some recommendations represented as follows:

1. Optimizing the Q-kit program, in order to make it easier to create composite circuits, if we try to create Grover circuits, it is difficult to create them all at once with the program.
2. Add the ability to manipulate and modify the qubit.
3. Propose the subject of Shor's Algorithm at the future for estimate this algorithm.
4. Shor's algorithm also need an other sub algorithm to calculate the:

$$gsd \left[N, x^{\frac{t}{2}} + 1 \right] = p$$

$$gsd \left[N, x^{\frac{t}{2}} - 1 \right] = q$$

5. Follow this work with other practical studies about Q-bit creation.

XII. Reference's

1. Wikipedia.
2. Michael A. Nielsen, Isaac L. Chuang-Quantum.
3. CSE 599d - Quantum Computing “One Qubit, Two Qubit”, Dave Bacon, Department of Computer Science & Engineering, University of Washington
4. Quantum Computation: A Tutorial, Benoit Valiron
benoit.valiron@monoidal.net
5. Lecture 6 : The Quantum Fourier Transform “Dr. Iain Styles”
I.B.Styles@cs.bham.ac.uk
6. Quantum Algorithms Tutorial “Ronald de Wolf”, page 15.
7. Lectures on Quantum Gravity and Black Holes, “Thomas Hartman”, page 165-173.
8. British Dictionary definitions for teleport.
9. Quantum Computation: a Tutorial “Benoit Valiron”,15 April 2012.
10. CSE 599d - Quantum Computing
11. Lectures 8 : Simon’s Algorithm, Dave Bacon, Department of Computer Science & Engineering, University of Washington.
12. and Communications, An Engineering Approach “Sandor Imre and Ferenc Bal”, ‘ azs ’.
13. Chapitre 3 : Algèbre de Boole, Faculty of New Technologies of Information and Communication UKMO. PPT
14. Explorations in Quantum Computing «second Edition », David Gries, Fred B. Schneider

XIII. Appendix's:

1. Appendix A: How to make a Q-bit.
2. Appendix B: QFT.
3. Appendix C: Classical Factorization.

Appendix A: How to make a Qu-bit

How To Make A Qubit ¹:

As discussed in Part 1 of this series, quantum information processing may offer elegant solutions to a number of important problems in computation. Actually building a quantum computer, however, is not so easy.

Part 1 used an isolated hydrogen molecule as a model two-qubit system. Molecular orbitals are simple to explain and readily monitored by well-established techniques. A viable qubit technology, however, will need a number of other characteristics as well. Some system requirements include:

The quantum state of interest must be stable. That is, it must be possible to preserve it long enough to actually do the calculation.

The qubit technology being used must be scalable. It must be possible to create large numbers of identical qubits, and to propagate information between them. In particular, qubits must be able to interact over distances while preserving their superposition of quantum states.

A set of operations must be available that manipulate the quantum state without collapsing it to a single measurement.

It must be possible to define the initial state of the qubits at the beginning of the computation, and measure the result at the end.

All of these requirements are challenging, and they contradict each other in a number of ways. In particular, the requirements of stability and scalability are in conflict: it is harder to maintain the stability of larger systems.

To make a qubit stable, it is important to isolate it from outside influences that can disrupt the quantum state. Thermal vibrations are particularly pernicious, and for this reason many proposed designs operate at cryogenic temperatures. Other designs depend on the rigid lattice of the surrounding material for stability. An important figure of merit is the “coherence time,” the length of time a prepared quantum state can be maintained before outside influences degrade it.

¹ <http://semiengineering.com/how-to-make-a-qubit/>

Appendix A: How to make a Qu-bit

For example, one structure that has attracted a lot of interest is the nitrogen-vacancy center in diamond. In diamond, as in silicon, each atom is bound to its four nearest neighbors. If a carbon atom is replaced with a nitrogen atom, the nitrogen-carbon bonds are a little weaker than the surrounding carbon-carbon bonds. Remove another carbon atom, creating a vacancy, and the result is a nitrogen-vacancy pair (N-V) with an extra electron, trapped in an otherwise rigid carbon lattice.

The physics of the nitrogen-vacancy center are beyond the scope of this article — a comprehensive review can be found here — for our purposes, it's enough to observe that the center has complex optical and electrical behavior. Appropriate wavelengths of light can be used to initialize and to measure the spin of the associated electron.

Point defects generally are attractive qubit candidates because they tend to behave like isolated atoms, and because the semiconductor industry has developed many tools for measuring and manipulating them. A few materials, among them diamond and silicon carbide, are especially promising. According to chief technical officer Daniel Twitchen, Element Six can grow 6" diameter diamond wafers, 2 to 3 mm thick, with part-per-trillion defect control. Diamond is a wide gap semiconductor, allowing a clear transition between the excited and ground states of the qubit. Furthermore, ^{12}C , the most naturally abundant carbon isotope, has no nuclear spin, minimizing the coupling between the electron associated with the N-V center and the surrounding carbon lattice. Even at room temperature, researchers have achieved near-millisecond coherence times for N-V quantum states. This is probably sufficient for quantum computation; as various error-correcting methods can refresh the quantum state before it decoheres.

Natural carbon also contains about 1.1% ^{13}C , which has a nuclear spin of $1/2$ due to its extra neutron. Researchers will often co-implant nitrogen and ^{12}C in order to minimize the effects of these spins. Co-implanting carbon also increases the vacancy density, and therefore the yield of N-V centers.

The N-V center offers an especially attractive combination of electrical and optical properties. In order to transmit data between qubits, any quantum computing architecture will need a mechanism allowing interactions over distances greater than quantum effects alone can support. Light is one such mechanism, and the N-V center offers both spin-

Appendix A: How to make a Qu-bit

preserving and spin-polarizing optical transitions. That is, Twitchen explained, light can be used to either transmit a qubit state or to initialize such a state.

All of these characteristics make N-V centers very attractive as a potential qubit technology, and have inspired substantial research efforts. As a result, a roadmap leading toward diamond-based quantum computers is starting to emerge. Which is not to say that all problems are solved. One of the main requirements for a scalable quantum computer is the ability to construct an array of identical qubits. One measure of this capability is the efficiency with which individual qubits can be produced. Only a small fraction (N) of implanted nitrogen atoms actually lead to the creation of an N-V center. The probability the two centers will exist in close proximity is thus N^2 ; the probability of three centers is N^3 . While co-implantation of ^{12}C increased yield substantially, researchers still achieved only a 4% yield of N-V center pairs.

Additionally, propagation of light between qubits will require an extensive network of waveguides and other photonic structures. Diamond is extremely inert, impervious to most etch chemistries and other patterning technologies. Ion milling can be used, but tends to graphitize and degrade the surrounding material. Diamond patterning remains an open challenge.

That the interest in N-V center-based qubits persists in the face of these obstacles is one measure of how difficult quantum computing implementation is. None of the alternatives are any easier. One alternative may be a bit closer to commercial implementation, though. The next article in this series will consider superconducting circuit technology, the foundation of D-Wave Systems' D-Wave Two.

Appendix B: FT, DFT, QFT

FT : Fourier Transformation

Fourier transformation is a mathematical tool, with the definition of classical FT we turn an non-periodic function to another periodic function in terms of $\sin(x)$ and $\cos(x)$ function.

Definition:

$$\hat{F}(x) = \frac{a_0}{2} + \sum (a_n \cos(n\omega x) + b_n \sin(n\omega x))$$
$$\text{with : } \begin{cases} a_0 = \frac{2}{T} \int_0^T f(x) dx \\ a_n = \frac{2}{T} \int_0^T f(x) \cos(n\omega x) dx \\ b_n = \frac{2}{T} \int_0^T f(x) \sin(n\omega x) dx \end{cases}$$

This formulation can have written as:

$$\hat{F} = \int_{-\infty}^{+\infty} f(x) e^{-2\pi i x \omega} dx \quad , \text{ where } f: \mathbb{R} \rightarrow \mathbb{C}$$

The previous formula used when the function are continue,

$$\forall x \in \mathbb{R}, \exists y, f(x) = y \wedge f(x) \neq 0 .$$

Example:

$$\text{Let de function: } f(x) = \begin{cases} 0, -\pi \leq x \leq \pi \\ x, 0 \leq x \leq \pi \end{cases}$$

Appendix B: FT, DFT, QFT

$$a_0 = \frac{2}{T} \int_0^T f(x) dx = \frac{1}{2\pi} \left[\int_{-\pi}^{\pi} 0 dx + \int_0^{\pi} x dx \right] = \frac{1}{2\pi} \frac{x^2}{2} \Rightarrow a_0 = \frac{\pi}{4}$$

$$a_n = \frac{2}{T} \int_0^T f(x) \cos(n\omega x) dx = \frac{2}{2\pi} \left[\int_{-\pi}^0 x \cos(nx) dx + \int_0^{\pi} x \cos(nx) dx \right]$$

$$= \frac{1}{\pi} \left[\int_0^{\pi} x \cos(nx) dx \right] = \frac{1}{\pi} \left[x \cdot \frac{1}{n} \sin(nx) \Big|_0^{\pi} - \int_0^{\pi} 0 \frac{1}{n} \sin(nx) dx \right] = 0$$

$$b_n = \frac{2}{T} \int_0^T f(x) \sin(n\omega x) dx = \frac{1}{\pi} \left[\int_0^{\pi} x \sin(n\omega x) dx \right]$$

$$= \frac{1}{\pi} \left[x \cdot \frac{-1}{n} \cos(n\omega x) \Big|_0^{\pi} - \int_0^{\pi} -\frac{1}{n} \cos(n\omega x) dx \right]$$

$$= \frac{1}{\pi} \left[\frac{-\pi}{n} \cos(n\pi) - \left(-\frac{1}{n} \sin(n\omega x) \Big|_0^{\pi} \right) \right] \Rightarrow b_n = \frac{-1}{n} \cos(n\pi)$$

DFT: Discrete Fourier Transformation.

so if the function defined just for the integer number, $x \in \mathbb{Z}$ the definition of Fourier Transformation changed, and we call it DFT.

$$y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j e^{2\pi i j k / N}$$

Example:

$$\text{Given } x_j = \{0,1\} \text{ calculate the } y_k = \frac{1}{\sqrt{2}} \sum_{j=0}^1 x_j e^{2\pi i j k / 2}$$

$$\text{So } y_0 = \frac{3}{\sqrt{2}}, y_1 = -\frac{1}{\sqrt{2}}.$$

QFT: Quantum Fourier Transformation.

Since our state vectors for qubits are just vectors of complex numbers, we should not be surprised to learn that the DFT can be applied to them.

$$\text{Give a vector state: } |\psi\rangle = \sum_{j=0}^{N-1} a_j |j\rangle$$

QFT, defined as:

Appendix B: FT, DFT, QFT

$$F|\psi\rangle = \sum_{k=0}^{N-1} b_k |k\rangle$$

$$\text{where : } b_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} a_j e^{2\pi i j k / N}$$

Consider a qubit state $|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$

$$b_0 = \frac{1}{2} \sum_{j=0}^3 a_j = \frac{1}{2} (\alpha_{00} + \alpha_{01} + \alpha_{10} + \alpha_{11})$$

$$b_1 = \frac{1}{2} \sum_{j=0}^3 a_j e^{2\pi i j / 4} = \frac{1}{2} (\alpha_{00} + \alpha_{01} e^{i\pi/2} + \alpha_{10} e^{i\pi} + \alpha_{11} e^{3i\pi/2})$$

$$b_2 = \frac{1}{2} \sum_{j=0}^3 a_j e^{4\pi i j / 4} = \frac{1}{2} (\alpha_{00} + \alpha_{01} e^{i\pi} + \alpha_{10} e^{2i\pi} + \alpha_{11} e^{3i\pi})$$

$$b_3 = \frac{1}{2} \sum_{j=0}^3 a_j e^{6\pi i j / 4} = \frac{1}{2} (\alpha_{00} + \alpha_{01} e^{3i\pi/2} + \alpha_{10} e^{3i\pi} + \alpha_{11} e^{9i\pi/2})$$

Appendix C

Classical calculation for factorization:

First step is to write a number in term: $x^a = r[N]$

X: Divided

N: divisor

r: rest of Euclidian division to X on N

Example:

Take a number 187.

$$187^0 \equiv 1[2]$$

$$187^1 \equiv 1[2]$$

$$187^2 \equiv 2[2]$$

$$187^3 \equiv 1[2]$$

a period are $r = 2$

$$gsd \left[N, x^{\frac{r}{2}} + 1 \right] = p$$

applied the next formula:

$$gsd \left[N, x^{\frac{r}{2}} - 1 \right] = q$$

$$\begin{aligned} gsd \left[2, 187^{\frac{2}{2}} + 1 \right] &= p \\ gsd \left[2, 187^{\frac{2}{2}} - 1 \right] &= q \end{aligned} \Rightarrow \begin{cases} p = 11 \\ q = 17 \end{cases}$$

Abstract:

This research aims at demonstrating the effectiveness of quantum algorithms in the treatment of some of the most difficult problems for classical algorithms. As an example of known problems, we have is a factorization the number into two prime factors. There are several algorithms that solve this problem, but it takes more steps, while by the quantum Shor algorithm can be solved in a few steps and less time.

As an illustration of how quantum computing is capable and expected, we have included two examples of the Simon algorithm and the Deutch-Jozsa algorithm.

Key Words:

Q-bit, Algorithm, Quantum gate, Hadamerd, QFT, Shor's Algorithm.

Cette recherche vise à démontrer l'efficacité des algorithmes quantiques dans le traitement de certains des problèmes les plus difficiles pour les algorithmes classiques. A titre d'exemple de problèmes connus, nous avons une factorisation du nombre en deux facteurs premiers. Il existe plusieurs algorithmes qui résolvent ce problème, mais par l'algorithme quantique Shor peut être résolu en quelques étapes et moins de temps.

Pour illustrer comment l'informatique quantique est capable de résoudre les problèmes nous avons inclus deux exemples : l'algorithme de Simon et l'algorithme de Deutch-Jozsa.

Les mots clé :

Q-bit, algorithme, porte quantique, Hadamerd, QFT, algorithme de Shor.

يهدف بحثنا هذا إلى إظهار مدى فعالية و نجاعة الخوارزميات الكمومية في معالجة بعض المشاكل العسيرة بالنسبة للخوارزميات الكلاسيكية، و أخذنا كمثال على المشاكل المعروفة، مشكل تحليل عدد إلى جداء عوامل أولية، صحيح أنه توجد عدة خوارزميات تقوم بحل هذا المشكل، إلا أنها تأخذ وقتا و خطوات أكثر، بينما بواسطة خوارزمية Shor الكمومية يمكن حلها في خطوات معدودة.

وكتوضيح لمدى القدرة التي يتيحها الحاسوب الكمومي والافاق المنتظر تحقيقها منه، أدرجنا مثالين خوارزمية Simon و خوارزمية Deutch-Jozsa.

الكلمات المفتاحية:

كيوبيت، خوارزمية، بوابات كمومية، هادامار، تحويل فوريي الكمومي، خوارزمية شور.