EMSI CASABLANCA

Internship report

From: 25/06/2022 To: 25/09/2022

Quantum information theory and basic quantum algorithms

Realised by: Yassine Boughroudi
Supervised: Pr. Mohammed Mestari
Date: September 29, 2022

Contents

1 Acknowledgement

“First and foremost, I would want to thank my family, especially my parents, for their support and encouragement; without them, this report would not be possible.

In Addition, I would like to express my gratitude and thanks to Pr Mohammed Mestari, my supervisor, for all the valuable advice and the information he gave me and for devoting the time to follow-up of this work.

Finally, thanks to everyone in the quantum computing community for generating such great open source and the opportunity to work on a real quantum computer.”

Yassine Boughroudi

Abstract

This report presents the basic mathematics of quantum information and shows the quantum computer's advantage over classical computers in solving the Deutsch–Jozsa and Simon algorithms. We have thoroughly analyzed these basic algorithms and provided examples for their implementations in Qiskit python framework.

2 Presentation of the laboratory

The ”Signals, Distributed Systems and Artificial Intelligence ” laboratory is a multidisciplinary laboratory, located at ENSET(Ecole Normale Supérieure de l'Enseignement Technique) Mohammedia and takes the designation SSDIA. It is made up of research teams covering several specialties that produce engineering sciences. These teams have in common, the use of mathematical tools to model physical phenomena and complex systems to respond to concrete and applied problems. The laboratory currently has 52 professors-researchers and more than 100 doctoral students working around the following unifying themes: Neural Networks and Artificial Intelligence, Information systems, parallel computing/High-Performance Computing, Functional analysis, Mathematical modeling, optimization, and numerical calculation...

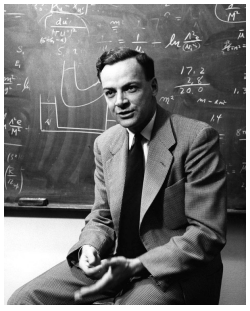
3 Introduction

Quantum information science is an interdisciplinary research endeavour that brings together computer scientists, mathematicians, physicists, chemists, and engineers to develop revolutionary information processing and communication technologies that are infeasible without exploiting the principles of quantum mechanics. The importance of quantum information was first widely recognized in 1982 when **Richard Feynman** conjectured that a quantum computer would efficiently simulate quantum systems, and a universal Turing machine ("classical computer") could not. In his paper[1], **quantum computing was born**.

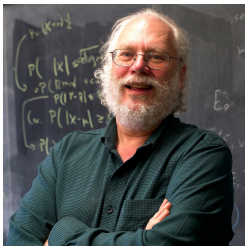
In the mid-1990s, **peter w. shor** showed that the quantum computer could efficiently determine the factors of large numbers whereas this problem is believed to be intractable on a classical computer[2]. Even earlier, in 1984, Bennett and Brassard proposed an information theoretically secure key distribution technique through public channels, as opposed to standard methods that are only computationally secure[3]. Originally proposed in 1984, quantum cryptography has since become commercial technology.

Quantum information technology is thus "disruptive" both technically and also at a fundamental level both to physics and to computer science. Quantum information leads to a violation of the strong Church-Turing thesis and could enable information-theoretic security over public channels. Moreover quantum computing and quantum cryptography damage and ameliorate, respectively, information security.

The classical computers manipulate individual bits, 0 and 1, to store information as binary data, whereas quantum computers use the probability of an object's state before it is measured. Therefore, it gives them the potential to process exponentially more data compared to classical computers. Unlike classical computers that use the binary bit, quantum computers use qubits that are produced by the quantum state of the object to perform operations. Since these qubits are quantum in nature, they follow phenomena like **superposition** and **entanglement**. Superposition is the ability of a quantum system to be in multiple states at the same time. Entanglement is the strong correlation between quantum particles. These phenomena help the quantum computer work with 0, 1, and superposition of 0 and 1, giving them the advantage in doing complex calculations that modern classical systems cannot do or would take a significant amount of time to get the desired result[4]. Such an advancement creates a world of opportunities, across almost every aspect of modern life. The following chart depicts the top quantum computing applications in the real world.



(a) Richard feynman



(b) peter w. shor

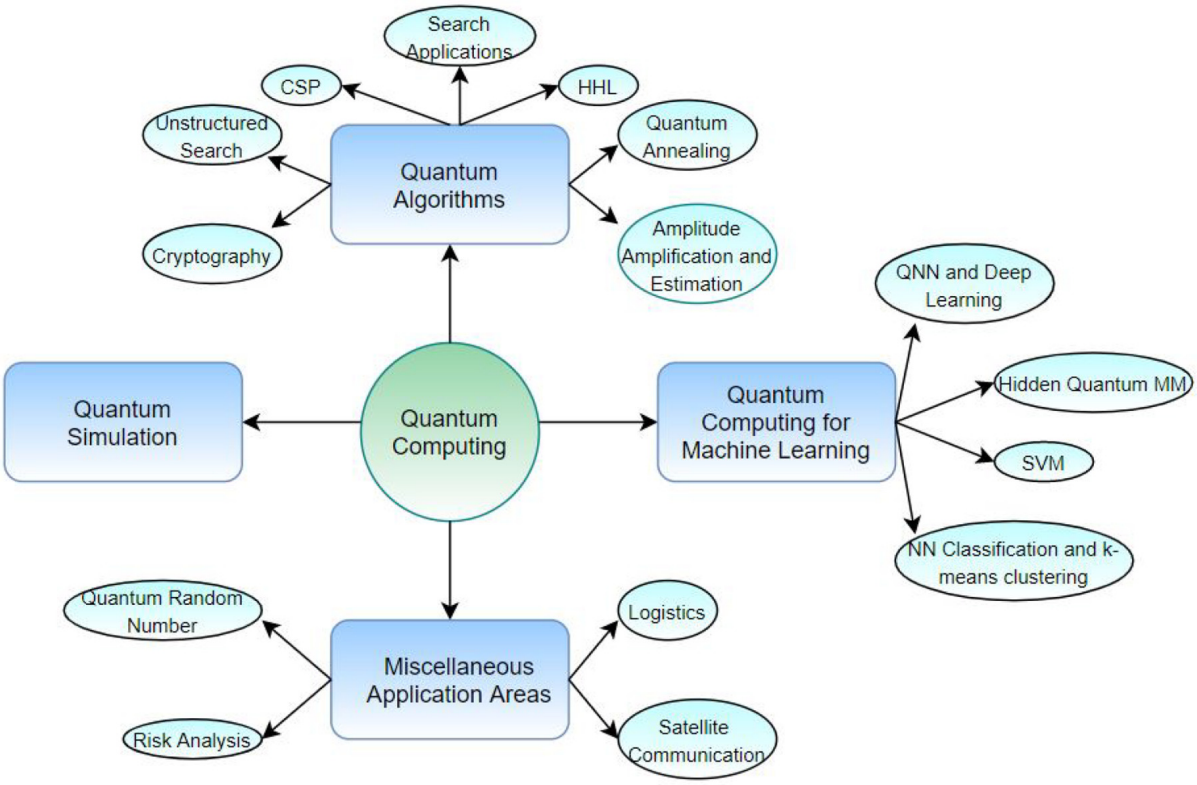


Figure 3.2: Overview of the applications of quatum computing [4]

4 The theoretical part

Theoretical research in quantum information relies on sophisticated mathematical methods. Therefore, the first part of this chapter will be dedicated to giving an introduction and basic definitions of some mathematical concepts in group theory, linear algebra, and functional analysis. I have followed [5]and [6] most of this chapter.

4.1 Basic abstract algebra

4.1.1 Groups

Definition 1 (Binary operation).

- A binary operation $*$ on a set G is a function $* : G \times G \rightarrow G$. For any a,b $\in$ G we shall write a$*$b for $*(a, b)$.
- A binary operation $*$ on a set G is associative if $\forall a, b, c \in G$ we have $(a*b)*c = a*(b*c)$.
- A binary operation $*$ on a set G is commutative if $\forall a, b \in G, a * b = b * a$

Definition 2 (Groups).

- A group is an ordered pair $(G, *)$ where G is a set and $*$ is a binary operations G satisfying the following axioms:
  1. Closure/associativity: There exists an associative binary operation $*$ on G.
  2. Identity: There exists an element e $\in$ G, called an identity element of G, such that $\forall a \in G, a * e = e * a$.
  3. Inverse: For each $a \in G$, there exists an element a^{-1} of G, called an inverse of a, such that $a * a^{-1} = a^{-1} * a$.

Definition 3 (Abelian Group). A group $(G, *)$ is called an abelian iff $*$ is a commutative operation.

4.1.2 Rings

Definition 4 (Rings).

- A ring R is a set endowed with two binary operations + and $*$ called (addition and multiplication) satisfying the following axioms:
  1. $(R, +)$ is an abelian group.
  2. Associativity: the binary opeation $*$ is associative.
  3. Distributivity: The distributive laws hold in R.

- The ring R is commutative if multiplication is commutative.

- Identity: The ring R is said to have an identity(or contain a 1) if there is an element $1 \in R$ with: $1 * a = a * 1 = a. \forall a \in R$.

4.1.3 Fields

Definition 5 (Fields). A field F is a commutative ring with unity satisfying the additional axiom that for each nonzero element $x \in F$, there exists an element $x^{-1} \in F$ such that: $x * x^{-1} = x^{-1} * x = 1$.

Definition 6 (Action of a field).

- Informally: An action of a field on an abelian group is an abstraction of the "scalar multiplication" of vectors by numbers.

- formally: An action of a field F on an abelian group G is a function $. : F \times G \to G$ with the following properties:

  1. Distributivity I: For all $a \in F$ and all $u, v \in G$: $a.(u + v) = a.u + a.v$

  2. Distributivity II: For all $a, b \in F$ and all $v \in G$: $(a + b).v = a.v + b.v$

  3. Compatibility of the action with multiplication in the field F: For all $a, b \in F$ and $v \in G$: $(ab).v = a.(b.v)$.

  4. Identity: For all $v \in G$: $1.v = v$

4.2 Basic Linear algebra

4.2.1 The Definition of a Vector Space

Definition 7 (The Definition of a Vector Space). A *vector space* V over a field F is an abelian group V equipped with an action of the field F on V.

Definition 8 (Subspace of a Vector Space). A subset $S \subset V$ of a vector space V over a field F is a subspace of V iff S is a vector space over F.

Proposition 1 (Conditions for a subspace). A subset U of V is a subspace of V if and only if U satisfies the following three conditions:

- additive identity: $0 \in$ U

- closed under addition: u,w $\in$ U $\implies$ u+w$\in U$

- closed under scalar multiplication: $a \in F$ and $u \in U \implies au \in U$

Definition (Direct sum). The direct sum of vector spaces V and W is the vector space $V \oplus W$ where:

- The elements: $V \oplus W = \{(a, b) | a \in V, b \in W\}$
- The addition operation is the function defined as:

$$+ : (a, b) \times (c, d) \mapsto (a + c, b + d)$$

- The multiplication operation is the function defined as:

$$\cdot : (s \cdot a, s \cdot b) \mapsto s \cdot (a, b)$$

4.2.2 Span, Linear Independence, Bases and Dimension

Definition 9 (linear combination). A linear combination of a list $v_1, v_2 \ldots, v_n$ of vectors in V is a vector of the form $a_1 v_1 + a_2 v_2 \cdots + a_n v_n$ where $a_1, a_2 \ldots a_n \in F$
Definition 10 (span). The span of a list of vectors in V is defined as:

$$span(v_1, v_2 \ldots, v_n) \equiv \{a_1 v_1 + a_2 v_2 \cdots + a_n v_n : a_1, a_2, \cdots + a_n \in F\}$$

Definition 11 (spans). if $span(v_1, v_2 \ldots, v_n)$ equals V, we say that $v_1, v_2 \ldots, v_n$ spans V.

Definition 12 (finite-dimensional vector space). A vector space is called finite-dimensional if some list of vectors in it spans the space.

Definition 12 (infinite-dimensional vector space). A vector space is called infinite-dimensional if it is not finite-dimensional.

Definition 13 (Linear independence). A list of vectors $v_1, v_2 \ldots, v_n$ in V is called linearly independent if the only choice of $a_1, a_2, \ldots, a_n$ that makes $a_1 v_1 + a_2 v_2 \cdots + a_n v_n$ equal 0 is $a_1 = a_2 = \cdots = a_n = 0$. The empty list () is also declared to be linearly independent.

Definition 14 (Linear map). A linear map is a function $f : V \to W$ between vector spaces, with the following properties, for all $a, b \in V$ and $s \in F$:

$$f(a + b) = f(a) + f(b) \tag{1}$$

$$f(s \cdot a) = s \cdot f(a) \tag{2}$$

Notation.

- The set of all linear maps from V to W is denoted $L(V, W)$.
- The set of all linear maps from V to V is denoted $L(V)$.

4.2.3 Bases and Matrices

Motivation. One of the most important structures a vector space can have is a basis. A basis give rise to the notion of dimension of a vector space, and lets us represent linear maps using matrices.

Definition 5 (Basis). For a vector space V, a family of elements $\{e_i\}$ is linearly independent when every element $v \in V$ can be expressed as a finite linear combination $v = \sum_i \alpha_i e_i$ with coefficients $\alpha_i \in F$ in at most one way. It is a basis if additionally any $v \in V$ can be expressed as such a finite linear combination.

Proposition 1. Every vector space admits a basis, and any two bases for the same vector space have the same cardinality.

Definition 6 (Dimension, finite-dimensionality). The dimension of a vector space V , written $dim(V)$, is the cardinality of any basis. A vector space is finite-dimensional when it has a finite basis.

Proposition 2. If vector spaces V and W have bases $\{d_i\}$ and $\{e_j\}$, and we fix some order on the bases, we can represent a linear map $f : V \mapsto W$ as the matrix with $dim(W)$ rows and $dim(V)$ columns, whose entry at row i and column j is the coefficient $f(d_j)_i$. Composition of linear maps then corresponds to matrix multiplication.

Definition 7(trace). For a square matrix with entries m_{ii} , its trace is the $\sum_i m_{ii}$ of its diagonal entries.

4.2.4 Eigenvalues, Eigenvectors, and Invariant Subspaces

Definition (invariant subspace). Suppose $T \in L(V)$. A subspace U of V is called invariant under T if $u \in U \implies Tu \in U$.

Definition (eigenvalue). Suppose $T \in L(V)$. A number $\lambda \in F$ is called an eigenvalue of T if $\exists v \in V$ s.t $v \neq 0$ and $Tv = \lambda v$.

Definition (eigenvector). Suppose $T \in L(V)$ and $\lambda \in F$ is an eigenvalue of T. A vector $v \in V$ is called an eigenvector of T corresponding to λ if $v \neq 0$ and $Tv = \lambda v$.

Theorem (Linearly independent eigenvectors).

Theorem (Number of eigenvalues) Suppose V is finite-dimensional. Then each operator on V has at most dim V distinct eigenvalues.

Theorem (Operators on complex vector spaces have an eigenvalue) Every operator on a finite-dimensional, nonzero, complex vector space has an eigenvalue.

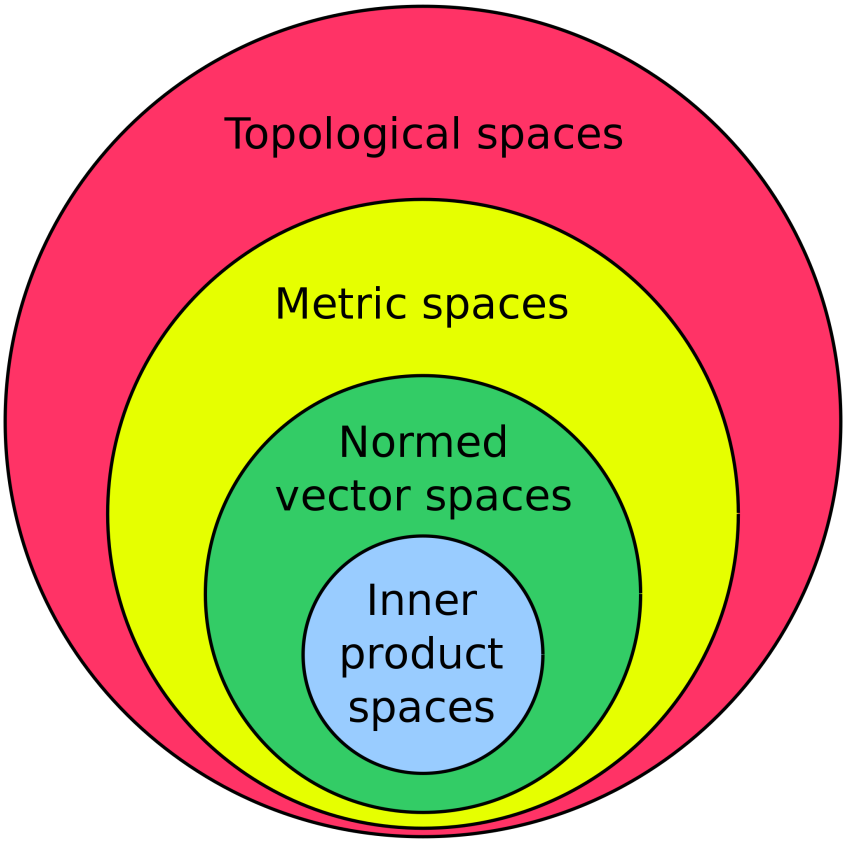
Definition (eigenspace, $E(\lambda, T)$). suppose $T \in L(V)$ and $\lambda \in F$. The eigenspace of T corresponding to λ, denoted $E(\lambda, T)$, is defined by

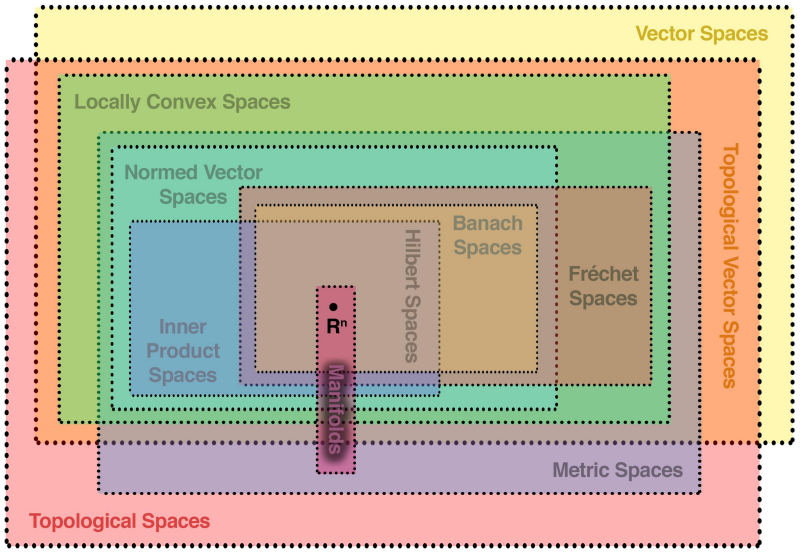
$$E(\lambda, T) \stackrel{\text{def}}{=} null(T - \lambda I)$$

Definition (diagonalizable). An operator $T \in V$ is called diagonalizable if the operator has a diagonal matrix with respect to some basis of V.

4.3 Basic functional analysis

Introduction. Functional analysis is an abstract branch of mathematics that originated from classical analysis. Its development started about eighty years ago, and nowadays functional analytic methods and results are important in various fields of mathematics and its applications(including quantum mechanics). The impetus came from linear algebra, linear ordinary and partial differential equations, calculus of variations, approximation theory and, in particular, linear integral equations, whose theory had the greatest effect on the development and promotion of the modern ideas.





4.3.1 Metric spaces

Definition (Metric space). A set X, whose elements we shall call points, is said to be a metric space if with any two points p and q of X there is associated a real number $d(p, q)$, called the distance from p to q, such that:

- $d(p, q) > 0$ if $p \neq q; d(p, p) = 0$;
- $d(p, q) = d(q, p)$;
- $d(p, q) \leq d(p, r) + d(r, q), \forall r \in X$

Any function with these three properties is called a distance function, or a metric.

4.3.2 NORMED SPACES. BANACH SPACES

Definition(Norm). A norm on (complex or real) vector space X is a real-valued function on X

$$|| - || : X \to R$$

$$x \mapsto ||x||$$

which has the properties:

- $||x|| \geq 0$
- $||x|| = 0 \iff x = 0$
- $||\alpha x|| = |\alpha||x||$
- $||x + y|| \leq ||x|| + ||y||$

Definition (Normed space, Banach space). A normed space X is a vector space with a norm defined on it. A Banach space is a complete normed space (complete in the metric defined by the norm). A norm on X defines a metric d on X which is given by:

$$d(x, y) \stackrel{\text{def}}{=} ||x - y||, (x, y \in X)$$

and is called the metric induced by the norm. The normed space just defined is denoted by $(X, || - ||)$ or simply by X.

Convention. In the case of normed spaces a mapping is called an operator.

Definition (Bounded linear operator). Let X and Y be normed spaces and

$$T : X \to Y$$

a linear operator. The linear operator T is said to be bounded if

$$\exists c \in R. \forall x \in X, ||Tx|| \leq c||x||$$

Definition (The norm of an operator). The norm of an operator $T : X \to Y$ is the quantity defined by:

$$||T|| \stackrel{\text{def}}{=} sup_{x \in X, x \neq 0} \frac{||Tx||}{||x||}$$

4.3.3 INNER PRODUCT SPACES. HILBERT SPACES

Motivation. Hilbert spaces are structures that are built on normed vector spaces. The extra structure lets us define angles and distances between vectors, and is used in quantum theory to calculate probabilities of measurement outcomes.

Definition 8(Inner product). An inner product on a complex vector space V is a function $\langle -|- \rangle : V \times V \to C$ that is:

1. conjugate-symmetric: for all $a, b \in V$

$$\langle a|b \rangle = \langle b|a \rangle^* \tag{3}$$

2. linear in the second argument: for all $a, b, c \in V$ and $s \in C$,

$$\langle a|s \cdot b \rangle = s \langle a|b \rangle \tag{4}$$

$$\langle a|b + c \rangle = \langle a|b \rangle + \langle a|c \rangle \tag{5}$$

3. positive definite: for all $a \in V$

$$\langle a|a \rangle \geq 0 \tag{6}$$

$$\langle a|a \rangle = 0 \implies v = 0 \tag{7}$$

Remark. An inner product on X defines a norm on X given by:

$$||x|| = \sqrt{\langle x|x \rangle}$$

Definition (Inner product space, Hilbert space). An inner product space (or pre-Hilbert space) is a vector space X with an inner product defined on X. A Hilbert space is a complete inner product space (complete in the metric defined by the inner product).

Proposition. The complex numbers carry a canonical inner product:

$$\langle s|t \rangle = s^* t$$

Proposition. Every linear map(operator) between finite-dimensional Hilbert spaces is bounded.

Riesz's Theorem (Functionals on Hibert spaces). Every bounded linear functional f on a Hilbert space H can be represented in terms of the inner product, namely,

$$f(x) = \langle x|z \rangle$$

where z depends on f, is uniquely determined by f and has norm

$$||x|| = ||f||$$

4.3.4 Operators on Hilbert spaces

The deepest results related to inner product(pre-hilbert) spaces deal with its operators. By exploiting properties of the adjoint, we will develop a detailed description of several important classes of operators on inner product spaces.

The inner product gives rise to the adjoint of a bounded linear map.

Definition (Adjoint). Let H_1, H_2 be two Hilbert spaces. A bounded linear map $f : H_1 \to H_2$, its adjoint $f^\dagger : H_2 \to H_1$ is the unique linear map with the following property,

$$\forall a \in H_1, b \in H_2. \langle f(a)|b\rangle = \left\langle a\middle|f^\dagger(b)\right\rangle$$

Remark. The existence of the adjoint follows from the Riesz representation theorem for Hilbert spaces. It follows immediately by the uniqueness of adjoints that they satisfy the following properties:

- $$(f^\dagger)^\dagger = f$$
- $$(g \circ f)^\dagger = f^\dagger \circ g^\dagger$$
- $$id_H^\dagger = id_H$$

Definition (classes of operators). A bounded linear map $f : H_1 \to H_2$ between Hilbert spaces is:

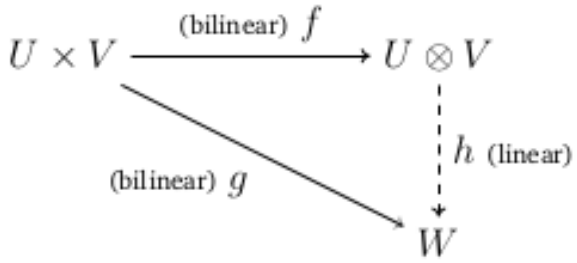
- self-adjoint when $f = f^\dagger$.
- a projection when $f = f^\dagger$ and $f \circ f = f$.
- unitary when both $f^\dagger \circ f = id_{H_1}$ and $f \circ f^\dagger = id_{H_2}$.
- an isometry when $f^\dagger \circ f = id_H$
- a partial isometry when $f^\dagger \circ f$ is a projection
- and positive when $f = g^\dagger \circ g$ for some linear map $g : H_1 \to H_2$

Definition (The dual of the Hilbert space). For a Hilbert space H, its dual Hilbert space H^* is the vector space of linear maps $f : H \to C$ also called linear functionals (on H).
Proposition. A Hilbert space is isomorphic to its dual in an anti-linear way: the map $H \to H^*$ given by $|a\rangle \to \langle a|$ s an invertible anti-linear function.
Proposition. The inner product on H^* is given by $\langle \phi_a|\phi_b\rangle_{H^*} = \langle a|b\rangle_H$ and makes the function $|a\rangle \to \langle b|$ bounded.

Proposition. Some bounded linear maps support a notion of trace.
Definition(Trace, trace class.) When it converges, the trace of a positive linear map $f : H \to H$ is given by $Tr(f) = \sum \langle e_i | f(e_i) \rangle$ for any orthornormal basis e_i, in which case the map is called trace class.

4.3.5 Tensor products

Motivation. The tensor product is a way to make a new vector space out of two given ones. With some work the tensor product can be constructed explicitly, but it is only important for us that it exists, and is defined up to isomorphism by a universal property. if U,V and W are vector spaces, a function $f : U \times V \to W$ is called bilinear when it is linear in each variable; that is, when the function $u \to f(u, v)$ is linear for $v \in V$, and the function $v \to f(u, v)$ is linear for each $u \in U$.
Definition(Tensor product of vector spaces). The tensor product of vector spaces U and V is a vector space $U \otimes V$ together with a bilinear function $f : U \times V \to U \otimes V$ such that for every bilinear function $g : U \times V \to W$ there exists a unique linear function $h : U \otimes V \to W$ such that $g = h \circ f$.



Remark. $U \times V$ is not itself a vector space, so it doesn't make sense to ask if f or g is linear. the function f usually stays anonymous and is written as $(a, b) \mapsto a \otimes b$. It follows that arbitrary elements of $U \times V$ take the form $\sum_{i=1}^{n} s_i a_i \otimes b_i$ for $s_i \in C, a_i \in U$ and $b_i \in V$.
Proposition. The tensor product also extends to linear maps.
Proposition. if $f_1 : U_1 \to V_1$ and $f_2 : U_2 \mapsto V_2$ are linear maps, there is a unique linear map $f_1 \otimes f_2 : U_1 \otimes U_2 \mapsto V_1 \otimes V_2$ that satisfies $(f_1 \otimes f_2)(a_1 \otimes a_2) = f_1(a_1) \otimes f_2(a_2)$ for $a_1 \in U_1$ and $a_2 \in U_2$.
Definition(The tensor product of Hilbert spaces). The tensor product of Hilbert spaces H and K is the Hilbert space $H \otimes K$ built by taking tensor product of the underlying vector spaces, giving it the inner product $\langle a_1 \otimes b_1 | a_2 \otimes b_2 \rangle = \langle a_1 | a_2 \rangle_H \langle b_1 | b_2 \rangle_K$ then completing it.

Proposition. if $\{e_i\}$ is an orthornormal basis for Hilbert space H, and $\{f_j\}$ is an orthornormal basis for K, then $\{e_i \otimes f_j\}$ is an orthornormal basis for $H \otimes K$.

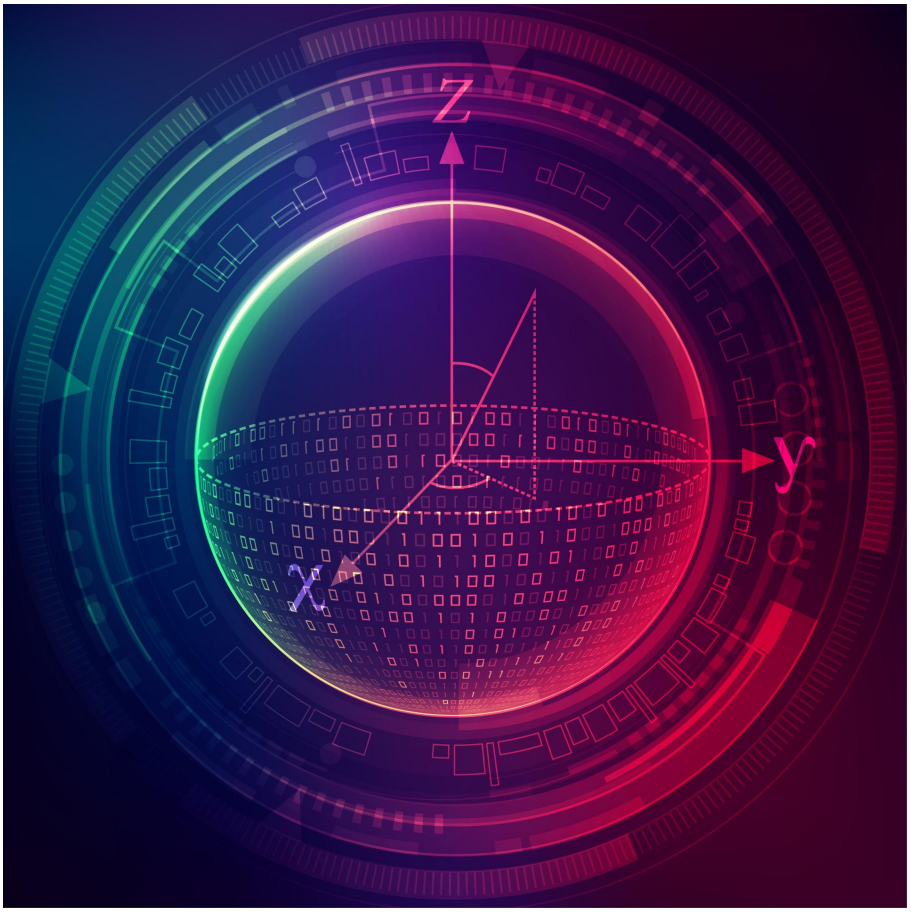
Proposition. When H and K are finite-dimensional, there is no difference between their tensor products as vector spaces and as Hilbert spaces.

Definition(Kronecker product). When finite-dimensional Hilbert spaces H_1, H_2, K_1, K_2 are equipped with fixed ordered orthonormal bases, linear maps $f : H_1 \to K_1$ and $g : H_2 \to K_2$ can be written as matrices. Their tensor product $f \otimes g : H_1 \otimes H_2 \to K_1 \otimes K_2$ corresponds to the

following block matrix, called their Kronecker product:

$$(f \otimes g) \stackrel{\text{def}}{=} \begin{bmatrix} (f_{11}g) & (f_{12}g) & \dots (f_{1n}g) \\ (f_{21}g) & (f_{22}g) & \dots (f_{2n}g) \\ \vdots & \ddots & \\ (f_{m1}g) & (f_{m2}g) & \dots (f_{mn}g) \end{bmatrix}$$

4.4 Basic Quantum information theory



Quantum information theory studies the information processing capabilities of quantum systems, using the mathematical abstractions of Hilbert spaces and linear maps. I have followed mainly [7] in this section.

4.4.1 State spaces

Classical computer science often considers systems to have a finite set of states. An important simple system is the bit, with state space given by the set 0,1.
Quantum information theory instead assumes that systems have state spaces given by finite-dimensional Hilbert spaces. The quantum version of the bit is the qubit.

Definition(Qubit).

- Physically: A qubit or quantum bit is a basic unit of quantum information—the quantum version of the classic binary bit physically realized with a two-state device. A qubit is a two-state (or two-level) quantum-mechanical system, one of the simplest quantum systems displaying the peculiarity of quantum mechanics.

- Mathematically: A qubit is a quantum system with state space C^2.

A pure state of a quantum system is given by a vector $v \in H$ in its associated Hilbert space. Such a state is normalized when the vector in the Hilbert space has norm 1:

$$\langle a|a\rangle = 1$$

In particular, a complex number of norm 1 is called a phase.
A pure state of a qubit is therefore a vector of the form:

$$a = \begin{pmatrix} s \\ t \end{pmatrix}$$

with $s, t \in C$, which is normalized when $|s|^2 + |t|^2 = 1$
When performing computations in quantum information, we often use the following privileged basis.

Definition(Computational basis, Z basis). For the Hilbert space C^n, the computational basis, or Z basis is the orthonormal basis given by the following vectors:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} |1\rangle = \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix} \ldots |n-1\rangle = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}$$

Every state $a \in C^n$ can be written in terms of the computational basis; for a qubit, we can write, $a = s\,|0\rangle + t\,|1\rangle$ for some $s, t \in C$. The following alternative qubit basis also plays an important role.

Definition(The X basis). The X basis for a qubit C^2 is given by the following states:

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

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

Processing quantum information takes place by applying unitary maps $f : H \to H$ to the Hilbert space of states. Such a map will take a normalized state $a \in H$ to a normalized state $f(a) \in H$. An example of a unitary map is the X gate.

4.4.2 Compound systems and entanglement

Given two quantum systems with state spaces given independently by Hilbert spaces H and K, as a joint system their overall state space is $H \otimes K$, the tensor product of the two Hilbert spaces. This is a postulate of quantum theory. As a result, state spaces of quantum systems grow large very rapidly: a collection of n qubits will have a state space isomorphic C^{2^n}, requiring 2^n complex numbers to specify its state vector exactly. In contrast, a classical system consisting of n bits can have its state specified by a single binary number of length n.
In quantum theory, (pure) product states and (pure) entangled states are defined as follows.

Definition(Product state, entangled state). For a compound system with state space $H \otimes K$, a product state is a state of the form $a \otimes b$ with $a \in H$ and $b \in K$. An entangled state is a state not of this form.
The definition of product and entangled state also generalizes to systems with more than two components. When using Dirac notation, if $|a\rangle \in H$ and $|b\rangle \in K$ are chosen states, we will often write $|ab\rangle$ for their product states $|a\rangle \otimes |b\rangle$.
The following family of entangled states plays an important role in quantum information theory.

Definition(Bell state). The Bell basis for a pair of qubits with state space $C^2 \otimes C^2$ is the orthornomal basis given by the following states:

$$|Bell_0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

$$|Bell_1\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$

$$|Bell_0\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$

$$|Bell_0\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

Remark. The state $|Bell_0\rangle$ is often called "The Bell state", and is very prominent in quantum information. The Bell states are maximally entangled, meaning that they induce an extremely strong correlation between the two systems involved.

4.4.3 Pure states and measurements

Introduction. For a quantum system in a pure state, the most basic notion of measurement is a projection-valued measure. Quantum theory is a set of rules that says what happens to the quantum state when a projection-valued measurement takes place, and the probabilities of the different outcomes. From the previous definition of projections-projections are maps satisfying $p = p^\dagger = p \circ p$.
Definition. A finite family of linear maps $f_i : H \to H$ is complete when the following holds:

$$\sum_i f_i = id_H$$

Definition. A family of linear maps $f_i : H \to H$ is orthogonal when for any $i \neq j$, the following holds:

$$f_i \circ f_j = 0$$

Definition(Projection-valued measure, nondegenerate).A projection-valued measure (PVM) on a Hilbert space H is a finite family of projections $p_i : H \to H$ which are complete and orthogonal. A PVM is nondegenerate when $tr(p_i)$ for all i.
Remark. In this definition of PVM, the orthogonality property is actually redundant; that is, a complete family of projections is necessarily also orthogonal. For simplicity, however, we include the orthogonality requirement here directly. Also note that while our PVMs are finite, in general infinite PVMs are possible; for simplicity, we focus on the finite case.

Lemma. For a finite-dimensional Hilbert space, nondegenerate projection-valued measures correspond to orthonormal bases, up to phase.

A projection-valued measure, when applied to a Hilbert space, will have a unique outcome, given by one of the projections. This outcome will be probabilistic, with distribution described by the Born rule, defined below.

Definition(Born rule). For a projection-valued measure $\{p_i\}$ on a system in a normalized state H, the probability of outcome i, is $\langle a| p_i |a\rangle$.

Result. The definition of a projection-valued measure guarantees that the total probability across all outcomes is 1:

$$\sum_i \langle a| p_i |a\rangle = \langle a| (\sum_i p_i) |a\rangle$$

After a measurement, the new state of the system is $p_i(a)$, where p_i is the projection corresponding to the outcome that occurred. This part of the standard interpretation is called the projection postulate. Note that this new state is not necessarily normalized. If the new state is not zero, it can be normalized in a canonical way, giving $\frac{p_i(a)}{\|p_i(a)\|}$.

Motivation. Given some classical information and some quantum information, it is often the case that we want to apply a unitary operator to the quantum information, in a way that depends on the classical information.

Definition (Controlled operation). Given a Hilbert space H and a set S, a controlled operation is a choice for all $s \in S$ of a unitary $U_s : H \to H$.

4.4.4 Mixed states and measurements

Motivation. Suppose there is a machine that produces quantum system with Hilbert space H. The machine has two buttons: one that will produce the system in state $a \in H$, and another that will produce it in state $b \in H$. You receive the system that the machine produces, but you cannot see it operating; all you know is that the operator of the machine flips a fair coin to decide which button to press. Taking into account this uncertainty, the state of the system that you receive cannot be described by an element of H; the system is in a more general type of state, called a mixed state.

Definition(Density matrix, normalized). A density matrix on a Hilbert space H is a positive map $m : H \to H$. A density matrix is normalized when $Tr(m) = 1$.

Remark. From Definition (0.47) that m is positive when there exists some g with $m = g^{\dagger}g$. Density matrices are more general than pure states, since every pure state $a \in H$ gives rise to a density matrix $m = |a\rangle \langle a|$ in a canonical way. This last piece of Dirac notation is the projection onto the line spanned by the vector a.

Definition(Pure state, mixed state) A density matrix $m : H \to H$ is pure when $m = |a\rangle \langle a|$ for some $a \in H$; generally, it is mixed.

Definition(Maximally mixed state). For a finite-dimensional Hilbert space H, the maximally mixed state is the density matrix $\frac{1}{dim(H)}.id_H$

Remark. There is a notion of convex combination of density matrices, which corresponds physically to the idea of probabilistic choice between alternative states.

Definition(Convex combination). For nonnegative real numbers s, t with $s + t = 1$, the convex combination of matrices $H \xrightarrow{m,n} H$ is the matrix $H \xrightarrow{s.m+t.n} H$.

Proposition. The convex combination of two density matrices is a density matrix.

The density matrix $sm + tn$ describes the state of a system produced by a machine that promises to output state m with probability s, and state n with probability t.

Proposition. In finite dimension, every mixed state can be produced as a convex combination of some number of pure states, which are not unique.

Proposition. the convex combination of distinct density matrices is always a mixed state.

Remark. There is a standard notion of measurement that generalizes the projection-valued measure in the same way that mixed states generalize pure states.

Definition(POVM). A positive operator-valued measure (POVM) on a Hilbert space H is a family of positive maps $f_i : H \to H$ satisfying

$$\sum_i f_i = id_H$$

Proposition. Every projection-valued measure p_i gives rise to a positive operator–valued measure in a canonical way, by choosing $f_i = p_i$.

Proposition. The outcome of a positive operator-valued measurement is governed by a generalization of the Born rule.

Definition (Born rule for POVMs). For a positive operator-valued measure f_i on a system with normalized density matrix $m : H \to H$, the probability of outcome i is $Tr(f_i m)$.

Remark. A density matrix on a Hilbert space $H \otimes K$ can be modified to obtain a density matrix on H alone.

Motivation. Partial traces give rise to a definition of maximally entangled state.

Definition(Partial trace). For Hilbert spaces H and K, there is a unique linear map

$$Tr_k : Hilb(H \otimes K, H \otimes K) \to Hilb(H \otimes H)$$

satisfying

$$Tr_k : (m \otimes n) = Tr(n).m$$

This linear map is called the partial trace over K.

Explicitly, the partial trace of $f : H \otimes K \to H \otimes K$ is computed as follows, using any orthonormal basis $|i\rangle$ for K:

$$Tr_k : \sum_i (id_H \otimes \langle i|) \circ f \circ (id_H \otimes |i\rangle)$$

Physically, this corresponds to discarding the subsystem K and retaining only the part with Hilbert space H.

Definition. A pure state $a \in H \otimes K$ is maximally entangled when tracing out either H or K from $|a\rangle \langle a|$ gives a maximally mixed state; explicitly this means the following, for some $s, t \in C$:

$$Tr_H(|a\rangle \langle a|) = s.id_k$$

$$Tr_H(|a\rangle \langle a|) = t.id_H$$

Remark. When $|a\rangle$ is normalized, its trace will be a normalized density matrix, so $s = \frac{1}{dim(H)}$ and $t = \frac{1}{dim(K)}$

Lemma. Any two maximally entangled states $a, b \in H \otimes K$ are related by $(f \otimes id_k)(a) = b$ for a unique unitary $f : H \to H$.

4.4.5 Decoherence

By Lemma 0.62, every nondegenerate projection-valued measure $p_1, ..., p_n$ on a Hilbert space H corresponds (up to a phase) to an orthonormal basis $|1\rangle, .., |n\rangle$ for H via $p_i = |i\rangle \langle i|$, and hence induces n pure states of H. We may regard this as a controlled preparation: depending on some classical data i = 1, . . . , n, we prepare state $|i\rangle$. Consider how this controlled preparation composes with a measurement in the same basis.
If we start with some classical information, use it to prepare a quantum system, and then immediately measure, we should end up with the same classical information we started with. Indeed, according to the Born rule of Definition 0.63, the probability of getting outcome j after preparing state i is:

$$\langle j| p_i |j\rangle = \langle j|i\rangle \langle i|j\rangle = ||\langle i|j\rangle||^2$$

which is 1 for i = j but 0 for i 6 = j.
The other way around is conceptually less straightforward: if you measure a quantum system, yielding a piece of classical data, and then immediately use that to prepare a state of a quantum

system, what do you get? Well, supposing that the quantum system starts in a mixed state given by a density matrix $m : H \to H$ with $m = \sum_{ij} c_{ij} |i\rangle \langle j|$, the measurement results in outcome $|i\rangle$ with probability $Tr(p_i m) = \langle i| m |i\rangle$, so the state eventually prepared is

$$\sum_i c_{ii} |i\rangle \langle i|$$

The nondiagonal elements of the density matrix m have vanished, and the mixed state has become a convex combination of pure states that no longer cohere. This process is called decoherence. Any quantum state undergoes decoherence constantly as it interacts with its environment. It takes extremely good experimental control to keep a quantum state from decohering rapidly.

4.4.6 Quantum teleportation

Quantum teleportation is a beautiful and simple procedure, which demonstrates some of the counterintuitive properties of quantum information. It involves two agents, Alice and Bob. Alice has a qubit, which she would like to give to Bob without changing its quantum state, but she is limited to sending classical information only. Assume that Alice and Bob share a maximally entangled state, say the Bell state.

Definition(Teleportation of a qubit). The procedure is as follows.

1. Alice prepares her initial qubit I which she would like to teleport to Bob.

2. Alice and Bob share a pair of maximally entangled qubits, in the Bell state $|BELL_0\rangle$. We write A for Alice's qubit and B for Bob's qubit.

3. Alice measures the system $I \otimes A$ in the Bell basis.

4. Alice communicates the result of the measurement to Bob as classical information.

5. Bob applies one of the following unitaries f_i to his qubit B, depending on which Bell state $|Bell_i\rangle$ was measured by Alice:

$$f_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} f_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} f_2 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} f_3 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

At the end of the procedure, Bob's qubit B is guaranteed to be in the same state in which I was at the beginning. Furthermore, the measurement result that Alice obtains by itself gives no information about the state that Alice is trying to teleport; each possible value has an equal probability.
At first quantum teleportation seems counterintuitive – impossible, even given basic knowledge of the principles of quantum information: the state of a qubit is a vector in C^2 , requiring an infinite amount of classical information to specify, yet in quantum teleportation only 2 classical bits are transferred from Alice to Bob. Nonetheless, the procedure is correct.

5 The practical part

5.1 Deutsch-Jozsa Algorithm

Figure 5.1: David Deutsch

The deusch-Jozsa algorithm solves the following problem: we are a given a function $f : \{0,1\}^n \to \{0,1\}$ that it is either constant(all inputs map to the same output) or balanced (the number of inputs that map to '0' and '1' is equal).

The goal is to determine whether f is constant or balanced.

5.1.1 The classical solution

Classically, in the best case, two queries to the oracle can determine if the hidden Boolean function, $f(x)$, is balanced.

In the worst case, if we continue to see the same output for each input we try, we will have to check exactly half of all possible inputs plus one in order to be certain that $f(x)$ is constant. Since the total number of possible inputs is 2^n, this implies that we need

$$\frac{2^n}{2} + 1 = 2^{n-1} + 1 = O(2^n)$$

trial inputs to be certain that $f(x)$ is constant in the worst case.

5.1.2 The quantum solution

Using a quantum computer, we can solve this problem with 100% confidence after only one call to the function $f(x)$. i.e. its time complexity is $O(1)$ instead of $O(2^n)$.

We first give the circuit description of the algorithm and then analyze each step of the computation.

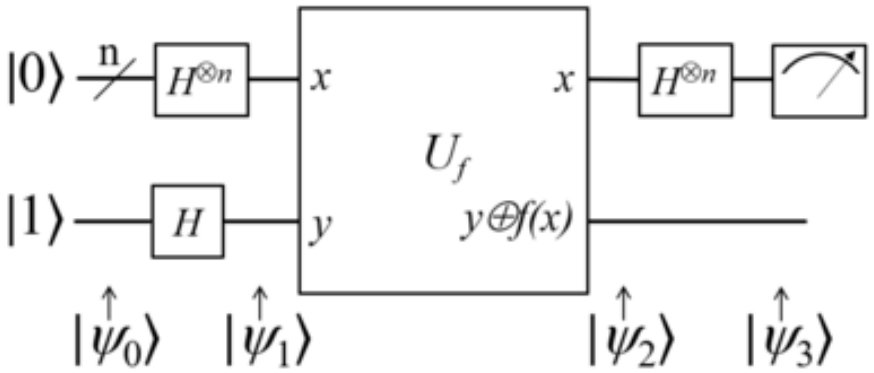


Figure 5.2: The DJ circuit Source:Wikipedia

1. Start with the n-qubit state:

$$|\Psi\rangle_0 = |0\rangle^n |1\rangle$$

2. Apply a Hadamard gate to each qubit:

$$\begin{aligned} |\Psi\rangle_1 &= |+\rangle^n |-\rangle \\ &= \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)\cdots\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)|-\rangle \\ &= \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle |-\rangle \end{aligned}$$

enumi

3. Apply Uf on the whole qubit state:

$$\begin{aligned} |\Psi\rangle_2 &= \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle \left|\frac{|0\rangle - |1\rangle}{\sqrt{2}} \oplus f(x)\right\rangle \\ &= \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle \left(\frac{|f(x)\rangle - \left|\bar{f}(x)\right\rangle}{\sqrt{2}}\right) \\ &= \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{f(x)} |x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \end{aligned}$$

4. At this point the second single qubit register may be ignored. Apply a Hadamard gate to each qubit in the first register:

$$\begin{aligned}|\Psi_3\rangle &= \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{f(x)} \left(\frac{1}{\sqrt{2^n}} \sum_{y\in\{0,1\}^n} (-1)^{x.y} |y\rangle \right) \\ &= \sum_{y\in\{0,1\}^n} \left[\frac{1}{2^n} \sum_{x\in\{0,1\}^n} (-1)^{f(x)+x.y} \right] |y\rangle \\ &= \sum_{y\in\{0,1\}^n} c_y |y\rangle \end{aligned}$$

where $x.y = x_0y_0 \oplus x_1y_1 \ldots \oplus x_{n-1}y_{n-1}$ and $c_y := \left[\frac{1}{2^n} \sum_{x\in\{0,1\}^n} (-1)^{f(x)+x.y}\right]$

5. Measure the first register. Notice that the probability of measuring $|0\rangle^{\otimes n}$ according to born rule:

$$\begin{aligned} P[y = 00\ldots0] &= |\langle 00\ldots0|\Psi_3\rangle|^2 \\ &= |c_{00\ldots0}|^2 \\ &= \left| \frac{1}{2^n} \sum_{x\in\{0,1\}^n} (-1)^{f(x)} \right|^2 \\ &= \frac{1}{2^{2n}} \left| \sum_{x\in\{0,1\}^n} (-1)^{f(x)} \right|^2 \end{aligned}$$

We distinguish 2 cases:

1. If f is a constant function, then $\exists b \in \{0,1\}$ st. $\forall x \in \{0,1\}^n, f(x) = b$. In this case, we have $P[y = 00\ldots0] = \frac{1}{2^{2n}} \left|2^n(-1)^b\right|^2 = 1$ and the algorithm gives the correct answer with probability 1.

2. If f is balanced, we can write:

$$P[y = 00\ldots0] = \frac{1}{2^{2n}} \left|(-1)^{f(x)}\right|^2 = \frac{1}{2^{2n}} \left| \sum_{x\in\{0,1\}^n : f(x)=0} 1 - \sum_{x\in\{0,1\}^n : f(x)=1} 1 \right|^2 = 0$$

and the algorithm gives the correct answer with probability 1.

5.1.3 Creating Quantum Oracles

In [8] a fine example is given on how to create a balanced oracle and I will follow those steps. For a constant function, it is simple:

1. if f(x)=0, then apply the I gate to the qubit in register 2.

2. if f(x)=1, then apply the X gate to the qubit in register 2.

For a balanced function, there are many different circuits we can create. One of the ways we can guarantee our circuit is balanced is by performing a CNOT for each qubit in register 1, with the qubit in register 2 as the target. For example: consider n=2. let $f(x) : \{0,1\}^2 \rightarrow \{0,1\}$ be a function giving by the following table:

x	00	01	10	11
$f(x)$	1	1	0	0

This function shall be represented by the following 8-by-8 unitary matrix:

$$
\begin{array}{c}
\\
\mathbf{00,0} \\
\mathbf{00,1} \\
\mathbf{01,0} \\
\mathbf{01,1} \\
\mathbf{10,0} \\
\mathbf{10,1} \\
\mathbf{11,0} \\
\mathbf{11,1}
\end{array}
\begin{array}{c}
\begin{array}{cccccccc}
\mathbf{00,0} & \mathbf{00,1} & \mathbf{01,0} & \mathbf{01,1} & \mathbf{10,0} & \mathbf{10,1} & \mathbf{11,0} & \mathbf{11,1}
\end{array} \\
\begin{bmatrix}
 & 1 & & & & & & \\
1 & & & & & & & \\
 & & & 1 & & & & \\
 & & 1 & & & & & \\
 & & & & 1 & & & \\
 & & & & & 1 & & \\
 & & & & & & 1 & \\
 & & & & & & & 1
\end{bmatrix}
\end{array}
$$

This is the circuit instantiation of the oracle when $f(10) = 10$ and the input register is 0. ie, $Uf : |10\rangle|0\rangle :\rightarrow |10\rangle|0\rangle$

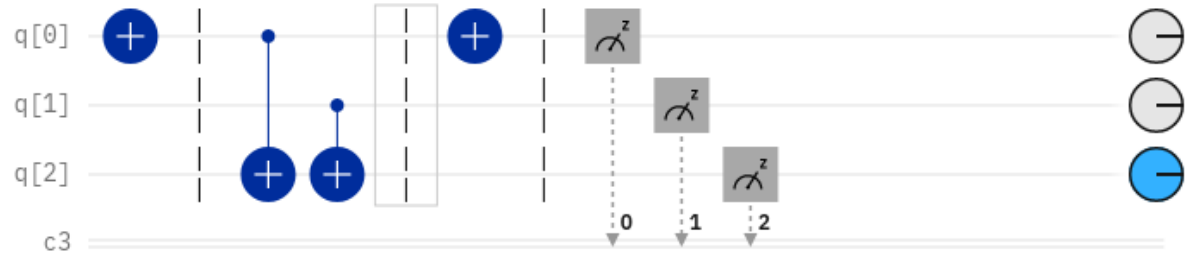
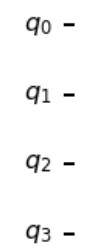
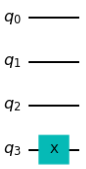


Figure 5.3: The circuit implementation of a balanced quantum oracle

5.1.4 Qiskit Implementation

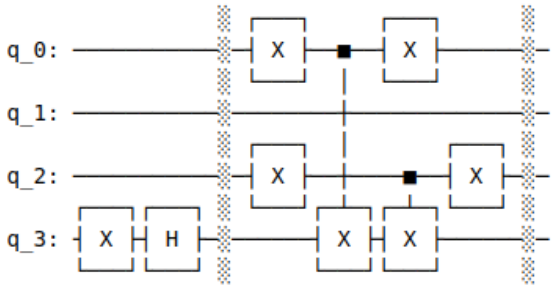
```
1
2
3
4  from qiskit import QuantumCircuit, execute, Aer, BasicAer
5  from qiskit.visualization import plot_histogram
6
7  import numpy as np
8
9
10 n=3
11 f0allx = QuantumCircuit(n+1) #constant oracle for f(x)=0 for all x
12
13
14 display(f0allx.draw('mpl'))
15
16 f1allx = QuantumCircuit(n+1) #constant oracle for f(x)=1 for all x
17 f1allx.x(n)
18
19 display(f1allx.draw('mpl'))
```





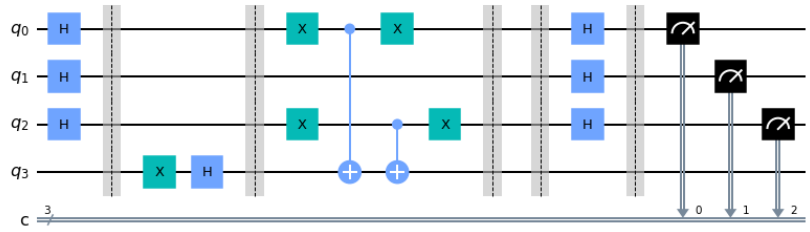

```
1
2
3  f01half = QuantumCircuit(n+1)
4  xgates = "101"
5  cxgates= "101"
6
7
8  # Put ancilia qubit in state |->
9  f01half.x(n)
10 f01half.h(n)
11
```

```
f01half.barrier()
# Place X-gates before implementing CX gates in the next loop
for i in range(n):
    if xgates[i] == '1':
        f01half.x(i)




# Place CX-gates to give phase at desired combinations
for m in range(n):
    if cxgates[m] == '1':
        f01half.cx(m,n)


# Place X-gates again to revert to original inputs on 0 to n-1
   qubits
for k in range(n):
    if xgates[k] == '1':
        f01half.x(k)
f01half.barrier()
# Show oracle
f01half.draw()
```




```

dj_circuit = QuantumCircuit(n+1, n)

# Apply H-gates
for qubit in range(n):
    dj_circuit.h(qubit)



dj_circuit.barrier()
# Add oracle
dj_circuit =dj_circuit + f01half
dj_circuit.barrier()
# Repeat H-gates
for qubit in range(n):
    dj_circuit.h(qubit)
dj_circuit.barrier()
```

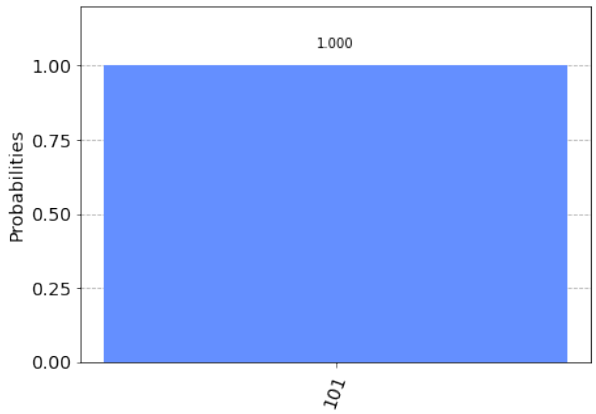
```
18
19 # Measure
20 for i in range(n):
21     dj_circuit.measure(i, i)
22
23 # Display circuit
24 dj_circuit.draw('mpl')
```



5.1.5 Simulating Using QasmSimulator:

```
1
2
3
4  # use local simulator
5  backend = BasicAer.get_backend('qasm_simulator')
6  shots = 1024
7  results = execute(dj_circuit, backend=backend, shots=shots).result()
8  answer = results.get_counts()
9
10 plot_histogram(answer)
```

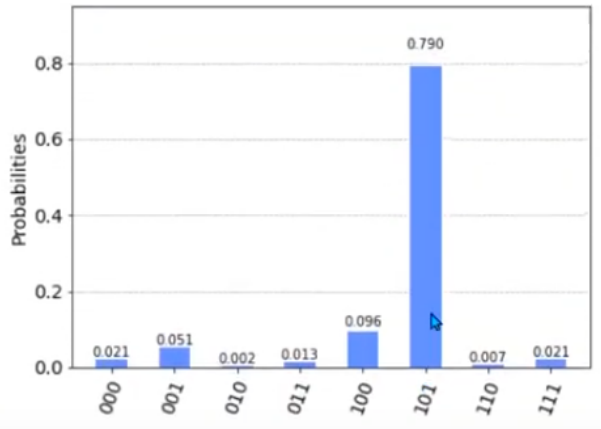
We perform the simulation using QasmSimulator and expect to see 101 for a balanced oracle. The circuit is executed and results are now visualized as count plot —



This shows that 0% chance of predicting 000, i.e. oracle is balanced.

5.1.6 Using IBM Quantum Computer

I've run the same circuit in a quantum computer. I've used IBM Quantum Computer and checked on IBM-Q (quantum simulator) which has the least number of jobs on queue.



Testing DJ algorithm with a balanced oracle, on a quantum computer shows us that most likely result is 101. Compared to the simulated case the real device is still susceptible to quantum noise and thus we can see components other than $|101\rangle$ are present too.

5.2 Bernstein–Vazirani algorithm

Figure 5.4: Umesh Vazirani

5.2.1 Introduction

The Bernstein-Vazirani algorithm, first introduced in [9], can be seen as an extension of the Deutsch-Jozsa algorithm we covered in the last section. It showed that there can be advantages in using a quantum computer as a computational tool for more complex problems than the Deutsch-Jozsa problem.

5.2.2 The Bernstein-Vazirani Problem

Given an oracle that implements a function:

$$f : \{0,1\}^n \to \{0,1\}$$

$$x \mapsto s.x \pmod 2,\ s \in \{0,1\}^n$$

Instead of the function being balanced or constant as in the Deutsch-Jozsa problem, now the function is guaranteed to return the dot product of the input with some string, s.

5.2.3 The Classical Solution

Classically, the most efficient method to find the secret string is by evaluating the function n times with the sequence of input values:

$$f(100...0) = s_1$$

$$f(010...0) = s_2$$

$$f(001...0) = s_3$$

$$\vdots$$

$$f(00...1) = s_n$$

5.2.4 The Quantum Solution

Contrast to the classical solution which needs at least n queries of the function to find s, only one query is needed using quantum computing. The quantum algorithm is as follows:

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

The reason that the last state is $|s\rangle$ is because, for a particular y:

$$\frac{1}{2^n} \sum_{x\in\{0,1\}^n} (-1)^{f(x)+x\cdot y} = \frac{1}{2^n} \sum_{x\in\{0,1\}^n} (-1)^{x\cdot s+x\cdot y} = \frac{1}{2^n} \sum_{x\in\{0,1\}^n} (-1)^{x\cdot(s\oplus y)} = 1 \text{ if } s\oplus y = \vec{0},\ 0 \text{ otherwise.}$$

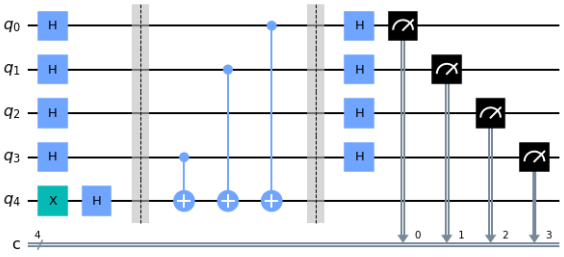
Since $s \oplus x = 0$ is only true when $s = y$.this means that the only non-zero amplitude is on $|s\rangle$. So, measuring the output of the circuit in the computational basis yields the secret string s.

5.2.5 Qiskit Implementation

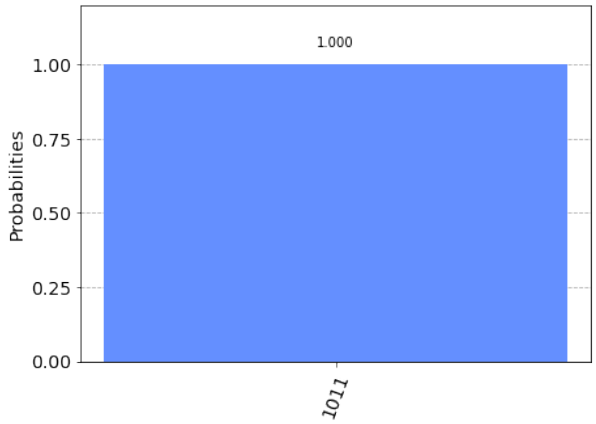
We'll now walk through the Bernstein-Vazirani algorithm implementation in Qiskit for a three bit function with $s = 000$

```
1
2 from qiskit import QuantumCircuit, execute, Aer, BasicAer
3 from qiskit.visualization import plot_histogram
4
5 import numpy as np
```

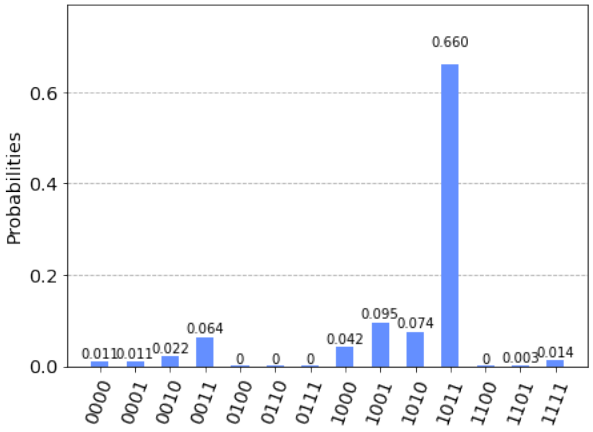
```
6
7  n =4  # number of qubits used to represent s
8  s = '1011'   # the hidden binary string
9
10 # We need a circuit with n qubits, plus one ancilla qubit
11 # Also need n classical bits to write the output to
12 bv_circuit = QuantumCircuit(n+1, n)
13
14
15
16 # Apply Hadamard gates before querying the oracle
17 for i in range(n):
18     bv_circuit.h(i)
19
20
21
22 # put ancilla in state |->
23 bv_circuit.x(n)
24 bv_circuit.h(n)
25
26 # Apply barrier
27 bv_circuit.barrier()
28
29 # Oracle to implement bit string multiplication
30  # reverse s to fit qiskit's qubit ordering
31 i=n-1
32 for q in s:
33     if q == '1':
34         bv_circuit.cx(i, n)
35     i-=1
36
37 # Apply barrier
38 bv_circuit.barrier()
39
40 #Apply Hadamard gates after querying the oracle
41 for i in range(n):
42     bv_circuit.h(i)
43
44 # Measurement
45 for i in range(n):
46     bv_circuit.measure(i, i)
47
48 bv_circuit.draw('mpl')
```




```
1
2  # use local simulator
3  backend = BasicAer.get_backend('qasm_simulator')
4  shots = 1024
5  job = execute(bv_circuit, backend=backend, shots=shots)
6  results=job.result()
7  answer = results.get_counts()
8
9  plot_histogram(answer)
```




```
1
2  from qiskit import IBMQ
3
4
5  IBMQ.save_account('
       b7c3d5261ffcdc9163d35371670119c46adb48436e35147c205928aa37c913fcbee976e715f85
       ', overwrite=True)
6  provider=IBMQ.load_account()
7  backend=provider.get_backend('ibmq_quito')
8
9  job = execute(bv_circuit, backend=backend, shots=1024)
10 counts=job.result().get_counts()
11 plot_histogram(counts)
```


Probabilities
0.0
0.2
0.4
0.6
0.011
0.011
0.022
0.064
0
0
0
0.042
0.095
0.074
0.660
0
0.003
0.014
0000
0001
0010
0011
0100
0110
0111
1000
1001
1010
1011
1100
1101
1111

6 Conclusion

Finally, to conclude, we have gone through the theory and necessary mathematics of quantum information, analyzed the basic quantum algorithms- Deutsch-Jozsa and Simon, and eventually checked our understanding by testing them against a balanced oracle using Qiskit.

References

[1] R. P. Feynman, "Simulating physics with computers," in *Feynman and computation*. CRC Press, 2018, pp. 133–153.

[2] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM review*, vol. 41, no. 2, pp. 303–332, 1999.

[3] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *arXiv preprint arXiv:2003.06557*, 2020.

[4] V. Hassija, V. Chamola, A. Goyal, S. S. Kanhere, and N. Guizani, "Forthcoming applications of quantum computing: peeking into the future," *IET Quantum Communication*, vol. 1, no. 2, pp. 35–41, 2020.

[5] S. Axler, *Linear algebra done right*. Springer Science & Business Media, 1997.

[6] D. S. Dummit and R. M. Foote, *Abstract algebra*. Wiley Hoboken, 2004, vol. 3.

[7] J. Preskill, "Lecture notes for physics 229: Quantum information and computation," *California Institute of Technology*, vol. 16, no. 1, pp. 1–8, 1998.

[8] "Qiskit-textbook," https://learn.qiskit.org/course/ch-algorithms/deutsch-jozsa-algorithm, accessed: 12 june 2022.

[9] E. Bernstein and U. Vazirani, "Quantum complexity theory," in *Proceedings of the twenty-fifth annual ACM symposium on Theory of computing*, 1993, pp. 11–20.