

# Quantum Computation and Quantum Information by Michael A. Nielsen and Isaac L. Chuang

Chris Doble

May 2024

## Contents

<b>I</b>	<b>Fundamental concepts</b>	<b>2</b>
<b>1</b>	<b>Introduction and overview</b>	<b>2</b>
1.2	Quantum bits . . . . .	2
1.2.1	Multiple Bits . . . . .	3
1.3	Quantum Computation . . . . .	3
1.3.1	Single Qubit Gates . . . . .	3
1.3.2	Multiple Qubit Gates . . . . .	4
1.3.3	Measurements in bases other than the computational basis	4
1.3.4	Quantum circuits . . . . .	4
1.3.5	Qubit copying circuit? . . . . .	5
1.3.6	Example: Bell states . . . . .	5
1.3.7	Example: quantum teleportation . . . . .	6
1.4	Quantum algorithms . . . . .	6
1.4.1	Classical computations on a quantum computer . . . . .	6
1.4.2	Quantum parallelism . . . . .	7
1.4.3	Deutsch's algorithm . . . . .	7
1.4.4	The Deutsch-Jozsa algorithm . . . . .	7
1.4.5	Quantum algorithms summarized . . . . .	8
1.5	Experimental quantum information processing . . . . .	8
1.5.1	The Stern-Gerlach experiment . . . . .	8
1.6	Quantum information . . . . .	9
1.6.1	Quantum information theory: example problems . . . . .	9
<b>2</b>	<b>Introduction to quantum mechanics</b>	<b>9</b>
2.1	Linear algebra . . . . .	9
2.1.1	Bases and linear independence . . . . .	9
2.1.2	Linear operators and matrices . . . . .	10

2.1.3	The Pauli matrices . . . . .	10
2.1.4	Inner products . . . . .	11

## Part I

# Fundamental concepts

## 1 Introduction and overview

### 1.2 Quantum bits

- The special states  $|0\rangle$  and  $|1\rangle$  form an orthonormal basis and are known as **computational basis states**.
- A quantum bit (**qubit**) is a linear combination of the computational basis states

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

where  $\alpha$  and  $\beta$  are complex numbers.

- When we measure a qubit we either get  $|0\rangle$  with probability  $|\alpha|^2$  or  $|1\rangle$  with probability  $|\beta|^2$ . Thus,  $|\alpha|^2 + |\beta|^2 = 1$  and a qubit can be thought of as a unit vector in a two-dimensional complex vector space.
- If a qubit is in the state

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

there's a 50/50 chance of measuring  $|0\rangle$  or  $|1\rangle$ .

- If we let

$$\alpha = e^{i\gamma} \cos \frac{\theta}{2}$$

and

$$\beta = e^{i\gamma} e^{i\varphi} \sin \frac{\theta}{2}$$

then

$$\begin{aligned} |\alpha|^2 + |\beta|^2 &= \alpha^* \alpha + \beta^* \beta \\ &= \cos^2 \frac{\theta}{2} + \sin^2 \frac{\theta}{2} \\ &= 1 \end{aligned}$$

so the qubit is still normalised and it can be written

$$|\psi\rangle = e^{i\gamma} \left( \cos \frac{\theta}{2} |0\rangle + e^{i\varphi} \sin \frac{\theta}{2} |1\rangle \right).$$

It turns out that  $e^{i\gamma}$  has no observable effects and we can effectively write

$$|\psi\rangle = \cos \frac{\theta}{2} |0\rangle + e^{i\varphi} \sin \frac{\theta}{2} |1\rangle.$$

This defines a point on a three-dimensional sphere known as the **Bloch sphere** where  $\theta$  and  $\varphi$  take on their usual roles in a spherical coordinate system.

- Before measurement a qubit is in a linear combination of  $|0\rangle$  and  $|1\rangle$  but when measured you get one or the other and the state of the system changes to match the measured result.

### 1.2.1 Multiple Bits

- A two qubit system has four computational basis state  $|00\rangle$ ,  $|01\rangle$ ,  $|10\rangle$ , and  $|11\rangle$  so the general expression for the state of such a system is

$$|\psi\rangle = \alpha_{00} |00\rangle + \alpha_{01} |01\rangle + \alpha_{10} |10\rangle + \alpha_{11} |11\rangle.$$

- If you were to measure the first qubit, you would get  $|0\rangle$  with probability  $|\alpha_{00}|^2 + |\alpha_{01}|^2$  and the system would be left in the state

$$|\psi\rangle = \frac{\alpha_{00} |00\rangle + \alpha_{01} |01\rangle}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}},$$

i.e. it is renormalised such that the normalisation condition still holds.

## 1.3 Quantum Computation

### 1.3.1 Single Qubit Gates

- The quantum NOT changes  $|0\rangle$  to  $|1\rangle$  and  $|1\rangle$  to  $|0\rangle$ . It acts linearly on superpositions of those states, i.e. it turns  $\alpha |0\rangle + \beta |1\rangle$  into  $\beta |0\rangle + \alpha |1\rangle$ . If a quantum state  $|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$  is written in vector notation as

$$|\psi\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$$

then the quantum NOT gate can be expressed in matrix form as

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

- In order to preserve the normalisation condition, matrix representations of quantum gates must be unitary, i.e.  $M^\dagger M = I$  where  $I$  is the identity matrix.
- An arbitrary unitary 2x2 matrix can be decomposed into a finite set of other 2x2 matrices. This means an arbitrary single qubit gate can be generated by a finite set of other gates.

### 1.3.2 Multiple Qubit Gates

- The controlled-NOT or CNOT gate is a multi-qubit gate that has two input qubits known as the control qubit and the target qubit. If the control qubit is set to  $|0\rangle$  the target qubit is left alone, but if it's set to  $|1\rangle$  the target qubit is flipped. Another way of writing this is  $|A, B\rangle \rightarrow |A, A \oplus B\rangle$  where  $\oplus$  is modulo-two addition. Yet another way of writing this is in matrix form

$$U_{CN} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

where the first column describes what happens to the  $|00\rangle$  basis state, etc.

- Other classical gates like NAND or XOR can't be represented as quantum gates as they're irreversible. For example, given the output  $A \oplus B$  from an XOR gate it's not possible to determine what the inputs  $A$  and  $B$  were.
- Any multiple qubit logic gate may be composed from CNOT and single qubit gates.

### 1.3.3 Measurements in bases other than the computational basis

- Given any basis states  $|a\rangle$  and  $|b\rangle$  it is possible to express an arbitrary state as a linear combination  $\alpha|a\rangle + \beta|b\rangle$  of those states. For example, if  $|a\rangle = |+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$  and  $|b\rangle = |-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$  then

$$|\phi\rangle = \alpha|0\rangle + \beta|1\rangle = \alpha \frac{|+\rangle + |-\rangle}{\sqrt{2}} + \beta \frac{|0\rangle - |1\rangle}{\sqrt{2}} = \frac{\alpha + \beta}{\sqrt{2}} |+\rangle + \frac{\alpha - \beta}{\sqrt{2}} |-\rangle.$$

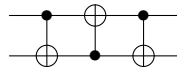
- If  $|a\rangle$  and  $|b\rangle$  are orthonormal, it's also possible to perform a measurement with respect to that basis. In the example above you would measure  $|+\rangle$  with probability  $|\alpha + \beta|^2/2$  and  $|-\rangle$  with probability  $|\alpha - \beta|^2/2$ .

### 1.3.4 Quantum circuits

- Applying a CNOT gate three times swaps the state of two qubits:

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

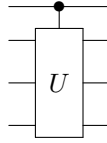
This can be represented in a quantum circuit diagram



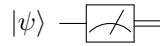
which is equivalent to



- Quantum circuits don't allow loops (they are acyclic), they don't allow multiple wires to be joined into one, and they don't allow one wire to be split into multiple wires.
- If  $U$  is a unitary matrix operating on  $n$  qubits then  $U$  can be regarded as a quantum gate. Then we can define a controlled- $U$  gate which takes a single control qubit and  $n$  target qubits. If the control qubit is set to 0 then nothing happens to the target qubits. If it's set to 1 then the  $U$  gate is applied to the target qubits.



- Measurement is represented as



where the double lines represent a classical bit.

### 1.3.5 Qubit copying circuit?

- A CNOT gate can be used to copy a classical bit. As input it takes a bit in state  $x$  and a “scratchpad” bit set to zero. The output is a bit in state  $x$  and a bit in state 0 if  $x = 0$  and 1 if  $x = 1$  — both bits are in state  $x$ .
- However, a CNOT gate cannot be used to copy quantum information. As input it takes a qubit in the state  $|\psi\rangle = a|0\rangle + b|1\rangle$  and a “scratchpad” qubit set to  $|0\rangle$ . The input state may be written as

$$[a|0\rangle + b|1\rangle]|0\rangle = a|00\rangle + b|01\rangle.$$

The gate negates the second bit if the first bit is 1 so the output is  $a|00\rangle + b|11\rangle$ . The desired output is

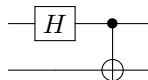
$$|\psi\rangle|\psi\rangle = a^2|00\rangle + ab|01\rangle + ab|10\rangle + b^2|11\rangle.$$

Unless  $a = 0$  or  $b = 0$ , i.e. it's a classical bit, the qubit hasn't been copied. This is known as the **no-cloning theorem**.

### 1.3.6 Example: Bell states

- The Hadamard gate acts on a single qubit, mapping  $|0\rangle$  to  $(|0\rangle + |1\rangle)/\sqrt{2}$  and  $|1\rangle$  to  $(|0\rangle - |1\rangle)/\sqrt{2}$ .

- This circuit



applies a Hadamard gate to the first qubit which then acts as the control input to the CNOT. The output states

$$\begin{aligned} |\beta_{00}\rangle &= \frac{|00\rangle + |11\rangle}{\sqrt{2}}, \\ |\beta_{01}\rangle &= \frac{|01\rangle + |10\rangle}{\sqrt{2}}, \\ |\beta_{10}\rangle &= \frac{|00\rangle - |11\rangle}{\sqrt{2}}, \text{ and} \\ |\beta_{11}\rangle &= \frac{|01\rangle - |10\rangle}{\sqrt{2}} \end{aligned}$$

are known as the **Bell states**, **EPR states**, or **EPR pairs**.

### 1.3.7 Example: quantum teleportation

- If Alice and Bob prepare a Bell pair, Alice takes the first qubit, and Bob takes the second qubit, it's possible to teleport an arbitrary qubit from Alice to Bob at a later time by communicating only classical information.
- This doesn't enable faster-than-light communication because Alice still needs to communicate classical information to Bob which is limited by the speed of light. Bob then uses this information to conditionally apply further gates to his qubit to get it into the teleported state.

## 1.4 Quantum algorithms

### 1.4.1 Classical computations on a quantum computer

- Classical circuits may contain irreversible operations, e.g. NAND gates, but quantum circuits must be reversible. In order to simulate classical circuits on a quantum computer we must find a way to make these irreversible operations reversible.
- Any classical circuit can be replaced by an equivalent classical circuit containing only reversible elements by making use of the **Toffoli gate**. This gate has three input bits and three output bits. Two bits are control bits and are unaffected by the gate. The third bit is a target bit that is flipped if both of the control bits are 1 and is otherwise left alone. Applying the Toffoli gate twice has the effect  $(a, b, c) \rightarrow (a, b, c \oplus ab) \rightarrow (a, b, c)$  and thus the gate is reversible.

- The Toffoli gate can also be used to simulate NAND gates and to do FANOUT. With this it is possible to make any classical circuit reversible.
- The equivalent quantum Toffoli gate works as expected, e.g. it changes  $|110\rangle$  to  $|111\rangle$ . This ensures quantum computers are capable of performing any classical computation.
- If the classical computer is non-deterministic, i.e. it can generate random numbers, this can be simulated on a quantum computer by preparing a qubit in the state  $|0\rangle$ , sending it through a Hadamard gate to produce  $(|0\rangle + |1\rangle)/\sqrt{2}$ , and then measuring the state. The result will be  $|0\rangle$  or  $|1\rangle$  with 50/50 probability.

#### 1.4.2 Quantum parallelism

- Quantum parallelism allows quantum computers to evaluate a function  $f(x)$  over many different values of  $x$  simultaneously. For example, if you have a gate that accepts two input qubits  $|x, y\rangle$  and produces two output qubits  $|x, y \oplus f(x)\rangle$  you can start with  $|0, 0\rangle$ , send the first bit through a Hadamard gate to produce  $(|0\rangle + |1\rangle)|0\rangle/\sqrt{2}$ , then send both bits through the  $f(x)$  gate to produce  $(|0, f(0)\rangle + |1, f(1)\rangle)/\sqrt{2}$ .
- The above process can be generalised to functions on an arbitrary number of bits by using a general operation known as the **Hadamard transform** which is  $n$  Hadamard gates operating in parallel on  $n$  qubits. This is denoted  $H^{\otimes n}$ , e.g.

$$H^{\otimes 2} = \left( \frac{|0\rangle + |1\rangle}{\sqrt{2}} \right) \left( \frac{|0\rangle + |1\rangle}{\sqrt{2}} \right) = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle).$$

- However, quantum parallelism isn't particularly useful in itself because upon measurement you only get a single value  $|x, f(x)\rangle$ .

#### 1.4.3 Deutsch's algorithm

- Deutsch's algorithm can determine  $f(0) \oplus f(1)$  — a global property of  $f(x)$  — using only one evaluation of  $f$ . A classical computer would require at least two.
- This demonstrates a property of quantum computers where in the state  $|0\rangle|f(0)\rangle + |1\rangle|f(1)\rangle$  it's possible to make the two alternatives interfere with each other resulting in some global property of the function  $f$ .

#### 1.4.4 The Deutsch-Jozsa algorithm

- The Deutsch-Jozsa algorithm can be used to determine if a function  $f$  is constant (always returns the same value) or balanced (returns 0 for half of its domain and 1 for the other half) with a single evaluation of  $f$ . The same problem on a classical computer requires  $2^n/2 + 1$  evaluations of  $f$ .

#### 1.4.5 Quantum algorithms summarized

- There are three classes of quantum algorithms which provide an advantage over known classical algorithms:
  - algorithms based on quantum versions of the Fourier transform,
  - quantum search algorithms, and
  - quantum simulation where a quantum computer is used to simulate a quantum system.
- Classically the fast Fourier transform takes roughly  $N \log(N) = n2^n$  steps to transform  $N = 2^n$  numbers. On a quantum computer this can be accomplished in about  $\log^2(N) = n^2$  steps which is an exponential saving.
- However, the Fourier transform is being performed on the amplitudes of the quantum state, not on the input vector itself. This means we need clever ways to extract this information.
- Classical search algorithms are typically  $\mathcal{O}(n)$  whereas the quantum equivalents are  $\mathcal{O}(\sqrt{n})$ .
- **Computational complexity theory** is the subject of classifying the difficulty of various computational problems. The most basic idea is a **complexity class** which can be thought of as a collection of computational problems that all share some common feature with respect to the computational resources needed to solve those problems.
- One complexity class is **P** — the class of problems that can be solved quickly on a classical computer.
- Another is **NP** — the class of problems whose solutions can be verified quickly on a classical computer.
- **P** is a subset of **NP**, but it's not known if they're equal.
- **NP**-complete problems are an important subclass of **NP** problems. They're important because: there are many problems that are known to be **NP**-complete, and any given **NP**-complete problem is known to be “at least as hard” as all other **NP** problems, i.e. an algorithm to solve a specific **NP**-complete problem can be modified to solve any other **NP** problem. If **P**  $\neq$  **NP** then it will follow that no **NP**-complete problem can be efficiently solved on a classical computer.

### 1.5 Experimental quantum information processing

#### 1.5.1 The Stern-Gerlach experiment

- The Stern-Gerlach device sends an atom through a magnetic field and measures its deflection. The atom is electrically neutral so it is not deflected by the Lorentz force. The electron is in the  $n = 1$  level so there



one possible angular momentum value. You would expect there to be a single measured value but there are two. This is due to the spin of the electron.

- If you chain Stern-Gerlach devices, the first measuring in the  $\hat{z}$  direction and the  $|+z\rangle$  output passing into another device measuring in the  $\hat{x}$  direction you see a 50/50 split in the output. If you pass the  $|+x\rangle$  output into another device measuring in the  $\hat{z}$  direction you again see a 50/50 split.

## 1.6 Quantum information

### 1.6.1 Quantum information theory: example problems

- Shannon’s noiseless channel coding theorem quantifies how many bits are required to store information being emitted by a source of information. A classical information source is described by a set of probabilities  $p_j$ ,  $j = 1, 2, \dots, d$ . Each use of the source results in the “letter”  $j$  being emitted, chosen at random with probability  $p_j$ , independently for each use of the source. If letters that occur more frequently can be represented using fewer bits, the information can be compressed. Shannon’s noiseless channel coding theorem quantifies exactly how well such a compression scheme can work.
- Shannon’s noisy channel coding theorem quantifies the amount of information that can be transmitted through a noisy channel. The idea is to encode the information using error-correcting codes so that any noise introduced by the channel can be corrected at the other end. For example, a single bit of information may be encoded across two bits, in which case the channel has a capacity of half a bit.

## 2 Introduction to quantum mechanics

### 2.1 Linear algebra

#### 2.1.1 Bases and linear independence

- A **spanning set** for a vector space is a set of vectors  $|v_1\rangle, \dots, |v_n\rangle$  such that any vector  $|v\rangle$  in the vector space can be written as a linear combination  $|v\rangle = \sum_i a_i |v\rangle_i$  of vectors in that set. We say that the vectors  $|v_1\rangle, \dots, |v_n\rangle$  **span** the vector space.
- A set of non-zero vectors  $|v_1\rangle, \dots, |v_n\rangle$  are **linearly dependent** if there exists a set of complex numbers  $a_1, \dots, a_n$  with  $a_i \neq 0$  for at least one value of  $i$  such that

$$a_1 |v_1\rangle + \dots + a_n |v_n\rangle = 0.$$

A set of vectors is **linearly independent** if it’s not linearly dependent.

- Any two sets of linearly independent vectors which span a vector space  $V$  contain the same number of elements. We call such a set a **basis** for  $V$ .

### 2.1.2 Linear operators and matrices

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

$$A \left( \sum_i a_i |v_i\rangle \right) = \sum_i a_i A(|v_i\rangle).$$

- We usually write  $A|v\rangle$  to denote  $A(|v\rangle)$ .
- Linear operators can be expressed as matrices. Suppose  $A : V \rightarrow W$  is a linear operator between the vector spaces  $V$  and  $W$ ,  $|v_1\rangle, \dots, |v_m\rangle$  is a basis for  $V$ , and  $|w_1\rangle, \dots, |w_n\rangle$  is a basis for  $W$ . Then for each  $j$  in the range  $1, \dots, m$  there exist complex numbers  $A_{1j}$  through  $A_{nj}$  such that

$$A|v_j\rangle = \sum_i A_{ij} |w_i\rangle,$$

i.e. the result of applying  $A$  to each basis vector  $|v_j\rangle$  can be expressed as a linear combination of the basis vectors  $|w_i\rangle$  and the coefficients  $A_{ij}$  form the matrix representation of  $A$ .

### 2.1.3 The Pauli matrices

- The Pauli matrices are defined as

$$\begin{aligned} \sigma_0 &= I \\ &= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \\ \sigma_1 &= \sigma_x \\ &= X \\ &= \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \\ \sigma_2 &= \sigma_y \\ &= Y \\ &= \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \\ \sigma_3 &= \sigma_z \\ &= Z \\ &= \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \end{aligned}$$

#### 2.1.4 Inner products

- An **inner product** is a function which takes as input two vectors  $|v\rangle$  and  $|w\rangle$  from a vector space and produces a complex number as output. It can be denoted  $(|v\rangle, |w\rangle)$ , but this isn't the standard quantum mechanical notation. The standard notation is  $\langle v|w\rangle$  where  $\langle v|$  is the dual vector to the vector  $|v\rangle$ . The dual vector is a linear operator from the inner product space  $V$  to the complex numbers  $\mathbb{C}$ , defined by

$$\langle v|(|w\rangle) = \langle v|w\rangle = (|v\rangle, |w\rangle).$$

- A function  $(\cdot, \cdot)$  from  $V \times V$  to  $\mathbb{C}$  is an inner product if
  - it is linear in the second argument

$$\left(|v\rangle, \sum_i \lambda_i |w_i\rangle\right) = \sum_i \lambda_i (|v\rangle, |w_i\rangle),$$

- $(|v\rangle, |w\rangle) = (|w\rangle, |v\rangle)^*$ , and
  - $(|v\rangle, |v\rangle) \geq 0$  with equality if and only if  $|v\rangle = 0$ .
- A vector space equipped with an inner product is called an **inner product space**.
- In finite dimensional complex vector spaces, a Hilbert space is the same as an inner product space.
- Vectors  $|w\rangle$  and  $|v\rangle$  are **orthogonal** if their inner product is zero.
- The **norm** of a vector is defined as

$$\| |v\rangle \| = \sqrt{\langle v, v \rangle}.$$

- A **unit vector** is a vector  $|v\rangle$  such that  $\| |v\rangle \| = 1$ . We also say such a vector is **normalised**.
- A vector can be normalised by dividing by its norm.
- A set  $|i\rangle$  of vectors with index  $i$  is **orthonormal** if each vector is a unit vector and distinct vectors in the set are orthogonal, i.e.  $\langle i|j\rangle = \delta_{ij}$ .
- If  $|v\rangle$  is a vector in an inner product space  $V$  and  $|w\rangle$  is a vector in an inner product space  $W$ , then  $|w\rangle \langle v|$  is the linear operator from  $V$  to  $W$  whose action is defined by

$$(|w\rangle \langle v|)(|v'\rangle) = |w\rangle \langle v|v'\rangle = \langle v|v'\rangle |w\rangle.$$

- Let  $|i\rangle$  be any orthonormal basis for the vector space  $V$ , so an arbitrary vector  $|v\rangle$  can be written  $|v\rangle = \sum_i v_i |i\rangle$  for some set of complex numbers  $v_i$ . Therefore

$$\left( \sum_i |i\rangle \langle i| \right) |v\rangle = \sum_i |i\rangle \langle i|v\rangle = \sum_i v_i |i\rangle = |v\rangle$$

and thus

$$\sum_i |i\rangle \langle i| = I.$$

This is known as the **completeness relation**.

- Suppose  $A : V \rightarrow W$  is a linear operator,  $|v_i\rangle$  is an orthonormal basis for  $V$ , and  $|w_j\rangle$  is an orthonormal basis for  $W$ . We can use the completeness relation twice to obtain

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

This is known as the **outer product representation** of  $A$ . From this we can see the matrix representation of  $A$  has  $\langle w_k| A |v_i\rangle$  in the  $i$ th column and  $j$ th row.