

---

# QUANTUM COMPUTING

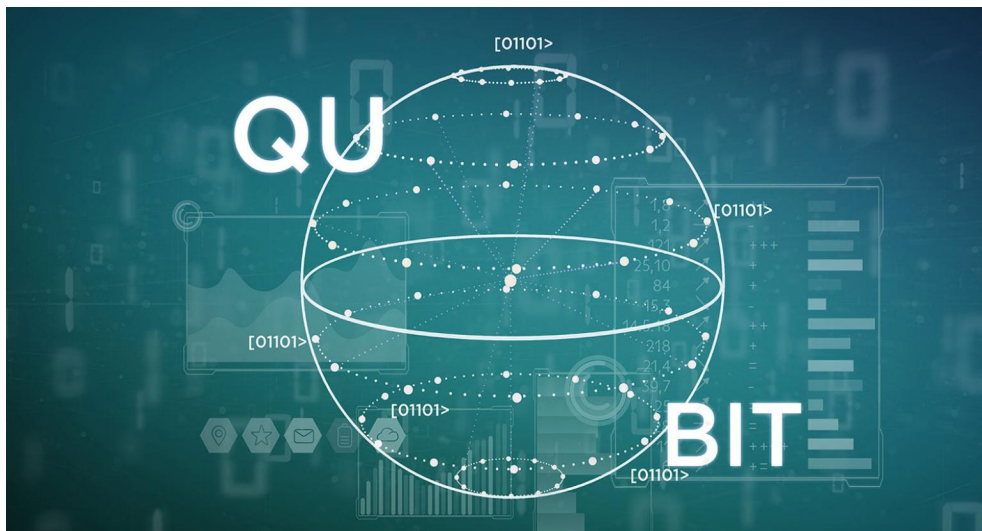
---

SUMMER OF SCIENCE 2021

EESHAAN JAIN

MENTOR: PRAVEEN SRIRAM

*INDIAN INSTITUTE OF TECHNOLOGY BOMBAY*



IF YOU CAN FATHOM QUANTUM MECHANICS WITHOUT GETTING DIZZY, YOU DON'T  
GET IT. ET KVANTEBITTE SPRING NÆRMERE SUPERCOMPUTEREN

- NIELS BOHR

# Contents









<b>0</b>	<b>Plan of Action</b>	<b>2</b>
<b>1</b>	<b>Brief Glance at Quantum Computing</b>	<b>3</b>
1.1	Quantum Bits . . . . .	3
1.1.1	Single Qubits . . . . .	3
1.1.2	Multiple Qubits . . . . .	4
1.2	Quantum Computation . . . . .	4
1.2.1	Single Qubit Gates . . . . .	4
1.2.2	Multiple Qubit Gates . . . . .	5
1.2.3	Quantum circuits . . . . .	5
1.3	Quantum Algorithms . . . . .	6
1.3.1	Doing classical computations . . . . .	6
1.3.2	Quantum Parallelism . . . . .	7
1.3.3	Deutsch's Algorithm . . . . .	7
1.3.4	Deustsch-Jozsa Algorithm . . . . .	7
1.3.5	Fourier transform . . . . .	8
<b>2</b>	<b>Review of Quantum Mechanics</b>	<b>9</b>

## Chapter 0

---

# Plan of Action

---

- 
- |   |                             |
|---|-----------------------------|
|  <b>Week 0</b> | Review of Quantum Mechanics |
|---|-----------------------------|
- 
- |   |                  |
|---|------------------|
|  <b>Week 1</b> | Quantum Circuits |
|---|------------------|
- 
- |   |   |
|---|---|
|  <b>Week 2</b> | Quantum Fourier transform and Search algorithms |
|---|---|
- 
- |   |   |
|---|---|
|  <b>Week 3</b> | Physical realization of Quantum Computers |
|---|---|
- 
- |   |     |
|---|-----|
|  <b>Week 4</b> | NMR |
|---|-----|
- 
- |   |                        |
|---|------------------------|
|  <b>Week 5</b> | Superconducting Qubits |
|---|------------------------|
- 
- |   |             |
|---|-------------|
|  <b>Week 6</b> | Spin Qubits |
|---|-------------|
- 
- |   |   |
|---|---|
|  <b>Week 7</b> | Buffer (to modify PoA as time progresses) |
|---|---|
- 
- 

- ▷ The above schedule is tentative, and bound to change depending on the complexity and nature of the topic going on.
- ▷ The book "Quantum Computation and Quantum Information" by Michael A. Nielsen and Isaac L. Chuang is going to be religiously followed for this SoS. Any other material referenced will be mentioned at the end of the document.
- ▷ The weekly updated notes will be uploaded at
  - ◇ [the github repository](#)
  - ◇ [my website](#)

# Brief Glance at Quantum Computing

## §1.1 Quantum Bits

### §1.1.1 Single Qubits

#### Definition 1.1.1: Qubit

A qubit is the mathematical analogue of the classical bit upon which quantum computing and information is based. Unlike a classical bit, the quantum bit can be in  $|0\rangle$  state,  $|1\rangle$  state, and a state defined by the linear combination i.e

$$|\psi\rangle = \alpha |0\rangle + \beta |1\rangle \quad \text{where} \quad |\alpha|^2 + |\beta|^2 = 1 \quad (1.1)$$

Some ways a qubit can be realised are:

- ◇ two different polarizations of a photon
- ◇ alignment of a nuclear spin in a uniform magnetic field
- ◇ two states of an electron orbiting a single atom

Since  $|\alpha|^2 + |\beta|^2 = 1$ , we can write (1.1) as

$$|\psi\rangle = e^{i\gamma} \left( \cos \frac{\theta}{2} |0\rangle + e^{i\varphi} \sin \frac{\theta}{2} |1\rangle \right) \quad \text{where} \quad \theta, \varphi, \gamma \in \mathbb{R} \quad (1.2)$$

The factor  $e^{i\gamma}$  doesn't have any observable effect and can be ignored.  $\theta$  and  $\varphi$  define a point on the unit three-dimensional sphere called the *Bloch sphere* which can be used for visualizing the state of a single qubit (though no simple generalization exists for multiple qubits).

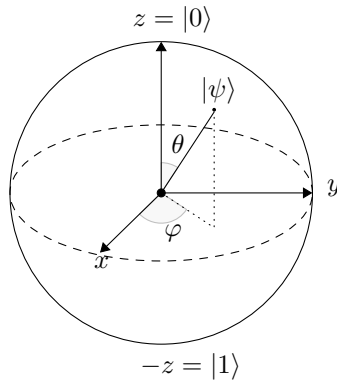


Figure 1.1: Bloch sphere for a single qubit

### §1.1.2 Multiple Qubits

A two qubit system has four computational basis states  $|00\rangle |01\rangle |10\rangle |11\rangle$ , and the pair can exist in a *superposition* of these too with a complex amplitude as

$$|\psi\rangle = \sum_{i,j \in \{0,1\}} \alpha_{ij} |ij\rangle \quad \text{where} \quad \sum_{x \in \{0,1\}^2} |\alpha_x|^2 = 1 \quad (1.3)$$

It is possible to measure a subset of qubits, say we measure the first qubit alone giving 0 with probability  $|\alpha_{00}|^2 + |\alpha_{01}|^2$  leaving the post measurement state as  $|\psi'\rangle = \frac{\alpha_{00}|00\rangle + \alpha_{01}|01\rangle}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}}$ .

The *Bell states* also called the *EPR pairs* are  $|\beta_{xy}\rangle = \frac{|0,y\rangle + (-1)^x |1,\bar{y}\rangle}{\sqrt{2}}$ , i.e

$$|\beta_{00}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}, \quad |\beta_{01}\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}, \quad |\beta_{10}\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}}, \quad |\beta_{11}\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}} \quad (1.4)$$

Upon measuring the first qubit, we can get two results:

- ◇ 0 with probability  $\frac{1}{2}$  leaving  $|\psi'\rangle = |00\rangle$
- ◇ 1 with probability  $\frac{1}{2}$  leaving  $|\psi'\rangle = |11\rangle$

The second qubit always follows the first in terms of measurement, i.e there is correlation between the measurements.

## §1.2 Quantum Computation

### §1.2.1 Single Qubit Gates

Let's first define the constraint there exists for a matrix to be called a single qubit gate. Consider the initial state to be  $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$  and the state after the gate has acted to be  $|\psi'\rangle = \alpha'|0\rangle + \beta'|1\rangle$ . Both of these must satisfy the normalization condition and the matrix  $U$  defining the gate must be unitary i.e

$$U^\dagger U = I$$

This defines the *only* constraint imposed on quantum gates, and we can clearly see that there exists infinitely many gates. Single qubit gates correspond to rotations and reflections of the Bloch Sphere.

Some important gates are:

- ◇ **NOT Gate:** The NOT gate takes the state  $\alpha|0\rangle + \beta|1\rangle$  to  $\alpha|1\rangle + \beta|0\rangle$  and realised as

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad (1.5)$$

- ◇ **Z Gate:** Leaves  $|0\rangle$  unchanged and flips the sign  $|1\rangle$  and realised as

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \quad (1.6)$$

- ◇ **H Gate:** The *Hadamard* gate turns  $|0\rangle$  to  $\frac{|0\rangle + |1\rangle}{\sqrt{2}}$  (first column of  $H$ ) and  $|1\rangle$  to  $\frac{|0\rangle - |1\rangle}{\sqrt{2}}$  (second column of  $H$ ). Note that  $H^2 = I$  and thus applying it twice leaves the state unchanged. The  $H$  operation is a rotation about the  $\hat{y}$  axis by  $90^\circ$  followed by about  $\hat{x}$  axis by  $180^\circ$

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \quad (1.7)$$

It can be proven that any arbitrary  $2 \times 2$  unitary matrix can be decomposed as

$$U = \underbrace{e^{i\alpha}}_{\text{phase shift}} \underbrace{\begin{bmatrix} e^{-i\beta/2} & 0 \\ 0 & e^{i\beta/2} \end{bmatrix}}_{\text{rotation about } \hat{z} \text{ axis}} \underbrace{\begin{bmatrix} \cos \frac{\gamma}{2} & -\sin \frac{\gamma}{2} \\ \sin \frac{\gamma}{2} & \cos \frac{\gamma}{2} \end{bmatrix}}_{\text{product of rotations}}, \quad \begin{bmatrix} e^{-i\delta/2} & 0 \\ 0 & e^{i\delta/2} \end{bmatrix} \quad (1.8)$$

We can build arbitrarily good approximation of gates using special fixed values of  $\alpha, \beta$  and  $\gamma$ . And thus, it is possible to build up an arbitrary single quantum gate using a *finite* set of quantum gates.

**Proposition 1.2.1**

Any arbitrary quantum computation on any number of qubits can be generated by a finite set of gates that is said to be *universal* for quantum computation.

**§1.2.2 Multiple Qubit Gates**

A prototypical multi-qubit quantum logic gate is the CNOT (controlled-NOT) gate. The gate takes a control qubit (top) and a target qubit (bottom) and if the control qubit is 0, the target is left alone else it is flipped. The operation is simply  $|A, B\rangle \rightarrow |A, B \oplus A\rangle$

$$\begin{array}{ccc}
 |A\rangle & \text{---} \bullet & |A\rangle \\
 |B\rangle & \text{---} \oplus & |B \oplus A\rangle
 \end{array}
 \qquad
 U_{CN} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \quad (1.9)$$

The CNOT gate is a type of generalization of the classical XOR gate. But we cannot realize the regular XOR or NAND gate because these operations are *irreversible*, i.e given  $A \oplus B$ , we cannot get back  $A$  and  $B$ , and an irretrievable loss of information is associated with them. A unitary matrix is always invertible and hence a quantum gate can always be inverted by another quantum gate.

**Theorem 1.2.1: Universality**

Any multiple qubit gate may be composed from CNOT and single qubit gates.

This is the quantum parallel of the universality of the NAND gate.

- ◇ Given any two basis states  $|a\rangle$  and  $|b\rangle$  for a qubit, it is possible to express an arbitrary state as a linear combination i.e  $\alpha|a\rangle + \beta|b\rangle$  and provided these are orthonormal, we can perform a measurement w.r.t these bases.

**§1.2.3 Quantum circuits**

A wire in a quantum circuit may not correspond to anything physical. It may be passage of time, or movement of a particle (photon) through space. Conventionally, the state input to the circuit is the computational basis state, i.e all  $|0\rangle$ s.

**The swap operation**

The swap operation swaps the state of the two qubits and can be realised as

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

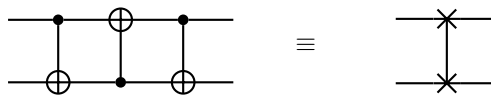


Figure 1.2: Circuit to swap two qubits

### Distinction between classical and quantum circuits

There are a few things allowed in classical circuits, which aren't in quantum circuits.

- ◇ Loops aren't allowed, hence circuit is acyclic.
- ◇ FanIn and FanOut aren't allowed as these are irreversible, and copying a qubit is forbidden.

Just like the CNOT gate, we can make a Controlled-U Gate.

### Quantum circuit for teleportation

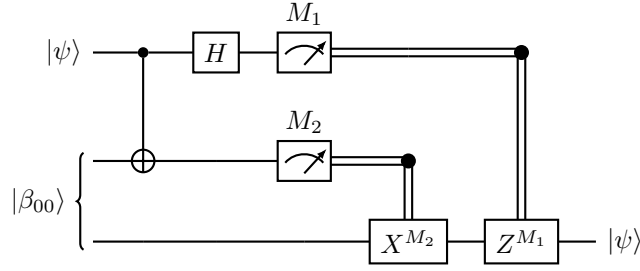


Figure 1.3: Quantum circuit for teleporting a qubit

Consider the state to be teleported as  $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$  and state input to the circuit is  $|\psi_0\rangle = |\psi\rangle|\beta_{00}\rangle$  which is  $\frac{1}{\sqrt{2}}[\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|00\rangle + |11\rangle)]$ . After passing through the CNOT gate, we get

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}[\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|01\rangle + |10\rangle)]$$

And after passing through the  $H$  gate, we get

$$\begin{aligned} |\psi_2\rangle &= \frac{1}{2}[\alpha(|0\rangle + |1\rangle)(|00\rangle + |11\rangle) + \beta(|0\rangle - |1\rangle)(|01\rangle + |10\rangle)] \\ &= \frac{1}{2} [|00\rangle(\alpha|0\rangle + \beta|1\rangle) + |01\rangle(\alpha|1\rangle + \beta|0\rangle) + |10\rangle(\alpha|0\rangle - \beta|1\rangle) + |11\rangle(\alpha|1\rangle - \beta|0\rangle)] \end{aligned}$$

Now after measurement, the receiver should know what the sender has measured to know what gates to apply to get the desired outcome (note that this places the restriction on speed of quantum teleportation). The gates to be applied can be written as  $Z^{M_1}X^{M_2}$  where  $M_1, M_2 \in \{0, 1\}$

## §1.3 Quantum Algorithms

### §1.3.1 Doing classical computations

Any classical circuit can be replaced by an equivalent quantum circuit having only reversible elements using the *Toffoli gate*.

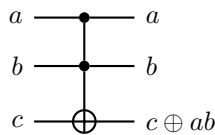


Figure 1.4: Toffoli gate circuit  
If  $a, b \neq 1$  then  $c$  unchanged else flipped

Toffoli gate can be used to simulate irreversible classical gates, for example  $c = 1$  gives us the NAND gate. Putting  $a = 1$  and  $c = 0$  gives us a FanOut.

### §1.3.2 Quantum Parallelism

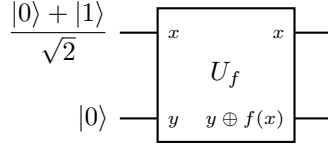


Figure 1.5: Circuit demonstrating the formulation below

We prepare the data register ( $x$ ) as  $\frac{|0\rangle + |1\rangle}{\sqrt{2}}$  (apply  $H$  on  $|0\rangle$ ) and apply a unitary gate  $U_f$  which maps  $|x, y\rangle \rightarrow |x, y \oplus f(x)\rangle$ . This gives us  $\frac{|0, f(0)\rangle + |1, f(1)\rangle}{\sqrt{2}}$  and we have information about both  $f(0)$  and  $f(1)$ !. Unlike classical circuits, a single  $f(x)$  circuit evaluated the values simultaneously. Generalization of the above is called the *Wash-Hadamard transform*. We apply  $n$   $H$  gates in parallel to  $n$  qubits (denoted as  $H^{\otimes n}$ ), and the result we get is

$$\frac{1}{\sqrt{2^n}} \sum_x |x\rangle \quad \text{given that all qubits were initially prepared as } |0\rangle \quad (1.10)$$

### §1.3.3 Deutsch's Algorithm

Modifying the above circuit,

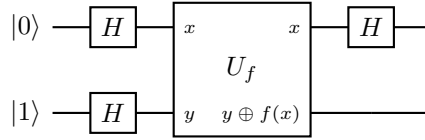


Figure 1.6: Circuit demonstrating the formulation below

The input  $|\psi_0\rangle = |01\rangle$  and passing through  $H$  gives  $|\psi_1\rangle = \left[ \frac{|0\rangle + |1\rangle}{\sqrt{2}} \right] \left[ \frac{|0\rangle - |1\rangle}{\sqrt{2}} \right]$  and noticing that  $U_f$  applied to  $|x\rangle \frac{|0\rangle + |1\rangle}{\sqrt{2}}$  gives  $(-1)^{f(x)} |x\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}}$ , we can write after applying  $U_f$  and taking  $H$  on the first qubit,

$$|\psi_3\rangle = \begin{cases} \pm |0\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}} & \text{if } f(0) = f(1) \\ \pm |1\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}} & \text{if } f(0) \neq f(1) \end{cases}$$

It can be simplified to

$$|\psi_3\rangle = \pm |f(0) \oplus f(1)\rangle \left[ \frac{|0\rangle - |1\rangle}{\sqrt{2}} \right] \quad (1.11)$$

### §1.3.4 Deutsch-Jozsa Algorithm

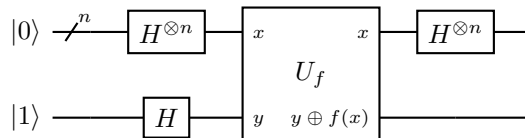


Figure 1.7: Circuit implementing the Deutsch-Jozsa algorithm

The *Deutsch's problem* is defined as the task to find in the least correspondence if a function  $f(x)$  is constant or balanced (equal number of 0 and 1 in output). If the function takes  $n$  inputs, classically, we need to query at least  $2^n/2 + 1$  times in the worst case. Instead, if we had qubits, we could proceed as



follows: The input state is  $|\psi_0\rangle = |0\rangle^{\otimes n} |1\rangle$  and after passing through the  $n+1$  parallel  $H$  gates, we get  $|\psi_1\rangle = \sum_{x \in \{0,1\}^n} \frac{|x\rangle}{\sqrt{2^n}} \left[ \frac{|0\rangle - |1\rangle}{\sqrt{2}} \right]$ . Now we apply  $U_f$  to get  $|\psi_2\rangle = \sum_x \frac{(-1)^{f(x)} |x\rangle}{\sqrt{2^n}} \left[ \frac{|0\rangle - |1\rangle}{\sqrt{2}} \right]$

Noticing that for a single qubit  $H|x\rangle = \sum_z (-1)^{xz} |z\rangle / \sqrt{2}$  and expanding for  $n$ ,

$$H^{\otimes n} |x_1, \dots, x_n\rangle = \frac{\sum_{z_1, \dots, z_n} (-1)^{x_1 z_1 + \dots + x_n z_n} |z_1, \dots, z_n\rangle}{\sqrt{2^n}} = \frac{\sum_z (-1)^{x \cdot z} |z\rangle}{\sqrt{2^n}}$$

Thus,

$$|\psi_3\rangle = \sum_z \sum_x \frac{(-1)^{x \cdot z + f(x)} |z\rangle}{2^n} \left[ \frac{|0\rangle - |1\rangle}{\sqrt{2}} \right] \quad (1.12)$$

From this, we measure the query register qubits, and notice that if they are all 0s, we have a constant function else a balanced function.

### §1.3.5 Fourier transform

We define a linear transformation  $U$  on  $n$  qubits as

$$|j\rangle \rightarrow \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{i j 2\pi k / 2^n} |k\rangle \quad (1.13)$$

Such a transform is unitary, and thus can be realised by a quantum circuit. Moreover, on a superposition :

$$\sum_{j=0}^{2^n-1} x_j |j\rangle \rightarrow \sum_{k=0}^{2^n-1} \left[ \sum_{j=0}^{2^n-1} e^{i j 2\pi k / 2^n} x_j \right] |k\rangle = \sum_{k=0}^{2^n-1} y_k |k\rangle \quad (1.14)$$

---

# Review of Quantum Mechanics

---