The PDF contains highlights (hand-written notes) of the first chapter from the book Quantum Computation and Quantum Information by Michael A. Nielsen and Isaac L. Chuang. Note that PDF contains the important topics from the chapter and can be used for revision purpose. However, it is recommended to read the book first.

I Fundamental Concepts

Chp 1. Introduction and Overview

→ 1.1 Global Perspectives

① Quantum Computation & Quantum Information is the study of the information processing tasks that can be accomplished using quantum mechanical systems.

② Quantum Computation & Quantum Information
- → i) Quantum Mechanics
- → ii) Computer Science
- → iii) Information Theory
- → iv) Cryptography

③ Quantum Mechanics is a mathematical framework or set of rules for the construction of physical theories.

④ The No. Cloning Theorem

⑤ Controlling Single Quantum Systems

⑥ Universal Turing Machine

⑦ Deutsch's Universal Quantum Computer

⑧ How to design a Quantum Algorithm?
Step 1: Switch off your classical intuition
Step 2: It must be better than any existing Classical Algorithm

(9) Shannon's noiseless channel coding theorem

(10) Shannon's Noisy channel coding theorem

(11) Error - correcting code

(12) Cryptography is the problem of doing communication/computation involving two or more parties who may not trust each other.
eg: Sending secret messages.

(13) Quantum Key Distribution

B

→ 1.1.2 Future Directions

(14) Think computationally about physics.

⟹ 1.2 Quantum Bits

(15) Bit is the fundamental concept of Classical Computation.

(16) We can treat Qubits as mathematical objects.

(17) $|\rangle$ → Dirac Notation

(18) linear Combination of states is called Superposition.

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

(19) α, β = Complex Numbers & $|\alpha|^2 + |\beta|^2 = 1$

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

(21) A Qubit can also be written as:

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

However, the term $e^{i\gamma}$ has no observable effect

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

→ 1.2.1 Multiple Qubits

(22) State Vector discribing two qubits:

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

Also,

$$\sum_{x \in \{0,1\}^2} |a_x|^2 = 1$$

(23) Bell State - $\frac{|00\rangle + |11\rangle}{\sqrt{2}}$

(24) For a n-qubit system, the quantum state will be specified by 2^n amplitudes.

⟹ 1.3 Quantum Computation

→ 1.3.1 Single Qubit Gates

(25) Quantum NOT Gate acts linearly

$$\alpha|0\rangle + \beta|1\rangle \longrightarrow \alpha|1\rangle + \beta|0\rangle$$

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

(26) For a matrix to represent Quantum State, it must be unitary
For eg: $X^T X = I$

(27) Any unitary gate specifies a valid Quantum Gate

(28) The Z - Gate : It leaves $|0\rangle$ unchanged & flips the sign of $|1\rangle$ i.e from $|1\rangle \rightarrow -|1\rangle$

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

(29) Hadamard Gate : It turns a $|0\rangle$ into $\frac{|0\rangle + |1\rangle}{\sqrt{2}}$

& turns $|1\rangle$ into $(|0\rangle - |1\rangle)/\sqrt{2}$.

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}.$$

Also, $H^2 = I$

The Hadamard operation is rotation of sphere about y axis by 90° & then followed by the rotation of 180° about X axis.

→ 1.3.2 Multiple Qubit Gates

(30) Controlled NOT (CNOT) : It flips the target qubit if the controlled qubit is in the state $|1\rangle$

$$CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

I/P	O/P
$\|00\rangle$	$\|00\rangle$
$\|01\rangle$	$\|01\rangle$
$\|10\rangle$	$\|11\rangle$
$\|11\rangle$	$\|10\rangle$

good

$$U_{CN}^{\dagger} U_{CN} = I$$

(31) 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

(32) An arbitrary state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ can be re-expressed in terms of the states $|+\rangle$ & $|-\rangle$:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \alpha\left(\frac{|+\rangle + |-\rangle}{\sqrt{2}}\right) + \beta\left(\frac{|+\rangle - |-\rangle}{\sqrt{2}}\right)$$

$$= \left(\frac{\alpha \pm \beta}{\sqrt{2}}\right)|+\rangle + \left(\frac{\alpha - \beta}{\sqrt{2}}\right)|-\rangle$$

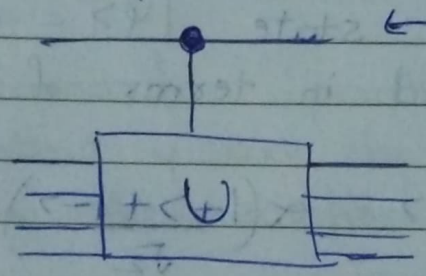
(33) To perform a measurement in the basis, it's important for the basis vectors to be orthogonal.

→ 1.3.4 Quantum Circuits

(34) The lines in the Quantum Circuits can be considered as passage of time or a physical particle such as photon and must be read from left to right.

(35) Features not allowed in Quantum Circuits:-
a) Loops are not allowed :- i.e feedback from one part of the Quantum Circuit to another
b) FANIN (Joining of Wires)
c) FANOUT (producing several copies of a bit)

(36) For any arbitrary unitary matrix U that acts on 'n' qubits, we can define a controlled-U gate which is just an extension of the CNOT Gate. If the Control qubit is in |0> state, nothing happens. However, if the control qubit is in |1> state, the U-gate is applied to the n qubits.



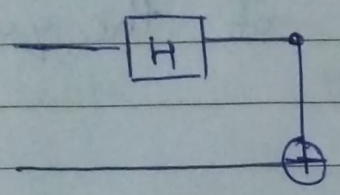
(37) The Measurement operation converts a Quantum Bit into a probabilistic bit m. It is drawn using two lines to distinguish it from a Qubit

→ 1.3.5 Qubit Copying Circuit?

(38) The property of qubits that they cannot be copied is known as the no-cloning theorem & is one of the chief differences between Quantum & Classical Information.

→ 1.3.6 Bell States

(39)



Circuit for Bell States

(40) First, the Hadamard transform the first qubit by putting it into superposition i.e

$$|00\rangle \rightarrow \frac{(|0\rangle+|1\rangle)}{\sqrt{2}}|0\rangle$$

After that CNOT is used that ~~convert~~ NOTs the second qubit if the first is $|1\rangle$

∴ We get $|00\rangle \rightarrow \frac{|00\rangle + |11\rangle}{\sqrt{2}}$

(41) Other Bell States:-

ii) $|01\rangle \Rightarrow \frac{|01\rangle + |10\rangle}{\sqrt{2}}$, iii) $|10\rangle \Rightarrow \frac{|00\rangle - |11\rangle}{\sqrt{2}}$

iv) $|11\rangle \Rightarrow \frac{|01\rangle - |10\rangle}{\sqrt{2}}$

(42) Representation of Bell States can be given as:

$$\beta_{xy} \equiv \frac{|0,y\rangle + (-1)^x |1,\bar{y}\rangle}{\sqrt{2}}$$

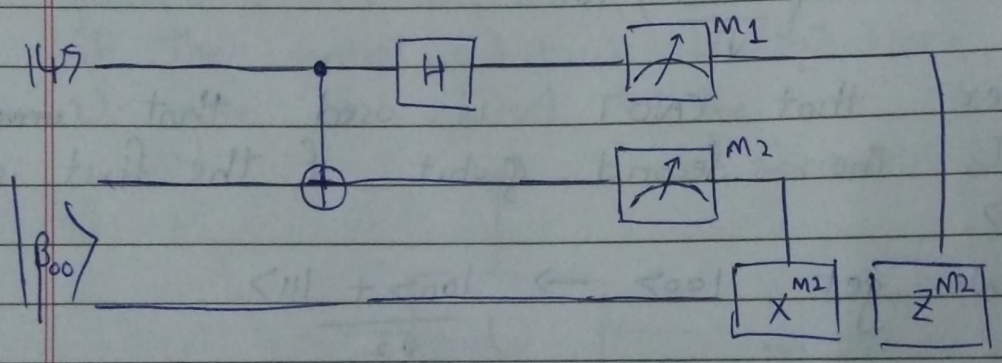
→ 1.3.7 Quantum Teleportation

(43) Quantum Teleportation is a technique for moving quantum states around, even in the absence of a quantum & communications channel linking the sender of the quantum state to the recipient.

(44) Circuit

$|\psi\rangle$ → Alice's First Qubit

$|\beta_{00}\rangle$ → The EPR state of Alice's Second Qubit & Bob's First Qubit

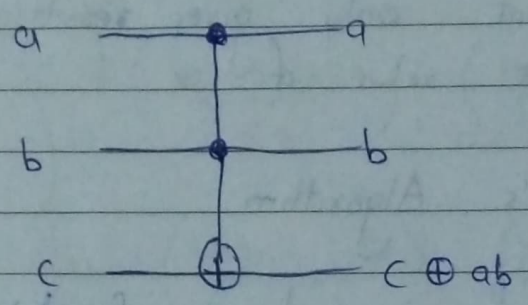


1.4 Quantum Algorithms

1.4.1 Classical Computation on Quantum Computer

(45) Toffoli Gate: It is a reversible Gate & it is the quantum analogue of AND Gate. It ~~is~~ operates on three qubits, namely two control qubits and one target qubit. If the two control qubits are in $|1\rangle$ state, a NOT is applied to the target qubit. The Toffoli Gate is the inverse of itself.

(46)



(47) Using Toffoli Gate, we can make operations like FANOUT & gates like NAND possible on Quantum Computer.

1.4.2 Quantum parallelism

(48) Quantum parallelism implies that a Quantum Computer can evaluate a function $f(x)$ for various values of x simultaneously.

(49) Walsh - Hadamard Transform:- When 'n' Hadamard gates are applied on 'n' qubits. It can be written as $H^{\otimes n}$.

If all qubits are in the initial state $|0\rangle$, we can also write

$$H^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_x |x\rangle$$

(50) 1) Initialize 'n+1' qubits
2) Apply Walsh Hadamard on 'n' qubits
3) Then apply U_f, producing the state

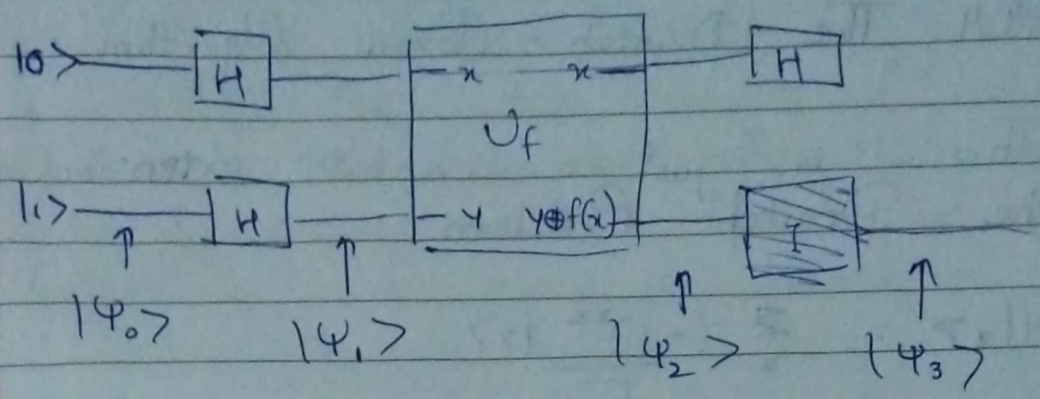
$$\frac{1}{\sqrt{2^n}} \sum_x |x\rangle |f(x)\rangle$$

Note:- Measurement only gives resulting of $f(x)$ for only one value of x.

→ 1.4.3 Deustch's Algorithm

(51) Deustch Problem is about finding if a given $f(x)$ is constant (independent of input) or balanced (dependent on input)?

Input	O/P1	O/P2	O/P3	O/P4
0	0	1	0	1
1	1	0	0	1
	Balanced		Constant	
	$f(0) \neq f(1)$		$f(0) = f(1)$	



$$|\psi_0\rangle = |01\rangle$$

$$|\psi_1\rangle = \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$

$$|\psi_2\rangle = \begin{cases} \pm\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right), & \text{if } f(0) = f(1) \text{ (f is constant)} \\ \pm\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right), & \text{if } f(0) \neq f(1) \text{ (f is balanced)} \end{cases}$$

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

Now measuring the first qubit only can help us determine if f is constant or balanced.

Date
Page

→ 1.4.4 The Deustch - Jozsa Algorithm

(52) This is just a n-bit extension of the Deustch Problem.

(53) $$H|x\rangle = \sum_{z} \frac{(-1)^{xz}}{\sqrt{2}} |z\rangle$$

→ 1.4.5 Quantum Algorithms Summarized

(54) Classes of Quantum Algorithms:-
a) Quantum Version of the Fourier Transform
b) Quantum Search Algorithms
c) Quantum Simulation Algorithm

(55) The Discrete Fourier Transform is described as transforming a set $x_0, x_1, \cdots x_{N-1}$ of N complex number into complex Numbers $y_0, y_1 \cdots y_{N-1}$ defined by

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

Quantum Mechanical form of the above eqn

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

(56) Quantum Computer calculates ~~exponenti~~ Fourier Transform exponentially faster than Classical Computer

(57) We can define BQP, a quantum complexity class, that consists of all computational problems that can be efficiently solved on a Quantum Computer; where a bounded probability of error is allowed.

⟹ 1.5 Experimental Quantum Information Processing

→ 1.5.1 The Stern-Gerlach experiment

(58) The experiment is one of the possible early evidences that "qubit" models actually do exist in Nature.

→ 1.5.2 Prospects for Practical Quantum Information Processing

(59) Noise in the Quantum systems is a serious problem that needs to be addressed.

(60) Quantum State tomography is a method for determining the quantum state of a system.

⟹ 1.6 Quantum Information

(61) Memory in Quantum Information Theory: The ability to store a quantum state over some period of time.

→ 1.6.1 : Quantum information theory

(62) Classical information source is described by a set of probabilities p_j ; $j = 1, 2, 3, 4, \ldots d$.

(63) Shannon's ~~noi~~ noiseless coding theorem quantifies exactly how well a compression scheme can be made. An element that occurs frequently ~~oftentimes~~ can be represented using fewer bits & other element that occurs very less compared to other, can be represented using more bits.

(64) Each use of classical information source

$$= H(p_j) = -\sum_j p_j \log(p_j)$$

$$= \text{Shannon Entropy}$$

(65) Shannon's noisy channel coding theorem describes the amount of information that can be reliably sent through a noisy channel. This is achieved using error correcting codes.

(66) A Quantum Source is described by a set of probabilities p_j, corresponding to quantum states $|\varphi_j\rangle$

(67) If the states are non-orthogonal, the von Neumann Entropy is strictly smaller than Shannon Entropy