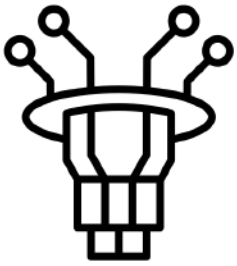
Simplifying Quantum Computing Fundamentals

Yugeeth Amarasinghe — Self-published



Handwritten technical notebook

Date : 28/07/25

Pages: 61

Abstract

This 60-page handwritten journal introduces core quantum-computing concepts (qubits, gates, circuits, measurement, and simple algorithms) using handwritten notes, worked examples, and implementation sketches. Created through self-directed online study and video lectures, it is intended as an accessible primer for motivated self-learners.

Non-technical summary

This handwritten notebook demystifies the basics of quantum computing for curious learners. Rather than formal proofs, it uses step-by-step examples, intuitive diagrams, and short implementation sketches to explain qubits, gates, circuits, and measurement. I compiled it while teaching myself the subject through online courses and videos; the goal is to give motivated high-school and early-undergraduate students a friendly, practical entry point to try small circuits and continue learning.

Quantum Computing

Superposition

- ability of a quantum system, like a qubit, to exist in multiple states at once. Both 1 and 0 simultaneously: can perform parallel computations.

Entanglements

* two or more qubits become linked, such that the state of one qubit instantly determines the state of the other, no matter how far apart they are. This creates strong correlations between particles, enabling powerful quantum algorithms and secure communication.

Representing qubits mathematically

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

$\alpha \Rightarrow$ How much the qubit is in the $|0\rangle$ state

$\beta \Rightarrow$ How much the qubit is in the $|1\rangle$ state.

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

- when we measure a quantum system, it collapses into the measured state.

- If we have a photon that is in a superposition of both vertically and horizontally polarized, when we measure it we can only measure it as horizontally or vertically polarized, and once it has been measured it will collapse into the measured state.

- If we measure ~~the~~ a photon in superposition which is both horizontally and vertically polarized, only the plane we measure will be its final state. ∴ Not in superposition anymore

- we only measure a qubit a 0 or a 1.

If we were to measure the qubit $|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$

we would not measure α or β, we still only measure a 0 or a 1

∴

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

Probability of measuring $|\psi\rangle$ as 0 is : $|\alpha|^2$

Probability of measuring $|\psi\rangle$ as 1 is : $|\beta|^2$

eg :- $|\psi_1\rangle = \begin{pmatrix} \sqrt{3}/2 \\ 1/2 \end{pmatrix}$

Probability of measuring 0 is : $\left|\frac{\sqrt{3}}{2}\right|^2 = \frac{3}{4}$

Probability of measuring 1 is $\left|\frac{1}{2}\right|^2 = \frac{1}{4}$

$$\therefore |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad \& \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Probability of measuring 0 is 1 — Probability of measuring 1 is 1
Probability of measuring 0 is 0 — Probability of measuring 0 is 0

$$|\alpha|^2 + |\beta|^2 = 1$$

∴ validity of a qubit is only true when probability is 1.

∴ If we measure $|\psi\rangle$ as 0, ∴ it $|\psi\rangle \Rightarrow |0\rangle$ due to collapse and vice versa.

Measuring a qubit collapses it's superposition.

Math & Theory

Imaginary ~~Complex~~ numbers

Date No

Let $i = \sqrt{-1}$

$$x^2 = -4$$
$$x = \pm\sqrt{-4}$$
$$x = \pm\sqrt{4}\sqrt{-1}$$
$$x = \pm 2\sqrt{-1}$$
$$x = \pm 2i$$

Complex Numbers

Real number + Imaginary number.

Standard form: $a + ib$, where $a, b \in \mathbb{R}$

Eg: $2 + 3i$ $\quad -1 - i$ $\quad \sqrt{2} + i\sqrt{3}$

Addition of complex numbers

eg:- $(2+3i)+(4-8i) = 6-5i$

$(1+9i)+(-3-8i) = -2+i$

Multiplication of complex numbers

$(2+3i)(4-8i) = 8-16i+12i-24i^2$

$(2+3i)(4-8i) = 8-4i-24i^2$

as $i = \sqrt{-1}$

$= 8-4i-24(-1)$

$= 32-4i$

Complex conjugate

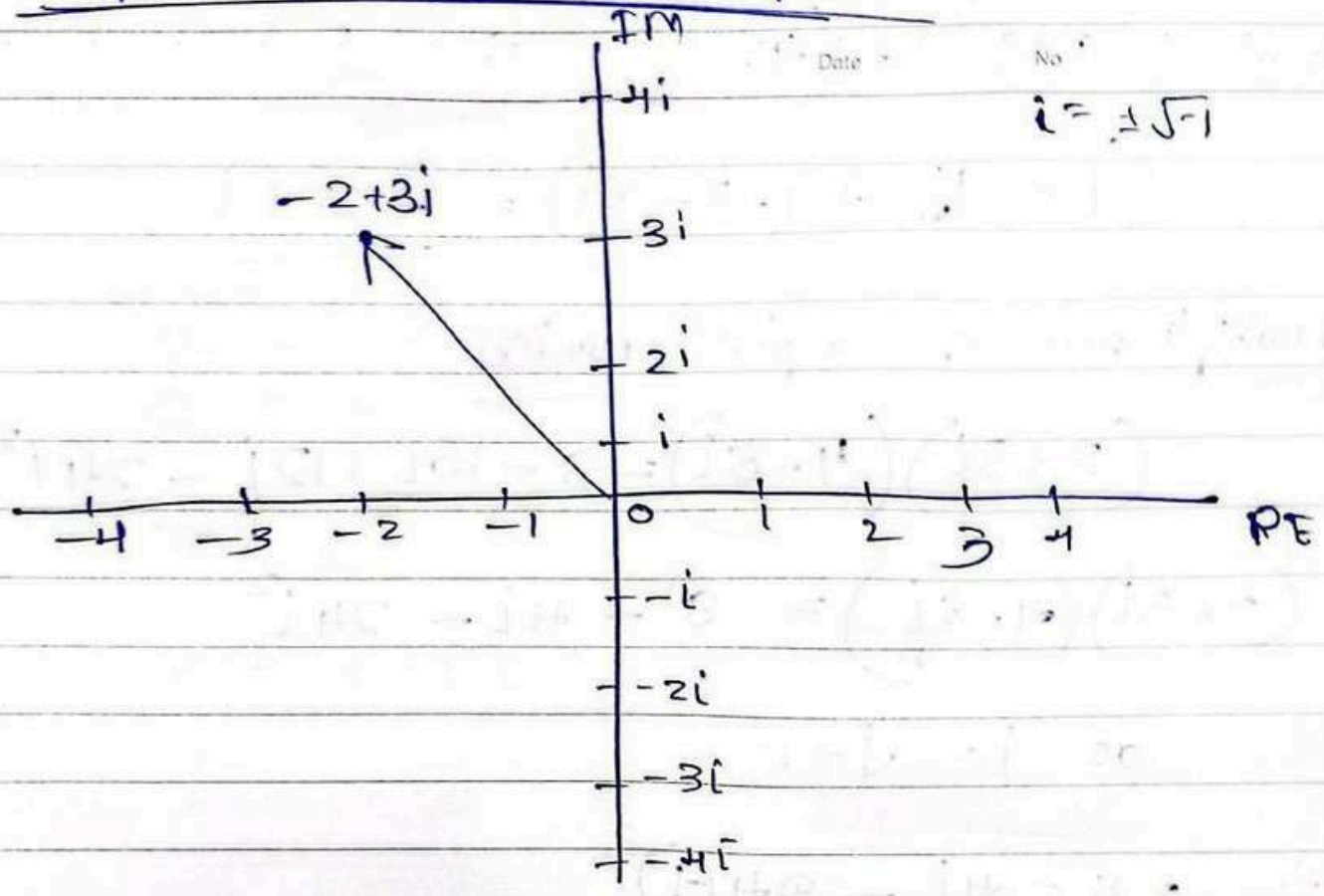
$a+ib = (a+ib)^* = a-ib$

eg:- $(-2+3i)^* = -2-3i$

$(3-i)^* = 3+i$

$$\boxed{(a+ib)(a-ib) = a^2+b^2}$$

Complex numbers on a number plane



$i = \pm\sqrt{-1}$

$$|-2+3i| = \sqrt{(-2)^2 + (3i)^2} = \sqrt{(-2)^2 + (3)^2}$$

$$|-2+3i| = \sqrt{13}$$

$$a + ib = r(\cos(\theta) + i\sin(\theta))$$

$r \equiv$ magnitude

$$a + ib = re^{i\theta}$$

Lesson 0.3 - Introduction to Matrices

Dimensions of matrices

eg :- $\begin{bmatrix} 1 \\ 2 \\ 0 \\ -9 \end{bmatrix}$ $\begin{bmatrix} 4 & 12 \\ -2 & 7 \\ 2 & 5 \end{bmatrix}$

4 × 1 matrix 3 × 2 matrix

colomn ↓ ↓

$\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ ← rows

Lesson 0.4 - Vectors & matrix multiplication

eg :- $\begin{bmatrix} 1 & 0 \\ 2 & -1 \end{bmatrix}\begin{bmatrix} 2 & 3 & 5 \\ 5 & 2 & 0 \end{bmatrix} = \begin{bmatrix} 2 & 3 & 5 \\ -1 & 4 & 10 \end{bmatrix}$

* To multiply matrices together, the no. of colomns of the left matrix must be equal to no. of rows on right matrix.

Identity matrix

2 × 2 Identity matrix

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \qquad IA = A$$

Inverse of matrices

Inverse of A is written as A^{-1}.

$$A^{-1}A = I$$

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \qquad A^{-1} = \frac{1}{ad - bc}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

0.5 lesson - Unitary & Hermitian matrices

$$A = \begin{bmatrix} 2+3i & 0 \\ 5 & 3-i \end{bmatrix} \quad A^* = \begin{bmatrix} 2-3i & 0 \\ 5 & 3+i \end{bmatrix}$$

The complex conjugate of a complex number in exponential form, $re^{i\theta}$ is $re^{-i\theta}$

$$\begin{bmatrix} 3+7i & 2e^{i\frac{\pi}{3}} \\ 5 & 3-i \end{bmatrix}^* = \begin{bmatrix} 3-7i & 2e^{-i\frac{\pi}{3}} \\ 5 & 3+i \end{bmatrix}$$

Transpose a matrix

$$\begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{bmatrix}^T = \begin{bmatrix} 1 & 4 \\ 2 & 5 \\ 3 & 6 \end{bmatrix}$$

$$(A^*)^T = (A^T)^* = A^\dagger \quad (A^\dagger : \text{dagger})$$

* we use 2 types of matrices to apply operations.

(1) Unitary matrices
(2) Hermitian matricies.

(1) Unitary matrices

$U^\dagger U = I$ Given that U is a unitary matrix

$U^\dagger \Rightarrow$ Inverse of U

* When acting on a vector, unitary matrixcies rotate/flip the vector, keeping magnitude the same;

eg:- original matrize $\Rightarrow \begin{bmatrix} 2+3i & i & 6-4i \\ 7 & 2-3i & -i \end{bmatrix}$

complex conjugate $\Rightarrow \begin{bmatrix} 2-3i & -i & 6+4i \\ 7 & 2+3i & i \end{bmatrix}$

conjugate transpose AKA Hermitian transpose $\Rightarrow \begin{bmatrix} 2-3i & 7 \\ -i & 2+3i \\ 6+4i & i \end{bmatrix}$

Unitary (complex)
- columns for orthonormal vectors

$U^H = U^{-1}$

(conjugate transpose = inverse)

0.6 Lesson : Eigenvectors & Eigenvalues

Date No.

$A\vec{v} = d\vec{v}$ where, A is a matrix, $\vec{v}$ is a vector and d is a scalar,

$A\vec{v}$ ↓ Eigenvector, $d\vec{v}$ ↓ Eigenvalue

d is a streching factor

~~Lesson 1.1 : Intro to Qubit & Superposition~~

Lesson 1.2 : Intro to Dirac Notation

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

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

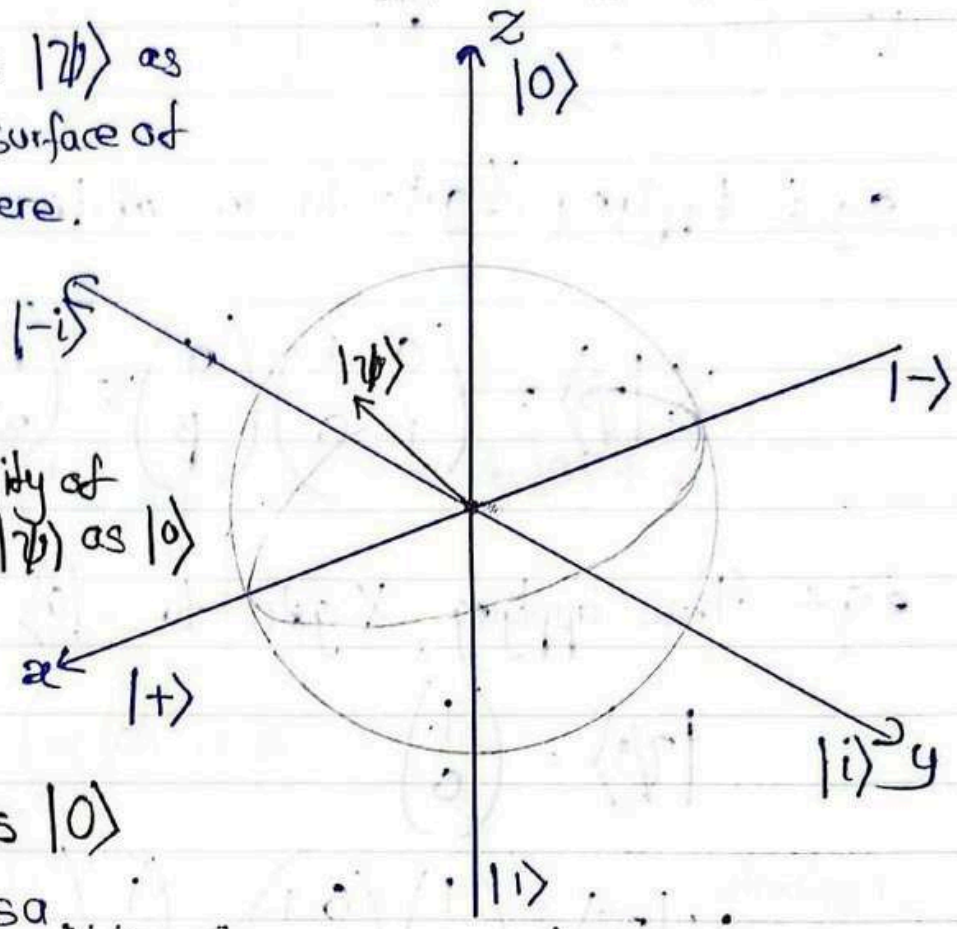
Dirac notation.

$|x\rangle$ are called ket vectors ↓ represents a quantum state

This is the standard of writing quantum computing states.

Lesson 1.3 : Representing a qubit on a Bloch sphere

- represent qubit $|\psi\rangle$ as a point on the surface of the Bloch Sphere.



- Higher vertically = Higher propability of measuring $|\psi\rangle$ as $|0\rangle$

⇒ if $|\psi\rangle$ is on the north pole, then $|\psi\rangle$ is $|0\rangle$ and vice versa...

Lesson 1.4 : Manipulating a qubit - the X, Y, Z Gates

The X gate ⇒ flips the qubit π radians around the x-axis on the bloch sphere.

The Y gate ⇒ flips the qubit π radians around the y-axis on the bloch sphere.

The Z gate ⇒ flips the qubit π radians around the z-axis on the bloch sphere.

1.4

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

eg ÷ Applying X gate to an arbitrary qubit $|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$

$$X|\psi\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \beta \\ \alpha \end{pmatrix}$$

eg ÷ Prove applying X gate to $|0\rangle$ gives $|1\rangle$.

$$|\psi\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

~~$X|\psi\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} \end{pmatrix}$~~

$$X|\psi\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$\therefore |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

∎

1.4

Applying quantum gates in dirac form

Let $U = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, be an arbitary gate.

$$U|0\rangle = \begin{pmatrix} a \\ c \end{pmatrix} \quad U|1\rangle = \begin{pmatrix} b \\ d \end{pmatrix}$$

$$U|0\rangle = a|0\rangle + c|1\rangle \quad U|1\rangle = b|0\rangle + d|1\rangle$$

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

$$U|\psi\rangle = U(\alpha|0\rangle + \beta|1\rangle)$$

$$U|\psi\rangle = \alpha U|0\rangle + \beta U|1\rangle$$, as this relationship is linear.

eg: $Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$

$$Y|\psi\rangle = \frac{\sqrt{3}}{2} Y|0\rangle + \frac{1}{2} Y|1\rangle$$

$$Y|\psi\rangle = \frac{\sqrt{3}}{2} \begin{pmatrix} 0 \\ i \end{pmatrix} + \frac{1}{2} \begin{pmatrix} -i \\ 0 \end{pmatrix}$$

$$Y|\psi\rangle = \frac{\sqrt{3}}{2} i \begin{pmatrix} 0 \\ 1 \end{pmatrix} - \frac{1}{2} i \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$$Y|\psi\rangle = \frac{\sqrt{3}}{2} i|1\rangle - \frac{1}{2} i|0\rangle$$

Lesson 15: Intro to Global & Relative Phase

Date No

eg of phase ÷ $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \xrightarrow{Z} \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$

$(-1 = e^{i\pi})$

$\therefore \frac{1}{\sqrt{2}}|0\rangle + e^{i\pi}\frac{1}{\sqrt{2}}|1\rangle$ * rotated around z-axis by π rad

eg(2) ÷ $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ $\frac{1}{\sqrt{2}}|0\rangle + i\frac{1}{\sqrt{2}}|1\rangle$.

$(i = e^{i\pi/2})$

$\therefore \frac{1}{\sqrt{2}}|0\rangle + e^{\frac{i\pi}{2}}\frac{1}{\sqrt{2}}|1\rangle$

* We use $e^{i\varphi}$ as it provides a visual change in phase as φ changes.

Q) But why is the $|1\rangle$ being multiplied by the complex no., but not the zero state?

Global phase

$$e^{i\varphi}(\alpha|0\rangle + \beta|1\rangle)$$

$$= e^{i\varphi}\alpha|0\rangle + e^{i\varphi}\beta|1\rangle$$

But it is irrelevent, ∴ we discard global phase.

eg :-

$$e^{i\varphi}\left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right)$$

$$\equiv \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

Relative phase

$$\alpha|0\rangle + e^{i\varphi}\beta|1\rangle$$

* Matters in calculations.

(Q) What if we have a complex no. in both global & relative phase.

$$e^{i\theta}\alpha|0\rangle + e^{i\varphi}\beta|1\rangle$$

$$= e^{i\theta}\left(\alpha|0\rangle + (e^{i\theta})^{-1}e^{i\varphi}\beta|1\rangle\right)$$

$$= \underbrace{e^{i\theta}}_{\text{global phase}}\left(\alpha|0\rangle + \underbrace{e^{i(\varphi-\theta)}}_{\text{Relative phase}}\beta|1\rangle\right)$$

· we can discard global phase,

$$= \alpha|0\rangle + e^{i(\varphi-\theta)}\beta|1\rangle \Rightarrow \text{Relative phase.}$$

(*) Phase does not affect probability of state being $|0\rangle$ or $|1\rangle$, Prove;

Date No

* $\alpha|0\rangle + e^{i\varphi}\beta|1\rangle$

Probability of measuring $|0\rangle = |\alpha|^2$

Probability of measuring $|1\rangle = |e^{i\varphi}\beta|^2$

$= |e^{i\varphi}|^2 |\beta|^2 = 1 \cdot |\beta|^2 = |\beta|^2$

magnitude of $e^{i\varphi}$ is 1 as $re^{i\varphi}$

∴ Probability is still $|\beta|^2$ for $|1\rangle$

Lesson 1.6 : The hadamard Gate & $+, -, i, -i$ states

$|+\rangle \Rightarrow \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$

$|i\rangle \Rightarrow \frac{1}{\sqrt{2}}|0\rangle + \frac{i}{\sqrt{2}}|1\rangle$

$|-\rangle \Rightarrow \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$

$|-i\rangle \Rightarrow \frac{1}{\sqrt{2}}|0\rangle - \frac{i}{\sqrt{2}}|1\rangle$

The hadamard Gate

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

$|0\rangle \xrightarrow{H} |+\rangle \qquad |+\rangle \xrightarrow{H} |0\rangle$

$|1\rangle \xrightarrow{H} |-\rangle \qquad |-\rangle \xrightarrow{H} |1\rangle$

∴ Hadamard Gate is its own inverse.

(Q) How do we apply hadamard gate to a arbitrarily qubit state?

* $H(\alpha|0\rangle + e^{i\varphi}\beta|1\rangle)$

$= \alpha H|0\rangle + e^{i\varphi}\beta H|1\rangle$

$= \alpha|+\rangle + e^{i\varphi}|-\rangle$

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

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

* Hadamade gate shows phase matters.

eg: $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \xrightarrow{H} |0\rangle$

$\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle \xrightarrow{H} |1\rangle$

* only differ by ~~phase~~ relative phase, applying gate they are different, pobability is altered.

Lesson 1.7 : The Phase gates (S & T gates)

$$S = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{2}} \end{pmatrix} \quad T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{pmatrix}$$

$$S^\dagger = \begin{pmatrix} 1 & 0 \\ 0 & e^{i(-\frac{\pi}{2})} \end{pmatrix} \quad T^\dagger = \begin{pmatrix} 1 & 0 \\ 0 & e^{i(-\frac{\pi}{4})} \end{pmatrix}$$

Adds a relative phase of $e^{i(-\pi/2)}$

Add a relative phase of $e^{i(-\pi/4)}$

$S^\dagger \equiv S^*$ $\quad T^\dagger = T^*$

$S|0\rangle = |0\rangle$

$S|1\rangle = i|1\rangle$

Lesson 2.1: Representing Multiple Qubits Mathematically

Tensor product

$$|0\rangle \otimes |0\rangle = |00\rangle$$

(⊗ : Tensor)

Representing qubits in superposition

$$(\alpha|0\rangle + \beta|1\rangle) \otimes (\gamma|0\rangle + \delta|1\rangle)$$

~~$= \alpha|0\rangle\gamma|0\rangle + 2\alpha|$~~

$$= \alpha|0\rangle \otimes \gamma|0\rangle + \alpha|0\rangle \otimes \delta|1\rangle + \beta|1\rangle \otimes \gamma|0\rangle + \beta|1\rangle \otimes \delta|1\rangle$$

$$= \alpha\gamma|0\rangle \otimes |0\rangle + \alpha\delta|0\rangle \otimes |1\rangle + \beta\gamma|1\rangle \otimes |0\rangle + \beta\delta|1\rangle \otimes |1\rangle$$

$$= \alpha\gamma|00\rangle + \alpha\delta|01\rangle + \beta\gamma|10\rangle + \beta\delta|11\rangle$$

$$\text{Prob}(\text{measuring } |00\rangle) = |\alpha\gamma|^2$$

$$\text{Prob}(\text{measuring } |01\rangle) = |\alpha\delta|^2$$

$$\text{Prob}(\text{measuring } |10\rangle) = |\beta\gamma|^2$$

$$\text{Prob}(\text{measuring } |11\rangle) = |\beta\delta|^2$$

eg:- $\left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right) \otimes \left(\frac{\sqrt{3}}{2}|0\rangle + \frac{1}{2}|1\rangle\right)$

Date No

~~$\frac{1}{\sqrt{2}} \cdot \frac{1}{\sqrt{2}}$~~

$= \frac{1}{\sqrt{2}} \cdot \frac{\sqrt{3}}{2}|00\rangle + \frac{1}{\sqrt{2}} \cdot \frac{1}{2}|01\rangle + \frac{1}{\sqrt{2}} \cdot \frac{\sqrt{3}}{2}|10\rangle + \frac{1}{\sqrt{2}} \cdot \frac{1}{2}|11\rangle$

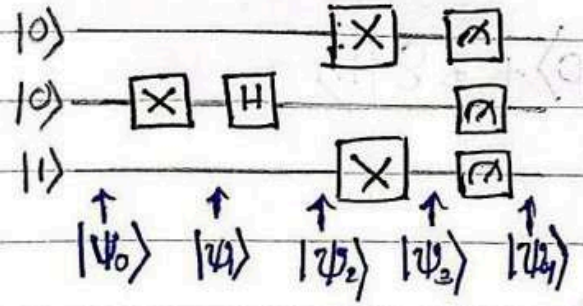
$= \frac{\sqrt{3}}{2\sqrt{2}}|00\rangle + \frac{1}{2\sqrt{2}}|01\rangle + \frac{\sqrt{3}}{2\sqrt{2}}|10\rangle + \frac{1}{2\sqrt{2}}|11\rangle$

notation

$$|0000\ldots0\rangle = |0\rangle^{\otimes n}$$ (n 0's)

eg:- $|1\rangle^{\otimes 5} = |11111\rangle$

Lesson 9.2 : Quantum Circuits



$|\psi_0\rangle = |001\rangle$

$|\psi_1\rangle = |011\rangle$

$|\psi_3\rangle = |0-1\rangle$

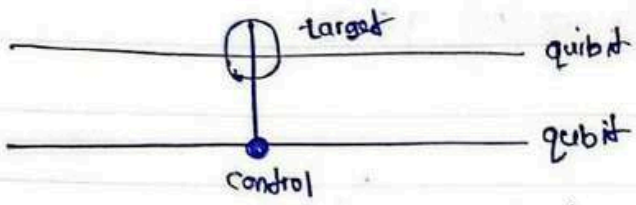
$|\psi_2| = |0\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \otimes -|1\rangle \quad |\psi_3\rangle = \frac{1}{\sqrt{2}}(|100\rangle - |110\rangle)$

$|\psi_2| = \frac{1}{\sqrt{2}}(|001\rangle - |011\rangle)$ ~~$|\psi_4\rangle$ will be $\frac{1}{2}$~~

$\therefore |\psi_4\rangle$ will be $|100\rangle$ $\frac{1}{2}$ of the time & $|110\rangle$ $\frac{1}{2}$ of the time.

Lesson 2.3 : Multi-qubit gates : CNOT, Toffoli & Controlled gates

CNOT / controlled X gate



- The CNOT gate applies an X gate to the target qubit if control qubit is 1.
- It does nothing if control is zero.

eg :- Consider first qubit as control & 2nd qubit as target.

$$\text{CNOT}\left(\frac{\sqrt{3}}{4}|00\rangle + \frac{1}{2}|01\rangle + \frac{1}{\sqrt{2}}|10\rangle + \frac{1}{4}|11\rangle\right)$$

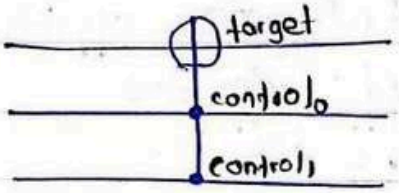
$$= \frac{\sqrt{3}}{4}\text{CNOT}|00\rangle + \frac{1}{2}\text{CNOT}|01\rangle + \frac{1}{\sqrt{2}}\text{CNOT}|10\rangle + \frac{1}{4}\text{CNOT}|11\rangle$$

$$= \frac{\sqrt{3}}{4}|00\rangle + \frac{1}{2}|01\rangle + \frac{1}{\sqrt{2}}|11\rangle + \frac{1}{4}|10\rangle$$

$$= \frac{\sqrt{3}}{4}|00\rangle + \frac{1}{2}|01\rangle + \frac{1}{4}|10\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

Toffoli Gate

Date No



* Has 2 control gates

eg:- $\text{TOFFOLI}\left(\frac{1}{\sqrt{2}}|0011\rangle + \frac{1}{\sqrt{2}}|0110\rangle\right)$

* consider 2nd, 3rd qubits are control. 4th qubit is target

$$= \frac{1}{\sqrt{2}}\text{TOFFOLI}|0011\rangle + \frac{1}{\sqrt{2}}\text{TOFFOLI}|0110\rangle$$

$$= \frac{1}{\sqrt{2}}|0011\rangle + \frac{1}{\sqrt{2}}|0111\rangle$$

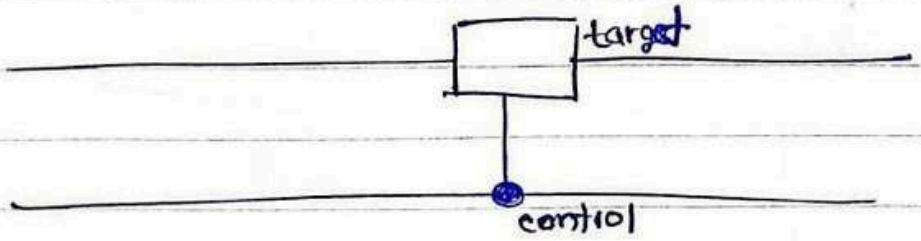
---

* CNOT gates can be ~~created~~ controlled versions of our single qubit gates.

CY, CZ, CS, CT, CH, ...

We write the gates as seen above; eg:- Controlled Y = CY

* applies if control is 1 but not 0.



Lesson 2.4 : Measuring singular qubits

(Q) How do we measure a single qubit?

(a) measure what is the probability of the 2nd qubit to be $|1\rangle$?

eg: * $|\psi\rangle = \frac{1}{2}|00\rangle + \frac{1}{4}|01\rangle + \frac{e^{i\frac{\pi}{2}}}{\sqrt{2}}|10\rangle + \frac{\sqrt{3}}{4}|11\rangle$

$$\text{Prob}\left(\text{measuring the 2nd qubit as a 1}\right) = \text{Prob}\left(\text{measuring } |01\rangle\right) + \text{Prob}\left(\text{measuring } |11\rangle\right)$$

$$= \left|\frac{1}{4}\right|^2 + \left|\frac{\sqrt{3}}{4}\right|^2 = \frac{1}{4}$$

eg: $|\psi_0\rangle = \frac{1}{2}|00\rangle + \frac{1}{4}|01\rangle + \frac{1}{\sqrt{2}}|10\rangle + \frac{\sqrt{3}}{4}|11\rangle$

(Q) what is the probability of getting $|1\rangle$ in first qubit?

* $|\psi_1\rangle = \frac{1}{\sqrt{2}}|10\rangle + \frac{\sqrt{3}}{4}|11\rangle$

we need to normalize;

$\therefore |\psi_1\rangle = \frac{A}{\sqrt{2}}|10\rangle + \frac{A\sqrt{3}}{4}|11\rangle$

$\left|\frac{A}{\sqrt{2}}\right|^2 + \left|\frac{A\sqrt{3}}{4}\right|^2 = 1$

$\frac{A^2}{2} + \frac{3A^2}{16} = 1$

$A = \frac{4}{\sqrt{11}}$

$\therefore |\psi_1\rangle = \frac{4}{\sqrt{22}}|10\rangle + \frac{\sqrt{3}}{\sqrt{11}}|11\rangle$

(i) what is the probability of obtaing $|0\rangle$ in the middle qubit?

$$|\psi_0\rangle = \frac{1}{2}|000\rangle + \frac{1}{2}|001\rangle + \frac{1}{2}|010\rangle + \frac{1}{2}|101\rangle$$

$$|\psi_1\rangle = A\left(\frac{1}{2}|000\rangle + \frac{1}{2}|001\rangle + \frac{1}{2}|101\rangle\right)$$

$$|\psi_1\rangle = \frac{A}{2}|000\rangle + \frac{A}{2}|001\rangle + \frac{A}{2}|101\rangle$$

$$\left|\frac{A}{2}\right|^2 + \left|\frac{A}{2}\right|^2 + \left|\frac{A}{2}\right|^2 = 1$$

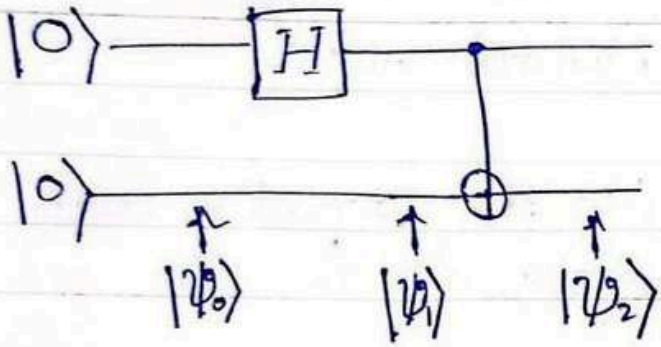
$$\frac{3A^2}{4} = 1$$

$$A = \frac{2}{\sqrt{3}}$$

$$|\psi_1\rangle = \frac{2}{\sqrt{3}}\left(\frac{1}{2}|000\rangle + \frac{1}{2}|001\rangle + \frac{1}{2}|101\rangle\right)$$

$$|\psi_1\rangle = \frac{1}{\sqrt{3}}|000\rangle + \frac{1}{\sqrt{3}}|001\rangle + \frac{1}{\sqrt{3}}|101\rangle$$

Lesson 2.5 : Entanglement & the Bell states



$$|\psi_0\rangle = |00\rangle$$

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) \otimes |0\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |10\rangle\right)$$

$$|\psi_2\rangle = \frac{1}{\sqrt{2}}\left(\text{CNOT}|00\rangle + \text{CNOT}|10\rangle\right)$$

$$|\psi_2\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$$

If we measure one of the qubits as a 0, $|\psi_2\rangle \rightarrow |00\rangle$

If we measure one of the qubits as a 1, $|\psi_2\rangle \rightarrow |11\rangle$

By measuring one of the qubits we know the state of the other qubit,

This called entanglement...

- A state is entangled if it cannot be factored into the tensor product of individual qubits.

- when qubits are entangled, they depend on each other to demine & their state.

Entangled States;

(a). Maximally entangled

* If ~~measured~~ measing one of the qubits, we can determine with certainty if the other qubits will be measured as 0 or 1.

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

~~(b) minimally entangled~~

Common Maximally entangled states (Bell states)

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

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

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

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

(b) Partially Minimally Entangled

* If partially entangled qubits are ~~entibits~~ identified if by measuring one of the qubits, the amplitudes of the ~~other~~ qubit is affected.

eg:- $|\psi\rangle = \sqrt{\frac{3}{5}}|00\rangle + \frac{1}{\sqrt{5}}|01\rangle + \frac{1}{2\sqrt{5}}|10\rangle + \frac{\sqrt{3}}{2\sqrt{5}}|11\rangle$

If we measure the first qubit as 0, the state collapses;

$$|0\rangle \otimes \left(\frac{\sqrt{3}}{2}|0\rangle + \frac{1}{2}|1\rangle\right)$$

2nd qubit;

If we measure the first qubit as 1, the state collapses;

$$|1\rangle \otimes \left(\frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle\right)$$

2nd qubit

~~they be~~ Both have different probabilities of measuring $|0\rangle$ or $|1\rangle$. If measuring one qubit affects the probability of the ~~the~~ other, ∴ it is partially entangled.

Maximally entangled ⇒ Qubits are maximally entangled if by measuring one of the qubits we know for certain what we will measure the other qubits as.

Partially entanged ⇒ If the measurement outcome of one of the qubits affects the state the other qubits collapse into once that qubit has been measured.

How do we know if Qubits are entangled ⇒ If we cannot factor the state into the tensor product of single-qubit states, then the state is entangled.

eg :- $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |01\rangle)$

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

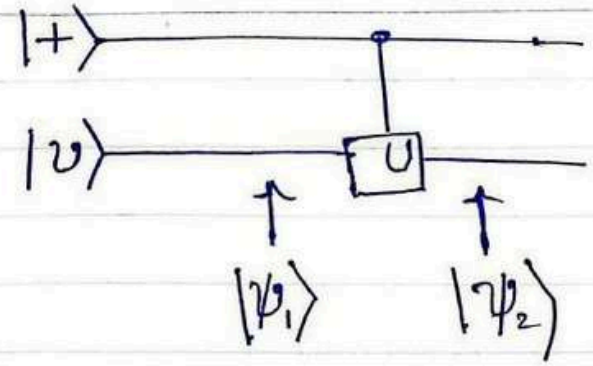
∴ It is not entangled.

eg ÷ $|\psi\rangle = \frac{\sqrt{3}}{2\sqrt{2}}|00\rangle + \frac{1}{2\sqrt{2}}|01\rangle + \frac{\sqrt{3}}{2\sqrt{2}}|10\rangle + \frac{1}{2\sqrt{2}}|11\rangle$

$|\psi\rangle = \left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right) \otimes \left(\frac{\sqrt{3}}{2}|0\rangle + \frac{1}{2}|1\rangle\right)$

∴ It is not entangled.

Lesson 2.6: Phase kickback



$|v\rangle$ is an eigenvector of U

$$U|v\rangle = e^{i\theta}|v\rangle$$

as all eigenvalues can be represented as $e^{i\theta}$

$$|\psi_1\rangle = |+\rangle|v\rangle$$

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

$$|\psi_2\rangle = \frac{1}{\sqrt{2}}\left(CU|0\rangle|v\rangle + CU|1\rangle|v\rangle\right)$$

$$|\psi_2\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle|v\rangle + |1\rangle \cdot CU|v\rangle\right)$$

$$|\psi_2\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle|v\rangle + e^{i\theta}|1\rangle|v\rangle\right)$$

$$|\psi_2\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\theta}|1\rangle\right)|v\rangle$$

This occurs if state $|v\rangle$ is an eigenvector of a gate U, by applying a controlled-U gate with $|v\rangle$ as a target, we can 'kick' the phase onto the control qubit.

Lesson 3.1 : Superdense coding

Date No

Quantum protocol that allows us to send two bits of classical information (00, 01, 10, 11) using 1 qubit. we use entanglement for this;

example :- Alice ⟹ Bob

(Alice wants to send 2 classical bits to Bob)

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

Alice wants to send 00 : Does nothing, Qubits: $|\psi\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$

Alice wants to send 01 : Applies X gate, $|\psi\rangle = \frac{1}{\sqrt{2}}\left(|10\rangle + |01\rangle\right)$

Alice wants to send 10 : Applies Z gate, $|\psi\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle - |11\rangle\right)$

Alice wants to send : Applies X, Z to her qubit ; $|\psi\rangle = \frac{1}{\sqrt{2}}\left(|10\rangle - |01\rangle\right)$

Then Alice sends her qubits to Bob, so he has both

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right) \xrightarrow[\text{as 1st qubit as control}]{\text{CNOT}} \frac{1}{\sqrt{2}}\left(|00\rangle + |10\rangle\right)$$

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|10\rangle + |01\rangle\right) \xrightarrow{\text{CNOT}} \frac{1}{\sqrt{2}}\left(|11\rangle + |01\rangle\right)$$

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle - |11\rangle\right) \xrightarrow{\text{CNOT}} \frac{1}{\sqrt{2}}\left(|00\rangle - |10\rangle\right)$$

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|10\rangle - |01\rangle\right) \xrightarrow{\text{CNOT}} \frac{1}{\sqrt{2}}\left(|11\rangle - |01\rangle\right)$$

then he applies a hadamard gate;

$$\frac{1}{\sqrt{2}}\left(|00\rangle + |10\rangle\right) \xrightarrow{H} H|+\rangle|0\rangle = |00\rangle$$

$$\frac{1}{\sqrt{2}}\left(|10\rangle + |01\rangle\right) \xrightarrow{H} H|+\rangle|1\rangle = |01\rangle$$

$$\frac{1}{\sqrt{2}}\left(|00\rangle - |10\rangle\right) \xrightarrow{H} H|-\rangle|0\rangle = |10\rangle$$

$$\frac{1}{\sqrt{2}}\left(|11\rangle - |01\rangle\right) \rightarrow H|-\rangle|1\rangle = |11\rangle$$

Lesson 3.2.A: Classical Operations Prerequisites

Date No

4 main operations we can perform on classical bits;

AND, OR, NOT, XOR

Classical NOT operation

x	$f(x)$
0	1
1	0

Classical AND Gate

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

Classical OR operation

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

Classical XOR Gate

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

A function f is reversible if give $f(x)$, we can find x.

f : Negate 2nd bit

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

⇒ Reversible,
as each row of the truth table is unique,
∴ we can map each output to a unique input.

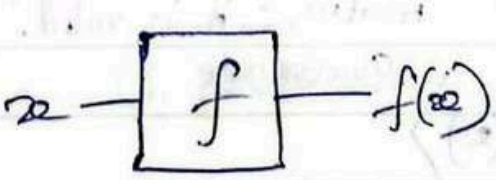
f : OR operation

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

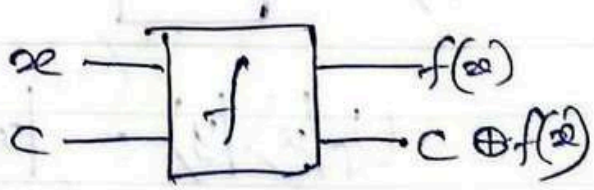
⇒ Not reversible,
it does not have a unique output which could be mapped to the input.

* to make any classical gate reversible we must have a arbitary unit,

Standard Classical operation

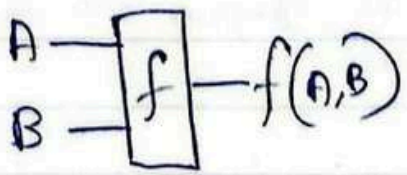


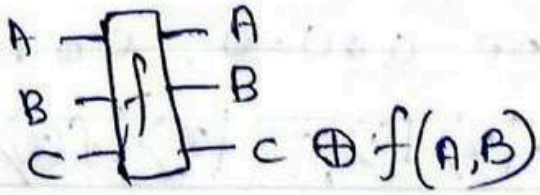
Reversible classical operation



⊕ denotes the XOR operation

eg:- $f(A, B)$ is the OR operation





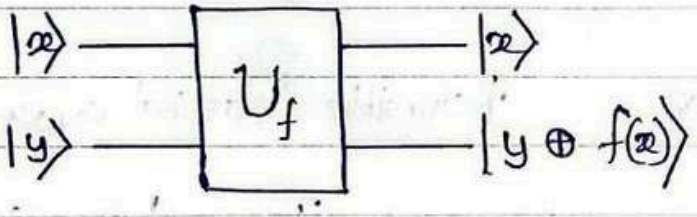
∴

A	B	C	A	B	C ⊕ f(A,B)
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	1
0	1	1	0	1	0
1	0	0	1	0	1
1	0	1	1	0	0
1	1	0	1	1	1
1	1	1	1	1	0

* In quantum computing, all operations we apply must be reversible (beside measurements)

Standard quantum function

3.2 B: Functions on quantum computers



* we can encode functions in a unitary matrix, ∴ it is valid quantum gate.

$$U_f|x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle$$

Set $y = |0\rangle$;

$$U_f|x\rangle|0\rangle = |x\rangle|0 \oplus f(x)\rangle$$

Since $0 \oplus 0 = 0$, $0 \oplus 1 = 1$

$$\therefore U_f|x\rangle|0\rangle = |x\rangle|f(x)\rangle$$

What happens when apply function f when output is $U_f|x\rangle|-\rangle$.

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

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

$$= \frac{1}{\sqrt{2}}\left(|x\rangle|f(x)\rangle - |x\rangle|\overline{f(x)}\rangle\right)$$

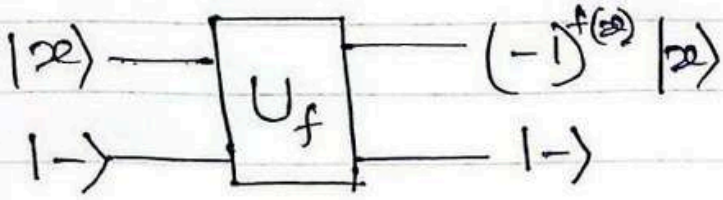
~~$$= \begin{cases} \frac{1}{\sqrt{2}}\left(|x\rangle|0\rangle - |x\rangle|1\rangle\right) & \text{if } f(x)=0 \\ \end{cases}$$~~

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

$$= (-1)^{f(x)}|x\rangle|-\rangle \quad \text{(as only sign is different)}$$

Applying a function,

$$U_f|x\rangle|-\rangle = (-1)^{f(x)}|x\rangle|-\rangle$$



If the output bit is in the $|-\rangle$, we call it a phase oracle.

No cloning theorum

- On a classical computer we can copy bits, but in quantum we cannot if the qubits are in unknown state

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

- If we don't know α and β, then we cannot copy the state of $|\psi\rangle$ to other qubits.

Lesson 3.3: Deutsch's Algorithm

- find if a function is constant or balanced?

$$f: \{0,1\} \longrightarrow \{0,1\}$$

Constant functions ⇒ If a function is constant, it returns a same bit, no matter the input, $f(0) = f(1)$

Constant-One

x	$f(x)$
0	1
1	1

Constant-zero

x	$f(x)$
0	0
1	0

* Balanced functions ⇒ Returns 0 for half the inputs & 1 for other half of inputs.

Bit flip (NOT Gate)

x	$f(x)$
0	1
1	0

Identity

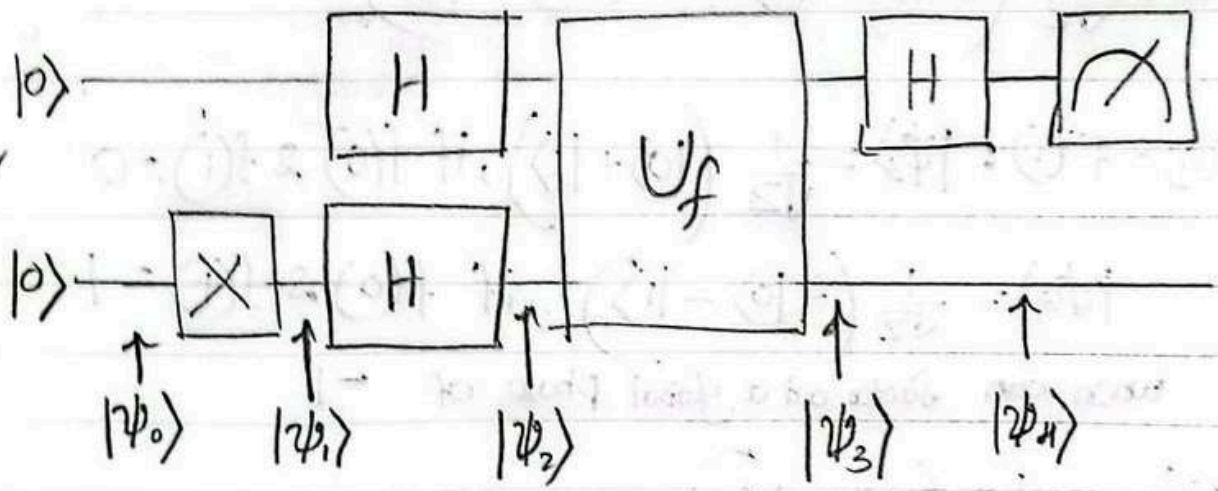
x	$f(x)$
0	0
1	1

- On a classical computer, we need to query the oracle twice. We input both 0 and 1 so we can check if $f(0) = f(1)$ or $f(0) \neq f(1)$ to determine whether f is constant or balanced. So operation must take place twice.

if $f(0) = f(1)$, then f is constant

if $f(0) \neq f(1)$, then f is balanced.

- Quantum computers only require one query of the function to determine if it is constant or balanced.



$|\psi_0\rangle = |00\rangle$

$|\psi_1\rangle = |01\rangle$

$|\psi_2\rangle = |+-\rangle$

$|\psi_2\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle|-\rangle + |1\rangle|-\rangle\right)$

$|\psi_3\rangle = U_f \frac{1}{\sqrt{2}}\left(|0\rangle|-\rangle + |1\rangle|-\rangle\right)$

$|\psi_3\rangle = \frac{1}{\sqrt{2}}\left(U_f|0\rangle|-\rangle + U_f|1\rangle|-\rangle\right)$

$|\psi_3\rangle = \frac{1}{\sqrt{2}}\left(U_f|0\rangle|-\rangle + U_f|1\rangle|-\rangle\right)$

$U_f|x\rangle|-\rangle = (-1)^{f(x)}|x\rangle|-\rangle$

$|\psi_3\rangle = \frac{1}{\sqrt{2}}\left((-1)^{f(0)}|0\rangle|-\rangle + (-1)^{f(1)}|1\rangle|-\rangle\right)$

$|-\rangle$ is not needed.

$|\psi_3\rangle = \frac{1}{\sqrt{2}}\left((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle\right)$

$$|\psi_3\rangle = \frac{1}{\sqrt{2}}\left((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle\right)$$

If $f(0)=f(1)$: $|\psi_3\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle+|1\rangle\right)$, if $f(0)$ & $f(1)=0$

~~If f(~~ $|\psi_3\rangle = \frac{1}{\sqrt{2}}\left(-|0\rangle-|1\rangle\right)$, if $f(0)$ & $f(1)=1$

when can factor out a global phase of -1

$\therefore |\psi_3\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle+|1\rangle\right)$.

$\therefore$ If $f(0)=f(1)$; $|\psi_3\rangle = |+\rangle$

If $f(0) \neq f(1)$:

$|\psi_3\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle-|1\rangle\right)$, if $f(0)=0$ & $f(1)=1$.

$|\psi_3\rangle = \frac{1}{\sqrt{2}}\left(-|0\rangle+|1\rangle\right)$, if $f(0)=1$ & $f(1)=0$

factor out global phase of -1,

$\therefore |\psi_3\rangle = |-\rangle$

If $f(0) = f(1)$;

$|\psi_3\rangle = |+\rangle$

$|\psi_4\rangle = |0\rangle$

If $f(0) \neq f(1)$:

$|\psi_3\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = |-\rangle$

$|\psi_4\rangle = |1\rangle$

$\therefore$ If $|0\rangle$ is measured $\Rightarrow$ function is constant.

$\therefore$ If $|1\rangle$ is measured $\Rightarrow$ function is balanced.

We completed the ~~query~~ function with one query on quantum computer, while classical computer required 2 queries.

Lesson 3.4: Deutsh-Jozsa Algorithm

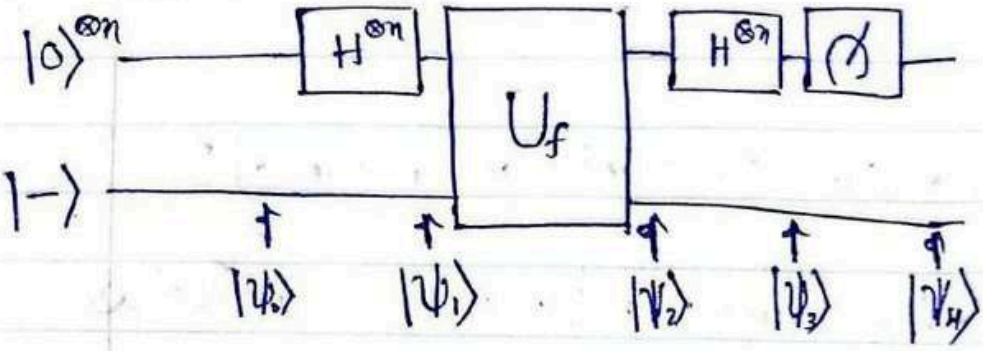
(Q) Is a function constant or balanced?

* Constant functions always returns the same value

* Balanced functions always return-0 for half and 1 for half.

- To determine whether f is a constant or balanced takes a classical computer @ worst $2^{n-1}+1$ queries of f, where n is length of the bit string the function takes as input.

- In the worst case we input half (2^{n-1}) inputs and get the same output, so we need to query the function one more time to determine if its constant or balanced.



$$|\psi_0\rangle = |0\rangle^{\otimes n} |-\rangle$$

$$|\psi_1\rangle = H^{\otimes n} |0\rangle^{\otimes n} |-\rangle$$

$$H^{\otimes n} |0\rangle^{\otimes n} = \underbrace{H|0\rangle H|0\rangle H|0\rangle \otimes \dots H|0\rangle}_{n \text{ times}}$$

Finding $H^{\otimes n} |0\rangle^{\otimes n}$

$$H^{\otimes n} |0\rangle^{\otimes n} = H|0\rangle H|0\rangle \dots H|0\rangle = |+++++\dots+\rangle$$

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

$$= \frac{1}{\sqrt{2^2}} \underbrace{(|00\rangle + |01\rangle + |10\rangle + |11\rangle)}$$

$$= \frac{1}{\sqrt{4}} \sum_{x \in \{0,1\}^2} |x\rangle$$

$\sum_{x \in \{0,1\}^n} |x\rangle$, is the sum over all bitstrings of length n.

Finding $H^{\otimes n}|0\rangle^{\otimes n}$,

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

$$\therefore |\psi_1\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle|-\rangle$$

$$|\psi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} U_f|x\rangle|-\rangle$$

$$U_f|x\rangle|-\rangle = (-1)^{f(x)}|x\rangle|-\rangle$$

$$\therefore |\psi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} (-1)^{f(x)}|x\rangle|-\rangle$$

ommit $|-\rangle$ as it is not needed for the algorithm.

$$|\psi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} (-1)^{f(x)}|x\rangle$$

$$|\psi_3\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} (-1)^{f(x)} H^{\otimes n}|x\rangle$$

finding $H^{\otimes n}|x\rangle$

$$H|x_i\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + (-1)^{x_i}|1\rangle\right), \text{ where } x_i \in \{0,1\}$$

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

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

finding $H^{\otimes n}|x\rangle$;

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

$$\therefore |\psi_3\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} (-1)^{f(x)} \frac{1}{\sqrt{2^n}} \sum_{z \in \{0,1\}^n} (-1)^{x \cdot z} |z\rangle$$

$$= \sum_{z \in \{0,1\}^n} \left(\frac{1}{2^n} \sum_{x \in \{0,1\}^n} (-1)^{f(x) + x \cdot z} \right) |z\rangle$$

If we consider amplitude of all $|000..0\rangle$:

$$\frac{1}{2^n}\sum_{x\in\{0,1\}^n}(-1)^{f(x)+x\cdot 000\ldots 0} = \frac{1}{2^n}\sum_{x\in\{0,1\}^n}(-1)^{f(x)}$$

If f is constant:

$$\frac{1}{2^n}\sum_{x\in\{0,1\}^n}(-1)^{f(x)} = \frac{1}{2^n}\sum_{x\in\{0,1\}^n} 1, \text{ if } f(x)=0 \text{ for all } x$$

$$= \frac{1}{2^n}\times 2^n = 1$$

$$\frac{1}{2^n}\sum_{x\in\{0,1\}^n}(-1)^{f(x)} = -1, \text{ if } f(x)=1 \text{ for all } x$$

∴ Amplitude of all zero states $(|000\ldots 0\rangle)$: ± 1

If f is balanced:

Since for half of the inputs $f(x)=0$ and the other half $f(x)=1$, the sum will be adding together an equal amount of 1's and -1's, resulting in 0.

$$\therefore \frac{1}{2^n}\sum_{x\in\{0,1\}^n}(-1)^{f(x)}=0$$

If f is constant:

Amplitude of $|00\ldots0\rangle = \pm 1$

$\Rightarrow$ Prob of measuring $|000..0\rangle = 1$

If f is balanced:

Amplitude of $|00\ldots0\rangle = 0$

$\Rightarrow$ Prob of measuring $|00\ldots0\rangle = 0$

$\therefore$ If we measure the $|00\ldots0\rangle$ state, then f is constant
If we measure any other state, then f is balanced.

* used commonly in algorythms.

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

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

Berstein-Vazarani Algorithm

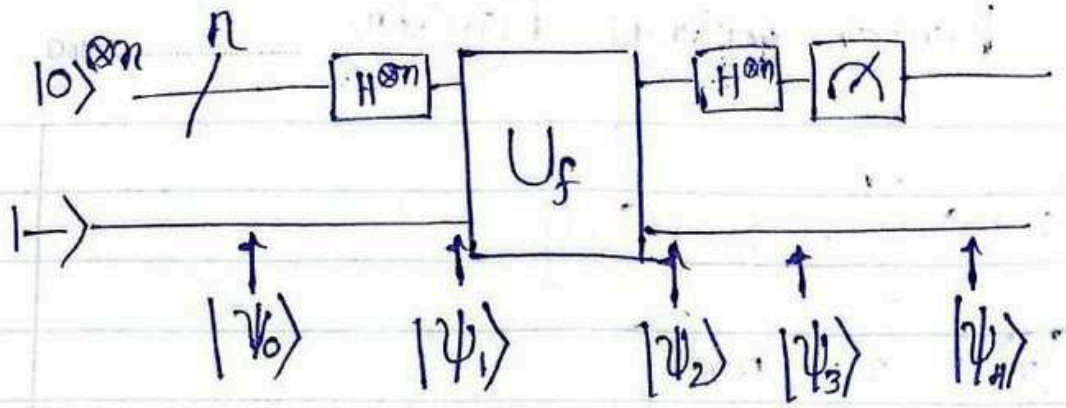
$$f: \{0,1\}^n \rightarrow \{0,1\}$$

$$f(x) = x \cdot s \pmod 2$$

Our task is to find the secret bit string s

$(\text{mod } 2)$ means we take the remainder of the answer divided by 2, so if $x \cdot s = s$ the $x \cdot s \pmod 2 = 1$

- In a classical computer we should input a bit string exept for 1 in one position.
- A classical computer needs to query the function n times where n is the length of the bit string s.



$$|\psi_0\rangle = |0\rangle^{\otimes n}|-\rangle$$

$$|\psi_1\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle|-\rangle$$

$$|\psi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} U_f|x\rangle|-\rangle$$

$$|\psi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} (-1)^{f(x)}|x\rangle|-\rangle$$

$$|\psi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} (-1)^{x \cdot s}|x\rangle$$

$$|\psi_3\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} (-1)^{x \cdot s} H^{\otimes n}|x\rangle$$

$$|\psi_3\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} (-1)^{x \cdot s} \frac{1}{\sqrt{2^n}} \sum_{z \in \{0,1\}^n} (-1)^{x \cdot z}|z\rangle$$

$$|\psi_3\rangle = \frac{1}{2^n} \sum_{x \in \{0,1\}^n} \sum_{z \in \{0,1\}^n} (-1)^{(s+z)x} |z\rangle$$

The '+' represents bitwise XOR;
$(s+z)_i = s_i + z_i$. For example $0110 + 1110 = 1000$

Amplitude of the $|s\rangle$ state:

$$\frac{1}{2^n} \sum_{x \in \{0,1\}^n} (-1)^{(z \oplus s) \cdot x}$$

Since $s+s$ means we xor every bit of s with the bit from s in the same position, it will result in $00\ldots0$ since $0 \oplus 0 = 0$ and $1 \oplus 1 = 0$.

$$= \frac{1}{2^n} \sum_{x \in \{0,1\}^n} 1 = \frac{1}{2^n} \times 2^n = 1$$

∴ Amplitude of the $|s\rangle$ state:

$$|s\rangle = 1$$

∴ Propability of measuring $|s\rangle$ is 1

Lesson 3.8: Quantum Fourier Transformation

State after QFT applied to $|101\rangle$

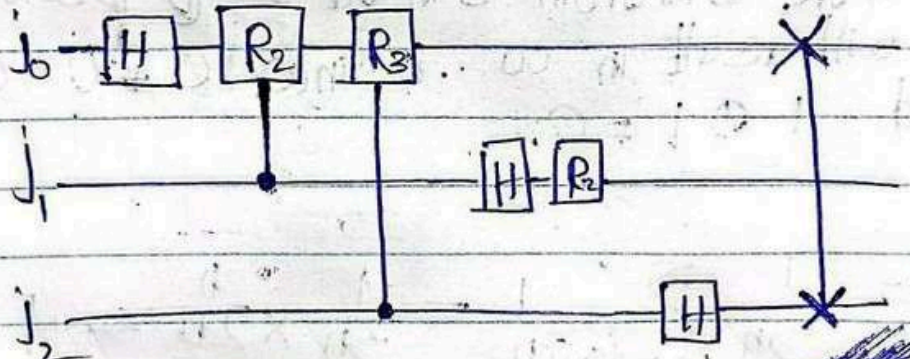
$$QFT|101\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\pi}|1\rangle\right)\frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\frac{\pi}{2}}|1\rangle\right) \times \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\frac{5\pi}{4}}|1\rangle\right)$$

controlled R gate

$$R_k = \begin{bmatrix} 1 & 0 \\ 0 & e^{\frac{2\pi i}{2^k}} \end{bmatrix} \qquad R_k|0\rangle = |0\rangle$$

$$R_k|1\rangle = e^{\frac{2\pi i}{2^k}}|1\rangle$$

ex (1) ⇒



$$|j\rangle = |j_0 j_1 j_2\rangle$$

$$H|j_0\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + (-1)^{j_0}|1\rangle\right)$$

$$H|j_0\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i\left(\frac{j_0}{2}\right)}|1\rangle\right)$$

$$R_2 H|j_0\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i\left(\frac{j_0}{2}\right)} e^{\left(\frac{2\pi i}{2^2}\right) j_1}|1\rangle\right)$$

- Since j_1 is the control, we can put the relative phase it adds to the power of j_1 since if $j_1 = 0$, then we dont apply the phase and if $j_1 = 1$, then we apply the phase.

$$R_2 H|j_0\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i\left(\frac{j_0}{2} + \frac{j_1}{4}\right)}|1\rangle\right)$$

$$R_3 R_2 H|j_0\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i\left(\frac{j_0}{2} + \frac{j_1}{4}\right)} e^{\left(\frac{2\pi i}{2^3}\right) j_2}|1\rangle\right)$$

$$R_3 R_2 H|j_0\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i\left(\frac{j_0}{2} + \frac{j_1}{4} + \frac{j_2}{8}\right)}|1\rangle\right)$$

$$H|j_1\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i\left(\frac{j_1}{2}\right)}|1\rangle\right)$$

$$R_2 H|j_1\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i\left(\frac{j_1}{2} + \frac{j_2}{4}\right)}|1\rangle\right)$$

$$H|j_2\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i\left(\frac{j_2}{2}\right)}|1\rangle\right)$$

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i\left(\frac{j_0}{2}+\frac{j_1}{4}+\frac{j_2}{8}\right)}|1\rangle\right)\otimes\frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i\left(\frac{j_1}{2}+\frac{j_2}{4}\right)}|1\rangle\right)$$

$$\otimes\frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i\left(\frac{j_2}{2}\right)}|1\rangle\right)$$

$$QFT|j\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i\left(\frac{j_2}{2}\right)}|1\rangle\right)\otimes\frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i\left(\frac{j_1}{2}+\frac{j_2}{4}\right)}|1\rangle\right)\otimes\frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i\left(\frac{j_0}{2}+\frac{j_1}{4}+\frac{j_2}{8}\right)}\times|1\rangle\right.$$

- we have encoded the value of j into the phase of the qubit.

we can mathematically represent the QFT on a basis state $|j\rangle$ through the following identity:

$$\boxed{QFT|j\rangle = \frac{1}{\sqrt{2^n}}\sum_{k=0}^{2^n-1} e^{\frac{2\pi ijk}{2^n}}|k\rangle.}$$

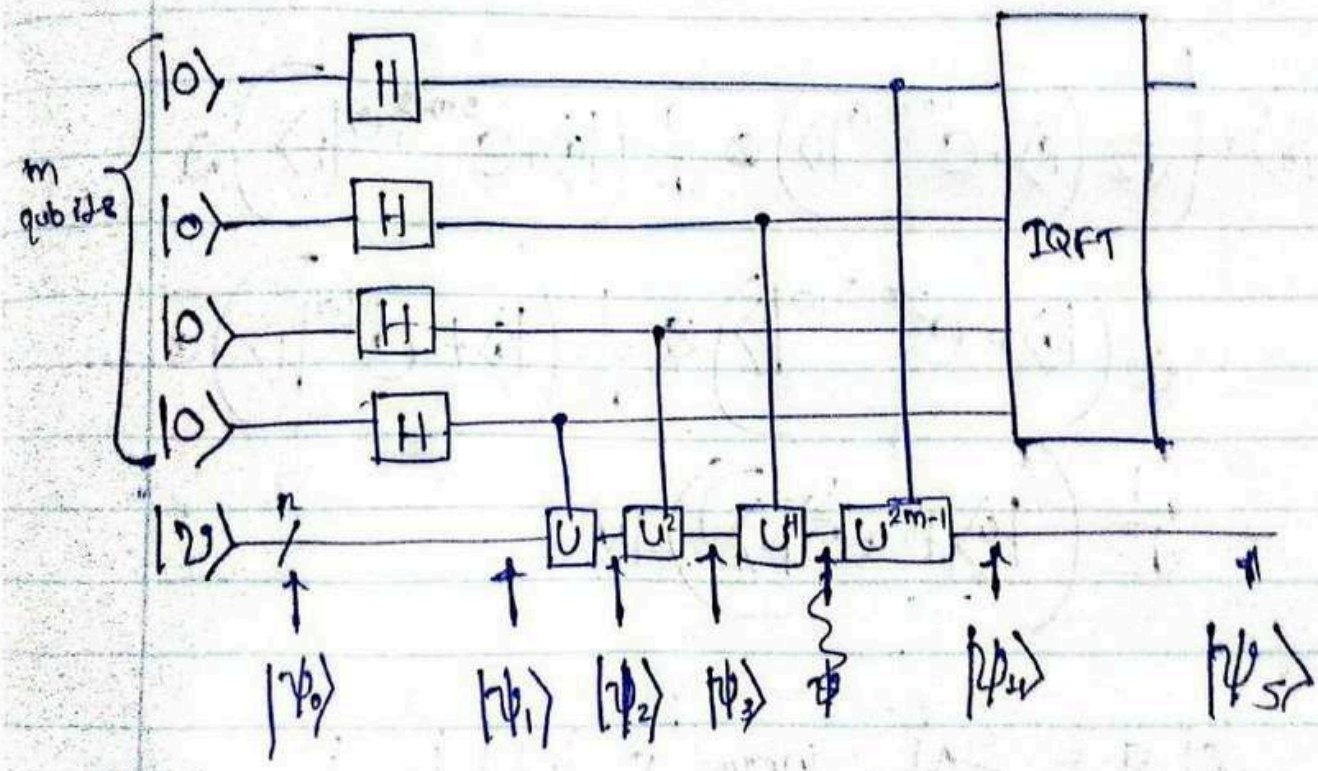
The inverse quantum Fourier transform is usually denoted by either IQFT or $QFT^\dagger$

3.7 : Quantum phase estimation

- Used to find the eigenvalue of an eigenvector given the matrix.

$$U|v\rangle = e^{i\theta}|v\rangle$$

The quantum phase estimation algorithm (QPE) finds $e^{i\theta}$ given its eigenvector $|v\rangle$ and matrix U



$$|\psi_0\rangle = |0\rangle^{\otimes m}|v\rangle$$

$$|\psi_1\rangle = \left(\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle+|1\rangle) \otimes \dots \otimes \frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\right) \times |v\rangle$$

$$|\psi_2\rangle = \left(\frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) \otimes \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) \otimes \cdots \otimes \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\theta}|1\rangle\right)\right)|\nu\rangle$$

$$|\psi_3\rangle = \left(\frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) \otimes \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) \otimes \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) \otimes \cdots \otimes \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2i\theta}|1\rangle\right) \otimes \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\theta}|1\rangle\right)\right)|\nu\rangle$$

$$|\psi_4\rangle = \left(\frac{1}{\sqrt{2}}\left(|0\rangle + e^{2^{m-1}i\theta}|1\rangle\right) \otimes \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2^{m-2}i\theta}|1\rangle\right) \otimes \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2^{m-3}i\theta}|1\rangle\right) \otimes \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2i\theta}|1\rangle\right) \otimes \cdots \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\theta}|1\rangle\right)\right)|\nu\rangle$$

let $\theta = 2\pi j$, where $j = 0.j_0 j_1 j_2 \cdots j_{m-1}$ and each $j_l \in \{0,1\}$

j is a bit string less than 1,

$\therefore j = \underbrace{0.j_0 j_1 j_2 \cdots j_{m-1}}_{\text{Binary}} = \frac{j_0}{2} + \frac{j_1}{4} + \frac{j_2}{8} + \cdots \frac{j_{m-1}}{2^m}$

$$|\psi_4\rangle = \left(\frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i\left(\frac{j_{m-1}}{2}\right)}|1\rangle\right) \otimes \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i\left(\frac{j_{m-2}}{4} + \frac{j_{m-1}}{4}\right)}|1\rangle\right) \otimes \cdots$$

$$\otimes \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i\left(\frac{j_1}{2} + \frac{j_2}{4} + \cdots + \frac{j_{m-1}}{2^{m-1}}\right)}|1\rangle\right) \otimes \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i\left(\frac{j_0}{2} + \frac{j_1}{4} + \cdots + \frac{j_{m-1}}{2^m}\right)}|1\rangle\right)$$

$$|\psi_5\rangle = IQFT|\psi_4\rangle = |j\rangle$$

$\theta = 2\pi j$

Eigenvalue $= e^{i\theta}$

RICHARD

Shor's Algorithm

$N = pq$, where p and q are both prime

Shor's Algorithm allows us to efficiently find p and q given N.

$a \equiv b \bmod(n)$ if the remainder of $\frac{a}{n}$ is b

Modular exponentiation

* It is a type of exponentiation performed over a modulus.

$$eg:\ a^b \bmod m \equiv a^b \pmod m$$

* $2^0 \equiv 1 \bmod(9)$ Repeated
  $2^1 \equiv 2 \bmod(9)$
  $2^2 \equiv 4 \bmod(9)$
  $2^3 \equiv 8 \bmod(9)$
  $2^4 \equiv 7 \bmod(9)$
  $2^5 \equiv 5 \bmod(9)$
* $2^6 = 1 \bmod(9)$
  $2^7 = 2 \bmod(9)$

$N = pq$, where p and q are prime.

For an a, where $1 < a < N$ and $\gcd(a, N) = 1$

Let r be the period of modular exponentiation of $a^x \bmod (N)$

with good approximation of r, the $\gcd(a^{\frac{r}{2}} - 1, N)$ and $\gcd(a^{r/2} + 1, N)$ has a good chance of containing p and/or q.

$$U_{a,N}|x\rangle = |xa \bmod (N)\rangle$$

$$U^0_{a,N}|1\rangle = |1 \bmod (N)\rangle$$

$$U^1_{a,N}|1\rangle = |a \bmod (N)\rangle$$

$$U^2_{a,N}|1\rangle = |a^2 \bmod (N)\rangle$$

$$\vdots$$

$$U^r_{a,N}|1\rangle = |a^r \bmod (N)\rangle = |1 \bmod (N)\rangle$$

$$\boxed{\frac{1}{\sqrt{r}}\sum_{s=0}^{r-1}|u_s\rangle = |1 \bmod (N)\rangle}$$

From quantum circuit we get $j = \frac{s}{r}$

Continued fractions

- we can find the factors of N.

$$\therefore \quad a^r \equiv 1 \bmod (N)$$

$$\Rightarrow \quad a^r - 1 \equiv 0 \bmod (N)$$

$\therefore$ $a^r - 1$ has N as a factor

$$a^r - 1 = \left(a^{r/2} - 1\right)\left(a^{r/2} + 1\right)$$

The $\gcd\left(a^{r/2} - 1, N\right)$ and/or $\gcd\left(a^{r/2} + 1, N\right)$ are containg a non-trivial factor of N, so with our estimation of r, we have a good chance of finding this factor.

Example for Shor's Algorithm;

$N = 15$, so $p = 3$, $q = 5$

(1) Choose and a such that $\gcd(a, 15) = 1$, for example we choose $a = 7$

(2) We use quantum computer to estimate r, we need r such that $7^r \equiv 1 \bmod (15)$. using algorithm we find $r = 4$

(3) $\gcd(7^{4/2} - 1, 15) = \gcd(48, 15) = 3$

$\gcd(7^{4/2} + 1, 15) = \gcd(50, 15) = 5$

Recap on
- Shor's algorithm
- Deutch-Jozsa Algorithm
- Bastein-Vazarani
- QFT
- Quantum phase estimation.