Presentation-2 24/05/2022

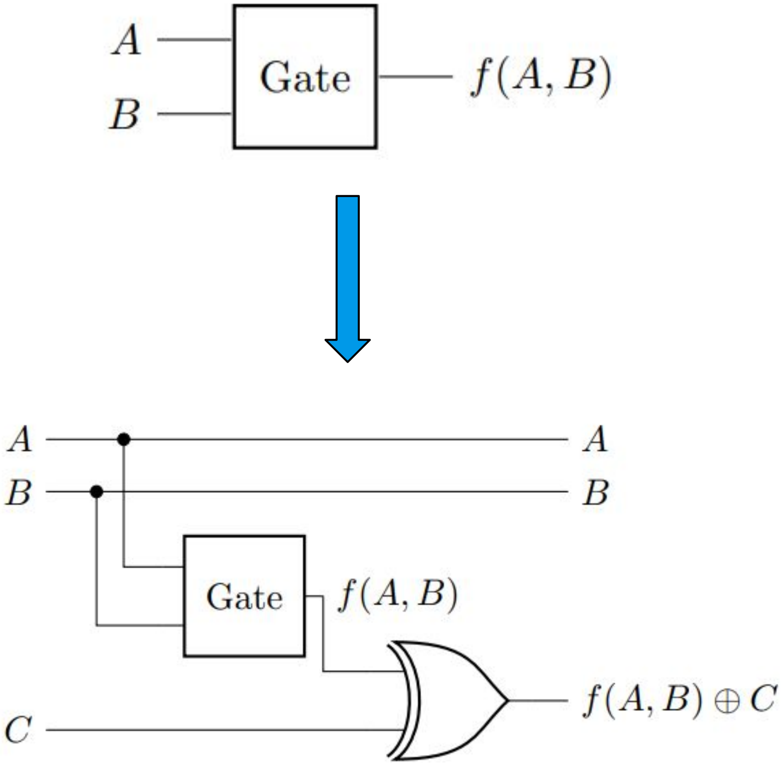
Chapters that will be presented are up to Chp-4

Difference between Classical and Quantum Computing

Concept	Classical	Quantum
Fundamental Unit	Bit	Qubit
Gates	Logic Gates	Unitary Gates
Gates Reversible	Sometimes	Always
Universal Gate Set (Example)	{NAND}	$\{H, T, \text{CNOT}\}$
Programming Language (Example)	Verilog	OpenQASM
Algebra	Boolean	Linear
Error Correcting Code (Example)	Repetition Code	Shor Code
Complexity Class	P	BQP
Strong Church-Turing Thesis	Supports	Possibly Violates

Making irreversible logic gates reversible

A	B	C	A	B	$f(A,B) \oplus C$
0	0	0	0	0	$f(0,0)$
0	0	1	0	0	$\overline{f(0,0)}$
0	1	0	0	1	$f(0,1)$
0	1	1	0	1	$\overline{f(0,1)}$
1	0	0	1	0	$f(1,0)$
1	0	1	1	0	$\overline{f(1,0)}$
1	1	0	1	1	$f(1,1)$
1	1	1	1	1	$\overline{f(1,1)}$



Error Correction

Codeword	$b_2 \oplus b_1$	$b_1 \oplus b_0$
000	0	0
001	0	1
010	1	1
011	1	0
100	1	0
101	1	1
110	0	1
111	0	0

Codeword - $b_2b_1b_0$
Determining the error bit

- If both parity bits are 0, the codeword is either 000 or 111, and there is no error.
- If the left parity bit is 0 and the right is 1, the rightmost bit was flipped.
- If the left parity bit is 1 and the second is 0, the left bit was flipped.
- If both parity bits are 1, the middle bit was flipped.

It is favorable to do error correction to a codeword with errors in its bits in case of a 3-bit codeword when the following holds true-

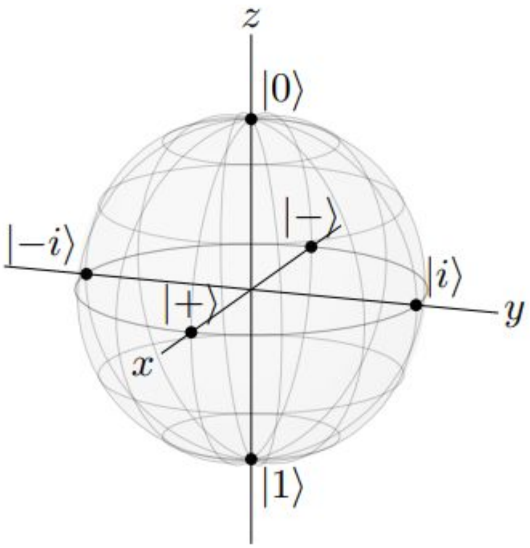
$$3p^2(1-p)+p^3 < p.$$

Where $3p^2(1-p)+p^3$ is the probability of an uncorrectable error occurring and p is the probability of an error occurring in bit.

On solving the above inequality, we get p less than 0.5.

Therefore, error correction is useful when p is less than 0.5 since there is a smaller chance that an uncorrectable error occurs.

Qubit - Measurement in Z, X and Y - bases



Bloch Sphere

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

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

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

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

Naming of Common Qubit States

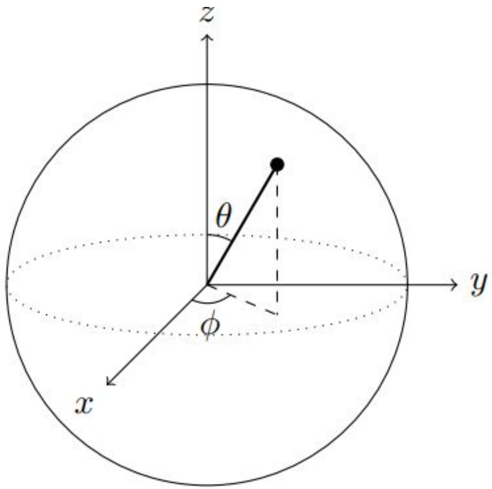
Measurement of a qubit can also be done with respect to any two states on opposite sides of the Bloch sphere.

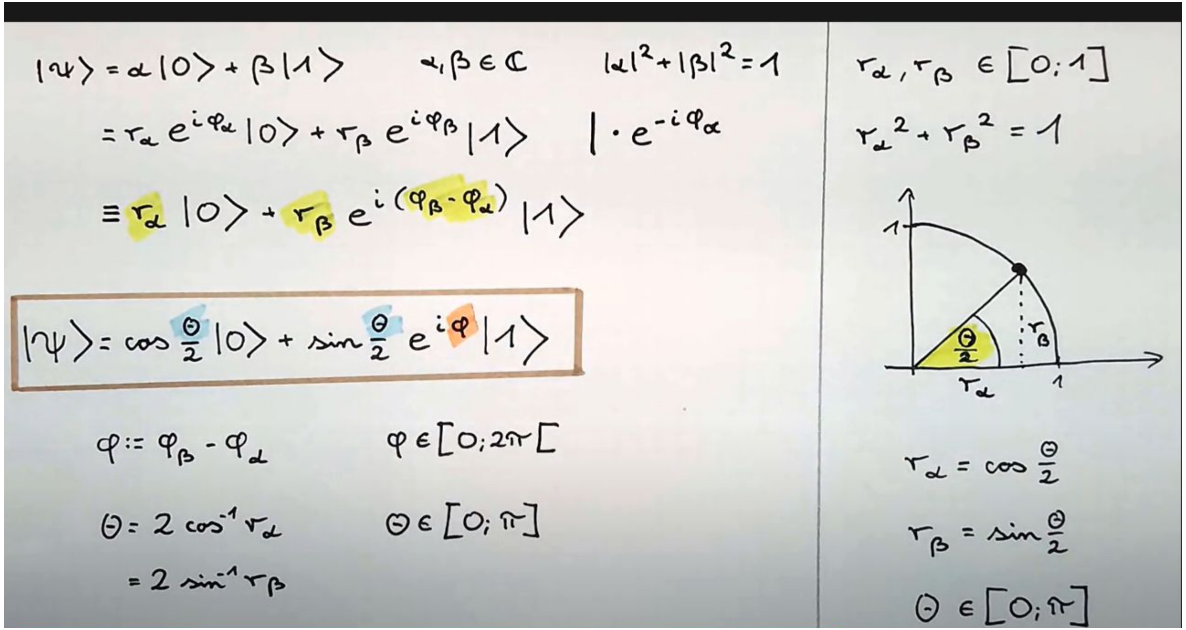
Z-basis $\{|0\rangle,|1\rangle\}$, the X-basis $\{|+\rangle,|-\rangle\}$, the Y-basis $\{|i\rangle,|-i\rangle\}$

Consecutive Measurements in two different bases does not affect the probability of each outcome remains the same. [Doubt]

Global phases are physically irrelevant since a qubit is a point on the bloch sphere and changing the global phases will point to the same qubit and does not affect the probability amplitude of each outcome.

Relative phases are significant since these correspond to different points on the Bloch sphere.





This corresponds to spherical coordinate system

Quantum Gates and Circuits

Quantum gates are linear maps that keep the total probability equal to 1 and are unitary matrices. Classical reversible logic gates can be quantum gates.

Single Qubit Quantum Gates are associated with rotations by some angle about some axis on the bloch sphere. Some common one-qubit quantum gates are *Identity(I), Pauli X gate, or NOT gate, Pauli Y gate* and *Pauli Z gate*.

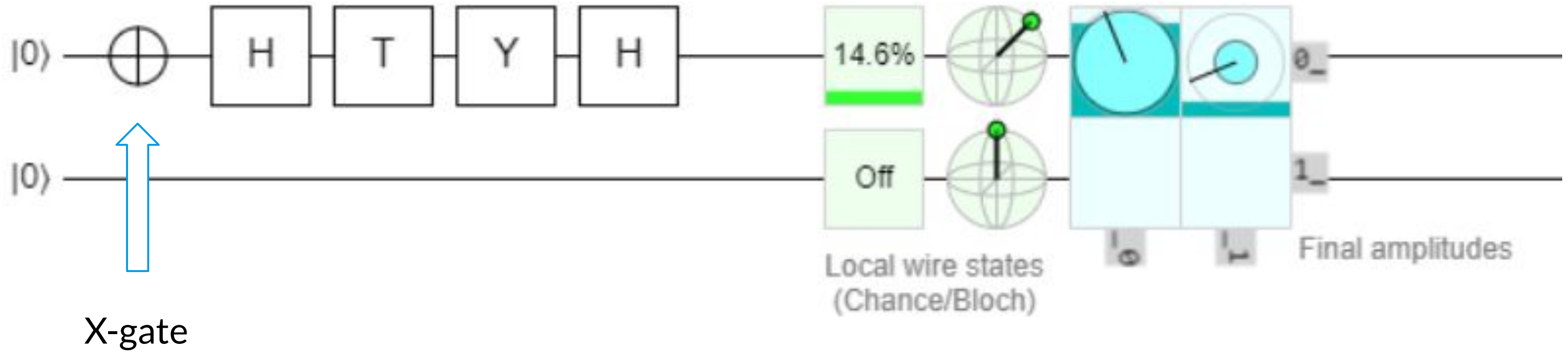
Phase Gates - rotate about some angle about Z-axis

$$R_z(\theta)|0\rangle = |0\rangle,$$
$$R_z(\theta)|1\rangle = e^{i\theta}|1\rangle.$$

Quantum Circuits are read from left-to-right and Quirk is a simulating software for Q-circuits.

Any one-qubit quantum state can be expressed in the following way-

$$U = e^{i\gamma}\left[\cos\left(\frac{\theta}{2}\right) I - i\sin\left(\frac{\theta}{2}\right)(n_x X + n_y Y + n_z Z)\right]$$



In Quirk, the default state is |0>. OFF signifies the default measurement of qubit collapsing to |1> which is zero.

Linear Algebra is the mathematical tool used to do the math of QC.

Inner product of two quantum states gives a scalar product and this can be used to find the probability amplitude associated with each outcome in different bases efficiently. If inner product is zero, it means the two vectors are orthogonal.

How to find the matrix of a quantum gate-

$$U|0\rangle = a|0\rangle + b|1\rangle = \begin{pmatrix} a \\ b \end{pmatrix},$$

$$U|1\rangle = c|0\rangle + d|1\rangle = \begin{pmatrix} c \\ d \end{pmatrix}.$$

$$\Longrightarrow \quad U = \left(\begin{pmatrix} a \\ b \end{pmatrix} \begin{pmatrix} c \\ d \end{pmatrix} \right) = \begin{pmatrix} a & c \\ b & d \end{pmatrix}.$$

Completeness Relation- indicates the state of qubit can be in terms of |a> and |b> of a bases and they are orthonormal to each other.

$$|\psi\rangle = |a\rangle \langle a|\psi\rangle + |b\rangle \langle b|\psi\rangle$$

$$|a\rangle\langle a| + |b\rangle\langle b| = I.$$

Common One-Qubit Quantum Gates

Gate	Action on Computational Basis	Matrix Representation
Identity	$I\|0\rangle = \|0\rangle$ $I\|1\rangle = \|1\rangle$	$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
Pauli X	$X\|0\rangle = \|1\rangle$ $X\|1\rangle = \|0\rangle$	$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
Pauli Y	$Y\|0\rangle = i\|1\rangle$ $Y\|1\rangle = -i\|0\rangle$	$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$
Pauli Z	$Z\|0\rangle = \|0\rangle$ $Z\|1\rangle = -\|1\rangle$	$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$
Phase S	$S\|0\rangle = \|0\rangle$ $S\|1\rangle = i\|1\rangle$	$S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$
T	$T\|0\rangle = \|0\rangle$ $T\|1\rangle = e^{i\pi/4}\|1\rangle$	$T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$
Hadamard H	$H\|0\rangle = \frac{1}{\sqrt{2}}(\|0\rangle + \|1\rangle)$ $H\|1\rangle = \frac{1}{\sqrt{2}}(\|0\rangle - \|1\rangle)$	$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

Doubts

How to plot this qubit on bloch sphere manually?

$$= \frac{1}{2}\left[\left(1+e^{i3\pi/4}\right)|0\rangle + \left(1-e^{i3\pi/4}\right)|1\rangle\right]$$

How is P different from NP?
P is the class of problems whose algorithms are found efficiently, NP- completeness- no solution found to these problems, NP - algorithms which are efficiently verified by a turing machine or computer.