

Introduction to Quantum Computing

A stack of five books with yellow, red, and blue spines is positioned on the right side of the image. To the left of the books is a black mesh pencil holder containing several colored pencils in shades of purple, yellow, and green. The background is a dark, out-of-focus chalkboard with some faint writing. A white circle is visible in the top right corner.

by
Kamonluk Suksen Ph.D.

Overview



From bits to qubits: Dirac notation, density matrices, measurement, Bloch sphere



Quantum circuits: basic single-qubit & two-qubit gates, multipartite quantum states

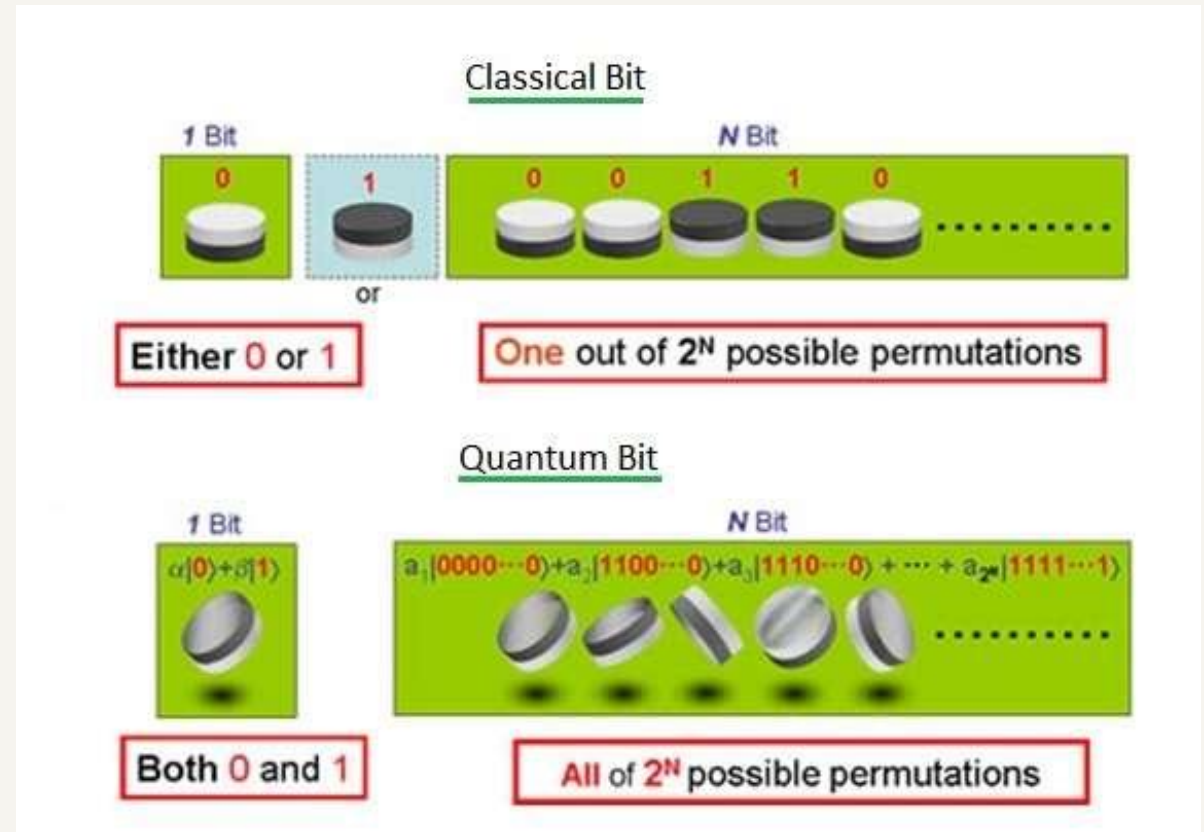


Entanglement: Bell states, Teleportation, Superdense coding



Quantum algorithms: Deutsch-Jozsa algorithm, Grover's algorithm

From bits to qubits



- Superpositions allow to perform calculations on many states at the same time.
 - Quantum algorithms with **exponential speed-up**.
- But: Once we measure the superposition state, it collapse to one of its states.
- We can use **interference effects** to keep the right answer.

Dirac notation & density matrices

- It used to describe quantum states: Let a, b are 2-dimensional vector with complex entries.

➤ ket: $|a\rangle = \begin{pmatrix} a_0 \\ a_1 \end{pmatrix}$

➤ bra: $\langle b| = |b\rangle^+ = \begin{pmatrix} b_0 \\ b_1 \end{pmatrix}^+ = (b_0^* \ b_1^*)$

➤ bra-ket: $\langle b|a\rangle = a_0 b_0^* + a_1 b_1^* = \langle a|b\rangle^* \in \mathbb{C}$ (inner product)

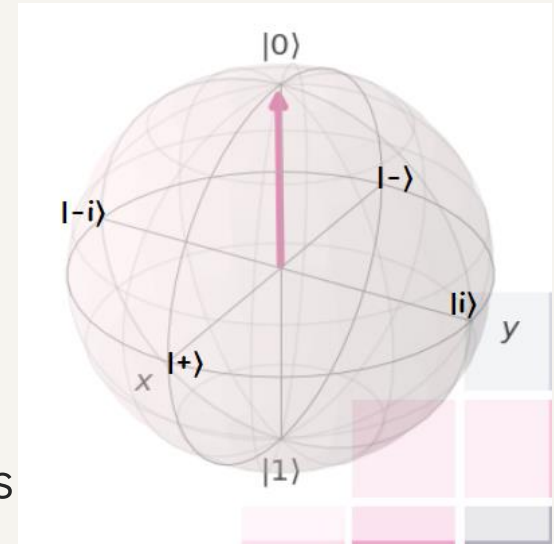
➤ ket-bra: $|a\rangle\langle b| = \begin{pmatrix} a_0 b_0^* & a_0 b_1^* \\ a_1 b_0^* & a_1 b_1^* \end{pmatrix}$ (2x2 matrix)

Dirac notation & density matrices

- The pure states are $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$, which are orthogonal: $\langle 0|1\rangle = 1 \cdot 0 + 0 \cdot 1 = 0$
- $|0\rangle\langle 0| = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, $|1\rangle\langle 1| = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$
- $P = \begin{pmatrix} P_{00} & P_{01} \\ P_{10} & P_{11} \end{pmatrix} = P_{00}|0\rangle\langle 0| + P_{01}|0\rangle\langle 1| + P_{10}|1\rangle\langle 0| + P_{11}|1\rangle\langle 1|$
- All quantum states can be described by density matrices.
- All quantum states are normalized, i.e., $\langle \psi|\psi\rangle = 1$, e.g., $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix}$
- A density matrix is pure, if $P = |\psi\rangle\langle\psi|$, otherwise it is mixed.
 - $P = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = |0\rangle\langle 0| \rightarrow \text{Pure}$, $P = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = |1\rangle\langle 1| \rightarrow \text{Pure}$
 - $P = \frac{1}{2} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|) \rightarrow \text{Mixed}$
 - $P = \frac{1}{2} \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} = \frac{1}{2}(|0\rangle\langle 0| - |0\rangle\langle 1| - |1\rangle\langle 0| + |1\rangle\langle 1|) = \frac{1}{2}(|0\rangle - |1\rangle)(\langle 0| - \langle 1|) \rightarrow \text{Pure}$

Measurement

- We choose orthogonal base to describe and measure quantum states (projective measurement).
- During a measurement onto the basis $\{|0\rangle, |1\rangle\}$, the states will collapse into either state $|0\rangle$ or $|1\rangle$, as those are the eigenstates of σ_z , we call this a Z-measurement.
- Other different bases are:
 - $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, corresponding to the eigenstates of σ_x ,
 - $|+i\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)$, $|-i\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)$, corresponding to the eigenstates of σ_y .



Measurement

- **Born rule:** the probability that a state $|\psi\rangle$ collapses during a project measurement onto the basis $\{|X\rangle, |X^\perp\rangle\}$ to the state $|X\rangle$ is given by $P(X) = |\langle X|\psi\rangle|^2$, $\sum_i P(X_i) = 1$

- Examples:

➤ $|\psi\rangle = \frac{1}{\sqrt{3}}(|0\rangle + \sqrt{2}|1\rangle)$ is measured in the basis $\{|0\rangle, |1\rangle\}$:

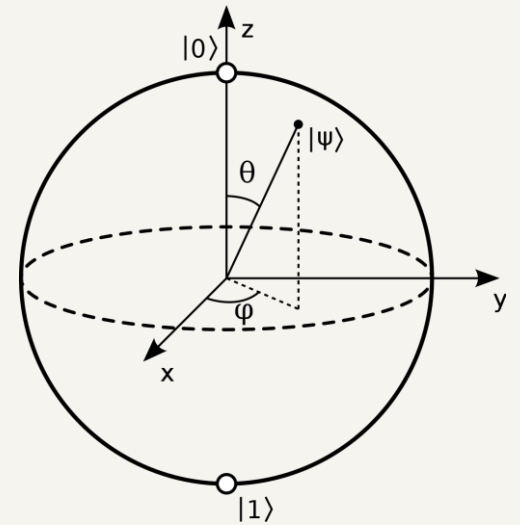
$$P(0) = \left\langle 0 \left| \frac{1}{\sqrt{3}}(|0\rangle + \sqrt{2}|1\rangle) \right. \right\rangle^2 = \left| \frac{1}{\sqrt{3}}\langle 0|0\rangle + \frac{\sqrt{2}}{\sqrt{3}}\langle 0|1\rangle \right|^2 = \frac{1}{3} \rightarrow P(1) = \frac{2}{3}$$

➤ $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ is measured in the basis $\{|+\rangle, |-\rangle\}$:

$$P(+)=|\langle +|\psi\rangle|^2=\left|\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)\right|^2=\frac{1}{4}|(\langle 0|0\rangle-\langle 0|1\rangle+\langle 1|0\rangle-\langle 1|1\rangle)|^2=0\rightarrow\text{expected as }\langle +|-\rangle=0,$$

$$P(-)=|\langle -|\psi\rangle|^2=1$$

Bloch sphere

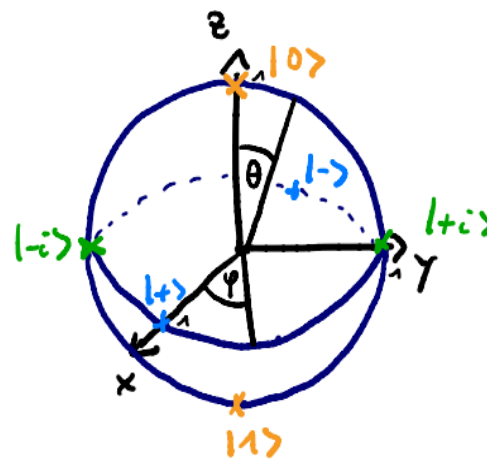


- We can write any normalized **pure state** as $|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle$, where $\varphi \in [0, 2\pi]$ describes the relative phase and $\theta \in [0, \pi]$ determines the probability to measure $|0\rangle, |1\rangle$:
 $P(|0\rangle) = \cos^2\frac{\theta}{2}$, $P(|1\rangle) = \sin^2\frac{\theta}{2}$.
- All normalized pure states can be illustrated on the surface of a sphere with radius $|\vec{r}| = 1$, which we call the **Bloch sphere**.
- The coordinates of such a state are given by the Bloch vector: $\vec{r} = \begin{pmatrix} \sin\theta \cos\varphi \\ \sin\theta \sin\varphi \\ \cos\theta \end{pmatrix}$

Bloch sphere

examples:

- $|0\rangle$: $\theta=0$, φ arbitrary $\rightarrow \vec{r} = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$
- $|1\rangle$: $\theta=\pi$, φ arb. $\rightarrow \vec{r} = \begin{pmatrix} 0 \\ 0 \\ -1 \end{pmatrix}$
- $|+\rangle$: $\theta=\frac{\pi}{2}$, $\varphi=0$ $\rightarrow \vec{r} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$
- $|-\rangle$: $\theta=\frac{\pi}{2}$, $\varphi=\pi$ $\rightarrow \vec{r} = \begin{pmatrix} -1 \\ 0 \\ 0 \end{pmatrix}$
- $|+i\rangle$: $\theta=\frac{\pi}{2}$, $\varphi=\frac{\pi}{2}$ $\rightarrow \vec{r} = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$
- $| -i\rangle$: $\theta=\frac{\pi}{2}$, $\varphi=\frac{3\pi}{2}$ $\rightarrow \vec{r} = \begin{pmatrix} 0 \\ -1 \\ 0 \end{pmatrix}$



- **Be careful:** On the Bloch sphere, angles are twice as big as in Hilbert space:
 - e.g., $|0\rangle$ & $|1\rangle$ are orthogonal, but on the Bloch sphere their angle is 180° .
 - For a general state, $|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + \dots \rightarrow \theta$ is the angle on the Bloch sphere, while $\frac{\theta}{2}$ is the actual angle in Hilbert space!

Quantum circuits: single qubit gates

- **Circuit model:** sequence of building block that carry out computations, called **gates**.

input ——— algorithm ——— output

- **Quantum gates** are represented by unitary matrices, A unitary matrix is a square matrix of complex numbers, whose inverse is equal to its conjugate transpose.

- **Single qubit gates:**

	Hadamard	$\text{---} \boxed{H} \text{---}$	$\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$	← creates superposition
rotation around X-axis by π	→ Pauli-X	$\text{---} \boxed{X} \text{---}$	$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$	← bit flip
rotation around Y-axis by π	→ Pauli-Y	$\text{---} \boxed{Y} \text{---}$	$\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$	← bit & phase flip
rotation around Z-axis by π	→ Pauli-Z	$\text{---} \boxed{Z} \text{---}$	$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$	← phase flip
	Phase	$\text{---} \boxed{S} \text{---}$	$\begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$	← used to change from Z to Y-basis
	$\pi/8$	$\text{---} \boxed{T} \text{---}$	$\begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$	

Quantum circuits: single qubit gates

- $\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = |0\rangle\langle 1| + |1\rangle\langle 0|$

$\hookrightarrow \sigma_x |0\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle$, $\sigma_x |1\rangle = (|0\rangle\langle 1| + |1\rangle\langle 0|) \cdot |1\rangle = \underbrace{|0\rangle\langle 1|1\rangle}_1 + \underbrace{|1\rangle\langle 0|1\rangle}_0 = |0\rangle$

- $\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = |0\rangle\langle 0| - |1\rangle\langle 1|$



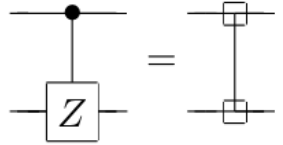
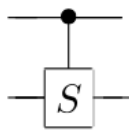
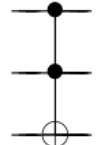
$\hookrightarrow \sigma_z |+\rangle = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \cdot \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} = |-\rangle$, $\sigma_z |-\rangle = (|0\rangle\langle 0| - |1\rangle\langle 1|) \cdot \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) = \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) = |+\rangle$

- Hadamard gate: one of the most important gates for quantum circuits

$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{1}{\sqrt{2}} (|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| - |1\rangle\langle 1|)$

$\hookrightarrow H|0\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = |+\rangle$, $H|1\rangle = \frac{1}{\sqrt{2}} (|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| - |1\rangle\langle 1|) \cdot |1\rangle = \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) = |-\rangle$

Quantum circuits: multiple-qubit gates

controlled-NOT		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$
swap		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$
controlled-Z		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$
controlled-phase		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & i \end{bmatrix}$
Toffoli		$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$

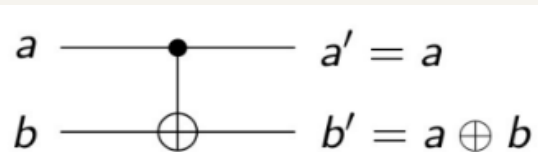
Quantum circuits: two-qubit gates

- Classical example: XOR



irreversible: given the output, we cannot recover the input.

- But as quantum theory is unitary, we only consider unitary and therefore reversible gates
- Quantum example: CNOT gate



a	b	a'	b'
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0

Quantum circuits can perform all function that can be calculated classically.

Quantum circuits: multipartite quantum states

- We use tensor product to describe multiple states:

$$\text{➤ } |a\rangle \otimes |b\rangle = \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} \otimes \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} = \begin{pmatrix} a_1 b_1 \\ a_1 b_2 \\ a_2 b_1 \\ a_2 b_2 \end{pmatrix}$$

- Example: system A is in state $|1\rangle_A$ and system B is in state $|0\rangle_B = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$, states of this form

are called **uncorrelated**.

- But there are also bipartite states that cannot be written as $|\psi\rangle_a \otimes |\psi\rangle_b$. These states are **correlated** and sometimes even entangled (very strong correlation), e.g. $|\psi\rangle_{AB}^{(00)} = \frac{1}{\sqrt{2}} (|00\rangle_{AB} + |11\rangle_{AB}) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$,

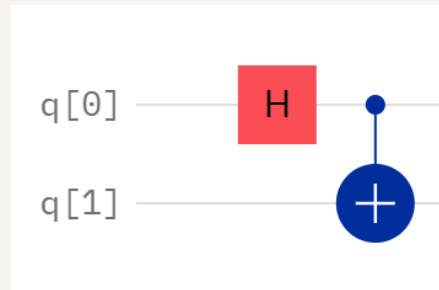
it so called Bell state, used for teleportation, cryptography, Bell tests, etc.

Entanglement

- If a pure state $|\psi\rangle_{AB}$ on system A,B cannot be written as $|\psi\rangle_a \otimes |\phi\rangle_b$, it is entangled.
- These are four so called **Bell states** that are maximally entangled and build on orthonormal basis:
 - $|\psi^{00}\rangle := \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle),$
 - $|\psi^{01}\rangle := \frac{1}{\sqrt{2}} (|01\rangle + |10\rangle),$
 - $|\psi^{10}\rangle := \frac{1}{\sqrt{2}} (|00\rangle - |11\rangle),$
 - $|\psi^{11}\rangle := \frac{1}{\sqrt{2}} (|01\rangle - |10\rangle).$

Entanglement

- Creation of Bell states:



$$|q_0q_1\rangle_{00} H_0 \rightarrow \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) CNOT_{01} \rightarrow \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = |\psi^{00}\rangle,$$

$$|q_0q_1\rangle_{01} H_0 \rightarrow \frac{1}{\sqrt{2}}(|01\rangle + |11\rangle) CNOT_{01} \rightarrow \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) = |\psi^{01}\rangle,$$

$$|q_0q_1\rangle_{10} H_0 \rightarrow \frac{1}{\sqrt{2}}(|00\rangle - |10\rangle) CNOT_{01} \rightarrow \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) = |\psi^{10}\rangle,$$

$$|q_0q_1\rangle_{11} H_0 \rightarrow \frac{1}{\sqrt{2}}(|01\rangle - |11\rangle) CNOT_{01} \rightarrow \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) = |\psi^{11}\rangle.$$

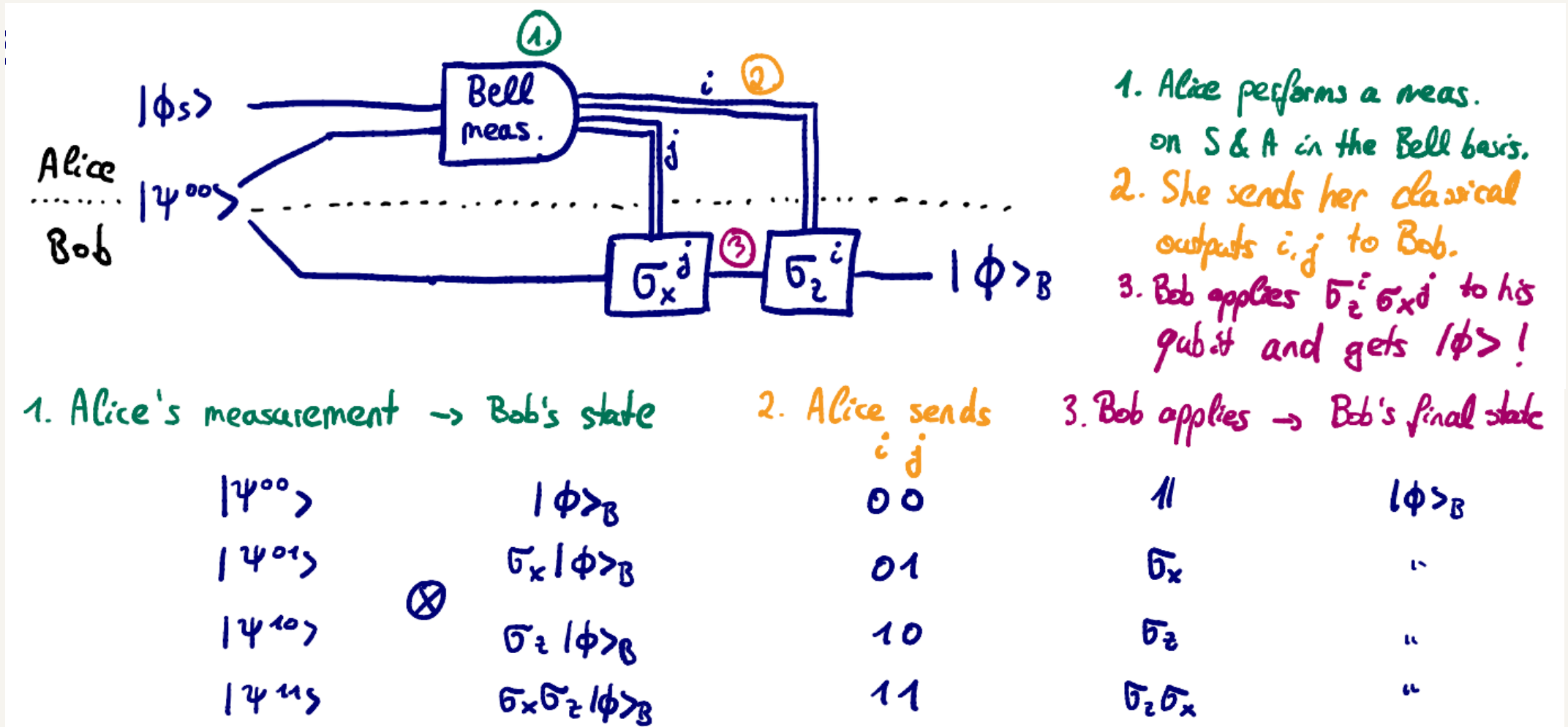
Teleportation

- Goal:
 - Alice want to send her (unknown) state $|\phi\rangle_s := \alpha|0\rangle_s + \beta|1\rangle_s$ to Bob.
 - She can only send him two classical bits though.
 - They both share the maximally entangled state $|\psi\rangle_{AB}^{(00)} = \frac{1}{\sqrt{2}}(|00\rangle_{AB} + |11\rangle_{AB})$.
- Initial states of the total system:

$$\begin{aligned}
 |\phi\rangle_s \otimes |\psi^{00}\rangle_{AB} &= \frac{1}{\sqrt{2}} (\alpha|000\rangle_{SAB} + \alpha|011\rangle_{SAB} + \beta|100\rangle_{SAB} + \beta|111\rangle_{SAB}) \\
 &= \frac{1}{2\sqrt{2}} [(|00\rangle_{SA} + |11\rangle_{SA}) \otimes (\alpha|0\rangle_B + \beta|1\rangle_B) + (|01\rangle_{SA} + |10\rangle_{SA}) \otimes (\alpha|1\rangle_B + \beta|0\rangle_B) \\
 &\quad + (|00\rangle_{SA} - |11\rangle_{SA}) \otimes (\alpha|0\rangle_B - \beta|1\rangle_B) + (|01\rangle_{SA} - |10\rangle_{SA}) \otimes (\alpha|1\rangle_B - \beta|0\rangle_B)] \\
 &= \frac{1}{2} [|\psi^{00}\rangle_{SA} \otimes |\phi\rangle_B + |\psi^{01}\rangle_{SA} \otimes (\sigma_x |\phi\rangle_B) \\
 &\quad + |\psi^{10}\rangle_{SA} \otimes (\sigma_z |\phi\rangle_B) + |\psi^{11}\rangle_{SA} \otimes (\sigma_x \sigma_z |\phi\rangle_B)]
 \end{aligned}$$

Teleportation

- Protocol:



- Alice's state collapsed during the measurement, so she doesn't have the initial state $|\phi\rangle_S$ anymore. This is expected due to the no-cloning theorem, as she cannot copy her state, but just send her state to Bob when destroying her own.

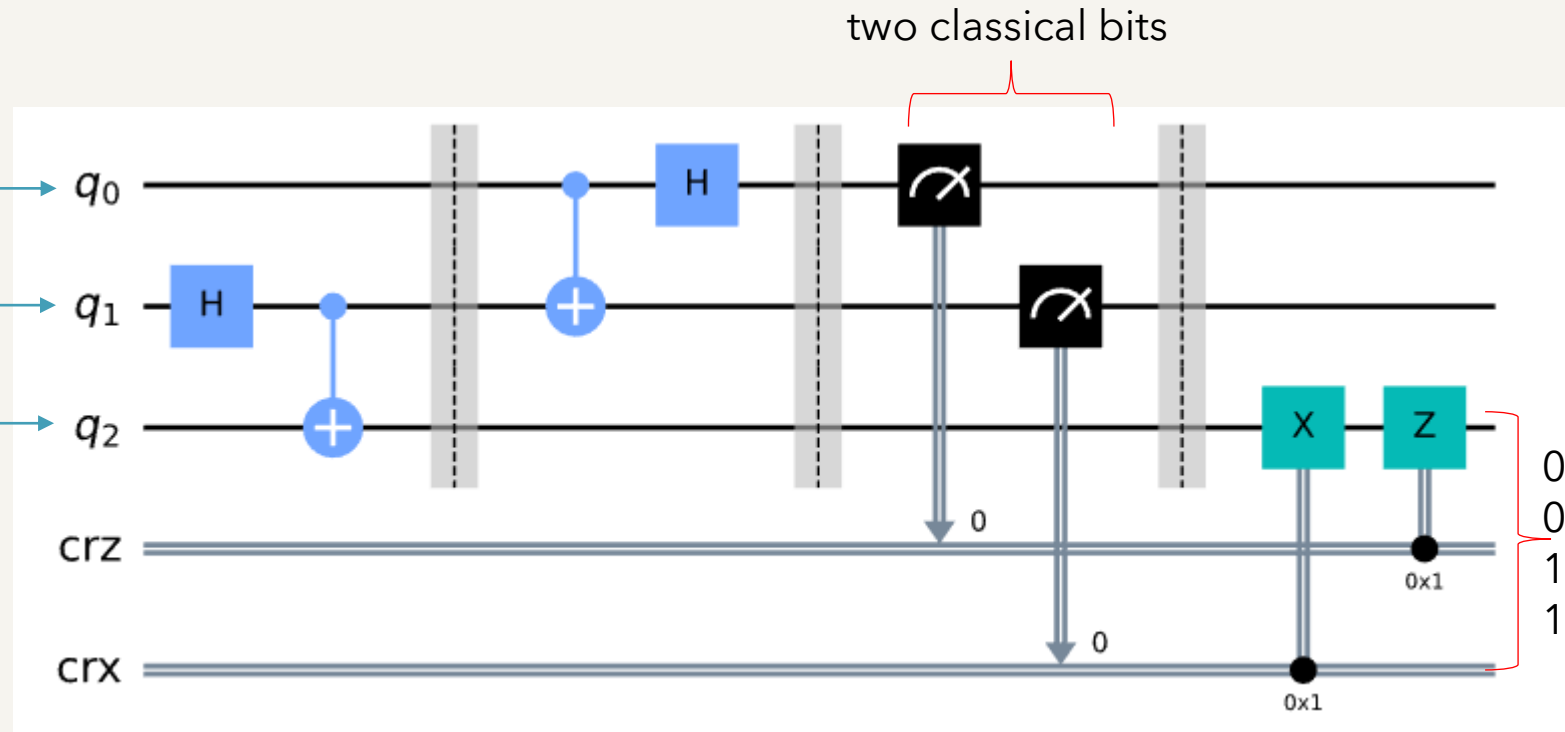
Teleportation

- Quantum circuit:

The qubit she is trying to send Bob.

Alice's qubit

Bob's qubit



00 → Do nothing
01 → Apply X gate
10 → Apply Z gate
11 → Apply ZX gate

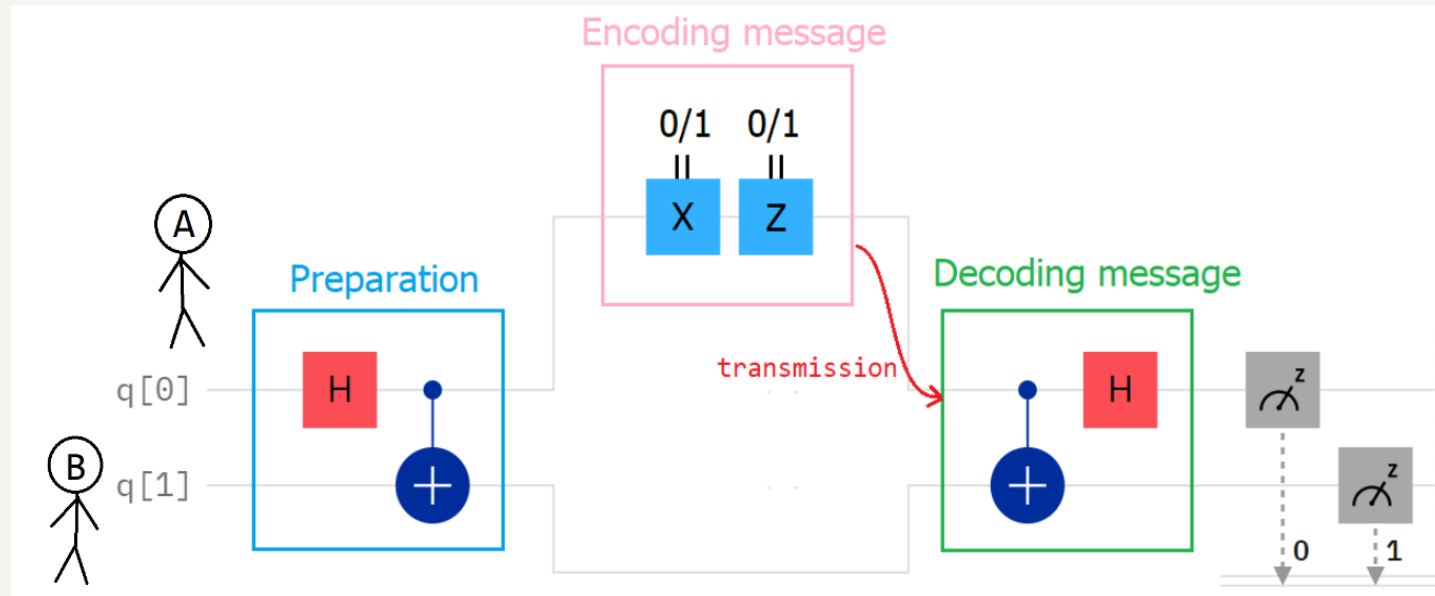
Superdense coding

- Superdense coding is a procedure that allows someone to send two classical bits to another party using just a single qubit of communication.
- Take advantage of quantum mechanics to more efficiently transmit classical information.
- Word “coding” means there are 2 essential processes, encoding and decoding:
 - encoding: classical state \rightarrow quantum state,
 - decoding: quantum state \rightarrow classical state.

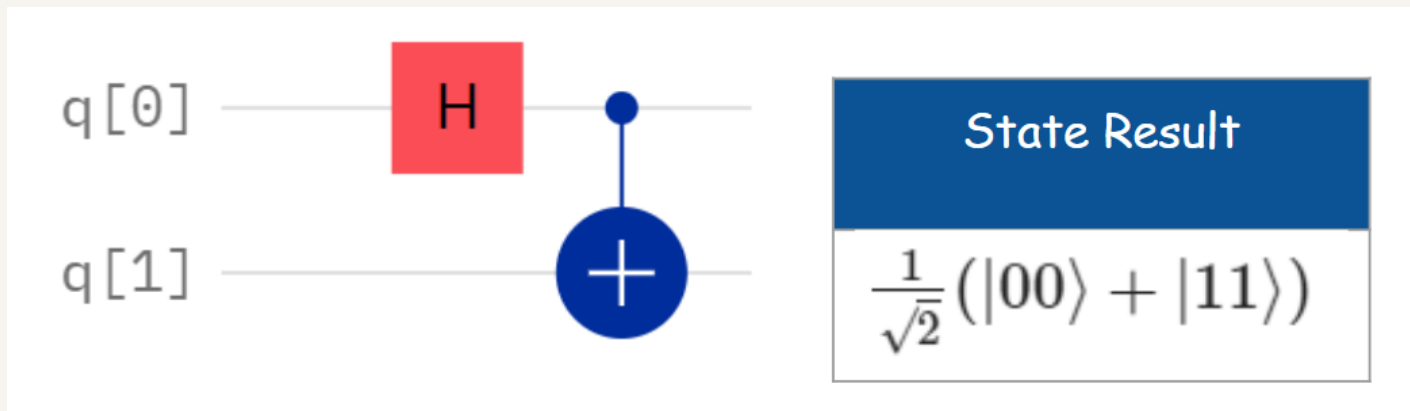
Teleportation	Superdense Coding
Transmit one qubit using two classical bits .	Transmit two classical bits using one qubit .

Superdense coding

- Superdense coding includes 4 steps:
 - preparation,
 - encoding message,
 - transmission,
 - decoding message.



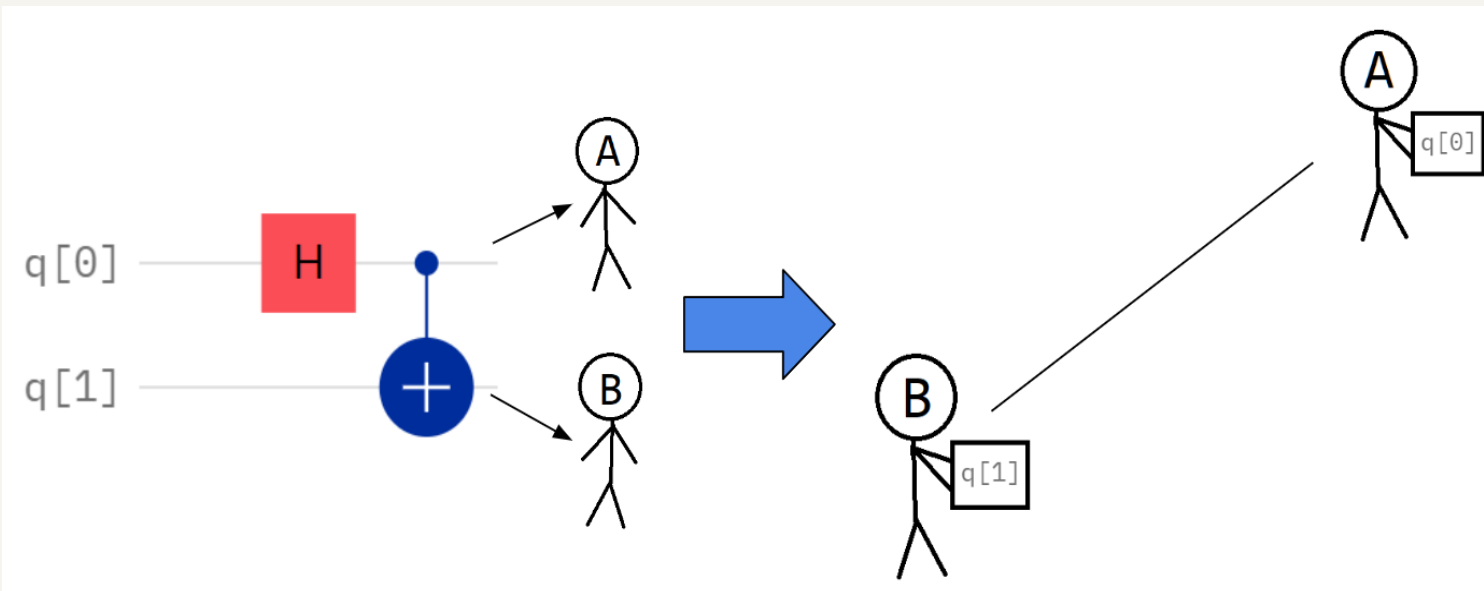
Superdense coding



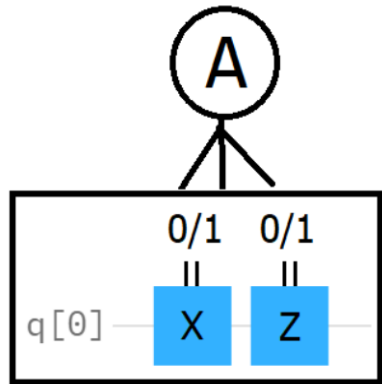
- Step 1: preparation
 - Start with 2 qubits in the basis state $|0\rangle$.
 - Applying Hadamard gate to the first qubit and CNOT gate (the first qubit as control, another qubit as target) accordingly.

Superdense coding

- Step 1: preparation
 - Give the first qubit to A and the second qubit to B.
 - A and B travel far away.



Superdense coding



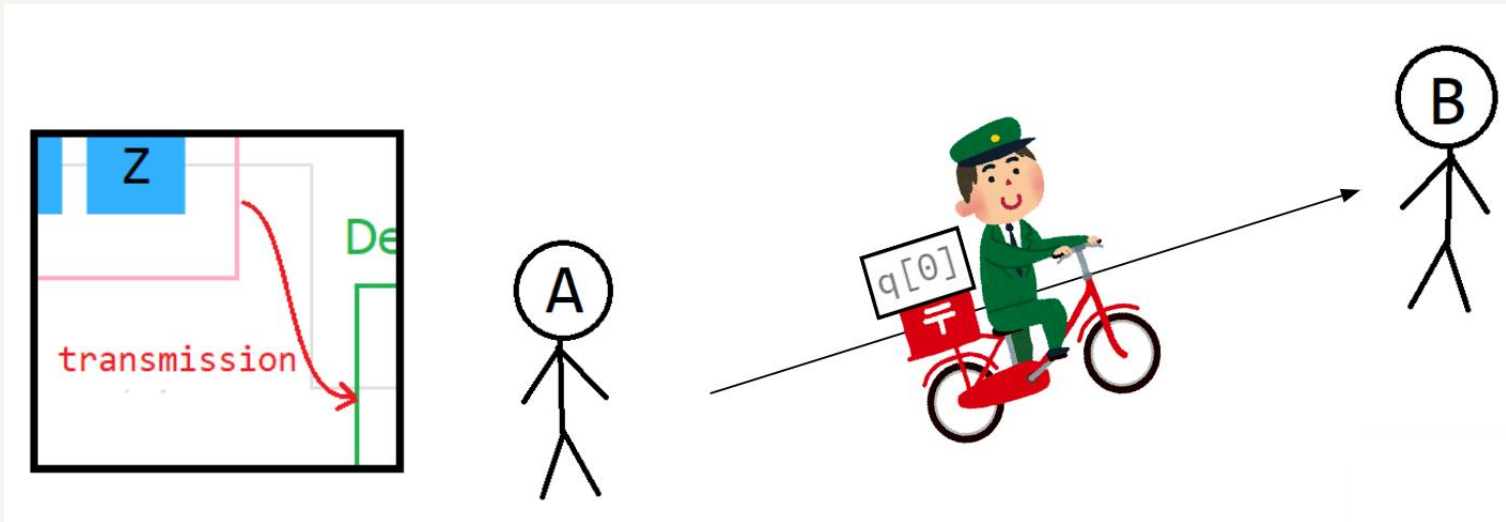
Message	Applied Gate	State Result
00	I	$\frac{1}{\sqrt{2}}(00\rangle + 11\rangle)$
01	X	$\frac{1}{\sqrt{2}}(10\rangle + 01\rangle)$
10	Z	$\frac{1}{\sqrt{2}}(00\rangle - 11\rangle)$
11	ZX	$\frac{1}{\sqrt{2}}(10\rangle - 01\rangle)$

- Step 2: encoding message
 - A encodes the classical state in the qubit by applying gate(s).

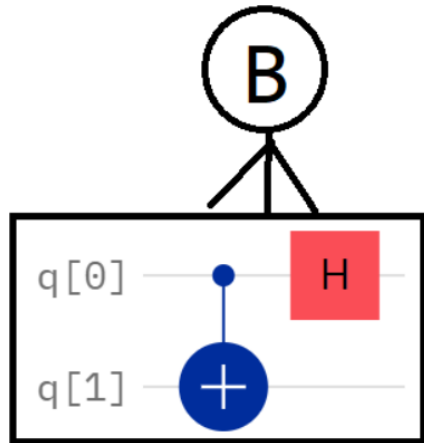
Message	Applied Gate
00	
01	X
10	Z
11	X Z

Superdense coding

- Step 3: transmission
 - A sends the first qubit to B.



Superdense coding

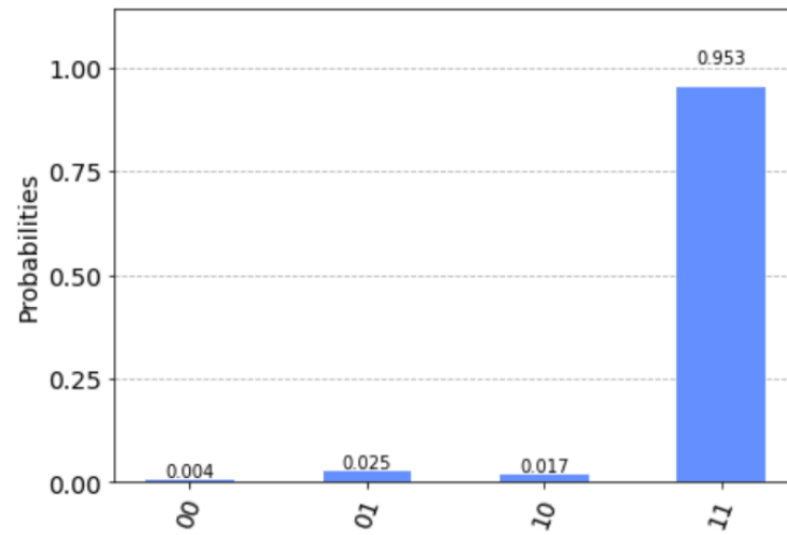
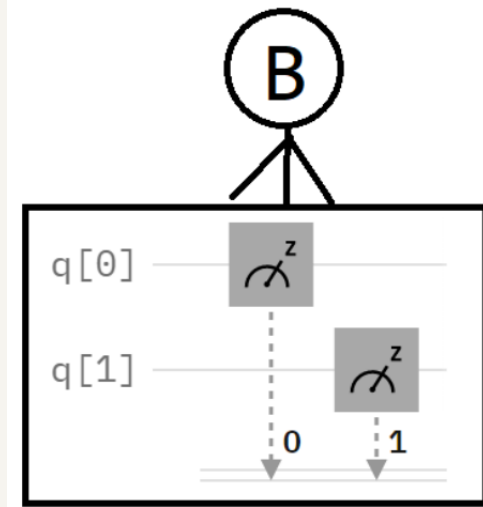


Message	State Result
00	$ 00\rangle$
01	$ 01\rangle$
10	$ 10\rangle$
11	$ 11\rangle$

- Step 4: decoding message
 - Applying CNOT gate (the first qubit as control, another qubit as target) and Hadamard gate to the first qubit accordingly.

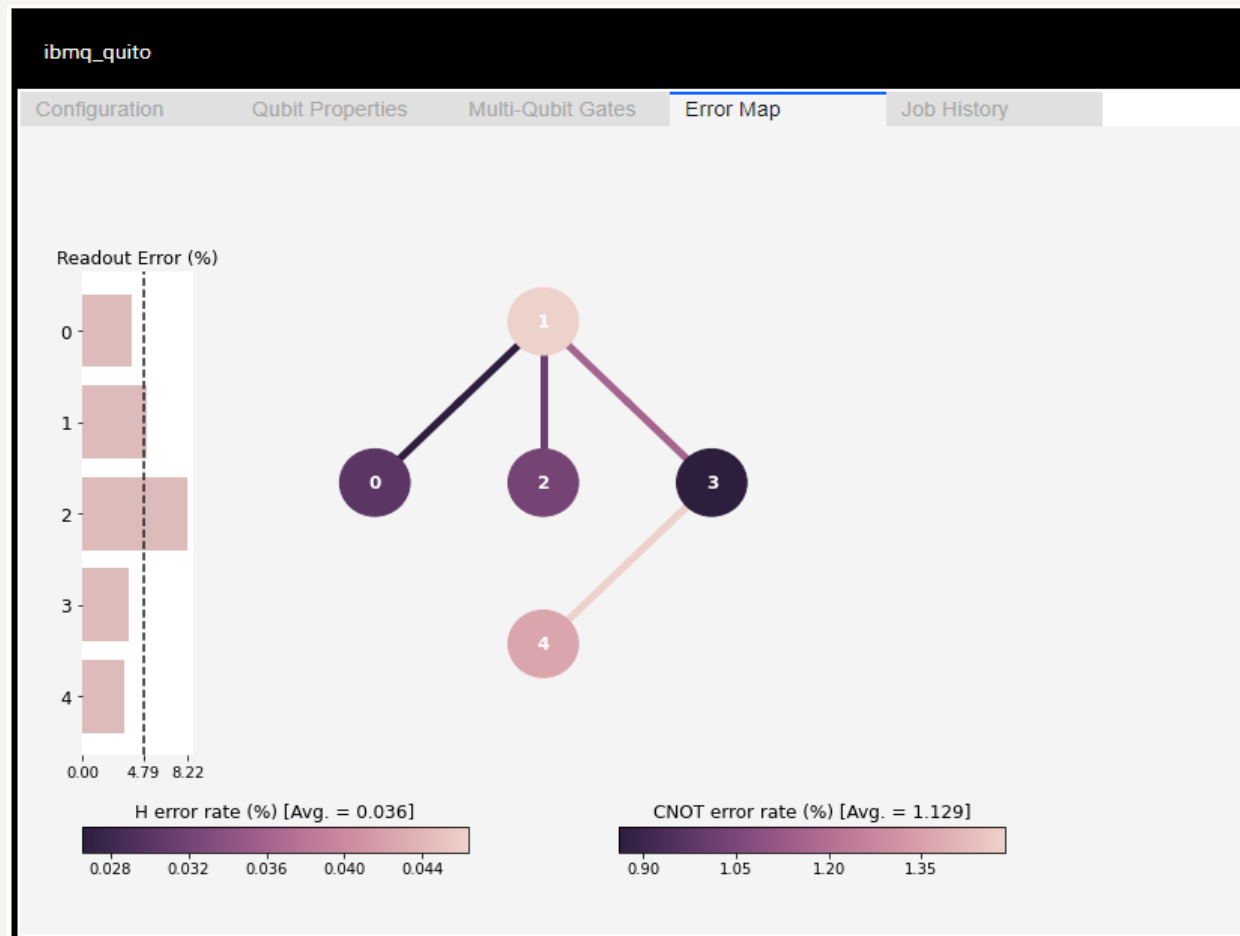
Superdense coding

Test the circuit which encodes message "11" and run on "ibm_oslo".



- Step 4: decoding message
 - Finally, measure both qubits.

How the noise properties affect the result



- There are often optimizations that the transpiler can perform that reduce the overall gate count, and thus total length of the input circuits.
- Qiskit library has a command "backend" to show the chosen backend information graphically such as "Error Map".
- We can select a good initial layout considering connectivity and error information that you can find from the map to initial layout onto the physical qubits with at least noise.

Assignment I: Basic Quantum Computing

- Required:
 - Go to <https://quantum-computing.ibm.com/>
 - Register IBMid account or sign in with Google, Github, LinkedIn, or Twitter.
 - Download source codes at [Assignment](#) and upload files "**Lab-1.ipynb**", "**Lab-2.ipynb**" and "**Lab-3.ipynb**" into IBM Quantum Lab.
- Assignments:
 - Lab-1: Operations on single qubit and multiple qubits gates by IBM Quantum.
 - Lab-2: Quantum circuits by IBM Quantum.
 - Lab-3: Superdense coding.

Quantum algorithms

- Deutsch-Jozsa algorithm

- We are given a hidden Boolean function f , which takes as input a string of bits, and returns either 0 or 1, that is:

$$f(\{x_0, x_1, x_2, \dots\}) \rightarrow 0 \text{ or } 1, \text{ where } x_n \text{ is } 0 \text{ or } 1$$

- The property of the given Boolean function is that it is guaranteed to either be balanced (returns 1 for half of the input domain and 0 for the other half) or constant (0 on all inputs or 1 on all inputs).
- Our task is to determine whether the given function is balanced or constant.

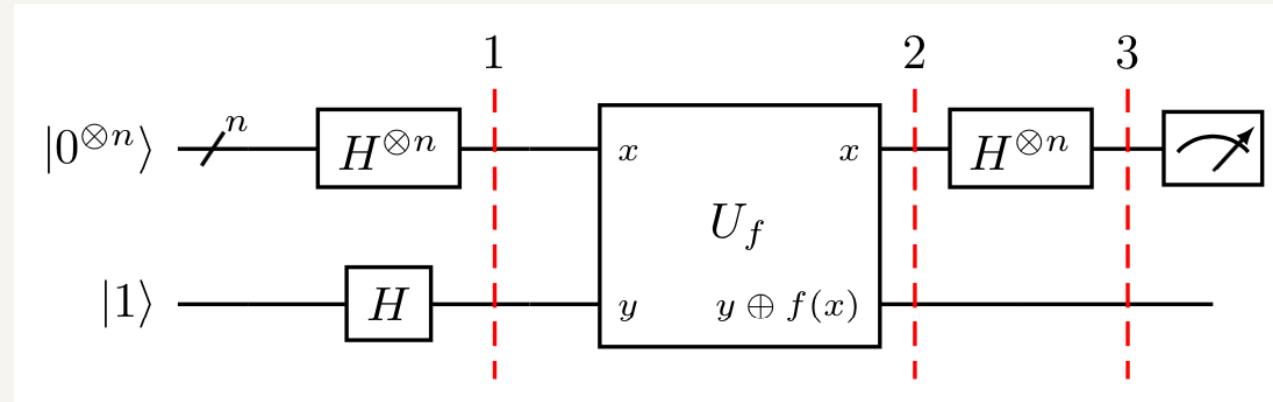
Quantum algorithms

- Deutsch-Jozsa algorithm

- For classical solution, we need to ask the oracle at least twice, but if we get twice the same output, we need to ask again. At most to query is $(N/2)+1$, where N is number of state.
- For quantum solution, need only one query. If the output is **the zero bit string**, we know that the oracle is **constant**. If it is **any other bit string**, we know that it is **balanced**.
- We have the function f implemented as a quantum oracle, which maps the state $|x\rangle|y\rangle$ to $|x\rangle|y\oplus f(x)\rangle$, where \oplus is addition modulo 2.

Quantum algorithms

- Deutsch-Jozsa algorithm



- The initial state of which can be expressed:

$$|\psi_0\rangle = |0\rangle^{\otimes n} |1\rangle$$

- which is then put into superposition, which can conveniently be expressed:

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

Quantum algorithms

- Deutsch-Jozsa algorithm

- Apply the quantum oracle $|x\rangle|y\rangle$ to $|x\rangle|y\oplus f(x)\rangle$:

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

- We now address the interference H on the first n wires, for which we use the expression:

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

- which allows us to express:

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

- where $x \cdot z = x_0 z_0 \oplus x_1 z_1 \oplus \dots \oplus x_{n-1} z_{n-1}$ is the sum of the bitwise product.

Quantum algorithms

- Deutsch-Jozsa algorithm

- We can now determine whether the function is constant or balanced by measuring the first n qubits of the final state.

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

- Specifically, we consider the probability of measuring zero on every qubit, which corresponds to the term in the superposition where $|x\rangle$ is $|0\rangle^{\otimes n}$

- In the case where the function is constant, then the co-efficient of $|0\rangle^{\otimes n}$, $\sum_x (-1)^{f(x)} / 2^n$ is equal to ± 1 ... as this has amplitude 1, then we measure $|0\rangle^{\otimes n}$ with probability one.
- In the case where the function is balanced then $\sum_x (-1)^{f(x)} / 2^n = 0$, and so we will never measure $|0\rangle^{\otimes n}$.

- So it follows that measuring the first n qubits allows us to determine with certainty whether the function is **constant (measure all zeros)** or **balanced (measure at least one 1)**.

Quantum algorithms

- **Deutsch-Jozsa algorithm**

- We can encode any mathematical function as a unitary matrix.
- Deutsch's algorithm was the first algorithm that demonstrated a quantum advantage: specifically, a reduction in query complexity compared to the classical case.
- The Deutsch-Jozsa algorithm generalises Deutsch's algorithm and reveals the possibility of exponential speed-ups using quantum computers.

Quantum algorithms

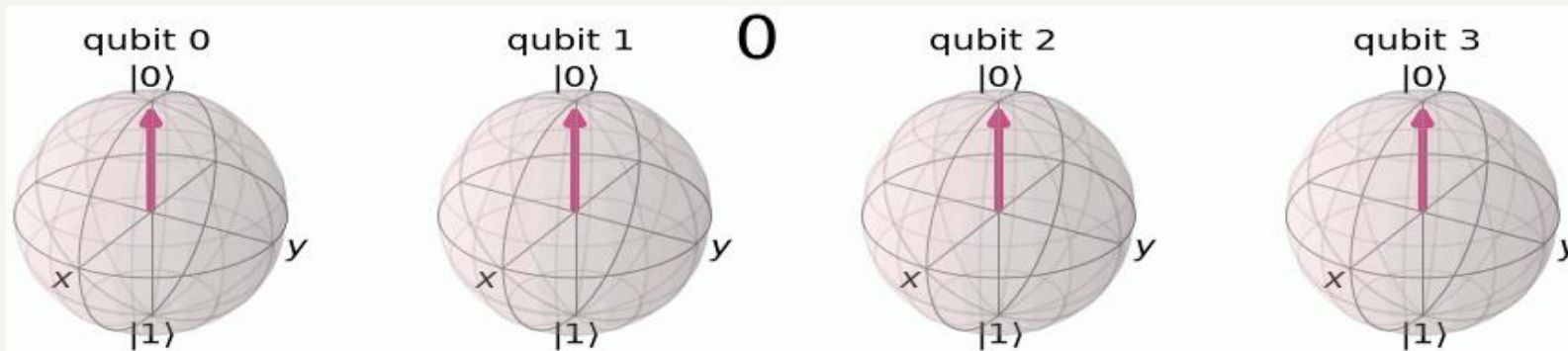
- **Quantum Fourier Transform (QFT)**

- The QFT is the quantum implementation of the discrete Fourier transform over the amplitudes of a wavefunction.
- The QFT simply transforms a qubit from its computational basis of $|0\rangle$ and $|1\rangle$ to the state in Fourier basis $|+\rangle$ and $|-\rangle$.

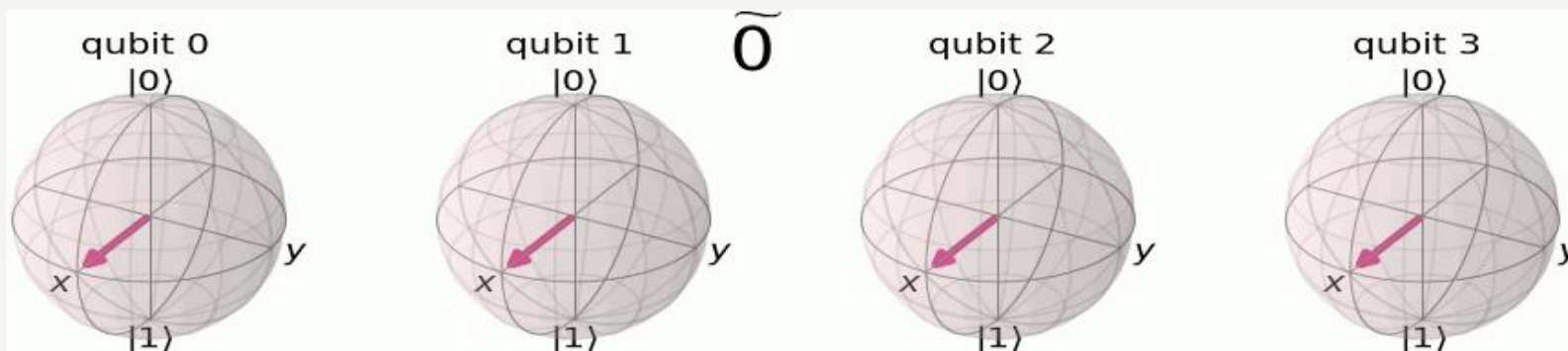
Quantum algorithms

- **Quantum Fourier Transform (QFT)**

- Computational basis:



- Fourier basis:



Try it out at [AssignmentII](#) and upload files "**quantum_fourier_transform.ipynb**" into IBM Quantum Lab.

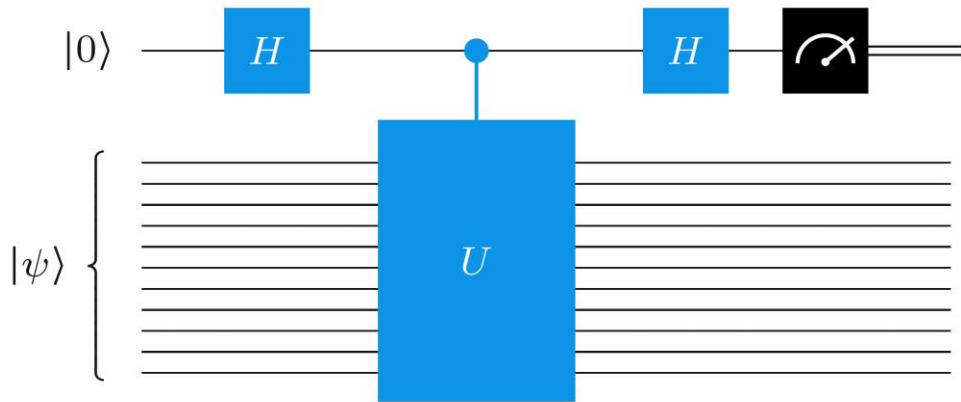
Quantum algorithms

- **Quantum Phase Estimation (QPE)**

- QPE aims to estimate the phase θ associated with an eigenvalue $e^{2\pi i\theta}$ of a unitary operator U .
- The quantum phase estimation algorithm uses phase kickback to write the phase of U , in the Fourier basis, to the t qubits in the counting register.

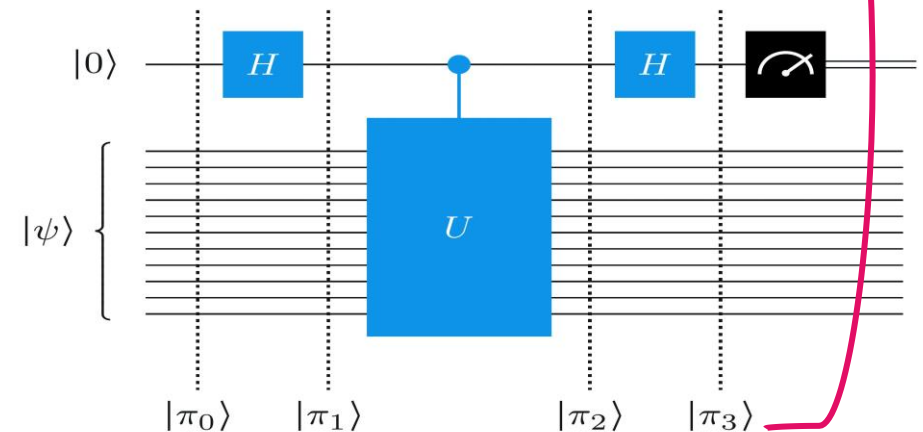
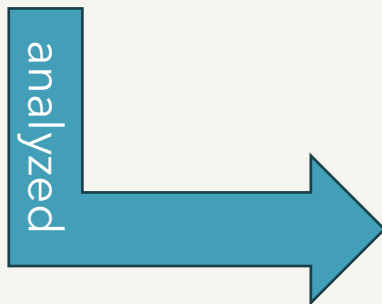
Quantum algorithms

- Quantum Phase Estimation (QPE): Single qubit



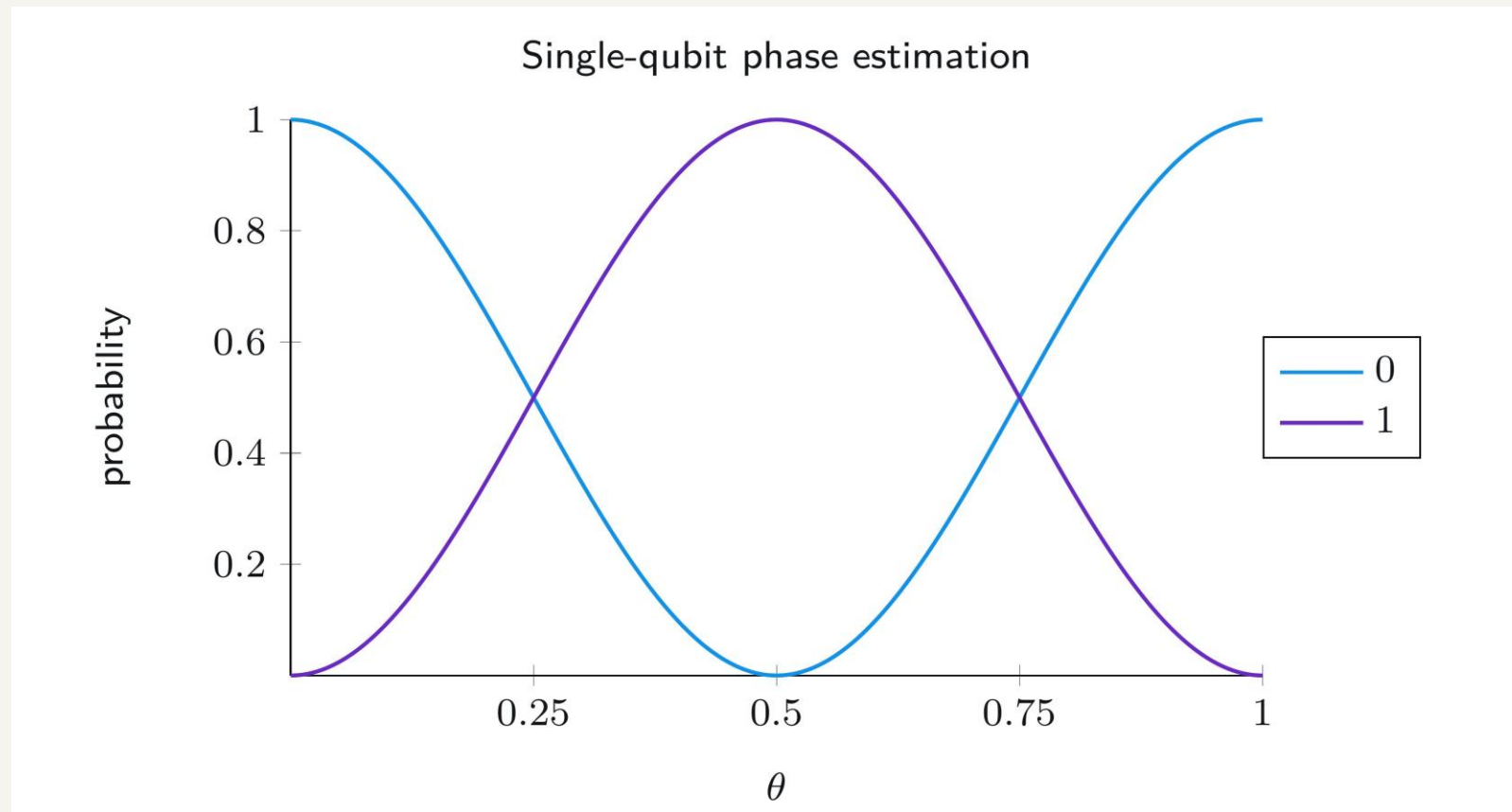
$$p_0 = \left| \frac{1 + e^{2\pi i \theta}}{2} \right|^2 = \cos^2(\pi \theta)$$

$$p_1 = \left| \frac{1 - e^{2\pi i \theta}}{2} \right|^2 = \sin^2(\pi \theta).$$



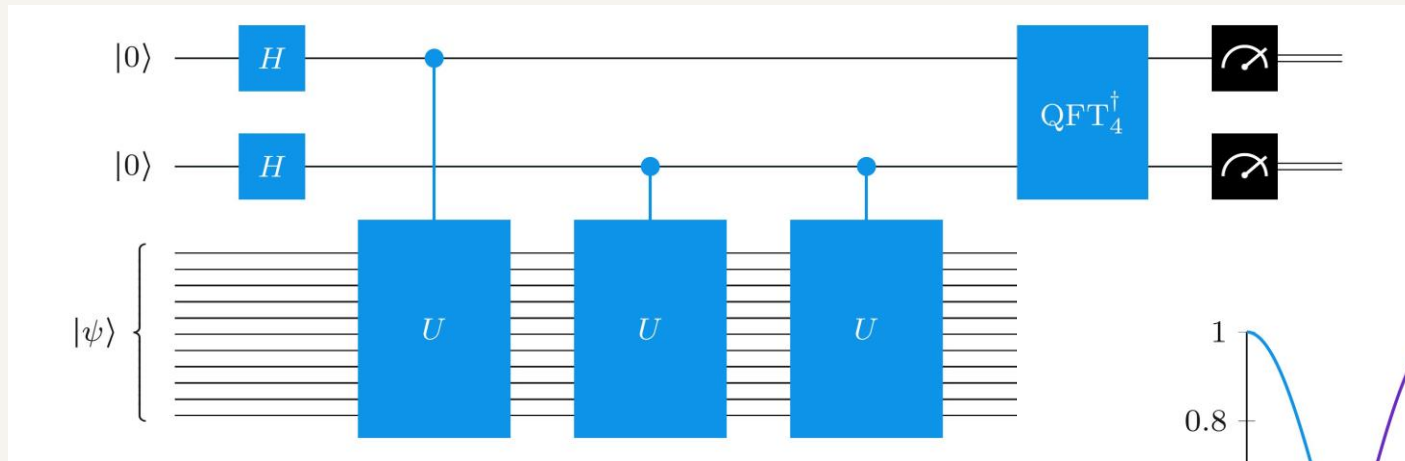
Quantum algorithms

- **Quantum Phase Estimation (QPE)**

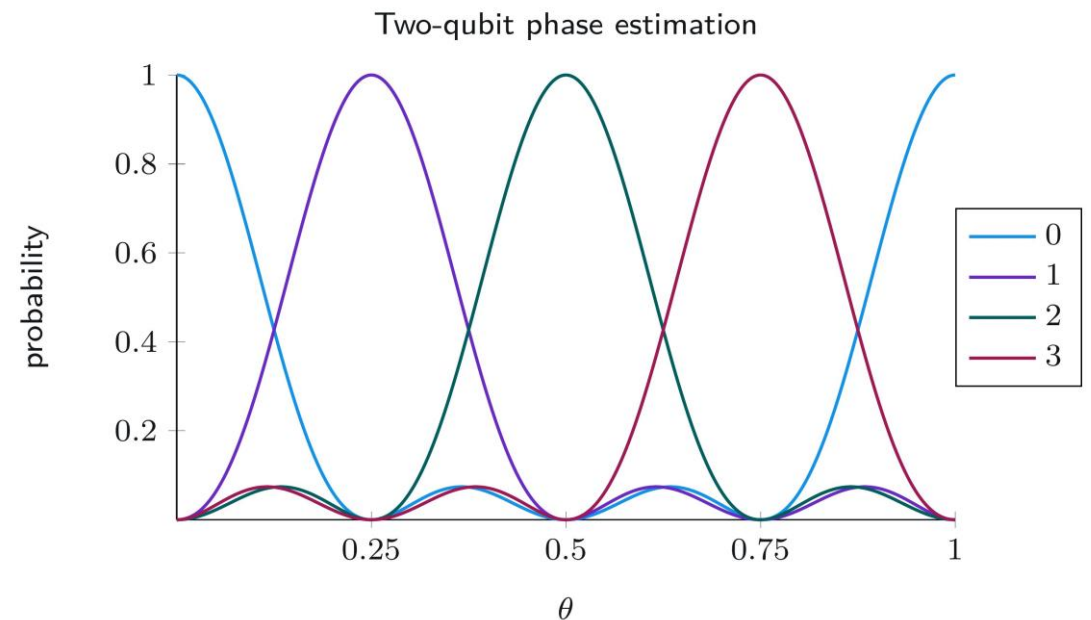


Quantum algorithms

- Quantum Phase Estimation (QPE): Two qubits



Try it out at [Assignment11](#) and upload files "**phase_estimation.ipynb**" into IBM Quantum Lab.



Quantum algorithms

• Shor's algorithm

- Let N be the integer we want to factor. Let's assume the example is number 35.
- Pick a random integer from 2 to $N-1$. Let's call this number a . Let's assume a is 4.
- Find the greatest common divisor (GCD) between a and N . If you get a value that is not 1, it means that the GCD obtained is the answer. It's finished. You don't have to do anything further. But if it is equal to 1, see the next step.
- Find the value of the function $f(x) = a^x \bmod n$.
- From the example $N=35$, $a=4$, the table between the values of x and $f(x)$ will be obtained as follows.

X	0	1	2	3	4	5	6	7	8	9
f(x)	1	4	16	29	11	9	1	4	16	29

- We have to check that $a^{r/2} = -1 \pmod{n}$. If so, we have to random new " a ".
- Then we find the GCD between $(a^{r/2} + 1, N)$ and $(a^{r/2} - 1, N)$. If we get 1 and N , go back to random new " a " again.

Quantum algorithms

- **Shor's algorithm**

- A reduction of the factoring problem to the problem of order-finding, which can be done on a classical computer.
- A quantum algorithm to solve the order-finding problem.

Quantum algorithms

- **Shor's algorithm**

- Classical part

1. Pick a pseudo-random number $a < N$
2. Compute $\gcd(a, N)$. This may be done using the Euclidean algorithm.
3. If $\gcd(a, N) \neq 1$, then there is a nontrivial factor of N , so we are done.
4. Otherwise, use the period-finding subroutine (below) to find r , the period of the following function:

$f(x) = a^x \bmod N$, i.e. the smallest integer r for which $f(x + r) = f(x)$.

5. If r is odd, go back to step 1.
6. If $a^{r/2} \equiv -1 \pmod{N}$ go back to step 1.
7. The factors of N are $\gcd(a^{r/2} \pm 1, N)$. We are done.

Quantum algorithms

- **Shor's algorithm**

- Quantum part: Period-finding subroutine

1. Start with a pair of input and output qubit registers with $\log_2 n$ qubits each, and initialize them to

$$N^{-1/2} \sum_x |x\rangle |0\rangle, \text{ where } x \text{ runs from } 0 \text{ to } N-1$$

2. Construct $f(x)$ as a quantum function and apply it to the above state, to obtain

$$N^{-1/2} \sum_x |x\rangle |f(x)\rangle$$

3. Apply the quantum Fourier transform on the input register. The quantum Fourier transform on N points is defined by:

$$U_{QFT}|x\rangle = N^{-1/2} \sum_y e^{2\pi i xy/N} |y\rangle$$

This leave us in the following state:

$$N^{-1} \sum_x \sum_y e^{2\pi i xy/N} |y\rangle |f(x)\rangle$$

4. Perform a measurement. We obtain some outcome y in the input register and $f(x_0)$ in the output register. Since f is periodic, the probability to measure some y is given by:

$$N^{-1} \left| \sum_x : f(x) = f(x_0) e^{2\pi i xy/N} \right|^2 = N^{-1} \left| \sum_b e^{2\pi i (x_0 + r_b)y/N} \right|^2$$

Analysis now shows that this probability is higher, the closer y/N is to an integer.

Quantum algorithms

- **Shor's algorithm**

- Quantum part: Period-finding subroutine

5. Turn y/N into an irreducible fraction, and extract the denominator r' , which is a candidate for r .
6. Check if $f(x) = f(x + r')$. If so, we are done.
7. Otherwise, obtain more candidates for r by using values near y , or multiples of r' . If any candidate works, we are done.
8. Otherwise, go back to step 1 of the subroutine.

*Try it out at [Assignment11](#) and upload files "**Shor's algorithm.ipynb**" into IBM Quantum Lab.*

Quantum algorithms

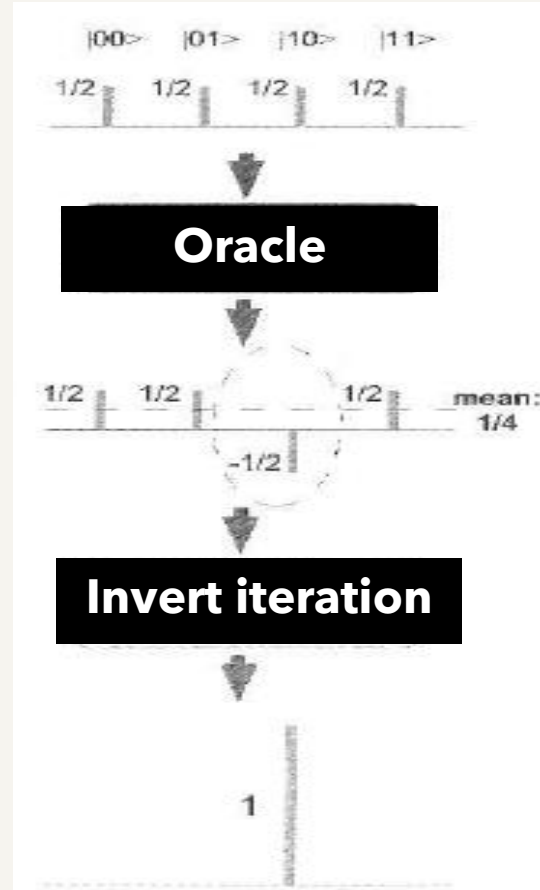
- **Grover's algorithm**

- It can be used to solve unstructured search problems in roughly \sqrt{N} steps, where N is the amount of data.
- This algorithm can speed up an unstructured search problem quadratically using the amplitude amplification trick.

4	6	8		W		$N=2^n$
----------	----------	----------	--	----------	--	---------------------------

Quantum algorithms

- Operation of searching data by Grover's algorithm for 2 qubits:



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

$$\frac{1}{2}(|00\rangle + |01\rangle - |10\rangle + |11\rangle)$$

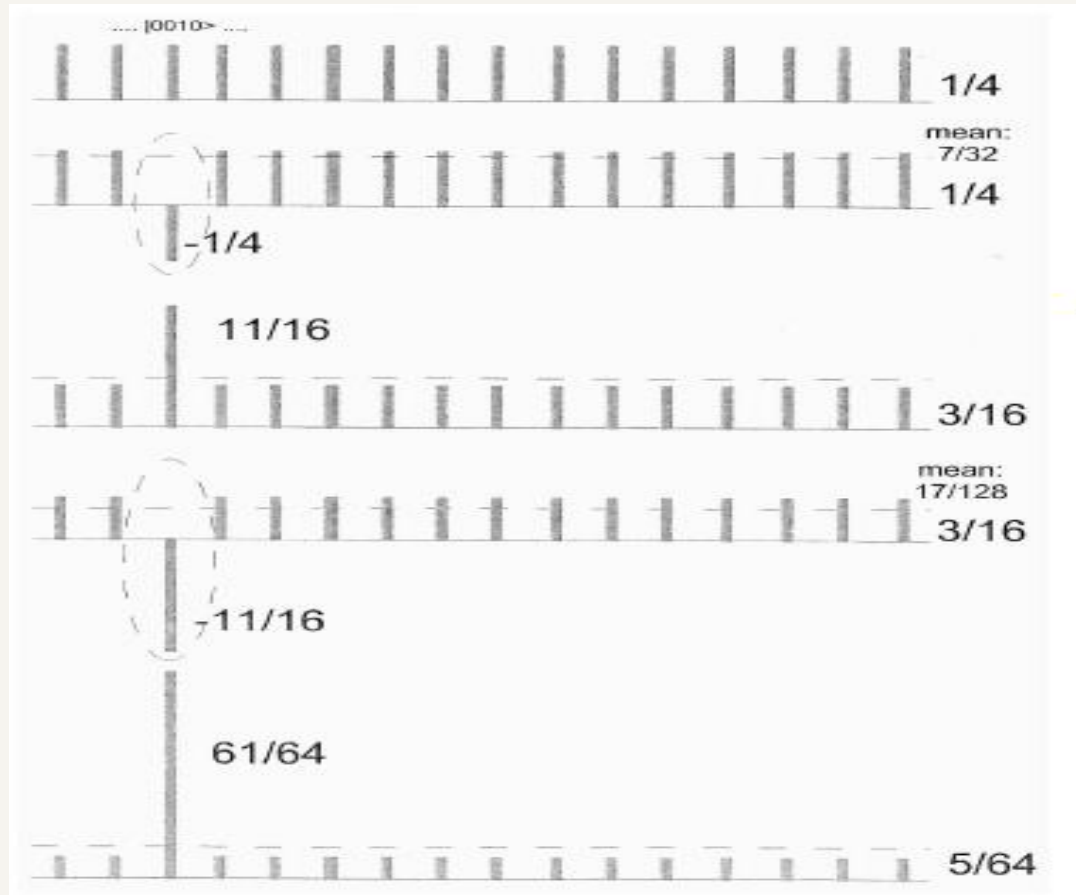
$$m = \frac{\left(\frac{1}{2} + \frac{1}{2} - \frac{1}{2} + \frac{1}{2}\right)}{4} = \frac{1}{4}$$

$$l_i|00\rangle, |01\rangle, |11\rangle = \frac{1}{4} - \left(\frac{1}{2} - \frac{1}{4}\right) = 0$$

$$l_i|10\rangle = \frac{1}{4} - \left(-\frac{1}{2} - \frac{1}{4}\right) = 1$$

Quantum algorithms

- Operation of searching data by Grover's algorithm for 4 qubits:



$$\text{Grover iterations} = \frac{\pi}{4} \times \sqrt{\frac{N}{t}} \text{ times,}$$

N is the number of data (states) and t is the number of target solutions.

Try it out at [AssignmentII](#) and upload files "**Grover's algorithm.ipynb**" into IBM Quantum Lab.

Quantum algorithms

- Grover's algorithm

- The example of Grover's algorithm for 3 qubits with two marked states $|101\rangle$ and $|110\rangle$.

Grover iterations $\sim \frac{\pi}{4} \sqrt{\frac{N}{t}}$

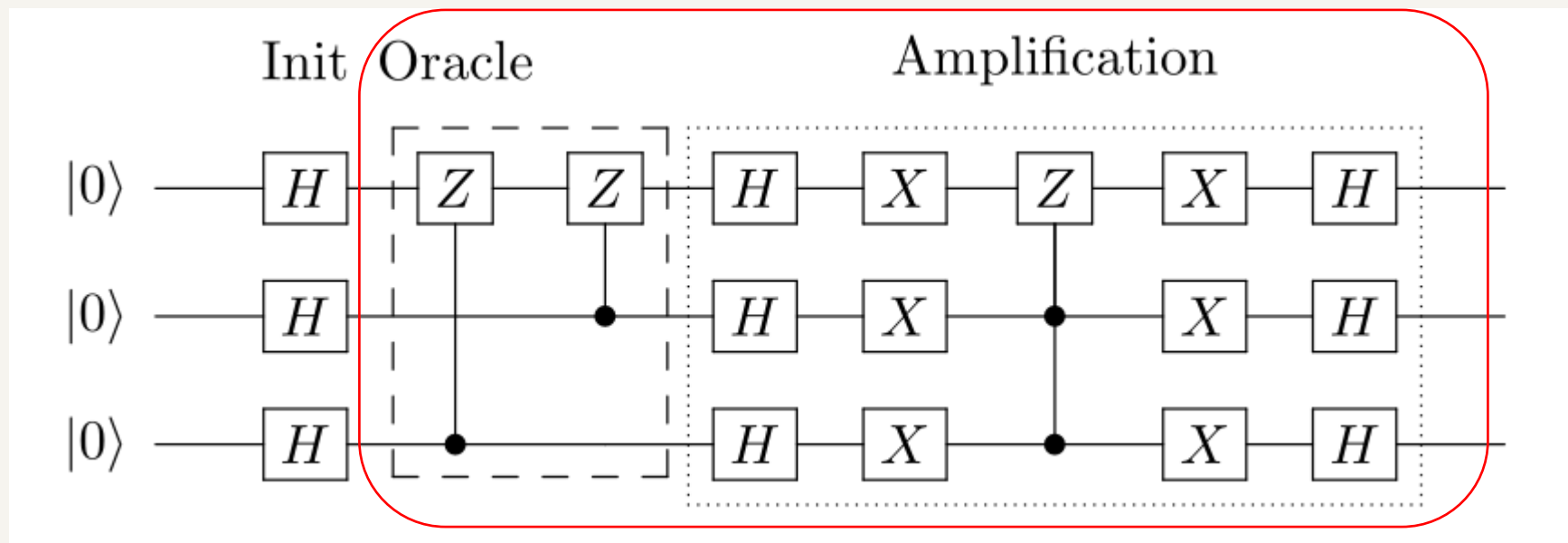


Photo courtesy of <https://qiskit.org/textbook/ch-algorithms/grover.html>

Quantum algorithms

- The implemented stages of the Grover's search algorithm:
 - Initialization: In the first stage of the algorithm all qubits are set to be in superposition by applying the Hadamard gate to each qubit. After this operation the amplitude of each state is $1/\sqrt{n}$.
 - Oracle: The oracle function performs a phase flip on the marked state. If the marked state is $|0110\rangle$, the phase flip inverts the amplitude α_{0110} of the state.
 - Amplification: The amplification stage performs an inversion of the average of the amplitudes.
 - Measurement: The qubits are measured in finally.

Grover iterations $\sim \frac{\pi}{4} \sqrt{\frac{N}{t}}$

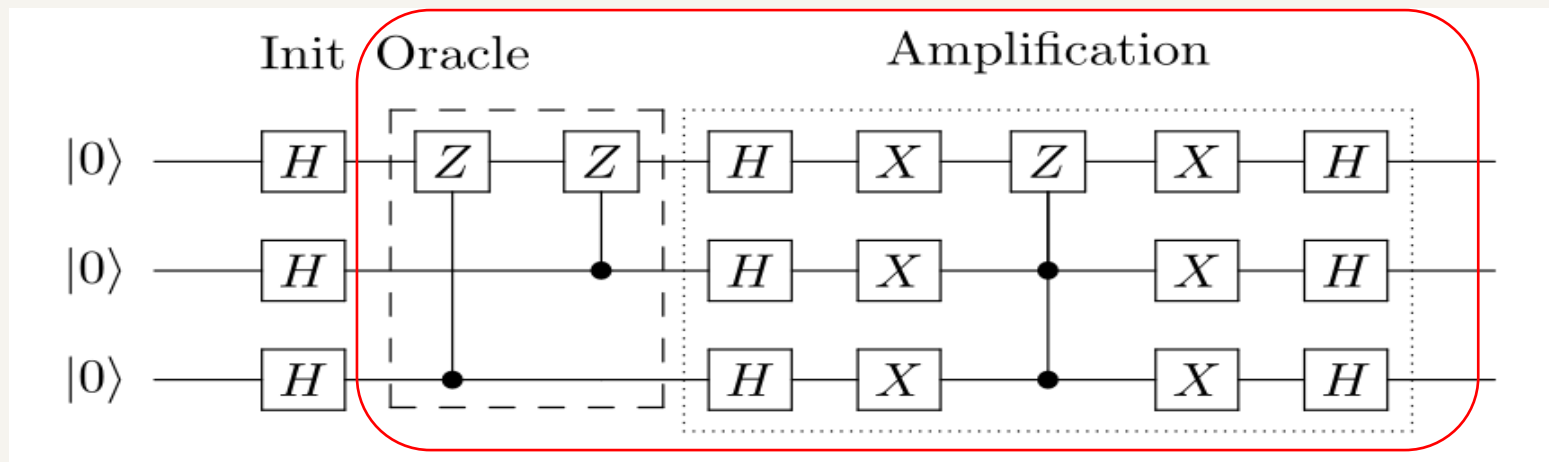
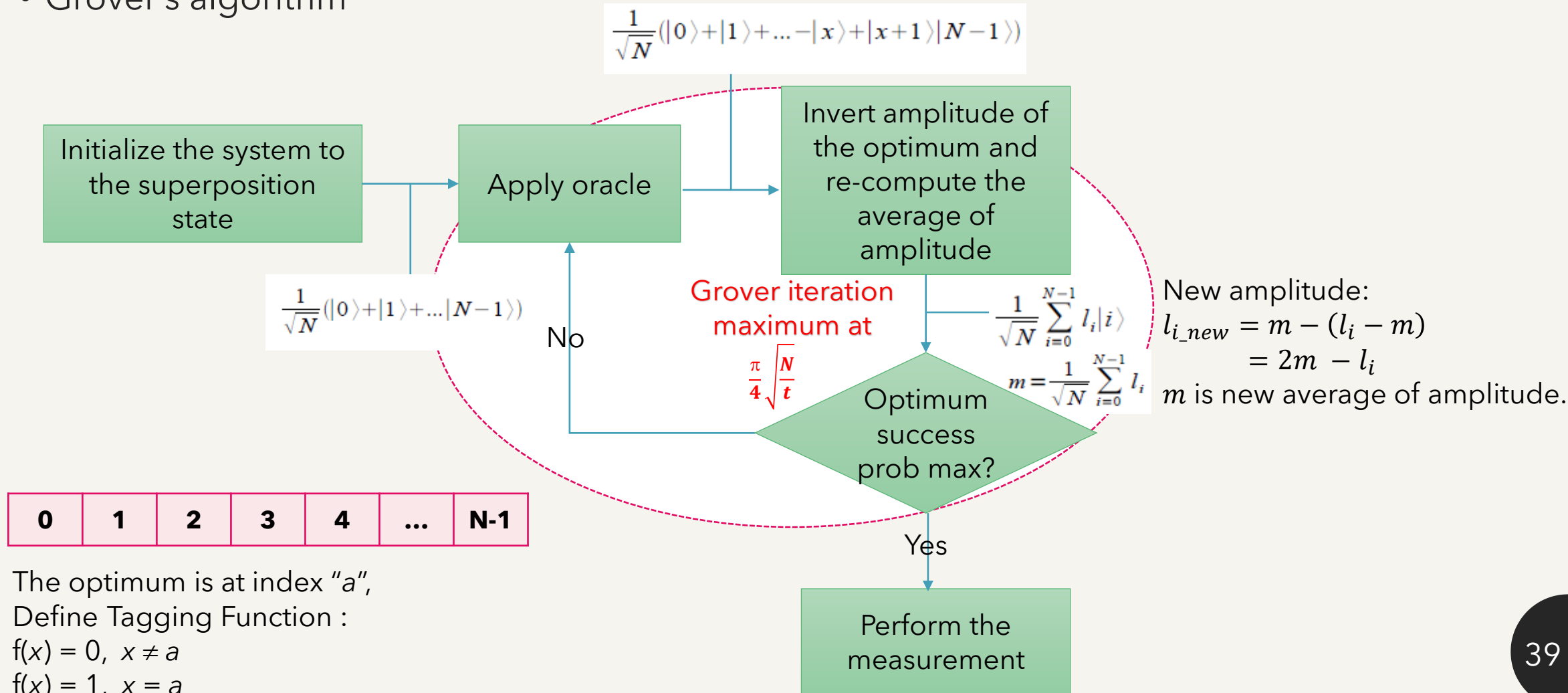


Photo courtesy of <https://qiskit.org/textbook/ch-algorithms/grover.html>

Quantum algorithms

- Grover's algorithm



Assignment II: quantum algorithms

- Required:
 - Go to <https://quantum-computing.ibm.com/>
 - Download source codes at Assignment and upload files "**Lab-4.ipynb**" into IBM Quantum Lab.
- Assignment:
 - Lab-4: Oracles and the Deutsch-Jozsa algorithm by IBM Quantum.