จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

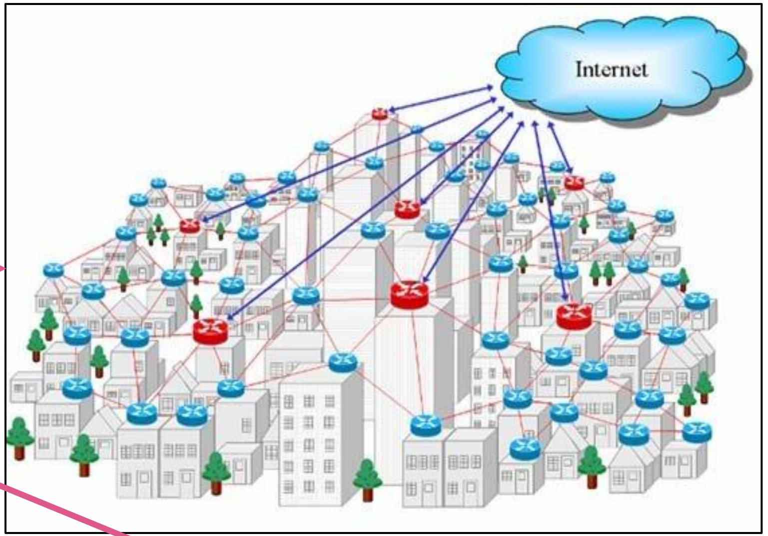
Understanding Quantum Computers

By Dr.Kamonluk Suksen

Outline

- Wanting quantum
- Being quantum
- Doing quantum
- Building quantum

SOLVING HARD PROBLEMS FASTER



Optimization problems

Moore's Law

A plot (logarithmic scale) of MOS transistor counts for microprocessors against dates of introduction, nearly doubling every two years.

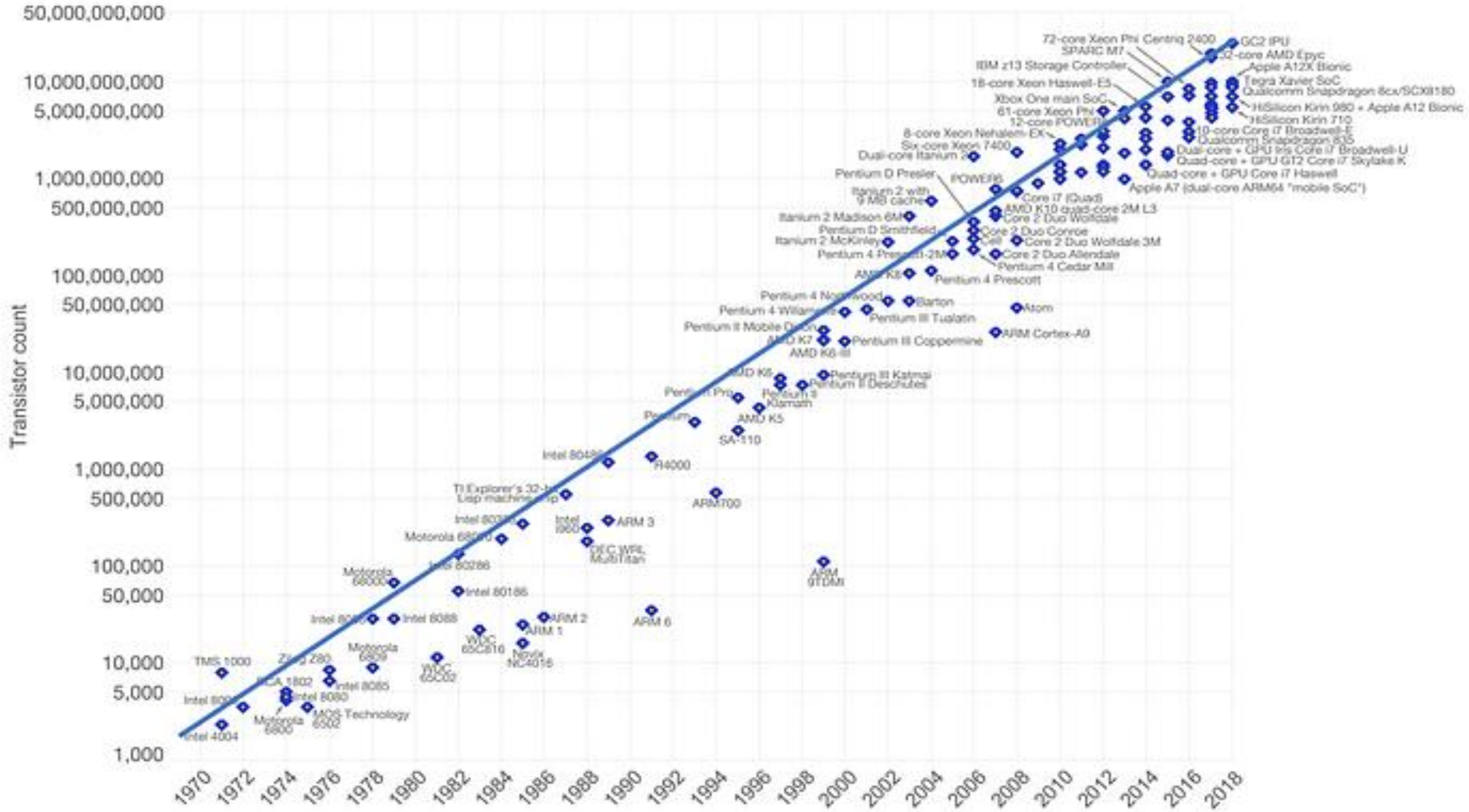
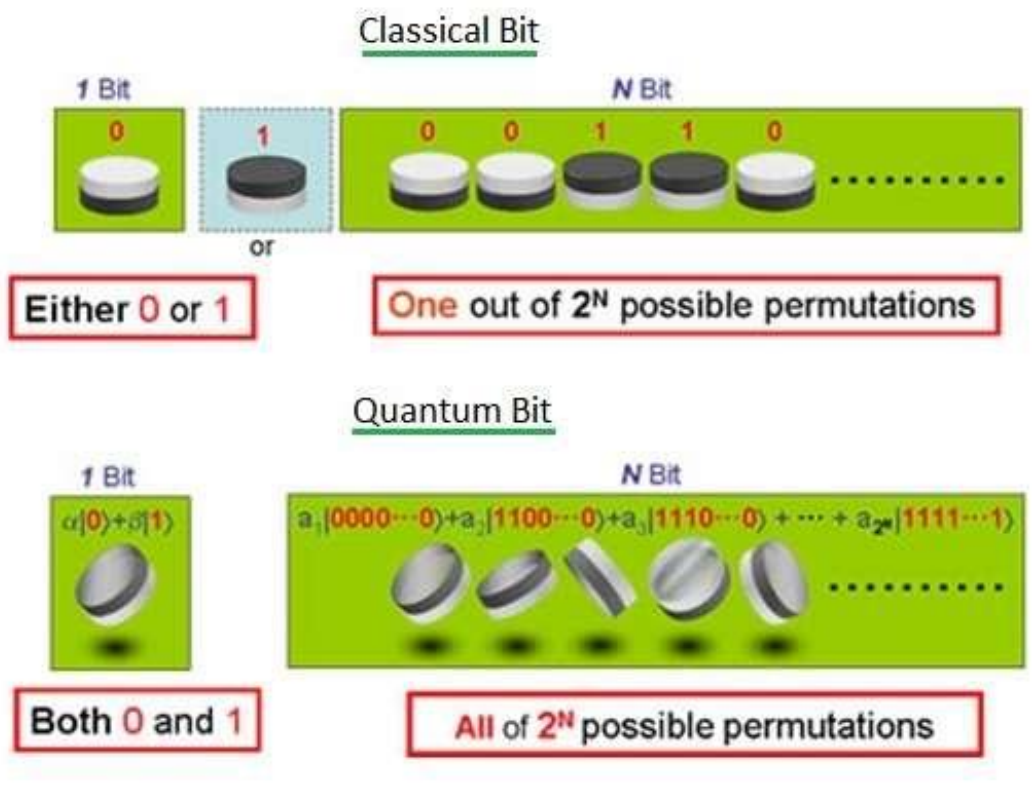


Photo courtesy of https://miro.medium.com/v2/resize:fit:720/format:webp/1*y1c5erN37iuC2zD_JSHGuA.png

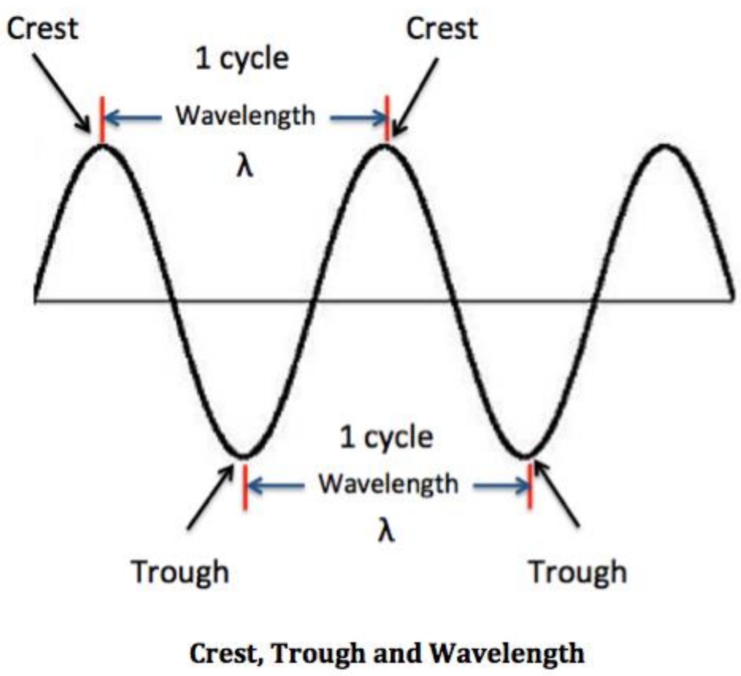
What's a quantum computer?



- 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.

Photo courtesy of https://medium.com/qntm/qntm-entering-the-era-of-quantum-computing

Waves



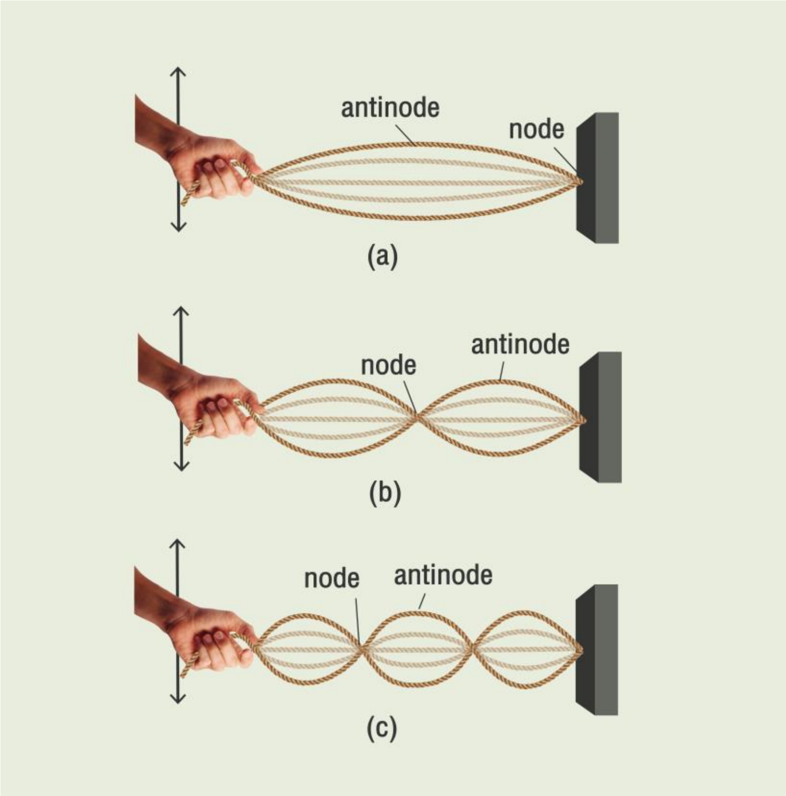
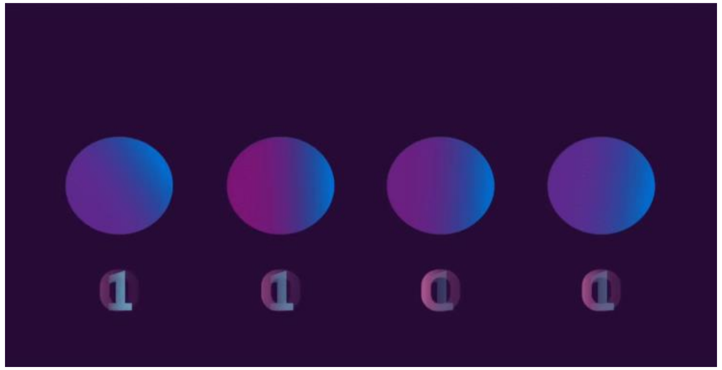


Photo courtesy of https://study.com/learn/lesson/how-to-find-period-of-a-wave.html

Photo courtesy of https://soundenthai.com/standing-wave/

Waves

Superposition



Interference

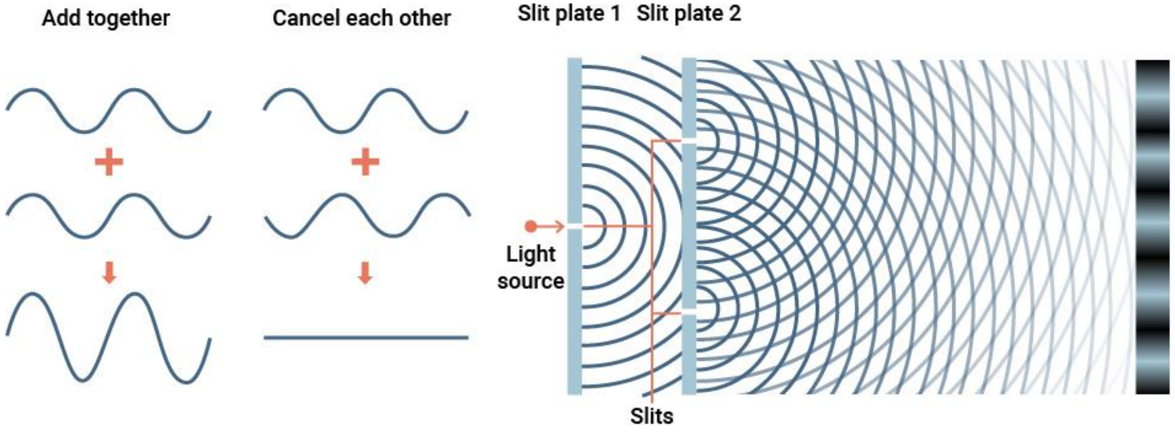


Photo courtesy of https://i.makeagif.com/media/12-14-2015/iJmqBd.mp4

Photo courtesy of https://www.breakingatom.com/learn-the-periodic-table/the-history-of-the-atomic-model-wave-particle-duality

Dirac notation & density matrices

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

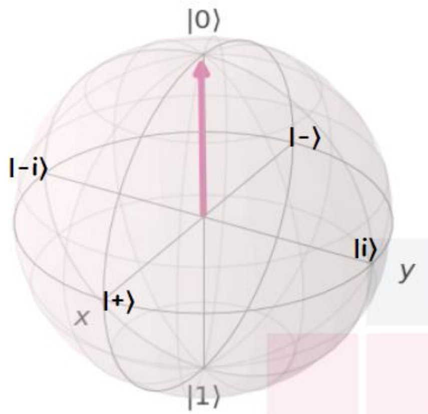
- ket: $|a\rangle = \begin{pmatrix} a_0 \\ a_1 \end{pmatrix}$
- bra: $\langle b| = |b\rangle^{+} = \begin{pmatrix} b_0 \\ b_1 \end{pmatrix}^{+} = (b_0^* \ b_1^*)$
- bra-ket: $\langle b|a\rangle = a_0 {b_0}^* + a_1 {b_1}^* = \langle a|b\rangle^* \in$ C (inner product)
- ket-bra: $|a\rangle\langle b| =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

Dirac notation & density matrices

- The pure states are $|0\rangle = \binom{1}{0}, |1\rangle = \binom{0}{1}$, which are orthogonal: $\langle 0|1\rangle = 1.0 + 0.1 = 0$
- $|0\rangle\langle 0| = \binom{1}{0}(1\ 0) = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, |1\rangle\langle 1| = \binom{0}{1}(0\ 1) = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$
- $P = \begin{pmatrix} P_{00} & P_{01} \\ P_{10} & P_{11} \end{pmatrix} = P_{00}|0\rangle\langle 0| + P_{01}|0\rangle\langle 1| + P_{10}|1\rangle\langle 0| + P_{11}|1\rangle\langle 1|$
- 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.
  - $P = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = |0\rangle\langle 0| \rightarrow \text{Pure}, P = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = |1\rangle\langle 1| \rightarrow \text{Pure}$
  - $P = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|) \rightarrow \text{Mixed}$
  - $P = \frac{1}{2}\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} = \frac{1}{2}(|0\rangle\langle 0| - |0\rangle\langle 1| - |1\rangle\langle 0| + |1\rangle\langle 1|) = \frac{1}{2}(|0\rangle - |1\rangle)(|0\rangle - |1\rangle) \rightarrow \text{Pure}$

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 $\{|0\rangle, |1\rangle\}$:

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

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

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

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

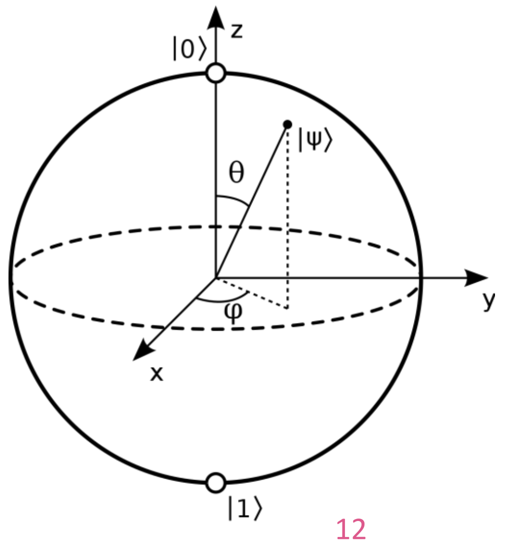
Bloch sphere

- 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 $|0\rangle, |1\rangle$:

  $$\mathrm{P}(|0\rangle) = \cos^2\frac{\theta}{2}, \mathrm{P}(|1\rangle) = \sin^2\frac{\theta}{2}.$$

- 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: $\vec{r} = \begin{pmatrix} \sin\theta\cos\varphi \\ \sin\theta\sin\varphi \\ \cos\theta \end{pmatrix}$



Quantum circuits: single qubit gates

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

- 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

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

Quantum circuits: single qubit gates

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

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

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

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

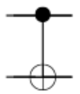
- Hadamard gate: one of the most important gates for quantum circuits

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

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

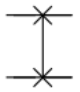
Quantum circuits: multiple-qubit gates

controlled-NOT



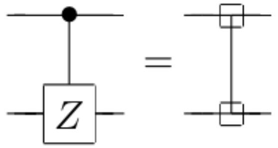
$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

swap



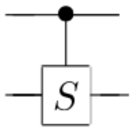
$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

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

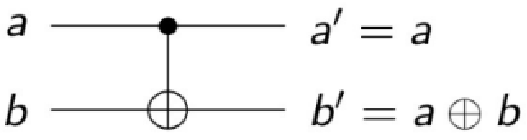
$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

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:

  - $|\mathrm{a}\rangle \otimes |\mathrm{b}\rangle = \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} \otimes \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} = \begin{pmatrix} a_1 b_1 \\ a_1 b_2 \\ a_2 b_1 \\ a_2 b_2 \end{pmatrix}$
  - Example: system A is in state $|1\rangle_{\mathrm{A}}$ and system B is in state $|0\rangle_{\mathrm{B}} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$, 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. $|\psi\rangle_{\mathrm{AB}}^{(00)} = \frac{1}{\sqrt{2}}(|00\rangle_{\mathrm{AB}} + |11\rangle_{\mathrm{AB}}) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$, it so called Bell state, used for teleportation, cryptography, Bell tests, etc.

Entanglement

- If a pure state $|\psi\rangle_{\mathrm{AB}}$ 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:

  - $|\psi^{\mathbf{00}}\rangle := \frac{\mathbf{1}}{\sqrt{\mathbf{2}}}(|00\rangle + |11\rangle),$
  - $|\psi^{\mathbf{01}}\rangle := \frac{\mathbf{1}}{\sqrt{\mathbf{2}}}(|01\rangle + |10\rangle),$
  - $|\psi^{\mathbf{10}}\rangle := \frac{\mathbf{1}}{\sqrt{\mathbf{2}}}(|00\rangle - |11\rangle),$
  - $|\psi^{\mathbf{11}}\rangle := \frac{\mathbf{1}}{\sqrt{\mathbf{2}}}(|01\rangle - |10\rangle).$

Entanglement

- Creation of Bell states:

$$\left|q_0 q_1\right\rangle_{00} \; H_0 \rightarrow \frac{\mathbf{1}}{\sqrt{\mathbf{2}}}(|00\rangle + |10\rangle) \; CNOT_{\mathbf{01}} \rightarrow \frac{\mathbf{1}}{\sqrt{\mathbf{2}}}(|00\rangle + |11\rangle) = \left|\psi^{\mathbf{00}}\right\rangle,$$

$$\left|q_0 q_1\right\rangle_{01} \; H_0 \rightarrow \frac{\mathbf{1}}{\sqrt{\mathbf{2}}}(|01\rangle + |11\rangle) \; CNOT_{\mathbf{01}} \rightarrow \frac{\mathbf{1}}{\sqrt{\mathbf{2}}}(|01\rangle + |10\rangle) = \left|\psi^{\mathbf{01}}\right\rangle,$$

$$\left|q_0 q_1\right\rangle_{10} \; H_0 \rightarrow \frac{\mathbf{1}}{\sqrt{\mathbf{2}}}(|00\rangle - |10\rangle) \; CNOT_{\mathbf{01}} \rightarrow \frac{\mathbf{1}}{\sqrt{\mathbf{2}}}(|00\rangle - |11\rangle) = \left|\psi^{\mathbf{10}}\right\rangle,$$

$$\left|q_0 q_1\right\rangle_{11} \; H_0 \rightarrow \frac{\mathbf{1}}{\sqrt{\mathbf{2}}}(|01\rangle - |11\rangle) \; CNOT_{\mathbf{01}} \rightarrow \frac{\mathbf{1}}{\sqrt{\mathbf{2}}}(|01\rangle - |10\rangle) = \left|\psi^{\mathbf{11}}\right\rangle$$

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:

$$|\phi\rangle_S \otimes |\psi^{00}\rangle_{AB} = \frac{1}{\sqrt{2}}\left(\alpha|000\rangle_{SAB} + \alpha|011\rangle_{SAB} + \beta|100\rangle_{SAB} + \beta|111\rangle_{SAB}\right)$$

$$= \frac{1}{2\sqrt{2}}\Big[\left(|00\rangle_{SA} + |11\rangle_{SA}\right)\otimes\left(\alpha|0\rangle_B + \beta|1\rangle_B\right) + \left(|01\rangle_{SA} + |10\rangle_{SA}\right)\otimes\left(\alpha|1\rangle_B + \beta|0\rangle_B\right)$$

$$+ \left(|00\rangle_{SA} - |11\rangle_{SA}\right)\otimes\left(\alpha|0\rangle_B - \beta|1\rangle_B\right) + \left(|01\rangle_{SA} - |10\rangle_{SA}\right)\otimes\left(\alpha|1\rangle_B - \beta|0\rangle_B\right)\Big]$$

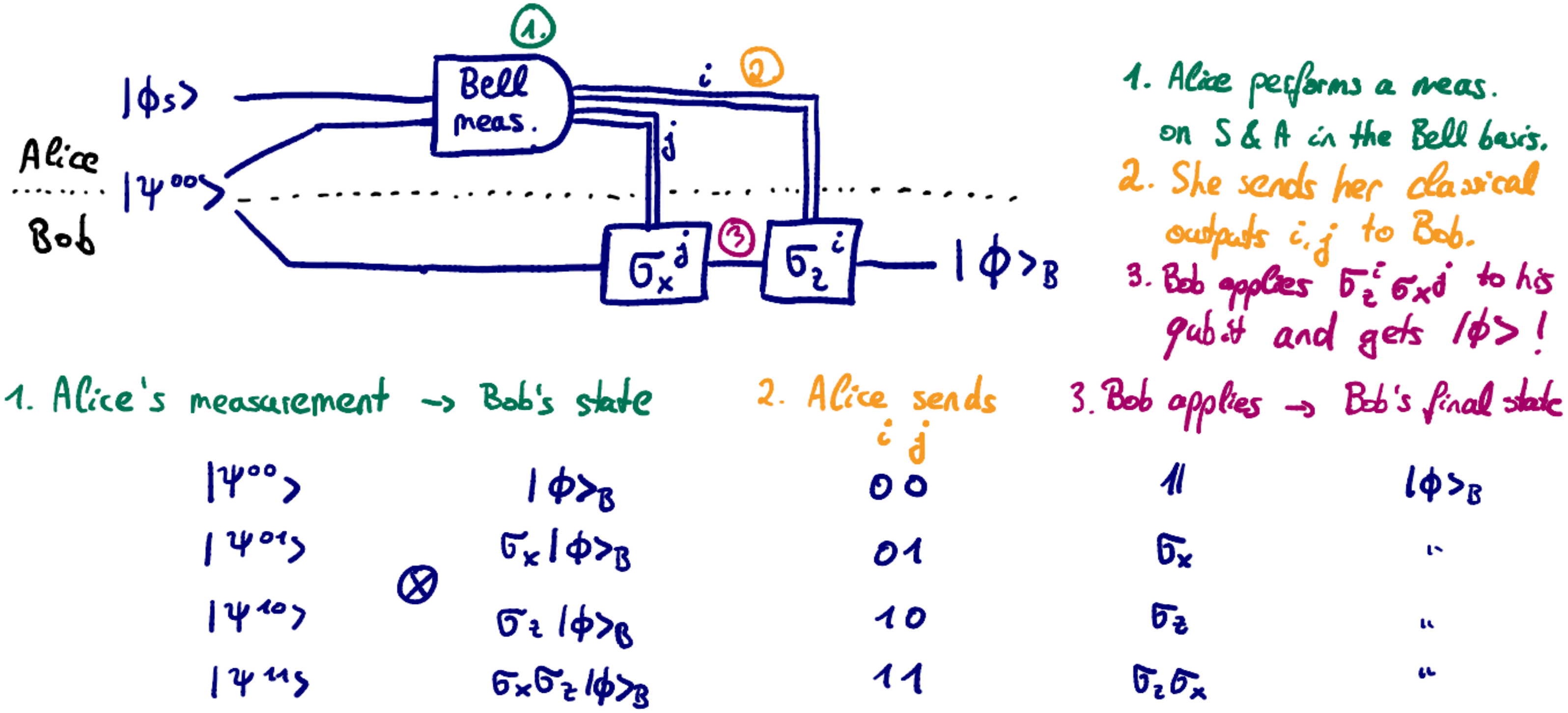
$$= \frac{1}{2}\Big[|\psi^{00}\rangle_{SA}\otimes|\phi\rangle_B + |\psi^{01}\rangle_{SA}\otimes(\sigma_x|\phi\rangle_B)$$

$$+ |\psi^{10}\rangle_{SA}\otimes(\sigma_z|\phi\rangle_B) + |\psi^{11}\rangle_{SA}\otimes(\sigma_x\sigma_z|\phi\rangle_B)\Big]$$

Photo courtesy of : IBM quantum summer school 2019

Teleportation

- Protocol:

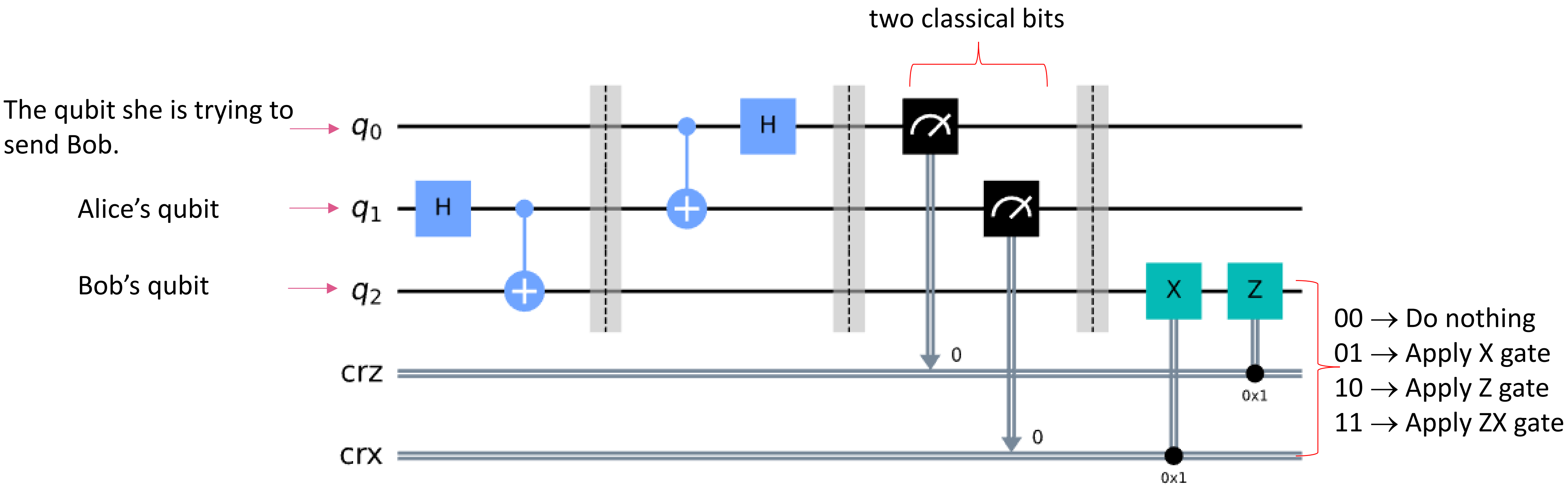


- Alice’s state collapsed during the measurement, so she doesn’t have the initial state $|\phi\rangle_S$ anymore. This is expected due to the no-cloning theorem, as she cannot copy her state, but just send her state to Bob when destroying her own.

Photo courtesy of : IBM quantum summer school 2019

Teleportation

- Quantum circuit:



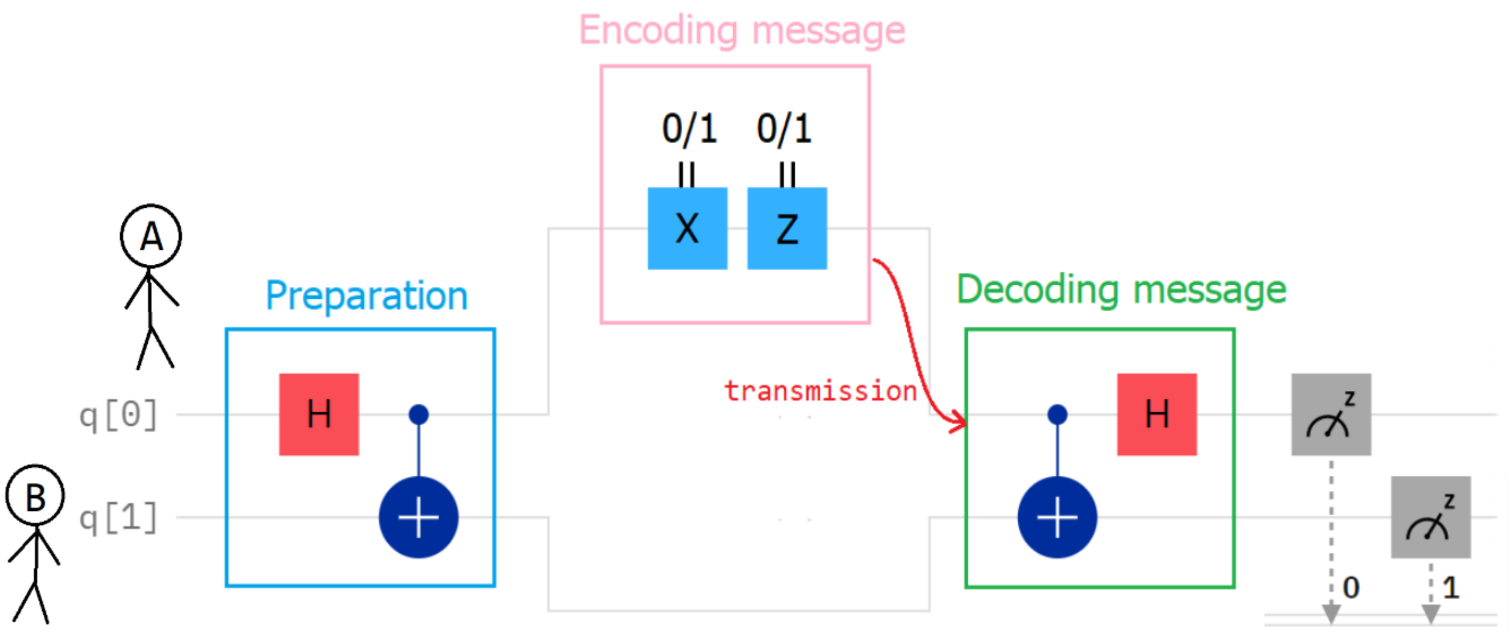
Superdense coding

- 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 → quantum state,
  - decoding: quantum state → classical state.

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

Superdense coding

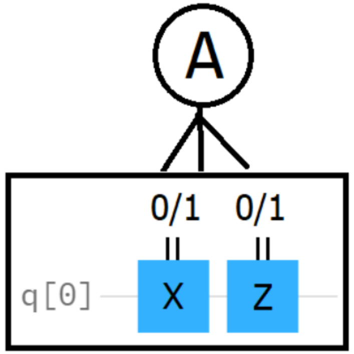
- Superdense coding includes 4 steps:
  - preparation,
  - encoding message,
  - transmission,
  - decoding message.



Superdense coding

Step 2: encoding message

- A encodes the classical state in the qubit by applying gate(s).

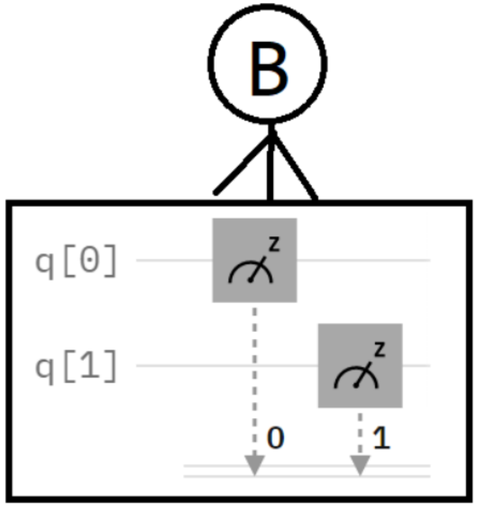


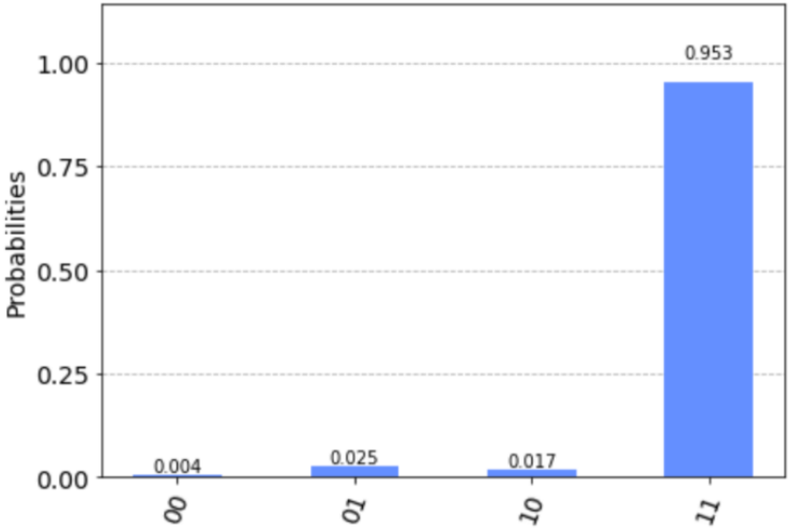
Message	Applied Gate	State Result
00	I	$\frac{1}{\sqrt{2}}(\|00\rangle + \|11\rangle)$
01	X	$\frac{1}{\sqrt{2}}(\|10\rangle + \|01\rangle)$
10	Z	$\frac{1}{\sqrt{2}}(\|00\rangle - \|11\rangle)$
11	ZX	$\frac{1}{\sqrt{2}}(\|10\rangle - \|01\rangle)$

Message	Applied Gate
00	
01	X
10	Z
11	X Z

Superdense coding

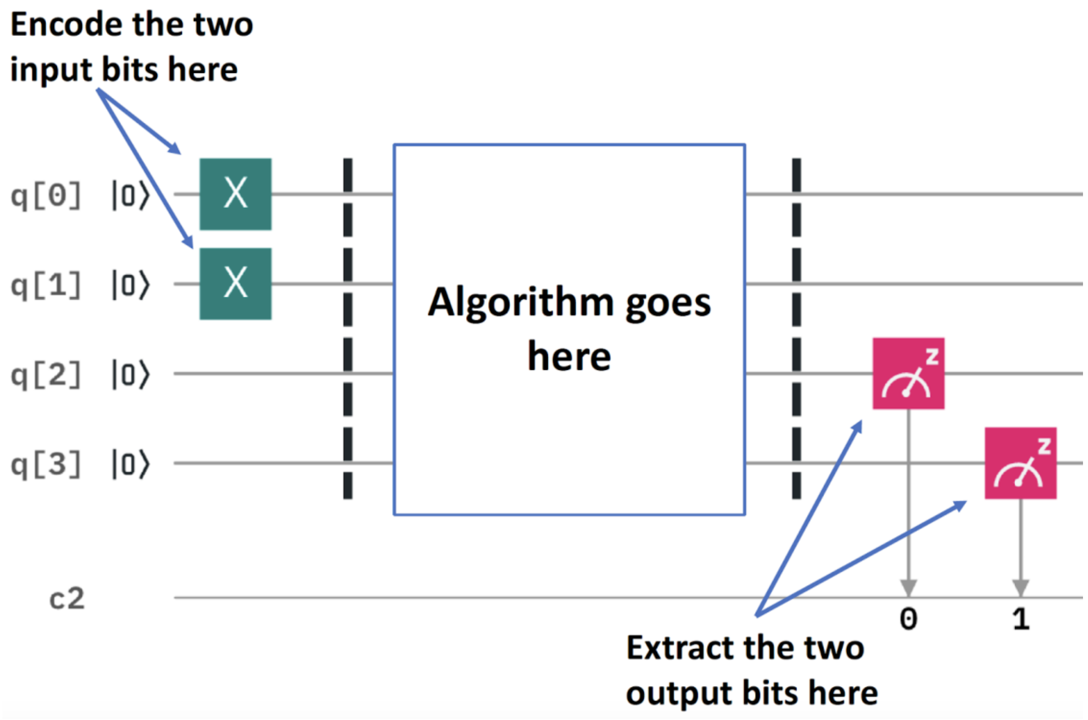
- Test the circuit which encodes message “11” and run on “ibm_oslo”.





Quantum programming using Qiskit

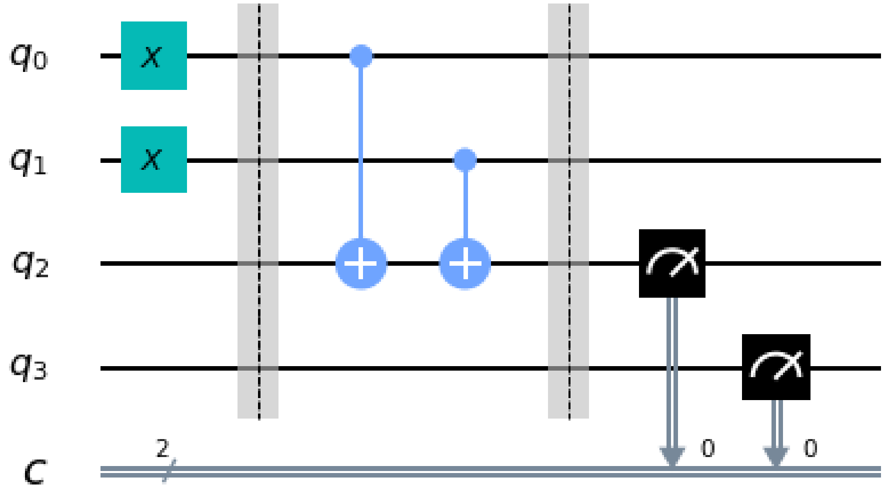
- Half adder circuit for input 11



- 0+0 = 00 (in decimal, this is 0+0 = 0)
- 0+1 = 01 (in decimal, this is 0+1 = 1)
- 1+0 = 01 (in decimal, this is 1+0 = 1)
- 1+1 = 10 (in decimal, this is 1+1 = 2)

Quantum programming using Qiskit

- Half adder circuit for input 11

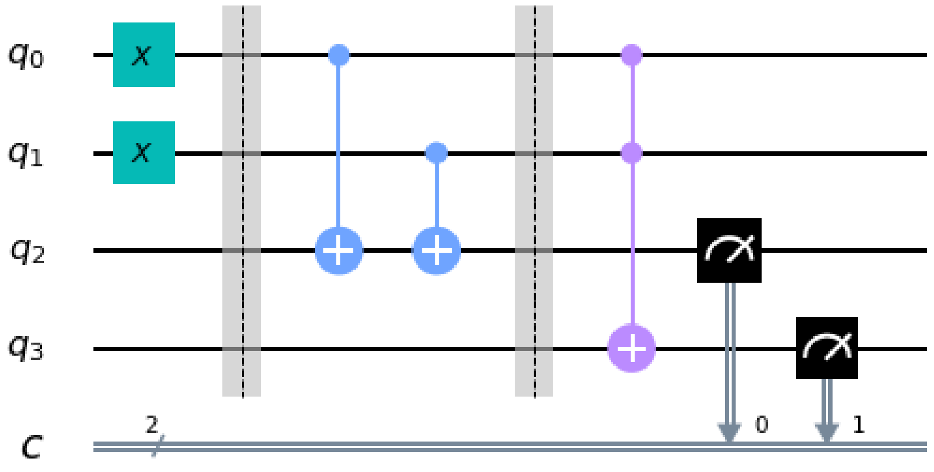



```
qc_ha = QuantumCircuit(4,2)
# encode inputs in qubits 0 and 1
qc_ha.x(0) # For a=0, remove the this line. For a=1, leave it.
qc_ha.x(1) # For b=0, remove the this line. For b=1, leave it.
qc_ha.barrier()
# use cnots to write the XOR of the inputs on qubit 2
qc_ha.cx(0,2)
qc_ha.cx(1,2)
qc_ha.barrier()
# extract outputs
qc_ha.measure(2,0) # extract XOR value
qc_ha.measure(3,0)

qc_ha.draw(output='mpl')
```

Quantum programming using Qiskit

- Half adder circuit for input 11




```
qc_ha = QuantumCircuit(4,2)
# encode inputs in qubits 0 and 1
qc_ha.x(0) # For a=0, remove the this line. For a=1, leave it.
qc_ha.x(1) # For b=0, remove the this line. For b=1, leave it.
qc_ha.barrier()
# use cnots to write the XOR of the inputs on qubit 2
qc_ha.cx(0,2)
qc_ha.cx(1,2)
# use ccx to write the AND of the inputs on qubit 3
qc_ha.ccx(0,1,3)
qc_ha.barrier()
# extract outputs
qc_ha.measure(2,0) # extract XOR value
qc_ha.measure(3,1) # extract AND value

qc_ha.draw()
```

Assignment I: Basic Quantum Computing

- Required:
  - Go to https://colab.research.google.com/
  - Sign in with Gmail
  - Download source codes at t.ly/PIGh5 and upload files “Lab-1.ipynb”, “Lab-2.ipynb” and “Lab-3.ipynb” into Colab.
  - Install required library for each assignment by typing the following:
    - pip install qiskit
    - pip install qiskit-aer
    - pip install pylatexenc
    - pip install qiskit-ibm-runtime (only Lab-2.ipynb and Lab-3.ipynb)
- 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:

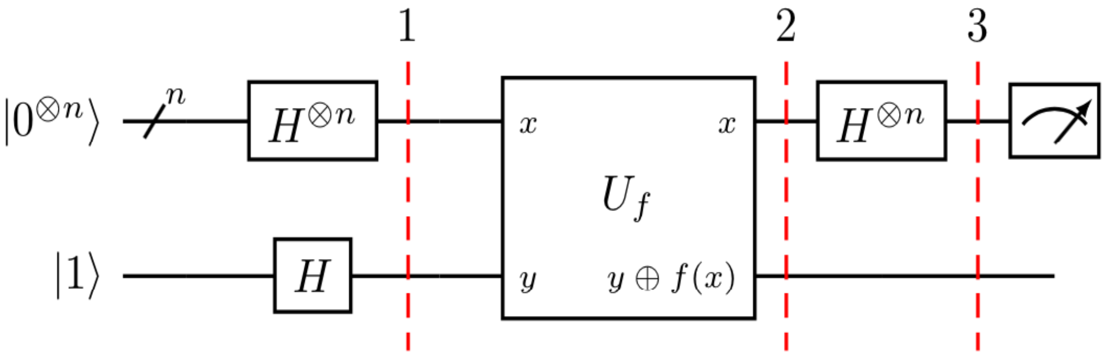
$$f(\{x_0, x_1, x_2, \ldots\}) \to 0 \text{ or } 1 \text{ , where } x_n \text{ is } 0 \text{ or } 1$$

- 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.

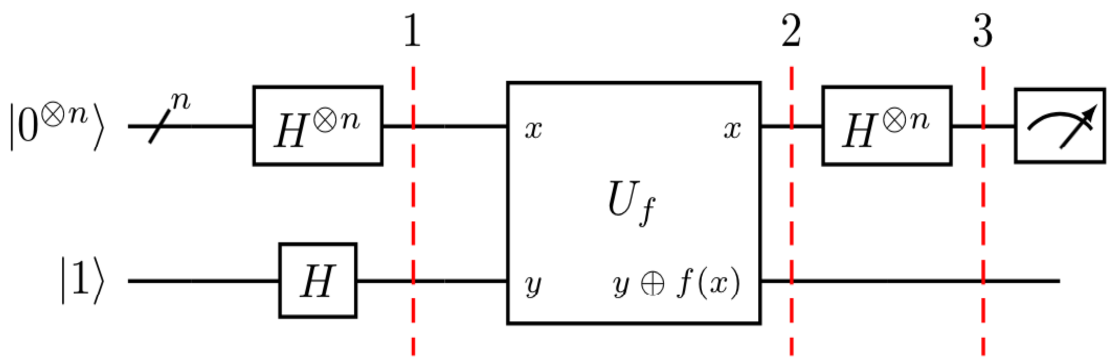


- In the case where the function is constant, then the co-efficient of $|0\rangle^{\otimes n}$, $\sum_x (-1)^{f(x)}/2^n$ is equal to ± 1... as this has amplitude 1, then we measure $|0\rangle^{\otimes n}$ with probability one.
- In the case where the function is balanced then $\sum_x (-1)^{f(x)}/2^n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

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.



- 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 $|0\rangle^{\otimes n}$.

Quantum algorithms

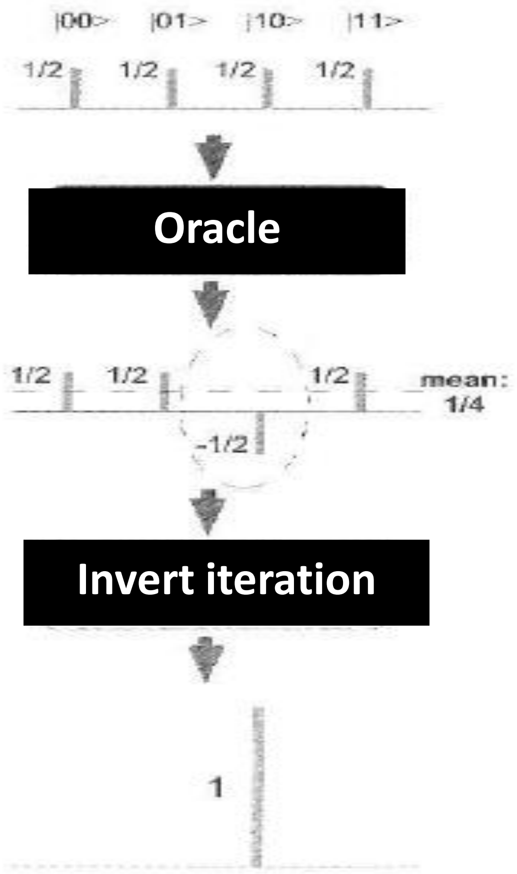
Grover's algorithm

- 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:



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

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

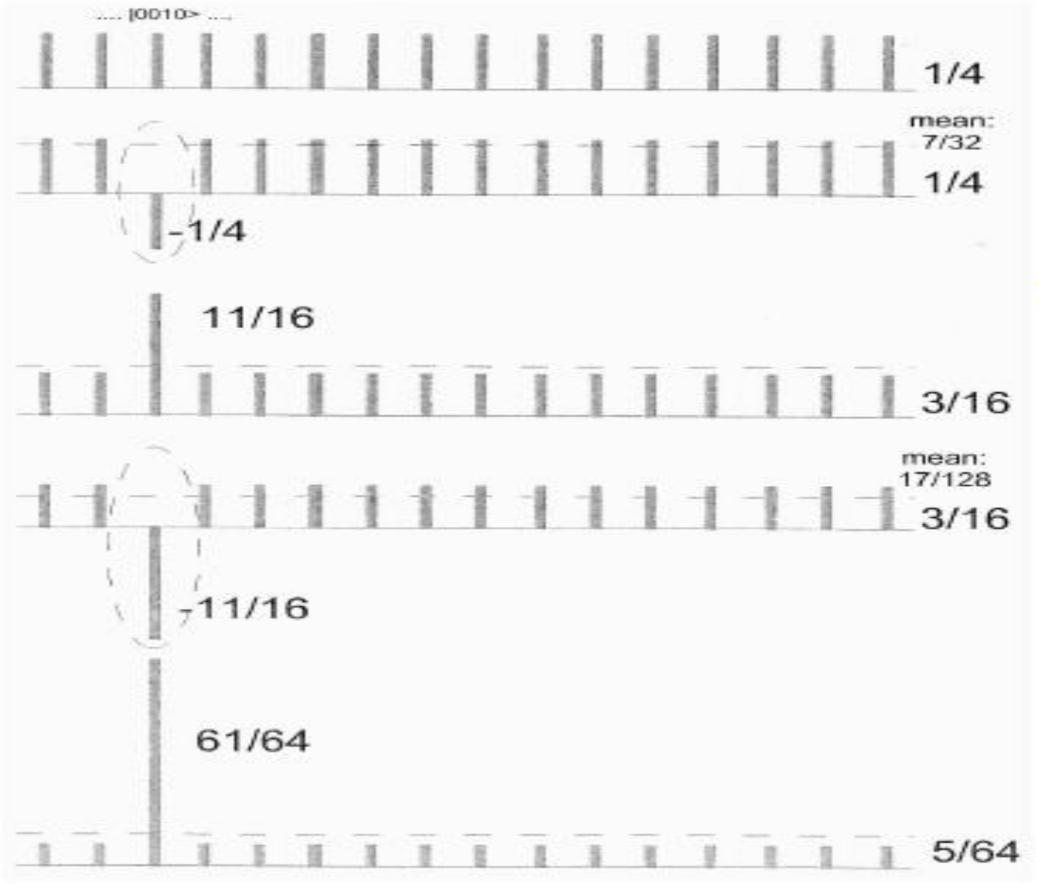
$$m=\frac{\left(\frac{1}{2}+\frac{1}{2}-\frac{1}{2}+\frac{1}{2}\right)}{4}=\frac{1}{4}$$

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

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

Quantum algorithms

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



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

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

Try it out at t.ly/PIGh5 *and upload files "**Grover's algorithm.ipynb**" into Colab.*

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 ~ $\frac{\pi}{4}\sqrt{\frac{N}{t}}$

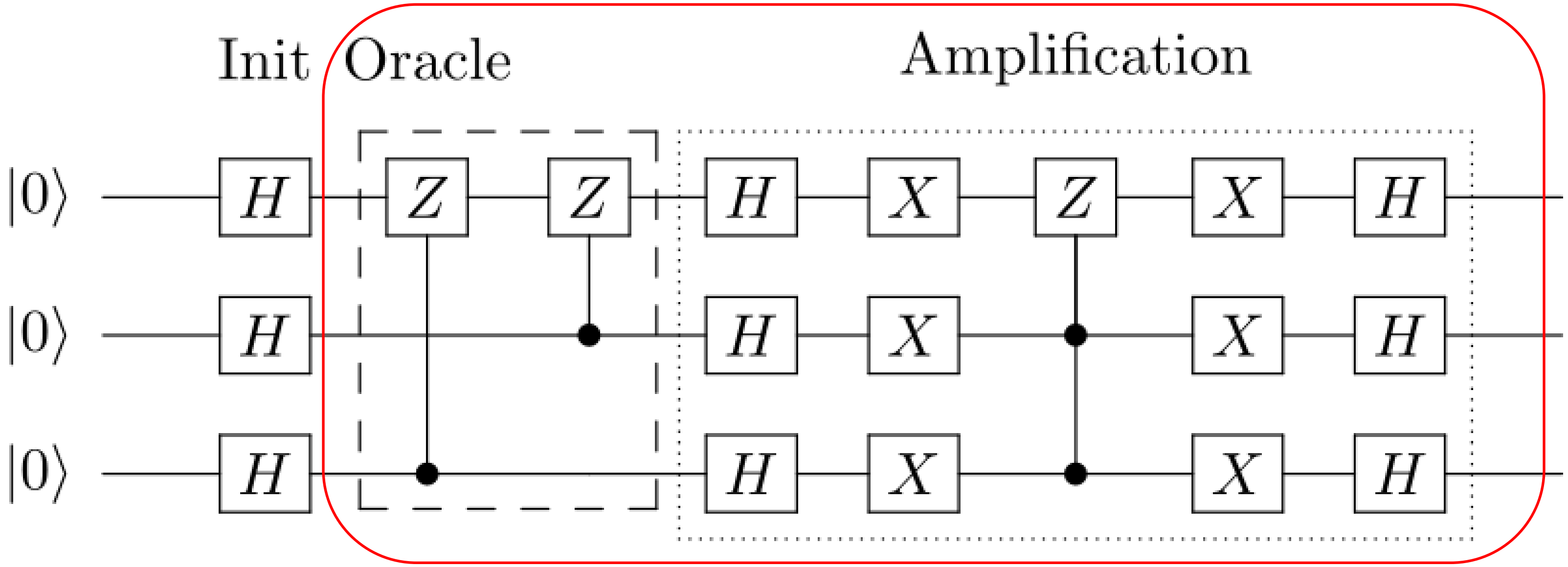
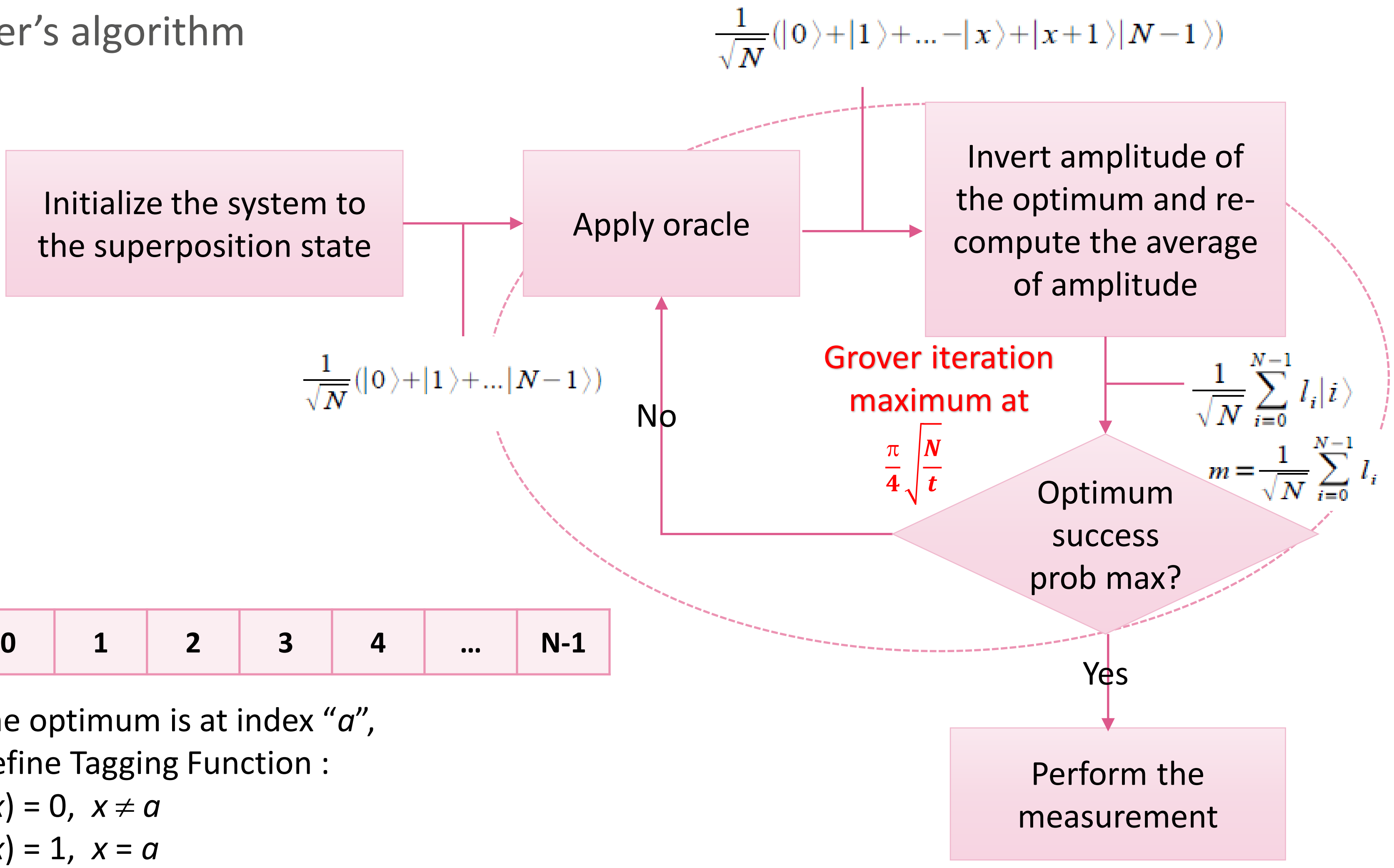


Photo courtesy of https://qiskit.org/textbook/ch-algorithms/grover.html

Quantum algorithms

Grover's algorithm



New amplitude:

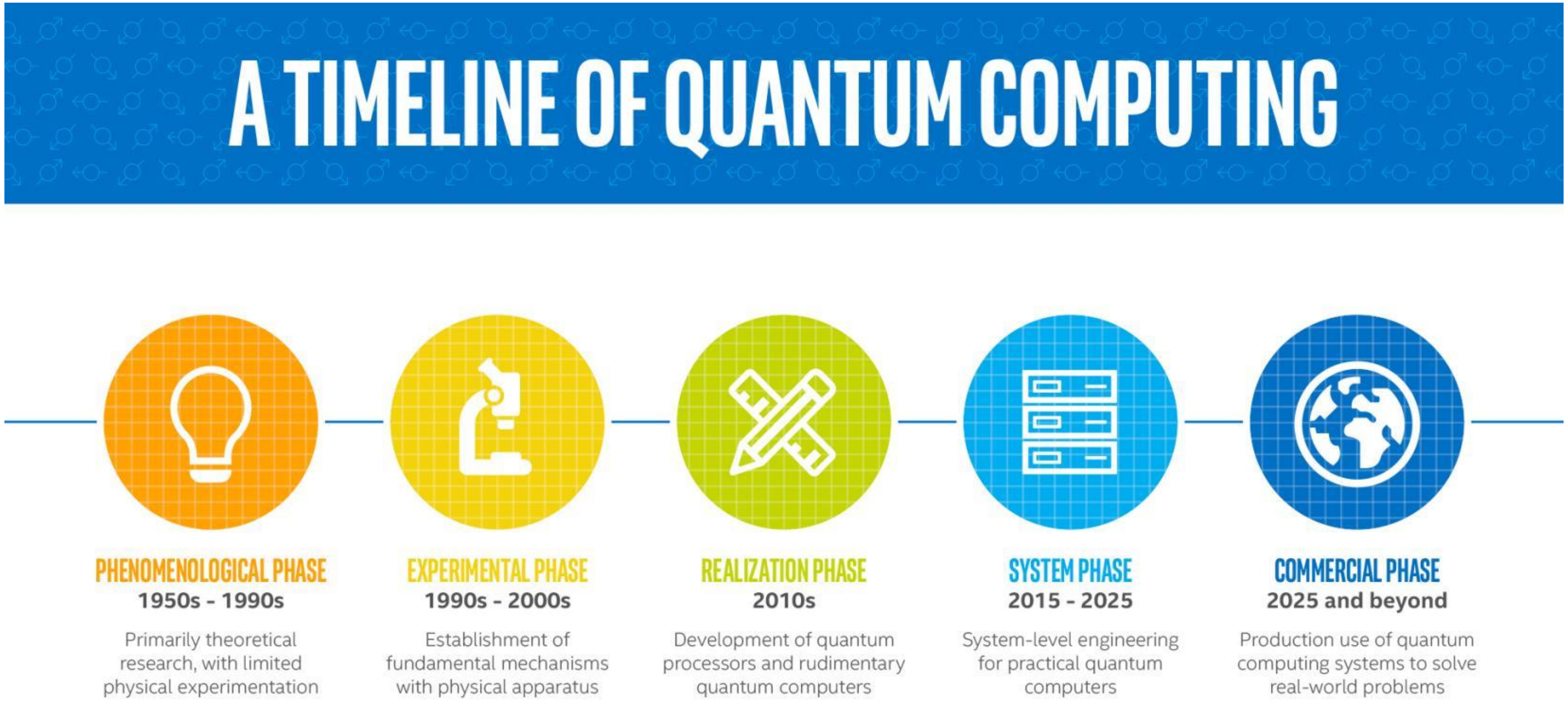
$$l_{i\_new} = m - (l_i - m)$$
$$= 2m - l_i$$

m is new average of amplitude.

0	**1**	**2**	**3**	**4**	**…**	**N-1**

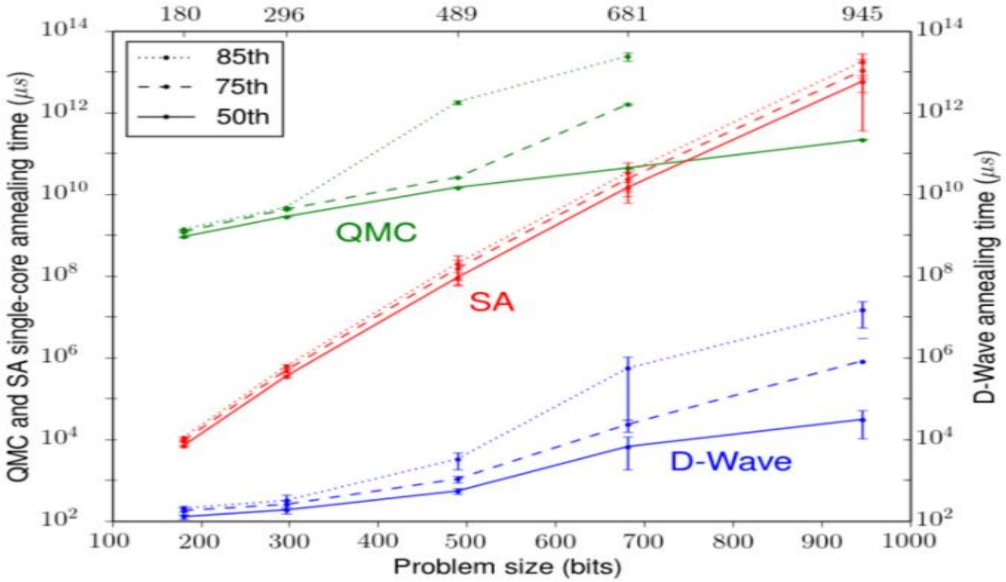
The optimum is at index "*a*",
Define Tagging Function :
$f(x) = 0, \; x \neq a$
$f(x) = 1, \; x = a$

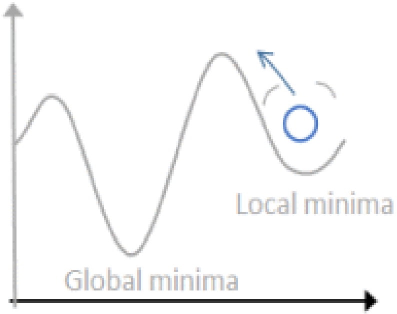
Quantum technology trends

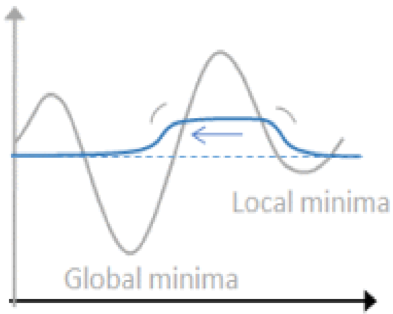


Quantum technology trends

“ OUR
QUANTUM COMPUTER
IS
100 MILLION TIMES FASTER
THAN PC.
- GOOGLE







IBM’s 1,121-Qubit Condor

IBM Quantum System Two

Qubit technologies

Organization	Adiabatic/Annealing	Superconducting	Trapped Ion	Cold/Neutral Atom	Spin/Quantum Dot	Photonic	NV Diamond	Topological
Total Number = 97	**7**	**23**	**17**	**9**	**12**	**16**	**6**	**7**
Alibaba/CAS		X						
Alpine Quantum Technologies			X					
Archer Exploration					X			
Atom Computing				X				
Bleximo		X						
CEA-Leti / Inac					X			
Centre for Quantum Computation & Communication Technology					X	X		
Chalmers University of Technology		X						X
ColdQuanta				X				
Duke University			X			X		
D-Wave	X							
EeroQ				X				
Google	X	X						
Griffith Univ./Univ. Of Queensland						X		
Honeywell			X					
IBM		X						
ID Quantique						X		
Institut d'Optique				X				
Intel		X			X			
IonQ			X					
IQM Finland		X						
Korea Institute of Science & Technology							X	
MDR	X	X						
Microsoft								X
MIT Lincoln Lab	X	X	X				X	
MIT/Univ. of Innsbruck			X					
NEC	X							
NextGenQ			X					
Niels Bohr Institute								X
Nokia Bell Labs								X
Northrop Grumman	X							
NQIT			X					

Source : *https://quantumcomputingreport.com/scorecards/qubit-technology/*


Q & A