Quantum Algorithms

Deutsch - Jozsa Algorithm.

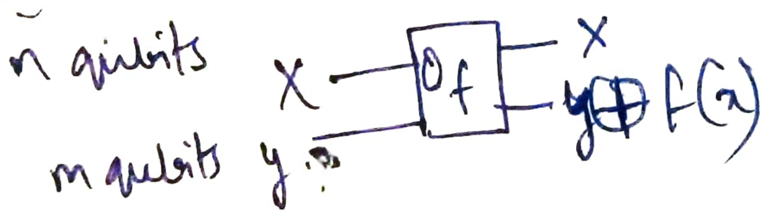
Oracles:

→ Assume we have access to an oracle, e.g. a physical device (black box), to which we can pass queries and it returns answers.

Goal: determine some property of the oracle using the minimal no. of queries.

→ On a classical computer, an oracle is given by a function $f : \{0,1\}^n \to \{0,1\}^m$

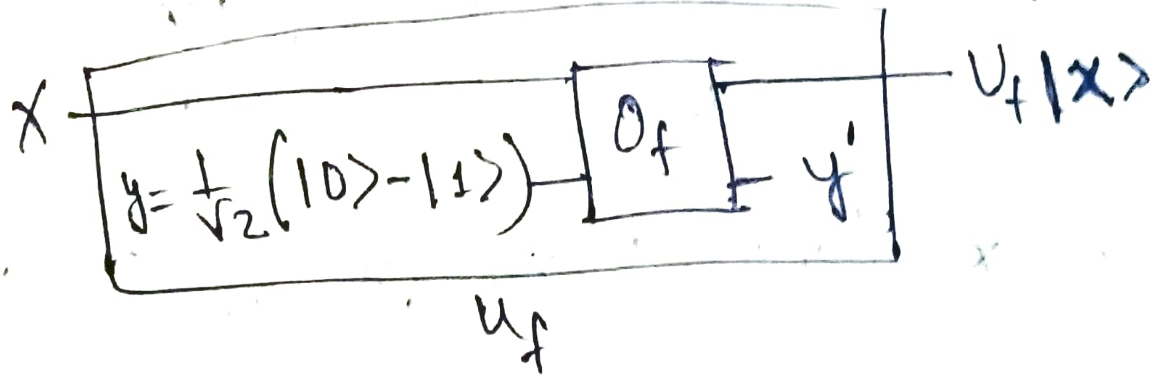
→ On a quantum computer, the oracle must be reversible.



O_f → Bit Oracle → Unitary gate which performs the map.

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

→ for $f: \{0,1\}^n \to \{0,1\}$, we can construct a phase oracle U_f



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

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

$f(x)$ can be either 0 and 1.

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

$$\boxed{|1 \oplus 1\rangle = |0\rangle}$$

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

→ Independent of $|y\rangle \Rightarrow U_f$: phase oracle which perform the map: $U_f|x\rangle = (-1)^{f(x)}|x\rangle$

Hadamard on n qubits.

Recall that $H|0\rangle = |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$

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

for $x \in \{0,1\}$: $|x\rangle - \boxed{H} - |y\rangle = \frac{1}{\sqrt{2}}(|0\rangle + (-1)^x|1\rangle)$

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

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

→ for $x \in \{0,1\}^n$

$$|x\rangle \left\{\begin{array}{l} |x_0\rangle \longrightarrow \boxed{H} \longrightarrow |y_0\rangle \\ |x_1\rangle \longrightarrow \boxed{H} \longrightarrow |y_1\rangle \\ \quad\vdots \\ |x_{n-1}\rangle \longrightarrow \boxed{H} \longrightarrow |y_{n-1}\rangle \end{array}\right\} |y\rangle = H^{\otimes n}|x\rangle$$

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

→ Every $|y_i\rangle$ is either $|+\rangle$ / $|-\rangle$

→ $|y\rangle$ must be superposition of all possible 2^n bitstrings

E.g: $|x\rangle = |01\rangle$

$$\left.\begin{array}{l} |0\rangle - \boxed{H} - |+\rangle \\ |1\rangle - \boxed{H} - |-\rangle \end{array}\right\} |y\rangle = \frac{1}{\sqrt{2^2}}\Big[(-1)^{(00)\binom{0}{1}}|00\rangle + (-1)^{(01)\binom{0}{1}}|01\rangle + (-1)^{(10)\binom{0}{1}}|10\rangle + (-1)^{(01)\binom{0}{1}}|11\rangle\Big]$$

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

Deutsch-Jozsa Algorithm

(1st Quantum Algorithm)

→ We are given a fn. $f: \{0,1\}^n \rightarrow \{0,1\}$, realized by an oracle (of which we know that it is either const. (All inputs gives same output) or balanced (No. of inputs maps to 0 = No. of inputs maps to 1)

<u>Goal</u>: Determine whether f(x) is constant or balanced.

<u>Classical Soln</u>: We need to ask the oracle at least twice, but if we get twice the same output, we need to ask again for

→ atmost $(N/2 + 1)$ times

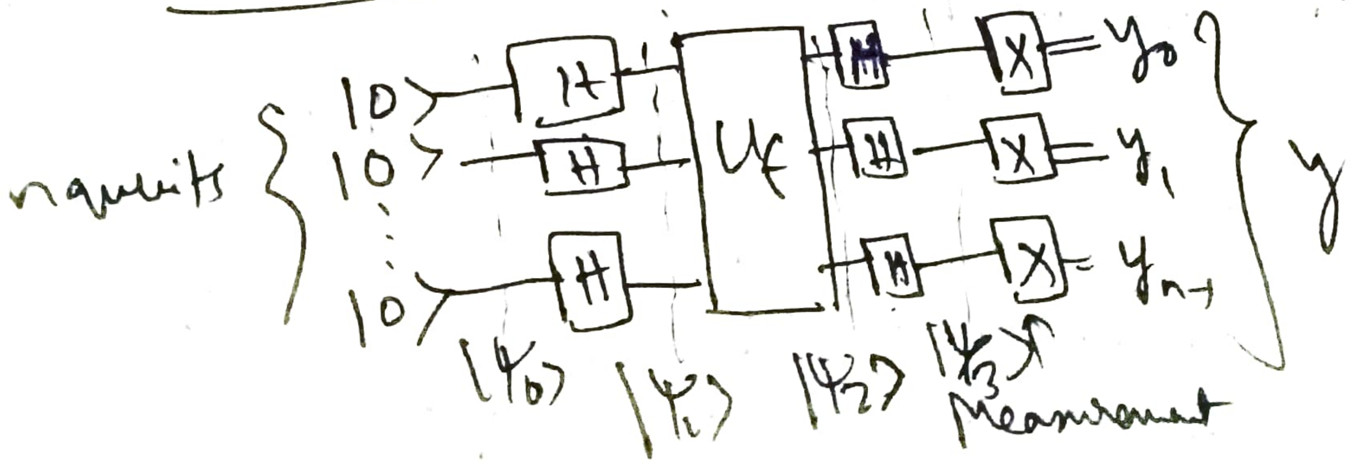
$= 2^{n-1} + 1$ queries

n = no. of input bits.

$N = 2^n$: Realizable bit strings.

<u>Quantum Soln</u>: Need only 1 query.

Circuit for Deutsch Jozsa (DJ)



Claim: If the total output y equals the bitstring $\underbrace{00\cdots0}_{n}$, then f is const.

otherwise f is balanced.

Proof: Let us check the state after each step:

- $|\psi_0\rangle = |00\cdots0\rangle = |0\rangle^{\otimes n}$
- $|\psi_1\rangle = H^{\otimes n}|\psi_0\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{\overbrace{x\cdot\psi_0}^{0}} |x\rangle$

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

- $|\psi_2\rangle = U_f|\psi_1\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} U_f|x\rangle$

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

- $|\psi_3\rangle = H^{\otimes n}|\psi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{f(x)} H^{\otimes n}|x\rangle$

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

$$= \sum_{k\in\{0,1\}} \Bigg[\underbrace{\frac{1}{2^n}\sum_{x\in\{0,1\}^n}(-1)^{f(x)+k\cdot x}}_{=C_k}\Bigg]|k\rangle$$

$$= \sum_{k\in\{0,1\}^n} C_k\,|k\rangle$$

<u>Probability to measure the zero-string $|00\cdots0\rangle$</u>

$$P[y=00\cdots0] = |\langle 00\cdots0|\psi_3\rangle|^2$$

$$= \Big|\sum_{k\in\{0,1\}^n} C_k \underbrace{\langle 00\cdots0|k\rangle}_{=\begin{cases}1, & k=00\cdots0\\ 0, & \text{else because (orthogonal)}\end{cases}}\Big|^2$$

$$= |C_{00\cdots0}|^2$$

$$= \Big|\frac{1}{2^n}\sum_{x\in\{0,1\}^n}(-1)^{f(x)+\overset{0^n}{k}\cdot x}\Big|^2$$

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

$$\underbrace{\sum_{x \in \{0,1\}^n} (-1)^{f(x)}} = \begin{cases} +2^n, & f(x)=0 \\ -2^n, & f(x)=1 \\ 0, & f(x) = \text{balanced}. \end{cases}$$

So, $$\left| \frac{1}{2^n} \sum_{x \in \{0,1\}^n} (-1)^{f(x)} \right|^2 = \begin{cases} 1, & f \to \text{const.} \\ 0, & f \text{ is balanced} \end{cases}$$

Probability of measuring 0 bitstring.