# Quantum Algorithms

✓ **Deutsch - Jozsa problem**

Given a function $f : \{0,1\}^n \to \{0,1\}$, s.t.

(1) $f(x) = 0$ for all input $x$ ($f$ is a constant function)

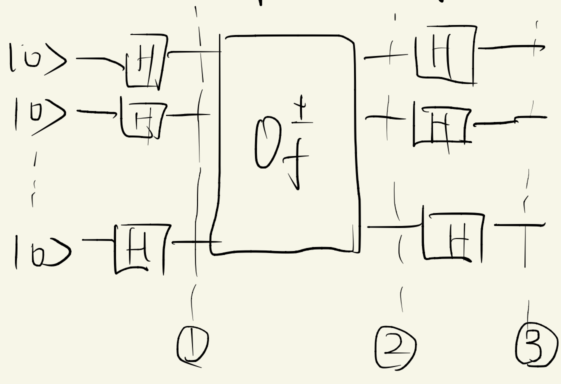
(2) $f(x) = 0$ for half of the input $x$ and $f(x) = 1$ for others ($f$ is a balanced function).

Question: is $f$ constant or balanced?

classically: worst case we need $2^{n-1}+1$ queries to $f$.

Quantumly: only 1 query to $O_f^{\pm}$.

Solution: suppose $O_f^{\pm}$ is the phase oracle we build for the function $f: \{0,1\}^n \to \{0,1\}$.




From last lecture:

① A uniform superposition state $\frac{1}{(\sqrt{2})^n} \sum_{x \in \{0,1\}^n} |x\rangle$

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

③ Let us compute the coefficient $\alpha_0$ for $|000\cdots0\rangle$ state

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

$y=0 \Rightarrow (-1)^{x\cdot y} = 1$

If we only focus on the term for $|00\cdots0\rangle$

$$|x\rangle \xrightarrow[\text{only for } |000\cdots0\rangle]{H^{\otimes n}} \frac{1}{(\sqrt{2})^n} |00\cdots0\rangle$$

plug in the result for ②

$$\frac{1}{(\sqrt{2})^n} \sum_{x\in\{0,1\}^n} (-1)^{f(x)} |x\rangle \xrightarrow[\text{only for } |00\cdots0\rangle]{H^{\otimes n}} \frac{1}{2^n} \sum_{x\in\{0,1\}^n} (-1)^{f(x)} |00\cdots0\rangle$$

If $f(x)=0$ for all $x$, $\alpha_0 = \frac{1}{2^n}\cdot 2^n = 1$

If $f(x)$ is balanced, $\alpha_0 = \frac{1}{2^n}\Big(\sum_{\substack{f(x)=0\\ x\in\{0,1\}^n}} (-1)^0 + \sum_{\substack{f(x)=1\\ x\in\{0,1\}^n}} (-1)^1\Big) = 0$

That is to say, after ③, we only need to measure all qubits in $Z$ basis.

If the results are 0 for all qubits, then $f$ is constant

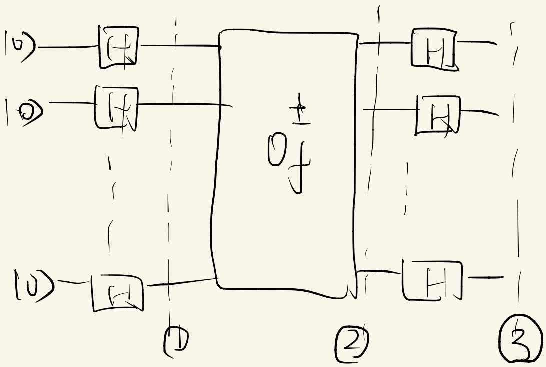
Otherwise, $f$ is balanced.

Insight: $O_f^{\pm}$ gives two different interference patterns for two different types of $f$.

Deutsch-Jozsa Algorithm is a very special algorithm with very special constraints on the function $f$.

Can we do something that is more general?

Let us review the basic computation pattern again.




If ② $= \frac{1}{(\sqrt{2})^n} \sum_{x \in \{0,1\}^n} |x\rangle$ ③ $= |00\cdots0\rangle$

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

Here $v \in \{0,1\}^n$ is a special n-bit number.

what is the result for ③ ?

Again, recall

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

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

Thus, the result for ③ will just be $|v\rangle$

## Bernstein–Vazirani Algorithm

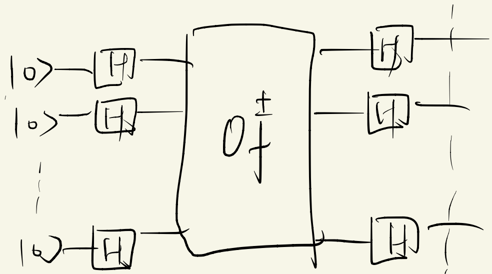
Give a function $f^v: \{0,1\}^n \to \{0,1\}$

$f^v(x) = x \cdot v$, where $v$ is a n-bit binary number.

For example for $v = 11$, $x = 11$

$$f^v(x) = 1 \cdot 1 \oplus 1 \cdot 1 = 0$$

$$= \sum_i x_i \cdot v_i \mod 2$$




$O_f^{\pm}$ is the phase oracle for the special function $f^v$.

$③ = |v\rangle$

measurement result is exactley $v$.

**Remark:** $H^{\otimes n}$ can extract hidden variable $v$ from $f^v(x) = x \cdot v$.

How many different $f^v$ functions are there? $2^n$

One query can determine the specific value of $v$.

**Key insight:** $x$ that is different from $v$ will have negative interference and cancel out with each other in the final output.

Only $x$ that equals $v$ remains after the interference

Summary so far:

Deutsch-Jozsa

$$f \text{ is } \begin{cases} \text{constant} : f(x) = 0 \\ \text{balanced} : \begin{array}{l} f(x) = 0 \text{ for half the inputs} \\ f(x) = 1 \text{ for half the inputs.} \end{array} \end{cases}$$

Bernstein Vazirani:

$$f^{v}(x) = x \cdot v = \sum_i x_i v_i \mod 2$$

Can we reveal more general patterns in $O_f$ ?

→ Yes. Simon's algorithm. → periodicity

→ Quantum Fourier transform over $\mathbb{Z}_2$, $\mathbb{Z}_2^n$, and $\mathbb{Z}_{2^n}$

→ Shor's algorithm

## Simon's algorithm:

√Given oracle $O_f$ for function $f: \{0,1\}^n \to \{0,1\}^m$ with the promise that for some unknow period $s \in \{0,1\}^n$, for all $x_1, x_2 \in \{0,1\}^n$, $f(x_1) = f(x_2)$ if and only if $x_1 = x_2$ or $x_1 \oplus s = x_2$ here $\oplus$ denotes bitwise XOR. How to get $s$? (suppose $s$ is non-trivial. i.e., $s \neq 0$)

Practice: $010 \oplus 110$

$= (0+1 \bmod 2,\ 1+1 \bmod 2,\ 0+0 \bmod 2)$

$= (1, 0, 0)$

$= 100$

Practice: Function with Simon's property.

| $x$ | $f(x)$ |
|---|---|
| 000 | 101 |
| 001 | 010 |
| 010 | 000 |
| 011 | 110 |
| 100 | 000 |
| 101 | 110 |
| 110 | 101 |
| 111 | 010 |

$\{0,1\}^3 \to \{0,1\}^3$

what is $s$ here? How many queries did you use?

✓ Guess what is the worst case complexity to solve this problem classically? : $O(\sqrt{2^n})$

Let us start with an easy case for $n = 2$. We first evaluate $f(00)$. ① → $f(10) ?= f(00)$ ② → $\begin{cases} f(11) ?= f(00) \\ f(11) ?= f(10) \end{cases}$

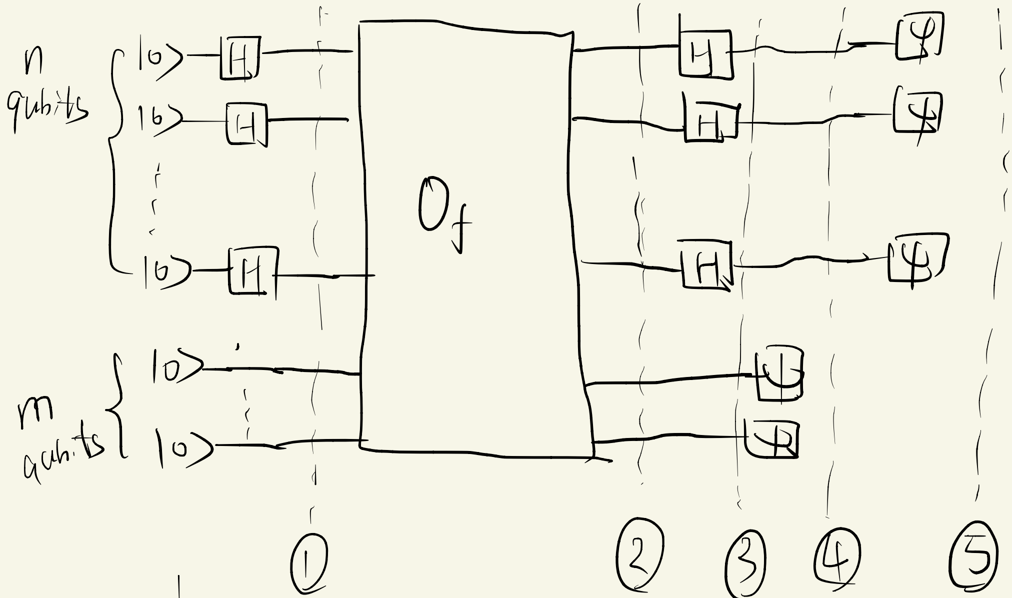
... ⓚ → $\frac{k \cdot (k-1)}{2}$ pairs of comparison

This is exactly the same as the birthday paradox.

→ In a set of 23 randomly choosen people, the propability that two will share a birthday is higher than 50%

→ Intuitively, there are $\frac{23 \cdot 22}{2} = 253$ pairs to consider, more than half the number of days in a year.

✓ Now let us work out the Simon's solution.




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

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

③ $\frac{1}{\sqrt{2^n}} \sum_{x} \left( \frac{1}{\sqrt{2^n}} \sum_{y} (-1)^{x \cdot y} |y\rangle \right) |f(x)\rangle$

$= \frac{1}{2^n} \sum_{x} \sum_{y} (-1)^{x \cdot y} |y\rangle |f(x)\rangle$

④ now the partial measurement, recall what we learnt before.

$= \frac{1}{\sqrt{2^n}} \sum_{c} \sum_{y} \sum_{f(x)=c} (-1)^{x \cdot y} |y\rangle |c\rangle$

key here is that we combine $x$ that generate the same $f(x)=c$

~~s~~uppose the measurement results for the ~~bottom~~ qubits is c.

The state will collapse to

normalization term $\rightarrow$ $$\frac{1}{\boxed{\phantom{x}}} \sum_y \sum_{f(x)=c} (-1)^{x \cdot y} |y\rangle |c\rangle$$

Now, let us ~~think~~ about what x can lead to $f(x)=c$, Given the assumption of the simon's algorithm, there shall be a pair of x, $x_1$ and $x_2$, and $x_2 = x_1 \oplus s$, s.t., $f(x_1) = f(x_2) = c$.

Thus, we can rewrite the state:

$$\frac{1}{\sqrt{2^n}} \sum_y \left((-1)^{x_1 \cdot y} + (-1)^{x_2 \cdot y}\right) |y\rangle |c\rangle$$

$$= \frac{1}{\sqrt{2^n}} \sum_y (-1)^{x_1 \cdot y} \left(1 + (-1)^{s \cdot y}\right) |y\rangle$$

$$\begin{cases} \text{if } s \cdot y = 0 & \rightarrow 2 \\ \text{if } s \cdot y = 1 & \rightarrow 0 \end{cases}$$

⑤ Now we measure the top n qubit, suppose the result is w.

what we have learned from this result?

$$s \cdot w = 0$$

Simon's algorithm tells us to run the quantum circuit $O(n)$ times.

$$\begin{aligned} s \cdot w_1 &= 0 \\ s \cdot w_2 &= 0 \\ s \cdot w_3 &= 0 \\ &\vdots \\ s \cdot w_{n-1} &= 0 \end{aligned} \qquad \left[ \begin{array}{c} \text{---}\; w_1 \;\text{---} \\ \text{---}\; w_2 \;\text{---} \\ \vdots \\ \text{---}\; w_{n-1} \;\text{---} \end{array} \right] \left[ \begin{array}{c} | \\ s \\ | \end{array} \right] \bmod 2 = 0$$

We can solve effeciently using classical methods, for example, Gaussian elimination. This is the second step of Simon's algorithm, classical post-processing

Example: If we measure and get $w_1 = 100$, what do we know?

$$(1 \cdot s_0 + 0 \cdot s_2 + 0 s_3) \bmod 2 = 0$$
$$\Rightarrow s_0 = 0$$

Repeat. if we get $W_2 = 111$

$$(1 \cdot s_0 + 1 \cdot s_2 + 1 s_3) \bmod 2 = 0$$
$$\Rightarrow s_2 = s_3 = 1 \quad \text{why?}$$

why $O(n)$, not exactly $n-1$, or $n$?

① $n \to n-1$

$S$ is has a trival answer that is $S=0$

If we have $n$ independent equations for $S \cdot V = 0$

then we will only have one unique answer $S=0$

② $n-1 \to O(n)$

Now the question is how to get $n-1$ independent equations.

1) First try: as long as $W_1 \neq 0$. It works

$$P_1 = \left(1 - \frac{1}{2^n}\right)$$

2) Second try $W_2 \neq 0$

$W_2 \neq W_1$

$$P_2 = \left(1 - \frac{2}{2^n}\right)$$

3) third try $W_3 \neq 0, W_1, W_2, W_1 \oplus W_2$

$$P_3 = \left(1 - \frac{2^2}{2^n}\right)$$

4) ... $k$ th try

$$P_k = \left(1 - \frac{2^{k-1}}{2^n}\right)$$

$$P_1 \cdot P_2 \cdots P_{n-1} \geq \frac{1}{4}$$ Some well-know inequality

Classical Fourier Transform $\longleftrightarrow$ Quantum Fourier Tranform

(Classical) Discrete Fourier Transform (DFT)

A sequence of complex numbers: $A = \alpha_0, \alpha_1, \cdots, \alpha_{N-1}$

Another sequence of complex numbers: $B = \beta_0, \beta_1, \cdots, \beta_{N-1}$

$$A = \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_{N-1} \end{bmatrix} \xrightarrow{F_N} B = F_N \cdot A = \begin{bmatrix} \beta_1 \\ \vdots \\ \beta_N \end{bmatrix}$$

$F_N$: Fourier matrix

$$= \frac{1}{\sqrt{N}} \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & w & w^2 & \cdots & w^{N-1} \\ 1 & w^2 & w^4 & \cdots & w^{2(N-1)} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 1 & w^{N-1} & w^{2(N-1)} & \cdots & w^{(N-1)^2} \end{bmatrix}$$

$F_N[k,j] = \frac{w^{jk}}{\sqrt{N}}$, where $w = e^{i2\pi/N}$ "Nth root of unity"

$$B = F_N \cdot A \Rightarrow \begin{cases} \beta_k = \frac{1}{\sqrt{N}} \sum_j \alpha_j w^{jk} \\ \alpha_j = \frac{1}{\sqrt{N}} \sum_k \beta_k w^{jk} \end{cases}$$

Note: $F_N$ is a unitary matrix.

# Quantum Fourier Transform

$$|\psi_A\rangle = A = \begin{bmatrix} \alpha_0 \\ \vdots \\ \alpha_{N-1} \end{bmatrix} = \sum_j \alpha_j |j\rangle$$

$$|\psi_B\rangle = B = \begin{bmatrix} \beta_0 \\ \vdots \\ \beta_{N-1} \end{bmatrix} = \sum_k \beta_k |k\rangle$$

Fourier matrix $F_N = \sum_j \sum_k \frac{1}{\sqrt{N}} w^{jk} |k\rangle\langle j|$

Example: $N=2$ for 1 qubit, $w = e^{i2\pi/N} = -1$

$$F_2 = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \underline{H}$$ Hadamard gate.

$$\beta_k = \frac{1}{\sqrt{2}} \sum_j w^{jk} \cdot \alpha_j = \frac{1}{\sqrt{2}} \sum_j \alpha_j (-1)^{jk}$$

$$\begin{cases} \beta_1 = \dfrac{\alpha_0 + \alpha_1}{\sqrt{2}} \\ \beta_2 = \dfrac{\alpha_0 - \alpha_1}{\sqrt{2}} \end{cases}$$

from Z basis to X basis

## Boolean Quantum Fourier Transform ($H^{\otimes n}$)

$$\begin{cases} H^{\otimes n} |x\rangle = \frac{1}{(\sqrt{2})^n} \sum_y (-1)^{x \cdot y} |y\rangle \\ H^{\otimes n} \left( \frac{1}{(\sqrt{2})^n} \sum_y (-1)^{x \cdot y} |y\rangle \right) = |x\rangle \end{cases}$$

$N=2$ but for $n$ qubits

$x \cdot y = \sum x_i y_i$ mod 2

Now let us look at the most general case that matches exactly the classical setting

Let us set $N = 2^n$ for $n$ qubits

$$w = e^{i2\pi/2^n}$$

$$F_{2^N} = \frac{1}{\sqrt{2^N}} \sum_{j,k} w^{jk} |k\rangle\langle j|$$

Take $n=4$ as an exaple, for a input state $|j\rangle$

what is $F_{n^2} \cdot |j\rangle$

$$|j\rangle \longrightarrow \frac{1}{4}\left(|0\rangle + w^{j \cdot 1}|1\rangle + w^{j \cdot 2}|2\rangle + \cdots + w^{j \cdot 15}|15\rangle\right)$$

$$= \frac{1}{4}\left(|0000\rangle + w^{j}|0001\rangle + w^{2j}|0010\rangle + \cdots + w^{15}|1111\rangle\right)$$

We know $F_N$ is a unitary matrix, but can we find a simple circuitt with just 1-qubit and 2-qubit gate to implement it? In this case, we just consider $F_{16}$ for 4 qubits.

key observation:

The output state is dis-entangled.

$$|j\rangle \xrightarrow{F16} \frac{1}{\sqrt{2}}(|0\rangle + w^{8j}|1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + w^{4j}|1\rangle)$$

$$\otimes \frac{1}{\sqrt{2}}(|0\rangle + w^{2j}|1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + w^{j}|1\rangle)$$

Rewrite $|j\rangle$ as $|j_3 j_2 j_1 j_0\rangle$

where $j = 8j_3 + 4j_2 + 2j_1 + j_0$ $\left(j = \sum_{s=0}^{n-1} 2^s j_s\right)$

Notice $W = e^{i2\pi/16}$, so $W^{16} = e^{i2\pi} = 1$

$$W^{8j} = e^{i\pi j} = e^{i\pi(8j_3 + 4j_2 + 2j_1 + j_0)}$$

$$= e^{i\pi j_0} = (-1)^{j_0}$$

First Qubit $\Rightarrow$ $|j_0\rangle \to \frac{1}{\sqrt{2}}(|0\rangle + w^{8j}|1\rangle) = \frac{1}{\sqrt{2}}(|0\rangle + (-1)^{j_0}|1\rangle)$

$$\left\{\begin{array}{l} |0\rangle \to \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ |1\rangle \to \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \end{array}\right. \Rightarrow H \text{ gate}$$

$$|j_0\rangle \;\text{———}\; \boxed{H} \;\text{———}\; \frac{1}{\sqrt{2}}(|0\rangle + (-1)^{j_0}|1\rangle)$$

Next qubit $|j_1\rangle$

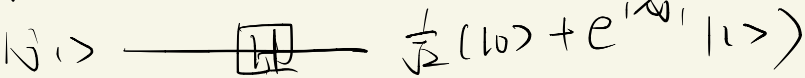
$$|j_1\rangle \longrightarrow \frac{1}{\sqrt{2}}\left(|0\rangle + w^{4j}|1\rangle\right)$$

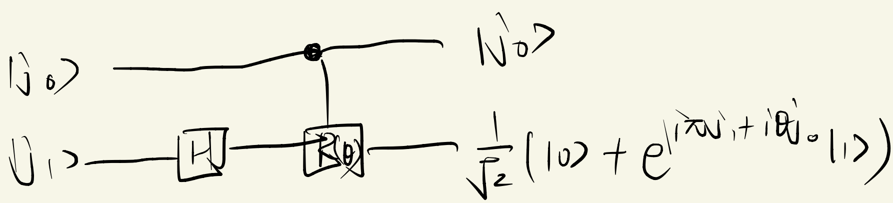
$$= \frac{1}{\sqrt{2}}\left(|0\rangle + e^{\frac{i2\pi}{16}\cdot 4j}|1\rangle\right)$$

$$= \frac{1}{\sqrt{2}}\left(|0\rangle + e^{\frac{i\pi}{2}(8j_3+4j_2+2j_1+j_0)}|1\rangle\right)$$

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

We have seen this before




set $\theta = \frac{\pi}{2}$, we are done

more on slides and book P217