Introduction to Quantum Computing | Lecturer: Tongyang, scribed by Shuo Zhou, Yexin Zhang
Fall 2023, Peking University | *Date: October 11, 2023*

Lecture 5

Introduction to Quantum Algorithms

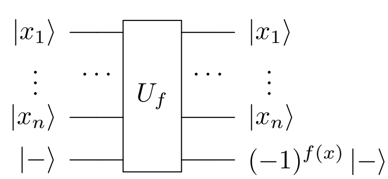
- Deutsch-Jozsa problem
- Simon's problem
- Quantum Fourier transform

1 Deustch-Jozsa problem

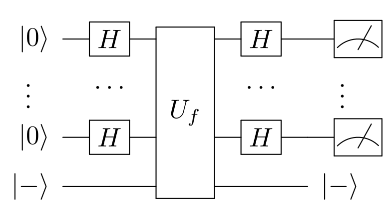
- Given: $f : \{0,1\}^n \longmapsto 0, 1$(by a black box).
- Promise: f is either constant or balanced.
  - constant: either all 2^n elements map to 0 or all 2^n elements map to 1;
  - balanced: exactly 2^{n-1} elements map to 0 and 2^{n-1} elements map to 1.
- Determine for sure which holds in the promise.

Classically: we need $2^{n-1} + 1$ queries.
Quantumly: $x \in \{0,1\}^n, \quad x = x_1 \cdots x_n,\ x_i \in \{0,1\}$.

$$|x\rangle |-\rangle \longmapsto \frac{1}{\sqrt{2}} |x\rangle \left(|f(x)\rangle - \overline{|f(x)\rangle}\right) = (-1)^{f(x)} |x\rangle |-\rangle$$



Algorithm:



$$|0\rangle^{\otimes n} |-\rangle \xmapsto{H^{\otimes n} \otimes I} |+\rangle^{\otimes n} |-\rangle = \sum_{x\in\{0,1\}^n} \frac{1}{\sqrt{2^n}} |x\rangle |-\rangle \xmapsto{U_f} \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{f(x)} |x\rangle |-\rangle \qquad (*)$$

Recall $H|x\rangle = \frac{|0\rangle + (-1)^x |1\rangle}{\sqrt{2}}, \quad x \in \{0,1\}$

As a result, for a certain $x \in \{0,1\}^n$, rewrite as $|x_1\rangle |x_2\rangle \dots |x_j\rangle$

$$H^{\otimes n} |x\rangle = \bigotimes_{j=1}^{n} \frac{|0\rangle + (-1)^{x_j} |1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2^n}} \sum_{y \in \{0,1\}^n} \prod_{j=1}^{n} (-1)^{x_j y_j} |y\rangle = \frac{1}{\sqrt{2^n}} \sum_{y \in \{0,1\}^n} (-1)^{x \cdot y} |y\rangle$$

Here $x \cdot y$ means bite-wise product $x \cdot y = x_1 y_1 + x_2 y_2 + \cdots + x_n y_n$

Plugging this into (*):

$$\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} (-1)^{f(x)} |x\rangle |-\rangle \overset{H^{\otimes n} \otimes I}{\longmapsto} \frac{1}{2^n} \sum_{x \in \{0,1\}^n} (-1)^{f(x)} \sum_{y \in \{0,1\}^n} (-1)^{x \cdot y} |y\rangle |-\rangle = \sum_{y \in \{0,1\}^n} a_y |y\rangle |-\rangle$$

where $a_y = \frac{1}{2^n} \sum_{\{0,1\}^n} (-1)^{f(x) + x \cdot y}$.

If f is a constant, then $a_y = \frac{(-1)^f}{2^n} \sum_{x \in \{0,1\}^n} (-1)^{x \cdot y}$

$a_{0\dots0} = (-1)^f$, $a_y = 0$ when $y \neq 0 \dots 0$ (say $y_i \neq 0$, then $x_i = 0$ and $x_i = 0$ cancel each other)

If f is balanced, $a_{0\dots0} = \frac{1}{2^n} \sum_{x \in \{0,1\}^n} (-1)^{f(x)} = 0$,

Conclusion: after we measure, if $y = 0 \dots 0$, output "constant". If $y \neq 0 \dots 0$, output "balanced".

Succeed with probability 1: $\begin{cases} \text{Classically, } 2^{n-1}+1 \text{ (determinisic) queries} \\ \text{Quantumly, } 1 \textit{ query} \end{cases}$

But with classical randomized algorithm, $O\left(\log \frac{1}{\epsilon}\right)$ queries with success probability $\geq 1 - \epsilon$:

Take $O\left(\log \frac{1}{\epsilon}\right)$ samples. If all same, output "constant". Otherwise output "balanced".

2 Simon's problem

- Given: a function $f : \{0,1\}^n \to X$ where $|X| \geq 2^{n-1}$.
- Promise: $\exists$ some $s \in \{0,1\}^n$, $s \neq 0^n$ such that $f(x) = f(y)$, if and only if $x = y$ or $x = y \oplus s$. "A structured 2-to-1 function"
- Find s.

Classically, without randomization: $2^{n-1} + 1$ queries with success probability 1.

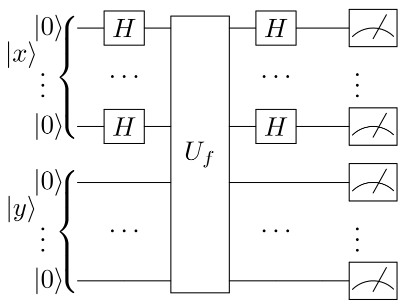
Classically, with randomization: Query $f(x_1), \dots f(x_k)$ with $x_i (1 \leq i \leq k)$ chosen at random from $\{0,1\}^n$, until we find $x_i \neq x_j$ such that $f(x_i) = f(x_j)$. Then return $s = x_i \oplus x_j$

By the analysis of the birthday paradox, we expect to find a collsion after $\Theta\left(\sqrt{2^n}\right) = \Theta\left(2^{\frac{n}{2}}\right)$ queries. In fact, this is optimal.

$$\begin{aligned} \Pr[\text{all different}] &= \left(1 - \frac{1}{N}\right) \cdots \left(1 - \frac{M}{N}\right) \\ &\geq 1 - \frac{1 + \cdots + M}{N} \geq \frac{7}{8} \quad \text{when } M = \frac{\sqrt{N}}{2} \end{aligned}$$

where $N = 2^n$.

Quantum algorithm: quantum black-box: $|x, y\rangle \xmapsto{U_f} |x, y \oplus f(x)\rangle$



$$
\begin{aligned}
|0\rangle^{\otimes n}|0\rangle^{\otimes m} &\xmapsto{H^{\otimes n} I^{\otimes m}} \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle |0^m\rangle \\
&\xmapsto{U_f} \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle |f(x)\rangle \\
&= \frac{1}{\sqrt{2^{n-1}}} \sum_{x \in R} \frac{|x\rangle + |x \oplus s\rangle}{\sqrt{2}} |f(x)\rangle
\end{aligned}
$$

$|R| = 2^{n-1}$, coset representation of f

Recall the effect of $H^{\otimes n}$(Hadamard transformation): $|x\rangle \xmapsto{H^{\otimes n}} \frac{1}{\sqrt{2^n}} \sum_{y \in \{0,1\}^n} (-1)^{x \cdot y} |y\rangle$.
Recall: $x \cdot y$ means bit-wise product $x \cdot y = x_1 y_1 + \cdots x_n y_n \pmod 2$
Plugging this into above:

$$
\begin{aligned}
\frac{1}{\sqrt{2^{n-1}}} \sum_{x \in R} \frac{|x\rangle + |x \oplus s\rangle}{\sqrt{2}} |f(x)\rangle \xrightarrow{H^{\otimes n} I^{\otimes m}} & \frac{1}{\sqrt{2^{n-1}}} \frac{1}{\sqrt{2^{n+1}}} \sum_{x \in R} \sum_{y \in \{0,1\}^n} \left[(-1)^{x \cdot y} + (-1)^{(x \oplus s) \cdot y}\right] |y\rangle |f(x)\rangle \\
&= \frac{1}{2^n} \sum_{x \in R} \sum_{y \in \{0,1\}^n} (-1)^{x \cdot y} \left[1 + (-1)^{s \cdot y}\right] |y\rangle |f(x)\rangle.
\end{aligned}
$$

We measure this state, for the first register, we get:

$$
\Pr[y] = \sum_{x \in R} \left|\frac{1}{2^n}(-1)^{x \cdot y}[1 + (-1)^{s \cdot y}]\right|^2 = \frac{1}{2^{n+1}} |1 + (-1)^{s \cdot y}|^2.
$$

Either $s \cdot y = 0 \Rightarrow \Pr[y] = \frac{1}{2^{n-1}}$ or $s \cdot y = 1 \Rightarrow \Pr[y] = 0 \bmod 2$.
Therefore, we get a random y, s.t. $s \cdot y = 0$ after the measurement.

Now we repeat this k times, we get $\begin{cases} s \cdot y_1 = 0 \\ \vdots \\ s \cdot y_k = 0 \end{cases}$

If we get $n-1$ linearly independent equations, we can solve for s. Each halves the possible solution space.
What's the probability?

$$
\begin{aligned}
\Pr[\text{linear independent}] &= \frac{2^n - 1}{2^n} \cdot \frac{2^n - 2}{2^n} \cdots\cdots \frac{2^n - 2^{n-1}}{2^n} \\
&= \prod_{i=1}^{n} \left(1 - \frac{1}{2^i}\right) \geq \prod_{i=1}^{\infty} \left(1 - \frac{1}{2^i}\right) \\
&\approx 0.289 \cdots > \frac{1}{4} \quad \text{(Euler's pentagonal constant).}
\end{aligned}
$$

Therefore, quantum algorithm can succeed with probability $\geq 1 - \epsilon$ using $O(n \log \frac{1}{\epsilon})$ queries.

3 Quantum Fourier transform

Hadamard transform: $|x\rangle \overset{H^{\otimes n}}{\longmapsto} \frac{1}{\sqrt{2^n}} \sum_{y \in \{0,1\}^n} (-1)^{x \cdot y} |y\rangle$ where x is an integer modulo 2^n.
This is a Fourier transform over $\underbrace{\mathbb{Z}_2 \otimes \cdots \otimes \mathbb{Z}_2}_{n}$.

How about Fourier transform over $\mathbb{Z}_{2^n}$? That has the form:

$$|x\rangle \longmapsto \frac{1}{\sqrt{2^n}} \sum_{y \in \mathbb{Z}_{2^n}} e^{\frac{2\pi i x y}{2^n}} \; |y\rangle := |\tilde{x}\rangle$$

where $x \in \mathbb{Z}_{2^n}$ represents an integer modulo 2^n.
These states form an orthonormal basis, the Fourier basis: $\langle \tilde{x} \mid \tilde{x}' \rangle = \delta_{x,x'}$.
When do we need the quantum Fourier transform?