CS6846 – Quantum Algorithms and Cryptography

Going beyond Classical: Deutsch and Deutsch-Jozsa

Instructor: Shweta Agrawal, IIT Madras
Email: shweta@cse.iitm.ac.in

Phase Kickback

Now consider superposition of function outputs.
Apply C_f to $(|+\rangle, |0\rangle)$.

Let $f: \{0,1\}^n \to \{0,1\}$

Recall $C_f(|x\rangle \underline{|b\rangle}) \to |x\rangle |b \oplus f(x)\rangle$.

When $b = 0$, I get $|x\rangle |f(x)\rangle$.

$b = 1$, I get $|x\rangle |1 \oplus f(x)\rangle$

$= |x\rangle |\neg f(x)\rangle$.

Concisely $\forall\ b \in \{0,1\}$

$$C_f(|x\rangle |b\rangle) = |x\rangle |(-1)^b f(x)\rangle$$

Swap b with $|-\rangle = \dfrac{|0\rangle - |1\rangle}{\sqrt{2}}$

Scratch Pad

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

$$= \frac{|x\rangle|f(x)\rangle - |x\rangle|\neg f(x)\rangle}{\sqrt{2}}.$$

$$= |x\rangle\left(\frac{|f(x)\rangle - |\neg f(x)\rangle}{\sqrt{2}}\right).$$

If $f(x)=0$, I get $|x\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}}$

$f(x)=1$ I get $|x\rangle \frac{|1\rangle - |0\rangle}{\sqrt{2}}$

In general, $C_f(|x\rangle \underline{\underline{|-\rangle}}) = (-1)^{f(x)} |x\rangle |-\rangle.$

$$C_f\left(\sum_x \frac{|x\rangle|-\rangle}{2^{n/2}}\right) = \sum_{x\in\{0,1\}^n} (-1)^{f(x)} \frac{|x\rangle|-\rangle}{2^{n/2}}$$

Deutsch's Algorithm

Quantum computation is . . . nothing less than a distinctly new way of harnessing nature . . . It will be the first technology that allows useful tasks to be performed in collaboration between parallel universes, and then sharing the results.

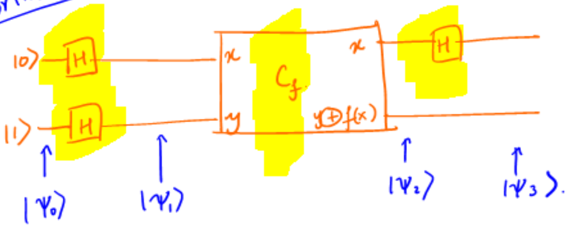
Deutsch's Algorithm

Promise.

Setup: Consider Boolean function $f : \{0,1\} \to \{0,1\}$. Given that f is either constant, i.e. $f(0) = f(1)$ or balanced, i.e. $f(0) \neq f(1)$. Which?

Query complexity to fn

Algorithm



$$|\psi_1\rangle = |+\rangle|-\rangle$$

Apply Phase Kickback:

Case 1: $f(0) = f(1)$

$$|\psi_2\rangle = \frac{1}{\sqrt{2}}\left[(-1)^{f(0)}\, |0\rangle|-\rangle + (-1)^{f(1)}\, |1\rangle|-\rangle\right]$$

Setup: Consider Boolean function $f : \{0,1\} \to \{0,1\}$. Given that f is either constant, i.e. $f(0) = f(1)$ or balanced, i.e. $f(0) \neq f(1)$. Which?

Figure this out using *single* query to f.

g get $(-1)^{f(0)} \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) (|-\rangle)$.

$= (-1)^{f(0)} |+\rangle |-\rangle$.

On the other hand if $f(0) \neq f(1)$

$|\Psi_2\rangle = \pm \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) |-\rangle$.

$= \pm |-\rangle |-\rangle$.

Scratch Pad

Apply Hadamard on first qubit,

$|\psi_3\rangle$ is $\pm |0\rangle |-\rangle$ if $f(0) = f(1)$

$\pm |1\rangle |-\rangle$ if $f(0) \neq f(1)$.

Note if $f(0) = f(1)$ then $f(0) \oplus f(1) = 0$

else $f(0) \oplus f(1) = 1$.

$$|\psi_3\rangle = \pm |f(0) \oplus f(1)\rangle |-\rangle$$

Generalizing to n bits: Deutsch-Jozsa

Setup: Consider Boolean function $f : \{0,1\}^n \to \{0,1\}$. Given that f is either constant or balanced. Which?

Generalizing to n bits: Deutsch-Jozsa

Setup: Consider Boolean function $f : \{0,1\}^n \to \{0,1\}$. Given that f is either constant or balanced. Which?

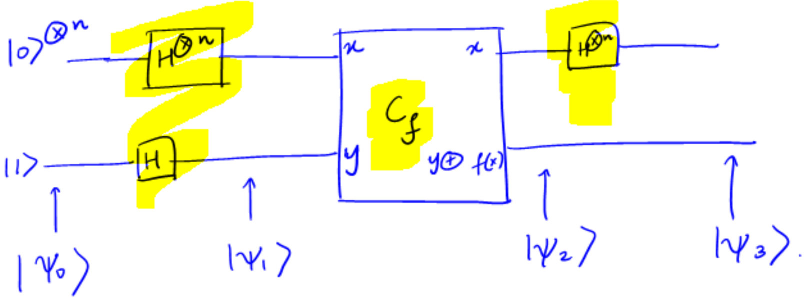
Classical Deterministic: $\Theta(2^n)$. Classical Randomized: constant.

Generalizing to n bits: Deutsch-Jozsa

Setup: Consider Boolean function $f : \{0,1\}^n \to \{0,1\}$. Given that f is either constant or balanced. Which?

Classical Deterministic: $\Theta(2^n)$. Classical Randomized: constant.

Quantum: *Single* query to f.



Measure top n qubits.

Scratch Pad

$$|\psi_0\rangle = |0\rangle^{\otimes n}|1\rangle. \qquad |\psi_1\rangle = \sum_{x\in\{0,1\}^n} |x\rangle / 2^{n/2} \; |-\rangle$$

Apply C_f (Phase kickback) $|\psi_2\rangle = \sum_{x\in\{0,1\}^n} \frac{(-1)^{f(x)} |x\rangle|-\rangle}{2^{n/2}}.$

Aside. For single bit.

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

$\Rightarrow$ $H(|x\rangle)$ can be written as $\sum_{z\in\{0,1\}} (-1)^{x\cdot z} \frac{|z\rangle}{\sqrt{2}}.$

For n bits:

$$H^{\otimes n} \underbrace{|x_1 \ldots x_n\rangle}_{\text{single pt}} = \sum_{z_1\cdots z_n \in\{0,1\}^n} \frac{(-1)^{\langle x, z\rangle \bmod 2} |z_1 \ldots z_n\rangle}{2^{n/2}}$$

Scratch Pad

$$|\psi_3\rangle = H^{\otimes n}\left(|x\rangle\right)|y \oplus f(x)\rangle$$

$$= \sum_{x\in\{0,1\}^n} \frac{H^{\otimes n}\left((-1)^{f(x)}|x\rangle\right)(|-\rangle)}{2^{n/2}}$$

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

Let us consider $|z\rangle = |0\cdots 0\rangle$. $\langle x;z\rangle = 0$.

$$|\psi_3\rangle = 2^{-n}\underbrace{\left(\sum_x (-1)^{f(x)}\right)}|00\cdots 0\rangle|-\rangle$$

$$\sum_{x:f(x)=0} 1 - \sum_{x:f(x)=1} 0 \quad = 0 \text{ if } f \text{ balanced}$$

$$= \pm 2^n \text{ o.w.}$$

Scratch Pad

Cryptography

Π

Encrypt $(PK, m) \to CT$

Decrypt $(SK, CT) \to m.$

A 

$CT. \not\to m.$

Does not distinguish $CT(m_0)$ & $CT(m_1)$ with prob. "somehow" better than $1/2$.

Reduction.

N 500 bits.

R.

Π

A.

Chall.

Factors of N.