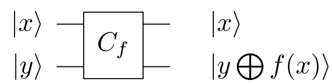
Quantum Algorithms, Spring 2022: Lecture 5 Scribe

Praguna Manvi, Samay Kathari

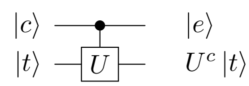
February 13, 2022

1 Recap

- Reversible circuits produce unwanted garbage bits that are dependent on the input and are entangle with the desired out bits, so we need : **Uncomputing!**



- Quantum Circuits
  - Single Qubit Gates: $X, Y, Z, R_\phi, h, \ldots$
  - Two Qubit Gates: CNOT, any $C - U$ where U is a single qubit gate.



$$\equiv \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & & \\ 0 & 0 & \multicolumn{2}{c}{\text{U}} \end{pmatrix}$$

$\forall$ U is any single qubit gate.

2 Universality of Quantum circuits

I will provide you some statements regarding the universality of quantum circuits without necessarily proving them.

- **Statement 1:** {CNOT, all single qubit gates} : universal for Quantum Computing
- **Statement 2:** The set of { CNOT, H, $R_{\pi/4}$} : universal for Quantum Computing
  Any other quantum circuit can be well approximated using quantum circuits of only these gates.

2.1 Formalizing Statement 2

Let $G = \{CNOT, H, R_{\pi/4}\}$, then for any quantum circuit U, $\in$ a number t, such that

$$||U - U_t U_{t-1} \ldots U_1|| \leq \epsilon, where$$

$$\text{each } U_j \in G$$
$$||\quad|| : \text{spectral norm}$$
$$||A|| = max_{\langle\psi||\psi\rangle=1}||A\,|\psi\rangle||$$

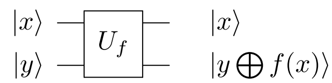
- How large should 't' be? Clearly, it better not be too large.
- Luckily 't' isn't too large owing to crucial result by Solvay and Kitaev

3 Solovay Ketanov Theorem

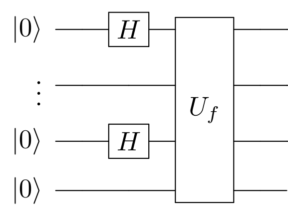
- Any 't'-gate quantum circuit can be ϵ approximated using only $\mathcal{O}(t \text{ polylog}(\frac{1}{\epsilon}))$ gates from G.
- **Proof:** Appendix of Neilsen and Chuang [**?**]
- There are also other universal gate sets: some are efficient than others.

4 Quantum Parallelism

- Suppose we are interested in some function $f : \{0,1\}^n \to \{0,1\}$



So, if $f(x) = 0$, $\quad |x\rangle\,|y\rangle \xrightarrow{U_f} |x\rangle\,|y\rangle$
and if $f(x) = 1$, $\quad |x\rangle\,|y\rangle \xrightarrow{U_f} |x\rangle\,|\bar{y}\rangle$

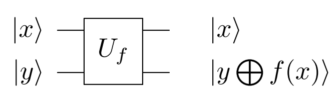


$$|0\rangle^{\bigotimes n}\,|0\rangle \xrightarrow{H^{\bigotimes n} I} \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle\,|0\rangle \xrightarrow{U_f} \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle\,|f(x)\rangle$$

- By applying U_f only once, we are able to obtain a quantum state that contains in it all 2^n possible values of $f(x)$ in superposition!
- This in itself is not very useful. If we make projective measurement, we will observe some $|z\rangle\,|f(z)\rangle$ with probability $1/2^n$.
- Quantum parallelism is not enough to demonstrate the power of quantum computing.
- Quantum parallelism needs to be combined with interference, entanglement, to something better than classical computing.

5 Quantum Oracle : Phase Kickback Oracle

- From the above sections we know that for some function : $f : \{0,1\}^n \to \{0,1\}$ and



$$\text{if} \quad f(x) = 0, \quad |x\rangle\,|y\rangle \xrightarrow{U_f} |x\rangle\,|y\rangle$$

$$\text{and if} \quad f(x) = 1, \quad |x\rangle\,|y\rangle \xrightarrow{U_f} |x\rangle\,|\bar{y}\rangle$$

If we substitute $|-\rangle$ for y we get :

$$\text{if} \quad f(x) = 0, \quad |x\rangle\,[\frac{|0\rangle - |1\rangle}{\sqrt{2}}] \xrightarrow{U_f} |x\rangle\,[\frac{|0\rangle - |1\rangle}{\sqrt{2}}]$$

$$\text{and if} \quad f(x) = 1, \quad |x\rangle\,[\frac{|0\rangle - |1\rangle}{\sqrt{2}}] \xrightarrow{U_f} -|x\rangle\,[\frac{|0\rangle - |1\rangle}{\sqrt{2}}]$$

- The phase get changed when $f(x) = 1$ (a kickback), hence we call this a phase kick back oracle with whose result we can guess $f(x)$! This can be rewritten as :

$$|x\rangle |-\rangle \xrightarrow{U_f} (-1)^{f(x)} |x\rangle |-\rangle$$

Rewriting the circuit for $y = |-\rangle$:

$$\Qcircuit @C=1em @R=1em { \lstick{|x\rangle} & \qw & \multigate{1}{U_f} & \qw & \rstick{(-1)^{f(x)} |x\rangle} \\ \lstick{|1\rangle} & \gate{H} & \ghost{U_f} & \qw & \rstick{|-\rangle} }$$

The second input and output lines can be dropped as they remain the same in another frequently used representation :

$$\Qcircuit @C=1em @R=1em { \lstick{|x\rangle} & \gate{U_f^{\pm}} & \qw & \rstick{(-1)^{f(x)} |x\rangle} }$$

$$|x\rangle \xrightarrow{U_f^{\pm}} (-1)^{f(x)} |x\rangle$$

On passing $H^{\bigotimes n} |0^{\bigotimes n}\rangle$ into the phase kickback $U_f^{\pm}$ we get :

$$H^{\bigotimes n} |0^{\bigotimes n}\rangle \xrightarrow{U_f^{\pm}} \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle \xrightarrow{U_f^{\pm}} \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} (-1)^{f(x)} |x\rangle$$

The important thing to note here is that after passing through the oracle the amplitudes of the states have the information of $f(x)$

6 Deutsch Algorithm

Given a U_f for some boolean function $f : \{0,1\} \to \{0,1\}$ with the promise that either : $f(0) = f(1)$ or $f(0) \neq f(1)$, the task is to find the number of queries to U_f to determine which is the case.

- Classical Algorithm requires 2 queries by comparing outputs of inputs 0 and 1.
- Quantum Algorithm requires only 1 query! with the design :

$$\Qcircuit @C=1em @R=1em { \lstick{|0\rangle} & \gate{H} & \gate{U_f^{\pm}} & \gate{H} & \meter }$$

$$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \xrightarrow{U_f^{\pm}} \frac{1}{\sqrt{2}}(-1^{f(0)} |0\rangle + -1^{f(1)} |1\rangle) \xrightarrow{H} \frac{(-1^{f(0)} + -1^{f(1)}) |0\rangle + (-1^{f(0)} - 1^{f(1)}) |1\rangle}{2}$$

we observe :

$$|0\rangle \text{ if } f(0) = f(1), and \ |1\rangle \text{ for } f(0) \neq f(1)$$

Therefore, only one query with input $|0\rangle$ is needed.

7 Physics Understanding of the Deutsch Problem

The physical setup of the Deutsch Algorithm is realised using Mach Zehnder Interferometer which consists of a beam splitter that creates an equal superposition of $|0\rangle$ and $|1\rangle$. The phase shifter adds a phase of 0 or π which passes through another beam splitter (acting as final H gate in Deutsch Algorithm) where the final states are recorded.

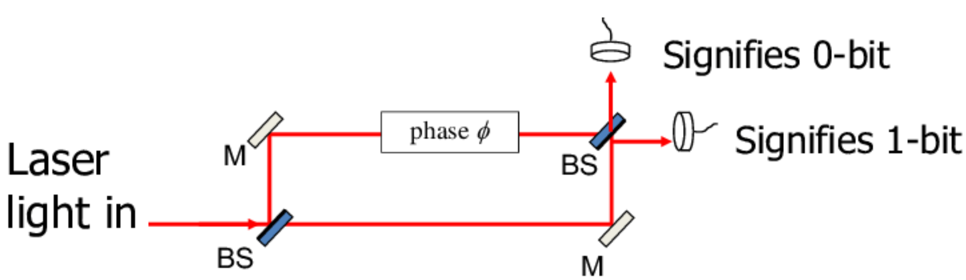


Figure 1: mach zehnder interferometer [2]