Intro to Quantum Information and Computation

Instructor: Shantanav Chakraborty

1 Where do we listen to Quantum Computation?

Quantum Computers

They are the "natural generalization of computing"
Machines that Obey Quantum Physics

Why Quantum Computing?

- Extended Church Turing Thesis (ECT): Any algorithmic process can be efficiently simulated by a probabilistic tuning machine.
  Here the word efficiently means it can be computed in polynomial time in terms of the size of the turning machine

Is there a physical model of computation that violates ECT?

- Computing devices built using the principles of Quantum Physics can offer a stronger version of this thesis.
- Do computing devices that obey QM violate ECT?

Can we simulate Quantum Physics on a computer?

- No.of.variables needed to be kept track of the Exponential size of a quantum system.

2 Quantum Computing in the Circuit Model

(Postulates of Quantum Mechanics in Action)

State Preparation:

Prepare the Quantum Computer in the given initial state

$$|\psi_0\rangle = |0\rangle^{\otimes n}$$

$|0^{\otimes n}\rangle$ is a 2^n dimensional Hilbert space with n qubit's.

Evolution:

$$|\psi(t)\rangle = e^{-iHt} \ |\psi(0)\rangle$$

Here u(t) = e^{-iHt} is a unitary operator
Every physical state is associated with observables.
Energy System has a Hamiltonian operator (H) . Energy values of Hamiltonian are energy levels of the system.
Quantum theory is reversible.

- The initial state $|\psi_0\rangle$ evolves based on the sequence of unitary operators. $|\psi_f\rangle = u_z u_{z-1} .... u_1 \ |\psi_0\rangle$

Measurements:

Measure the final state in the computational basis
$M_j = \{|jXj|\}$ where j $\in \{0,1\}^n$ and j's are bit strings in the computational basis.

$$u_j = e^{-iH_j t}$$
$$|\psi_j\rangle = u_j \ |\psi_0\rangle$$

We can write $|\psi_0\rangle = {u_j}^\dagger |\psi_j\rangle$
We can go from state j to state 0 just by multiplying with the conjugate transpose of u_j.

$$(u_z u_{z-1} .... u_1)^\dagger |\psi_t\rangle = |\psi_0\rangle$$
$${u_1}^\dagger u_2^\dagger .... u_z^\dagger \ |\psi_t\rangle = |\psi_0\rangle$$
$${u_1}^{-1} u_2^{-1} .... u_z^{-1} \ |\psi_t\rangle = |\psi_0\rangle$$

This proves that states are reversible.

Evolution constraint for quantum states:

Evolution of quantum states and be assumed as unitary operator action on that particular state and as the interference of two states. The interference of states must happen constructively. Destructive interference leads to a decrease in amplitude.

3 Classical Logic gates:

Any Boolean function can be written as a propositional statement of n-variables.

$$f : \{0,1\}^n \rightarrow \{0,1\}^k$$

A function $y = f(x)$ can be assumed to be computed by a circuit. The evolution of Quantum states is reversible. This means the evolution of states does not

lead to losing information about the previous state. But the Logic circuits are irreversible. So, We increase the number of inputs, making the function bijective, which helps us to estimate the information of the previous states.

Shannon Entropy:

The Entropy of a random variable is the surprise or uncertainty of a possible outcome.

$$s = E[-log(P(x)]$$

Here $P(x)$ represents the PMF of the random variable. If $p_i's$ represents the probabilities of the possible outcomes then

$$s = \sum_i -p_i log(p_i)$$

A process proceeds in the direction of increase of the entropy.

Landauer's Principle:

The erasure of a single bit of transformation is accompanied by at least $k_B T ln2$ amount of energy being dissipated into the environment. In simple words, in order to erase information it is necessary to dissipate energy. The minimum amount of energy lost can be found using Clausius inequality.

Clausius Inequality:

$$\frac{\Delta Q}{T} \geq k_B \Delta s$$

Here,
ΔQ represents heat lost by the system,
k_B is the Boltzmann constant,
T is the temperature and
Δs represents the change in entropy

Szilard's Engine:

The Szilárd engine is a mechanism for converting information into energy, which seemingly violates the second law of thermodynamics.

Note: Reversible gates do not dissipate energy, unlike irreversible gates.

4 Reversible Logic gates:

Fredkin gate(Controlled Swap gate):

Fredkin gate is a universal, controlled swap gate that maps three inputs (C, a, b) onto three outputs (C, a', b').
Here C represents the control bit.

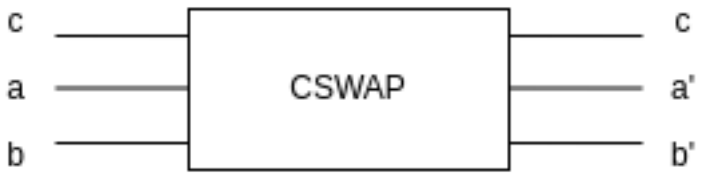


Figure 1: CSWAP

$$\begin{array}{cc} c = 0 & c = 1 \\ a' = a & a' = b \\ b' = b & b' = a \end{array}$$

When the control bit is turned on, the swap operation is executed.

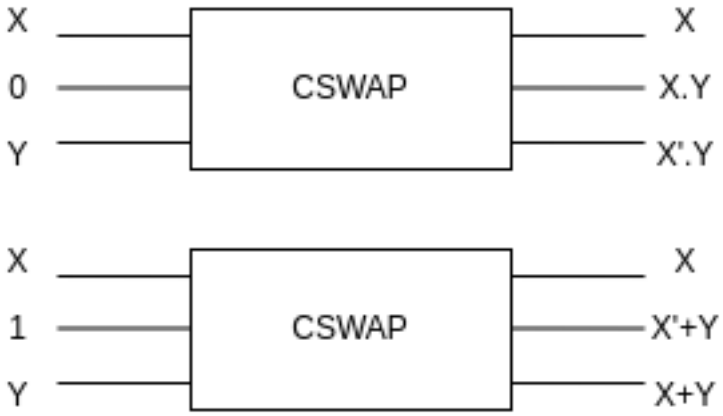


Figure 2: General CSWAP

Controlled NOT gate(CNOT gate):

The Controlled Not gate or controlled-X gate is a 2-input and output gate. One of the inputs is the control bit. $f_{CNOT} : \{0,1\}^2 \to \{0,1\}^2$

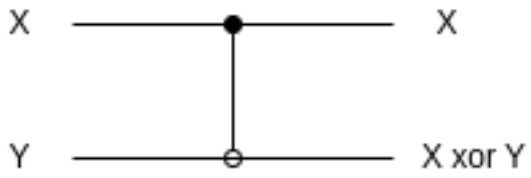


Figure 3: General CNOT

$$\begin{array}{ll} X = 0 & X = 1 \\ Y = a & Y' = a' \end{array}$$

C.C.NOT Gate(Tofolli Gate)

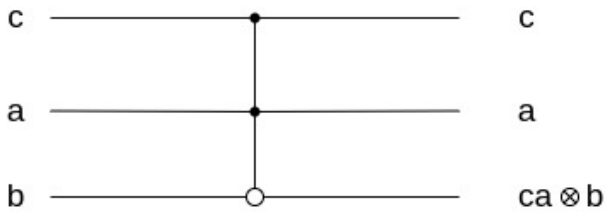


Figure 4: Tofolli Gate

$$(x,0,0) \xrightarrow{c_f} (x, f(x), g(x))$$
$$|x,0,0\rangle \xrightarrow{u_f} \sum_{x^1} \alpha_{x^1} |x^1\rangle \ |f(x^1)\rangle |g(x^1)\rangle$$

- Garbage depends on the input.
- This is a problem for the Quantum Computation
- The Garbage Register gets entangled with the register computing f(x)

Uncomputation

$$(x,0,0,y) \xrightarrow{c_f} (x, f(x), g(x), y) \xrightarrow{C-NOT_{2,4}} (x, f(x), g(x), y \otimes f(x)) \xrightarrow{c_f^{-}1} (x,0,0, y \otimes f(x))$$

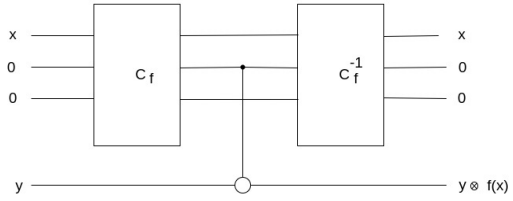
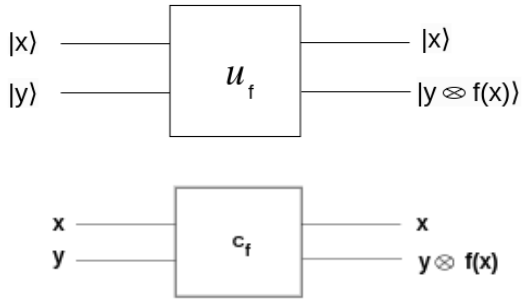


Figure 5: R.C



5 Quantum Circuits

- Quantum gates are unitary operations on Quantum States.
- G_u: Set of gates that are universal for Q.C.
- There exists a small number of 1 qubit gates + 2 qubit gates

Single qubit Gates

Pauli Matrices :

$$X = \sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$Y = \sigma_y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

$$Z = \sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

$$\sigma_x|0\rangle = |1\rangle \ , \sigma_y|1\rangle = |0\rangle$$
$$\sigma_y|0\rangle = i|1\rangle \ , \sigma_y|1\rangle = -i|0\rangle$$
$$\sigma_z|0\rangle = |0\rangle \ , \sigma_z|1\rangle = -|1\rangle$$
$$\sigma_z|+\rangle = |-\rangle \ , \sigma_z|-\rangle = |+\rangle$$
$$\text{Hadamard Gate : H} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

$$\text{H } |0\rangle = \tfrac{1}{\sqrt{2}} \left(|0\rangle \ + |1\rangle \right)$$
$$\text{H } |1\rangle \ = \tfrac{1}{\sqrt{2}} \left(|0\rangle \ - |1\rangle \right)$$
$$R_\phi = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{bmatrix} \quad R_\phi|0\rangle \ = |0\rangle \quad R_\phi|1\rangle \ = e^{i\phi}|1\rangle$$
$$R_\phi(\alpha|0\rangle \ + \beta|1\rangle \ ) = \alpha|0\rangle \ + \beta e^{i\phi}|1\rangle$$
$$R_{\frac{\pi}{2}} = S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$$
$$R_{\frac{\pi}{4}} = T = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{bmatrix}$$

Two Qubit Gates

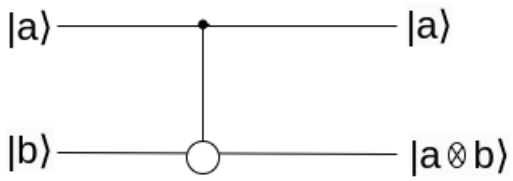
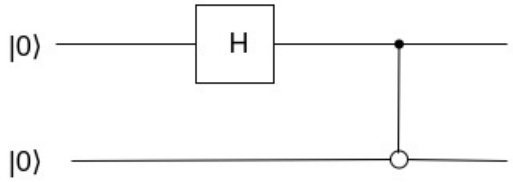
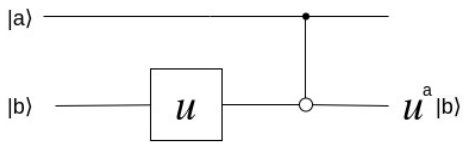


Figure 6: C.NOT Gate

$$|00\rangle \rightarrow |00\rangle$$
$$|01\rangle \rightarrow |01\rangle$$
$$|10\rangle \rightarrow |11\rangle$$
$$|11\rangle \rightarrow |10\rangle$$
$$\mu_{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$



$$|00\rangle \ \rightarrow |00\rangle$$
$$|01\rangle \ \rightarrow |01\rangle$$
$$|10\rangle \ \rightarrow |1\rangle \ \ (\text{u}|0\rangle \ )$$
$$|11\rangle \ \rightarrow |1\rangle \ \ (\text{u}|1\rangle \ )$$
$$(\text{H} \otimes I)|00\rangle \ = \tfrac{1}{\sqrt{2}}(|0\rangle \ + |1\rangle \ )|0\rangle \ = \tfrac{1}{\sqrt{2}}(|00\rangle \ + |10\rangle \ ) \rightarrow \tfrac{1}{\sqrt{2}} \left(|00\rangle \ + |11\rangle \ \right)$$



6 General Quantum Circuits:

Elementary gates can be composed into bigger quantum circuits. They are

Tensor Product:

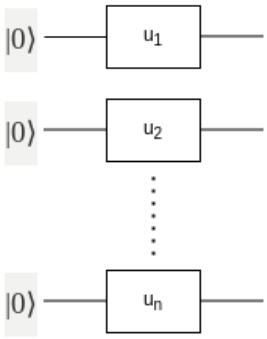


Figure 7: tensor product

If $|\psi\rangle$ represents the combined output state, it is computed by,

$$|\psi\rangle = {u_i}^{\otimes n}|00...0\rangle$$

$$|\psi\rangle = (u_1 \otimes u_2 \otimes ... \otimes u_n)|00...0\rangle$$

$$|\psi\rangle = (u_1|0\rangle \otimes u_2|0\rangle \otimes ... \otimes u_n|0\rangle)$$

Ordinary Matrix Product:

If $|\psi\rangle$ represents the combined output state, it is computed by,

$$|\psi\rangle = (u_n u_{n-1} ... u_2 u_1)|0\rangle$$

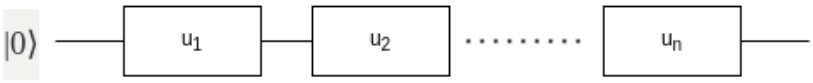
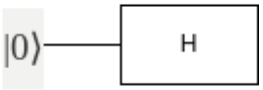


Figure 8: ordinary matrix product



Hadamard Gate:

It creates an equal superposition state of given a computational basis state.

- The above gate converts
  - $|0\rangle$ to $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$
  - $|1\rangle$ to $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

Note:

- $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ is sometimes written as $|+\rangle$
- $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ is sometimes written as $|-\rangle$

Let H be the matrix representation of the function of transformation of the Hadamard gate.

Then H = $\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$

Therefore if $|X\rangle$ is the input, then the output of the above gate is $H|X\rangle$.

$$H|0\rangle = |+\rangle$$

$$H|1\rangle = |-\rangle$$

The output for the combination of n-Hadamard gates in parallel is $H^{\otimes n}|X\rangle$ where $|X\rangle$ represents the input state.

Note:

- $H^{\otimes n}|0\rangle^{\otimes n} = |+\rangle^{\otimes n}$
- $H^{\otimes n}|1\rangle^{\otimes n} = |-\rangle^{\otimes n}$
- $H^{\otimes n}|X\rangle = \frac{1}{\sqrt{2^n}} \sum_{z\in(0,1)^n} (-1)^{xz}|z\rangle$, where x $\in (0,1)^n$

Universality of Quantum Gates:

A set of gates is said to be universal if, for any integer n ≥ 1, any n-qubit unitary operator can be approximated to arbitrary accuracy by a quantum circuit using only gates from that set.

- The sets {CNOT}, {H, T} are universal for single-qubit gates.
- The set {CNOT, H, T} is universal set of gates

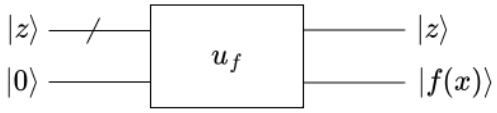
Solovay-Kitaev Theorem:

Let $G = \{CNOT, H, T\}$, it is possible to approximate any unitary in one or two qubits upto an error ϵ by using only $polylog(\frac{1}{\epsilon})$ gates from G.
In simple words, G is the set of unitaries, and if we select one of it, say U, then it can be achieved using other gates in G, say S, with an error upto ϵ i.e, $\|S - U\| \leq \epsilon$, the length of S is given by $polylog(\frac{1}{\epsilon})$.

$$S = u_n u_{n-1} .... u_1, \text{ where n} \in polylog(\tfrac{1}{\epsilon})$$

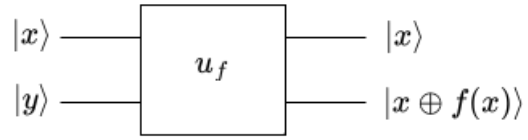
Quantum Parallelism

Classical circuit that computes $f : \{0,1\}^n \to \{0,1\}$
$Z \in \{0,1\}^n$



Quantum BlackBox: Phase kickback oracle

$|x\rangle\,|y\rangle \xrightarrow{u_f} |x\rangle\,|y\rangle\ f(x) = 0$
$|x\rangle\,|y\rangle \xrightarrow{u_f} |x\rangle\,|\overline{y}\rangle\ f(x) = 1$



$when\ |y\rangle = |-\rangle$?
$|x\rangle|-\rangle \xrightarrow{u_f} |x\rangle|-\rangle\ f(x) = 0$
$|x\rangle|-\rangle \xrightarrow{u_f} -|x\rangle|-\rangle\ f(x) = 1$
$\Rightarrow |x\rangle|-\rangle \xrightarrow{u_f} (-1)^{f(x)}|x\rangle|-\rangle$
$H|x\rangle = \frac{1}{\sqrt{2}} \sum_{z\ \in\ \{0,1\}^n} |z\rangle \qquad |y\rangle = |-\rangle$
$|x\rangle|-\rangle \xrightarrow{u_f} \frac{1}{\sqrt{2^n}} \sum_{z\ \in\ \{0,1\}^n} |z\rangle|-\rangle$

Deutsch Algorithm

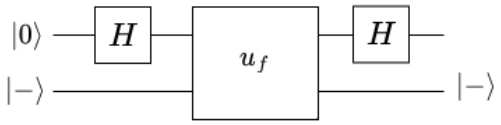
Suppose we are given u_f as a black box for a booleam function $f : \{0,1\} \to \{0,1\}$, with the promise that either

$(i)\ f(0) = f(1)$
or
$(ii)\ f(0) \neq f(1)$

How many queries to u_f are required to determine which of these two cases holds?

Classical: 2 queries

Quantum: 1 query



$$|0\rangle|-\rangle \xrightarrow{H\ \otimes\ 1} \tfrac{1}{\sqrt{2}}[\ |0\rangle\ +\ |1\rangle\ ]|-\rangle \xrightarrow{u_f} \tfrac{1}{\sqrt{2}}\left[\ (-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle\ \right]|-\rangle$$
$$\downarrow H \otimes 1$$
$$\tfrac{1}{\sqrt{2}}\left[\ (-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle\ \right]|-\rangle$$
$$\downarrow H \otimes 1$$
$$\tfrac{1}{\sqrt{2}}\left[\ (-1)^{f(0)}\left(\tfrac{|0\rangle+|1\rangle}{\sqrt{2}}\right) + (-1)^{f(1)}\left(\tfrac{|0\rangle-|1\rangle}{\sqrt{2}}\right)\right]$$
$$\downarrow$$
$$|\psi\rangle = \tfrac{1}{2}\left[\ (-1)^{f(0)} + (-1)^{f(1)}\right]|0\rangle + \tfrac{1}{2}\left[\ (-1)^{f(0)} + (-1)^{f(1)}\right]|1\rangle$$

$(i)\ f(0) = f(1)$
$\langle 0|\psi\rangle = 1$
$\langle 1|\psi\rangle = 0$
on measurement,
we always get 0

$(ii)\ f(0) \neq f(1)$
$\langle 0|\psi\rangle = 0$
$\langle 1|\psi\rangle = 1$
on measurement,
we always get 1

Deutsch-Josza Algorithm

$f : \{0,1\}^n \to \{0,1\}$
(i) *f is "CONSTANT" or* $f(x) = 0$ *or* $f(x) = 1$

(ii) *f is "BALANCED" or*
$f(x) = 0$ for $\frac{2^n}{2}$ values of x
and
$f(x) = 1$ for other $\frac{2^n}{2}$ values of x

Q: How many Queries?

Classical: $\frac{2^n}{2} + 1$ with probability 1

$$|0\rangle^{\otimes n}|Z\rangle|-\rangle \xrightarrow{H^{\otimes n}\otimes 1} \frac{1}{\sqrt{2^n}} \sum_{z\in\{0,1\}^n} |Z\rangle|-\rangle \xrightarrow{u_f} \frac{1}{\sqrt{2^n}} \sum_{z\in\{0,1\}^n} (-1)^{f(z)}|-\rangle$$

$$\downarrow u_f$$

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

$$\downarrow H^{\otimes n}\otimes 1$$

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

$$\downarrow$$

$$|\psi\rangle = \frac{1}{2^n} \sum_{z\in\{0,1\}^n} \sum_{t\in\{0,1\}^n} (-1)^{f(z)+zt}|t\rangle$$

$$\downarrow$$

$$\langle 0....0|\psi\rangle = \frac{1}{2^n} \sum_{z\in\{0,1\}^n} (-1)^{f(z)} = \begin{cases} \pm 1 & f(x) = const \\ 0 & f(x) = balanced \end{cases}$$

$(i)\ f(0)$ = constant
on measurement,
we always get 0
with probability 1

$(ii)\ f(0)$ = balanced
on measurement,
we always get
some state $\neq 0$
with probability 1

Brainstorm: Classical random:

How many Queries to c_f to determine f is *const* or *balanced* with $p \geq 1-\epsilon$?

7 The Quantum Search Algorithm/Grover's Algorithm

It offers a quadratic speedup.
The problem: Let us have a set $N = 2^n$ elements, i.e., $X = \{x_1, x_2, ..., x_N\}$ and a Boolean function $f : X \longmapsto \{0, 1\}$. Find an element $x^* \in X$ such that $f(x^*) = 1$.

Classical: $O(N)$ queries are needed.

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

if $x = x^*$, $U_f |x^*\rangle \longmapsto - |x^*\rangle$
if $x \neq x^*$, $U_f |x\rangle \longmapsto |x\rangle$

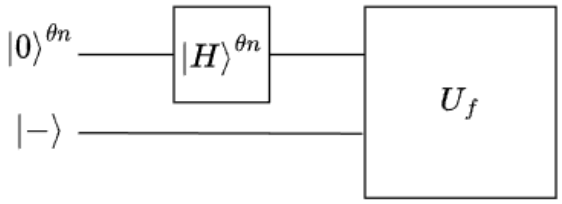


Figure 9: initial circuit.

$$|s\rangle = \frac{1}{\sqrt{N}} \sum_z |z\rangle \, U_f \frac{1}{\sqrt{N}} \sum_z (-1)^{f(z)} |z\rangle \\ \frac{1}{\sqrt{N}} (- |z^*\rangle + (...)) \tag{1}$$

Thus, $(DU_f)^k (\frac{1}{\sqrt{N}} \sum_z |z\rangle)$
$G = (DU_f) and \, |s\rangle = \frac{1}{\sqrt{N}} \sum_z |z\rangle$
Choose k such that $(DU_f)^k |s\rangle \approx |x^*\rangle$

Let us say we have M solutions where $M << N$
$(DU_f)^k |s\rangle \approx \frac{1}{\sqrt{M}} \sum_{f(x^*)=1} |x^*\rangle$
$|X| = N$ out of which there are M solutions $(M << N)$

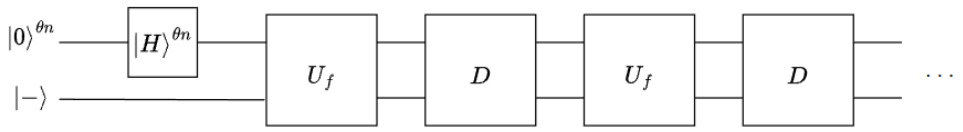


Figure 10: final circuit.

$$
\begin{aligned}
H^{\otimes n}|0\rangle^{\otimes n} \longmapsto & \frac{1}{\sqrt{N}} \sum_{x\in\{0,1\}^n} |x\rangle \\
& \frac{1}{\sqrt{N}}\Big(\sum_{f(x')=1} |x'\rangle + \sum_{f(x'')} |x''\rangle\Big) \\
& \frac{1}{\sqrt{N}}\Big(\frac{\sqrt{M}}{\sqrt{M}} \sum_{f(x')=1} |x'\rangle + \frac{\sqrt{N-M}}{\sqrt{N-M}} \sum_{f(x'')=0} |x''\rangle\Big)
\end{aligned} \tag{2}
$$

Let $|w\rangle = \frac{1}{\sqrt{M}} \sum_{f(x')=1} |x'\rangle \; and \; |S_{\bar{w}}\rangle = \frac{1}{\sqrt{N-M}} \sum_{f(x'')=0} |x''\rangle$
Clearly, $\langle w|S_{\bar{w}}\rangle = 0$

Thus, continuing from equation 2, we have

$$
\begin{aligned}
|s\rangle &= \frac{\sqrt{M}}{\sqrt{N}} |w\rangle + \frac{\sqrt{N-M}}{\sqrt{N}} |S_{\bar{w}}\rangle \\
&= \sin\left(\frac{\theta}{2}\right)|w\rangle + \cos\left(\frac{\theta}{2}\right)|S_{\bar{w}}\rangle
\end{aligned} \tag{3}
$$

where $\sin\big(\frac{\theta}{2}\big) = \frac{\sqrt{M}}{\sqrt{N}} and \cos\big(\frac{\theta}{2}\big) = \frac{\sqrt{N-M}}{\sqrt{N}}$

Thus, $\theta = 2\sin^{-1}(\frac{\sqrt{M}}{\sqrt{N}})$

G rotates $|s\rangle$ by θ always
$\sin\big(\frac{\theta}{2} + k\theta\big) \approx 1$
$\frac{\theta}{2} + k\theta \approx \frac{\pi}{2}$

$$
U_f|s\rangle \longmapsto -\sin\left(\frac{\theta}{2}\right)|w\rangle + \cos\left(\frac{\theta}{2}\right)|S_{\bar{w}}\rangle
$$

V_0 performs a controlled phase shift
if $X = 0^n$, then no phase shift
if $X \neq 0^n$, then flip the phase

$$
\begin{aligned}
V_0 &= (2\langle 0^n|0^n\rangle - I) \; where \; |0^n\rangle = |0...0\rangle \\
V_0|0^n\rangle &= 2|0^n\rangle - |0^n\rangle = |0^n\rangle \\
V_0|x\rangle &= 2\langle 0^n|0^n\rangle|x\rangle - |x\rangle = -|x\rangle
\end{aligned} \tag{4}
$$

For any $|x_1, x_2, ..., x_n\rangle$ if $x_1 + x_2 + ... + x_n = 1$, then phase flips ($x_i \in \{0, 1\}$)

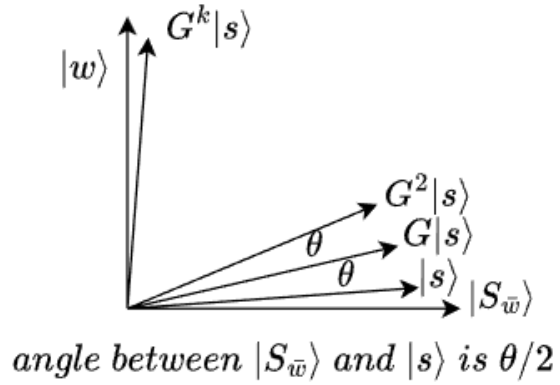


Figure 11: Effect of G.

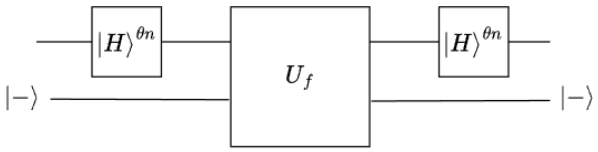


Figure 12: black box D.

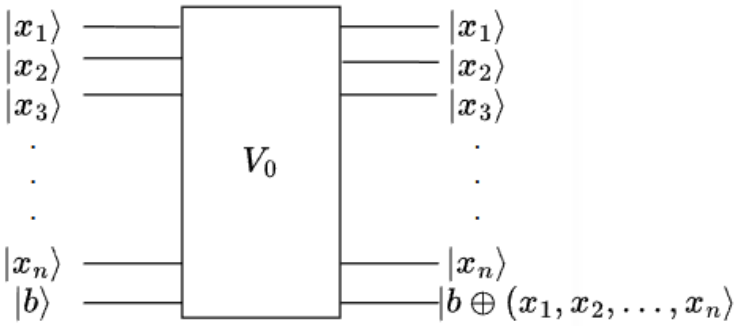


Figure 13: $V_0 circuit$.

we have $|b\rangle = |-\rangle$
$|x\rangle |-\rangle U_f(-1)^{f(x)} |x\rangle |-\rangle$
$|x\rangle U_f(-1)^{OR(x_1,x_2,\ldots,x_n)} |x\rangle$

Considering, $|b\rangle = |-\rangle$, we get phase kickback oracle
Thus,

$$\begin{aligned} D &= H^{\otimes n} V_0 H^{\otimes n} \\ &= 2H{\otimes}n\,|0\rangle\langle 0|\,H^{\otimes n} - H{\otimes}nH^{\otimes n} \\ &= 2\,|s\rangle\langle s| - I \end{aligned} \tag{5}$$

We know that

$$|s\rangle = \sin\left(\frac{\theta}{2}\right)|w\rangle + \cos\left(\frac{\theta}{2}\right)|S_{\bar{w}}\rangle$$

Now substituting this value of $|s\rangle$ in D we get

$$D = -\cos(\theta)\,|w\rangle\,\langle w| + \sin\theta\,|w\rangle\,\langle S_w| + \sin\theta\,|S_w\rangle\,\langle w| + \cos(\theta)\,|S_w\rangle\,\langle S_w|$$

Mapping D from n-dimensional space to 2-dimensional space with basis elements $[S_w,\ w]$, we can represent D as

$$D = \begin{bmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{bmatrix}$$

Similarly, U_f can be mapped from n-dimensional space to 2-dimensional space with basis elements $[S_w\ ,\ w]$ according to the equations:

$$U_f\,|w\rangle = -\,|w\rangle$$

$$U_f\,|S_w\rangle = |S_w\rangle$$

From these equations U_f can be represented as

$$U_f = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

From figure 2 the overall matrix representation(G) of U_f, D acting on the starting state could be found from the equation

$$G = DU_f$$

$$G = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$$

In Grover's algorithm, this operation G is applied K times. If it is applied one time, the output after one operation is

$$= G\,|s\rangle$$

$$= \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \begin{bmatrix} \cos\frac{\theta}{2} \\ \sin\frac{\theta}{2} \end{bmatrix}$$

$$= \begin{bmatrix} \cos(\theta + \frac{\theta}{2}) \\ \sin(\theta + \frac{\theta}{2}) \end{bmatrix}$$

i.e an additional angle of θ has been added to the starting state. Therefore if this is applied for K times then the final state of the circuit would be

$$\begin{bmatrix} \cos(k \times \theta + \frac{\theta}{2}) \\ \sin(k \times \theta + \frac{\theta}{2}) \end{bmatrix}$$

Since we need the probability of measuring $|w\rangle$ to be maximum

$$\sin(k\theta + \frac{\theta}{2}) = 1$$

$$\frac{(2k+1)}{2}\theta = \frac{\pi}{2}$$

But we know that

$$\theta = 2\sin^{-1}\sqrt{\frac{M}{N}}$$

therefore

$$k = \frac{(\frac{\pi}{2\sin^{-1}\sqrt{\frac{M}{N}}}) - 1}{2}$$

since

$$M << N$$

$$k = \frac{(\frac{\pi}{2\sqrt{\frac{M}{N}}}) - 1}{2}$$

i.e

$$k \propto \sqrt{\frac{N}{M}}$$

Therefore this algorithm provides a quadratic speed-up as compared to its classical counterpart

Issues with these algorithms

If you don't know the value of M then we cannot determine the correct value of K. Hence we may tend to undershoot or overshoot the value of K.

Strategies to overcome this issue

- Estimate the value of M. This can be achieved using quantum counting
- We can randomize Grover's algorithm

Team Members:

- Kunukulagunta Anupama –2021101087

- Devisetti Sai Asrith – 2021111022
- Thota Venkata Sai Lakshmi Geethika – 2021101020
- Chekkapalli Naveen – 2021101025
- Pericharla Phani Sathvika – 2021101030
- Chikkala Sri Lakshmanarao – 2021101011
- Anusha Nemani - 2021101082
- Mareddy Sriharshitha – 2021101067
- Amogha Halhalli - 2021101007