Cheat sheet:

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \qquad H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \qquad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

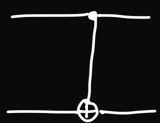
$$X|0\rangle = |1\rangle$$

$$X|1\rangle = |0\rangle$$

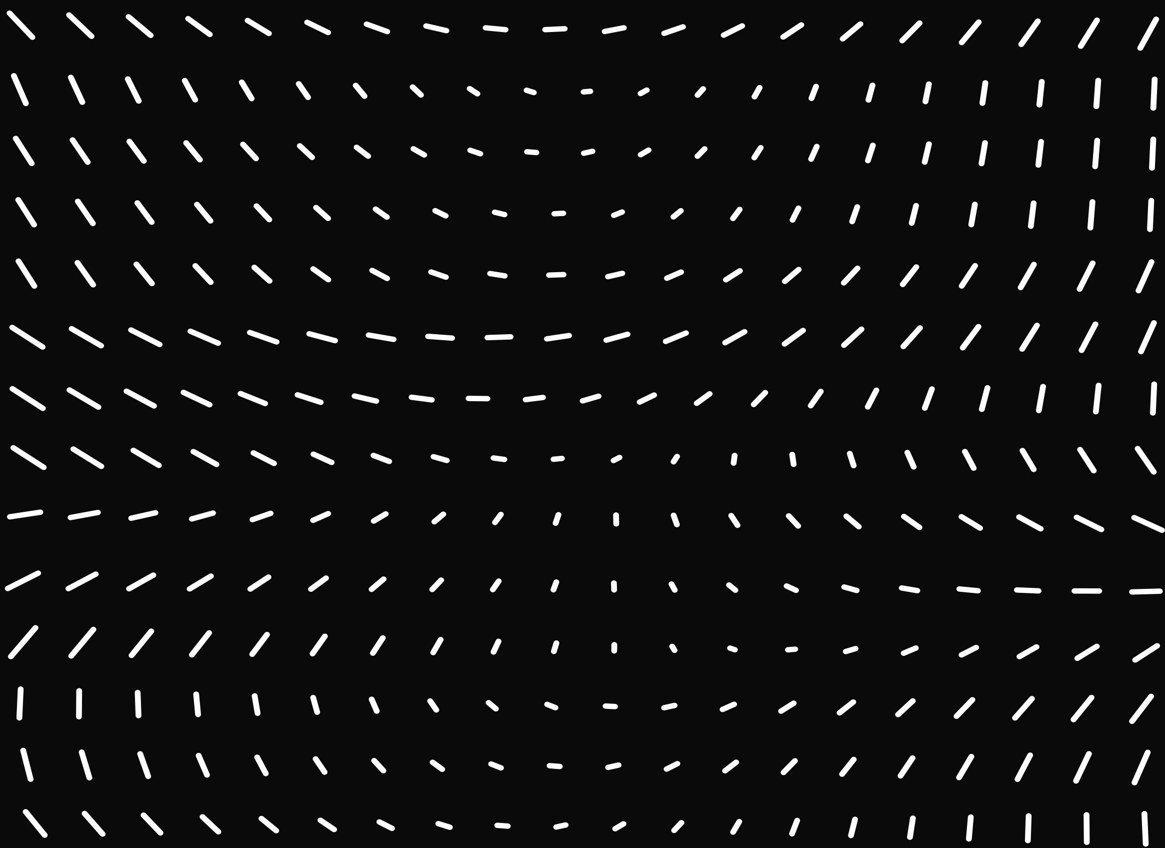
$$H|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} = |+\rangle \qquad Z|0\rangle = |0\rangle$$

$$H|1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}} = |-\rangle \qquad Z|1\rangle = -|1\rangle$$

CNOT



0	0
0	1
1	0
1	1



Classical to Quantum Logic

Classical

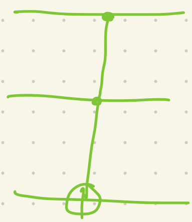
AND

0	0	0
0	1	0
1	0	0
1	1	1

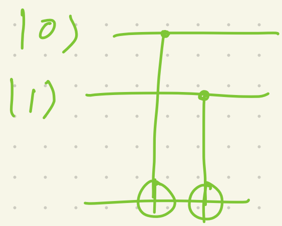
XOR

0	0	0
0	1	1
1	0	1
1	1	0

Quantum



Toffoli Gate

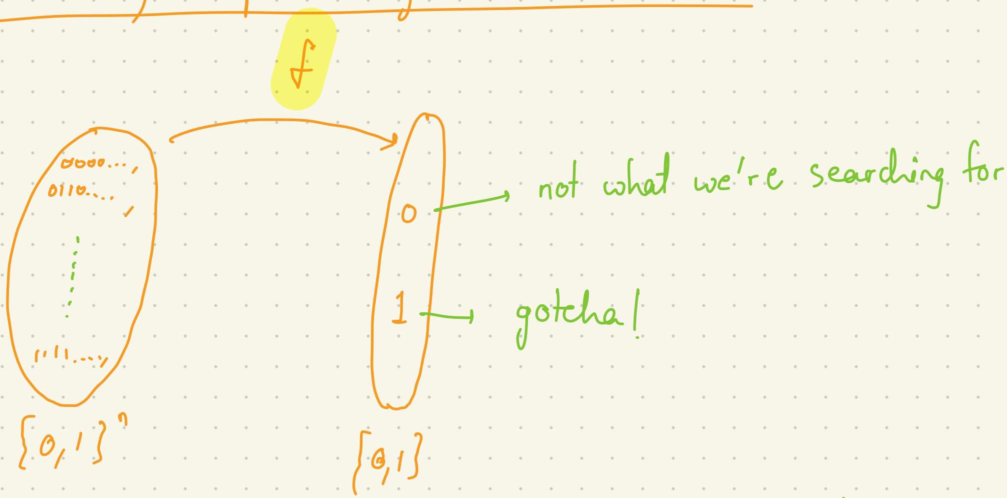


XOR

Grover's Algorithm (Search Algorithm)

- Size of search space = N
- Classical search takes $\frac{N}{2}$ queries on average
- Grover's algorithm does it in $\sqrt{N}$ queries to the quantum oracle.

Mathematically representing a search function:



$$f(x) = \begin{cases} 0 & x = x_0 \\ 1 & x \neq x_0 \end{cases}$$

This is the logic we'll have to insert into the oracle.

What is an oracle?

→ Oracle is a black box that does some specific unitary operation.

Q) Create an oracle that outputs the state $|1\rangle$ on the third qubit when the input on the first two qubits is $|10\rangle$.

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

$X|0\rangle = |1\rangle$
$X|1\rangle = |0\rangle$

Phase flipping:

$$|-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

Apply the $\boxed{X}$ gate

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

$$\equiv -|-\rangle$$

$$X|-\rangle = -|-\rangle$$

Q) Convert state $\frac{|00\rangle + |01\rangle + |10\rangle + |11\rangle}{2}$

to $\frac{|00\rangle + |01\rangle - |10\rangle + |11\rangle}{2}$

$\boxed{\text{Hint : } X|-\rangle = -|-\rangle}$

Idea and steps of the algorithm:

Step 1: Initialize in $|0\rangle^{\otimes n}$

Step 2: Put the state in a quantum superposition (equal superposition) of the search space

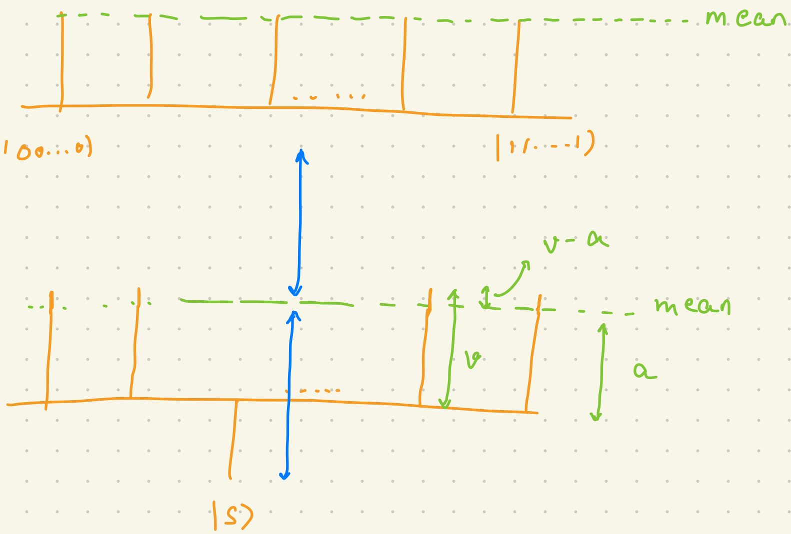
Step 3: Apply the oracle and flip the phase of the state you are looking for.

Step 4: Apply the diffusion operator that does the flip about mean operation.

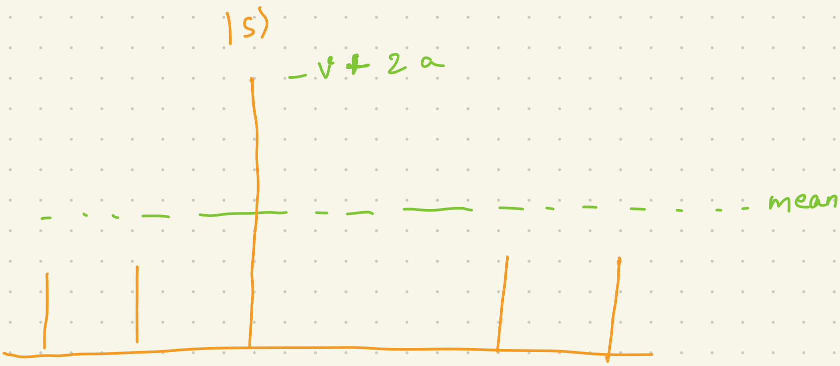
$$|000\ldots 0\rangle \longrightarrow \frac{|0000\ldots 0\rangle + \cdots + |1111\ldots 1\rangle}{\sqrt{N}} \longrightarrow \frac{|00\ldots 0\rangle \overset{\text{phase flip}}{-} |101\ldots\rangle + \ldots |111\rangle}{\sqrt{N}}$$

$\boxed{\text{Step 4}}$

Understanding Step 4 :



↳ state we are searching for



Classical example:

$$\begin{bmatrix} 10 & 10 & 10 & 10 & 10 \end{bmatrix}^T \equiv \text{equal superposition}$$

$$\Big\downarrow \text{phase flip}$$

$$\begin{bmatrix} 10 & 10 & 10 & -10 & 10 \end{bmatrix}$$

$a = 6$

for the $\underline{\underline{10}}$ entries: $-v + 2a = -10 + 12 = 2$

for the $\underline{\underline{-10}}$ entries: $-v + 2a = +10 + 12 = 22$

$$\begin{bmatrix} 2 & 2 & 2 & 22 & 2 \end{bmatrix}$$

we have managed to increase the magnitude.

How do we implement $-v + 2a$ on a quantum computer?

$-v + 2a \leftarrow$ for each entry

$(-I + 2A)V \leftarrow$ for all the entries at once

$n \rightarrow$ no. of qubits

$N \rightarrow$ search space (or) 2^n

I = Identity matrix of order n

$$A = \begin{bmatrix} \frac{1}{N} & \frac{1}{N} & \cdots & \\ \frac{1}{N} & \ddots & & \\ \vdots & \vdots & & \ddots \end{bmatrix}_{n \times n} \stackrel{?}{\equiv} H^{\otimes n} |0^{\otimes n}\rangle\langle 0^{\otimes n}| H^{\otimes n}$$

→ Essentially we have to implement $(-I + 2A)$ as an operator.

$$-I + 2A = H^{\otimes n}\left(-I + 2|0^n\rangle\langle 0^n|\right)H^{\otimes n}$$

Implementing $(-I + 2|0^n\rangle\langle 0^n|)$:

To look at the effect of any operator it's enough to look at its effect on the basis set.

Basis set in our case: $\{|0^n\rangle, \ldots\ldots, |1^n\rangle\} = T$

$$(-I + 2|0^n\rangle\langle 0^n|)|0^n\rangle = |0^n\rangle$$

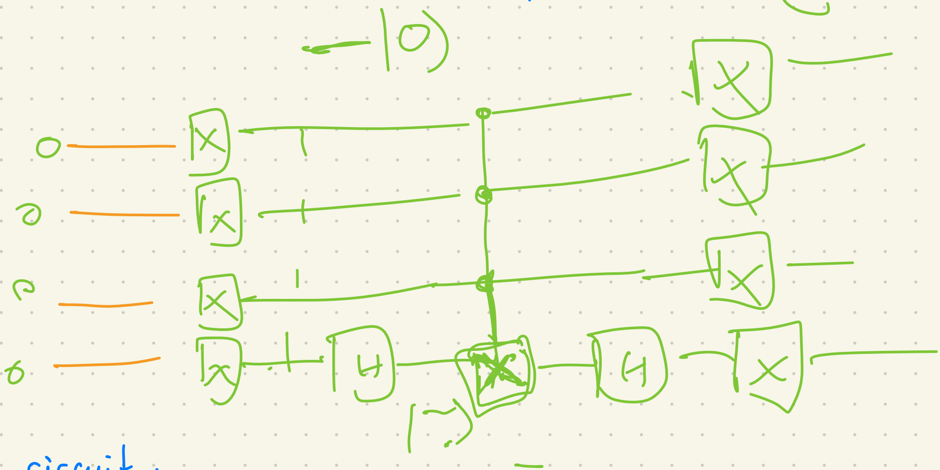
$$(-I + 2|0^n\rangle\langle 0^n|)|\psi\rangle = -|\psi\rangle + \underline{\underline{0}}$$

$|\psi\rangle \in T$ where $|\psi\rangle \neq |0^n\rangle$

any other $|\psi\rangle$ will be orthogonal to $|0^n\rangle$

Implementing $(-I + 2|0^n\rangle\langle 0^n|)$ is the same as implementing $(2|0^n\rangle\langle 0^n| - I)$

Circuit which doesn't flip the phase only when the all zero state is an input. → $(-I + 2A)$



Full circuit: