Introduction To Quantum Computing.

Grover's Search Algorithm

- Also known as "Unordered Search": Search through an unstructured data base till you find the "key" you are looking for.
- In terms of an oracle:
  Given oracle acess to a function $f:\{0,1,\dots,N-1\}\to\{0,1\}$ such that $f(x)=1$ for a <u>single</u> x, and $f(y)=0$ $\forall y\neq x$, find the key x.
- Classically: $\Omega(N)$ Queriss to f till we "hit" x.
- Incorporating Randomness: $\sim N/2$ Queries to find the hidden x with probability $1/2$.
- Imagine $N=2^n$ for some n (Typical Search Space for Combinatorial Optimization Problems of size $=n$).
- Exponential Complexity on n !.

Grover's Algorithm Solves this Search Problem in time $O(\sqrt{N})$, using $O(\log N)$ Qbits and roughly $\sqrt{N}\log N$ Quantum Gates.

$\Rightarrow$ Quadratic Speedup. !
Not very dramatic, but quite useful.

- Grover's Algo is Optimal !

STEPS OF GROVER'S ALGORITHM

- We have a unique solution, call it x^* : $f(x^*) = 1$ and $f(x) = 0$. $x \neq x^*$
- Without loss, and for simplicity, assume $N = 2^n$ for some positive integer n.

- Prepare $n = \log N$ qbits in $|0\rangle^{\otimes n}$
- At the beginning, each possible x is equally likely to be the special x^*
- We can describe this lack of information by "Hadamarig" $|0\rangle^{\otimes n}$ to produce an equal superposition of all possible n-bit strings x:

$$H^{\otimes n} |0\rangle^{\otimes n} = \frac{1}{2^{n/2}} \sum_{x \in \{0,1\}^N} |x\rangle = |\psi_1\rangle$$

- If we sample from $|\psi_1\rangle$ we will get uniformly at random a singe x
- Probability $[x = x^*] = \left[\frac{1}{\sqrt{N}}\right]^2 = \left[\frac{1}{2^{n/2}}\right]^2 = \frac{1}{2^n}$

- Then we implement an oracle for f that corresponds to a unitary transform, let's call it U_f.:

$$|x\rangle \otimes |\alpha\rangle = |x\rangle \otimes |\alpha \oplus f(x)\rangle$$

if $|\alpha\rangle = |0\rangle$ we get $|x\rangle \otimes |f(x)\rangle$

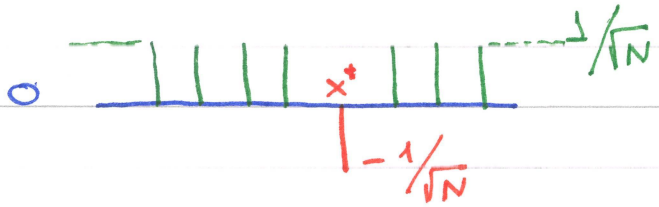
if $|\alpha\rangle = |1\rangle$ we get $|x\rangle \otimes |1 \oplus f(x)\rangle$ → flips $f(x)$!

if $|\alpha\rangle = |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ we get: $|x\rangle \otimes \left(\frac{1}{\sqrt{2}}|f(x)\rangle - \frac{1}{\sqrt{2}}|1 \oplus f(x)\rangle\right)$

which is equal to $(-1)^{f(x)}|x\rangle$!

$$U_f\left(|x\rangle \otimes |-\rangle\right) = (-1)^{f(x)} |x\rangle = \begin{cases} |x\rangle & \text{if } f(x)=0 \\ -|x\rangle & \text{if } f(x)=1 \Rightarrow x = x^* \end{cases}$$

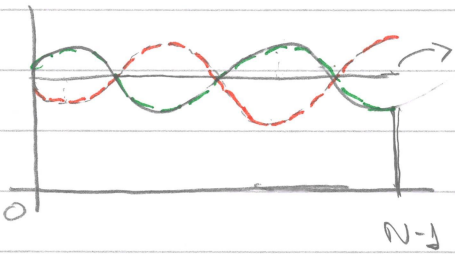
So, the Query Oracle flips the amplitude of the Single marked Element x^* !
all the other amplitudes Remain Unchanged.



Inversion About the Mean.

- The Phase Inversion of x^* from $1/\sqrt{N}$ to $-1/\sqrt{N}$ lowers the Mean just a little Bit.

- In General, we Start With Some Superposition $\sum_x \alpha_x |x\rangle$
- Let μ = mean = $\sum_x \alpha_x / N$ (average value of all amplitudes)
- Let's say the amplitudes of the N Elements can Be Graphed as follows:



The new amplitudes change as follows:
- if $\alpha_x < \mu$ then $\alpha_x := \mu + (\mu - \alpha_x)$
- if $\alpha_x > \mu$ then $\alpha_x := \mu - (\alpha_x - \mu)$

$\alpha_x := 2\mu - \alpha_x$!

- Flip each amplitude about the mean !

So: $\sum_x \alpha_x |x\rangle \rightarrow \sum_x (2\mu - \alpha_x)|x\rangle$

⚠ How do we Implement Inversion About the Mean? Is it even Unitary Transformation?

- After the Phase Inversion followed By the Inversion About the Mean, the amplitude of x^* becomes:

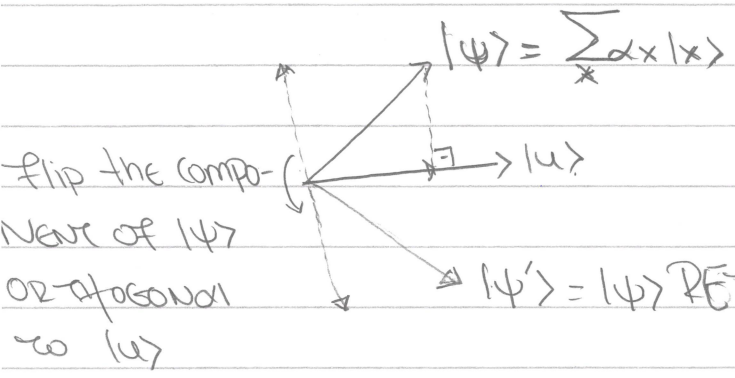
$$\frac{1}{\sqrt{N}} \rightarrow -\frac{1}{\sqrt{N}} \rightarrow 2\mu - \left(-\frac{1}{\sqrt{N}}\right) = 2\cdot\frac{1}{\sqrt{N}} + \frac{1}{\sqrt{N}} = \frac{3}{\sqrt{N}}.$$

- We have amplified the amplitude of x^* By $\frac{2}{\sqrt{N}}$.
- Another application of the above procedures would further increase it By $\frac{2}{\sqrt{N}}$ To $\frac{5}{\sqrt{N}}$
- $\frac{7}{\sqrt{N}} \rightarrow \frac{9}{\sqrt{N}} \rightarrow \dots \rightarrow \frac{1}{\sqrt{2}}$ after roughly $\sqrt{\frac{N}{2}}$ steps

- At the point the amplitude of x^* gets $1/\sqrt{2}$, if we measure, we would have probability $= \left(1/\sqrt{2}\right)^2 = \frac{1}{2}$ To observe x^*
- It takes us $O(\sqrt{N})$ steps to find x^* with high probability.

Implementing the transform $\sum_x \alpha_x |x\rangle \to \sum_x (2\mu - \alpha_x)|x\rangle$

- It turns out (no proof) that inversion about the mean is **the same** as doing a **reflection** about the uniform superposition $|u\rangle = \frac{1}{\sqrt{N}} \sum_x |x\rangle$!



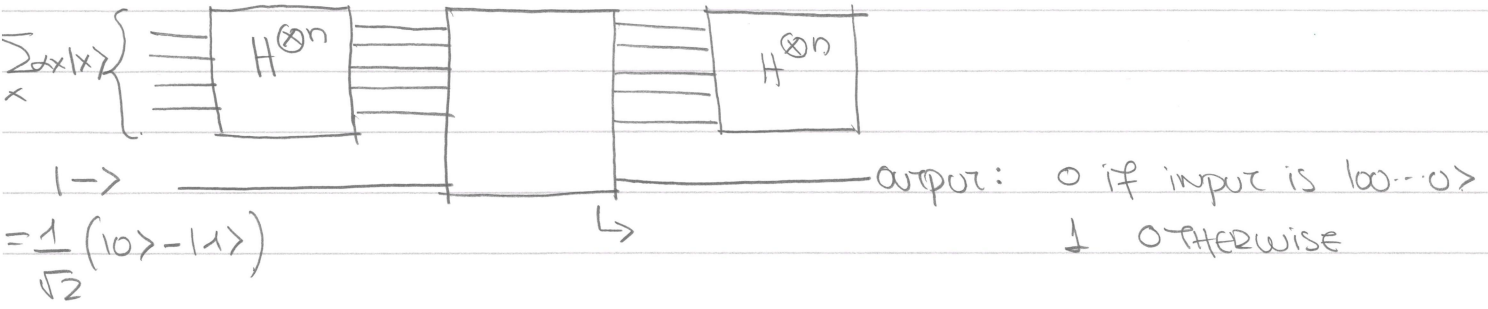
- How do we carry out such a reflection?
- Here is one way (not the only way) to do it:

(1) Transform $|u\rangle$ to the all-$|0\rangle$ vector $|00\cdots0\rangle = |0\rangle^{\otimes n}$
(2) Do a reflection about $|0\rangle^{\otimes n}$
(3) Transform back to $|u\rangle$

- All steps (1)-(3) are unitary!
- For (1): apply $H^{\otimes n}$
- How do we reflect about $|00\cdots0\rangle$?
  - Leave $|00\cdots0\rangle$ unchanged.
  - Multiply with (-1) all vectors in the orthogonal subspace of $|00\cdots0\rangle$ (i.e. all vectors that are orthogonal to $|00\cdots0\rangle$):

$$\begin{bmatrix} 1 & & & \\ & -1 & & \\ & & -1 & \\ & & & \ddots \\ & & & & -1 \end{bmatrix} = \boxed{2|0\rangle\langle 0| - I}$$

- THEN, TRANSFORM BACK BY AGAIN APPLYING $H^{\otimes n}$ (THE HADAMARD IS ITS OWN INVERSE).



- BUT WHY IS THIS INVERSION ABOUT THE MEAN?

$$H^{\otimes n}\begin{bmatrix} 1 & & \\ & -1 & 0 \\ & 0 & \ddots \\ & & -1 \end{bmatrix} H^{\otimes n} = H^{\otimes n}\left(\begin{bmatrix} 2 & & \\ & 0 & \\ & & \ddots \\ & & & 0 \end{bmatrix} - I\right) H^{\otimes n}$$

$$= H^{\otimes n}\begin{bmatrix} 2 & & \\ & 0 & \\ & & \ddots \\ & & & 0 \end{bmatrix} H^{\otimes n} - \underbrace{H^{\otimes n} I H^{\otimes n}}_{I}$$

- MULTIPLYING $H^{\otimes n}$ BY THIS MATRIX, THE ONLY THING THAT SURVIVES IS THE 1ST COLUMN OF $H^{\otimes n}$:

$$\begin{bmatrix} 2/\sqrt{N} & 0 & \cdots & 0 \\ 2/\sqrt{N} & & & \\ \vdots & & & \\ 2/\sqrt{N} & 0 & \cdots & 0 \end{bmatrix} \cdot H^{\otimes n} - I = \begin{bmatrix} 2/N & 2/N & \cdots & 2/N \\ \vdots & & & \\ 2/N & \cdots & & 2/N \end{bmatrix} - I$$

- NOW WE PICK THE 1ST ROW OF $H^{\otimes n}$

$$= \begin{bmatrix} (2/N - 1) & 2/N & \cdots & 2/N \\ 2/N & & & \\ & & & 2/N \\ 2/N & \cdots & 2/N & (2/N - 1) \end{bmatrix}$$

- THE PREVIOUS MATRIX DOES INVERSION ABOUT THE MEAN!
- MULTIPLY IT WITH A GENERAL VECTOR OF AMPITUDES:

$$\begin{bmatrix} 2/N-1 & 2/N & \cdots & 2/N \\ 2/N & 2/N-1 & \ddots & 2/N \\ \vdots & \ddots & \ddots & \vdots \\ 2/N & \cdots & 2/N & 2/N-1 \end{bmatrix} \begin{bmatrix} \alpha_0 \\ \vdots \\ \alpha_y \\ \vdots \\ \alpha_{N-1} \end{bmatrix} \rightarrow \begin{bmatrix} \frac{2}{N} \cdot \sum_y \alpha_y - \alpha_x \end{bmatrix}$$

BUT $$\frac{2}{N}\sum_y \alpha_y - \alpha_x = 2 \cdot \left(\frac{\sum \alpha_y}{y} \right) - \alpha_x$$

$$= 2 \cdot \mu - \alpha_x \; \nabla_0$$