# Quantum Computing

## Grover Algorithm.

"Unstructured Search.

Classically: If # entries in DataBase is $M$, then you need to search through all to be sure of finding the one you want.

on average $M/2$

Grove $\sim \sqrt{M}$ searches.

A friend has some # t

state :

$$|t\rangle \longrightarrow -|t\rangle$$

$$|t' \neq t\rangle \longrightarrow |t'\rangle$$

$|t\rangle$ is state of N bits.

$|t_N\rangle|t_{N-1}\rangle \ldots |t_1\rangle$ are the bits

of the ~~#~~ t. in binary.

$$|1\rangle|0\rangle|1\rangle \equiv |101\rangle = |5\rangle$$

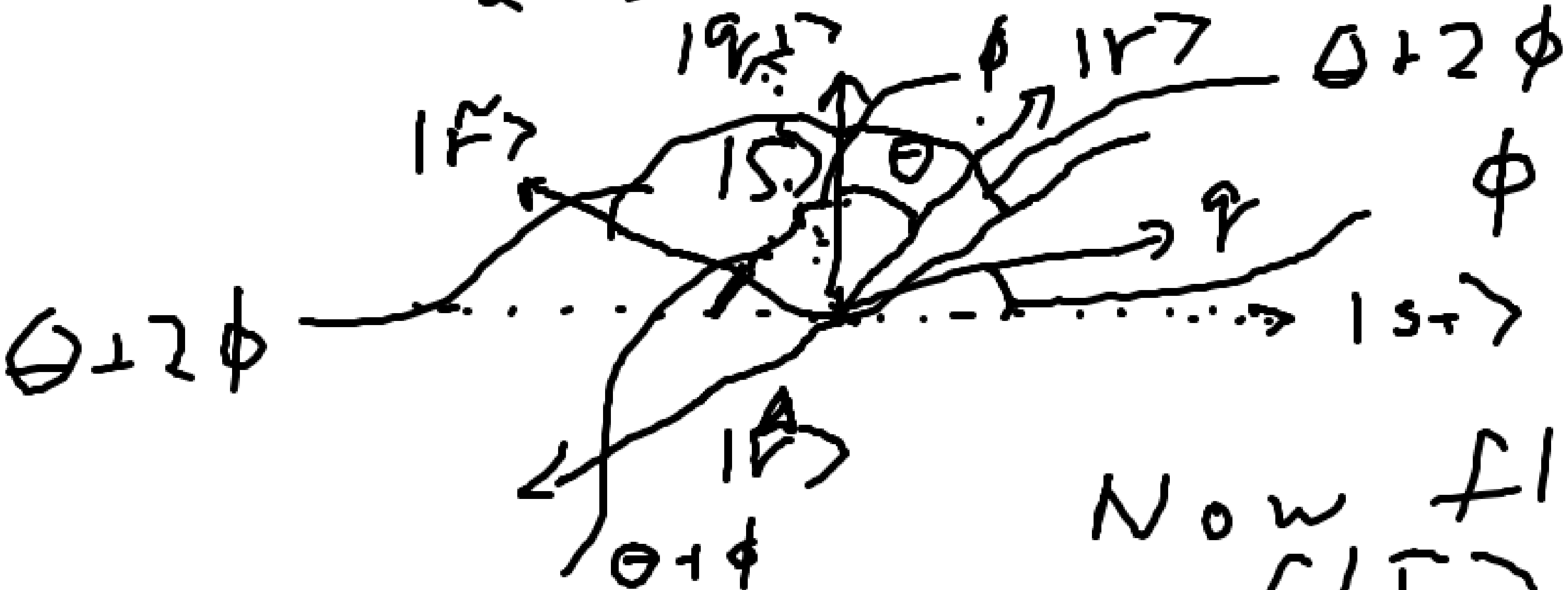
$$\frac{1}{\sqrt{16}}\left(|0\rangle + |1\rangle + |2\rangle + |3\rangle + \ldots |15\rangle\right)$$

$$(|0\rangle + |1\rangle + |2\rangle - |3\rangle + |4\rangle + \ldots + |15\rangle)$$

How Many Queries of friend will tell you what he has.

---

2-D Hilbert space.




$q_T$ and $|r\rangle$ is $\theta+\phi$

Now flip $|S\rangle$ component of $|\bar{r}\rangle$

$|\hat{r}\rangle \longrightarrow -|\hat{r}\rangle$

Angle has increased by $2\phi$ $\theta \to \theta+2\phi$

Keep doing this procedure.

until $\theta + r2\phi = \frac{\pi}{2} - b$

Then $-|\hat{r}\rangle$ will point in dir of

$|\hat{q}\rangle$. $\rightarrow$ measure every bit

of final $|\hat{r}\rangle \rightarrow$ gives me $q$

start with $\theta = 0$. $|r_i\rangle = |s\rangle$

Total trials will be

$$(2R+1)\phi = \frac{\pi}{2}$$

$$R = \frac{1}{2\phi}\left(\frac{\pi}{2}\right) - \frac{1}{2}$$

$\sin\phi = \langle q | s \rangle$

$$|s\rangle = \frac{1}{\sqrt{2^N}} \left( \sum_{m=0}^{2^N-1} |m\rangle \right)$$

H - Hadamard transf.

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

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

$$\prod_{r=0}^{N-1} H_r \, |0\rangle = |s\rangle$$

Then $|q\rangle$ is state of unknown #

$$\langle q | s \rangle = \frac{1}{\sqrt{2^N}}$$

$$\sin\phi = \frac{1}{\sqrt{2^N}}$$ if N large

$$\sin\phi \approx \phi = \frac{1}{\sqrt{2^N}}$$

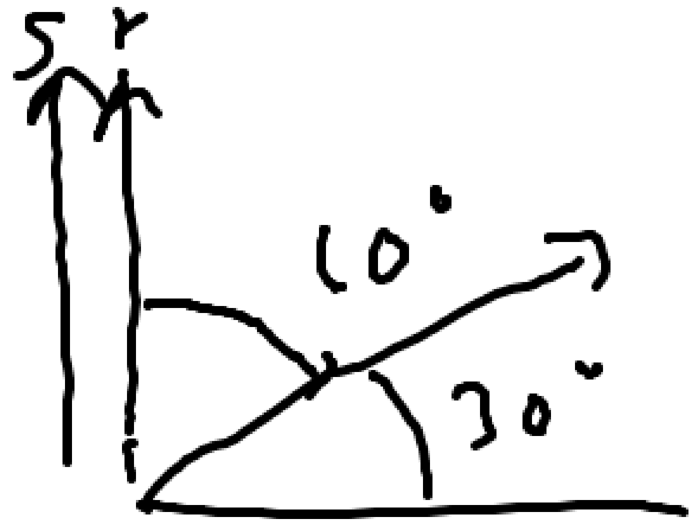
$$R \simeq \frac{\pi}{4}\underbrace{\sqrt{2^N}}_{\sqrt{M}} - \frac{1}{2}$$

R is # times I have to give the state to my friend

$\Rightarrow$ If I give $\sqrt{M}$ times I have v v high $(1-\phi^2)$ prob of finding $|q\rangle$

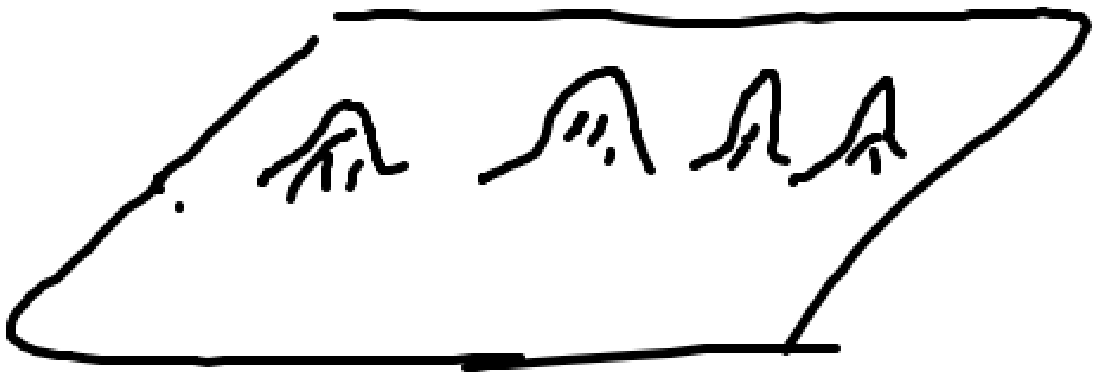
II $N=2$

$\phi = 30^\circ$




$\langle r|s\rangle = \frac{1}{2}$

1 query of friend. know with certainty.



III 1 query know where the "pea" is.

(Scully, ...)

This all depended on flipping sign of $|s\rangle$ component

$|r\rangle \rightarrow$ How do I flip the "s" component?

$$|s\rangle = \prod_{r=0}^{N-1} H_r \; |0\rangle$$

$$H_r^2 = \mathbb{1}$$

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

$$= |0\rangle$$

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

$$\underbrace{\prod_r H_r}^{\mathcal{H}} |s\rangle = |0\rangle$$

$$\prod_r H_r |r\rangle$$

$$\langle s | r \rangle = \langle s | \mathcal{H} \mathcal{H} | r \rangle$$

$$= \langle s | r \rangle$$

So How to flip $|0\rangle$ comp. of $H|r\rangle$ ?

$$|r\rangle = \sum \alpha_m |m\rangle = \underline{\alpha_0} |0\rangle + \sum_1^{2^n-1} \alpha_m |m\rangle$$

$\Downarrow$

flip sign of this?

NOT Gate $N$

$|0\rangle \to |1\rangle$

$|1\rangle \to |0\rangle$

$$N = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad N^2 = \mathbb{1}$$

$$\mathcal{N} = \prod_{r=0}^{n-1} N_{r} \; |r\rangle \qquad \mathcal{N}|0\rangle = |1111\ldots1\rangle$$

If we And all bits then only $|111\ldots1\rangle$ will give 1 at end.

| | |
|---|---|
| 0 0 | $\rightarrow$ 0 |
| 0 1 | $\rightarrow$ 0 |
| 1 0 | $\rightarrow$ 0 |
| 1 1 | $\rightarrow$ 1 |

No way of using only 2 bits to get answer.

There exist a 3 bit operation which gives "AND"

- Ancilla bit.

Start with ancilla being 0

$$
\begin{array}{ccc}
000 & \longrightarrow & 000 \\
010 & \longrightarrow & 010 \\
100 & \longrightarrow & 100 \\
110 & \longrightarrow & 111 \\
001 & \longrightarrow & 001 \\
011 & \longrightarrow & 011 \\
101 & \longrightarrow & 101 \\
111 & \longrightarrow & 110
\end{array}
$$

Unitary Trans on 3 bits.

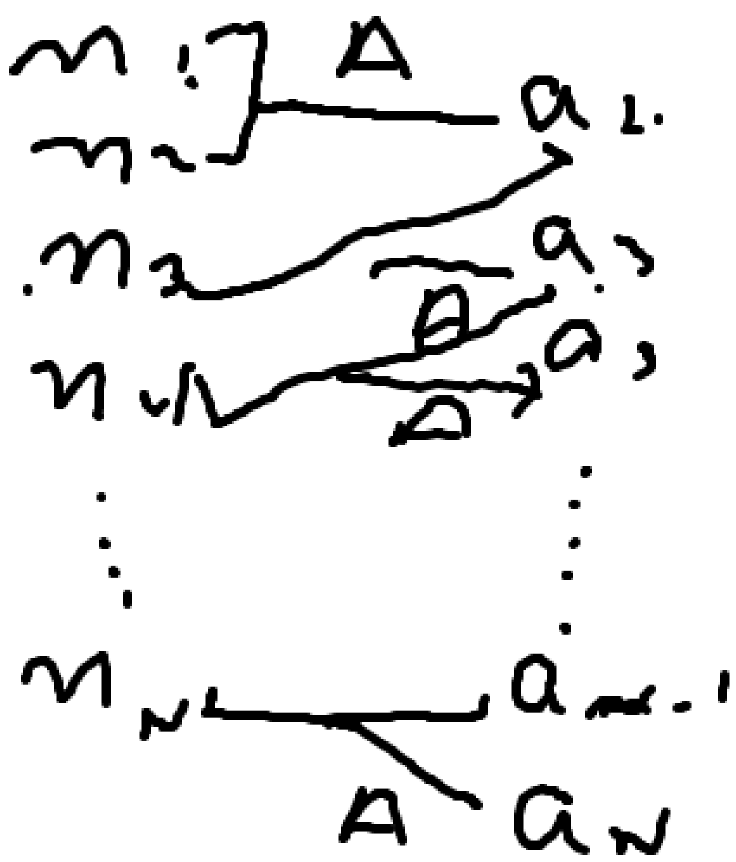
Toffoli gate.

Control Control Not CCNOT

(If 1st bit and 2nd bit are 1, then 3rd bit is reversed)

Note: $(\text{CCNOT})^2 = 1$

bits:




$$|\phi\rangle|\chi\rangle$$
$$|\phi\rangle(-|\chi\rangle)$$
$$= -|\phi\rangle|\chi\rangle$$
$$= (-|\phi\rangle)|\chi\rangle$$

$a_N$ will be 1 only if all of $n_1 \ldots n_N$ are 1.

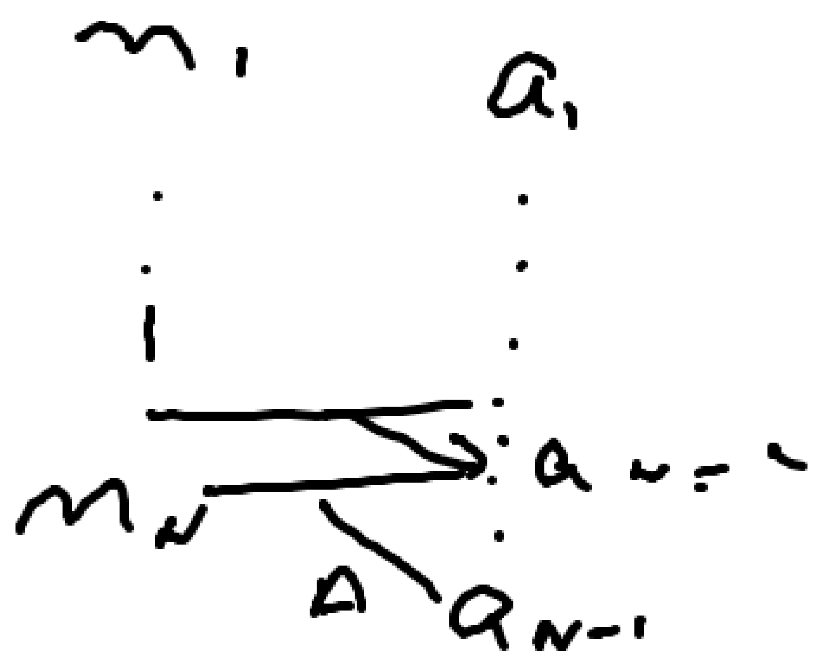
$$H\,a_N = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \quad a_N = 1$$
$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \quad a_N = 0$$

$$\text{NOT } a_N = \frac{1}{\sqrt{2}}(|1\rangle - |0\rangle) = -\frac{1}{\sqrt{2}} \quad H|0\rangle$$
$$= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = (|0\rangle + |1\rangle)/\sqrt{2}$$

So NOT changes sign of state only if $a_N = 1$

Run all operations in reverse.

Run all opns back.




$m_1$ 0

0

$\vdots$ 0

$m_N$ 0

0

0

get back origina state
except − sign if
$|m_1 n_2 n_N \ldots n_1\rangle = |0\rangle$
flip sign only of $|0\rangle$ state
$\mathcal{H}\,|\tilde{r}\rangle \longrightarrow$ flip sign only of the $|s\rangle$ component of
$|v\rangle$.
Only used of order $\sim N$ operations
$(\sim \ln(M))$ small.)

# GROVER