Quantum Computing.

Benniof (IBM), Feynman Mid 1980's

- Calculating a quantum system really hard. Exponential # states

N 2 level systems → 2^N possible states. → 10 systems → 1000 states.

Very hard to canculate a gneric time evolution.

Yet Quantum system has no trouble "calculating" the ground state say of the system. - Quantum Computer should be vastly more efficient at calculating (simulating) a Q. system.

- Great interest in "understanding" Q. systems in the 20, 30's.
- Vastly successful but many questions still not answered.

GROVER ALGORITHM.

"Database" with $N = 2^n$ entries
All are 0 except one is 1 but
which is unknown.
Consider $n+1$ bits. Start all
bits in $|0\rangle$ state. Rotate each
n bit to give $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. $|1\rangle$

$$|\underbrace{0,0,\ldots,0}_{n},0\rangle \rightarrow \frac{1}{\sqrt{2^n}}(|0\rangle+|1\rangle)(|0\rangle+|1\rangle)\ldots(|0\rangle+|1\rangle)\,|0\rangle$$

The n bits can be taken as an expression
of the numbers from 0 to $N-1$ in binary.

Rotations $|0\rangle|1\rangle|1\rangle|0\rangle|1\rangle \equiv |13\rangle$

Rotate the last bit to do $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

$$\frac{1}{\sqrt{2^n}} \sum_r |r\rangle(|0\rangle - |1\rangle)$$

$U U|q\rangle(|0\rangle - |1\rangle) \Rightarrow |r\rangle|1\rangle$ if q is the entry in database.

$$U|q\rangle|1\rangle = |q\rangle|0\rangle$$

$$U|r\neq q\rangle|0\rangle = |r\rangle|0\rangle$$

$$U|r\neq q\rangle|1\rangle = |r\rangle|1\rangle$$

$$U\Big(\sum |r\rangle(|0\rangle - |1\rangle)\Big)$$

$$= (\Sigma|1\rangle + |2\rangle + \cdots - |q\rangle + \cdots)(|0\rangle - |1\rangle)$$

Thus the sign has been flipped of the
key item.

$U = I - 2|q\rangle\langle q|$

$U_s = 2|s\rangle\langle s| - I$

$U_s U = -I + 2|s\rangle\langle s| + 2|q\rangle\langle q| - \frac{4}{\sqrt{2^N}}|s\rangle\langle q|$

$U_s U\ (\alpha|s\rangle + \beta|q\rangle) = -(\alpha|s\rangle + \beta|q\rangle)$

$+ 2\alpha|s\rangle + \frac{2\beta}{\sqrt{2^N}}|q\rangle + 2\beta|q\rangle$

$+ \frac{2}{2^N}|q\rangle\alpha + 2\beta|q\rangle$

$- \frac{4}{2^N}\alpha|s\rangle - \frac{4\beta}{\sqrt{2^N}}|s\rangle$

$= \left(\alpha + 2\left(1 - \frac{4}{2^N}\right) - \frac{2}{\sqrt{2^N}}\beta\right)|s\rangle$

$+ \left(\beta + \frac{2}{\sqrt{2^N}}\alpha\right)|q\rangle \qquad \beta'$

β keeps increasing

α keeps decreasing until it goes -ve.

Start with $\alpha = 1, \beta = 0$

$\alpha = \left(1 - \frac{1}{2^{N-2}}\right) \quad \beta = \frac{1}{\sqrt{2^{N-2}}} \qquad \beta' =$

$\alpha = \left(1 - \frac{1}{2^{N-2}}\right)\left(1 - \frac{1}{2^{N-2}}\right) + \frac{1}{\sqrt{2^{N-3}}}$

$\beta = \frac{1}{\sqrt{2^{N-2}}} + \frac{1}{\sqrt{2^{N-2}}}\left(1 - \frac{1}{2^{N-2}}\right)$

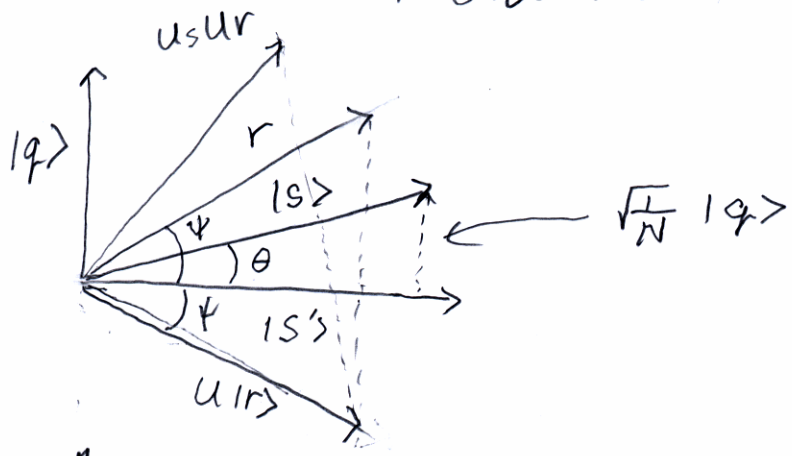
$N=0$, no steps. (classical)

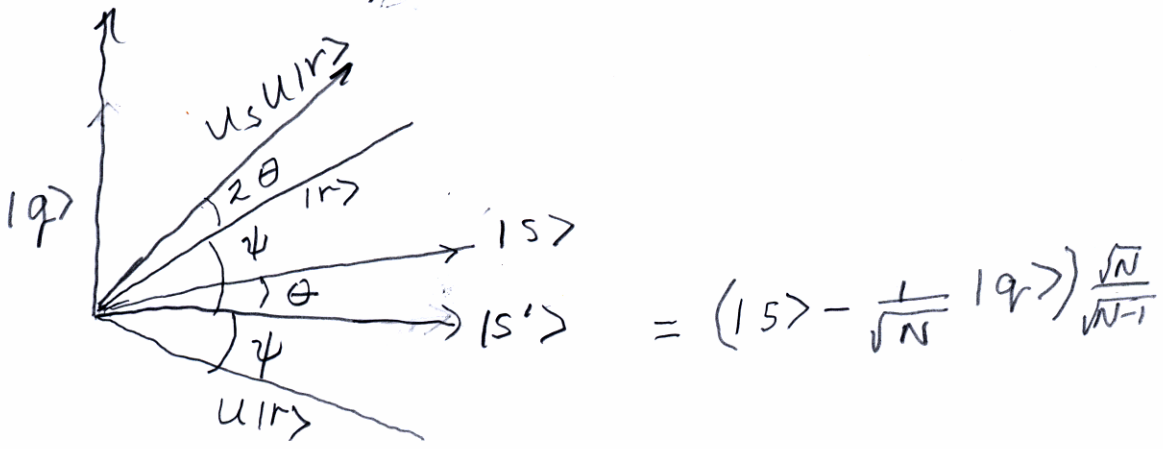
$N=1$, 1 step. (classical)

$N=2$, 1 step. with certainty.

$N=3$, 2 steps. high prob.

Geometric Groveris





$U_s U|r\rangle$ has angle $\psi + 2\theta$ with respect to $|s'\rangle$ if $|r\rangle$ had angle $|\psi\rangle$

Apply q times and get angle

$\psi + 2m\theta$

Take initial $|r\rangle = |s\rangle$ - angle θ

after q steps $(2m+1)\theta$.

$\sin\theta = \frac{1}{\sqrt{N}}$ for large N

$\theta \approx \frac{1}{\sqrt{N}} \Rightarrow \frac{(2m+1)}{\sqrt{N}} \stackrel{?}{\approx} \frac{\pi}{2}$ q integer good choice.

$q \approx \left[\frac{1}{2}\left(\frac{\pi}{2}\sqrt{N} - 1\right)\right]$ - nearest integer

$\Delta\theta < \theta = \frac{1}{\sqrt{N}}$ Prob $> (\cos\Delta\theta)^2$

$$P_q \geq \approx \left(1 - \frac{\Delta\theta^2}{2} + \cdots\right)^2 \approx 1 - \Delta\theta^2 > 1 - \theta^2 = 1 - \frac{1}{N}$$

Measurement of each bit gives q.

$$\underbrace{|0\rangle|1\rangle|1\rangle|0\rangle|0\rangle\ldots}_{q}$$

q is determined to high accuracy

in $m \approx \frac{\pi}{4}\sqrt{N}$ steps.

Note m is completely determined by N. not by unknown q.

$|s\rangle$ is known so U_s is known.

$|q\rangle$ not known but U is determined by a known procedure even if $|q\rangle$ is unknown (by querying the "data base")

Note the querying of data base must be done in a way that no information is left behind as to which element of data base was queried. → "Hard" but possible

Grover really "shines" if say you have a function $f(n)$. You know for some n, $f(n)=0$, and non zero for all other n.

Convert to function which is 1 for that n and 0 for all others.

```
If ( f(n) = 0)
     {print (1);}
else
     {print (0);}
```

In calculating $f(n)$ and running if..else you can leave no trace behind of what n is or what was printed except the output.

$|A\rangle\ |n\rangle|0\rangle \Rightarrow |A\rangle|n\rangle|\tilde{f}(n)\rangle$

(Quantum computers must be reversible. Ie given only the output, run the program in reverse to get input.)

[R Landauer emphasised – erasures are bad.
Erasure leaves evidence in environment of the calculation without the environment cannot reverse.]