S. KIMMEL

Goal:

- Learn analysis technique of reducing to a smaller subspace
- Analyze quantum search algorithm

Search Problem

Given $f:\{0,1\}^n \to \{0,1\}$, find s such that $f(s)=1$, promised exactly 1 such s.

- Classical Case:

Given classical f, what is deterministic / probabilistic query complexity?

A) 2^n, $O(2^n/\log(n))$

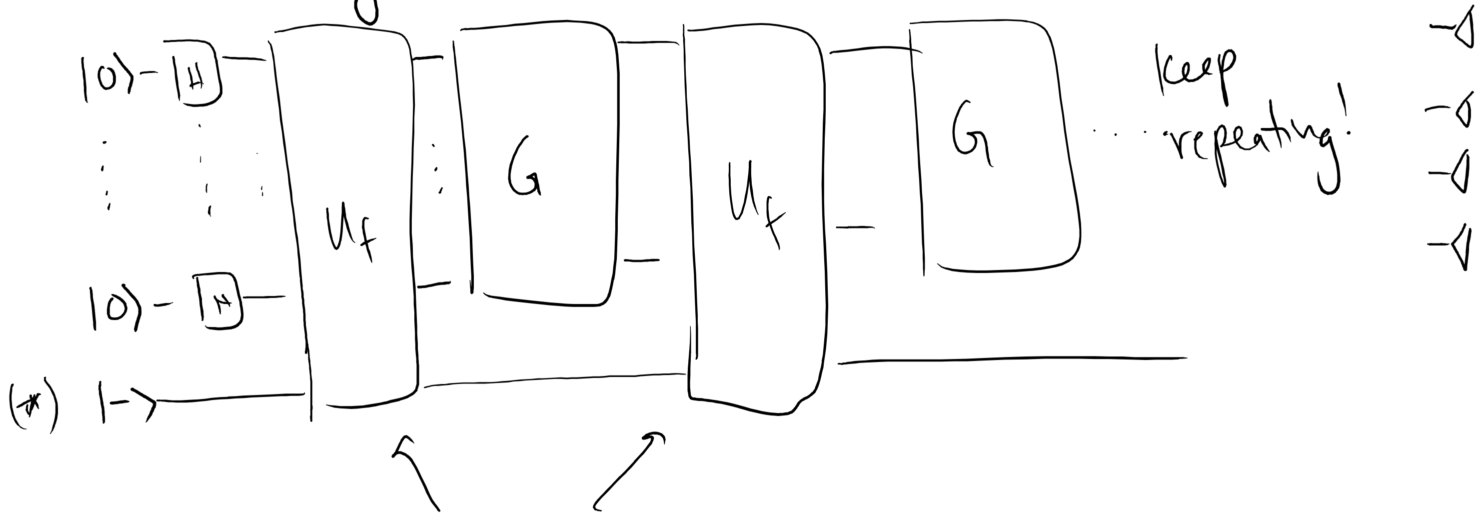
B) 2^n-1, $O(2^n)$

C) 2^n-1, $O(2^n/\log(n))$

D) 2^n, $O(2^n)$

S. KIMMEL

Quantum Alg:



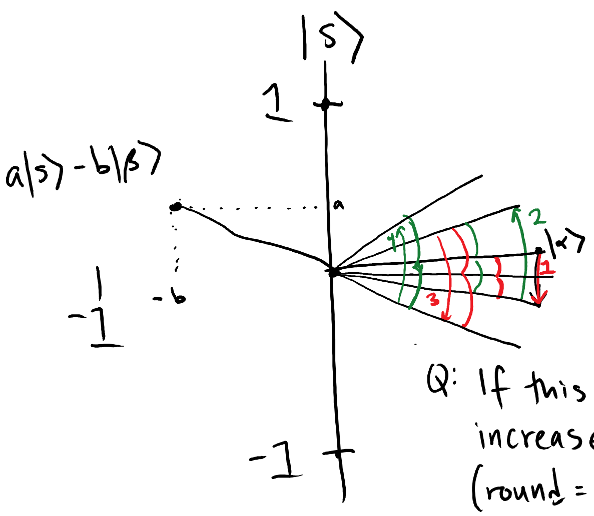
phase kickback

$$|x\rangle|-\rangle \rightarrow (-1)^{f(x)}|x\rangle|-\rangle$$

U_f: $\mathbb{I} - 2|s\rangle\langle s|$ (applies -1 to $|s\rangle$, $+1$ to all other standard basis states

G_f: $-\mathbb{I} + 2|\alpha\rangle\langle\alpha|$ (applies $+1$ to equal superposition state, -1 to any orthogonal state)

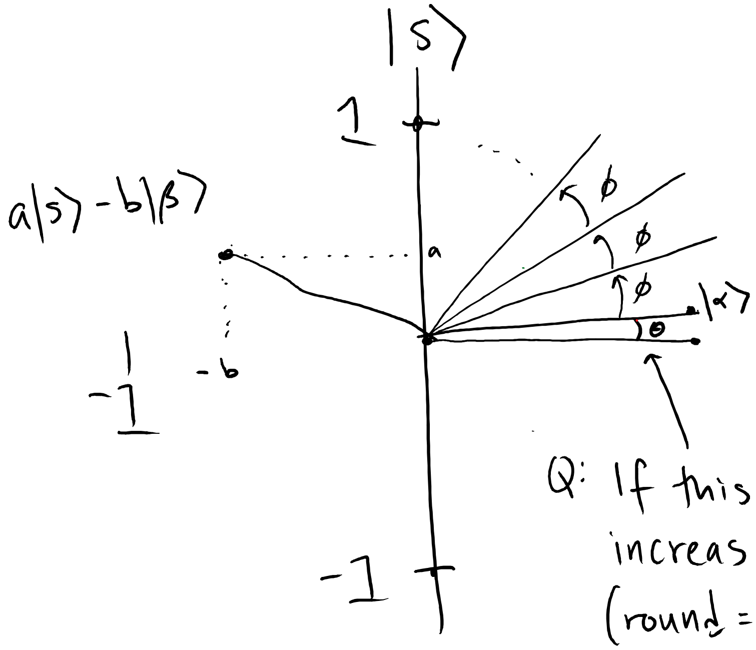
$$|\alpha\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle$$



$$|\beta\rangle = \frac{1}{\sqrt{2^n-1}} \sum_{x \neq s} |x\rangle$$

Q: If this angle is θ, what angle increase after each round (round = 2 reflections)

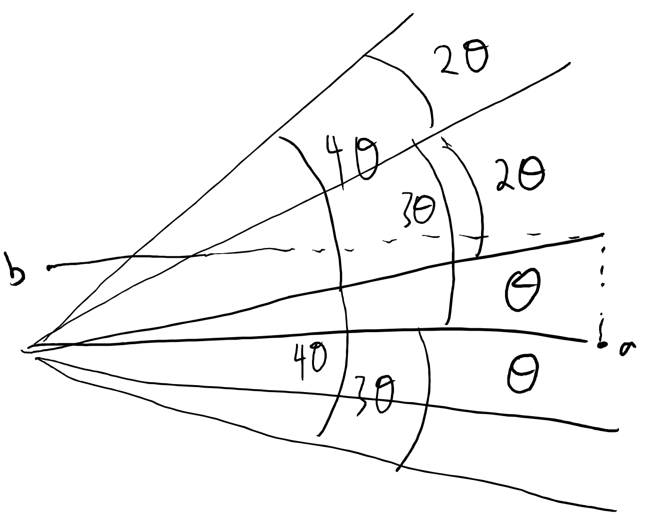
S.KIMMEL



$$|\beta\rangle = \frac{1}{\sqrt{2^n - 1}} \sum_{x \neq s} |x\rangle$$

Q: If this angle is θ, what angle increase after each round (round = 2 reflections)

Q: What is θ in terms of n?



- 2θ each time

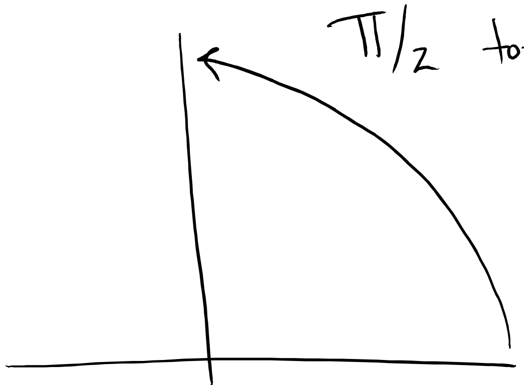
$$a \sum_{x \neq s} \frac{1}{\sqrt{2^n - 1}} |x\rangle + b|s\rangle = \sum_x \frac{1}{\sqrt{2^n}} |x\rangle$$

$$a = \frac{\sqrt{2^n - 1}}{\sqrt{2^n}} \qquad b = \frac{1}{\sqrt{2^n}}$$

$$\theta = \tan^{-1}\left(\frac{b}{a}\right) = \tan^{-1}\left(\frac{1}{\sqrt{2^n - 1}}\right)$$

$$= O\left(\frac{1}{\sqrt{2^n}}\right)$$

S.KIMMEL



$\pi/2$ total, $\frac{1}{\sqrt{2^n}}$ each round,

$\Rightarrow O(\sqrt{2^n})$ rounds

Query complexity $= O(\sqrt{2^n})$

(If repeat too many times, over-rotate!)

Applications

- Any classical algorithm that succeeds with prob $p \rightarrow$ can create quantum version that succeeds with prob $\sqrt{p}$.

ex: One of the best $\underbrace{\text{3-SAT}}_{\text{NP hard problem}}$ alg: $p = \left(\frac{3}{4}\right)^n$ ⇐ so need to repeat $O\left(\left(\frac{4}{3}\right)^n\right)$ times to be successful

$\Rightarrow$ Quantum version $\rightarrow$ $O\left(\left(\frac{4}{3}\right)^{n/2}\right)$ times.

Square Root Speed Up is less impressive than exponential, but:

$n = 200$ (200 cities in traveling salesman $\rightarrow$ 10^{24} classical

10^{12} quantum

1 GHz processor : 31 million years (classical)

16 min (quantum)