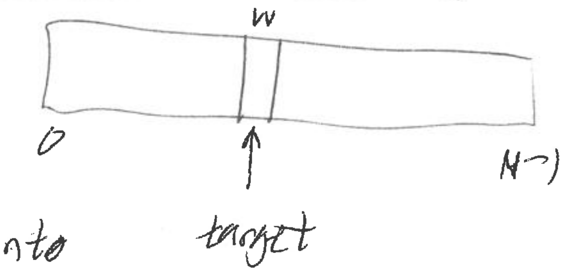
CSCE 785
11/9/2023

Grover's Algo for Quantum Search

N items in an array



$N = 2^n$: n qubits, values as indices into the array. Let w be the index of the target.

Have
An n-qubit quantum gate I_f such that $\forall x \in \{0,1\}^n$,

$$I_f|x\rangle = (-1)^{f(x)}|x\rangle = \begin{cases} -|x\rangle & \text{if } x = w \\ |x\rangle & \text{o.w.} \end{cases}$$

where $f : \{0,1\}^n \to \{0,1\}$ is such that $f(w) = 1$ and $f(x) = 0$ for all $x \neq w$.

$$I_f = \begin{array}{c c} & \begin{matrix} & & w & & \\ & & \downarrow & & \end{matrix} \\ w \rightarrow & \begin{bmatrix} 1 & & & & 0 \\ & 1 & & & \\ & & \ddots & & \\ & & & -1 & \\ & & & & \ddots \\ 0 & & & & 1 \end{bmatrix} \end{array} = I - 2|w\rangle\langle w|$$

Each use of I_f we be a "probe". [Classically, $\Theta(N)$ probes needed in the worst or avg case.]

Define $$I_0 = I - 2|0^n\rangle\langle 0^n| = \begin{bmatrix} -1 & & & 0 \\ & 1 & & \\ & & \ddots & \\ 0 & & & 1 \end{bmatrix}$$

I_0 has an efficient quantum circuit.

Also: assume we have an n-qubit unitary U such that $\langle w|U|0^n\rangle \neq 0$. Set $x := \langle w|U|0^n\rangle$.

not necessarily → Can assume $x > 0$ by adjusting the global phase of U.

Ex: $U = H^{\otimes n}$; $\quad U|0^n\rangle = \frac{1}{2^{n/2}} \sum_{z \in \{0,1\}^n} |z\rangle$

So $x = \langle w|U|0^n\rangle = \boxed{\frac{1}{2^{n/2}}}$ [Bigger x is better, but Can't do better than this]

$x \leq 1$ [If $x=1$, then done! So assume $x<1$.]

So $\underline{0 < x < 1}$. So there is a unique θ, $0<\theta<\frac{\pi}{2}$ such that $x = \sin\theta$ $\quad (\theta = \sin^{-1} x = \arcsin x)$

$\theta \approx x$ when x is small

<u>Grover's algo</u>

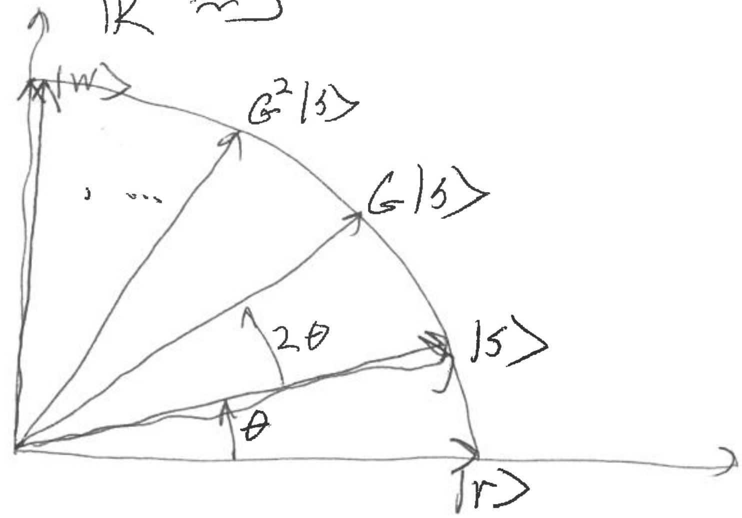
1. Initialize n qubits to $|0^n\rangle$
2. Apply U to get $|s\rangle := U|0^n\rangle$ [$|s\rangle$ is the <u>start state</u>] $\quad x = \langle w|s\rangle$
3. Apply G to $|s\rangle$ $\left\lfloor \frac{\pi}{4\theta} \right\rfloor = \left\lfloor \frac{\pi}{4\sin^{-1}x} \right\rfloor$ many times $\quad \approx \frac{\pi}{4} 2^{n/2} = \frac{\pi}{4}\sqrt{N}$

   where
   $$G := -U I_0 U^* I_f$$
   is the <u>Grover iterate</u>.

4. Measure all n qubits in the comp. basis, get y.
   [$y = w$ with <u>very</u> high probability.

Let S be the (real!) plane spanned by $|s\rangle$ and $|w\rangle$. G maps S into S.

$\mathbb{R}^2 \simeq S$



$$G = -U I_0 U^* I_f = -U(I - 2|0^n\rangle\langle 0^n|)U^*(I - 2|w\rangle\langle w|)$$

$$= -(I - 2U|0^n\rangle\langle 0^n|U^*)(I - 2|w\rangle\langle w|)$$

$$= -(I - 2|s\rangle\langle s|)(I - 2|w\rangle\langle w|)$$

$$= -I + 2|s\rangle\langle s| + 2|w\rangle\langle w| - 4x|s\rangle\langle w|$$

$$G|s\rangle = (1 - 4x^2)|s\rangle + 2x|w\rangle$$

$$G|w\rangle = -2x|s\rangle + |w\rangle$$

Set $|r\rangle := \dfrac{|s\rangle - x|w\rangle}{\sqrt{1-x^2}}$

Check: $\{|r\rangle, |w\rangle\}$ is an ortho. basis for the plane S.

Also check:

$$|s\rangle = \sqrt{1-x^2}\,|r\rangle + x|w\rangle = \cos\theta\,|r\rangle + \sin\theta\,|w\rangle$$

Express G with respect to the $\{|r\rangle, |w\rangle\}$ basis

Restricted to S

$$G = -I + 2|s\rangle\langle s| + 2|w\rangle\langle w| - 4x|s\rangle\langle w|.$$

$$= -(|r\rangle\langle r| + |w\rangle\langle w|) + 2|s\rangle\langle s| + 2|w\rangle\langle w| - 4x|s\rangle\langle w|$$

$-|w\rangle\langle w|$

$$= -|r\rangle\langle r| - |w\rangle\langle w| + 2(\cos\theta|r\rangle + \sin\theta|w\rangle)(\cos\theta\langle r| + \sin\theta\langle w|)$$
$$+ 2|w\rangle\langle w| - 4\,\overset{\sin\theta}{\cancel{x}}\,[(\cos\theta|r\rangle + \sin\theta|w\rangle)]\langle w|$$

$$= (2\cos^2\theta - 1)|r\rangle\langle r|$$
$$+ (-2\sin\theta\cos\theta)|r\rangle\langle w|$$
$$+ (2\cos\theta\sin\theta)|w\rangle\langle r|$$
$$+ (1 - 2\sin^2\theta)|w\rangle\langle w|$$

$$= \begin{bmatrix} \cos(2\theta) & -\sin(2\theta) \\ \sin(2\theta) & \cos(2\theta) \end{bmatrix}$$ w.r.t. the $|r\rangle, |w\rangle$ basis

Apply G m times, get angle

$(2m+1)\theta$ from $|r\rangle$ want $(2m+1)\theta$ to be as close to $\frac{\pi}{2}$ as possible.