Grover's Algorithm

→ Algorithm "searching an unsorted database" with $N = 2^n$ elements in $O(\sqrt{N})$ time.

Rather : find x, $\to$ $f(x) = 1$

Classical algorithm : Needs on avg $\frac{N}{2} = O(N)$ time.

Goal: Find element (final), w, given an oracle U_f with $f : \{0,1\}^n \to \{0,1\}$.

$$f(x) = \begin{cases} 1, & \text{if } x = w \\ 0, & \text{else} \end{cases}, \quad f_0(x) = \begin{cases} 0, & \text{if } x = 00\ldots0 \\ 1, & \text{else} \end{cases}$$

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

$$U_f : |w\rangle \to -|w\rangle$$

$$|x\rangle \to |x\rangle \quad \forall x \neq w$$

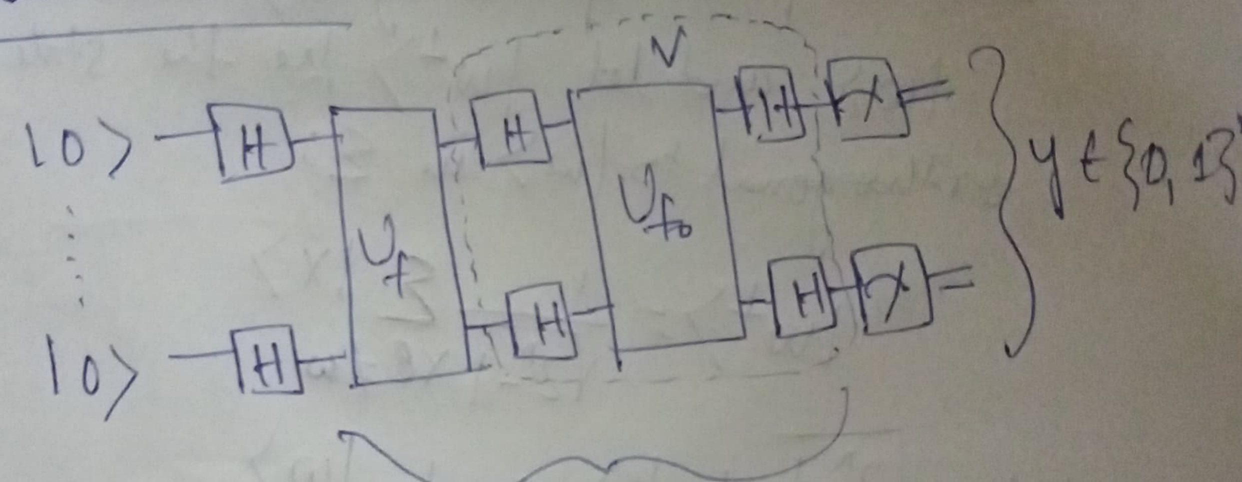
$$U_f = I - 2|w\rangle\langle w|$$

$$U_{f_0} : |0\rangle^{\otimes n} \rightarrow |0\rangle^{\otimes n}$$

$$|x\rangle \rightarrow -|x\rangle \quad \forall x \neq 00\cdots0$$

$$U_{f_0} = 2|0\rangle\langle 0|^{\otimes n} - I$$

<u>Quantum Circuit :</u>



Repeat 'r' times.

<u>Claim</u>: $y = \omega$ (with high probability)

<u>Proof</u>: Let us define the uniform superposition state

$$|s\rangle = H^{\otimes n} |0\rangle^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle$$

and, $V = H^{\otimes n} U_{f_0} H^{\otimes n} = H^{\otimes n}\, 2|0\rangle\langle 0|^{\otimes n}\, H^{\otimes n} -$
$H^{\otimes n} \cdot I \cdot H^{\otimes n}$

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

Grover's Algorithm carries out the operation $(V_s U_f)^r$ on the state $|s\rangle$

Let Σ be the plane spanned by $|s\rangle$ and $|w\rangle$ and let $|w^\perp\rangle$ be the state orthogonal to $|w\rangle$ in Σ:

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

$$\Rightarrow |s\rangle = \sqrt{\frac{2^n-1}{2^n}}\, |w^\perp\rangle + \frac{1}{\sqrt{2^n}} |w\rangle$$

$$=: \cos\frac{\theta}{2} |w^\perp\rangle + \sin\frac{\theta}{2} |w\rangle$$

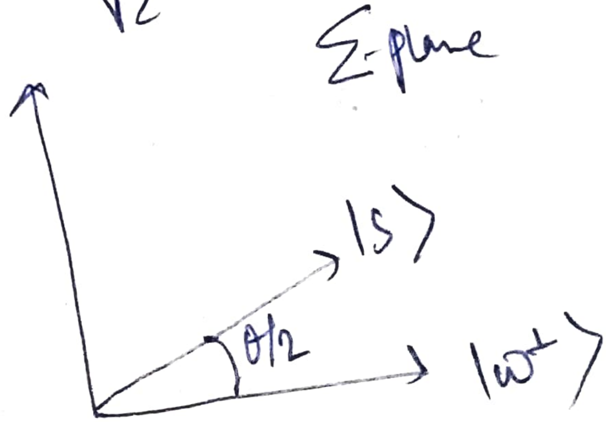
$\uparrow$

define θ,

$$\sin\frac{\theta}{2} = \frac{1}{\sqrt{2^n}}$$

$$\rightarrow \theta = 2 \arcsin \frac{1}{\sqrt{2^n}}$$

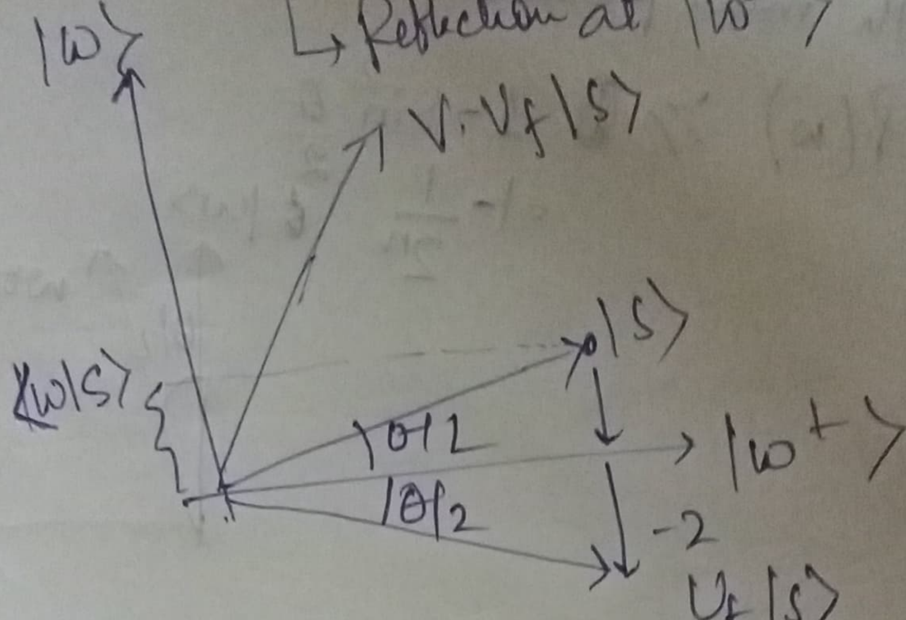
Protocol:



Step 1: Prepare $|s\rangle$

Step 2: Apply $U_f = I - 2|w\rangle\langle w|$

↳ Reflection at $|w^\perp\rangle$



3) Apply $V = 2|s\rangle\langle s| - I$

↳ Reflection at $|s\rangle$

→ $V \cdot U_f$ corresponds to a rotation by an angle θ

→ after r application of Step 2 and 3, the state is rotated by $r \cdot \theta$.

→ Choose r, s.t. $r \cdot \theta + \frac{\theta}{2} \approx \pi/2$

→ $r = \frac{\pi}{2\theta} - \frac{1}{2}$ θ → depends on no. of qubits

$= \frac{\pi}{4 \arcsin \frac{1}{\sqrt{2^n}}} - \frac{1}{2} \underset{\text{if } n \text{ large}}{\approx} \frac{\pi}{4}\sqrt{2^n} = O(\sqrt{N})$

→ After r calls to the orale, the final measurement will result in state $|\omega\rangle$, with min. probability.

$$P(\omega) \geq 1 - \sin^2\frac{\theta}{2}$$

$$= 1 - \frac{1}{2^n}$$