GROVER'S SEARCH ALGORITHM II

▸ GROVER'S STEPS CAN BE SUMMARIZED AS follows:

INPUT: A function $f:\{0,1\}^n \to \{0,1\}$ for which $f(x)=0$ for all $x\in\{0,1\}^n$ except for a single x_0, for which $f(x_0)=1$. The function f is given is an oracle form that performs the unitary transform $|x\rangle|b\rangle \to |x\rangle|b\oplus f(x)\rangle$.

OUTPUT: x_0 (with high probability)

1) Input initialization: $|0\rangle^{\otimes n}|0\rangle$

2) Apply Hadamard $H^{\otimes n}$ on the 1st n qbits and H on the last qbit $|0\rangle$:

$$\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle\otimes\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)$$

3) Apply the oracle $|x\rangle|b\rangle\to|x\rangle|b\oplus f(x)\rangle$:

$$\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle\cdot(-1)^{f(x)}\otimes|-\rangle$$

This performs the <u>PHASE INVERSION</u> step: the amplitudes of all $|x\rangle: x\neq x_0$ stay the same but the amplitude of $|x_0\rangle$ gets inverted ($|x_0\rangle\to-|x_0\rangle$).

4) Inversion about the mean: apply $H^{\otimes n}[2|0\rangle\langle 0|-I]\cdot H^{\otimes n}$

- Perform steps (3)-(4) for about $\sim\sqrt{2^n}$ times
⇒ amplitude of $|x_0\rangle$ gets amplified to $1/\sqrt{2}$.

- REFLECTION ABOUT THE UNIFORM SUPERPOSITION $|u\rangle = \frac{1}{\sqrt{2^n}} \sum_x |x\rangle$ IS EQUIVALENTO TO INVERSION ABOUT THE MEAN.

- THE UNITARY OPERATOR $2|0\rangle\langle 0| - I$ PERFORMS REFLECTION ABOUT $|0\rangle$.

FACT: $2|u\rangle\langle u| - I = H^{\otimes n}\left[2|0\rangle\langle 0| - I\right]H^{\otimes n}$

I.E: REFLECTING ABOUT $|u\rangle$ IS THE SAME AS 1st) TRANSFORMING $|u\rangle$ TO $|0\cdots 0\rangle$, 2ND) REFLECTING ABOUT $|0\cdots 0\rangle$ AND 3RD) TRANSFORMING BACK.

PROOF: $|u\rangle\langle u| = H^{\otimes n}|0\rangle\left(H^{\otimes n}|0\rangle\right)^T$ $\quad (Ax)^T = x^T A^T$

$= H^{\otimes}|0\rangle(|0\rangle)^T(H^{\otimes n})^T$ $\quad |a\rangle = \langle a|^T$ BY DEFINITION

$= H^{\otimes}|0\rangle\langle 0|H^{\otimes n}$ $\quad H^T = H$

REFLECTION OPERATOR: GIVEN ANY VECTOR $|a\rangle$, THE UNITARY OPERATOR $2|a\rangle\langle a| - I$ PERFORMS A REFLECTION ABOUT $|a\rangle$

REMEMBER THAT IN ORDER TO REFLECT $|b\rangle$ ABOUT $|a\rangle$, WE RESOLVE $|b\rangle$ INTO THE COMPONENT PARALLEL TO $|a\rangle$ AND ORTHOGONAL TO $|a\rangle$, AND WE FLIP THE ORTHOGONAL COORDINATE:

$|b\rangle = c\cdot|a\rangle + d|a^\perp\rangle$ ($|a^\perp\rangle$ IS PERPENDICULAR/ORTHOGONAL TO $|a\rangle$)

THEN: $\left[2|a\rangle\langle a| - I\right]\cdot|b\rangle = \left[2|a\rangle\langle a| - I\right]\cdot(c\cdot|a\rangle + d\cdot|a^\perp\rangle)$

$= 2c|a\rangle\langle a|a\rangle - c\cdot|a\rangle + 2d|a\rangle\langle a|a^\perp\rangle - d|a^\perp\rangle =$

$= 2c|a\rangle - c|a\rangle - d|a^\perp\rangle$

$= c|a\rangle - d|a\rangle$ ✓

(IN THE ABOVE WE HAVE USED: $\langle a|a\rangle = 1$ SINCE $|a\rangle$ BY ASSUMPTION IS UNIT VECTOR AND $\langle a|a^\perp\rangle = 0$ SINCE THEY ARE ORTHOGONAL.)

- Identically $I - 2|\alpha\rangle\langle\alpha|$ Reflects about $|\alpha^{\perp}\rangle$, i.e., the subspace orthogonal to $|\alpha\rangle$ ∎

- **Corollary**: Phase Inversion operator is in fact an Inversion about the subspace orthogonal to $|x_0\rangle$ ∎

- But what is the subspace orthogonal to $|x_0\rangle$?
- It is simply the state $|\psi\rangle = \frac{1}{\sqrt{2^n - 1}} \sum_{x \neq x_0} |x\rangle$
- Why? Because $x \in \{0,1\}^n$ and $|x_0\rangle$ is orthogonal (inner product zero) to each $x \neq x_0$ ∎

$$\langle x_0|\psi\rangle = \frac{1}{\sqrt{2^n - 1}} \sum_{x \neq x_0} \langle x_0|x\rangle = 0$$

- But why Phase Inversion should be a Reflection about $|\psi\rangle$?
- We know that Phase Inversion flips the sign of the amplitude of $|x_0\rangle$ and leaves everything else alone.
- $|x_0\rangle$ is orthogonal to $|\psi\rangle$.
- A general vector $|z\rangle$ can be decomposed as

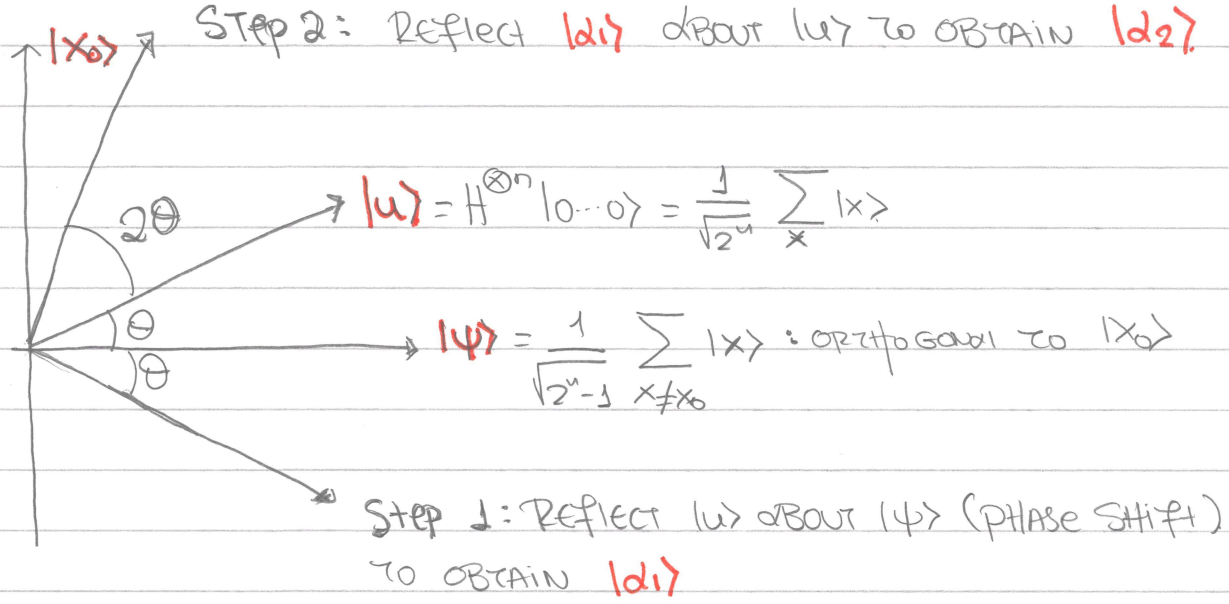
$$|z\rangle = a_1|x_0\rangle + b_1|\psi\rangle$$

- Applying the oracle which performs a Phase Shift, will change the sign of $|x_0\rangle$ but leave $|\psi\rangle$ alone, so $|z\rangle$ will be trasformed to:

$$|z'\rangle = -a_1|x_0\rangle + b_1|\psi\rangle$$

which is equivalent to a Reflection about $|\psi\rangle$ ∎.

GEOMETRIC INTERPRETATION OF GROVER'S ALGORITHM



- WHAT IS θ?
- APPLYING THE ORACLE (PHASE SHIFT OPERATOR) TO OUR INITIAL STATE $|u\rangle$ GIVES US THAT.

$$|\alpha_1\rangle = \cos\theta|\psi\rangle - \sin\theta|x_0\rangle$$

$$\Rightarrow \sin\theta = \frac{1}{\sqrt{2^n}} \quad \text{AND} \quad \cos\theta = \sqrt{\frac{2^n-1}{2^n}}$$

$$\Rightarrow |u\rangle = \cos\theta|\psi\rangle + \sin\theta|x_0\rangle.$$

$\Rightarrow |u\rangle, |\alpha_1\rangle, |\alpha_2\rangle$ ARE ALWAYS ON THE 2-DIMENSIONAL VECTOR SPACE SPANNED BY $|x_0\rangle$ AND $|\psi\rangle$.

⚠ IN GENERAL, IF WE HAD N ELEMENTS AND M SOLUTIONS THEN $\sin\theta = \sqrt{\frac{M}{N}}$ AND $\cos\theta = \sqrt{\frac{N-M}{M}}$ ⚠

- PHASE SHIFT + INVERSION ABOUT THE MEAN PRODUCE THE STATE $|\alpha_2\rangle$:

$$|\alpha_2\rangle = \cos 3\theta|\psi\rangle - \sin 3\theta|x_0\rangle$$

△ If we apply PHASE SHIFT + INVERSION ABOUT THE MEAN k TIMES THEN:

$$|\alpha_{2k}\rangle = \cos(2k+1)\theta\,|\psi\rangle + \sin(2k+1)\theta\,|x_0\rangle.$$

LOOK: if $N = 2^2 = 4$ AND $M = 1$
THEN $\sin\theta = \frac{1}{\sqrt{4}} = \frac{1}{2} \Rightarrow \theta = 30°$

AFTER A SINGLE GROVER STEP, $|\alpha_2\rangle$ WILL MAKE ANGLE $2\theta + \theta$ WITH $|\psi\rangle = 3\theta = 90°$, I.E. $|\alpha_2\rangle$ PERFECTLY ALIGNS WITH THE UNIQUE SOLUTION $|x_0\rangle$ ▽

SAME IS TRUE FOR $N = 8, M = 2$ ETC. ▽