Grover's algorithm — solves SAT (NP-complete)

$N = 2^n$

for a satisfying assignment a (a bit string of size n) → what we want to find

$$^{*} f(x) = \begin{cases} 1 & \text{if } x = a \\ 0 & \text{otherwise} \end{cases}$$

$$|\psi_0\rangle = H^{\otimes n} \underbrace{|0\ldots0\rangle}_{n \text{ q-bits}} = \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)^{\otimes n}$$

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

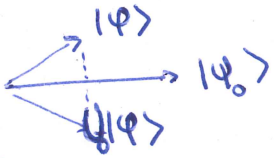
$$H^{\otimes n} I H^{\otimes n} = I$$

$$U_0 = 2|\psi_0\rangle\langle\psi_0| - I = H^{\otimes n}\left[2|0\ldots0\rangle\langle 0\ldots0| - I\right] H^{\otimes n}$$

$O(n)$ H gates

$$\begin{cases} U_0|\psi_0\rangle = |\psi_0\rangle \\ |\varphi\rangle \perp |\psi_0\rangle \Rightarrow U_0|\varphi\rangle = -|\varphi\rangle \end{cases}$$

reflection around $|\psi_0\rangle$

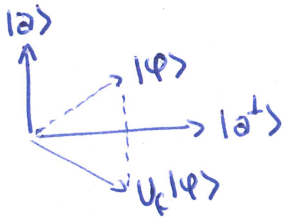


$$U_f : |x\rangle \longrightarrow (-1)^{f(x)} |x\rangle \quad ^{*}\begin{cases} |x\rangle \text{ for } x \neq a \\ -|a\rangle \text{ for } x = a \end{cases}$$

(see phase kick-back)

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

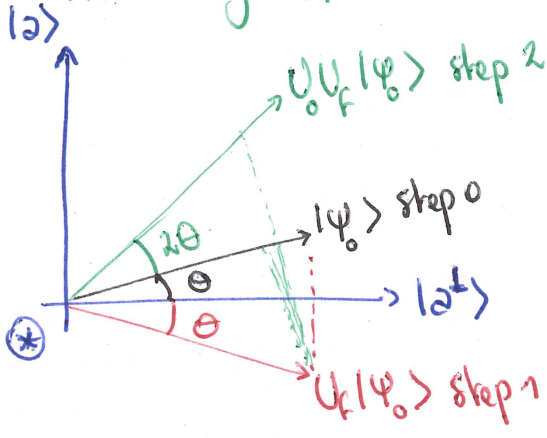
reflection around $|a^{\perp}\rangle$



Grover iteration: $G = U_0 U_f$ $(1+2)^{*}$

U_0 & U_f leave the subspace spanned by $(|\psi_0\rangle, |a\rangle)$ invariant

The orthogonal basis of the subspace is: $\begin{cases} |a\rangle \\ |a^{\perp}\rangle = \frac{1}{\sqrt{2^n - 1}} \sum_{x \neq a} |x\rangle \end{cases}$



$$\cos\theta = \langle\psi_0|a^{\perp}\rangle \Rightarrow \sin\theta = \langle\psi_0|a\rangle = \frac{1}{\sqrt{N}}$$

since $\theta \approx \sin\theta$ for small $\theta \Rightarrow \theta \approx \frac{1}{\sqrt{N}}$

need to rotate by angle $\frac{\pi}{2} - \theta \approx \frac{\pi}{2}$

each iteration → 2θ

$T \longmapsto S \rightarrow 2\theta T \approx \frac{\pi}{2} \rightarrow T \approx \frac{\pi}{4\theta} = \frac{\pi}{4}\sqrt{N}$

$\sqrt{N} = 2^{n/2}$

QUADRATIC SPEED UP