Grover's algorithm

Unstructured search problem: X set, $S \subseteq X$ subset of objects that satisfy a certain property $P(x)$.

Let $N = |X|$. Classical approach: $O(N)$; Grover: $O(\sqrt{N})$ (probabilistic) and it is optimal.

We can assume $N = 2^n$. Let $m = |S|$ (known in advance).

Input-output space is $\mathcal{H}^{\otimes n}$ and we use one ancilla qubit.

Associate binary string $\in \{0,1\}^n$ with each $x \in X$.

Each $x \in X$ "is" a basis state $|x\rangle \in \mathcal{H}^{\otimes n}$ and conversely.

We need an oracle, i.e. a boolean function $g : \{0,1\}^n \to \{0,1\}$, $g(x) = 1 \iff x \in S$. Let $S^\perp = X \setminus S$.

Oracle gate: $U_g : \mathcal{H}^{\otimes n} \otimes \mathcal{H} \to \mathcal{H}^{\otimes n} \otimes \mathcal{H}$.
$|x\rangle \otimes |y\rangle \mapsto |x\rangle \otimes |y \oplus g(x)\rangle$

Ancilla qubit is initialized to $\frac{|0\rangle - |1\rangle}{\sqrt{2}}$ $(= H|1\rangle)$.

If $|x\rangle$ is a basis state in $\mathcal{H}^{\otimes n}$, then $U_g\left(|x\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) = (-1)^{g(x)} |x\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}$.

I/O register is initialized to $H^{\otimes n} |0\rangle^n$.

$m = 1$: let $S = \{w\}$. $|\psi_0\rangle = \frac{1}{2^{n/2}} \sum_{x \in \{0,1\}^n} |x\rangle$ initial state of I/O register.

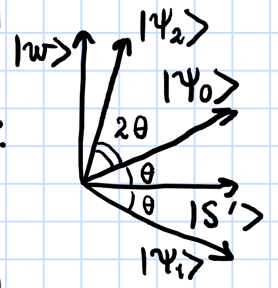
If I measure now, I obtain w with probability $\frac{1}{2^n}$.

Perform amplitude amplification (increase amplitude of $|w\rangle$).

Consider plane spanned by $|w\rangle$ and $|\psi_0\rangle$.

Let $|S'\rangle$ be in this plane orthogonal to $|w\rangle$.

$|\psi_0\rangle = \cos\theta |S'\rangle + \sin\theta |w\rangle$ where



$\theta = \arcsin(1/2^{n/2}) \in [0, \pi/2]$. Apply the oracle: $|\psi_1\rangle = U_g |\psi_0\rangle = \cos\theta |S'\rangle - \sin\theta |w\rangle$. We apply reflection w.r.t. $|\psi_0\rangle$, i.e. $U_{\psi_0} = 2|\psi_0\rangle\langle\psi_0| - \mathbb{1}$. $|\psi_2\rangle = U_{\psi_0}|\psi_1\rangle$. Now the amplitude of $|w\rangle$ in $|\psi_2\rangle$ is larger. $U_{\psi_0} U_g$: diffusion operator.

General case: define states $|\psi_0\rangle = \frac{1}{2^{n/2}} \sum_{x \in \{0,1\}^n} |x\rangle$,
$|\psi_S\rangle = \frac{1}{\sqrt{m}} \sum_{x \in S} |x\rangle$, $|\psi_{S^\perp}\rangle = \frac{1}{\sqrt{N-m}} \sum_{x \in S^\perp} |x\rangle$.

Projections: $P_S = \sum_{x \in S} |x\rangle\langle x|$, $P_{S^\perp} = \sum_{x \in S^\perp} |x\rangle\langle x|$.

acting on the whole space (with ancilla)

$$\hat{U}_g |\psi\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} = \sum_x (-1)^{g(x)} \alpha_x |x\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} =$$

$|\psi\rangle = \sum_{x \in \{0,1\}^n} \alpha_x |x\rangle$

$$= (R_{S^\perp} \otimes \mathbb{1}) |\psi\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}, \quad R_{S^\perp} = 2P_{S^\perp} - \mathbb{1}^{\otimes n}$$ reflection w.r.t. $S^\perp$.

Diffusion operator is $R_{\psi_0} = 2|\psi_0\rangle\langle\psi_0| - \mathbb{1}^{\otimes n}$.

Start with state $|\psi_0\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}$, $|\psi_0\rangle = \frac{1}{\sqrt{N}} \sum_x |x\rangle$.

Grover operator: $\hat{G} = (R_{\psi_0} \otimes \mathbb{1}) \hat{U}_g$.

$|\psi_0\rangle = \sqrt{\frac{N-m}{N}} |\psi_{S^\perp}\rangle + \sqrt{\frac{m}{N}} |\psi_S\rangle = \cos\theta_0 |\psi_{S^\perp}\rangle + \sin\theta_0 |\psi_S\rangle$,

$\theta_0 = \arcsin\sqrt{\frac{m}{N}}$.

Prop.: let $|\hat{\psi}_j\rangle = \hat{G}^j |\psi_0\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}$. Then $|\hat{\psi}_j\rangle = |\psi_j\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}$,
$|\psi_j\rangle = \cos\theta_j |\psi_{S^\perp}\rangle + \sin\theta_j |\psi_S\rangle$, $\theta_j = (2j+1)\theta_0$.

Proof: induction on j. $\square$

Measure I/O register in state $|\psi_j\rangle$: $P(S) = \sin^2\theta_j$.

Lemma: let $j_N = \left\lfloor \frac{\pi}{4 \arcsin\sqrt{m/N}} \right\rfloor$. If we perform j_N iterations of $\hat{G}$ and measure I/O register, we obtain a solution with probability $P(S) \geq 1 - \frac{m}{N}$.

Proof: easy trigonometry. $\square$

$j_N = O(\sqrt{N/m})$.

Remark: because of $R_{\psi_0} = H^{\otimes n} R_{|0\rangle} H^{\otimes n}$, the "complexity" number of gates is $O(\sqrt{N} \log N)$.