Grover's Search Algorithm

Raj Kumar Maity

September 29, 2017

Search: Classical Approach

Problem Statement: Given $N(=2^n)$ elements forming set $X = \{x_1, x_2, \ldots x_N\}$ and given a boolean function $f : X \rightarrow \{0, 1\}$ the goal is to find an element x^* in X such that $f(x^*) = 1$

- If structured (sorted) then do a binary search in logarithmic time.
- unstructured for example searching in a database:
  - Deterministic: Worst case: $N - 1 = 2^n - 1$ queries
  - Randomized: Say we have an oracle O_f. If we input i it returns $f(i)$ in constant time. Still need $\Theta(N)$ queries or running time.

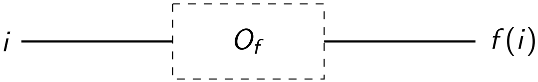


Figure: Oracle

- Caveat: the randomize algorithm gets correct answer with high probability. Say the probability of correctness is greater than $2/3$. Then run multiple time to get better bound.
- Pr[failure after m times]$< (1/3)^m$
- The upper and the lower bound is tight .
- Can we do better ?
- Quantum Setting .Grover's Algorithm. $O(\sqrt{N})$ queries.

Quantum Setting:

Assumption:

- There is only one element x^* such that $f(x^*) = 1$.
  Can be extended to relax the uniqueness assumption.
- The number of data in the set is power of 2. If not ; make it.
  Put some garbage values.
- Each data is labeled with a string of boolean variable of length n.
  The boolean function is $f : \{0,1\}^n \rightarrow \{0,1\}$

Grover's Algorithm

1. Initial state $|0\rangle^{\otimes n}$
2. Apply Hadamard transform to all the qubit to get uniform superposition.

$$H^{\otimes n}|0\rangle^{\otimes n} = \frac{1}{\sqrt{N}}\sum_{i=1}^{N}|x\rangle = \psi$$

3. Apply Grover's Iteration $O(\sqrt{N})$ times
   - Quantum Oracle :$|x\rangle \rightarrow (-1)^{f(x)}|x\rangle$
   - Grover's Diffusion Operator $[2|\psi\rangle\langle\psi| - I]$
4. measure the register.

Quantum Oracle

- A black box. It modifies the configuration without collapsing to a classical state.
- $|x\rangle \rightarrow (-1)^{f(x)} |x\rangle$

$$(-1)^{f(x)} |x\rangle = \begin{cases} -|x\rangle & \text{if } f(x) = 1 \\ |x\rangle & \text{if } f(x) = 0 \end{cases}$$

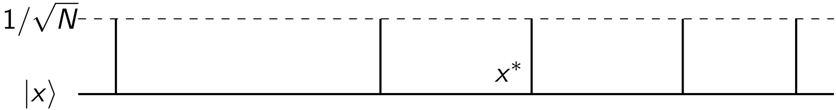
- The black box changes the phase by π
- Amplitude negates but probability remains same.
- The state is now $-\frac{1}{\sqrt{N}} |x^*\rangle + \sum_{x \in \{0,1\}^n x \neq x^*} \frac{1}{\sqrt{N}} |x\rangle$

Diffusion Operator

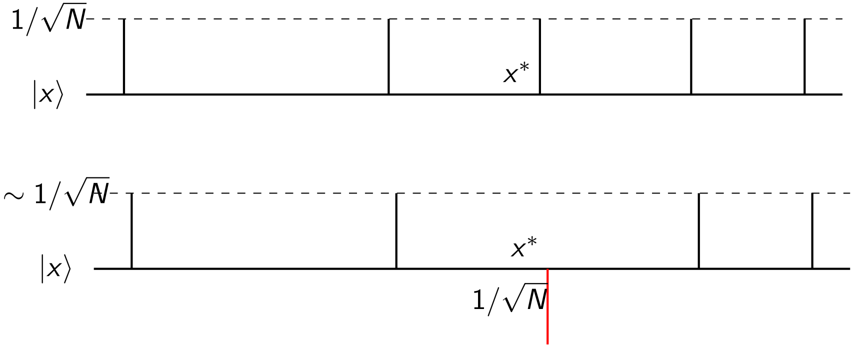
- We want to increase the amplitude of x^* absolutely.
- Diffusion Operator :inversion about the average.
- Say α_x is the amplitude of x and $\mu = \frac{1}{N}\sum \alpha_x$

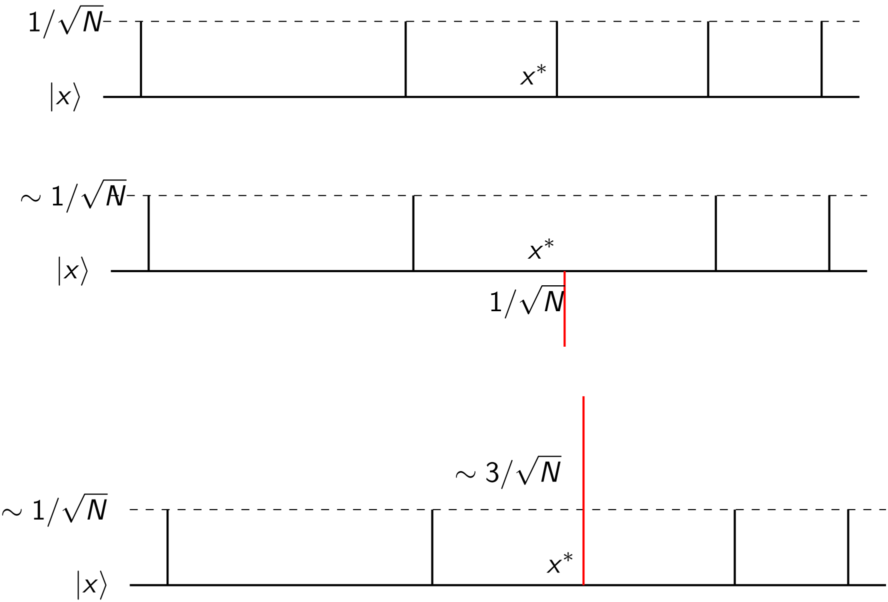
$$\sum \alpha_x \left|x\right\rangle \rightarrow \sum (2\mu - \alpha_x) \left|x\right\rangle$$

- Before diffusion operator $\mu = \frac{1}{N}(-\frac{1}{\sqrt{N}} + \frac{N-1}{\sqrt{N}}) \simeq \frac{1}{\sqrt{N}}$
- So the amplitude of x^* is $\sim \frac{3}{\sqrt{N}}$ after Diffusion transformation.



$1/\sqrt{N}$
$|x\rangle$
x^*


$1/\sqrt{N}$
$|x\rangle$
x^*
$\sim 1/\sqrt{N}$
$|x\rangle$
x^*
$1/\sqrt{N}$


$1/\sqrt{N}$
$|x\rangle$
x^*
$\sim 1/\sqrt{N}$
$|x\rangle$
x^*
$1/\sqrt{N}$
$\sim 3/\sqrt{N}$
$\sim 1/\sqrt{N}$
x^*
$|x\rangle$

Analysis

- Say α^t is the amplitude of x^* after $t-$th iteration and β^t for others.
- Obviously $\alpha^0 = \beta^0 = \frac{1}{\sqrt{N}}$
- **Proposition 1 :** Suppose $\alpha^t \leq 1/2$ and $N \geq 4$. Then $\alpha^{(t+1)} \geq \alpha^t + \frac{1}{\sqrt{N}}$
- **Proposition 2 :** For any $t, \alpha^{(t+1)} \leq \alpha^t + \frac{2}{\sqrt{N}}$
- if we run the algorithm $\sqrt{N}/8$ times for $N \geq 16$ from Proposition 2 we get $\alpha^t \leq 1/2$ -condition we need for Proposition 1.
- Now we can apply this to proposition 1 : $\alpha^{(\sqrt{N}/8)} \geq \frac{\sqrt{N}}{8}\frac{1}{\sqrt{N}} = \frac{1}{8} > .1$
- Probability of measuring $x^* = (.1)^2 = .01$
- Pr[all of the output not x^* in m times]$< (.99)^m < \frac{1}{3}$ for $m = 110$

Grover's Diffusion Gate:

- Invent a gate Z_0 defined as

$$Z_0 |x\rangle = \begin{cases} |x\rangle & \text{if } |x\rangle = |0^n\rangle \\ -|x\rangle & \text{otherwise} \end{cases}$$

- In the unitary form $Z_0 = 2|0^n\rangle\langle 0^n| - I$
- $Z_0 |0^n\rangle = (2|0^n\rangle\langle 0^n| - I)|0^n\rangle = |0^n\rangle$
  $Z_0 |x\rangle = (2|0^n\rangle\langle 0^n| - I)|x\rangle = -|x\rangle$
- Diffusion Operator $D = H^{\otimes n} Z_0 H^{\otimes n} = 2|+^n\rangle\langle +^n| - I$
- For any input $|\psi\rangle = \sum_{x\in\{0,1\}^n} \alpha_x |x\rangle$; $D|\psi\rangle = \sum_{x\in\{0,1\}^n} (2\mu - \alpha_x)|x\rangle$
- So with Z_0 and only $O(\log(N))$ of Hadamard gates we can implement this.So the gate complexity is $O(\sqrt{N}\log(N))$

- $D = 2\left|+^n\right\rangle\left\langle+^n\right| - I$
- $\left\langle+^n\right| = (\frac{\langle 0|+\langle 1|}{\sqrt{2}})^{\otimes n} = \sum_{x\in\{0,1\}^n} \frac{1}{\sqrt{N}}\left|x\right\rangle$
- $\left\langle+^n|\psi\right\rangle = \sum_{x\in\{0,1\}^n} \frac{\alpha_x}{\sqrt{N}}\left\langle x|x\right\rangle = \mu\sqrt{N}$

$$
\begin{aligned}
D\left|\psi\right\rangle &= 2\left|+^n\right\rangle\left\langle+^n|\psi\right\rangle - \left|\psi\right\rangle = 2(\sum_{x\in\{0,1\}^n} \frac{1}{\sqrt{N}}\left|x\right\rangle)\mu\sqrt{N} - \left|\psi\right\rangle \\
&= 2(\sum_{x\in\{0,1\}^n} \mu\left|x\right\rangle) - \sum_{x\in\{0,1\}^n} \alpha_x\left|x\right\rangle \\
&= (\sum_{x\in\{0,1\}^n} (2\mu - \alpha_x)\left|x\right\rangle)
\end{aligned}
$$

Summary

- Compared to the classical approach which needs $\Theta(N)$ queries , Grover's algorithm can search in $O(\sqrt{N})$.
- The gate complexity is $O(\sqrt{N} \log N)$
- Can be extended to the case where you want to find one out of many entries that meets the desired criterion.

Thank You