

GROVER SEARCH

Plan:

- ①. What is the search problem and what is its formulation in terms of a Boolean function / circuit?
- ②. Quantum Mechanics axioms
 - (a) State vector
 - (b) Unitary operators
 - (i) Introduce the $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$ operation and ask what it is reminiscent of?
 - (ii) Discuss the example for $N=4$ (or $n=2$)
 - (c) Measurements
- ③. How can we convert a Boolean function to a Unitary operation: "Quantumification"?
- ④. What is the idea behind formulating the search as a Quantum problem? Ideally, what do we require to solve it?
- ⑤. Graphically explain the idea behind Grover's algorithm. What do we need to achieve this?

[1]: "Quantum Computation and Quantum Information" by Michael Nielsen & Isaac

[2]: Lectures 9a, 9b, 9c of Ryan O'Donnell (CS Theory toolkit) on YouTube. ^{Chuang.}

[3]: Grover's Algorithm, Lesson 08, Qiskit's channel on YouTube. (John Watrous).

[4]: "A fast quantum mechanical algorithm for database search" by Lov Grover, 1996.

Axioms of Quantum mechanics: [1], chapter 2.

①. Quantum Mechanics is about describing the configuration of particles: state space

- What is the state space? for N particles, there are 2^N configurations
- [QM]: we also consider their interference.

→ data vector of coefficients: $|v\rangle := \begin{pmatrix} v(0 \dots 0) \\ v(0 \dots 1) \\ \vdots \\ v(1 \dots 1) \end{pmatrix} \left. \vphantom{\begin{pmatrix} v(0 \dots 0) \\ v(0 \dots 1) \\ \vdots \\ v(1 \dots 1) \end{pmatrix}} \right\} 2^N \text{ coefficients.}$

Eg.: $\begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix} \propto \underbrace{0.8|0\rangle + 0.6i|1\rangle}_{|v\rangle}$

The probability of any configuration is: $|v(\vec{x})|^2$.

②. Measurement: If we "observe" the system, we will obtain one of the configurations and the state "collapses": $P(\vec{x}) = |v(\vec{x})|^2$.

Note: If we want to measure the system $|v\rangle$, we find $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$ with Probability 0.64 and $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ with prob. 0.36.

- If we want to measure the system and find x^* , we must ensure that $|v(x^*)|^2$ is the largest.

③. Operations on quantum states:

• $\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \xrightarrow{U} \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix} = Ux$ such that total probability does not change!

$\langle v|v \rangle = \langle x|x \rangle \Rightarrow U^\dagger U = \mathbb{1}$

- This is a reversible transformation: $U^{-1} = U^\dagger \equiv \text{unitary}$.

Ex: $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad H|0\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

$$H|1\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}$$

$$\begin{pmatrix} f(00) \\ f(01) \\ f(10) \\ f(11) \end{pmatrix} \xrightarrow{H_2 \otimes H_2} \begin{pmatrix} \hat{f}(\{\emptyset\}) \\ \hat{f}(\{1\}) \\ \hat{f}(\{2\}) \\ \hat{f}(\{3\}) \end{pmatrix} \rightarrow \text{Fourier coefficients, and } \hat{f}(\{x\}) = \mathbb{E}_x f(x) = f(00) + f(01) + \dots + f(11)$$

• How can we map a Boolean function to a Quantum operation?

$$\begin{array}{ll} 000 \longrightarrow c(0,0,0)=0 \\ 001 \longrightarrow c(0,0,1)=1 \\ 010 \longrightarrow c(0,1,0)=1 \\ 100 \longrightarrow c(0,1,1)=0 \\ 011 \longrightarrow c(1,0,1)=0 \\ 101 \longrightarrow c(1,0,1)=0 \\ 110 \longrightarrow c(1,1,0)=0 \\ 111 \longrightarrow c(1,1,1)=1 \end{array}$$

we want our Quantum operation to take

$$\begin{pmatrix} 000 \\ 001 \\ \vdots \\ 111 \end{pmatrix} \xrightarrow{U} \begin{pmatrix} \phi_1(0,0,0) \\ \phi_2(0,0,1) \\ \vdots \\ \phi_{2^n}(1,1,1) \end{pmatrix}$$

where $\phi = 1$ if $c(\vec{x}) = 0$
 $= -1$ if $c(\vec{x}) = 1$.

The Quantum gate flips the $\vec{x}$ where the circuit outputs 1, with a -1 phase.

$$U = \begin{pmatrix} (-1)^{c(0,0,0)} & & & 0 \\ & \ddots & & \\ 0 & & & (-1)^{c(1,1,1)} \end{pmatrix}$$

Exercise: Is this unitary?
 Hint: what is the inverse?

Ex: What is the Quantification of the "OR" gate?

Grover Search chapter 6.

• we have all the ingredients we need.

• Recall: Input a Boolean function / circuit $C(x) \in \{0, 1\}$, such that $\exists x^*$ such that $C(x^*) = 1$ and $C(x) = 0 \forall x \in \{0, 1\}^n$ where $x \neq x^*$.

Hint: we want to arrive at a state such that:

$$|\psi\rangle = \begin{pmatrix} f(0 \dots 0) \\ \vdots \\ f(x^*) \\ \vdots \\ f(1 \dots 1) \end{pmatrix} \text{ such that } |f(x^*)|^2 \text{ is high, e.g., } \geq 0.01.$$

Grover's Algorithm:

① Prepare the quantum states of all possible (solution) configurations:

$$\begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} f(0 \dots 0) \\ \vdots \\ f(x^*) \\ \vdots \\ f(1 \dots 1) \end{pmatrix}$$

and apply $H^{\otimes n} = \underbrace{H_2 \otimes H_2 \otimes \dots \otimes H_2}_{n\text{-times}}$

and we find: $\frac{1}{\sqrt{N}} \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix} \equiv \text{equal superposition of all possible configurations.}$

②. Apply the "Quantumification" of C : O_C . It negates the amplitude of the states at x^* : $\frac{1}{\sqrt{N}} \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix} \rightarrow \frac{1}{\sqrt{N}} \begin{pmatrix} 1 \\ \vdots \\ -1 \\ \vdots \\ 1 \end{pmatrix} \rightarrow \text{corresponding to } x^*.$

Ex: what if we measure, what is the probability of finding x^* ?

③. Crucial step: Grover: [4]

(a) Apply $H_N = \underbrace{H_2 \otimes H_2 \otimes \dots \otimes H_2}_{n\text{-times}}$

$$\begin{pmatrix} f(0\dots 0) \\ f(0\dots 1) \\ \vdots \\ -f(x^*) \\ \vdots \\ f(1\dots 1) \end{pmatrix} \xrightarrow{H_N} \begin{pmatrix} \hat{f}(\phi) \\ \hat{f}(\{1\}) \\ \vdots \\ \hat{f}(\{n\}) \end{pmatrix}$$

where (expressing $f(x)$ as a multilinear polynomial).
 $f(x) = \sum_{S \text{ (subset)}} \hat{f}(S) \prod_{i \in S} x_i$

Ex: what is $\hat{f}(\phi)$? $\hat{f}(\phi) = f(0\dots 0) + f(0\dots 1) + \dots + f(1\dots 1) \equiv \underbrace{\mathbb{E}_x f(x)}_{\mu}$

(b) Apply the Quantification of the OR function:

$$\begin{pmatrix} \hat{f}(\phi) \\ \hat{f}(\{1\}) \\ \vdots \\ \hat{f}(\{n\}) \end{pmatrix} \mapsto \begin{pmatrix} \hat{f}(\phi) \\ -\hat{f}(\{1\}) \\ \vdots \\ -\hat{f}(\{n\}) \end{pmatrix}$$

Note:
 $f(x) = \sum_{S \in [n]} \hat{f}(S) \prod_{i \in S} x_i$

$$\xrightarrow{\text{OR}} \hat{f}(\phi) - \hat{f}(\{1\}) x_1 - \hat{f}(\{1\}) x_2 - \dots - \hat{f}(\{n\}) x_1 \dots x_n$$

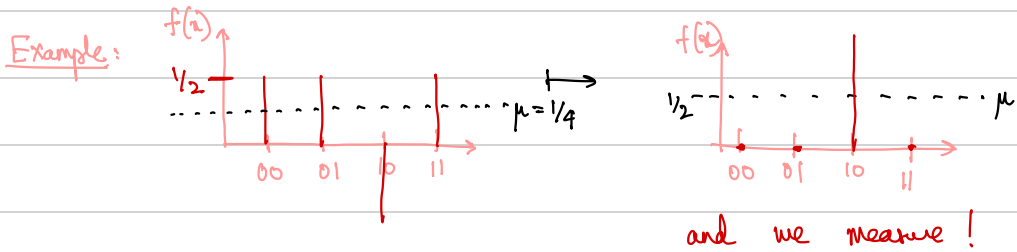
$$= \mu - \hat{f}(\{1\}) x_1 - \dots - \hat{f}(\{n\}) x_1 \dots x_n$$

$$\text{So: } f(x) \mapsto \mu - (\hat{f}(x) - \mu)$$

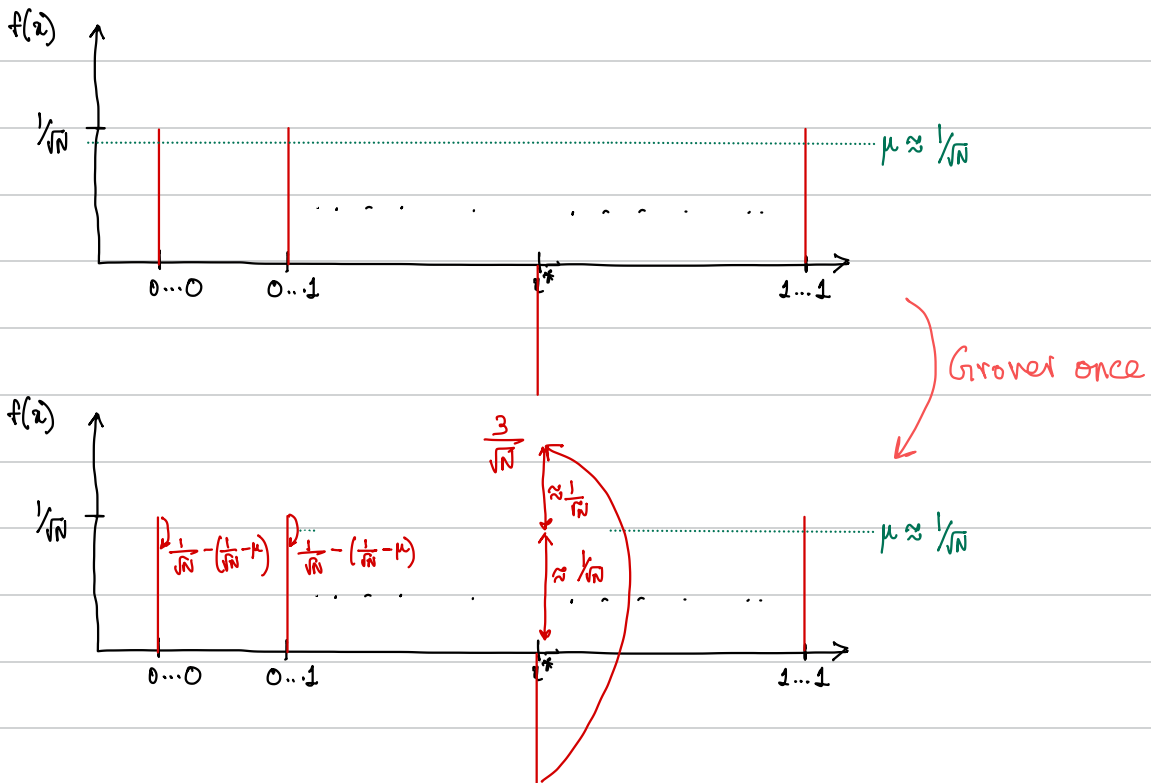
(c) Applying the inverse fourier transformation:

$$f(x) \mapsto \mu - (f(x) - \mu)$$

Overall effect: f 's values are flipped (reflected across their average).



Ex: the general case



we can repeat this until $\frac{k}{\sqrt{N}} \approx 0.01$. (or any constant, large enough).

For this, we want $k = \mathcal{O}(\sqrt{N})$.