COL863: Quantum Computation and Information

Ragesh Jaiswal, CSE, IIT Delhi

Quantum Search Algorithms

Search problem

Let $N = 2^n$ and let $f : \{0, ..., N-1\} \rightarrow \{0, 1\}$ be a function that has $1 \leq M \leq N$ solutions. That is, there are M values for which f evaluates to 1. Find one of the solutions.

- Question: What is the running time for the classical solution?

Search problem

Let $N = 2^n$ and let $f : \{0, ..., N-1\} \rightarrow \{0, 1\}$ be a function that has $1 \leq M \leq N$ solutions. That is, there are M values for which f evaluates to 1. Find one of the solutions.

- Question: What is the running time for the classical solution? $O(N)$

Search problem

Let $N = 2^n$ and let $f : \{0, ..., N-1\} \rightarrow \{0, 1\}$ be a function that has $1 \leq M \leq N$ solutions. That is, there are M values for which f evaluates to 1. Find one of the solutions.

- Let $\mathcal{O}$ be a quantum oracle with the following behaviour:

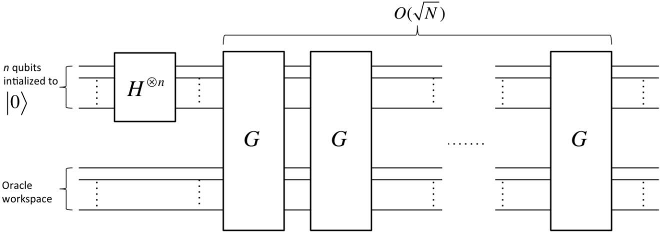
$$|x\rangle\,|q\rangle \xrightarrow{\mathcal{O}} |x\rangle\,|q \oplus f(x)\rangle .$$

- Claim 1: $|x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \xrightarrow{\mathcal{O}} (-1)^{f(x)}\,|x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$
- We will always use the state $|-\rangle$ as the second register in the discussion. So, we may as well describe the behaviour of the oracle $\mathcal{O}$ in short as:

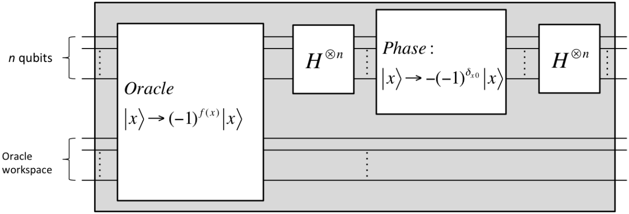
$$|x\rangle \xrightarrow{\mathcal{O}} (-1)^{f(x)}\,|x\rangle .$$

- Claim 2: There is a quantum algorithm that applies the search oracle $\mathcal{O}$, $O(\sqrt{\frac{N}{M}})$ times in order to obtain a solution.

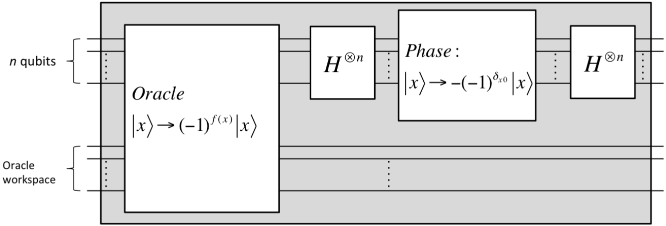
- Here is the schematic circuit for quantum search:



- Where G, called the Grover operator or Grover iteration, is:

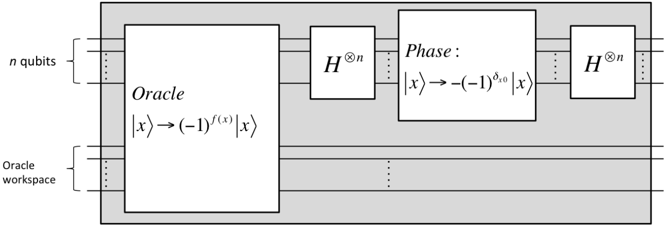


- Where G, called the Grover operator or Grover iteration, is:



- Exercise: Show that the unitary operator corresponding to the phase shift in the Grover iteration is $(2|0\rangle\langle 0| - I)$.

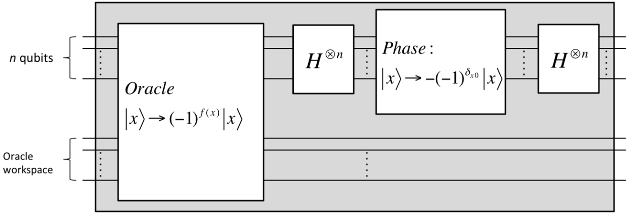
- Where G, called the Grover operator or Grover iteration, is:



- Exercise: Show that the unitary operator corresponding to the phase shift in the Grover iteration is $(2|0\rangle\langle 0| - I)$.
- Let $|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle$.
- Exercise: The operation after the oracle call in the Grover operator, that is $H^{\oplus n}(2|0\rangle\langle 0| - I)H^{\oplus n}$, may be written as $2|\psi\rangle\langle\psi| - I$.

Quantum Search Algorithms
The Grover operator

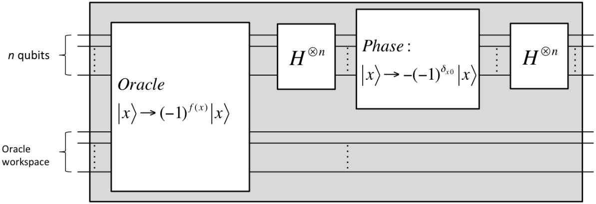
- Where G, called the Grover operator or Grover iteration, is:



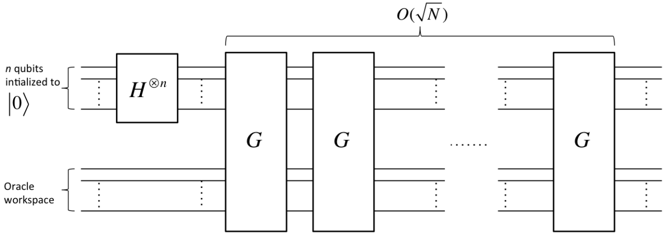
- Exercise: Show that the unitary operator corresponding to the phase shift in the Grover iteration is $(2|0\rangle\langle 0| - I)$.
- Let $|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle$.
- Exercise: The operation after the oracle call in the Grover operator, that is $H^{\oplus n}(2|0\rangle\langle 0| - I)H^{\oplus n}$, may be written as $2|\psi\rangle\langle\psi| - I$.
- The Grover operator G can then be written as $G = (2|\psi\rangle\langle\psi| - I)\mathcal{O}$.

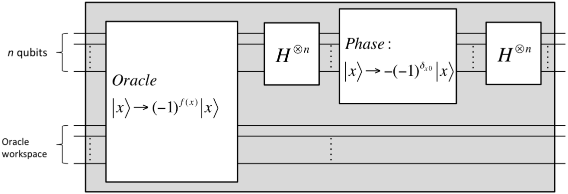
Quantum Search Algorithms
The Grover operator

- Where G, called the Grover operator or Grover iteration, is:



- Exercise: Show that the unitary operator corresponding to the phase shift in the Grover iteration is $(2|0\rangle\langle 0| - I)$.
- Let $|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle$.
- Exercise: The operation after the oracle call in the Grover operator, that is $H^{\oplus n}(2|0\rangle\langle 0| - I)H^{\oplus n}$, may be written as $2|\psi\rangle\langle\psi| - I$.
- The Grover operator G can then be written as $G = (2|\psi\rangle\langle\psi| - I)\mathcal{O}$.
- Exercise: Show that the operation $(2|\psi\rangle\langle\psi| - I)$ applied to a general state $\sum_k \alpha_k |k\rangle$ gives $\sum_k (-\alpha_k + 2\langle\alpha\rangle)|k\rangle$.





- Question: Intuitively, what is going on in this circuit? How does this circuit help in pulling out a solution? Why $O(\sqrt{N})$ repetitions?

- Question: Intuitively, what is going on in this circuit? How does this circuit help in pulling out a solution? Why $O(\sqrt{N})$ repetitions?
- Let

$$
\begin{aligned}
|\alpha\rangle &= \frac{1}{\sqrt{N-M}} \sum_{x \text{ s.t. } f(x)=0} |x\rangle, \\
|\beta\rangle &= \frac{1}{\sqrt{M}} \sum_{x \text{ s.t. } f(x)=1} |x\rangle.
\end{aligned}
$$

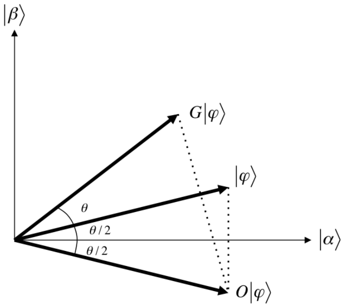
- Question: Intuitively, what is going on in this circuit? How does this circuit help in pulling out a solution? Why $O(\sqrt{N})$ repetitions?
- Let

$$|\alpha\rangle = \frac{1}{\sqrt{N-M}} \sum_{x \text{ s.t. } f(x)=0} |x\rangle ,$$

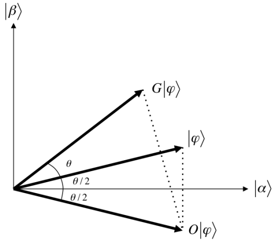
$$|\beta\rangle = \frac{1}{\sqrt{M}} \sum_{x \text{ s.t. } f(x)=1} |x\rangle .$$

- Observation: $|\psi\rangle = \sqrt{\frac{N-M}{N}} |\alpha\rangle + \sqrt{\frac{M}{N}} |\beta\rangle$.
- Consider the plane defined by the vectors $|\alpha\rangle$ and $|\beta\rangle$.
- Claim 1: The effect of $\mathcal{O}$ on a vector on the plane is reflection about the vector $|\alpha\rangle$.
- Claim 2 The effect of $(2 |\psi\rangle \langle\psi| - I)$ on a vector on the plane is reflection about the vector $|\psi\rangle$.

- Question: Intuitively, what is going on in this circuit? How does this circuit help in pulling out a solution? Why $O(\sqrt{N})$ repetitions?
- Let $|\alpha\rangle = \frac{1}{\sqrt{N-M}} \sum_{x \text{ s.t. } f(x)=0} |x\rangle$, and $|\beta\rangle = \frac{1}{\sqrt{M}} \sum_{x \text{ s.t. } f(x)=1} |x\rangle$.
- Observation: $|\psi\rangle = \sqrt{\frac{N-M}{N}} |\alpha\rangle + \sqrt{\frac{M}{N}} |\beta\rangle$.
- Consider the plane defined by the vectors $|\alpha\rangle$ and $|\beta\rangle$.
- Claim 1: The effect of $\mathcal{O}$ on a vector on the plane is reflection about the vector $|\alpha\rangle$.
- Claim 2 The effect of $(2|\psi\rangle\langle\psi| - I)$ on a vector on the plane is reflection about the vector $|\psi\rangle$.

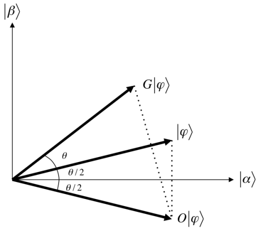


- Let $|\alpha\rangle = \frac{1}{\sqrt{N-M}} \sum_{x \text{ s.t. } f(x)=0} |x\rangle$, and $|\beta\rangle = \frac{1}{\sqrt{M}} \sum_{x \text{ s.t. } f(x)=1} |x\rangle$.
- Observation: $|\psi\rangle = \sqrt{\frac{N-M}{N}} |\alpha\rangle + \sqrt{\frac{M}{N}} |\beta\rangle$.
- Consider the plane defined by the vectors $|\alpha\rangle$ and $|\beta\rangle$.
- Claim 1: The effect of $\mathcal{O}$ on a vector on the plane is reflection about the vector $|\alpha\rangle$.
- Claim 2 The effect of $(2|\psi\rangle\langle\psi| - I)$ on a vector on the plane is reflection about the vector $|\psi\rangle$.

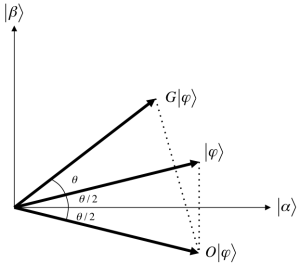


- Let $\cos\frac{\theta}{2} = \sqrt{\frac{N-M}{N}}$. So, $|\psi\rangle = \cos\frac{\theta}{2}|\alpha\rangle + \sin\frac{\theta}{2}|\beta\rangle$ and $G|\psi\rangle = \cos\frac{3\theta}{2}|\alpha\rangle + \sin\frac{3\theta}{2}|\beta\rangle$

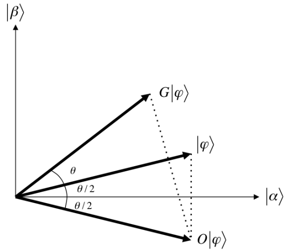
- Let $|\alpha\rangle = \frac{1}{\sqrt{N-M}} \sum_{x \text{ s.t. } f(x)=0} |x\rangle$, and $|\beta\rangle = \frac{1}{\sqrt{M}} \sum_{x \text{ s.t. } f(x)=1} |x\rangle$.
- Observation: $|\psi\rangle = \sqrt{\frac{N-M}{N}} |\alpha\rangle + \sqrt{\frac{M}{N}} |\beta\rangle$.
- Consider the plane defined by the vectors $|\alpha\rangle$ and $|\beta\rangle$.
- Claim 1: The effect of $\mathcal{O}$ on a vector on the plane is reflection about the vector $|\alpha\rangle$.
- Claim 2 The effect of $(2|\psi\rangle\langle\psi| - I)$ on a vector on the plane is reflection about the vector $|\psi\rangle$.



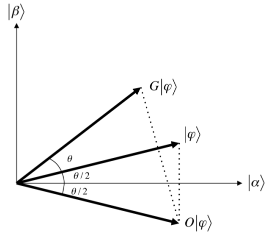
- Let $\cos\frac{\theta}{2} = \sqrt{\frac{N-M}{N}}$. So, $|\psi\rangle = \cos\frac{\theta}{2}|\alpha\rangle + \sin\frac{\theta}{2}|\beta\rangle$ and $G|\psi\rangle = \cos\frac{3\theta}{2}|\alpha\rangle + \sin\frac{3\theta}{2}|\beta\rangle$
- Exercise: Show that $G^k|\psi\rangle = \cos\frac{(2k+1)\theta}{2}|\alpha\rangle + \sin\frac{(2k+1)\theta}{2}|\beta\rangle$.



- Let $\cos\frac{\theta}{2} = \sqrt{\frac{N-M}{N}}$. So, $|\psi\rangle = \cos\frac{\theta}{2}|\alpha\rangle + \sin\frac{\theta}{2}|\beta\rangle$ and $G|\psi\rangle = \cos\frac{3\theta}{2}|\alpha\rangle + \sin\frac{3\theta}{2}|\beta\rangle$
- Exercise: Show that $G^k|\psi\rangle = \cos\frac{(2k+1)\theta}{2}|\alpha\rangle + \sin\frac{(2k+1)\theta}{2}|\beta\rangle$.
- Question: How many Grover iterations are required to sample a solution with good probability?



- Let $\cos\frac{\theta}{2} = \sqrt{\frac{N-M}{N}}$. So, $|\psi\rangle = \cos\frac{\theta}{2}|\alpha\rangle + \sin\frac{\theta}{2}|\beta\rangle$ and $G|\psi\rangle = \cos\frac{3\theta}{2}|\alpha\rangle + \sin\frac{3\theta}{2}|\beta\rangle$
- Exercise: Show that $G^k|\psi\rangle = \cos\frac{(2k+1)\theta}{2}|\alpha\rangle + \sin\frac{(2k+1)\theta}{2}|\beta\rangle$.
- Question: How many Grover iterations are required to sample a solution with good probability?
- Let $R = CI\left(\frac{\arccos\sqrt{M/N}}{\theta}\right)$, where $CI(.)$ denotes closest integer.
- Exercise: Show that if R Grover iterations are executed, then the probability of measuring a solution is at least $1/2$.



- Let $\cos\frac{\theta}{2} = \sqrt{\frac{N-M}{N}}$. So, $|\psi\rangle = \cos\frac{\theta}{2}|\alpha\rangle + \sin\frac{\theta}{2}|\beta\rangle$ and $G|\psi\rangle = \cos\frac{3\theta}{2}|\alpha\rangle + \sin\frac{3\theta}{2}|\beta\rangle$
- Exercise: Show that $G^k|\psi\rangle = \cos\frac{(2k+1)\theta}{2}|\alpha\rangle + \sin\frac{(2k+1)\theta}{2}|\beta\rangle$.
- Question: How many Grover iterations are required to sample a solution with good probability?
- Let $R = CI\left(\frac{\arccos\sqrt{M/N}}{\theta}\right)$, where $CI(.)$ denotes closest integer.
- Exercise: Show that if R Grover iterations are executed, then the probability of measuring a solution is at least $1/2$.
- Exercise: If $M \leq N/2$, then $R \leq \lceil \frac{\pi}{4}\sqrt{\frac{N}{M}} \rceil$.

End