COL863: Quantum Computation and Information

Ragesh Jaiswal, CSE, IIT Delhi

Quantum Computation: Discrete logarithm

Discrete logarithm problem

Given positive integers a, b, N such that $b = a^s \pmod N$ for some unknown s, find s.

- Question: What is the running time of the naive classical algorithm?

Discrete logarithm problem

Given positive integers a, b, N such that $b = a^s \pmod N$ for some unknown s, find s.

- Question: What is the running time of the naive classical algorithm? $\Omega(N)$

Discrete logarithm problem

Given positive integers a, b, N such that $b = a^s \pmod N$ for some unknown s, find s.

- Consider a bi-variate function $f(x_1, x_2) = a^{sx_1 + x_2} \pmod N$.
- Claim 1: f is a periodic function with period $(\ell, -\ell s)$ for any integer ℓ.
    - So it may be possible for us to pull out s using some of the previous ideas developed.
- Question: How does discovering s for the above function help us in solving the discrete logarithm problem?

Discrete logarithm problem

Given positive integers a, b, N such that $b = a^s \ (mod\ N)$ for some unknown s, find s.

- Consider a bi-variate function $f(x_1, x_2) = a^{sx_1 + x_2} \ (mod\ N)$.
- Claim 1: f is a periodic function with period $(\ell, -\ell s)$ for any integer ℓ.
    - So it may be possible for us to pull out s using some of the previous ideas developed.
- Question: How does discovering s for the above function help us in solving the discrete logarithm problem?
    - Main idea: $f(x_1, x_2) \equiv b^{x_1} a^{x_2} \ (mod\ N)$.

Bi-variate period

Let f be a function such that $f(x_1, x_2) = a^{sx_1+x_2} \ (mod\ N)$ and let r be the order of a modulo N. Let U be a unitary operator that performs the transformation: $U|x_1\rangle|x_2\rangle|y\rangle \rightarrow |x_1\rangle|x_2\rangle|y \oplus f(x_1, x_2)\rangle$. Find s.

Discrete logarithm

1. $|0\rangle|0\rangle|0\rangle$ (Initial state)
2. $\rightarrow \frac{1}{2^t}\sum_{x_1=0}^{2^t-1}\sum_{x_2=0}^{2^t-1}|x_1\rangle|x_2\rangle|0\rangle$ (Create superposition)
3. $\rightarrow \frac{1}{2^t}\sum_{x_1=0}^{2^t-1}\sum_{x_2=0}^{2^t-1}|x_1\rangle|x_2\rangle|f(x_1, x_2)\rangle$ (Apply U)
   $= \frac{1}{\sqrt{r}2^t}\sum_{\ell_2=0}^{r-1}\sum_{x_1=0}^{2^t-1}\sum_{x_2=0}^{2^t-1} e^{(2\pi i)\frac{s\ell_2 x_1+\ell_2 x_2}{r}}|x_1\rangle|x_2\rangle\left|\hat{f}(s\ell_2, \ell_2)\right\rangle$
   $= \frac{1}{\sqrt{r}2^t}\sum_{\ell_2=0}^{r-1}\left[\sum_{x_1=0}^{2^t-1} e^{(2\pi i)\frac{s\ell_2 x_1}{r}}|x_1\rangle\right]\left[\sum_{x_2=0}^{2^t-1} e^{(2\pi i)\frac{\ell_2 x_2}{r}}|x_2\rangle\right]\left|\hat{f}(s\ell_2, \ell_2)\right\rangle$
4. $\rightarrow \frac{1}{\sqrt{r}}\sum_{\ell_2=0}^{r-1}\left|\widetilde{\left(\frac{s\ell_2}{r}\right)}\right\rangle\left|\widetilde{\left(\frac{\ell_2}{r}\right)}\right\rangle\left|\hat{f}(s\ell_2, \ell_2)\right\rangle$ (Apply invFT to register 1,2)
5. $\rightarrow \left(\widetilde{\left(\frac{s\ell_2}{r}\right)}, \widetilde{\left(\frac{\ell_2}{r}\right)}\right)$ (Measure register 1, 2)
6. $\rightarrow s$ (Use continued fractions algorithm)

- Claim: Let $\left|\hat{f}(\ell_1, \ell_2)\right\rangle \equiv \frac{1}{\sqrt{r}}\sum_{j=0}^{r-1} e^{-(2\pi i)\frac{\ell_2 j}{r}}|f(0, j)\rangle$. Then

$$|f(x_1, x_2)\rangle = \frac{1}{\sqrt{r}}\sum_{\ell_2=0}^{r-1} e^{(2\pi i)\frac{s\ell_2 x_1+\ell_2 x_2}{r}}\left|\hat{f}(s\ell_2, \ell_2)\right\rangle.$$

Quantum Computation: Hidden Subgroup Problem (HSG)

- The algorithms for order-finding, factoring, discrete logarithm, period-finding follow the same general pattern.
- It would be useful if we could extract the main essence and define a general problem that can be solved using these ideas.

Hidden Subgroup Problem (HSG)

Given a group G and a function $f : G \rightarrow X$ with the promise that there is a subgroup $H \subseteq G$ such that f assigns a unique value to each coset of H. Find H.

- The algorithms for order-finding, factoring, discrete logarithm, period-finding follow the same general pattern.
- It would be useful if we could extract the main essence and define a general problem that can be solved using these ideas.

Hidden Subgroup Problem (HSG)

Given a group G and a function $f : G \rightarrow X$ with the promise that there is a subgroup $H \subseteq G$ such that f assigns a unique value to each coset of H. Find H.

- Question: Can order-finding, period finding etc. be seen as just a special case of the HSG problem?

Hidden Subgroup Problem (HSG)

Given a group G and a function $f : G \rightarrow X$ with the promise that there is a subgroup $H \subseteq G$ such that f assigns a unique value to each coset of H. Find H.

- Question: Can order-finding, period finding etc. be seen as just a special case of the HSG problem?

Name	**G**	**X**	**H**	**f**
Simon	$(\{0,1\}^n, \oplus)$	$\{0,1\}^n$	$\{0, s\}$	$f(x \oplus s) = f(x)$
Order finding	$(\mathbb{Z}_N, +)$	a^j $j \in \mathbb{Z}_r$ $a^r = 1$	$\{0, r, 2r, ...\}$ $r \in G$	$f(x) = a^x$ $f(x + r) = f(x)$

Hidden Subgroup Problem (HSG)

Given a group G and a function $f : G \rightarrow X$ with the promise that there is a subgroup $H \subseteq G$ such that f assigns a unique value to each coset of H. Find H.

- Question: How does a Quantum computer solve the hidden subgroup problem?

Quantum algorithm for HSG

- Create uniform superposition $\frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle |f(g)\rangle$.
- Measure the second register to create a uniform superposition over a coset of H: $\frac{1}{\sqrt{H}} \sum_{h \in H} |h + k\rangle$.
- Apply Fourier transform
- Measure and extract generating set of the subgroup H.

Hidden Subgroup Problem (HSG)

Given a group G and a function $f : G \rightarrow X$ with the promise that there is a subgroup $H \subseteq G$ such that f assigns a unique value to each coset of H. Find H.

- Question: How does a Quantum computer solve the hidden subgroup problem?

Quantum algorithm for HSG

- Create uniform superposition $\frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle |f(g)\rangle$.
- Measure the second register to create a uniform superposition over a coset of H: $\frac{1}{\sqrt{H}} \sum_{h \in H} |h + k\rangle$.
- Apply Fourier transform
- Measure and extract generating set of the subgroup H.

- Question: How does Fourier transform help?
  - Shift-invariance property: If $\sum_{h \in H} \alpha_h |h\rangle \rightarrow \sum_{g \in G} \tilde{\alpha}_g |g\rangle$, then $\sum_{h \in H} \alpha_h |h + k\rangle \rightarrow \sum_{g \in G} e^{(2\pi i) \frac{gk}{|G|}} \tilde{\alpha}_g |g\rangle$.

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:

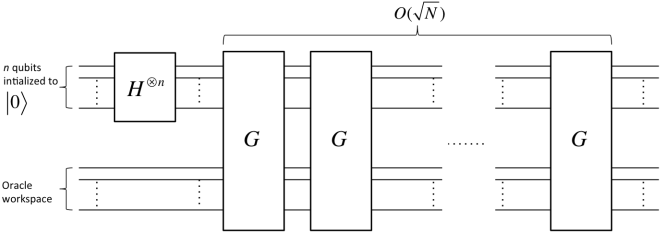
$$|x\rangle |q\rangle \xrightarrow{\mathcal{O}} |x\rangle |q \oplus f(x)\rangle .$$

- 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:

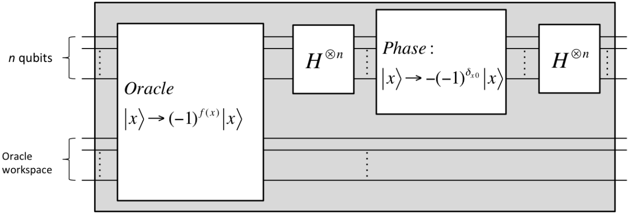
$$|x\rangle \xrightarrow{\mathcal{O}} (-1)^{f(x)} |x\rangle .$$

- 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.

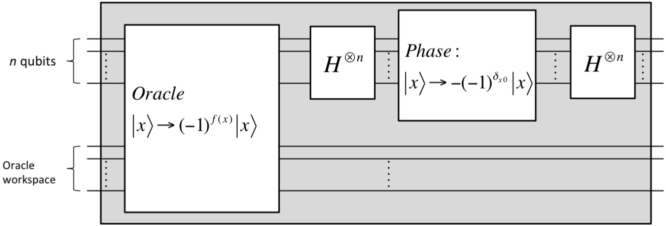
- Here is the schematic circuit for quantum search:



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

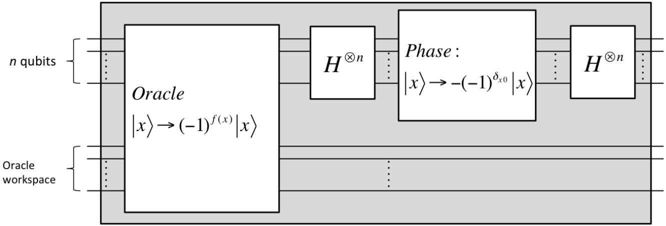


- Where G, called the Grover operator or Grover iteration, is:



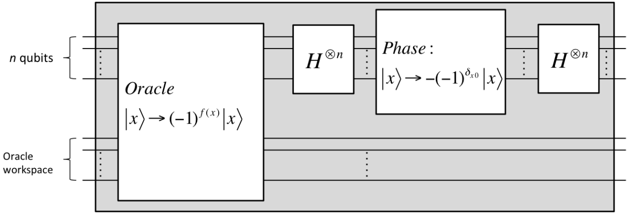
- Exercise: Show that the unitary operator corresponding to the phase shift in the Grover iteration is $(2|0\rangle\langle 0| - I)$.

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



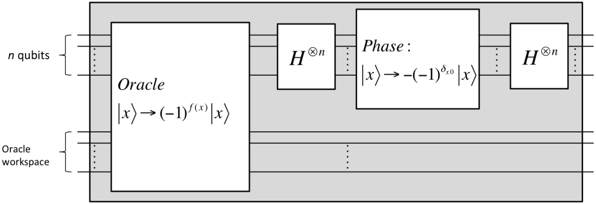
- Exercise: Show that the unitary operator corresponding to the phase shift in the Grover iteration is $(2|0\rangle\langle 0| - I)$.
- Let $|\psi\rangle = \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle$.
- Exercise: The operation after the oracle call in the Grover operator, that is $H^{\oplus n}(2|0\rangle\langle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

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

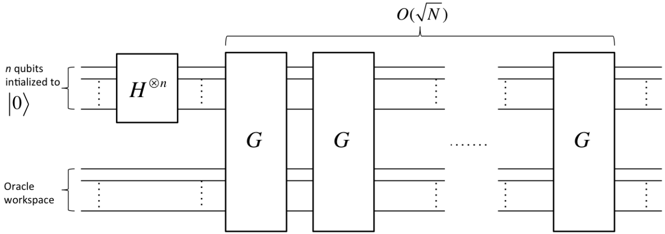


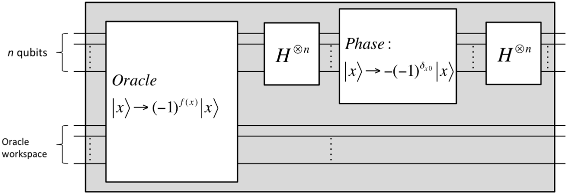
- Exercise: Show that the unitary operator corresponding to the phase shift in the Grover iteration is $(2|0\rangle\langle 0| - I)$.
- Let $|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle$.
- Exercise: The operation after the oracle call in the Grover operator, that is $H^{\oplus n}(2|0\rangle\langle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

- 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

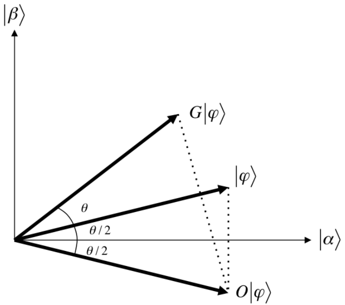
$$
\begin{aligned}
|\alpha\rangle &= \frac{1}{\sqrt{N-M}} \sum_{x \text{ s.t. } f(x)=0} |x\rangle, \\
|\beta\rangle &= \frac{1}{\sqrt{M}} \sum_{x \text{ s.t. } f(x)=1} |x\rangle.
\end{aligned}
$$

- 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

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

- 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 $|\psi\rangle$.



End