COL863: Quantum Computation and Information

Ragesh Jaiswal, CSE, IIT Delhi

Quantum Computation: Factoring

Factoring

Given a positive composite integer N, output a non-trivial factor of N.

- We will solve the factoring problem by reduction to the order finding problem.
- Theorem 1: Suppose N is an L bit composite number, and x is a non-trivial solution to the equation $x^2 = 1 \ (mod \ N)$ in the range $1 \leq x \leq N$, that is, neither $x = 1 \ (mod \ N)$ nor $x = -1 \ (mod \ N)$. Then at least one of $gcd(x-1, N)$ and $gcd(x+1, N)$ is a non-trivial factor of N that can be computed using $O(L^3)$ operations.
- Theorem 2: Suppose $N = p_1^{\alpha_1} ... p_m^{\alpha_m}$ is the prime factorisation of an odd composite positive integer. Let x be an integer chosen uniformly at random, subject to the requirement that $1 \leq x \leq N-1$ and x is co-prime to N. Let r be the order of x modulo N. Then

$$\mathbf{Pr}[r \text{ is even and } x^{r/2} \neq -1 \ (mod \ N)] \geq 1 - \frac{1}{2^m}.$$

Factoring

Given a positive composite integer N, output a non-trivial factor of N.

Quantum Factoring Algorithm

1. If N is even, return 2 as a factor.
2. Determine if $N = a^b$ for integers $a, b \geq 2$ and if so, return a.
3. Randomly choose $1 \leq x \leq N - 1$. If $gcd(x, N) > 1$, then return $gcd(x, N)$.
4. Use the Quantum order-finding algorithm to find the order r of x modulo N.
5. If r is even and $x^{r/2} \neq -1 \ (mod \ N)$, then compute $p = gcd(x^{r/2} - 1, N)$ and $q = gcd(x^{r/2} + 1, N)$. If either p or q is a non-trivial factor of N, then return that factor else return "Failure".

Quantum Computation: Period finding

Period finding problem

Given a boolean function f such that $f(x) = f(x + r)$ for some unknown $0 < r < 2^L$, where $x, r = \{0, 1, 2, ...\}$ and given a unitary transform U_f that performs the transformation $U|x\rangle|y\rangle \rightarrow |x\rangle|y \oplus f(x)\rangle$, determine the least such $r > 0$.

Period-finding algorithm

1. $|0\rangle|0\rangle$ (Initial state)
2. $\rightarrow \frac{1}{2^{t/2}} \sum_{x=0}^{2^t-1} |x\rangle|0\rangle$ (Create superposition)
3. $\rightarrow \frac{1}{2^{t/2}} \sum_{x=0}^{2^t-1} |x\rangle|f(x)\rangle$ (Apply U)
   $\approx \frac{1}{\sqrt{r}2^{t/2}} \sum_{\ell=0}^{r-1} \sum_{x=0}^{2^t-1} e^{(2\pi i)\frac{\ell x}{r}} |x\rangle \left|\hat{f}(\ell)\right\rangle$
4. $\rightarrow \frac{1}{\sqrt{r}} \sum_{\ell=0}^{r-1} \left|\widetilde{(\ell/r)}\right\rangle \left|\hat{f}(\ell)\right\rangle$ (Apply inverse FT to 1^{st} register)
5. $\rightarrow \widetilde{(\ell/r)}$ (Measure first register)
6. $\rightarrow r$ (Use continued fractions algorithm)

Period finding problem

Given a boolean function f such that $f(x) = f(x+r)$ for some unknown $0 < r < 2^L$, where $x, r = \{0, 1, 2, ...\}$ and given a unitary transform U_f that performs the transformation $U|x\rangle|y\rangle \rightarrow |x\rangle|y \oplus f(x)\rangle$, determine the least such $r > 0$.

Period-finding algorithm

1. $|0\rangle|0\rangle$ (Initial state)
2. $\rightarrow \frac{1}{2^{t/2}} \sum_{x=0}^{2^t-1} |x\rangle|0\rangle$ (Create superposition)
3. $\rightarrow \frac{1}{2^{t/2}} \sum_{x=0}^{2^t-1} |x\rangle|f(x)\rangle$ (Apply U)
   $= \frac{1}{\sqrt{r}2^{t/2}} \sum_{\ell=0}^{r-1} \sum_{x=0}^{2^t-1} e^{(2\pi i)\frac{\ell x}{r}} |x\rangle \left|\hat{f}(\ell)\right\rangle$
4. $\rightarrow \frac{1}{\sqrt{r}} \sum_{\ell=0}^{r-1} \left|\widetilde{(\ell/r)}\right\rangle \left|\hat{f}(\ell)\right\rangle$ (Apply inverse FT to 1^{st} register)
5. $\rightarrow \widetilde{(\ell/r)}$ (Measure first register)
6. $\rightarrow r$ (Use continued fractions algorithm)

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

- The basic ideas involved in order finding and period finding seems to be the same.
- Question: *Can we generalise the core ideas and design a canonical algorithm for a very general problem so that order finding, factoring, period finding etc. are just special cases of this general problem?*
  - Yes. The general problem is called the Hidden Subgroup Problem.
- Before we see the hidden subgroup problem, we will see another special case: Discrete Logarithm.

Quantum Computation: Discrete logarithm

Discrete logarithm problem

Given positive integers a, b, N such that $b = a^s \ (mod \ N)$ 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 $b = a^s \pmod{N}$ 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?
  - Main idea: $f(x_1, x_2) \equiv b^{x_1} a^{x_2} \pmod{N}$.

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:

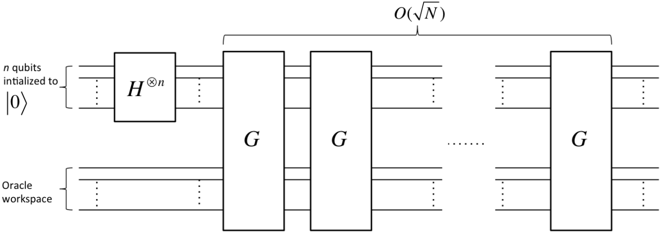
$$|x\rangle |q\rangle \xrightarrow{\mathcal{O}} |x\rangle |q \oplus f(x)\rangle .$$

- 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:

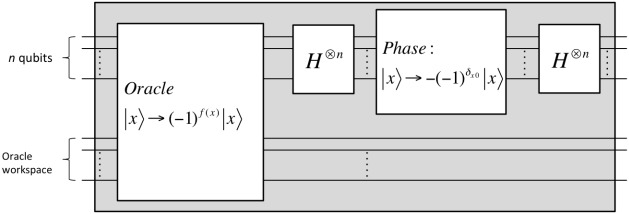
$$|x\rangle \xrightarrow{\mathcal{O}} (-1)^{f(x)} |x\rangle .$$

- 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.

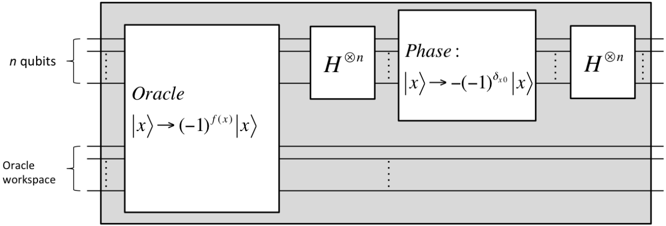
- Here is the schematic circuit for quantum search:



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

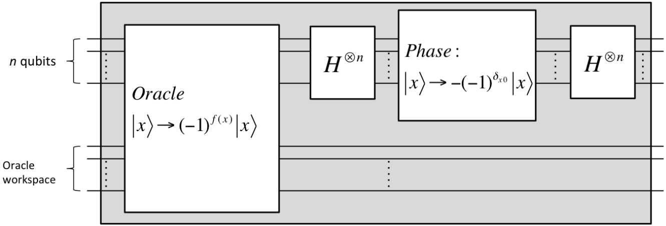


- Where G, called the Grover operator or Grover iteration, is:



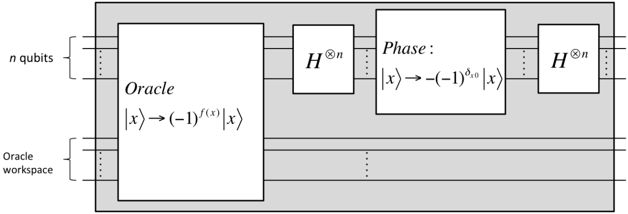
- Exercise: Show that the unitary operator corresponding to the phase shift in the Grover iteration is $(2|0\rangle\langle 0| - I)$.

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



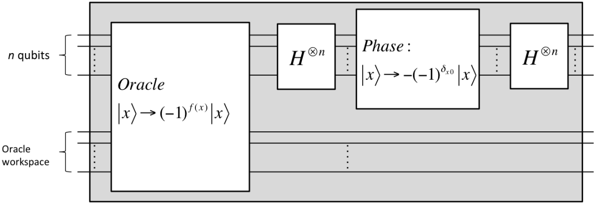
- Exercise: Show that the unitary operator corresponding to the phase shift in the Grover iteration is $(2|0\rangle\langle 0| - I)$.
- Let $|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle$.
- Exercise: The operation after the oracle call in the Grover operator, that is $H^{\oplus n}(2|0\rangle\langle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

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

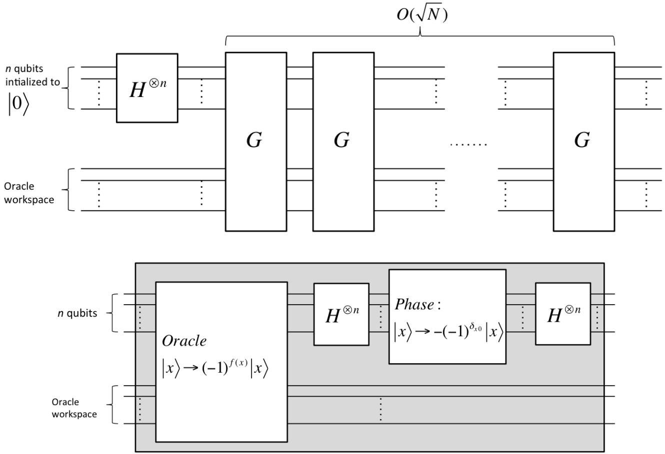


- Exercise: Show that the unitary operator corresponding to the phase shift in the Grover iteration is $(2|0\rangle\langle 0| - I)$.
- Let $|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle$.
- Exercise: The operation after the oracle call in the Grover operator, that is $H^{\oplus n}(2|0\rangle\langle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

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

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

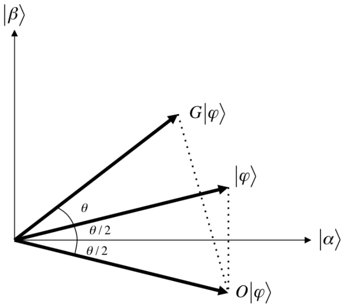
- Question: Intuitively, what is going on in this circuit? How does this circuit help in pulling out a solution? Why $O(\sqrt{N})$ repetitions?
- Let

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

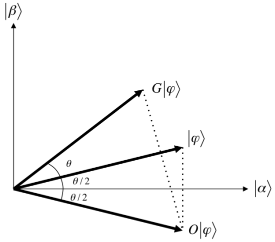
$$|\beta\rangle = \frac{1}{\sqrt{M}} \sum_{x \text{ s.t. } f(x)=1} |x\rangle .$$

- 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 $|\psi\rangle$.

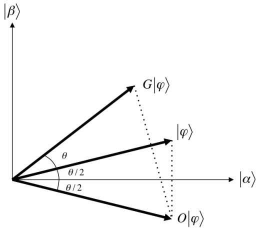


- Let $|\alpha\rangle = \frac{1}{\sqrt{N-M}} \sum_{x \text{ s.t. } f(x)=0} |x\rangle$, and $|\beta\rangle = \frac{1}{\sqrt{M}} \sum_{x \text{ s.t. } f(x)=1} |x\rangle$.
- Observation: $|\psi\rangle = \sqrt{\frac{N-M}{N}} |\alpha\rangle + \sqrt{\frac{M}{N}} |\beta\rangle$.
- Consider the plane defined 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 $|\psi\rangle$.

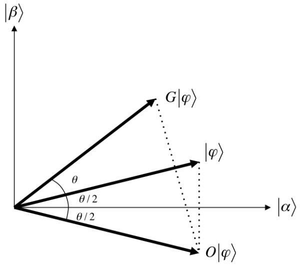


- Let $\cos\frac{\theta}{2} = \sqrt{\frac{N-M}{N}}$. So, $|\psi\rangle = \cos\frac{\theta}{2}|\alpha\rangle + \sin\frac{\theta}{2}|\beta\rangle$ and $G|\psi\rangle = \cos\frac{3\theta}{2}|\alpha\rangle + \sin\frac{3\theta}{2}|\beta\rangle$

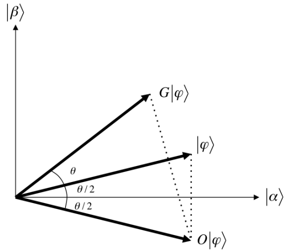
- Let $|\alpha\rangle = \frac{1}{\sqrt{N-M}} \sum_{x \text{ s.t. } f(x)=0} |x\rangle$, and $|\beta\rangle = \frac{1}{\sqrt{M}} \sum_{x \text{ s.t. } f(x)=1} |x\rangle$.
- Observation: $|\psi\rangle = \sqrt{\frac{N-M}{N}} |\alpha\rangle + \sqrt{\frac{M}{N}} |\beta\rangle$.
- Consider the plane defined 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 $|\psi\rangle$.



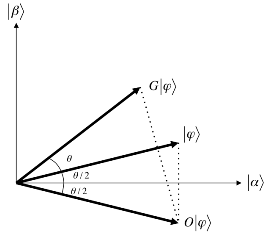
- Let $\cos\frac{\theta}{2} = \sqrt{\frac{N-M}{N}}$. So, $|\psi\rangle = \cos\frac{\theta}{2}|\alpha\rangle + \sin\frac{\theta}{2}|\beta\rangle$ and $G|\psi\rangle = \cos\frac{3\theta}{2}|\alpha\rangle + \sin\frac{3\theta}{2}|\beta\rangle$
- Exercise: Show that $G^k|\psi\rangle = \cos\frac{(2k+1)\theta}{2}|\alpha\rangle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



- 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