COL7160 : Quantum Computing

Lecture 19: Grover's Search Algorithm and Amplitude Amplification

Instructor: Rajendra Kumar **Scribe:** Mridul Gupta

1 Definitions

Definition 1 (Search Problem)**.** Given a function $f : \{0,1\}^n \to \{0,1\}$, find a x such that $f(x) = 1$

Definition 2. Lets denote the following notation for convinience

- Domain U : which in this case is $\{0,1\}^n$
- Total number of elements : $N = |U| = 2^n$
- Set of tagged elements : $A = \{x \in U \mid f(x) = 1\}$
- Number of tagged elements : $t = |A|$
- Complement of A : $B = A^c = \{x \in U \mid f(x) = 0\}$

Classicaly, if you pick an element at random from U, the probability of it being tagged is $|A| / |U| = t/N$, so the expected number of elements we'd need to sample would be N/t

2 Quantum Setting

Definition 3 (Function Oracle)**.** Access to the function f is provided as an oracle Z_f defined by its action on the basis states

$$Z_f |x\rangle = (-1)^{f(x)} |x\rangle \tag{1}$$

Definition 4 (Uniform Superposition State)**.** The uniform superposition state on a set S is $|S\rangle$ such that

$$|S\rangle = \frac{1}{\sqrt{|S|}} \sum_{x \in S} |x\rangle \tag{2}$$

Lemma 5 (Uniform State)**.** *The uniform superposition state over the domain $U = \{0,1\}^n$ is generated by applying n Hadamard gates in parallel to $|0^n\rangle$*

$$|U\rangle = H^{\otimes n} |0^n\rangle \tag{3}$$

Proof. The action of a single Hadamard gate on the basis state $|0\rangle$ is given by $H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. Applying n such gates in parallel to $|0^n\rangle = |0\rangle \otimes \cdots \otimes |0\rangle$ yields:

$$H^{\otimes n} |0^n\rangle = \bigotimes_{i=1}^{n} H|0\rangle = \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle = |U\rangle \tag{4}$$

□

Definition 6 (OR Function)**.**

$$\mathrm{OR}(x) = \begin{cases} 0 & \text{if } x = 0 \\ 1 & \text{otherwise} \end{cases} \tag{5}$$

Lemma 7 (OR Oracle)**.** *The oracle for OR, acting as defined in 3 can be written as*

$$Z_{OR} = 2|0\rangle\langle 0| - I \tag{6}$$

Proof. By Definition 3, the oracle Z_{OR} can be expanded in the computational basis as:

$$Z_{\text{OR}} = \sum_{x \in \{0,1\}^n} (-1)^{\text{OR}(x)} |x\rangle \langle x| \tag{7}$$

Splitting the sum into the $x = 0$ and $x \neq 0$ terms, and using the definition of the OR function:

$$Z_{\text{OR}} = (-1)^0 |0\rangle \langle 0| + \sum_{x \neq 0} (-1)^1 |x\rangle \langle x| = |0\rangle \langle 0| - \sum_{x \neq 0} |x\rangle \langle x| \tag{8}$$

Using the completeness relation $I = |0\rangle \langle 0| + \sum_{x \neq 0} |x\rangle \langle x|$, we can substitute $\sum_{x \neq 0} |x\rangle \langle x| = I - |0\rangle \langle 0|$:

$$Z_{\text{OR}} = |0\rangle \langle 0| - (I - |0\rangle \langle 0|) = 2 |0\rangle \langle 0| - I \tag{9}$$

□

Lemma 8 (Reflections)**.** *Any operator of the form $Z = 2 |\psi\rangle \langle \psi| - I$ is a reflection about $|\psi\rangle$*

Proof. Using the resolution of identity $I = |\psi\rangle \langle \psi| + \sum_i |\psi_i^\perp\rangle \langle \psi_i^\perp|$, where $\{|\psi_i^\perp\rangle\}$ is an orthonormal basis for the subspace orthogonal to $|\psi\rangle$:

$$Z = 2 |\psi\rangle \langle \psi| - \left(|\psi\rangle \langle \psi| + \sum_i |\psi_i^\perp\rangle \langle \psi_i^\perp| \right) = |\psi\rangle \langle \psi| - \sum_i |\psi_i^\perp\rangle \langle \psi_i^\perp| \tag{10}$$

This operator preserves the component along $|\psi\rangle$ and negates all components in the orthogonal subspace, defining a reflection about $|\psi\rangle$. □

Corollary 9 (Reflection about U)**.** *The operator $H^{\otimes n} (2 |0\rangle \langle 0| - I) H^{\otimes n}$ is a reflection about the uniform state U.*

Proof. Let $Z = 2 |0\rangle \langle 0| - I$ be the reflection about $|0\rangle$ (as in Lemma 7). Applying the similarity transformation $H^{\otimes n}$ to Z:

$$H^{\otimes n} Z H^{\otimes n} = H^{\otimes n} (2 |0\rangle \langle 0| - I) H^{\otimes n} = 2 \left(H^{\otimes n} |0\rangle \right) \left(\langle 0| H^{\otimes n} \right) - H^{\otimes n} I H^{\otimes n} \tag{11}$$

By Lemma 5, $H^{\otimes n} |0\rangle = |U\rangle$. Since $H^{\otimes n}$ is unitary and self-adjoint ($H = H^\dagger, H^2 = I$), we have:

$$2 |U\rangle \langle U| - I \tag{12}$$

By Lemma 8, this operator is a reflection about $|U\rangle$. □

Proposition 10. *The uniform superposition can be written as a combinantion of the uniform superposition states over A, B as:*

$$|U\rangle = \sqrt{\frac{t}{N}} |A\rangle + \sqrt{\frac{N-t}{N}} |B\rangle \tag{13}$$

Proof. By Definition 4, the uniform superposition state $|U\rangle$ is given by:

$$|U\rangle = \frac{1}{\sqrt{N}} \sum_{x \in U} |x\rangle \tag{14}$$

Splitting the sum into tagged ($x \in A$) and untagged ($x \in B$) elements:

$$|U\rangle = \frac{1}{\sqrt{N}} \left(\sum_{x \in A} |x\rangle + \sum_{x \in B} |x\rangle \right) \tag{15}$$

From Definition 4, we have $\sum_{x \in A} |x\rangle = \sqrt{t} |A\rangle$ and $\sum_{x \in B} |x\rangle = \sqrt{N-t} |B\rangle$. Substituting these:

$$|U\rangle = \frac{1}{\sqrt{N}} \left(\sqrt{t} |A\rangle + \sqrt{N-t} |B\rangle \right) = \sqrt{\frac{t}{N}} |A\rangle + \sqrt{\frac{N-t}{N}} |B\rangle \tag{16}$$

□

3 Grover's Algorithm

Definition 11 (Grover Iterate)**.** The Grover iterate G (also called the Grover operator) is defined as:

$$G = H^{\otimes n}(2\left|0\right\rangle\left\langle 0\right| - I)H^{\otimes n}Z_f \tag{17}$$

where Z_f is the function oracle and $H^{\otimes n}(2\left|0\right\rangle\left\langle 0\right| - I)H^{\otimes n}$ is the reflection about the uniform superposition state $\left|U\right\rangle$ (as shown in Corollary 9).

Grover's algorithm consists of starting with the uniform superposition state $\left|U\right\rangle$ and repeatedly applying the Grover iterate G. Geometrically, each application of G rotates the state vector in the 2D plane spanned by $\left|A\right\rangle$ and $\left|B\right\rangle$ towards the target state $\left|A\right\rangle$.

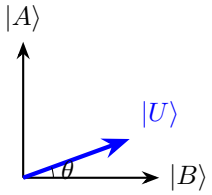

Figure 1: Uniform state $\left|U\right\rangle$

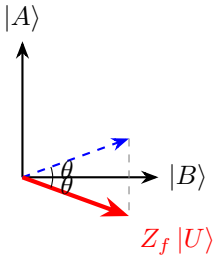

Figure 2: Action of Z_f

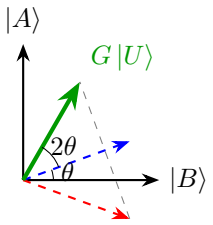

Figure 3: Action of G

Definition 12 (Grover Angle)**.** Define the angle θ such that:

$$\sin\theta = \sqrt{\frac{t}{N}} \quad \text{and} \quad \cos\theta = \sqrt{\frac{N-t}{N}} \tag{18}$$

This allows us to write the uniform superposition state (from Proposition 10) as:

$$\left|U\right\rangle = \sin\theta\left|A\right\rangle + \cos\theta\left|B\right\rangle \tag{19}$$

where θ is the angle between the initial state $\left|U\right\rangle$ and the *bad* state superposition $\left|B\right\rangle$.

Proposition 13 (G as a Rotation)**.** *The Grover iterate $G = (2\left|U\right\rangle\left\langle U\right| - I)Z_f$ is a rotation by 2θ in the plane spanned by $\{\left|A\right\rangle, \left|B\right\rangle\}$.*

Proof. The operator G is the composition of two reflections:

1. Z_f is a reflection about the axis $\left|B\right\rangle$. For any state $\left|\psi\right\rangle = \alpha\left|A\right\rangle + \beta\left|B\right\rangle$, $Z_f\left|\psi\right\rangle = -\alpha\left|A\right\rangle + \beta\left|B\right\rangle$, which negates the component orthogonal to $\left|B\right\rangle$ ($x \in A \implies f(x) = 1 \implies Z_f\left|x\right\rangle = -\left|x\right\rangle$).
2. $2\left|U\right\rangle\left\langle U\right| - I$ is a reflection about the axis $\left|U\right\rangle$ (as shown in Lemma 8).

From geometry, the composition of two reflections about lines intersecting at an angle θ is a rotation by 2θ in the direction from the first reflection axis to the second. Since the angle between $\left|B\right\rangle$ and $\left|U\right\rangle$ is θ, the result is a rotation by 2θ towards $\left|A\right\rangle$. □

Definition 14 (State After k Iterations)**.** Let $\left|\varphi_k\right\rangle$ be the state obtained after k applications of the Grover iterate G starting from the initial uniform superposition $\left|U\right\rangle$:

$$\left|\varphi_k\right\rangle = G^k\left|U\right\rangle \tag{20}$$

From Proposition 13, since G is a rotation by 2θ in the plane $\{\left|A\right\rangle, \left|B\right\rangle\}$ and the starting state $\left|U\right\rangle$ is at an angle θ with the axis $\left|B\right\rangle$, the state after k iterations is:

$$\left|\varphi_k\right\rangle = \sin((2k+1)\theta)\left|A\right\rangle + \cos((2k+1)\theta)\left|B\right\rangle \tag{21}$$

Definition 15 (Optimal Iterations)**.** To maximize the probability of measuring a *good* state $|A\rangle$, we want $(2k+1)\theta \approx \pi/2$. The optimal number of Grover iterations k^* is given by the closest integer:

$$k^* = \left\lfloor \frac{\pi}{4\theta} - \frac{1}{2} \right\rceil \tag{22}$$

For small $\theta \approx \sin\theta = \sqrt{t/N}$, this yields $k^* \approx \frac{\pi}{4}\sqrt{\frac{N}{t}}$.

Proposition 16 (Success Probability)**.** *Using k^* Grover iterations ensures the probability of measuring a good state $x \in A$ is at least $1/2$.*

Proof. If $\sin^2\theta \geq 1/2$, the initial uniform superposition state $|U\rangle$ already has a high probability of yielding a tagged element. In this case, $k^* = 0$, and we succeed with probability $\sin^2\theta \geq 1/2$.
Otherwise, we have $\sin^2\theta < 1/2$. The optimal number of iterations k^* is chosen such that the final angle $(2k^*+1)\theta$ is as close as possible to $\pi/2$. Since k^* is the closest integer to $\frac{\pi}{4\theta} - \frac{1}{2}$, the distance from the target angle is at most θ:

$$\left| k^* - \left(\frac{\pi}{4\theta} - \frac{1}{2} \right) \right| \leq \frac{1}{2} \implies |(2k^*+1)\theta - \pi/2| \leq \theta \tag{23}$$

The probability of failure (measuring a state in B) is given by:

$$P(B) = \cos^2((2k^*+1)\theta) = \sin^2\left(\frac{\pi}{2} - (2k^*+1)\theta\right) \leq \sin^2\theta \tag{24}$$

Since we assumed $\sin^2\theta < 1/2$, the failure probability is bounded by $1/2$, which implies the success probability is $P(A) = 1 - P(B) \geq 1 - \sin^2\theta > 1/2$. □

4 Amplitude Amplification

Definition 17 (Amplitude Amplification Problem)**.** Given a unitary operator A such that:

$$A|0^n\rangle = \sqrt{p}\,|\psi_0\rangle + \sqrt{1-p}\,|\psi_1\rangle \tag{25}$$

where:

- $|\psi_0\rangle$ is the superposition of *good* states: $|\psi_0\rangle = \sum_i \alpha_i |x_i\rangle$, where $\alpha_i \neq 0$ if and only if $f(x_i) = 1$.
- $|\psi_1\rangle$ is the superposition of *bad* states: $|\psi_1\rangle = \sum_i \beta_i |x_i\rangle$, where $\beta_i \neq 0$ if and only if $f(x_i) = 0$.

The task is to amplify the probability of $|\psi_0\rangle$ (initially p) while keeping the relative amplitudes α_i and β_i within each superposition intact.

Remark 18 (Grover Operator in Amplitude Amplification). Given the unitary operator A and its adjoint $A^\dagger$, we can construct the generalized Grover iterate G:

$$G = A\,(2\,|0\rangle\langle 0| - I)\,A^\dagger Z_f \tag{26}$$

where Z_f is the reflection about the *good* state subspace (as defined before). The geometric analysis remains the same, with $\sin^2\theta = p$, allowing us to use Grover's algorithm to amplify the success probability from p to at least $1/2$ (or higher).

4.1 Exact Amplitude Amplification

Proposition 19 (Reaching Success Probability 1)**.** *By introducing an auxiliary qubit and a rotation operator U, it is possible to reach the good state $|\psi_0\rangle$ with probability exactly 1.*

Proof. Introduce an auxiliary qubit and define the rotation operator U:

$$U = \begin{bmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{bmatrix} \tag{27}$$

We define a new preparation operator $A^* = A \otimes U$ acting on $n+1$ qubits. Its action on the state $|0^{n+1}\rangle$ is:

$$A^* |0^{n+1}\rangle = \left(\sqrt{p}\,|\psi_0\rangle + \sqrt{1-p}\,|\psi_1\rangle\right) \otimes (\cos\varphi\,|0\rangle + \sin\varphi\,|1\rangle) \tag{28}$$

Expanding this yields:

$$A^* |0^{n+1}\rangle = \underbrace{\sqrt{p}\cos\varphi\,|\psi_0\rangle\,|0\rangle}_{\text{Good State}} + \underbrace{\left(\sqrt{p}\sin\varphi\,|\psi_0\rangle\,|1\rangle + \sqrt{1-p}\cos\varphi\,|\psi_1\rangle\,|0\rangle + \sqrt{1-p}\sin\varphi\,|\psi_1\rangle\,|1\rangle\right)}_{\text{Bad States}} \tag{29}$$

Define a new oracle $f^*(x, y)$ (where $x \in \{0,1\}^n$ and $y \in \{0,1\}$) such that:

$$f^*(x,y) = \begin{cases} f(x) & \text{if } y = 0 \\ 0 & \text{if } y = 1 \end{cases} \tag{30}$$

Under this oracle, the only tagged states are of the form $|x\rangle\,|0\rangle$ where $f(x) = 1$. The initial success amplitude is $\sin\theta^* = \sqrt{p}\cos\varphi$.
To ensure we reach probability 1, we first choose the number of iterations k^* as:

$$k^* = \left\lceil \frac{\pi}{4\theta} - \frac{1}{2} \right\rceil \tag{31}$$

where $\sin\theta = \sqrt{p}$. This choice of k^* ensures that:

$$2k^* + 1 \geq \frac{\pi}{2\theta} \implies \theta^* = \frac{\pi}{2(2k^*+1)} \leq \theta \tag{32}$$

Since $\theta^* \leq \theta$, we have $\sin\theta^* \leq \sin\theta = \sqrt{p}$. Thus, we can always find a rotation angle φ such that:

$$\sqrt{p}\cos\varphi = \sin\theta^* \implies \cos\varphi = \frac{\sin\theta^*}{\sqrt{p}} \leq 1 \tag{33}$$

With this choice of φ, the state after k^* iterations of the Grover operator G^* (constructed using A^* and f^*) will be:

$$|\varphi_{k^*}\rangle = \sin((2k^*+1)\theta^*)\,|\text{Good}\rangle + \cos((2k^*+1)\theta^*)\,|\text{Bad}\rangle \tag{34}$$

Substituting $(2k^*+1)\theta^* = \pi/2$ yields:

$$|\varphi_{k^*}\rangle = \sin(\pi/2)\,|\text{Good}\rangle + \cos(\pi/2)\,|\text{Bad}\rangle = |\text{Good}\rangle \tag{35}$$

Thus, we reach the target state $|\psi_0\rangle\,|0\rangle$ with probability exactly 1. □