COL7160 : Quantum Computing

Lecture 19: Grover's Search Algorithm and Amplitude Amplification

Instructor: Rajendra Kumar **Scribe:** Rohit Baraik

1 The Search Problem

Definition 1 (Search Problem)**.** Let $N = 2^n$ and let $f : \{0,1\}^n \to \{0,1\}$ be a Boolean function given as a black-box oracle. The **search problem** asks us to find an $x \in \{0,1\}^n$ such that $f(x) = 1$. We call such an x a *marked* or *good* element. Let t denote the total number of marked elements, i.e. $t = |\{x : f(x) = 1\}|$.

Classically, any algorithm requires $\Omega(N/t)$ oracle queries in the worst case. Grover's algorithm solves this with $O(\sqrt{N/t})$ quantum oracle queries.

1.1 Setup and Initial State

We work in the n-qubit Hilbert space $(\mathbf{C}^2)^{\otimes n}$. Starting from $|0^n\rangle$, we apply the n-fold Hadamard transform $H^{\otimes n}$ to get the uniform superposition

$$H^{\otimes n} |0^n\rangle \;=\; \frac{1}{\sqrt{N}} \sum_{x \in \{0,1\}^n} |x\rangle \,.$$

We decompose this state into two orthogonal components. Define

$$|A\rangle \;=\; \frac{1}{\sqrt{t}} \sum_{x\,:\,f(x)=1} |x\rangle \,, \qquad |B\rangle \;=\; \frac{1}{\sqrt{N-t}} \sum_{x\,:\,f(x)=0} |x\rangle \,.$$

Then the uniform superposition can be written as

$$|u\rangle \;=\; \sqrt{\frac{t}{N}}\, |A\rangle + \sqrt{\frac{N-t}{N}}\, |B\rangle \,.$$

Define the angle θ by $\sin\theta = \sqrt{t/N}$, so that

$$|u\rangle \;=\; \sin\theta\, |A\rangle + \cos\theta\, |B\rangle \,.$$

2 Grover's Algorithm

2.1 The Phase Oracle

The phase oracle Z_f acts on basis states as

$$Z_f |x\rangle \;=\; \begin{cases} \;\;|x\rangle & \text{if } f(x) \neq 1, \\ -|x\rangle & \text{if } f(x) = 1. \end{cases}$$

Geometrically, Z_f is a reflection about $|B\rangle$ in the plane spanned by $\{|A\rangle, |B\rangle\}$.

2.2 The Grover Iterate

The **Grover diffusion operator** is

$$\mathcal{W} \;=\; H^{\otimes n}\big(2\,|0^n\rangle\langle 0^n| - I\big)H^{\otimes n} \;=\; 2\,|u\rangle\langle u| - I.$$

It is a reflection about $|u\rangle$ in the same plane. The full **Grover iterate** is $G = \mathcal{W} \circ Z_f$.

2.3 Geometric Analysis: One Grover Iteration

Lemma 2 (Grover Rotation). *One application of $G = \mathcal{W} \circ Z_f$ rotates the state vector by 2θ towards $|A\rangle$ in the $\{|A\rangle, |B\rangle\}$ plane.*

Proof. Write the current state as $|\psi\rangle = \sin\alpha\ |A\rangle + \cos\alpha\ |B\rangle$ for some angle α.

Step 1 — Apply Z_f. The oracle flips the sign of the $|A\rangle$ component:

$$Z_f\,|\psi\rangle \;=\; -\sin\alpha\ |A\rangle + \cos\alpha\ |B\rangle\,.$$

Step 2 — Apply $\mathcal{W} = 2\,|u\rangle\langle u| - I$. Let $|v\rangle = Z_f\,|\psi\rangle$. Since $|u\rangle = \sin\theta\ |A\rangle + \cos\theta\ |B\rangle$,

$$\langle u|v\rangle \;=\; \sin\theta(-\sin\alpha) + \cos\theta\cos\alpha \;=\; \cos(\alpha+\theta).$$

Then

$$\begin{aligned}\mathcal{W}\,|v\rangle &= 2\cos(\alpha+\theta)\ |u\rangle - |v\rangle \\ &= 2\cos(\alpha+\theta)\big(\sin\theta\ |A\rangle + \cos\theta\ |B\rangle\big) - \big(-\sin\alpha\ |A\rangle + \cos\alpha\ |B\rangle\big).\end{aligned}$$

Collecting coefficients and using the sum-to-product identities:

$$\begin{aligned}\text{coefficient of } |A\rangle: &\quad 2\cos(\alpha+\theta)\sin\theta + \sin\alpha \;=\; \sin(\alpha+2\theta),\\ \text{coefficient of } |B\rangle: &\quad 2\cos(\alpha+\theta)\cos\theta - \cos\alpha \;=\; \cos(\alpha+2\theta).\end{aligned}$$

Hence $G\,|\psi\rangle = \sin(\alpha+2\theta)\ |A\rangle + \cos(\alpha+2\theta)\ |B\rangle$, which is a rotation by 2θ towards $|A\rangle$. □

2.4 State After k Iterations

Starting from $|u\rangle$ (angle $\alpha = \theta$) and applying Lemma 2 inductively,

$$G^k\,|u\rangle \;=\; \sin\big((2k+1)\theta\big)\ |A\rangle + \cos\big((2k+1)\theta\big)\ |B\rangle\,.$$

The probability of measuring a marked element after k iterations is $\Pr[\text{success}] = \sin^2((2k+1)\theta)$.

2.5 Optimal Number of Iterations and Error Probability

We want $(2k+1)\theta \approx \pi/2$, giving the optimal iteration count

$$k^* \;\approx\; \frac{\pi}{4\theta} - \frac{1}{2} \;\approx\; \frac{\pi}{4}\sqrt{\frac{N}{t}} \;=\; O\left(\sqrt{\frac{N}{t}}\right).$$

Theorem 3 (Error Bound for Grover's Algorithm). *With $k^* = \lfloor K \rceil$ iterations (nearest integer to K), where $K = \frac{\pi}{4\theta} - \frac{1}{2}$, the error probability satisfies*

$$\Pr[\textit{failure}] \;=\; \cos^2\big((2k^*+1)\theta\big) \;\le\; \frac{1}{2}.$$

Proof. Since $k^* = \lfloor K \rceil$, we have $|k^* - K| \le \frac{1}{2}$, so

$$\left|(2k^*+1)\theta - \frac{\pi}{2}\right| = 2\theta\,|k^* - K| \le \theta.$$

For $t \le N/2$, we have $\theta \le \pi/4$, so $(2k^*+1)\theta \in [\pi/4,\, 3\pi/4]$. On this interval $|\cos z| \le |\sin z|$, which gives $\cos^2((2k^*+1)\theta) \le \sin^2((2k^*+1)\theta)$, and since both sum to 1, the error satisfies $\cos^2((2k^*+1)\theta) \le \frac{1}{2}$. □

2.6 The Full Grover Algorithm

Algorithm 1 Grover's Search Algorithm

Input: Oracle Z_f for $f : \{0,1\}^n \to \{0,1\}$; t = number of marked elements.
Output: x with $f(x) = 1$, with probability $\geq \frac{1}{2}$.
Prepare uniform superposition: $|u\rangle \leftarrow H^{\otimes n} |0^n\rangle$
Set $k^* \leftarrow \left\lfloor \frac{\pi}{4}\sqrt{\frac{N}{t}} \right\rceil$ ▷ nearest integer
for $k = 1$ to k^* **do**
    Apply phase oracle Z_f ▷ Reflect about $|B\rangle$
    Apply diffusion $\mathcal{W} = 2|u\rangle\langle u| - I$ ▷ Reflect about $|u\rangle$
end for
Measure in the computational basis; output x.

Theorem 4 (Grover's Theorem)**.** *Grover's algorithm solves the search problem using $O(\sqrt{N/t})$ oracle queries, with success probability at least $\frac{1}{2}$.*

3 Improving Success Probability When t is Known

Problem 5. Suppose we know the value of t (and hence $\theta = \sin^{-1}\sqrt{t/N}$). How can we improve the success probability of Grover's algorithm to be exactly 1?

When t is known, we know θ exactly. From the analysis above, the ideal (possibly non-integer) number of iterations is

$$K = \frac{\pi}{4\theta} - \frac{1}{2}.$$

If K happens to be an integer, we set $k^* = K$ and obtain success probability $\sin^2((2k^*+1)\theta) = \sin^2(\pi/2) = 1$ exactly.
However, K is generally *not* an integer. Setting $k^* = \lfloor K \rceil$ already gives success probability $\geq \frac{1}{2}$ by Theorem 3, but we want to do better. The fix is to *change the angle* θ — i.e. replace the uniform superposition with a different starting state — so that the condition $(2k^*+1)\theta = \pi/2$ is met exactly for some integer k^*. We will resolve this problem foe the generalized version of search problem: **Amplitude Amplification**.

4 Amplitude Amplification

4.1 Problem Setup

Definition 6 (Amplitude Amplification Setup)**.** Let A be a quantum algorithm acting on n qubits such that

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

where $|\psi_0\rangle$ (the *good* subspace, $f(x) = 1$) and $|\psi_1\rangle$ (the *bad* subspace, $f(x) = 0$) are orthogonal normalised states, and p is the initial success probability of A. Writing

$$|\psi_0\rangle = \sum_x \alpha_x |x\rangle, \qquad |\psi_1\rangle = \sum_x \beta_x |x\rangle,$$

we have $f(x) = 1$ iff $\alpha_x \neq 0$, and $f(x) = 0$ iff $\alpha_x = 0$.

Goal. Boost the probability of measuring a good state from p to near 1, using as few applications of A, A^{-1}, and Z_f as possible.

Step 1. Prepare $A|0^n\rangle$.

Step 2. Apply the Grover iterate, but now with respect to A. However, directly applying Z_f followed by the original Grover diffusion $H^{\otimes n}(2\,|0^n\rangle\,\langle 0^n| - I)H^{\otimes n}$ will *not* work, because the diffusion was designed to reflect about the uniform superposition $H^{\otimes n}\,|0^n\rangle$, not about $A\,|0^n\rangle$. We must instead reflect about $|\psi\rangle = A\,|0^n\rangle$.

Remark 7. Grover's algorithm is the special case $A = H^{\otimes n}$, $|\psi_0\rangle = |A\rangle$, $|\psi_1\rangle = |B\rangle$, and $p = t/N$.

4.2 The Amplitude Amplification Operator

The correct generalisation of the diffusion operator is

$$\mathcal{W}_A \;=\; A\big(2\,|0^n\rangle\langle 0^n| - I\big)A^{-1} \;=\; 2\,|\psi\rangle\langle\psi| - I, \qquad |\psi\rangle = A\,|0^n\rangle\,.$$

Define the **amplitude amplification operator**

$$\mathcal{Q} \;=\; \mathcal{W}_A \circ Z_f \;=\; \big(2\,|\psi\rangle\langle\psi| - I\big)\,Z_f.$$

Let $\varphi = \sin^{-1}\sqrt{p}$, so that $|\psi\rangle = \sin\varphi\;|\psi_0\rangle + \cos\varphi\;|\psi_1\rangle$. By the identical geometric argument as Lemma 2 (with φ in place of θ, $|\psi_0\rangle$ in place of $|A\rangle$, $|\psi_1\rangle$ in place of $|B\rangle$), each application of $\mathcal{Q}$ rotates the state by 2φ towards $|\psi_0\rangle$. After k steps,

$$\mathcal{Q}^k\,|\psi\rangle \;=\; \sin\big((2k+1)\varphi\big)\;|\psi_0\rangle + \cos\big((2k+1)\varphi\big)\;|\psi_1\rangle\,,$$

and the success probability is $\sin^2((2k+1)\varphi)$.

4.3 Algorithm and Complexity

Algorithm 2 Amplitude Amplification

1: **Input:** Algorithm A with $A\,|0^n\rangle = \sqrt{p}\;|\psi_0\rangle + \sqrt{1-p}\;|\psi_1\rangle$; oracle Z_f.
2: **Output:** A good state $|x\rangle$ with $f(x) = 1$, with probability $\geq \frac{1}{2}$.
3: Prepare $|\psi\rangle \leftarrow A\,|0^n\rangle$
4: Set $k^* \leftarrow \left\lfloor \dfrac{\pi}{4\varphi} - \dfrac{1}{2} \right\rceil$, where $\varphi = \sin^{-1}\sqrt{p}$ ▷ nearest integer
5: **for** $k = 1$ to k^* **do**
6: Apply Z_f ▷ Flip sign of good states
7: Apply $\mathcal{W}_A = A(2\,|0^n\rangle\,\langle 0^n| - I)A^{-1}$ ▷ Reflect about $|\psi\rangle$
8: **end for**
9: Measure in the computational basis; output x.

Theorem 8 (Amplitude Amplification)**.** *Amplitude amplification produces a good state (i.e. $f(x) = 1$) with probability at least $\frac{1}{2}$ using $O(1/\sqrt{p})$ applications of A, A^{-1}, and Z_f. When $p = t/N$, this is $O(\sqrt{N/t})$ oracle calls.*

Proof. With $k^* = \lfloor K \rceil$ and $K = \frac{\pi}{4\varphi} - \frac{1}{2}$, we have $|k^* - K| \leq \frac{1}{2}$, so $|(2k^*+1)\varphi - \frac{\pi}{2}| \leq \varphi$. For $p \leq \frac{1}{2}$, this places $(2k^*+1)\varphi \in [\pi/4, 3\pi/4]$, giving $\sin^2((2k^*+1)\varphi) \geq \frac{1}{2}$. The number of iterations is $k^* \leq \frac{\pi}{4\varphi} + \frac{1}{2} = O(1/\varphi) = O(1/\sqrt{p})$. □

4.4 Resolution of Problem 5

We now see how amplitude amplification answers Problem 5. When t is known, $\varphi = \sin^{-1}\sqrt{t/N}$ is known exactly. We compute

$$k^* \;=\; \left\lfloor \frac{\pi}{4\varphi} - \frac{1}{2} \right\rceil.$$

To achieve success probability exactly 1, we need $(2k^*+1)\varphi^* = \pi/2$ for some adjusted angle φ^*. Since k^* is now fixed, we solve for

$$\varphi^* \;=\; \frac{\pi}{2(2k^*+1)}, \qquad \varphi^* \;\le\; \varphi.$$

Constructing a new algorithm A^* with angle φ^*. We extend the state space by one ancilla qubit and define

$$f^*(x_1,\ldots,x_n,x_{n+1}) \;=\; \begin{cases} f(x_1,\ldots,x_n) & \text{if } x_{n+1}=0, \\ 0 & \text{if } x_{n+1}=1. \end{cases}$$

This ensures that marked states of f^* are exactly the marked states of f with the ancilla qubit in state $|0\rangle$. Define the new algorithm A^* acting on $(n+1)$ qubits as

$$A^*\,|0^{n+1}\rangle \;=\; A\,|0^n\rangle \otimes U\,|0\rangle\,,$$

where U is the single-qubit rotation

$$U \;=\; \begin{pmatrix} \cos\varphi^* & -\sin\varphi^* \\ \sin\varphi^* & \cos\varphi^* \end{pmatrix}, \qquad \text{so } U\,|0\rangle = \cos\varphi^*\,|0\rangle + \sin\varphi^*\,|1\rangle\,.$$

Expanding,

$$\begin{aligned} A^*\,|0^{n+1}\rangle &= \left(\sqrt{p}\,|\psi_0\rangle + \sqrt{1-p}\,|\psi_1\rangle\right) \otimes \left(\cos\varphi^*\,|0\rangle + \sin\varphi^*\,|1\rangle\right) \\ &= \sqrt{p}\cos\varphi^*\;|\psi_0\rangle\,|0\rangle + \sqrt{p}\sin\varphi^*\;|\psi_0\rangle\,|1\rangle + \sqrt{1-p}\cos\varphi^*\;|\psi_1\rangle\,|0\rangle + \sqrt{1-p}\sin\varphi^*\;|\psi_1\rangle\,|1\rangle\,. \end{aligned}$$

The good states of f^* (ancilla $= 0$ and $f(x) = 1$) receive total amplitude $\sqrt{p}\cos\varphi^*$, so the initial success probability for f^* is $p^* = p\cos^2\varphi^*$, and $\sin^{-1}\sqrt{p^*} = \varphi^*$ (since $\sin\varphi^* \approx \varphi^*$ for small φ^* and the geometry works out exactly by construction). Running amplitude amplification with k^* steps now gives

$$\sin^2((2k^*+1)\varphi^*) \;=\; \sin^2\!\left(\frac{\pi}{2}\right) \;=\; 1.$$

The total number of oracle calls remains $O(\sqrt{N/t})$, and accounting for the $O(\log N)$ cost of state preparation, the overall complexity is

$$O\left(\sqrt{\frac{N}{t}}\cdot\log N\right).$$

Exercise

When the number of solutions t is *not* known, show that there exists a quantum algorithm that finds a solution with constant success probability using an *expected* $O(\sqrt{N/t})$ oracle calls.