COL7160 : Quantum Computing

Lecture 20 : Grover's Algorithm with Unknown Number of Solutions

Instructor: Rajendra Kumar **Scribe:** Seerat Kaur

1 Introduction

This lecture continues the study of algorithms in the Grover family. We first address the case where t (the number of marked elements) is *unknown*, and show how a randomised schedule achieves the optimal $O(\sqrt{N/t})$ query complexity even without knowing t. We then study **Amplitude Estimation**, which uses Quantum Phase Estimation to estimate $\sin^2\theta = t/N$ to additive precision ε using $O(1/\varepsilon)$ quantum queries — a quadratic improvement over classical sampling, which requires $O(1/\varepsilon^2)$.

2 Grover's Algorithm: Recap

Grover's algorithm proceeds in three steps:

1. **Construct initial state.**

$$A|0\rangle = |v\rangle = \sqrt{p}\,|\psi_{\text{good}}\rangle + \sqrt{1-p}\,|\psi_{\text{bad}}\rangle$$

   where $p = t/N$ and $\sqrt{p} = \sin\theta$.

2. **Repeat k times.** Apply the Grover operator

$$G = A\big(2|0\rangle\langle 0| - I\big)A^{-1}\cdot Z_f$$

3. **Measure** in the standard (computational) basis.

For known p, the optimal number of iterations is $k^* = \lfloor \frac{\pi}{4}\sqrt{N/t}\rfloor$, giving success probability at least $1 - t/N$.

3 Unknown t: How to Maximise the Probability of Finding a Good State

When t (and hence $p = t/N$) is unknown, we cannot compute k^* directly. We consider three strategies.

Strategy 1: Try $k = 1, 2, 3, \ldots$ One idea is to iterate $k = 1, 2, 3, \ldots$ until a marked element is found. However, the total number of queries is

$$1 + 2 + 3 + \cdots + k^* \;=\; O\big((k^*)^2\big) \;=\; O\left(\frac{N}{t}\right),$$

which is higher than the target $O\left(\sqrt{N/t}\right)$. This strategy does not give a quantum speedup.

Strategy 2: Try $k = 1, 2, 4, \ldots$ A natural refinement is to use a geometrically growing schedule $k = 1, 2, 4, 8, \ldots$ The total number of queries up to level i (where $2^i \approx k^* = O(\sqrt{N/t})$) is

$$1 + 2 + 4 + \cdots + 2^i \;=\; 2^{i+1} - 1 \;=\; O(2^i) \;=\; O\Big(\sqrt{N/t}\Big).$$

So the query count is of the correct order. However, the problem is that the success probability after k steps is $\sin^2((2k+1)\theta)$, which oscillates. For a fixed unknown t, it is possible that every value $k = 1, 2, 4, 8, \ldots$ up to k^* happens to land near a zero of $\sin^2((2k+1)\theta)$, giving a consistently small success probability. The strategy therefore has no guaranteed constant success probability, and in the worst case never finds a marked element.

Strategy 3: Randomised Geometric Schedule A natural suggestion is to take $k = 1, 2, 4, \ldots$ and at each level i, pick the number of iterations *uniformly at random* from $\{1, 2, \ldots, 2^i\}$, and run G^{k^*}. One can show that with a uniform random choice up to 2^i, the probability of success is at least 1/4. Fix the level i such that the true optimal k^* satisfies $2^i \le k^* < 2^{i+1}$. The expected total number of queries is then obtained by accounting for failure at each level: with probability 3/4 we fail at level i and must proceed to level $i+1$ (costing $\sim 2^{i+2}$ queries), with probability $(3/4)^2$ we fail again at level $i+1$ (costing $\sim 2^{i+3}$), and so on:

$$\frac{3}{4}\cdot 2^{i+2} \;+\; \left(\frac{3}{4}\right)^2 \cdot 2^{i+3} \;+\; \cdots \;=\; 2^{i+2}\sum_{\ell=1}^{\infty}\left(\frac{3}{2}\right)^{\ell}\cdot\left(\frac{1}{2}\right)^{\ell} \;=\; 2^{i+2}\sum_{\ell=1}^{\infty}\left(\frac{3}{4}\cdot 2\right)^{\ell}.$$

The ratio of successive terms is $\frac{3}{4} \times 2 = \frac{3}{2} > 1$, so this series *diverges.* The doubling schedule does not work.

The fix: instead of doubling, grow k by a factor of $\lambda < 4/3$ at each step. Then the ratio of successive terms becomes $\frac{3}{4} \cdot \lambda < 1$, and the series converges. With $\lambda < 4/3$, the schedule of maximum iteration counts is

$$k = 1,\; \lambda,\; \lambda^2,\; \ldots,\; \lambda^j \;\lesssim\; \sqrt{N/t},$$

and the expected total number of queries is

$$\frac{3}{4}\cdot \lambda^{j+1} \;+\; \left(\frac{3}{4}\right)^2 \cdot \lambda^{j+2} \;+\; \cdots \;=\; \lambda^{j+1}\sum_{\ell=0}^{\infty}\left(\frac{3\lambda}{4}\right)^{\ell} \;=\; O(\lambda^j) \;=\; O\Big(\sqrt{N/t}\Big),$$

where convergence holds because $3\lambda/4 < 1$.

Theorem 1 (Brassard et al.)**.** *The randomised geometric schedule finds a marked element with constant success probability using* $O\Big(\sqrt{N/t}\Big)$ *expected quantum queries, even when* t *is unknown.*

4 Amplitude Amplification

The Grover operator generalises naturally. Let A be *any* unitary that prepares the initial state from $|0\rangle$. Define:

$$G \;=\; A\big(2\,|0\rangle\langle 0| - I\big)A^{-1}\cdot Z_f \;=\; \big(2\,|v\rangle\langle v| - I\big)\cdot Z_f.$$

This is **Amplitude Amplification**: applying G rotates the state by 2θ per step in the $\{|\psi_{\text{good}}\rangle, |\psi_{\text{bad}}\rangle\}$ plane, just as in Grover's algorithm. The action on the basis states is:

- $G\,|\psi_{\text{bad}}\rangle = \cos 2\theta\;|\psi_{\text{bad}}\rangle + \sin 2\theta\;|\psi_{\text{good}}\rangle$
- $G\,|\psi_{\text{good}}\rangle = \cos 2\theta\;|\psi_{\text{good}}\rangle - \sin 2\theta\;|\psi_{\text{bad}}\rangle$

5 Amplitude Estimation

5.1 Problem Statement

Definition 1 (Amplitude Estimation)**.** *Given oracle access to A with $A|0\rangle = \sin\theta\,|\psi_{good}\rangle + \cos\theta\,|\psi_{bad}\rangle$ and $p = \sin^2\theta = t/N$, estimate p to additive error ε, i.e. find $\hat{p}$ such that $|\hat{p} - p| < \varepsilon$.*

Classical complexity. To distinguish p from $p \pm \varepsilon$ using sampling requires $O(1/\varepsilon^2)$ repetitions.

Quantum complexity. Using the Phase Estimation subroutine applied to G, we can achieve $O(1/\varepsilon)$ queries — a quadratic quantum speedup.

5.2 Eigenstructure of the Grover Operator

The key insight is that G acts as a rotation by 2θ in a two-dimensional invariant subspace. Its eigenvectors are:

$$|\Psi_+\rangle = \frac{1}{\sqrt{2}}\Big(|\psi_{\text{good}}\rangle + i\,|\psi_{\text{bad}}\rangle\Big), \qquad |\Psi_-\rangle = \frac{1}{\sqrt{2}}\Big(|\psi_{\text{good}}\rangle - i\,|\psi_{\text{bad}}\rangle\Big),$$

with eigenvalues $e^{i2\theta}$ and $e^{-i2\theta}$, respectively. Indeed:

$$G\,|\Psi_+\rangle = e^{i2\theta}\,|\Psi_+\rangle\,, \qquad G\,|\Psi_-\rangle = e^{-i2\theta}\,|\Psi_-\rangle\,.$$

5.3 Decomposition of the Initial State

We claim that the initial state can be written in the eigenbasis of G as:

$$A\,|0\rangle \;=\; \sin\theta\,|\psi_{\text{good}}\rangle + \cos\theta\,|\psi_{\text{bad}}\rangle \;=\; \frac{e^{i\theta}}{\sqrt{2}\,i}\,|\Psi_+\rangle \;-\; \frac{e^{-i\theta}}{\sqrt{2}\,i}\,|\Psi_-\rangle\,.$$

Derivation. We expand the right-hand side using the definitions of $|\Psi_\pm\rangle$:

$$\begin{aligned}
\frac{e^{i\theta}}{\sqrt{2}\,i}\,|\Psi_+\rangle - \frac{e^{-i\theta}}{\sqrt{2}\,i}\,|\Psi_-\rangle &= \frac{e^{i\theta}}{2i}\Big(|\psi_{\text{good}}\rangle + i\,|\psi_{\text{bad}}\rangle\Big) - \frac{e^{-i\theta}}{2i}\Big(|\psi_{\text{good}}\rangle - i\,|\psi_{\text{bad}}\rangle\Big) \\
&= \frac{1}{2i}\Big[\big(e^{i\theta} - e^{-i\theta}\big)\,|\psi_{\text{good}}\rangle + i\big(e^{i\theta} + e^{-i\theta}\big)\,|\psi_{\text{bad}}\rangle\Big] \\
&= \frac{1}{2i}\Big[2i\sin\theta\,|\psi_{\text{good}}\rangle + 2i\cos\theta\,|\psi_{\text{bad}}\rangle\Big] \\
&= \sin\theta\,|\psi_{\text{good}}\rangle + \cos\theta\,|\psi_{\text{bad}}\rangle\,,
\end{aligned}$$

where we used $e^{i\theta} - e^{-i\theta} = 2i\sin\theta$ and $e^{i\theta} + e^{-i\theta} = 2\cos\theta$.

5.4 Phase Estimation Applied to G

We run Quantum Phase Estimation with G and initial state $A|0\rangle$. Since $A|0\rangle$ is a superposition of the two eigenstates $|\Psi_\pm\rangle$ with phases $\pm 2\theta$, the algorithm measures a phase $\hat{\theta}$ approximating θ. From $\hat{\theta}$ we obtain the estimate

$$\hat{p} = \sin^2\hat{\theta}.$$

Using m ancilla qubits in the phase estimation circuit, the phase is estimated to precision $2\pi/2^m$, giving:

$$|\sin^2\hat{\theta} - \sin^2\theta| \;<\; \varepsilon \quad \text{using} \quad O\left(\frac{1}{\varepsilon}\right) \text{ applications of } G.$$

Classical vs. quantum comparison.

	Precision	**Query complexity**
Classical sampling	$\|\hat{p} - p\| < \varepsilon$	$O(1/\varepsilon^2)$
Quantum (Phase Est.)	$\|\hat{p} - p\| < \varepsilon$	$O(1/\varepsilon)$

Theorem 2 (Brassard et al., 2002)**.** *Amplitude Estimation computes $\hat{p}$ with $|\hat{p} - p| < \varepsilon$ using $O(1/\varepsilon)$ applications of G (and hence $O(1/\varepsilon)$ oracle queries), succeeding with constant probability.*