COL7160 : Quantum Computing

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

Instructor: Rajendra Kumar **Scribe:** Ansh Gupta

1 The Search Problem

Definition 1. The *unstructured search problem* is defined as follows. Let $N = 2^n$ for some positive integer n. We are given an arbitrary binary string $x \in \{0,1\}^N$, which we think of as indexing an N-slot database. The goal is to find an index $i \in \{0, 1, \ldots, N-1\}$ such that $x_i = 1$, or to report "no solutions" if no such index exists.

We denote by t the number of *marked* (or "good") elements, i.e., the **Hamming weight** of x:

$$t \;=\; |\{i : x_i = 1\}|.$$

1.1 Classical vs. Quantum Complexity

- **Classical (deterministic):** Any deterministic algorithm requires $\Omega(N)$ queries in the worst case, since the marked element could be the last one checked.
- **Classical (randomized):** A randomized algorithm still needs $\Theta(N)$ queries on average, because the database is unordered—there is no structure to exploit.
- **Quantum (Grover):** Grover's algorithm [GW96] solves the problem using only $O\left(\sqrt{N}\right)$ queries to the oracle and $O\left(\sqrt{N}\log N\right)$ additional elementary gates.

Remark 2. The quadratic quantum speedup in Grover's algorithm is *provably optimal* for unstructured search: any quantum algorithm requires $\Omega(\sqrt{N})$ queries. This lower bound was established via the polynomial method and the adversary method [dW23].

2 The Oracle Model

Grover's algorithm, like most quantum query algorithms, is described in the *quantum oracle* (or *black-box*) model.

Definition 3 (Boolean Oracle)**.** Let $f : \{0, 1, \ldots, N-1\} \to \{0, 1\}$ be the function where $f(i) = 1$ iff $x_i = 1$. The *phase oracle* U_f is the unitary operator defined by

$$U_f \left|i\right\rangle \;=\; (-1)^{f(i)} \left|i\right\rangle .$$

It acts diagonally in the computational basis: it leaves "bad" states unchanged and flips the phase of every "good" (marked) state.

Remark 4. A phase oracle can be implemented from a standard bit-flip oracle $O_f \left|i\right\rangle \left|b\right\rangle = \left|i\right\rangle \left|b \oplus f(i)\right\rangle$ by preparing the ancilla in the state $\left|-\right\rangle = \frac{1}{\sqrt{2}}(\left|0\right\rangle - \left|1\right\rangle)$ and using the phase-kickback trick.

3 Grover's Algorithm

3.1 Preliminary Definitions

Before describing the algorithm, it is useful to define two orthonormal states that span the relevant 2-dimensional subspace.

Definition 5 (Good and Bad superpositions)**.** Define the uniform superposition over all *marked* indices as

$$|\psi_{\text{good}}\rangle \;=\; \frac{1}{\sqrt{t}} \sum_{\substack{i=0 \\ f(i)=1}}^{N-1} |i\rangle \,,$$

and the uniform superposition over all *unmarked* indices as

$$|\psi_{\text{bad}}\rangle \;=\; \frac{1}{\sqrt{N-t}} \sum_{\substack{i=0 \\ f(i)=0}}^{N-1} |i\rangle \,.$$

The states $|\psi_{\text{good}}\rangle$ and $|\psi_{\text{bad}}\rangle$ are orthonormal: $\langle\psi_{\text{good}}|\psi_{\text{bad}}\rangle = 0$.

The initial uniform superposition can be written in this basis. Define the angle θ by

$$\sin\theta \;=\; \sqrt{\frac{t}{N}}, \qquad \cos\theta \;=\; \sqrt{\frac{N-t}{N}}, \quad \theta \in \left(0, \frac{\pi}{2}\right).$$

Then the state $|s\rangle = H^{\otimes n} |0\rangle^{\otimes n}$ satisfies

$$|s\rangle \;=\; \sin\theta \; |\psi_{\text{good}}\rangle + \cos\theta \; |\psi_{\text{bad}}\rangle \,.$$

3.2 Algorithm Steps

Algorithm 1 Grover's Search Algorithm

1: **Input:** Oracle U_f, number of qubits n (so $N = 2^n$), number of solutions t (or an estimate).
2: **Output:** An index i^* such that $f(i^*) = 1$, with high probability.
3: Initialize: $|\psi_0\rangle \leftarrow |0\rangle^{\otimes n}$
4: Apply Hadamard: $|s\rangle \leftarrow H^{\otimes n} |0\rangle^{\otimes n} = \dfrac{1}{\sqrt{N}} \displaystyle\sum_{i=0}^{N-1} |i\rangle$
5: Set $k \leftarrow \left\lfloor \dfrac{\pi}{4}\sqrt{\dfrac{N}{t}} - \dfrac{1}{2} \right\rfloor$
6: **for** $j = 1$ to k **do**
7: Apply Phase Oracle: $|\psi\rangle \leftarrow U_f |\psi\rangle$
8: Apply Diffusion Operator: $|\psi\rangle \leftarrow D |\psi\rangle$
9: **end for**
10: Measure in the computational basis and return the result i^*.

We now describe each step in detail.

Step 1: State Initialization

We begin with all n qubits in the ground state $|0\rangle^{\otimes n}$ and apply the n-fold Hadamard transform to obtain the uniform superposition

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

In the $\{|\psi_{\text{good}}\rangle, |\psi_{\text{bad}}\rangle\}$ basis, this state makes a small angle θ with the $|\psi_{\text{bad}}\rangle$ axis (since $t \ll N$ in typical applications), so it is initially almost entirely in the "bad" subspace.

Step 2: The Phase Oracle (U_f)

The oracle U_f flips the sign of every marked basis state:

$$U_f |i\rangle = (-1)^{f(i)} |i\rangle .$$

In the 2D picture, applying U_f reflects the state vector across the $|\psi_{\text{bad}}\rangle$ axis. More precisely, if $|\psi\rangle = \alpha |\psi_{\text{good}}\rangle + \beta |\psi_{\text{bad}}\rangle$, then $U_f |\psi\rangle = -\alpha |\psi_{\text{good}}\rangle + \beta |\psi_{\text{bad}}\rangle$.

Step 3: The Diffusion Operator (D)

The diffusion operator, also called *inversion about the mean* or the *Grover diffusion operator*, is defined as

$$D = 2 |s\rangle \langle s| - I.$$

Proposition 6. *The diffusion operator D reflects the current state about the initial uniform superposition $|s\rangle$.*

Proof. Decompose any state $|\psi\rangle$ into its component along $|s\rangle$ and its orthogonal complement: $|\psi\rangle = c |s\rangle + |\psi^{\perp}\rangle$ where $\langle s|\psi^{\perp}\rangle = 0$. Then

$$D |\psi\rangle = (2 |s\rangle \langle s| - I)(c |s\rangle + |\psi^{\perp}\rangle) = 2c |s\rangle - c |s\rangle - |\psi^{\perp}\rangle = c |s\rangle - |\psi^{\perp}\rangle ,$$

which is indeed the reflection of $|\psi\rangle$ about $|s\rangle$. □ □

The diffusion operator has a simple circuit implementation:

$$D = H^{\otimes n}\big(2 |0\rangle \langle 0| - I\big)H^{\otimes n}.$$

The inner operator $2 |0\rangle \langle 0| - I$ flips the phase of all basis states except $|0\rangle$, and the Hadamard conjugation transforms this into the required reflection about $|s\rangle$.

The Grover Iterate

One application of $G = D \cdot U_f$ is called a **Grover iterate**. Each iterate rotates the state vector by 2θ toward $|\psi_{\text{good}}\rangle$ in the $\{|\psi_{\text{good}}\rangle , |\psi_{\text{bad}}\rangle\}$ plane.

4 Geometric Interpretation

Grover's algorithm is best understood as a sequence of **rotations in a 2-dimensional plane**. The entire N-dimensional Hilbert space is effectively compressed into the plane spanned by $|\psi_{\text{good}}\rangle$ and $|\psi_{\text{bad}}\rangle$.

We work in the 2D subspace $\text{span}\{|\psi_{\text{good}}\rangle , |\psi_{\text{bad}}\rangle\}$ and use polar coordinates within it. The state after initialization is

$$|\psi_0\rangle = |s\rangle = \cos\theta \, |\psi_{\text{bad}}\rangle + \sin\theta \, |\psi_{\text{good}}\rangle ,$$

which makes angle θ with $|\psi_{\text{bad}}\rangle$ (or equivalently $\pi/2 - \theta$ with $|\psi_{\text{good}}\rangle$).

4.1 Effect of Each Grover Iterate

Oracle reflection. U_f reflects $|\psi\rangle$ across $|\psi_{\text{bad}}\rangle$. If $|\psi\rangle$ makes angle α with $|\psi_{\text{bad}}\rangle$, after U_f it makes angle $-\alpha$ with $|\psi_{\text{bad}}\rangle$.

Diffusion reflection. D reflects the resulting state across $|s\rangle$, which makes angle θ with $|\psi_{\text{bad}}\rangle$. Composing two reflections (one across $|\psi_{\text{bad}}\rangle$ at 0° and one across $|s\rangle$ at θ) produces a *rotation* by 2θ.

4.2 State after k Iterations

Theorem 7. *After k Grover iterates, the state is*

$$|\psi_k\rangle \;=\; \sin\big((2k+1)\theta\big)\;|\psi_{\text{good}}\rangle \;+\; \cos\big((2k+1)\theta\big)\;|\psi_{\text{bad}}\rangle\,.$$

Proof. By induction. The base case $k=0$ gives $|\psi_0\rangle = \sin\theta\;|\psi_{\text{good}}\rangle + \cos\theta\;|\psi_{\text{bad}}\rangle$, consistent with the formula. For the inductive step, each iterate increases the angle with $|\psi_{\text{bad}}\rangle$ by 2θ, so after k steps the angle is $(2k+1)\theta$. □ □

4.3 Success Probability

The probability of measuring a marked element after k iterations is

$$P_{\text{success}}(k) \;=\; \sin^2\big((2k+1)\theta\big).$$

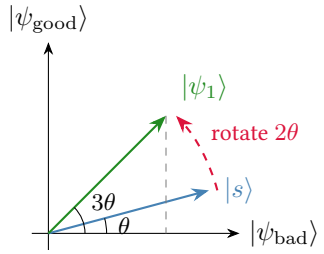

Figure 1: One Grover iterate rotates the state vector by 2θ in the $\{|\psi_{\text{good}}\rangle\,, |\psi_{\text{bad}}\rangle\}$ plane. Starting from angle θ, after one step the angle becomes 3θ.

5 Optimal Number of Iterations

5.1 Known t: Exact Formula

To maximize P_{success}, we want $(2k+1)\theta \approx \pi/2$, i.e.,

$$k \;\approx\; \frac{\pi/2-\theta}{2\theta} \;=\; \frac{\pi}{4\theta} - \frac{1}{2}.$$

For $t \ll N$ we have $\theta \approx \sin\theta = \sqrt{t/N}$, giving the celebrated

$$\boxed{k_{\text{opt}} \;=\; \left\lfloor \frac{\pi}{4}\sqrt{\frac{N}{t}} \right\rfloor .}$$

With this choice, $P_{\text{success}} \geq 1 - t/N$, which is close to 1 when $t \ll N$.

Remark 8. **Overshooting:** Running Grover's algorithm for more than k_{opt} iterations does *not* improve the success probability; instead it causes the state to rotate *past* $|\psi_{\text{good}}\rangle$, and the probability of success begins to *decrease*. This is a fundamental quantum interference effect with no classical analogue.

5.2 Unknown t: Handling the General Case

In practice, the number of solutions t may be unknown. We want to find a marked element with high probability using $O(\sqrt{N/t})$ queries, without knowing t in advance. Two main strategies are described below.

5.2.1 Method 1: Linear Search (Sequential Doubling of Target)

Run Grover's algorithm for $k = 1, 2, 3, 4, \ldots$ iterations and measure after each run. Stop when a marked element is found.

Analysis. Let $k^* = \lfloor \pi/(4\theta) \rfloor$ be the (unknown) optimal number of iterations. The probability of success after exactly k iterations is $\sin^2((2k+1)\theta)$.
By a standard trigonometric argument, if k is chosen *uniformly at random* from $\{0, 1, \ldots, k^*\}$, the expected success probability is at least $1/2$. Summing the cost of the sequential runs:

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

Thus Method 1 finds a solution in expected $O(N/t)$ queries—a quadratic *improvement* over the classical $\Theta(N/t)$ expected queries, but not yet achieving the $O(\sqrt{N/t})$ bound.

5.2.2 Method 2: Exponential Search (Geometric Schedule)

Run Grover's algorithm for $k = 1, 2, 4, 8, \ldots$ (powers of 2) iterations and measure after each run. Stop when a marked element is found.

Key observation. Let 2^i be the largest power of 2 that does not exceed k^*. At $k = 2^i$ iterations, the angle satisfies $(2 \cdot 2^i + 1)\theta \le \pi/2$, so $P_{\text{success}}(2^i) \ge 1/2$.

Probability analysis. At iteration $k = 2^{i+1}$, the angle $(2 \cdot 2^{i+1} + 1)\theta$ may exceed $\pi/2$, so we no longer have a direct lower bound. We bound the probability of *failure* up to step 2^{i+1} using the following telescoping argument. For each subsequent doubling $j > i$, since $2^j > k^*$, we can still lower bound:

$$P_{\text{success}}(2^j) \;\ge\; \frac{1}{4}.$$

Expected query complexity. The total number of oracle calls in the geometric schedule up to and including the successful round at $2^{i+\ell}$ (for some small ℓ) is

$$1 + 2 + 4 + \cdots + 2^{i+\ell} \;=\; O(2^{i+\ell}) \;=\; O(k^*) \;=\; O\left(\sqrt{\frac{N}{t}}\right).$$

Convergence issue and fix. The naive geometric schedule has a subtle convergence problem. Suppose the success probability at step $2^{i+\ell}$ is bounded below by some constant $c > 0$. The probability that we have *not yet* succeeded by step $2^{i+\ell}$ is at most $(1-c)^\ell$. The total expected cost is

$$\sum_{\ell=0}^{\infty} (1-c)^\ell \cdot 2^{i+\ell+1} \;=\; 2^{i+1} \sum_{\ell=0}^{\infty} \big[(1-c)\cdot 2\big]^\ell,$$

which **diverges** if $2(1-c) \ge 1$, i.e., $c \le 1/2$. Since our bound gives $c = 1/4$, the series diverges.

Resolution: step size $4/3-\varepsilon$. To restore convergence, we replace the doubling factor 2 with a factor of $\lambda = 4/3-\varepsilon$ for a small constant $\varepsilon > 0$. The schedule becomes $k_j = \lceil \lambda^j \rceil$ for $j = 0, 1, 2, \ldots$
With this choice, the convergence factor of the series becomes $\lambda(1-c) = (4/3-\varepsilon)(1-1/4) = (4/3-\varepsilon)(3/4) = 1 - 3\varepsilon/4 < 1$, so the geometric series converges. The total expected number of oracle queries is

$$\sum_{\ell=0}^{\infty} \left(\frac{3}{4}\right)^\ell \cdot \lambda^{i+\ell+1} \;=\; O(\lambda^i) \;=\; O(k^*) \;=\; O\left(\sqrt{\frac{N}{t}}\right).$$

Remark 9. **Summary of Method 2.** By using a geometric schedule with growth factor $\lambda = 4/3-\varepsilon < 4/3$, Grover's algorithm with unknown t achieves an expected query complexity of $O(\sqrt{N/t})$, matching the optimal known-t bound up to constants.

The following table summarizes the query complexity of the two methods.

Setting	Algorithm	Query Complexity
Classical (randomized)	Random sampling	$\Theta(N/t)$
Quantum, t known	Grover (fixed k)	$O(\sqrt{N/t})$
Quantum, t unknown	Method 1 (linear)	$O(N/t)$
Quantum, t unknown	Method 2 (geometric, $\lambda = 4/3 - \varepsilon$)	$O(\sqrt{N/t})$

6 Amplitude Estimation

Amplitude estimation is a powerful generalization of Grover's algorithm. Instead of *finding* a marked element, the goal is to *estimate the fraction* of marked elements.

6.1 Problem Setup

Definition 10 (Amplitude Estimation Problem)**.** Let A be a unitary operator acting on $n+1$ qubits such that

$$A\,|0\rangle^{\otimes n}\,|0\rangle \;=\; \sqrt{\frac{t}{N}}\;|\psi_{\text{good}}\rangle\,|1\rangle \;+\; \sqrt{\frac{N-t}{N}}\;|\psi_{\text{bad}}\rangle\,|0\rangle\,.$$

Here the last qubit serves as a *flag*: it is $|1\rangle$ for good states and $|0\rangle$ for bad states. The amplitude estimation problem asks: given oracle access to A, estimate the amplitude $a = \sqrt{t/N}$ (or equivalently, estimate t/N).

Remark 11. In the context of Grover's algorithm, $A = H^{\otimes n}$ (up to a re-labeling), so $a = \sin\theta$. The goal is to determine θ (and hence t).

6.2 Reduction to Phase Estimation

Amplitude estimation reduces to *quantum phase estimation* (QPE) applied to the Grover iterate $G = D \cdot U_f$. The key observation is:

Theorem 12. *The Grover iterate G has eigenvalues $e^{\pm 2i\theta}$, with corresponding eigenstates*

$$|\varphi_\pm\rangle \;=\; \frac{1}{\sqrt{2}}\big(|\psi_{\text{good}}\rangle \mp i\;|\psi_{\text{bad}}\rangle\big).$$

Proof. In the $\{|\psi_{\text{good}}\rangle\,, |\psi_{\text{bad}}\rangle\}$ plane, G is the rotation matrix $\begin{pmatrix}\cos 2\theta & -\sin 2\theta \\ \sin 2\theta & \cos 2\theta\end{pmatrix}$, whose eigenvalues are $e^{\pm 2i\theta}$. The eigenstates are as stated. □ □

Quantum phase estimation on G with $|s\rangle$ as the input state estimates $\theta/(2\pi)$ to m bits of precision using $O(2^m)$ applications of G, i.e., $O(2^m\sqrt{N/t})$ oracle queries.

6.3 Amplitude Amplification

More generally, the *amplitude amplification* framework [dW23] replaces the Hadamard initialization with an arbitrary quantum algorithm A and shows:

Theorem 13 (Amplitude Amplification)**.** *Let A be any quantum algorithm that prepares a state with "good" amplitude a. Then $O(1/a)$ applications of the Grover iterate (built from A and U_f) suffice to find a good outcome with constant probability.*

This subsumes Grover's algorithm (where $a = \sqrt{t/N}$, giving $O(\sqrt{N/t})$ queries) and extends it to more general settings such as quantum walk-based algorithms and quantum Monte Carlo estimation.

References

[GW96] Lov K. Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing (STOC '96)*, pages 212–219. ACM, 1996. https://doi.org/10.1145/237814.237866.

[dW23] Ronald de Wolf. Quantum computing: Lecture notes. arXiv preprint arXiv:1907.09415, 2023. https://arxiv.org/abs/1907.09415.