COL7160 : Quantum Computing

Lecture 18 : Grover's Search Algorithm

Instructor: Rajendra Kumar **Scribe:** Shashank Kumar

1 Introduction

This lecture introduces Grover's Search Algorithm [Gro96]. It is the foundation for a family of related algorithms sharing the same core idea: Amplitude Amplification, Amplitude Estimation, Approximate Counting, and Quantum Random Walks. Unlike Simon's algorithm, which exploits algebraic structure in f, Grover's algorithm makes no structural assumption on f and still provides a provable quantum speedup.

2 The Search Problem

Definition 1 (Search Problem)**.** Given a string $x \in \{0,1\}^N$ and oracle access to $f : \{0,1\}^n \to \{0,1\}$ with $N = 2^n$, find x^* such that $f(x^*) = 1$. There are $t \geq 1$ such inputs.
In the *unique search* case, $t = 1$:

$$\exists\, i \;\text{ s.t. }\; x_i = 1, \qquad \forall\, j \neq i,\; x_j = 0.$$

Classical complexity. A deterministic algorithm requires $\Omega(N)$ queries. A randomised algorithm requires $\Omega(N/t)$ queries for constant success probability. Grover's algorithm achieves $O(\sqrt{N/t})$ quantum queries.

Remark 2. The circuit for f is known but is useless for finding x^* directly; the only use is to construct the oracle. A canonical example is SAT: evaluating f on any assignment is efficient, but finding a satisfying assignment is computationally hard.

2.1 Quantum RAM

To create the superposition $\frac{1}{\sqrt{N}} \sum_i |i\rangle |x_i\rangle$ when x_i cannot be expressed as an efficient function of i, the data must be stored in **Quantum Random Access Memory (QRAM)**:

$$\frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i\rangle |0\rangle \xrightarrow{\text{QRAM}} \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i\rangle |x_i\rangle .$$

For most applications, $x_i = f(i)$ for an efficiently computable f, so QRAM is not needed.

3 Grover's Algorithm

3.1 Setup and Key States

Prepare the uniform superposition:

$$|v\rangle = H^{\otimes n} |0\rangle^{\otimes n} = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle .$$

Definition 3 (Good and Bad States)**.**

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

$|A\rangle$ is the uniform superposition over marked (good) states; $|B\rangle$ over unmarked (bad) states. They are orthonormal.

The initial state decomposes as:

$$|v\rangle = \sqrt{\frac{t}{N}}\, |A\rangle + \sqrt{\frac{N-t}{N}}\, |B\rangle = \sin\theta\, |A\rangle + \cos\theta\, |B\rangle , \qquad \sin\theta = \sqrt{\frac{t}{N}}.$$

3.2 The Phase Oracle

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

Implemented via the bit-flip oracle $\mathcal{O}_f : |x\rangle |b\rangle \mapsto |x\rangle |b \oplus f(x)\rangle$ with ancilla in $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ (phase kickback). Circuit size equals that of f.

3.3 The Diffusion Operator: Flip Around the Mean

Definition 4 (Diffusion Operator)**.**

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

Lemma 5. *If* $|\psi\rangle = \sum_x \alpha_x |x\rangle$ *with mean* $\bar{\alpha} = \frac{1}{N} \sum_x \alpha_x$*, then* $D |\psi\rangle = \sum_x (2\bar{\alpha} - \alpha_x) |x\rangle$.

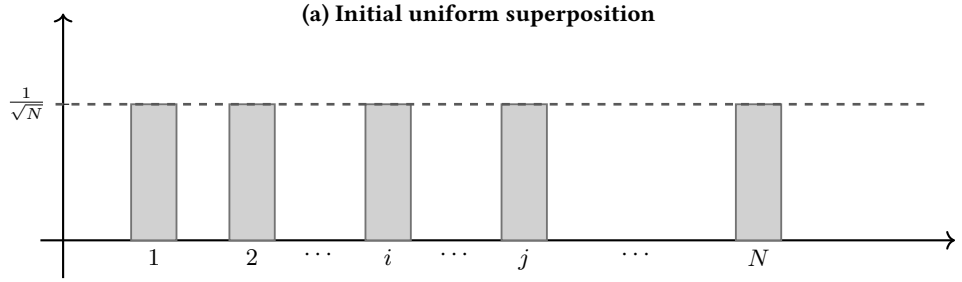
Proof. Since $\langle v|\psi\rangle = \sqrt{N}\, \bar{\alpha}$,

$$D |\psi\rangle = 2 |v\rangle \langle v|\psi\rangle - |\psi\rangle = \sum_x (2\bar{\alpha} - \alpha_x) |x\rangle . \qquad \square$$

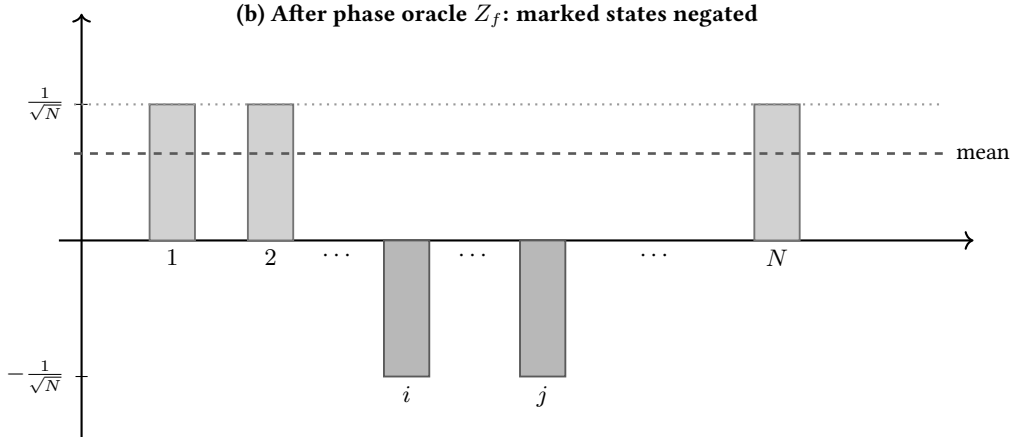
Thus D reflects each amplitude about the mean: $\alpha_x \mapsto 2\bar{\alpha} - \alpha_x$.

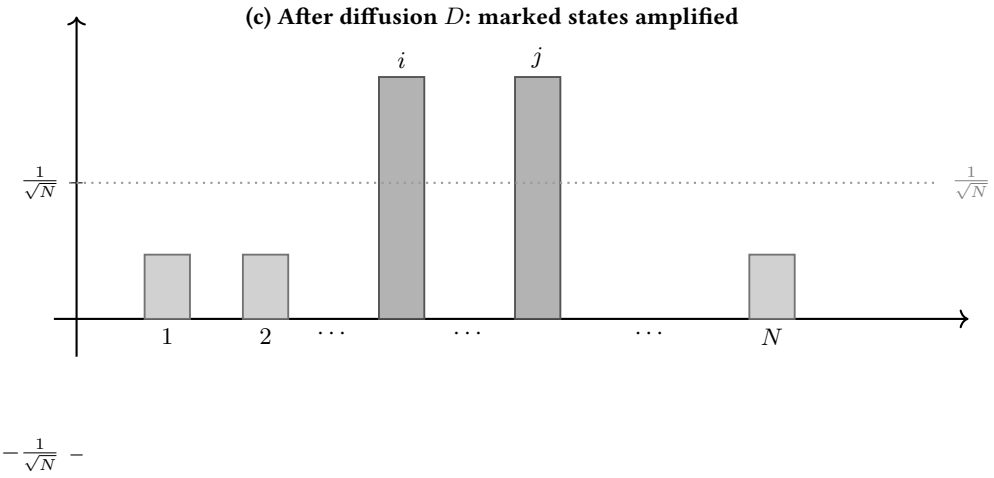
The three figures below illustrate one complete Grover iteration. Indices i and j are the marked states ($f(x) = 1$); all others are unmarked.

(a) Initial uniform superposition



(b) After phase oracle Z_f: marked states negated





In (a), all amplitudes equal $1/\sqrt{N}$ and the mean equals $1/\sqrt{N}$. In (b), the phase oracle negates the amplitudes of the marked states i and j to $-1/\sqrt{N}$, causing the mean to drop below $1/\sqrt{N}$. In (c), the diffusion operator maps $\alpha_x \mapsto 2\bar{\alpha} - \alpha_x$: the marked states (at $-1/\sqrt{N}$, far below the mean) are reflected to a value well above $1/\sqrt{N}$, while unmarked states (slightly above the mean) decrease. Repeated application increases the probability of measuring a marked state.

3.4 The Grover Operator

Definition 6 (Grover Operator)**.**

$$G = D \cdot Z_f = (2 |v\rangle \langle v| - I) \cdot Z_f.$$

Applying Z_f to $|v\rangle$ gives:

$$Z_f |v\rangle = -\sqrt{\frac{t}{N}} |A\rangle + \sqrt{\frac{N-t}{N}} |B\rangle .$$

3.5 Geometric Analysis

Theorem 7. *In the plane* $\mathrm{span}\{|A\rangle, |B\rangle\}$*, each application of* G *rotates the state vector by* 2θ *towards* $|A\rangle$*. After* k *applications:*

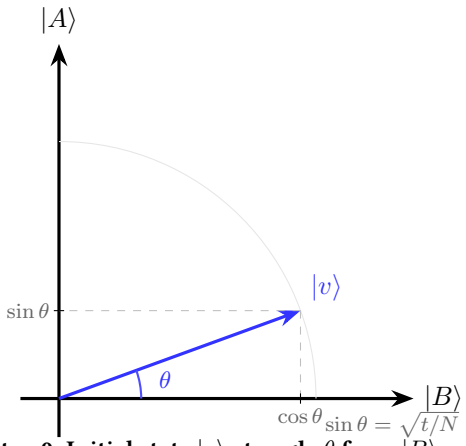
$$G^k |v\rangle = \sin\big((2k+1)\theta\big) |A\rangle + \cos\big((2k+1)\theta\big) |B\rangle .$$

Proof. The initial state $|v\rangle = \sin\theta |A\rangle + \cos\theta |B\rangle$ lies at angle θ from $|B\rangle$.
Step 1 — Z_f: The phase oracle negates the $|A\rangle$ component, acting as the reflection $I - 2 |A\rangle \langle A|$ in this plane. This maps the state from angle θ to $-\theta$ (reflection about $|B\rangle$):

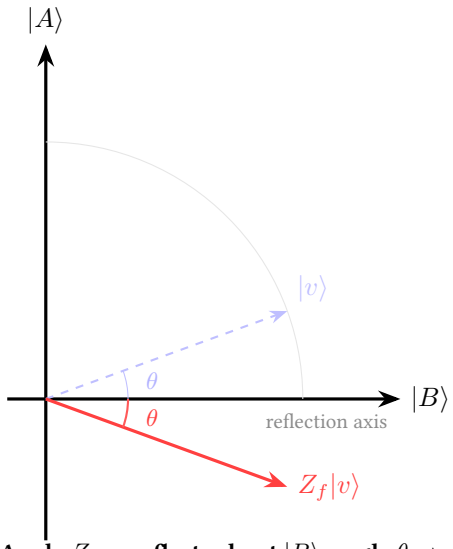
$$Z_f |v\rangle = -\sin\theta |A\rangle + \cos\theta |B\rangle .$$

Step 2 — D: The diffusion $D = 2 |v\rangle \langle v| - I$ reflects about $|v\rangle$, which lies at angle θ. Reflecting the vector at angle $-\theta$ about the line at angle θ produces a vector at angle $\theta + 2\theta = 3\theta$.
The composition of these two reflections is a rotation by 2θ. After k applications the state is at angle $(2k+1)\theta$ from $|B\rangle$, giving the stated formula. □

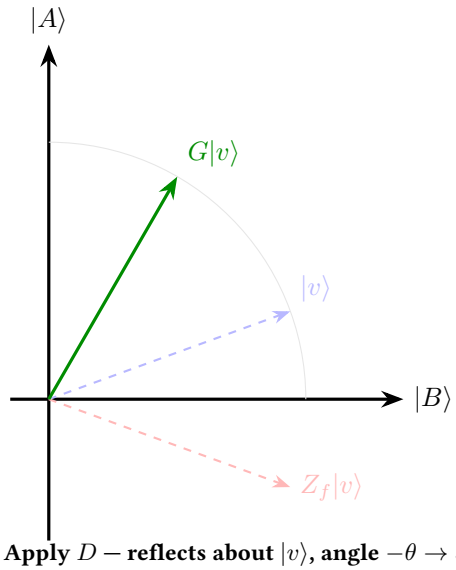
The four diagrams below show the geometric effect of one Grover step. Angles are colour-coded: blue for θ between $|B\rangle$ and $|v\rangle$, red for θ between $|B\rangle$ and $Z_f |v\rangle$, and orange for the net 2θ rotation between $|v\rangle$ and $G |v\rangle$.



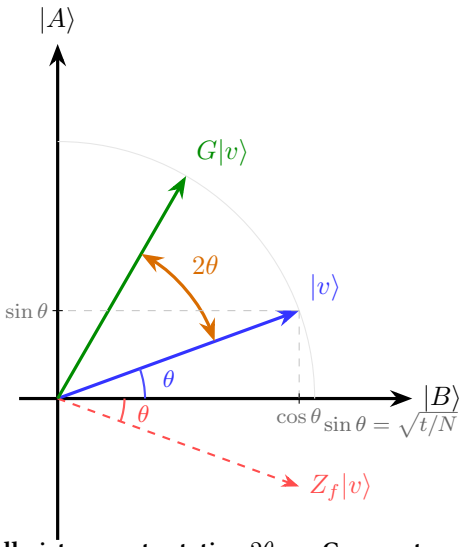
Step 0: Initial state $|v\rangle$ at angle θ from $|B\rangle$



Step 1: Apply Z_f — reflects about $|B\rangle$, angle $\theta \to -\theta$



Step 2: Apply D — reflects about $|v\rangle$, angle $-\theta \to 3\theta$



Full picture: net rotation 2θ per Grover step

3.6 Query Complexity

The success probability after k steps is $\sin^2((2k+1)\theta)$. Setting $(2k+1)\theta \approx \pi/2$ gives:

$$k^* = \left\lfloor \frac{\pi}{4}\sqrt{\frac{N}{t}} \right\rfloor = O\left(\sqrt{\frac{N}{t}}\right).$$

Theorem 8 (Grover [Gro96])**.** *Grover's algorithm finds a marked element among N inputs with $t \geq 1$ solutions using $O(\sqrt{N/t})$ oracle queries, succeeding with probability at least $1 - t/N$.*

3.7 Algorithm

Algorithm 1 Grover's Search

Input: Phase oracle Z_f for $f : \{0,1\}^n \to \{0,1\}$ with t solutions; $N = 2^n$.
Output: x^* with $f(x^*) = 1$.
$|\psi\rangle \leftarrow H^{\otimes n} |0\rangle^{\otimes n}$
$k \leftarrow \lfloor \frac{\pi}{4}\sqrt{N/t} \rfloor$
for $j = 1$ **to** k **do**
    $|\psi\rangle \leftarrow Z_f |\psi\rangle$ ▷ Phase oracle: negate amplitudes of marked states
    $|\psi\rangle \leftarrow (2|v\rangle\langle v| - I)|\psi\rangle$ ▷ Diffusion: flip around the mean
end for
Measure $|\psi\rangle$ in the computational basis and **return** outcome.

References

[Gro96] Lov K. Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the 28th Annual ACM Symposium on Theory of Computing (STOC)*, pages 212–219, 1996.