Detailed Proof and Analysis of Grover's Search Algorithm

Raunak Kumar Singh

November 24, 2025

1 Introduction and Problem Statement

The unstructured search problem is a fundamental challenge in computer science. Classically, searching an unsorted database of N items requires $O(N)$ queries in the worst case. Grover's algorithm provides a quadratic speedup, solving the problem in $O(\sqrt{N})$ queries.

1.1 Formal Setup

We are given a search space of size $N = 2^n$. We assume the existence of a black box function (oracle) $f : \{0,1\}^n \to \{0,1\}$ defined as:

$$f(x) = \begin{cases} 1 & \text{if } x \text{ is a solution (marked item)} \\ 0 & \text{if } x \text{ is not a solution} \end{cases} \tag{1}$$

Let M be the number of solutions such that $f(x) = 1$. Our objective is to find a state x^* such that $f(x^*) = 1$ with high probability.

2 Geometric Formalism

To understand the algorithm, we analyze the evolution of the state vector within a specific 2-dimensional subspace of the Hilbert space $\mathcal{H} = \mathbb{C}^N$.

2.1 Defining the Basis States

We define two normalized superposition states:

Definition 1 (Good and Bad States)**.** *The uniform superposition of all solution states ($|good\rangle$) and non-solution states ($|bad\rangle$) are:*

$$|good\rangle = \frac{1}{\sqrt{M}} \sum_{x:f(x)=1} |x\rangle \quad , \quad |bad\rangle = \frac{1}{\sqrt{N-M}} \sum_{x:f(x)=0} |x\rangle \tag{2}$$

2.2 The Initial State

The algorithm begins by initializing n qubits to $|0\rangle$ and applying Hadamard gates ($H^{\otimes n}$). This creates the uniform superposition $|\psi\rangle$, which lies entirely within the plane spanned by $|\text{good}\rangle$ and $|\text{bad}\rangle$:

$$|\psi\rangle = H^{\otimes n} |0\rangle^{\otimes n} = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle \tag{3}$$

We can rewrite $|\psi\rangle$ using an angle θ:

$$|\psi\rangle = \sin\theta\,|\text{good}\rangle + \cos\theta\,|\text{bad}\rangle \tag{4}$$

where the angle θ is determined by the ratio of solutions to the total space:

$$\sin\theta = \sqrt{\frac{M}{N}} \tag{5}$$

2.3 The Orthogonal State

For the algebraic derivation of the rotation, it is useful to define a state $|\bar{\psi}\rangle$ that is orthogonal to $|\psi\rangle$ in this 2D plane:

$$|\bar{\psi}\rangle = \cos\theta\,|\text{good}\rangle - \sin\theta\,|\text{bad}\rangle \tag{6}$$

Note that $\langle\psi|\bar{\psi}\rangle = 0$.

3 The Grover Iteration

The core of the algorithm is the Grover Iterator G, which is applied k times. The iterator consists of two reflections:

$$G = U_s U_f \tag{7}$$

where U_f is the Oracle and U_s is the Diffusion Operator.

3.1 Step 1: The Oracle (U_f)

The oracle marks solutions by flipping their phase: $|x\rangle \to (-1)^{f(x)}\,|x\rangle$. Geometrically, this is a reflection about the $|\text{bad}\rangle$ axis.

$$U_f\,|\psi\rangle = -\sin\theta\,|\text{good}\rangle + \cos\theta\,|\text{bad}\rangle \tag{8}$$

To understand the rotation, let us express this reflection in terms of the $|\psi\rangle, |\bar{\psi}\rangle$ basis. Using the substitutions $|\text{good}\rangle = \sin\theta\,|\psi\rangle + \cos\theta\,|\bar{\psi}\rangle$ and $|\text{bad}\rangle = \cos\theta\,|\psi\rangle - \sin\theta\,|\bar{\psi}\rangle$:

$$\begin{aligned} U_f\,|\psi\rangle &= -\sin\theta(\sin\theta\,|\psi\rangle + \cos\theta\,|\bar{\psi}\rangle) + \cos\theta(\cos\theta\,|\psi\rangle - \sin\theta\,|\bar{\psi}\rangle) \\ &= (-\sin^2\theta + \cos^2\theta)\,|\psi\rangle - 2\sin\theta\cos\theta\,|\bar{\psi}\rangle \end{aligned}$$

Using the double-angle trigonometric identities ($\cos 2\theta = \cos^2\theta - \sin^2\theta$ and $\sin 2\theta = 2\sin\theta\cos\theta$):

$$U_f\,|\psi\rangle = \cos 2\theta\,|\psi\rangle - \sin 2\theta\,|\bar{\psi}\rangle \tag{9}$$

3.2 Step 2: The Diffusion Operator (U_s)

The diffusion operator is defined as $U_s = 2\,|\psi\rangle\langle\psi| - I$. Geometrically, this is a reflection about the vector $|\psi\rangle$. When we apply U_s to Equation (9):

- The component parallel to $|\psi\rangle$ remains unchanged.
- The component orthogonal to $|\psi\rangle$ (i.e., $|\bar{\psi}\rangle$) gets flipped.

$$\begin{aligned} G\,|\psi\rangle &= U_s(\cos 2\theta\,|\psi\rangle - \sin 2\theta\,|\bar{\psi}\rangle) \\ &= \cos 2\theta\,|\psi\rangle - \sin 2\theta(-\,|\bar{\psi}\rangle) \\ &= \cos 2\theta\,|\psi\rangle + \sin 2\theta\,|\bar{\psi}\rangle \end{aligned}$$

3.3 Step 3: Calculating the Total Rotation (The 3θ Term)

We have established that one Grover iteration rotates the state by 2θ relative to the start state. Let us convert this back to the $|\text{good}\rangle, |\text{bad}\rangle$ basis to see the new amplitude.

Substituting $|\psi\rangle$ and $|\bar{\psi}\rangle$ back into the equation:

$$\begin{aligned}|\psi_1\rangle &= \cos 2\theta(\sin\theta\,|\text{good}\rangle + \cos\theta\,|\text{bad}\rangle) + \sin 2\theta(\cos\theta\,|\text{good}\rangle - \sin\theta\,|\text{bad}\rangle) \\ &= (\sin\theta\cos 2\theta + \cos\theta\sin 2\theta)\,|\text{good}\rangle + (\cos\theta\cos 2\theta - \sin\theta\sin 2\theta)\,|\text{bad}\rangle\end{aligned}$$

We use the angle addition formulas:

- $\sin(A+B) = \sin A\cos B + \cos A\sin B$
- $\cos(A+B) = \cos A\cos B - \sin A\sin B$

Setting $A = \theta$ and $B = 2\theta$, we obtain:

$$|\psi_1\rangle = \sin(3\theta)\,|\text{good}\rangle + \cos(3\theta)\,|\text{bad}\rangle \tag{10}$$

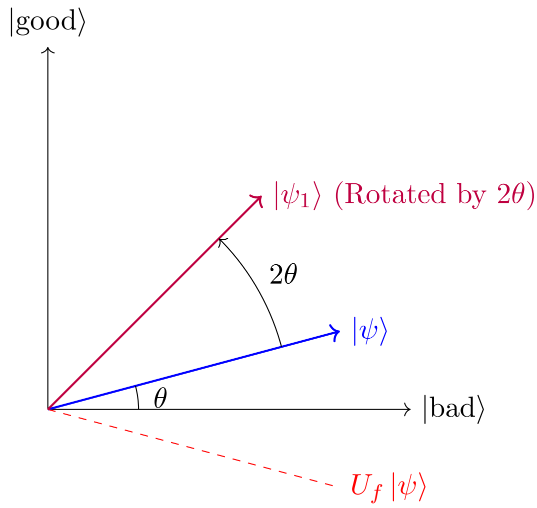

Figure 1: Geometric interpretation of one Grover Iteration. The state is rotated by 2θ towards $|\text{good}\rangle$.

4 Complexity and Convergence

By induction, applying the Grover iterator k times results in the state:

$$|\psi_k\rangle = \sin((2k+1)\theta)\,|\text{good}\rangle + \cos((2k+1)\theta)\,|\text{bad}\rangle \tag{11}$$

The probability of measuring a solution is $P_k = \sin^2((2k+1)\theta)$.

4.1 Optimal Iterations

We wish to stop when the probability is maximal, i.e., $(2k+1)\theta \approx \pi/2$.

$$k \approx \frac{\pi}{4\theta} - \frac{1}{2} \tag{12}$$

Assuming $N \gg M$, $\theta \approx \sin\theta = \sqrt{M/N}$. This yields the complexity:

$$k \approx \frac{\pi}{4}\sqrt{\frac{N}{M}} = O(\sqrt{N}) \tag{13}$$

5 Error Analysis and Bounds

A crucial question is what happens if the optimal k is not an integer. Let $\tilde{k}$ be the exact real number that satisfies $(2\tilde{k}+1)\theta = \pi/2$. Let $\bar{k}$ be the closest integer to $\tilde{k}$.

$$|\bar{k} - \tilde{k}| \leq \frac{1}{2} \tag{14}$$

5.1 Probability of Failure

If we iterate $\bar{k}$ times, the probability of *not* observing a solution (failure) is given by the cosine component squared:

$$P(\text{fail}) = \cos^2((2\bar{k}+1)\theta) \tag{15}$$

We can substitute $(2\bar{k}+1)\theta$ by utilizing the deviation from the optimal angle:

$$\begin{aligned}
(2\bar{k}+1)\theta &= (2\tilde{k} + 2(\bar{k}-\tilde{k}) + 1)\theta \\
&= (2\tilde{k}+1)\theta + 2(\bar{k}-\tilde{k})\theta \\
&= \frac{\pi}{2} + 2(\bar{k}-\tilde{k})\theta
\end{aligned}$$

Substituting this back into the failure probability:

$$\begin{aligned}
P(\text{fail}) &= \cos^2\left(\frac{\pi}{2} + 2(\bar{k}-\tilde{k})\theta\right) \\
&= \sin^2(2(\bar{k}-\tilde{k})\theta)
\end{aligned}$$

Since $|\bar{k}-\tilde{k}| \leq 1/2$, the argument of the sine function is bounded by θ:

$$|2(\bar{k}-\tilde{k})\theta| \leq \theta \tag{16}$$

Using the inequality $\sin x \leq x$ for small x, and specifically here $\sin^2(\theta) = M/N$:

$$P(\text{fail}) \leq \sin^2(\theta) = \frac{M}{N} \tag{17}$$

6 Conclusion

Grover's algorithm successfully rotates the initial state vector from the superposition of all states towards the solution states.

1. It provides a quadratic speedup over classical search.
2. Even with discrete iteration steps, the error is bounded by M/N, which is negligible for large N.