CS 506 : Quantum Computing

Scribe : Rujuta Tambewagh

December 1, 2025

1 Introduction and Problem Setup

The goal of Grover's search is to find a unique solution x^* in an unstructured database of size $N = 2^n$ with quadratic speedup, requiring $O(\sqrt{N})$ queries.

- $N = 2^n$, where $n = \log_2 N$.
- Given a black box function $f : \{0,1\}^n \to \{0,1\}$.
- There are t possible x^* such that $f(x^*) = 1$. Assume t is known.
- We can find x^* with probability $\geq \frac{t}{N}$.

1.1 Geometric Basis States

The analysis takes place in the 2D subspace spanned by the "good" (solution) and "bad" (non-solution) states:

$$|good\rangle = \frac{1}{\sqrt{t}} \sum_{x:f(x)=1} |x\rangle$$

$$|bad\rangle = \frac{1}{\sqrt{N-t}} \sum_{x:f(x)=0} |x\rangle$$

2 Trigonometric and Geometric Formalism

The uniform initial state $|\psi\rangle$ is written in the 2D subspace as:

$$|\psi\rangle = \sqrt{\frac{t}{N}}|good\rangle + \sqrt{\frac{N-t}{N}}|bad\rangle = \sin\theta|good\rangle + \cos\theta|bad\rangle$$

where the amplitude rotation angle is:

$$\sin\theta = \sqrt{\frac{t}{N}} \quad \text{and} \quad \theta = \arcsin\sqrt{\frac{t}{N}}$$

2.1 State After k Iterations

After the k-th Grover's iterate, the state rotates towards the $|good\rangle$ subspace:

$$|\psi_k\rangle = \sin((2k+1)\theta)|good\rangle + \cos((2k+1)\theta)|bad\rangle$$

The probability of success is $Pr[\text{observing a state in } |good\rangle] = \sin^2((2k+1)\theta)$.

We maximize the probability $P_k = \sin^2((2k+1)\theta)$ by setting the angle equal to the maximal value:

$$\begin{aligned}(2k+1)\theta &= \frac{\pi}{2} \\ 2k+1 &= \frac{\pi}{2\theta} \\ 2k &= \frac{\pi}{2\theta} - 1 \\ k &\approx \frac{\pi}{4\theta} - \frac{1}{2}\end{aligned}$$

Since k must be an integer, k is chosen as the closest integer to this value.

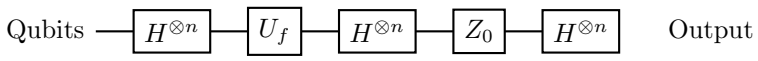
2.2 Optimal Iterations

The optimal number of iterations k is chosen as the closest integer to maximize probability:

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

2.3 Circuit Structure

The Grover iteration circuit, often labeled as the Kth iterate, is composed of the Oracle U_f and the Diffusion Operator U_s, where U_s is implemented by Hadamard gates (H) and a phase-flip operator (Z_0):



3 Recurrence Relations and Inductive Proof

3.1 Recurrence Setup (The Alternative Proof)

The state $|\psi_k\rangle$ can be written in terms of amplitudes a_k and b_k over the computational basis:

$$|\psi_k\rangle = a_k \sum_{x:f(x)=1} |x\rangle + b_k \sum_{x:f(x)=0} |x\rangle$$

The state must satisfy the normalization condition: $t|a_k|^2 + (N-t)|b_k|^2 = 1$. The initial coefficients are $a_0 = \frac{1}{\sqrt{N}}$ and $b_0 = \frac{1}{\sqrt{N}}$.

3.1.1 Grover Recurrence Equations

The application of the Grover operator leads to the following linear recurrence relations for a_{k+1} and b_{k+1}:

$$\begin{aligned} a_{k+1} &= \frac{N-2t}{N} a_k + \frac{2(N-t)}{N} b_k \\ b_{k+1} &= \frac{-2t}{N} a_k + \frac{N-2t}{N} b_k \end{aligned}$$

The a_{k+1} relation is derived from the reflection formula for U_s:

$$a_{k+1} = 2\left(\frac{t(-a_k) + (N-t)b_k}{N}\right) - (-a_k)$$

which simplifies to:

$$a_{k+1} = \left(1 - \frac{2t}{N}\right) a_k + \frac{2(N-t)}{N} b_k$$

3.1.2 Goal:

Show that the closed-form solution satisfies the recurrence:

$$a_k = \frac{1}{\sqrt{t}} \sin((2k+1)\theta)$$

3.2 Verification using Trigonometric Substitution

Substituting the proposed closed-form solutions a_k and b_k into the recurrence for a_{k+1}:

$$a_{k+1} = \frac{N-2t}{N}\left(\frac{1}{\sqrt{t}} \sin((2k+1)\theta)\right) + \frac{2(N-t)}{N}\left(\frac{1}{\sqrt{N-t}} \cos((2k+1)\theta)\right)$$

Using the trigonometric identity substitutions ($\cos 2\theta = 1 - 2\sin^2\theta$, etc.):

$$\begin{aligned} a_{k+1} &= \frac{1}{\sqrt{t}}\left[(1-2\sin^2\theta)\sin((2k+1)\theta) + 2\sin\theta\cos\theta\cos((2k+1)\theta)\right] \\ &= \frac{1}{\sqrt{t}}\left[\cos(2\theta)\sin((2k+1)\theta) + \sin(2\theta)\cos((2k+1)\theta)\right] \\ &= \frac{1}{\sqrt{t}}\sin((2k+1)\theta + 2\theta) \\ &= \frac{1}{\sqrt{t}}\sin((2k+3)\theta) \end{aligned}$$

This verifies the closed-form solution for the $(k+1)$-th iteration.

4 Matrix Implementation and Inductive Proof for U_s

The Diffusion Operator is $U_s = H^{\otimes n} Z_0 H^{\otimes n}$, which must equal the claimed general form:

$$U_s = \left[\frac{2}{N}\right] - I_N$$

4.1 Basis Case: $n = 1$

The explicit unitary matrix forms for the $n = 1$ basis ($N = 2$):

$$H = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} \end{pmatrix} \quad \text{and} \quad Z_0 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

The calculation of $U_s = HZ_0H$ yields:

$$HZ_0H = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

This result is equivalent to the general form for $N = 2$:

$$\left[\frac{2}{N}\right] - I_2 = \begin{pmatrix} \frac{2}{2} & \frac{2}{2} \\ \frac{2}{2} & \frac{2}{2} \end{pmatrix} - \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

4.2 Multi-Qubit Hadamard ($\mathbf{H}^{\otimes n}$)

The matrix for n qubits is built using the tensor product. For $n = 2$, the 4×4 matrix is:

$$\mathbf{H}^{\otimes 2} = H \otimes H = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

4.3 Inductive Step Setup

Claim: $H^{\otimes n} Z_0 H^{\otimes n} = \left[\frac{2}{N}\right] - I_N$

- **Basis:** $n = 1$ is proved above.
- **Assumption (for $n-1$):** Assume the claim is true for $n-1$:

$$H^{\otimes n-1} Z_0 H^{\otimes n-1} = \left[\frac{2}{(N/2)}\right] - I_{N/2} \quad (N/2 \times N/2 \text{ matrix})$$

- **Goal:** Prove the claim for n (an $N \times N$ matrix).