CS 506 Quantum Computing Fall 2025

November 17th, 2025

Lecturer: Bhaskar DasGupta *Scribe: Brian Rosca*

1 Problem Statement

Let $N = 2^n$. Given a black box function $f : \{0,1\}^n \to \{0,1\}$, find x^* such that $f(x^*) = 1$.

- Assumption: There exists exactly one solution x^*.
- Complexity: The algorithm uses $O(\sqrt{N})$ queries to f and $O(\sqrt{N}\log N)$ gates.

2 The Oracle Gate U_f

We define the oracle U_f acting on $n+1$ qubits:

$$U_f|x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle$$

Phase Kickback Mechanism: Using an auxiliary qubit in state $|-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$:

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

This creates a phase flip specifically for the solution x^*:

- If $x = x^*$: $U_f|x^*\rangle \to -|x^*\rangle$
- If $x \neq x^*$: $U_f|x\rangle \to |x\rangle$

Sometimes denoted as $O_f^{\pm}$.

3 Grover's Diffusion Operator D

The diffusion operator performs an "inversion about the mean."

$$D : \sum_x \alpha_x|x\rangle \longrightarrow \sum_x (2\mu - \alpha_x)|x\rangle$$

Where μ is the mean of all amplitudes: $\mu = \frac{1}{N}\sum_x \alpha_x$.

3.1 Proof of Unitary (Norm Preservation)

Let the state be $|\psi\rangle = \sum \alpha_x |x\rangle$ with $\sum |\alpha_x|^2 = 1$.

$$\begin{aligned}
\left\| \sum (2\mu - \alpha_x)|x\rangle \right\|^2 &= \sum_x (2\mu - \alpha_x)^2 \\
&= \sum_x (4\mu^2 - 4\mu\alpha_x + \alpha_x^2) \\
&= 4\mu^2 N - 4\mu \underbrace{\left(\sum_x \alpha_x \right)}_{N\mu} + \underbrace{\sum_x \alpha_x^2}_{1} \\
&= 4N\mu^2 - 4N\mu^2 + 1 \\
&= 1
\end{aligned}$$

4 Implementation of D

The diffusion operator is defined structurally as:

$$D = H^{\otimes n} Z_0 H^{\otimes n}$$

Where Z_0 is a conditional phase shift operator:

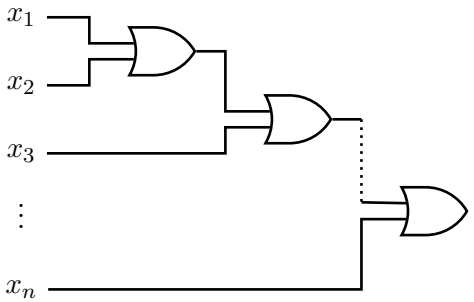
$$Z_0|x\rangle = \begin{cases} +|x\rangle & \text{if } x = 0\ldots0 \\ -|x\rangle & \text{otherwise} \end{cases}$$

In Dirac notation (Reflection about $|0\rangle$):

$$Z_0 = 2|0\ldots0\rangle\langle 0\ldots0| - I$$

4.1 Logical Implementation of Z_0

To implement Z_0, we need a circuit that applies a -1 phase if any bit is 1. This is equivalent to applying a phase if $(x_1 \vee x_2 \vee \cdots \vee x_n)$ is true.



If $\bigvee x_i, ..., x_n = 0$ (all inputs 0), phase is $+1$. If $\bigvee x_i = 1$ (any input 1), phase is -1.

4.2 Mathematical derivation of $D = 2|+\rangle\langle+| - I$

Using the identity $H^{\otimes n}|0\rangle = |+\rangle$:

$$\begin{aligned} D &= H^{\otimes n} Z_0 H^{\otimes n} \\ &= H^{\otimes n}(2|0\rangle\langle 0| - I)H^{\otimes n} \\ &= 2(H^{\otimes n}|0\rangle)(\langle 0|H^{\otimes n\dagger}) - H^{\otimes n} I H^{\otimes n} \\ &= 2|+\rangle\langle+| - I \end{aligned}$$

Applying this to a general state $|\psi\rangle$:

$$D|\psi\rangle = 2|+\rangle\langle+|\psi\rangle - |\psi\rangle$$

Noting that $\langle+|\psi\rangle = \frac{1}{\sqrt{N}}\sum_x \alpha_x = \sqrt{N}\mu$:

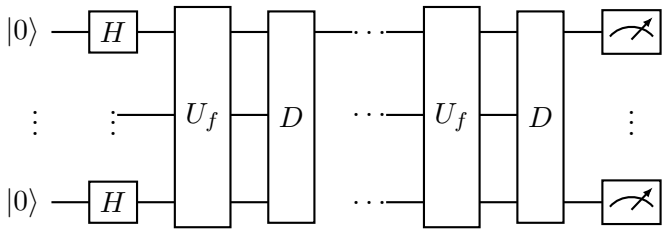
$$D|\psi\rangle = 2|+\rangle(\sqrt{N}\mu) - |\psi\rangle = \sum_x (2\mu)\frac{|x\rangle}{\sqrt{N}}\sqrt{N} - \sum_x \alpha_x|x\rangle = \sum_x (2\mu - \alpha_x)|x\rangle$$

5 Recursion and Amplitude Analysis

Claim: Using $\approx \frac{\sqrt{N}}{8}$ queries, we identify x^* with probability > 0.1.

5.1 Grover Iteration Circuit

We perform t steps of the sequence $D \cdot U_f$.



5.2 Amplitude Update Rule

Let the state at step t be $|\psi^{(t)}\rangle = \alpha^{(t)}|x^*\rangle + \sum_{x\neq x^*}\beta^{(t)}|x\rangle$.

1. **Apply Oracle U_f:** The amplitude of the marked state flips:

$$\alpha^{(t)} \xrightarrow{U_f} -\alpha^{(t)}, \quad \beta^{(t)} \xrightarrow{U_f} \beta^{(t)}$$

2. **Calculate Mean $M^{(+)}$:** The mean of the amplitudes *after* the oracle flip is:

$$M^{(+)} = \frac{1}{N}\left(-\alpha^{(t)} + (N-1)\beta^{(t)}\right)$$

3. **Apply Diffusion D (Reflection):** The operator maps amp $x \to 2M^{(+)} - x$.

$$\begin{aligned} \alpha^{(t+1)} &= 2M^{(+)} - (-\alpha^{(t)}) = 2M^{(+)} + \alpha^{(t)} \\ \beta^{(t+1)} &= 2M^{(+)} - \beta^{(t)} \end{aligned}$$

Initialization ($t = 0$):

$$\alpha^{(0)} = \beta^{(0)} = \frac{1}{\sqrt{N}}$$

By iterating this process, α is amplified while β diminishes.