CS 506: An Introduction to Quantum Computing

Scribe: Zhenghao Zhao

Date: November 19, 2025

Grover's Search Problem

The goal of Grover's algorithm is to solve the unstructured search problem. Suppose we are given a large database of N items, and we want to find a specific item that satisfies a certain condition. In the classical setting, checking items one by one requires $O(N)$ queries in the worst case. Grover's algorithm provides a quadratic speedup, requiring only $O(\sqrt{N})$ queries.

Formally, we are given a black-box function (or oracle)

$$f : \{0, 1, \dots, N - 1\} \to \{0, 1\}, \tag{1}$$

which returns 1 if the input is the solution we are looking for, and 0 otherwise. We assume that there exists a unique marked element x^* such that

$$f(x^*) = 1. \tag{2}$$

For the sake of simpler analysis, let us assume the search space size N is a power of 2:

$$N = 2^n, \qquad n = \log_2 N, \tag{3}$$

where n represents the number of qubits required to index the database.

Initial State

The algorithm begins by initializing the quantum system in the state of all zeros:

$$|0\rangle^{\otimes n}. \tag{4}$$

To search the entire space simultaneously, we create a uniform superposition over all possible basis states. This is achieved by applying the Hadamard transform $H^{\otimes n}$ to the initial state:

$$\left|\psi^{(0)}\right\rangle = H^{\otimes n} |0\rangle^{\otimes n} = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle. \tag{5}$$

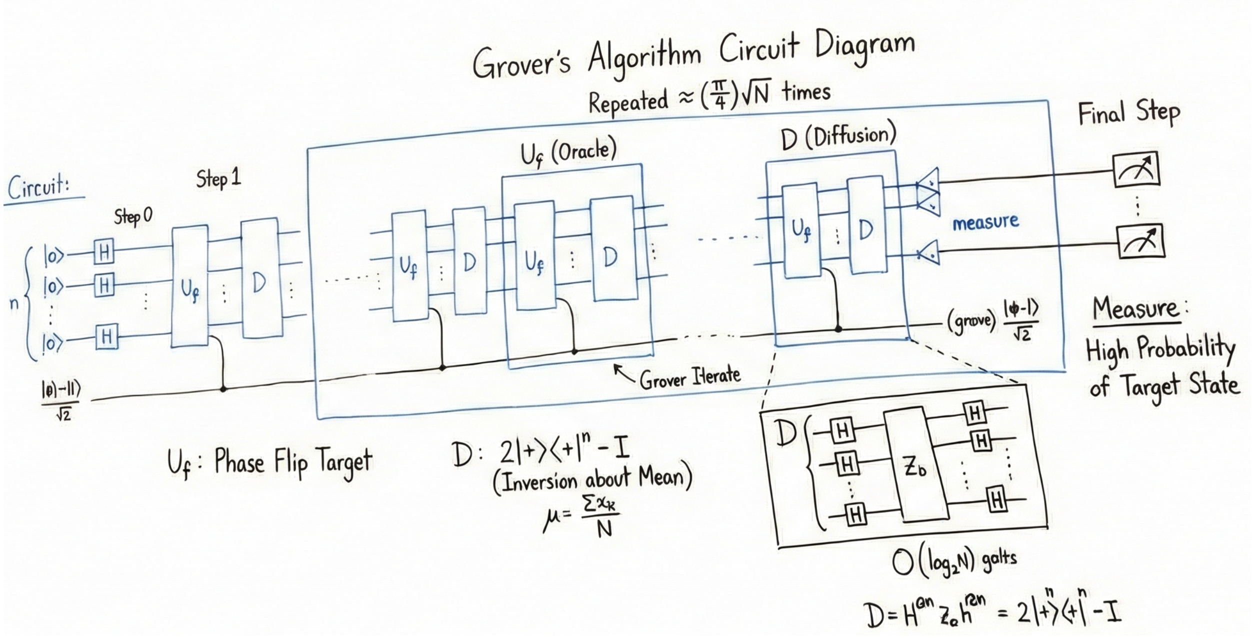

Figure 1: Grover Circuit

It is useful to decompose this state into two components: the amplitude associated with the solution x^* and the amplitudes associated with all other non-solution states. We can write:

$$\left|\psi^{(0)}\right\rangle = \frac{1}{\sqrt{N}} \left|x^*\right\rangle + \frac{1}{\sqrt{N}} \sum_{x \neq x^*} \left|x\right\rangle = \alpha^{(0)} \left|x^*\right\rangle + \beta^{(0)} \sum_{x \neq x^*} \left|x\right\rangle . \tag{6}$$

Initially, the probability is distributed equally, so the amplitudes are identical:

$$\alpha^{(0)} = \beta^{(0)} = \frac{1}{\sqrt{N}}. \tag{7}$$

Oracle Application

The core of the algorithm involves repeated queries to the quantum oracle U_f. This operator identifies the solution state $|x^*\rangle$ not by measuring it, but by flipping its phase. The action of the oracle is defined as:

$$U_f \left|x^*\right\rangle = -\left|x^*\right\rangle , \tag{8}$$

$$U_f \left|x\right\rangle = \left|x\right\rangle , \quad x \neq x^*. \tag{9}$$

Applying this oracle to our superposition state flips the sign of the amplitude for the marked item, while leaving the others unchanged:

$$\left|\psi^{(1)}\right\rangle = -\alpha^{(0)} \left|x^*\right\rangle + \beta^{(0)} \sum_{x \neq x^*} \left|x\right\rangle . \tag{10}$$

This phase flip distinguishes the target state from the rest, though it does not yet increase the probability of measuring it.

Diffusion Operator

To convert the phase difference into a magnitude difference (which can be measured), we apply the Grover diffusion operator. This operator performs an ”inversion about the mean.”

First, define the average amplitude of the system at time t:

$$\mu^{(t)} = \frac{1}{N}\left(\alpha^{(t)} + (N-1)\beta^{(t)}\right). \tag{11}$$

The diffusion operator transforms each amplitude x into $2\mu - x$. The update rules for the amplitudes are:

$$\alpha^{(t+1)} = 2\mu^{(t)} - \alpha^{(t)}, \tag{12}$$

$$\beta^{(t+1)} = 2\mu^{(t)} - \beta^{(t)}. \tag{13}$$

Because the marked amplitude α was made negative by the oracle, it is far below the mean. Reflecting it across the mean results in a large positive amplitude, thereby amplifying the probability of finding the solution. This combination of the Oracle and Diffusion operator constitutes one Grover iteration.

Two-Dimensional Subspace and Angle Representation

A key insight in analyzing Grover's algorithm is that the state vector is always confined to a two-dimensional subspace spanned by the starting superposition of ”good” (solution) and ”bad” (non-solution) states.

Let us define the normalized basis vectors for this subspace:

$$|\psi_{\text{good}}\rangle = |x^*\rangle, \tag{14}$$

$$|\psi_{\text{bad}}\rangle = \frac{1}{\sqrt{N-1}}\sum_{x\neq x^*}|x\rangle. \tag{15}$$

We can rewrite the initial uniform superposition $\left|\psi^{(0)}\right\rangle$ in this basis using an angle θ:

$$\left|\psi^{(0)}\right\rangle = \frac{1}{\sqrt{N}}|\psi_{\text{good}}\rangle + \sqrt{\frac{N-1}{N}}|\psi_{\text{bad}}\rangle = \sin\theta\,|\psi_{\text{good}}\rangle + \cos\theta\,|\psi_{\text{bad}}\rangle, \tag{16}$$

where θ is determined by the size of the database:

$$\sin\theta = \frac{1}{\sqrt{N}}, \qquad \theta \approx \frac{1}{\sqrt{N}}. \tag{17}$$

Geometrically, the Grover iteration $G = DU_f$ rotates the state vector in this 2D plane towards $|\psi_{\text{good}}\rangle$ by an angle of 2θ. After t iterations, the state becomes:

$$\left|\psi^{(t)}\right\rangle = \sin((2t+1)\theta)\,|\psi_{\text{good}}\rangle + \cos((2t+1)\theta)\,|\psi_{\text{bad}}\rangle. \tag{18}$$

Amplitude Inequalities and Convergence Analysis

We can rigorously show that the probability of success increases with each step. First, normalization implies the total probability must sum to 1:

$$1 = (\alpha^{(t)})^2 + (N-1)(\beta^{(t)})^2. \tag{19}$$

Assume we are in the early stages of the algorithm where the amplitude of the solution is still relatively small, i.e., $|\alpha^{(t)}| \leq \frac{1}{2}$ (assuming $N \geq 4$). Then the total probability mass of the incorrect states is:

$$(N-1)(\beta^{(t)})^2 = 1 - (\alpha^{(t)})^2 \geq \frac{3}{4}, \tag{20}$$

which implies a lower bound on the unmarked amplitudes:

$$\beta^{(t)} \geq \sqrt{\frac{3}{4(N-1)}}. \tag{21}$$

The average amplitude $\mu^{(t)}$ is dominated by the many small β terms. We can bound it as:

$$\mu^{(t)} = \frac{-\alpha^{(t)} + (N-1)\beta^{(t)}}{N} \geq \frac{1}{\sqrt{N}}. \tag{22}$$

Substituting this into the diffusion update rule, we see the growth of the solution amplitude:

$$\alpha^{(t+1)} = 2\mu^{(t)} - \alpha^{(t)} \tag{23}$$

$$\geq \alpha^{(t)} + \frac{1}{\sqrt{N}}. \tag{24}$$

This result states that in each iteration, the amplitude of the marked element increases by at least $1/\sqrt{N}$, provided we haven't overshot the target yet.

Stopping Condition

Using the recurrence derived above, we can estimate the number of steps required. After t steps:

$$\alpha^{(t)} \geq \alpha^{(0)} + \frac{t}{\sqrt{N}} = \frac{1}{\sqrt{N}} + \frac{t}{\sqrt{N}}. \tag{25}$$

If we choose the number of iterations to be $t = \frac{\sqrt{N}}{8}$, the amplitude becomes:

$$\alpha^{(t)} \geq \frac{1}{\sqrt{N}} + \frac{1}{8} \approx \frac{1}{8}. \tag{26}$$

Consequently, the probability of measuring the correct state $|x^*\rangle$ is:

$$P(\text{success}) = |\alpha^{(t)}|^2 \geq \left(\frac{1}{8}\right)^2 = \frac{1}{64} \approx 0.015. \tag{27}$$

While 1.5% seems low, it is significantly higher than the $1/N$ probability of random guessing.

Boosting Success Probability

To achieve a high probability of success, we do not need to run the quantum circuit longer (which risks over-rotation). Instead, we can simply repeat the entire experiment (run the circuit with $t \approx \sqrt{N}/8$ and measure) multiple times.

Suppose we repeat the experiment 110 times. The probability of failing to find the solution in a single run is at most $1 - 0.015 = 0.985$ (conservatively using 0.99). The probability of failing all 110 times is:

$$\Pr(\text{no success in 110 trials}) = (0.99)^{110} \leq \frac{1}{3}. \tag{28}$$

Thus, the probability of finding the solution at least once is:

$$\Pr(\text{success at least once}) = 1 - (0.99)^{110} \geq \frac{2}{3}. \tag{29}$$

This confirms that with $O(\sqrt{N})$ quantum queries and constant classical repetitions, we can find the marked element with high probability.