Grover's Algorithm

2025-07-07

Grover's search algorithm represents one of the most significant achievements in quantum computing, providing a quadratic speedup for searching unsorted databases. While classical algorithms require O(N) operations to find a specific item among N entries, Grover's algorithm accomplishes this task in just O($\sqrt{N}$) operations. This article explores the mathematical foundations of the algorithm, including the oracle function, diffusion operator, and the geometric interpretation of quantum state rotations in Hilbert space. The algorithm's elegance lies in its systematic amplification of the target state's amplitude through repeated applications of oracle and diffusion operations, demonstrating quantum computing's practical advantages for search problems.

blog: https://tetraquark.vercel.app/posts/quantum_grover/?src=pdf

email: quarktetra@gmail.com

Basic Elements of Quantum Algorithms

The most basic element of a QC is a quantum bit, qubit for short, which is a two-level quantum system. It spans a two-dimensional Hilbert space denoted as H_2. H_2 is equipped with a fixed basis $(|0\rangle, |1\rangle)$, a so-called computational basis. States $|0\rangle$ and $|1\rangle$ are called the basis states. A general state of a single quantum bit is a vector that can be written as:

$$c_0|0\rangle + c_1|1\rangle, \tag{1}$$

where $|c_0|^2 + |c_1|^2 = 1$

We can extend this definition to multiple qubits: for example, a system of two qubits describes a four-dimensional Hilbert space $H_4 = H_2 \otimes H_2$ having an orthonormal basis $(|00\rangle, |01\rangle, |10\rangle, |11\rangle)$. A state of a two-qubit system is a unit-length vector

$$c_0|00\rangle + c_1|01\rangle + c_2|10\rangle + c_3|11\rangle, \tag{2}$$

with $|c_0|^2 + |c_1|^2 + |c_2|^2 + |c_3|^2 = 1$.

One of the most important gates in QC is the Hadamard gate, denoted by H, and it is defined as follows:

$$H|\mathbf{x}\rangle = \frac{1}{\sqrt{2}} \sum_{\mathbf{y}} (-1)^{\mathbf{x}.y} |\mathbf{y}\rangle \tag{3}$$

Applying H to the computational basis we get

$$\begin{aligned} H|0\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \\ H|1\rangle &= \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \end{aligned} \tag{4}$$

The Hadamard gate basically creates superpositions out of pure states, and it can also be written in matrix form as follows:

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \tag{5}$$

Using Hadamard transformations along with phase shift operations, one can implement the quantum Fourier transform (QFT), which is basically the classical discrete Fourier transform applied to the quantum state vector:

$$QFT|x\rangle = \frac{1}{\sqrt{N}} \sum_{y=1}^{N-1} e^{\frac{-2\pi i x.y}{N}} |y\rangle \tag{6}$$

This transformation is a key element in many quantum algorithms, including Shor's factorization algorithm.

Grover's Algorithm

Grover's search algorithm enables a QC to find a specific item in an unsorted database of N entries using $\mathcal{O}(\sqrt{N})$ operations whereas a classical algorithm would require $\mathcal{O}(N)$ operations.

Consider a database with N entries, one of which is the target entry. The goal is to find the index of that particular entry with the least number of queries. The database can be treated as a black box, which is usually referred to as an *oracle*, that calculates a simple function:

$$f(x) = \begin{cases} 1 & x = w \\ 0 & x \neq w, \end{cases} \tag{7}$$

where w is the entry we are trying to locate. We are going to feed a state $|x\rangle|q\rangle$ into the oracle where x represents the index we are querying and q is an ancillary bit which will be used by the oracle to return the query result. If we hit the index of the special entry, i.e. $x = w$, the oracle will flip the ancillary bit, otherwise it will return the same value1. So mathematically, what the oracle is doing is the following transformation:

$$|x\rangle|q\rangle \rightarrow |x\rangle|f(x) \oplus q\rangle. \tag{8}$$

Here are the steps of the algorithm:

1. Prepare a uniform superposition of numbers 0 to $N-1$: $|s\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle$,
2. Append the ancillary bit $|q\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$,
3. Feed this input to the oracle,
4. Apply the Grover diffusion operator $2|s\rangle\langle s| - I$,
5. Return to Step 3 and repeat $\sqrt{N}$ times,
6. Measure the output.

The algorithm steps are illustrated below:

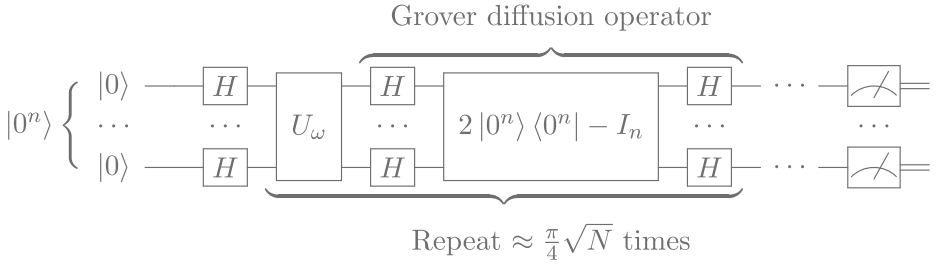

Figure 1: Grover's search algorithm circuit Wikipedia.

Note that we are feeding in all of the possible indices at once, so the special index w is indeed fed into the oracle. However, it is just one of the N states appearing in the input. With no clever algorithm, the output will also be in a superposition of N states. It will collapse into one of them when a measurement is done. The probability of this state being the correct one is just $1/N$, just like in the classical case. A QC's ability to process all inputs at once is not

useful unless you can sift through the output using a good algorithm. To understand how Grover's algorithm enhances the chances of getting the correct output, let's take a look at what the oracle returns for that particular input: $x = w$ and $|q\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$. Using Eq. 8, we get:

$$|w\rangle|q\rangle = |w\rangle\frac{|0\rangle - |1\rangle)}{\sqrt{2}} \rightarrow |w\rangle\frac{|1 \oplus 0\rangle - |1 \oplus 1\rangle}{\sqrt{2}} = |w\rangle\frac{|1\rangle - |0\rangle}{\sqrt{2}} = -|w\rangle|q\rangle, \tag{9}$$

which is simply the negative of the input value. One can repeat the same calculation and show that when $x \neq w$, the oracle output is equal to its input. Based on these two observations, we can define the effect of the oracle in the operator form:

$$U_w = I - |w\rangle\langle w|, \tag{10}$$

which is easy to understand: if the object it operates on has $|w\rangle$ content, then the sign on that component will be flipped. Let's apply the oracle operation U_w to the uniform superposition $|s\rangle$:

$$U_w|s\rangle \quad = (I - |w\rangle\langle w|)|s\rangle = |s\rangle - \tfrac{2}{\sqrt{N}}|w\rangle. \tag{11}$$

The diffusion operation, $U_s = 2|s\rangle\langle s| - I$ will act on the state in Eq. 11 to yield

$$U_s U_w|s\rangle \quad = \quad (2|s\rangle\langle s| - I)(|s\rangle - \frac{2}{\sqrt{N}}|w\rangle) = \frac{N-4}{N}|s\rangle + \frac{2}{\sqrt{N}}|w\rangle, \tag{12}$$

which shows the ingenuity of the algorithm: the amplitude of the state $|w\rangle$ increased from $1/\sqrt{N}$ to $\frac{2}{\sqrt{N}}$ in one iteration. In fact, if $N = 4$, the amplitude becomes 1, which means that Grover's algorithm can locate the special entry out of four in a single iteration with 100% probability. For larger N, you need to keep iterating $U_s U_w$ operations $\sqrt{N}$ times to enhance the amplitude of $|w\rangle$. At each step of the iteration, you are moving the output state closer to the state represented by $|w\rangle$. The operations can be visualized as rotations in Hilbert space of quantum states as illustrated below.

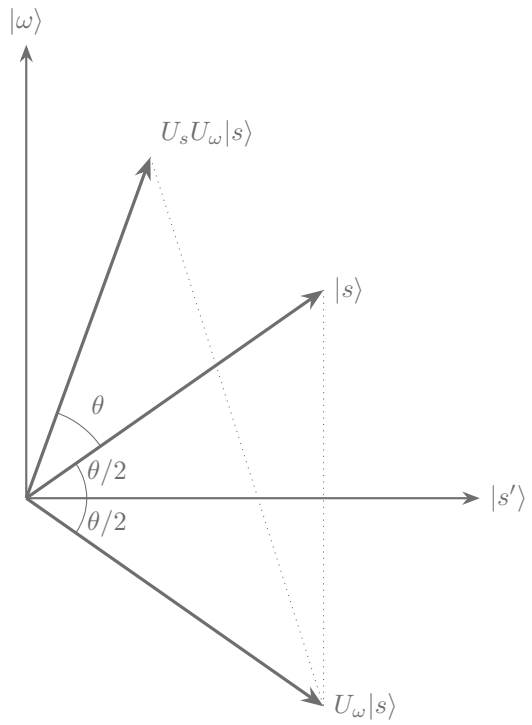

Figure 2: The rotations involved in the search algorithm.

1 You may ask why we simply do not return 1 or 0 depending on $x = w$. This is because all the operations in QC have to be reversible. If the oracle overwrote $|q\rangle$ with 0 or 1, the previous information on $|q\rangle$ would not be recoverable. This is also the reason why there is no quantum AND gate: one cannot uniquely recover the inputs of the AND gate from its output.