Grover's Algorithm

Omar Hussein, Moustafa Elsayed, Walid El Maouaki

April 2020

1 Introduction

Grover's algorithm solves the problem of unstructured search, which is simply finding a specific item in a given database. Classically, this problem is solved in N steps; however, it is solved quantum mechanically in $\sqrt{N}$ steps. In this simple report, we will state the motivation of the idea from a physics point of view and the details of the algorithm. We will also explain our design of the 8-qubits circuit as we go through the details of the algorithm.

2 Motivation

The idea behind the algorithm is really simple: physical systems tend to move toward the lowest potential. Surprisingly, this simple law is also true in the bizarre world of quantum mechanics. To elaborate more, any minimum point in a given potential can be approximated as a harmonic oscillator through Taylor expansion; thus, studying the harmonic oscillator alone may verify the simple idea that physical systems tend to go to the lowest potential. If you made a simple simulation where your wavefunction is made of a superposition of different states, you will notice that the maxima of your probability density function always oscillates around the minimum point in the harmonic oscillator. You can verify this by yourself through this nice website: https://physics.weber.edu/schroeder/software/HarmonicOscillator.html .

Based on this simple idea, we need to think of certain gates that acts as an analogy for the evolution of the wavefunctions depending on Schrodinger equation. To think of these gates, we may discretize Schrodinger's equation to derive a matrix form that later can be modified to our quantum gates. First, discretizing our Schrodinger equation and considering only a finite number of states provides us with the following matrix that describes the evolution of the wavefunction in an infinitesimal time (We are skipping the details since it is not our main focus; however, you can ask us anytime to make sure that we understand it):

$$\psi(t+dt) = DR\psi(t) \tag{1}$$

$$\psi(\tau) = (DR)^n\psi(t) \tag{2}$$

Where,

$$D = \begin{bmatrix} 1-2i\epsilon & i\epsilon & 0 & i\epsilon \\ i\epsilon & 1-2i\epsilon & i\epsilon & 0 \\ 0 & i\epsilon & 1-2i\epsilon & i\epsilon \\ i\epsilon & 0 & i\epsilon & 1-2i\epsilon \end{bmatrix} \tag{3}$$

$$R = \begin{bmatrix} exp(-iV(x_1)dt) & 0 & 0 & 0 \\ 0 & exp(-iV(x_2)dt) & 0 & 0 \\ 0 & 0 & exp(-iV(x_3)dt) & 0 \\ 0 & 0 & 0 & exp(-iV(x_4)dt) \end{bmatrix} \tag{4}$$

Notice that the R corresponds to the operator that involves the effect of our potential. This operator will be used to derive the inversion operator, which flips the sign of the amplitude of the state we want to find. The inversion operator will be discussed in the next section. The D operator is responsible for the increase of the amplitude of the wanted state, and it of course reduces the amplitudes of the other states since the probability should be always equal to 1. The D operator will be used to derive the Grover's diffusion operator that we will discuss later. Note that we won't get into the derivations; however, we will state the result with all its implications and exact function. We will also mention how such gates are constructed. In conclusion of this section,we will state the modified D and R that are used in Grover's Algorithm. It is important to note from the -1 in the second row and from its dimension that the following operators function on 4 states where the second one is the one we want to find. Note also that $N = 2^n$ where n is the number of qubits.

$$R = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \tag{5}$$

$$D = \begin{bmatrix} -1+2/N & 2/N & 2/N & 2/N \\ 2/N & -1+2/N & 2/N & 2/N \\ 2/N & 2/N & -1+2/N & 2/N \\ 2/N & 2/N & 2/N & -1+2/N \end{bmatrix} \tag{6}$$

3 Inversion Operator

(In this section we are considering the case of one solution).
Suppose there is a stack of $N = 2^n$ items, randomly placed, we need to find an algorithm that picks out a particular item which satisfies a certain condition. There is a binary function f that operates on strings of length n $f : \{0,1\}^n \rightarrow \{0,1\}$; a function of this sort is often called an oracle. When we apply f we get back a 1 if the criteria of the oracle is met, 0 otherwise. In quantum computing we need to translate this oracle to a unitary matrix; this latter will be chosen to flip the sign of a ket that meets the oracle criteria, and this one is the R operator seen above.

The recognition of the right ket is signaled by making use of an auxiliary qubit initialized as $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. So that if the item desired (we will call it x or $|x\rangle$ from now on) is signaled, the $|0\rangle$ and $|1\rangle$ interchange by the action of the oracle and 0 else way. Therefore the oracle's action is:

$$|x\rangle\,(\frac{|0\rangle - |1\rangle}{\sqrt{2}}) \to (-1)^{f(x)}\,|x\rangle\,(\frac{|0\rangle - |1\rangle}{\sqrt{2}}). \tag{7}$$

Since the auxiliary qubit looks unchanged, we can simplify the description and write:

$$|x\rangle \to (-1)^{f(x)}\,|x\rangle\,. \tag{8}$$

hence we can describe the process as:
1- The oracle:

$$f(|\psi\rangle) = \begin{cases} |1\rangle & \text{if } |\psi\rangle = |x\rangle\,. \\ |0\rangle & \text{otherwise.} \end{cases} \tag{9}$$

2- The unitary matrix R change the sign of the state $|x\rangle$ (a sign flip is simply a phase shift by $e^{i\pi} = -1$):

$$R\,|\psi\rangle = \begin{cases} -\,|x\rangle & \text{if } |\psi\rangle = |x\rangle\,. \\ |\psi\rangle & \text{otherwise.} \end{cases} \tag{10}$$

To sum up the overall effect in a small line:

$$R(|x\rangle \otimes H\,|1\rangle) = (e^{i\pi}\,|x\rangle) \otimes H\,|1\rangle\,. \tag{11}$$

Where H is the Hadamard gate. In our quantum circuit, we constructed our inversion operator using the auxiliary mentioned above, some X-gate placed in specific places, and a n-qubit toffoli gate that is constructed from $2{*}n = log_2 N$ toffoli gates.

4 Grover's Diffusion Operator

(In this section we are considering the case of one solution).
After the application of R operator, we get a balanced superposition state with a flipped sign on the target ket:

$$|\psi\rangle = -\frac{1}{\sqrt{N}}\,|x\rangle + \sum_{y\in\{0,1\}^n y\neq x} \frac{1}{\sqrt{N}}\,|y\rangle \tag{12}$$

the square of the coefficients are all equal to $1/\sqrt{N}$. If we now measure the qubits, we have an equal chance to get each of the N-basis kets.
A process called amplitude amplification which amplify the amplitude of the desired ket at each applied step by given amount demonstrated below, this is carried out with the operator D its composed from three transformations:
1- Hadamard transform $H^{\otimes n}$.

2- Z_0: A conditional phase shift I, which add a phase shift of -1 to every ket except $|0\rangle$, this effect can be written as:

$$|x\rangle \rightarrow -(-1)^{\delta_{x0}} |x\rangle . \tag{13}$$

and the unitary operator that translate this operation is defined as: $2|0\rangle\langle 0| - I$.
3- Hadamard transform $H^{\otimes n}$.
Then, combining all those transformations leads to the Grover diffusion operator:

$$D = H^{\otimes n}(2|0\rangle\langle 0| - I)H^{\otimes n} = 2|\psi\rangle\langle\psi| - I. \tag{14}$$

This diffusion gate D is meant to increase the amplitude of the desired state (in our case it is $|x\rangle$); which is proven as follow:
Suppose we have a general state $\sum_k \alpha_k |k\rangle$. Here $|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{k\in\{0,1\}^n} |k\rangle$, express a balanced superposition.

$$\Longrightarrow$$

$$D = \sum_k \frac{2}{N} |k\rangle\langle k| - I$$

Hence:

$$(\sum_k \frac{2}{N}|k\rangle\langle k| - I)(\sum_k \alpha_k |k\rangle) = \sum_k \frac{2\alpha_k}{N}|k\rangle\langle k| - \sum_k \alpha_k |k\rangle = \sum_k (2\mu - \alpha_k)|k\rangle . \tag{15}$$

Where $\mu = \sum_k \frac{\alpha_k}{N}$, is the mean value of the α_k. For this reason, the operator D is somrtimes called the inversion about the mean operation.
Let us illustrate how this increase in amplitude act on our state (eq.12). The average of the coefficients after negating the amplitude of $|x\rangle$ slightly decrease by a small value ϵ, thus $\mu = \frac{1}{\sqrt{N}} - \epsilon$. Applying D produce the state:

$$D|\psi\rangle = (\frac{2}{\sqrt{N}} - 2\epsilon + \frac{1}{\sqrt{N}})|x\rangle + \sum_{y\neq x}(\frac{2}{\sqrt{N}} - 2\epsilon - \frac{1}{\sqrt{N}})|y\rangle = (\frac{3}{\sqrt{N}} - 2\epsilon)|x\rangle + \sum_{y\neq x}(\frac{1}{\sqrt{N}} - 2\epsilon)|y\rangle . \tag{16}$$

Therefore, after applying D, the probability amplitude has been added to $|x\rangle$. Thus the coefficient of $|x\rangle$ increases at each operation of the Grover iteration DR, but with a decreasing rate since the average of all the coefficients decrease also. Ultimately, after $O(\sqrt{N})$ iterations the amplitude of the target ket will be in $O(1)$. Regarding the construction of Z_0, we constructed it using $2log_2N$ toffoli gates. Thus, its computational complexity is $O(log_2N)$

5 Complexity

In this section, we will talk about the query complexity and computational complexity.

5.1 Query Complexity

Query complexity can simply be defined as how many times you need to run a quantum circuit or, to be more precise, a part of the circuit to get the solution of your problem with the desired probability; it is important to note that the number of queries of course depends on the size of your input. For example, we need to run the DR operators $\sqrt{N}$ times in Grover's algorithm to get the state that we are looking for. We intend to prove this $\sqrt{N}$. Proof: Let's assume that our target state has amplitude of $t/\sqrt{N}$ and $t << \sqrt{N}$ and the other states have amplitude of $u/\sqrt{N}$. Let's first calculate the new amplitude of the nth non-target state after applying the DR operators:

$$DR\psi_n = -u/\sqrt{N}+2u/N\sqrt{N}+2u(N-2)/N\sqrt{N}-2t/N\sqrt{N} \approx -u/\sqrt{N}+2u/\sqrt{N} = u/\sqrt{N} \tag{17}$$

which shows that the amplitude nearly doesn't change. Let's now calculate the amplitude of the target qubit written as ψ_t:

$$DR\psi_t = t/\sqrt{N}-2t/N\sqrt{N}+2(N-1)u/N\sqrt{N} \approx= t/\sqrt{N}+2u/\sqrt{N} = (t+2u)/\sqrt{N} \tag{18}$$

since the amplitude always increase by about $2u/\sqrt{N}$ and since also the u is of order unity, we can say that we need to repeat the DR operator about $\sqrt{N}$ times to cancel the denominator and get something of order unity. So, this shows why our algorithm of of query complexity $O(\sqrt{N})$.

5.2 Computational Complexity

Computational complexity can be defined as the number of gates used in the algorithm; it is somehow related to time complexity since these gates need a certain amount of time to function. For Grover's algorithm, both the inversion and diffusion operator has parts that constructed from an n-qubit toffoli gate uses log_2N toffoli gates. So, since we use log_2N gates in both operators for $\sqrt{N}$ times to achieve the result we want, we can say that our computational complexity is $O(\sqrt{N}log_2N)$.

References

[1] Grover, L.K. From Schrödinger's equation to the quantum search algorithm. Pramana - J Phys **56**, 333–348 (2001). https://doi.org/10.1007/s12043-001-0128-3

[2] Wright, J., Lecture 4: Grover'S Algorithm. [online] Cs.cmu.edu.(2015) Available at: ¡ https://www.cs.cmu.edu/ odonnell/quantum15/lecture04.pdf¿ [Accessed11 May 2020].

[3] M. A. Nielsen and I. L. Chuang, Quantum Computation and Quantum Information, edited by C. S. o. Information and t. N. Sciences (Cambridge University Press, 2000).