Quantum Search Algorithm
FQC Online Classes 2020

By

Dr. Vivekanand Bhat

Dept. of CSE

MIT Manipal

The Grover's Quantum Search Algorithm

- The Grover's algorithm solves the problem of searching for an element in an unordered database with N entries in $O(\sqrt{N})$ time.
- The best classical algorithm for a search over unordered data requires $O(N)$ time.
- It is important to note that this searching problem is completely *unstructured*.
- Since there are no promises on the function f, so it is not possible to use binary search or any other fast searching method to efficiently solve the problem classically.

The search problem

- We wish to search through a list of N elements y_x .
- Each element has an index x in the range: 0 to N-1.
- We assume for convenience that $N = 2^n$, so we can store x in n qubits.
- Our search problem has M solutions: $1 \leq M \leq N$.
- Rather than dealing with the list itself, we focus on the *index* of the list, x
- The key idea is that given some value of x, we can tell whether y_x solves the search problem.

The search problem

- Suppose that we have a function

$$f : \{0,1\}^n \rightarrow \{0,1\}$$

defined as f(x) = 1, if x is a solution to the search problem, and f(x) = 0 if x is not solution to a search problem.

The Oracle

- The search problem can be formulated as an oracle or "black box" problem- with ability to recognize solutions to the search problem
- More precisely, the oracle is a unitary operator, O, defined by

$$|x\rangle|q\rangle \xrightarrow{O} |x\rangle|q \oplus f(x)\rangle$$

where |x> is the index register, and the oracle qubit |q> is a single qubit which is flipped if f(x) = 1, and is unchanged otherwise.

- We can check whether x is a solution to our search problem by preparing |x>|0>, applying oracle, and checking to see if the oracle qubit has been flipped to |1>

The Oracle

- In quantum search algorithm it is useful to apply the oracle with the oracle qubit initially in the state

$$|q> = \frac{1}{\sqrt{2}}(|0> - |1>)$$

- If x is not a solution to the search problem, applying the oracle to the state $\frac{|x>(|0>-|1>)}{\sqrt{2}}$ does not change the state.

- On the other hand, if x is a solution to the search problem, then |0> and |1> are interchanged by the action of the oracle, giving final state

$$\frac{-|x>(|0>-|1>)}{\sqrt{2}}$$

The Oracle

- Hence the action of oracle is given by:

$$|x\rangle\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)\xrightarrow{O}(-1)^{f(x)}|x\rangle\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)$$

- Notice that the state of the oracle qubit is not changed. It turns out that this remains $(|0>-|1>)/\sqrt{2}$ throughout the quantum search algorithm, and can be omitted from further discussion of the algorithm.
- With this convention, the action of the oracle may be written as:

$$|x\rangle\xrightarrow{O}(-1)^{f(x)}|x\rangle$$

Grover's Quantum Search Algorithm

- The Grover's algorithm is given below:

1. Begin with $|x\rangle = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} |j\rangle$.
2. Apply the Oracle to $|x\rangle$:

$$|x\rangle \mapsto \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} (-1)^{f(x)} |j\rangle$$

3. Apply the QFT to $|x\rangle$.
4. Reverse the sign of all terms in $|x\rangle$ except for the term $|0\rangle$.
5. Apply the Inverse QFT.
6. Return to step 2 and repeat.

A Very Simple Example

Apply Grover's algorithm on a system with N= 4 and solution is indexed by x = 0

1. Begin with the state $|\psi\rangle = \frac{1}{2}(|0\rangle + |1\rangle + |2\rangle + |3\rangle)$.

2. Apply the Oracle to the state, which flips the sign of $|0\rangle$: $|\psi\rangle \mapsto \frac{1}{2}(-|0\rangle + |1\rangle + |2\rangle + |3\rangle)$

3. Apply the QFT to this state. I think it's easiest to do this in matrix form, where we have

$$|\psi\rangle \mapsto F_2|\psi\rangle = \frac{1}{4}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & \mathrm{i} & -1 & -\mathrm{i} \\ 1 & -1 & 1 & -1 \\ 1 & -\mathrm{i} & -1 & \mathrm{i} \end{pmatrix}\begin{pmatrix} -1 \\ 1 \\ 1 \\ 1 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1 \\ -1 \\ -1 \\ -1 \end{pmatrix} \equiv \frac{1}{2}(|0\rangle - |1\rangle - |2\rangle - |3\rangle)$$

4. Flip the signs of all terms except $|0\rangle$: $|\psi\rangle \mapsto \frac{1}{2}(|0\rangle + |1\rangle + |2\rangle + |3\rangle)$

5. Apply the inverse QFT:

$$|\psi\rangle \mapsto F_2|\psi\rangle = \frac{1}{4}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -\mathrm{i} & -1 & \mathrm{i} \\ 1 & -1 & 1 & -1 \\ 1 & \mathrm{i} & -1 & -\mathrm{i} \end{pmatrix}\begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \equiv |0\rangle$$

A Very Simple Example

So after one iteration, the state of the system is $|\psi\rangle = |0\rangle$, and so a measurement guarantees us the correct answer. What happens if we apply the second iteration?

1. Apply the Oracle: $|\psi\rangle \mapsto -|0\rangle$
2. Apply the QFT: $|\psi\rangle \mapsto \frac{1}{2}(-|0\rangle - |1\rangle - |2\rangle - |3\rangle)$
3. Flip the signs of all terms except $|0\rangle$: $|\psi\rangle \mapsto \frac{1}{2}(-|0\rangle + |1\rangle + |2\rangle + |3\rangle)$
4. Inverse QFT: $|\psi\rangle \mapsto \frac{1}{2}(|0\rangle - |1\rangle - |2\rangle - |3\rangle)$

So a measurement of the state no longer guarantees the correct result. This illustrates the importance of measuring the result of Grover's algorithm after the correct number of iterations.