CS 405 - Quantum Computing
3-SAT Problem using Grover's Search

1. Kush Vasani - (202003012)
2. Jainil Patel - (202003027)
3. Pratap Ratiya - (202003036)

Table of Contents

Intoduction

- The 3-SAT problem is a well-known NP-complete problem in computer science that is notoriously difficult to answer economically.
- The 3-SAT problem is significant because many optimization and decision problems in computer science may be simplified to the 3-SAT problem.
- In this presentation, we will describe how Grover's algorithm can solve the 3-SAT problem and provide an example implementation using Qiskit.

Boolean satisfiability problem

- The boolean satisfiability problem is a well-known problem in computer science and mathematics. The problem is whether a valid assignment of truth values exists so that the whole boolean formula becomes true.
- A boolean formula in conjunctive normal(CNF) form is a logical expression composed of clauses, where each clause is a disjunction (logical OR) of one or more literals, and the entire expression is a conjunction (logical AND) of the clauses.

3 SAT

- It is the more general form of the SAT problem. In the 3-SAT problem, each clause is required to have exactly three literals.
- Here's an example of a 3-SAT problem:

$$(x \vee y \vee z) \wedge (x \vee \neg y \vee \neg z) \wedge (\neg x \vee \neg y \vee z)$$

- We want to find a set of Boolean values that can be assigned to the variables x, y, and z to make the CNF formula true.

3-SAT

- The 3-SAT problem is known to be NP-complete, which indicates that big cases are computationally challenging to answer with traditional computers.
- There are several methods and algorithms that may be useful to solve the 3-SAT problem here, we will use the Grover Search algorithm to solve 3 SAT problem
- Grover's approach can solve the 3-SAT problem by repeatedly using an oracle and the Grover diffusion operator to find a satisfied assignment of the Boolean variables.

Grover Search Algorithm

- Grover's algorithm is a quantum algorithm that solves the unstructured search problem faster than classical techniques. Grover's approach can solve the search problem in O(sqrt(N)).
- The quadratic speedup is due to the fact that each iteration of the method decreases the number of candidates by a constant factor, while it is just one for each query in the traditional brute-force technique.
- Grover's algorithm has applications in a variety of domains, including cryptography, database search, optimization, the 3 SAT problem, and many more.

How Grover Search Algorithm works

1. Initial state: Apply a Hadamard gate to each qubit to prepare the starting state.
2. The oracle: A quantum operation that inverts the sign of the amplitude of the marked state. This is accomplished by applying a -1 phase shift to the designated state.
3. Diffusion operator: Another quantum operation that amplifies the amplitude of the marked state by reflecting the state vector around the average amplitude of all states. This enhances the likelihood of finding the marked state in the subsequent iteration.
4. Repeat: Repeatedly apply the oracle and diffusion operator sqrt(N) times.

Solving 3-SAT using Grover algorithm :

It can be used to solve the 3-SAT problem as follows:

- Represent the boolean variables as qubits.
- We can then use the clauses in the boolean formula to construct a state that satisfies the formula. For example, if our formula is :

$$(x \wedge y \wedge z) \vee (x \wedge y \wedge \neg z) \vee (x \wedge \neg y \wedge z)$$

- We can use gates to represent the boolean operations. For example, boolean expression $\neg$ could be achieved by X gate and $\wedge$ by multiple-control toffoli gate.
- In this case, the initial states that satisfy the formula are our marked states.

Steps :

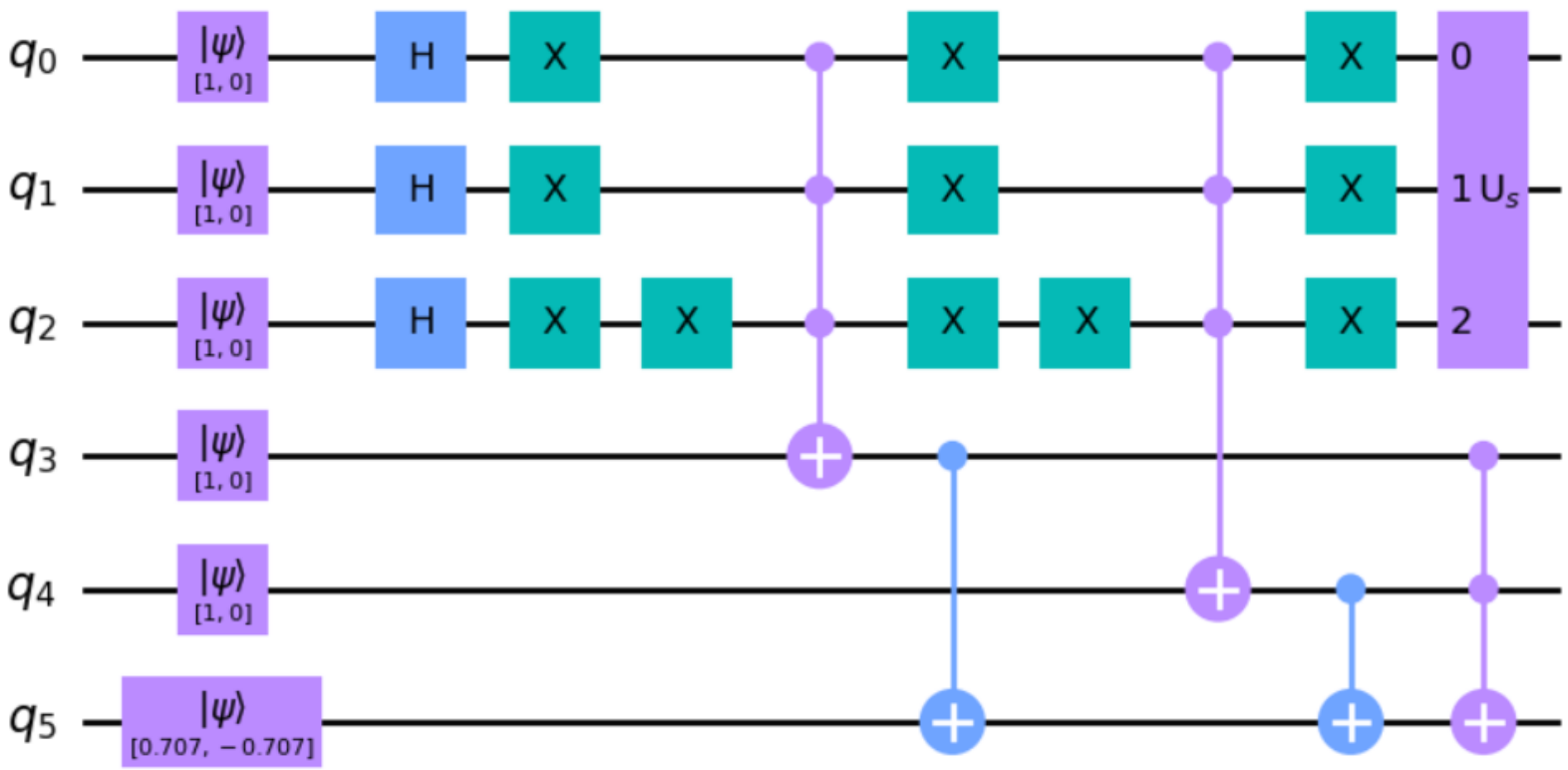
- Apply a phase inversion operator: To invert the sign of the amplitudes corresponding to the states that match the formula, we create an oracle. Oracle basically outputs the value of the expression. By applying different kinds of gates, we can change the sign of the marked state.
- Diffuser: Applying the Grover diffusion operator will allow us to amplify the satisfied state's amplitude while decreasing the amplitudes of the other states. This is done by a combination of hadamard gates and X gates. Below is the circuit showing the oracle and the diffuser.

Steps :

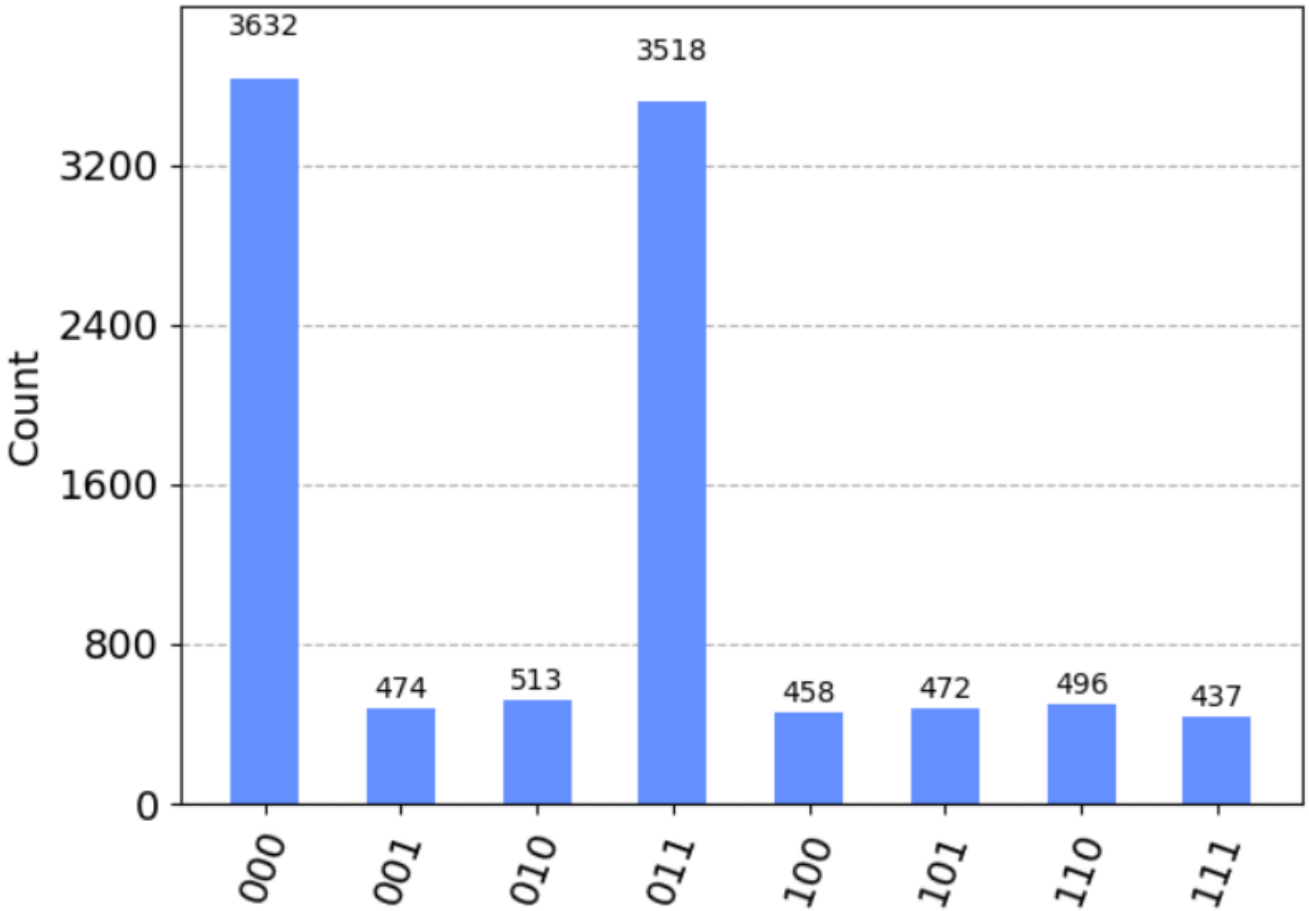
- Repeat steps 1 and 2: To increase the amplitude of the satisfied state and reduce the other states, we can repeat steps 1 and 2 for a predetermined number of iterations. As n is the number of qubits used to represent the variables, the number of iterations needed is proportional to n.
- Measure the state: If the boolean formula has a satisfying assignment, we can measure the state to find it. The amplitude squared of the satisfying state determines the likelihood of measuring it.

Example:

$$(x \wedge y \wedge \neg z) \vee (\neg x \wedge \neg y \wedge \neg z)$$



Measurement:



Output:

These are two assignments of truth values that satisfy our expression:

$$(x \wedge y \wedge \neg z) \vee (\neg x \wedge \neg y \wedge \neg z)$$

1. x=0, y=0, z=0
2. x=1, y=1, z=0

In measurement, these are the states whose count is the highest.

Conclusion :

- The Grover search algorithm is a quantum method that can solve unstructured search problems quadratically quicker than conventional algorithms. The 3-SAT problem is a well-known NP-complete problem that can be solved using Grover's algorithm.
- The Grover search algorithm can solve the 3-SAT problem by modeling the boolean formula as a quantum state, flipping the sign of the amplitudes, and applying the Grover diffusion operator. If the formula exists, the state can be measured to produce a satisfied assignment.

References :

1. “wikipedia.org/wiki/Boolean$_s$*atisfiability*$_p$*roblem*”
2. “www.cs.umd.edu/ gasarch/TOPICS/sat/SATtalk.pdf”
3. “qiskit.org/course/ch-algorithms/grovers-algorithm”
4. “qiskit.org/course/ch-applications/solving-satisfiability-problems-using-grovers-algorithm”

Team members :

Thank you!

Group 16
Kush Vasani - 202003012
Jainil Patel - 202003027
Pratap Ratiya - 202003036