Introduction to Quantum Information and Quantum Computing Assignment 2

Manuel Santos – 2019231352

January 2026

Introduction

This report presents the solution to Assignment 2 of the Introduction to Quantum Information and Quantum Computing course.

The objective of this assignment is to explore and implement Grover's Algorithm. In Grover's algorithm, an oracle marks a secret computational basis state by inverting the sign of its amplitude, while leaving all other computational basis states unchanged. The goal of the algorithm is to identify the secret state using the smallest possible number of oracle queries.

The assignment involves the following tasks:

1. Prepare the oracle state $|101\rangle$.
2. Construct the diffusion operator circuit.
3. Combine the oracle and diffusion operator to form the full Grover's algorithm circuit.
4. Analyze the quantum state after the initial Hadamard gates and calculate the probability of measuring the secret state.
5. Determine the number of Grover cycles needed for a 3-qubit system to achieve a probability above 50% of measuring the marked state.
6. Evaluate the number of queries required for a classical oracle to find the secret state in the worst and average cases.
7. Demonstrate that for a 2-qubit system, applying one Grover cycle results in a 100% probability of measuring the secret state.

1 Preparation of Grover's Oracle

In order to implement Grover's algorithm, we first need to prepare the oracle state. For this assignment, we will prepare the oracle state $|101\rangle$ as the one to be marked by the oracle. The circuit for preparing the oracle state is shown in Figure 1.

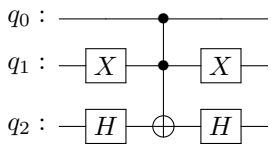

Figure 1: Circuit for Grover's Oracle Preparation

In order to understand how this circuit works, we can represent it in an equivalent way, as shown in Figure 2.

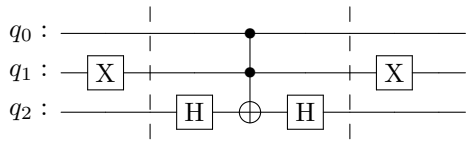

Figure 2: Deconstructed Oracle Circuit

It's important to note that the oracle circuit flips the sign of the amplitude of the state $|101\rangle$, while leaving all other states unchanged. The use of a Toffoli gate sandwiched by H gates is equivalent to a controlled-Z gate, which applies a phase flip to the target qubit when both control qubits are in the state $|1\rangle$. This construction allows us to effectively mark the desired state in Grover's algorithm, previously prepared by the X gate on the second qubit.

2 Diffusion Operator Circuit

The diffusion operator, also known as the inversion about the mean, is a crucial component of Grover's algorithm. The circuit for the diffusion operator is shown in Figure 3.

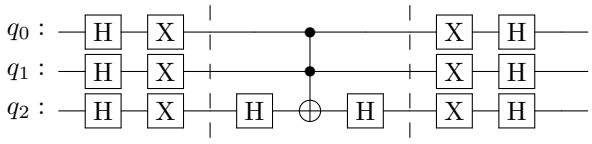

Figure 3: Diffusion Operator Circuit

The diffusion operator works by first applying Hadamard gates to all qubits, followed by X gates. Then, a controlled-Z operation is performed using a Toffoli gate sandwiched by H gates. Finally, the X and H gates are applied again to complete the diffusion process. This operator amplifies the amplitude of the marked state, increasing the probability of measuring it in the final step of Grover's algorithm.

3 Grover's Algorithm Circuit

The full Grover's algorithm circuit with oracle and diffusion operators is shown in Figure 4.

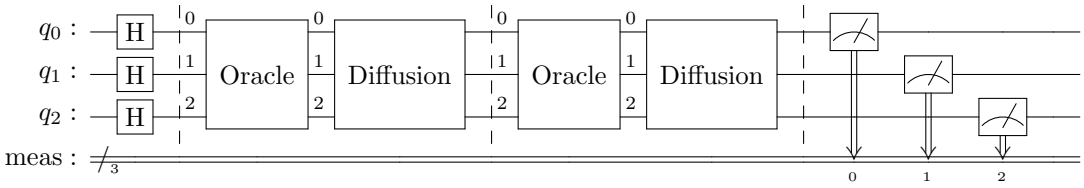

Figure 4: Full Grover's Algorithm Circuit

In this circuit, we start by applying Hadamard gates to all qubits to create an equal superposition of all possible states. Then, we apply the oracle and diffusion operators multiple times to amplify the amplitude of the marked state $|101\rangle$. Finally, we measure the qubits to obtain the result.

After executing the circuit, we expect to measure the state $|101\rangle$ with high probability, demonstrating the effectiveness of Grover's algorithm in searching for a marked item in an unsorted database. Running the circuit 1024 times yields the expected result, confirming the successful implementation of Grover's algorithm, as shown in Figure 5.

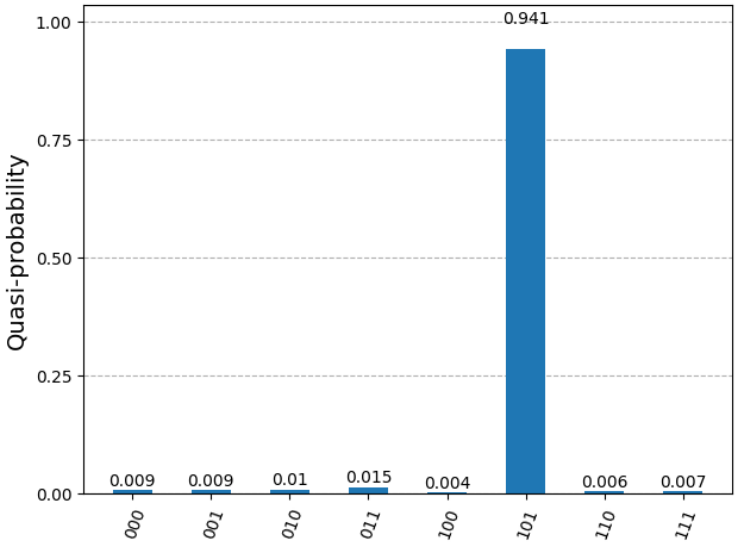

Figure 5: Measurement Results after Executing 2 cycles of Grover's Algorithm

4 What is the quantum state in which the circuit is after the initial application of Hadamard gates? At this point in the circuit, what is the probability of measuring the secret state?

After the initial application of Hadamard gates, the quantum state of the system is an equal superposition of all possible states for 3 qubits. The state can be expressed as:

$$|\psi\rangle = \frac{1}{\sqrt{8}}(|000\rangle + |001\rangle + |010\rangle + |011\rangle + |100\rangle + |101\rangle + |110\rangle + |111\rangle)$$

As so, the probability of measuring the secret state $|101\rangle$ at this point in the circuit is given by the square of the amplitude associated with that state. Since the amplitude of each state in the superposition is $\frac{1}{\sqrt{8}}$, the probability of measuring the secret state is:

$$P(|101\rangle) = \left|\frac{1}{\sqrt{8}}\right|^2 = \frac{1}{8} = 0.125$$

Thus, the probability of measuring the secret state $|101\rangle$ after the initial application of Hadamard gates is 12.5%.

5 For n qubits, the oracle marks only one state out of the $N = 2^n$ states of the computational basis. To obtain the marked state with probability above 50%, it is typical to apply k Grover cycles, with $k \approx \frac{\pi}{4}\sqrt{N}$. What should k be for a system of 3 qubits (round to the nearest integer)? What is the relationship with the number of cycles used in this problem?

For a system of 3 qubits, we have $n = 3$, which means the total number of states in the computational basis is $N = 2^n = 2^3 = 8$. To determine the number of Grover cycles k needed to obtain the marked state with

probability above 50%, we can use the formula:

$$k \approx \frac{\pi}{4}\sqrt{N}$$

Substituting $N = 8$ into the formula, we get:

$$k \approx \frac{\pi}{4}\sqrt{8} = \frac{\pi}{4} \times 2\sqrt{2} = \frac{\pi\sqrt{2}}{2}$$

Calculating this value numerically:

$$\frac{\pi\sqrt{2}}{2} \approx \frac{3.1416 \times 1.4142}{2} \approx \frac{4.4429}{2} \approx 2.22145$$

Rounding to the nearest integer, we find:

$$k \approx 2$$

In this problem, we used 2 Grover cycles, which aligns perfectly with the calculated value of k for a system of 3 qubits. This confirms that the number of Grover cycles used in the problem is appropriate for achieving a high probability of measuring the marked state.

6 On a classical computer, we can only give the oracle one state $|a\rangle$ at a time. In turn, the oracle can give only one of two answers: "Yes, $|a\rangle$ is the secret state" or "No, $|a\rangle$ is not the secret state." In the worst case, for three bits (as in this problem), how many queries would we need to make to find the secret state using a classical oracle? And on average?

In the worst-case scenario, using a classical oracle to find the secret state among 3 bits (which corresponds to 8 possible states: $|000\rangle$, $|001\rangle$, $|010\rangle$, $|011\rangle$, $|100\rangle$, $|101\rangle$, $|110\rangle$, and $|111\rangle$), we would need to query the oracle for each state until we find the secret state.

In the worst case, the secret state is the last one we check, so we would need to make 8 queries. On average, assuming each state is equally likely to be the secret state, we would expect to check half of the states before finding the secret one. Therefore, the average number of queries needed is:

$$\frac{8}{2} = 4$$

Thus, in the worst case, we would need 8 queries to find the secret state using a classical oracle, and on average, we would need 4 queries.

7 In general, the amplitude associated with the secret state before applying the Grover cycles is $1/\sqrt{N}$, where $N = 2^n$ and n is the number of qubits. We can define the angle θ such that $\sin\theta = 1/\sqrt{N}$. With k Grover cycles, the probability of measuring the secret state is $|\sin((2k+1)\theta)|^2$. Show that, for $n = 2$ qubits, the probability of measuring the secret state is 100% by applying just one Grover cycle.

For $n = 2$ qubits, the total number of states in the computational basis is $N = 2^n = 2^2 = 4$. The amplitude associated with the secret state before applying the Grover cycles is given by:

$$\frac{1}{\sqrt{N}} = \frac{1}{\sqrt{4}} = \frac{1}{2}$$

We can define the angle θ such that:

$$\sin\theta = \frac{1}{\sqrt{N}} = \frac{1}{2}$$

This implies that:

$$\theta = \sin^{-1}\left(\frac{1}{2}\right) = \frac{\pi}{6}$$

Now, we apply one Grover cycle, which means $k = 1$. The probability of measuring the secret state after applying k Grover cycles is given by:

$$P = |\sin((2k+1)\theta)|^2$$

Substituting $k = 1$ and $\theta = \frac{\pi}{6}$:

$$P = |\sin((2 \cdot 1 + 1) \cdot \frac{\pi}{6})|^2 = |\sin(3 \cdot \frac{\pi}{6})|^2 = |\sin(\frac{\pi}{2})|^2$$

Since $\sin(\frac{\pi}{2}) = 1$, we have:

$$P = |1|^2 = 1$$

Thus, the probability of measuring the secret state after applying just one Grover cycle for $n = 2$ qubits is 100%.

Conclusion

This report has detailed the implementation and analysis of Grover's algorithm for a 3-qubit system. We have successfully prepared the oracle state, constructed the diffusion operator, and combined them to form the full Grover's algorithm circuit.

The analysis of the quantum state after the initial Hadamard gates revealed a 12.5% probability of measuring the secret state, which was significantly amplified through the application of Grover cycles. We determined that 2 Grover cycles are optimal for a 3-qubit system to achieve a probability above 50% of measuring the marked state.

Additionally, we compared the performance of Grover's algorithm with a classical oracle, highlighting the efficiency of the quantum approach. Finally, we demonstrated that for a 2-qubit system, applying one Grover cycle results in a 100% probability of measuring the secret state.

I personally found this assignment a good opportunity to explore in more detail Grover's algorithm and its components, as well as to understand the advantages of quantum computing over classical methods in search problems. Besides that, I took the chance to read the original paper by Lov K. Grover, which provided valuable insights into the algorithm's design and functionality.