


Implementation of Algorithm using Qiskit



Deutsch Jozsa Algorithm

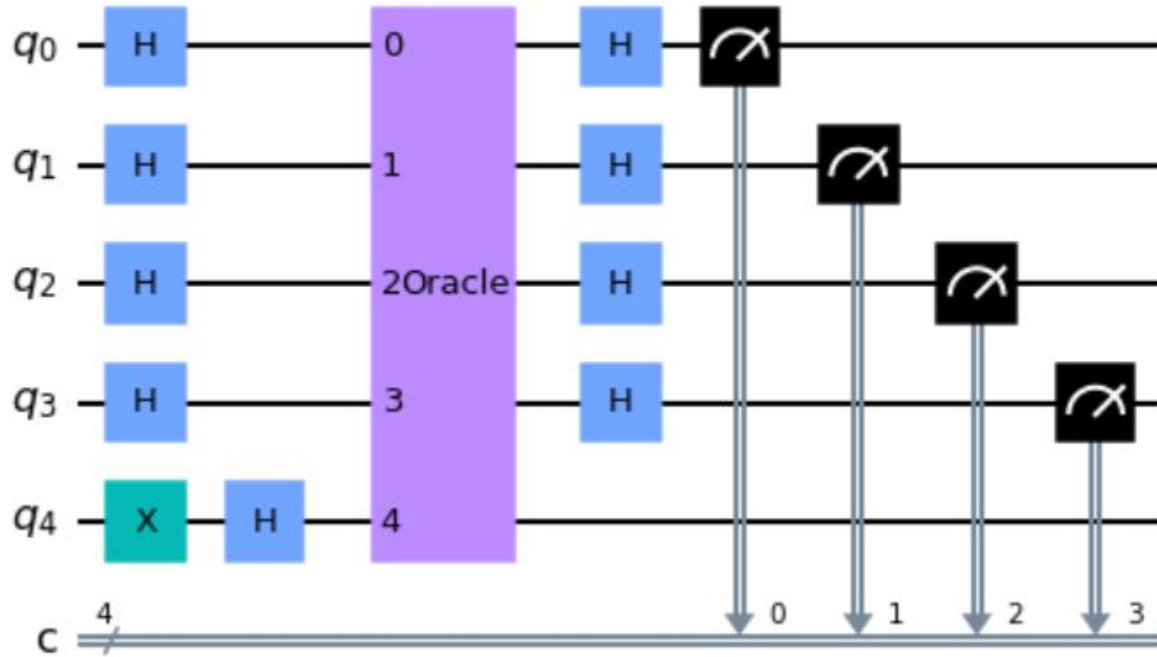
- Deutsch-Jozsa algorithm solves the problem of determining whether a given function is constant or balanced.
- Initialization: Applying Hadamard gates (H) to each qubit.
- Oracle Gate: Constructing the oracle gate based on the case ('constant' or 'balanced').

For a constant function, the oracle gate flips the output qubit state, resulting in a definite output of 0 or 1.

For a balanced function, the oracle gate creates interference patterns that cause the measurement outcomes to be equally distributed between 0 and 1.

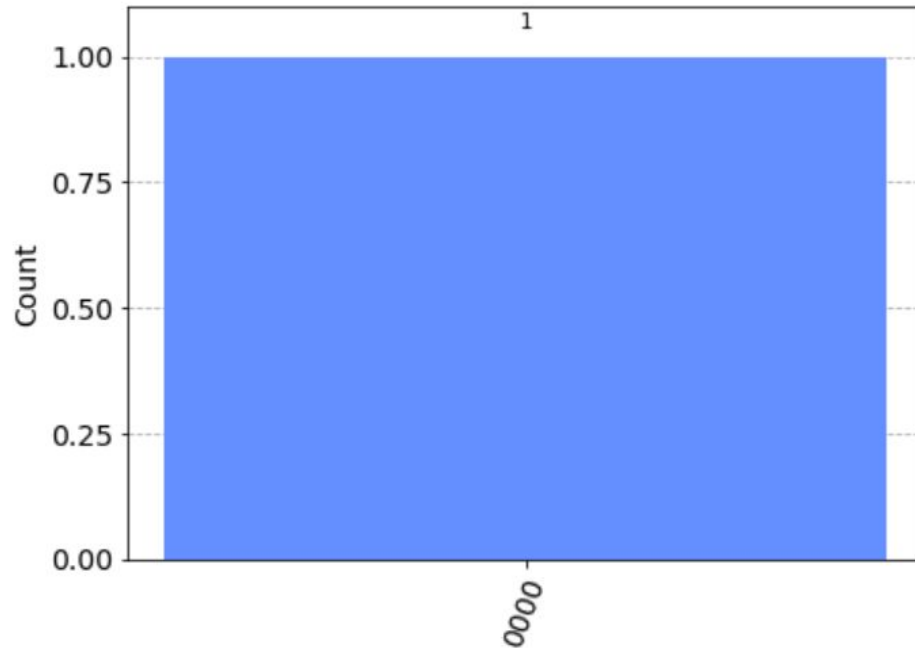
- Measurement: Applying Hadamard gates (H) and measuring each qubit.

N = 4 circuit diagram



Testing the circuit

Probability when f is constant



Grover's Algorithm

- Grover's algorithm is a quantum search algorithm that can efficiently solve certain searching and optimization problems.
- Quantum circuit representation:

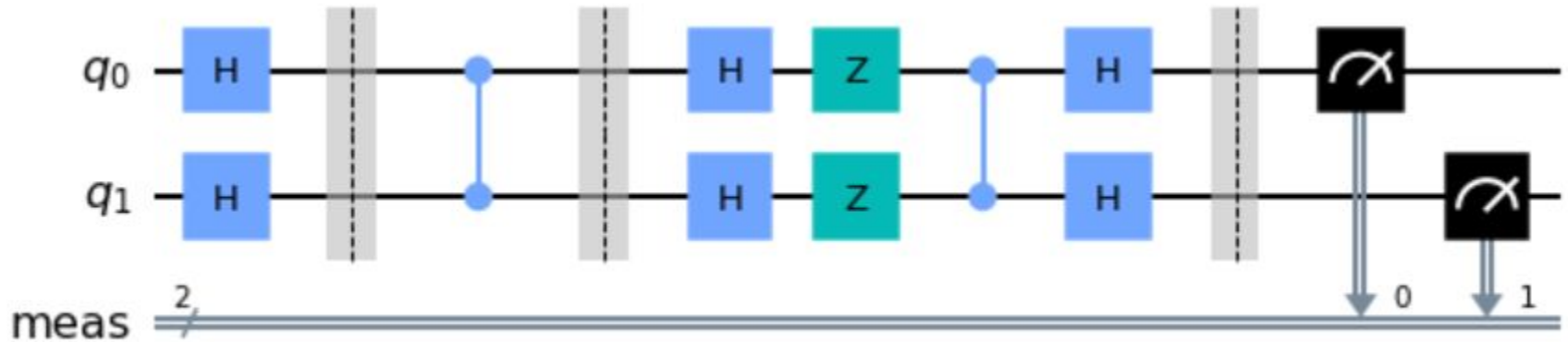
Initialization: Applying the Hadamard gate (H) to both qubits.

Oracle: Applying the Controlled-Z gate (CZ) between the qubits.

Diffuser: Applying a series of gates (H, Z, CZ, and H) to both qubits.

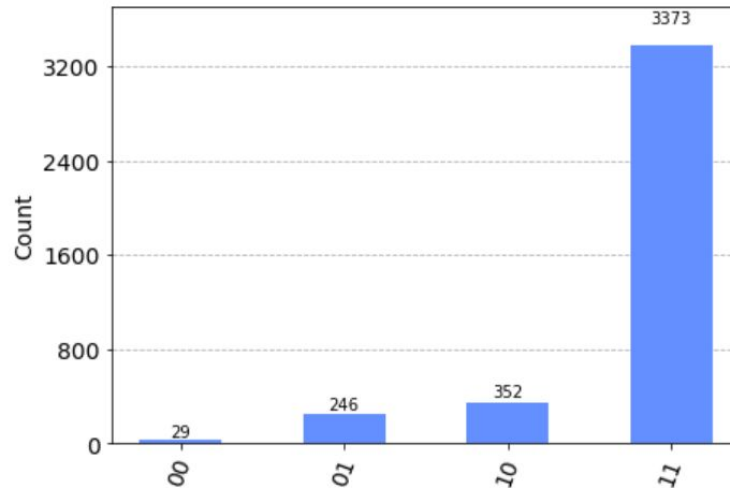
- Barriers are used to separate the different steps of the algorithm and improve clarity.

N = 2 Circuit diagram



Results and Conclusion

- The least busy quantum device is selected using IBM Quantum provider and the `least_busy()` function.
- The histogram represents the measurement outcomes and their respective probabilities.
- We confirm that in the majority of the cases the state $|11\rangle$ is measured. The other results are due to errors in the quantum computation.



Shor's Algorithm

- Given an odd composite number N , find an integer d , strictly between 1 and N , that divides N .
- A quantum computer is used to determine the unknown period p of the function $f(x) = a^x \bmod N$.
- If p is an odd integer, then go back to **Step 1**. Else move to the next step.
- Since p is an even integer so, $(a^{p/2} - 1)(a^{p/2} + 1) = a^p - 1 = 0 \bmod N$.
- Now, if the value of $a^{p/2} + 1 = 0 \bmod N$, go back to **Step 1**.
- If the value of $a^{p/2} + 1 \neq 0 \bmod N$, Else move to the next step.
- Compute $d = \gcd(a^{p/2} - 1, N)$.
- The answer required is ' d '.

Steps

- Step 1: Initialization

Applying Hadamard gates (H) and X gates (NOT gates) to prepare the qubits. Hadamard gates create a superposition of states, allowing the qubits to be in multiple states simultaneously. X gates are used to set the last qubit to the $|1\rangle$ state, which is necessary for the factoring process.

- Step 2: Modular Exponentiation

This step involves mapping the factoring problem onto qubits using controlled modular exponentiation operations. The modular exponentiation function performs repeated modular exponentiation of a chosen number (a) to the power of increasing values.

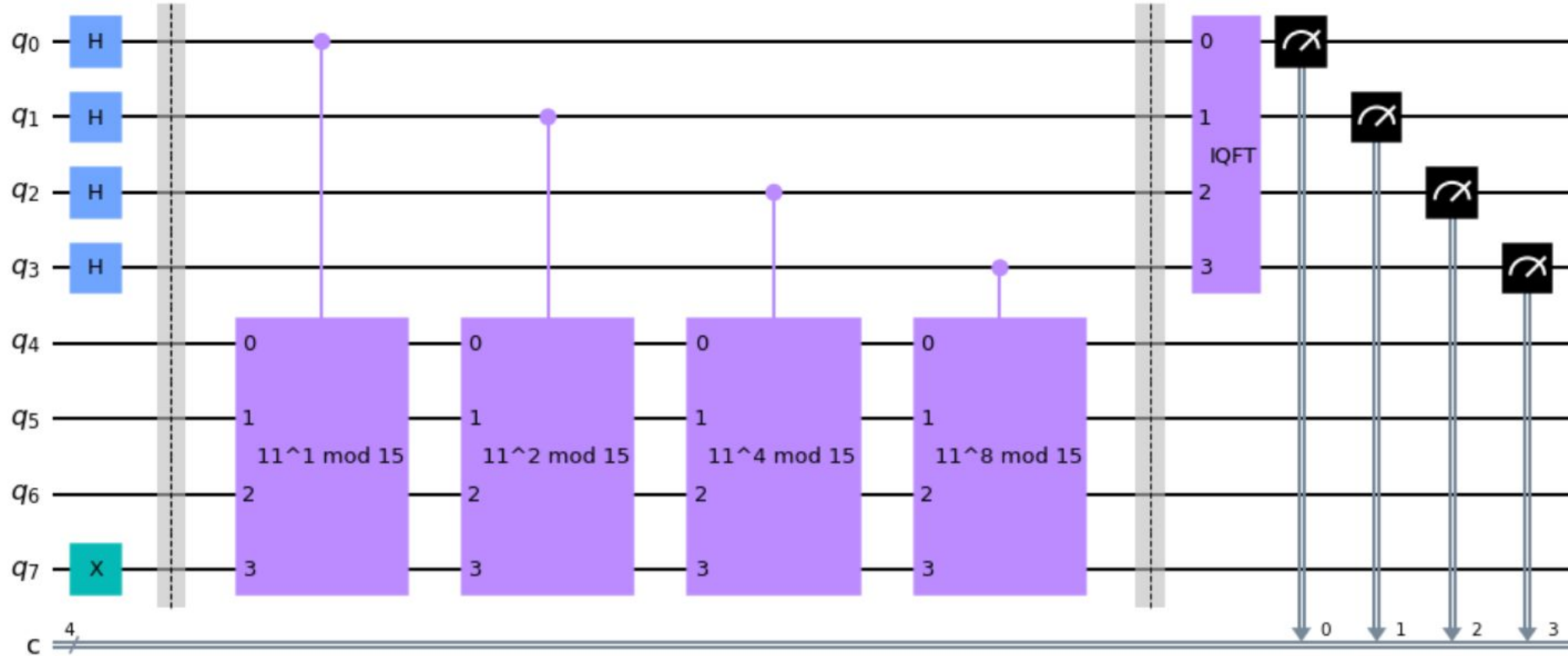
- Step 3: Inverse QFT

By applying the inverse QFT, the period of the modular exponentiation function is revealed.

- Step 4: Measurement

Measuring the qubits to obtain the period as measurement outcomes.

Circuit Diagram



Results and Prime factors

Measured 15

Failed. Measured value is not an even number

Measured 0

(1, 15)

Measured 9

Failed. Measured value is not an even number

Measured 8

(1, 15)

Measured 12

(1, 15)

Measured 10

(3, 5)

Measured 13

Failed. Measured value is not an even number

Measured 11

Failed. Measured value is not an even number

Measured 14

(3, 5)

****The prime factors are 3 and 5****