EMSI Casablanca

The analysis of Deutsch–Jozsa quantum algorithm and its implementation on IBM quantum computer using Python

Prepared by: Yassine Boughroudi
Date: June 23,2022

Abstract

This report presents the basic postulates of quantum mechanics and shows the quantum computer's advantage over classical computers in solving the Deutsch–Jozsa algorithm. I have thoroughly analyzed this algorithm and provided examples for its implementation in the Qiskit python framework.

Contents

1 Introduction

Quantum mechanics is one of the most important discoveries of the last century in theoretical physics. Thanks to quantum mechanics, we know that particles behave very differently at a very small scale than we thought before. At this scale, particles can be in several states simultaneously, and they are modified when observed. Even though these concepts were developed in the late 1930s, there are still many mysteries related to this theory because of its counterintuitive nature. Still, many experiments have confirmed the quantum nature of the world. In the mid-80s, the physicist Richard Feynman had a remarkable idea: If we can control some quantum particles, we are able to simulate physical systems in a more efficient way. From his article[1], **quantum computing was born**.

The classical computers manipulate individual bits, 0 and 1, to store information as binary data, whereas quantum computers use the probability of an object's state before it is measured. Therefore, it gives them the potential to process exponentially more data compared to classical computers. Unlike classical computers that use the binary bit, quantum computers use qubits that are produced by the quantum state of the object to perform operations. Since these qubits are quantum in nature, they follow phenomena like **superposition** and **entanglement**. Superposition is the ability of a quantum system to be in multiple states at the same time. Entanglement is the strong correlation between quantum particles. These phenomena help the quantum computer work with 0, 1, and superposition of 0 and 1, giving them the advantage in doing complex calculations that modern classical systems cannot do or would take a significant amount of time to get the desired result[2].

2 Postulates of Quantum Mechanics

Postulates are a set of axioms that cannot be proved but are consistent with experimental observation. There is no standard on what constitutes the minimum set of such norms, and it depends a lot on one's own point of view. We have followed [3] in the formulation.

Postulate-1:

A state is a complete description of a physical system. In quantum mechanics, a state is described by a ray in an abstract linear complex vector space known as Hilbert space.

- What is a Hilbert space?

    1. It is a vector space over the complex numbers C . Vectors will be denoted $|\psi\rangle$ (Dirac's ket notation).

    2. It is equipped by an inner product structure $\langle\psi|\phi\rangle$ that maps an ordered pair of vectors to C:

$$\langle \cdot \ , \ \cdot \rangle : H \times H \to C$$

and defined by the properties:

(a) Positivity: $\langle\psi|\psi\rangle \geq 0$, equality applies when $|\psi\rangle$ is a null vector.

(b) Linearity: $\langle\phi|\left(a\,|\psi_1\rangle + b\,|\psi_2\rangle\right) = a\,\langle\phi|\psi_1\rangle + b\,\langle\phi|\psi_2\rangle$

(c) Skew symmetry: $\langle\phi|\psi\rangle = \langle\psi|\phi\rangle^*$

(d) Schwartz Inequality: $||\,\langle\psi|\phi\rangle\,||^2 = \langle\psi|\psi\rangle\,\langle\phi|\phi\rangle$.

The dimension of the Hilbert space may be finite or infinite. For most of the time in Quantum Computing and Information the dimension will be finite.

- What is a ray? It is an equivalence class of vectors that differ by multiplication by a nonzero complex scalar. This class of vectors have the same physical meaning. That is, The state $|\psi\rangle$ and $e^{i\alpha}\,|\psi\rangle$ describe the same physical state, where $|e^{i\alpha}| = 1$.

The set of states $\{e_n\}$, n=1,2,3,... d, where d is the dimension of the space, is called a set of basis vectors, an arbitrary state $|\psi\rangle$ can be expressed as a linear superposition of the $|e_n\rangle$, i.e.,

$$|\psi\rangle = \sum_n \alpha_n\,|e_n\rangle \tag{1}$$

where

$$\langle e_i|e_j\rangle = \delta_{i,j} \tag{2}$$

if the basis is chosen we get

$$\alpha_n = \langle e_n|\psi\rangle \tag{3}$$

According to the *Copenhagen Interpretation* of quantum mechanics, $|\alpha_n|^2$ is postulated to be the probability that the state $|\psi\rangle$ will be found in the state $|e_n\rangle$.

Postulate-2:

An observable is a property of a physical system that in principle can be measured. In quantum mechanics, an observable is a self-adjoint operator . An operator is a linear map taking vectors to vectors, but since we operate on Hilbert space, the operators we deal with map the Hilbert space onto itself.

$$\hat{A} : |\psi\rangle \rightarrow \hat{A}\,|\psi\rangle$$

The operators have the following properties:

1. Linearity: if α and β are complex scalars, we have:

$$\hat{A}(a\,|\psi_1\rangle + b\,|\psi_2\rangle) = a\hat{A}\,|\psi\rangle + b\hat{B}\,|\psi\rangle$$

2. A unit operator has the property:

$$\hat{I}\,|\psi\rangle = |\psi\rangle$$

3. (a) A product of two operators $\hat{A}$ and $\hat{B}$ is also an operator, i.e., both $\hat{A}\hat{B}$ and $\hat{B}\hat{A}$ are operators. However, in general, $\hat{A}\hat{B} \neq \hat{B}\hat{A}$.

   (b) the operator product is associative, i.e. $\hat{A}(\hat{B}\hat{C}) = (\hat{A}\hat{B})\hat{C}$

   (c) The operator addition is both commutative and associative, i.e., $\hat{A}+\hat{B} = \hat{B}+\hat{A}$ and $\hat{A} + (\hat{B} + \hat{C}) = (\hat{A} + \hat{B}) + \hat{C}$.

   (d) If there exists an operator such that $\hat{A}\hat{B} = \hat{B}\hat{A} = \hat{I}$, then $\hat{B}$ is called the inverse of $\hat{A}$ and we write $\hat{B} = \hat{A}^{-1}$.

4. Adjoint of an operator: is an operator $\hat{A}$ that acts to the left on a bra vector, giving another bra vector $\langle\psi|\,\hat{A}$ on the dual space, and is defined by:

$$[\hat{A}\,|\psi\rangle]^* = \langle\psi|\,\hat{A}^\dagger$$

   By using this definition and the property of skew symmetry of the inner product we will derive the following interesting property:

$$\left\langle \phi' \middle| \psi \right\rangle = \left\langle \psi \middle| \phi' \right\rangle^* \Rightarrow \langle\phi|\,\hat{A}^\dagger\,|\psi\rangle = \langle\psi|\,A\,|\phi\rangle$$

   for all vectors $|\phi\rangle$, $|\psi\rangle$.
   It follows that if $\hat{A} = |\alpha\rangle\,\langle\beta|$, then $\hat{A}^\dagger = |\beta\rangle\,\langle\alpha|$

5. An operator is self-adjoint or hermitian if $\hat{A}^\dagger = \hat{A}$.

   (a) If $\hat{A}$ and $\hat{B}$ are self-adjoint, then so is $\hat{A} + \hat{B}$ (because $(\hat{A} + \hat{B})^\dagger = \hat{A}^\dagger + \hat{B}^\dagger$).

   (b) The product $\hat{A}\hat{B}$ is self-adjoint only if $\hat{A}$ and $\hat{B}$ commute, i.e., $(\hat{A}\hat{B})^\dagger = \hat{A}^\dagger\hat{B}^\dagger$

   (c) $\hat{A}\hat{B} + \hat{B}\hat{A}$ and $i(\hat{A}\hat{B} - \hat{B}\hat{A})$ are always self-adjoint if $\hat{A}$ and $\hat{B}$ are.

   According to the second postulate of quantum mechanics, a state $|\psi\rangle$ has a definite value λ for an observable represented by $\hat{A}$ if and only if $|\psi\rangle$ is an eigenstate of $\hat{A}$ with eigenvalue λ.

$$\hat{A}\,|\psi\rangle = \lambda\,|\psi\rangle$$

   The eigenstates of $\hat{A}$ form a complete orthonormal basis for the Hilbert space H. If $\hat{P}_n$ is orthogonal projection of $\hat{A}$ onto the eigen vector basis having eigenvalues λ_n, we can write:

$$\hat{A} = \sum_n \lambda_n \hat{P}_n \tag{4}$$

   The projection operators satisfy:

$$\hat{P}_n\hat{P}_m = \delta_{m,n}\hat{P}_n$$

$$\hat{P}_n^\dagger = \hat{P}_n$$

Equation (4) is a statement of the spectral theorem. Suppose an operator $\hat{A}$ is such that $\hat{A}\,|\psi\rangle = |\phi\rangle$ where $|\psi\rangle$ and $|\phi\rangle$ have the same norm. we then have

$$\langle\psi|\,\hat{A}^\dagger\hat{A}\,|\psi\rangle = \langle\phi|\phi\rangle = \langle\psi|\psi\rangle$$

so that

$$\hat{A}^\dagger\hat{A} = \hat{I}$$

Such an operator is called a **unitary operator** which has a special place in quantum mechanics in general and in Quantum Information and computation in particular.

Postulate-3:

Time evolution of a quantum state is unitary it is gener- ated by a self-adjoint operator, called the Hamiltonian of the system.In the Schrrodinger picture of dynamics, the vector describing the system moves in time as governed by the Schrodinger equation:

$$\frac{\partial\,|\Psi(t)\rangle}{\partial t} = -i\hat{H}\,|\Psi(t)\rangle$$

where $\hat{H}$ is the Hamiltonian. We may reexpress this equation, to first order in the in infinitesimal quantity dt , as

$$|\psi(t+dt)\rangle = (1 - i\hat{H}dt)\,|\psi(t)\rangle$$

The operator $\hat{H(dt)} \equiv 1 - i\hat{H}dt$ is unitary; because $\hat{H}$ is self-adjoint it satisfies $\hat{U}^\dagger U = \hat{I}$ to linear order in dt. Since a product of unitary operators is finite, time evolution over a finite interval is also unitary:

$$|\psi(t)\rangle = \hat{U}(t)\,|\psi(0)\rangle$$

In the case where $\hat{H}$ is t-independent. We may write $\hat{H} = e^{-it\hat{H}}$

Postulate-4:

The outcome of observation of A is an eigenvalue of the operator $\hat{A}$. Immediately after the measurement, the quantum state continues to be the eigenstate corresponding to this eigenvalue. If the state of the system before the measurement was $|\psi\rangle$, the measurement outcome will be λ_n with a probability:

$$\frac{P_n\,|\psi\rangle}{|\,\langle\psi|\,P_n\,|\psi\rangle\,|^{1/2}}$$

There is an inherent dualism in the way a quantum state evolves with time. On one hand the linearity of the Schrrodinger equation implies that the state develops unitarily when it is not being measured while on the other hand the measurement postulate is probabilistic in that it only assigns a probability of possible outcomes.

Postulate-5:

If $\hat{A}$ and $\hat{B}$ are two hermitian operators corresponding respectively to two classical observables a and b, then the commutator of $\hat{A}$ and $\hat{B}$ is given by

$$[\hat{A}, \hat{B}] = i\hbar\hat{C}$$

where $\hat{C}$ is an operator corresponding to a classical variable c which is given by the classical Poisson bracket of the variables a and $b, c = a, b$ and $\hbar$ is Planck's constant.

This completes the mathematical formulation of quantum mechanics. We immediately notice some curious features. One oddity is that the Schrodinger equation is linear, while we are accustomed to nonlinear dynamical equations in classical physics. This property seems to beg for an explanation. But far more curious is the mysterious dualism. There are two quite distinct ways for a quantum state to change.

On the one hand there is unitary evolution, which is deterministic; If we specify $|\psi(0)\rangle$, the theory predicts the state $|\psi(t)\rangle$ at a later time. But on the other hand there is measurement, which is probabilistic. The theory does not make definite predictions about the measurement outcomes; it only assigns probabilities to the various alternatives. This is troubling, because it is unclear why the measurement process should be governed by different physical laws than other processes.

3 The Qubit

The indivisible unit of classical information is the bit , which takes one of the two possible values {0,1}. The corresponding unit of quantum information is called the "quantum bit" or qubit . It describes a state in the simplest possible quantum system.

The smallest nontrivial Hilbert space is two-dimensional. We may denote an orthonormal basis for a two-dimensional vector space as $\{|0\rangle, |1\rangle\}$. Then the most general normalized state can be expressed as

$$a|0\rangle + b|1\rangle \tag{5}$$

where a,b are complex numbers that satisfy $|a|^2 + |b|^2 = 1$, and the overall phase is physically irrelevant. **A qubit is a state in a two-dimensional Hilbert space that can take any value of the form eq. (5).**

We can perform a measurement that projects the qubit onto the basis $\{|0\rangle, |1\rangle\}$. Then we will obtain the outcome $|0\rangle$ with probability $|a|^2$, and the outcome $|1\rangle$ with probability $|b|^2$, according to postulate number 4.

4 Deutsch-Jozsa Algorithm

4.1 Introduction

In this section, I will first introduce the Deutsch-Jozsa problem, which was introduced by Deutsch and Joszsa in [4]. Subsequently, I will present the solution in the

classical case and in the quantum case. Then I will implement the quantum algorithm using Qiskit, and run it on a simulator and device. I have mainly followed [5] and [6] for the entire section.

4.2 Deutsch-Jozsa Problem

The deusch-Jozsa algorithm solves the following problem: we are a given a function $f : \{0,1\}^n \to \{0,1\}$ that it is either constant(all inputs map to the same output) or balanced (the number of inputs that map to '0' and '1' is equal).

The goal is to determine whether f is constant or balanced.

4.3 The classical solution

Classically, in the best case, two queries to the oracle can determine if the hidden Boolean function, $f(x)$, is balanced.

In the worst case, if we continue to see the same output for each input we try, we will have to check exactly half of all possible inputs plus one in order to be certain that$f(x)$ is constant. Since the total number of possible inputs is 2^n, this implies that we need

$$\frac{2^n}{2} + 1 = 2^{n-1} + 1 = \mathcal{O}(2^n)$$

trial inputs to be certain that $f(x)$ is constant in the worst case.

4.4 The quantum solution

Using a quantum computer, we can solve this problem with 100% confidence after only one call to the function $f(x)$. i.e. its time complexity is $\mathcal{O}(1)$ instead of $\mathcal{O}(2^n)$.
We first give the circuit description of the algorithm and then analyze each step of the computation.

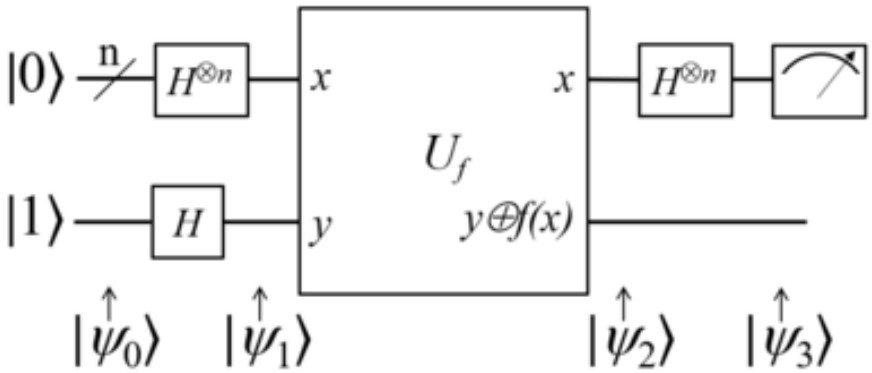


Figure 4.1: The DJ circuit Source:Wikipedia

1. Start with the n-qubit state:

$$|\Psi\rangle_0 = |0\rangle^n |1\rangle$$

2. Apply a Hadamard gate to each qubit:

$$\begin{aligned}
|\Psi\rangle_1 &= |+\rangle^n |-\rangle \\
&= \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)\cdots\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)|-\rangle \\
&= \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle |-\rangle
\end{aligned}$$

3. Apply Uf on the whole qubit state:

$$\begin{aligned}
|\Psi\rangle_2 &= \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle \left|\frac{|0\rangle + |1\rangle}{\sqrt{2}} \oplus f(x)\right\rangle \\
&= \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle \left(\frac{|f(x)\rangle - |\bar{f}(x)\rangle}{\sqrt{2}}\right) \\
&= \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{f(x)} |x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)
\end{aligned}$$

4. At this point the second single qubit register may be ignored. Apply a Hadamard gate to each qubit in the first register:

$$\begin{aligned}
|\Psi_3\rangle &= \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{f(x)} \left(\frac{1}{\sqrt{2^n}} \sum_{y\in\{0,1\}^n} (-1)^{x.y} |y\rangle\right) \\
&= \sum_{y\in\{0,1\}^n} \left[\frac{1}{2^n} \sum_{x\in\{0,1\}^n} (-1)^{f(x)+x.y}\right] |y\rangle \\
&= \sum_{y\in\{0,1\}^n} c_y |y\rangle
\end{aligned}$$

where $x.y = x_0y_0 \oplus x_1y_1 \ldots \oplus x_{n-1}y_{n-1}$ and $c_y := \left[\frac{1}{2^n}\sum_{x\in\{0,1\}^n}(-1)^{f(x)+x.y}\right]$

5. Measure the first register. Notice that the probability of measuring $|0\rangle^{\otimes n}$ according

to born rule:

$$\begin{aligned} P\left[y = 00\ldots0\right] &= \left|\langle 00\ldots0|\Psi_3\rangle\right|^2 \\ &= \left|\sum_{y\in\{0,1\}^n} c_y \langle 00\ldots0|\Psi_3\rangle\right|^2 \\ &= \left|c_{00\ldots0}\right|^2 \\ &= \left|\frac{1}{2^n}\sum_{x\in\{0,1\}^n}(-1)^{f(x)}\right|^2 \\ &= \frac{1}{2^{2n}}\left|\sum_{x\in\{0,1\}^n}(-1)^{f(x)}\right|^2 \end{aligned}$$

We distinguish 2 cases:

1. If f is a constant function, then $\exists b \in \{0,1\}$ st. $\forall x \in \{0,1\}^n$,$f(x) = b$. In this case, we have $P\left[y = 00\ldots0\right] = \frac{1}{2^{2n}}\left|2^n(-1)^b\right|^2 = 1$ and the algorithm gives the correct answer with probability 1.

2. If f is balanced, we can write:

$$P\left[y = 00\ldots0\right] = \frac{1}{2^{2n}}\left|(-1)^{f(x)}\right|^2 = \frac{1}{2^{2n}}\left|\sum_{x\in\{0,1\}^n:f(x)=0} 1 - \sum_{x\in\{0,1\}^n:f(x)=1} 1\right|^2 = 0$$

   and the algorithm gives the correct answer with probability 1.

4.5 Creating Quantum Oracles

In [6] a fine example is given on how to create a balanced oracle and I will follow those steps. For a constant function, it is simple:

1. if f(x)=0, then apply the I gate to the qubit in register 2.

2. if f(x)=1, then apply the X gate to the qubit in register 2.

For a balanced function, there are many different circuits we can create. One of the ways we can guarantee our circuit is balanced is by performing a CNOT for each qubit in register 1, with the qubit in register 2 as the target. For example: consider n=2. let $f(x) : \{0,1\}^2 \to \{0,1\}$ be a function giving by the following table:

x	00	01	10	11
$f(x)$	1	1	0	0

This function shall be represented by the following 8-by-8 unitary matrix:

$$
\begin{array}{c}
 \\
\mathbf{00,0} \\
\mathbf{00,1} \\
\mathbf{01,0} \\
\mathbf{01,1} \\
\mathbf{10,0} \\
\mathbf{10,1} \\
\mathbf{11,0} \\
\mathbf{11,1}
\end{array}
\begin{array}{c}
\begin{array}{cccccccc}
\mathbf{00,0} & \mathbf{00,1} & \mathbf{01,0} & \mathbf{01,1} & \mathbf{10,0} & \mathbf{10,1} & \mathbf{11,0} & \mathbf{11,1}
\end{array} \\
\begin{bmatrix}
 & 1 & & & & & & \\
1 & & & & & & & \\
 & & & 1 & & & & \\
 & & 1 & & & & & \\
 & & & & 1 & & & \\
 & & & & & 1 & & \\
 & & & & & & 1 & \\
 & & & & & & & 1
\end{bmatrix}
\end{array}
$$

This is the circuit instantiation of the oracle when $f(10) = 10$ and the input register is 0. ie, $Uf : |10\rangle |0\rangle :\rightarrow |10\rangle |0\rangle$

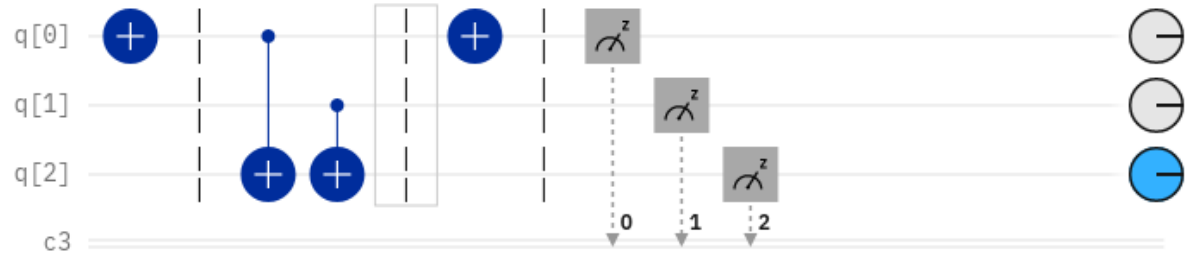
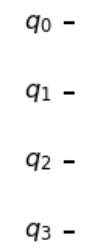
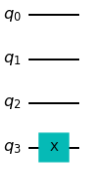


Figure 4.2: The circuit implementation of a balanced quantum oracle

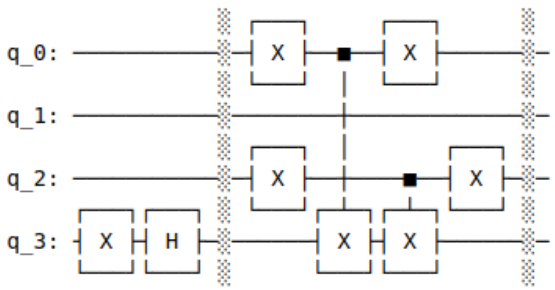
4.6 Qiskit Implementation

```
from qiskit import QuantumCircuit, execute, Aer, BasicAer
from qiskit.visualization import plot_histogram

import numpy as np
n=3
f0allx = QuantumCircuit(n+1) #constant oracle for f(x)=0 for all x


display(f0allx.draw())

f1allx = QuantumCircuit(n+1) #constant oracle for f(x)=1 for all x
f1allx.x(n)

display(f1allx.draw())
```

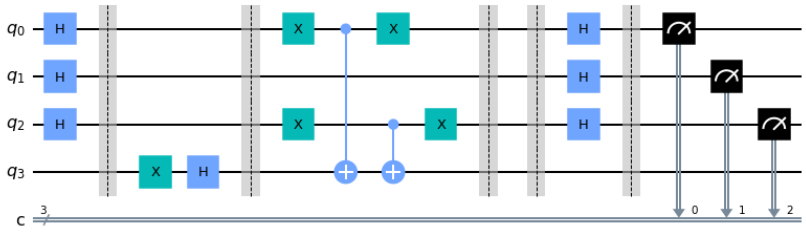




```
f01half = QuantumCircuit(n+1)
xgates = "101"
cxgates= "101"


# Put ancilia qubit in state |->
f01half.x(n)
f01half.h(n)

f01half.barrier()
# Place X-gates before implementing CX gates in the next loop
for i in range(n):
    if xgates[i] == '1':
        f01half.x(i)




# Place CX-gates to give phase at desired combinations
for m in range(n):
    if cxgates[m] == '1':
        f01half.cx(m,n)


# Place X-gates again to revert to original inputs on 0 to n-1
↪  qubits
for k in range(n):
    if xgates[k] == '1':
        f01half.x(k)
f01half.barrier()
# Show oracle
f01half.draw()
```



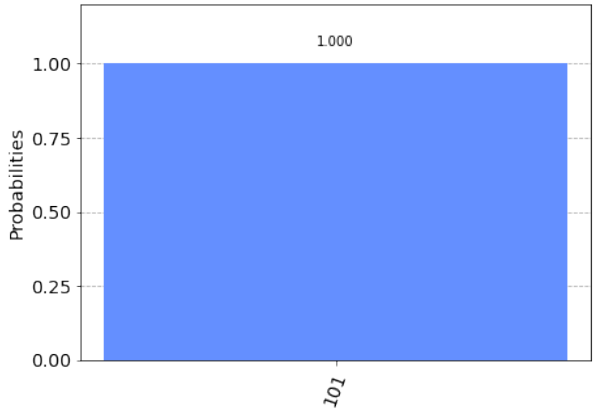
```
dj_circuit = QuantumCircuit(n+1, n)

# Apply H-gates
for qubit in range(n):
    dj_circuit.h(qubit)



dj_circuit.barrier()
# Add oracle
dj_circuit =dj_circuit + f01half
dj_circuit.barrier()
# Repeat H-gates
for qubit in range(n):
    dj_circuit.h(qubit)
dj_circuit.barrier()

# Measure
for i in range(n):
    dj_circuit.measure(i, i)

# Display circuit
dj_circuit.draw('mpl')
```



4.7 Simulating Using QasmSimulator:

```
# use local simulator
backend = BasicAer.get_backend('qasm_simulator')
shots = 1024
results = execute(dj_circuit, backend=backend, shots=shots).result()
answer = results.get_counts()

plot_histogram(answer)
```

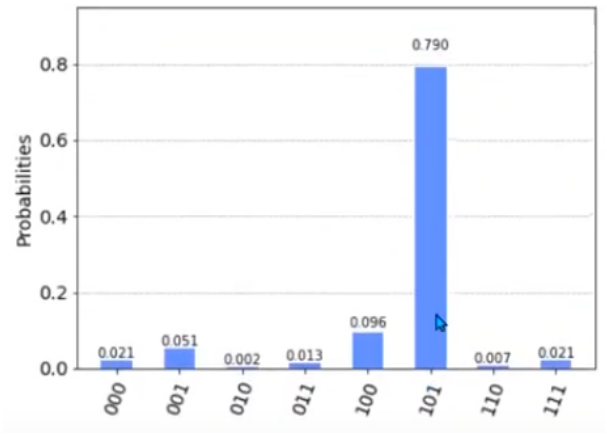
We perform the simulation using QasmSimulator and expect to see 101 for a balanced oracle. The circuit is executed and results are now visualized as count plot —



This shows that 0% chance of predicting 000, i.e. oracle is balanced.

4.8 Using IBM Quantum Computer

I've run the same circuit in a quantum computer. I've used IBM Quantum Computer and checked on IBM-Q (quantum simulator) which has the least number of jobs on queue.



Testing DJ algorithm with a balanced oracle, on a quantum computer shows us that most likely result is 101. Compared to the simulated case the real device is still susceptible to quantum noise and thus we can see components other than $|101\rangle$ are present too.

5 Conclusion

Finally, to conclude we have gone through the theory, necessary mathematics of one of the fundamental quantum computing algorithms, Deutsch-Jozsa algorithm, and eventually checked our understanding by testing it against a balanced oracle using Qiskit.

References

[1] R. P. Feynman, "Simulating physics with computers," in *Feynman and computation*. CRC Press, 2018, pp. 133–153.

[2] V. Hassija, V. Chamola, A. Goyal, S. S. Kanhere, and N. Guizani, "Forthcoming applications of quantum computing: peeking into the future," *IET Quantum Communication*, vol. 1, no. 2, pp. 35–41, 2020.

[3] J. Preskill, "Lecture notes for physics 229: Quantum information and computation," *California Institute of Technology*, vol. 16, no. 1, pp. 1–8, 1998.

[4] D. Deutsch and R. Jozsa, "Rapid solution of problems by quantum computation," *Proceedings of the Royal Society of London. Series A: Mathematical and Physical Sciences*, vol. 439, no. 1907, pp. 553–558, 1992.

[5] N. S. Yanofsky and M. A. Mannucci, *Quantum computing for computer scientists*. Cambridge University Press, 2008.

[6] "Qiskit-textbook," https://learn.qiskit.org/course/ch-algorithms/deutsch-jozsa-algorithm, accessed: 12 june 2022.