Deutsch's Algorithm and the Deutsch-Jozsa Algorithm

P. Venkata Subba Reddy
Department of CSE
NIT Warangal

One Week Hybrid Workshop on
Quantum Computing & Algorithms
Department of Information Technology, NIT Raipur

October 09, 2024

Outline

- Constant and Balanced Functions
- Deutsh's Problem
- Query Model of Computation
- Deutsch's Algorithm
- Deutsh-Jozsa Problem
- Deutsh-Jozsa Algorithm
- Summary
- References

Function : Definition

A function f from a set X to a set Y, denoted $f : X \rightarrow Y$, is a rule that assigns to every element $x \in X$ exactly one element $y \in Y$, where $y = f(x)$.

Example:

Determine the number of distinct functions from $\{0, 1\}$ to $\{0, 1\}$.

Determine the number of distinct functions from $\{0, 1\}$ to $\{0, 1\}$.

Input (x)	$f_1(x)$	$f_2(x)$	$f_3(x)$	$f_4(x)$
0	0	0	1	1
1	0	1	0	1

Table 1: All Boolean functions from $\{0, 1\}$ to $\{0, 1\}$.

Determine the number of distinct functions from $\{0,1\}^2 = \{00, 01, 10, 11\}$ to $\{0,1\}$.

Determine the number of distinct functions from $\{0,1\}^2 = \{00, 01, 10, 11\}$ to $\{0,1\}$.

x_1	x_2	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8	f_9	f_{10}	f_{11}	f_{12}	f_{13}	f_{14}	f_{15}	f_{16}
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	1	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
1	0	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
1	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1

Table 2: All Boolean functions from $\{0,1\}^2 = \{00, 01, 10, 11\}$ to $\{0,1\}$.

Constant Function

- A function f is called a constant function if there exists a constant c such that for every input x in the domain of f, the output is always c. This can be written as:

$$f(x) = c,$$

where c is a fixed number.

Constant Function

- A function f is called a constant function if there exists a constant c such that for every input x in the domain of f, the output is always c. This can be written as:

  $$f(x) = c,$$

  where c is a fixed number.

- A Boolean function that returns either 0 for every possible input in its domain, or 1 for every input in its domain, is called a constant function.

Constant Function

- A function f is called a constant function if there exists a constant c such that for every input x in the domain of f, the output is always c. This can be written as:

$$f(x) = c,$$

  where c is a fixed number.

- A Boolean function that returns either 0 for every possible input in its domain, or 1 for every input in its domain, is called a constant function.

- A Boolean function $f : \{0, 1\} \rightarrow \{0, 1\}$, is called constant if $f(0) = f(1)$.

Constant Function : Example

A Boolean function $f : \{0,1\} \to \{0,1\}$, is called constant if $f(0) = f(1)$.

Determine the number of distinct constant functions from $\{0,1\}$ to $\{0,1\}$.

Constant Function : Example

A Boolean function $f : \{0,1\} \to \{0,1\}$, is called constant if $f(0) = f(1)$.

Determine the number of distinct constant functions from $\{0,1\}$ to $\{0,1\}$.

Input (x)	$f_1(x)$	$f_2(x)$	$f_3(x)$	$f_4(x)$
0	0	0	1	1
1	0	1	0	1

Balanced Function

- A Boolean function $f : \{0, 1\} \to \{0, 1\}$, is called balanced if $f(0) \neq f(1)$.

Balanced Function

- A Boolean function $f : \{0,1\} \to \{0,1\}$, is called balanced if $f(0) \neq f(1)$.
- A Boolean function $f : \{0,1\} \to \{0,1\}$, is called balanced if it returns:
  - 0 for exactly half of the inputs, and
  - 1 for the other half of the inputs.

Balanced Function : Example

A Boolean function $f : \{0,1\} \rightarrow \{0,1\}$, is called balanced if $f(0) \neq f(1)$.

Determine the number of distinct balanced functions from $\{0,1\}$ to $\{0,1\}$.

Balanced Function : Example

A Boolean function $f : \{0,1\} \to \{0,1\}$, is called balanced if $f(0) \neq f(1)$.

Determine the number of distinct balanced functions from $\{0,1\}$ to $\{0,1\}$.

Input (x)	$f_1(x)$	$f_2(x)$	$f_3(x)$	$f_4(x)$
0	0	0	1	1
1	0	1	0	1

Deutsch's Problem

Given a Boolean function, $f\colon \{0,1\} \rightarrow \{0,1\}$, determine whether it is a constant function or a balanced function.

Given a Boolean function, $f : \{0,1\} \to \{0,1\}$, determine whether it is a constant function or a balanced function.

Classical Algorithm :

Deutsch's Problem

Given a Boolean function, $f: \{0, 1\} \rightarrow \{0, 1\}$, determine whether it is a constant function or a balanced function.

Classical Algorithm :

1. Query f with input 0 and determine $f(0)$.

Deutsch's Problem

Given a Boolean function, $f: \{0,1\} \rightarrow \{0,1\}$, determine whether it is a constant function or a balanced function.

Classical Algorithm :

1. Query f with input 0 and determine $f(0)$.
2. Query f with input 1 and determine $f(1)$.

Deutsch's Problem

Given a Boolean function, $f: \{0,1\} \to \{0,1\}$, determine whether it is a constant function or a balanced function.

Classical Algorithm :

1. Query f with input 0 and determine $f(0)$.
2. Query f with input 1 and determine $f(1)$.
3. If $f(0) = f(1)$ then print "f is a constant function."

Deutsch's Problem

Given a Boolean function, $f: \{0,1\} \rightarrow \{0,1\}$, determine whether it is a constant function or a balanced function.

Classical Algorithm :

1. Query f with input 0 and determine $f(0)$.
2. Query f with input 1 and determine $f(1)$.
3. If $f(0) = f(1)$ then print "f is a constant function."
4. Else print "f is a balanced function."

Deutsch's Problem

Given a Boolean function, $f : \{0, 1\} \to \{0, 1\}$, determine whether it is a constant function or a balanced function.

Classical Algorithm :

1. Query f with input 0 and determine $f(0)$.
2. Query f with input 1 and determine $f(1)$.
3. If $f(0) = f(1)$ then print "f is a constant function."
4. Else print "f is a balanced function."

Note. Classical algorithm requires two queries i.e., two evaluations of f to solve the Deutsch problem.

Deutsch's Problem

Given a Boolean function, $f\colon \{0,1\} \to \{0,1\}$, determine whether it is a constant function or a balanced function.

Classical Algorithm :

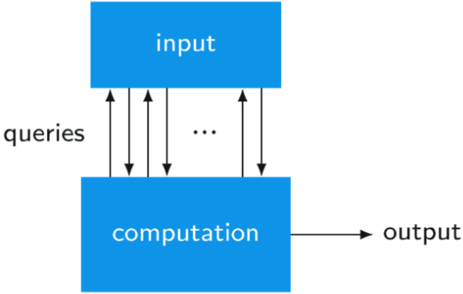
1. Query f with input 0 and determine $f(0)$.
2. Query f with input 1 and determine $f(1)$.
3. If $f(0) = f(1)$ then print "f is a constant function."
4. Else print "f is a balanced function."

Note. Classical algorithm requires two queries i.e., two evaluations of f to solve the Deutsch problem.

The Deutsch algorithm, a quantum algorithm, solves the Deutsch problem using only one query.

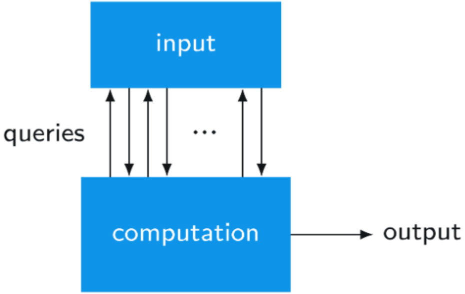
What is query model of computation?

- The query model of computation, also known as the black-box model, is a computational framework where an algorithm gains information about a problem instance by querying an oracle.



What is query model of computation?

- The query model of computation, also known as the black-box model, is a computational framework where an algorithm gains information about a problem instance by querying an oracle.



- In the query model of computation, the entire input is not provided to the computation. Rather, the input is made available in the form of a function, which the computation accesses by making queries.

Quantum Algorithm - Definition

Quantum Algorithm - Definition

A quantum algorithm is a step-by-step procedure for solving a problem using the principles of quantum mechanics.

Quantum Algorithm - Definition

A quantum algorithm is a step-by-step procedure for solving a problem using the principles of quantum mechanics.

A quantum algorithm involves the following steps:

Quantum Algorithm - Definition

A quantum algorithm is a step-by-step procedure for solving a problem using the principles of quantum mechanics.

A quantum algorithm involves the following steps:

1. Input: Initialize the quantum system in a desired state.

Quantum Algorithm - Definition

A quantum algorithm is a step-by-step procedure for solving a problem using the principles of quantum mechanics.

A quantum algorithm involves the following steps:

1. Input: Initialize the quantum system in a desired state.
2. Computation: Sequentially apply quantum gates to the entire system or a subsystem to solve the desired problem.

Quantum Algorithm - Definition

A quantum algorithm is a step-by-step procedure for solving a problem using the principles of quantum mechanics.

A quantum algorithm involves the following steps:

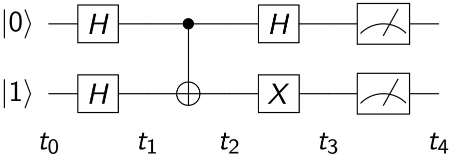
1. Input: Initialize the quantum system in a desired state.
2. Computation: Sequentially apply quantum gates to the entire system or a subsystem to solve the desired problem.
3. Output: Measure the resulting quantum state of the system or a subsystem to obtain a desired outcome with a specified probability.

A quantum algorithm is a step-by-step procedure for solving a problem using the principles of quantum mechanics.

A quantum algorithm involves the following steps:

1. Input: Initialize the quantum system in a desired state.
2. Computation: Sequentially apply quantum gates to the entire system or a subsystem to solve the desired problem.
3. Output: Measure the resulting quantum state of the system or a subsystem to obtain a desired outcome with a specified probability.

Example:



Quantum Algorithms Timeline

1. Deutsch Algorithm (1985)
2. Deutsch-Jozsa Algorithm (1992)
3. Bernstein-Vazirani Algorithm (1992)
4. Simon's Algorithm (1993)
5. Shor's Algorithm (1994)
6. Grover's Algorithm (1996)
7. Variational Quantum Eigensolver (2014)
8. Quantum Approximate Optimization Algorithm (2014)
9. Quantum Computing in Cloud by IBM (2016)
10. Quantum Machine Learning (2018)

In the study of quantum query complexity, one is given a black box U_f implementing some function f, and asked what the minimum number of required queries to U_f is in order to determine some desired property of f.

Deutsch's Algorithm

- Deutsch Algorithm was proposed by David Deutsch in 1985.

- Deutsch Algorithm was proposed by David Deutsch in 1985.
- Deutsch algorithm was one of the first examples demonstrating the potential of quantum computing to solve certain problems more efficiently than classical computing.

Prof. David Deutsch

Quantum Circuit for the Deutsch's Algorithm

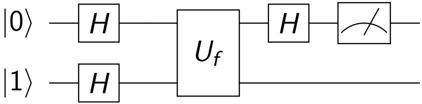
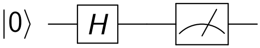


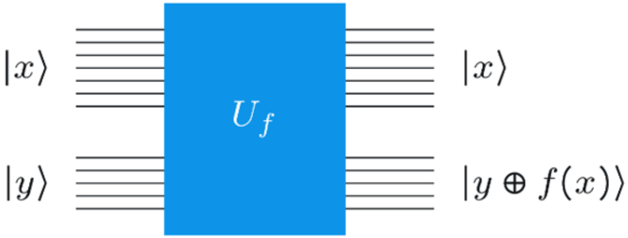
Figure 1: Quantum circuit for the Deutsch algorithm

Hadamard Gate

- The Hadamard gate is a single qubit gate.
- The Hadamard gate has the matrix : $\begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix}$
- Circuit with H gate: $|q\rangle \;—\boxed{H}—$
- 

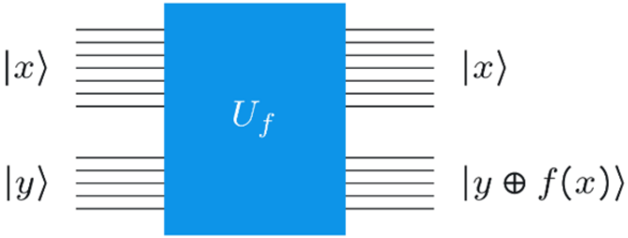
- Matrix for $|0\rangle$ is : $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$
- Output of the above circuit is : $\mathrm{H}(|0\rangle) =$
$\begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = |+\rangle.$
- Similarly, $\mathrm{H}(|1\rangle) =$
$\begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = |-\rangle.$

Quantum Query Gates



- In circuit model of computation, queries are made by special gates called query gates.

Quantum Query Gates



- In circuit model of computation, queries are made by special gates called query gates.
- An operation which takes qubits $|x\rangle$ and $|y\rangle$ as input and produces $|x\rangle$ and $|y \oplus f(x)\rangle$ as output is an unitary operation.

Analysis of Deutsch Algorithm

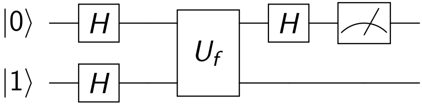


Figure 2: Quantum circuit for the Deutsch algorithm

Constant and Balanced Functions - A Generalization

- A Boolean function $f : \{0,1\}^n \to \{0,1\}$, is called constant if the function produces the same output (either all 0s or all 1s) for every input x, i.e.,

$$f(x) = f(y) \text{ for all } x, y \in \{0,1\}^n.$$

Constant and Balanced Functions - A Generalization

- A Boolean function $f : \{0,1\}^n \to \{0,1\}$, is called constant if the function produces the same output (either all 0s or all 1s) for every input x, i.e.,

$$f(x) = f(y) \text{ for all } x, y \in \{0,1\}^n.$$

- A Boolean function $f : \{0,1\}^n \to \{0,1\}$, is called balanced if it returns:
  - 0 for exactly half of the inputs, and
  - 1 for the other half of the inputs.

  i.e.,

Constant and Balanced Functions - A Generalization

- A Boolean function $f : \{0,1\}^n \to \{0,1\}$, is called constant if the function produces the same output (either all 0s or all 1s) for every input x, i.e.,

$$f(x) = f(y) \text{ for all } x, y \in \{0,1\}^n.$$

- A Boolean function $f : \{0,1\}^n \to \{0,1\}$, is called balanced if it returns:
  - 0 for exactly half of the inputs, and
  - 1 for the other half of the inputs.

  i.e.,

$$f(x) = 0 \text{ for half of the } 2^n \text{ inputs, and } f(x) = 1 \text{ for the other half.}$$

Example

Determine the number of distinct constant functions and the balanced functions from $\{0,1\}^2 = \{00, 01, 10, 11\}$ to $\{0,1\}$.

x_1	x_2	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8	f_9	f_{10}	f_{11}	f_{12}	f_{13}	f_{14}	f_{15}	f_{16}
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	1	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
1	0	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
1	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1

Table 3: All Boolean functions from $\{0,1\}^2 = \{00, 01, 10, 11\}$ to $\{0,1\}$.

Example

Determine the number of distinct constant functions and the balanced functions from $\{0,1\}^2 = \{00, 01, 10, 11\}$ to $\{0,1\}$.

x_1	x_2	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8	f_9	f_{10}	f_{11}	f_{12}	f_{13}	f_{14}	f_{15}	f_{16}
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	1	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
1	0	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
1	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1

Table 3: All Boolean functions from $\{0,1\}^2 = \{00, 01, 10, 11\}$ to $\{0,1\}$.

f_1:

Determine the number of distinct constant functions and the balanced functions from $\{0,1\}^2 = \{00, 01, 10, 11\}$ to $\{0,1\}$.

x_1	x_2	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8	f_9	f_{10}	f_{11}	f_{12}	f_{13}	f_{14}	f_{15}	f_{16}
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	1	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
1	0	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
1	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1

Table 3: All Boolean functions from $\{0,1\}^2 = \{00, 01, 10, 11\}$ to $\{0,1\}$.

f_1:

f_4:

Example

Determine the number of distinct constant functions and the balanced functions from $\{0,1\}^2 = \{00, 01, 10, 11\}$ to $\{0,1\}$.

x_1	x_2	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8	f_9	f_{10}	f_{11}	f_{12}	f_{13}	f_{14}	f_{15}	f_{16}
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	1	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
1	0	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
1	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1

Table 3: All Boolean functions from $\{0,1\}^2 = \{00, 01, 10, 11\}$ to $\{0,1\}$.

f_1:
f_4:
f_2:

Determine the number of distinct constant functions and the balanced functions from $\{0,1\}^2 = \{00, 01, 10, 11\}$ to $\{0,1\}$.

x_1	x_2	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8	f_9	f_{10}	f_{11}	f_{12}	f_{13}	f_{14}	f_{15}	f_{16}
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	1	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
1	0	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
1	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1

Table 3: All Boolean functions from $\{0,1\}^2 = \{00, 01, 10, 11\}$ to $\{0,1\}$.

f_1:
f_4:
f_2:
How many queries, i.e., evaluations of f_1, are needed to determine if f_1 is a constant function?

Example

Determine the number of distinct constant functions and the balanced functions from $\{0,1\}^2 = \{00, 01, 10, 11\}$ to $\{0,1\}$.

x_1	x_2	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8	f_9	f_{10}	f_{11}	f_{12}	f_{13}	f_{14}	f_{15}	f_{16}
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	1	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
1	0	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
1	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1

Table 3: All Boolean functions from $\{0,1\}^2 = \{00, 01, 10, 11\}$ to $\{0,1\}$.

f_1:
f_4:
f_2:
How many queries, i.e., evaluations of f_1, are needed to determine if f_1 is a constant function?

Minimum number of queries, i.e., evaluations of f_1, needed to determine if f_1 is a constant function is :

Example

p	q	r	$f(p,q,r)$	$g(p,q,r)$	$h(p,q,r)$
0	0	0	0	1	0
0	0	1	0	0	1
0	1	0	0	0	0
0	1	1	0	1	0
1	0	0	0	0	1
1	0	1	0	1	1
1	1	0	0	1	1
1	1	1	0	0	1

- The function f is :

Example

p	q	r	$f(p,q,r)$	$g(p,q,r)$	$h(p,q,r)$
0	0	0	0	1	0
0	0	1	0	0	1
0	1	0	0	0	0
0	1	1	0	1	0
1	0	0	0	0	1
1	0	1	0	1	1
1	1	0	0	1	1
1	1	1	0	0	1

- The function f is : constant
- The function g is :

Example

p	q	r	$f(p,q,r)$	$g(p,q,r)$	$h(p,q,r)$
0	0	0	0	1	0
0	0	1	0	0	1
0	1	0	0	0	0
0	1	1	0	1	0
1	0	0	0	0	1
1	0	1	0	1	1
1	1	0	0	1	1
1	1	1	0	0	1

- The function f is : constant
- The function g is : balanced
- The function h is :

Example

p	q	r	$f(p,q,r)$	$g(p,q,r)$	$h(p,q,r)$
0	0	0	0	1	0
0	0	1	0	0	1
0	1	0	0	0	0
0	1	1	0	1	0
1	0	0	0	0	1
1	0	1	0	1	1
1	1	0	0	1	1
1	1	1	0	0	1

- The function f is : constant
- The function g is : balanced
- The function h is : neither constant nor balanced

Example

p	q	r	$f(p,q,r)$	$g(p,q,r)$	$h(p,q,r)$
0	0	0	0	1	0
0	0	1	0	0	1
0	1	0	0	0	0
0	1	1	0	1	0
1	0	0	0	0	1
1	0	1	0	1	1
1	1	0	0	1	1
1	1	1	0	0	1

- The function f is : constant
- The function g is : balanced
- The function h is : neither constant nor balanced
- Minimum number of queries, i.e., evaluations of g, needed to determine if g is a balanced function is :

Deutsch-Jozsa Problem

Given a Boolean function $f(x)$, where $f : \{0,1\}^n \to \{0,1\}$ for an n-bit input string x, and where the function is either constant or balanced, determine whether the function $f(x)$ is constant or balanced.

Classical Algorithm for the Deutsh-Jozsa Problem

- Given a Boolean function $f\colon \{0,1\}^n \to \{0,1\}$, there are 2^n different input strings corresponding to the decimal values $0, 1, 2, \ldots, 2^n - 1$.

Classical Algorithm for the Deutsh-Jozsa Problem

- Given a Boolean function $f\colon \{0,1\}^n \to \{0,1\}$, there are 2^n different input strings corresponding to the decimal values $0, 1, 2, \ldots, 2^n - 1$.
- Any classical algorithm for the Deutsch-Jozsa problem on an n-bit input string requires at least $2^{n-1} + 1$ queries in the worst case to determine if the function is constant or balanced.

Classical Algorithm for the Deutsh-Jozsa Problem

- Given a Boolean function $f : \{0,1\}^n \to \{0,1\}$, there are 2^n different input strings corresponding to the decimal values $0, 1, 2, \ldots, 2^n - 1$.
- Any classical algorithm for the Deutsch-Jozsa problem on an n-bit input string requires at least $2^{n-1} + 1$ queries in the worst case to determine if the function is constant or balanced.
- The Deutsch-Jozsa algorithm, solves the Deutsch-Jozsa problem using only one query.

The Deutsch-Jozsa Algorithm

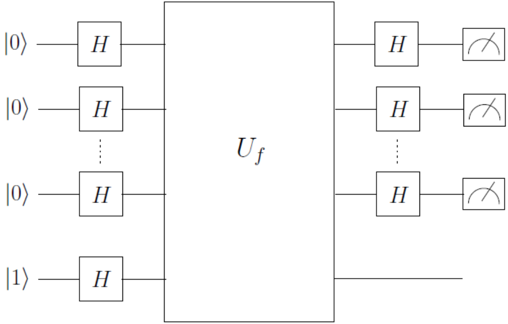
The Deutsch-Jozsa Algorithm was proposed by Deutsch and Jozsa in 1992 to solve the Deutsch-Jozsa problem.

The Deutsch-Jozsa Algorithm

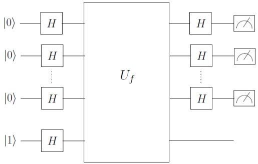
The Deutsch-Jozsa Algorithm was proposed by Deutsch and Jozsa in 1992 to solve the Deutsch-Jozsa problem. It solves the problem using only one query.

The Deutsch-Jozsa Algorithm was proposed by Deutsch and Jozsa in 1992 to solve the Deutsch-Jozsa problem. It solves the problem using only one query.

Quantum circuit for the Deutsch-Jozsa algorithm:



Analysis of the Deutsch-Jozsa Algorithm



Summary

- Query Model of Computation
- Deutsch's Algorithm
- Deutsch-Jozsa Algorithm
  The Deutsch-Jozsa highlights the potential for quantum algorithms to outperform classical counterparts in specific tasks.

References

1. Michael A. Nielsen and Issac L. Chuang, Quantum Computation and Quantum Information,. Cambridge, 2010, 10^{th} Anniversary Edition.
2. IBM Quantum Learning Course: https://learning.quantum.ibm.com/.
3. Lecture Notes : CMSC 491: Introduction to Quantum Computation by Prof. Sevag Gharibian.
4. YouTube Link: Introduction to Quantum Computing Complete Course - Quantum Soar.

Thank You