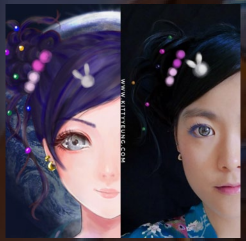
Introduction to Quantum Computing



Kitty Yeung, Ph.D. in Applied Physics

Creative Technologist + Sr. PM
Microsoft

www.artbyphysicistkittyyeung.com
@KittyArtPhysics
@artbyphysicistkittyyeung

May 10, 2020
Hackaday, session 7

Class structure

- Comics on Hackaday – Introduction to Quantum Computing every Wed & Sun

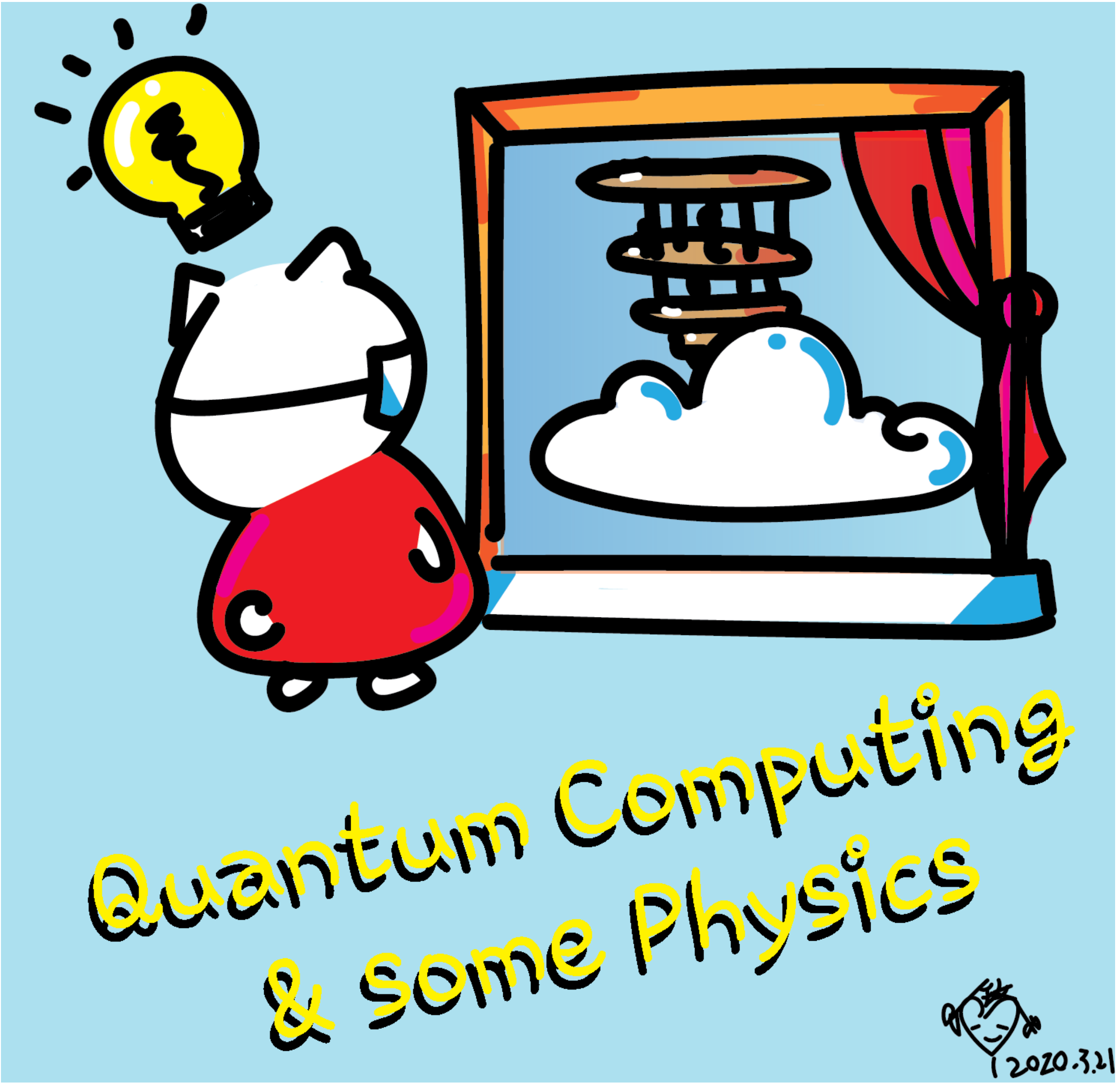
- 30 mins every Sun, one concept (theory, hardware, programming), Q&A

- Contribute to Q# documentation http://docs.microsoft.com/quantum

- Coding through Quantum Katas https://github.com/Microsoft/QuantumKatas/

- Discuss in Hackaday project comments throughout the week

- Take notes



Certificate 1

- Complete any one quantum katas
- Take a screenshot or photo
- Post on Twitter or LinkedIn
- **Twitter:** @KittyArtPhysics @MSFTQuantum @QSharpCommunity #QSharp #QuantumComputing #comics #physics
- **LinkedIn:** @Kitty Y. M Yeung #MSFTQuantum #QSharp #QuantumComputing #comics #physics

Quantum Algorithms

- Deutsch's: determines if a function $f(x)$ is *Balanced* ($f(0) \neq f(1)$, which is 1-to-1) or
- *Constant* ($f(0) = f(1)$, which is 2-to-1)

- Deutsch-Jozsa: a general case of Deutsch's algorithm for n-qubits

- Grover's: search for an item in an unordered list

- Simon's: query complexity, solves the problem exponentially faster than any deterministic or probabilistic classical algorithm, finds repeats in a list

- Shor's: given an integer N, find its prime factors

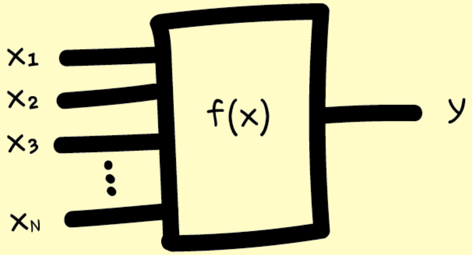
Can you come up with more useful algorithms?

- http://quantumalgorithmzoo.org/

Quantum Oracle

- An **oracle** was usually a priest or a priestess through whom the gods were supposed to speak or prophesize.
- An **oracle** is a person or agency considered to provide wise and insightful counsel or prophetic predictions or precognition of the future, inspired by the gods. As such it is a form of divination.

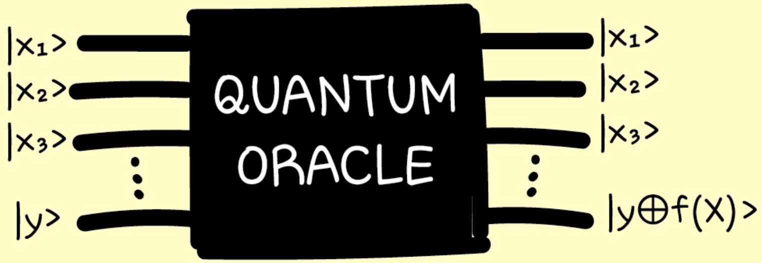
- An oracle is a "black box" operation that is used as input to another algorithm
- represent classical functions which return real numbers instead of only a single bit
- quantum operations which implement certain classical functions



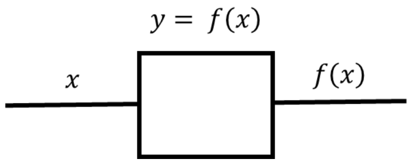
A classical algorithm takes inputs and produces an output. This algorithm is a function, f(x).

(This construction is not possible for a quantum algorithm, as f(x) can not guarantee to be a reversible.)

In many quantum algorithms, we put both the inputs and the output through a black box – a quantum **oracle**. The classical function f(x) is used to construct the black box.

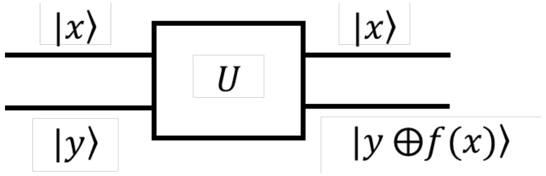


Oracles



Quantum needs unitary gates = reversible

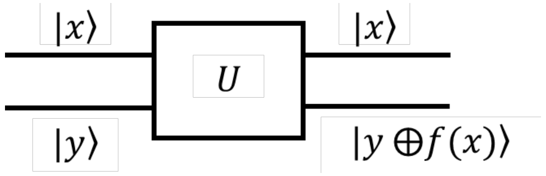
$$A^{\dagger}(y) = A^{-1}(y) = A^{-1}(Ax) = x$$



x	$y = f(x) = x \% 4$
0	0
1	1
2	2
3	3
4	0
5	1
6	2
7	3

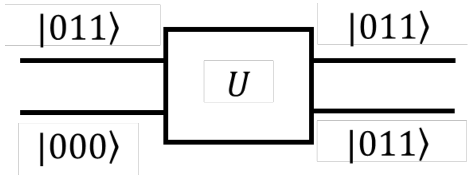
Cannot exist for circuit on the left

Oracles

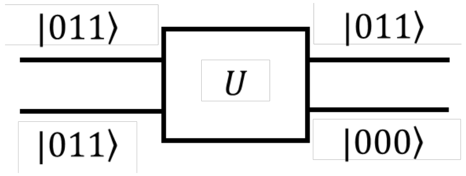


x	$y = f(x) = x \,\%\, 4$
0	0
1	1
2	2
3	3
4	0
5	1
6	2
7	3

for $x = 3 = |011\rangle$, with y initialized to $0 = |000\rangle$

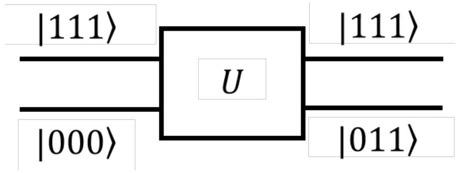


$U(|011\rangle, |000\rangle) = (|011\rangle, |000\rangle \oplus f(|011\rangle)) = (|011\rangle, |000\rangle \oplus |011\rangle) = (|011\rangle, |011\rangle)$

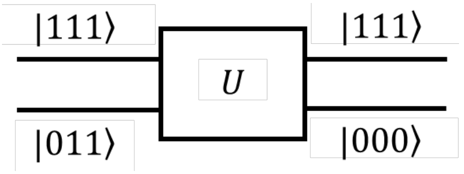


$U(|111\rangle, |000\rangle) = (|111\rangle, |000\rangle \oplus f(|111\rangle)) = (|111\rangle, |000\rangle \oplus |011\rangle) = (|111\rangle, |011\rangle)$

for $x = 7 = |111\rangle$, with y initialized to $0 = |000\rangle$

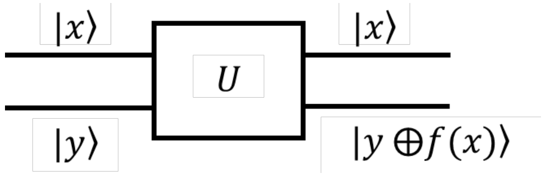


$U(|111\rangle, |000\rangle) = (|111\rangle, |000\rangle \oplus f(|111\rangle)) = (|111\rangle, |000\rangle \oplus |011\rangle) = (|111\rangle, |011\rangle)$



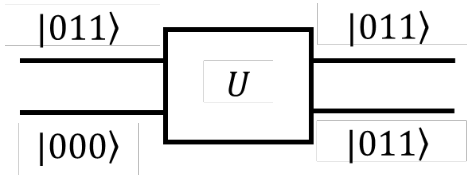
$U(|111\rangle, |011\rangle) = (|111\rangle, |011\rangle \oplus f(|111\rangle)) = (|111\rangle, |011\rangle \oplus |011\rangle) = (|111\rangle, |000\rangle)$

Oracles

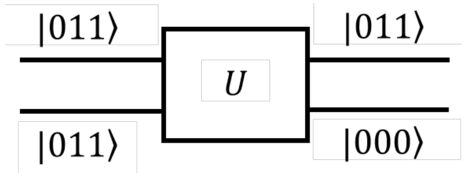


x	$y = f(x) = x \,\%\, 4$
0	0
1	1
2	2
3	3
4	0
5	1
6	2
7	3

for $x = 3 = |011\rangle$, with y initialized to $0 = |000\rangle$

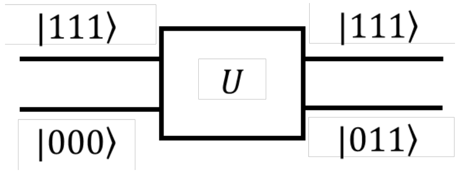


$U(|011\rangle, |000\rangle) = (|011\rangle, |000\rangle \oplus f(|011\rangle)\ = (|011\rangle, |000\rangle \oplus |011\rangle) = (|011\rangle, |011\rangle)$

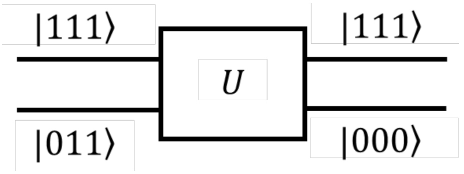


$U(|111\rangle, |000\rangle) = (|111\rangle, |000\rangle \oplus f(|111\rangle)\ = (|111\rangle, |000\rangle \oplus |011\rangle) = (|111\rangle, |011\rangle)$

for $x = 7 = |111\rangle$, with y initialized to $0 = |000\rangle$

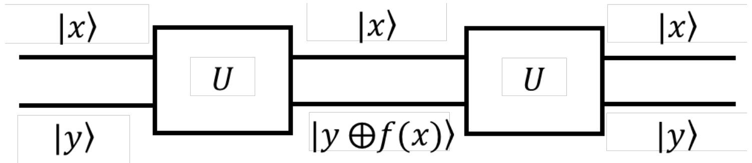


$U(|111\rangle, |000\rangle) = (|111\rangle, |000\rangle \oplus f(|111\rangle)\ = (|111\rangle, |000\rangle \oplus |011\rangle) = (|111\rangle, |011\rangle)$

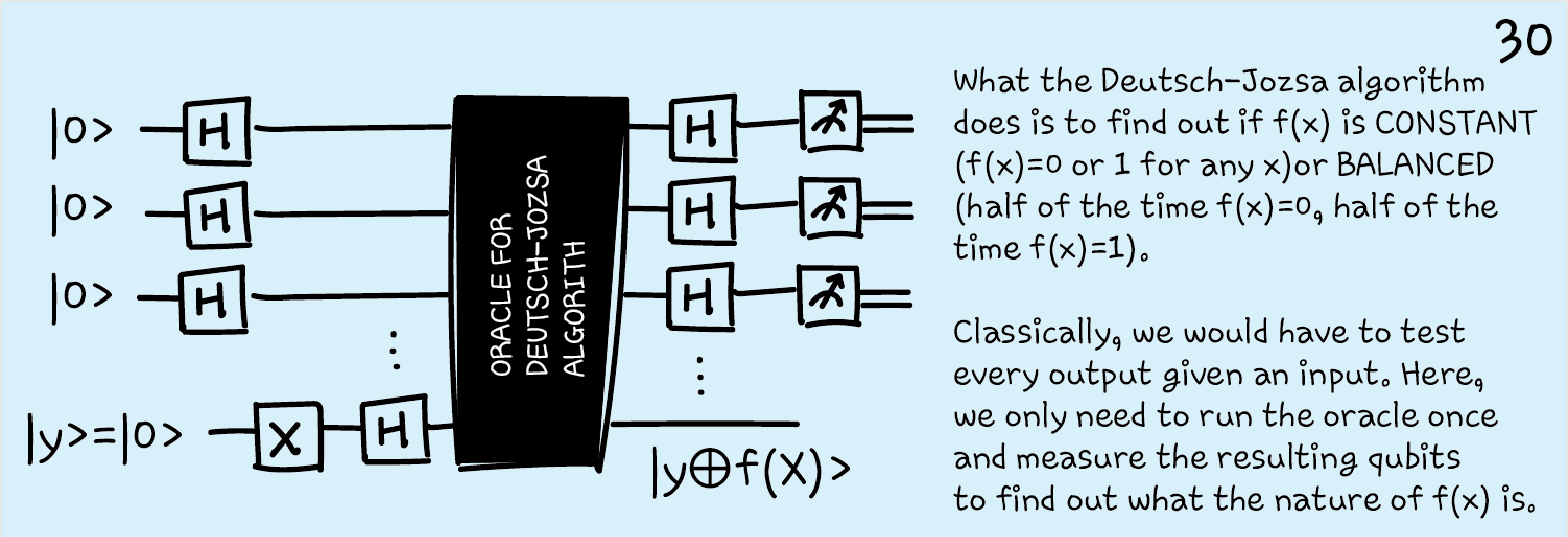


$U(|111\rangle, |011\rangle) = (|111\rangle, |011\rangle \oplus f(|111\rangle)\ = (|111\rangle, |011\rangle \oplus |011\rangle) = (|111\rangle, |000\rangle)$

$$U = U^{-1}$$



Deutsch-Jozsa algorithm

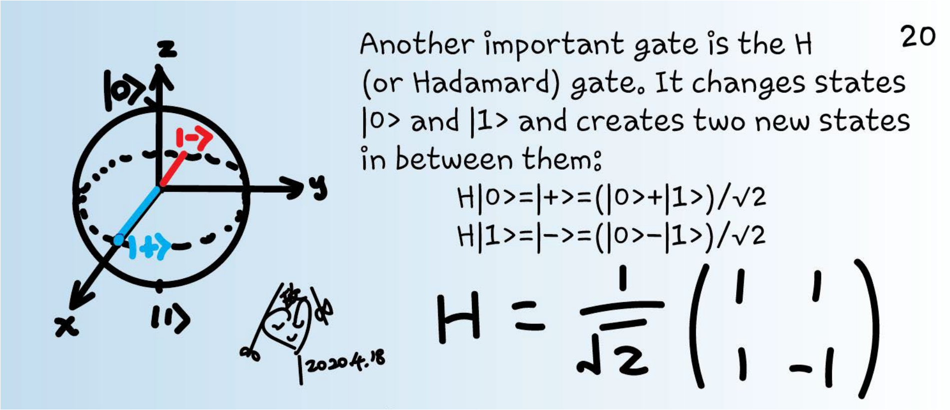


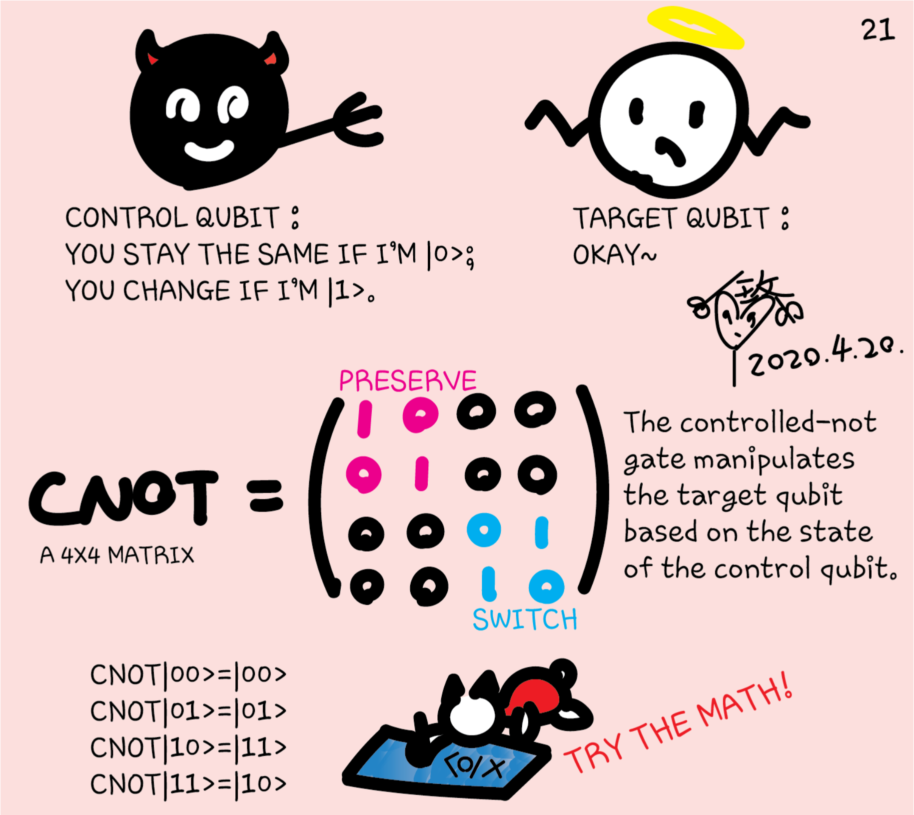
David Deutsch (physicist) - Wikipedia Translate this page
https://de.wikipedia.org/wiki/David_Deutsch_(Physiker) ▾

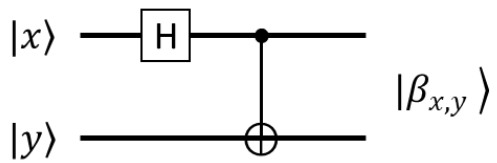
Overview Life literature Web links

David Deutsch (born May 18, 1953 in Haifa) is an Israeli-British physicist in the field of quantum information theory.

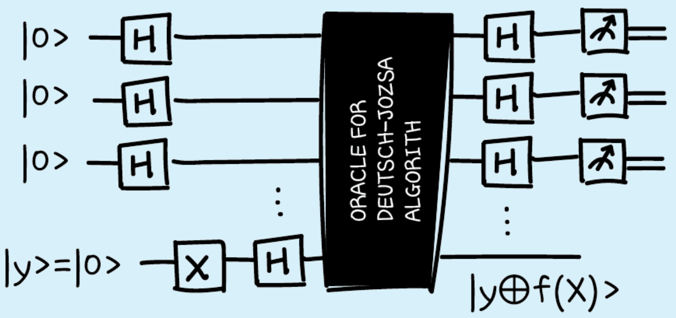
Richard Jozsa FRS is an Australian mathematician who holds the Leigh Trapnell Chair in Quantum Physics at the University of Cambridge.[3] He is a Fellow of King's College, Cambridge where his research investigates quantum information science. A pioneer of his field, he is the co-author of the Deutsch–Jozsa algorithm and one of the co-inventors of quantum teleportation.







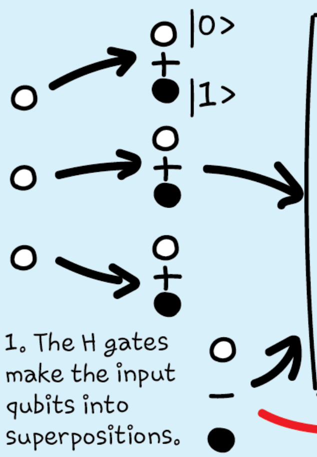
In	Out
$\|00\rangle$	$(\|00\rangle + \|11\rangle)/\sqrt{2} \equiv \|\beta_{00}\rangle$
$\|01\rangle$	$(\|01\rangle + \|10\rangle)/\sqrt{2} \equiv \|\beta_{01}\rangle$
$\|10\rangle$	$(\|00\rangle - \|11\rangle)/\sqrt{2} \equiv \|\beta_{10}\rangle$
$\|11\rangle$	$(\|01\rangle - \|10\rangle)/\sqrt{2} \equiv \|\beta_{11}\rangle$



What the Deutsch-Jozsa algorithm does is to find out if f(x) is CONSTANT (f(x)=0 or 1 for any x) or BALANCED (half of the time f(x)=0, half of the time f(x)=1).

Classically, we would have to test every output given an input. Here, we only need to run the oracle once and measure the resulting qubits to find out what the nature of f(x) is.

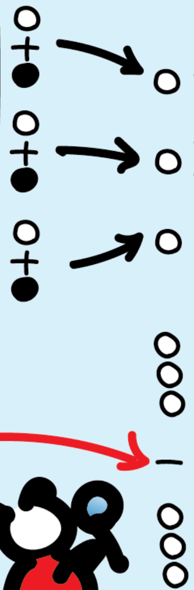
But intuitively, what is this algorithm really doing ?



1. The H gates make the input qubits into superpositions.

2. The last qubit comes in, introducing a negative sign in half of the amplitudes.

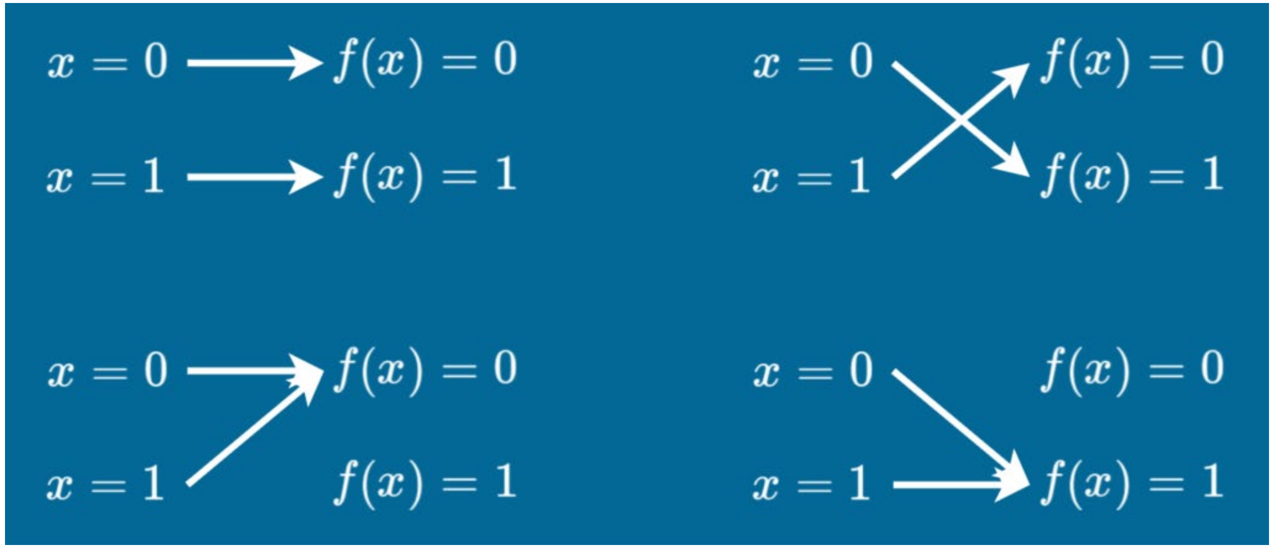
3. If f(x) is constant, the oracle does nothing to the input qubits. If it is balanced, it entangles the last qubit to one of the input qubits.



4(a). If nothing happens to the input qubits, they come out unchanged. The H gates put the superpositions back to |000...>. Hence, if |000...> is the state measured after the oracle, f(x) must be constant.

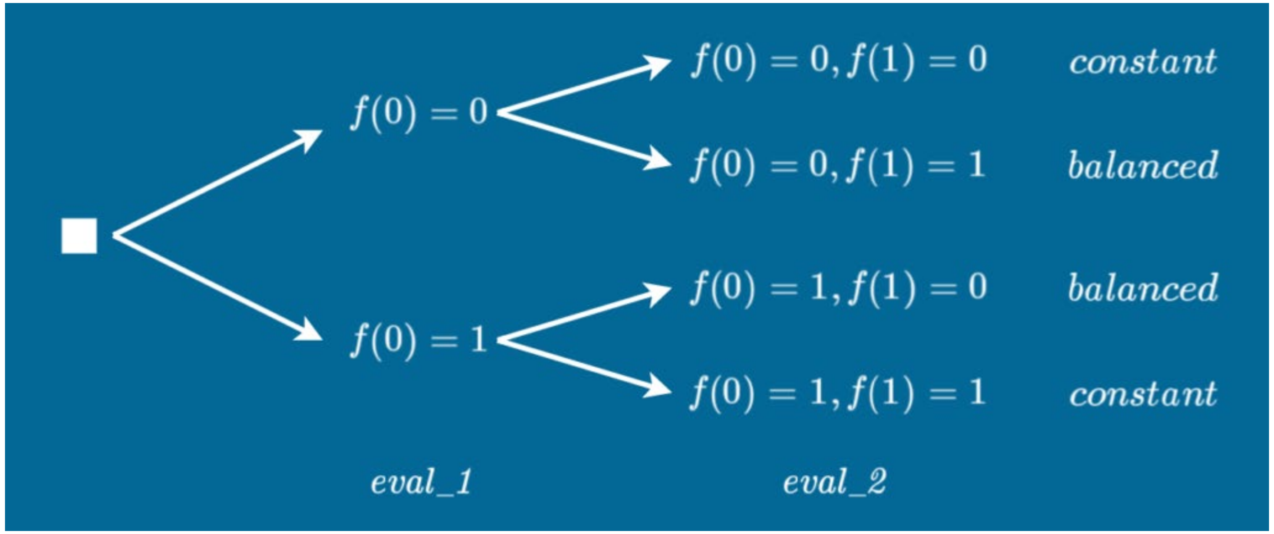
4(b). If entanglement happens the negative sign gets carried over. Half of the time there's |000...>, half of the time there's -|000...>. They destructively interfere. Thus, if we measure a |1> for any qubit at all, f(x) must be balanced, since there's zero probability of getting |000...> after the oracle.

Is a function balanced or constant?



Balanced

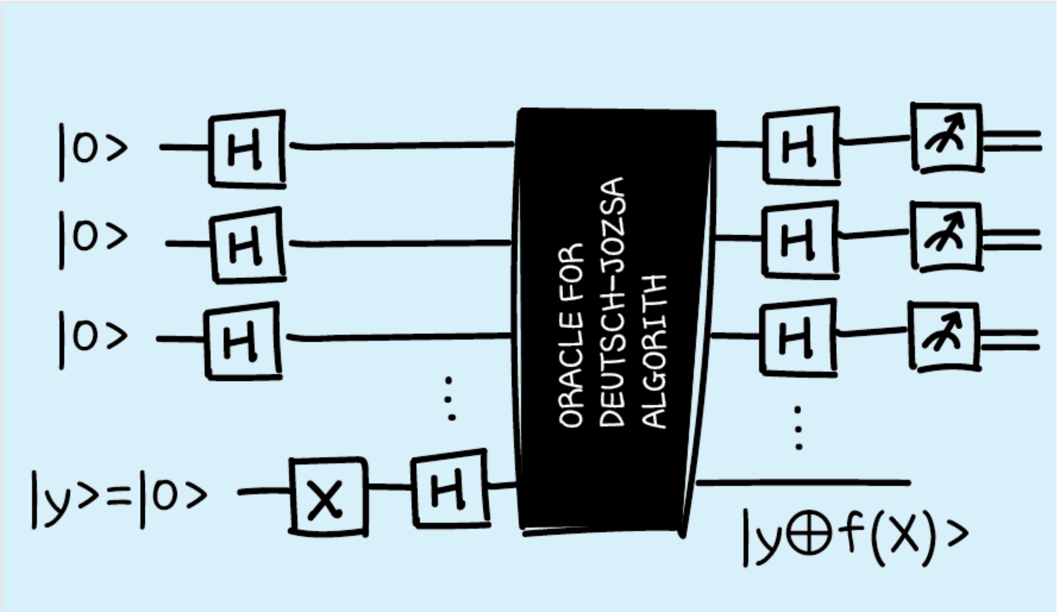
Constant

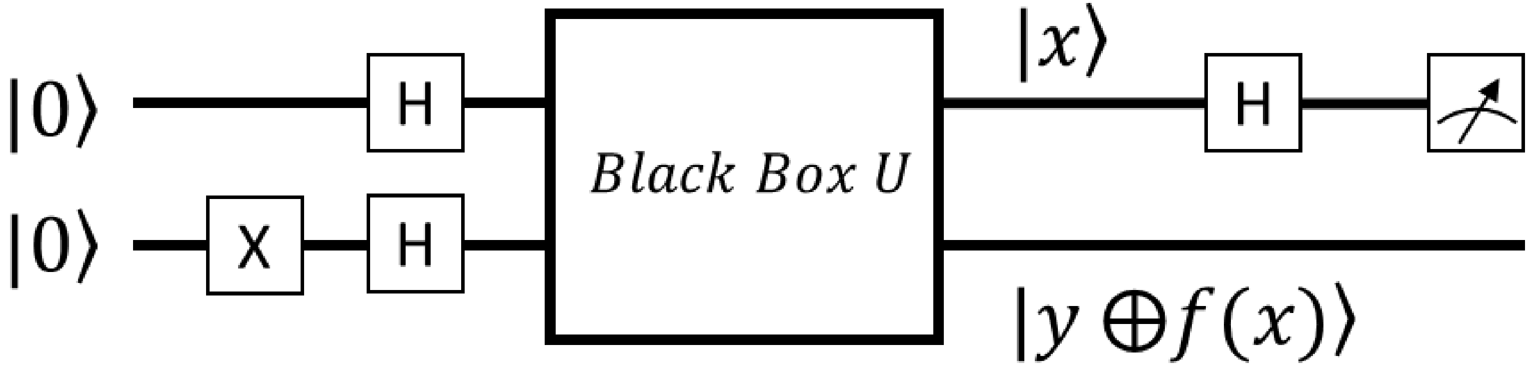


Classically

http://dkopczyk.quantee.co.uk/deutschs-algorithm/

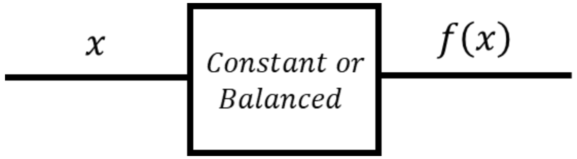
Deutsch's algorithm (2-qubit version of Deutsch-Jozsa)

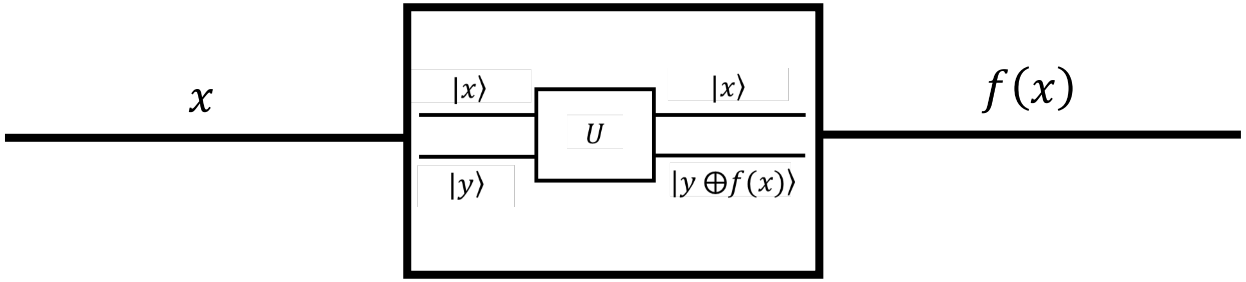


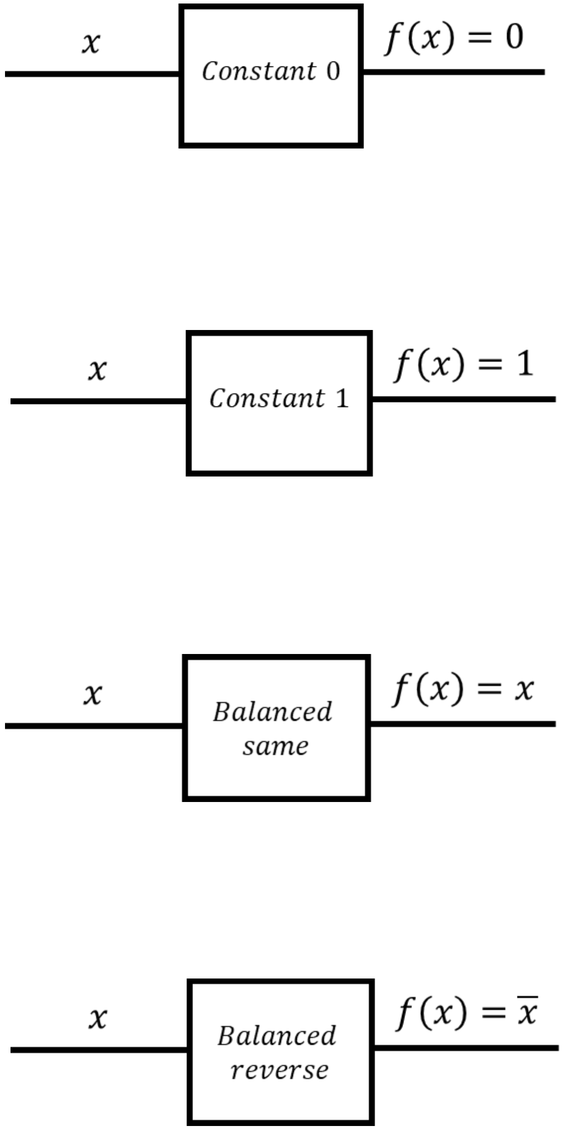


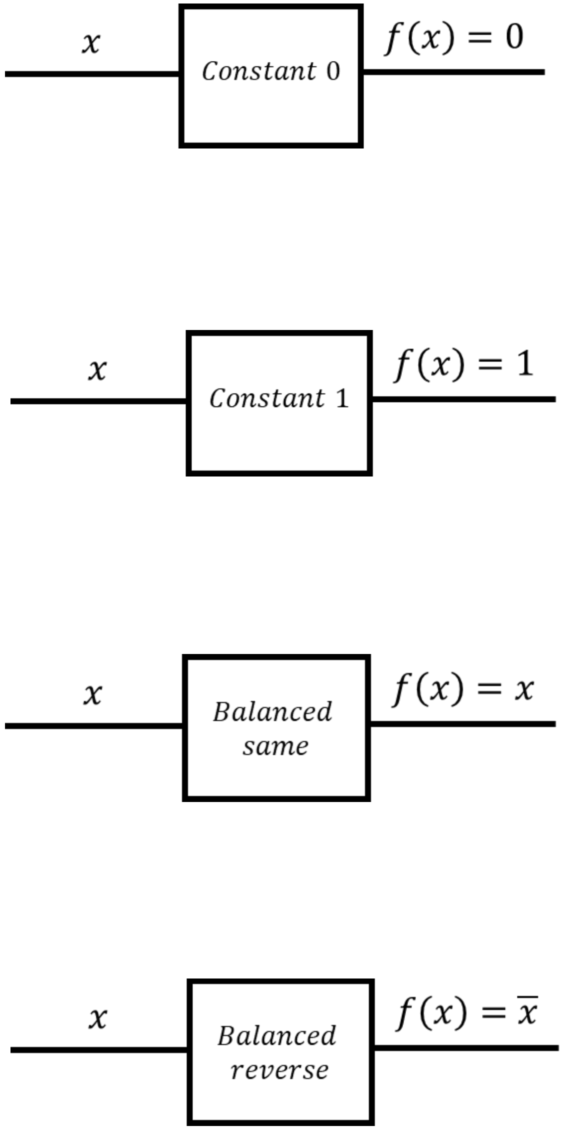
Deutsch’s algorithm

- Go to notes





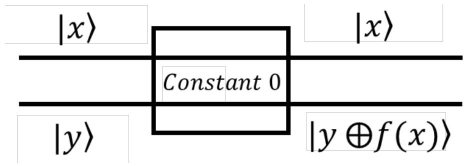

x
Constant 0
$f(x) = 0$
x
Constant 1
$f(x) = 1$
x
Balanced same
$f(x) = x$
x
Balanced reverse
$f(x) = \overline{x}$

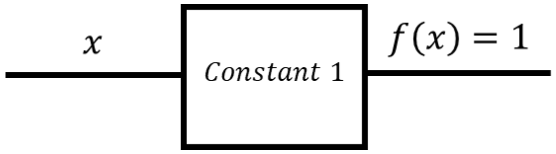


x	Constant 0: $f(x) = 0$
0	0
1	0

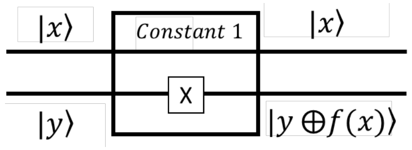
x	**Constant 0: $f(x) = 0$**
0	0
1	0

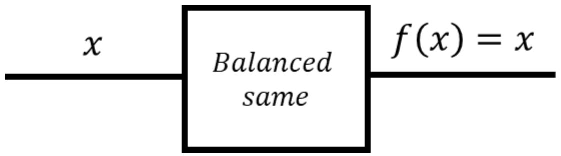
$\|x\rangle$	$\|y\rangle$	$f(x)$	$\|y \oplus f(x)\rangle$
$\|0\rangle$	$\|0\rangle$	0	$\|0\rangle$
$\|0\rangle$	$\|1\rangle$	0	$\|1\rangle$
$\|1\rangle$	$\|0\rangle$	0	$\|0\rangle$
$\|1\rangle$	$\|1\rangle$	0	$\|1\rangle$



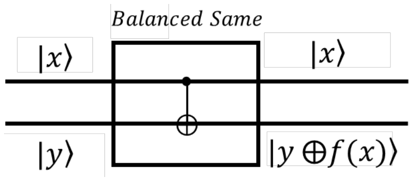


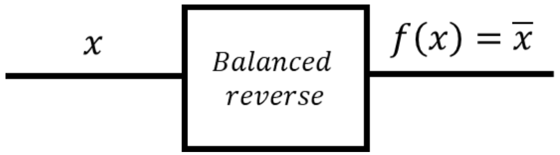
$\|x\rangle$	$\|y\rangle$	$f(x)$	$\|y \oplus f(x)\rangle$
$\|0\rangle$	$\|0\rangle$	1	$\|1\rangle$
$\|0\rangle$	$\|1\rangle$	1	$\|0\rangle$
$\|1\rangle$	$\|0\rangle$	1	$\|1\rangle$
$\|1\rangle$	$\|1\rangle$	1	$\|0\rangle$



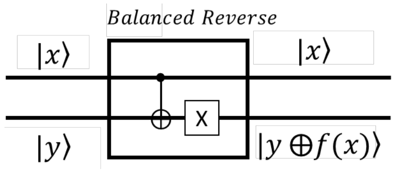


$\|x\rangle$	$\|y\rangle$	$f(x)$	$\|y \oplus f(x)\rangle$
$\|0\rangle$	$\|0\rangle$	0	$\|0\rangle$
$\|0\rangle$	$\|1\rangle$	0	$\|1\rangle$
$\|1\rangle$	$\|0\rangle$	1	$\|1\rangle$
$\|1\rangle$	$\|1\rangle$	1	$\|0\rangle$





$\|x\rangle$	$\|y\rangle$	$f(x)$	$\|y \oplus f(x)\rangle$
$\|0\rangle$	$\|0\rangle$	1	$\|1\rangle$
$\|0\rangle$	$\|1\rangle$	1	$\|0\rangle$
$\|1\rangle$	$\|0\rangle$	0	$\|0\rangle$
$\|1\rangle$	$\|1\rangle$	0	$\|1\rangle$



Math insert – Proof of Deutsch's algorithm for Constant black boxes-------------------------

The two-qubit system has an input $|0\rangle|0\rangle$. After applying X gate on the second qubit, the system changes to $|0\rangle|1\rangle$. Applying H gates on both the qubits brings the state to

$$\left(\frac{|0\rangle}{\sqrt{2}}+\frac{|1\rangle}{\sqrt{2}}\right)\otimes\left(\frac{|0\rangle}{\sqrt{2}}-\frac{|1\rangle}{\sqrt{2}}\right)$$

$$=\left(\frac{|0\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle}{\sqrt{2}}\right)-\left(\frac{|0\rangle}{\sqrt{2}}\right)\left(\frac{|1\rangle}{\sqrt{2}}\right)+\left(\frac{|1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle}{\sqrt{2}}\right)-\left(\frac{|1\rangle}{\sqrt{2}}\right)\left(\frac{|1\rangle}{\sqrt{2}}\right).$$

Applying the black box (applying $|x\rangle|y\rangle => |x\rangle|y\oplus f(x)\rangle$ on all the four parts in the superposition):

$$\left(\frac{|0\rangle}{\sqrt{2}}\right)\left(\frac{|0\oplus f(0)\rangle}{\sqrt{2}}\right)-\left(\frac{|0\rangle}{\sqrt{2}}\right)\left(\frac{|1\oplus f(0)\rangle}{\sqrt{2}}\right)+\left(\frac{|1\rangle}{\sqrt{2}}\right)\left(\frac{|0\oplus f(1)\rangle}{\sqrt{2}}\right)-\left(\frac{|1\rangle}{\sqrt{2}}\right)\left(\frac{|1\oplus f(1)\rangle}{\sqrt{2}}\right)$$

$$=\left(\frac{|0\rangle}{\sqrt{2}}\right)\left(\frac{|f(0)\rangle}{\sqrt{2}}\right)-\left(\frac{|0\rangle}{\sqrt{2}}\right)\left(\frac{|1\oplus f(0)\rangle}{\sqrt{2}}\right)+\left(\frac{|1\rangle}{\sqrt{2}}\right)\left(\frac{|f(1)\rangle}{\sqrt{2}}\right)-\left(\frac{|1\rangle}{\sqrt{2}}\right)\left(\frac{|1\oplus f(1)\rangle}{\sqrt{2}}\right)$$

(because $0\oplus f(0) = f(0)$ and $0\oplus f(1) = f(1)$)

$$=\left(\frac{|0\rangle}{\sqrt{2}}\right)\left(\frac{|f(0)\rangle}{\sqrt{2}}\right)-\left(\frac{|0\rangle}{\sqrt{2}}\right)\left(\frac{|\overline{f(0)}\rangle}{\sqrt{2}}\right)+\left(\frac{|1\rangle}{\sqrt{2}}\right)\left(\frac{|f(1)\rangle}{\sqrt{2}}\right)-\left(\frac{|1\rangle}{\sqrt{2}}\right)\left(\frac{|\overline{f(1)}\rangle}{\sqrt{2}}\right) \qquad \text{eq.(2.2.1)}$$

(because $1\oplus f(0) = \overline{f(0)}$ and $1\oplus f(1) = \overline{f(1)}$).

Let's evaluate the above result if the black box is *Constant* 0 ($i.e$ $f(0) = 0$ and $f(1) = 0$):

$$\left(\frac{|0\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle}{\sqrt{2}}\right)-\left(\frac{|0\rangle}{\sqrt{2}}\right)\left(\frac{|\overline{0}\rangle}{\sqrt{2}}\right)+\left(\frac{|1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle}{\sqrt{2}}\right)-\left(\frac{|1\rangle}{\sqrt{2}}\right)\left(\frac{|\overline{0}\rangle}{\sqrt{2}}\right)$$

$$=\left(\frac{|0\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle}{\sqrt{2}}\right)-\left(\frac{|0\rangle}{\sqrt{2}}\right)\left(\frac{|1\rangle}{\sqrt{2}}\right)+\left(\frac{|1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle}{\sqrt{2}}\right)-\left(\frac{|1\rangle}{\sqrt{2}}\right)\left(\frac{|1\rangle}{\sqrt{2}}\right).$$

Refactoring above:

$$\left(\frac{|0\rangle}{\sqrt{2}}\right)\otimes\left(\frac{|0\rangle}{\sqrt{2}}-\frac{|1\rangle}{\sqrt{2}}\right)+\left(\frac{|1\rangle}{\sqrt{2}}\right)\otimes\left(\frac{|0\rangle}{\sqrt{2}}-\frac{|1\rangle}{\sqrt{2}}\right)$$

$$=\left(\frac{|0\rangle}{\sqrt{2}}+\frac{|1\rangle}{\sqrt{2}}\right)\otimes\left(\frac{|0\rangle}{\sqrt{2}}-\frac{|1\rangle}{\sqrt{2}}\right).$$

Now, apply H gate on the first qubit:

$$|0\rangle\otimes\left(\frac{|0\rangle}{\sqrt{2}}-\frac{|1\rangle}{\sqrt{2}}\right).$$

We prove that if the given black box is *Constant* 0, executing the above circuit and measuring the first qubit will give 0. But we haven't proven the converse - if we get 0 after measuring the first qubit, does it mean that *Constant* 0 black box is used?

So, let's evaluate eq.(2.2.1) for *Constant* 1 ($i.e$ $f(0) = 1$ and $f(1) = 1$):

$$\left(\frac{|0\rangle}{\sqrt{2}}\right)\left(\frac{|f(0)\rangle}{\sqrt{2}}\right)-\left(\frac{|0\rangle}{\sqrt{2}}\right)\left(\frac{|\overline{f(0)}\rangle}{\sqrt{2}}\right)+\left(\frac{|1\rangle}{\sqrt{2}}\right)\left(\frac{|f(1)\rangle}{\sqrt{2}}\right)-\left(\frac{|1\rangle}{\sqrt{2}}\right)\left(\frac{|\overline{f(1)}\rangle}{\sqrt{2}}\right)$$

$$=\left(\frac{|0\rangle}{\sqrt{2}}\right)\left(\frac{|1\rangle}{\sqrt{2}}\right)-\left(\frac{|0\rangle}{\sqrt{2}}\right)\left(\frac{|\overline{1}\rangle}{\sqrt{2}}\right)+\left(\frac{|1\rangle}{\sqrt{2}}\right)\left(\frac{|1\rangle}{\sqrt{2}}\right)-\left(\frac{|1\rangle}{\sqrt{2}}\right)\left(\frac{|\overline{1}\rangle}{\sqrt{2}}\right)$$

$$=\left(\frac{|0\rangle}{\sqrt{2}}\right)\left(\frac{|1\rangle}{\sqrt{2}}\right)-\left(\frac{|0\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle}{\sqrt{2}}\right)+\left(\frac{|1\rangle}{\sqrt{2}}\right)\left(\frac{|1\rangle}{\sqrt{2}}\right)-\left(\frac{|1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle}{\sqrt{2}}\right).$$

After refactoring:

$$\left(\frac{|0\rangle}{\sqrt{2}}\right)\otimes\left(\frac{|1\rangle}{\sqrt{2}}-\frac{|0\rangle}{\sqrt{2}}\right)+\left(\frac{|1\rangle}{\sqrt{2}}\right)\otimes\left(\frac{|1\rangle}{\sqrt{2}}-\frac{|0\rangle}{\sqrt{2}}\right)$$

$$=\left(\frac{|0\rangle}{\sqrt{2}}+\frac{|1\rangle}{\sqrt{2}}\right)\otimes\left(\frac{|1\rangle}{\sqrt{2}}-\frac{|0\rangle}{\sqrt{2}}\right)$$

$$=\left(\frac{|0\rangle}{\sqrt{2}}+\frac{|1\rangle}{\sqrt{2}}\right)\otimes-\left(\frac{|0\rangle}{\sqrt{2}}-\frac{|1\rangle}{\sqrt{2}}\right)$$

$$=-\left(\frac{|0\rangle}{\sqrt{2}}+\frac{|1\rangle}{\sqrt{2}}\right)\otimes\left(\frac{|0\rangle}{\sqrt{2}}-\frac{|1\rangle}{\sqrt{2}}\right)$$

Applying H gate on the first qubit:

DO IT AT HOME!

Now, apply H gate on the first qubit:

$$|0\rangle\otimes\left(\frac{|0\rangle}{\sqrt{2}}-\frac{|1\rangle}{\sqrt{2}}\right).$$

We prove that if the given black box is *Constant* 0, executing the above circuit and measuring the first qubit will give 0. But we haven't proven the converse - if we get 0 after measuring the first qubit, does it mean that *Constant* 0 black box is used?

So, let's evaluate eq.(2.2.1) for *Constant* 1 ($i.e$ $f(0) = 1$ and $f(1) = 1$):

$$\left(\frac{|0\rangle}{\sqrt{2}}\right)\left(\frac{|f(0)\rangle}{\sqrt{2}}\right)-\left(\frac{|0\rangle}{\sqrt{2}}\right)\left(\frac{|\overline{f(0)}\rangle}{\sqrt{2}}\right)+\left(\frac{|1\rangle}{\sqrt{2}}\right)\left(\frac{|f(1)\rangle}{\sqrt{2}}\right)-\left(\frac{|1\rangle}{\sqrt{2}}\right)\left(\frac{|\overline{f(1)}\rangle}{\sqrt{2}}\right)$$

$$=\left(\frac{|0\rangle}{\sqrt{2}}\right)\left(\frac{|1\rangle}{\sqrt{2}}\right)-\left(\frac{|0\rangle}{\sqrt{2}}\right)\left(\frac{|\overline{1}\rangle}{\sqrt{2}}\right)+\left(\frac{|1\rangle}{\sqrt{2}}\right)\left(\frac{|1\rangle}{\sqrt{2}}\right)-\left(\frac{|1\rangle}{\sqrt{2}}\right)\left(\frac{|\overline{1}\rangle}{\sqrt{2}}\right)$$

$$=\left(\frac{|0\rangle}{\sqrt{2}}\right)\left(\frac{|1\rangle}{\sqrt{2}}\right)-\left(\frac{|0\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle}{\sqrt{2}}\right)+\left(\frac{|1\rangle}{\sqrt{2}}\right)\left(\frac{|1\rangle}{\sqrt{2}}\right)-\left(\frac{|1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle}{\sqrt{2}}\right).$$

After refactoring:

$$\left(\frac{|0\rangle}{\sqrt{2}}\right)\otimes\left(\frac{|1\rangle}{\sqrt{2}}-\frac{|0\rangle}{\sqrt{2}}\right)+\left(\frac{|1\rangle}{\sqrt{2}}\right)\otimes\left(\frac{|1\rangle}{\sqrt{2}}-\frac{|0\rangle}{\sqrt{2}}\right)$$

$$=\left(\frac{|0\rangle}{\sqrt{2}}+\frac{|1\rangle}{\sqrt{2}}\right)\otimes\left(\frac{|1\rangle}{\sqrt{2}}-\frac{|0\rangle}{\sqrt{2}}\right)$$

$$=\left(\frac{|0\rangle}{\sqrt{2}}+\frac{|1\rangle}{\sqrt{2}}\right)\otimes-\left(\frac{|0\rangle}{\sqrt{2}}-\frac{|1\rangle}{\sqrt{2}}\right)$$

$$=-\left(\frac{|0\rangle}{\sqrt{2}}+\frac{|1\rangle}{\sqrt{2}}\right)\otimes\left(\frac{|0\rangle}{\sqrt{2}}-\frac{|1\rangle}{\sqrt{2}}\right)$$

Applying H gate on the first qubit:

$$-|0\rangle\otimes\left(\frac{|0\rangle}{\sqrt{2}}-\frac{|1\rangle}{\sqrt{2}}\right).$$

Here, if we measure the first qubit, it is 100% certain that we will still get $|0\rangle$, because probability is the square of the amplitude (-1 in this case). So, we just proved that if the given black box is *Constant* 1, executing the above circuit and measuring the first qubit will give 0.

$(|0\rangle+|1\rangle)\otimes(|0\rangle-|1\rangle)$

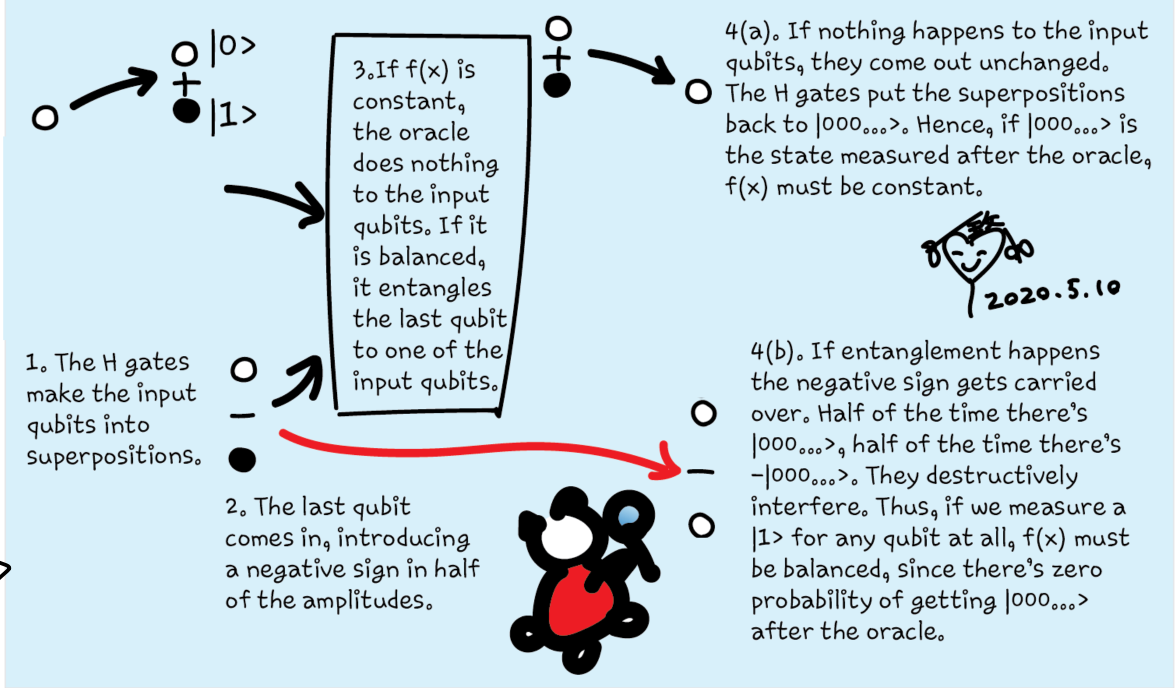
$= |00\rangle - |01\rangle + |10\rangle - |11\rangle$

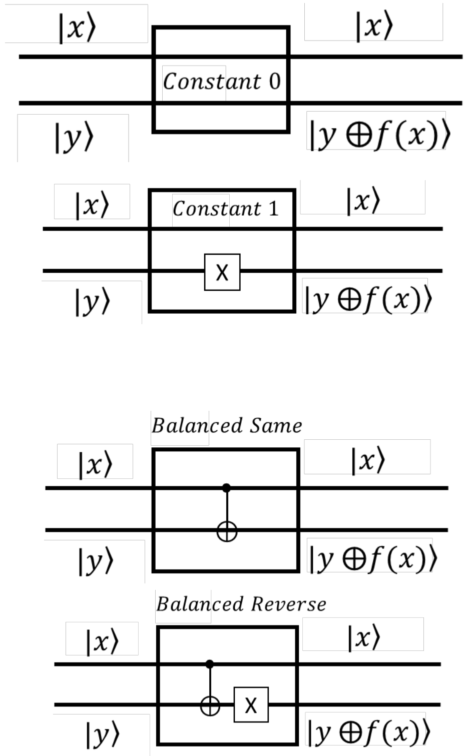
$|00\rangle - |01\rangle + |11\rangle - |10\rangle$

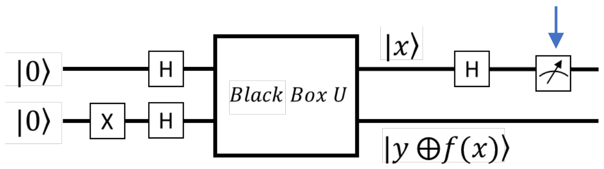
$|+\rangle \; |-\rangle \; |-\rangle \; -|+\rangle$

$|-\rangle$

$= |1\rangle$







Obtains result with corresponding probability

0 means *Constant*

1 means *Balanced*

Q# exercise:

- The Quantum Katas project (tutorials and exercises for learning quantum computing) https://github.com/Microsoft/QuantumKatas

  - Tutorials https://github.com/microsoft/QuantumKatas/tree/master/tutorials/ExploringDeutschJozsaAlgorithm

  - DeutschJozsaAlgorithm https://github.com/microsoft/QuantumKatas/tree/master/DeutschJozsaAlgorithm

- Documentation sample

https://github.com/microsoft/Quantum/tree/master/samples/getting-started/simple-algorithms

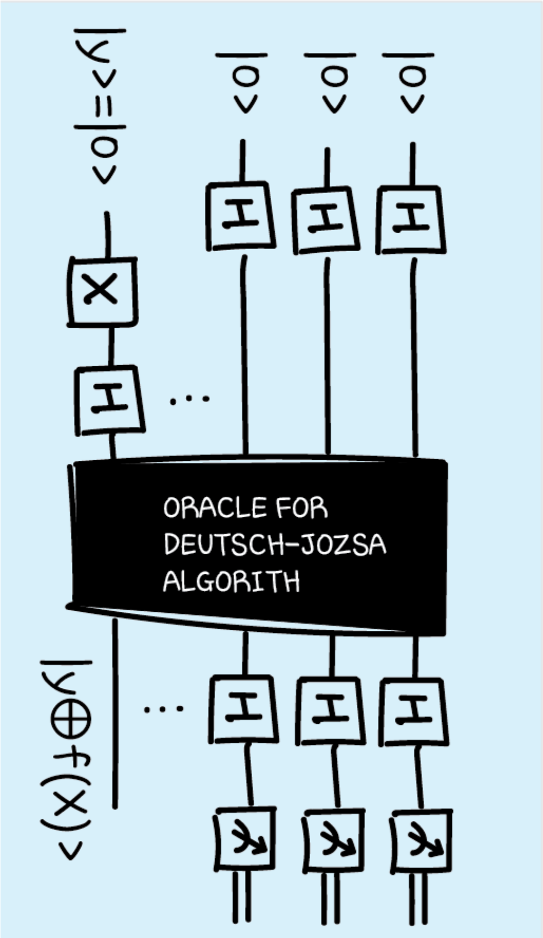
Task 2.1. Deutsch-Jozsa Algorithm

Inputs:

1. the number of qubits N in the input register for the function f
2. a quantum operation which implements the oracle $|x, y\rangle \rightarrow |x, y \oplus f(x)\rangle$, where x is an N-qubit input register, y is a 1-qubit answer register, and f is a Boolean function

Output: `true` if the function f is constant, or `false` if the function f is balanced.

```
%kata T31_DJ_Algorithm_Test

operation DJ_Algorithm (N : Int, oracle : ((Qubit[], Qubit) => Unit)) : Bool {
    // Create a boolean variable for storing the return value.
    // You'll need to update it later, so it has to be declared as mutable.
    // ...

    // Allocate an array of N qubits for the input register x and one qubit for the answer register y.
    using ((x, y) = (Qubit[N], Qubit())) {
        // Newly allocated qubits start in the |0⟩ state.
        // The first step is to prepare the qubits in the required state before calling the oracle.
        // Each qubit of the input register has to be in the |+⟩ state.
        // ...

        // The answer register has to be in the |-⟩ state.
        // ...

        // Apply the oracle to the input register and the answer register.
        // ...

        // Apply a Hadamard gate to each qubit of the input register again.
        // ...

        // Measure each qubit of the input register in the computational basis using the M operation.
        // If any of the measurement results is One, the function implemented by the oracle is balanced.
        // ...

        // Before releasing the qubits make sure they are all in the |0⟩ state.
        // ...
    }

    // Return the answer.
    // ...
}
```



Certificate 2

- 1. Who came up with the term "Quantum Oracle"?
- 2. Who is this on page 6?
- 3. Who is this on page 26?