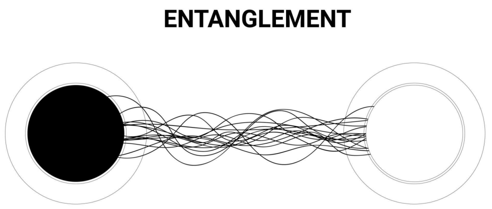
Deutsch algorithm

Before looking at the Deutsch algorithm, there are four concepts related to quantum mechanics that we need to understand:

1. Entanglement (reminder + more detail)
2. Hadamar gate
3. Reversible quantum functions (reminder + more detail)
4. Phase oracle (quantum circuit) form

Entanglement (formal definition)



Entanglement

- Two qubits are entangled if their joint quantum state cannot be decomposed into independent states of each qubit
- Measuring one determines the outcome of the other according to their correlation.

A Quantum state is entangled if it cannot be factored into a tensor product of individual qubits (cannot be written as a product of independent states)

Example:

$$|\Psi> = \frac{1}{\sqrt{2}}(\,|00> + |11>)$$

If we measure one of the qubits as a 0, $|\psi\rangle$ will collapse to $|00\rangle$
If we measure one of the qubits as a 1, $|\psi\rangle$ will collapse to $|11\rangle$

How to check if two qubits are entangled ?

Let's assume that $|\psi\rangle$ (a system of two qubits) is not entangled

$\Rightarrow \exists$ $|a\rangle$ and $|b\rangle$ such that

- $|a\rangle = a_0|0\rangle + a_0|1\rangle$
- $|b\rangle = b_0|0\rangle + b_1|1\rangle$ and

$$|\psi\rangle = |a\rangle \otimes |b\rangle$$

$|\psi\rangle = c_{00}|00\rangle + c_{01}|01\rangle + c_{10}|10\rangle + c_{11}|11\rangle$

With : $c_{00}=a_0b_0$ $\quad c_{01}=a_0b_1$ $\quad c_{10}=a_1b_0$ $\quad c_{11}=a_1b_1$

$c_{00}\, c_{11} = c_{01}\, c_{10} = a_0b_0a_1b_1$

If $c_{00}\, c_{11} \neq c_{01}\, c_{10}$ then $\nexists$ $|a\rangle$ & $|b\rangle$ verifying cond I $\Rightarrow$ the system is entangled

Entanglement (Bell states)

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

$$|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

List of **maximally** entangled states with two qubits

strong, perfect correlations

Exercise

Is ψ entangled ?

$$|\Psi> \; = \frac{1}{\sqrt{3}} \left(|100> \; - \; |010> \; + \; |001> \right)$$

If measuring the first qubit leads to 0 then the other two will be entangled:

$$\frac{1}{\sqrt{2}} \left(|10> \; + \; |01> \right)$$

If measuring the first qubit leads to 1 then the other two will be both in state 0.

Weak, distributed correlations

Hes·so Exercise

Is ψ entangled ?

$$|\Psi> = \frac{1}{2}(\underbrace{|00> - |01>} + \underbrace{|10> + |11>})$$

$$|\Psi> = \frac{1}{2}(\overbrace{|0>(|0> - |1>)} + \overbrace{|1>(|0> + |1>)})$$

$$|\Psi> = \frac{1}{\sqrt{2}}\left(|0>\underbrace{\frac{1}{\sqrt{2}}(|0> - |1>)} + |1>\underbrace{\frac{1}{\sqrt{2}}(|0> + |1>)}\right)$$

$$|\Psi> = \frac{1}{\sqrt{2}}(|0>|-> + |1>|+>)$$

$$|\Psi> = \frac{1}{\sqrt{2}}(|0-> + |1+>)$$

The two qubits depend on each others. Ψ cannot be written as a tensor product → ψ is entangled

Hadamard gate: H

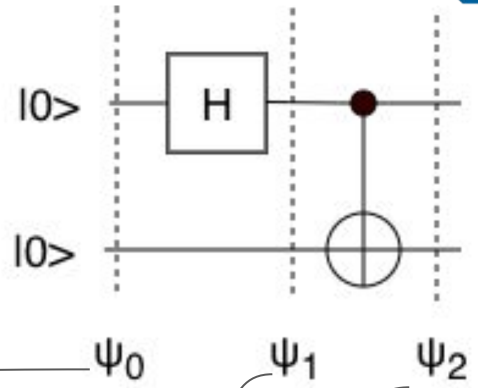
$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

$$H(|0>) = \frac{1}{\sqrt{2}}(|0> + |1>) = |+>$$

$$H(|1>) = \frac{1}{\sqrt{2}}(|0> - |1>) = |->$$

Hes·so

Using *H* and *CNOT* to obtain an entangled system



$$|\psi_0> \; = |00>$$

$$|\psi_1> = |+0> \; = \frac{1}{\sqrt{2}}(\,|0> + |1>)\;\;|0>$$

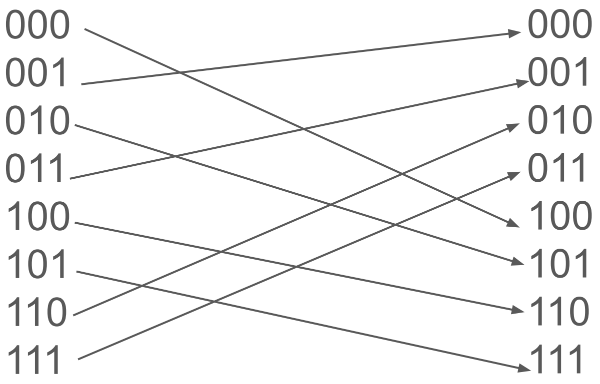
$$|\psi_1> = \frac{1}{\sqrt{2}}(\,|0>|0> + |1>|0>)$$

$$|\psi_1> = \frac{1}{\sqrt{2}}(\,|00> + |10>)$$

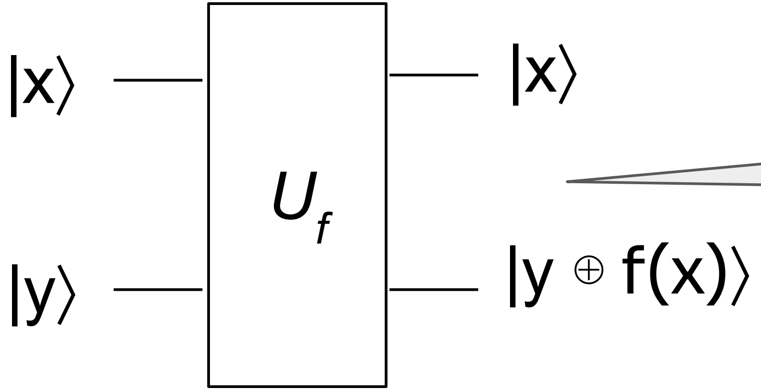
$$|\psi_2> \; = \frac{1}{\sqrt{2}}(\,|00> + |11>)$$

Reversible functions in quantum computing

- All operations (functions) in Quantum computing (except the measurement) must be reversible → all gates are reversible
- In classical math, a function *f* is reversible if, given *f(x)*, we can find *x*.
- In quantum computing, a function is reversible iff it is a bijection from a space to itself
  - Same number of qubits *in* and *out*
  - Reversible = no output repetition AND no missing outputs



Reversible quantum function



This function is reversible because XOR undoes it self.

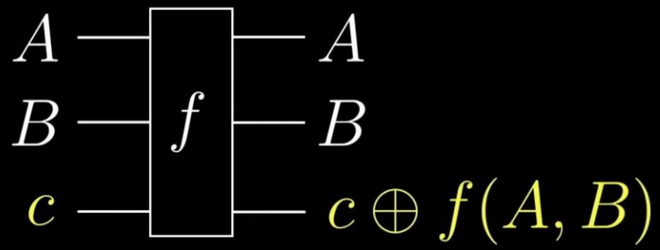
If $|y\rangle = |0\rangle$ the output will be $|x\rangle\,|0 \oplus f(x)\rangle = |x\rangle\,|f(x)\rangle$

The first qubit is the input ($|x\rangle$) and the second qbit is the output $|f(x)\rangle$

Example of a reversible quantum function

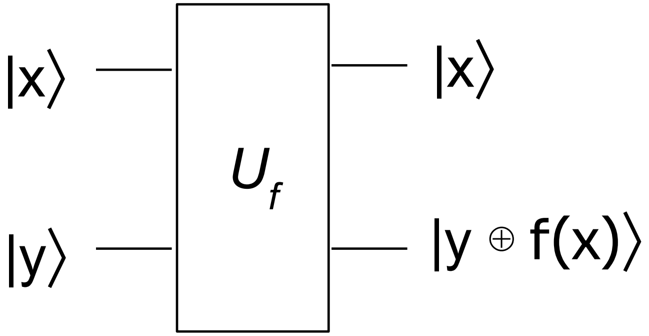
$f(A, B)$ is the OR operation

A	B	c	A	B	$c \oplus f(A,B)$
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	1
0	1	1	0	1	0
1	0	0	1	0	1
1	0	1	1	0	0
1	1	0	1	1	1
1	1	1	1	1	0



$$\underbrace{\{0,\ 1\}^3}_{\text{Input space}} \rightarrow \underbrace{\{0,\ 1\}^3}_{\text{Output space}}$$

Phase Oracle form



$$Let's\ calculate\ U_f |x\rangle |-\rangle$$

$$U_f |x\rangle |-\rangle = (-1)^{f(x)} |x> |-\rangle$$

$$U_f |x> |-> = U_f |x> \frac{1}{\sqrt{2}} (|0> - |1>)$$

$$U_f |x> |-> = U_f \frac{1}{\sqrt{2}} (|x>|0> - |x>|1>)$$

$$U_f |x> |-> = \frac{1}{\sqrt{2}} \left(U_f |x>|0> - U_f |x>|1> \right)$$

$$U_f |x> |-> = \frac{1}{\sqrt{2}} \left(|x>|f(x)> - |x>|\overline{f(x)}> \right)$$

$$if\ f(x) = 0 \Rightarrow U_f |x>|-> = \frac{1}{\sqrt{2}} (|x>|0> - |x>|1>) = |x>|->$$

$$if\ f(x) = 1 \Rightarrow U_f |x>|-> = \frac{1}{\sqrt{2}} (|x>|1> - |x>|0>) = -|x>|->$$

Deutsch-Jozsa algorithm

$$f : \{0,\ 1\}^n \rightarrow \{0,\ 1\}$$

Goal: to calculate if the function *f* is constant or balanced ?

The function *f* is constant if:

$$f(x) = 0 \quad for\ every\ x \in \{0,\ 1\}^n\ or$$
$$f(x) = 1 \quad for\ every\ x \in \{0,\ 1\}^n$$

The function *f* is balanced if:

- Half of the input (2^{n-1}) is equal 0
- Half of the input (2^{n-1}) is equal 1

Deutsch-Jozsa algorithm

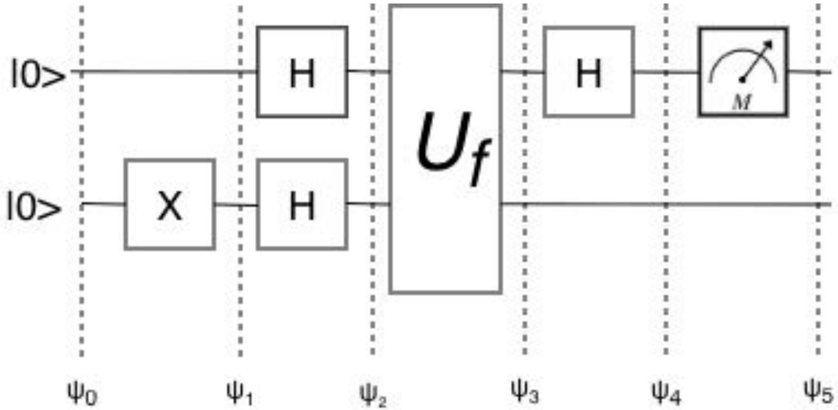
$$\textit{In classical computers, we need } 2^{n-1} + 1 \textit{ queries to determine if}$$
$$\textit{the function } f \textit{ is contant or balanced.}$$
$$n \textit{ is the length of the bit string}$$
$$\textit{In quantum computing, we need only one query}$$

Deutsch algorithm

$$|\psi_o> \; = |00>$$

$$|\psi_1> \; = |01>$$

$$|\psi_2> \; = |+ \; - \; >$$

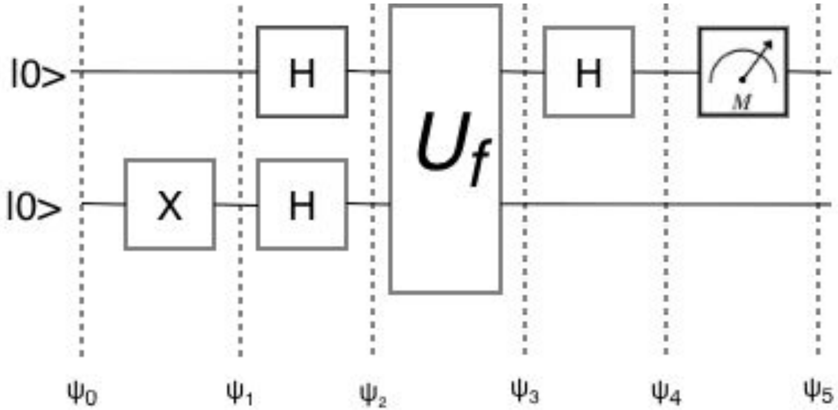


$$|+ \; > \; = \frac{1}{\sqrt{2}}(\,|0> \; + \; |1>)$$

Just to remind you ...

$$|- \; > \; = \frac{1}{\sqrt{2}}(\,|0> \; - \; |1>)$$

Deutsch algorithm



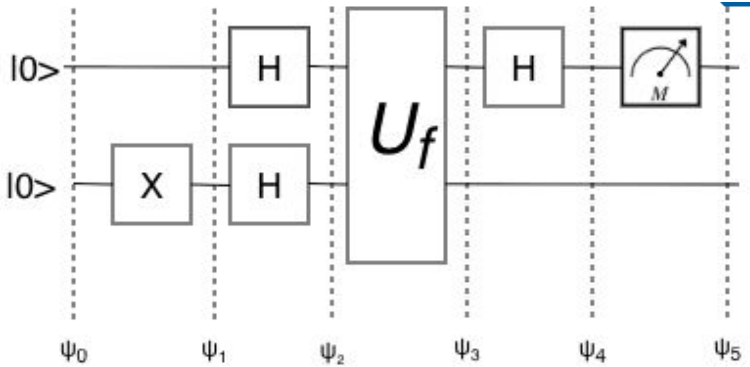
$$|\psi_o> = |00>$$

$$|\psi_1> = |01>$$

$$|\psi_2> = |+ - > = \frac{1}{\sqrt{2}}(|0> + |1>)|- > = \frac{1}{\sqrt{2}}(|0>|- > + |1>|- >)$$

$$|\psi_3> = U_f\left(\frac{1}{\sqrt{2}}(|0>|- > + |1>|- >)\right) = \frac{1}{\sqrt{2}}\left(U_f(|0>|- >) + U_f(|1>|- >)\right)$$

Deutsch algorithm



$$|\psi_3> \;=\; \frac{1}{\sqrt{2}}\Big(U_f(\,|0>\,|->) \;+\; U_f(\,|1>\,|->)\Big)$$

$$\boxed{U_f(\,|x>|->) \;=\; (-1)^{f(x)}\,|x>\,|->}$$

Just to remind you …:
Phase oracle form

$$f(0)=f(1)=0 \rightarrow |\psi_3> \;=\; \frac{1}{\sqrt{2}}(\,|0> \;+\; |1>) \;=\; |+>$$

$$f(0)=f(1)=1 \rightarrow |\psi_3> \;=\; -\frac{1}{\sqrt{2}}(\,|0> \;+\; |1>) \;=\; -|+> \;\rightarrow\; |+>$$

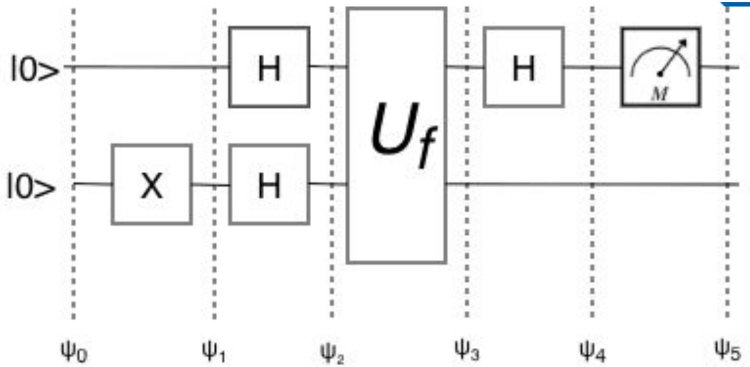
Constant function

$$f(0) = 0 \; and \; f(1)=1 \rightarrow |\psi_3> \;=\; \frac{1}{\sqrt{2}}(\,|0> \;-\; |1>) \;=\; |->$$

$$f(0) = 1 \; and \; f(1)=0 \rightarrow |\psi_3> \;=\; \frac{1}{\sqrt{2}}(-|0> \;+\; |1>) \;=\; -|-> \;\rightarrow\; |->$$

Balanced function

Deutsch algorithm



Constant function

$$|\psi_4> \ = |0> \ if \ \ |\psi_3> \ = |+ \ >$$

$$|\psi_4> \ = |1> \ if \ \ |\psi_3> \ = |- \ >$$

Balanced function