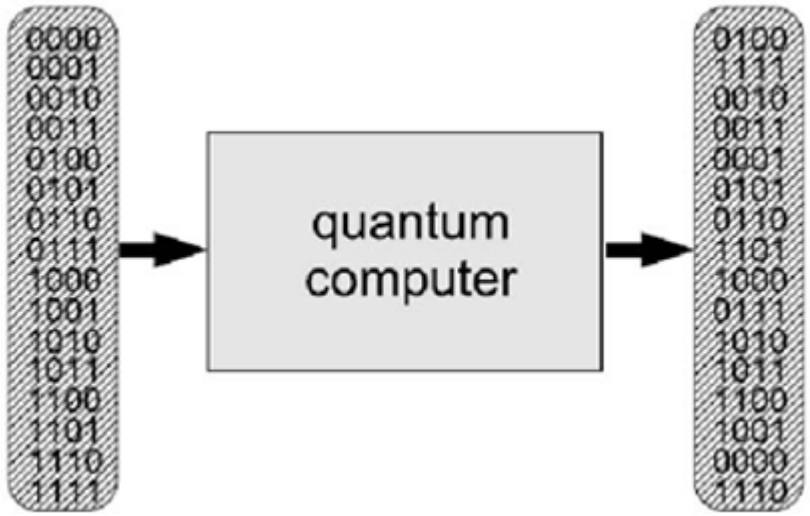
18. Deutsch’s algorithm



Quantum speedups

Up to this point, we haven't demonstrated that any actual benefit of using a quantum computer.

In fact it seems even more restrictive since we can't even do some basic tasks like copying (cloning).

In 1985 David Deutsch invented the first quantum algorithm that showed that quantum computers might be faster than classical computers.

It solves a problem without any practical use, but it shows the how quantum superposition can put to use in an information sense.

Deutsch, "Quantum Theory, the Church-Turing Principle and the Universal Quantum Computer" Proceedings of the Royal Society of London A. **400,** 97 (1985).

The problem

Consider the function f(x), which has a binary input x={0,1} and output f={0,1}.

There are actually only 4 types of such functions:

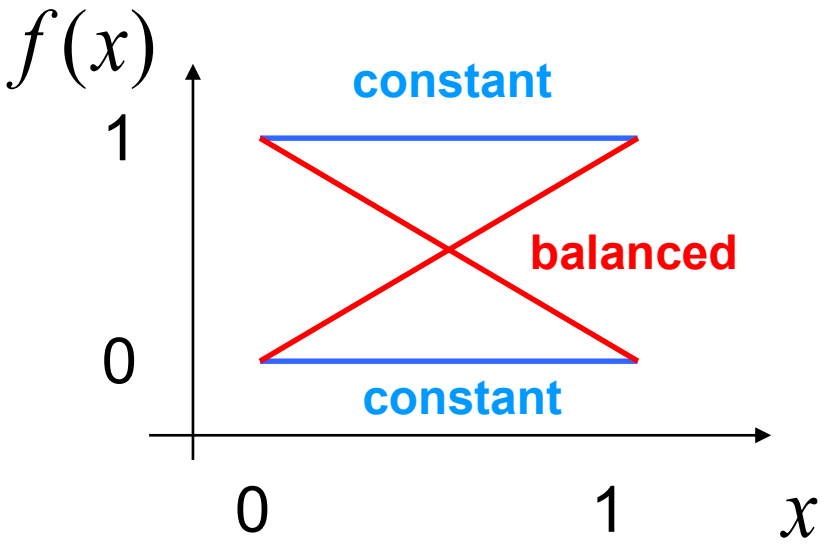
Define two classes of functions according to

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

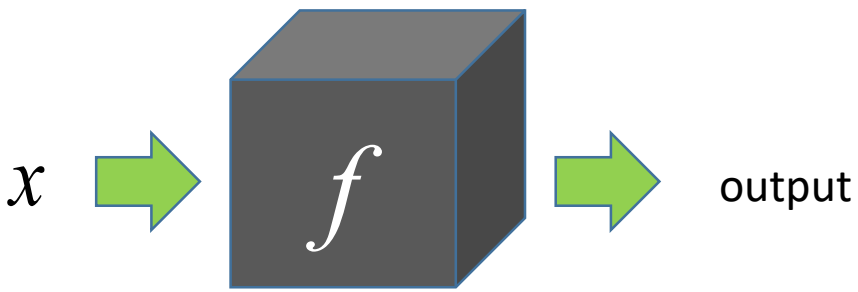
i.e. the function is a constant (flat)

Balanced functions: $f(0) \neq f(1)$

Half the function values are 0, half are 1



Now suppose we have a black-box (the oracle) that implements one of the 4 functions



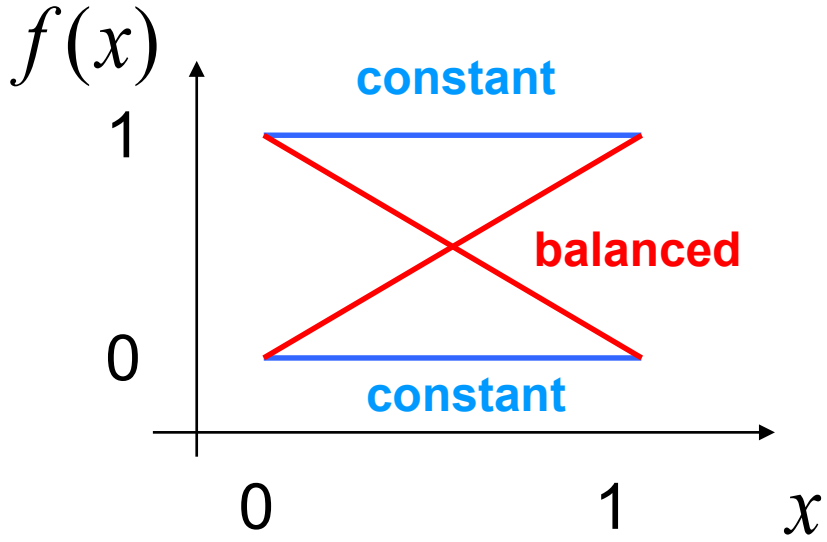
Task: Figure out whether we have a "constant" or "balanced" function with as few calls of the oracle as possible.

Classical solution

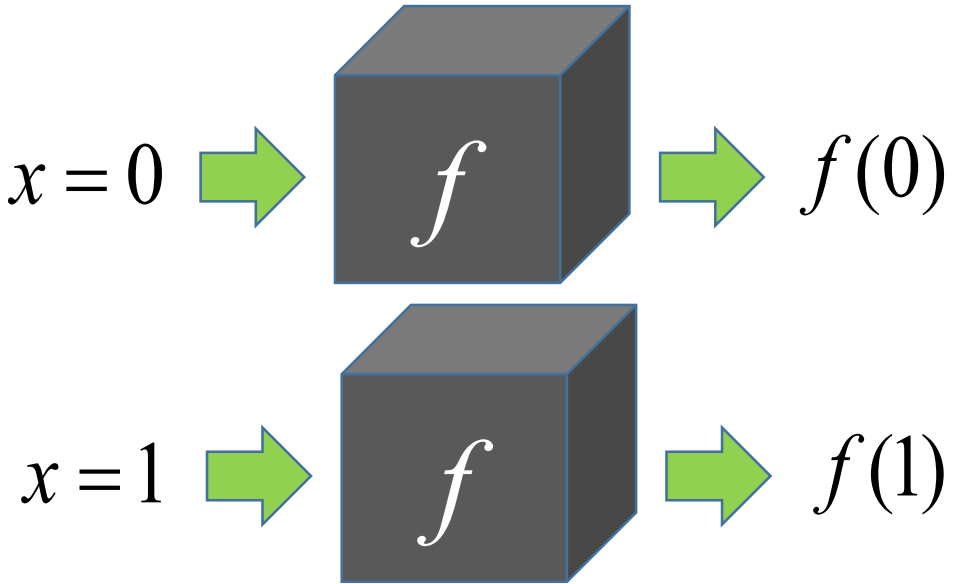
The property of being constant or balanced is by definition a global property of the function

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

Balanced functions: $f(0) \neq f(1)$



We must compare the x=0 and x=1 inputs to see which type it is.



We need **two** calls of the oracle minimum to solve the problem.

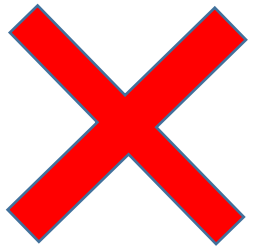
Quantum superposition

The basic idea of Deutsch's algorithm is that with quantum mechanics you can put in a superposition of inputs

$$\left|x=0\right\rangle+\left|x=1\right\rangle \Rightarrow \boxed{f} \Rightarrow \left|f(0)\right\rangle+\left|f(1)\right\rangle$$

BUT actually this doesn't work since this would be non-unitary. E.g. for f(x) = 1

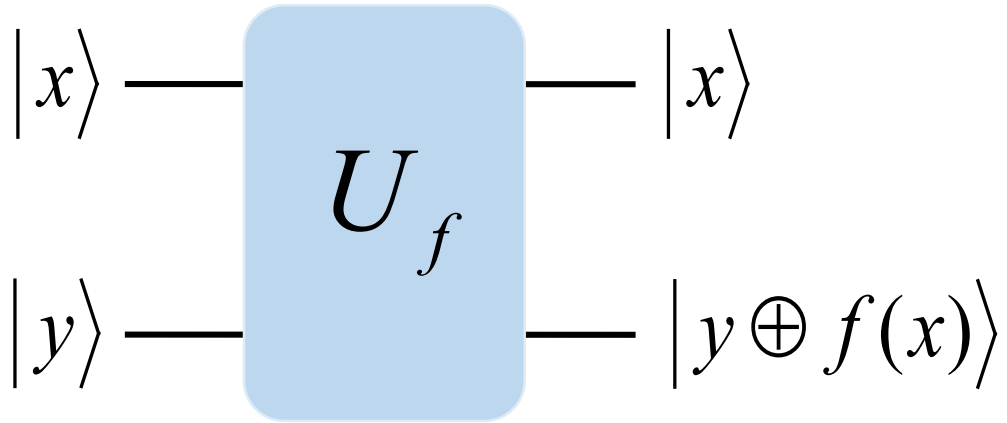
$$\left|0\right\rangle \rightarrow \left|1\right\rangle$$
$$\left|1\right\rangle \rightarrow \left|1\right\rangle$$



This is not reversible, so it cannot be a quantum gate.

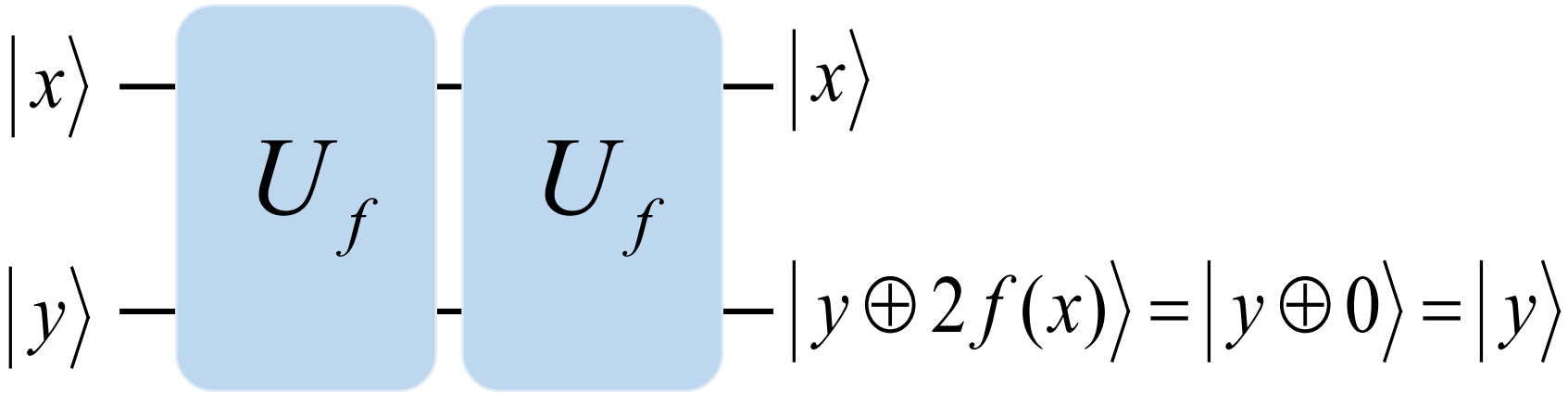
Quantum oracle

To make a unitary oracle for the function f(x) let's instead define it like



$\oplus$ =addition modulo 2

This is reversible because

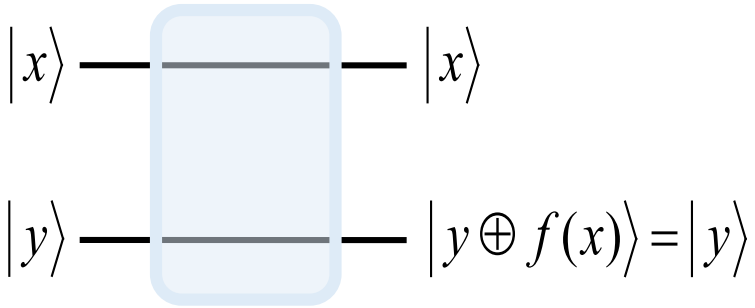


2x=0 modulo 2

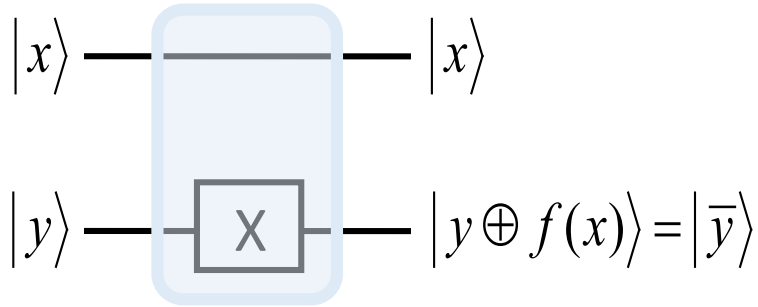
Quantum circuits for the oracle

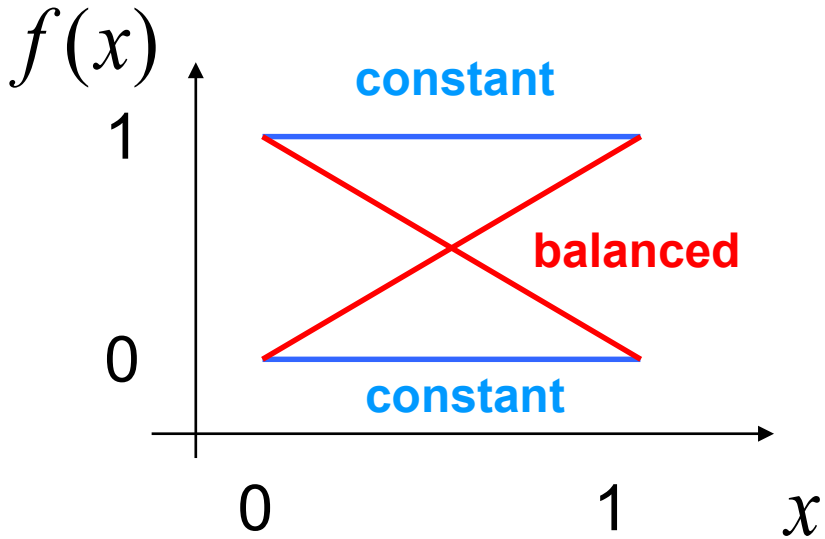
We can make the following quantum circuits for the 4 types of oracle:

$f(x)=0$

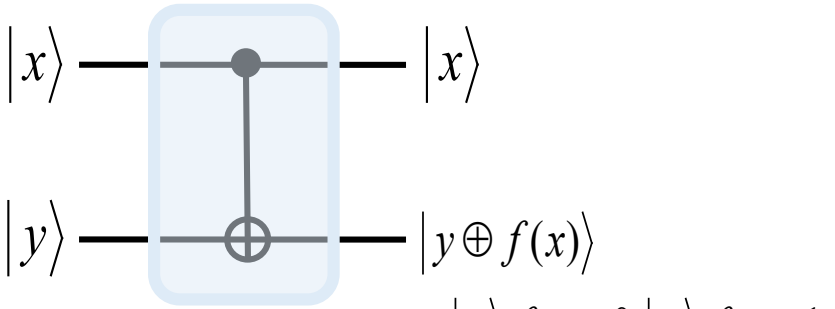


$f(x)=1$



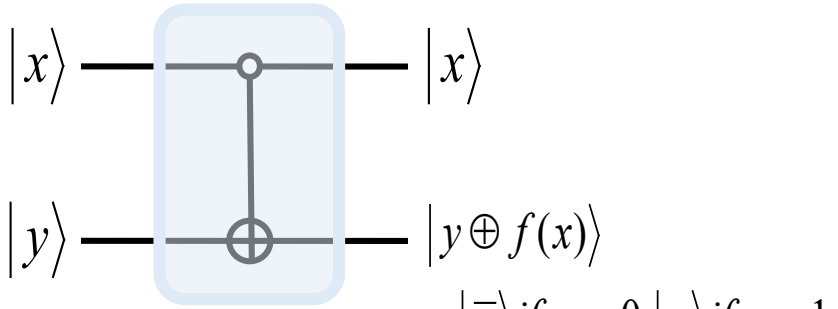


$f(0)=0, f(1)=1$



$= |y\rangle \text{if } x=0, |\bar{y}\rangle \text{if } x=1,$

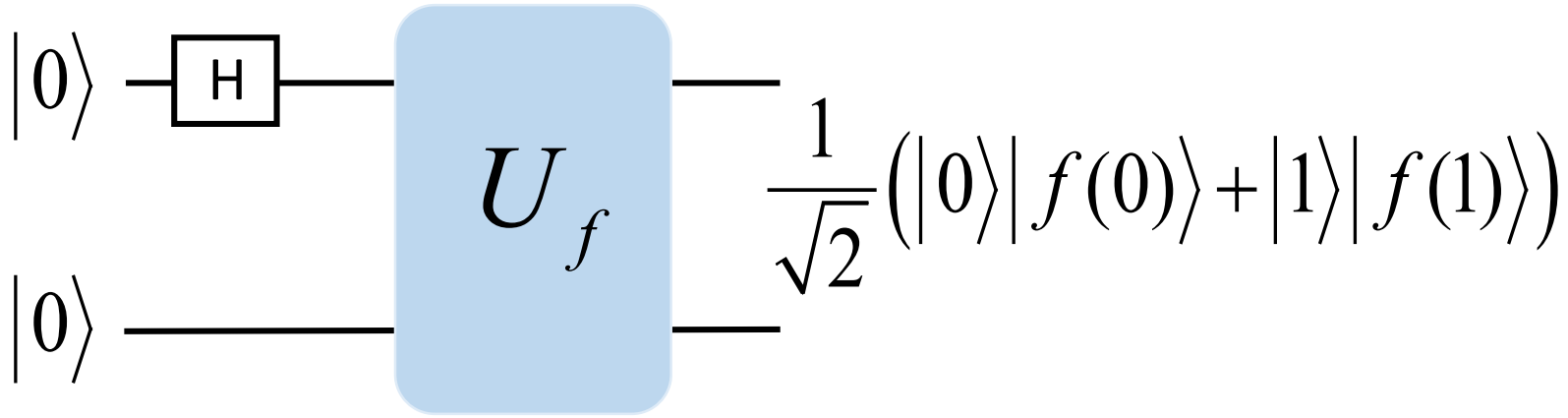
$f(0)=1, f(1)=0$



$= |\bar{y}\rangle \text{if } x=0, |y\rangle \text{if } x=1,$

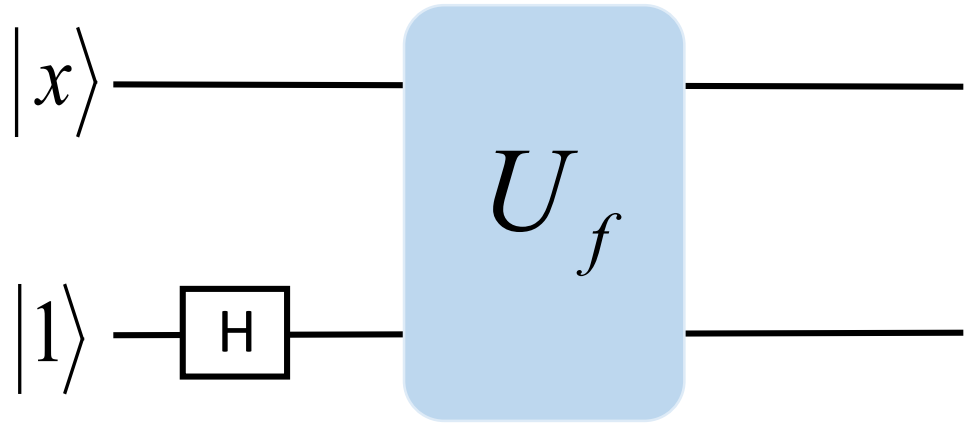
Superposition state

With this definition, one oracle call can get both input values of the function since



But this doesn't quite solve the task because a measurement of the top qubit would collapse the state as

$$\frac{1}{\sqrt{2}}\left(|0\rangle|f(0)\rangle+|1\rangle|f(1)\rangle\right) \rightarrow \begin{cases} |0\rangle|f(0)\rangle & p=\frac{1}{2} \\ |1\rangle|f(1)\rangle & p=\frac{1}{2} \end{cases}$$



But if instead we put the Hadamard on the second qubit, we have

$$|x\rangle\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)\rightarrow|x\rangle\frac{1}{\sqrt{2}}(|0\oplus f(x)\rangle-|1\oplus f(x)\rangle)$$

$$=\begin{cases}|x\rangle\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle) & \text{if f(x)=0}\\ |x\rangle\frac{1}{\sqrt{2}}(|1\rangle-|0\rangle) & \text{if f(x)=1}\end{cases}$$

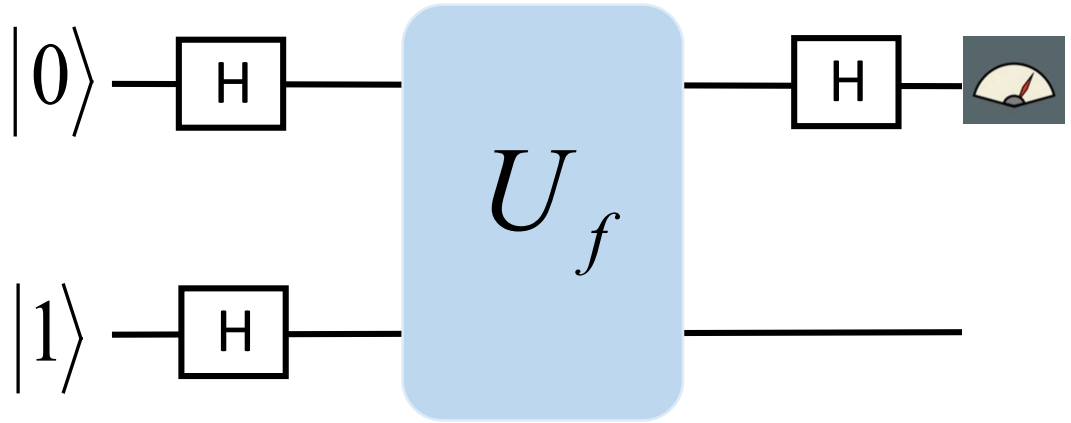
$$=(-1)^{f(x)}|x\rangle\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)$$

Since the second qubit doesn't change, a simple way to view this is

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

i.e. it flips the sign of the f(x)=1 terms

Deutsch's algorithm



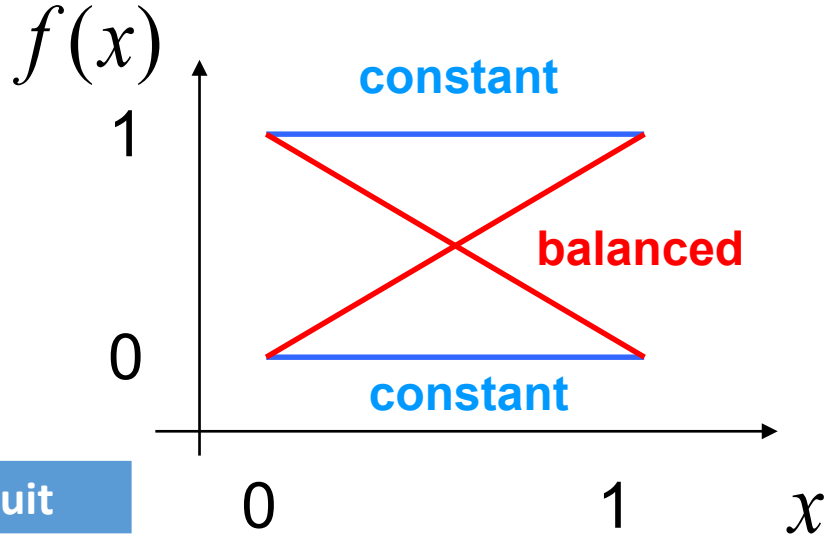
By modifying this we can get a circuit that will solve the task with one call of the oracle

Basic idea: If we put in a superposition on the first qubit then since $U_f |x\rangle = (-1)^{f(x)} |x\rangle$

$$U_f \left(|0\rangle + |1\rangle \right) = (-1)^{f(0)} |0\rangle + (-1)^{f(1)} |1\rangle$$

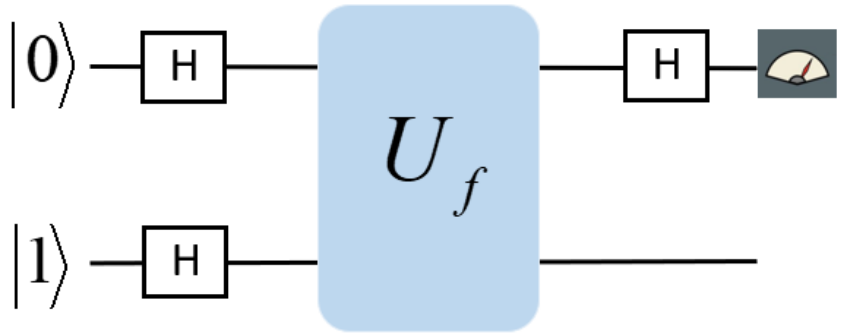
Then for the four cases we will have

$$U_f\left(|0\rangle+|1\rangle\right)=(-1)^{f(0)}|0\rangle+(-1)^{f(1)}|1\rangle$$



Function	Type	Output of oracle	Output of circuit
$f(x)=0$	constant	$\|0\rangle+\|1\rangle$	$\|0\rangle$
$f(0)=0, f(1)=1$	balanced	$\|0\rangle-\|1\rangle$	$\|1\rangle$
$f(x)=1$	constant	$-(\|0\rangle+\|1\rangle)$	$-\|0\rangle$
$f(0)=1, f(1)=0$	balanced	$-\|0\rangle+\|1\rangle$	$-\|1\rangle$

Constant and balanced cases are same up to a global phase!

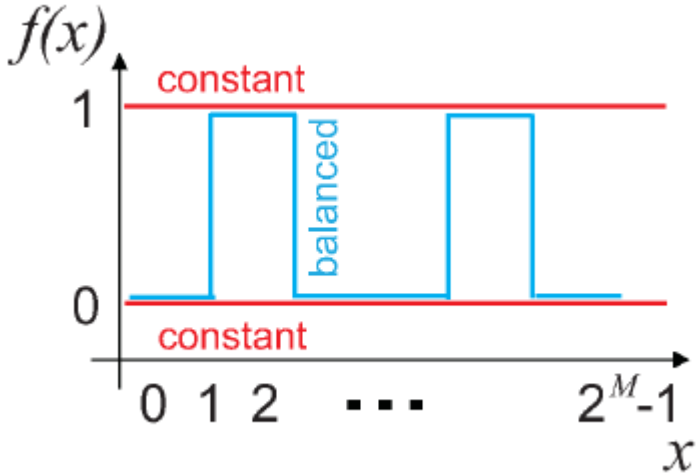


We can distinguish the two cases with one call of the oracle.

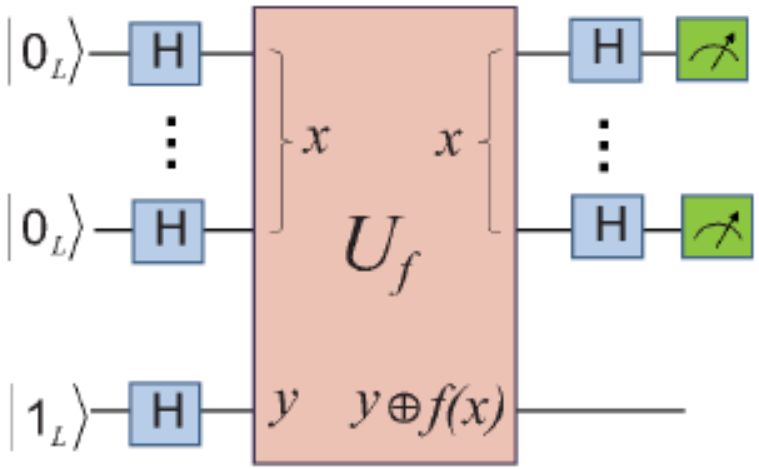
Deutsch-Jozsa algorithm

The quantum speedup of Deutsch's algorithm is only a factor of 2.

Deutsch-Jozsa is the multi-qubit generalization of Deutsch's algorithm where the speed up is 2^M, which is a bit more impressive



Aim: Distinguish between constant and balanced oracles with certainty



e.g. $U_f\left(|0\rangle+|1\rangle\right)\left(|0\rangle+|1\rangle\right)=$

$$(-1)^{f(00)}|00\rangle+(-1)^{f(01)}|01\rangle+(-1)^{f(10)}|10\rangle+(-1)^{f(11)}|11\rangle$$

Will affect the state if the function is balanced

$$|1\rangle|x=0\rangle \rightarrow \begin{cases} \left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)|x=0\rangle & f(x)\in \text{ constant} \\ \left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)|x>0\rangle & f(x)\in \text{ balanced} \end{cases}$$