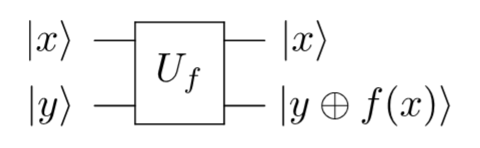
Deutch's algorithm

1985 ?

Assume the Oracle is a "black box" that encodes an unknown function f(x)



CONSTANT
BAL

	$x=0$	$x=1$
f_0	0	0
f_1	0	1
f_2	1	0
f_3	1	1

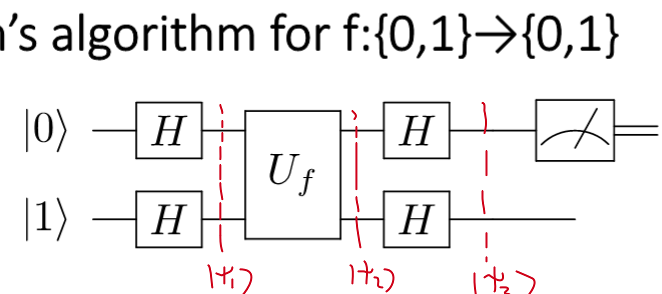
- How many times do we need to query the Oracle in order to determine whether f(x) is constant or balanced? (i.e. whether it's EITHER f_0, f_3 OR f_1, f_2)

CLASSICAL COMPUTER. QUERY $x=0$: $f(0) = \begin{cases} 0 \Rightarrow f_0 \text{ OR } f_1 \\ 1 \Rightarrow f_2 \text{ OR } f_3 \end{cases} \Rightarrow$ STILL SO-SO BAL/CONST. !

$x=1$ $f(1) \Rightarrow$ YOU DETERMINE THE ACTUAL f_i!

QUANTUM COMPUTER: ONLY ONE QUERY DETERMINES WHETHER f IS BALANCED OR CONSTANT. HOWEVER, YOU WON'T BE ABLE TO TELL WHICH FUNCTION IT IS ..

Deutch's algorithm for f:{0,1}→{0,1}



$x=0 \Rightarrow$ f IS CONSTANT!
$x=1 \Rightarrow$ f IS BALANCED!

$$|\psi_1\rangle = H\otimes H\,|01\rangle = \left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right) = \frac{1}{2}\left(|0\rangle|0\rangle - |0\rangle|1\rangle + |1\rangle|0\rangle - |1\rangle|1\rangle\right)$$

$$|\psi_2\rangle = U_f\left\{\frac{1}{2}\left[|0\rangle|0\rangle - |0\rangle|1\rangle + |1\rangle|0\rangle - |1\rangle|1\rangle\right]\right\} = \frac{1}{2}\left\{|0\rangle|f(0)\rangle - |0\rangle|\overline{f(0)}\rangle + |1\rangle|f(1)\rangle - |1\rangle|\overline{f(1)}\rangle\right\}$$

$U_f(|x\rangle|y\rangle) = |x\rangle|y\oplus f(x)\rangle$

$$= \frac{1}{2}\left\{|0\rangle\left(|f(0)\rangle - |\overline{f(0)}\rangle\right) + |1\rangle\left(|f(1)\rangle - |\overline{f(1)}\rangle\right)\right\} = \frac{1}{\sqrt{2}}\sum_{x=0,1}|x\rangle\underbrace{\left(\frac{|f(x)\rangle - |\overline{f(x)}\rangle}{\sqrt{2}}\right)}$$

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

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

$$= \underbrace{\frac{1}{\sqrt{2}}\sum_{x=0,1}(-1)^{f(x)}|x\rangle}\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)$$

"PHASE KICK-BACK TRICK"

$= \pm|+\rangle$ IF f IS CONSTANT!
$= \pm|-\rangle$ IF f IS BALANCED!

APPLY $H\otimes H$ $\Rightarrow |\psi_3\rangle = \begin{cases} \pm|0\rangle|1\rangle \text{ IF } f(x) = \text{CONST.} \\ \pm|1\rangle|1\rangle \text{ IF } f(x) = \text{BALANCED.} \end{cases}$

READ-OUT x: $\begin{cases} \text{IF } x=0 \Rightarrow f \text{ CONST.} \\ \text{IF } x=1 \Rightarrow f \text{ BALANCED.} \end{cases}$

Remarks about Deutch's algorithm

- It took advantage of "quantum paralelism"

$|\text{INPUT}\rangle = H\otimes H\,|01\rangle = \frac{1}{2}\left\{|00\rangle - |01\rangle + |10\rangle - |11\rangle\right\}$

$U_f|\text{INPUT}\rangle = \sum_{\text{all } x}(-1)^{?}\,U_f(|x1\rangle)$

- The input |0>|1> was chosen so that after applying the algorithm the input register |x> interfered "constructively" for f(x) constant and "destructively" for f(x) balanced.

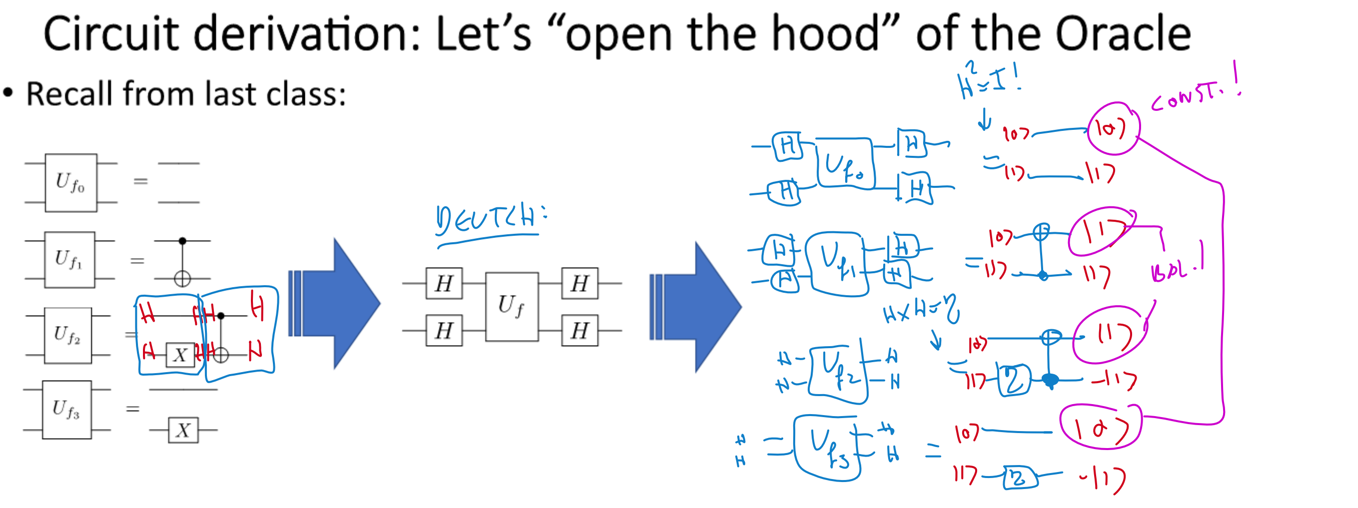
$\Rightarrow |x\rangle$ BECOMES $|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$ IF $f(x)$ CONSTANT

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

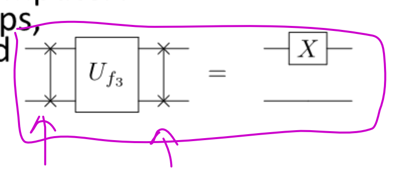
- No info whatsoever would be gained by measuring output register |y>. Also, the quantum procedure yielded no information on the actual value of f(0) or f(1)! Note the trade-off here: We gave up the knowledge of f(x) in order to obtain "relational" or "global" information on f(x) for all x!

Circuit derivation: Let's "open the hood" of the Oracle

- Recall from last class:



- Note how the H "flipped" the CNOT of the balanced f's only. Could we get the same result with a classical-reversible computer? The answer is no: If we replaced the H's with classical swaps, the trick fails! Check for yourself: End state of input would be f(1), no info on whether it's constant or balanced.



Action of Hadamard on n qubits

- To generalize Deutch to many qubits, we need this:

$$H\otimes H\otimes\cdots\otimes H\,|x_{n-1}x_{n-2}\cdots x_0\rangle = \left(H|x_{n-1}\rangle\right)\left(H|x_{n-2}\rangle\right)\cdots H(|x_0\rangle)$$

$x_{n-1} = 0$ OR 1 ; 0,1 ; 0,1

$$= \left(\frac{|0\rangle + (-1)^{x_{n-1}}|1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle + (-1)^{x_{n-2}}|1\rangle}{\sqrt{2}}\right)\cdots\left(\frac{|0\rangle + (-1)^{x_0}|1\rangle}{\sqrt{2}}\right)$$

$$= \frac{1}{\sqrt{2^n}}\sum_{y\in\{0,1\}^n}(-1)^{x\cdot y}|y\rangle$$

- "Bitwise modulo 2 inner product":

REG PRODUCT

$$x\cdot y = (x_{n-1}y_{n-1}) \oplus (x_{n-2}y_{n-2}) \oplus \cdots \oplus (x_0 y_0)$$

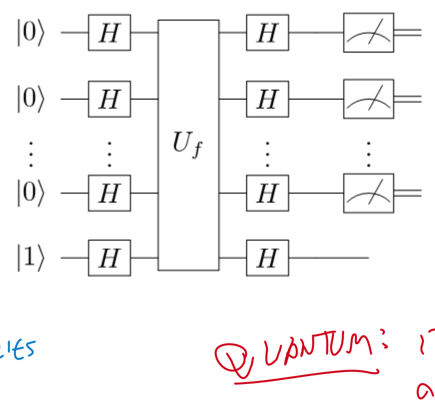
- Example:

$$H\otimes H\,|10\rangle = \left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right) = \frac{1}{\sqrt{4}}\left\{\underbrace{(-1)^{10\cdot 00}}_{+1}|00\rangle + \underbrace{(-1)^{10\cdot 01}}_{=+1}|01\rangle + \underbrace{(-1)^{10\cdot 10}}_{-1}|10\rangle + \underbrace{(-1)^{10\cdot 11}}_{=-1}|11\rangle\right\}$$

$x = 10$

Generalizing Deutch to f:{0,1}ⁿ→{0,1}

- Now there are 2^n inputs "x". Suppose you know a priori that f(x) is either constant or balanced. How many queries to certify that it's constant?



CLASSICALLY:

IF f HAPPENS TO BE BALANCED, YOU WILL PROBABLY FIND OUT AFTER A FEW QUERIES (≥ 2).

IF IT'S CONSTANT $\Rightarrow$ IT WILL TAKE $\frac{2^n}{2} + 1 = 2^{n-1} + 1$ QUERIES! HUGE!

QUANTUM: IT TAKES ONLY ONE QUANTUM QUERY!

PROOF NEXT CLASS.

Summary

- Deutch's algorithm inputs a superposition state containing ALL computational basis states into the Oracle:

$$H\otimes H\otimes\cdots\otimes H\,|00\cdots 0\rangle = \frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle$$

- Due to linearity, when the Oracle acts on this state, it evaluates f(x) for all x simultaneously! This is called *"quantum paralelism"*.

- The resulting state can now be "engineered" with additional unitaries in order to yield useful information when read out. For example, applying H⊗H⊗..⊗H again converts the state into 00…0 if and only if f(x)=constant. This enables the certification that f(x)=const. with a speed exponentially faster than classical! In this case *quantum advantage increases exponentially with the size of the problem.*