Generalization of CNOT gate

Suppose $f(x): \{0,1\} \Rightarrow \{0,1\}$ is a function of a one-bit domain and range.

To compute this function on a quantum computer, we consider a 2-qbit QC which starts in state $|x, y\rangle$.

With an appropriate sequence of logic gates, it is possible to transform this state in $|x, y \oplus f(x)\rangle$, where $\oplus$ is addition modulo 2.

data register

$|x, y\rangle$

target register

$$|x, y\rangle \xrightarrow{U_f} |x, y \oplus f(x)\rangle$$

U_f is unitary. If $y = 0$, the final state of the second qubit is $f(x)$. Indeed

if $y = 0$

$y \oplus f(x) = f(x)$

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

addition modulo 2.

Can we use U_f ~~for~~ evaluate $f(0)$ & $f(1)$ simultaneously.

(1b)

$$|x\rangle, |y\rangle \rightarrow \boxed{U_f} \rightarrow |x\rangle, |y \oplus f(x)\rangle$$

$\boxed{\text{is unitary}}$

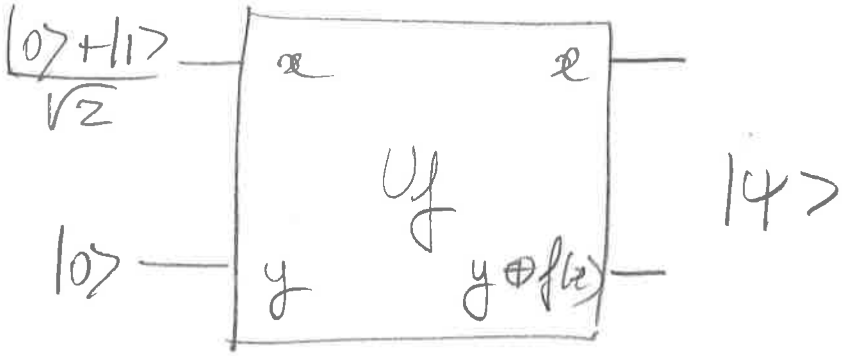
x	y	$f_1(x)$	$f_2(x)$	$f_3(x)$	$f_4(x)$	$y \oplus f_1$	$y \oplus f_2$	$y \oplus f_3$	$y \oplus f_4$
0	0	0	0	1	1	0	0	1	1
0	1	0	0	1	1	1	1	0	0
1	0	0	1	0	1	0	1	1	0
1	1	0	1	0	1	1	0	0	1

all 4 possible outcomes

//

//

//



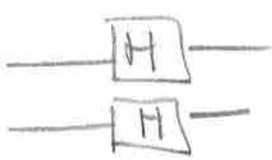
$$U_f \; \frac{|0\rangle+|1\rangle}{\sqrt{2}} \otimes |0\rangle = \left\{ \frac{|0, f(0)\rangle + |1, f(1)\rangle}{\sqrt{2}} \right\} = |\psi\rangle$$

This is a remarkable state! The different terms contain information about $f(0)$ & $f(1)$. It is as if we have evaluated $f(x)$ for 2 values of x simultaneously, a feature known as quantum parallelism.

A single U_f gate is used to evaluate the function for different x simultaneously!

How do we generalize the process to an arbitrary number of bits? We use the Hadamard transform! This operation is just n Hadamard gates acting in parallel on n qubits

For $n = 2$



$$|0\rangle - \boxed{H} - \frac{|0\rangle+|1\rangle}{\sqrt{2}}$$
$$|0\rangle - \boxed{H} - \frac{|0\rangle+|1\rangle}{\sqrt{2}}$$
$$\Bigg\} |\psi\rangle$$

$$\rightarrow |\psi\rangle = \frac{1}{\sqrt{2}}\left[|0\rangle+|1\rangle\right] \otimes \frac{1}{\sqrt{2}}\left[|0\rangle+|1\rangle\right] = \frac{|00\rangle+|01\rangle+|10\rangle+|11\rangle}{2}$$

we write $H^{\otimes 2}$ the parallel action of the 2 Hadamard gates

More generally $|0\rangle\otimes|0\rangle \cdots \otimes|0\rangle \rightarrow H^{\otimes n}$

$$\rightarrow \frac{1}{\sqrt{2^n}} \sum_x |x\rangle \Leftarrow \left[\begin{array}{l} 2^n \text{ states} \\ \text{superposition} \\ \text{using } n \text{ gates} \end{array}\right]$$

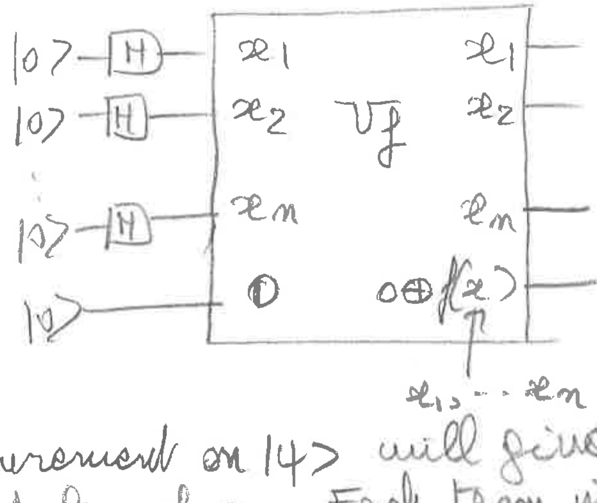
Σ is over all possible value of x.

The Hadamard transform produces an equal superposition of all computational basis states in $\mathbb{C}^n$.

Quantum parallel evaluation of a function with an n bit input x and 1 bit output, $f(x)$, can then be performed as follows

prepare the $n+1$ qubit state $|0\rangle^{\otimes n}|0\rangle$

Apply H to first n qubit with U_f



$$|\psi\rangle = \frac{1}{\sqrt{2^n}} \sum_x |x\rangle|f(x)\rangle$$

$\triangle$ measurement on $|\psi\rangle$ will give $f(x)$ for a single value of x. Each term in the sum has an equal probability.

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

$$(H \otimes H \otimes \cdots \otimes H)|00\cdots0\rangle = \frac{1}{\sqrt{2^n}}(|0\rangle+|1\rangle)(|0\rangle+|1\rangle)\cdots(|0\rangle+|1\rangle)$$

$$= \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle$$

$|0, 0, \ldots 1, \ldots 0\rangle$

all possible combinations

How do we extract information about more than one value of $f(x)$ from superposition states like $\sum_x |x, f(x)\rangle$

Deutsch's algorithm.

Suppose Alice has 2 bits 0, 1 she can send to Bob. Bob evaluates some Boolean function of the bit sent by Alice. What are the results that Bob can get

Alice	f_1	f_2	f_3	f_4
0	0	0	1	1
1	0	1	0	1

$\underbrace{\qquad\qquad\qquad\qquad}_{\text{only 4 possibilities.}}$

The two functions can be regrouped in two subsets. f_1, f_4 give the constant value 0 or 1 for the two bits 0 & 1 sent by Alice. f_2 f_3 gives either 0 or 1 after Alice sends her 2 bits. These are referred to as balanced functions.

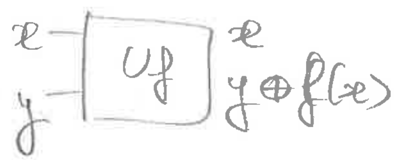
<u>Question</u>: Classically, can Alice send either 0 <u>or</u> 1 and find out if Bob selected a constant or balanced function to evaluate $f(x)$?

<u>Answer</u>: No, Alice must send both 0 & 1 before being able to answer that question.

Bob \ Alice	0	1	$f_i(0) \oplus f_i(1)$	
f_1	0	0	constant	0
f_2	1	1		0
f_3	0	1	balanced	1
f_4	1	0		1

↳ If we can find a circuit which can compute $f_i(0) \oplus f_i(1)$ in one shot, Alice will be able to answer the question of a constant or balanced function used by Bob in one shot!

How can we use U_f to do this?



y	$f(x)$		$y \oplus f(x)$
0	0	$\rightarrow$	0
0	1		1
1	0		1
1	1		0

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

$$|x\rangle\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \Rightarrow \frac{|x\rangle}{\sqrt{2}}\left[\underbrace{|0 \oplus f(x)\rangle} - |1 \oplus f(x)\rangle\right]$$

If $f(x)=0$ $\quad [|0\rangle - |1\rangle]$

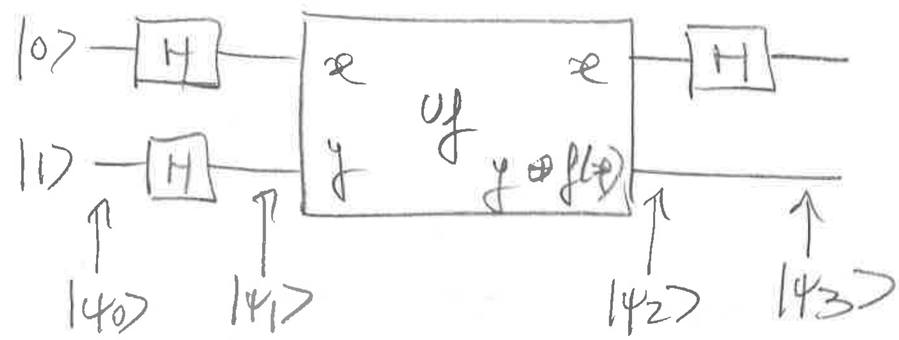
If $f(x)=1$ $\quad [|1\rangle - |0\rangle]$

So $$\frac{|x\rangle}{\sqrt{2}}\left[|0 \oplus f(x)\rangle - |1 \oplus f(x)\rangle\right] = \begin{cases} \dfrac{|x\rangle}{\sqrt{2}}\left(|0\rangle - |1\rangle\right) & \text{if } f(x) = 0 \\[2ex] -\dfrac{|x\rangle}{\sqrt{2}}\left(|0\rangle - |1\rangle\right) & \text{if } f(x) = 1 \end{cases}$$

These 2 results can be regrouped into one expression

$$|x\rangle \frac{1}{\sqrt{2}}\left[|0\rangle-|1\rangle\right] \to U_f \to (-1)^{f(x)}\,|x\rangle \left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)$$

The Deutsch* algorithm



$$|\psi_0\rangle = |0\rangle \otimes |1\rangle$$

$$|\psi_1\rangle = H|0\rangle \otimes H|1\rangle = \left[\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]$$

U_f to $|\psi_1\rangle$ $= (-1)^{f(0)}\frac{1}{\sqrt{2}}|0\rangle\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right] + (-1)^{f(1)}\frac{1}{\sqrt{2}}|1\rangle\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]$

if $f(0)=f(1) \Rightarrow U_f|\psi_1\rangle = \underbrace{(-1)^{f(0)}}_{\pm 1} \frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)$

± 1 depending if $f(0)=f(1)=0$ or 1

if $f(0)\neq f(1) \Rightarrow U_f|\psi_1\rangle \overset{?}{=}$ $\qquad (-1)^{f(1)} = -(-1)^{f(0)}$

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

or $$|\psi_2\rangle = U_f|\psi_1\rangle = \begin{cases} \pm\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right) & \underline{\text{if } f(0)=f(1)} \\ \pm\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right] & \underline{\text{if } f(0)\neq f(1)} \end{cases}$$

Finally The final Hadamard gate acting on the first qubit gives

$$|\psi_3\rangle = \begin{cases} \pm|0\rangle\left[\dfrac{|0\rangle-|1\rangle}{\sqrt{2}}\right] & \text{if } f(0)=f(1) \\ \pm|1\rangle\left[\dfrac{|0\rangle-|1\rangle}{\sqrt{2}}\right] & \text{if } f(0)\neq f(1) \end{cases}$$

but $f(0)\oplus f(1)$ is 0 if $f(0)=f(1)$
is 1 if $f(0)\neq f(1)$

see table top of page 5!

So, we can rewrite $|\psi_3\rangle$ more concisely

$$|\psi_3\rangle = \pm\,|f(0)\oplus f(1)\rangle\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]$$

We have accomplished our goal! By measuring the first qubit we may determine $f(0)\oplus f(1)$. This is a global property of $f(x)$... using only one evaluation of $f(x)$! This is faster than with a classical apparatus, which would require at least <u>2</u> evaluations.

The Deutsch-Jozsa Algorithm

Alice in Amsterdam selects a number x between 0 & 2^n-1, mails it to Bob in Boston. Bob calculates $f(x)$ and replies with the result 0 or 1.

f is either constant $\forall x$, or else balanced, that is, equal to 1 for exactly half x, and 0 for the other half.

Alice's goal is to determine if $f(x)$ is constant or balanced by corresponding with Bob as little as possible.

Classically, it will take $\frac{2^n}{2}+1$ communications

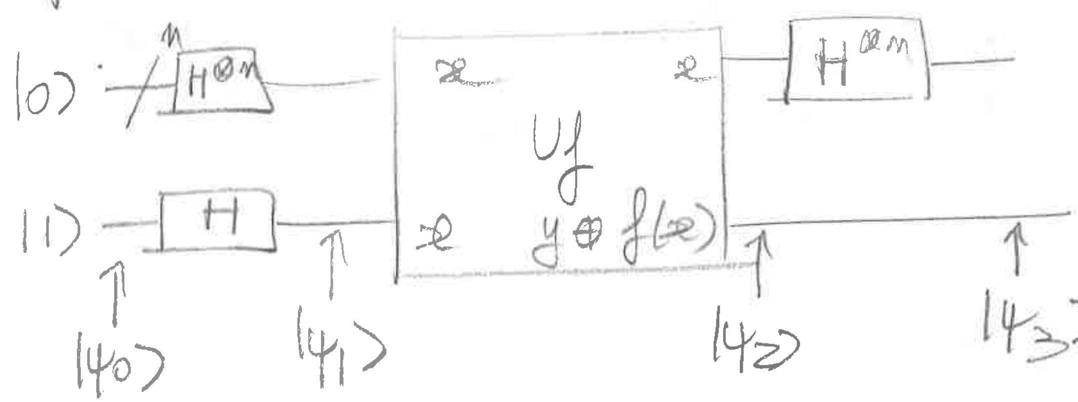
With qubits, Alice can achieve this in ONE query!

Alice has a n qubit register to store her query in.

Bob has one qubit

Bob will evaluate $f(x)$ using quantum parallelism.

The quantum circuit looks as follows



Input state $|\psi_0\rangle = |0\rangle^{\otimes n} \otimes |1\rangle$

$$|\psi_1\rangle = \underbrace{\sum_x \frac{|x\rangle}{\sqrt{2^n}}}_{\text{query is a superposition of all states}} \underbrace{\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]}_{\text{answer register is an evenly weighted superposition of 0 and 1.}}$$

$$U_f \rightarrow \quad |\psi_2\rangle = \sum_x \frac{(-1)^{f(x)}|x\rangle}{\sqrt{2}} \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$$

$f(x)$ is affecting the amplitude of each term in the n qubit register served by Alice.

$|\psi_3\rangle$? For a single qubit

$$H|x\rangle = \sum_{z=0,1} (-1)^{xz} \frac{|z\rangle}{\sqrt{2}} \leftarrow \checkmark$$

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

$$|x\rangle = |0\rangle \rightarrow \quad H|0\rangle = \frac{1}{\sqrt{2}}\left[|0\rangle + |1\rangle\right] = \frac{(-1)^{0\cdot 0}|0\rangle}{\sqrt{2}} + \frac{(-1)^{0\cdot 1}|1\rangle}{\sqrt{2}}$$

$$|x\rangle = |1\rangle \rightarrow \quad H|0\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right] = \frac{(-1)^{1\cdot 0}|0\rangle}{\sqrt{2}} + \frac{(-1)^{1\cdot 1}|1\rangle}{\sqrt{2}}$$

So for the Hadamard transform, we have

$$H^{\otimes n}|x_1, \ldots, x_n\rangle = \sum_{z_1 \ldots z_n = \{0,1\}} \frac{(-1)^{x_1 z_1 + \ldots + x_n z_n}|z_1, \ldots z_n\rangle}{\sqrt{2^n}}$$

$$H^{\otimes n}|x\rangle = \sum_z \frac{(-1)^{x.z}|z\rangle}{\sqrt{2^n}}$$

$x.z$ = bit wise inner product of x & z (modulo 2).

$$\rightarrow |\psi_3\rangle = \sum_z \sum_x \frac{(-1)^{x.z + f(x)}|z\rangle}{2^n}\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$$

Alice now observes the query register

The amplitude for the state $|0\rangle^{\otimes n}$ is

$$\sum_x (-1)^{f(x)}/2^n$$

If $f(x)$ = constant, amplitude is $(-1)^0$ or $(-1)^1$ ← 2^n times so +1 or −1

But $|\psi_3\rangle$ has unit length → all other amplitudes must be 0

→ an observation will lead 0s for ALL qubits in the query register.

If f is balanced, we have an even number of terms → half will be positive, half negative, and their sums will exactly balance out. → there is a zero amplitude for the state $|0\rangle^{\otimes n}$. So, a measurement must leave a result other than 0 on at least one qubit in the query register.

Summarizing,

If Alice measures all 0s then the function is constant; otherwise the function is balanced!

Deutsch's problem is not unfortunately an important problem.

There are algorithms which are quantum versions of the Fourier transform → Shor's algorithm for factoring and discrete algorithm. Also, the Grover or quantum search algorithm.