INTRO TO QUANTUM COMPUTING.

DEUTSCH - JOZSA ALGORITHM.

- It is a generalization of Deutsch-Algorithm that we have seen.
- It now concerns multivariable functions:

  $f(x_1, x_2, \dots, x_n) \in \{0,1\}$.

  where $x_i, i \in [n] \in \{0,1\}$.
- As before, we are again told that the function f is either constant (it maps either all inputs to 0 or all inputs to 1.). or, it is BALANCED: f maps exactly half of the inputs to 0, and the other half of the inputs to 1.
- Remember that given n binary variables $x_1, x_2, \dots, x_n$ $x_i \in \{0,1\}$, we can have 2^n possible inputs.

- So, suppose we are given a binary function f. How many function evaluations we need to make in order to correctly distinguish constant from balanced functions?

- $2^{n-1}+1$: 2^{n-1} evaluations give us half of the inputs. What if all of them are 1?

  → The function can still be balanced or constant.

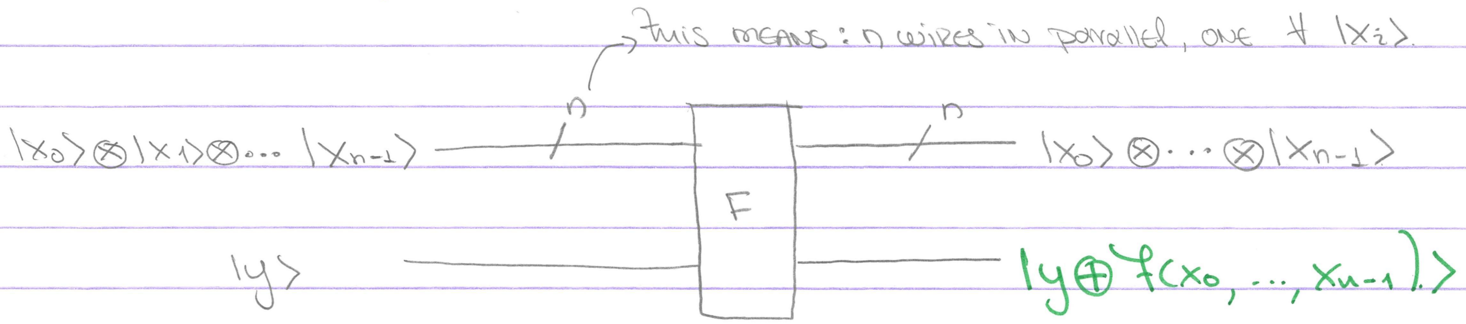
  → We need one more query in order to distinguish the two cases:

  If it is 1 → f is constant

  If it is 0 → f is balanced.

- As before, we will construct an orthogonal matrix that corresponds to a quantum circuit for f.

- Given any Boolean function $f(x_1, \dots, x_n)$ we construct the quantum gate F:



- Input: $n+1$ kets (qbits) $|x_i\rangle$, $|y\rangle$.
- Output: $n+1$ kets: the first n are exactly the same as the first n input kets $|x_i\rangle$. The last output is $|f(x_0, \dots, x_{n-1})\rangle$ if $y=0$ or its opposite value if $y=1$.

Interlude: Kronecker products of Hadamard.

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

$$H|0\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle, \quad H|1\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle.$$

- Suppose now we have as input 2 qbits, both going through Hadamard gates:

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

$$= \frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle + \frac{1}{2}|10\rangle + \frac{1}{2}|11\rangle.$$

Similarly we have:

2) $|0\rangle \otimes |1\rangle$ Goes to: $\frac{1}{2}|00\rangle - \frac{1}{2}|01\rangle + \frac{1}{2}|10\rangle - \frac{1}{2}|11\rangle$

3) $|1\rangle \otimes |0\rangle$ Goes to: $\frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle - \frac{1}{2}|10\rangle - \frac{1}{2}|11\rangle$

4). $|1\rangle \otimes |1\rangle$ Goes to: $\frac{1}{2}|00\rangle - \frac{1}{2}|01\rangle - \frac{1}{2}|10\rangle + \frac{1}{2}|11\rangle$

So...

$$|0\rangle \otimes |0\rangle = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} \text{ Goes to } \frac{1}{2}\begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}$$

$$|0\rangle \otimes |1\rangle = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} \text{ to } \frac{1}{2}\begin{bmatrix} 1 \\ -1 \\ 1 \\ -1 \end{bmatrix}$$

$$|1\rangle \otimes |0\rangle = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} \text{ to } \frac{1}{2}\begin{bmatrix} 1 \\ 1 \\ -1 \\ -1 \end{bmatrix}, \text{ and}$$

$$|1\rangle \otimes |1\rangle = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} \text{ Goes to } \frac{1}{2}\begin{bmatrix} 1 \\ -1 \\ -1 \\ 1 \end{bmatrix}$$

An orthonormal basis is sent to another orthonormal basis. We call the new basis

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

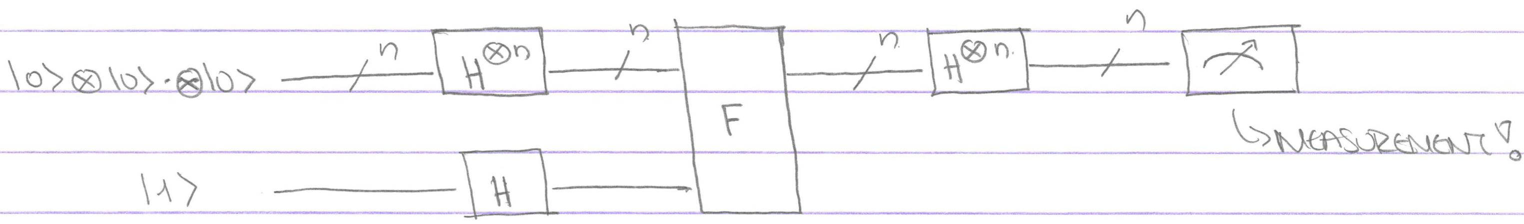
WE CAN FURTHER GENERALIZE:

$$H^{\otimes 3} = \frac{1}{\sqrt{2}} \begin{bmatrix} H^{\otimes 2} & H^{\otimes 2} \\ H^{\otimes 2} & -H^{\otimes 2} \end{bmatrix}, \ldots, H^{\otimes n} = \frac{1}{\sqrt{2}} \begin{bmatrix} H^{\otimes n-1} & H^{\otimes n-1} \\ H^{\otimes n-1} & -H^{\otimes n-1} \end{bmatrix}$$

and this gives us a neat and easy expression to calculate the composite state of n QBits that all pass through Hadamard gates.

BACK TO DEUTSCH-JOZSA:

- THE CIRCUIT THAT WILL INCORPORATE OUR FUNCTION f IS A GENERALIZATION OF DEUTSCH'S CIRCUIT.



ANALYSIS

- all the top n QBits are prepared in $|0\rangle$. For $n=2$ we get $|0\rangle \otimes |0\rangle = |00\rangle$.
- all of them pass through Hadamard gate i.e the state of the first n QBits is $H^{\otimes n}|0\cdots0\rangle$
- For $n=2$: $H^{\otimes 2}|00\rangle = \frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle + \frac{1}{2}|10\rangle + \frac{1}{2}|11\rangle$
- after all n QBits pass through Hadamard, they will be in a superposition of all possible states, each having the same probability amplitude: $\left(\frac{1}{\sqrt{2}}\right)^n$

▷ THE $(n+1)$th INPUT IS $|1\rangle$. IT PASSES THROUGH HADAMARD AND BECOMES : $\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$.

▷ FOR $n=2$, THE COMPOSITE STATE AT THIS POINT WILL BE:

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

$$= \frac{1}{2\sqrt{2}}|00\rangle \otimes \left(|0\rangle - |1\rangle\right) + \frac{1}{2\sqrt{2}}|01\rangle \otimes \left(|0\rangle - |1\rangle\right) +$$

$$+ \frac{1}{2\sqrt{2}}|10\rangle \otimes \left(|0\rangle - |1\rangle\right) + \frac{1}{2\sqrt{2}}|11\rangle \otimes \left(|0\rangle - |1\rangle\right).$$

STAGE 2: THE $n+1$ QBITS PASS THROUGH F

▷ THE QBIT y IS NOW $(|0\rangle - |1\rangle)$.
▷ THE CORRESPONDING OUTPUT WILL NOW BE $|y \oplus f(x_1, x_2)\rangle =$

$$= |y \oplus f(0,0)\rangle = |(|0\rangle - |1\rangle) \oplus f(0,0)\rangle =$$

$$= |f(0,0) \oplus 0\rangle - |f(0,0) \oplus 1\rangle = |f(0,0)\rangle - |f(0,0) \oplus 1\rangle$$

AND SO THE SYSTEM WILL BE IN COMPOSITE STATE

$$\frac{1}{2\sqrt{2}}|00\rangle \otimes \left(|f(0,0) \oplus 0\rangle - |f(0,0) \oplus 1\rangle\right) +$$

$$+ \frac{1}{2\sqrt{2}}|01\rangle \otimes \left(|f(0,1) \oplus 0\rangle - |f(0,1) \oplus 1\rangle\right) + \frac{1}{2\sqrt{2}}|10\rangle \otimes \left(|f(1,0)\rangle - |f(1,0) \oplus 1\rangle\right)$$

$$+ \frac{1}{2\sqrt{2}}|11\rangle \otimes \left(|f(1,1)\rangle - |f(1,1) \oplus 1\rangle\right)$$

▷ We use the same trick as in the previous lecture to write:

- $|f(0,0)\oplus 0\rangle - |f(0,0)\oplus 1\rangle = (-1)^{f(0,0)}(|0\rangle - |1\rangle)$
- $|f(0,1)\oplus 0\rangle - |f(0,1)\oplus 1\rangle = (-1)^{f(0,1)}(|0\rangle - |1\rangle)$
- $|f(1,0)\oplus 0\rangle - |f(1,0)\oplus 1\rangle = (-1)^{f(1,0)}(|0\rangle - |1\rangle)$
- $|f(1,1)\oplus 0\rangle - |f(1,1)\oplus 1\rangle = (-1)^{f(1,1)}(|0\rangle - |1\rangle)$

⇒ We have that the previous state can be rewritten:

$$(-1)^{f(0,0)}\frac{1}{2}|00\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) +$$

$$+ (-1)^{f(0,1)}\frac{1}{2}|01\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) +$$

$$+ (-1)^{f(1,0)}\frac{1}{2}|10\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) +$$

$$+ (-1)^{f(1,1)}\frac{1}{2}|11\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).$$

⇒ Bottom qbit is **NOT** entangled with the upper n qbits.

. These upper qbits are in state

$$\frac{1}{2}\left((-1)^{f(0,0)}|00\rangle + (-1)^{f(0,1)}|01\rangle + (-1)^{f(1,0)}|10\rangle + (-1)^{f(1,1)}|11\rangle\right).$$

- In General each state $|x_0, \ldots x_n\rangle$ will be multiplied by $\left(\frac{1}{\sqrt{2}}\right)^n (-1)^{f(x_0,\ldots,x_n)}$.

Stage 3: The upper n Qbits pass through Hadamard.

- For $n=2$, the previous state passes through $H^{\otimes 2}$
- The result is given by:

$$H^{\otimes 2} \begin{bmatrix} (-1)^{f(0,0)} \\ (-1)^{f(0,1)} \\ (-1)^{f(1,0)} \\ (-1)^{f(1,1)} \end{bmatrix} = \frac{1}{4} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \cdot \begin{bmatrix} (-1)^{f(0,0)} \\ (-1)^{f(0,1)} \\ (-1)^{f(1,0)} \\ (-1)^{f(1,0)} \end{bmatrix}.$$

Now, the probability amplitude of $|00\rangle$ is simply.

$$\frac{1}{4}\left((-1)^{f(0,0)} + (-1)^{f(0,1)} + (-1)^{f(1,0)} + (-1)^{f(1,1)} \right) = \alpha_{00}$$

Now let's see what happens depending on whether f is balanced or constant:

1) f is constant and $f(x_1,x_2)=0$

$\Rightarrow \alpha_{00} = 1/4\,(1+1+1+1) = 1$

2) f is constant and $f(x_1,x_2)=1$

$\Rightarrow \alpha_{00} = 1/4\,(-1-1-1-1) = -1$

3) f is balanced: half of $f(x_1,x_2)=0$, the other half $=1$

$\Rightarrow \alpha_{00} = 1/4\,(1+1\ \overset{-1\ -1}{\cancel{}}) = 0$ in each case.

So ....

- If the function is constant we will get final measurement outcome $|0\rangle$ with probability 1 !
- If f is balanced we will get $|0\rangle$ with probability 0 !

⇒ If at least one of the measurements is 1 ⇒ function is balanced !.

1 circuit evaluation (query) vs. $2^{n-1}+1$ classical function queries.

→ Dramatic speedup !.