3) Quantum Parallelism : The Deutsch - Josza problem.

This problem illustrates nicely the notion of quantum parallelism and where the power of quantum computation might lie. We start with a special case due to Deutsch.

• Deutsch Problem

We are given a black box representing $f: \{0,1\} \to \{0,1\}$ and are assured that f is either constant i.e $f(0) = f(1)$ or balanced $f(0) \neq f(1)$.

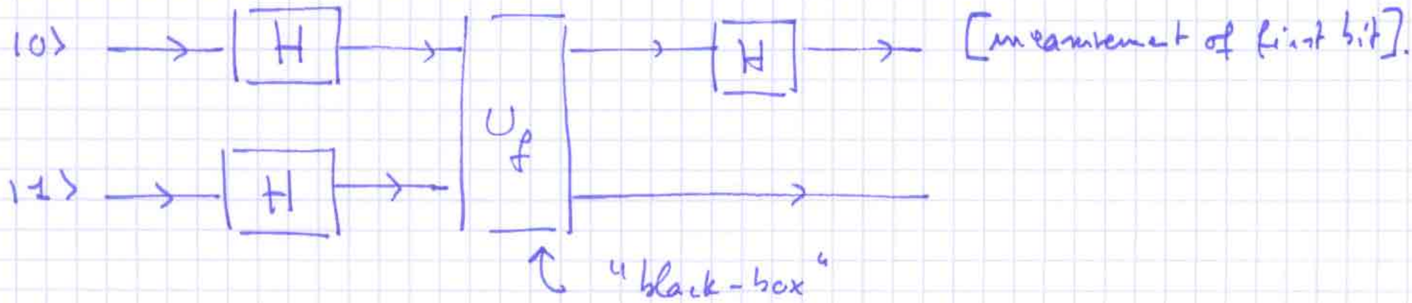
$$\text{input} \longrightarrow \boxed{\text{black Box}} \longrightarrow \text{output}.$$

The black-box gives us an output when it is queried with an input. How many queries are needed to decide if is constant or balanced?

Classicaly we need two queries. Indeed we present the input 0 and get $f(0)$. Then we present the input 1 and get $f(1)$ and check wether $f(0) = f(1)$ or $f(0) \neq f(1)$.

We will show that quantum mechanicaly one query suffices! This is because we can present a query $\alpha|0\rangle + \beta|1\rangle$ and get a global answer about f (even though we do learn what specific f is in the black box).

Consider the circuit:



where H is the Hadamard gate and

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

[Note that U_f can be represented by T, S, H, CNOT but this is not the point here; We view U_f as a black-box or "oracle" which gives us an output for a given input].

We query the black-box with $|0\rangle \otimes |1\rangle$. Let us compute the action of the circuit:

$$(H \otimes \mathbb{1})\, U_f \,(H \otimes H)\, |0\rangle \otimes |1\rangle$$

$$= (H \otimes \mathbb{1})\, U_f \,(H|0\rangle \otimes H|1\rangle)$$

$$= (H \otimes \mathbb{1})\, U_f \, \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle))$$

$$= (H \otimes \mathbb{1})\, \frac{1}{2}\left(U_f|00\rangle - U_f|01\rangle + U_f|10\rangle + U_f|11\rangle \right)$$

$$= (H \otimes \mathbb{1})\, \frac{1}{2}\left(\underbrace{|0\, f(0)\rangle - |0\; 1+f(0)\rangle} + \underbrace{|1\, f(1)\rangle + |1\; 1+f(1)\rangle} \right)$$

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

$$= (H \otimes \mathbb{1}) \frac{1}{2} \left((-1)^{f(0)} |0\rangle \otimes (|0\rangle - |1\rangle) + (-1)^{f(1)} |1\rangle \otimes (|0\rangle - |1\rangle) \right)$$

$$= (H \otimes \mathbb{1}) \frac{1}{2} \left((-1)^{f(0)} |0\rangle + (-1)^{f(1)} |1\rangle \right) \otimes (|0\rangle - |1\rangle) .$$

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

$$= \left\{ \frac{1}{2} \left((-1)^{f(0)} + (-1)^{f(1)} \right) |0\rangle + \frac{1}{2} \left((-1)^{f(0)} - (-1)^{f(1)} \right) |1\rangle \right\} \otimes \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle).$$

This last state is the output of the circuit. We now do a measurement of the first Qbit :

$$\text{Prob (outcome is } |0\rangle) = \frac{1}{4} \left| (-1)^{f(0)} + (-1)^{f(1)} \right|^2 = \begin{cases} 1 & \text{if } f(0) = f(1) \\ 0 & \text{if } f(0) \neq f(1) \end{cases}$$

$$\text{Prob (outcome is } |1\rangle) = \frac{1}{4} \left| (-1)^{f(0)} - (-1)^{f(1)} \right|^2 = \begin{cases} 0 & \text{if } f(0) = f(1) \\ 1 & \text{if } f(0) \neq f(1). \end{cases}$$

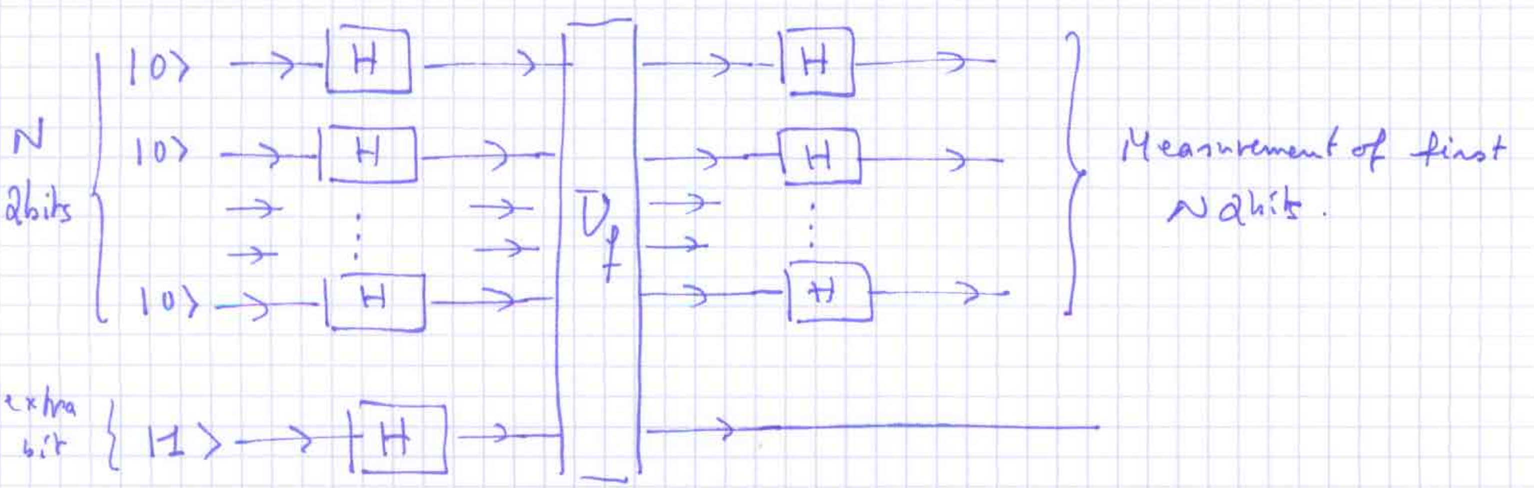
Thus if the function happens to balanced the measurement surely yields $|1\rangle$ and if it happens to be constant the measurement surely yields $|0\rangle$. Therefore with one "query" we can know if f is constant or balanced.

• Deutsch - Josza Problem.

This is a generalization of the previous problem to functions $f: \{0,1\}^N \rightarrow \{0,1\}$. We are assured that f is either constant or balanced. Here balanced means that it takes the value 0 for half of the inputs & the value 1 for the other half.

If f happens to be constant, classically we have to query the black box <u>at least</u> $\frac{2^N}{2} + 1 = 2^{N-1} + 1$ times to determine if it is constant. If we are very unlucky we might even have to use 2^N queries. On the other hand if f happens to be balanced we need at least 2 queries and at most $\frac{2^N}{2} + 1 = 2^{N-1} + 1$ queries.

We will now show that there is a quantum circuit for which only <u>one query</u> suffices! Consider the generalization of the previous circuit :



The effect of the Hadamard gates on the input is

$$|0\rangle\ldots|0\rangle|1\rangle \to \underbrace{(H\otimes\cdots\otimes H)}_{(N+1)\text{ times}} |0\rangle\otimes\cdots\otimes|0\rangle\otimes|1\rangle$$

$$= H|0\rangle\otimes\cdots H|0\rangle \otimes H|1\rangle$$

$$= \frac{1}{2^{N/2}} \underbrace{(|0\rangle+|1\rangle)\otimes\cdots\otimes(|0\rangle+|1\rangle)}_{N\text{ times}} \otimes\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle).$$

$$= \frac{1}{2^{N/2}} \sum_{b_1\cdots b_N\in\{0,1\}^N} |b_1\ldots b_N\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle-|1\rangle).$$

We query the U_f box with this input. The output is:

$$\frac{1}{2^{N/2}} \sum_{b_1\cdots b_N\in\{0,1\}^N} \left(\frac{1}{\sqrt{2}}|b_1\ldots b_N, f(b_1\cdots b_N)\rangle - \frac{1}{\sqrt{2}}|b_1\cdots b_N, 1+f(b_1\cdots b_N)\rangle\right)$$

$$= \frac{1}{2^{N/2}} \sum_{b_1\cdots b_N} \left(\frac{1}{\sqrt{2}}(-1)^{f(b_1\cdots b_N)}|b_1\cdots b_N, 0\rangle - \frac{1}{\sqrt{2}}(-1)^{f(b_1\cdots b_N)}|b_1\cdots b_N, 1\rangle\right).$$

$$= \frac{1}{2^{N/2}} \left(\sum_{b_1\cdots b_N} (-1)^{f(b_1\cdots b_N)} |b_1\cdots b_N\rangle\right) \otimes \frac{1}{\sqrt{2}}(|0\rangle-|1\rangle).$$

We apply again the Hadamard $H\otimes\cdots\otimes H$ on the first N qbit and leave the last qbit intact: This yields:

$$\frac{1}{2^{N/2}} \sum_{b_1\cdots b_N} (-1)^{f(b_1\cdots b_N)} (H|b_1\rangle\otimes\cdots\otimes H|b_N\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)$$

Since $\quad H|b_i\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + (-1)^{b_i}|1\rangle\right)$

we obtain

$$H|b_1\rangle \otimes \ldots \otimes H|b_N\rangle = \frac{1}{2^{N/2}} \sum_{a_1 \ldots a_N} (-1)^{\vec{a}\cdot\vec{b}} \, |a_1 \ldots a_N\rangle$$

where $\quad \vec{a}\cdot\vec{b} = \sum_{i=1}^{N} a_i b_i$

The net result for the output of the circuit is therefore :

$$\frac{1}{2^N}\left[\sum_{a_1 \ldots a_N} |a_1 \ldots a_N\rangle \cdot \left\{ \sum_{b_1 \ldots b_N} (-1)^{f(b_1 \ldots b_N)} (-1)^{\vec{a}\cdot\vec{b}} \right\}\right] \otimes \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right).$$

Now we measure the first N qbits : The probability of an outcome $(a_1 \ldots a_N) = (0 \ldots 0)$ is

$$\text{Prob}(0 \ldots 0) = \frac{1}{2^{2N}} \left| \sum_{b_1 \ldots b_N} (-1)^{f(b_1 \ldots b_N)} \right|^2 .$$

* If f happens to be constant we find $\text{Prob}(0 \ldots 0) = 1$ so the measurement will surely yield $(0 \ldots 0)$.

* If f happens to be balanced we find $\text{Prob}(0 \ldots 0) = 0$ so the measurement will surely yield $\underbrace{}_{\text{some}}$ $(a_1 \ldots a_N) \neq (0 \ldots 0)$

Summarizing we see that with only one query of the quantum circuit we can know if f is constant or balanced !