Query model of computation

Boolean functions $F : \{0,1\}^n \longmapsto \{0,1\}$

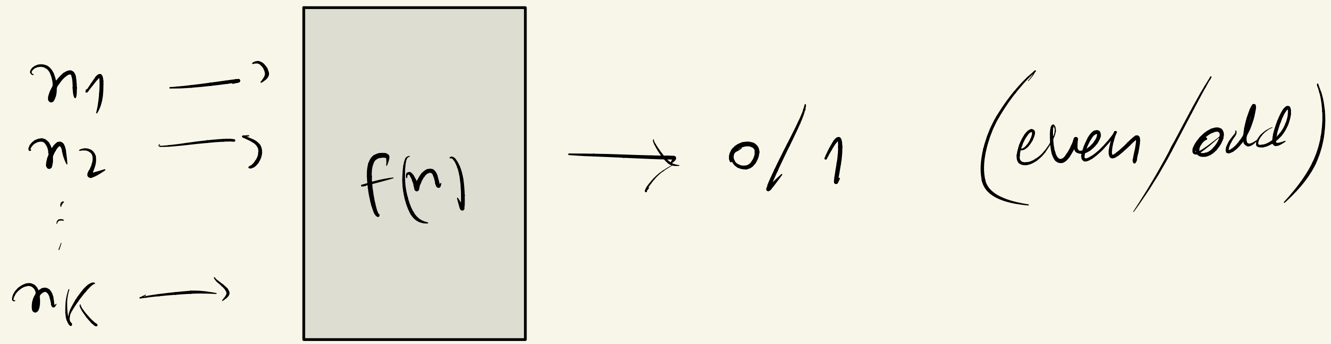
input binary strings $\quad x_1 \rightarrow,\ x_2 \rightarrow,\ \vdots,\ x_k \rightarrow \quad \boxed{F(x)} \longrightarrow$ output of computational model

$F(x)$ is also called an oracle, function that evaluates x.

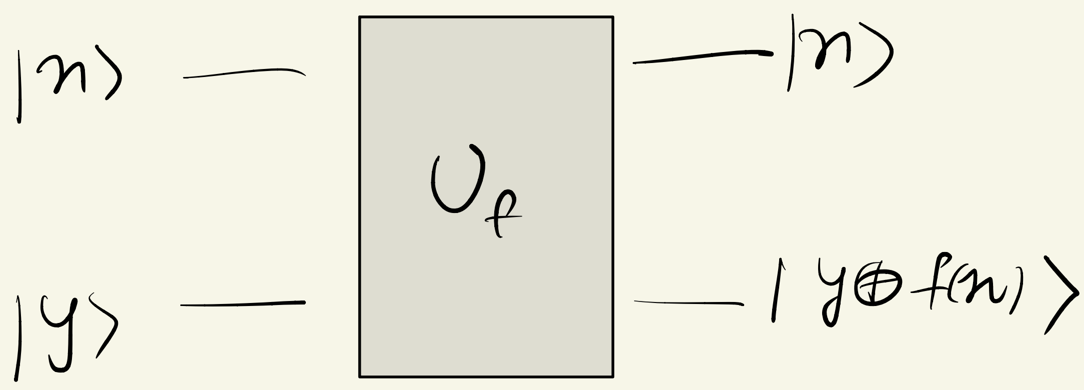
Efficiency of the query algorithm:

# of queries to f.

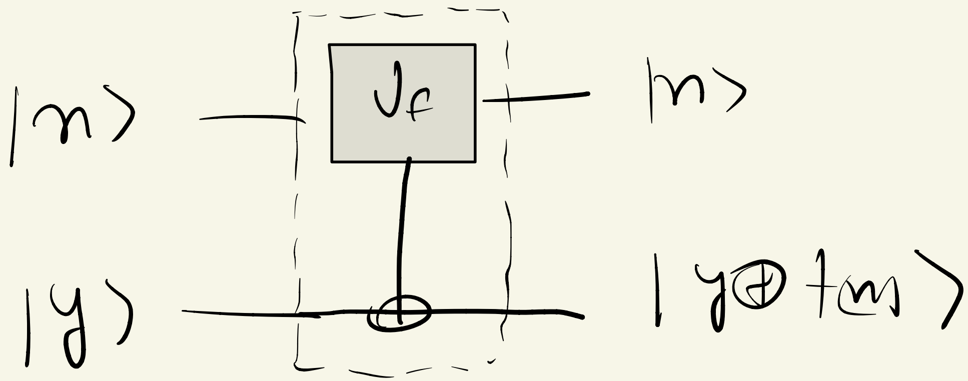
Example: whether number of strings such that $f(x) = 1$ is even/odd



Quantum Query gates



U_f makes bitflip on $|y\rangle$:



Deutsch-Jozsa Algorithm

let $f : \{0,1\}^n \mapsto \{0,1\}$

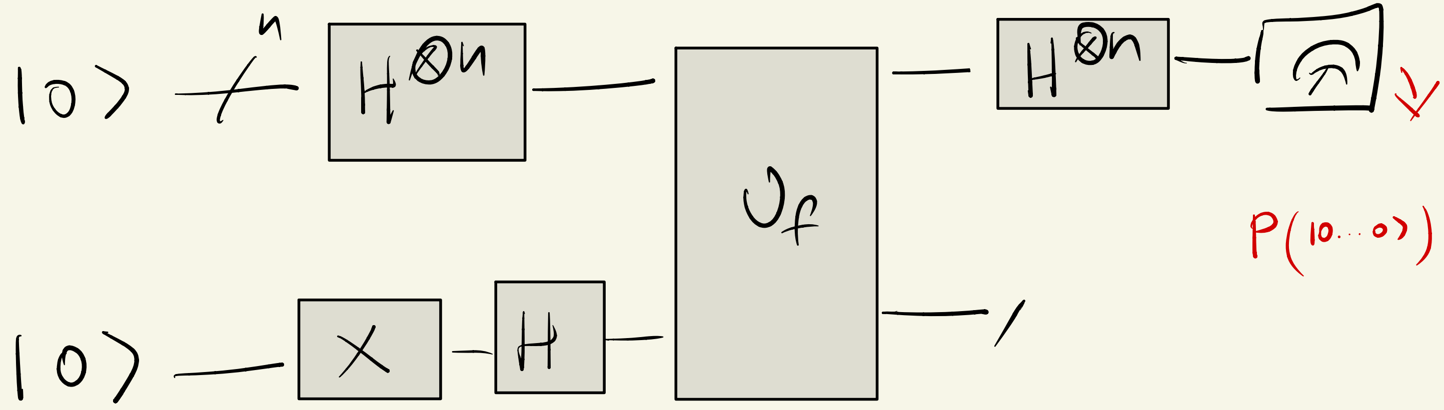
classify f as either constant / balanced (guaranteed)

classically: one needs $\frac{2^n}{2} + 1$ queries to f.

Quantum: promises 1 query!

Exponential Reduction in the # of queries!

(note that we did not specify U_f)



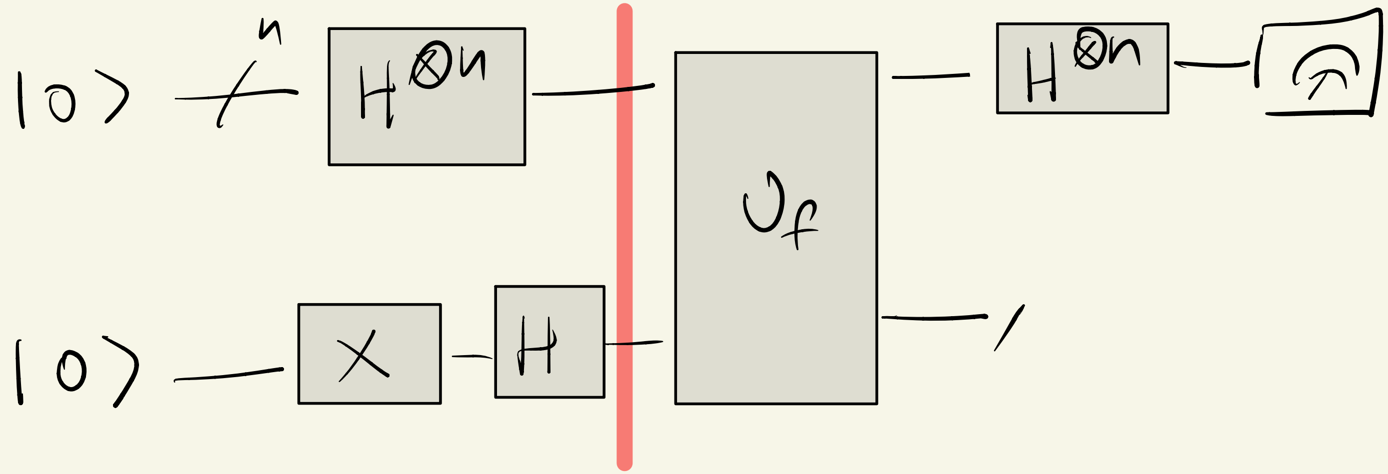
$$P(|0\dots0\rangle) = \begin{cases} 1, & f \text{ is constant} \\ 0, & f \text{ is balanced} \end{cases}$$

Superposition of inputs $|x\rangle = \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} |x_i\rangle$

Ancilla stores the output of f.

$f : \{0,1\}^n \mapsto \{0,1\}$

($|-\rangle$ state is useful for phase kickback)

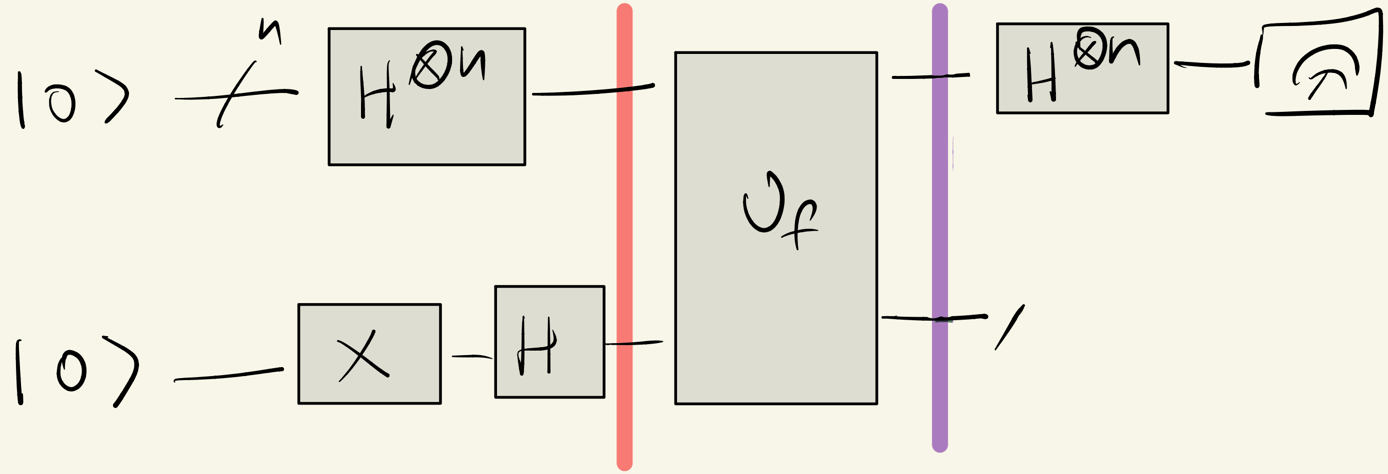


$f : \{0,1\} \mapsto \{0,1\}$

for $n = 1$:

$$|\psi\rangle = |+\rangle|-\rangle$$

$$= \frac{1}{2}|0\rangle\big(|0\rangle - |1\rangle\big) + \frac{1}{2}|1\rangle\big(|0\rangle - |1\rangle\big)$$

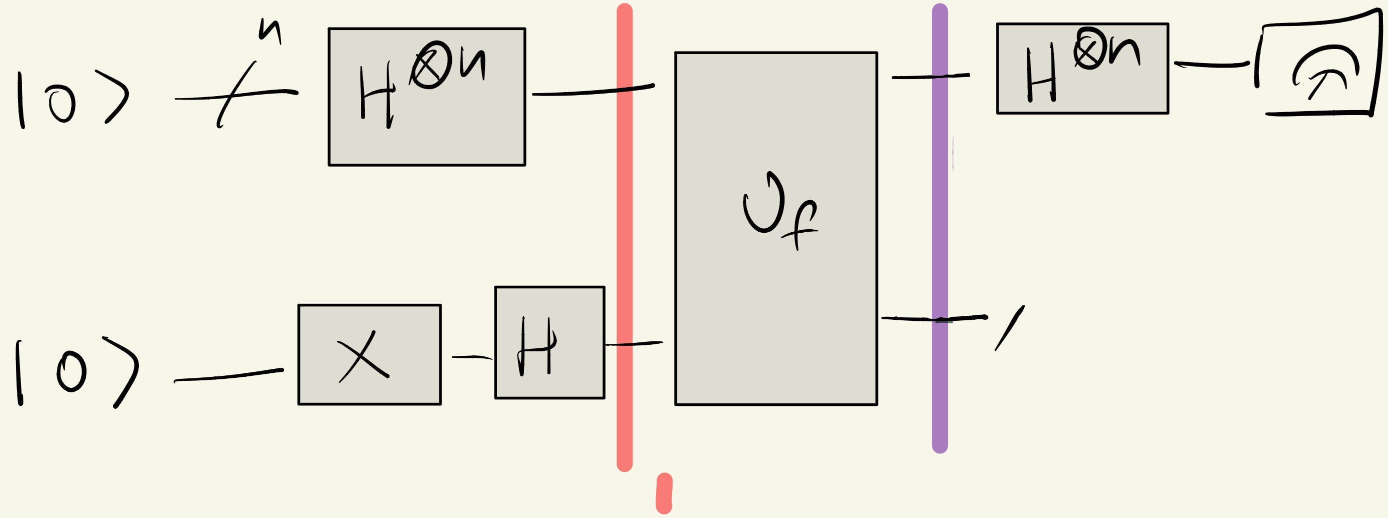


$$|\psi\rangle = \frac{1}{2}|0\rangle\left(|0\rangle - |1\rangle\right) + \frac{1}{2}|1\rangle\left(|0\rangle - |1\rangle\right)$$

$$U_f|\psi\rangle = \frac{1}{2}|0\rangle\left(|0\oplus f(0)\rangle - |1\oplus f(0)\rangle\right) + \frac{1}{2}|1\rangle\left(|0\oplus f(1)\rangle - |1\oplus f(1)\rangle\right)$$

if $f(0) = f(1) = 0 \rightarrow \quad |+\rangle|-\rangle$

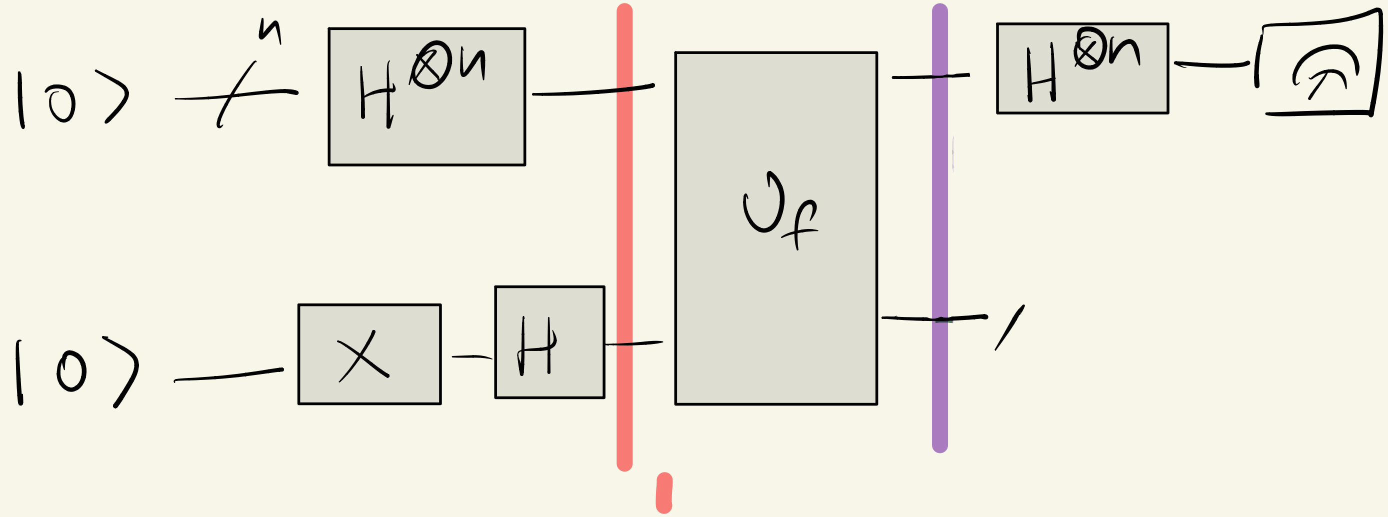
(one constant setting)



$$U_f|\psi\rangle = \frac{1}{2}|0\rangle\left(|0\oplus f(0)\rangle - |1\oplus f(0)\rangle\right) + \frac{1}{2}|1\rangle\left(|0\oplus f(1)\rangle - |1\oplus f(1)\rangle\right)$$

⊗ if either $f(0)$ or $f(1) = 1$ then bitflip happen.

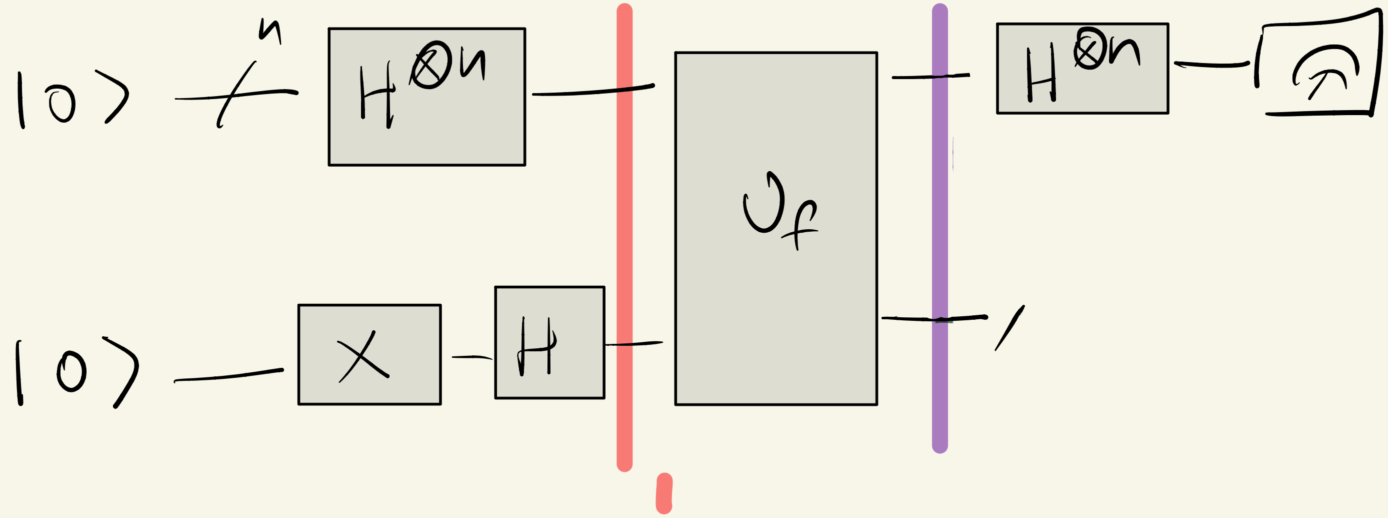
e.g: $f(0)=1 \rightarrow \frac{1}{2}|0\rangle\left(|1\rangle - |0\rangle\right)$



e.g: $f(0) = 1 \rightarrow \frac{1}{2}|0\rangle(|1\rangle - |0\rangle)$

$$= \frac{1}{2}|0\rangle \ominus (|0\rangle - |1\rangle)$$

$$= -\frac{1}{2}|0\rangle(|0\rangle - |1\rangle)$$



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

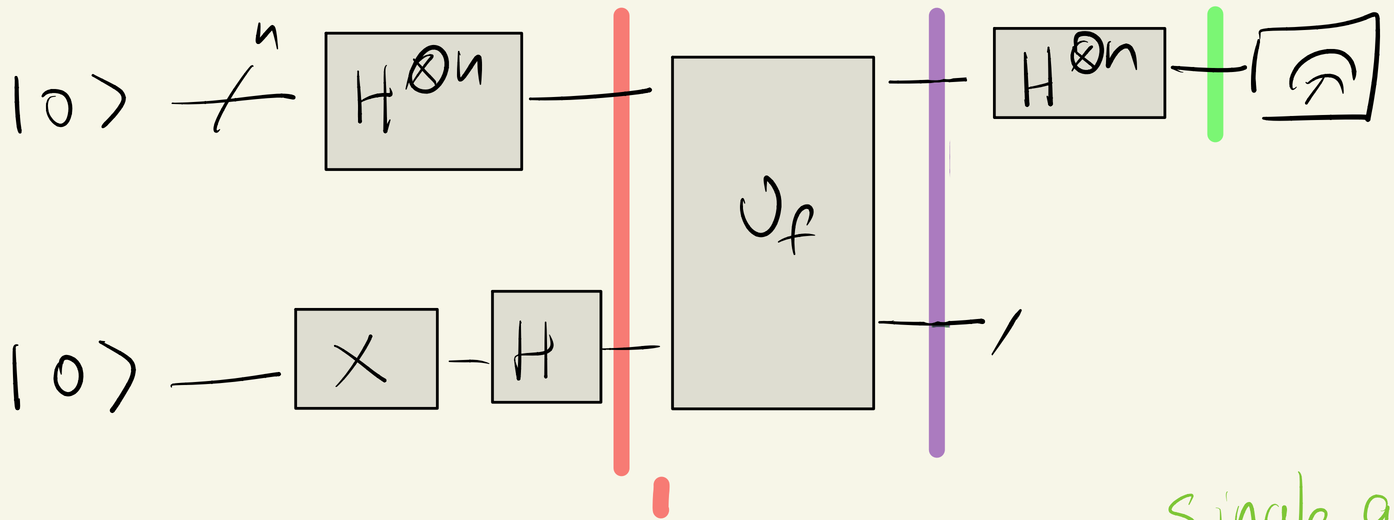
$$= \frac{1}{\sqrt{2}}(-1)^{f(0)}|0\rangle|-\rangle + \frac{1}{\sqrt{2}}(-1)^{f(1)}|1\rangle|-\rangle$$

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

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

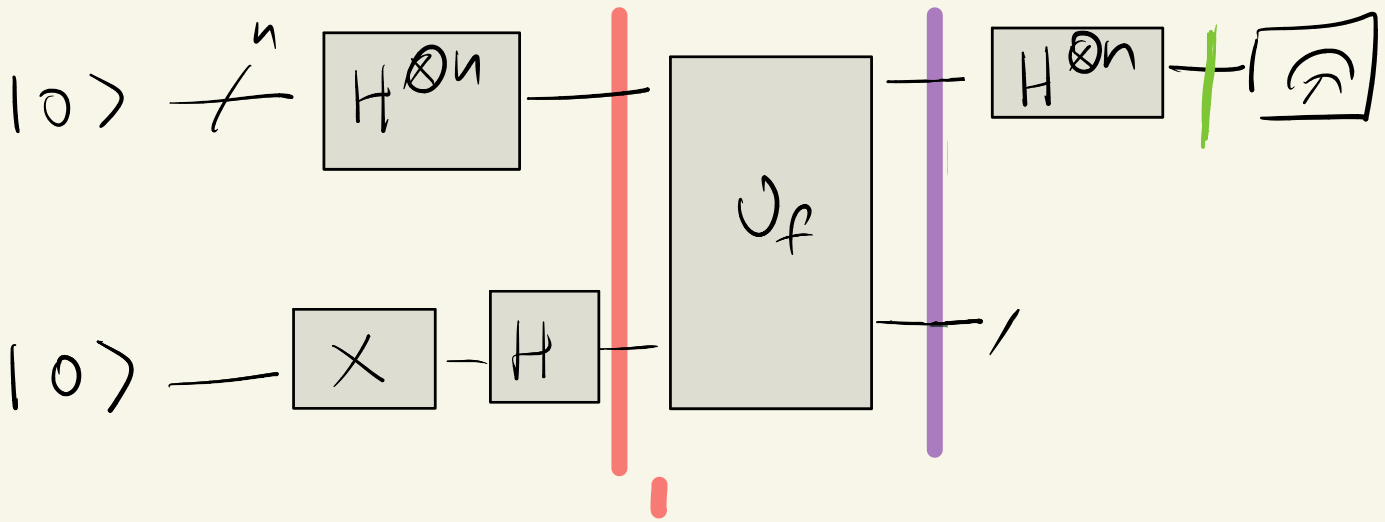
if $f(0) = f(1)$ (constant) $\rightarrow |+\rangle|-\rangle$

if $f(0) \neq f(1)$ (balanced) $\rightarrow |-\rangle|-\rangle$



$H|+\rangle = |0\rangle$

single quantum circuit execution needed because probability 1.



generalization for $n > 1$ and 2^n inputs

$$U_f\, |\psi\rangle = \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} (-1)^{f(x_i)} |x_i\rangle \, |-\rangle$$

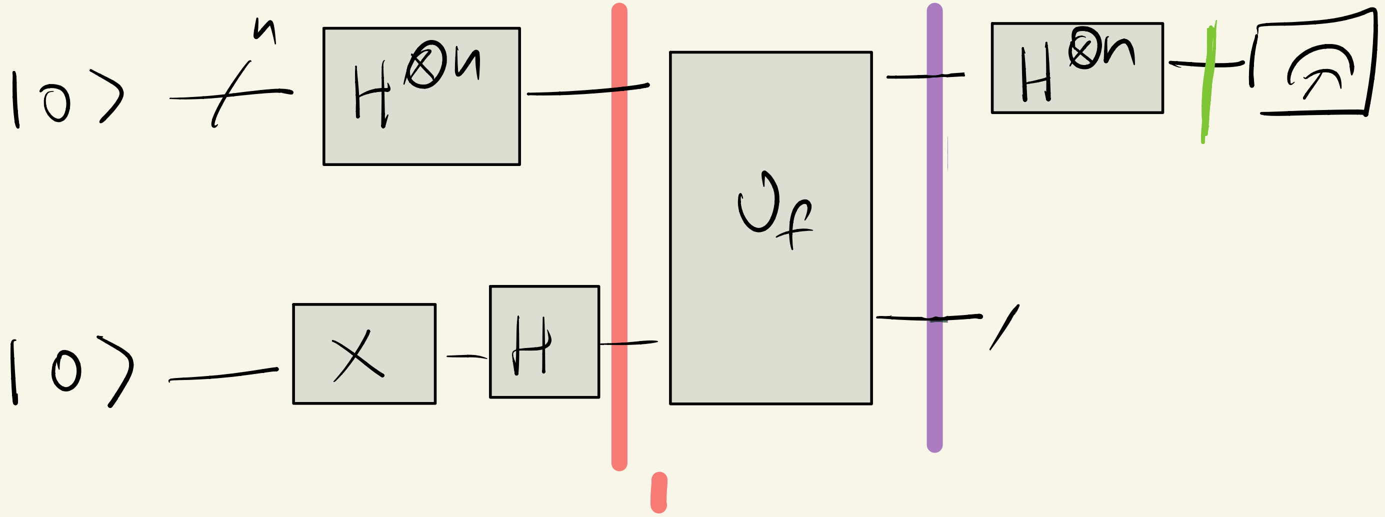
last Hadamard ?

$$H^{\otimes n} \, |x_n \; x_{n-1} \; \dots \; x_1\rangle$$

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

$$= \frac{1}{\sqrt{2}} \sum_{y_n \in \{0,1\}} (-1)^{y_n x_n} |y_n\rangle + \frac{1}{\sqrt{2}} \sum_{y_{n-1} \in \{0,1\}} (-1)^{y_{n-1} x_{n-1}} + \dots$$

$$= \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n - 1} (-1)^{y_n x_n + y_{n-1} x_{n-1} + \dots + y_1 x_1} |y_i\rangle$$



generalization for $n>1$ and 2^n inputs

$$U_f\,|\psi\rangle = H^{\otimes n}\frac{1}{\sqrt{2^n}}\sum_{i=0}^{2^n-1}(-1)^{f(x_i)}\,|x_i\rangle \; |-\rangle$$

$$\frac{1}{2^n}\sum_{i=0}^{2^n-1}(-1)^{f(x_i)}\sum_{j=0}^{2^n-1}(-1)^{y_nx_n+y_{n-1}x_{n-1}+\dots+y_1x_1}\,|y_j\rangle$$

state $|00\dots0\rangle$ measured with probability :

$$\left| \frac{1}{2^n} \sum_{i=0}^{2^n-1} (-1)^{f(x_i)} \right|^2$$

if f is <u>constant</u> then :

$$f(x_i) = 0 \quad \forall x_i \rightarrow P(00\dots0) = 1$$

$$f(x_i) = 1 \quad \forall x_i \rightarrow P(00\dots0) = 1$$

if f is <u>balanced</u> then $P(0\dots0) = 0$