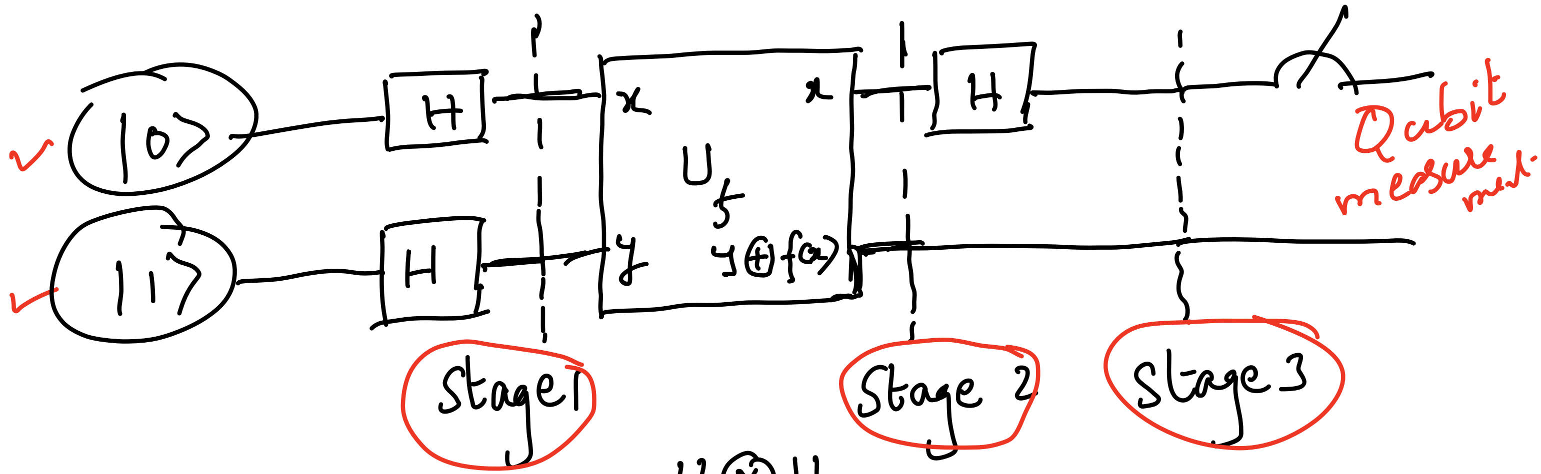


$$|0\rangle \otimes |1\rangle = |0,1\rangle \xrightarrow{H \otimes H} |+,-\rangle$$

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

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

Stage 1

Recall

$$U_f |x,-\rangle = (-1)^{f(x)} |x,-\rangle$$

where $x = \{0, 1\}$

$$\Big\downarrow U_f$$

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

Stage 2

H

$$\Big\downarrow H \otimes I$$

H

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

Stage 3

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

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

$$= \frac{1}{2}\left[\left\{(-1)^{f(0)} + (-1)^{f(1)}\right\} |0,-\rangle\right] \longrightarrow T1 \times$$

$$+ \frac{1}{2}\left[\left\{\underbrace{(-1)^{f(0)}} - \underbrace{(-1)^{f(1)}}\right\} |1,-\rangle\right] \longrightarrow T2$$

f is constant or balanced

If f is constant : $f(0) = f(1)$

f is balanced : $f(0) \neq f(1)$

* Let us consider if f is constant $f(0) = f(1)$

<u>output of stage 3</u>

$T2 = 0$ (because $(-1)^{f(0)} = (-1)^{f(1)}$)

$$T1 :\to \frac{1}{2}\left\{\left\{(-1)^{f(0)} + (-1)^{f(0)}\right\} |0,-\rangle\right\}$$

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

$$= \pm |0,-\rangle$$ because $f(0) = f(1) = 0$ or 1

Output of stage 3 will turn out to be $\pm|0\rangle$ if f is a constant function.

So I will get 0 as my measurement value!

* Let us consider the case if f is balanced $f(0) \neq f(1)$

output at stage 3

T1 → 0

T2 → $\pm|1\rangle$

Measurement of first qubit will always give me $|1\rangle$ whenever $f(0) \neq f(1)$

Extend the algorithm to the case where you have $2^n = N$

$\Rightarrow 2^n$ possible inputs

$N = 2^n$ boxes and each box can have either an apple/orange

i.e (i) All have same kind of fruit

(ii) half of the boxes have apple and other half boxes have orange

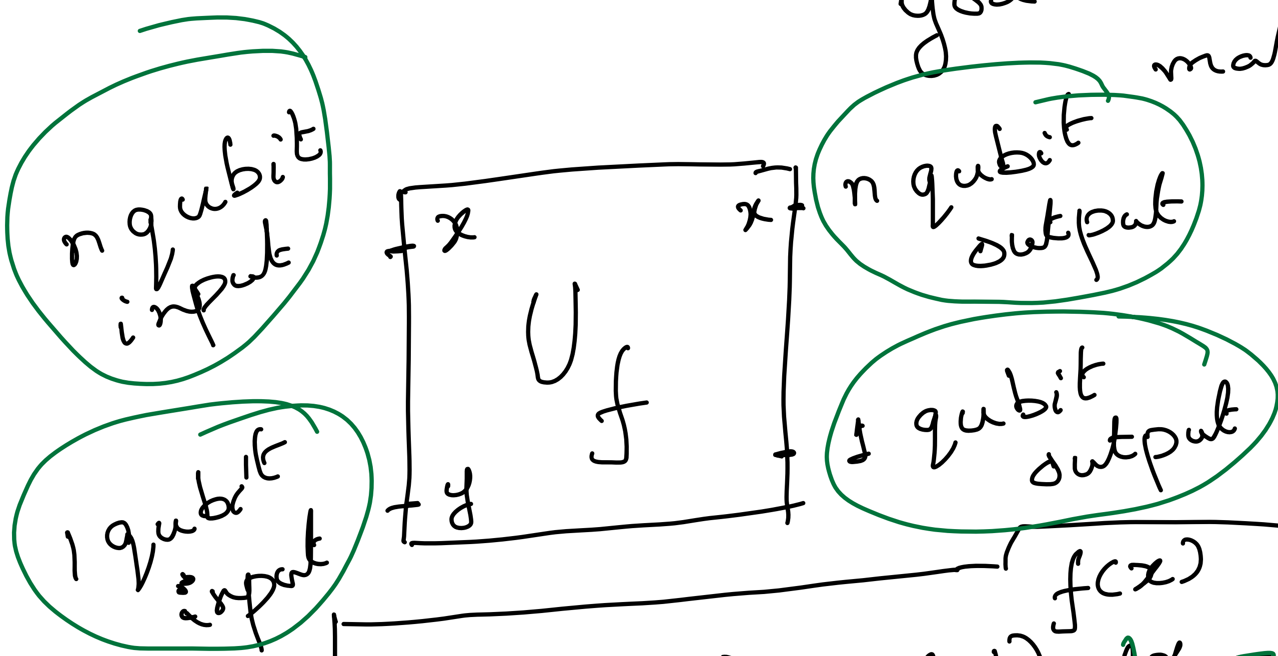
Problem Statement :-

* Oracle/black box access to a function f $f: \{0,1\}^n \rightarrow \{0,1\}$

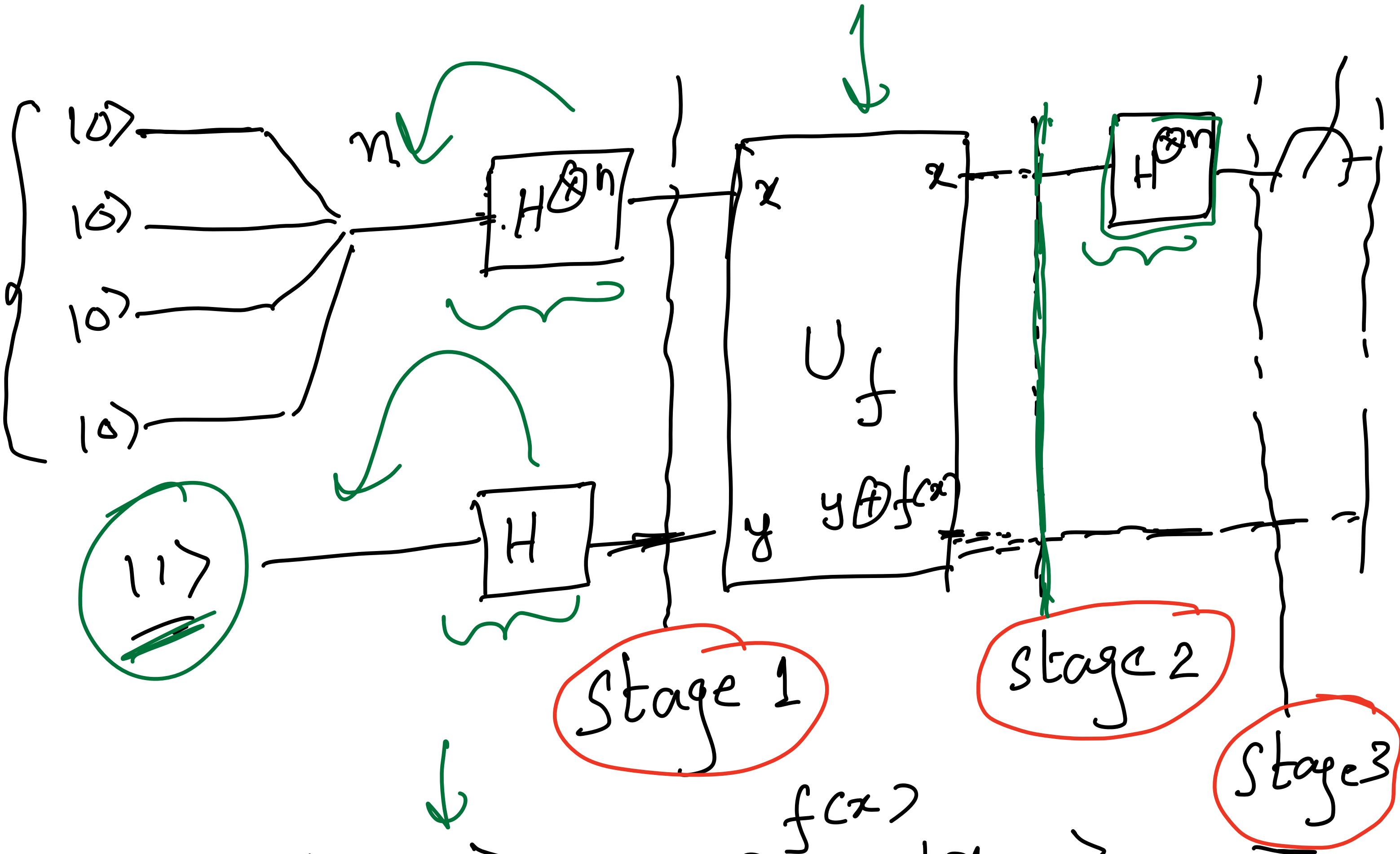
- Input : n bits (2^n possible inputs)
- Output : Single bit either 0 or 1
- f is either a constant or a balanced function.

* **Task**: To find f is constant or balanced?

Classical Algo:- $2^{n-1} + 1$ number of queries you need to make



$$\boxed{U_f |x, -\rangle = (-1)^{f(x)} |x, -\rangle}$$



(1) $U_f|x,-\rangle = (-1)^{f(x)}|x,-\rangle$

eg

$$U_f|000\ldots0,-\rangle = (-1)^{f(x)}|00\ldots0,-\rangle$$

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

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

$$H|1\rangle = |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \quad \text{— (2)}$$

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

$a = \{0, 1\}$

$(-1)^0 = 1$

$\underline{\underline{a = 0}}$

$(-1)^1 = -1$

$a = 1$

1-qubit case

$$\boxed{H|a\rangle = \frac{1}{\sqrt{2}} \sum_{x \in \{0,1\}} (-1)^{a \cdot x} |x\rangle}$$ ✓

$a = \{0, 1\}$

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

$$\boxed{H^{\otimes 2}|a\rangle = \frac{1}{\sqrt{2^2}} \sum_{x \in \{0,1\}^2} (-1)^{a \cdot x} |x\rangle}$$

$x = (0,1)$
$= (1,0)$
$= (0,0)$
$= (1,1)$

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

$a = \{0,1\}^2$

$|a\rangle = |0, 0\rangle$

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

$a = 1\ 1\ 0$
$y = 1\ 1\ 1$
$a \cdot y = (1*1 + 1*1 + 0*1) \bmod 2$

$$\boxed{H^{\otimes n}|0\ldots0\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle}$$

$|x\rangle = |0\ldots0\rangle$ or $|1\ldots1\rangle$ or $|010\ldots\rangle$

<u>Input</u>:-

$|0\ldots0\rangle \otimes |1\rangle \leftarrow$ $\{0,1\}^n$

$$\Big\downarrow H^{\otimes n} \otimes H$$

$$\frac{1}{\sqrt{2^n}}\left(\sum_{x\in\{0,1\}^n} |x\rangle \otimes |-\rangle\right)$$

stage 1

$$\Big\downarrow U_f$$

$$\boxed{U_f|x,-\rangle = (-1)^{f(x)}|x,-\rangle}$$

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

stage 2

$|x\rangle$ is a n qubit representation

$$\frac{1}{\sqrt{2^n}}\left[\sum_{x\in\{0,1\}^n}(-1)^{f(x)}|x\rangle \otimes |-\rangle\right]$$

$$\Big\downarrow H^{\otimes n}\otimes I$$

Note that

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

$$\frac{1}{\sqrt{2^n}}\left[\sum_{x\in\{0,1\}^n}(-1)^{f(x)}\left\{\frac{1}{\sqrt{2^n}}\sum_{y\in\{0,1\}^n}(-1)^{x\cdot y}|y\rangle\right\}\right]\otimes|-\rangle$$

$$\Big\downarrow \text{Rearrangement}$$

$$\frac{1}{2^n}\sum_{y\in\{0,1\}^n}\left[\left(\sum_{x\in\{0,1\}^n}(-1)^{f(x)}(-1)^{x\cdot y}\right)|y\rangle\right]\otimes|-\rangle$$

Stage 3

My claim is

If measurement output is all zeros 'f' is a constant, for any other output 'f' is balanced

How?

$x \cdot y = 0$

$|y\rangle = |0 \ldots 0\rangle \leftarrow$

$$\frac{1}{2^n}\left[\underbrace{\sum_{x \in \{0,1\}^n} (-1)^{f(x)}}\right] \longrightarrow$$ Term in the summation over y when $|y\rangle = |0\ldots 0\rangle$

$$= \frac{1}{2^n}\left[(-1)^{f(x)} 2^n\right]$$ if $f(x)$ is constant when $|y\rangle = |0\ldots 0\rangle$

$= \pm 1$

If $f(x)$ is constant we showed the term in the summation over y when $|y\rangle = |0\ldots 0\rangle$ is having a coefficient ± 1

the state at stage 3 only has the term involving $|y\rangle = |00\ldots 0\rangle$

$$\frac{1}{2^n}\left\{\sum_{y\in\{0,1\}^n}\left(\left[\sum_{x\in\{0,1\}^n}(-1)^{f(x)}(-1)^{x\cdot y}\right]\right)|y\rangle\right\}\otimes|-\rangle$$

Summation over y

$\alpha_1\,\underbrace{|0\ldots0\rangle} + \alpha_2\,|010\ldots0\rangle + \alpha_3\,|001\ldots0\rangle + \cdots$

$$\boxed{\alpha_1 = \frac{1}{2^n}\sum_{x\in\{0,1\}^n}(-1)^{f(x)}(-1)^{x\cdot y}}$$

$= \pm 1$

n-qubit

If $\alpha_1 = \pm 1$, for the state at stage to be normalized

$\alpha_2 = \alpha_3 = \cdots \alpha_{2^n} = 0$

1. If $f(x)$ is constant, the state at stage at 3 will be $|000\ldots0\rangle$

(2) If $f(x)$ is balanced

$$\alpha_1 = \frac{1}{2^n} \sum_{x \in \{0,1\}^n} (-1)^{f(x)} (-1)^{x \cdot y}$$

$$= \frac{1}{2^n} \left[(-1)^0 2^{n-1} + (-1)^1 2^{n-1} \right]$$

$$= 0$$

Output at stage 3 will always have linear combination of n qubit basis states except $|00\ldots0\rangle$

Bernstein – Vazirani Algorithm

Given :-

Oracle for function $f: \{0,1\}^n \rightarrow \{0,1\}$

→ Input n bits

→ output : 1 bit either 0 or 1

→ There exists a secret n-bit string 's' such that

$$f(x) = s \cdot x$$

Task is to find n-bit string s

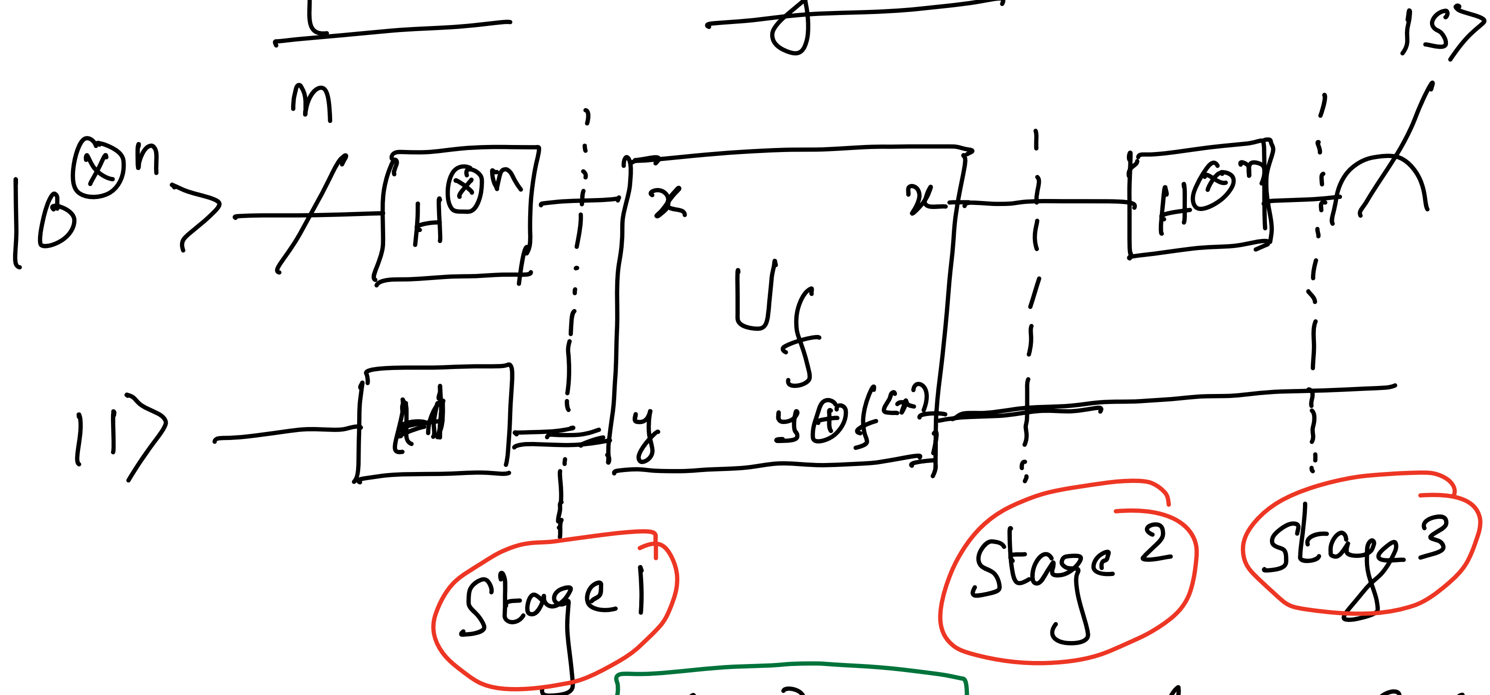
$$f(x) = s \cdot x$$

$n = 4$ bits

x	s	$s \cdot x$
1 0 0 0	$s_1\, s_2\, s_3\, s_4$	s_1
0 1 0 0	$s_1\, s_2\, s_3\, s_4$	s_2
0 0 1 0	$s_1\, s_2\, s_3\, s_4$	s_3
0 0 0 1	$s_1\, s_2\, s_3\, s_4$	s_4

Classically → n queries to the oracle

Quantum Algorithm



$$U_f|x,-\rangle = (-1)^{f(x)}|x,-\rangle \quad -(1) \qquad f(x) = s\cdot x$$

$$|a\rangle \xrightarrow{H^{\otimes n}} \frac{1}{\sqrt{2^n}} \sum_{y\in\{0,1\}^n} (-1)^{a\cdot y}|y\rangle \quad -(2)$$

$$|0\ldots0\rangle \xrightarrow{H^{\otimes n}} \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle \quad -(3)$$

To compute what happens at stage 1

$$|0^{\otimes n}\rangle \otimes |1\rangle$$
$$\downarrow H^{\otimes n} \otimes H$$

$$= \frac{1}{\sqrt{2^n}} \left[\sum_{x \in \{0,1\}^n} |x\rangle \right] \otimes |-\rangle \quad \text{[output at stage 1]}$$

$$\Big\downarrow U_f$$

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

$f(x) = s \cdot x$

$$\Big\downarrow$$

$$= \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} (-1)^{s \cdot x} |x\rangle \otimes |-\rangle \quad \text{[output at stage 2]}$$

$$\Big\downarrow H^{\otimes n} \otimes I$$

$$= \underbrace{\frac{1}{\sqrt{2^n}}} \sum_{x \in \{0,1\}^n} (-1)^{s \cdot x} \left[\underbrace{\frac{1}{\sqrt{2^n}}} \sum_{y \in \{0,1\}^n} (-1)^{x \cdot y} |y\rangle \right] \otimes |-\rangle$$

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

[output at stage 3]

$$\Downarrow$$

$$\boxed{(-1)^{x\cdot s}\,(-1)^{x\cdot y} = (-1)^{x\cdot(s\oplus y)}}$$

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

$$\Downarrow$$

$$\boxed{= \frac{1}{2^n}\left\{\left(\sum_{y\in\{0,1\}^n}\left[\underbrace{\sum_{x\in\{0,1\}^n} (-1)^{x\cdot(s\oplus y)}}\right]|y\rangle\right\}\otimes|-\rangle}$$

How will I deduce my "s" $\hookrightarrow \oplus$ by making a measurement of n qubit system after stage 3?

What will happen if I consider my $|y\rangle = |s\rangle$

$$x \cdot (s \oplus y) = 0$$

$$(-1)^{x \cdot (s \oplus y)} = 1$$

If I focus on the state $|y\rangle = |s\rangle$

$$\alpha_1 |0 \ldots 0\rangle + \alpha_2 |010 \ldots 0\rangle + \alpha_y |\underbrace{\quad\quad}\rangle + \ldots \alpha_{2^n}$$

$$\frac{1}{2^n}\left(\sum_{x \in \{0,1\}^n} \underbrace{(-1)^{x \cdot (s \oplus y)}}_{1}\right)$$

$$\frac{1}{2^n}\left(2^n\right) = 1$$

$\alpha_y = 1$ where $y = s$

$\alpha_1 = \alpha_2 = \ldots \alpha_{2^n} = 0$

The only term which will survive in the above equation (7) is when $|y\rangle = |s\rangle$

i.e n bits of $|y\rangle$ match with n bits of $|s\rangle$

Hence my measurement of "n" qubits after stage 3 will give me what is the value of n bit string "s" in my function $f(x)$