$$|x\rangle|a\rangle \longrightarrow |x\rangle|a \oplus f(x)\rangle$$

Algorithm Involves 6 Steps

1. The Two n-qubit input register are initialized to zero state

$$|\psi_1\rangle = |0\rangle^{\otimes n} |0\rangle^{\otimes 1}$$

2. Apply Hadamard to first register

$$|\psi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle |0^{\otimes 1}\rangle$$

3. Apply the query function

$$|\psi_3\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle |f(x)\rangle$$

4. Measure the second register. A certain value of $f(x)$ will be observed, $f(x)$ could correspond to two possible input

x and $y = x \oplus b$

$$|\psi_4\rangle = \frac{1}{\sqrt{2}} (|x\rangle + |y\rangle)$$

5. Apply Hadamard

$$|\psi_5\rangle = \frac{1}{\sqrt{2^{n+1}}} \sum |(-1)^{x \cdot z} + (-1)^{y \cdot z}| z\rangle$$

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

6.

$$x \cdot y = y \cdot z$$

$$x \cdot z = (x \oplus b) \cdot z$$

$$x \cdot z = x \cdot z \oplus b \cdot z$$

Simon Algorithm

We are given an unknown blackbox function f which is guaranteed either one to one (1:1) or two to one (2:1)

One to one → map exactly one unique output for every input

$f(1) \to 1$, $f(2) \to 2$, $f(3) \to 3$, $f(4) \to 4$

two to one → map exactly two input to every unique output

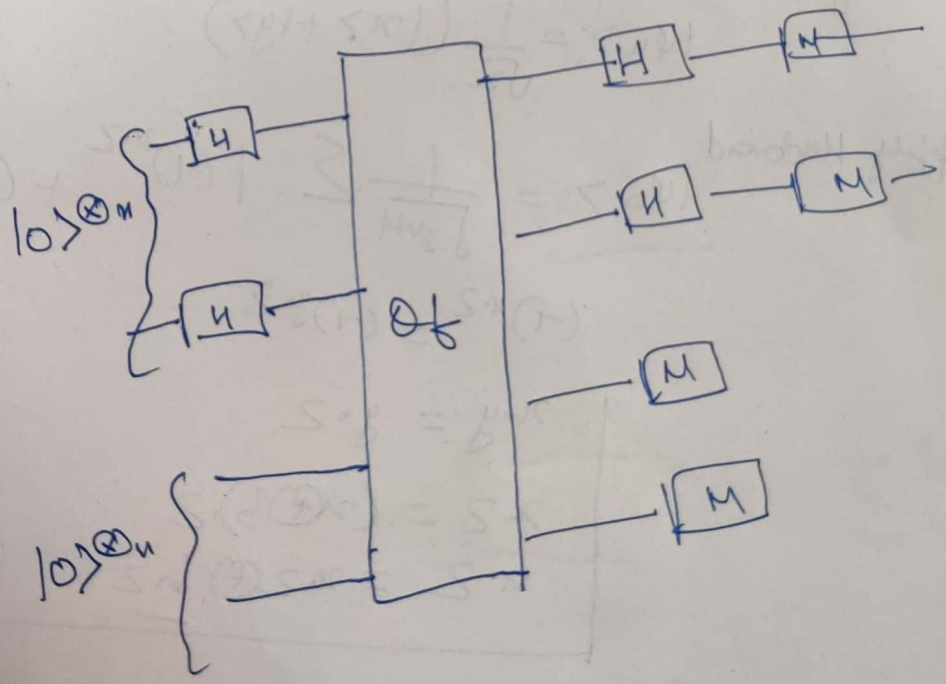
$f(1) \to 1$, $f(2) \to 2$, $f(3) \to 1$, $f(4) \to 2$

This two-to-one mapping is ac to hidden string b

given x_1, x_2: $f(x_1) = f(x_2)$

it is guaranteed $x_1 \oplus x_2 = b$

for one to one Mapping $b = 000\ldots$ represent one to one f



Scanned with CamScanner

~~$|x\rangle \xrightarrow{f_a} (-1)^{g \cdot x}$~~

$|x\rangle \xrightarrow{f_a} (-1)^{a \cdot x} |x\rangle$

$|00\cdots0\rangle \xrightarrow{H_n} \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle \xrightarrow{f_a} \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} (-1)^{a \cdot x} |x\rangle$

We can obtain a by

$$\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} (-1)^{a \cdot x} |x\rangle \xrightarrow{H_n} |a\rangle$$

Hence we get the value of a in just one oracle query

→ The Algorithm reveal the hidden bit naturally by quering the quantum oracle fs with the quantum superposition obtained from the Hadamard trasformation $|00\cdots0\rangle$

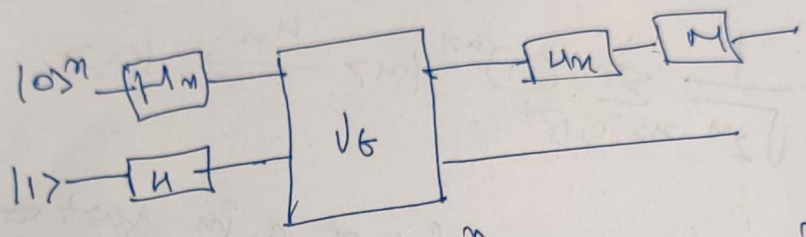
BERNSTEIN – VAZIRANI ALGORITHM

It is the extension of Deutsch Jozsa Algorithm

$f: \{0,1\}^n \to \{0,1\}$ → function MAP n bits to 1 bits

$f(x) = a \cdot x$

We have to use only one oracle query



$$|0\rangle^n |1\rangle \xrightarrow{H^{n+1}} \frac{1}{2^{\frac{n+1}{2}}} \sum_{x=0}^{2^n-1} |x\rangle (|0\rangle - |1\rangle) \xrightarrow{U_f}$$

$$\xrightarrow{U_f} \frac{1}{2^{\frac{n+1}{2}}} \sum_{x=0}^{2^n-1} (-1)^{f x} |x\rangle (|0\rangle - |1\rangle)$$

$$\to \frac{1}{2^{\frac{n}{2}}} \sum_{x=0}^{2^n-1} (-1)^{f(x)} |x\rangle$$

Here $f(x) = a x$

So after H^n — M → we will get as a result of Measurement, the value of a is just one oracle query

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

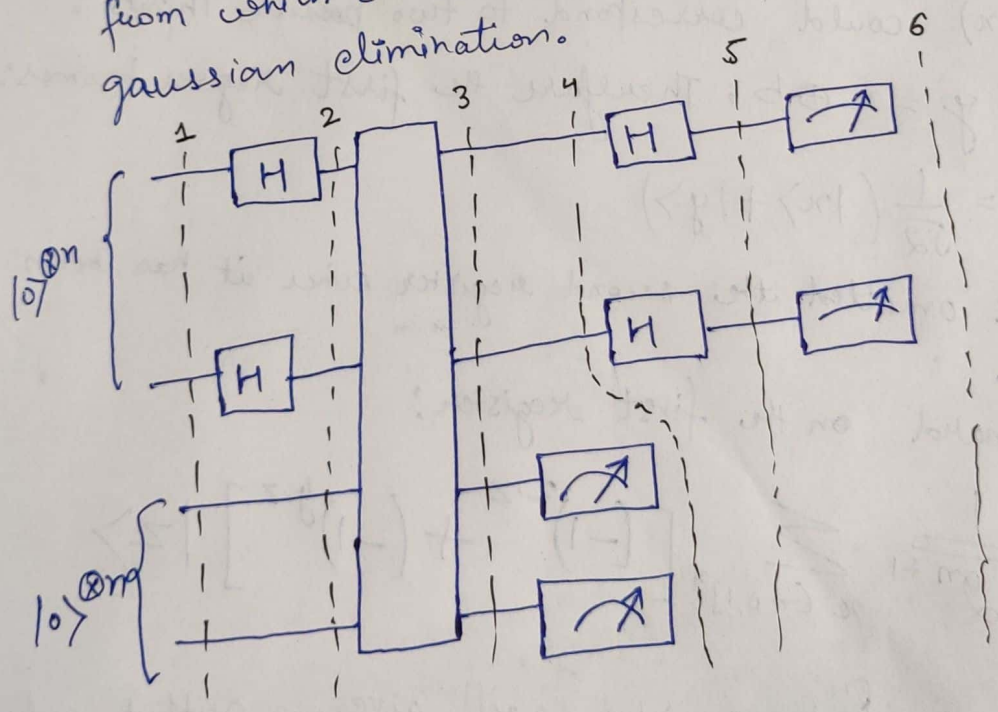
which means

$$x\cdot z = y\cdot z$$
$$x\cdot z = (x \oplus b)\cdot z$$
$$x\cdot z = x\cdot z \oplus b\cdot z$$
$$b\cdot z = 0 \pmod 2$$

A string z will be measured, whose inner product with $b=0$. Thus, repeating the algorithm $\approx n$ times, we will be able to obtain n different values of z and the following system of equation can be written:

$$\left.\begin{aligned} b\cdot z_1 &= 0 \\ b\cdot z_2 &= 0 \\ &\vdots \\ b\cdot z_n &= 0 \end{aligned}\right\}$$

from which b can be determined, for example by gaussian elimination.



Bunce
10191605 6

SIMON'S ALGORITHM :-

The algorithm involves the following steps :-

i) Two n-qubit registers are initialized to the zero state :

$$|\psi_1\rangle = |0\rangle^{\otimes n} |0\rangle^{\otimes n}$$

ii) Apply Hadamard transform to the first register :

$$|\psi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle |0\rangle^{\otimes n}$$

iii) Apply the query function O_f :-

$$|\psi_3\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle |f(x)\rangle$$

iv) Measure the second register. A certain value of $f(x)$ will be observed. Because of the setting of the problem, the observed value $f(x)$ could correspond to two possible inputs : x and $y = x \oplus b$. Therefore the first register becomes :

$$|\psi_4\rangle = \frac{1}{\sqrt{2}} (|x\rangle + |y\rangle)$$

where we omitted the second register since it has been measured.

v) Apply Hadamard on the first register :

$$|\psi_5\rangle = \frac{1}{\sqrt{2^{n+1}}} \sum_{x \in \{0,1\}^n} \left[(-1)^{x \cdot z} + (-1)^{y \cdot z} \right] |z\rangle$$

vi) Measuring the first register will give an output only if :

* $f(x)$ = balanced

$$\rightarrow \frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} (-1)^{f(x)} |x\rangle$$

$$= \frac{1}{2^{n/2}} \left[\underbrace{\sum_{x:f(x)=0} |x\rangle}_{2^{n-1}\,|100\cdots0\rangle} - \underbrace{\sum_{x:f(x)=1} |x\rangle}_{-2^{n-1}\,|000\cdots1\rangle} \right]$$

$\Rightarrow$ Same terms will self destruct

$\Rightarrow$ But different will add up to give ans

So general formula

$$H|x\rangle = \frac{1}{2^{n/2}} \sum_{y=0}^{2^n-1} (-1)^{x \cdot y} |y\rangle$$

$\longrightarrow$ So we have to run only one application to find const & balanced

So after measurement

(i) If we obtain all zeroes $\equiv |0\rangle^n \Rightarrow$ Const f^n

(ii) If any $|0\rangle^n$ output $\Rightarrow$ balanced

③ Applying Hadamard on n qubits and then measuring

$$\frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} (-1)^{f(x)} |x\rangle$$

⇒ Not focusing on $|-\rangle$ as that was just for help

Now there are 2 cases ↓

* $f(x)$ = constant

$$\Rightarrow \frac{1}{2^{\frac{n}{2}}} \sum_{x=0}^{2^n-1} (-1)^{f(x)} |x\rangle$$

$$= \boxed{\frac{(-1)^{f(x)}}{2^{n/2}} \sum_{x=0}^{2^n-1} |x\rangle}$$

$f(x) = 0 \Rightarrow (-1)^0 = 1$
OR
$f(x) = 1 \Rightarrow (-1)^1 = -1$

} This const is just for phase so we will focus on terms

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

---

③ Applying Hadamard on n qubits & then measuring

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

$$= \underbrace{|00\ldots0\rangle}_{n \text{ zeroes}}$$

Deutsh - Jozsa Problem

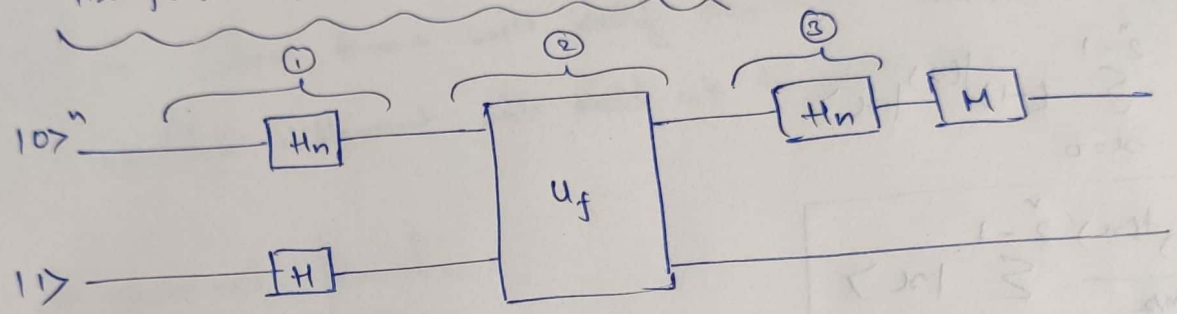
$f: \{0,1\}^n \longrightarrow \{0,1\}$ ⇒ Maps n bits to one bit

There are 2 types of f's ↓

(i) const f^n

(ii) balanced f^n → return equal amt of 0's & 1's

$|x : f(x) = 1| = |x : f(x) = 0|$



① Applying n-qubit Hadamard transform

$$|0\rangle^n |1\rangle \xrightarrow{H_{n+1}} \frac{1}{2^{\frac{n+1}{2}}} \sum_{x=0}^{2^n-1} |x\rangle (|0\rangle - |1\rangle)$$

② Applying quantum oracle $\xrightarrow{U_f}$

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

We have to focus on this

This is just for helping purpose

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

$$\frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} (-1)^{g(x)} |x\rangle$$

$$\frac{1}{2^{n/2}} \left(\sum_{x:f(x)=0} |x\rangle - \sum_{x=g(x)=1} |x\rangle \right)$$

$$= \frac{1}{2^{n/2}} \left(\sum_{x.f(x)=0} |x\rangle - \sum_{x.f(x)=1} |x\rangle \right)$$

vector $|y\rangle$ to all zeroes $|y\rangle = |0 \ldots 0\rangle$

we have equal amounts of $\frac{1}{2^{n/2}} \left(\sum_{x.f(x)=0} |x\rangle - \sum_{x.f(x)=1} |x\rangle \right)$ and $f(x)$ is balanced

$$\frac{1}{2^{n/2}} \left(\sum_{x.f(x)=0} |x\rangle - \sum_{x.f(x)=1} |x\rangle \right)$$

$(2^{n-1} |000 \ldots 0\rangle)$ $(2^{n-1} |000 \ldots 0\rangle)$

these vectors will self Destruct(+ −)

Now we will measure

± If we obtain all zeros $|0\rangle^n$ then $f(x)$ is constant

2 If result is other than vector except $|0\rangle^n$ then $f(x)$ is balanced

→ Here we can distinguish b/w balanced & constant function

balanced → NO $|0\rangle^n 0/p$, constant → only $|0\rangle^n 0/p$

→ The self Destruction is related to interference