BERNSTEIN - VAZIRANI :

Input : $f : \{0,1\}^n \to \{0,1\}$

Assumption : $f(x)$ = linear function

$= (a \cdot x) \oplus b \longrightarrow$ bit

$\uparrow$ dot product

$\hookrightarrow$ XOR

$a, x \to$ bit vectors of length n.

Output : a, b

CLASSICAL :

$$f(00\ldots0) = (a \cdot (00\ldots0)) \oplus b = 0 \oplus b = b$$

$$a = a_1 \ldots a_n$$

Get a_i : $f(00\ldots0100\ldots0) = (0\cdot0 \oplus \cdots \oplus a_i \cdot 1 \oplus \cdots 0\cdot0) \oplus b$

$\uparrow$ position i

$$= a_i \oplus b$$

$(n+1)$ calls of f //

QUANTUM:

$$f(x) = (a \cdot x) \oplus b$$

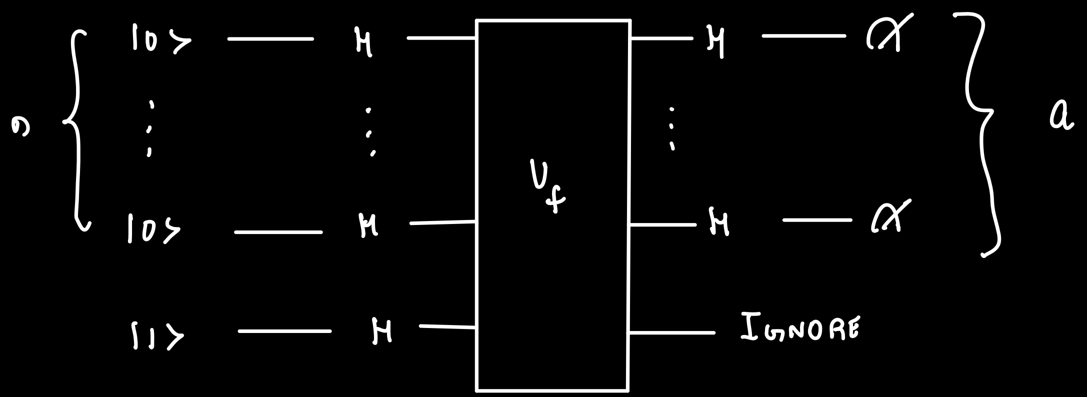
$n = 1$

a	b	f(0)	f(1)	
0	0	0	0	CONSTANT FUNCTION
0	1	1	1	
1	0	0	1	BALANCED FUNCTION
1	1	1	0	

$n = 2$

a	b	f(00)	f(01)	f(10)	f(11)	
0 0	0	0	0	0	0	CONSTANT
0 0	1	1	1	1	1	
0 1	0	0	1	0	1	
0 1	1	1	0	1	0	BALANCED
1 0	0	0	0	1	1	
1 0	1	1	1	0	0	
1 1	0	0	1	1	0	
1 1	1	1	0	0	1	

DEUTSCH-JOZSA CIRCUIT:



So find b classically and get a using the quantum model.

The final state of the circuit, before measurement :

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

Here $f(x) = (a \cdot x) \oplus b$

$$= \frac{1}{2^n} \cdot \sum_{x \in \{0,1\}^n} \sum_{y \in \{0,1\}^n} (-1)^{\underbrace{(x \cdot y) \oplus ((a \cdot x)}_{} \oplus b)} |y\rangle$$

$$\downarrow$$

$$((a \oplus y) \cdot x) \oplus b$$

$$\left[(-1)^x \cdot (-1)^y = (-1)^{x \oplus y} \right]$$

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

What is the amplitude of $|a\rangle$

↳ Tells what is the chanie to get a as output. If 100%, we have solved it.

$$y = a$$

$$\frac{1}{2^n} (-1)^b \sum_{x \in \{0,1\}^n} (-1)^{(a \oplus a) \cdot x}$$

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

$$= \frac{1}{2^n} (-1)^b \, 2^n$$

$$= (-1)^b$$

$$\text{PROBABILITY}(a) = |(-1)^b|^2 = 1^2 = 1 \,//$$

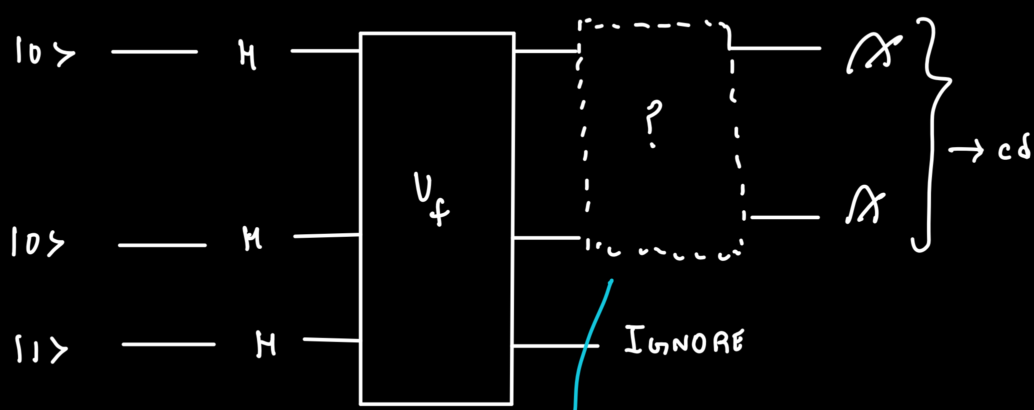
Special Case of Grover's Algorithm:

Input: function $f: \{0,1\}^2 \to \{0,1\}$

Assume: $f(cd) = 1$, for exactly one case of cd.

Output: cd

f is 1 for one input combination and 0 for the rest.



$$U = \frac{1}{2}\begin{bmatrix} -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \end{bmatrix}$$

$$\phi_{00} = \frac{1}{2}\left(-|00\rangle + |01\rangle + |10\rangle + |11\rangle\right)$$

$$\phi_{01} = \frac{1}{2}\left(|00\rangle - |01\rangle + |10\rangle + |11\rangle\right)$$

$$\phi_{10} = \frac{1}{2}\left(|00\rangle + |01\rangle - |10\rangle + |11\rangle\right)$$

$$\phi_{11} = \frac{1}{2}\left(|00\rangle + |01\rangle + |10\rangle - |11\rangle\right)$$

LEMMA :

$$U\phi_{00} = \frac{1}{2}\begin{bmatrix} -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \end{bmatrix} \frac{1}{2}\begin{bmatrix} -1 \\ 1 \\ 1 \\ 1 \end{bmatrix}$$

$$= \frac{1}{4}\begin{bmatrix} 4 \\ 0 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} = |00\rangle$$

$$U\phi_{cd} = |cd\rangle$$

$$U\phi_{cd} = |cd\rangle$$

$$(U \otimes I) \cdot U_f \cdot H^{\otimes 3} |001\rangle$$

$$= (U \otimes I) \cdot U_f |{+}{+}{-}\rangle \qquad |+\rangle = 1/\sqrt{2} \, (|0\rangle + |1\rangle)$$

$$= (U \otimes I) \cdot U_f \left(1/_2 \left(|00\rangle + |01\rangle + |10\rangle + |11\rangle \right) \right) |-\rangle$$

FACE KICKBACK LEMMA

$$\forall x \in \{0,1\}^n : \quad U_f |x\rangle |-\rangle = (-1)^{f(x)} \quad |x\rangle |-\rangle$$

$$= (U \otimes I) \cdot \frac{1}{2} \Big((-1)^{f(00)} |00\rangle + (-1)^{f(01)} \cdot |01\rangle +$$

$$(-1)^{f(10)} |10\rangle + (-1)^{f(11)} \cdot |11\rangle \Big) |-\rangle$$

We know one of the $f(x_{ij})$ is 1 and all others are 0.

$$= U \phi_{cd} |-\rangle$$

where $f(cd) = 1$

$$= |cd\rangle |-\rangle$$

Gets $|cd\rangle$ with $P = 1$ //

"Search in an unstructured Database".