Deutsch & DJ algorithm problem:
→ determine whether a binary function is balanced or constant

Bernstein-Vazirani algorithm

→ Given a function $f: \{0,1\}^n \to \{0,1\}$, which $f(x) = x \cdot s \to$ hidden string
↳ inner product mod of 2

$$f(x) = x \cdot s = \sum_{i=1}^{n} x_i s_i \mod 2$$

$$= x_1 s_1 \oplus x_2 s_2 \oplus \cdots \oplus x_n s_n$$

$x = 1000$ $\quad$ $S = 1101$

$$x \cdot s = [1.1 + 0.1 + 0.0 + 1.0] \pmod 2$$
$$= [1 + 0 + 0 + 0] \mod 2$$
$$= 1 \mod 2 = 1$$

So, the problem truly is finding the "s" hidden string only looking at the oracle results

→ Classical Solution

$x = x_1\ x_2\ x_3$
$s = s_1\ s_2\ s_3$

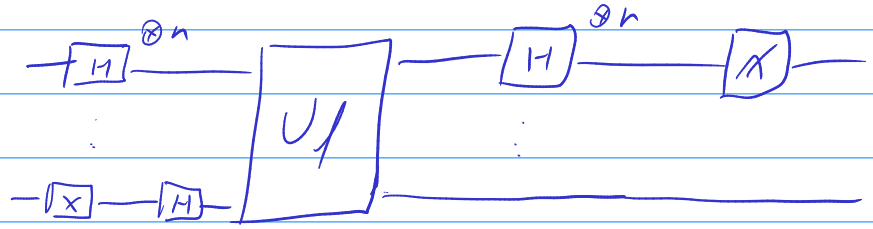
x_1	x_2	x_3	$f(x)$
1	0	0	s_1
0	1	0	s_2
0	0	1	s_3

← that happen because

$x_1 s_1 \oplus x_2 s_2 \oplus x_3 s_3$
$1 \cdot s_1 \oplus 0 s_2 \oplus 0 s_3$
$0 \cdot s_1 \oplus 1 \cdot s_2 \oplus 0 \cdot s_3$
$0 s_1 \oplus 0 s_2 \oplus 1 \cdot s_3$

so it requires $O(n)$ with n = n° of bit

→ Quantum solution



(same as DJ, but the oracle U_f may change accordingly with the problem

$U_f = |x\rangle|y\rangle \to |x\rangle|y \oplus (x \cdot s)\rangle$
← $f(x)$

$H^{\otimes n}|a\rangle = |b\rangle \iff H^{\otimes n}|b\rangle = |a\rangle$

(after applying the last $H^{\otimes n}$ the $|s\rangle$ appears

as DJ the BV is $O(1)$

Simon's algorithm

→ Given $f : \{0,1\}^n \to \{0,1\}^n$ such that $f(x) = f(x \oplus s)$ $\quad s \in \{0,1\}^n$

→ The goal is to find s with as few queries as possible

→ This is different from BV, once the definition of f is x XOR s on the output has size n

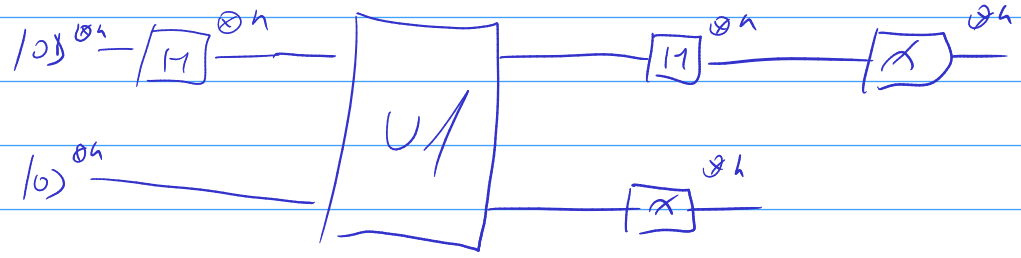
x	$f(x)$	$s = 10$
00	$00 \oplus 10 = 10$	
01	$01 \oplus 10 = 11$	
10	$10 \oplus 10 = 00$	
11	$11 \oplus 10 = 01$	

$f(00) = f(10)$ $\quad f(01) = f(11)$

a period in the function

classically → $O(2^{n/2})$ → also known as the birthday paradox (how many people has the same birthday)

→ Quantum

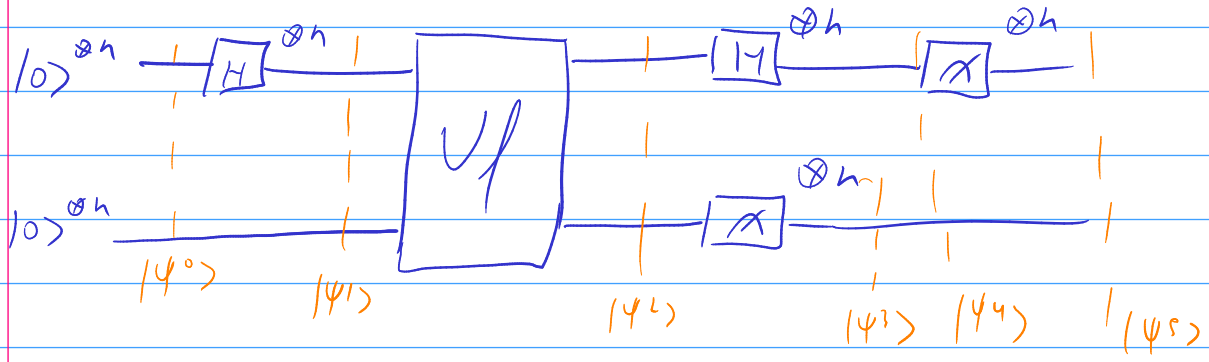


$$U_f : |x\rangle|y\rangle \to |x\rangle|f(x) \oplus y\rangle$$

must follow
$f(x) = f(x \oplus s)$

Steps:
1: Apply $H^{\otimes n}$ to the first register
2: Apply U_f
3: Measure the second register
4: Apply $H^{\otimes n}$ to the first register
5: Measure the first register and save the result
6: Repeat the above till you get $n-1$ or n distinct result values
7: construct linear equations using these values and solve for s

Note: is required $n-1$ steps, because only $n-1$ states will be orthogonal to s, but you can also use n steps for more certainty



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

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

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

$|\psi^3\rangle$ = randomly one of the output is observed, so that we can have 2 cases

Case 1: two-to-one function $\rightsquigarrow s \neq 0^n$
2 inputs that produce the same output

Case 2: one-to-one function $s = 0^n$
each input has only one output

in the case I we have a superposition of 2 values $(|z\rangle, |z \oplus s\rangle)$ that produce $f(z)$ in the second register

$$|\psi^3\rangle = \frac{1}{\sqrt{2}} \overbrace{(|z\rangle + |z \oplus s\rangle)}^{\text{first register}} \overbrace{|f(z)\rangle}^{\text{second register}}$$

$$|\psi_y\rangle = \frac{1}{\sqrt{2^{n+1}}} \left[(-1)^{2 \cdot y} + (-1)^{(2 \oplus s) \cdot y} \right] |y\rangle$$

$\sqrt{2^{n+1}}$: one we have of superposition

$|y\rangle$: for each result

$$|\psi_s\rangle = (-1)^{2 \cdot y} + (-1)^{(2 \oplus s) \cdot y} = 0$$

one the two terms are different

if it occurs so the prob. of seeing y is 0

if $(-1)^{2 \cdot y} = (-1)^{(2 \oplus s) \cdot y}$ so the prob of seeing y is nonzero

$$(-1)^{2 \cdot y} = (-1)^{(2 \oplus s) \cdot y}$$

$$2 \cdot y = (2 \oplus s) \cdot y$$

$$(a \oplus b) \cdot c = (a \cdot c) \oplus (b \cdot c)$$

$$2 \cdot y = (2 \cdot y) \oplus (s \cdot y)$$

$(s \cdot y) = 0$ to be equal

$$(-1)^{2 \cdot y} + (-1)^{(2 \oplus s) \cdot y} = |+1| = 2 \in \text{amplitude of } y$$

$$\left(\frac{2}{\sqrt{2^{n+1}}} \right)^2 = \frac{2^2}{2^{n+1}} \to \frac{1}{2^{n+1-2}} \to \frac{1}{2^{n-1}}$$

every bit string with $s \cdot y = 0$ will be observed with prob

$s \cdot y = 1$ won't be observed

In the second case ($s = 0^n$)

$$|\psi_3\rangle = |z\rangle |f(z)\rangle$$
$$|\psi_4\rangle = \frac{1}{(\sqrt{2^n})} \sum_y (-1)^{z \cdot y} |y\rangle$$

$$\begin{array}{r} 0\ 0\ 0 \\ \oplus\ a\ b\ c \\ \hline c\ b\ c \end{array}$$

$0 \oplus 0 = 1 \oplus 1 = 0$
$0 \oplus 1 = 1 \oplus 0 = 1$
result is the same as the input

any observed bit string for the same probability $\rightarrow \left(\frac{1}{\sqrt{2^n}}\right)^2 \rightarrow \frac{1}{2^n}$

(not the best case, as we did nothing)

→ Post Processing
→ After all the quantum part, we'll have many results y, then we need to check $s \cdot y = 0$ for each y

example: $s \cdot y_1 = 0 \rightarrow s_1 \cdot y_{11} + s_2 \cdot y_{12} + \dots + s_n \cdot y_{1n}$

Eq