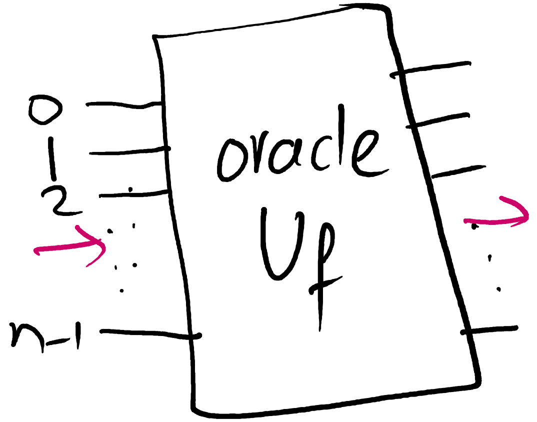
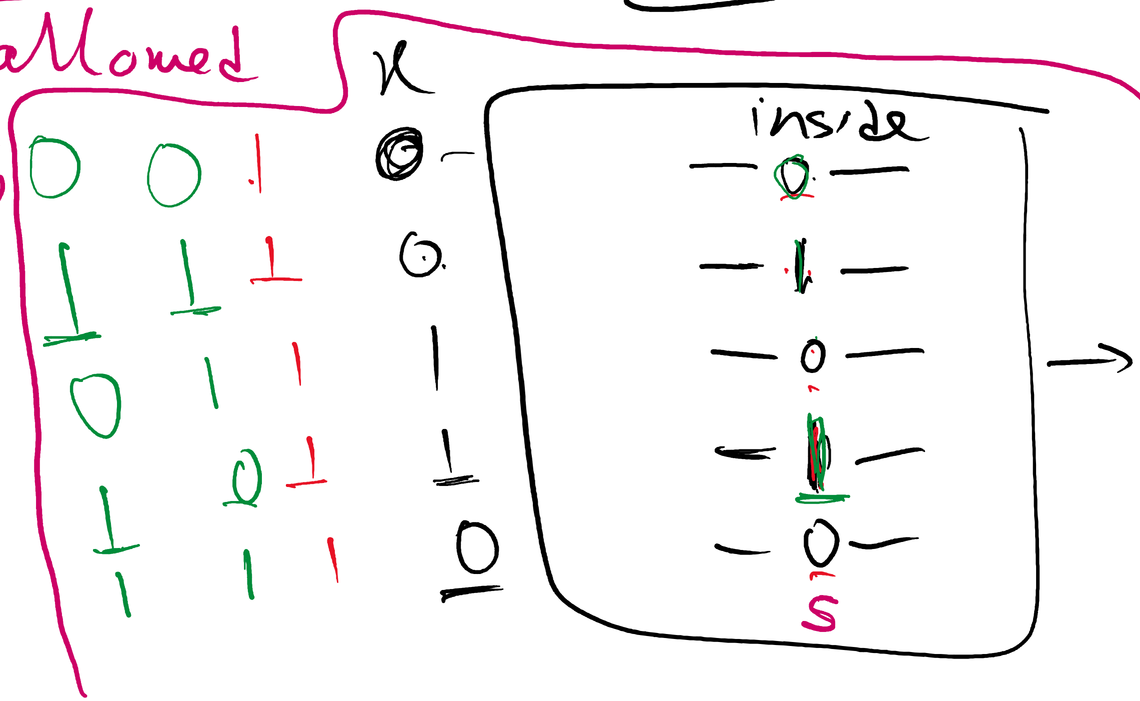
Bernstein–Vazirani Problem and Quantum Algorithm:

Problem Definition:

- There is a secret code
- Find secret code
- only allowed inputs/outputs





What oracle does:

- multiplies the input x with minus sign as many times as bit is 1 in some secret locations

x $\quad$ x'

01100 → −01100

11111

10110 → −10110

11010 → +11010

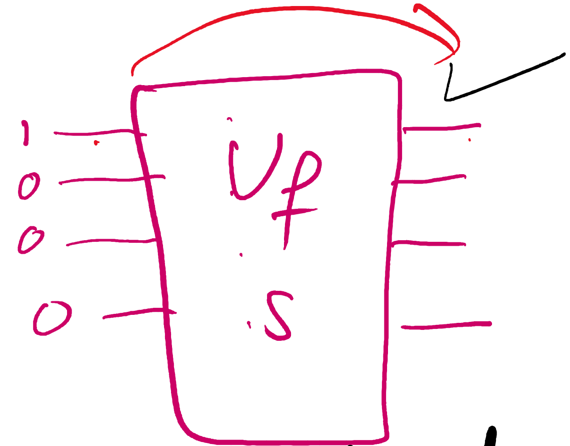
Classical Solution:

- How many times we need to ask oracle = 4

inputs	outputs
0 0 0 1	0 0 0 1
0 0 1 0	0 0 1 0
0 1 0 0	0 1 0 0
1 0 0 0	1 0 0 0

- if 10 bits number of queries = 10
- if n bits ⇒ $\boxed{\text{queries} = n}$

Complexity = n



For n bit oracle, we need n queries

if +ve S

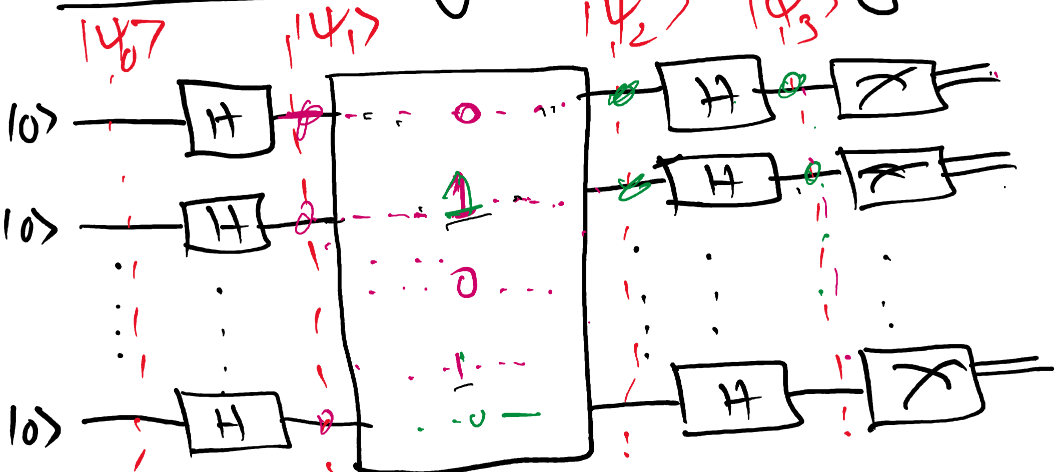
+ve

0	0	1	0

+ve

if -ve

Quantum Algorithm: by BV :



Analysis/Proof of this Algorithm:

(0) $|\psi_0\rangle = |0\rangle\otimes|0\rangle\otimes|0\rangle \cdots \otimes|0\rangle = |0\rangle^{\otimes n}$

$= |0\rangle|0\rangle|0\rangle \cdots |0\rangle = |0\rangle$

$= |0000\cdots 0\rangle$

(1) $|\psi_1\rangle = H|0\rangle\otimes H|0\rangle\otimes \cdots \otimes H|0\rangle$

$|\psi_1\rangle = |+\rangle|+\rangle|+\rangle \cdots |+\rangle$

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

(2) $|\psi_2\rangle = |+\rangle|-\rangle|+\rangle \cdots |-\rangle|+\rangle$

(3) $H|+\rangle = |0\rangle, \ H|-\rangle = |1\rangle$

$|\psi_3\rangle = |0\rangle|1\rangle|0\rangle \cdots |1\rangle|0\rangle$

(4) Measure

$= \boxed{010\cdots010}$

Only 1 query needed!

Q.C. Solved problem 1 query

$\boxed{\text{complexity} = 1}$