QUANTUM COMPUTING

MGS 2025 – Sheffield

Venanzio Capretta

LECTURE 4:

- Phase kickback
- The Bernstein – Vazirani Algorithm

PHASE KICKBACK

You may think that the CNOT gate only changes the target qubit, leaving the control qubit in its original state:

CNOT: 

$|00\rangle \mapsto |00\rangle$ $\quad |10\rangle \mapsto |11\rangle$

$|01\rangle \mapsto |01\rangle$ $\quad |11\rangle \mapsto |10\rangle$

But if the target qubit is in a superposition with phase, the phase is "kicked back" to the control qubit:

$|0+\rangle \mapsto |0+\rangle$ $\quad |1+\rangle \mapsto |1+\rangle$

$|0-\rangle \mapsto |0-\rangle$ $\quad |1-\rangle \mapsto -|1-\rangle$

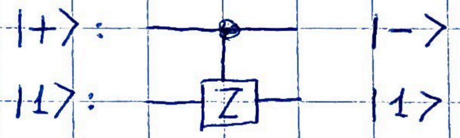
$$\left.\begin{array}{ll} |++\rangle \mapsto |++\rangle & |-+\rangle \mapsto |-+\rangle \\ |+-\rangle \mapsto |--\rangle & |--\rangle \mapsto |+-\rangle \end{array}\right\}$$

CNOT acts on the Hadamard basis $\{|+\rangle, |-\rangle\}$ like a reversed CNOT

Phase Kickback in General

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

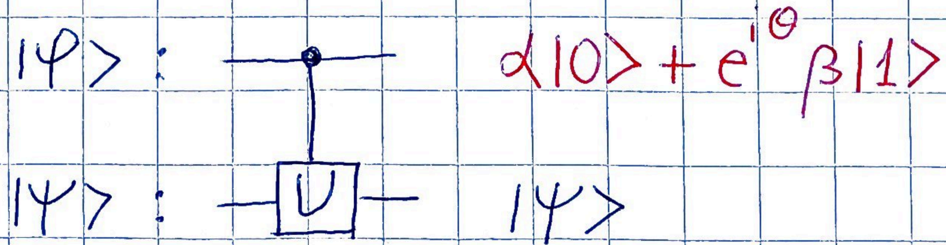
Other example of Phase kickback : C-Z



In general, for any unitary operation U, if we apply C-U to a control qubit $|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle$ and a target qubit $|\psi\rangle$ that is an eigenvector of U:

$$U|\psi\rangle = e^{i\theta}|\psi\rangle$$

Then



THE BERNSTEIN - VAZIRANI ALGORITHM

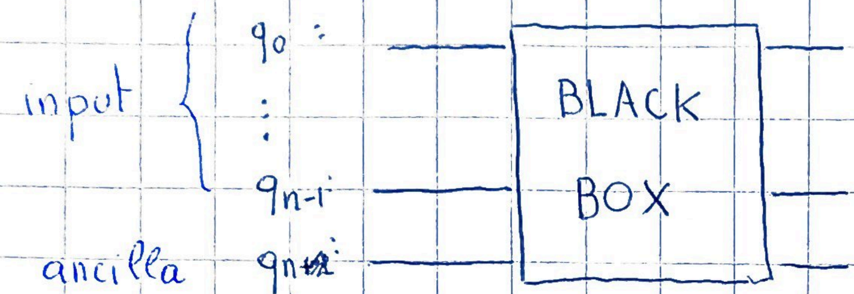
Problem: We are given a <u>black box</u> based on a secret binary code.

We must guess the secret code with the least possible calls to the black box.

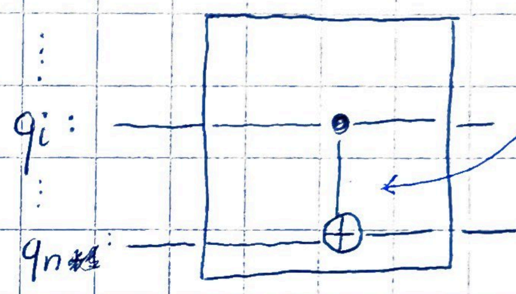
If the secret code has n bits, the black box operate on $n+1$ qubits.

The first n qubits are input qubits, the last is the result (ancilla)

The box perform a CNOT between qubit i and the result if the i^{th} bit of the secret code is 1.

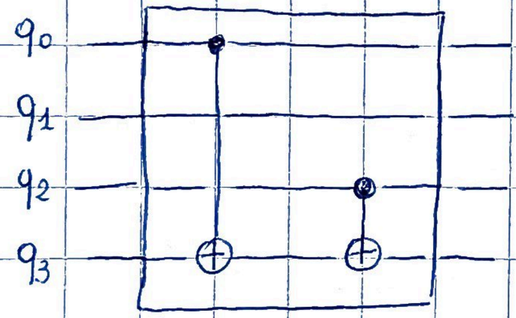


inside the black box:

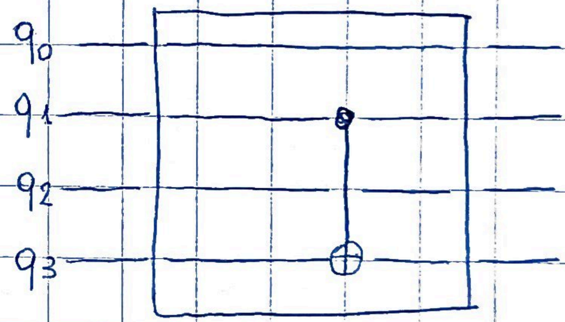


if the i^{th} bit of the secret code is 1

Examples $(n=3)$:



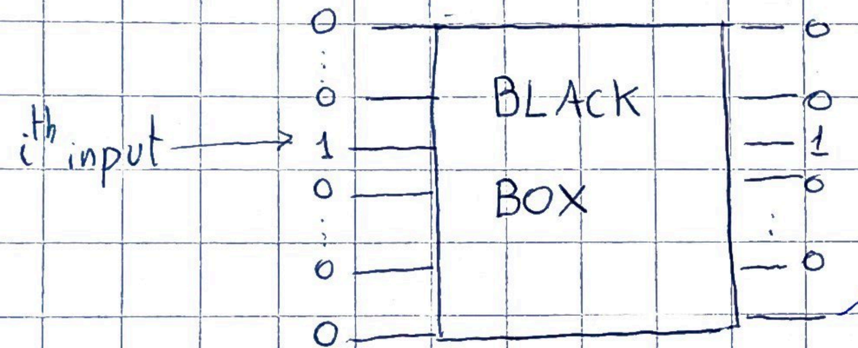
code 101



code 101

Classically, if we run the black box with input n classical bits, the result bit will apply k NOT operations, where k is the number of bits that have 1 both in the secret code and the input

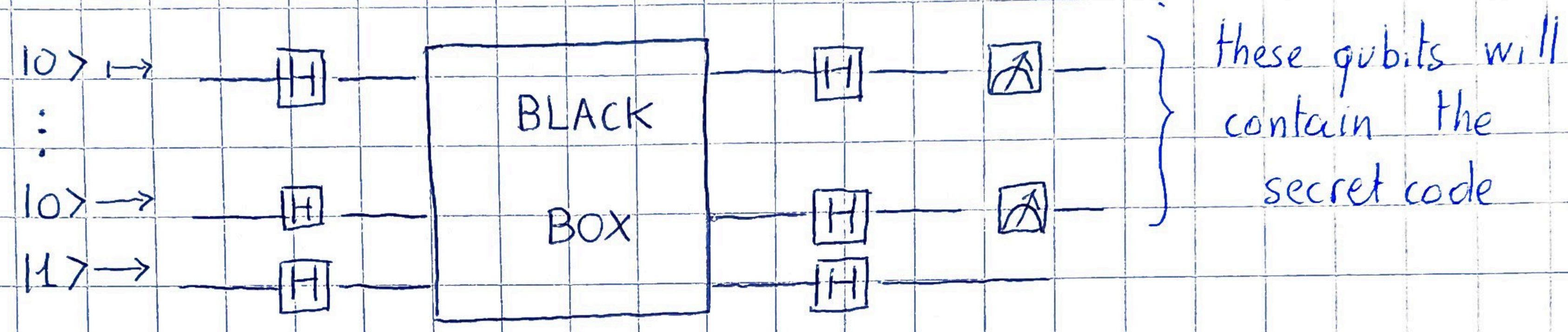
Classical solution: The best we can do is to run the black box n times with inputs $10\cdots0, 010\cdots0, \cdots, 0\cdots01$:



$= i^{th}$ bit of the secret code $= \begin{cases} 1 & \text{if the } i^{th} \text{ bit of the secret code is } 1 \\ 0 & \text{otherwise} \end{cases}$

Since the black box gives us 1 bit of information as result an the secret code consists of n bits we can't do better than this.

QUANTUM SOLUTION (BV Algorithm)



We need to run it just once:

(1) Prepare the input qubit in state $|0\rangle$, the ancilla in state $|1\rangle$

(2) Apply the Hadamard gate to each qubit

(3) Run the black box

(4) Apply the Hadamard gate to each qubit

(5) Measure the input qubits

Here is what happened:

(1) The state is $|0^n 1\rangle$

(2) The state becomes $|+^n -\rangle$

(3) If the i^{th} bit of the secrete code is 1, a CNOT gate is applied between qubits q_i (control) and q_n (target)

Phase kickback: q_i is in state $|+\rangle$, q_n in state $|-\rangle$

after CNOT: q_i is $|-\rangle$, q_n unchanged

(4) The Hadamard gates turn $|+\rangle$ into $|0\rangle$ and $|-\rangle$ into $|1\rangle$

The final state is: $|\underbrace{c_0 \cdots c_{n-1}}_{\text{secret code}} 1\rangle$