Quantum Computing

From Zero to Classification

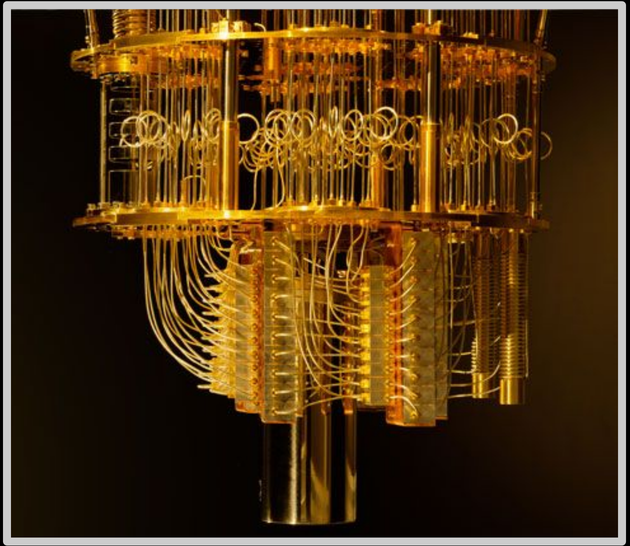
Alessandro Berti

Università di Pisa

TARGET(S)

Show my research topic but..

I do believe that collaboration is THE thing



So, my objective is to trigger in you ideas!

UNIVERSITÀ DI PISA

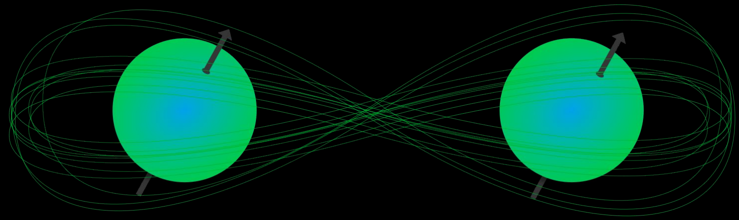
What is Quantum Computing?

Quantum computing is the use of **quantum phenomena** to perform computation

Two Quantum Phenomena

SUPERPOSITION

ENTANGLEMENT



SUPERPOSITION

Classical Bit

0

1

Quantum Bit

0 1

a.k.a "qubit"

SUPERPOSITION

Given 2 bit/qubit:

	Bit	Qubit
N° combinations	4 { 00, 01, 10, 11	4 { 00, 01, 10, 11
N° value you can manipulate in a given moment	1 00 or 01 or 10 or 11	4 00 and 01 and 10 and 11

"In general, given x qubit, you have 2^x values"

20 qubit → 1 Mb

50 qubit → 1 Pb

So?

It’s a kind of SUPER - PARALLELISM!

Classical Input

You can’t observe what is happening Step-by-step.

There is no “if” or “for” instruction

Classical Output

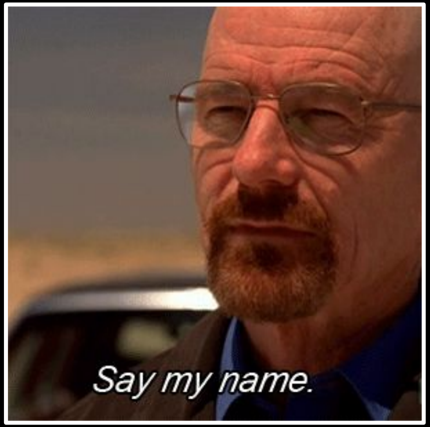
Qubit Encoding + Quantum Computation

WHY?

We said that Quantum Computing deals with quantum phenomena, right?

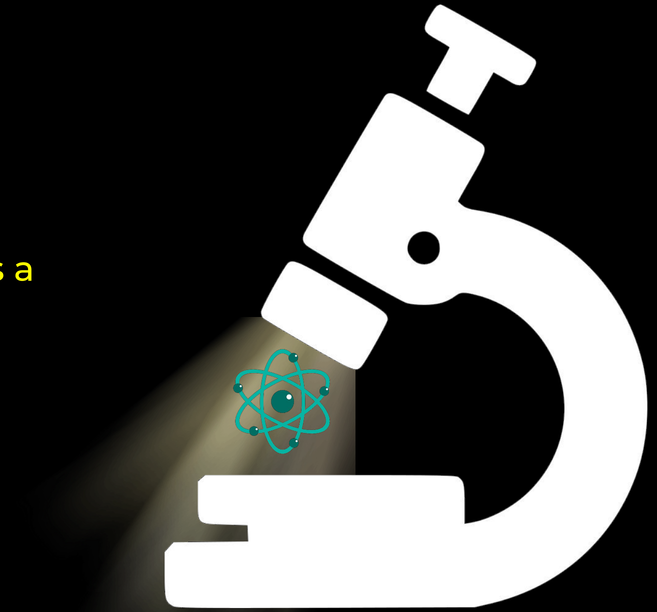
BUT, quantum phenomena show themselves only at a "particle level" and <u>particles are very fragile!</u>

<u>Heisenberg's Uncertainty Principle</u>



"Observing" implies using light. Light produces heat, thus there is a transfer of energy!

Since the particle is very fragile, this energy "corrupts" its original state!



Measurements

That does not means that you cannot observe anything!

But simply that if you want to exploit quantum phenomena…
…you can’t do observations during computations.

You CAN measure only at the end of your quantum algorithm

The “measurement” collapses quantum data into classical one!

ALERT: MATHS COMING
Linear Algebra + Probability

Superposing a qubit

A qubit is represented by a 2x1 vector $\begin{pmatrix} a \\ b \end{pmatrix}$

a,b are said “amplitudes”

Condition

$$|a^2| + |b^2| = 1$$

So, which are the “a,b” such that the qubit represent the 0 value?

$$\begin{array}{cc} \begin{pmatrix} 1 \\ 0 \end{pmatrix} & \begin{array}{c} 0 \\ 1 \end{array} \end{array} \xrightarrow{\text{Shorthand notation (Ket notation)}} |0\rangle$$

$$\begin{array}{cc} \begin{pmatrix} 0 \\ 1 \end{pmatrix} & \begin{array}{c} 0 \\ 1 \end{array} \end{array} \xrightarrow{\text{Shorthand notation (Ket notation)}} |1\rangle$$

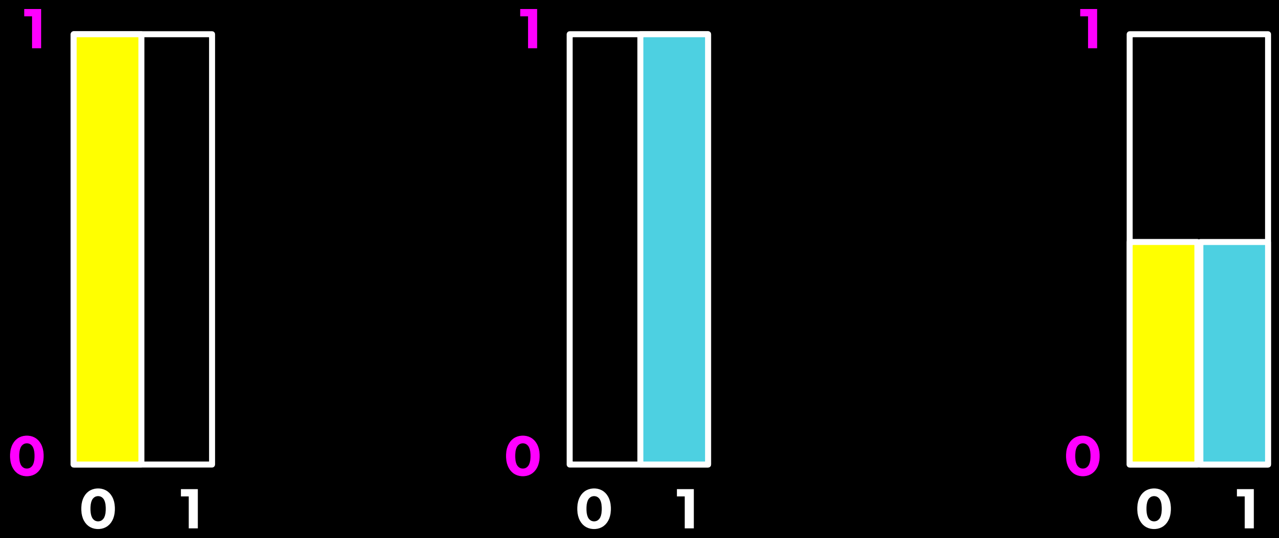
This is equivalent to say: “When the qubit will be measured, the probability to observe the 0-value is 1”

An important detail:
a is an amplitude while $|a^2|$ represents the probability.
“Do the square” is like “apply a measurement (observe).”

$$\begin{array}{cc} \begin{pmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{pmatrix} & \begin{array}{c} 0 \\ 1 \end{array} \end{array} \Longrightarrow 1/\sqrt{2}\ |0\rangle + 1/\sqrt{2}\ |1\rangle$$

Qubit Superposition in math

Superposing a qubit



$$\begin{pmatrix}1\\0\end{pmatrix} \qquad \begin{pmatrix}0\\1\end{pmatrix} \qquad \begin{pmatrix}1/\sqrt{2}\\1/\sqrt{2}\end{pmatrix}$$

$$|0\rangle \qquad |1\rangle \qquad 1/\sqrt{2}\,|0\rangle + 1/\sqrt{2}\,|1\rangle$$

Università di Pisa

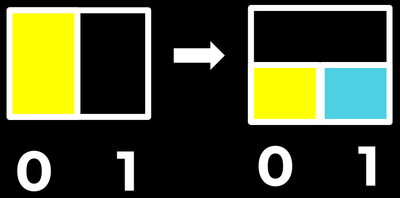
How to superpose

It's super simple: **H|0⟩**

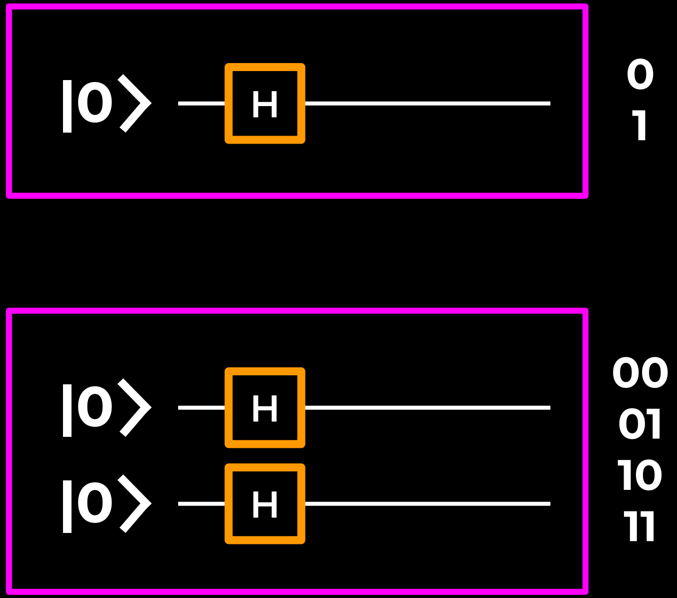
H is said "gate"

H is an unitary matrix

$$\overset{H}{\begin{pmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & -1/\sqrt{2} \end{pmatrix}} \overset{|0\rangle}{\begin{pmatrix} 1 \\ 0 \end{pmatrix}} = \begin{pmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{pmatrix}$$



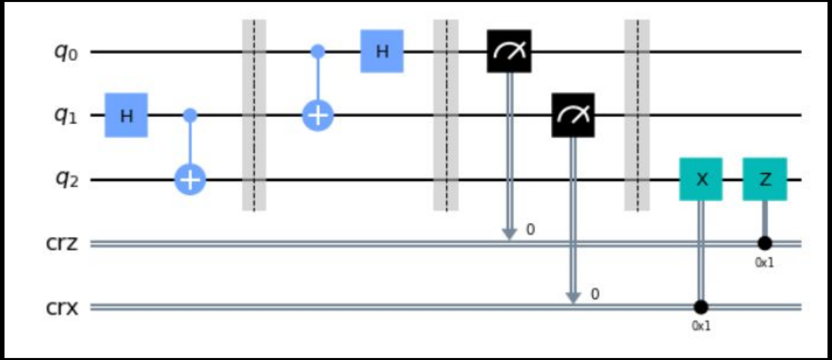
Quantum Circuits



A small note

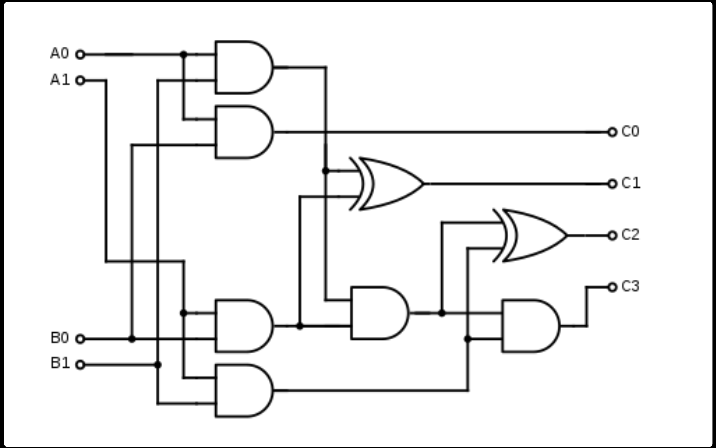
The abstraction level we are reasoning on is at “circuit” level!

Quantum Teleportation



$\simeq$

Binary Multiplier



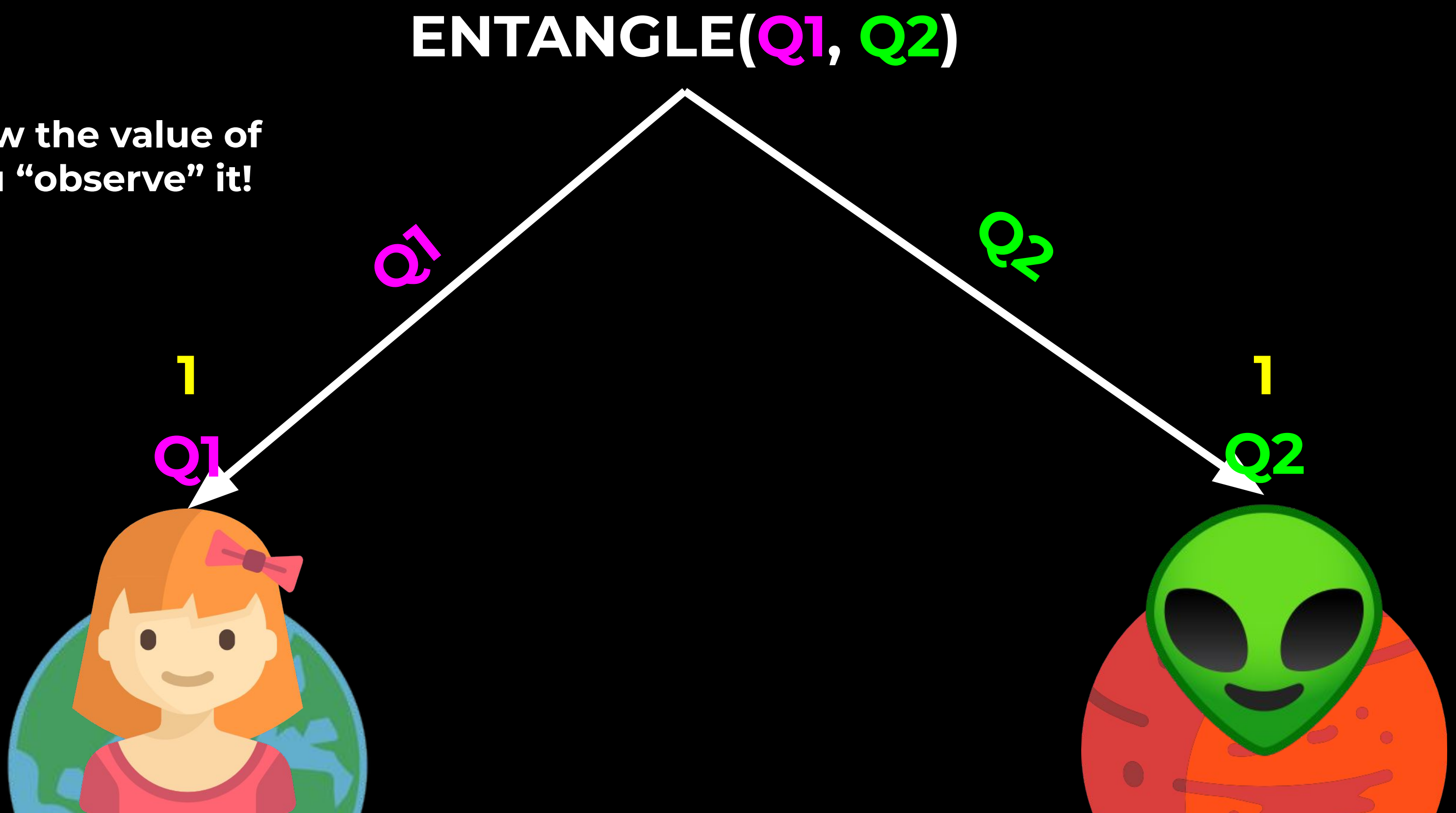
“How do you quantum-compute $\frac{2*3}{22}$ *?”*

It is equivalent to:

”Which is the classical circuit (AND, NOT) that computes multiplication and division?” → ***Not Trivial!***

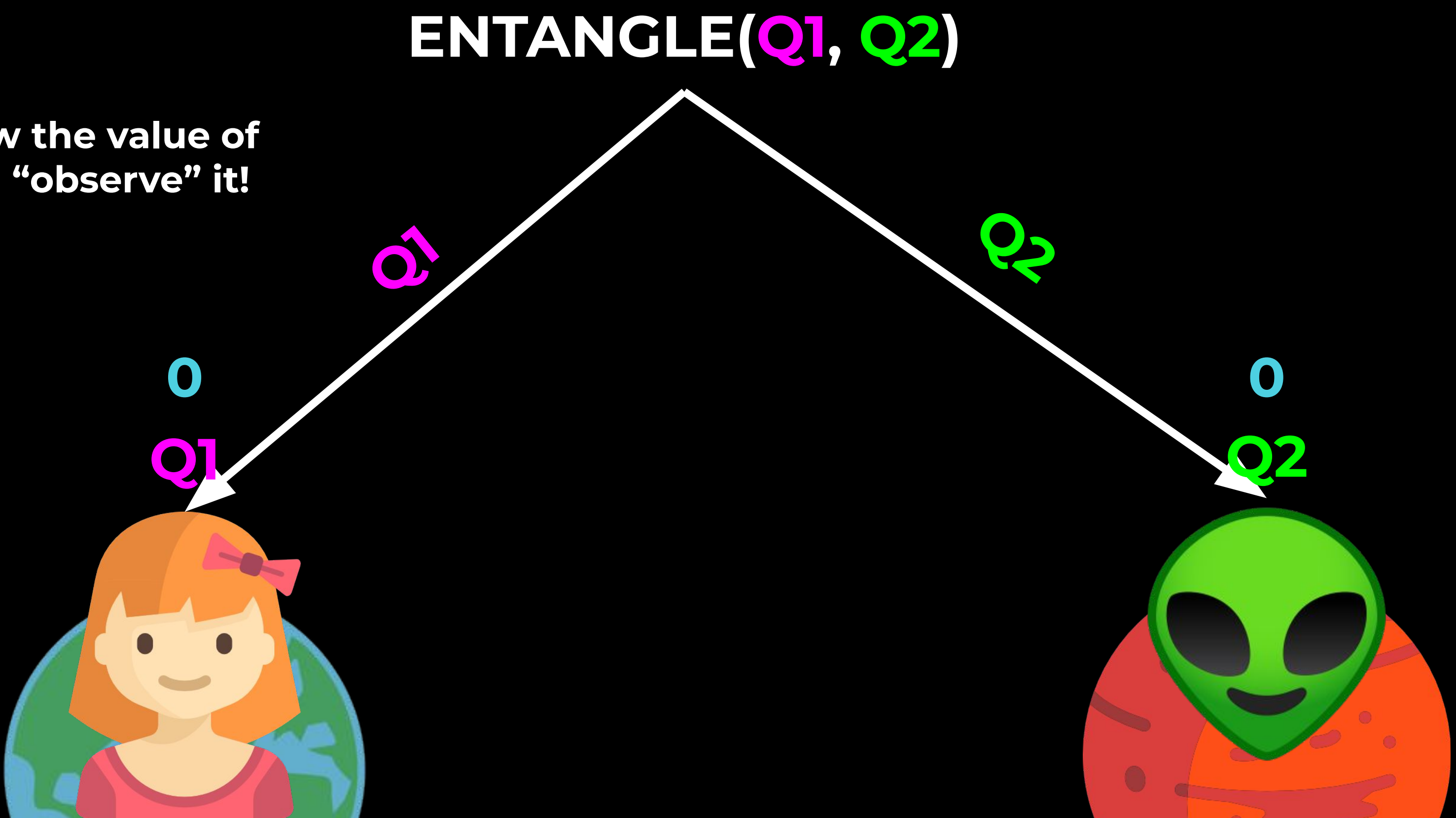
ENTANGLEMENT

ACHTUNG!
You cannot know the value of a qubit until you “observe” it!



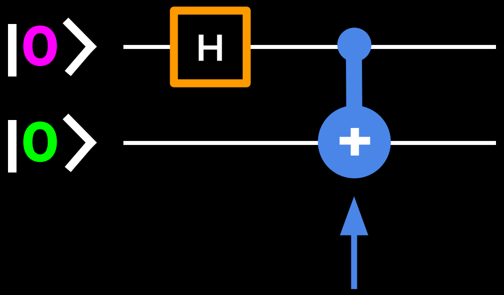
ENTANGLEMENT

ACHTUNG!
You cannot know the value of a qubit until you “observe” it!



How to entangle

<u>Quantum Circuit</u>



Controlled-Not
(CNOT)

"when the control qubit is 1
then flip the target qubit"

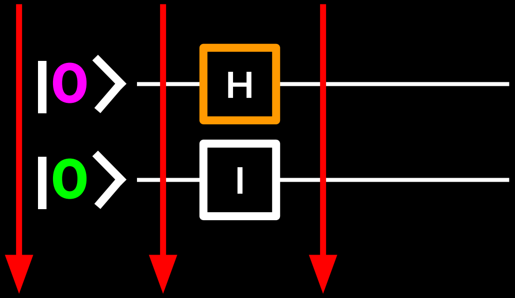
But... Let's do step-by-step...

How 2 systems can <u>mathematically</u> described?

THE TENSOR PRODUCT!

<u>ALERT: MATHS COMING</u>
(sry)

TENSOR PRODUCT



$$|0\rangle \otimes |0\rangle$$

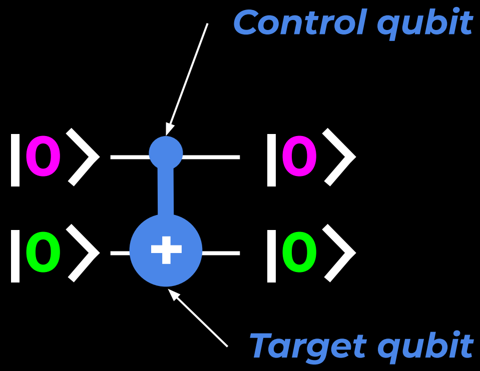
$$\begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}1\\0\end{pmatrix} = \begin{array}{c|l} \begin{pmatrix}1\\0\\0\\0\end{pmatrix} & \begin{array}{l}00\\01\\10\\11\end{array}\end{array}$$

$$\begin{pmatrix}1/\sqrt{2} & 1/\sqrt{2}\\ 1/\sqrt{2} & -1/\sqrt{2}\end{pmatrix} \otimes \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$$

$$\Downarrow$$

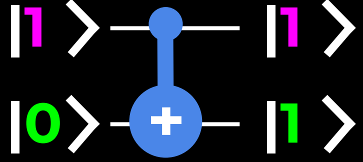
$$\left(\begin{array}{c|c} 1/\sqrt{2}\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} & 1/\sqrt{2}\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\\ \hline 1/\sqrt{2}\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} & -1/\sqrt{2}\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\end{array}\right) = \begin{pmatrix}1/\sqrt{2} & 0 & 1/\sqrt{2} & 0\\ 0 & 1/\sqrt{2} & 0 & 1/\sqrt{2}\\ 1/\sqrt{2} & 0 & -1/\sqrt{2} & 0\\ 0 & 1/\sqrt{2} & 0 & -1/\sqrt{2}\end{pmatrix}$$

CNOT



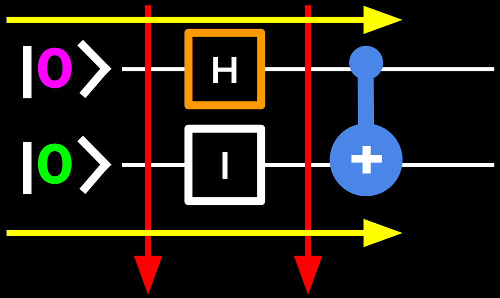
$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{array}{c} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \end{array} \begin{array}{c} 00 \\ 01 \\ 10 \\ 11 \end{array} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \begin{array}{c} 00 \\ 01 \\ 10 \\ 11 \end{array}$$

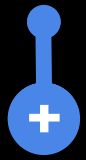
"when the control qubit is 1
then flip the target qubit"



$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \begin{array}{c} 00 \\ 01 \\ 10 \\ 11 \end{array} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \begin{array}{c} 00 \\ 01 \\ 10 \\ 11 \end{array}$$

ALL TOGETHER





$$\times \left(\boxed{H} \otimes \boxed{I} \right) \times \left(|0\rangle \otimes |0\rangle \right) = \begin{array}{cc} \begin{pmatrix} 1/\sqrt{2} \\ 0 \\ 0 \\ 1/\sqrt{2} \end{pmatrix} & \begin{array}{c} 00 \\ 01 \\ 10 \\ 11 \end{array} \end{array}$$

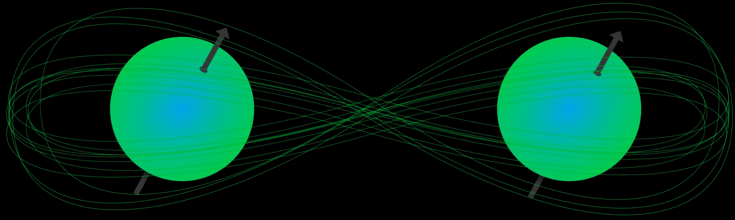
By now, you know how to entangle qubit!

<u>They cannot be anymore described as two distinct systems!</u>
That's what "entanglement" means.

Again!

Quantum entanglement occurs when a system of multiple particles in quantum mechanics interact in such a way so that **the particles cannot be described as independent systems but only as one system as a whole.**

In entanglement, one constituent cannot be fully described without considering the other(s)



Mathematically: **A vector that cannot be written as the tensor of two vector shall be called <u>entangled</u>.**

$$\cancel{[\;\;]} \otimes \cancel{[\;\;]} = \begin{pmatrix} 1/\sqrt{2} \\ 0 \\ 0 \\ 1/\sqrt{2} \end{pmatrix}$$

They don't exist!

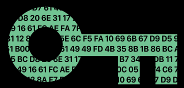
Why?

I stressed entanglement because it is the main ingredients of quantum algorithms.

An Example?

E91 protocol - Ekert

(Quantum Key Exchange)



Any attempt at eavesdropping by an attacker destroys the entanglement correlations.

<u>Eavesdropping-resistant!</u>

LET'S TAKE A BREATH

What we have seen so far:

- What mea… …antum-compute"
- What is a q…
- Why yo… …es during a computation
- The "H…
- Wh…
- Ho…
- The…
- How to e…
- What … …t

I’m going to impress you!

“Which is the complexity of searching an element in an <u>unsorted</u> dataset?”

Θ(n)

i.e. to find an element you need to scan the entire the dataset.
i.e. (x2) You need to know each element to answer correctly, right?

GROVER’S ALGORITHM (Quantum Algorithm)

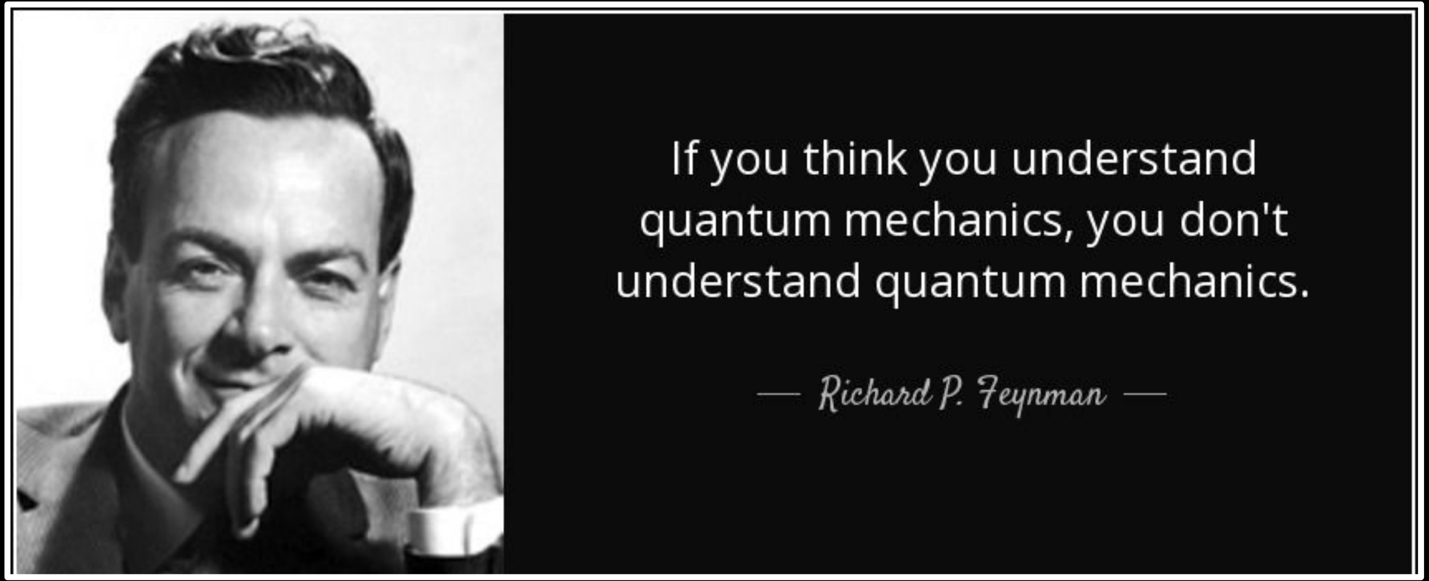
O(√n)

i.e. Grover’s Algorithm finds the element <u>without</u> scanning the entire dataset!!

Don’t you think that is incredible?

WHY?

These incredible quantum phenomena just happen.
No one knows why.



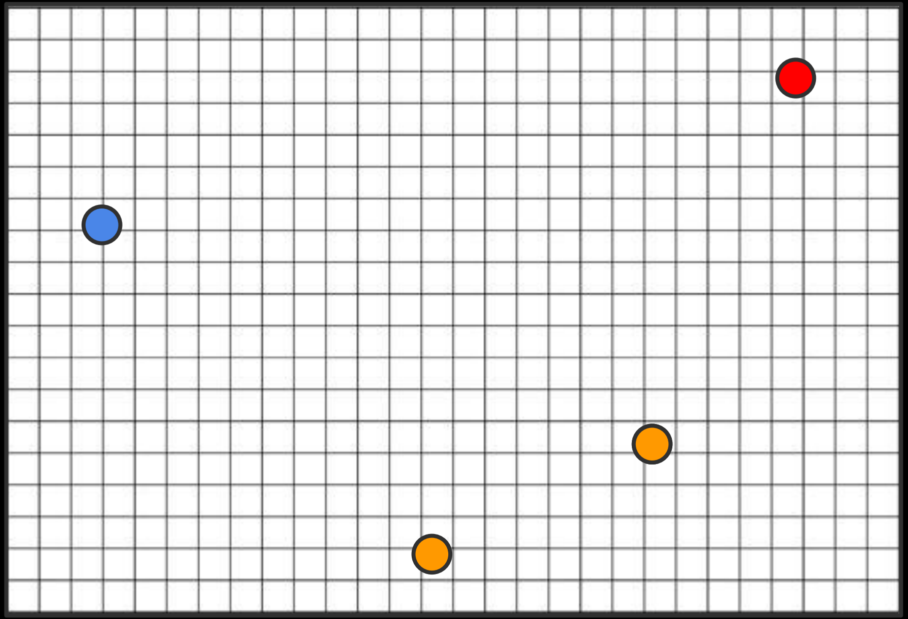
To

Classification

Distance Based Classifier

The Task:

- Given 3 different training vectors
- Given a test vector
- What is the closest training vector to test one?



Key-Elements

You compute the distances between each training vectors and the test vector

(3 training vectors → 3 distances to compute)

Then you are able to establish which is the closest element to the new input

CLASSICAL

```
def computeDistance(p1, p2):
    a = (p1[0] - p2[0])**2
    b = (p1[1] - (p2[1])**2
    return math.sqrt( a + b )


def belongsTo(test, trainings):
    distances = []
    for tr in trainings:
        dist = computeDistance(test, tr)
        distances.append(dist)
    return min(distances)
```

High Abstraction Level

$\simeq$

QUANTUM

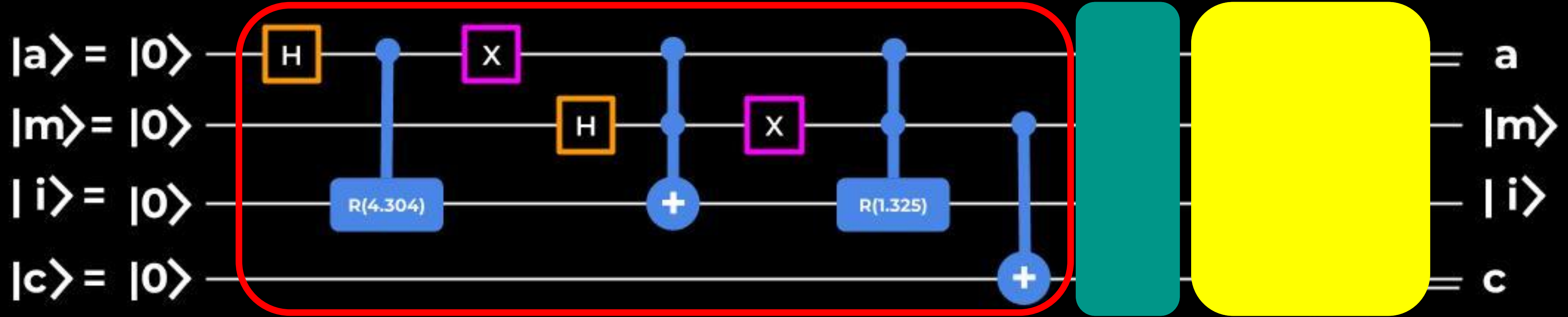
$\boxed{H}$

Very Low Abstraction Level

Quantum Distance Based Classifier (by Schuld, Fingerhuth, Petruccione)

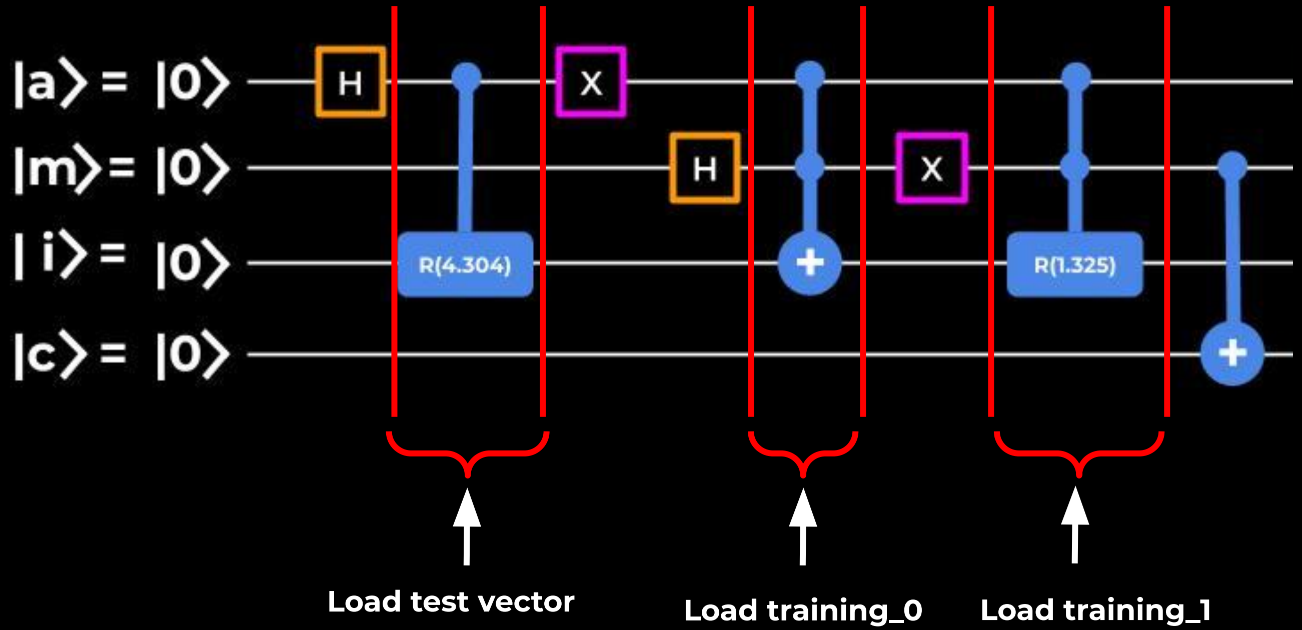
Quantum Computing algorithms can be splitted in 3 phases:

- **Quantum Data Encoding**
  - i.e. Encodes classical bits into quantum bits
- **Quantum Computation**
  - i.e. Computes (such as computing distances)
- **Measurement**
  - i.e. Converts the “quantum-solution” into the “classical one”



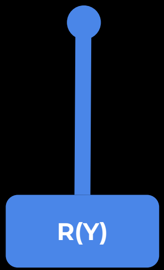
Quantum Data Encoding

Let's try to understand what's happening...



Amplitude Encoding

But what is this gate?

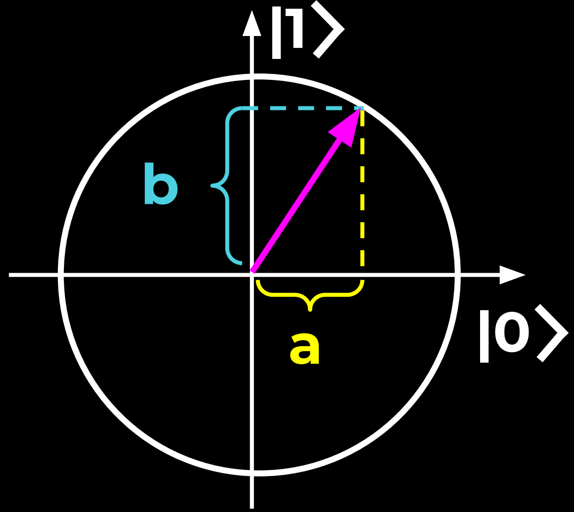


It is a "Controlled Rotation".
i.e. when the control qubit is 1 then rotate the target qubit by Y.

$a|0\rangle + b|1\rangle$

Condition

$|a^2| + |b^2| = 1$



$\cos\alpha|0\rangle + \sin\alpha\,|1\rangle$

Amplitude Encoding

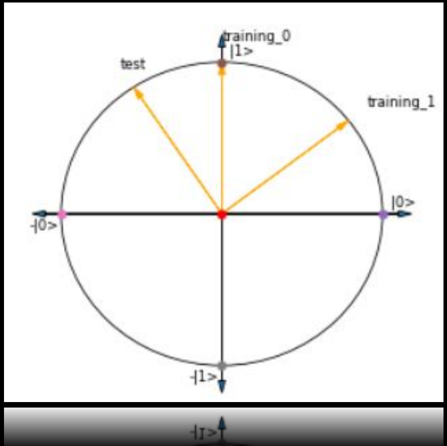
Given a dataset D such that each element has 2 features $[x_0, x_1]$ **:**

Standardize and Normalize the dataset D

training_0 = [0,1]
training_1 = [0.789, 0.615]
test = [-0.549, 0.836]

Now you have to encode this values in qubit.

i.e. you have to find a degree α values such that "rotate" a qubit in such a way that it represents a vector in the dataset.

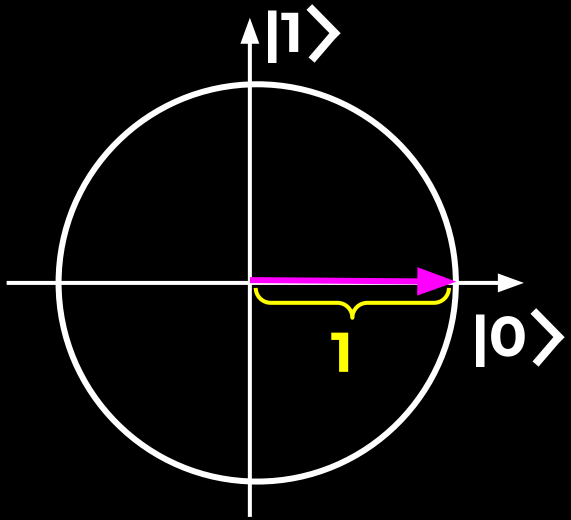


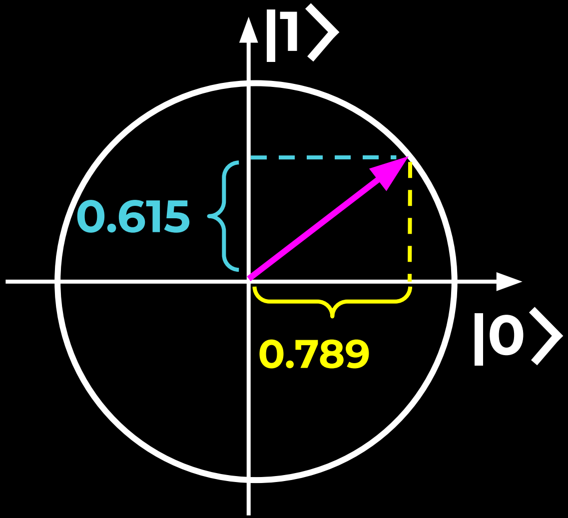
Amplitude Encoding

Rotate such that

training_1 = [0.789, 0.615]

$1|0\rangle \longrightarrow 0.789|0\rangle + 0.615|1\rangle$

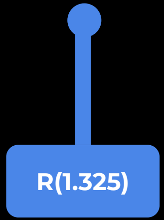




$\cos\alpha|0\rangle + \sin\alpha\,|1\rangle$

So how to obtain this α?

$\arctan(\sin\alpha/\cos\alpha)$

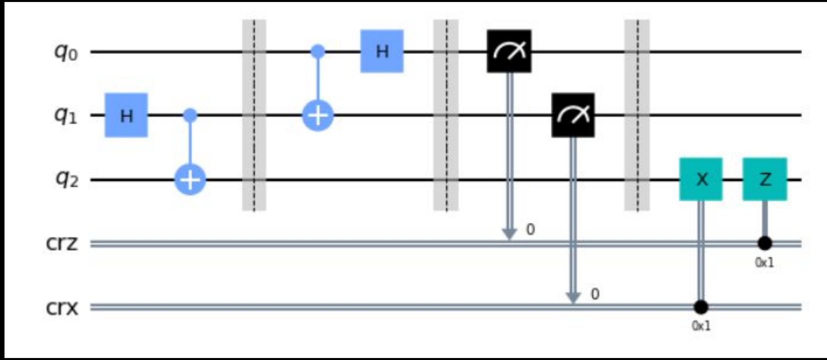


Università di Pisa

Map in memory

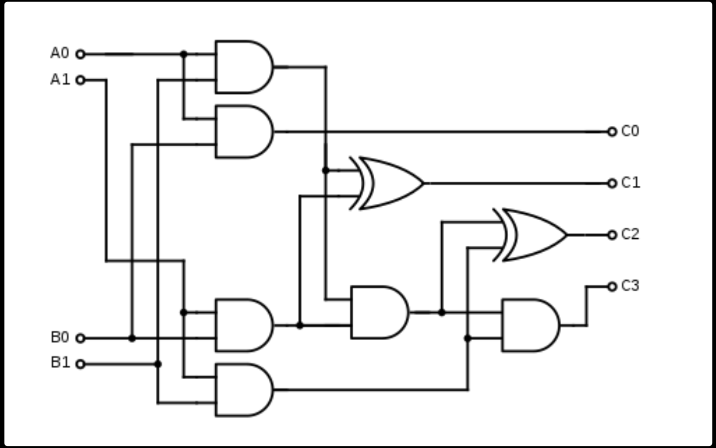
We said that:

Quantum Teleportation



≃

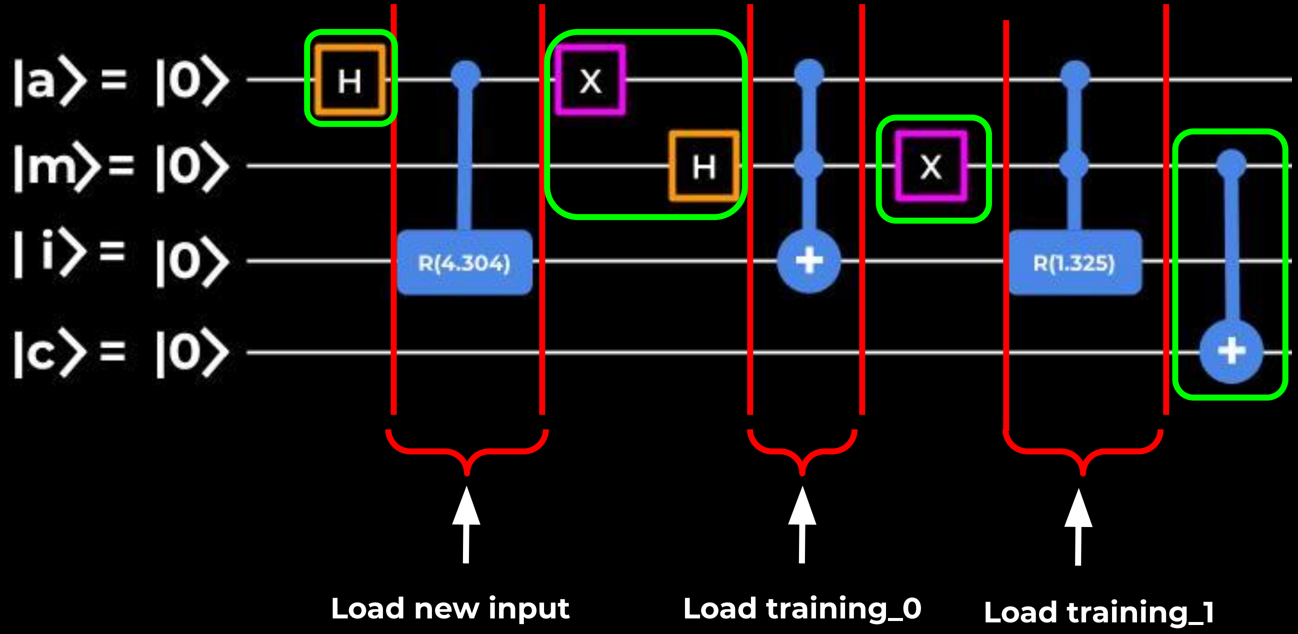
Binary Multiplier



They are at the same abstraction level → Lack of memory structures

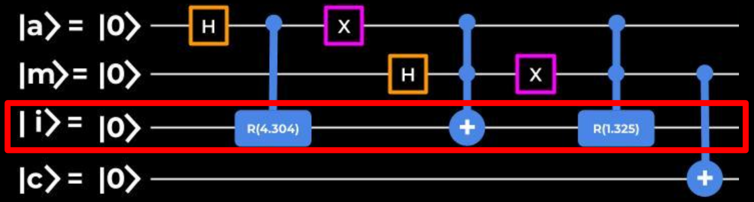
So, in our quantum circuit, we need also to map values in memory by hand!

Map in memory

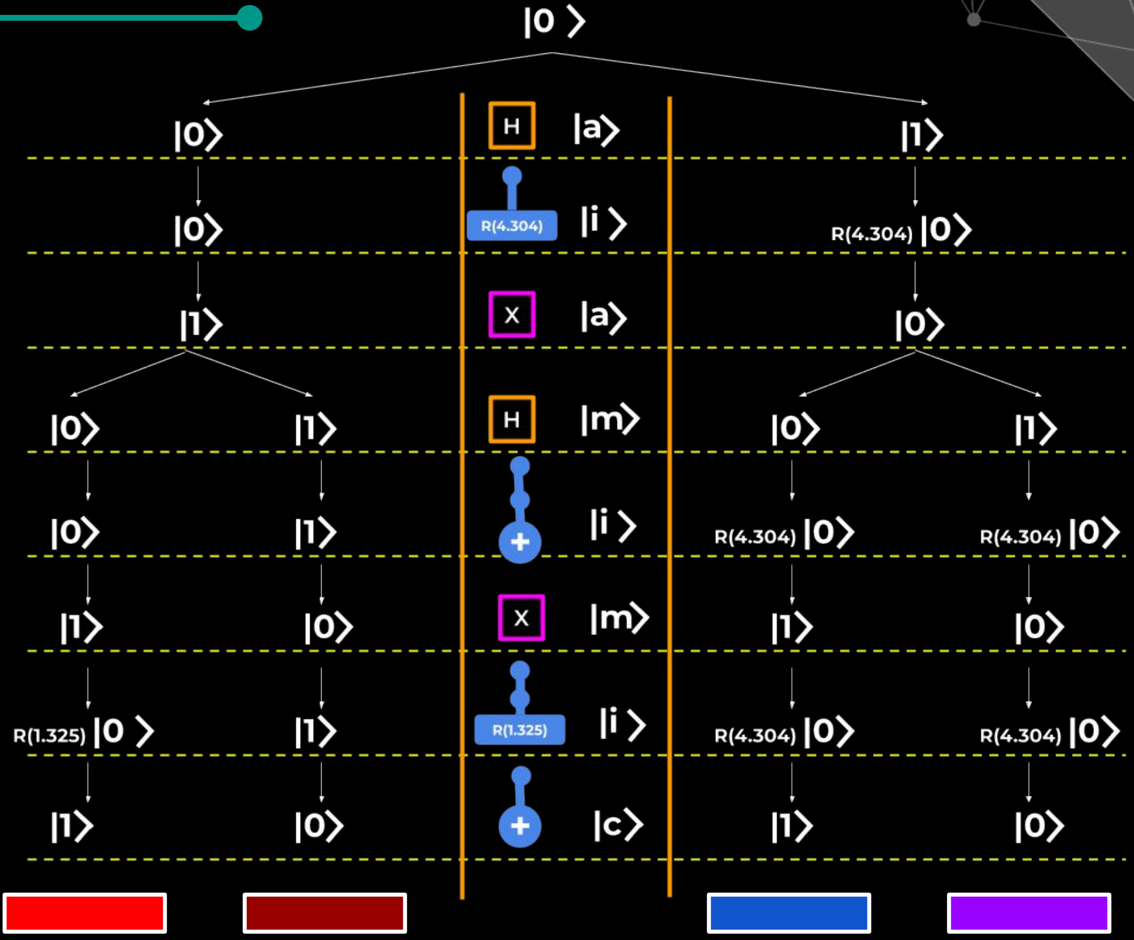


Let's try to visualize what is happening...

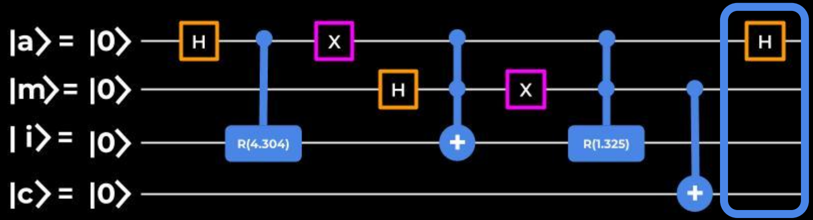
Visual Quantum Tree - Encoding

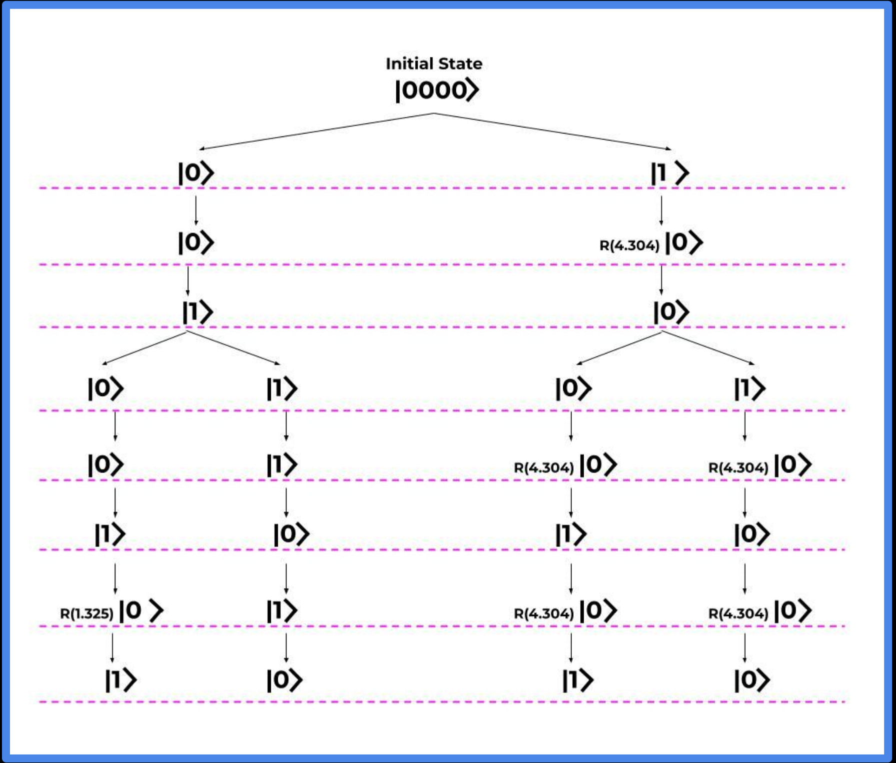


	Training_1	Training_0	Test Vector	Test Vector
|a⟩	|1⟩	|1⟩	|0⟩	|0⟩
|m⟩	|1⟩	|0⟩	|1⟩	|0⟩
| i⟩	R(1.325)|0⟩	|1⟩	R(4.304)|0⟩	R(4.304)|0⟩
|c⟩	|1⟩	|0⟩	|1⟩	|0⟩



Visual Quantum Tree - Computing





The Hadamard Clashes/Compares:

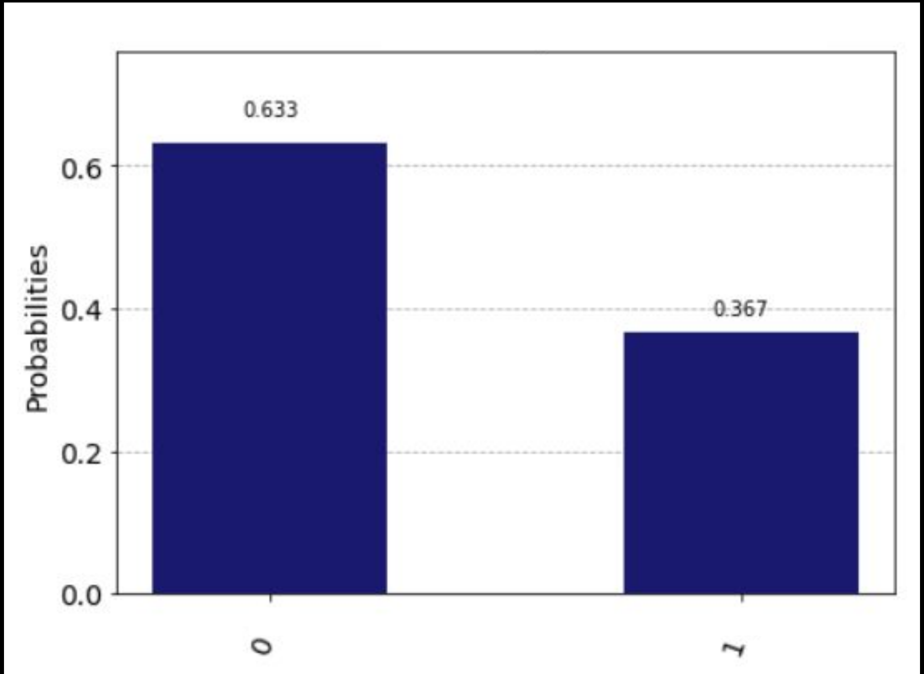
- Training_0 and Test (class 0)
- Training_1 and Test (class 1)

In one single shot!

The Hadamard Effect

UNIVERSITÀ DI PISA

MEASUREMENT



What does it mean?

Short Story
The test belongs to class 0

The truth:
Running the algorithm 10 times:
- 6 times the algorithm classifies the test in class 0
- 4 times the algorithm classifies the test in class 1

TODAY

“ALL THAT GLITTERS IS NOT GOLD”

a.k.a. “Non è tutto oro ciò che luccica”

Quantum Computers suffers from the “decoherence problem”

- **i.e. qubits gets corrupted very quickly**

The deeper the circuit, the more unreliable the qubits are.

The encoding phase “deeps” the circuit a lot → <u>decoherence</u>

Quantum Computing is 10 years away from a real use-case

BUT…

TODAY

OUR MISSION IS TO PREPARE THE GROUND FOR TOMORROW

Because for sure:

- **The decoherence problem will be handled** → Deeper circuits
- **A Quantum Memory storage will be developed** → No more quantum encoding phase

Fields of Application

Cryptography

Quantum computers have the potential to keep private communications safe from snoops.

Medicine & Materials

Quantum Computer mimics the computing style of nature, allowing it to simulate, understand and improve upon natural things.

Machine Learning

Research indicates that quantum computing could significantly accelerate machine learning and data analysis tasks.

Searching Big Data

Quantum Computing can search the ever-growing amount of data being created, and locate connections within it, significantly faster than classical computers

QUESTION TIME!

alessandro.berti@phd.unipi.it

in/aleberti

Brotherhood94

Brotherhood94