Escuela de invierno en computo cuántico

Centro de Estudios en Computación Avanzada CECAV

Posgrado en Ciencias Físicas

Miguel de Jesús González Martínez

24/01/2022

¿Para qué necesitamos una computadora cuántica?

- A groso modo, un algoritmo se dice que es eficiente si corre en un tiempo polinomial, es decir, el tiempo que tarda en correr dicho algoritmo crece con el número de bits de entrada n de manera polinomial n^x, con x algún número entero.

- Se dice entonces que un problema computacionalmente difícil es aquel cuyo mejor algoritmo clásico que lo resuelve, lo hace de manera exponencial en el número n de bits de entrada, es decir, como a^n, con a alguna constante.

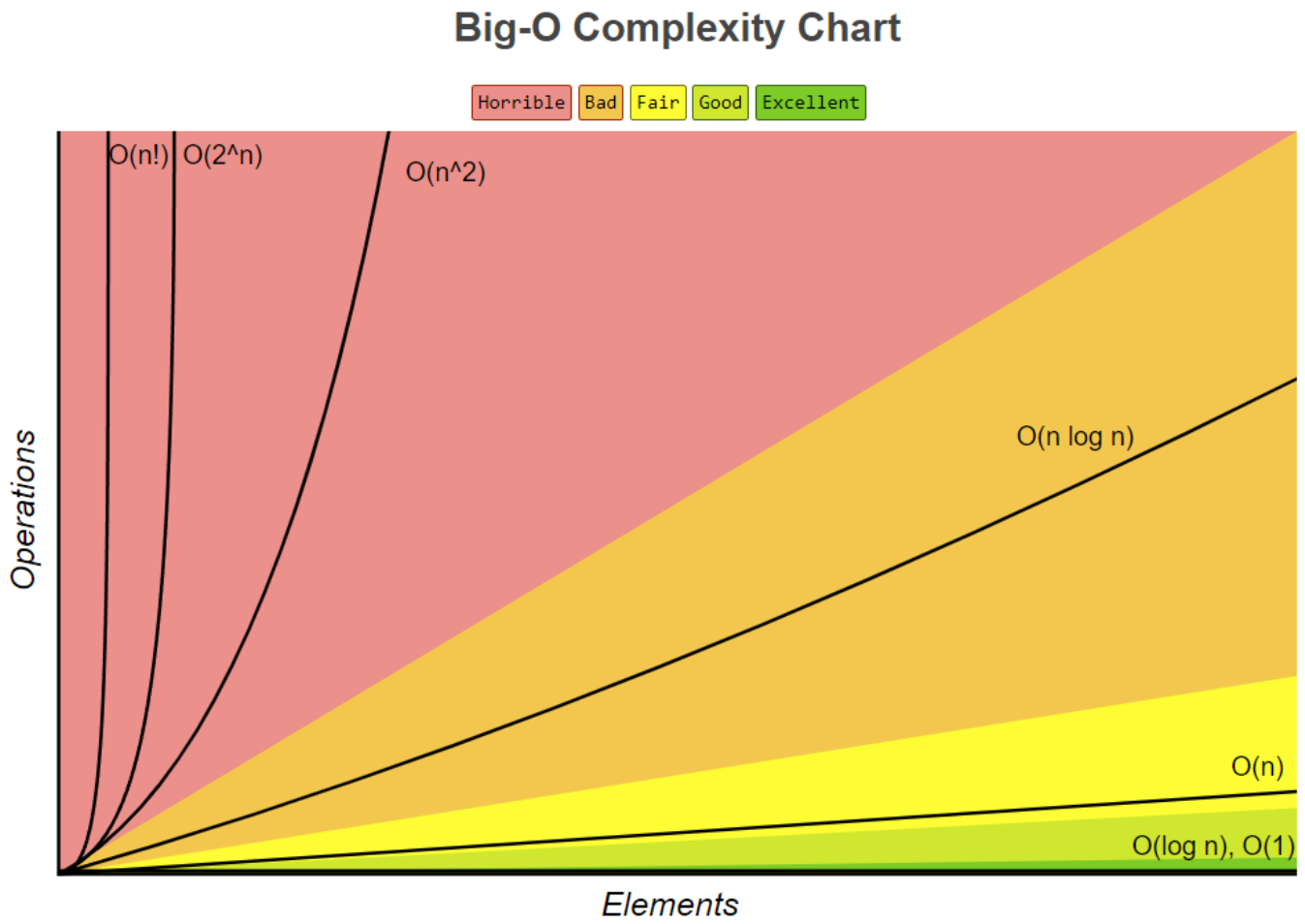


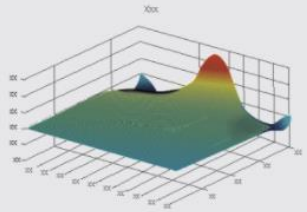
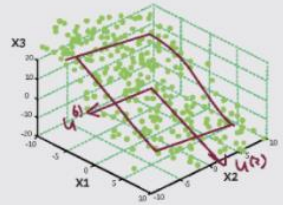
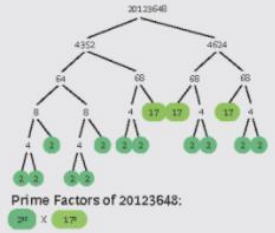
Figura tomada de: Big-O Algorithm Complexity Cheat Sheet (Know Thy Complexities!) @ericdrowell (bigocheatsheet.com)

¿Qué tipo de problemas se busca resolver con la computación cuántica ?

- Encriptación y seguridad
  - Factorización de números primos en protocolos como el RSA
  - Criptografía cuántica
- Problemas de optimización
  - Buscar la solución más óptima en cierto rango de parámetros
  - Logística, Meteorología, Finanzas
- Desarrollo de materiales
  - Simulación de sistemas cuánticos para determinar los elementos necesarios para obtener determinada característica
  - Química cuántica, Medicina, Biología
- Análisis de datos
  - Se estima que el 90% de toda la información producida por la humanidad, se ha creado en los últimos años. El contar con un gran poder de computo para tareas como ordenar o buscar información, sería de gran ayuda.
- Física básica
  - Simulación de la evolución temporal de ciertos Hamiltonianos
  - Cálculo del espectro de energía

¿En qué tipo de problemas se ha estado implementando la computación cuántica ?

EXHIBIT 1 | Quantum-Advantaged Computational Problems

Type of problem	Useful for...	Industry applications include...
 Combinatorial optimization	Minimizing or maximizing an objective function, such as finding the most efficient allocation of resources or the shortest total distance among a set of points (e.g., the traveling salesman problem)	• Network optimization (e.g., for airlines, taxis) • Supply chain and logistics optimization • Portfolio optimization in financial services
 Differential equations	Modeling the behavior of complex systems involving fundamental laws of physics (e.g., Navier Stokes for fluid dynamics and chemistry)	• Fluid dynamics simulations for automotive and aeronautical design and medical devices (e.g., blood flow analysis) • Molecular simulation for specialty materials design and drug discovery
 Linear algebra	Machine learning tasks involving matrix diagonalization, such as clustering, pattern matching, and principal components analysis, as well as support vector machines, which are ubiquitous in applications across industries	• Risk management in quantitative finance • DNA sequence classification • Marketing and customer segmentation
 Factorization	Cryptography and computer security, where the most common protocols today (e.g., RSA) rely on the infeasibility (for classical computers) of factoring the product of two large prime numbers	• Decryption and code breaking (e.g., for governments)

Source: BCG analysis.

Figura tomada de: Where Will Quantum Computers Create Value—and When? (bcg.com)

¿Quiénes están invirtiendo?

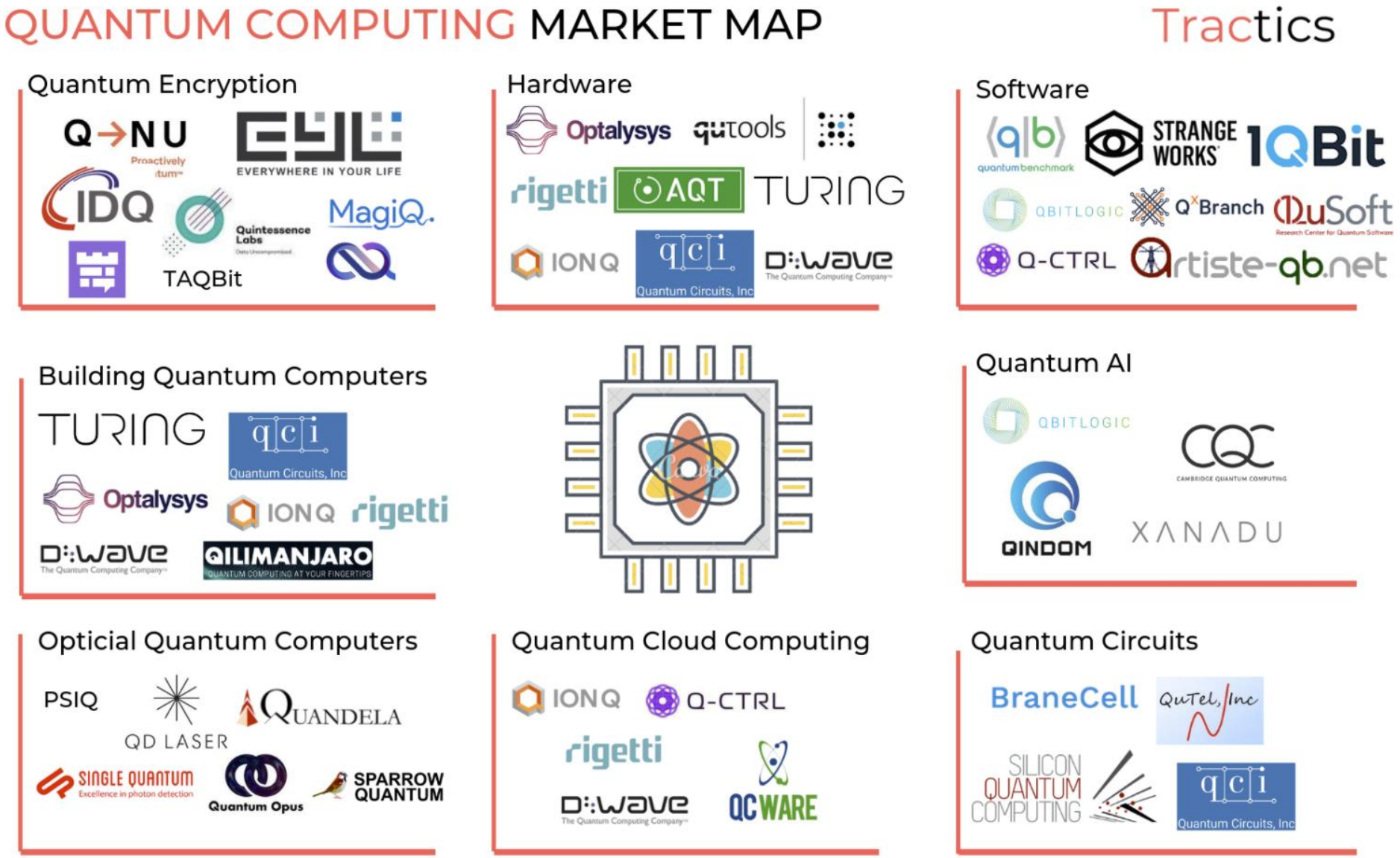


Figura tomada de: QC companies of 2022: Guide based on 4 ecosystem maps (aimultiple.com)

Implementaciones

Universal Gate Based Quantum Computers

Superconducting Architecture

Alibaba Group · intel · rigetti · Google · IBM · 1950

Trapped Ions	Topological	Photonic
IONQ · NSF	Microsoft	XANADU · hp

Annealing

Quantum Annealing

D-Wave The Quantum Computing Company™

QNNcloud · iP

Superconducting loops	Trapped ions	Silicon quantum dots	Topological qubits	Diamond vacancies
Company support				
Google, IBM, Quantum Circuits	ionQ	Intel	Microsoft, Bell Labs	Quantum Diamond Technologies

Figura tomada de: QC companies of 2022: Guide based on 4 ecosystem maps (aimultiple.com)

Lenguajes disponibles

qiskit 0.23.4
see release notes

Open-Source Quantum Development

Qiskit [kiss-kit] is an open source SDK for working with quantum computers at the level of pulses, circuits and application modules.

XANADU

PENNYLANE

A cross-platform Python library for differentiable programming of quantum computers. Train a quantum computer the same way as a neural network.

Quantum Inspire - By QuTech

The multi hardware Quantum Technology platform

Run your own quantum algorithms on one of our simulators or hardware backends and experience the possibilities of quantum computing. Find out more below or get started immediately.

QuTiP

Quantum Toolbox in Python

TensorFlow Quantum

ZAPATA

PRODUCT SOLUTIONS RESEARCH

solutions.

We build software to get the enterprise quantum-ready™.

We help industry-leading companies understand—and capitalize on—the capabilities of quantum devices in the next 2-5 years and beyond.

ProjectQ

Powerful open source software for quantum computing

Visual Studio | Marketplace

Visual Studio > Tools > Microsoft Quantum Development Kit

Microsoft Quantum Development Kit

Microsoft DevLabs | 65.801 installs | ★★★★★ (35)

Microsoft Quantum Development Kit provides support for developing quantum algorithms in the Q# programming language.

Download

Leap

The quantum cloud service built **for business**

Sign Up

Cirq

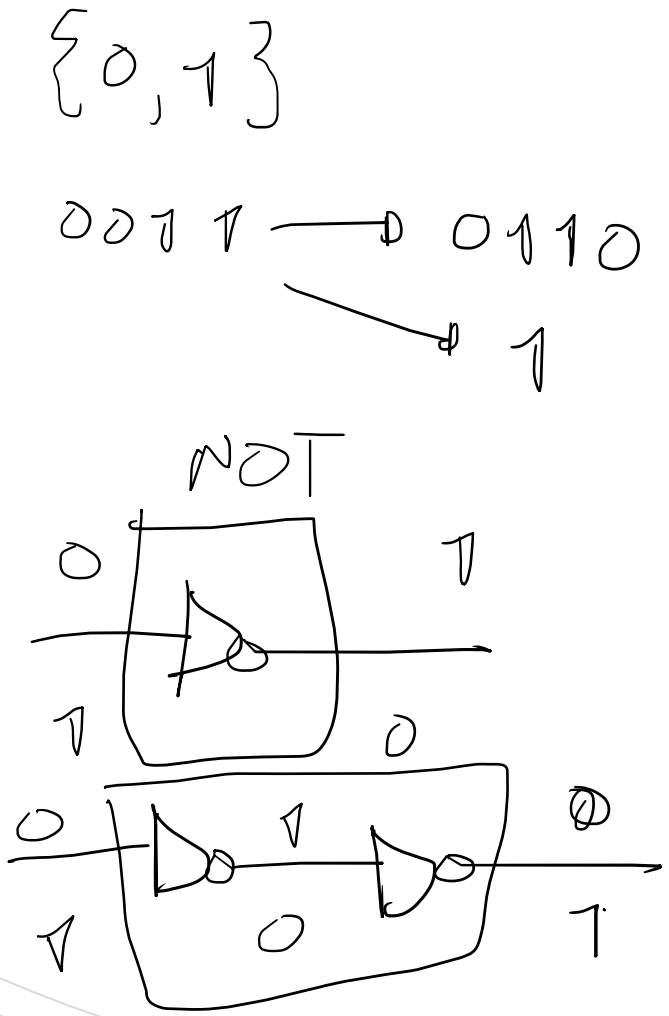
An open source framework for programming quantum computers

Escuela de invierno en computo cuántico

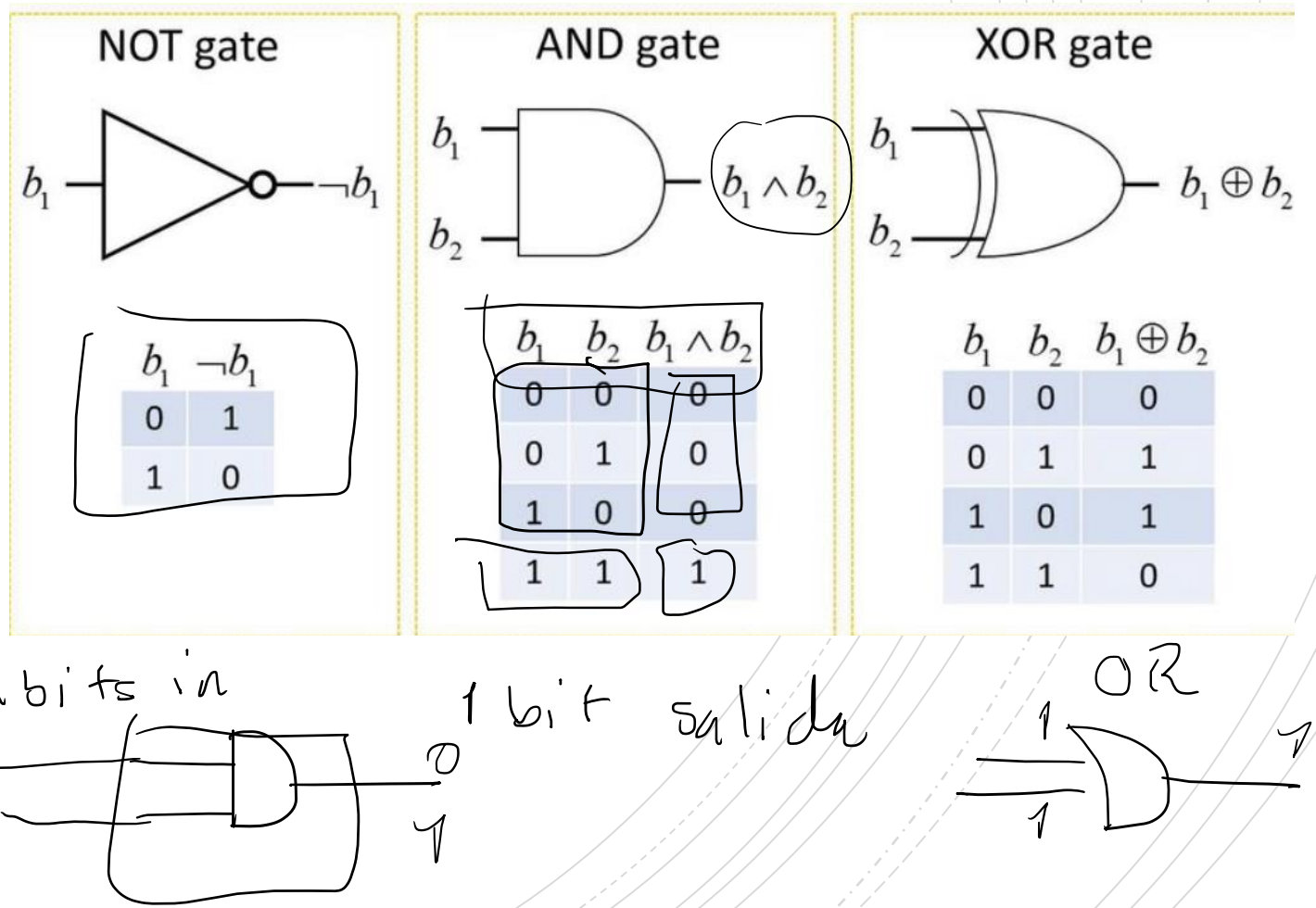
Iniciamos

Algoritmo clásico

Elementos básicos



Compuertas (operadores)

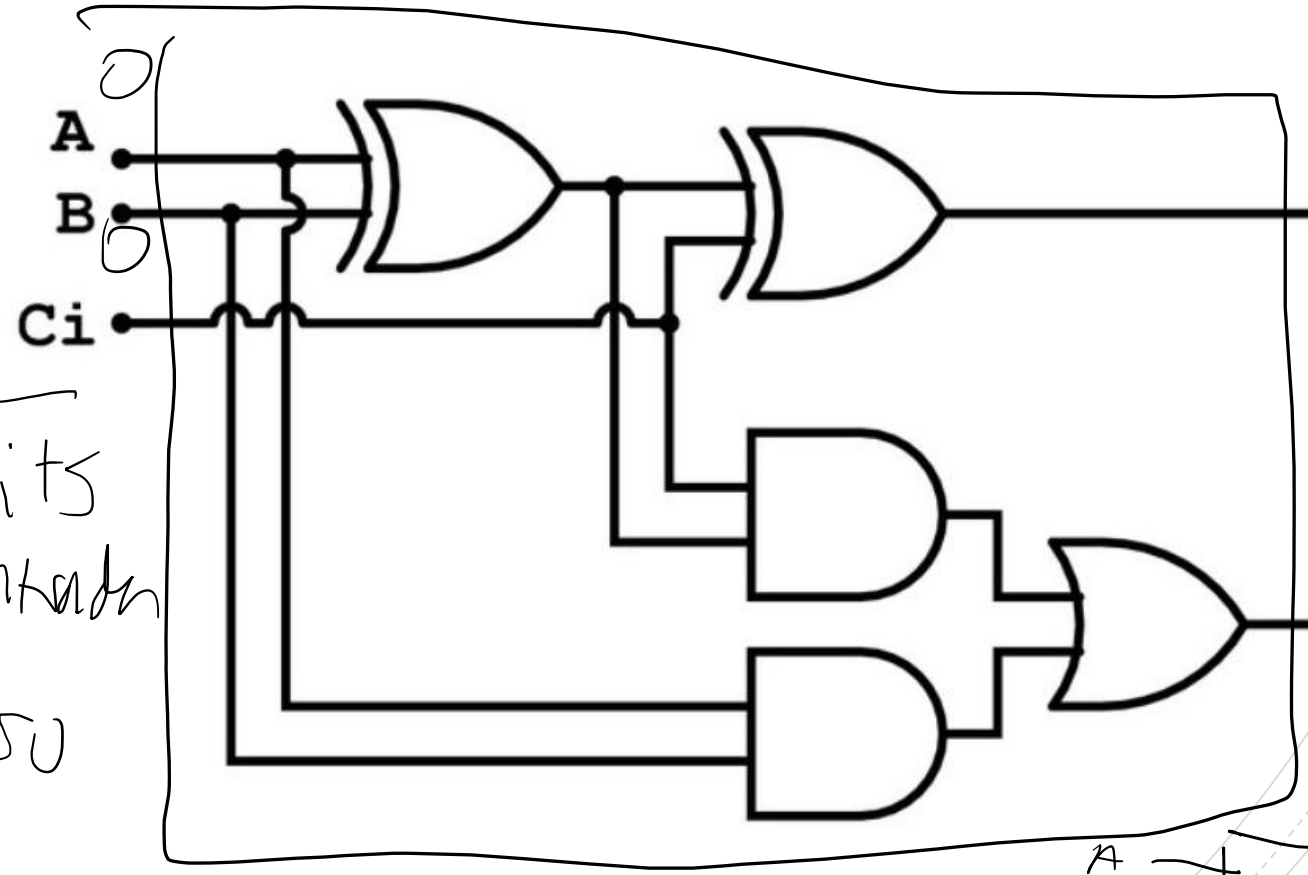


Algoritmo clásico

Circuito sumador de un bit

A, B {0, 1}

0 + 0 = 0 0
1 + 0 = 0 1
0 + 1 = 0 1
1 + 1 = 1 0



S = A + B = 0
1

Bits entrada

Bits salida

5V

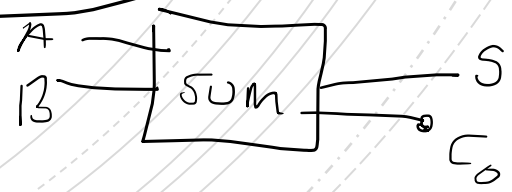
0 0V

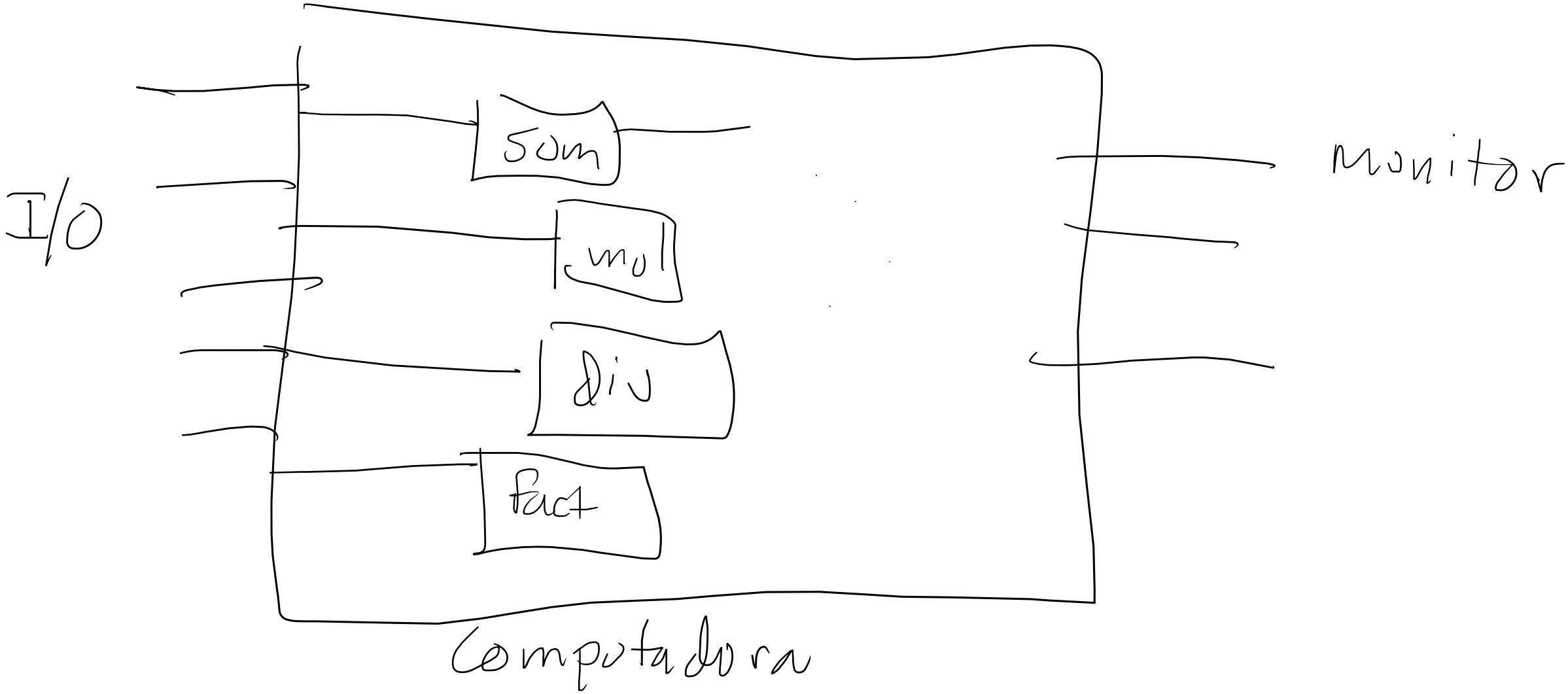
0 a 1

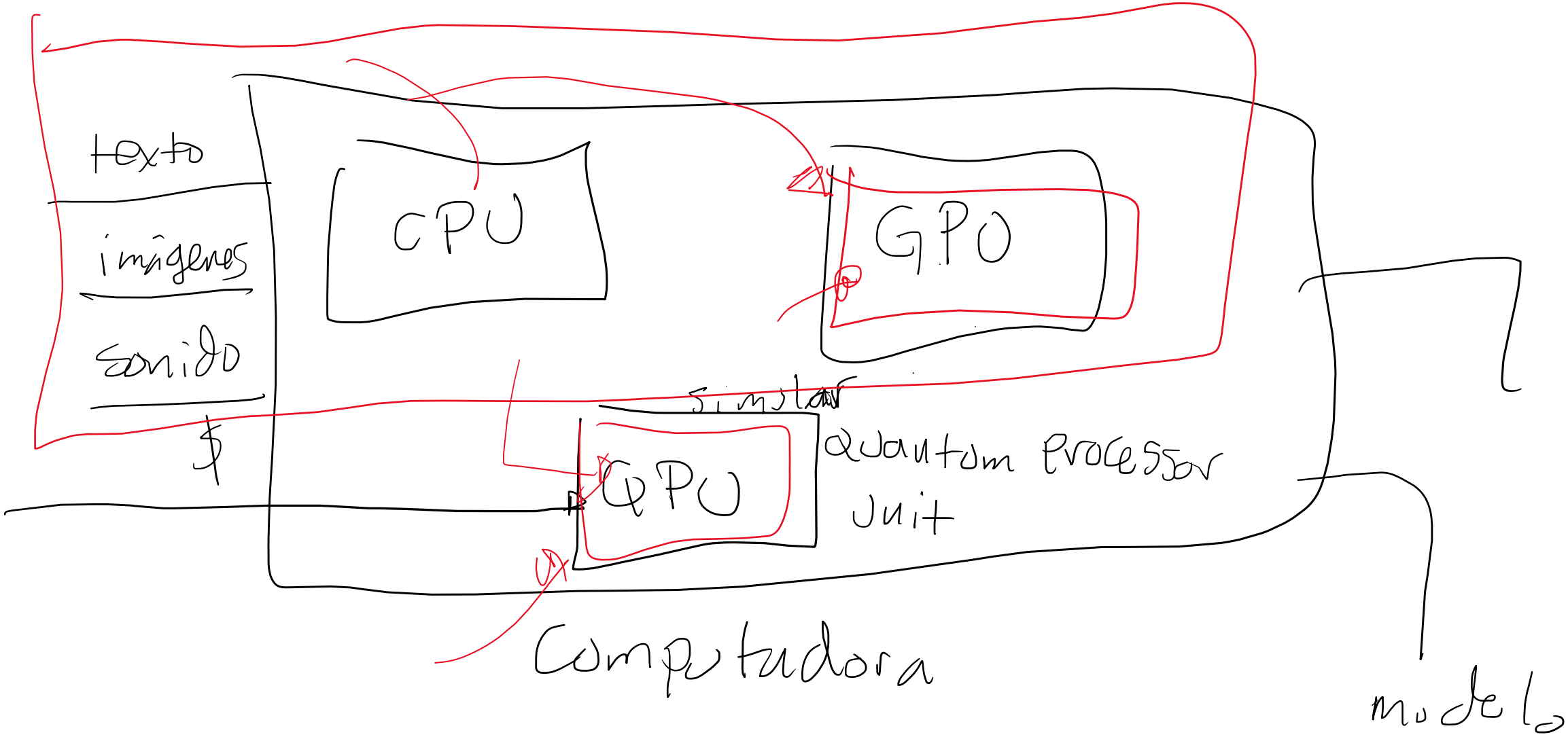
0V

Sum

Compuerta



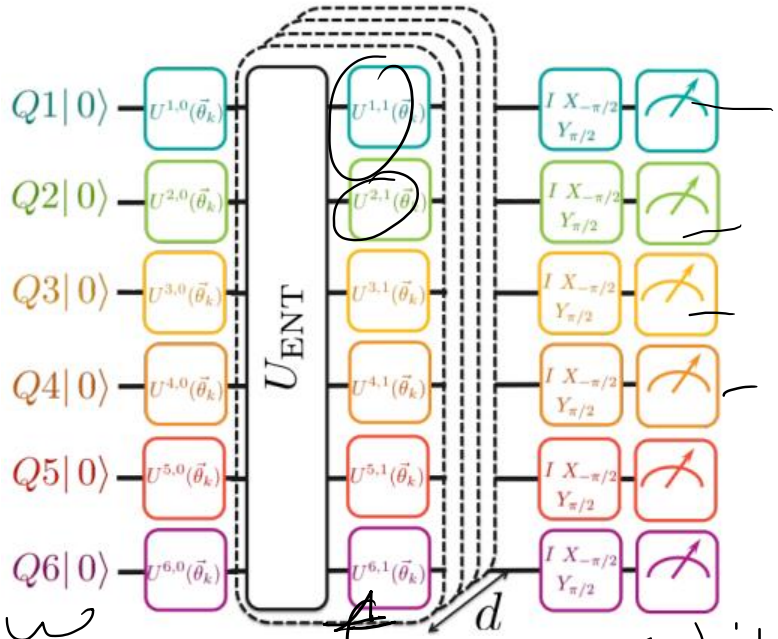

I/O
som
mul
div
fact
monitor
Computadora


texto
imágenes
sonido
$
CPU
GPU
similar
QPU
quantum processor unit
Computadora
modelo

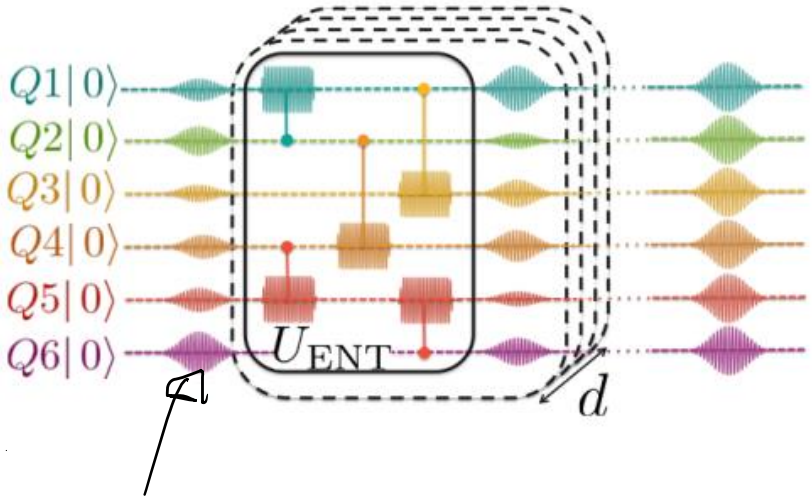
Computadora cuántica

Niveles de abstracción

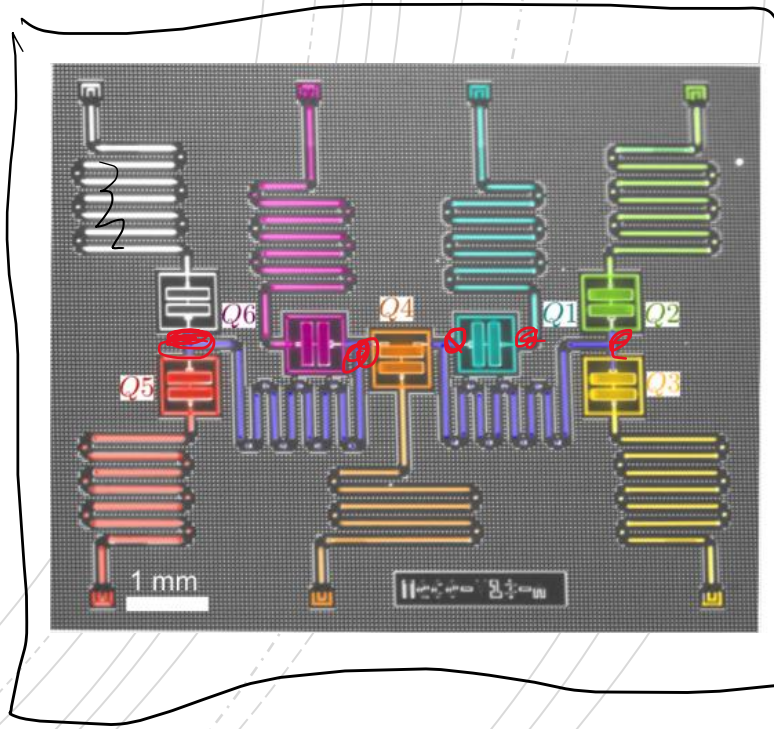
1



2



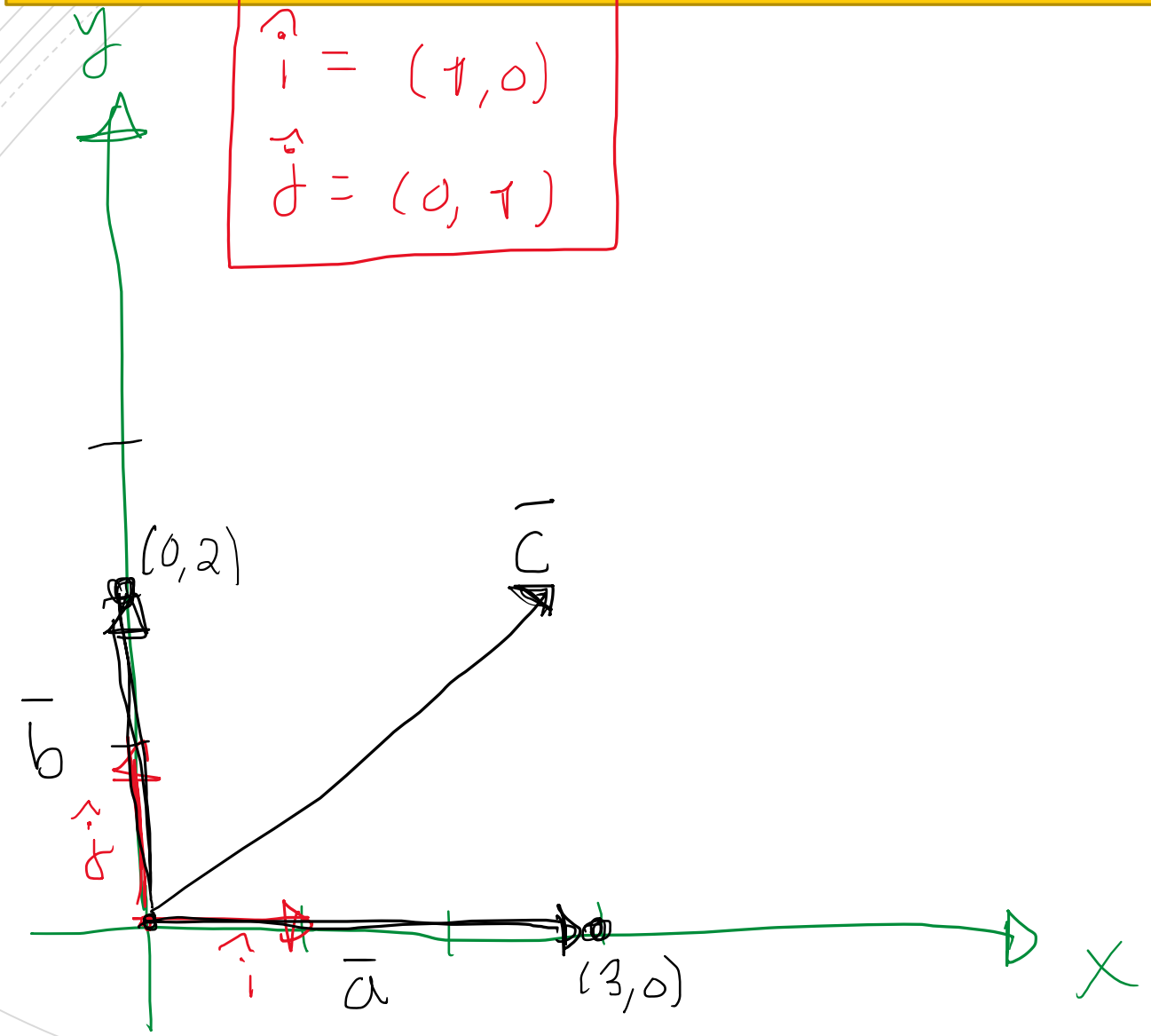
3



Vectores en R^2 y "notación de Dirac"

$\hat{i} = (1,0)$

$\hat{j} = (0,1)$



(3,0) , (0,2)

$\bar{a} = 3\hat{i}$ $\quad \bar{b} = 2\hat{j}$

$\bar{c} = \bar{a} + \bar{b}$

$\bar{c} = 3\hat{i} + 2\hat{j}$

cuántico

ket

$|c\rangle = 3|i\rangle + 2|j\rangle$

$|c\rangle = 3|0\rangle + 2|1\rangle$

Elementos básicos de un algoritmo cuántico

Estados cuánticos

$|\psi\rangle$:= Estado cuántico (Ket)

psi

$\{|0\rangle, |1\rangle\}$

Base computacional
Para 1 qubit

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \qquad \alpha, \beta \in \mathbb{C}$$

$|\psi_1\rangle = |0\rangle$

$|\psi_2\rangle = |1\rangle$

$$|\alpha|^2 + |\beta|^2 = 1$$

condición de normalización

α, β := amplitudes de probabilidad

$|\alpha|^2$:= Probabilidad del estado $|\psi\rangle$ de estar en $|0\rangle$

Espacio de Hilbert (pre-Hilbert)

un qubit

$\{|0\rangle, |1\rangle\}$ $2^1 = 2$

Base computacional

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

Vector, vector de estado, qubit

- Base computacional $\{|0\rangle, |1\rangle\}$

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$$|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$|a\rangle = 1/\sqrt{2}\begin{pmatrix} 1 \\ 0 \end{pmatrix} + 1/\sqrt{2}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1/\sqrt{2} \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 1/\sqrt{2} \end{pmatrix} = \begin{pmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{pmatrix}$$

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

* Ket $|a\rangle$

* Bra $\langle a|$

$$|a\rangle = \begin{pmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{pmatrix} \Longrightarrow \langle a| = \begin{pmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{pmatrix}^{*T}$$

conjugada

traspuesta

* vector columna

$$= \left(1/\sqrt{2},\ 1/\sqrt{2} \right)$$

* vector renglón

$$\langle 0| = \begin{pmatrix} 1 \\ 0 \end{pmatrix}^{*T} = (1,\ 0) \qquad \langle 1| = \begin{pmatrix} 0 \\ 1 \end{pmatrix}^{*T} = (0,\ 1)$$

$|a\rangle = 1/\sqrt{2}\,|0\rangle + 1/\sqrt{2}\,|1\rangle$ • Ket

• let $|a\rangle$

$\langle a| = (1/\sqrt{2},\ 1/\sqrt{2}) = 1/\sqrt{2}\,\langle 0| + 1/\sqrt{2}\,\langle 1|$ • Bra

---

$|b\rangle = \frac{i}{\sqrt{3}}|0\rangle - i\sqrt{2/3}\,|1\rangle$

$\langle b| = \left(\frac{i}{\sqrt{3}}|0\rangle\right)^{*T} - \left(i\sqrt{2/3}\,|1\rangle\right)^{*T}$

$$|b\rangle = \frac{i}{\sqrt{3}}|0\rangle - i\sqrt{2/3}\,|1\rangle$$

$$\langle b| = \left(\frac{i}{\sqrt{3}}|0\rangle\right)^{*T} - \left(i\sqrt{2/3}\,|1\rangle\right)^{*T}$$

$$(|0\rangle)^{*T} = \langle 0|$$

$$(|1\rangle)^{*T} = \langle 1|$$

$$\langle b| = \frac{-i}{\sqrt{3}}\langle 0| - -i\sqrt{2/3}\,\langle 1|$$

Bra

$$\langle b| = \frac{-i}{\sqrt{3}}\langle 0| + i\sqrt{2/3}\,\langle 1|$$

Let $|a\rangle$

$z = \alpha + \beta i$

$z^* = \alpha - \beta i$

$\alpha, \beta \in \mathbb{R}$

- Norma $|\psi\rangle$

$$|\psi| = \sqrt{\langle\psi|\psi\rangle}$$

$$\langle\psi|\psi\rangle =$$

$$|\psi\rangle = 1/\sqrt{2}\,|0\rangle - \frac{i}{\sqrt{2}}\,|1\rangle \qquad |a\rangle = 1/\sqrt{2}\,|0\rangle + 1/\sqrt{2}\,|1\rangle$$

$$|\psi| = ?$$

¿ $|a\rangle$ y $|\psi\rangle$ son diferentes?

$$|\psi| = \sqrt{\langle\psi|\psi\rangle}$$

$$|\psi\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -i \end{pmatrix} = \begin{pmatrix} 1/\sqrt{2} \\ -i/\sqrt{2} \end{pmatrix}$$

$$\langle\psi| = \begin{pmatrix} 1/\sqrt{2} \\ -i/\sqrt{2} \end{pmatrix}^{*T} = \begin{pmatrix} 1/\sqrt{2} & i/\sqrt{2} \end{pmatrix}$$

$$\langle\psi|\psi\rangle = \begin{pmatrix} 1/\sqrt{2} & i/\sqrt{2} \end{pmatrix}\begin{pmatrix} 1/\sqrt{2} \\ -i/\sqrt{2} \end{pmatrix} = (1/\sqrt{2})(1/\sqrt{2}) + \left(\frac{i}{\sqrt{2}}\right)\left(\frac{-i}{\sqrt{2}}\right)$$

$$= 1/2 + \frac{1}{2} = 1 \checkmark$$

$$|\psi| = \sqrt{\langle\psi|\psi\rangle} = \sqrt{1} = 1$$

$$|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{i}{\sqrt{2}}|1\rangle \qquad |a\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

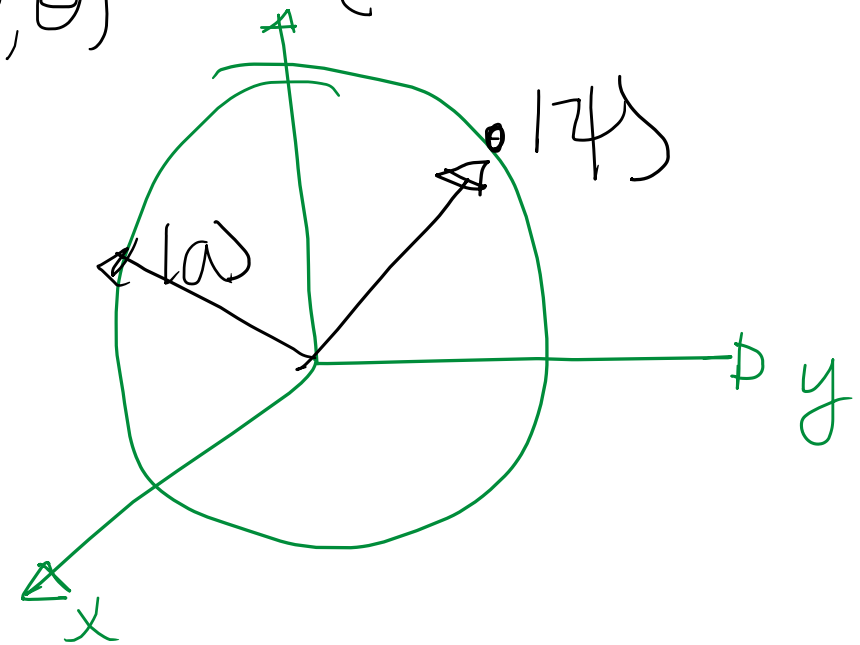
$$|\alpha|^2 + |\beta|^2 = 1$$

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

$$|\psi\rangle = \cos\theta|0\rangle + e^{i\phi}\operatorname{sen}\theta|1\rangle$$

• Esfera de Bloch

$(1, \phi, \theta)$



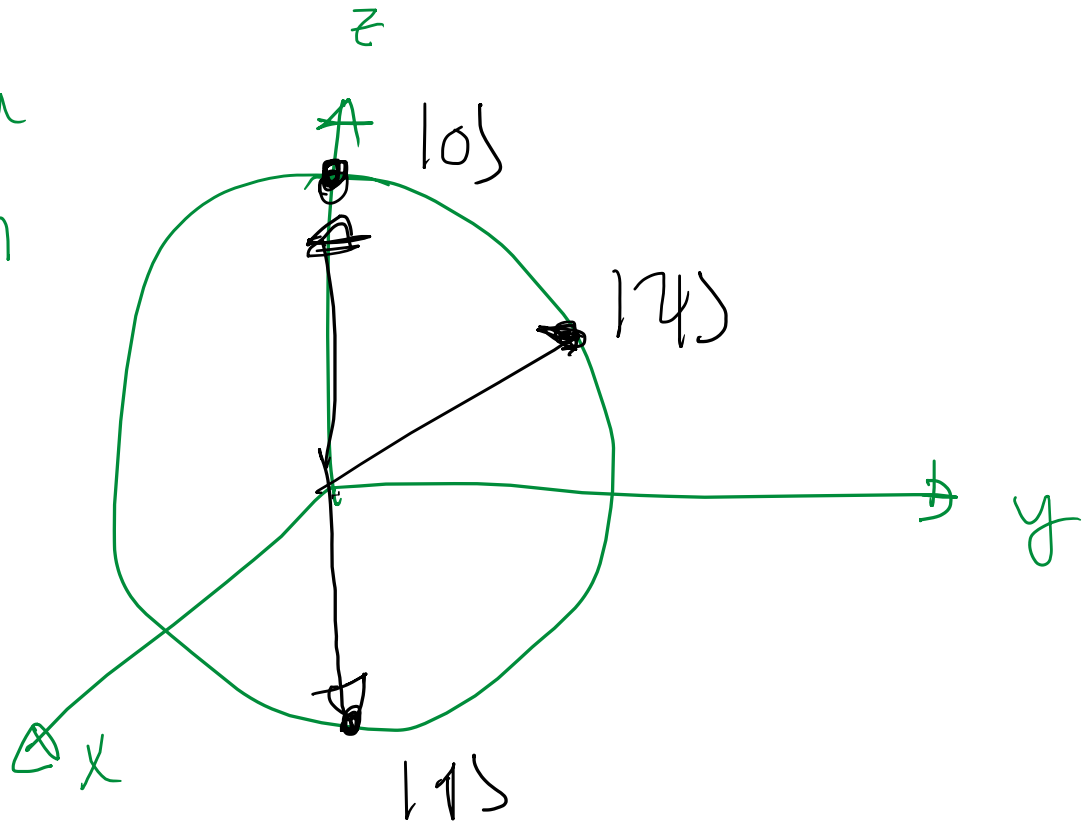
$\alpha, \beta \sim \theta, \phi$

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \longrightarrow \sim|0\rangle + \sim|1\rangle$$

$$|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$|\psi\rangle = \cos\theta\,|0\rangle + e^{i\phi}\,\mathrm{sen}\,\theta\,|1\rangle$$

Esfera Bloch



Herramientas matemáticas

Compuertas cuánticas

$\hat{\sigma}_z = \hat{Z}$:= Matriz de Pauli z

$\hat{\sigma}_z|0\rangle = |0\rangle$

$\hat{\sigma}_z|1\rangle = -|1\rangle$

$\Longleftrightarrow$

$$\hat{\sigma}_z = \begin{pmatrix} 1_1 & 0_2 \\ 0_3 & -1_4 \end{pmatrix}$$

$\langle 0|0\rangle = (1\ 0)\begin{pmatrix}1\\0\end{pmatrix} = 1$

$\langle 0|1\rangle = 0$

$\langle 1|0\rangle = 0$

$\langle 1|1\rangle = 1$

$\langle 0|\hat{\sigma}_z|0\rangle = 1_0$ $\quad \langle 0|\hat{\sigma}_z|1\rangle = 2_0$

$\langle 1|\hat{\sigma}_z|0\rangle = 3_0$ $\quad \langle 1|\hat{\sigma}_z|1\rangle = 4_0$

$$\hat{\sigma}_z|0\rangle = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} (1)(1)+(0)(0) \\ (0)(1)+(-1)(0) \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle$$

$$\hat{\sigma}_z|1\rangle = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0+0 \\ 0+-1 \end{pmatrix} = \begin{pmatrix} 0 \\ -1 \end{pmatrix} = -1\begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$= -1|1\rangle$$

$$= -|1\rangle$$

- Cómo actúan los operadores $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

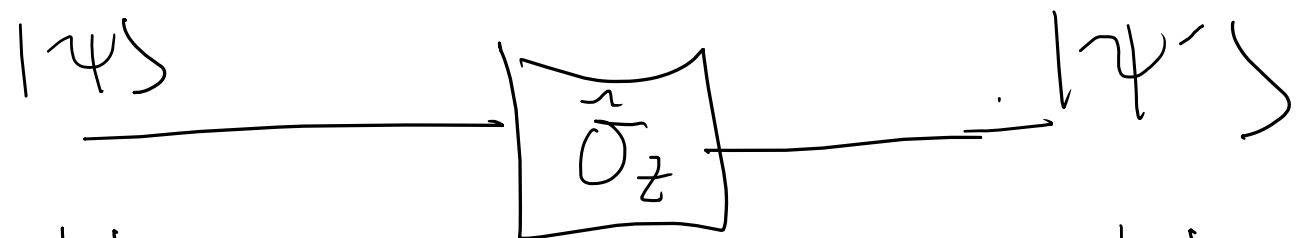
$$\hat{A}|\psi\rangle = \hat{A}(\alpha|0\rangle + \beta|1\rangle)$$

$$= \alpha\hat{A}|0\rangle + \beta\hat{A}|1\rangle$$

$$=$$

$$=$$

- Modelo de circuito



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

$$\hat{\sigma}_z|a\rangle = 1/\sqrt{2}\,\hat{\sigma}_z|0\rangle + 1/\sqrt{2}\,\hat{\sigma}_z|1\rangle$$

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

$$\hat{\sigma}_z|0\rangle = |0\rangle$$

$$\hat{\sigma}_z|1\rangle = -|1\rangle$$

$$\hat{\sigma}_z|a\rangle = 1/\sqrt{2}\,\hat{\sigma}_z|0\rangle + 1/\sqrt{2}\,\hat{\sigma}_z|1\rangle$$

$$= 1/\sqrt{2}\,|0\rangle + 1/\sqrt{2}\,(-|1\rangle)$$

$$= \underline{1/\sqrt{2}\,|0\rangle - 1/\sqrt{2}\,|1\rangle}$$

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

$$\hat{\sigma}_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$\hat{\sigma}_z|a\rangle = \hat{\sigma}_z\left(\begin{pmatrix} 1/\sqrt{2} \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 1/\sqrt{2} \end{pmatrix}\right)$$

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

$$= \begin{pmatrix} 1/\sqrt{2} \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ -1/\sqrt{2} \end{pmatrix} = 1/\sqrt{2}\,|0\rangle - 1/\sqrt{2}\,|1\rangle = \begin{pmatrix} 1/\sqrt{2} \\ -1/\sqrt{2} \end{pmatrix} = |b\rangle$$

* Matrices de Pauli $(\hat{x}, \hat{y}, \hat{z})$

$$\hat{\sigma}_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \qquad \hat{\sigma}_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad \hat{\sigma}_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

$\hat{\sigma}_x |0\rangle =$

$\hat{\sigma}_x |1\rangle =$

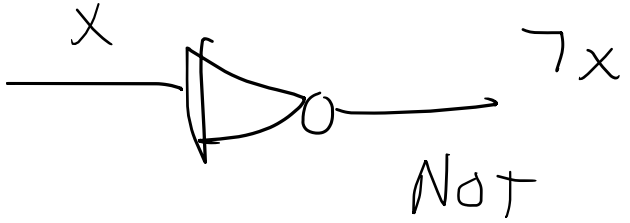
$\hat{\sigma}_y |0\rangle =$

$\hat{\sigma}_y |1\rangle =$

$$\hat{\sigma}_x |0\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}; \quad \hat{\sigma}_x |1\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$$\hat{\sigma}_x |0\rangle = |1\rangle \; ; \; \hat{\sigma}_x |1\rangle = |0\rangle$$

análogo cuántico a



{ AND, NOT, COPY }

XOR, OR, NAND

$$\hat{\sigma}_y|0\rangle = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ i \end{pmatrix} = i\begin{pmatrix} 0 \\ 1 \end{pmatrix} = i|1\rangle$$

$$\hat{\sigma}_y|1\rangle = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} -i \\ 0 \end{pmatrix} = -i\begin{pmatrix} 1 \\ 0 \end{pmatrix} = -i|0\rangle$$

$$\hat{\sigma}_y|0\rangle = i|1\rangle$$

$$\hat{\sigma}_y|1\rangle = -i|0\rangle$$

- Identidad

$$\hat{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\hat{I}|0\rangle = |0\rangle$$

$$\hat{I}|1\rangle = |1\rangle$$

Herramientas matemáticas

Medición de los estados cuánticos

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

α, β := amplitudes de probabilidad (son complejas en general)

$|\alpha|^2$ =: Probabilidad del estado $|\psi\rangle$ de estar en $|0\rangle$

$|\beta|^2$ =: " " " " " " " " $|1\rangle$

$$P_{|\psi\rangle}(|0\rangle) = |\langle 0|\psi\rangle|^2$$

¿cuál es la probabilidad del estado $|\psi\rangle$ de estar en $|0\rangle$?

Regla de Born

$$P_{|\psi\rangle}(|0\rangle) = |\langle 0|\psi\rangle|^2 = |\langle 0|(\alpha|0\rangle + \beta|1\rangle)|^2$$

$$= |\alpha\langle 0|0\rangle + \beta\langle 0|1\rangle|^2$$

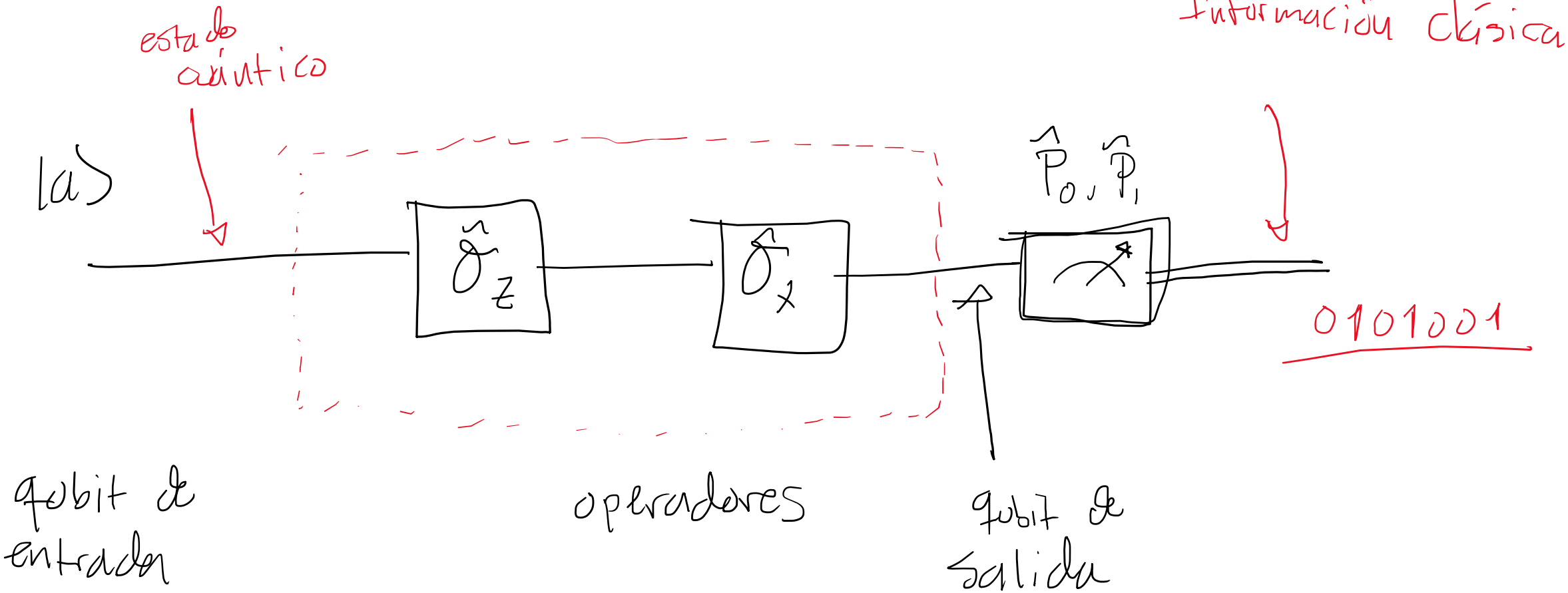
$$= |\alpha(1) + \beta[0]|^2$$

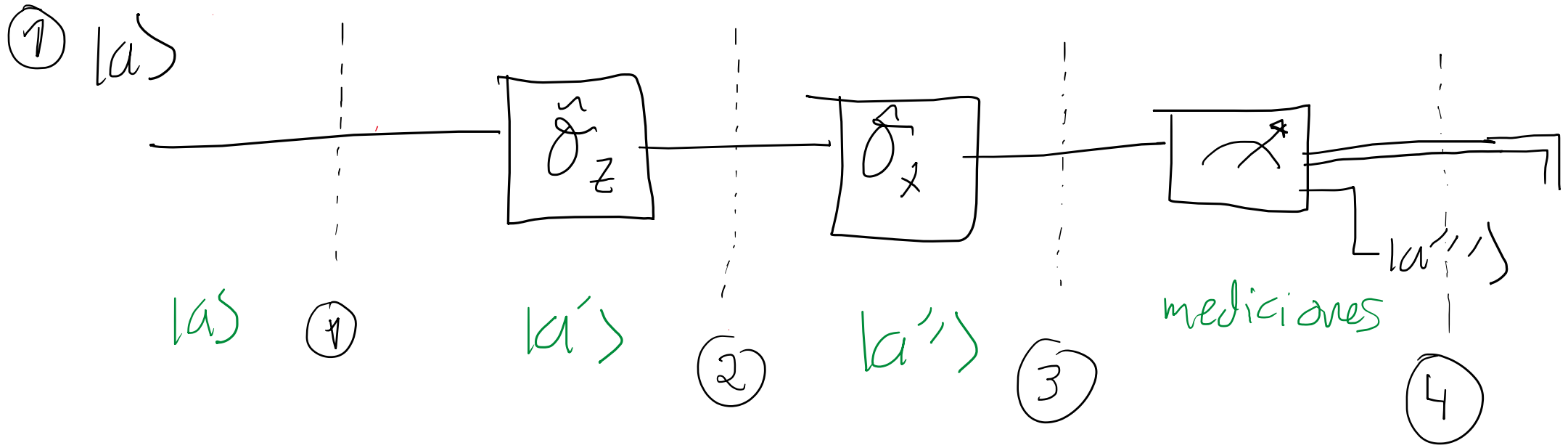
$$= |\alpha|^2$$

$$P_{|\psi\rangle}(|1\rangle) = |\langle 1|\psi\rangle|^2 = |\beta|^2$$

$$|a\rangle = 1/\sqrt{3}\,|0\rangle - i\sqrt{2/3}\,|1\rangle$$

$$\langle a|a\rangle = 1$$





② $\hat{\sigma}_z |a\rangle = 1/\sqrt{3}\,|0\rangle + i\sqrt{2/3}\,|1\rangle = |a'\rangle$

③ $\hat{\sigma}_x |a'\rangle = 1/\sqrt{3}\,|1\rangle + i\sqrt{2/3}\,|0\rangle = |a''\rangle$

④ $P_{|a''\rangle}(|0\rangle)$, $P_{|a''\rangle}(|1\rangle)$

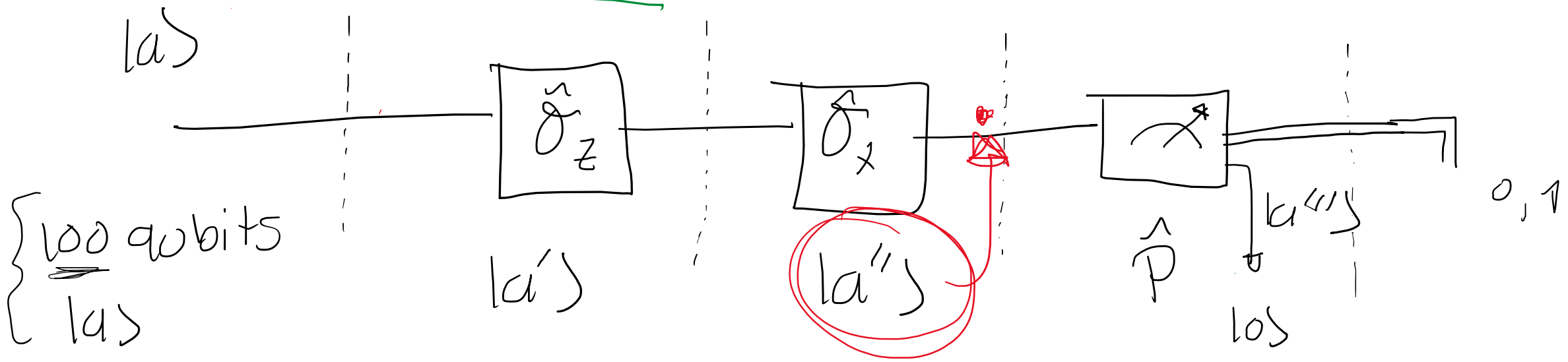
$$P(|0\rangle) = |\langle 0|a''\rangle|^2 = |\langle 0|\left(\tfrac{1}{\sqrt{3}}|1\rangle + i\sqrt{\tfrac{2}{3}}|0\rangle\right)|^2$$

$$= |i\sqrt{\tfrac{2}{3}}|^2 = |i|^2\,|\sqrt{\tfrac{2}{3}}|^2 = \tfrac{2}{3} =$$

$$P(|1\rangle) = |\langle 1|a''\rangle|^2 = |\langle 1|\left(\tfrac{1}{\sqrt{3}}|1\rangle + i\sqrt{\tfrac{2}{3}}|0\rangle\right)|^2$$

$$= |\tfrac{1}{\sqrt{3}}|^2 = \tfrac{1}{3}$$

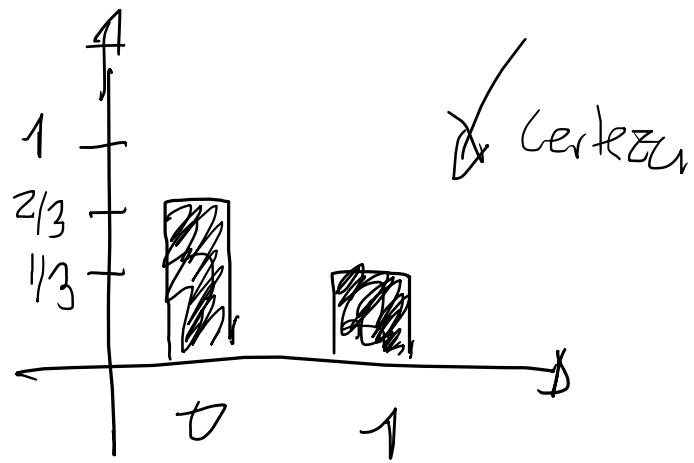
- "colapso del estado después de medir"



Aleatorio

$\hat{P}|a''\rangle = |0\rangle$ ¿?

$\hat{P}|a''\rangle = |1\rangle$



Herramientas matemáticas

Más compuertas de 1 qubit

$$\hat{H} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

$$\hat{P} = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix}$$

apliquen 2 veces $\hat{S}$

$$\hat{S} = \sqrt{\hat{\sigma}_z} = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$

$$\hat{T} = \sqrt{\hat{S}} = \sqrt[4]{\hat{\sigma}_z} = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$$

apliquen 4 veces $\hat{T}$

$$\hat{H}|0\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \left[\begin{pmatrix} 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right]$$

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

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

$$\hat{H}|1\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix} = \frac{1}{\sqrt{2}}\left[\begin{pmatrix} 1 \\ 0 \end{pmatrix} - \begin{pmatrix} 0 \\ 1 \end{pmatrix}\right]$$

$$\hat{H}|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = |-\rangle$$

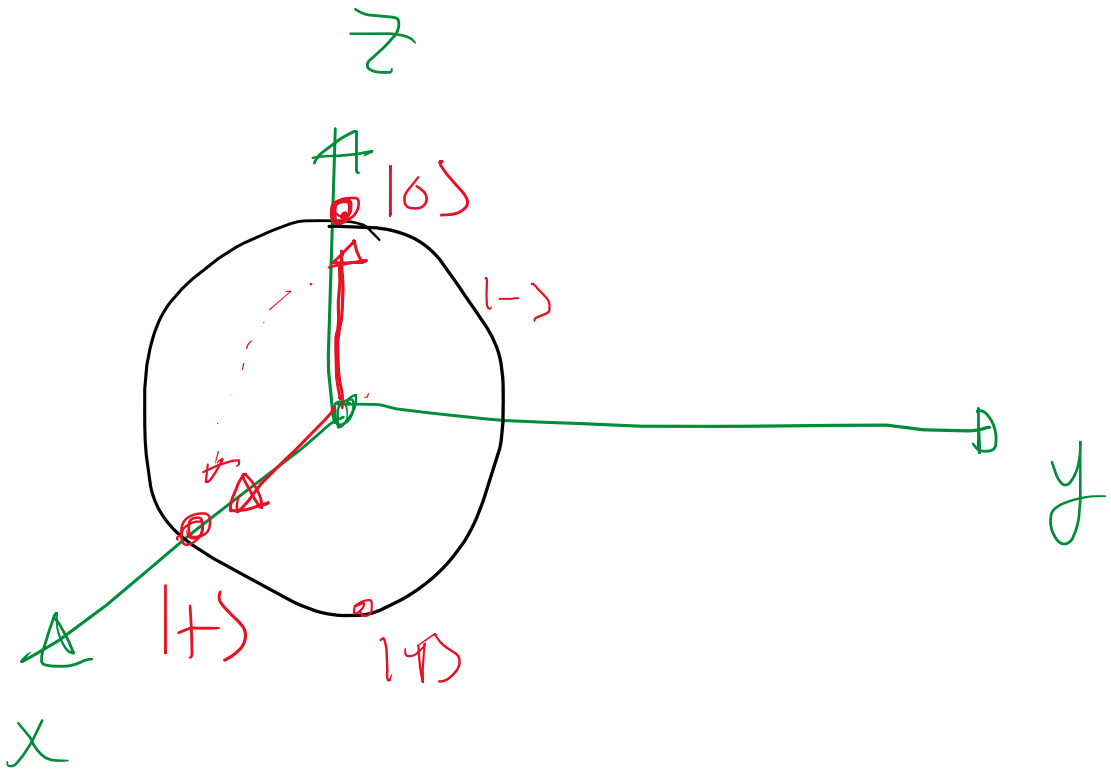
- Base computacional $\{|0\rangle, |1\rangle\}$ $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$
- Base $\hat{\sigma}_x$ $\{|+\rangle, |-\rangle\}$ $|\psi\rangle = \delta|+\rangle + \gamma|-\rangle$

$$\hat{P} = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix}; \quad |\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

$$\hat{P}|\psi\rangle = \hat{P}(\alpha|0\rangle + \beta|1\rangle) = \alpha\hat{P}|0\rangle + \beta\hat{P}|1\rangle$$

$$= \alpha \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \beta \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$\hat{P}|\psi\rangle = \alpha \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \beta \begin{pmatrix} 0 \\ e^{i\theta} \end{pmatrix} = \alpha|0\rangle + \beta e^{i\theta}|1\rangle$$



$$\hat{H}|0\rangle = |+\rangle$$

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

Herramientas matemáticas

Operación daga

- Bra, Ket

$$\langle 0| = \begin{pmatrix} 1 \\ 0 \end{pmatrix}^{*T} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}^{\dagger} = |0\rangle^{\dagger}$$

$$|1\rangle^{\dagger} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}^{\dagger} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}^{*T} = (0 \; 1) = \langle 1|$$

$$\hat{\sigma}_z^{+} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}^{*T} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \hat{\sigma}_z$$

$$\hat{\sigma}_y^{+} = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}^{*T} = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} = \hat{\sigma}_y$$

$$\hat{H}^{+} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}^{*T} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \hat{H}$$

$$\hat{P}^{+} = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix}^{*T} = \begin{pmatrix} 1 & 0 \\ 0 & e^{-i\theta} \end{pmatrix}$$

Herramientas matemáticas

Producto tensorial y compuertas de 2 qubits

- Producto tensorial

$$|a\rangle \otimes |b\rangle = |a\rangle|b\rangle = |ab\rangle$$

Estado de 2 qubits

$$\hat{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad \hat{A} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

$$\hat{I} \otimes \hat{A} = \underset{2\times2}{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}} \otimes \underset{2\times2}{\begin{pmatrix} a & b \\ c & d \end{pmatrix}} = \underset{4\times4}{\begin{pmatrix} 1\begin{pmatrix} a & b \\ c & d \end{pmatrix} & 0\begin{pmatrix} a & b \\ c & d \end{pmatrix} \\ 0\begin{pmatrix} a & b \\ c & d \end{pmatrix} & 1\begin{pmatrix} a & b \\ c & d \end{pmatrix} \end{pmatrix}}$$

$$\hat{I} \otimes \hat{A} = \begin{pmatrix} a & b & 0 & 0 \\ c & d & 0 & 0 \\ 0 & 0 & a & b \\ 0 & 0 & c & d \end{pmatrix}$$

$$\hat{\sigma}_z \otimes \hat{\sigma}_x = (\quad)_{4\times 1}$$

$$\hat{\sigma}_x \otimes \hat{\sigma}_z$$

$$\hat{\sigma}_z \otimes \hat{\sigma}_y$$

$$|0\rangle \otimes |0\rangle = \underset{2\times 1}{\begin{pmatrix} 1 \\ 0 \end{pmatrix}} \otimes \underset{2\times 1}{\begin{pmatrix} 1 \\ 0 \end{pmatrix}} = \begin{pmatrix} 1\begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ 0\begin{pmatrix} 1 \\ 0 \end{pmatrix} \end{pmatrix} = \underset{4\times 1}{\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}}$$

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

$$|\psi\rangle \otimes |1\rangle = (\alpha|0\rangle + \beta|1\rangle) \otimes |1\rangle$$

$$= \alpha|0\rangle \otimes |1\rangle + \beta|1\rangle \otimes |1\rangle$$

$$= \alpha \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} + \beta \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$|\psi\rangle|1\rangle = \alpha \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} + \beta \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \alpha|01\rangle + \beta|11\rangle$$

$d^2 = 4$

- Base computacional de 2 qubits $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$

$$\begin{pmatrix}1\\0\\0\\0\end{pmatrix} \quad \begin{pmatrix}0\\1\\0\\0\end{pmatrix} \quad \begin{pmatrix}0\\0\\1\\0\end{pmatrix} \quad \begin{pmatrix}0\\0\\0\\1\end{pmatrix}$$

* Producto punto con 2 qubits

$$|A\rangle = \alpha|01\rangle + \beta|11\rangle \quad , \quad |B\rangle = \delta|01\rangle$$

$$\langle A| = |A\rangle^{\dagger} = (\alpha|01\rangle + \beta|11\rangle)^{*T} = (\alpha^*\langle 01| + \beta^*\langle 11|)$$

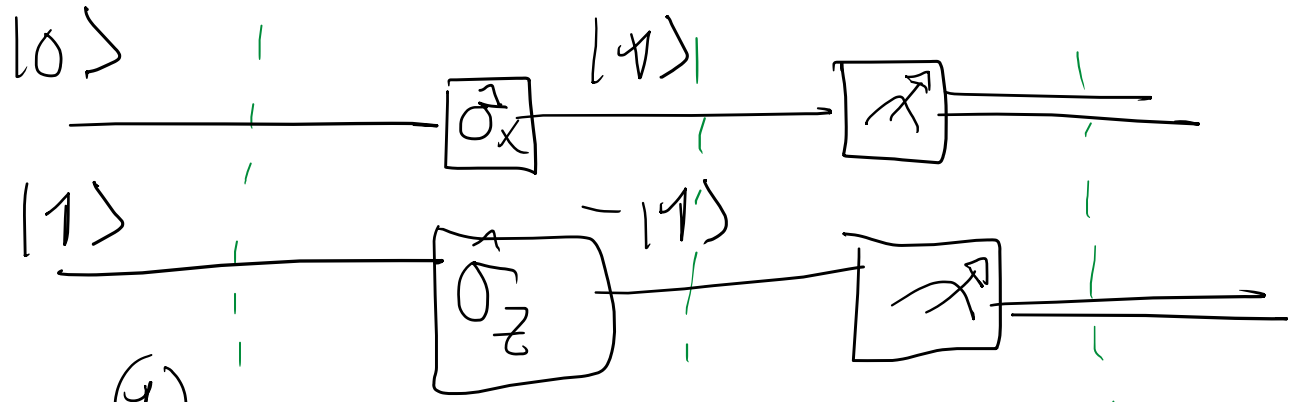
$$\langle A|B\rangle = (\alpha^*\langle 01| + \beta^*\langle 11|)(\delta|01\rangle)$$

$$\langle A|B\rangle = (\alpha^* \langle 0+| + \beta^* \langle 1+|)(\delta|0+\rangle$$

$$= \alpha^* \delta \langle 0+|0+\rangle + \beta^* \delta \langle 1+|0+\rangle$$

$$= \alpha^* \delta |1\rangle + \cancel{\beta^* \delta |0\rangle}$$

$$= \underline{\alpha^* \delta |}$$



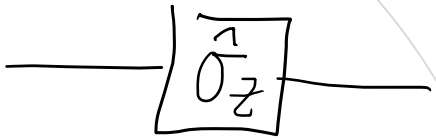
1

$|0+\rangle$

2 $-|--\rangle$

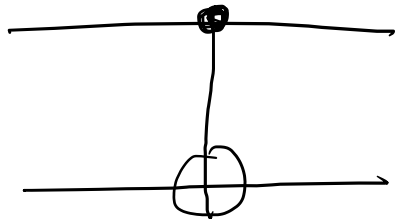
3 Mediciones

Herramientas matemáticas



Compuertas de 2 o más qubits

$$\text{C-NOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$



$$\text{CNOT}\,|00\rangle = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = |00\rangle$$

$$\mathrm{CNOT}\,|01\rangle = \begin{pmatrix} 1&0&0&0 \\ 0&1&0&0 \\ 0&0&0&1 \\ 0&0&1&0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = |01\rangle$$

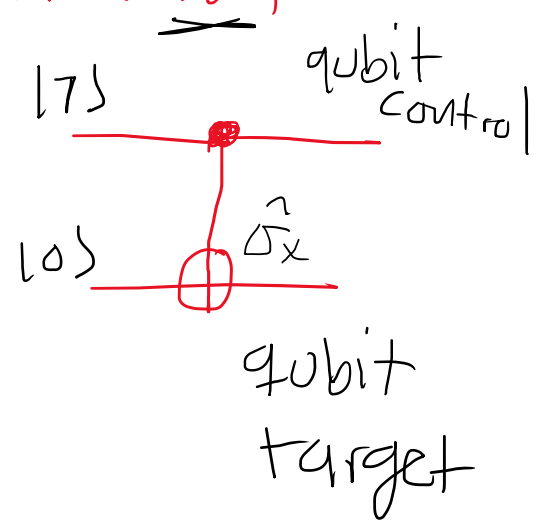
$$\mathrm{CNOT}\,|10\rangle = \begin{pmatrix} 1&0&0&0 \\ 0&1&0&0 \\ 0&0&0&1 \\ 0&0&1&0 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = |11\rangle$$

$$\mathrm{CNOT}\,|11\rangle = \begin{pmatrix} 1&0&0&0 \\ 0&1&0&0 \\ 0&0&0&1 \\ 0&0&1&0 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = |10\rangle$$

$$CNOT|00\rangle = |00\rangle \qquad CNOT|01\rangle = |01\rangle$$

$$CNOT|10\rangle = |11\rangle \qquad CNOT|11\rangle = |10\rangle$$

control-not

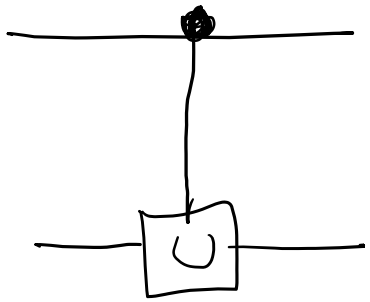


$$C\text{-}P = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\theta} \end{pmatrix}$$

$$C\text{-}P|00\rangle = |00\rangle$$

$$C\text{-}P|10\rangle = |10\rangle \qquad CP|11\rangle = e^{i\theta}|11\rangle$$

C - U



$$CU|00\rangle = |00\rangle$$

$$CU|01\rangle = |01\rangle$$

$$CU|10\rangle = |1\rangle \otimes \hat{U}|0\rangle$$

$$CU|11\rangle = |1\rangle \otimes \hat{U}|1\rangle$$

Enredamiento cuántico

Estados productos y estados enredados

$$|00\rangle = |0\rangle \otimes |0\rangle$$

estado de 2 qubits

estado producto de dos estados de 1 qubit

$$|\psi_1\rangle = \alpha_1 |0\rangle + \beta_1 |1\rangle \qquad |\psi_2\rangle = \alpha_2 |0\rangle + \beta_2 |1\rangle$$

$$|\psi_1\rangle \otimes |\psi_2\rangle = \begin{pmatrix} \alpha_1 \\ \beta_1 \end{pmatrix} \otimes \begin{pmatrix} \alpha_2 \\ \beta_2 \end{pmatrix} = \begin{pmatrix} \alpha_1\alpha_2 \\ \alpha_1\beta_2 \\ \beta_1\alpha_2 \\ \beta_1\beta_2 \end{pmatrix}$$

$$|\phi\rangle_2 = C_0|00\rangle + C_1|01\rangle + C_2|10\rangle + C_3|11\rangle$$

$C_0 C_3 = C_1 C_2$ Estados producto $|C_0|^2 + |C_1|^2 + |C_2|^2 + |C_3|^2 = 1$

$$|\beta_{00}\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right) \quad \checkmark$$

$$= \frac{1}{\sqrt{2}}|00\rangle + 0|01\rangle + 0|10\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

$$\left(\frac{1}{\sqrt{2}}\right)\left(\frac{1}{\sqrt{2}}\right) = (0)(0) \quad \nabla \underset{0}{} \text{ contradicción}$$

$\therefore$ $|\beta_{00}\rangle$ es un estado enredado

$$|\beta_{00}\rangle \neq |\phi_1\rangle \otimes |\phi_2\rangle$$

Sistema (1) $|\psi_1\rangle$ — correlaciones en las propiedades del sistema global — $|\psi_2\rangle$ Sistema (2)

¿Cómo es el estado global de ambos sistemas?

a) $|\psi_1\rangle \otimes |\psi_2\rangle$

b) $\boxed{|B_{00}\rangle} \neq |\psi_1\rangle \otimes |\psi_2\rangle$

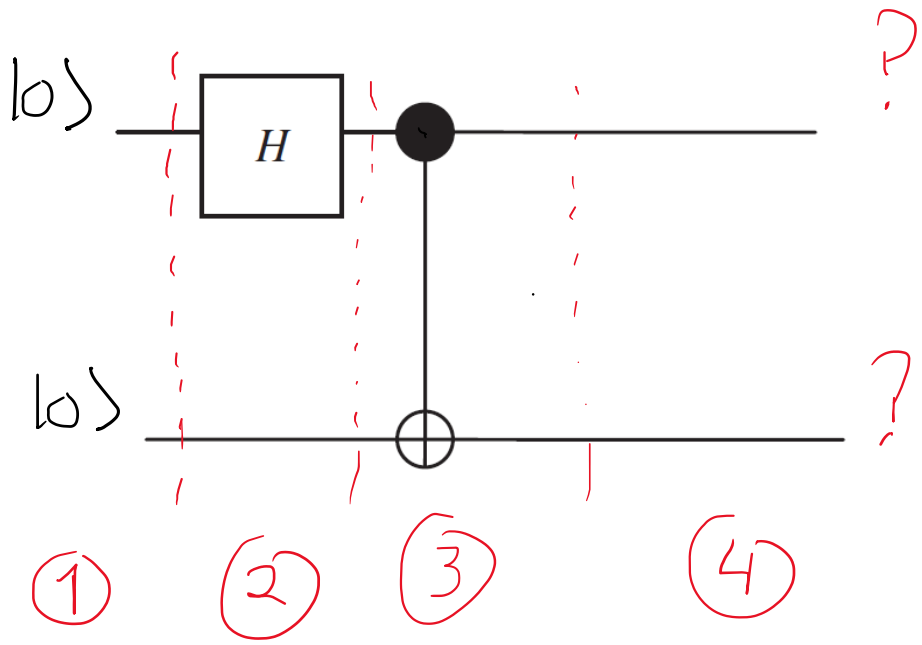
Alice $|\psi\rangle$ → Bob $|0\rangle \dots |\psi\rangle$

Tierra — Luna

Sí, alg. Tel. Cuant.

Enredamiento cuántico

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



① $|0\rangle \otimes |0\rangle = |00\rangle$ Estados iniciales

② $\underset{1}{\hat{H}} \otimes \underset{2}{\hat{I}} |00\rangle_{1\,2} = \hat{H} \otimes \hat{I} |0\rangle \otimes |0\rangle = \hat{H}|0\rangle \otimes \hat{I}|0\rangle$ Preparación del estado

(2) $\hat{H}_1 \otimes \hat{I}_2 |00\rangle = \hat{H} \otimes I |0\rangle \otimes |0\rangle = \hat{H}|0\rangle \otimes \hat{I}|0\rangle$

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

q control — q target

$= \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)$

(3) $CNOT \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) = \frac{1}{\sqrt{2}}(CNOT|00\rangle + CNOT|10\rangle)$

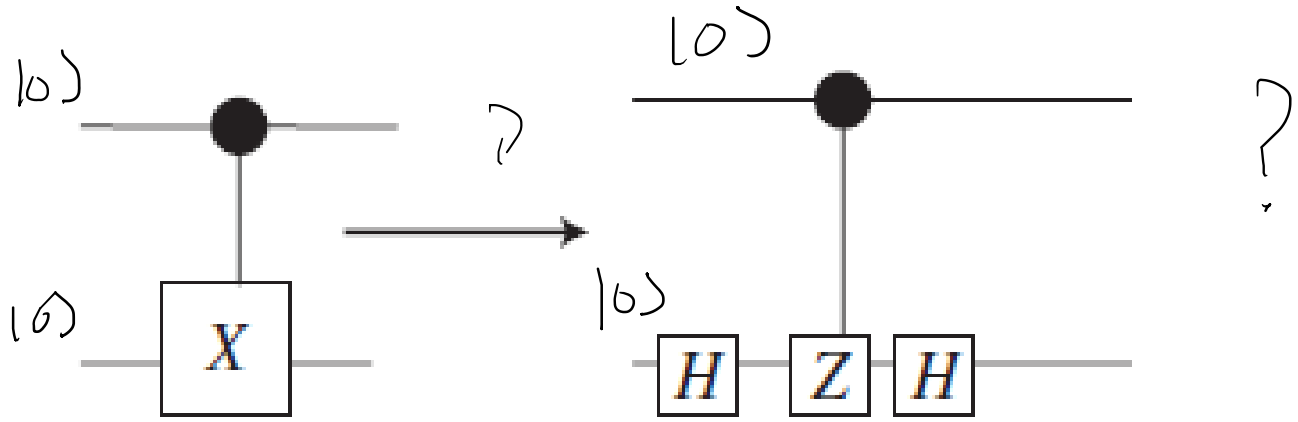
Computo cuântico

$= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = |\beta_{00}\rangle$

Estado de Bell

Herramientas matemáticas

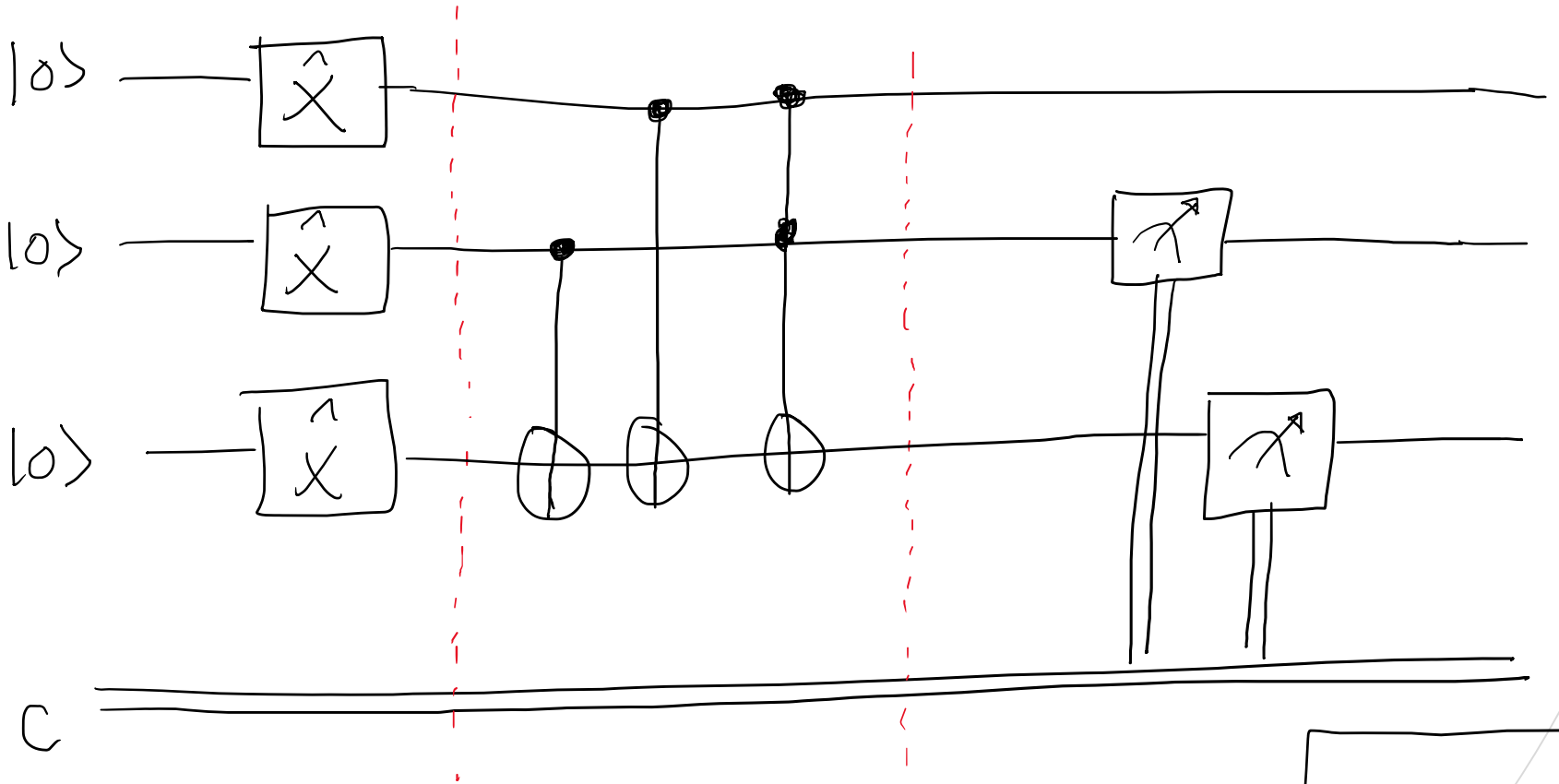
Descomposición de compuertas



CNOT

$\hat{H} - C - \hat{Z} - \hat{H}$

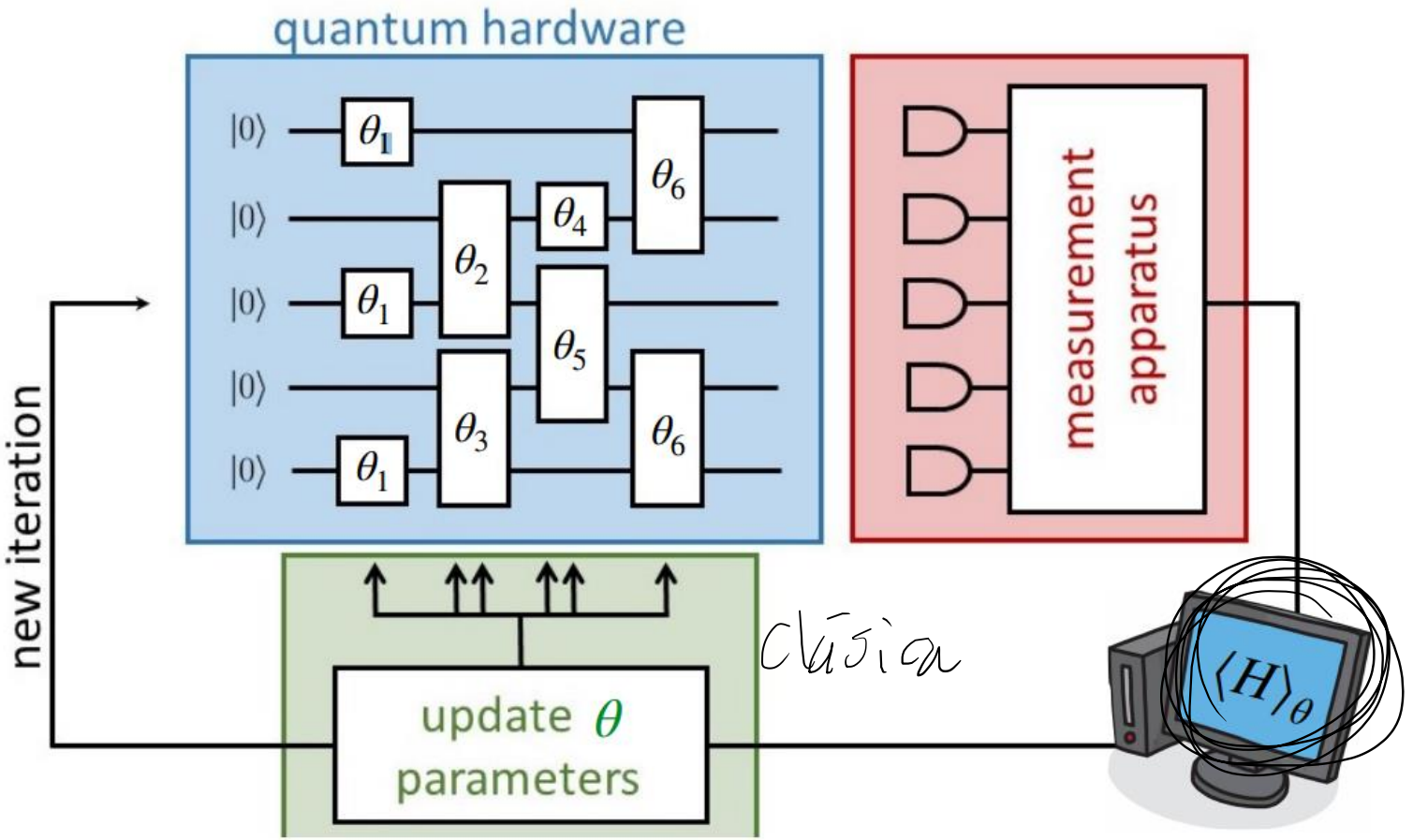
Algoritmo de suma de 3 bits



Toffoli C-C-Not
compuerta de 3
qubits $2^3 = 8$

Aplicaciones (variational quantum eigensolver)

Peruzzo et al, Nat. Comm. '13



Quantum circuit as a variational ansatz

Herramientas matemáticas

Producto exterior

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$$\langle 0| = (1, 0)$$

$$|0\rangle\langle 0| = \begin{pmatrix} 1 \\ 0 \end{pmatrix}_{2\times 1} (1\ 0)_{1\times 2} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}_{2\times 2}$$

← operadores (compuerta)

$$|0\rangle\langle 1| = \begin{pmatrix} 1 \\ 0 \end{pmatrix} (0\ 1) = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

$$|1\rangle\langle 0| = \begin{pmatrix} 0 \\ 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$$

$$|1\rangle\langle 1| = \begin{pmatrix} 0 \\ 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

$$|00\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

$$|00\rangle\langle 01| = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Herramientas matemáticas

Proyección

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

- Proyector del estado cero $\hat{P}_0 = |0\rangle\langle 0|$

$$\hat{P}_0|\psi\rangle = \alpha\hat{P}_0|0\rangle + \beta\hat{P}_0|1\rangle$$

$$= \alpha(|0\rangle\langle 0|)|0\rangle + \beta(|0\rangle\langle 0|)|1\rangle$$

$$\hat{P}_0 |\psi\rangle = \alpha \hat{P}_0 |0\rangle + \beta \hat{P}_0 |1\rangle$$

$$= \alpha (|0\rangle\langle 0|)|0\rangle + \beta (|0\rangle\langle 0|)|1\rangle$$

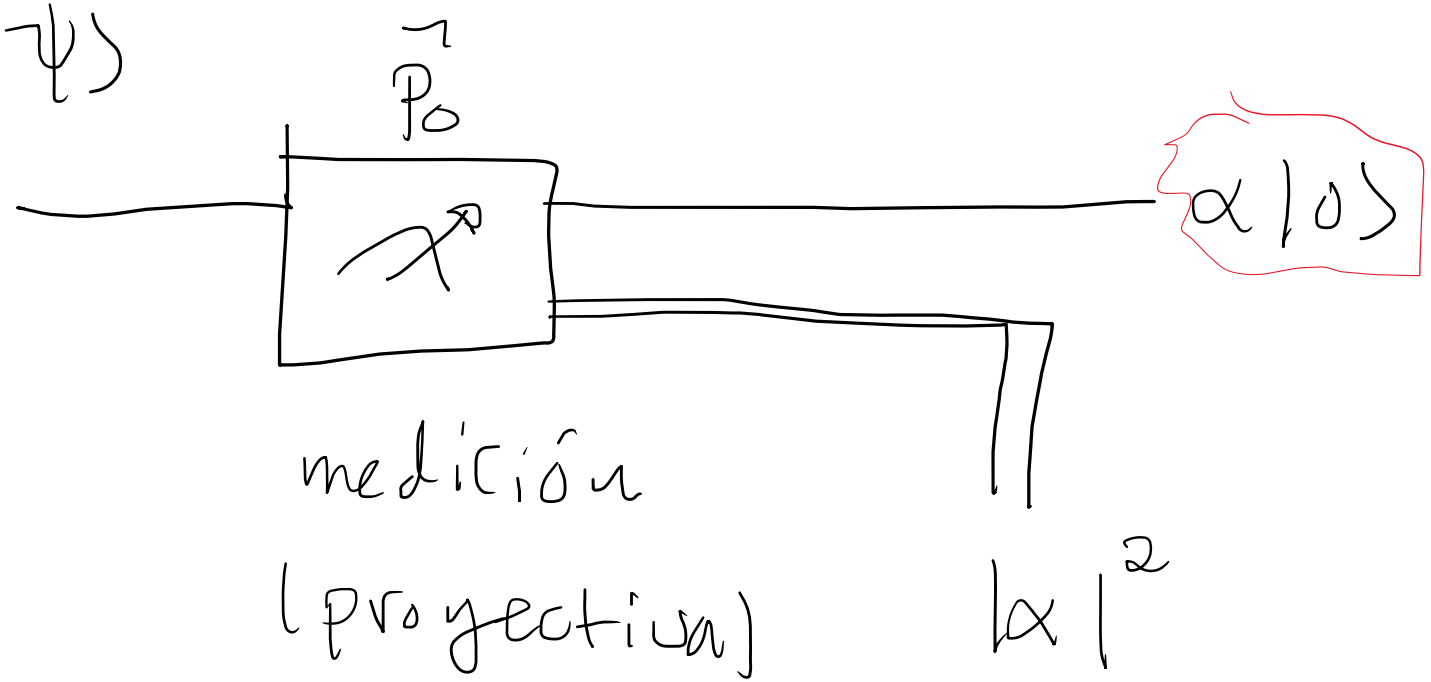
$$= \alpha |0\rangle \langle 0|0\rangle + \beta |0\rangle\langle 0|1\rangle$$

$$= \alpha |0\rangle (1) + \cancel{\beta |0\rangle (0)}$$

$$= \alpha |0\rangle$$

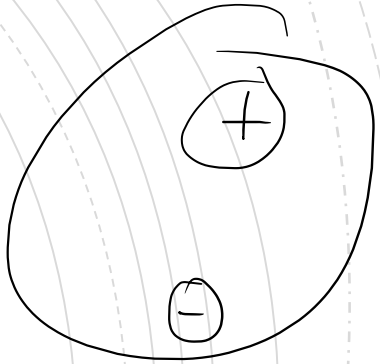
$$\hat{P}_1 = |1\rangle\langle 1| \quad ; \quad \hat{P}_1 |\psi\rangle = \beta |1\rangle$$

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$



$$\hat{P}_0|\psi\rangle = \alpha|0\rangle$$

Algoritmo de teleportación cuántica



Correlaciones

clásica

anticorrelación

color del calcetín

correlación

- Enredamiento es un tipo de correlación cuántica (Teorema de Bell)

$H^{\uparrow}$: 1S' spin $\uparrow\downarrow$

Algoritmo de teleportación cuántica

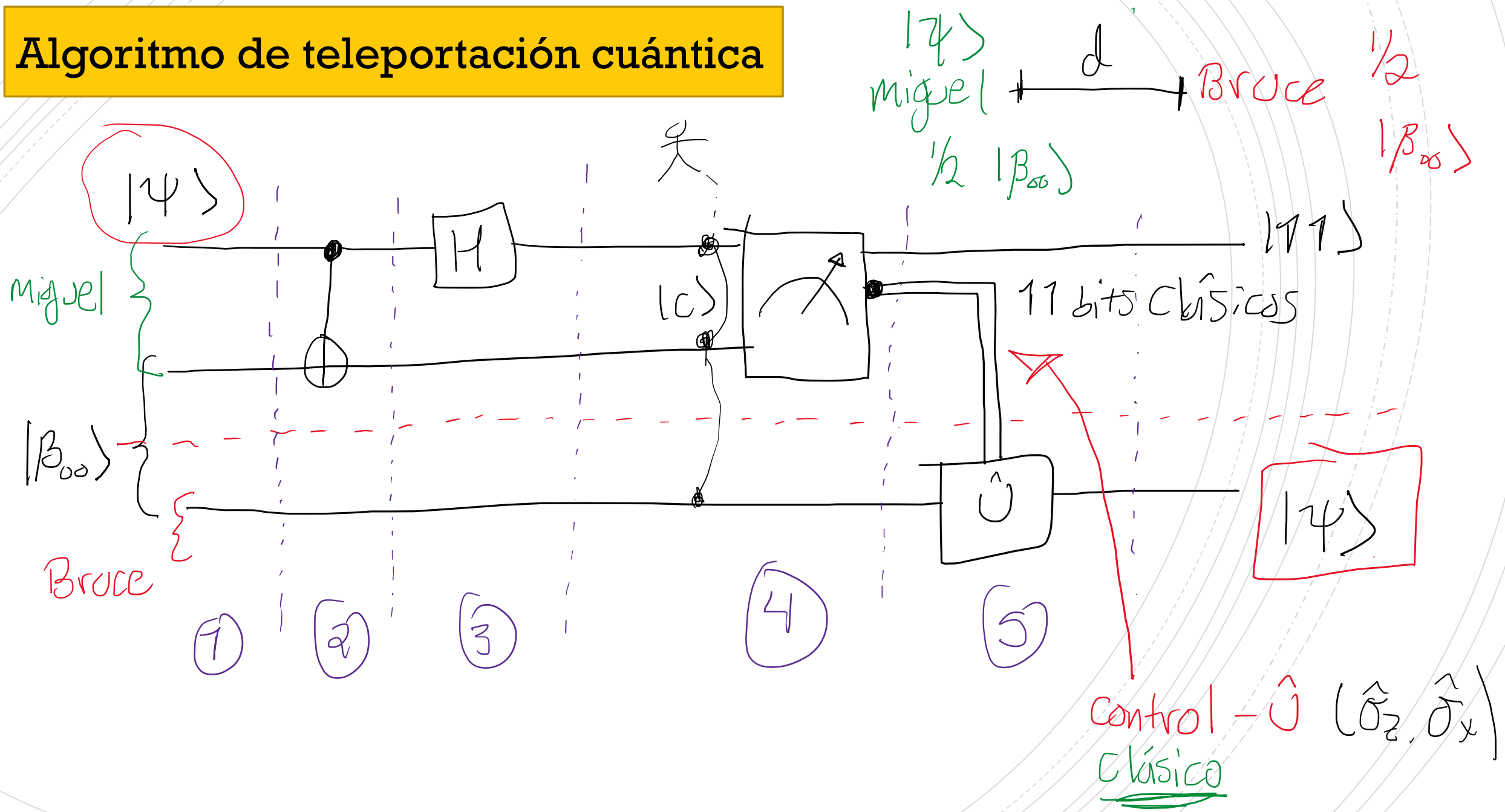
$O\ |\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

Problema

$|\beta_{08}\rangle \neq |\phi\rangle_1 \otimes |\phi_2\rangle$

$|\beta_{00}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$

Algoritmo de teleportación cuántica



$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad ; \quad |\beta_{00}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

(1)

$$|\psi\rangle \otimes |\beta_{00}\rangle = (\alpha|0\rangle + \beta|1\rangle) \otimes \left(\frac{|00\rangle + |11\rangle}{\sqrt{2}}\right)$$

3 qubits

$\{|000\rangle \cdots |111\rangle\}$

$2^3 = 8$

$$= \frac{\alpha(|000\rangle + |011\rangle) + \beta(|100\rangle + |111\rangle)}{\sqrt{2}} = |a\rangle$$

(2)

$$CNOT \otimes \hat{I}\left(|\psi\rangle|\beta_{00}\rangle\right) =$$

$$CNOT \otimes \hat{I}\left(|\psi\rangle|\beta_{00}\rangle\right) = \frac{\alpha\left(CNOT|000\rangle + CNOT|011\rangle\right) + \beta\left(CNOT|100\rangle + CNOT|111\rangle\right)}{\sqrt{2}}$$

$$= \frac{\alpha\left(|000\rangle + |011\rangle\right) + \beta\left(|110\rangle + |101\rangle\right)}{\sqrt{2}} = |b\rangle$$

(3) $$\hat{H} \otimes \hat{I} \otimes \hat{I}|b\rangle = \frac{\alpha\left(\hat{H}_1|000\rangle + \hat{H}_1|011\rangle\right) + \beta\left(\hat{H}_1|110\rangle + \hat{H}_1|101\rangle\right)}{\sqrt{2}}$$

$$\vdots$$

$$|c\rangle = \alpha\frac{(|0\rangle+|1\rangle)}{\sqrt{2}} \otimes \frac{(|00\rangle+|11\rangle)}{\sqrt{2}} + \beta\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right) \otimes \frac{(|10\rangle+|01\rangle)}{\sqrt{2}}$$

(4) Medición

Base Comp. $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ — P — $(|11\rangle)$

$$|c\rangle = \frac{1}{2}\Big[|00\rangle(\alpha|0\rangle + \beta|1\rangle) + |01\rangle(\alpha|1\rangle + \beta|0\rangle) + |10\rangle(\alpha|0\rangle - \beta|1\rangle) + |11\rangle(\alpha|1\rangle - \beta|0\rangle)\Big]$$

caso (1)

- Después de medir, el estado que me sale es $|11\rangle$

$\Rightarrow$) El estado del sistema completo (miguel-Bruce)

$$|\Psi\rangle = |11\rangle \otimes (\alpha|1\rangle - \beta|0\rangle) \quad :=\ \text{Estado Producto!}$$

miguel — Bruce — $|\Psi\rangle$

(5) El resultado de la medición fue $|1\rangle$, se lo mando clásicamente a Bruce

(*) NOTA

$\Rightarrow$ Aplicar $\hat{\sigma}_z$ y $\hat{\sigma}_x$ a tu estado

$$\hat{\sigma}_z |\psi'\rangle = \hat{\sigma}_z (\alpha|1\rangle - \beta|0\rangle) = -\alpha|1\rangle - \beta|0\rangle$$

$$\hat{\sigma}_x (-\alpha|1\rangle - \beta|0\rangle) = -\alpha|0\rangle - \beta|1\rangle$$

$$= -1(\alpha|0\rangle + \beta|1\rangle) = \underbrace{(-1)}_{\text{Fase global}} |\psi\rangle$$

Teorema de no clonación

- No-go theorems
  - i) No signaling
  - ii) No cloning
  - iii) No deleting

- Supongamos que $\hat{U}_{cl}(|\psi\rangle + |\phi\rangle)|0\rangle = \hat{U}_{cl}|\psi\rangle|0\rangle + \hat{U}_{cl}|\phi\rangle|0\rangle$

$$= |\psi\rangle|\psi\rangle + |\phi\rangle|\phi\rangle = a$$

$$\hat{U}_{cl}(|\psi\rangle + |\phi\rangle)|0\rangle = (|\psi\rangle + |\phi\rangle)(|\psi\rangle + |\phi\rangle)$$

$$= |\psi\rangle|\psi\rangle + |\psi\rangle|\phi\rangle + |\phi\rangle|\psi\rangle + |\phi\rangle|\phi\rangle = b$$

$a \neq b \quad \forall$

Componentes de qiskit

Qiskit aer → simulator q.cx(0,1)

Qiskit

aqua

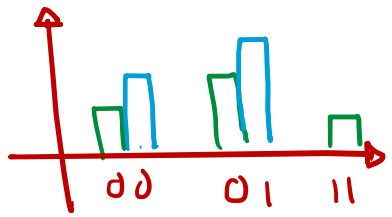
↕

Applications

Qiskit

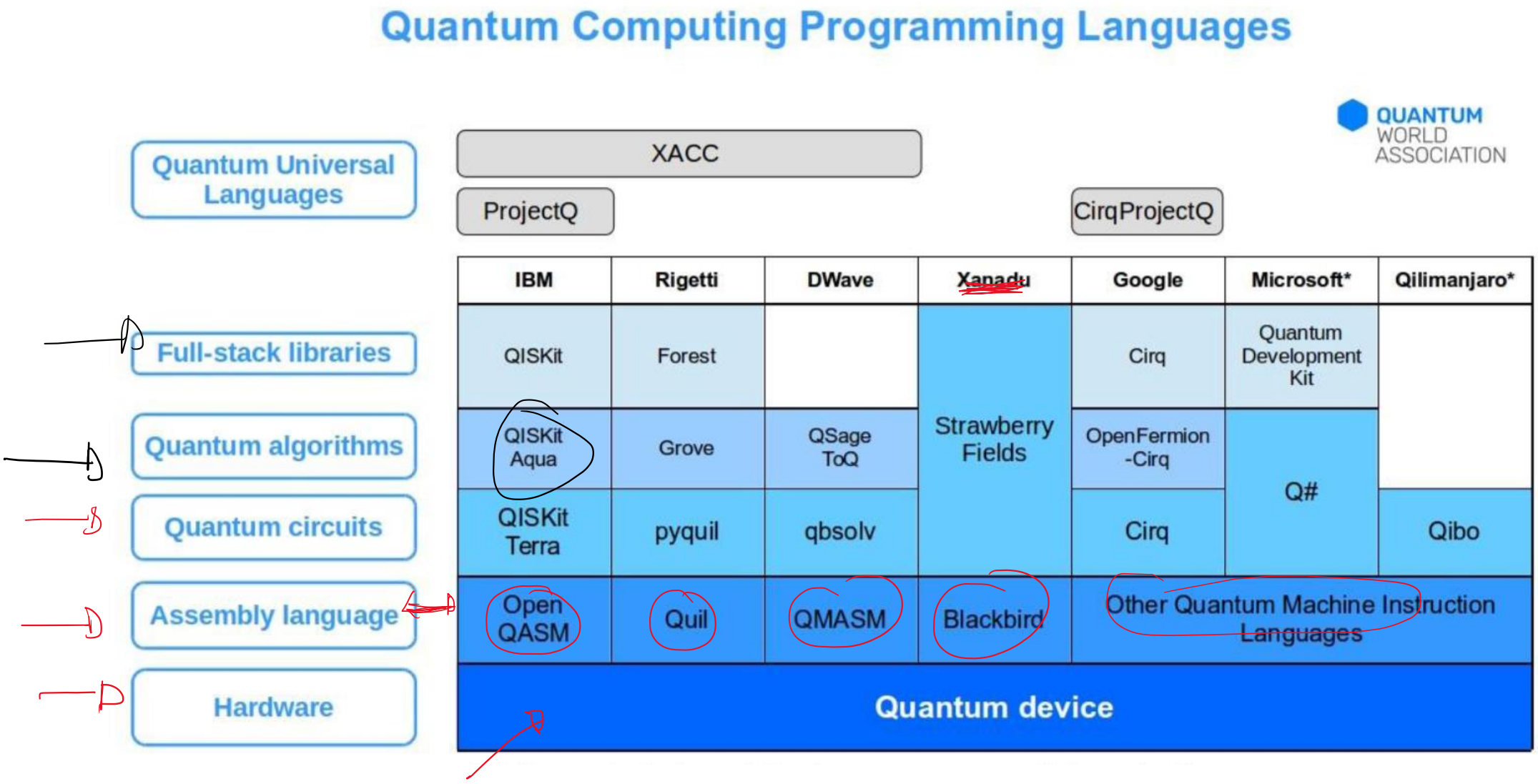
Qiskit ignis

error and optimization



Qiskit terra

Niveles de lenguaje computacional



Algoritmo de Shor

* Problema: Sea $N = pq$, encontrar p y q ; $N, p, q \in \mathbb{Z}$

① Aritmética modular

$5/3 \rightarrow 3\overline{)5}$ (1) cociente, (2) residuo

congruente

$5 \equiv 2 \pmod 3$

5 es congruente a 2 (mod 3)

② módulo 3

$x = 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ \ldots$

$x \equiv 1\ 2\ 0\ 1\ 2\ 0\ 1\ 2\ 0 \pmod 3$

- Note que si $x \equiv 0 \pmod 3 \Rightarrow x$ es un múltiplo de 3

  $x \equiv 1 \pmod 3 \Rightarrow x$ es múltiplo de $3+1$

- De forma general $\boxed{x \equiv y \pmod 3 \Rightarrow x = 3k + y}$ $k \in \mathbb{Z}$

$$
\begin{aligned}
4^0 &= 1 &&= 0 \times 7 + 1 && \equiv 1 \pmod 7 \\
4^1 &= 4 &&= 0 \times 7 + 4 && \equiv 4 \pmod 7 \\
4^2 &= 16 &&= 2 \times 7 + 2 && \equiv 2 \pmod 7 \\
4^3 &= 64 &&= 9 \times 7 + 1 && \equiv 1 \pmod 7 \\
4^4 &= 256 &&= 36 \times 7 + 4 && \equiv 4 \pmod 7 \\
4^5 &= 1024 &&= 146 \times 7 + 2 && \equiv 2 \pmod 7 \\
&\vdots
\end{aligned}
$$

1
4
2
.

El orden de esta función $\boxed{4^k \equiv 1 \pmod 7}$ es $\boxed{r = 3}$

Algoritmo de Shor

$N = 15$ → 1111 (4 bits) — LLLL (L)

1. Escoge $a < N$ tal que a es coprimo de N

2. Calcula el "orden" r de la función $a^r \pmod N$
   con r el más pequeño que cumpla $a^r \equiv 1 \pmod N$

   ↑ La computadora cuántica solo sirve para calcular el orden r

3. If r es par
   - $x \equiv a^{r/2} \pmod N$
   - If $x+1 \not\equiv 0 \pmod N$
     - $\{p, q\}$ está en al menos (4) $MCD(x+1, N)$, $MCD(x-1, N)$

   else: busca otra a

* Ejemplo $N = 15 \rightarrow 1111$ (binario)

① $a = 13$

② Encuentra el periodo de la función $13^r \pmod{15}$

x	=	0	1	2	3	4	5	6	7	...
$13^x \pmod{15}$	=	1	13	4	7	1	13	4	7	...

$\Rightarrow 13^4 \equiv 1 \pmod{15}$; $r = 4$ orden

③ $x = a^{r/2} \pmod{N} = 13^{4/2} \pmod{15} = 4 \pmod{15}$

$x + 1 = 4 + 1 = 5 \equiv 5 \pmod{15} \not\equiv 0 \pmod{15}$

4

$N = 15$

$MCD(x+1, N) = MCD(4+1, 15) = 5$

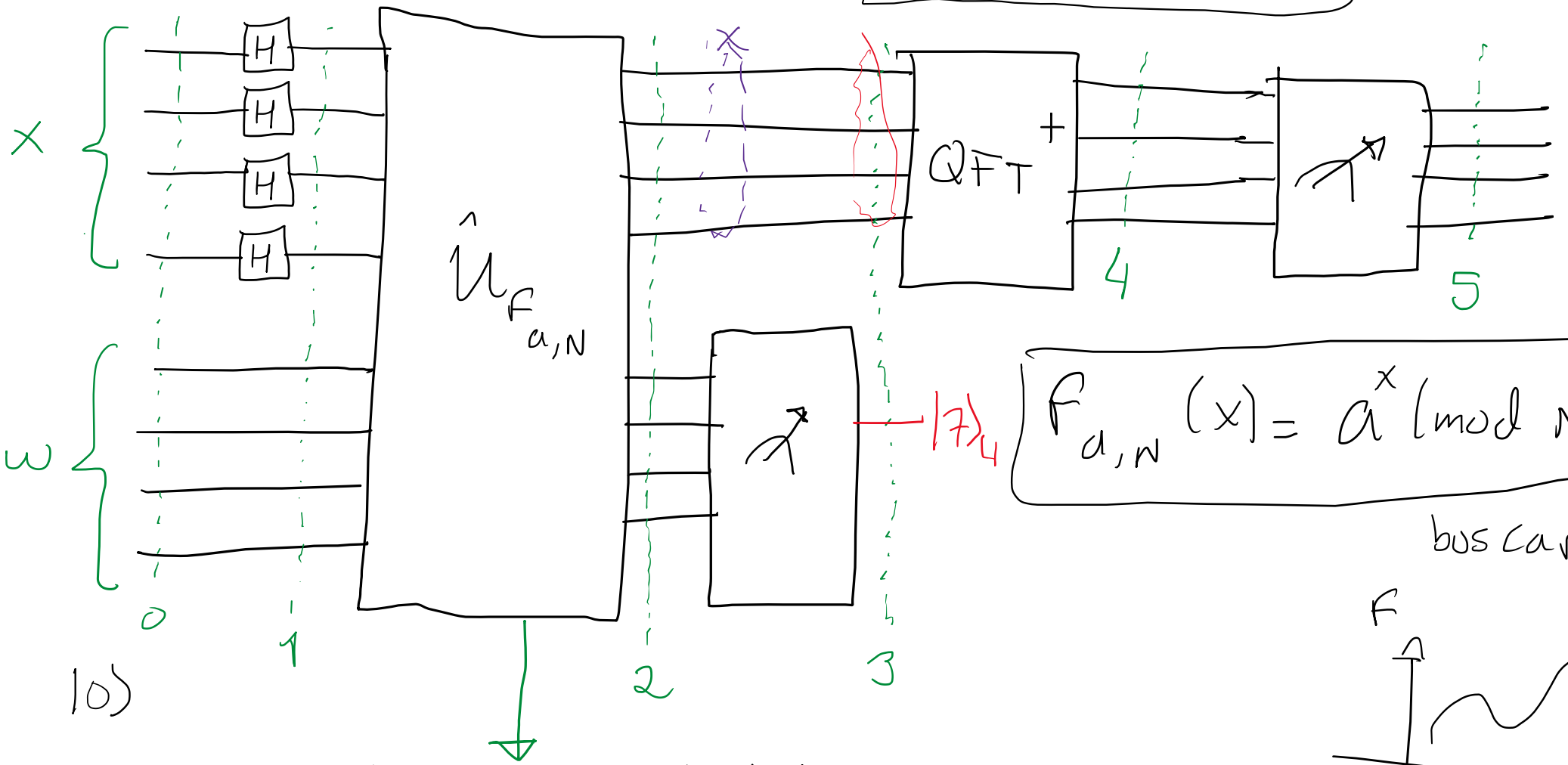
$MCD(x-1, N) = MCD(4-1, 15) = 3$

$\therefore$ 5 y/o 3 son factores de $N = 15$

Clásica

⊛ Implementación cuántica

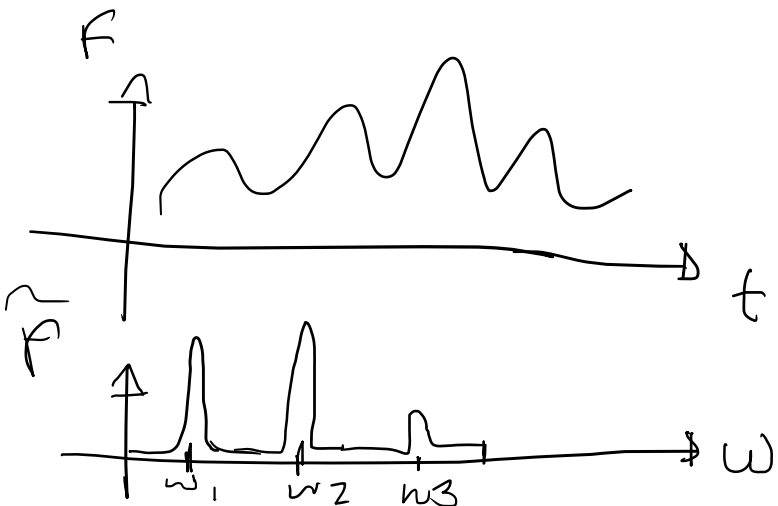
$N = 15 = 1111$



$$F_{a,N}(x) = a^x \pmod N$$

buscar el orden r

$$|x\rangle|w\rangle \longrightarrow |x\rangle|w \oplus F_{a,N}(x)\rangle$$



① $|0\rangle^{\otimes 4}|0\rangle^{\otimes 4}$; $|0\rangle^{\otimes 4} = |0\rangle\otimes|0\rangle\otimes|0\rangle\otimes|0\rangle = |0000\rangle$ $2^4 = 16$

① $(\hat{H}^{\otimes 4}|0\rangle)|0\rangle^{\otimes 4} = 1/4\left(|1\rangle_4 + |2\rangle_4 + \dots |15\rangle_4\right)|0\rangle_4$

$|0\rangle_4 +$

$|15\rangle_4 = |1111\rangle$

② $\frac{1}{4}\left(|0\rangle_4 |0\oplus 13^0 \pmod{15}\rangle + |1\rangle|0\oplus 13 \pmod{15}\rangle + \dots \right)$; $a\oplus b$ = adición modular 2

$= 1/4\left(|0\rangle_4 |13^0 \pmod{15}\rangle + |1\rangle|13 \pmod{15} + 12\rangle_4 |13^2 \pmod{15}\rangle + \dots \right)$

$= \dots$

$$\mu^{\otimes 4}|0\rangle = \frac{1}{4}\left(|0000\rangle + |0001\rangle + |0010\rangle + \cdots + |1111\rangle\right)$$

$$= \frac{1}{4}\left(|0\rangle_4 + |2\rangle_4 + |3\rangle_4 + \cdots |15\rangle_4\right)$$

$0 - 15 = 16$ elemento

$$\cdots = 1/4 \Big[|0\rangle_4|\uparrow\rangle_4 + |\uparrow\rangle_4|13\rangle_4 + |2\rangle_4|4\rangle_4 + |3\rangle_4|7\rangle_4$$
$$|4\rangle_4|\uparrow\rangle_4 + |5\rangle_4|13\rangle_4 + |6\rangle_4|4\rangle_4 + |7\rangle_4|7\rangle_4$$
$$|8\rangle_4|\uparrow\rangle_4 + |9\rangle_4|13\rangle_4 + |10\rangle_4|4\rangle_4 + |11\rangle_4|7\rangle_4$$
$$|12\rangle_4|1\rangle_4 + |13\rangle_4|13\rangle_4 + |14\rangle_4|4\rangle_4 + |15\rangle_4|7\rangle_4 \Big]$$

$\left(\frac{1}{4}\right)^2 = \frac{1}{16}$

(3) Al medir el registro de $|w\rangle$, los posibles resultados son $\{|\uparrow\rangle, |13\rangle, |4\rangle, |7\rangle\}$

- Si la medición nos da $|7\rangle$, el estado en el registro $|x\rangle$ es

$$|x\rangle|7\rangle_4 = 1/2\left[|3\rangle_4 + |7\rangle_4 + |11\rangle_4 + |15\rangle_4\right]$$

- Normalización después de medir

(4) Aplicamos QFT^+ al registro x

$N = 2^n = 16$

$$QFT|x\rangle = |\tilde{x}\rangle = \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} e^{\frac{2\pi i}{N} xy} |y\rangle \quad ; \quad N = 16 = 2^4$$

$$= \frac{1}{4}\left(|0\rangle_4 + e^{\frac{2\pi i x}{16}} |1\rangle_4 + e^{\frac{2\pi i}{16} x(2)} |2\rangle_4 + e^{\frac{2\pi i}{16} x(3)} |3\rangle_4 + \cdots \right)$$

$$QFT^+ |\tilde{x}\rangle = |x\rangle = \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} e^{\frac{-2\pi i}{N} xy} |y\rangle$$

$$QFT^+ |3\rangle_4 = \frac{1}{\sqrt{16}} \sum_{y=0}^{15} e^{\frac{-2\pi i}{16} 3y} |y\rangle$$

$$QFT^{+}|7\rangle_4 = \frac{1}{\sqrt{16}} \sum_{y=0}^{15} e^{-\frac{2\pi i 7y}{16}} |y\rangle$$

$$QFT^{+}|11\rangle_4 = \frac{1}{\sqrt{16}} \sum_{y=0}^{15} e^{-\frac{2\pi i 11y}{16}} |y\rangle$$

$$QFT^{+}|15\rangle_4 = \frac{1}{\sqrt{16}} \sum_{y=0}^{15} e^{-\frac{2\pi i 15y}{16}} |y\rangle$$

- Nos olvidamos de la parte del registro de $\boxed{|w\rangle = |7\rangle_4}$

$$QFt^{+}|x\rangle = \frac{1}{8} \sum_{y=0}^{15} \left[e^{-i3\pi y/8} + e^{-i7\pi y/8} + e^{-i\pi y/8} + e^{-i15\pi y/8} \right] |y\rangle$$

• Usando $e^{-i 3\pi y/4} = \cos(3\pi/8 y) - i \operatorname{Sen}(3\pi/8 y)$

$\Rightarrow$

• Interferencia

$$QFT^{+}|x\rangle = \frac{1}{8}\left[4|0\rangle_4 + 4i|4\rangle_4 - 4|8\rangle_4 - 4i|12\rangle_4\right]$$

$$= 1/2\left[|0\rangle_4 + i|4\rangle_4 - |8\rangle_4 - i|12\rangle_4\right]$$

(5) Medimos el estado anterior ↑ y podríamos obtener

$\{|0\rangle_4, |4\rangle_4, |8\rangle_4, |12\rangle_4\}$

4 4 4

- Los resultados de la medición se acentúan (o su probabilidad tiene un pico) al rededor de $\frac{j}{r}N = x'$, $j \in \mathbb{Z}$

x' := resultado de la medición

- Supongamos que la medición nos devuelve $(|4\rangle)_4$

$$\Rightarrow \frac{j(16)}{r} = 4 \iff j = 1 \text{ y } r = 4$$

- Como r es par, seguimos con la 2a. condición

$$x \equiv a^{r/3} \pmod{15} = 13^{4/2} \pmod{15} = 13^2 \pmod{15} = 4$$

$$x+1 = 5 \qquad mcd(x+1, 15) = mcd(5, 15) = 5 \checkmark$$

$$x-1 = 3 \qquad mcd(x-1, 15) = mcd(3, 15) = 3 \checkmark$$

- Si el resultado de la medición es $|8\rangle_4$

$\frac{j(16)}{r} = 8 \iff j = 1,\ r = 2$ ó $j = 2$ y $r = 4$ (caso anterior) ✓

$$x \equiv 13^{r/2} \pmod{15} = 13 \pmod{15} = 2$$

$x + 1 = 3$; $MCD(3, 15) = 3$ • Pero aquí ya encontré un factor

$x - 1 = 1$; $MCD(1, 15) = 1$ • Este no me sirve

$\frac{15}{3} = 5$ ∴ $p = 5$ y $q = 3$

$$|x\rangle = \frac{1}{2}\left[|0\rangle_4 + i|4\rangle_4 - |8\rangle_4 - i|12\rangle_4 \right]$$

0 → $1/4 = 25\%$

3,5 ; 3 ; 3,5 → $3/4 = 75\%$

- Superposición con igual probabilidad

$N = 15$

* Clásicamente:

$$t_c(N) \approx e^{1.9 (\log_2 N)^{1/3} (\log_2 (\log_2 N))^{2/3}}$$

* Cuánticamente:

$$t_Q(N) \approx (\log_2 N)^3$$

i.e. Si $\log_2(N) \approx 128$ → **N = 340282366920938463463374607431768211456**

$\Rightarrow t_c(N) \approx 10^7$ años

Pero $t_Q(N) \approx$ 24 días

Si además agregamos el algoritmo de Grover (128 → 64) $\Rightarrow t_Q(N) \approx$ 3 días

$10 \cdot 10 \cdot 10 \cdots 10 = 10{,}000{,}000$

RSA

$d = 39$

~~A~~ Cómo podemos implementar $\hat{U}_{f_{a,N}}$, $f_{a,N}(x) \equiv a^x \pmod N$

$$x = [x_1 x_2 x_3 \dots x_n] = 2^{n-1} x_1 + 2^{n-2} x_2 + \dots 2^0 x_n \qquad (15 = 1111)$$

$$\Rightarrow f_{a,N}(x) = a^{2^{n-1} x_1 + 2^{n-2} x_2 + \dots + 2^0 x_n} \pmod N$$

$$= a^{2^{n-1} x_1} \; a^{2^{n-2} x_2} \dots a^{2^0 x_n} \pmod N$$