

$$\Delta x \times \Delta p \geq \frac{\hbar}{2}$$

$$|\psi\rangle = a |0\rangle + b |1\rangle$$
$$|a|^2 + |b|^2 = 1$$

INTRODUCCIÓN A LA MECÁNICA CUÁNTICA II

Clase II

- **Otras consecuencias de la cuántica**
- **Introducción a la computación cuántica**
 - Computadores clásicos versus cuánticos
 - Bit cuántico
 - Compuertas cuánticas
 - Medidas
 - Estados de bell
 - Teleportación cuántica
- **Circuitos cuánticos**

Más consecuencias de la MC

Principio de superposición

Los sistemas cuánticos pueden estar **en dos estados al mismo tiempo** con una cierta **probabilidad**

$$|\text{colorful circle}\rangle = a |\text{red circle}\rangle + b |\text{blue circle}\rangle$$

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

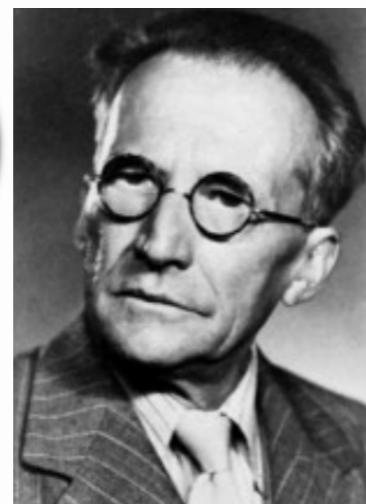
Más consecuencias de la MC

Entrelazamiento

El gato está **vivo y muerto** al mismo tiempo...



1933



¿Para qué nos sirve la cuántica?



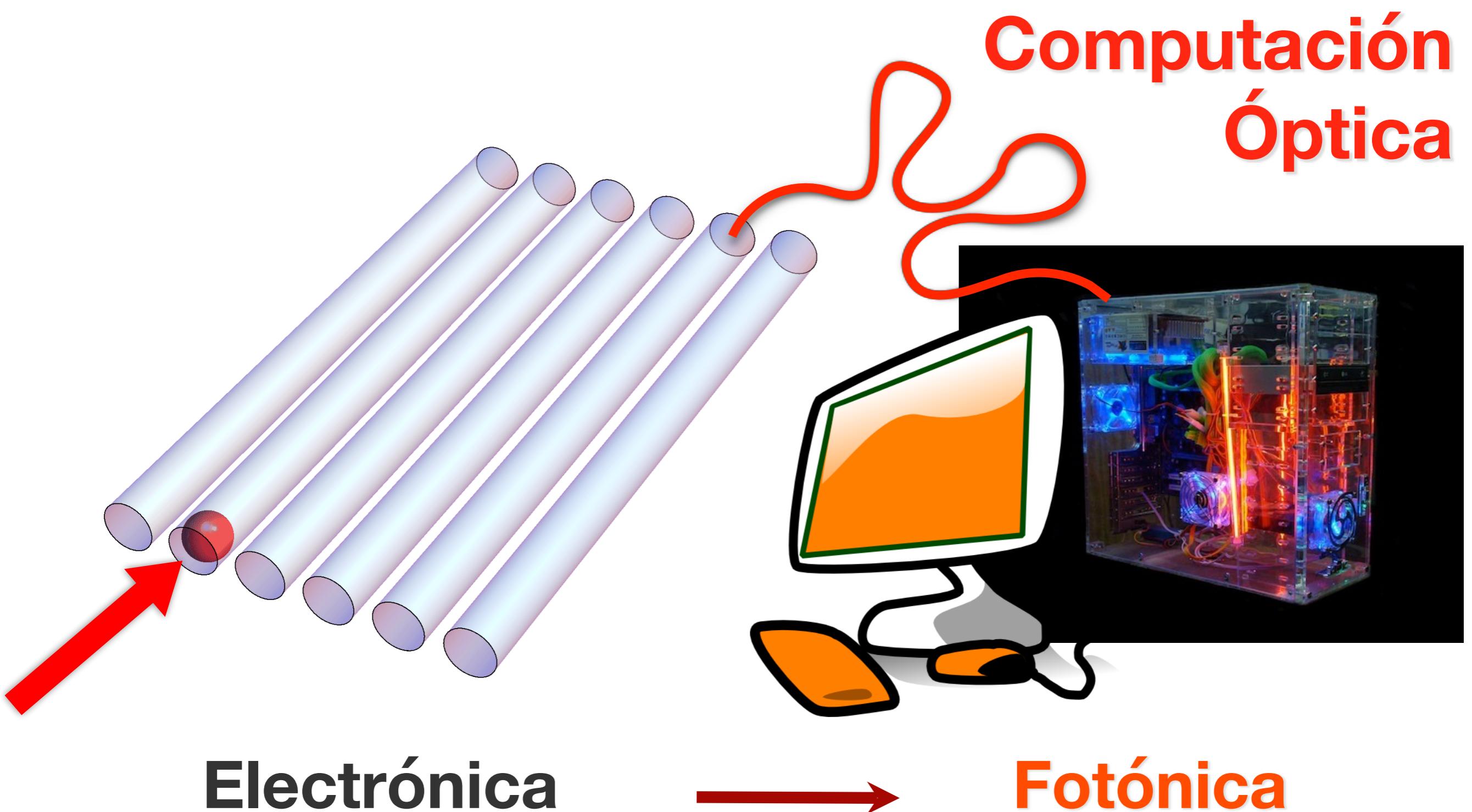
Metrología cuántica

Computación cuántica

Información cuántica

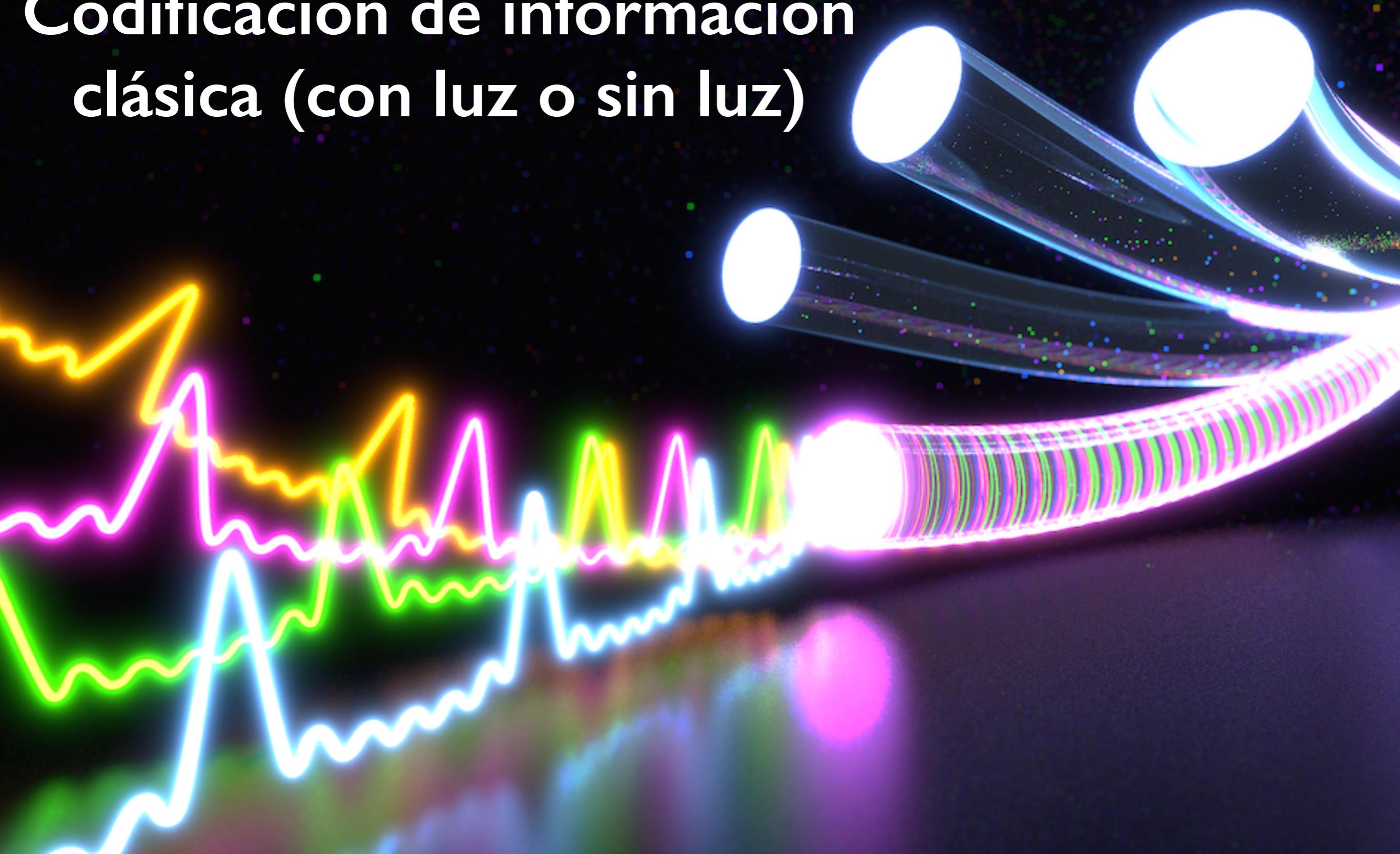
Entre otros...

No es...



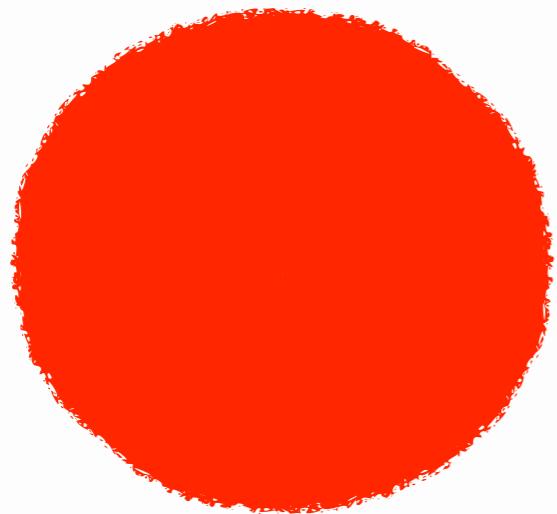
(video de Rodrigo Vicencio, U de Chile)

Codificación de información clásica (con luz o sin luz)

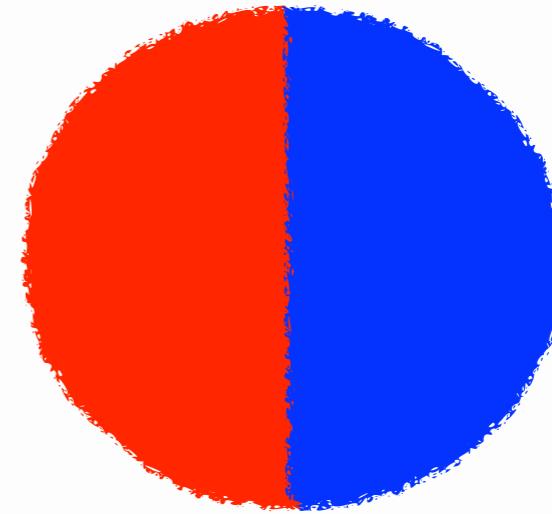


Computadores clásicos

(en el contexto del procesamiento de información)



Esta es una pelota



Esta pelota puede ser roja o azul

Se necesita **un bit** (0 o 1) para guardar esta información

Codificación de Información digital

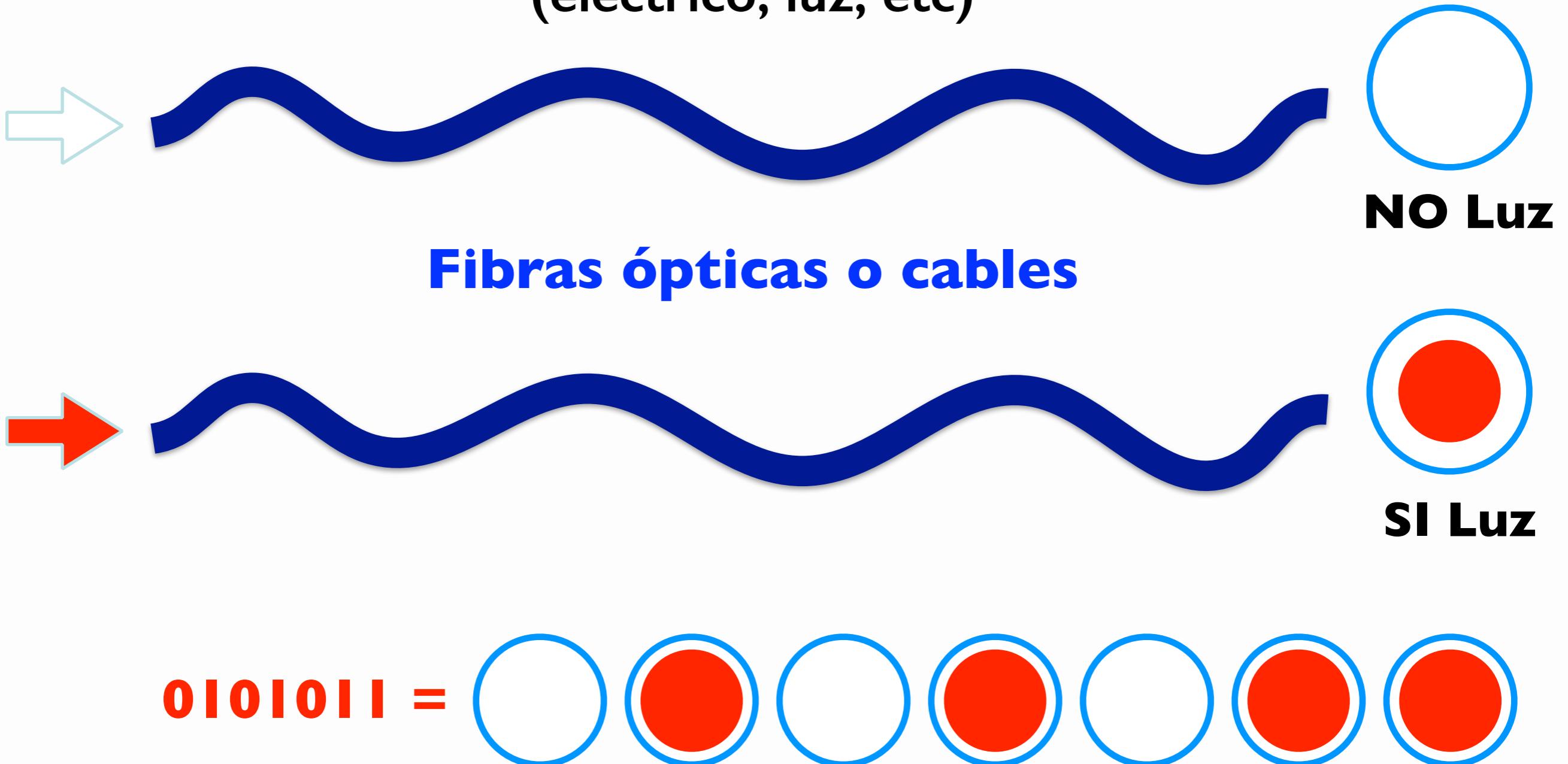
Se lleva a cabo a través de una secuencia de ceros y unos que codifica números y letras:

01000001 = A
01000010 = B
01000011 = C
01000100 = D
01000101 = E
01000110 = F
01000111 = G
01001000 = H
01001001 = I
01001010 = J
01001011 = K
01001100 = L
01001101 = M

01001110 = N
01001111 = O
01010000 = P
01010001 = Q
01010010 = R
01010011 = S
01010100 = T
01010101 = U
01010110 = V
01010111 = W
01011000 = X
01011001 = Y
01011010 = Z

0000 = 0
0001 = 1
0010 = 2
0011 = 3
0100 = 4
0101 = 5
0110 = 6
0111 = 7
1000 = 8
1001 = 9

Se genera así un código (eléctrico, luz, etc)



Transmisión de información limitada por las características de la luz y la extracción y procesamiento de la información

Factorización en computadores clásicos

La encriptación de datos clásica se basa
en este mecanismo

$$6 = 3 \times 2$$

$$211 = 13 \times 17$$

$$2.185.189.842 = ?$$

Factorización en computadores clásicos

2.185.189.842 =

45678 x 47839

Factorización en computadores clásicos

27910032096669336172976091660
38894252011457236525404768416
76044961104821396625894385263
63500454095893469490269597213
44496708100256800960993459519
73790797453689690160396619700
655169013196639779692740608= ?

Ya no es tan fácil. De hecho, ni el mejor
computador del mundo puede hacerlo

Un computador cuántico si podría

Segunda revolución cuántica

¡amenaza a la ciberseguridad!

SeQure Spa

Startup que nace en MIRO y la Udec



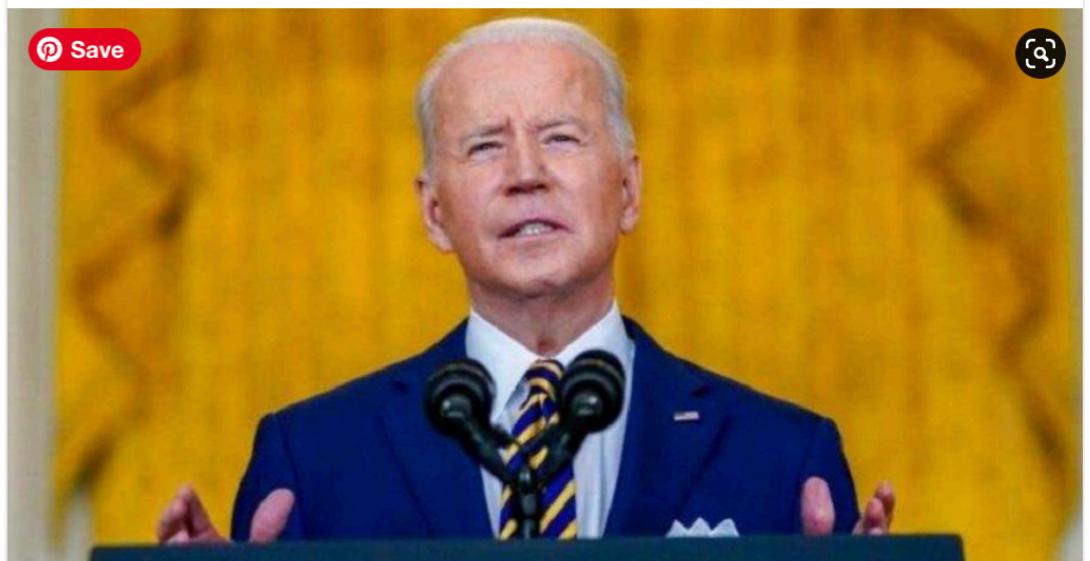
Carolina Pizarro Díaz • 2nd

4d ·

+ Follow

El Presidente de Estados Unidos, Joe Biden, ha firmado esta semana la Ley de Preparación para la Ciberseguridad de la Computación Cuántica. El objetivo de la ley es proteger los sistemas y datos del gobierno federal frente a la amenaza de filtraciones de datos de origen cuántico, antes del "Día Q", el momento en que los ordenadores cuánticos sean capaces de descifrar los algoritmos criptográficos existentes. Los expertos creen que la computación cuántica avanzará hasta este punto en los próximos cinco a diez años, dejando potencialmente toda la información digital vulnerable a las ciberamenazas bajo los actuales protocolos de cifrado. [#ciberseguridad](#) [#digital](#) [#Computacioncuantica](#)

[See translation](#)



El Presidente Biden firma la Ley Quantum de Preparación para la Ciberseguridad

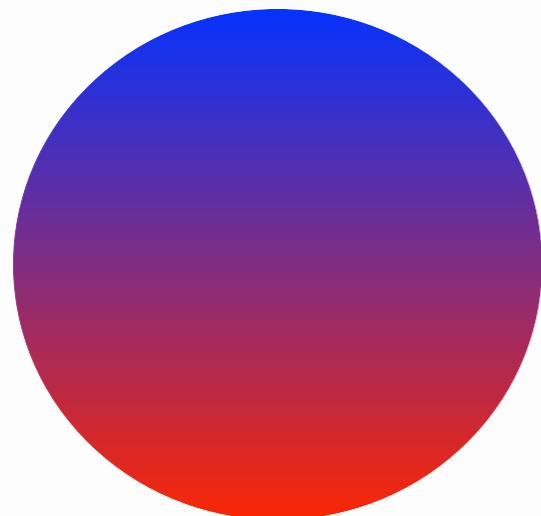
ciberseguridadlatam.com • 2 min read

¿Qué es un computador cuántico?



En vez de corriente, cables, compuertas lógicas, transistores, diodos, etc., tendremos cables cuánticos, compuertas cuánticas, etc. que servirán para almacenar/manipular/procesar información.

Computadores cuánticos



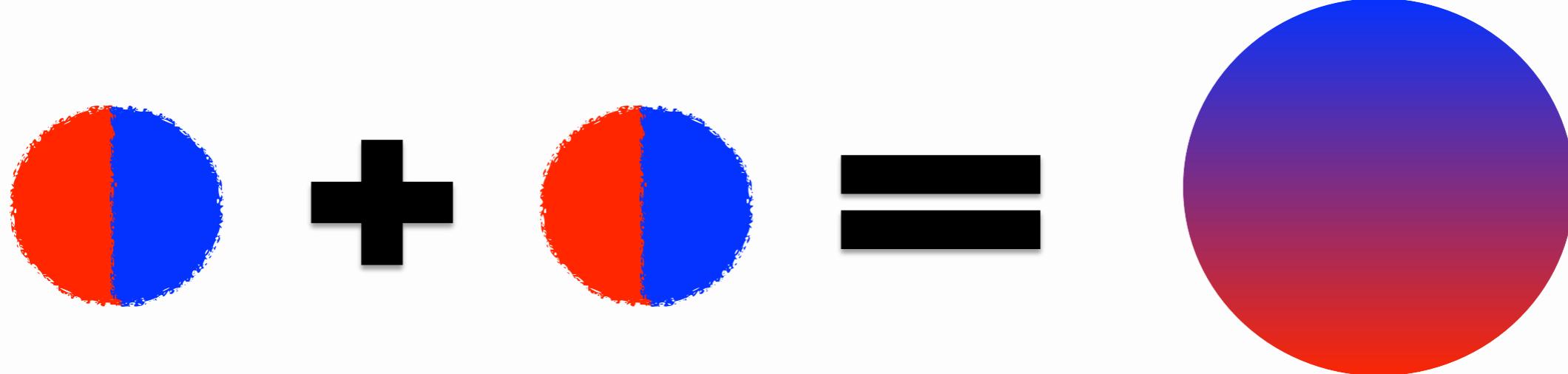
Una partícula cuántica es como una pelota que puede estar en una superposición de estados

$$|\text{circle}\rangle = a |\text{red}\rangle + b |\text{blue}\rangle$$

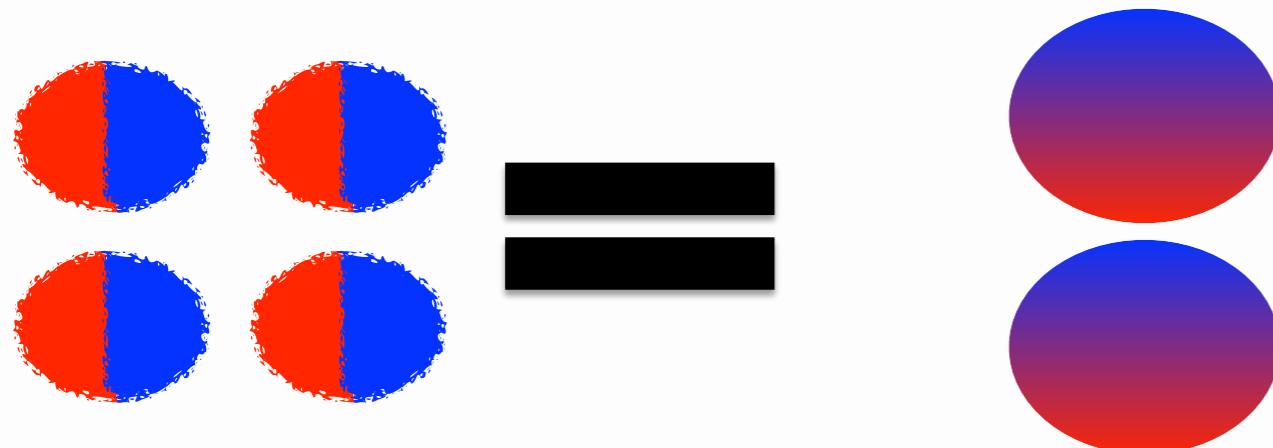
$$|a|^2 + |b|^2 = 1$$

A esto se le conoce como un bit cuántico o **qubit**

Computadores cuánticos



Dos bits para describir un **qubit**



4 bits para describir 2 **qubit**

n **qubits** = 2^n **bits**

Computadores clásicos versus cuánticos

¿cómo se traduce esto?



mil millones de bits

30 qubits

Computadores clásicos versus cuánticos

Un computador cuántico de **300** 
qubits tendrían aproximadamente el mismo
número de estados posibles que el número
total de átomos en el universo
conocido.

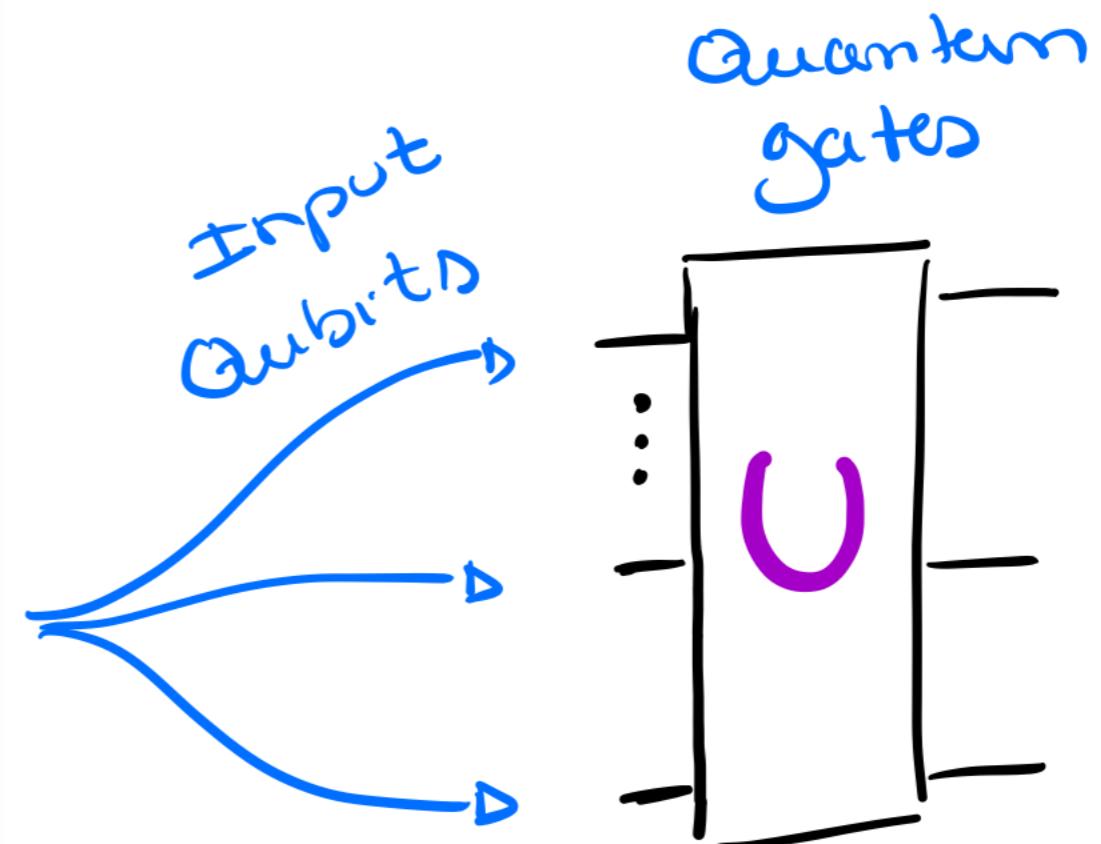
Factorización

279100320966693361729760916603889425201145723
652540476841676044961104821396625894385263635
004540958934694902695972134449670810025680096
099345951973790797453689690160396619700655169
013196639779692740608=

366905830534589915808070762834465013289099915
587915826624738090239973117307823390176963595
4395253637 **x**
760686524278008950945631346924946623361406181
865457854711346644260565168661782999883757560
34332349590

Computador cuántico

Qubits <=> “cables”



Compuertas cuánticas <=>
“operaciones o transformaciones”

Se genera así un circuito
cuántico con diferentes
algoritmos cuánticos

Bits cuánticos



Qubit: lo trataremos como un **objeto matemático**, un vector de norma uno en un espacio de 2-dimensiones (que se puede generar en un laboratorio).

Bases computacionales

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

$$\alpha \text{ y } \beta \in \mathbb{C} \quad |\alpha|^2 + |\beta|^2 = 1$$

Al medir este qubit, vamos a medir en realidad 0 o 1 con una cierta probabilidad. No vamos a medir directamente el estado original de superposición.

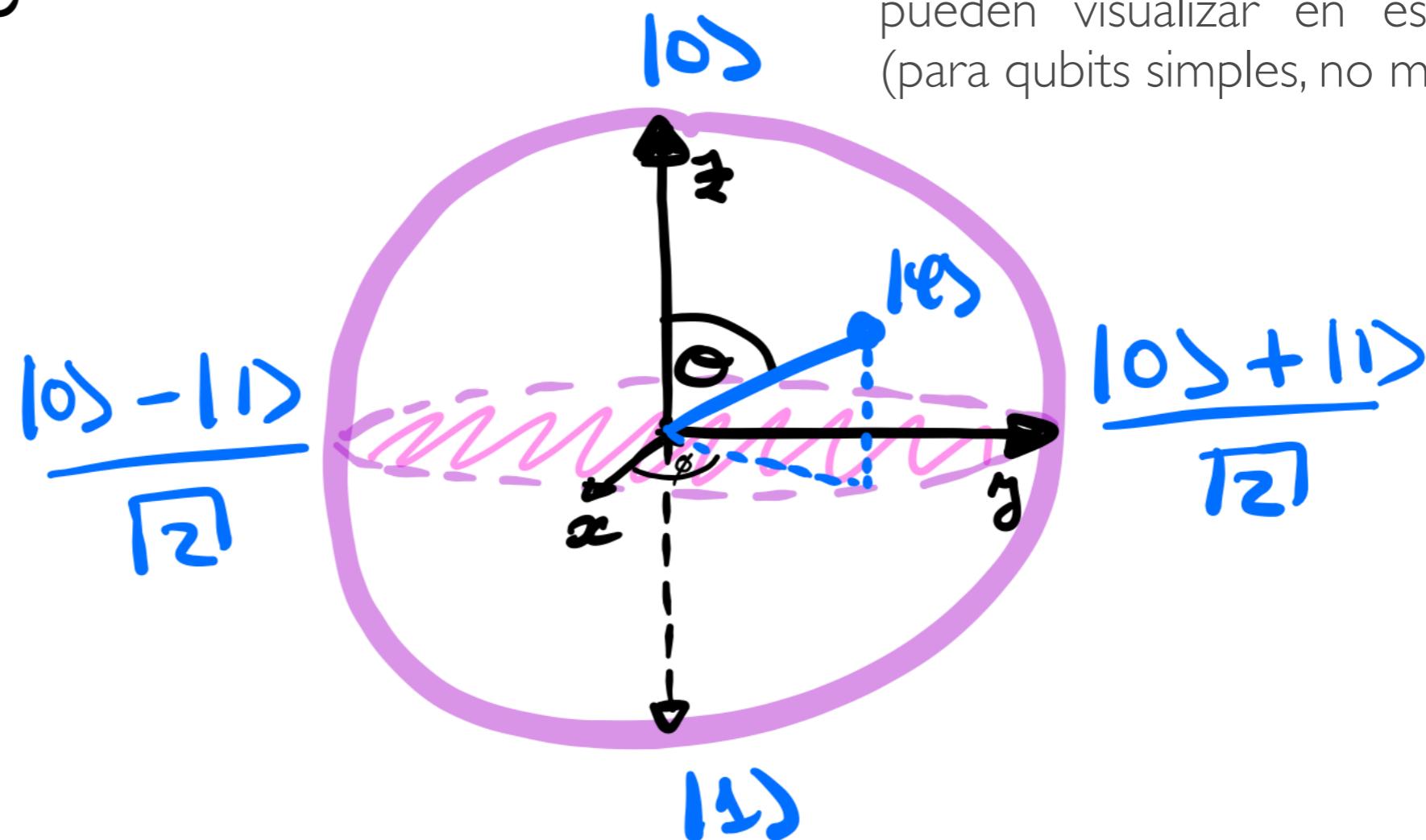
Esta peculiaridad de lo no-observable y lo que se puede medir, está en el corazón de la computación e información cuántica.

El estado es real, se puede construir en el lab, y tiene consecuencias experimentales medibles, solo que no tiene una correspondencia directa al mundo como lo conocemos.

Bits cuánticos

Representación de un qubit en la esfera de Bloch:

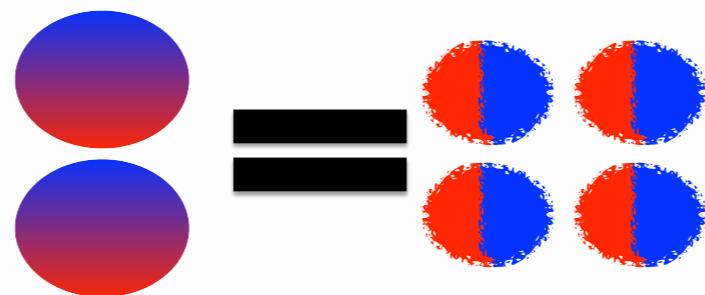
$$|\Psi\rangle = \cos \frac{\theta}{2} |0\rangle + e^{i\phi} \sin \frac{\theta}{2} |1\rangle$$



Varias de las operaciones que se pueden realizar en qubits se pueden visualizar en esta esfera (para qubits simples, no múltiples)

Múltiples Bits cuánticos

Supongamos que tenemos ahora 2 qubits.



Se necesitan 4 bits para describir 2 **qubit**

00 01 10 00

$$|\Psi\rangle = \alpha_{00} |00\rangle + \alpha_{01} |01\rangle + \alpha_{10} |10\rangle + \alpha_{11} |11\rangle$$

$$|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1$$

Múltiples Bits cuánticos

Dentro de estos estados, hay unos de gran interés, los estados de Bell (4 en total):

Estado clave en teleportación y super-dense coding

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

También se conoce como **estado EPR**, y **esta entrelazado**

Las medidas o posibles resultados están correlacionadas

MAY 15, 1935 PHYSICAL REVIEW VOLUME 47

Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?

A. EINSTEIN, B. PODOLSKY AND N. ROSEN, *Institute for Advanced Study, Princeton, New Jersey*
(Received March 25, 1935)

In a complete theory there is an element corresponding to each element of reality. A sufficient condition for the reality of a physical quantity is the possibility of predicting it with certainty, without disturbing the system. In quantum mechanics in the case of two physical quantities described by non-commuting operators, the knowledge of one precludes the knowledge of the other. Then either (1) the description of reality given by the wave function in quantum mechanics is not complete or (2) these two quantities cannot have simultaneous reality. Consideration of the problem of making predictions concerning a system on the basis of measurements made on another system that had previously interacted with it leads to the result that if (1) is false then (2) is also false. One is thus led to conclude that the description of reality as given by a wave function is not complete.

Múltiples Bits cuánticos

PERO llega el trabajo de John Bell, que prueba que las correlaciones de las medidas en un estado EPR, son mucho más fuertes de lo que nunca existirá entre sistemas clásicos (ver libro Q if for quantum)

ON THE EINSTEIN PODOLSKY ROSEN PARADOX*

J. S. BELL†

Department of Physics, University of Wisconsin, Madison, Wisconsin

(Received 4 November 1964)

I. Introduction

THE paradox of Einstein, Podolsky and Rosen [1] was advanced as an argument that quantum mechanics could not be a complete theory but should be supplemented by additional variables. These additional variables were to restore to the theory causality and locality [2]. In this note that idea will be formulated mathematically and shown to be incompatible with the statistical predictions of quantum mechanics. It is the requirement of locality, or more precisely that the result of a measurement on one system be unaffected by operations on a distant system with which it has interacted in the past, that creates the essential difficulty. There have been attempts [3] to show that even without such a separability or locality requirement no "hidden variable" interpretation of quantum mechanics is possible. These attempts have been examined elsewhere [4] and found wanting. Moreover, a hidden variable interpretation of elementary quantum theory [5] has been explicitly constructed. That particular interpretation has indeed a grossly non-local structure. This is characteristic, according to the result to be proved here, of any such theory which reproduces exactly the quantum mechanical predictions.

Compuertas simples

$$U|\psi\rangle = |\psi'\rangle$$



Unitaria $U^\dagger U = \mathbb{I}$

Para qubits simples, la única condición que deben tener estas compuertas lógicas es que sean **operaciones unitarias**.

Luego, lo interesante será cómo llevarlas a cabo en forma experimental.

NOT quantum gate

En una **NOT gate** clásica, si entra 0, sale un 1, y vice versa. Es una operación del “no es”, del opuesto.

En qubits esto
sería:

$$\alpha|0\rangle + \beta|1\rangle \xrightarrow{\text{not}} \beta|0\rangle + \alpha|1\rangle$$

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}; |\Psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

$$X|\Psi\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \beta \\ \alpha \end{pmatrix}$$

Z gate

Esta compuerta deja el 0 igual, y solo actúa en el 1, cambiándolo de signo.

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

$$Z |0\rangle = \alpha |0\rangle - \beta |1\rangle$$

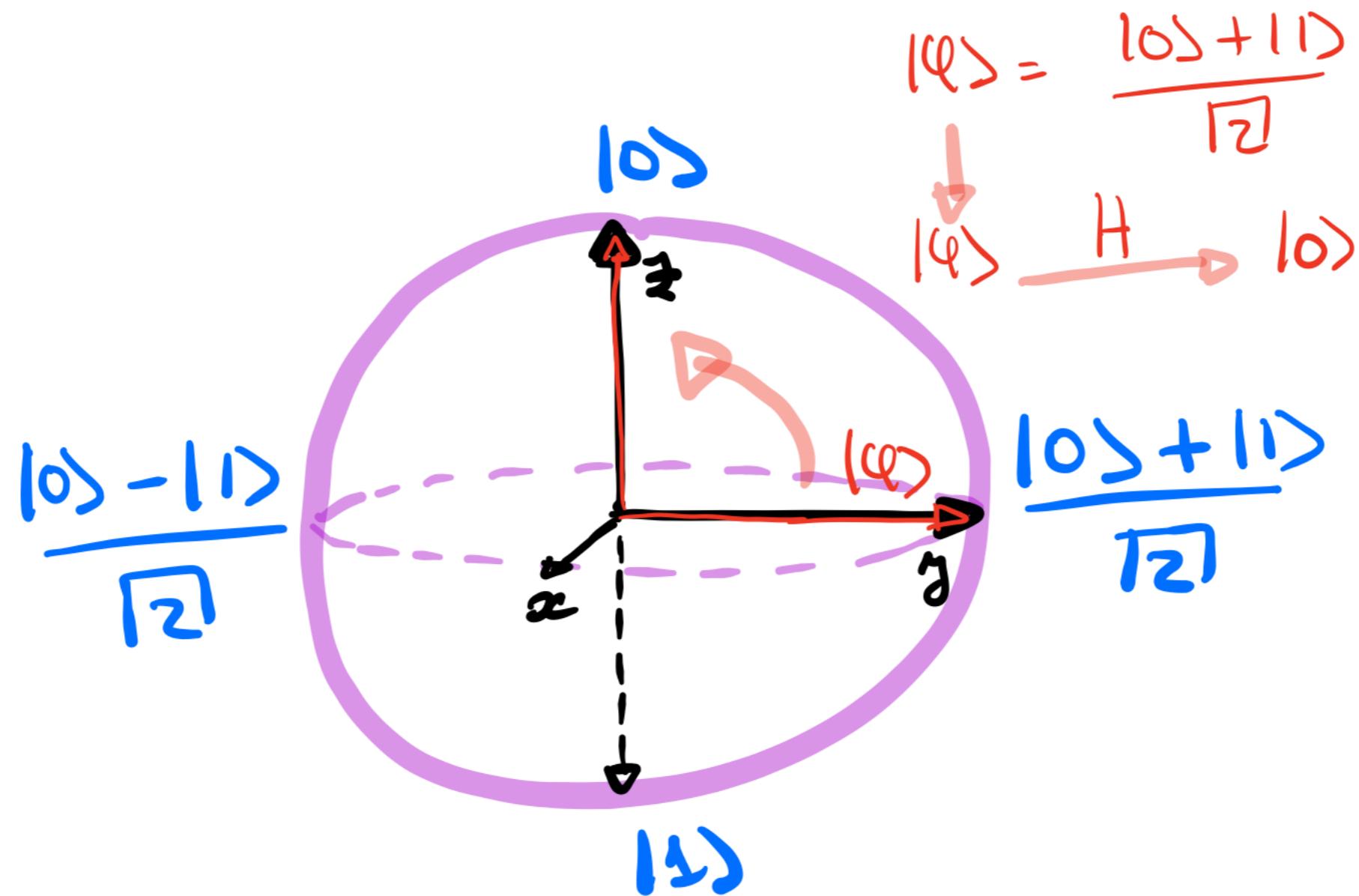
Compuerta Hadamard

Esta compuerta nos lleva de los polos de la esfera de Bloch al ecuador de esta y vice-versa.

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

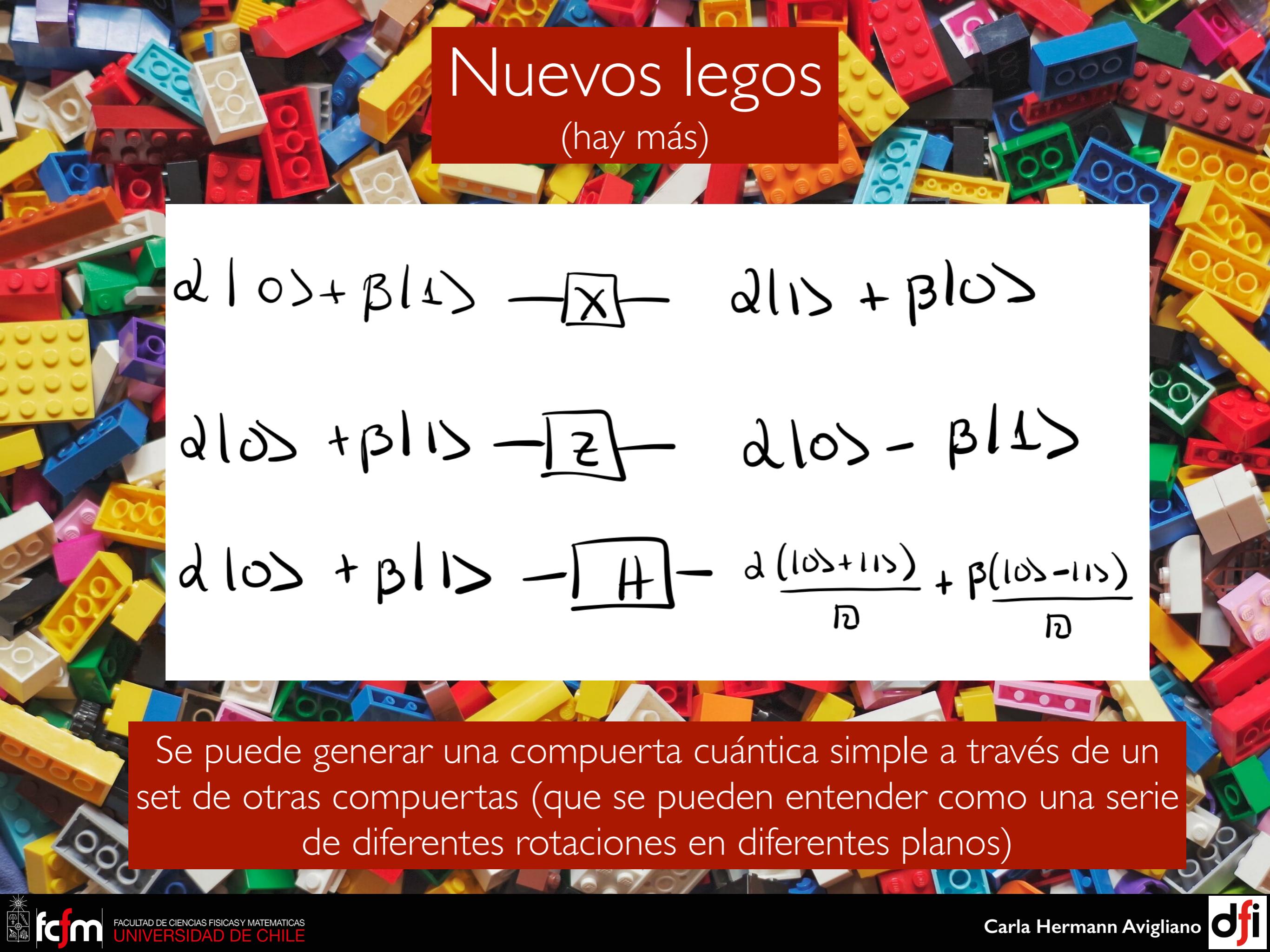
$$\begin{aligned} |0\rangle &\xrightarrow{\text{unify}} (|0\rangle + |1\rangle)/\sqrt{2} \\ |1\rangle &\xrightarrow{\text{unify}} (|0\rangle - |1\rangle)/\sqrt{2} \end{aligned}$$

Compuerta Hadamard



Claramente no tiene un análogo clásico

$(H^2 = \mathbb{I})$
NO HACE
NADA



Nuevos legos

(hay más)

$$\alpha|0\rangle + \beta|1\rangle - \boxed{x} - \alpha|1\rangle + \beta|0\rangle$$

$$\alpha|0\rangle + \beta|1\rangle - \boxed{z} - \alpha|0\rangle - \beta|1\rangle$$

$$\alpha|0\rangle + \beta|1\rangle - \boxed{H} - \frac{\alpha(|0\rangle + |1\rangle)}{\sqrt{2}} + \frac{\beta(|0\rangle - |1\rangle)}{\sqrt{2}}$$

Se puede generar una compuerta cuántica simple a través de un set de otras compuertas (que se pueden entender como una serie de diferentes rotaciones en diferentes planos)

Compuertas múltiples

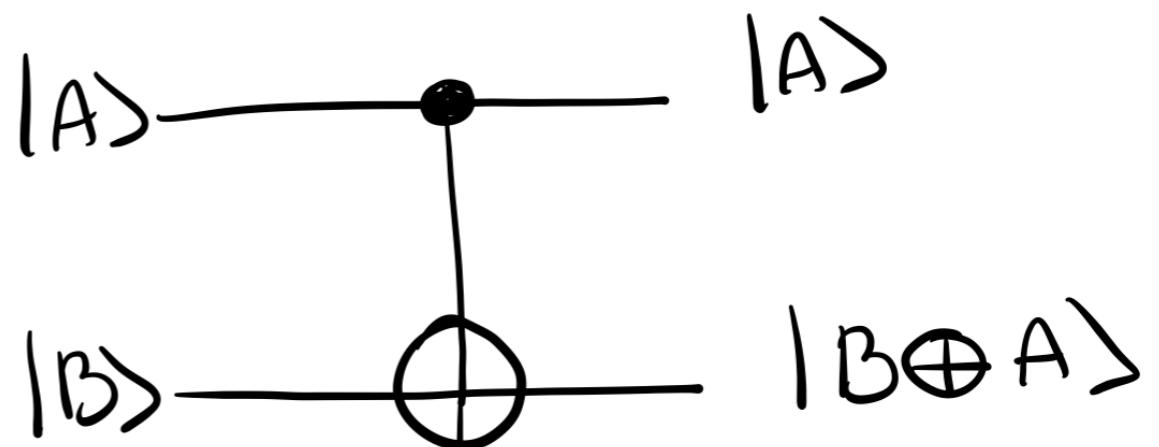
Así como en computación clásica hay operaciones que requieren de dos inputs (por ejemplo una compuerta **and** o **or**), también podemos tener compuertas que operen en dos o más qubits.

Controlled- NOT o CNOT

- {
- 2 inputs
 - qubit controlador
 - qubit objetivo o target

Su representación matricial y de circuito es la siguiente:

$$U_{CN} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$



CNOT

Si el qubit de control esta en 0, entonces el qubit target no se toca.
Si el qubit de control esta en 1, entonces el qubit target se invierte.

$$|00\rangle \rightarrow |00\rangle$$

$$|10\rangle \rightarrow |11\rangle$$

$$|01\rangle \rightarrow |01\rangle$$

$$|11\rangle \rightarrow |10\rangle$$

Si consideramos un estado de Bell

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

$$U_{C_N} |\psi\rangle = \frac{|00\rangle + |10\rangle}{\sqrt{2}}$$

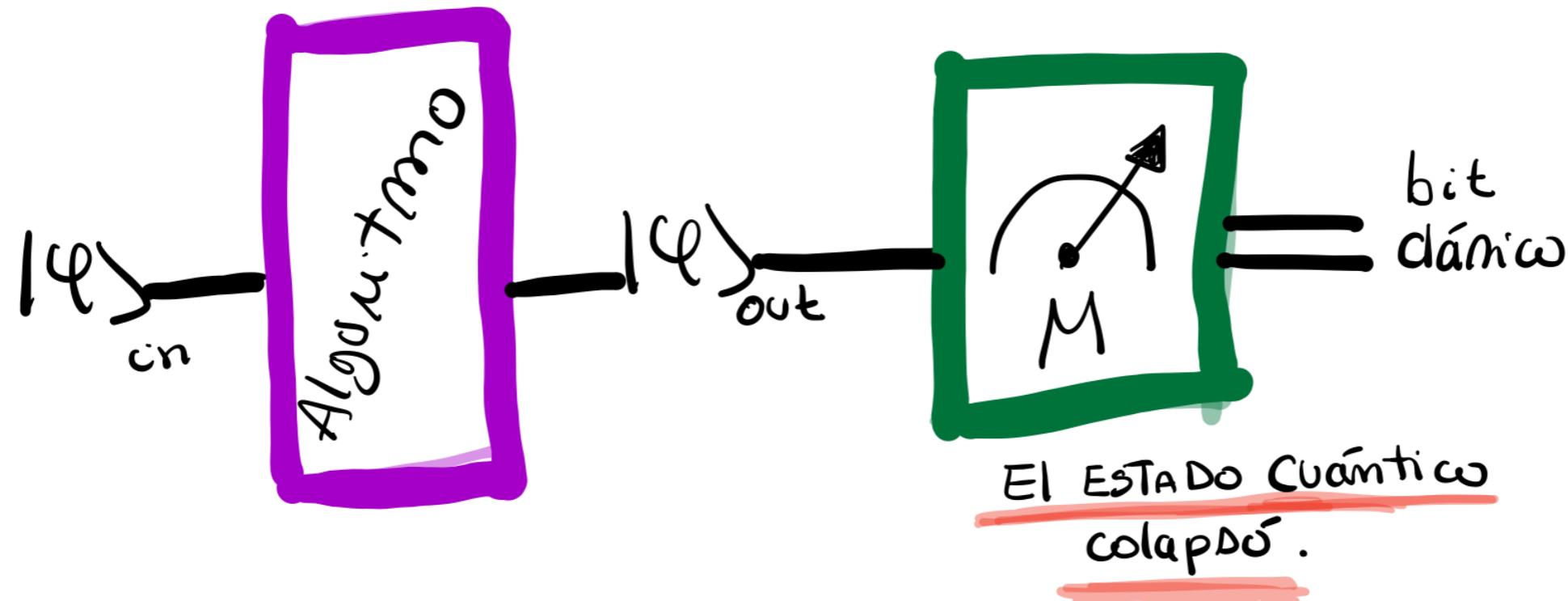
$$U_{C_N}^\dagger U_{C_N} = \mathbb{1}$$

Cualquier compuerta multiple cuántica puede ser generada por una CNOT y compuertas simples

No todas las compuertas clásicas tienen un análogo cuántico, pues algunas son irreversibles, y por lo tanto, no unitarias

Medidas en computación cuántica

CIRCUITO



Generamos nuestro estado cuántico, lo hacemos pasar a través de diferentes operaciones, también cuánticas, tenemos un output cuántico.... y luego medimos algo clásico!

Medidas en computación cuántica

Medir en cuántica definitivamente no es tan sencillo o directo como medir en clásica. Hay que tener en mente que los postulados de la cuántica son dados en el contexto de sistemas cerrados, pero eso en la realidad es casi imposible de generar.

Postulado III

Las medidas cuánticas son descritas por operadores de medidas \mathbf{M}_m . Estos operadores actúan en el espacio de Hilbert del sistema que se está midiendo.

El subíndice **m** denota el valor de la medida que saldrá del proceso de medición (que es un autovalor de \mathbf{M}).



$$P(m) = \sqrt{\langle \psi | M_m^+ M_m | \psi \rangle}$$

Probabilidad de medir m para un estado cualquiera

$$\sum_m M_m^+ M_m = 1$$

La suma de todas las probabilidades deben sumar 1.

Medidas proyectivas

Distintos tipos de medidas:

- Medidas proyectivas
- Medidas POVM

Medidas proyectivas: es descrita por un observable **M** hermítico

$$M = \sum_m m P_m$$

Descomposiciónpectral del operador M.

P_m es un proyector $|><|$

Probabilidad de medir m:

$$P(m) = \langle \psi | P_m | \psi \rangle$$

y por lo tanto el sistema colapsa a

$$|\psi\rangle \xrightarrow{\quad} \frac{P_m |\psi\rangle}{\sqrt{P(m)}}$$

$$\sum_m M_m^+ M_m = 1$$

Completitud (probabilidades suman uno)

$$M_m M_{m'} = \delta_{mm'} M_m$$

Ortonormalidad

Medidas proyectivas

Consideremos el siguiente qubit:

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

Los operadores para medir $|0\rangle$ o $|1\rangle$ serían:

$$\begin{aligned} M_0 &= |0\rangle\langle 0| \\ M_1 &= |1\rangle\langle 1| \end{aligned} \quad \text{PROYECTORES}$$

Probabilidades de medir serían:

$$P(0) = \langle \psi | M_0^+ M_0 | \psi \rangle = |\alpha|^2 \rightarrow$$

$$\frac{\alpha}{|\alpha|} |0\rangle$$

$$P(1) = \langle \psi | M_1^+ M_1 | \psi \rangle = |\beta|^2 \rightarrow$$

$$\frac{\beta}{|\beta|} |1\rangle$$

Medidas proyectivas

¿Qué pasa si nuestro estado inicial estuviese en otra base?

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \rightarrow \gamma|+\rangle + \delta|- \rangle$$

$$\gamma = \frac{\alpha + \beta}{\sqrt{2}}, \quad \delta = \frac{\alpha - \beta}{\sqrt{2}}$$

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} ; \quad |- \rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

Podemos mantener nuestros sistemas de medidas, y medir 0 y 1, pero la respuesta no la podemos interpretar de la misma forma que antes.

Podemos cambiar nuestros medidores, y $|+\rangle <+|$ y $|-\rangle <-|$

Medidas POVM

Positive Operator-Valued Measurement

Son una generalización de las medidas proyectivas (POVM= proyectivas + entorno).



Operadores semidefinidos positivos, que suman la identidad

$$E \equiv M_m^+ M_m$$

¿Cuándo esto es relevante?

$$P(m) = \langle \psi | E_m | \psi \rangle$$

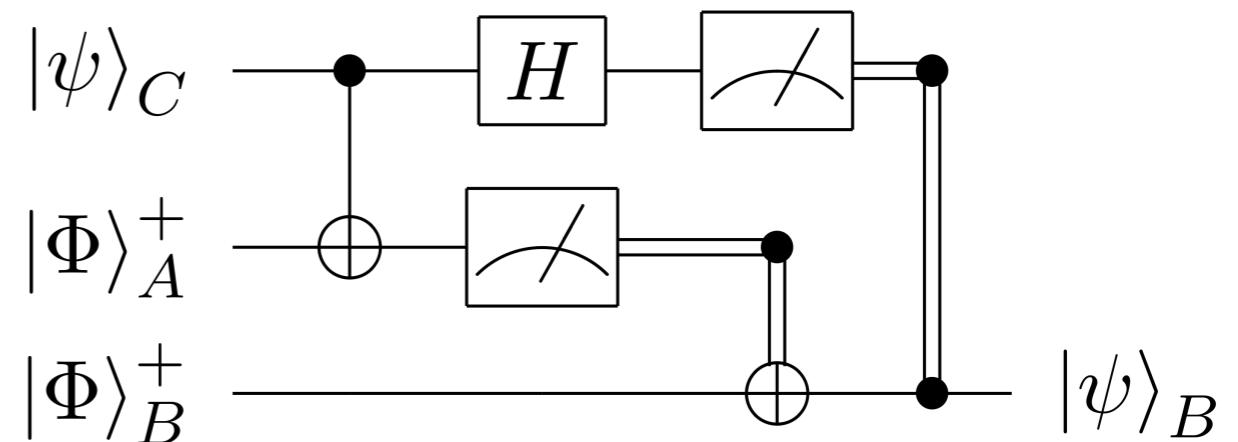
$$\sum_m E_m = \mathbb{1}$$

Circuitos cuánticos

Un **circuito clásico**, se compone de cargas y corrientes, cables, fuentes de energía, disipadores, almacenadores, mediciones, etc. en alguna secuencia. También tienen reglas: leyes de mallas, leyes de voltajes, leyes de corriente, etc.

Un **circuito cuántico**, es una secuencia de compuertas cuánticas (todas reversibles, operadores unitarios), medidas, qubits como inputs, etc. El proceso de medida rompe la reversibilidad al colapsar la función de onda.

- El eje horizontal denota secuencia temporal
- Lineas horizontales denotan qubits
- Dos lineas horizontales denotan bits clásicos
- Cajas denotan compuertas cuánticas
- Lineas verticales denotan acciones sobre qubits



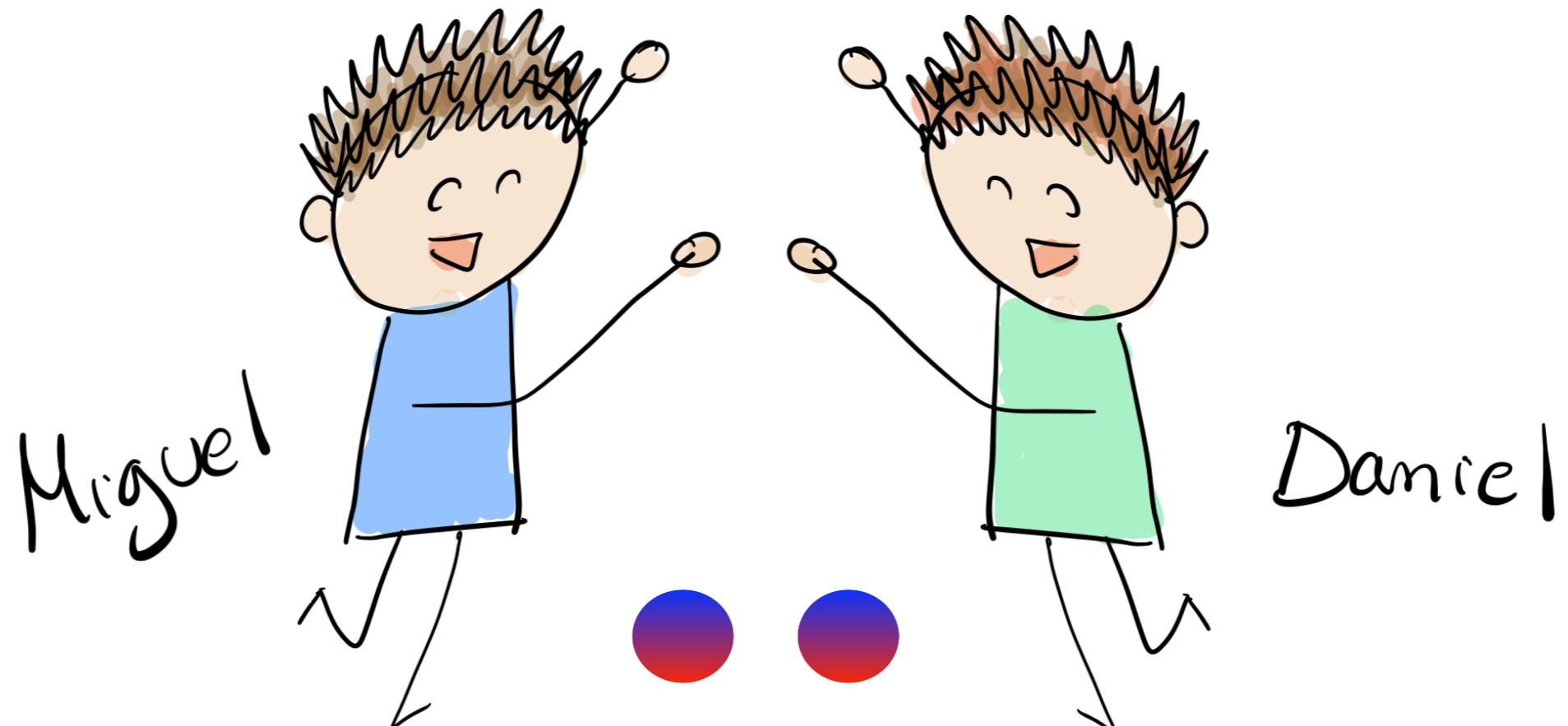
Teleportación cuántica

El objetivo es **transmitir un qubit desconocido** mediante el envío de bits clásicos, entre dos personajes muy muy distantes.

Para eso, se necesita que el emisor y el receptor del mensaje compartan previamente un estado entrelazado, en este caso un EPR.

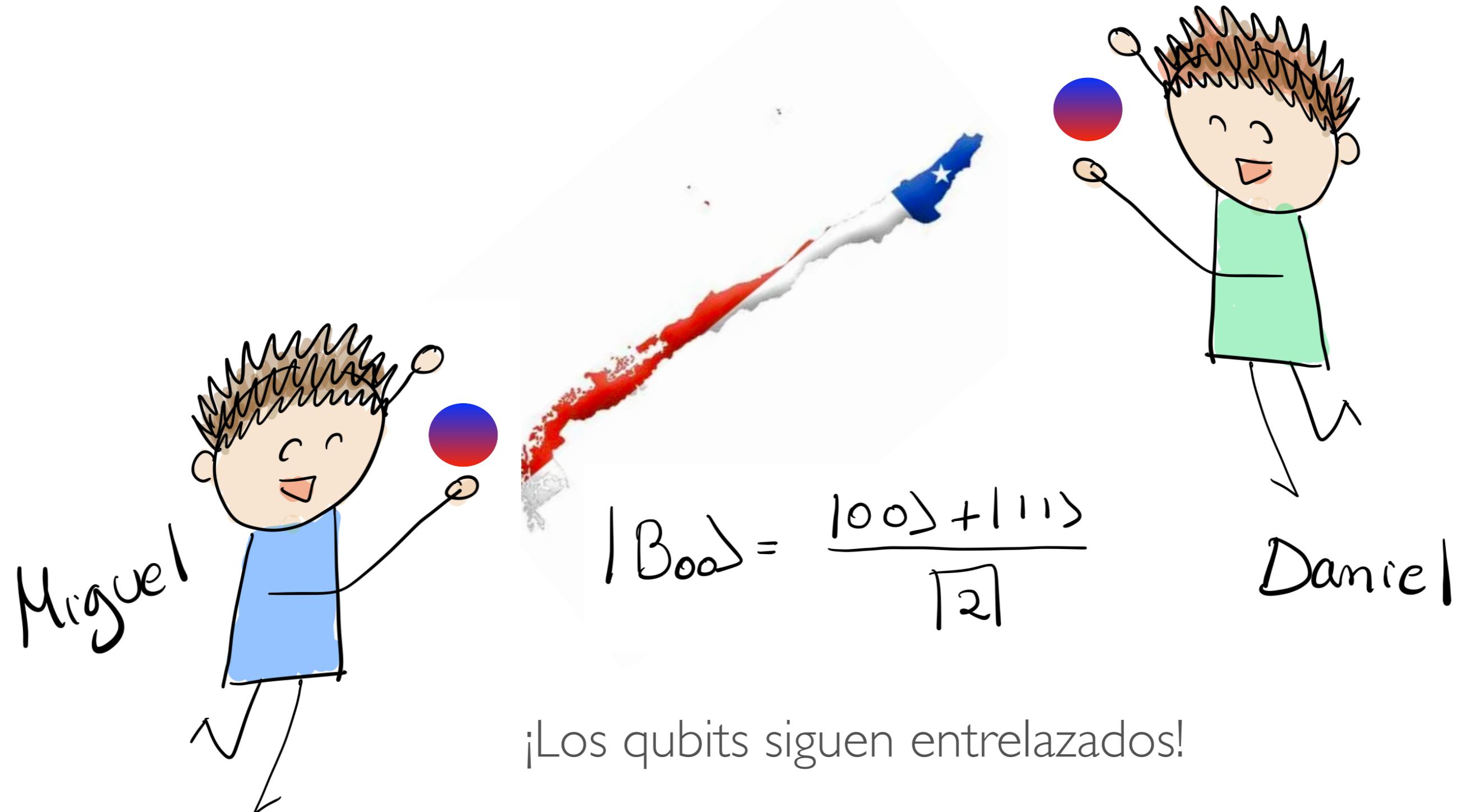
El entrelazamiento sirve como un medio de comunicación. Ni el emisor ni el receptor conocen el estado que se quieren transmitir.

Teleportación cuántica

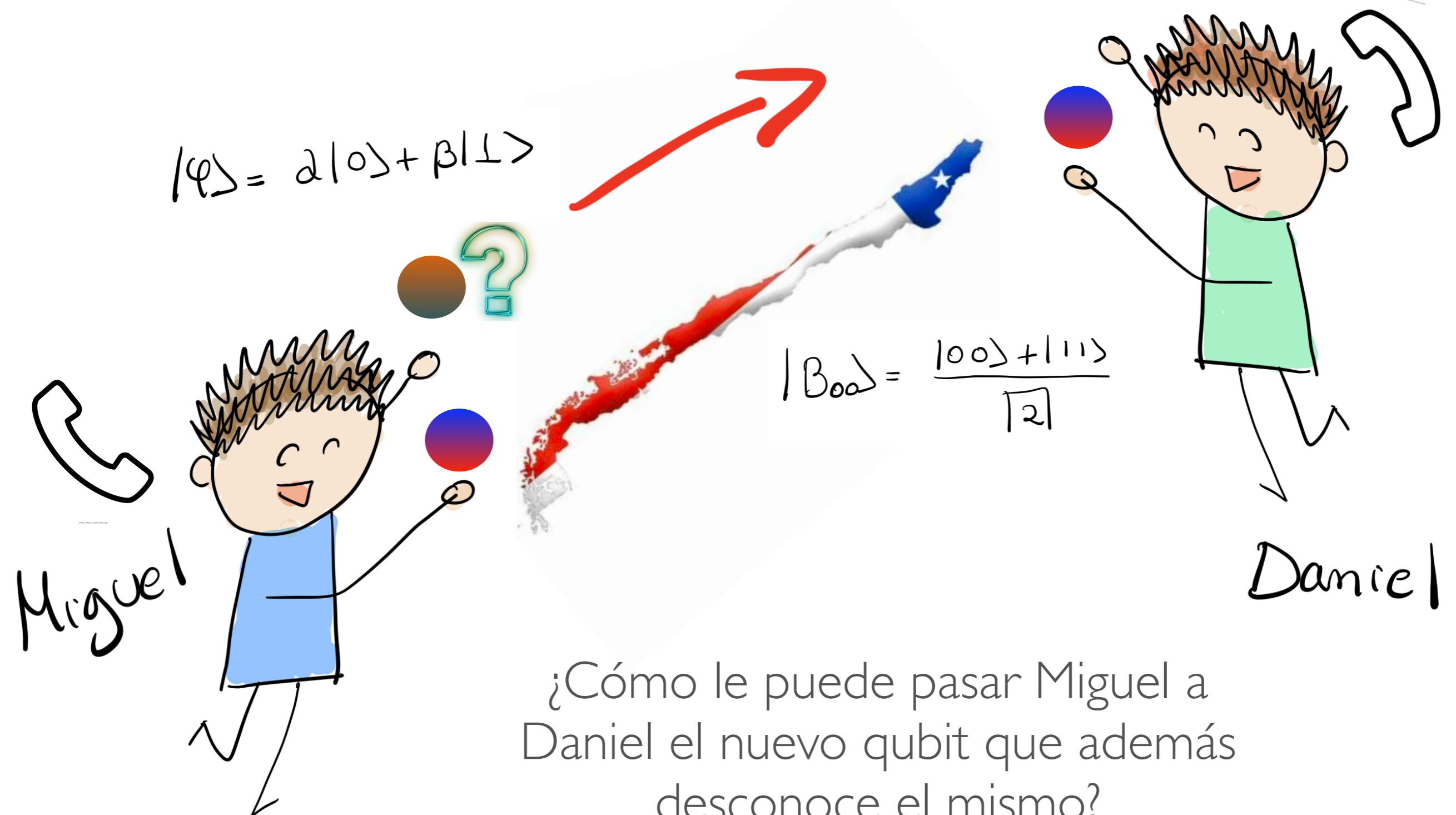


$$|B_{00}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

Teleportación cuántica

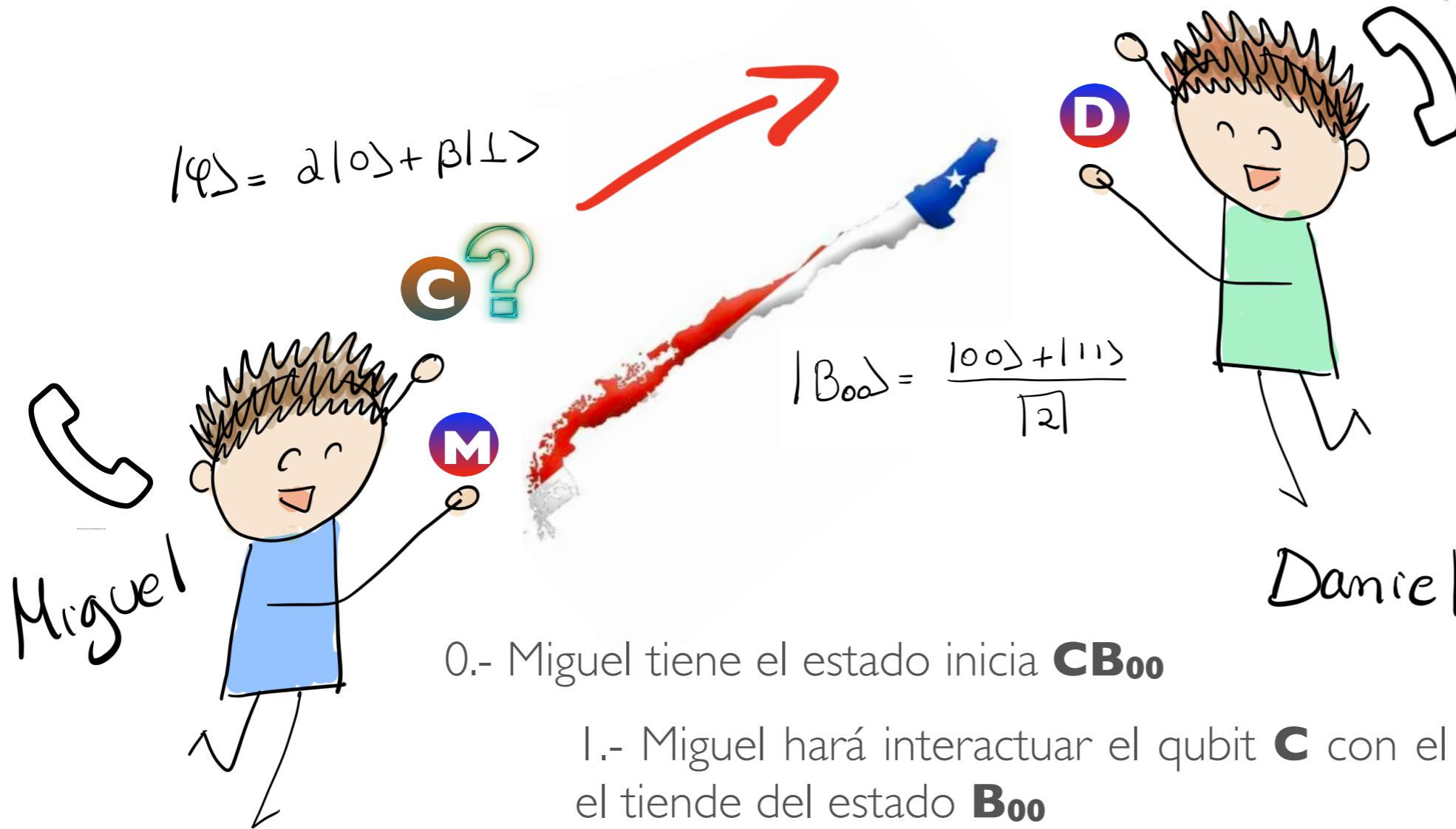


Teleportación cuántica



¿Cómo le puede pasar Miguel a Daniel el nuevo qubit que además desconoce el mismo?

Teleportación cuántica



0.- Miguel tiene el estado inicial **CB₀₀**

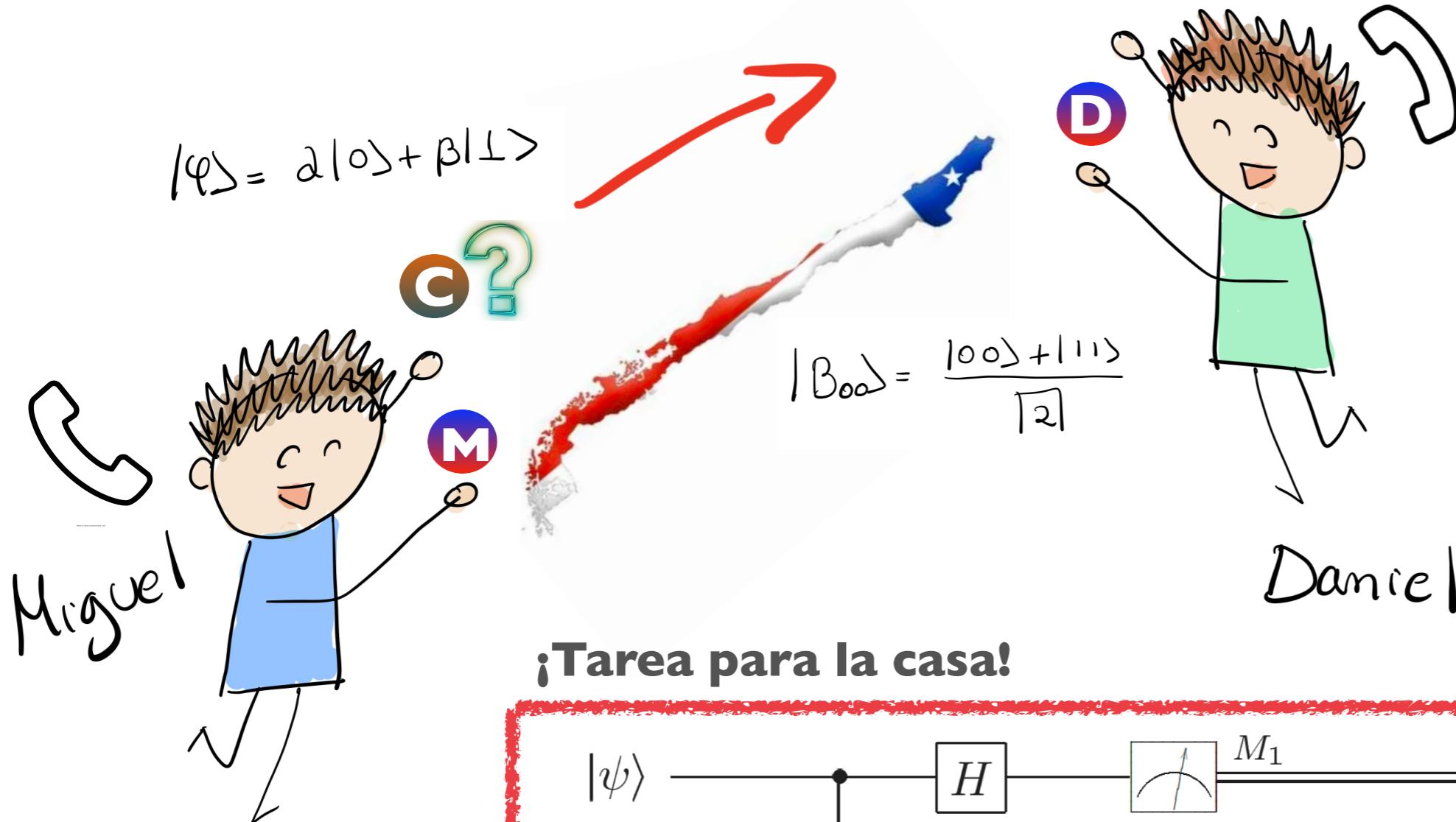
1.- Miguel hará interactuar el qubit **C** con el pedazo que tiene del estado **B₀₀**

2.- Luego Miguel va a realizar mediciones en esos 2 qubits que posee, y obtendrá 1 de los 4 posibles resultados 00, 01, 10, 11.

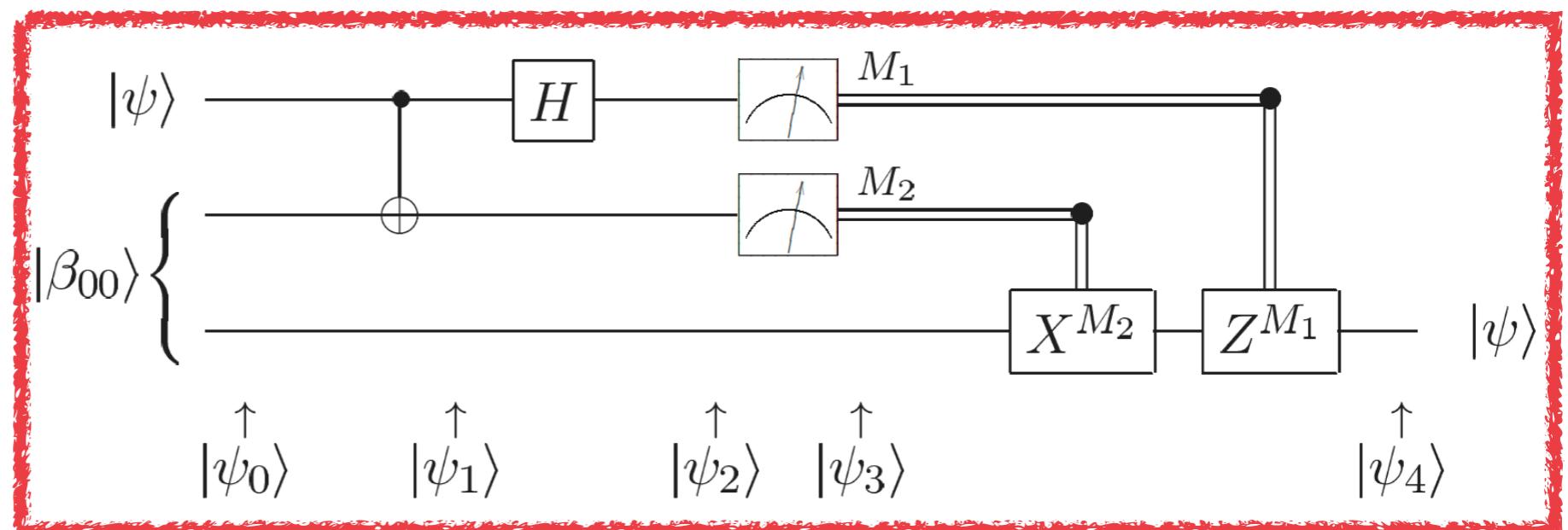
3.- Miguel le dará esta información a Daniel **por teléfono**.

4.- Daniel efectuará una medición (de las 4) en su pedacito del estado **B₀₀**, dependiendo del mensaje de Miguel. **Y magia! Daniel obtiene el estado C que nadie conoce!**

Teleportación cuántica



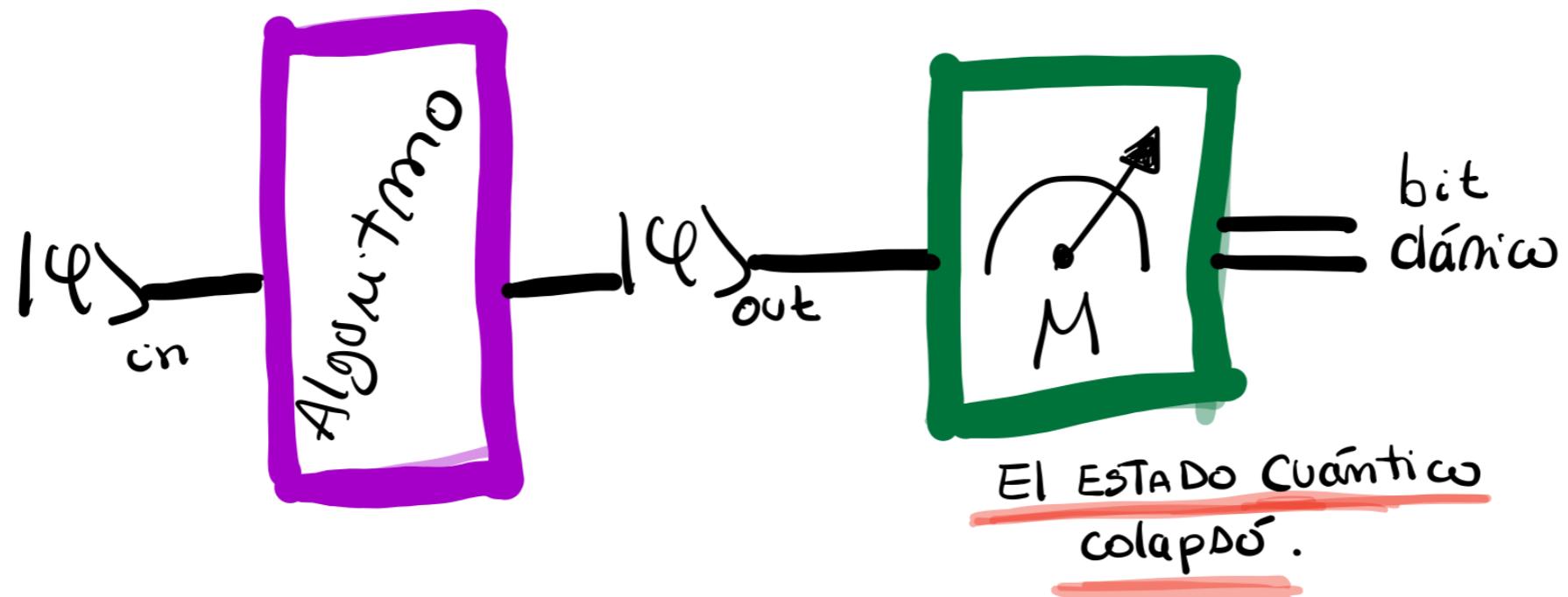
¡Tarea para la casa!



Resumen

- No perder la vista global del problema que están enfrentando, ni perder de vista la magia de la cuántica, compleja y contra-intuitiva, pero que funciona para describir lo que observamos.
- Atrévanse a pensar lo impensable y cuestionárselo todo

CIRCUITO



¡GRACIAS!
SOBRETODO A LOS Y LAS
ORGANIZADORES



FACULTAD DE CIENCIAS FISICAS Y MATEMATICAS
UNIVERSIDAD DE CHILE

