A decorative graphic on the left side of the slide consisting of two overlapping parallelograms. The front one is blue and the back one is a light green. They are positioned diagonally, with the blue one partially covering the green one.

Introducción a la Programación Cuántica

Particularidades del curso

- **Contenido:**
 - Lo más autocontenido posible. No asume ningún conocimiento previo en el tema.
 - Se comenzará repasando la matemática necesaria.
- **Modalidad:**
 - Clases teórico-prácticas.
 - Se requiere participación activa.
- **Requisitos de aprobación:**
 - 70 % de asistencia.
 - Aprobar examen integrador con nota 6 o más.
 - Promoción directa: se aprueba cursada y promoción.

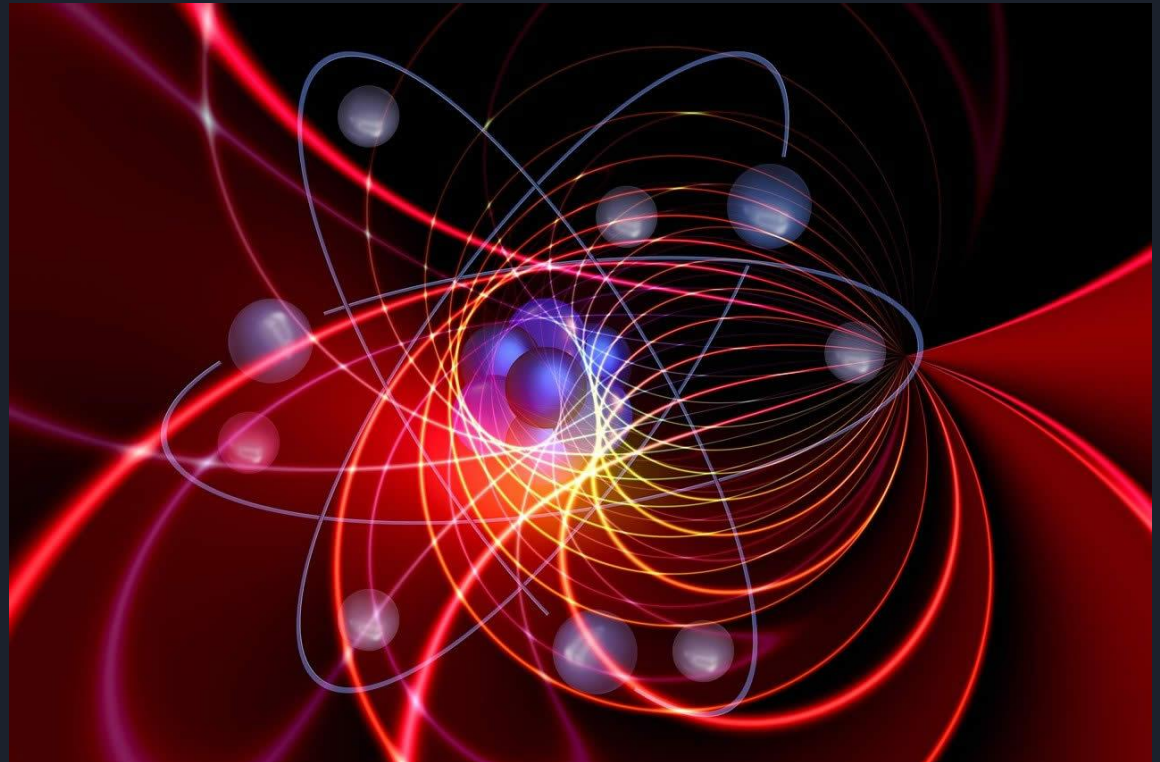
Introducción

Mecánica cuántica

Experimentos con extraños resultados

Mecánica cuántica

- La mecánica cuántica sirve para describir “lo micro” a escala de un electrón, por ejemplo. Las leyes de Newton no aplican a esa escala.
- Tampoco la Teoría de la Relatividad General de Einstein

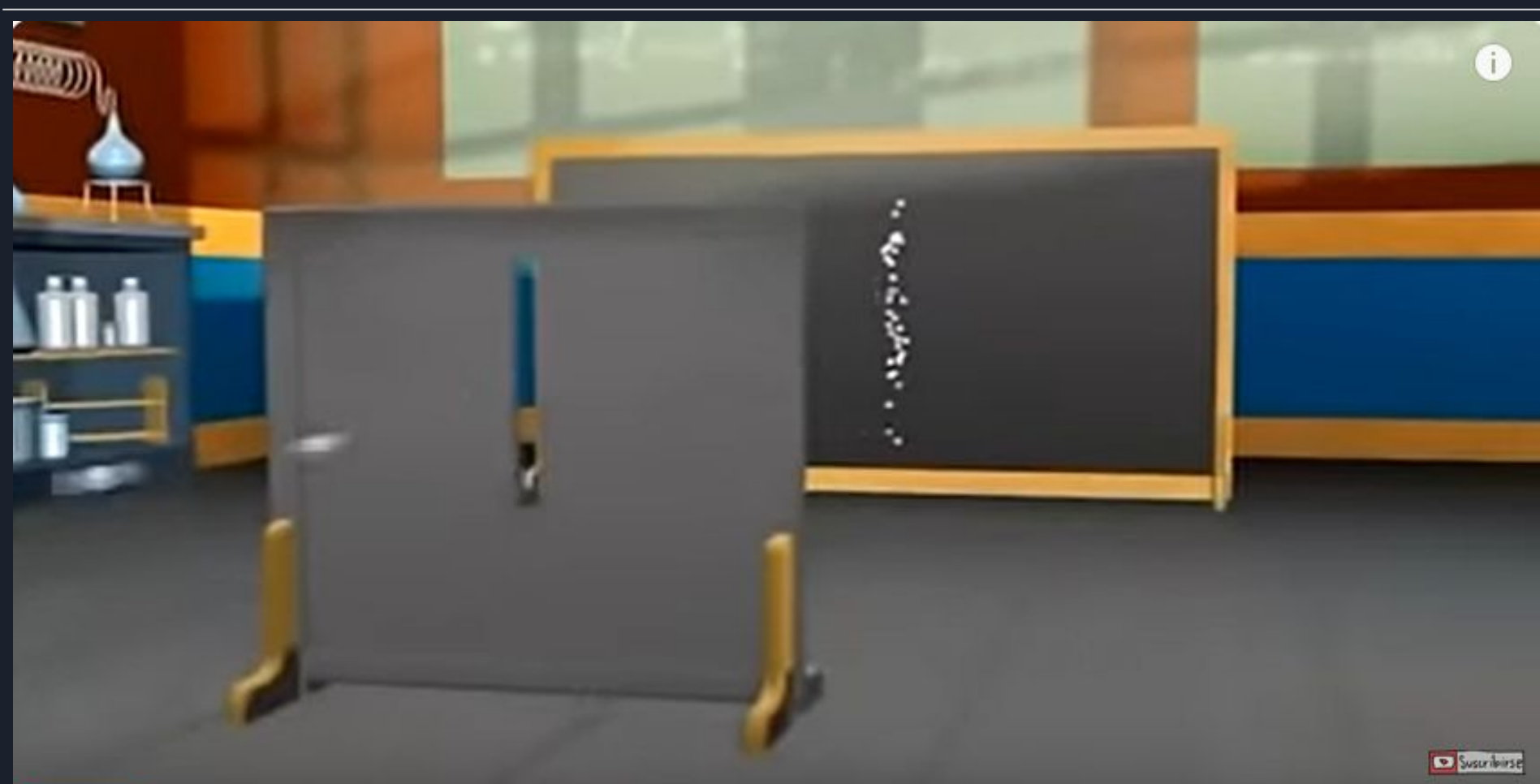


Partículas vs. ondas

- Los físicos siempre han entendido la diferencia entre las partículas y las ondas
- Las partículas están confinadas
- Las ondas se expanden que se transmiten a través de un medio
- Las ondas generan interferencias mientras que las partículas no lo hacen

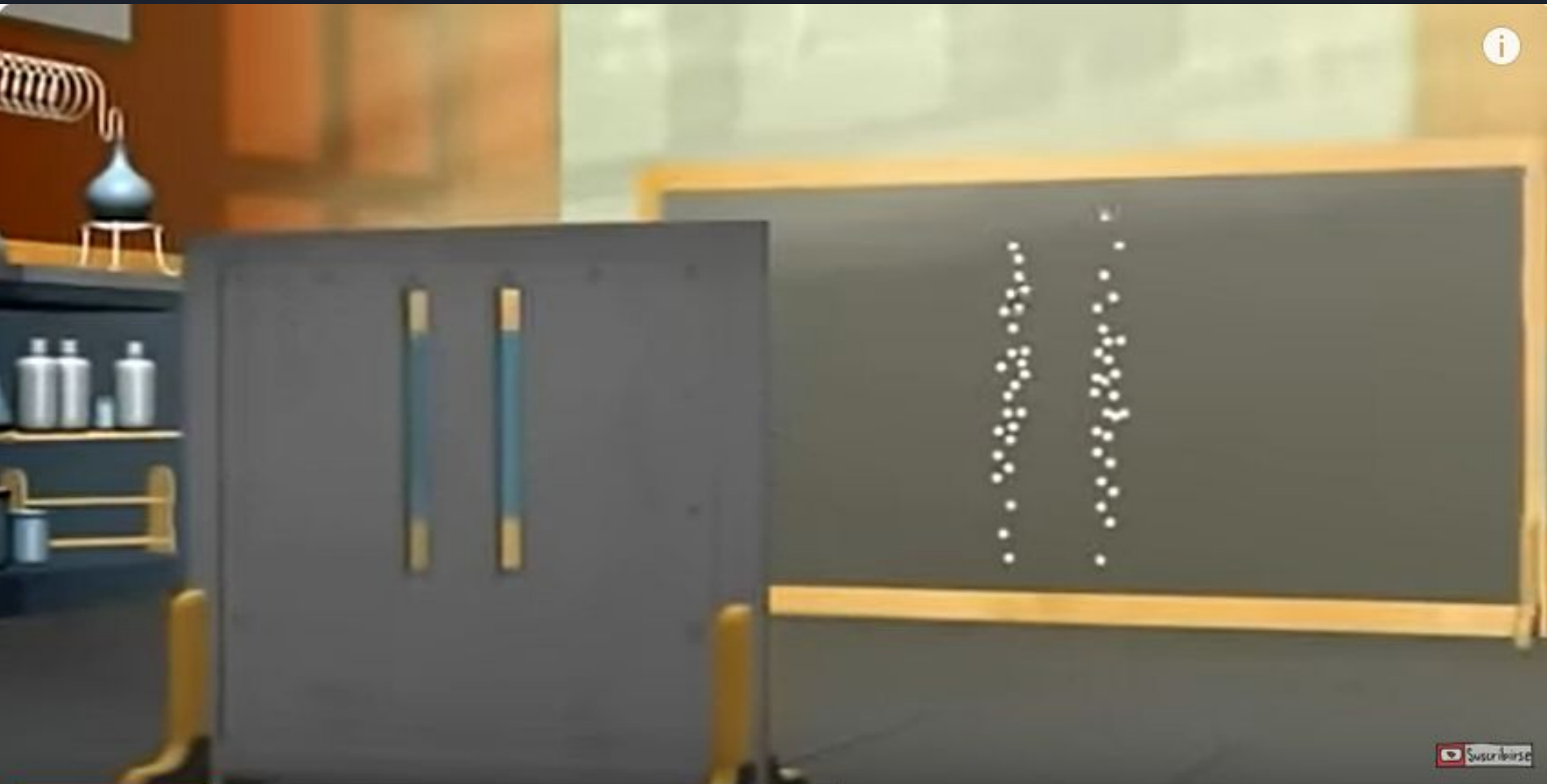
Experimento 1 (nivel macroscópico)

Arrojamos bolitas de pintura a través de una ranura



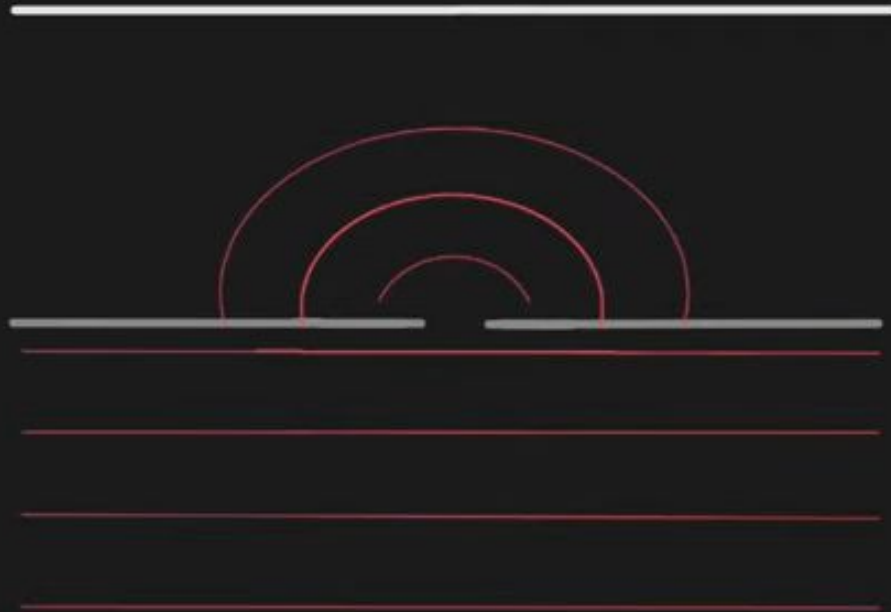
Experimento 2 (nivel macroscópico)

Arrojamos bolitas de pintura a través de dos ranuras

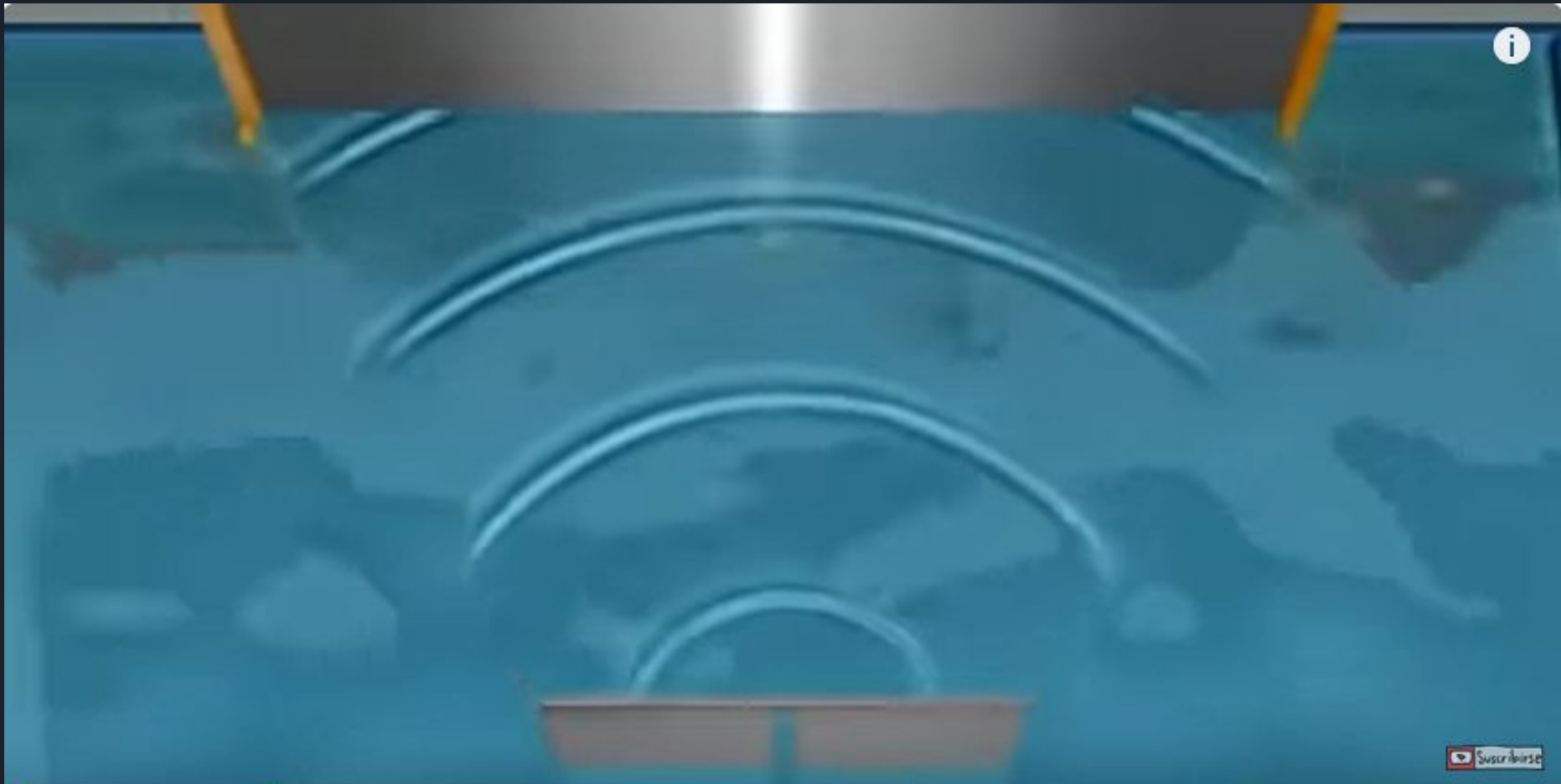


Experimento 3 (nivel macroscópico)

Propagamos una onda a través de una ranura

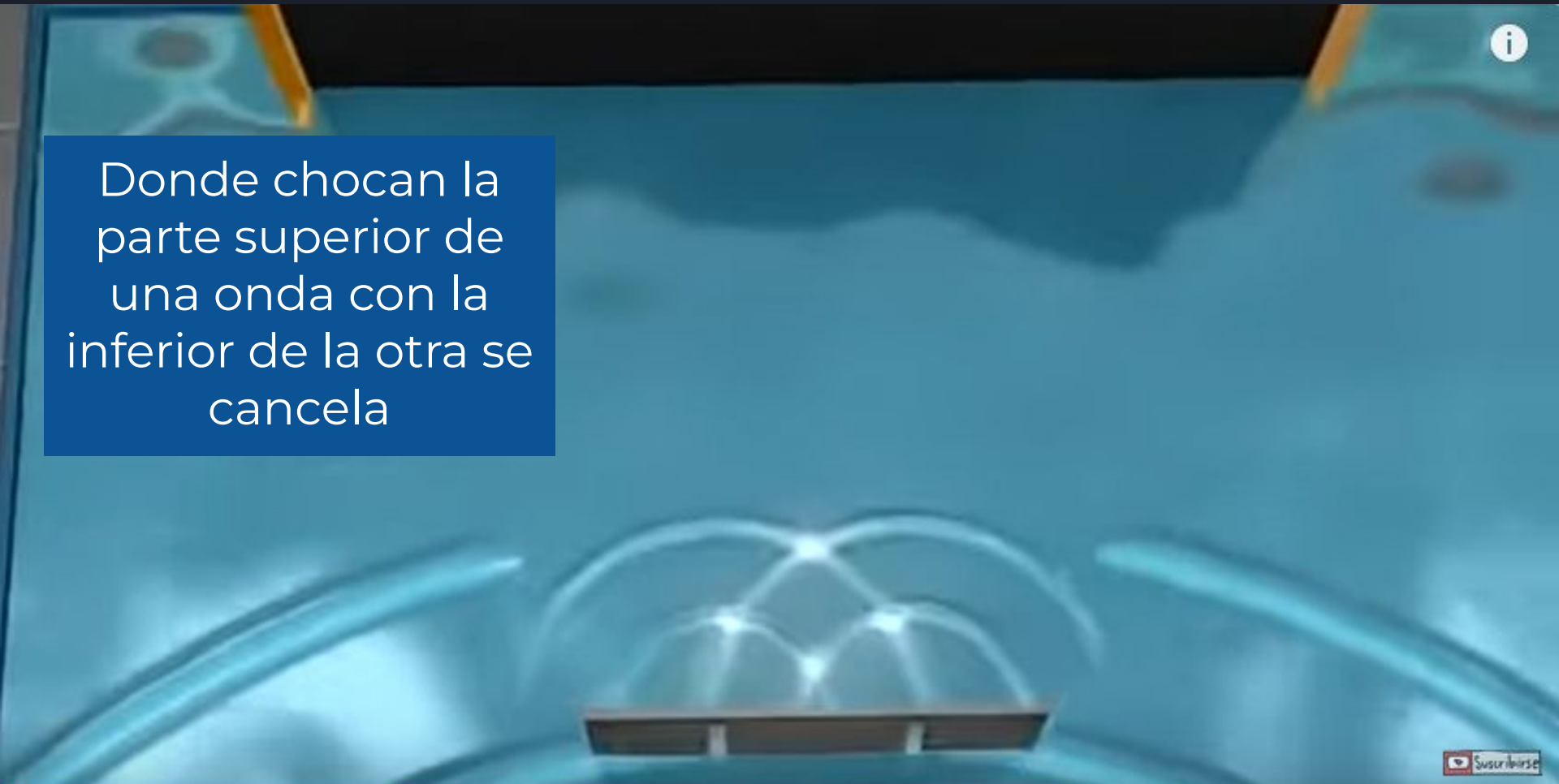


Experimento 3 (nivel macroscópico) Propagamos una onda a través de una ranura

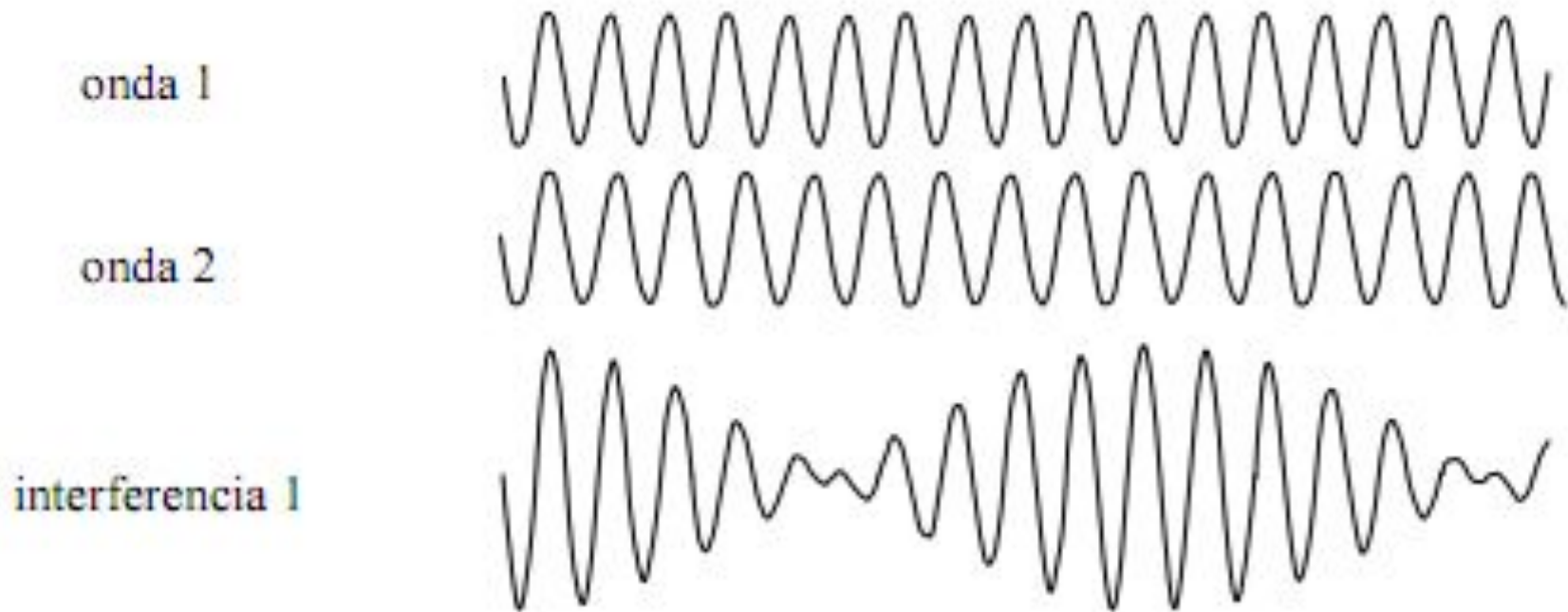


Experimento 4 (nivel macroscópico) Propagamos una onda a través de dos ranuras

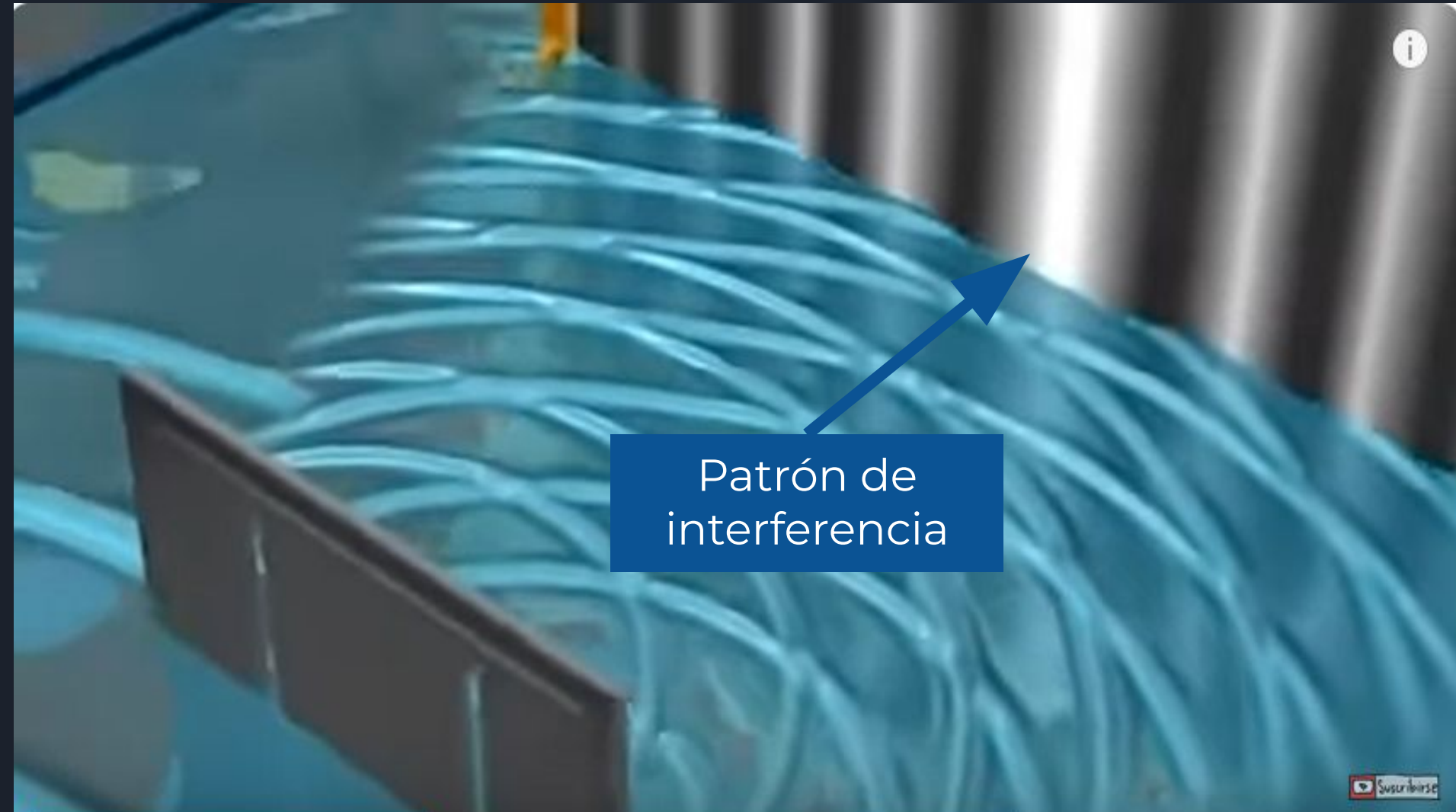
Donde chocan la parte superior de una onda con la inferior de la otra se cancela



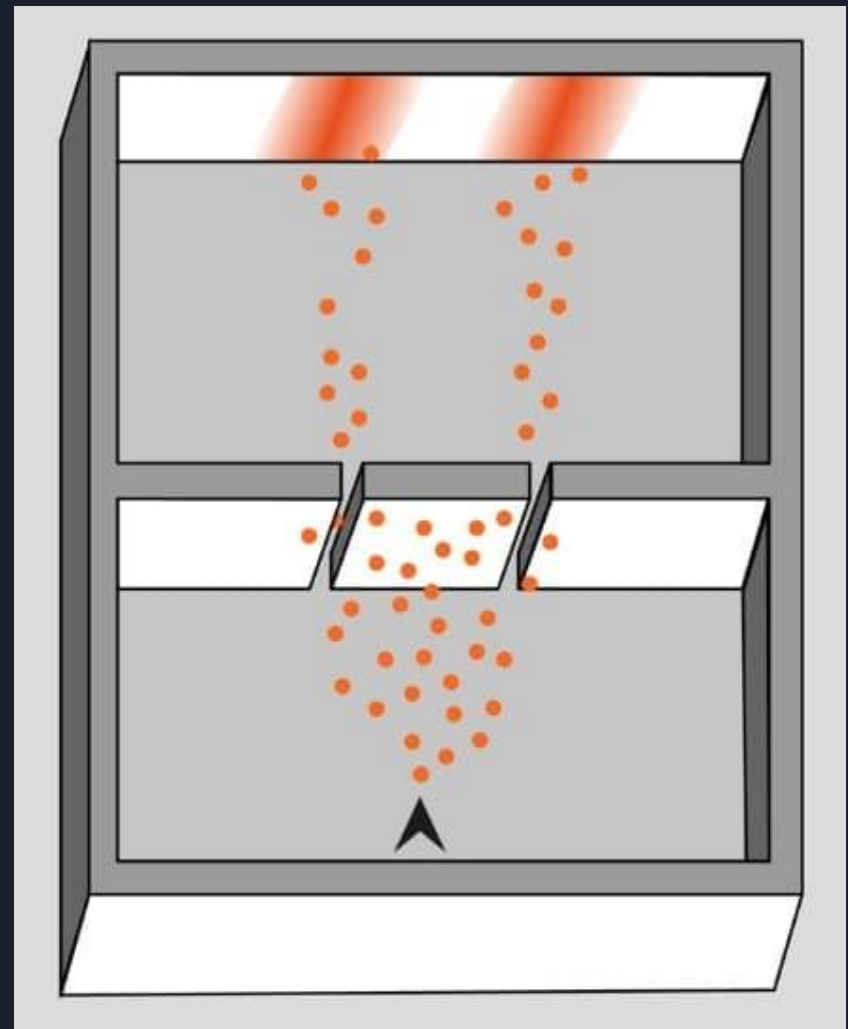
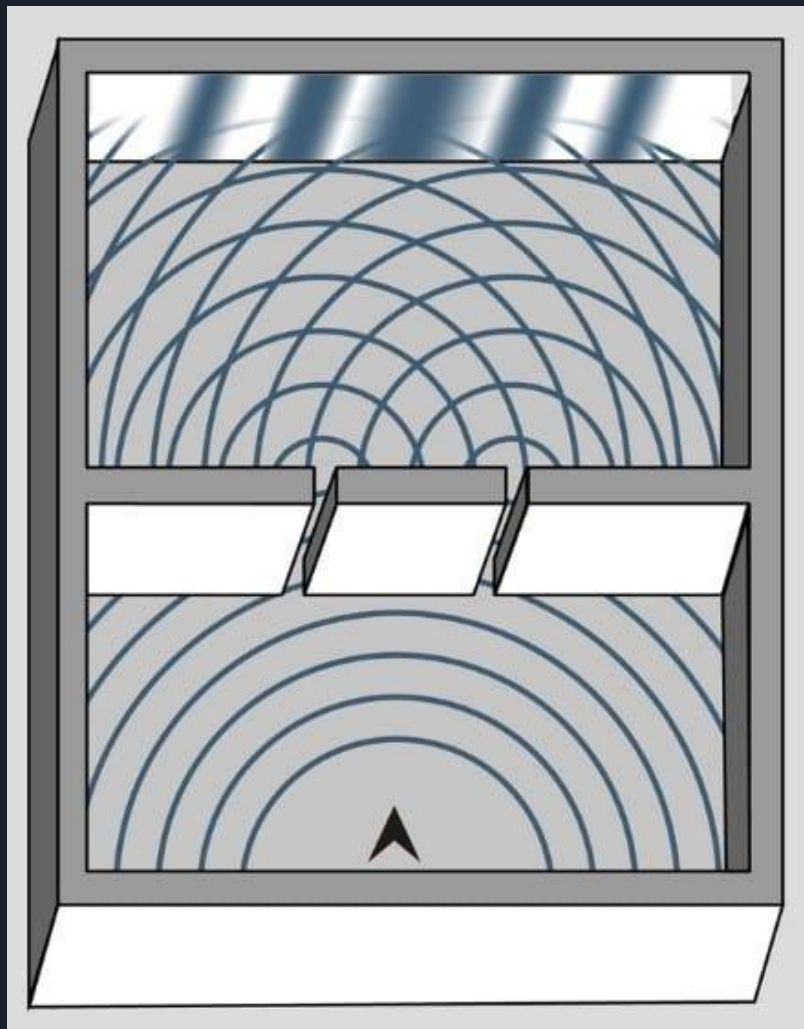
Interferencia de ondas




Experimento 4 (nivel macroscópico) Propagamos una onda a través de dos ranuras



A la izquierda vemos la firma de la naturaleza ondulatoria y a la derecha la de partículas





Experimento 5 (nivel microscópico) Arrojamos electrones a través de una ranura

¿ Qué pasará si en lugar de arrojar objetos macroscópicos **arrojamos objetos microscópicos**, por ejemplo: electrones ?

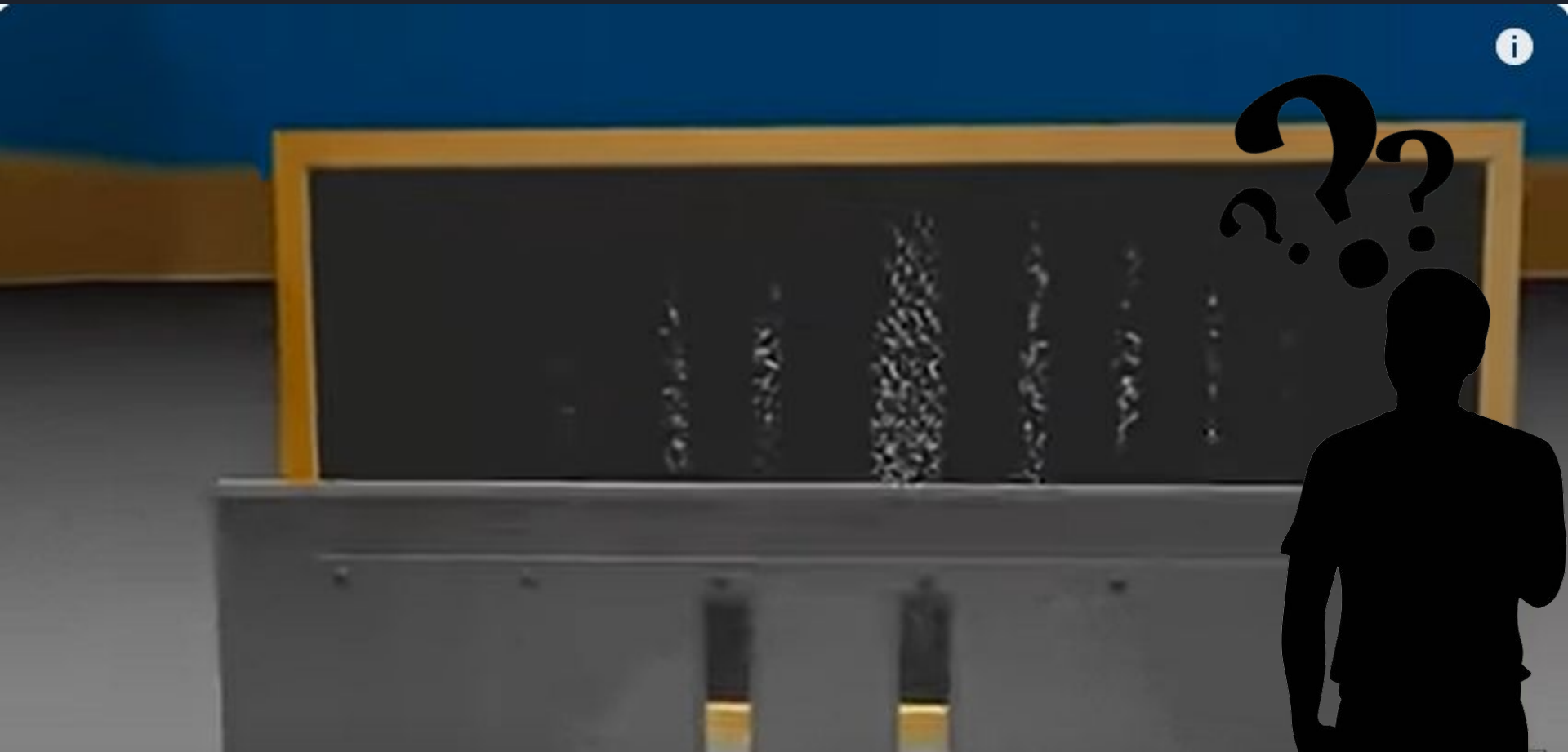
Cuando se hizo este experimento los físicos ya habían medido la masa de un electrón, estaba claro que el **electrón** es una **partícula confinada** y con masa bien definida

Experimento 5 (nivel microscópico) Arrojamos electrones a través de una ranura



Con una ranura los electrones se comportan como las
bolitas de pintura

Experimento 6 (nivel microscópico) Arrojamos electrones a través de dos ranuras



Pero con dos ranuras los electrones se comportan como las ondas (patrón de interferencia)

Experimento 6 (nivel microscópico) Arrojamos electrones a través de dos ranuras

Para ver este patrón es necesario que algunos electrones hayan pasando por una rendija y otros por la otra y hayan interferido de alguna manera entre sí



Pero con dos ranuras los electrones se comportan como las ondas (patrón de interferencia)



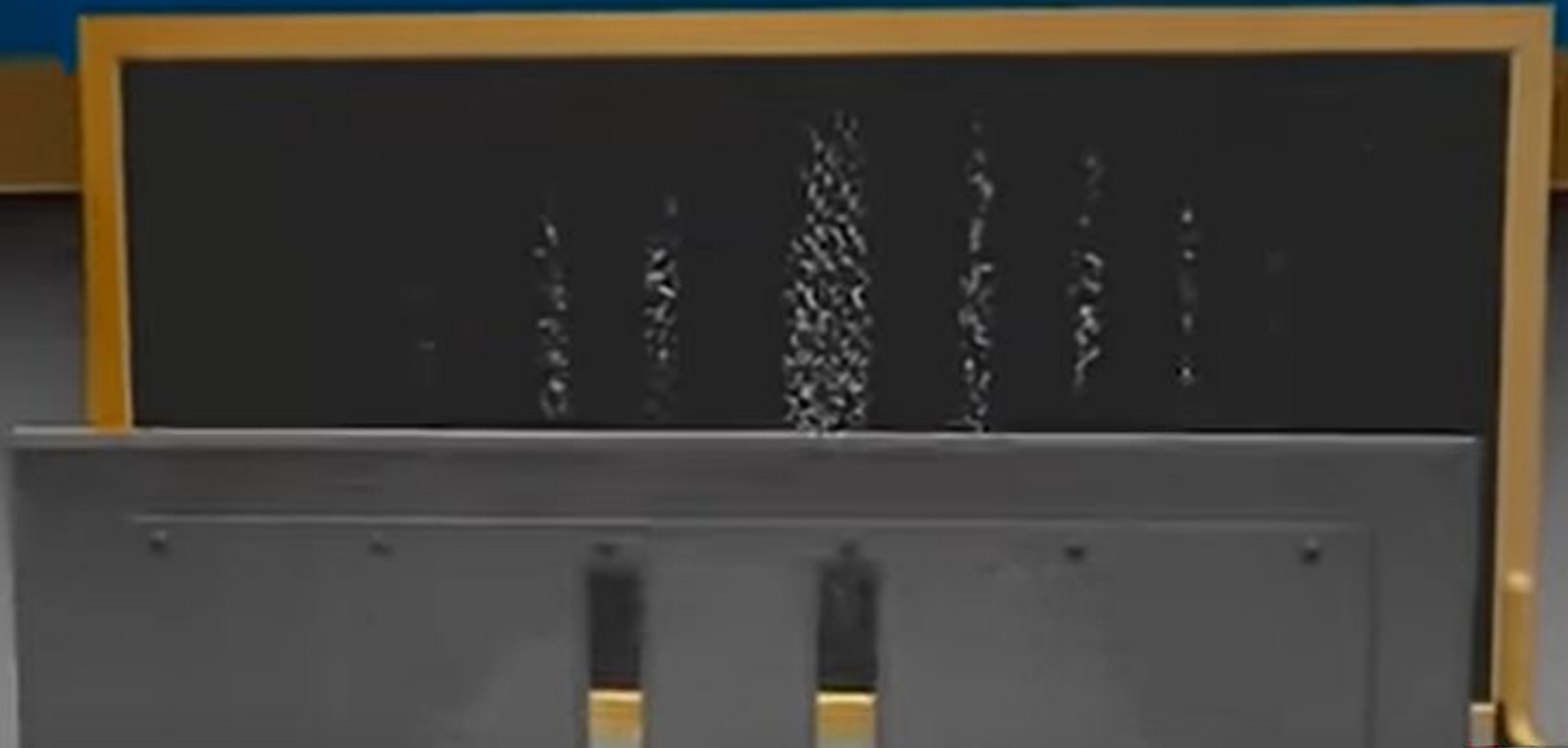
Experimento 7 (nivel microscópico) Arrojamos electrones a través de dos ranuras

¿Y si enviamos electrones de a uno por vez?

De esta manera un electrón no podrá interferir con
otro electrón

Experimento 7 (nivel microscópico)

Arrojamos electrones de a uno por vez a través de dos ranuras



Enviando electrones de a uno por vez, volvemos a tener el mismo patrón de interferencia

Experimento 7 (nivel microscópico) Arrojamos electrones de a uno por vez a través de dos ranuras



¿¿ Cómo puede ser ??

Experimento 7 (nivel microscópico)

Arrojamos electrones de a uno por vez a través de dos ranuras



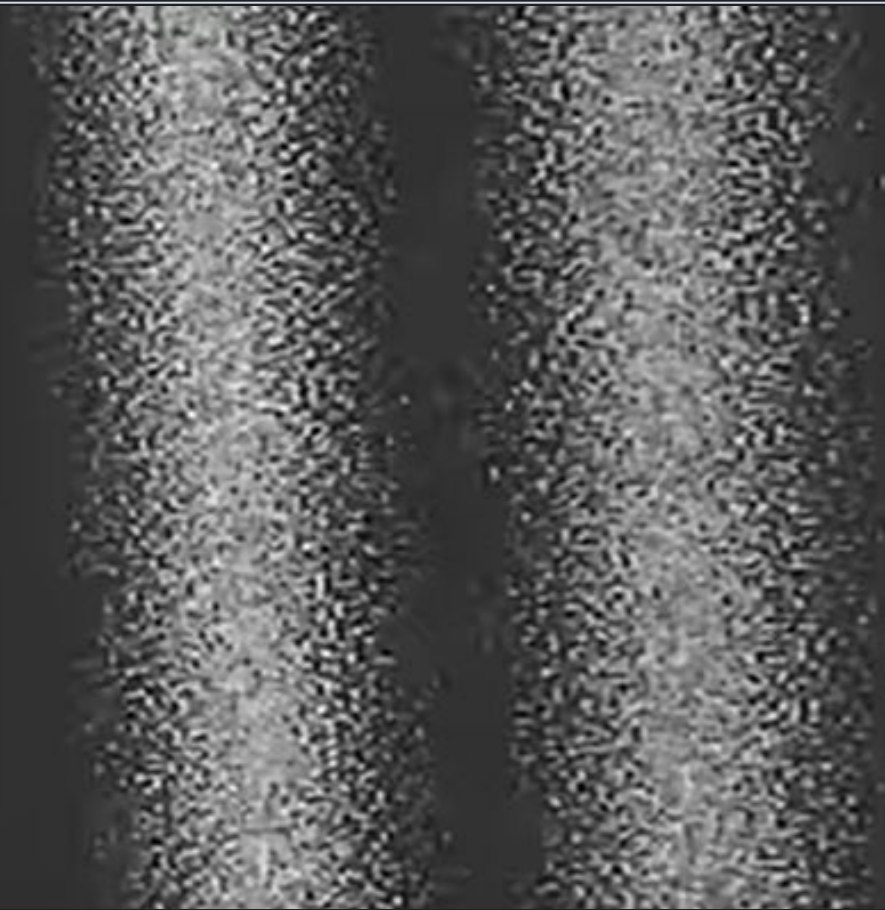
¿¿ Acaso cada electrón pasó por las dos ranuras a la vez ??

Experimento 8 (nivel microscópico) Agregamos un detector



Colocamos un detector para identificar la ranura por la que
pasa cada electrón

Experimento 8 (nivel microscópico) Agregamos un detector



El sólo hecho de observar provocó que los electrones
volvieran a comportarse como partículas

Conclusiones e interrogantes a partir de estos experimentos

- Antes de la mecánica cuántica estaba claro que las partículas y las ondas son cosas distintas, incluso antagonistas
- Ahora podemos ver que los electrones se comportan a veces como partículas y otras como ondas
- ¿Son los electrones a la vez ondas y partículas? ¿O no son ni una cosa ni la otra? ¿Mientras no lo observes, un electrón está al mismo tiempo en dos lugares distintos?
- Hay una matemática precisa que modela estos fenómenos cuánticos y nos permite predecirlos, sin embargo nadie sabe bien cómo interpretarlos.

La función de onda de Schrodinger



Del canal de Youtube QuantumFracture

La función de onda de Schrodinger



La función de onda es un campo que asigna a cada instante en cada punto del espacio un número complejo

La función de onda de Schrodinger



Born se dio cuenta que elevando al cuadrado el módulo del nro. complejo obtenía otro campo que capturaba la esencia del mundo cuántico

La función de onda de Schrodinger



Cuanto mayor sea este número, mayor la probabilidad de encontrar allí a la partícula cuando colapse

La función de onda de Schrodinger



Antes del colapso, la partícula se propaga en el espacio como una onda de probabilidades. En cada instante la partícula está en todas partes en un estado de superposición cuántica

La función de onda de Schrodinger



¿Qué es la función de onda? ¿Qué refleja del mundo real?
En realidad, no lo sabemos, eso corresponde al área de las
interpretaciones de la física cuántica

¿En qué consisten las ciencias fácticas?



¿En descubrir lo que es la realidad?

o

¿En descubrir cómo se comporta la realidad?

¿En qué consisten las ciencias fácticas?

¿Queremos **EXPLICAR**
o sólo **DESCRIBIR**?

¿Queremos **ENTENDER**
o sólo poder **PREDECIR**?

¿En qué consisten las ciencias fácticas?

¿Tenemos que entender cómo es en realidad un sistema para poder predecir cómo se va a comportar?

La respuesta es que no, la mecánica cuántica es una muestra de ello.

¿En qué consisten las ciencias fácticas?

- El **instrumentalismo** es una postura dentro de la ciencia.
- Los instrumentalistas no se preocupan por las interpretaciones (debates ontológicos), les alcanza con contar con un modelo que les permita predecir el estado del sistema. Frase representativa: “**Calla y calcula!**”

Otros principios cuánticos

Complementariedad

Ciertas propiedades de un sistema cuántico son complementarias.

*Esto significa que **no pueden ser medidas o conocidas simultáneamente** con precisión arbitraria.*

Otros principios cuánticos

Complementariedad

El ejemplo clásico es la **dualidad
onda-partícula**.

No podemos observar ambas naturalezas
simultáneamente.

Otros principios cuánticos

Entrelazamiento

Dos o más partículas pueden estar vinculadas de forma que el estado de una depende del de la otra, sin importar la distancia. Al medir una, se define instantáneamente el estado de su partícula entrelazada

Otros principios cuánticos

Entrelazamiento

Einstein lo llamó “acción espeluznante a distancia” (spooky action at a distance).

*“¿Por qué es importante en computación? El entrelazamiento permite **crear correlaciones complejas** entre qubits, esencial para algoritmos cuánticos avanzados y para la corrección de errores.”*



De la Curiosidad Cuántica al Poder Computacional

Los fenómenos que hemos visto, como la **superposición** la **interferencia** y el **entrelazamiento** no son solo rarezas teóricas.

Son los **recursos fundamentales** que la **computación cuántica** explota para procesar información de una manera radicalmente nueva y potente.

Computación cuántica



Enero de 2024

Del canal de Youtube Instituto de Física
Teórica IFT

Computación cuántica

- ★ Los ordenadores cuánticos no son aún eficientes. Se trata de una tecnología en desarrollo
- ★ No se pueden hacer promesas, pero tienen un potencial revolucionario
- ★ No son simplemente unos ordenadores más rápidos. Es un cambio de paradigma en la computación.

Computación cuántica

Física Cuántica

- ★ Superposición de estados
- ★ Probabilidad en la medida

Computación cuántica



Computación cuántica



Computación cuántica

$$|A\rangle + |B\rangle$$



Computación cuántica

Cuando lo observo (lo mido) **COLAPSA** a uno de los dos estados (interpretación de Copenhage)



$$|A\rangle + |B\rangle \rightarrow |A\rangle$$

Computación cuántica

QUBITS

El qubit es la versión cuántica del bit

Se trata de un objeto abstracto que puede estar en dos estados:

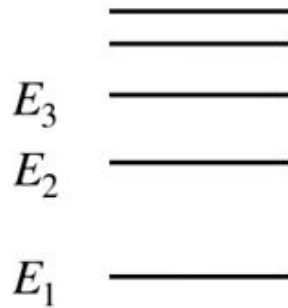
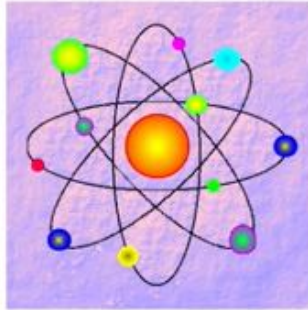
$$|0\rangle, \quad |1\rangle$$

...o en una superposición arbitraria de ellos:

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

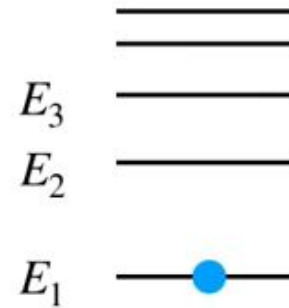
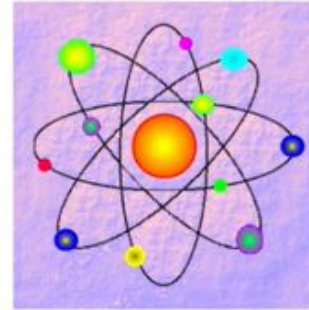
Computación cuántica

Átomo



$|0\rangle$

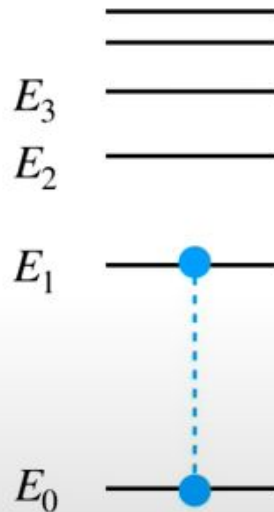
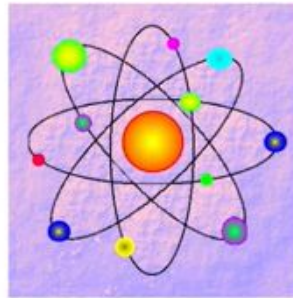
Átomo



$|1\rangle$

Computación cuántica

Átomo



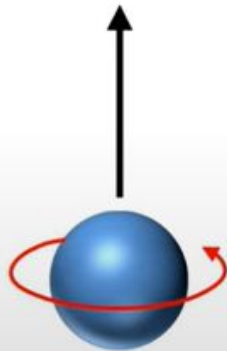
$$a|0\rangle + b|1\rangle$$

Computación cuántica

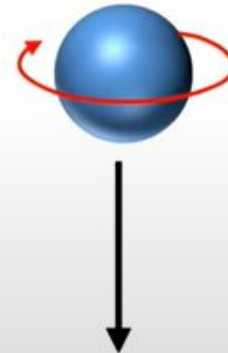
QUBITS

Espín del electrón

$|0\rangle$

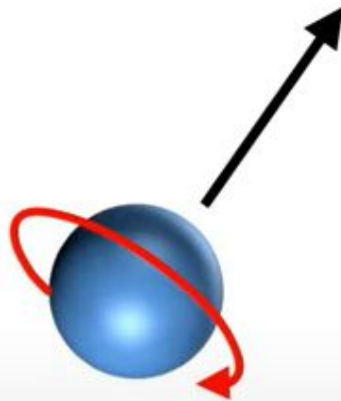


$|1\rangle$

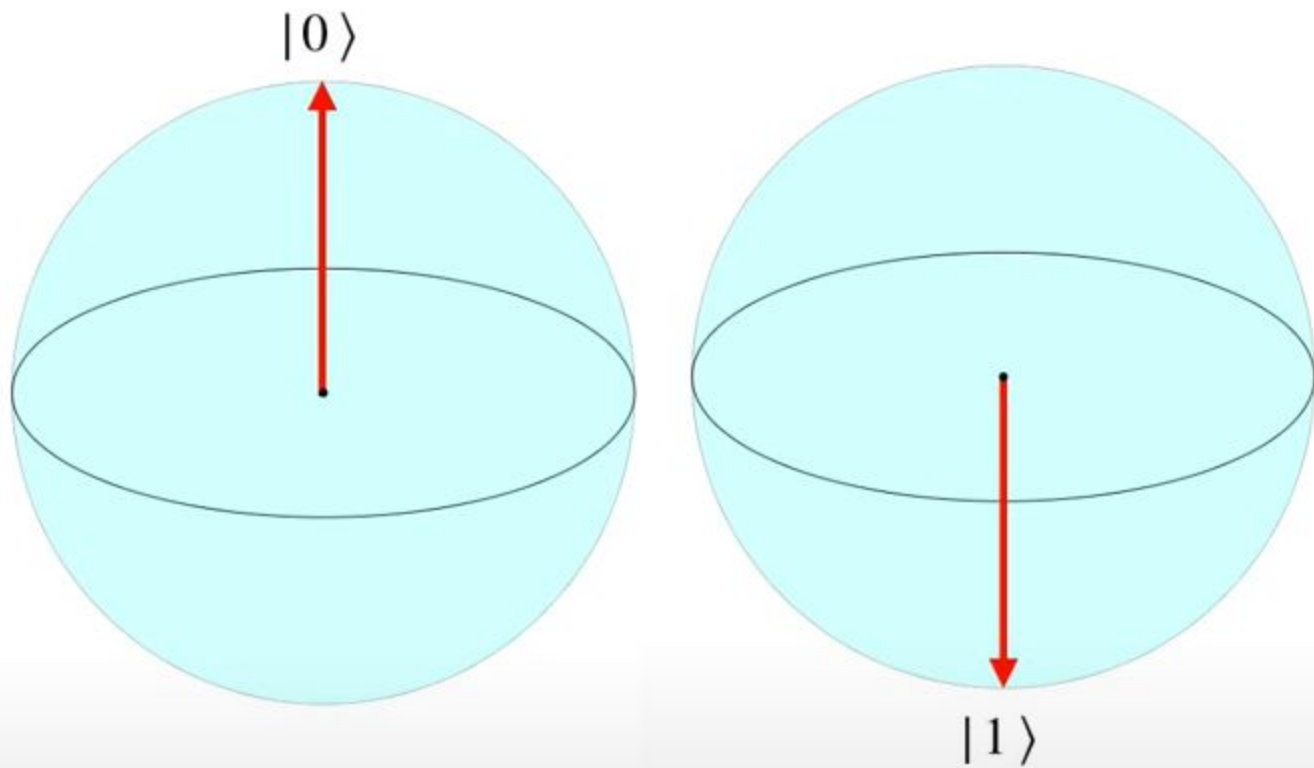


Computación cuántica

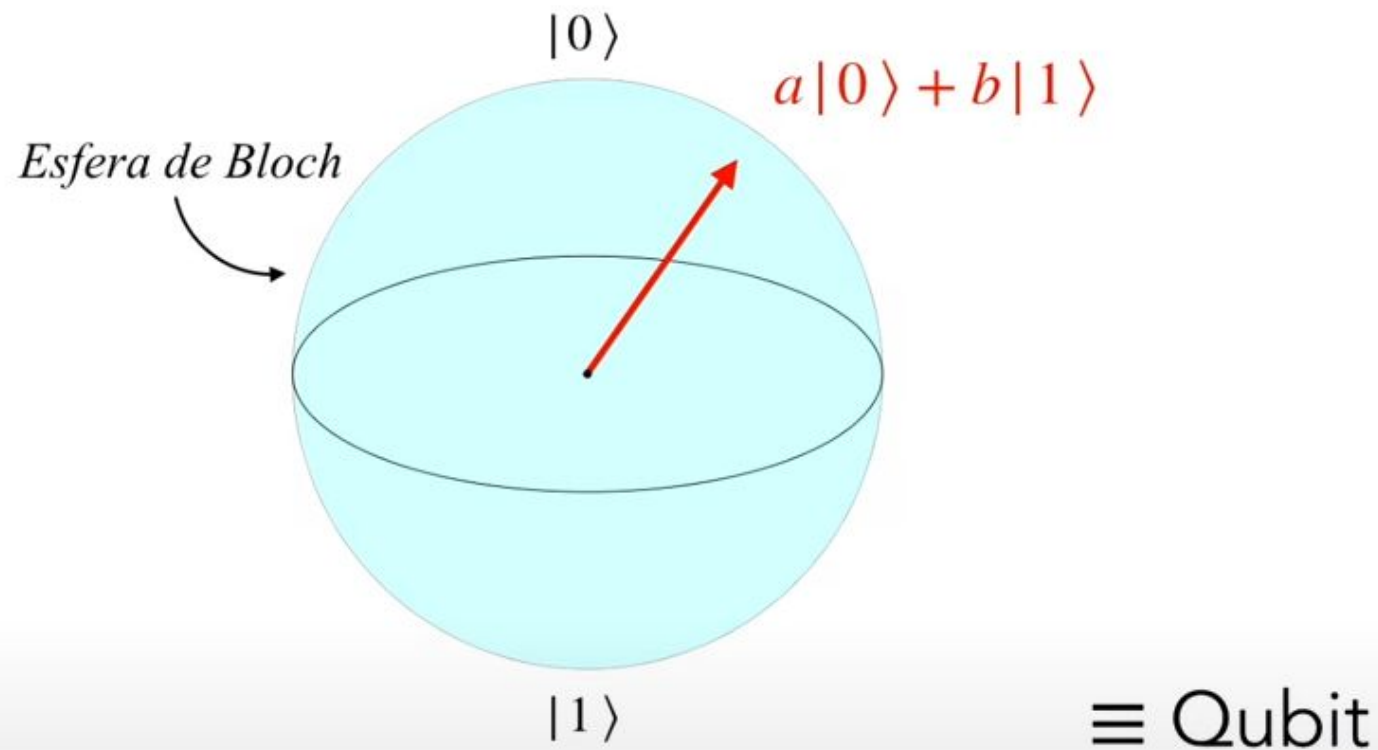
$$a|0\rangle + b|1\rangle$$



Computación cuántica



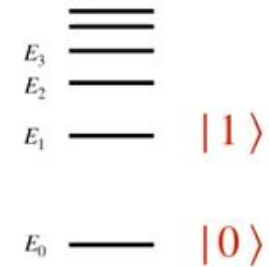
Computación cuántica



Computación cuántica

Realización de QUBITS en la práctica

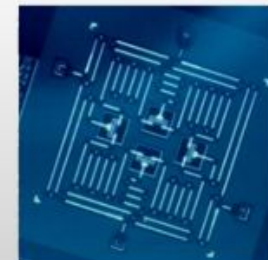
- ★ Estados de iones atrapados
"Trapped ions"



- ★ Fotones

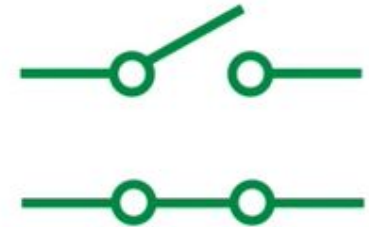


- ★ Estados de circuitos superconductores



Computación cuántica

En principio, cualquier sistema físico con dos estados, $|0\rangle$ y $|1\rangle$, puede servir como qubit

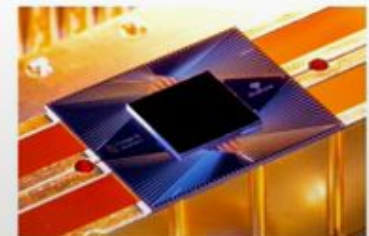


Pero además hace falta que se puedan crear superposiciones arbitrarias $a|0\rangle + b|1\rangle$

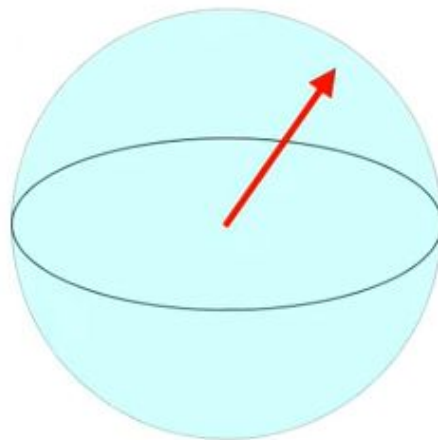
... y que puedan manipularse.



Ordenador Cuántico



Computación cuántica



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

Dado que los coeficientes a y b son arbitrarios, el qubit puede estar en infinitos estados



Computación cuántica

Sin embargo...

Los qubits tienen una limitación:

La forma de extraer la información que contienen

Computación cuántica

¿Cómo podemos extraer la información almacenada en el estado de un qubit?

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

¡Realizando alguna observación sobre él!

Pero al observar se produce el colapso del estado

Computación cuántica



$$|A\rangle + |B\rangle \rightarrow |A\rangle$$

Computación cuántica

$$a|0\rangle + b|1\rangle \longrightarrow \begin{cases} |0\rangle \\ |1\rangle \end{cases}$$

Casi toda la información previa se pierde

Computación cuántica

Sin embargo, mientras el qubit no sea medido, conserva toda la información.

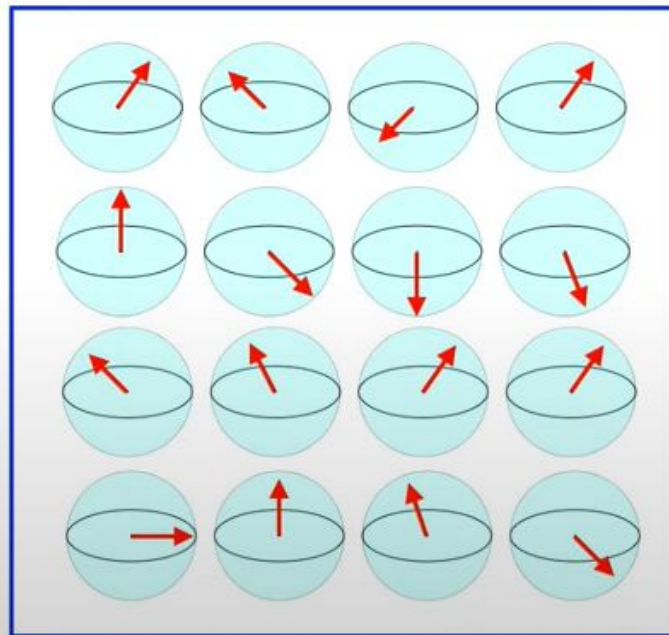


Se pueden manipular los qubits, sin perder ninguna información, hasta la medida final.

Computación cuántica

El verdadero poder de los qubits surge cuando se consideran colectivamente.

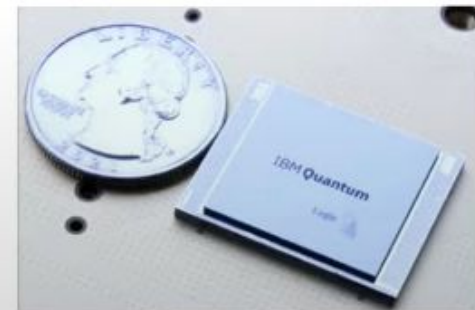
Un ordenador cuántico es un conjunto de qubits que interactúan entre ellos



Computación cuántica

Memoria

- ★ Un ordenador portátil convencional tiene **billones de bits** en su memoria
- ★ El superordenador más potente tiene **~ 1 trillón de bits**
- ★ Los ordenadores cuánticos más potentes tienen **~ 100 qubits**



Computación cuántica

Comparemos 2 bits con 2 qubits

En 2 bits podemos almacenar 2 números binarios.

0	0
0	1
1	0
1	1

Computación cuántica

Comparemos 2 bits con 2 qubits

2 qubits pueden estar en los estados

$$|0\rangle_1 |0\rangle_2$$

$$|0\rangle_1 |1\rangle_2$$

$$|1\rangle_1 |0\rangle_2$$

$$|1\rangle_1 |1\rangle_2$$

... o en una superposición de ellos

Computación cuántica

Comparemos 2 bits con 2 qubits

El estado más general de 2 qubits es:

$$a|0\rangle_1|0\rangle_2 + b|0\rangle_1|1\rangle_2 + c|1\rangle_1|0\rangle_2 + d|1\rangle_1|1\rangle_2$$

4 números

La información se almacena en los coeficientes de la superposición

Computación cuántica

En general

N bits \longrightarrow $\sim N$ números

N qubits \longrightarrow $\sim 2^N$ números

La ventaja cuántica aumenta de forma exponencial:

Computación cuántica

2 qubits \longrightarrow 4 números
4 qubits \longrightarrow 16 números
⋮
60 qubits \sim



143 qubits \sim



Un supercomputador donde cada átomo de todo el silicio de la tierra almacena un bit

273 qubits \sim



Un bit en cada partícula del universo

Computación cuántica



- ★ Al medir se pierde casi toda la información

$$\begin{aligned}
 & a_1 |0000\rangle + a_2 |0001\rangle + a_3 |0010\rangle + a_4 |0011\rangle \\
 & + a_5 |0100\rangle + a_6 |0101\rangle + a_7 |0110\rangle + a_8 |0111\rangle \\
 & + a_9 |1000\rangle + a_{10} |1001\rangle + a_{11} |1010\rangle + a_{12} |1011\rangle \\
 & + a_{13} |1100\rangle + a_{14} |1101\rangle + a_{15} |1110\rangle + a_{16} |1111\rangle
 \end{aligned}
 \quad \Rightarrow \quad |1101\rangle$$

- ★ Pero hasta el momento de medir es información útil

Computación cuántica

Computación clásica = Manipulación de bits



$\{100111011000101101\dots\}$ $\{001110101110100100\dots\}$

Computación cuántica = Manipulación de qubits

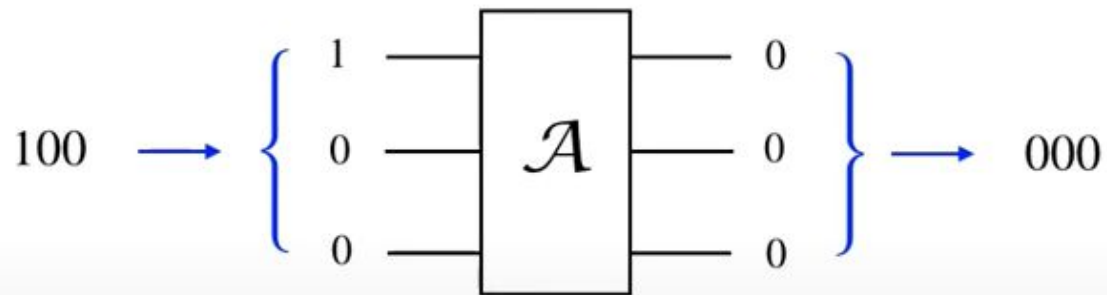


$\{|\psi_1\rangle, |\psi_2\rangle, |\psi_3\rangle, \dots\}$ $\{|\psi'_1\rangle, |\psi'_2\rangle, |\psi'_3\rangle, \dots\}$

Computación cuántica

PARALELISMO CUÁNTICO

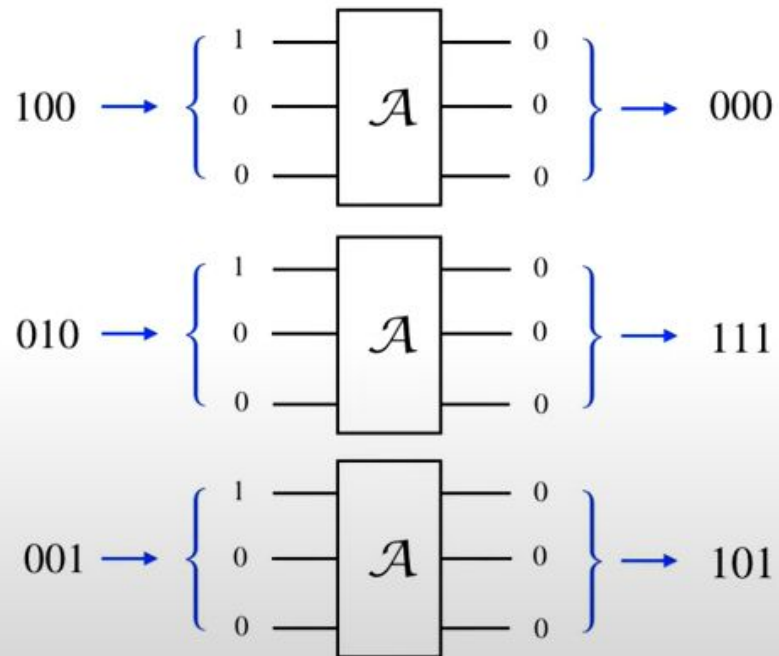
Supongamos que en ordenador convencional hay instalado un algoritmo que funciona con un input de 3 bits



Computación cuántica

PARALELISMO CUÁNTICO

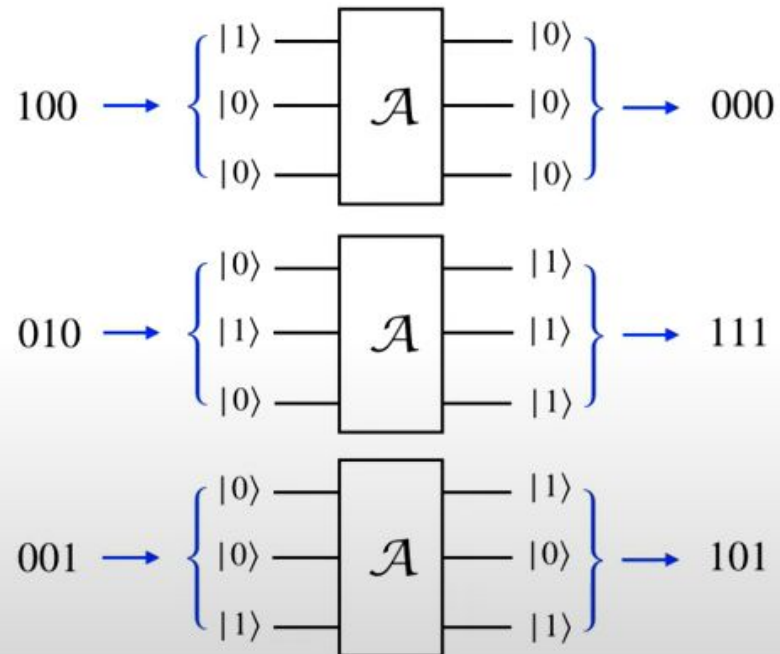
Imaginemos ahora que necesitamos conocer el resultado para 3 inputs distintos: 100, 010, 001



Computación cuántica

PARALELISMO CUÁNTICO

Procesos cuánticos equivalentes:

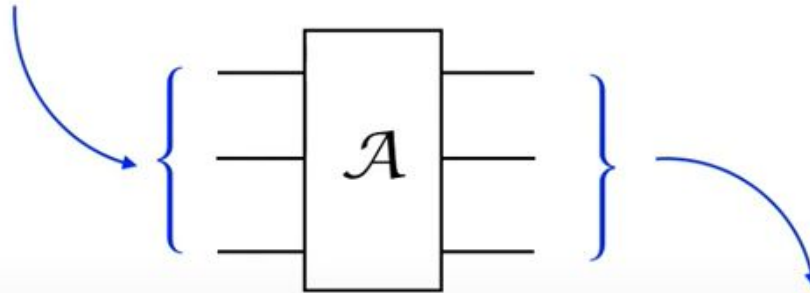


Computación cuántica

PARALELISMO CUÁNTICO

Superposición de estados:

$$|1\rangle|0\rangle|0\rangle + |0\rangle|1\rangle|0\rangle + |0\rangle|0\rangle|1\rangle$$



$$|0\rangle|0\rangle|0\rangle + |1\rangle|1\rangle|1\rangle + |1\rangle|0\rangle|1\rangle$$

Computación cuántica

PARALELISMO CUÁNTICO

¡El procedimiento se puede extrapolar fácilmente a casos donde hay millones o trillones de estados superpuestos!

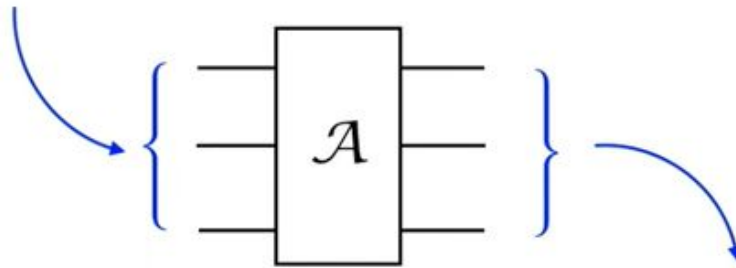
PROBLEMA

¡Al medir se pierde la información!

Computación cuántica

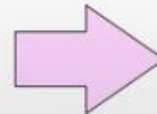
PARALELISMO CUÁNTICO

$$|1\rangle|0\rangle|0\rangle + |0\rangle|1\rangle|0\rangle + |0\rangle|0\rangle|1\rangle$$



$$|0\rangle|0\rangle|0\rangle + |1\rangle|1\rangle|1\rangle + |1\rangle|0\rangle|1\rangle$$

$$|0\rangle|0\rangle|0\rangle + |1\rangle|1\rangle|1\rangle + |1\rangle|0\rangle|1\rangle$$



$$|1\rangle|1\rangle|1\rangle$$



Computación cuántica

PARALELISMO CUÁNTICO

¡Aprovechar las ventajas de la computación cuántica requiere mucho ingenio!

Requiere manipular los qubits de forma que la medida final tenga significado y aporte información útil.

Computación cuántica

PARALELISMO CUÁNTICO

★ Algoritmo de Shor (1994)

Factorización en números primos

★ Algoritmo de Grover (1996)

Búsqueda de un elemento en un conjunto

Computación cuántica

ALGORITMO DE SHOR

Dado un número de N dígitos, hallar su descomposición en factores primos.

★ Mejor algoritmo "clásico" (GNFS, 1996):

$$N^{\circ} \text{ de pasos} \sim e^{1.9 N}$$

Problema "difícil" (?)



Aplicación a criptografía

★ Algoritmo de Shor (1994):

$$N^{\circ} \text{ de pasos} \sim N^2$$

Problema "fácil" (factible)

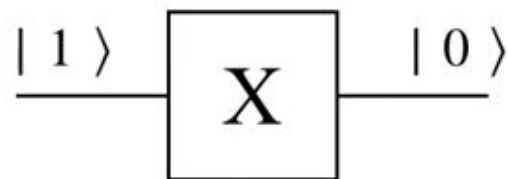
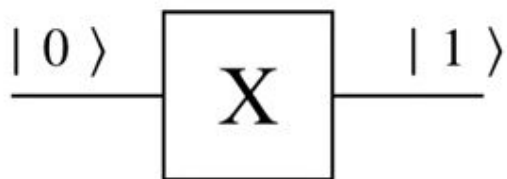
Computación cuántica

¿Qué aspecto tiene un algoritmo de computación cuántica?

$ 0\rangle$	_____
$ 0\rangle$	_____
$ 0\rangle$	_____
$ 0\rangle$	_____
\vdots	\vdots

Computación cuántica

Los qubits son manipulados con operaciones elementales (puertas cuánticas). Por ejemplo (puerta NOT)



Computación cuántica

Puerta Hadamard

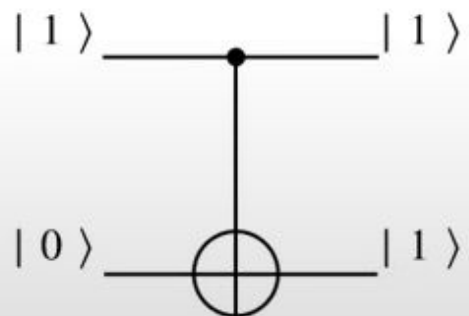
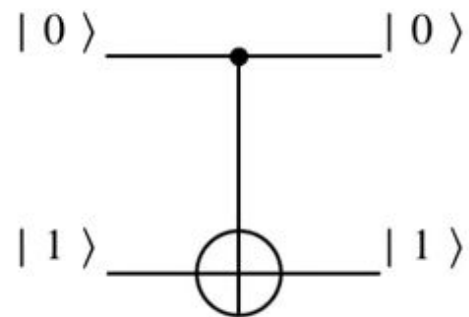
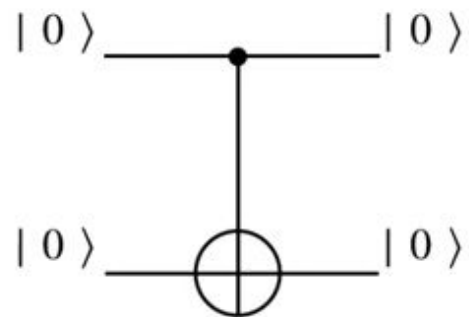
$$|0\rangle \text{ --- } \boxed{\text{H}} \text{ --- } |0\rangle + |1\rangle$$

$$|1\rangle \text{ --- } \boxed{\text{H}} \text{ --- } |0\rangle - |1\rangle$$

“Crea superposición”

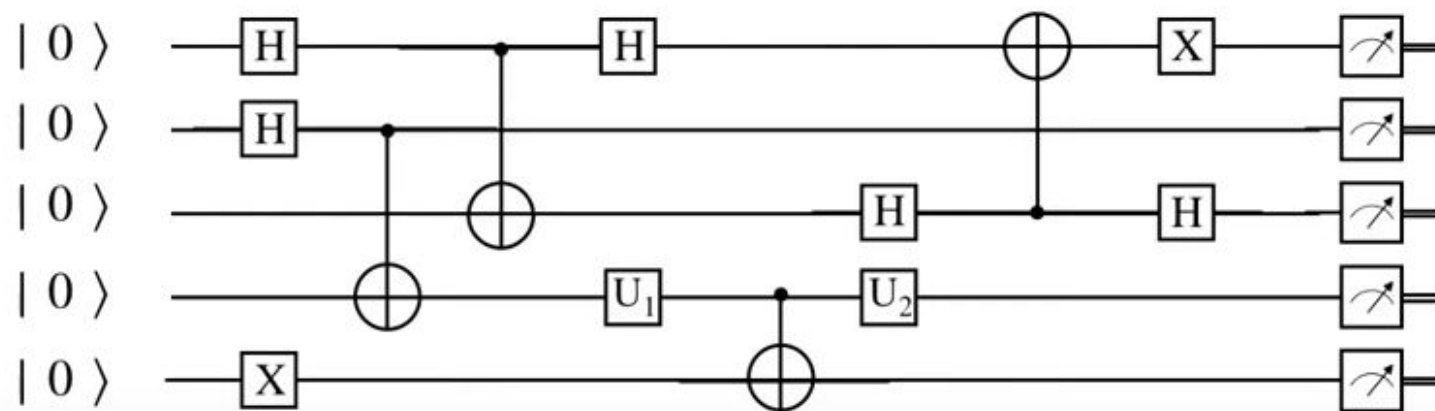
Computación cuántica

Puerta CNOT



Computación cuántica

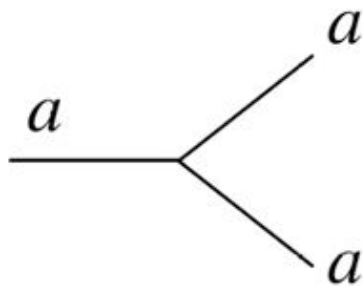
Aspecto típico de un circuito cuántico



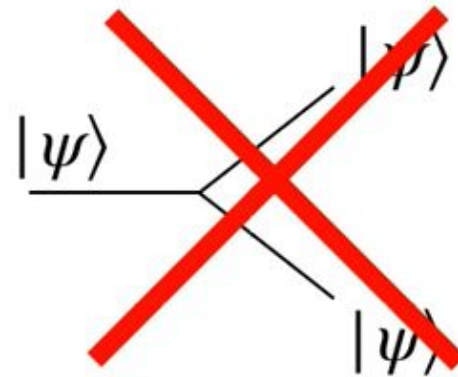
Computación cuántica

Limitaciones de la Computación Cuántica

- ★ Al medir, se destruye mucha de la información
- ★ Ciertas operaciones están prohibidas



**No es posible
la clonación**



- ★ Errores producidos por deficiencias técnicas y la pérdida de coherencia cuántica

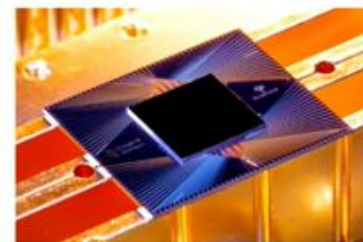
Computación cuántica

ORDENADORES CUÁNTICOS MÁS POTENTES

- ★ Eagle (IBM), 127 qubits, 2021



- ★ Sycamore (Google), 53 qubits, 2019



- ★ Zuchongzi (China), 63 qubits, 2021



Computación cuántica

ORDENADORES CUÁNTICOS MÁS POTENTES

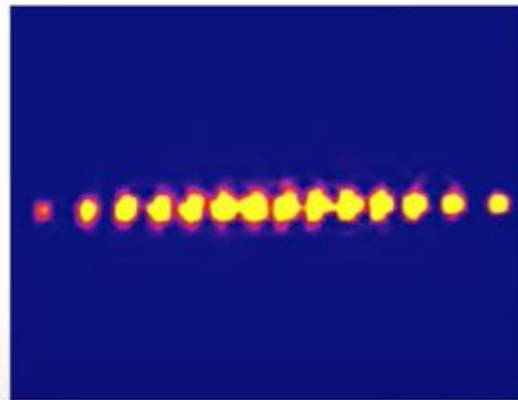
★ Jiuzhang 2.0 (China), 76 qubits, 2020



Computación cuántica

ORDENADORES CUÁNTICOS MÁS POTENTES

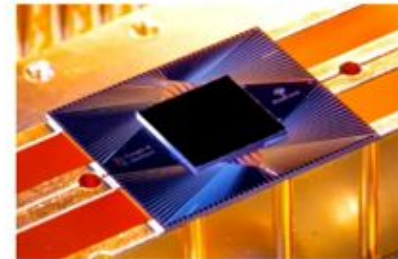
★ IonQ (USA), 32 qubits, 2020



Computación cuántica

HITO IMPORTANTE

En octubre, 2019 el ordenador cuántico de 53 qubits Sycamore (Google) realizó una tarea en menor tiempo que el ordenador convencional más potente.



Supremacía Cuántica

La carrera actual por los qubits

- **Atom Computing** (Átomos Neutros): Cuentan con prototipos de +1,000 qubits.
- **IBM** (Superconductores): Foco en la hoja de ruta. Superaron los 1,000 qubits (**Procesador Cóndor**) y apuntan a la tolerancia a fallos para 2029.
- **Google** (Superconductores): Enfocados en la corrección de errores. Demuestran que la calidad puede reducir drásticamente los fallos.
- **Quantinuum** (Iones Atrapados): Lideran en calidad y fidelidad

El Gran Desafío: El "Ruido"

- Tenemos miles de **qubits**... pero son **imperfectos**.
- Son **extremadamente sensibles** a su entorno.
- Esto genera **errores** y destruye la información cuántica.

Qubits Físicos: Los Ladrillos Ruidosos

- Son las **unidades reales** en el procesador.
- Muy **susceptibles al ruido** y la decoherencia.
- Su **vida útil** cuántica es de **microsegundos**.
- Los +1,000 qubits de **IBM Condor** son físicos.

Qubits Físicos: La decoherencia cuántica

- La decoherencia cuántica es el **principal enemigo**. Ocurre cuando un **qubit interactúa con su entorno** (calor, vibraciones, campos electromagnéticos), **perdiendo su estado de superposición** y 'colapsando' a un estado clásico (0 o 1). Esto destruye la información cuántica y genera errores.
- Por eso los **qubits necesitan** un **aislamiento** extremo y temperaturas cercanas al cero absoluto.



Qubits Lógicos: El Santo Grial

- Un qubit "perfecto" y tolerante a fallos.
- No es una unidad física única.
- Se construye protegiendo la información con muchos qubits físicos y códigos de corrección de errores.

¿Cuántos Físicos para un Lógico?

1000 a 10000
(qubits físicos)



1
(qubit lógico)

¿Cuántos Físicos para un Lógico?

- También hay avances en esta área
 - En experimentos recientes, Google logró un qubit lógico formado por aproximadamente 105 qubits físicos, mostrando que aumentar el número de qubits físicos mejora la supresión de errores (Willow).
 - Otros estudios sugieren que para tasas de error útiles se puede oscilar entre decenas y cientos de qubits físicos por qubit lógico

¿Ya Tenemos Qubits Lógicos?

Aún no. Tenemos prototipos.

- La investigación (ej. Google) ha demostrado que el concepto funciona: al usar más qubits físicos, la tasa de error del qubit lógico disminuye.
- Sin embargo, todavía no superan el rendimiento de un qubit físico de alta calidad, pero el techo a dónde llegarán los qubits lógicos está mucho más alto.

La carrera por el primer qubit lógico ya comenzó.



Mientras Tanto: La Era "NISQ"

Noisy Intermediate-Scale Quantum

- Noisy (Ruidoso): Aceptamos que los qubits tienen errores.
- Intermediate-Scale (Escala Intermedia): Tenemos entre 50 y pocos miles de qubits.

El objetivo: ¿Podemos encontrar una ventaja cuántica a pesar del ruido?



Conclusión: La Verdadera Métrica

La cantidad de qubits es el titular.

La **calidad** y el progreso hacia la **tolerancia a fallos** es la verdadera noticia.



Más allá de Shor y Grover: El Futuro Impacto Cuántico

- **Diseño de Fármacos y Materiales:** Simular el comportamiento de moléculas para crear nuevos medicamentos y materiales con propiedades específicas (ej. superconductores a temperatura ambiente).
- **Optimización Compleja:** Resolver problemas de logística, planificación financiera y cadenas de suministro que son intratables para los ordenadores clásicos.



Más allá de Shor y Grover: El Futuro Impacto Cuántico

- **Inteligencia Artificial:** Potenciar algoritmos de machine learning y desarrollar modelos de IA más avanzados.
- **Criptografía Segura:** Desarrollar nuevos protocolos de comunicación cuántica inherentemente seguros (gracias a los principios cuánticos).