Teoría de la información cuántica (curso electivo ICM y Magíster Física)

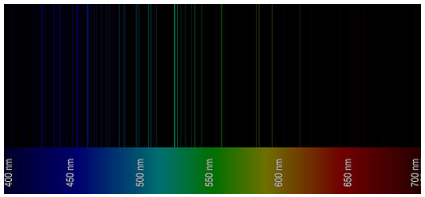
Introducción

Dominique Spehner

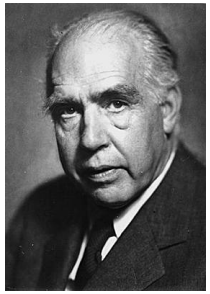
Departamento de Ingeniería Matemática
Universidad de Concepción, Chile

Física del mundo microscópico

La mecánica cuántica describe la física a escala de las moléculas, átomos y partículas subátomicas (quarks, fotón, electrón, protón, neutrón, neutrinos, ...)



espectro de emisión del Cesio Cs



Sus padres fundadores son :

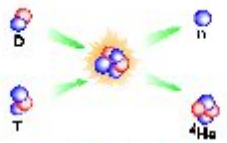
M. Planck (1858-1947), N. Bohr (1885-1962),

E. Schrödinger (1887-1961), W. Heisenberg (1901-1976),

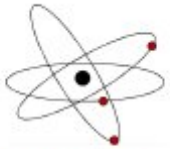
W. Pauli (1900-1958), P. Dirac (1902-1984),

M. Born (1882-1970), P. Jordan (1902-1980)

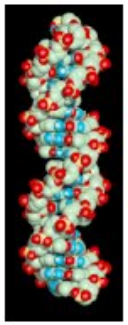

La física cuántica logra explicar :



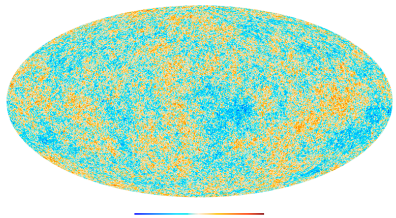
10 -15 M
(noyaux, radioactivité
Énergie nucléaire)



10 -10 M
(atomes)



10 -8 M
(molécules
biologiques)



(radiación fósil del universo, satélite Planck)

- → las colisiones a alta energía del CERN
- → las reacciones nucleares
- → la estructura de la materia (moléculas, sólidos, líquidos y gases)
- → las propiedades de conducción de los materiales
- → el magnetismo (imanes,...)
- → las reacciones químicas
- → ...
- → la fotosíntesis (?)
- → ...
- → el órigen del universo (Big Bang)

Física cuántica en el siglo XX

Las predicciones de la teoria cuántica nunca han fallado hasta ahora ! Algunas predicciones se verifican experimentalmente con una precisión mayor a 10^{-10} *(momento magnético del electrón).*

Gracias a la mecánica cuántica, se logro avances tecnológicos significativos en el siglo XX, por ejemplo :

- *transistores, diodos* $\rightarrow$ *electronica*
- *láser*
- *Resonancia Magnética Nuclear*
- *medida precisa del tiempo*
  $\hookrightarrow$ *Sistema de Posicionamiento Global (GPS)*

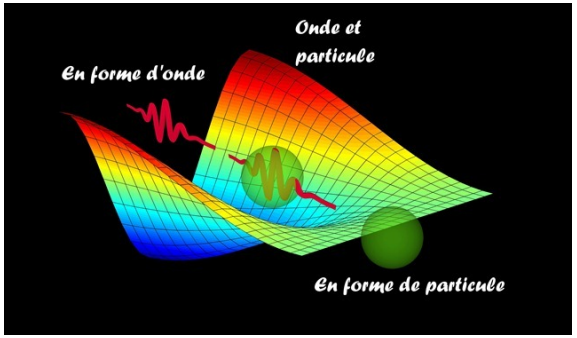
(Reloj atómico)

¿ Que seran sus logros en el siglo XXI ?

Una teoria muy precisa y muy extraña...

"Pienso que puedo decir con seguridad que nadie entiende la mecánica cuántica" (R. Feynman).

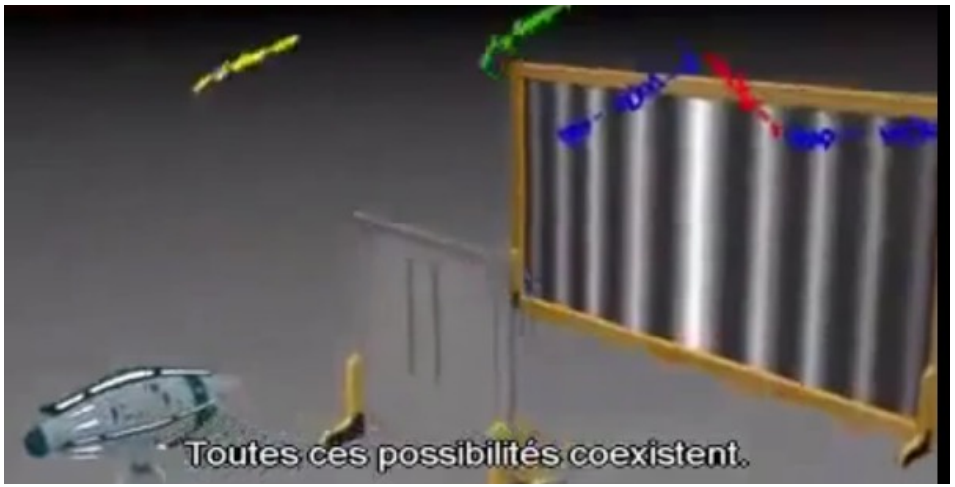
Un partícula cuántica (fotón, electrón, molécula,...) puede exhibir comportamientos típicos de ondas.



Dualidad onda-partícula : L. de Broglie (1892-1987)

El concepto de trayectoría pierde todo sentido : si la partícula tiene una posición bien définida, luego su velocidad no está definida (es completamente impredecible) y viceversa.

Experimento de la doble rendija



(source: "Dr Quantum" YouTube)

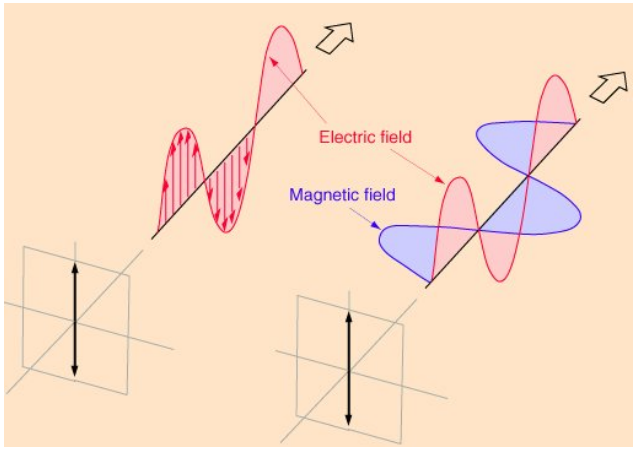
↪ Experimento realizado en Tokyo en 1989 con **electrones** atraviesando la rendija **uno por uno** (A. Tonomura $et\ al.$).

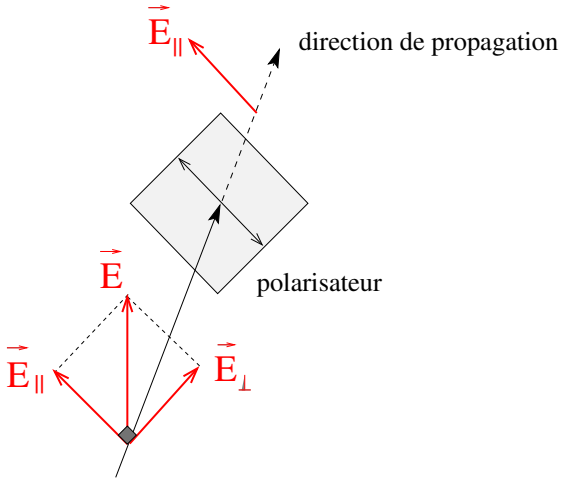
↪ Observación en Viena en 1999 de la figura de interferencia con **moléculas** C_{60} (A. Arndt $et\ al.$),

Polarización del fotón

Un **filtro polarizador** transmite de forma selectiva una dirección determinada del campo electrico $\vec{E}$

$\hookrightarrow$ *luz linealmente polarizada.*





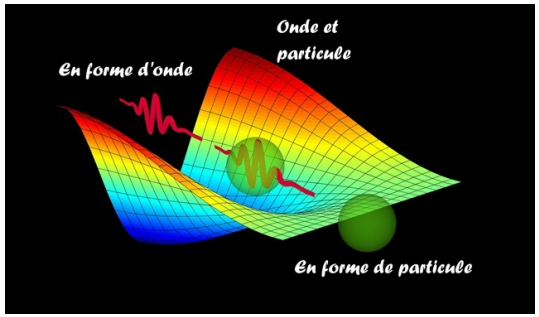
El fotón (= quanta de luz) es transmitido/absorbido con una probabilidad $1/2$.

$\Rightarrow$ es imposible conocer de antemano el resultado de la medida !

Solamente se puede predecir la **probabilidad del resultado** de la medida $\leftrightarrow$ *"Dios no juega a los dados" (A. Einstein)*

Principio de superposición

El **estado de un sistema cuántico** se representa por un **vector de** $\mathbb{C}^N$ (o de un espacio de Hilbert $\mathcal{H}$ de dim. infinita) **de norma** 1**.**



★ **Ejemplo 1 :** estado de polarización de un fotón :

$$|\psi\rangle = c_0|\uparrow\rangle + c_1|\rightarrow\rangle \quad \in \mathbb{C}^2$$

$|\uparrow\rangle$ ($|\rightarrow\rangle$) corresponde a la polarización vertical (horizontal)
$c_{0,1} \in \mathbb{C}$ son componentes complejos tales que $|c_0|^2 + |c_1|^2 = 1$

★ **Ejemplo 2 :** estado de polarización de 2 "fotones gemelos" :

$$|\psi_{\mathrm{EPR}}\rangle = \frac{1}{\sqrt{2}}(|\uparrow,\rightarrow\rangle - |\rightarrow,\uparrow\rangle) \quad \in \mathbb{C}^4$$

Gato de Schrödinger y decoherencia

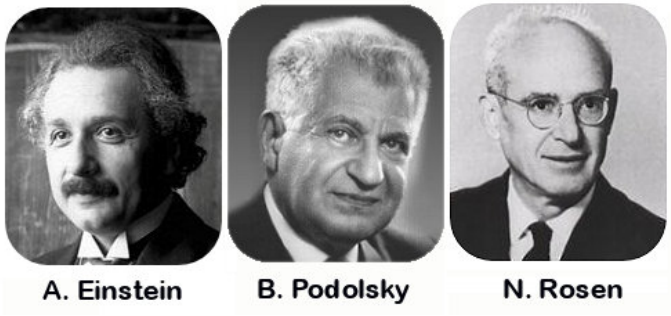
E. Schrödinger imagino en 1935 un dispositivo que conduce a una superposición de un gato vivo y un gato muerto :

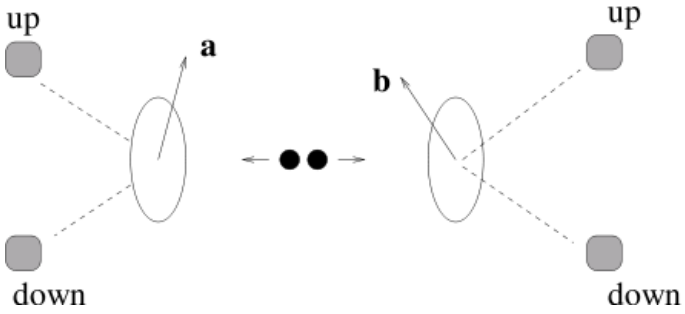
$$|GATO\rangle = \frac{1}{\sqrt{2}}(|\text{vivo}\rangle + |\text{muerto}\rangle)$$

Estos tipos de superposiciones suelen existir durante *intervalos de tiempo extramadamente cortos*, debido a la **decoherencia** que **transforma los estados cuánticos en estados clásicos.**

No localidad y paradoja EPR

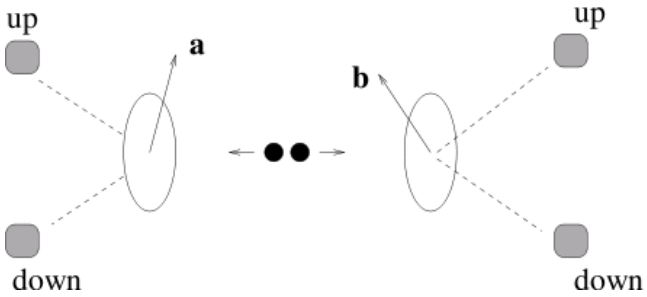
En 1935, Einstein, Podolsky y Rosen proponen un experimento mental que demuestra que la teoria cuántica es (1) incompleta ó (2) no local: una medida puede tener un *efecto instantaneo en un lugar arbitrariamente lejano de ella!*





En un cristal no-lineal un átomo puede emitir un par de *fotones gemelos* tal que si el 1^{er} fotón es transmitido por un polarizador de eje $\vec{a}$, luego el 2^{do} fotón se polariza instantaneamente $\perp \vec{a}$.

Violación de la desigualdad de Bell



$$\langle ab\rangle+\langle a'b\rangle+\langle a'b'\rangle-\langle ab'\rangle \leqslant 2$$

(J.Bell, 1964)

correlaciones clásicas *correlaciones cuánticas*

↪ Experimento realizado en 1982 por L. Aspect en Paris, luego en muchos otros laboratorios ⇒ **las desigualdad es violada.**

Un computador cuántico para hacer simulaciones...
sobre sistemas cuánticos

Los computadores clásicos no logran calcular la evolución de un sistema cuántico con $\gtrsim 100$ partículas. Un computador obedeciendo a los principios cuánticos sería mucho $+$ eficiente *(R. Feynman 1982)*.

▷ Un computador clásico se compone de **bits** en los estados 0 ó 1, utilizados para representar los números y ejecutar las operaciones lógicas.

▷ Un computador cuántico se compone de **"qubits"**, cuyos estados son **combinaciones lineales** de 2 vectores $\perp$, $|0\rangle$ y $|1\rangle$:

$$|\psi\rangle = c_0|0\rangle + c_1|1\rangle \text{ con } c_{0,1} \in \mathbb{C},\ |c_0|^2 + |c_1|^2 = 1.$$

→ Un computador con 150 qubits "perfectos" sería mas poderoso que todos los supercomputadores clásicos del mundo reunidos !

Factorizar en números primos

$$N = p_1^{n_1} \times p_2^{n_2} \times \ldots$$

- Es muy difícil factorizar en números primos un entero $N \gg 1$: **no** tenemos un algoritmo que lo pueda hacer en un tiempo $\sim n^k$ algebraico en el número de bits $n \sim \log(N)$.
- En contrario, la operación inversa $\times$ se hace muy rapidamente.

  $\hookrightarrow$ *el algoritmo RSA encripta mensajes usando la factorización* $N = p_1 p_2$*, para decriptar se requieren* p_1 *y* p_2*.*

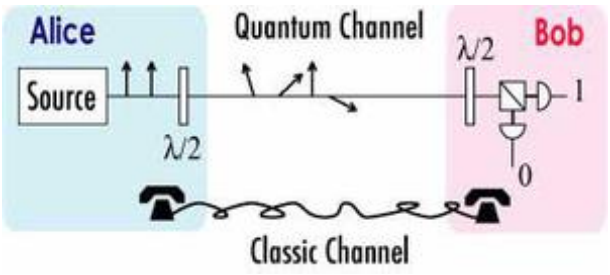
  - En 1994, P. Schor propone un algoritmo cuántico capaz de factorizar un entero de n bits en tiempo $O(n^3)$.

  $\Rightarrow$ un computador cuántico podría decriptar facilmente los mensajes encriptados con RSA !

Criptografía cuántica

- ¿ Podría Alice distribuir a Bob una llave secreta que le permita a Bob decriptar un mensaje publico, de manera que ellos puedan darse cuenta si un espía interceptó la llave ?


- Es imposible clasicamente, pero C. Bennett y G. Brassard (y S. Wiesner) propusieron en 1984 usar fotones polarisados :



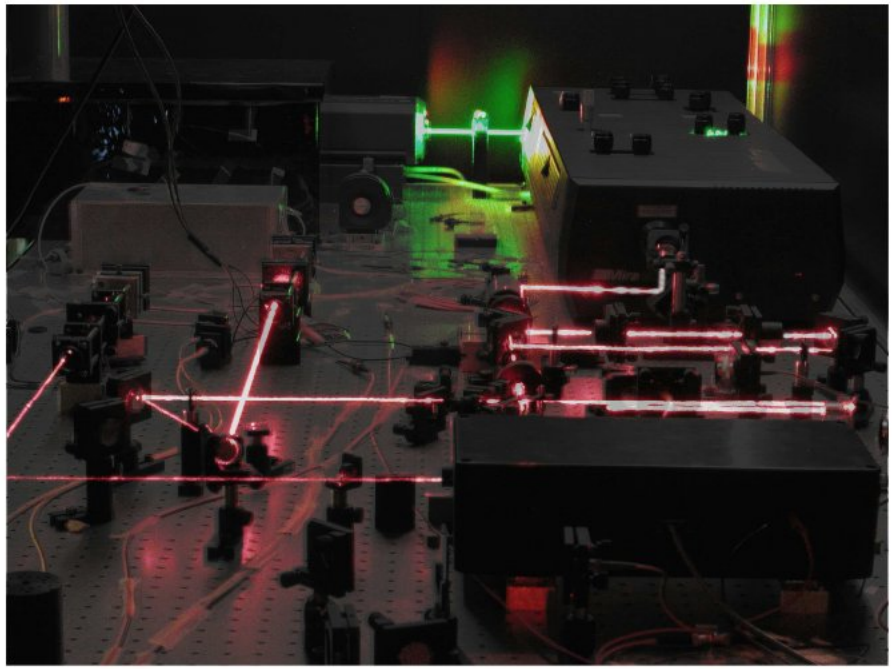
Polarizador Alice	$\times$	$+$	$\times$	$+$	$+$	$\times$	$\times$	$+$
Estado Alice	0	0	1	0	1	1	1	0
Polarizador Bob	$+$	$\times$	$\times$	$+$	$+$	$+$	$\times$	$\times$
Resultado Bob	0	1	1	0	1	1	1	0
Llave secreta			1	0	1		1	

Si Eva mide la polarización en la dirección $\times$ y Alice y Bob miden en la dirección $+$, estos últimos tienen resultados $\neq$ con proba $1/2 \Rightarrow \exists$ espía, llave insegura!

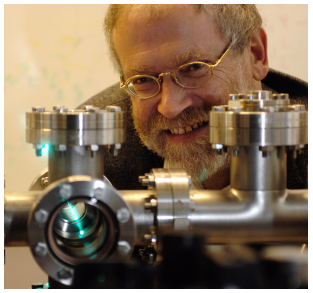
Teleportación cuántica

$\hookrightarrow$ transmitir un estado cuántico desconicido de un lugar a otro.

Alice y Bob necesitan compartir *fotones gemelos entrelazados* (par EPR) y intercambiar informaciones clásicas

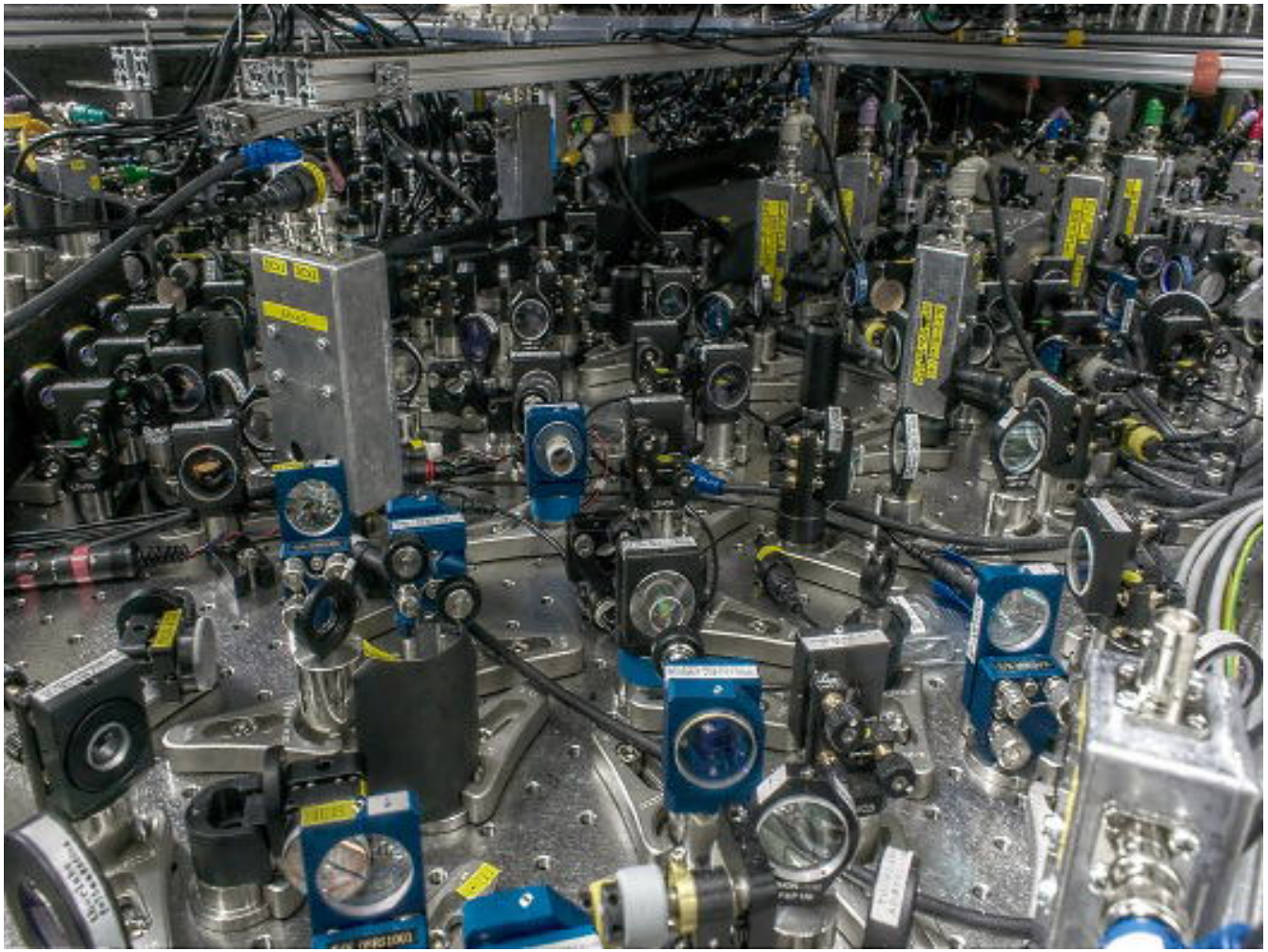


Experimento en Ginebra (N. Gisin)



$\hookrightarrow$ experimento realizado por 1^{ra} vez en 1997 en Innsbruck (A. Zeilinger).

Teleportación de "gatos de Schrödinger"



Experimento de Tokyo, School of engineering (A. Furusawa)

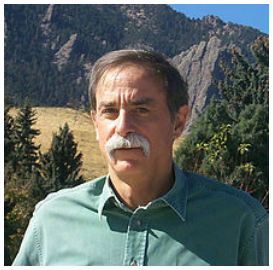
Realizaciones experimentales

★ Espines nucleares de moléculas en disolución en un aparato de RMN (IBM y Universidad de Stanford, 2000: factorización de 15 con 7 qubits)

★ Iones atrapados (R. Blatt, Innsbruck: teleportación, puertas cuánticas, 2005: primer qbyte $= 8$ qubits)

★ Fotones en una cavidad óptica (S. Haroche, Paris, premio Nobel 2012: gatos de Schrödinger, medidas cuánticas)

★ átomos frios manipulados con laseres (D. Wineland, Colorado, premio Nobel 2012: gatos de Schrödinger,...)



★ espines de electrones en semiconductores, espines nucleares en defectos del diamante, etc...

★ Circuitos supraconductores (SQUID), puntos cuánticos

Últimos logros con supraconductores:

2018: computador de INTEL-universidad de Deft (49 qubits)

2019: primer computador de uso comercial IBM (20 qubits)
computador de Google (53 qubits) supera a un computador clásico

2020: IBM (53 qubits), Google: simulación de una reacción química

Los grandes desafios...

- es necesario lograr **controlar** y **manipular** el sistema cuántico (espines, átomos, fotones,...)

- los efectos de decoherencia inducen una pérdida rápida de las propiedades cuánticas
  $\hookrightarrow$ efectuar los cálculos en un **tiempo muy corto**

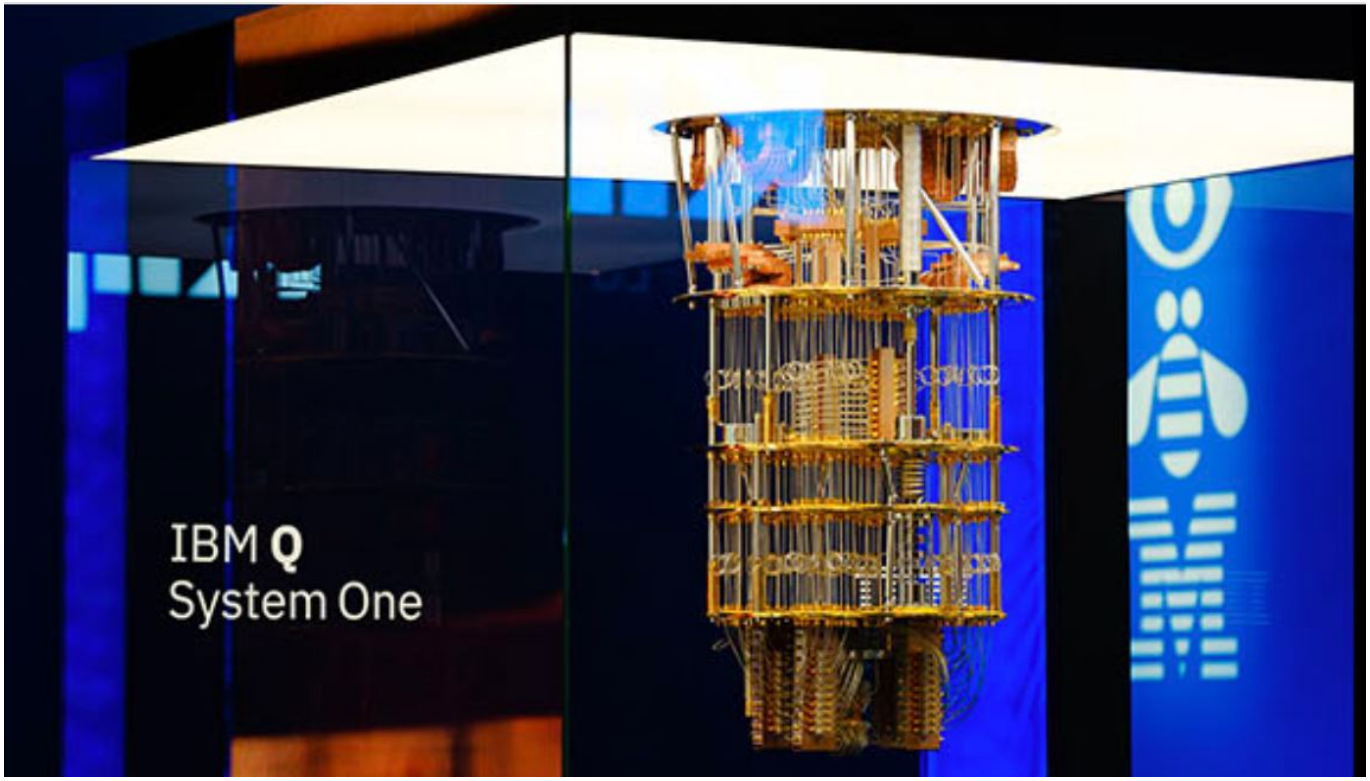
- los qubits deben **interactuar entre sí** de manera controlada, para así crear entrelazamiento.

$\rightsquigarrow$ es necesario usar **códigos de corrección de errores**
$\Rightarrow$ se necesitan mucho mas qubits (extra qubits).

Conclusiones

- ✓ La teoría de la información cuántica es inter-disciplinar, abarca la **física**, la **matemática** y las **ciencias de la computación**
  $\hookrightarrow$ *motiva cientificos de estas disciplinas a trabajar juntos!*
- ✓ Una mejor comprensión de la física cuántica surge gracias a :
  - ► experimentos de laboratorio con sistemas bien controlados de pocas párticulas medidos precisamente
  - ► rol importantissimo de la teoría de la información.
- ✓ Algunas aplicaciones ya existen, como comunicaciones encriptadas cuanticamente y computadores con decenas de qubits. *Mucha inversión privada/pública para construir un computador cuántico capaz de resolver problemas útiles insolubles con computadores clásicos.*

¿ Que ha de esperar en el futuro cercano?



IBM anuncia un computador de 1000 qubits para 2023...