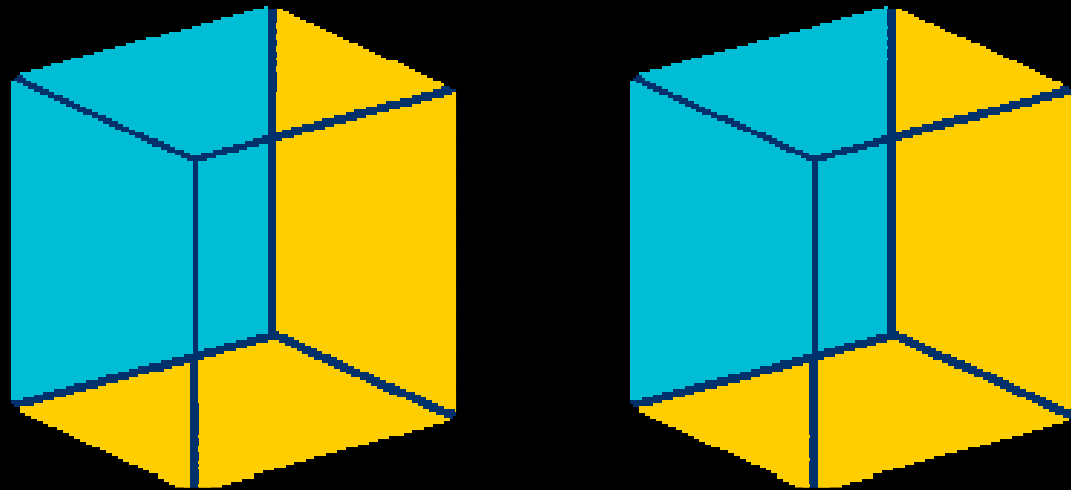


L'EXTRANYA MECÀNICA QUÀNTICA



SUPERPOSICIÓ

No hi ha **elements de realitat**
fins al moment de l'observació.

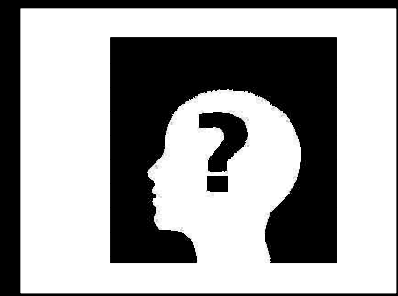
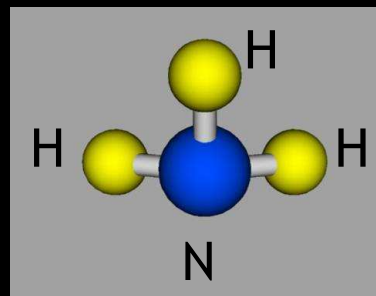
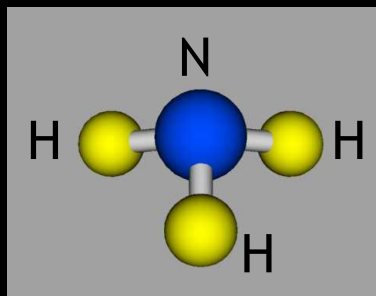
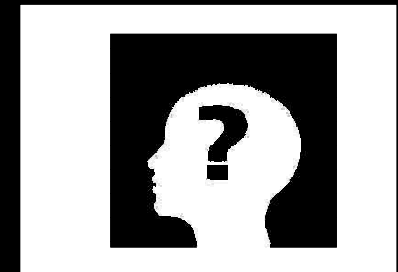
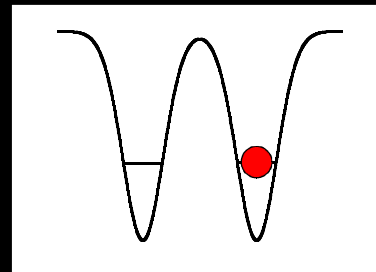
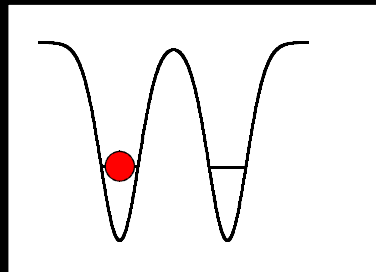
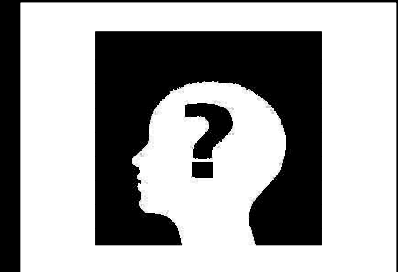
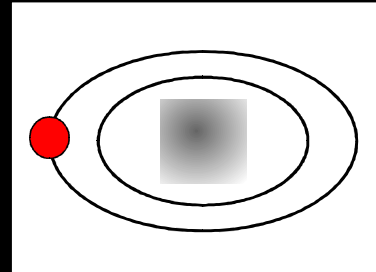
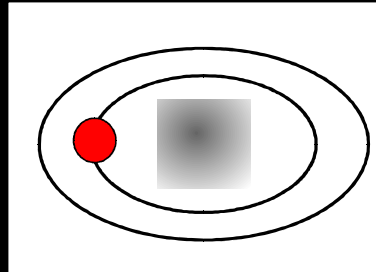


ENTRELLAÇAMENT

Entanglement

Vershänkrung

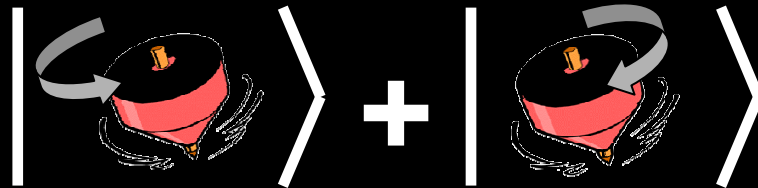
Exemples físics:



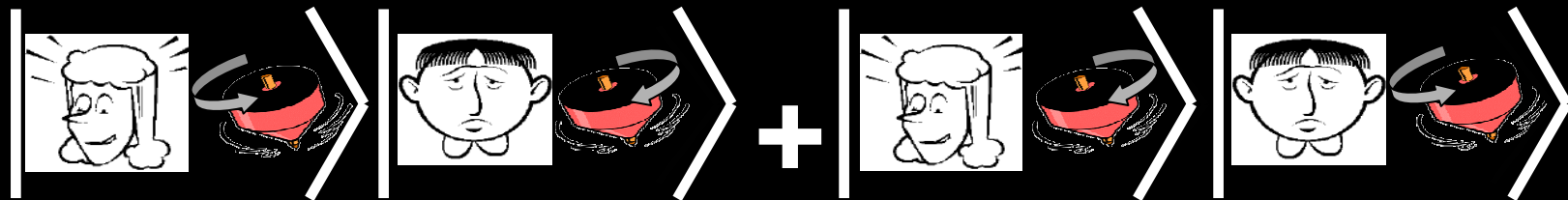
L'espí d'una partícula:

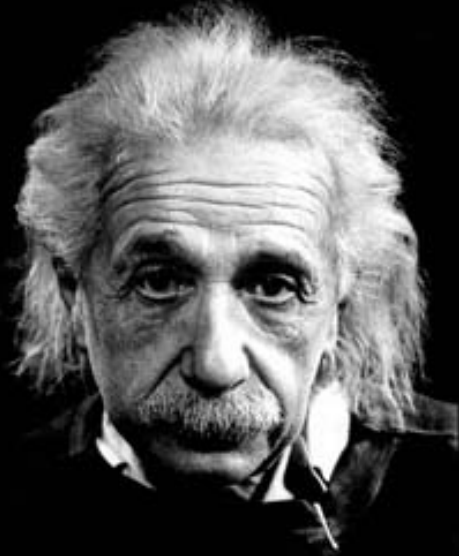


Estats de superposició:



Estats entrellaçats:





“La teoria quàntica és
incompleta.”

Albert Einstein

Premi Nobel de Física (1921)

Un dels fundadors de la teoria quàntica



“Ningú entén la mecànica
quàntica”

Richard Feynman

*Premi Nobel de Física (1965)
per les seves contribucions a la mecànica quàntica*



John Bell

Un dels fundadors de la teoria quàntica de la informació

“De dilluns a dissabte sóc un
enginyer quàntic.
Els diumenges tinc principis.”

ELS COMPUTADORS



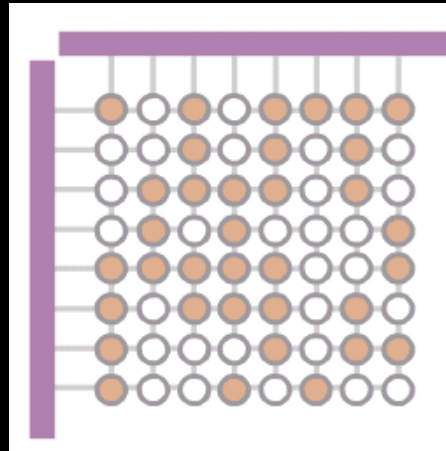
- Bits
- Memòries (registres)
- Operacions entre bits

- Bits:
 - 0 = condensador descarregat
 - 1 = condensador carregat

0 = 00000000 ← 1 byte = 8 bits
1 = 00000001
2 = 00000010
3 = 00000011
...
255 = 11111111

- Memòries:

- Memòria RAM



- condensador descarregat
 - condensador carregat

- Disc dur

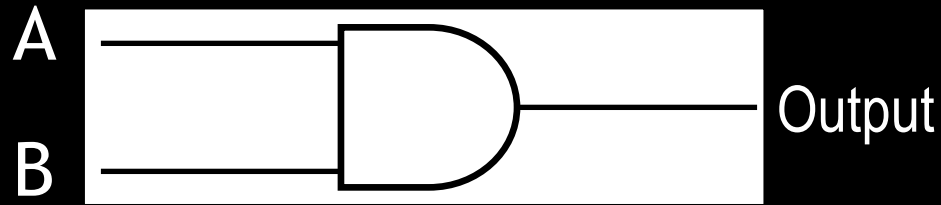
- CD, DVD,...

Les memòries actuals emmagatzemen ~
250 000 000 000 bytes



**Western Digital
WD2500JB HDD
250 GBytes**

- Operacions entre bits: Portes lògiques



A	B	Output
0	0	1
0	1	1
1	0	1
1	1	0

NAND

Amb les portes NAND un computador realitza qualsevol operació



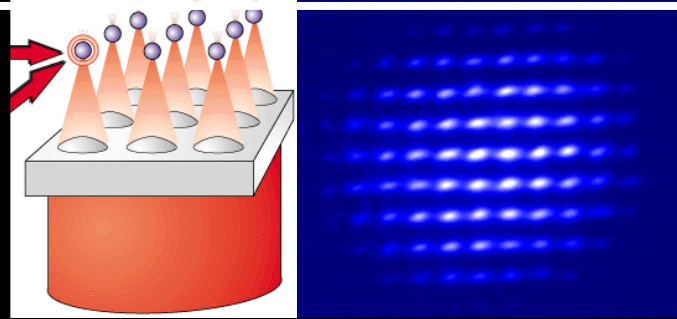
COMPUTACIÓ QUÀNTICA

PRADA DE CONFLENT, 22 D'AGOST DE 2010

1 MOTIVACIÓ



2 COMPUTACIÓ QUÀNTICA



3 CRIPTOGRAFIA QUÀNTICA



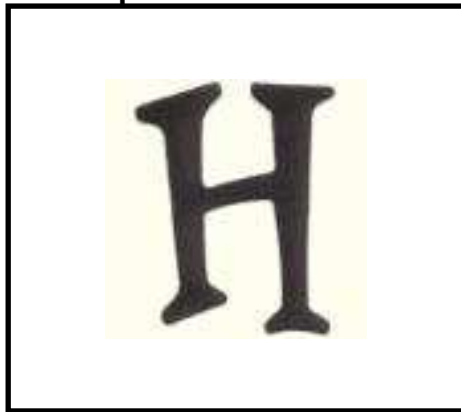
1 MOTIVACIÓ



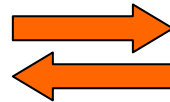
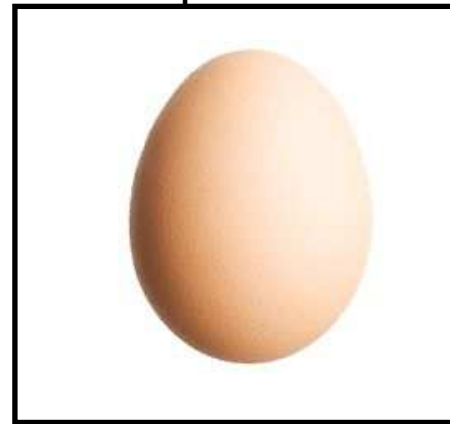
MOTIVACIÓ

DE L'ESPAI MATEMÀTIC A L'ESPAI FÍSIC

Espai matemàtic



Espai físic



$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle \in \mathbb{C}^2$$

$$\begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle \in \mathbb{C}^2$$

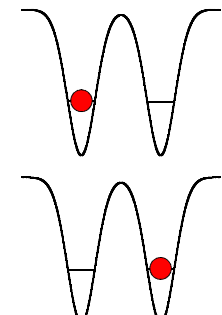
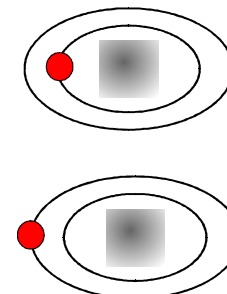
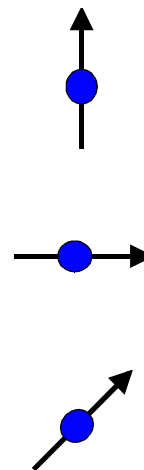
$$\begin{pmatrix} 1 \\ 1 \end{pmatrix} = |0\rangle + |1\rangle \in \mathbb{C}^2$$

la informació
és física

Polarització Fotons

Nivells Electrònics

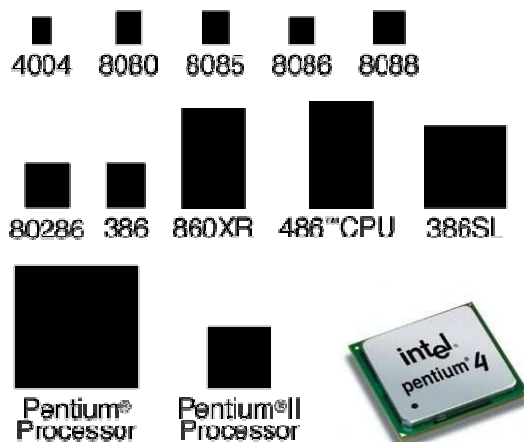
Posició



MOTIVACIÓ (I): ELS LÍMITS DE LA COMPUTACIÓ CLÀSSICA

Gordon Moore (1965):
(cofundador d'Intel)

El número de transistors per circuit integrat es doble cada 18-24 mesos

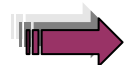
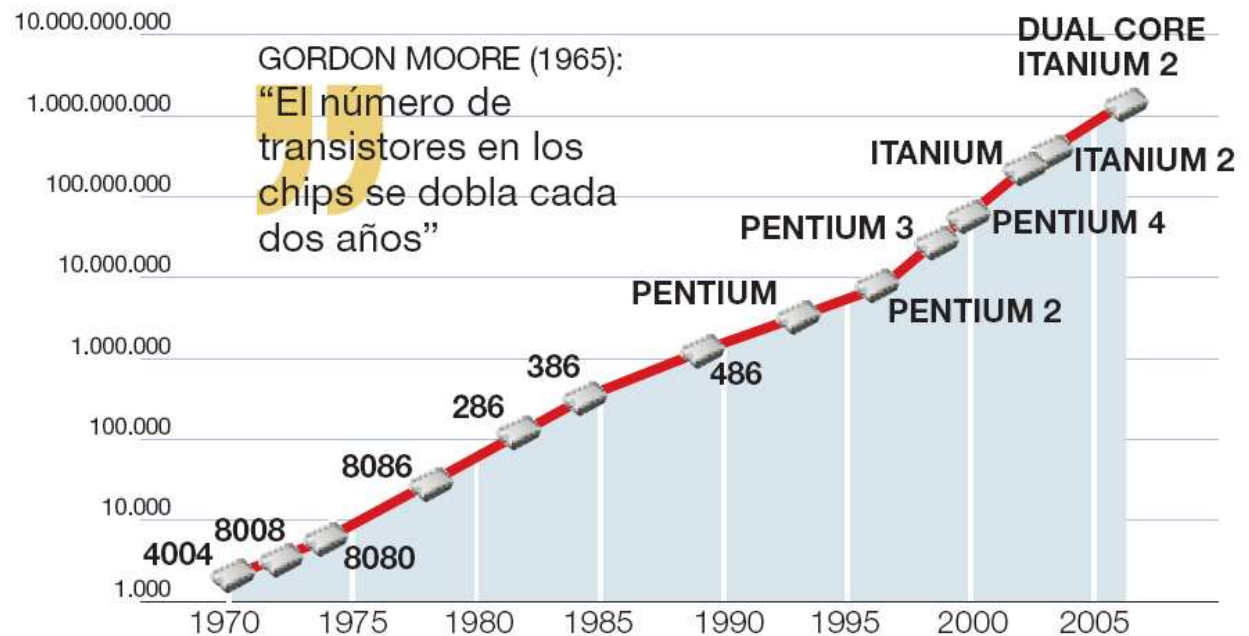


80 milions de transistors

elPeriódico.com

14/5/2007

NÚMERO DE TRANSISTORES EN LOS CHIPS



L'any 2020 els transistors tindran la grandària d'un àtom

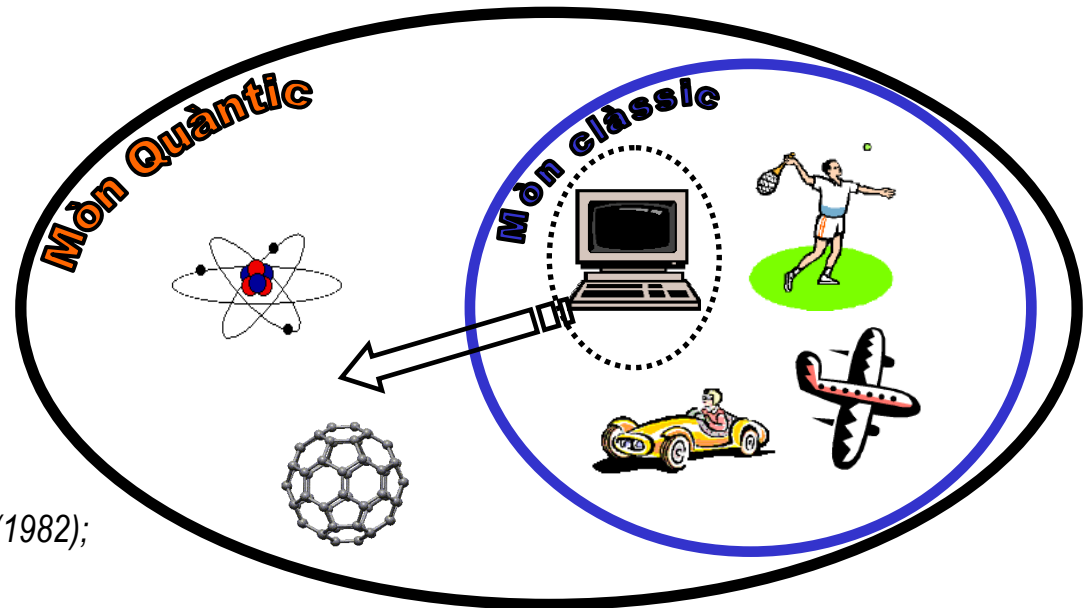
- Saturació en la potència (velocitat de càlcul) dels computadors "clàssics"
- Els computadors "clàssics" començaran a patir efectes quàntics

MOTIVACIÓ (II): LA SIMULACIÓ QUÀNTICA

➔ El punt de vista de Feynman (1982):



R. Feynman, *Int. J. Theor. Phys.* **21**, 467 (1982);
Found. Phys. **16**, 507 (1986)

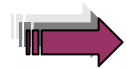


➔ Simular el món quàntic (models mesoscòpics d'estat sòlid, superconductivitat, química, farmàcia,...) amb un computador quàntic d'uns pocs qubits

$$C. \text{ Quàntic} \quad |\psi\rangle = \overbrace{a_{000\dots} |0\rangle \otimes |0\rangle \dots \otimes |0\rangle}^{n \text{ qubits}} + a_{100\dots} |1\rangle \otimes |0\rangle \dots \otimes |0\rangle + \dots$$

$$C. \text{ Clàssic} \quad \left\{ \begin{array}{l} \text{Si } n = 30 \Rightarrow 2^{30} \cdot 2 \cdot 2^2 = 2^{33} \approx 10^{10} \text{ bytes} = 10 \text{ GBytes} \\ \text{Si } n = 100 \Rightarrow 2^{100} \cdot 2 \cdot 2^2 = 2^{103} \approx 10^{31} \text{ Bytes} \end{array} \right.$$

MOTIVACIÓ (III): UN NOU PARADIGME



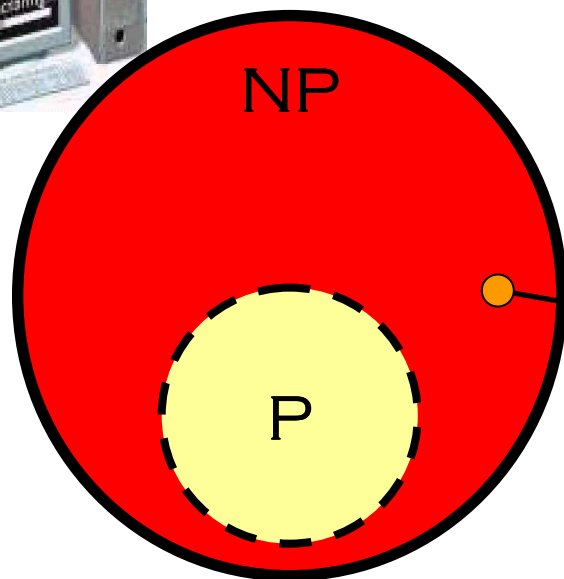
D. Deutsch (1985):

- Mecànica Clàssica = Límit particular de la Mecànica Quàntica
- Un computador quàntic tindrà almenys el mateix poder computacional que el seu anàleg clàssic. De fet, més.

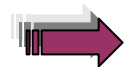
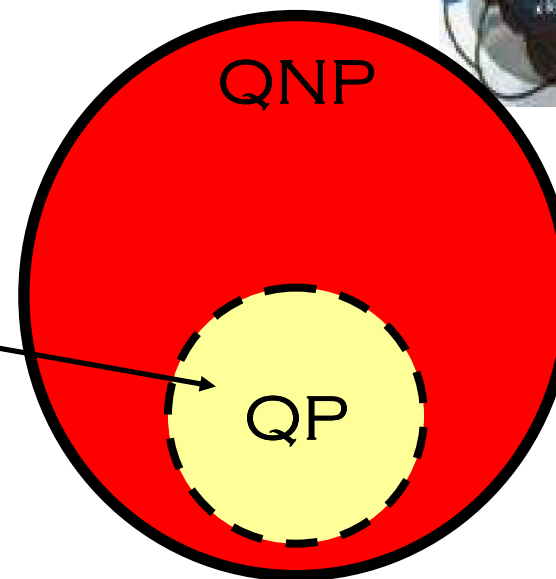
D. Deutsch, Proc. R. Soc. London A **400**, 97 (1985); **425**, 73 (1989)



C. Clàssic



C. Quàntic



Guany exponencial: factorització (alg. de Shor), discrete log, equació de Pell, sumes de Gauss, els “random walks”,...

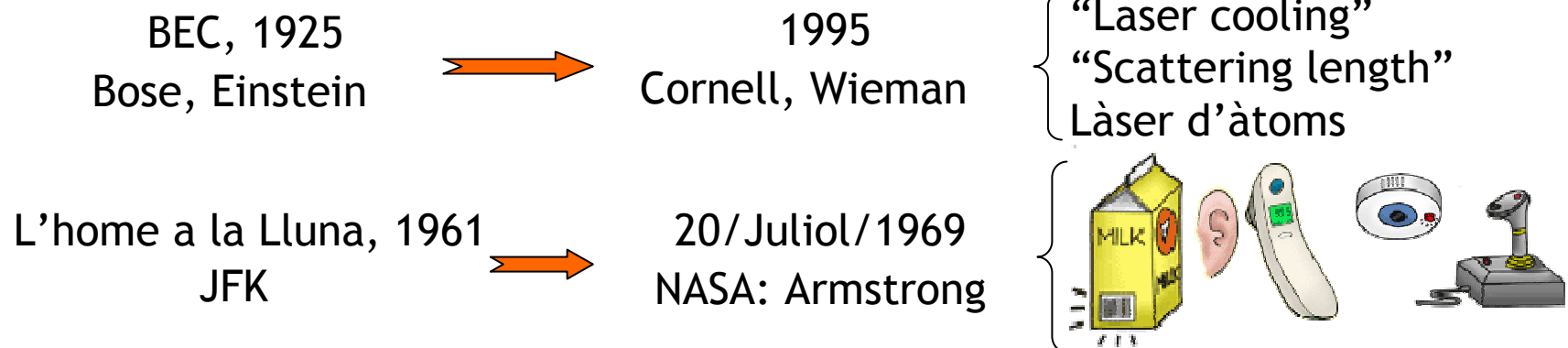
MOTIVACIÓ (IV): UNA FITA ESTIMULANT

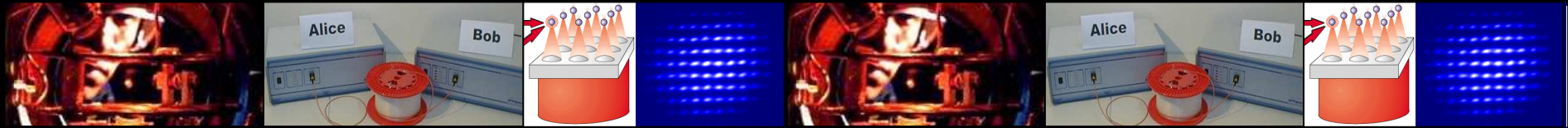
➡ En el procés de construcció d'un computador quàntic s'està aprenent molta física. Alguns exemples:

- Què és la superposició?
- Què és la no-localitat? Quines implicacions té?
- Com es poden generar estats entortolligats?
- Què és la decoherència? Com es pot controlar?
- ...

Aplicacions en física (interferometria, òptica atòmica, òptica quàntica, mesures d'alta precisió,...), en informàtica (teoria de la informació) en matemàtiques (caracterització d'estats en espais de Hilbert complexes)...

➡ Altres Exemples:





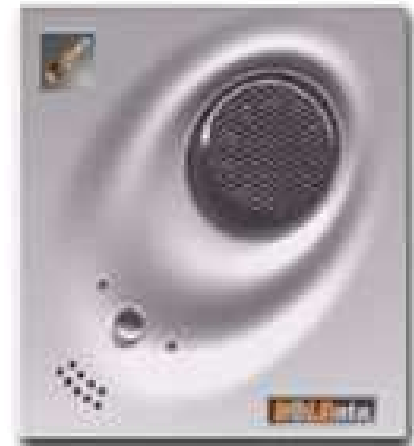
ALGUNES FRASES CURIOSAS (I)

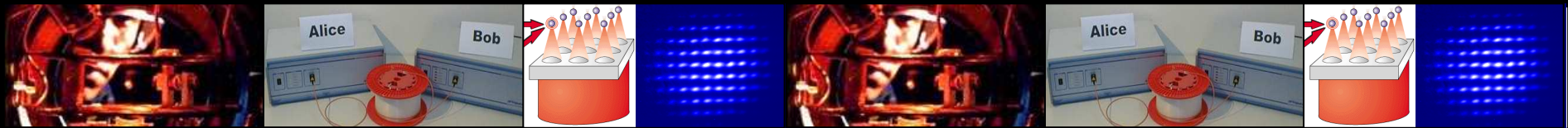
- ❖ *“I think there is a world market for maybe five computers.”*
- Thomas Watson, Chairman of IBM, 1943.
- ❖ *“There is no reason anyone would want a computer in their home.”*
- Ken Olson, president, chairman and founder of Digital Equipment Corp., 1977.

Des dels anys 70 fins l'abril del 2003 s'han fabricat uns 1000 milions de computadors. El 25% són d'ús domèstic.

- ❖ *“Computers in the future may weigh no more than 1.5 tonnes.”*
- *Popular Mechanics* forecasting the relentless march of science, 1949.

BOLData Mini PC, 860 grams





ALGUNES FRASES CURIOSAS (II)

- “640 K ought to be enough for anybody.”
- Bill Gates, 1981.



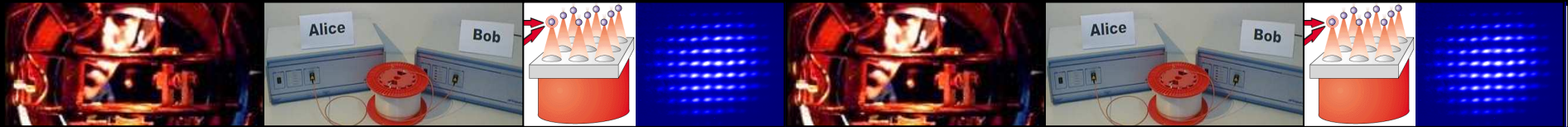
**Western Digital
WD2500JB HDD
250 GBytes**

- L'any 1977 Scientific American va reptar la comunitat científica a desxifrar un missatge encriptat mitjançant la tècnica RSA amb un nombre (producte de dos primers) de 129 dígit (Gardner M., Scientific American 237, 120-124 (1977)). Ron Rivest (MIT) estimà que es tardarien $4 \cdot 10^{16}$ anys en factoritzar aquest nombre

Va ésser desxifrat l'any 1994

Atkins D., Graff M., Lenstra A. K., and Leyland, P. C. in Advances in Cryptology — ASIACRYPT '94 (eds Pieprzyk, J. & Safavi-Naini, R.) 263–277 (Springer, Heidelberg, 1995).

- “Prediction is very difficult, especially about the future.”
- Niels Bohr



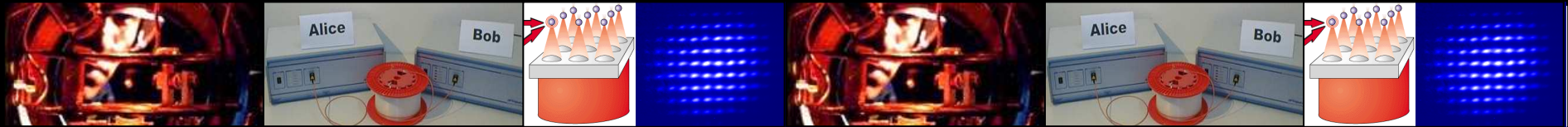
BIBLIOGRAFIA

▶ INTERACCIÓ LLUM-MATÈRIA:

- C. Cohen-Tannoudji, J. Dupont-Roc, G. Grynberg, *Photons and Atoms. Introduction to Quantum Electrodynamics; i Atom-Photon Interactions*. John Wiley & Sons 1992
- M.O. Scully, M.S. Zubairy, *Quantum Optics*, Cambridge U. P. 1997
- D.F. Walls, G.J. Milburn, *Quantum Optics*, Springer-Verlag 1994
- Apunts Teoria Semiclàssica: <http://einstein.uab.es/optica/qoptics/cap2.pdf>
Teoria Quàntica: <http://einstein.uab.es/optica/qoptics/cap3.pdf>

▶ IMPLEMENTACIÓ FÍSICA DE LES TECNOLOGIES QUÀNTIQUES DE LA INFORMACIÓ:

- Eds. D. Bouwmeester, A. Eckert, A. Zeilinger, *The Physics of Quantum Information*, Springer 2000
- Ed. D. Heiss, *Fundamentals of Quantum Information*, Springer 2002
- Internet: <http://www.qubit.org>



CONTACTE

Jordi Mompart

Grup d'Òptica

Departament de Física

Universitat Autònoma de Barcelona

jordi.mompart@uab.cat