Què ens diu i què no ens diu la FQ

Lluís Ametller

Departament de Física i Enginyeria Nuclear
Universitat Politècnica de Catalunya

Prada, agost 2006

Física Quàntica (FQ)

La Física Quàntica és la teoria més exitosa
i la més estranya de la història de la Física

Estudi del món petit: microcosmos

Moment magnètic de l'electró:

Experiment ⟶ 1.0011596521 ± 0.0000000093

Teoria ⟶ 1.001159652 ± 0.0000000046

No és un model del que passa físicament.
Només prediu valors possibles i les seves probabilitats !!!

Índex a grans trets

- El microcosmos
- Perquè la física quàntica ? (El passat)
- Quina actitud prenem ? (… els científics)
- On és present, com es manifesta ? (avui)
- Què en podem esperar ? (futur… proper)

Microcosmos

- Anem a intentar entendre el món dels àtoms, nuclis, electrons,..
- No són objectes macroscòpics. No sabem “com són” !
- Només en podrem esbrinar propietats indirectes
- La nostra experiència (macroscòpica) no serà bona guia
- Haurem d’acceptar algunes sorpreses

Algú en principi ben informat…

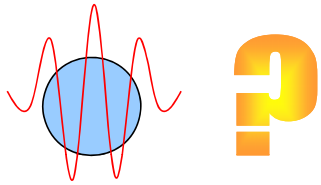
*"…**crec que puc dir amb tota tranquilitat que ningú entén la Física Quàntica**…*

…no vagin preguntant-se però com pot ser?, perquè s'endinsaran en un carreró del que ningú ha pogut sortir-ne encara…"

R. Feynman, Premi Nobel, 1965

A tall d'exemple: Què és la llum?

- ~1690 Huygens: La llum és una ona (Reflexió/Refracció)
- ~1690 Newton: Creia que la llum consisteix en corpuscles
- 1873 Maxwell: la radiació e.m. (llum) són ones
- 1888 Hertz: Produeix ones e.m. amb circuits elèctrics
- ~1920 Einstein: La llum consisteix en partícules (fotons)
- La llum es manifesta de manera dual en funció del fenòmen que estudiem



Perquè la física quàntica ? (El passat)

~ 1900: Sorpreses sorprenents

Radiació del cos negre

L'estabilitat de l'àtom

Espectres atòmics de radiació

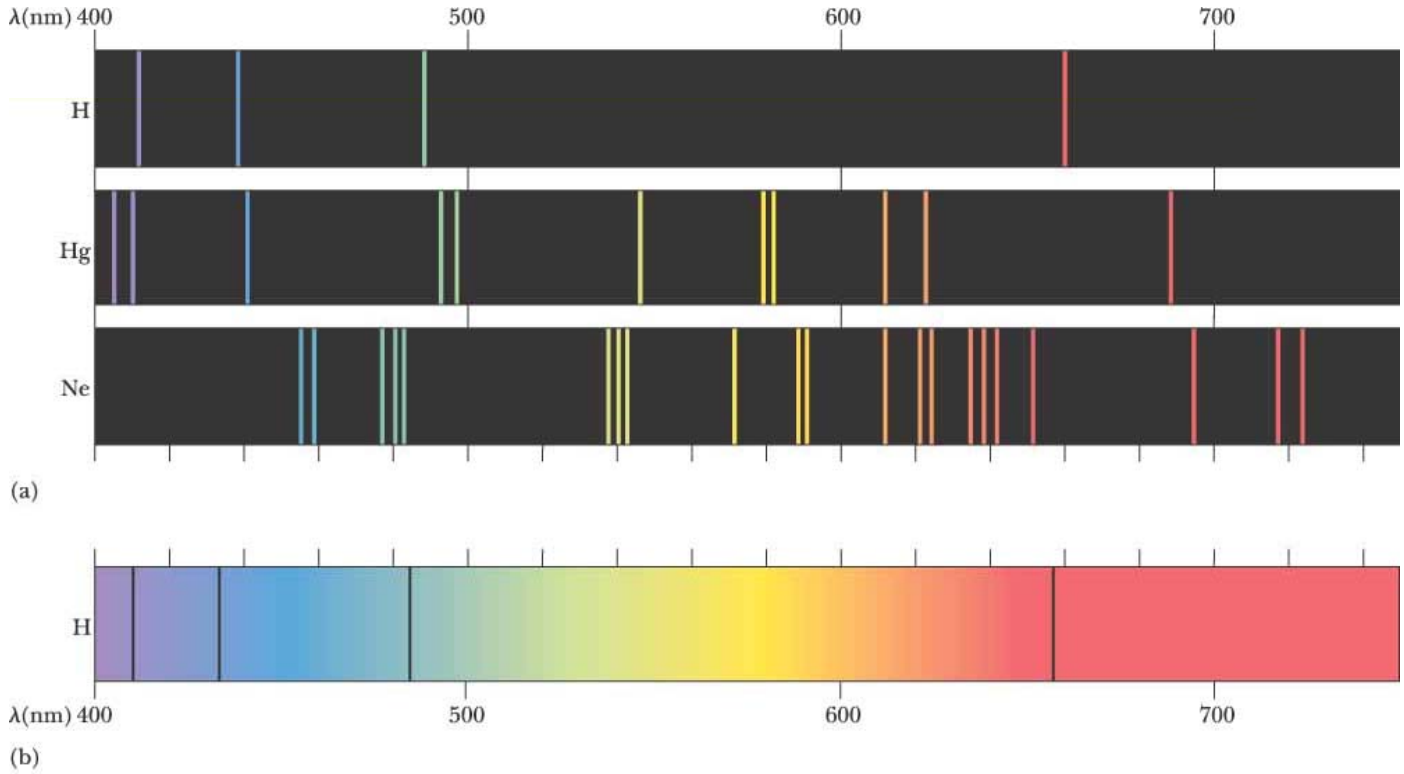
L'efecte fotoelèctric

Efecte Compton

Difracció d'electrons

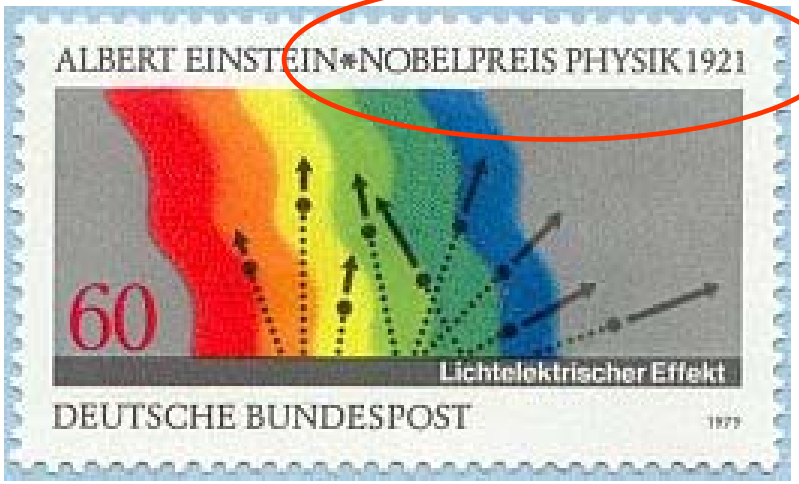
Avui això no toca

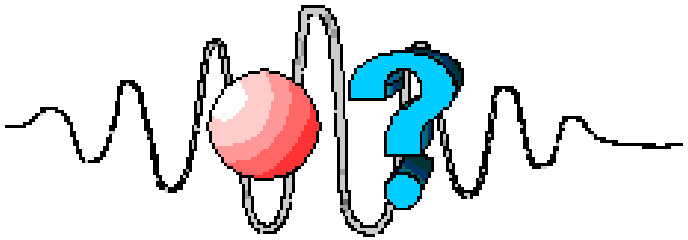
Espectres atòmics d'emissió



Espectre d'absorció de l'hidrògen

Efecte fotoelèctric





FOTÓ

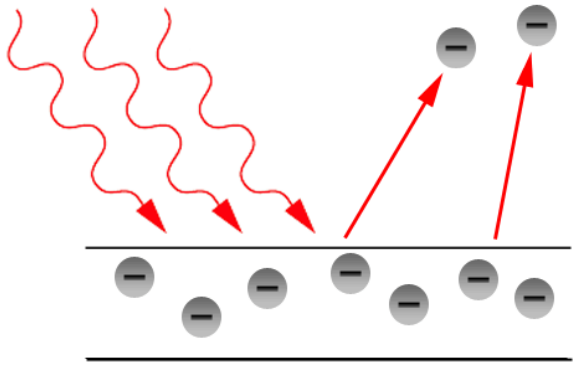
primera partícula predita teòricament

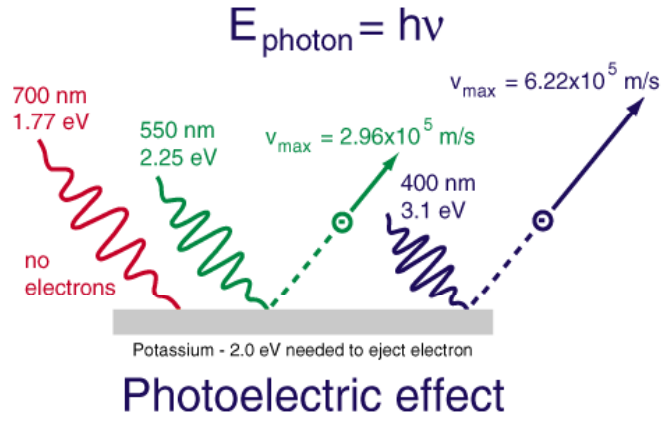
Efecte fotoelèctric: L'explicació

Per molt intensa que sigui la llum, si la freqüència és baixa, $\nu \leq \nu_L$,
no escapen electrons

El nombre d'electrons emesos és proporcional a la intensitat de la llum

Els electrons que escapen del metall ($\nu > \nu_L$) tenen una energia proporcional a ν





h és la constant de Planck

Fotó = quantum de llum

però…

“A l’Albert Einstein pels seus serveis a la Física Teòrica i especialment per la seva descoberta de la llei de l’efecte fotoelèctric”

Premi Nobel, 1922

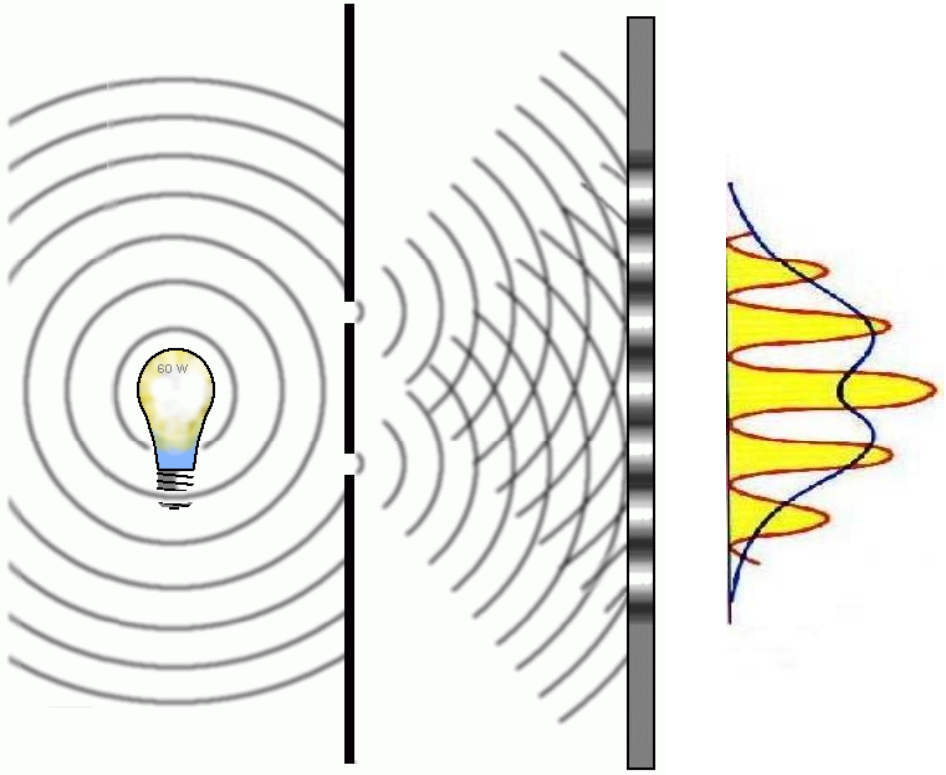
Quin era el problema?

"…semblava violar tot el que sabíem sobre la interferència de la llum"

R.A. Millikan, 1948

Premi Nobel, 1923 (en part per intentar demostrar experimentalment que la teoria d'Einstein era incorrecta!)

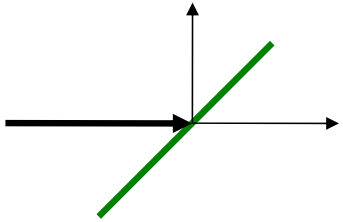
Les ones interfereixen



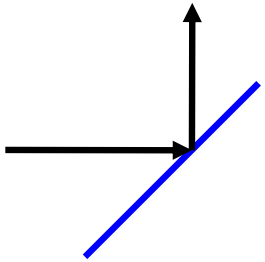
Només les ones ?

Experiment d'Interferometria

FOTONS

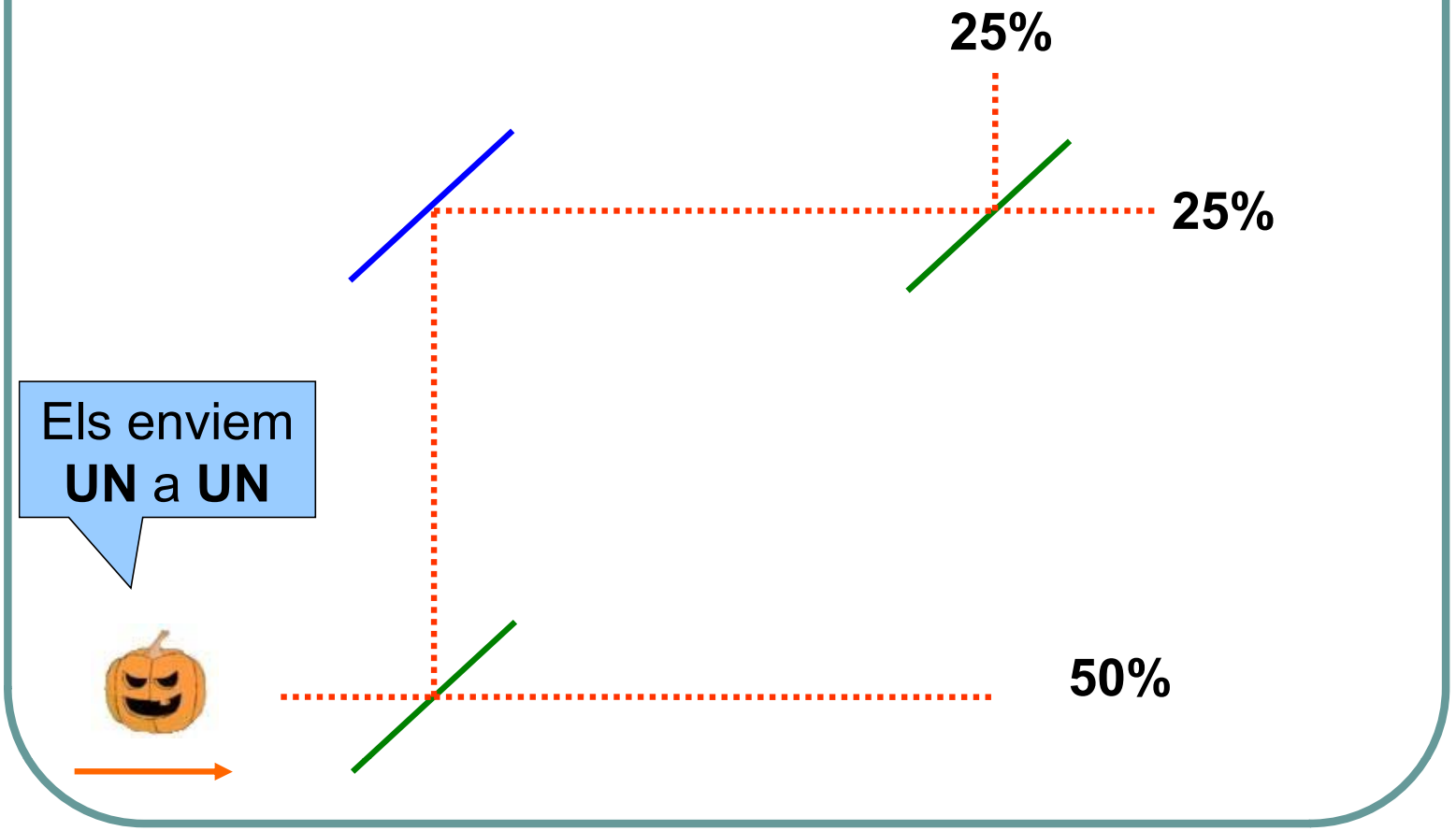


VIDRES SEMITRANSPARENTS

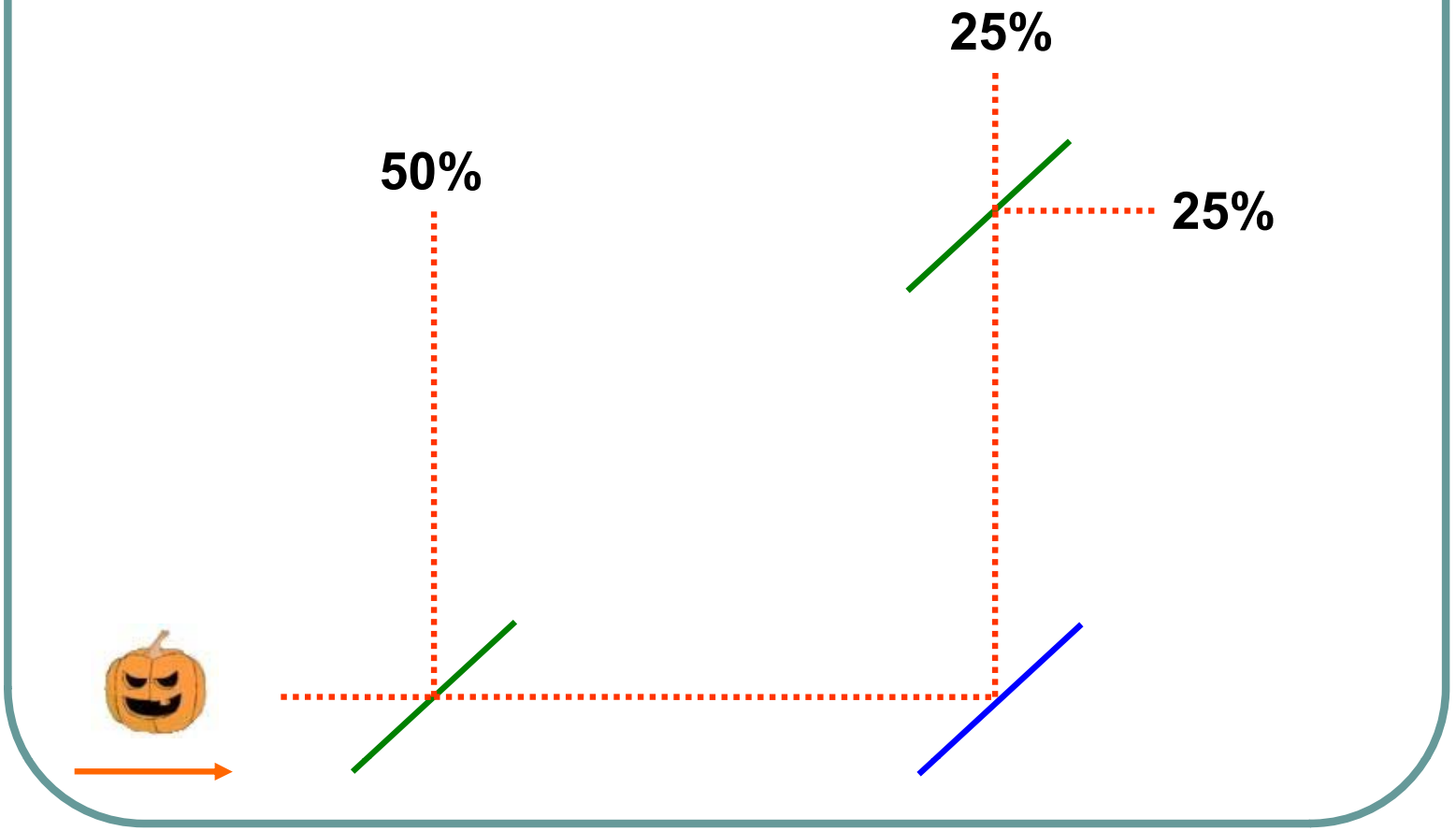


MIRALLS

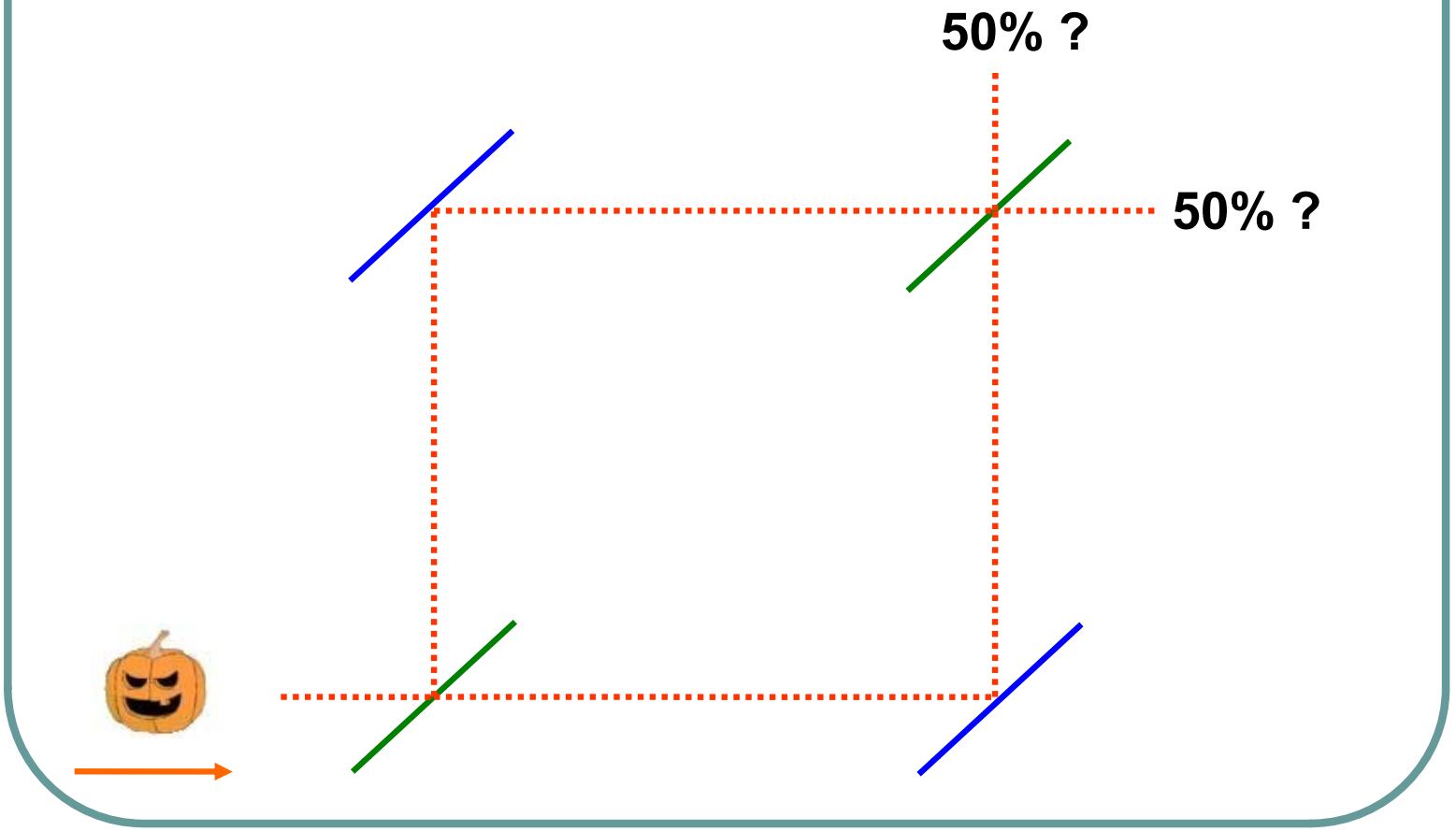
Semblen molt avorrits …



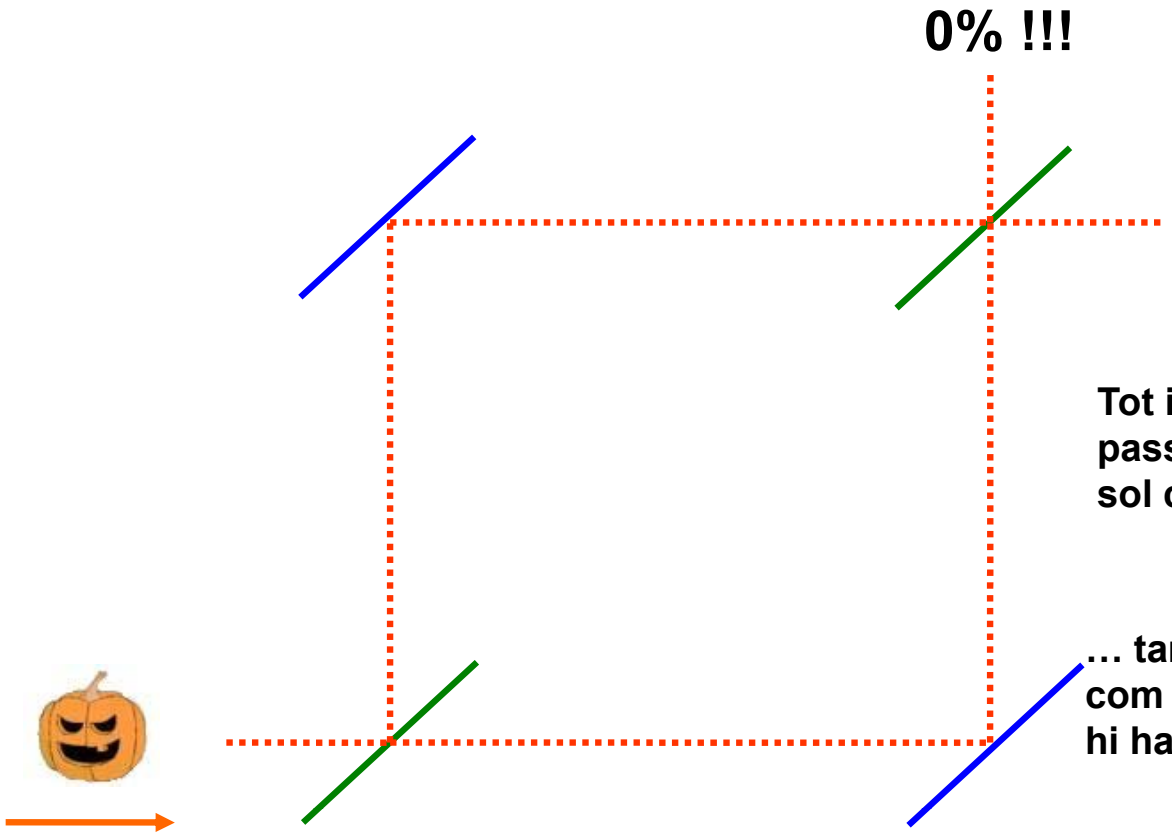
Res de nou …



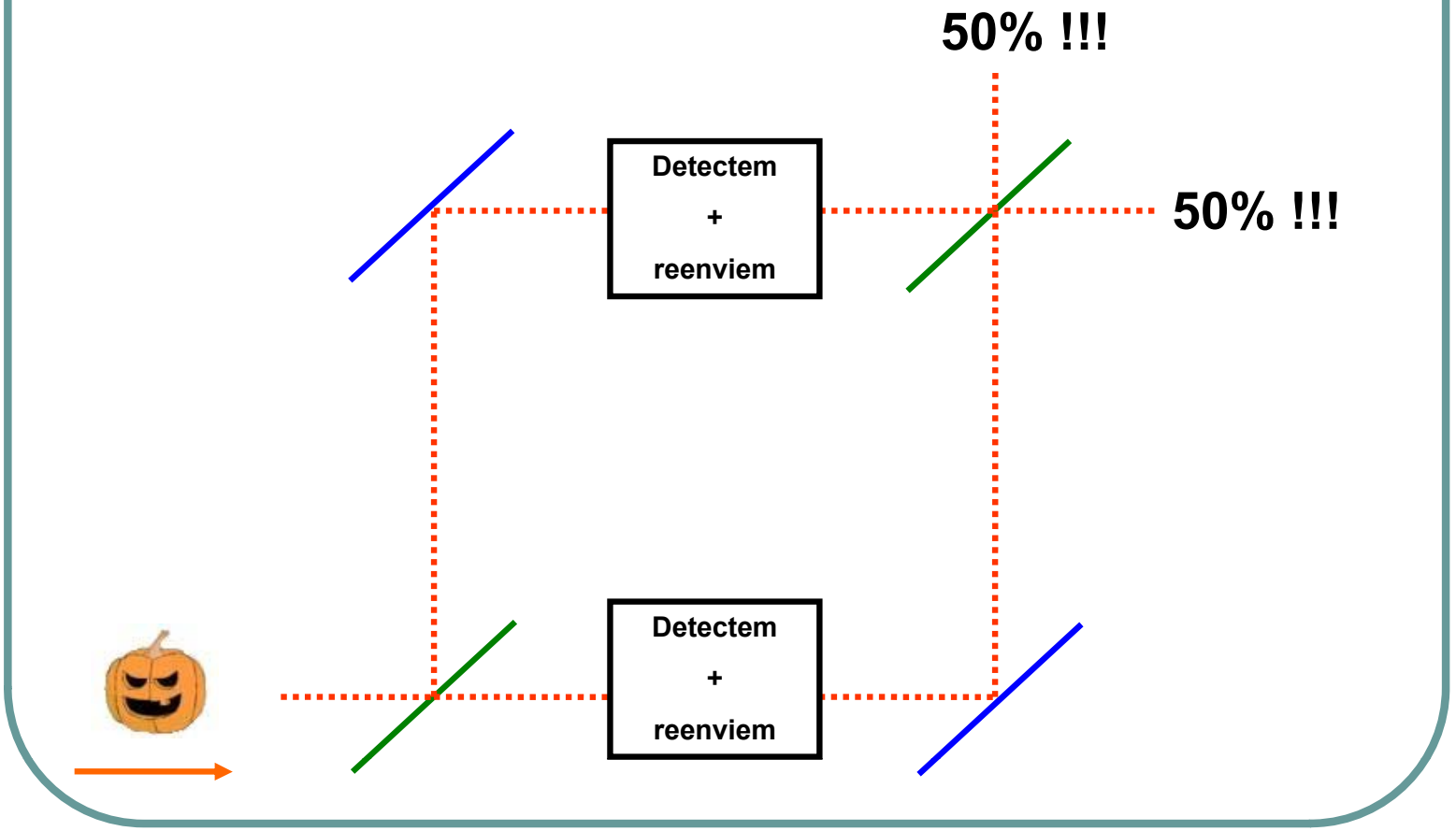
Interferòmetre Mach-Zehnder



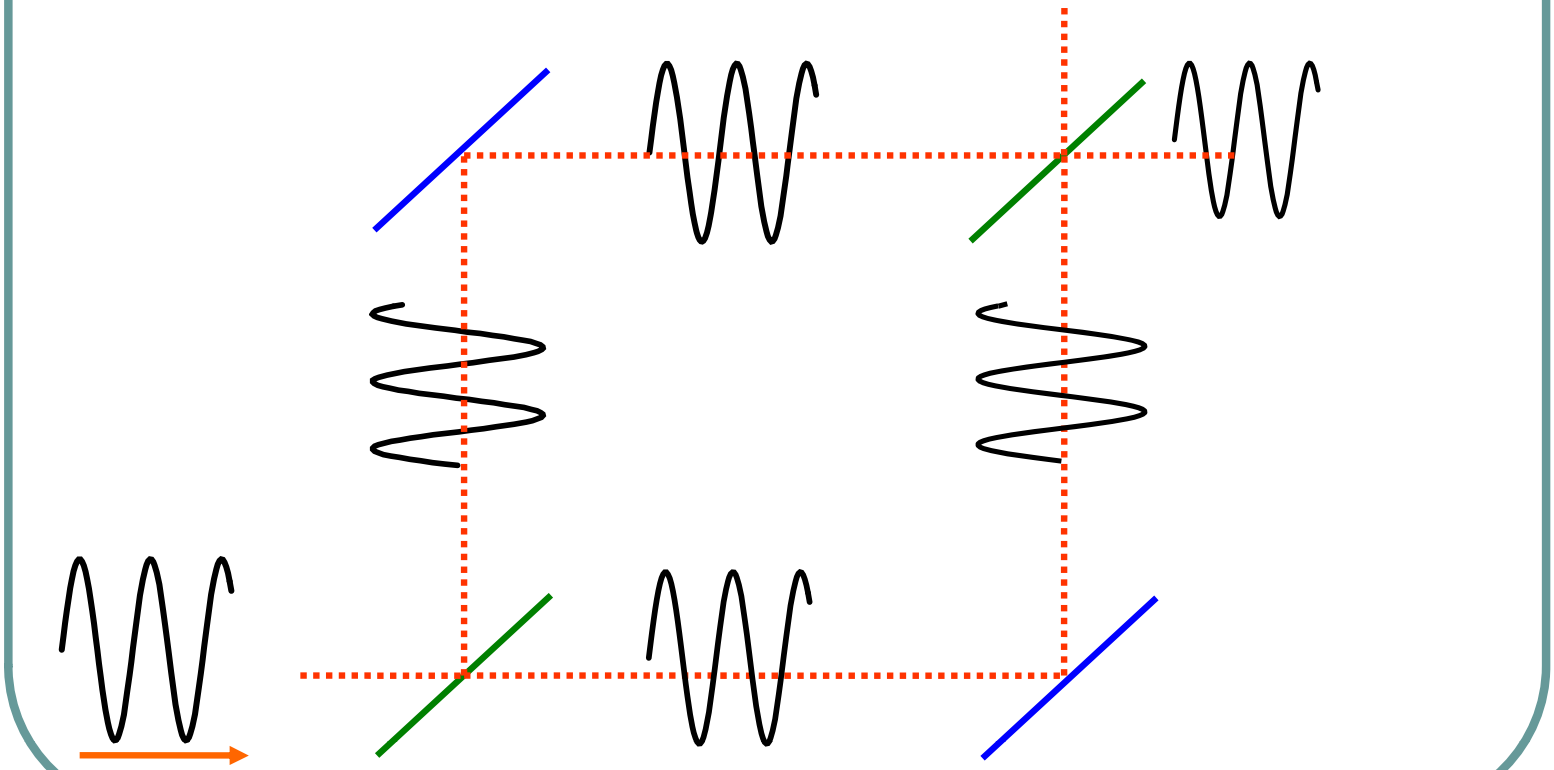
Sorpresa!


0% !!!
100% !!!
Tot i que sembla passar per un sol camí…
… també sembla com si sabés que hi ha dos camins

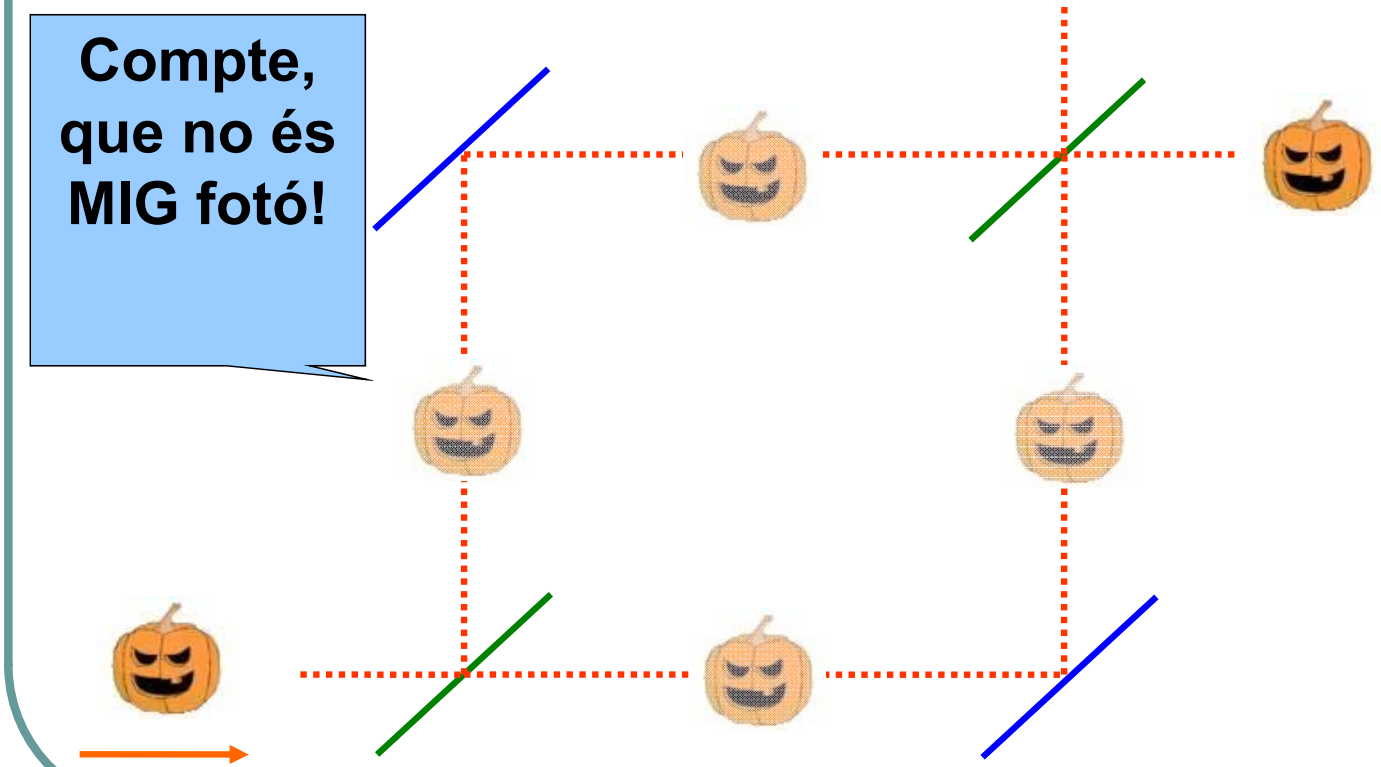
I si els espiem?



Tot “funciona” si pensem en ones



Costa MOLT d'imaginar…

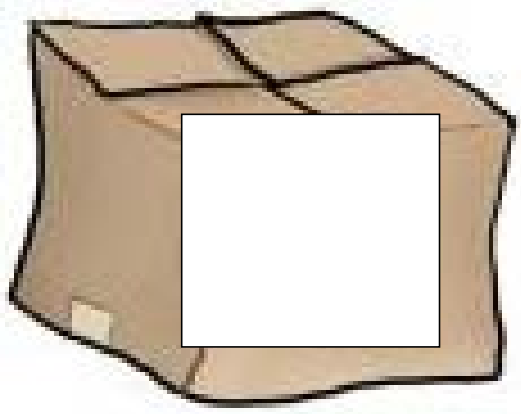


“Doble personalitat”

- Quan mirem on és, es comporta com una PARTÍCULA !
- Quan no estem mirant, es comporta com una ONA !

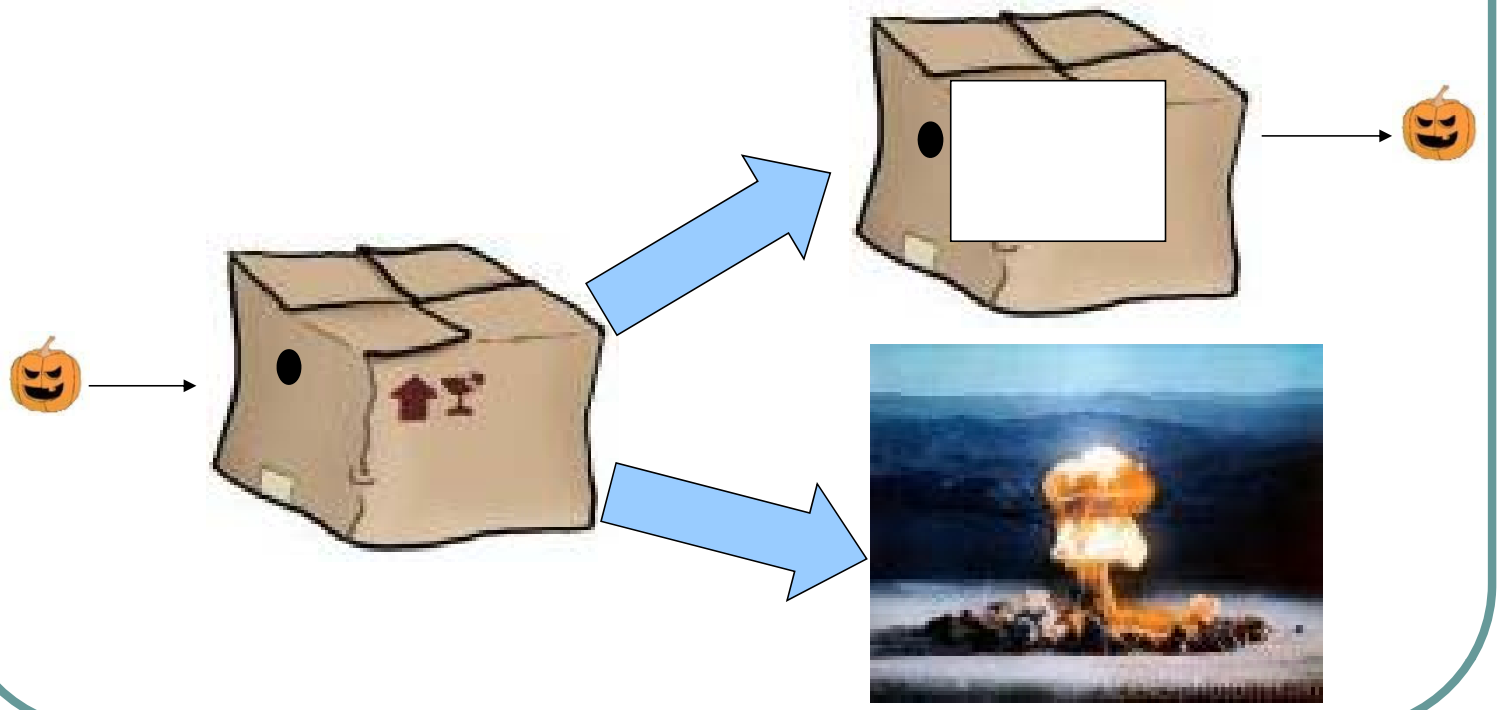
Veure-hi sense mirar

Una caixa pot contenir una bomba …

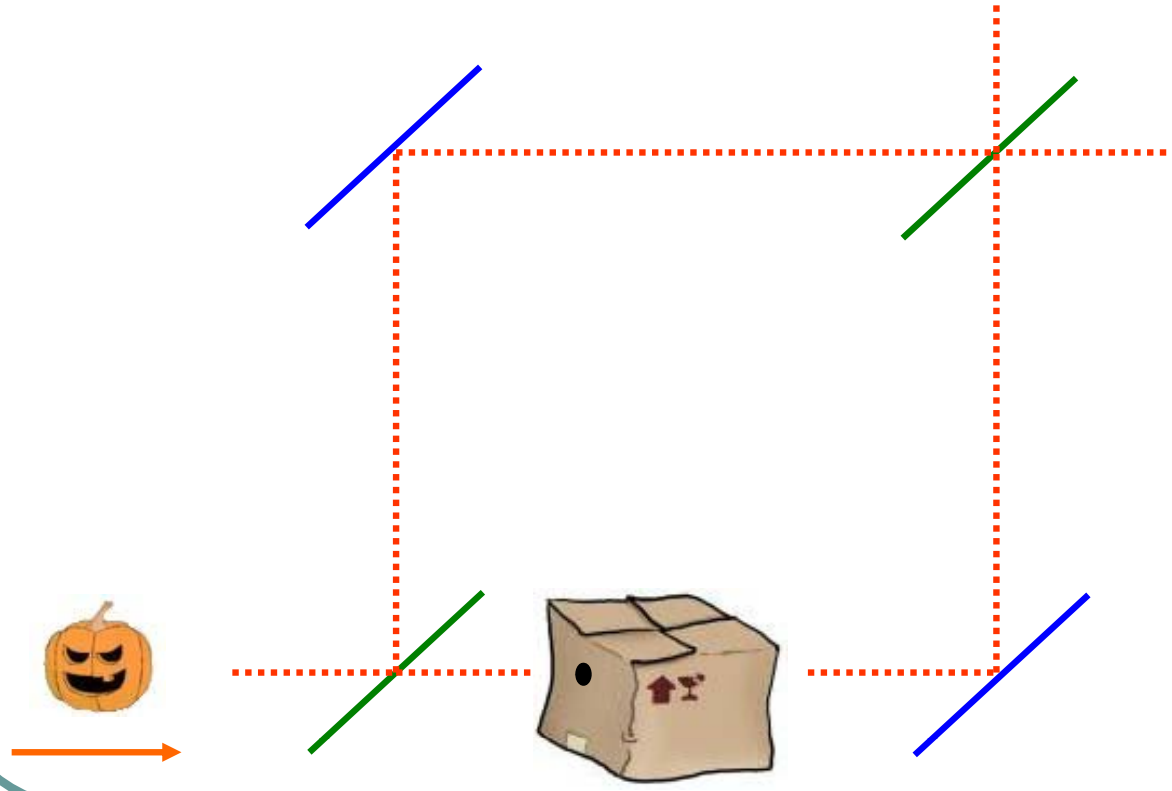


…ultrasensible

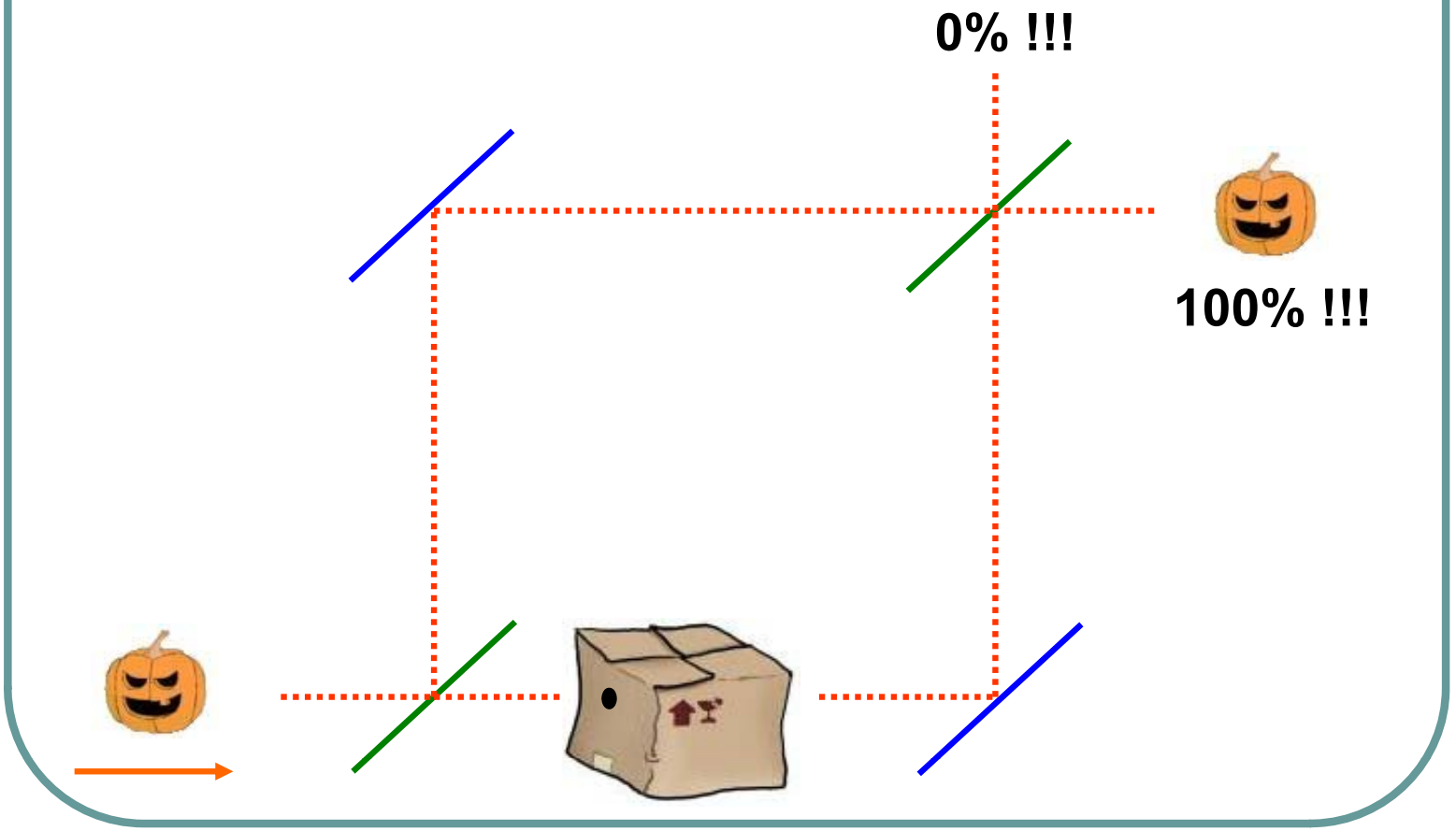
Un sol fotó pot fer-la explotar



Posem la caixa en un Mach-Zender

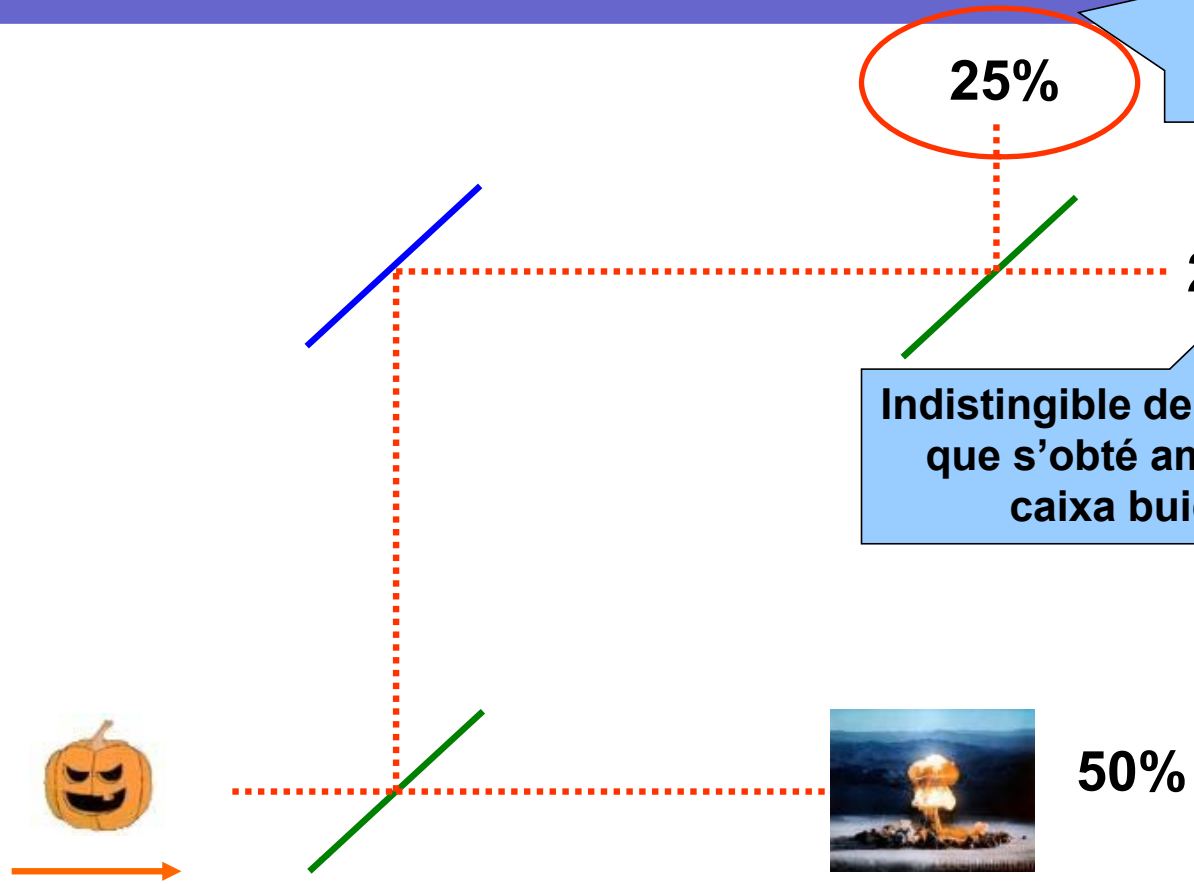


Si la caixa és buida…



Si sempre hi ha bomba…

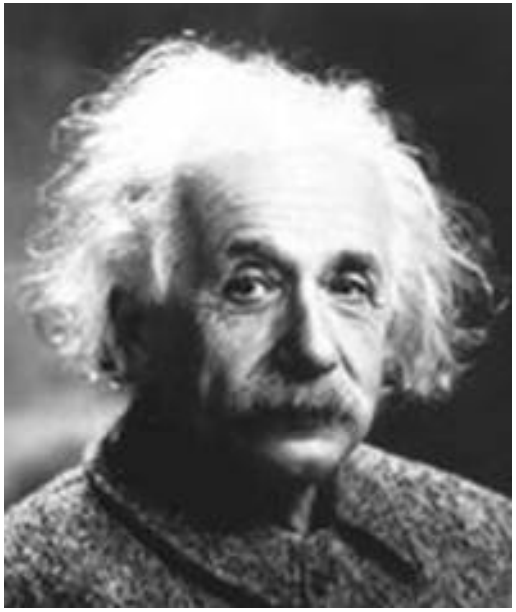
Aquests fotons ens diuen que hi ha una bomba sense fer-la explotar!



Màgia!

- Podem detectar ¼ de les bombes sense fer-les explotar i, per tant, sense que cap fotó hagi entrat per “comprovar” si hi ha una bomba o no.
- Es pot refinar fins que la probabilitat pugi des de ¼ fins a un nombre tant proper a 1 com es vulgui.

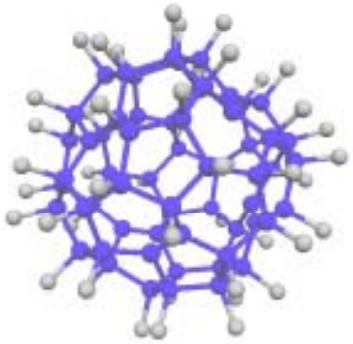
Què n'opina Einstein?



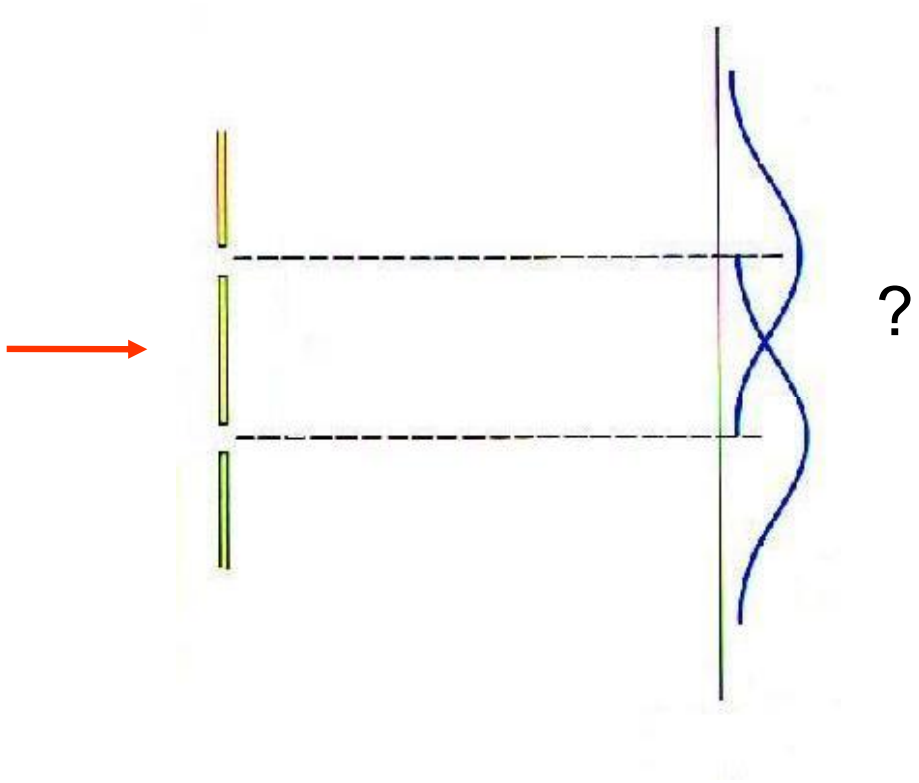
"Aquests cinquanta anys de cavilacions no m'han portat més prop de respondre la pregunta: què és el quantum de llum?

A. Einstein, 1951

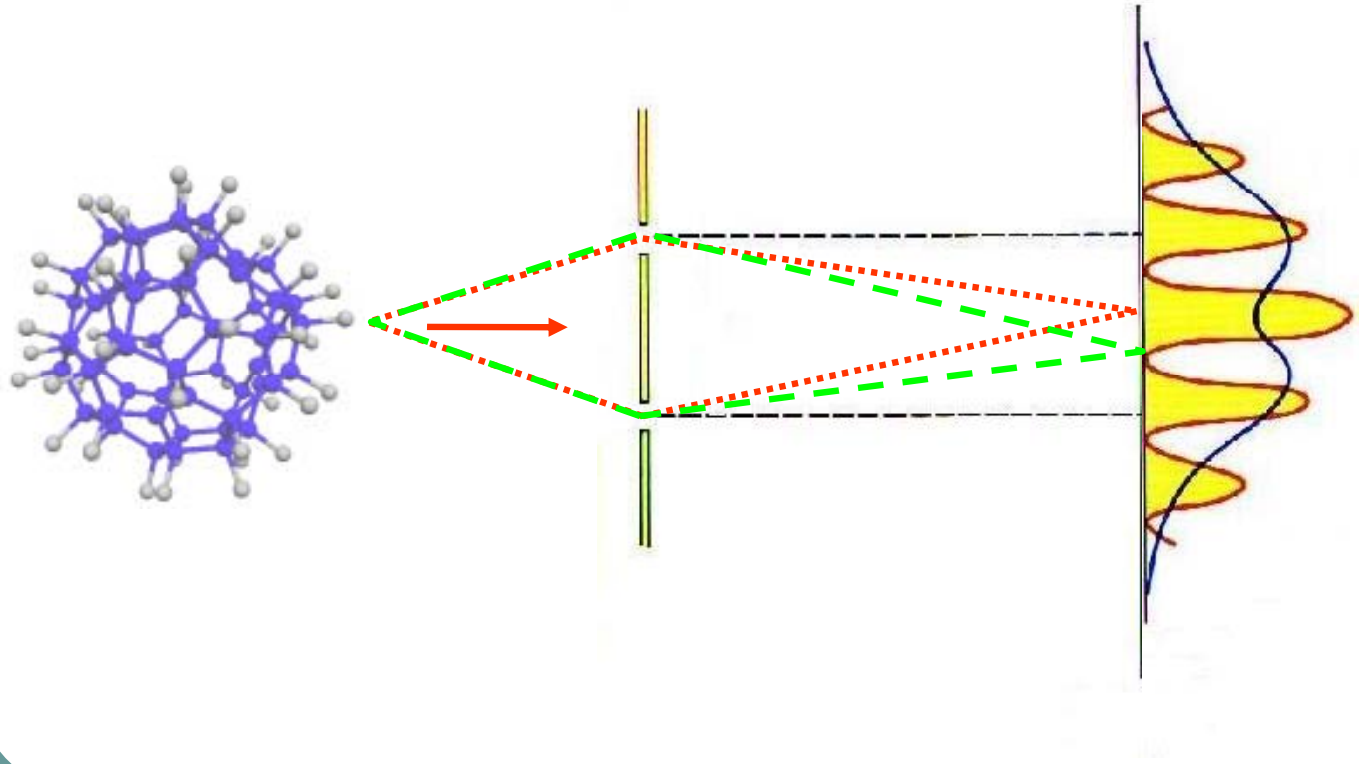
Tothom té doble personalitat!



Fluorofullerè
Rècord de l'any 2003



Es comporta com una ona … !!!



Implicacions filosòfiques

- Dualitat ona-partícula
- La “realitat” depèn de si s’observa ! (Qui ?)

Actitud pragmàtica: Oblidem els nostres prejudicis, basats en la nostra experiència del món macroscòpic, i intentem formular una teoria que ens permeti explicar tot el que observem en el món microscòpic.

De fet, hi ha més sorpreses…

Mesura i incerteses

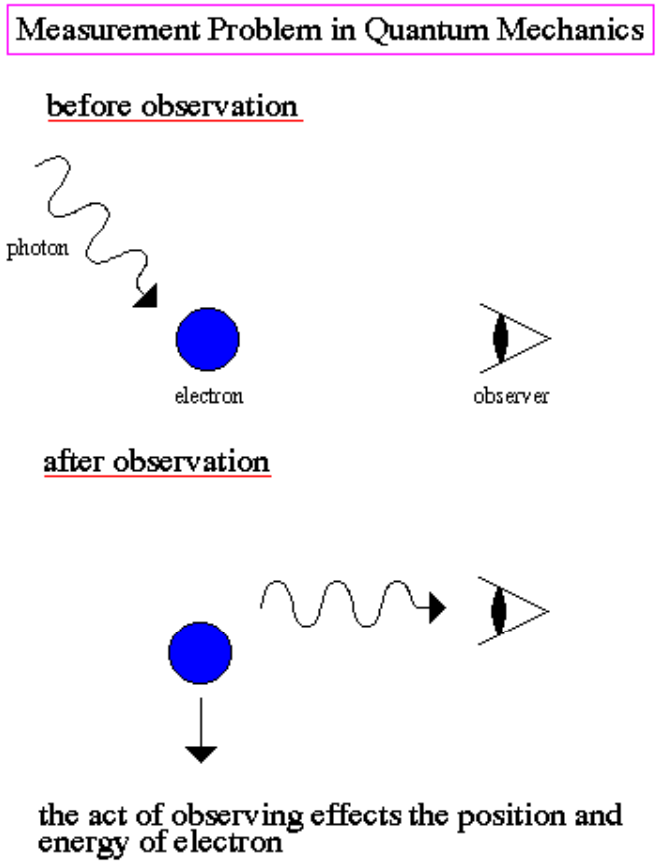
Estem acostumats (Física Clàssica) a mesurar la posició i la velocitat d'objectes macroscòpics

Com ho fem?

Llum d'alguna font xoca amb l'objecte i rebota cap a nosaltres

Què passaria si, en lloc de llum, enviéssim cotxes per mesurar la posició i velocitat d'un cotxe?

La mesura en FQ



En mesurar…

No podem estar segurs de quina velocitat adquirirà l'electró

No podem saber si inicialment estava quiet

La nostra mesura afecta a l'estat de l'electró !

Com més vegades mesurem, pitjor !!!

Podem usar fotons molt poc energètics i modificar "molt poc" l'estat de l'electró? (En Física Clàssica podem millorar les mesures utilitzant aparells cada vegada més sensibles):

Principi d'incertesa de Heisenberg: És impossible determinar simultàniament la posició i la velocitat (moment) d'un electró amb precissió infinita

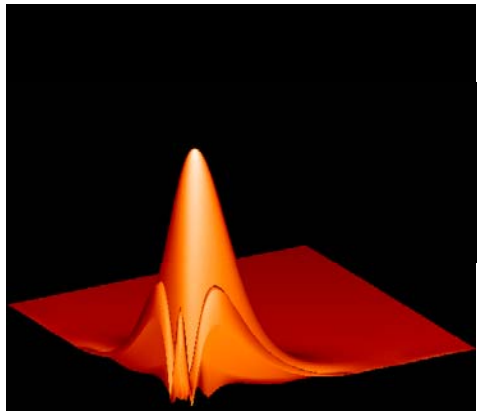
No podem parlar de trajectòries !

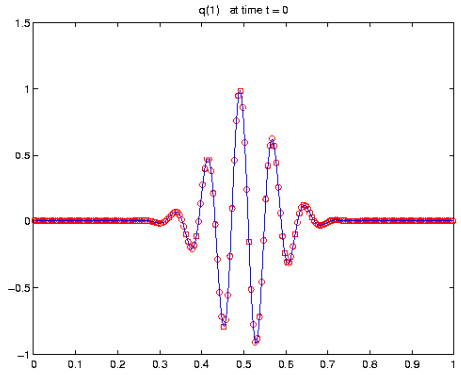
Postulats Física Quàntica

- Funció d'ona
- Operadors
- Valors mesurables
- Completitud
- Valors esperats (mitjanes)
- Càlcul de funcions d'ona i la seva evolució temporal

Funció d'ona

- Tota partícula vindrà descrita per una funció d'ona $\Psi(x,y,z,t)$
- $\Psi(x,y,z,t)$ és una funció complexa, en general. (Part real i part imaginària)
- On és la partícula? No ho sabem! $|\Psi(x,y,z,t)|^2$ ~ probabilitat ! Incertesa en la posició Δx
- Incertesa en el moment Δp (velocitat)
- Es verifica el principi d'incertesa de Heisenberg $\Delta x \, \Delta p \geq h / 4\pi$
- Tota partícula, descrita per una funció d'ona, serà susceptible de produïr interferències





Operadors i Observables

- Operadors: Eines per mesurar Observables com la posició, el moment, l'energia,… d'una partícula/funció d'ona
- Si mesurem un observable, posició, per exemple, i trobem un lloc, la funció d'ona col.lapsa.
- Els valors possibles en mesurar observables són els valors propis i corresponen a estats propis

Completitud i superposició

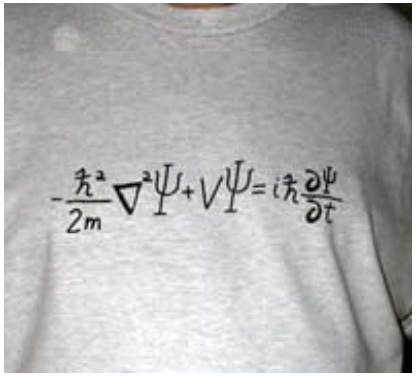
- Qualsevol funció d'ona pot expressar-se com a combinació lineal d'estats propis d'algun observable

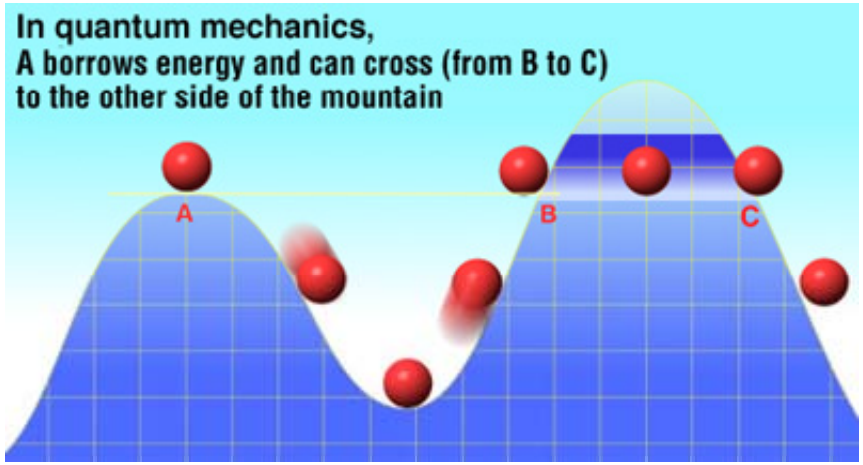
Valors esperats (mitjanes)

- La física quàntica (FQ) no permet predir quin resultat obtindrem en fer una mesura d'un estat superposició conegut. Només ens diu quines probabilitats tenen els valors possibles.
- Si tinguéssim moltes còpies idèntiques, el valor esperat -valor mitjà- seria predictible per la FQ
- Semblant a quin valor sortirà quan tirem un dau?
- I si el tirem moltes vegades, quin serà el valor mitjà que obtindríem?

Equació de Schrödinger

- Càlcul de funcions d'ona i la seva evolució temporal





- Efecte túnel

Conseqüències dels postulats

- Model d'àtom: Orbitals
- Energies possibles quantificades. Expliquen els espectres atòmics
- Evolució temporal: Descrita per l'eq. de Schrödinger. Efecte túnel
- Superposició d'estats
- Mesura: Col.lapse de la funció d'ona

Si Ψ_1 i Ψ_2 són estats propis de l'observable A, amb valors propis a_1 i a_2.
Si $\Psi = c_1 \Psi_1 + c_2 \Psi_2$ és l'estat inicial.
Quan mesurem A, trobarem amb probabilitat $|c_1|^2$: el valor a_1 col.lapsant a l'estat final Ψ_1

probabilitat $|c_2|^2$: el valor a_2 col.lapsant a l'estat final Ψ_2

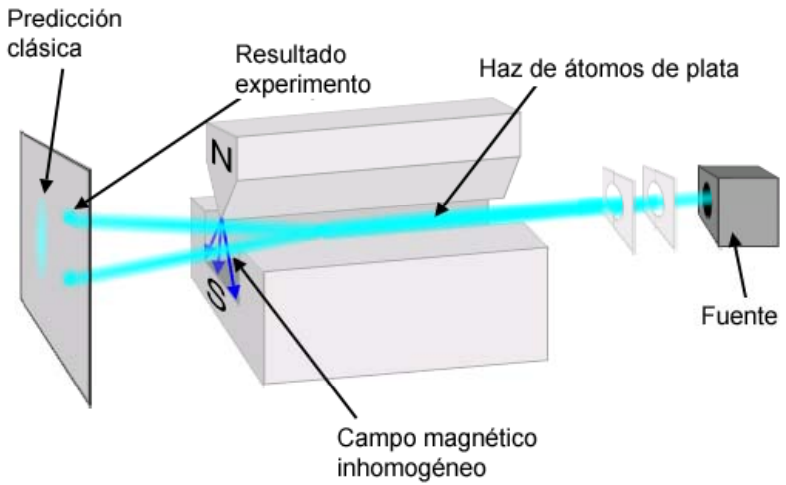
Si Ψ_1 i Ψ_2 són estats possibles,

a Ψ_1 + b Ψ_2 també ho és

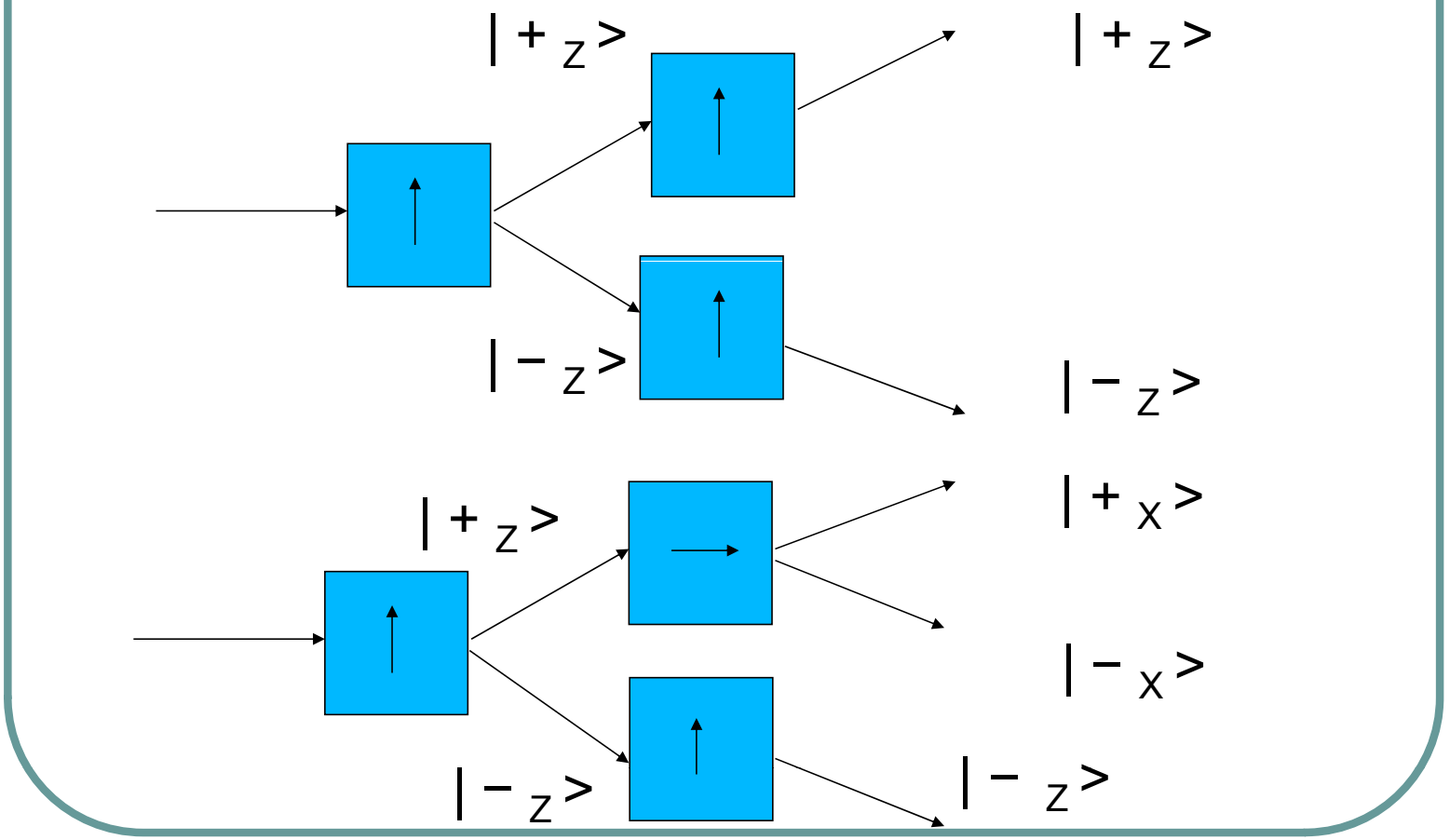
Conse

Col.lapse?

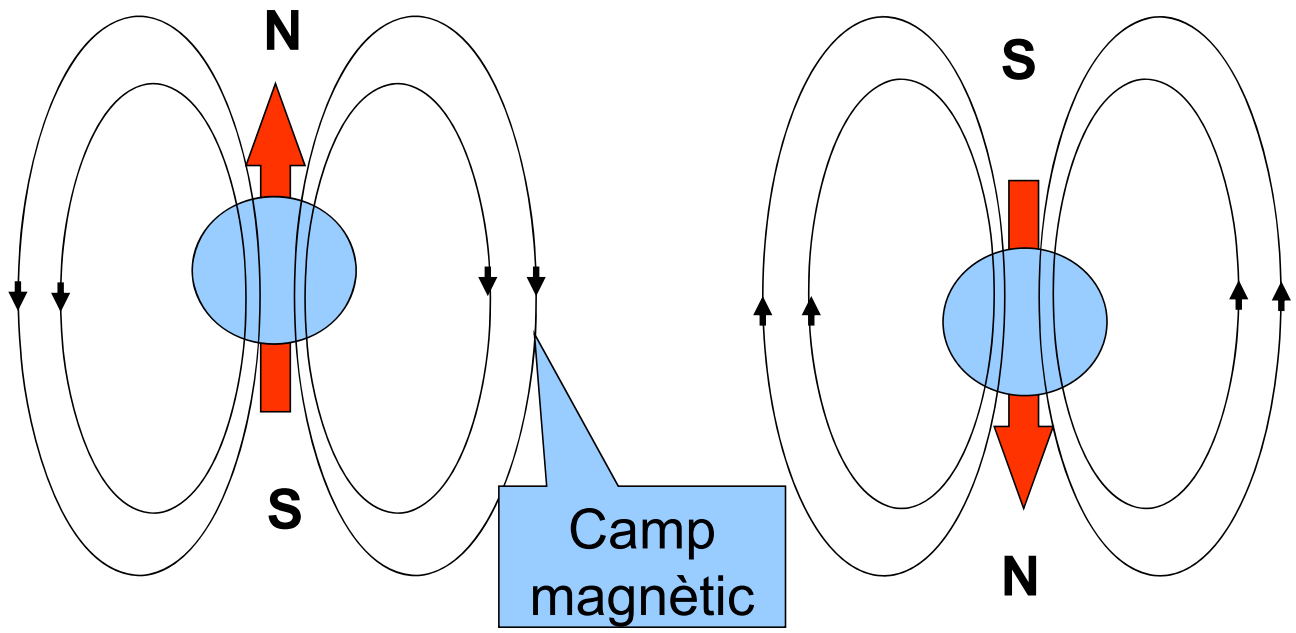
Exemple: Moment magnètic electró



Què passa en realitat ?



Del moment magnètic de l'electró en direm spin



Pot trobar-se en els dos estats simultàniament... **fins que mirem!**

Un cop hem mirat, sabem amb certesa en quin estat es troba !

La certesa en Z esdevé incertesa en X !!!

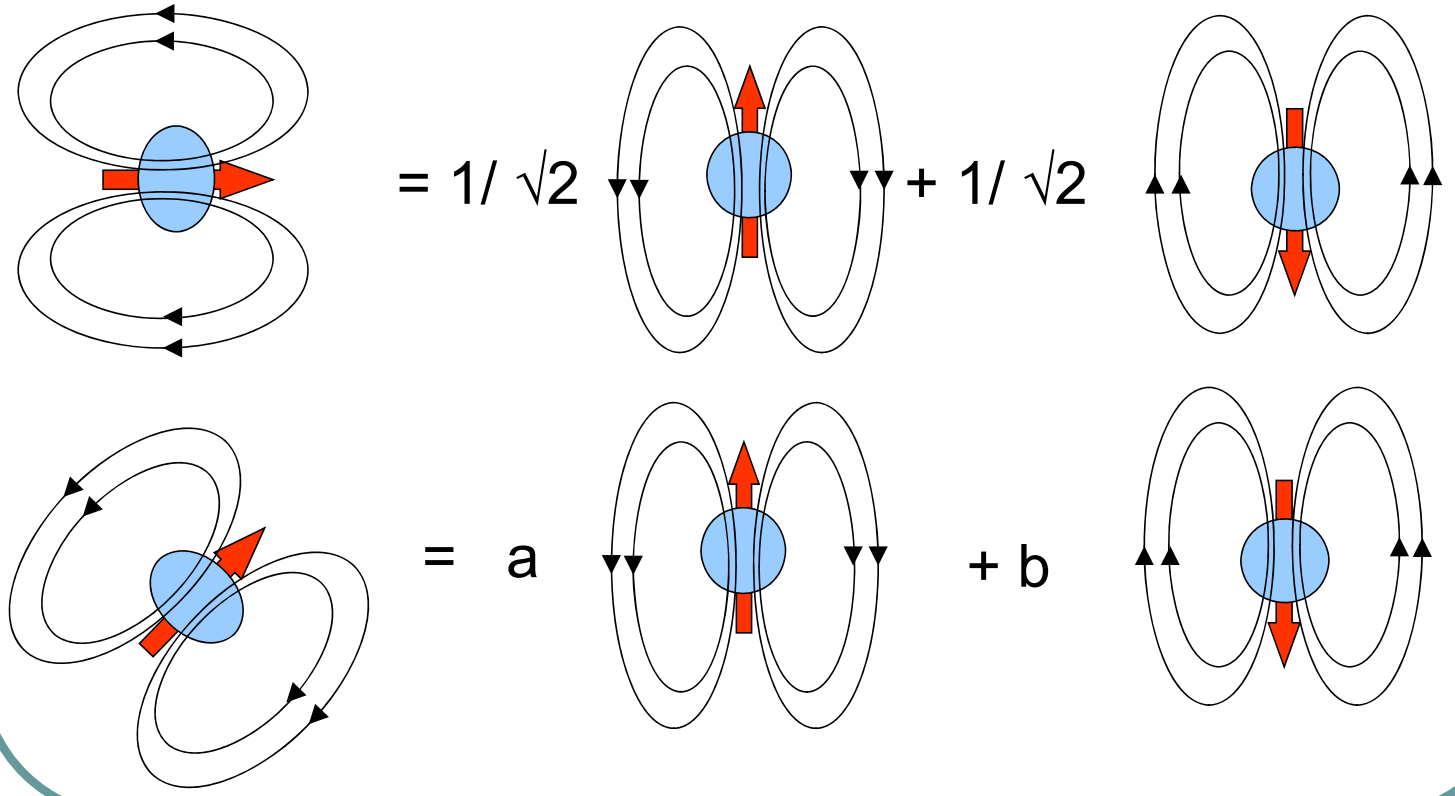
Superposició?

- Els estats $\{|+>_z, |->_z\}$ formen una base.
- Els estats $\{|+>_x, |->_x\}$ també formen una base.
- $|+>_x = 1/\sqrt{2}\ (|+>_z + |->_z)$
- $|->_x = 1/\sqrt{2}\ (|+>_z - |->_z)$

Si de l'estat $|+>_x$ en mesurem l'spin segons x, trobarem + amb probabilitat 1

Si de l'estat $|+>_x$ en mesurem l'spin segons z, trobarem { + amb probabilitat 50%
- amb probabilitat 50%

Superposició (intuïtiva)

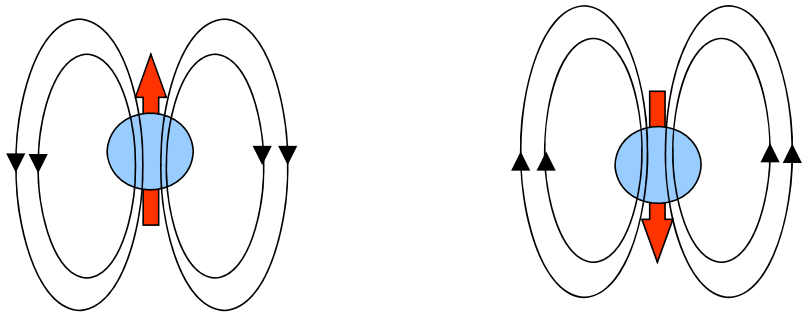


El futur ?

- Dels bits als qubits (bits quàntics)
- Computació Quàntica
- Avantatges? Algorisme de Grover
  Algorisme de Shor
- Conseqüències? Seguretat RSA compromesa
- Solucions: La propia Física Quàntica
  Criptografia Quàntica !!! (ja present)

QUBITS

Molt més sofisticat que els 0 o 1 que són possibles en els bits

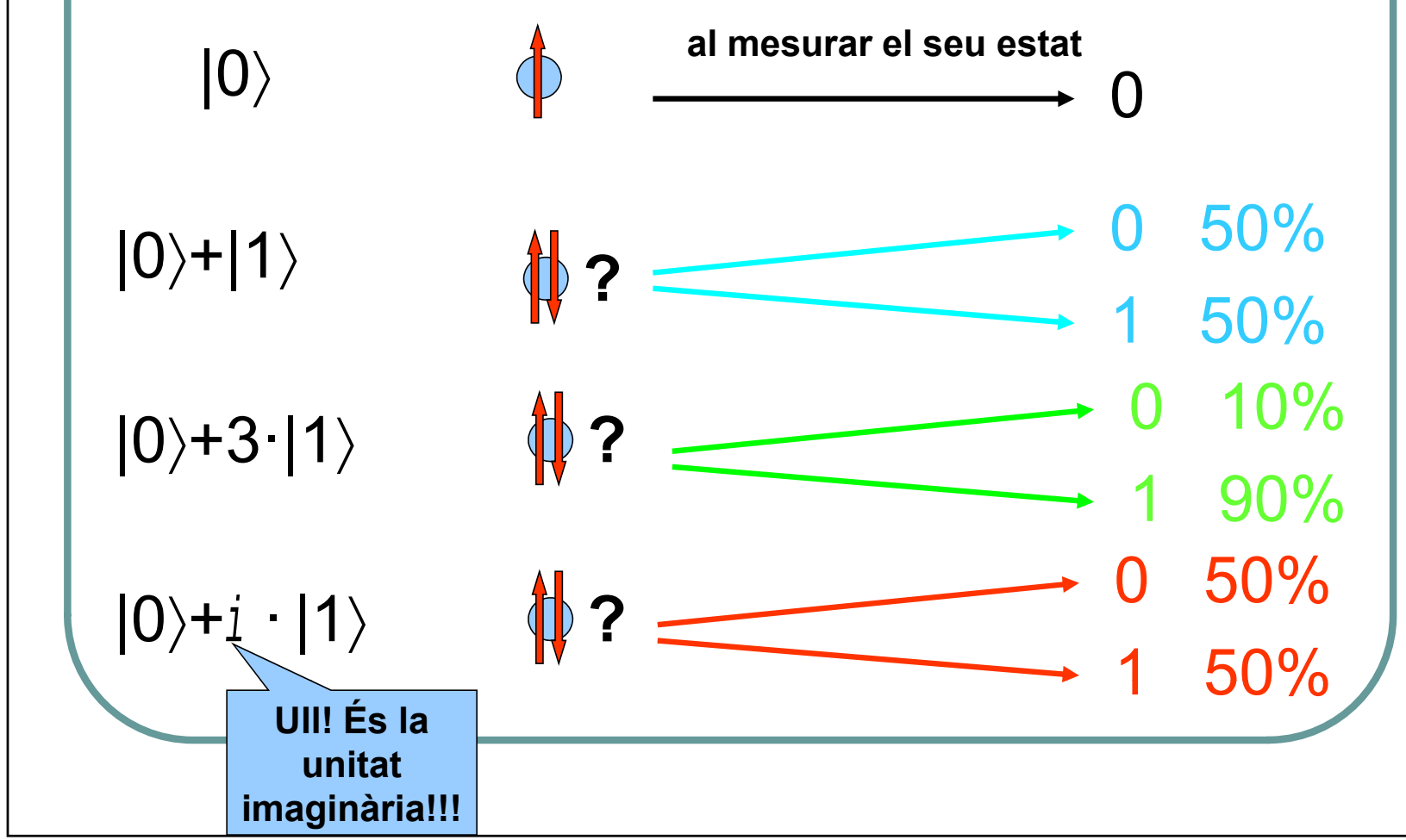


$$|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$$

α i β són nombres complexos!

~ probabilitat de trobar l'estat |0> o |1> al mirar

Uns quants exemples



Generador de nombres Random

Sigui un qubit descrit per: $1/\sqrt{2}\,|0\rangle + 1/\sqrt{2}\,|1\rangle$

Sigui un altre qubit idèntic: $1/\sqrt{2}\,|0\rangle + 1/\sqrt{2}\,|1\rangle$

Sigui un tercer qubit idèntic: $1/\sqrt{2}\,|0\rangle + 1/\sqrt{2}\,|1\rangle$

Els tres qubits poden agrupar-se en:

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

$$1/\sqrt{8}\,(|0\rangle|0\rangle|0\rangle + |0\rangle|0\rangle|1\rangle + |0\rangle|1\rangle|0\rangle + |0\rangle|1\rangle|1\rangle + |1\rangle|0\rangle|0\rangle + |1\rangle|0\rangle|1\rangle + |1\rangle|1\rangle|0\rangle + |1\rangle|1\rangle|1\rangle)$$

És una combinació lineal de 8 termes, tots ells amb el mateix coeficient. Si mesurem els tres qubits, trobarem un resultat dels 8 possibles, per exemple, $|0\rangle|1\rangle|1\rangle$, amb probabilitat 1/8.

$= 1/\sqrt{8}\,(0 + 1 + 2 + 3 + 4 + 5 + 6 + 7)$ ⟶ en notació binària !

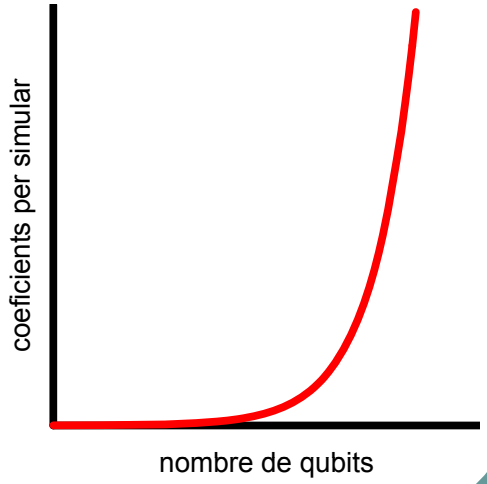
Suposem N d'aquests

$a|0\rangle + b|1\rangle$ **2** coeficients que s'han de calcular

$a|0\rangle|0\rangle + b|0\rangle|1\rangle + c|1\rangle|0\rangle + d|1\rangle|1\rangle$ $4=2^2$

2^N

N=100 $\Rightarrow 2^{100}$> nombre d'àtoms del Sol !



Fer de la necessitat virtut

- Feynman (1982): per què no utilitzar un sistema quàntic que puguem controlar per simular-ne un altre?

- David Deutsch (1985): és possible que un ordinador quàntic resolgui problemes computacionals que no tenen solució eficient en un ordinador clàssic?

Sí!!! Algorisme de Deutsch

- Donada una moneda, podem determinar amb **una sola tirada** si és bona o està falsificada?

Bona: cara i creu
Falsa: dues cares o dues creus

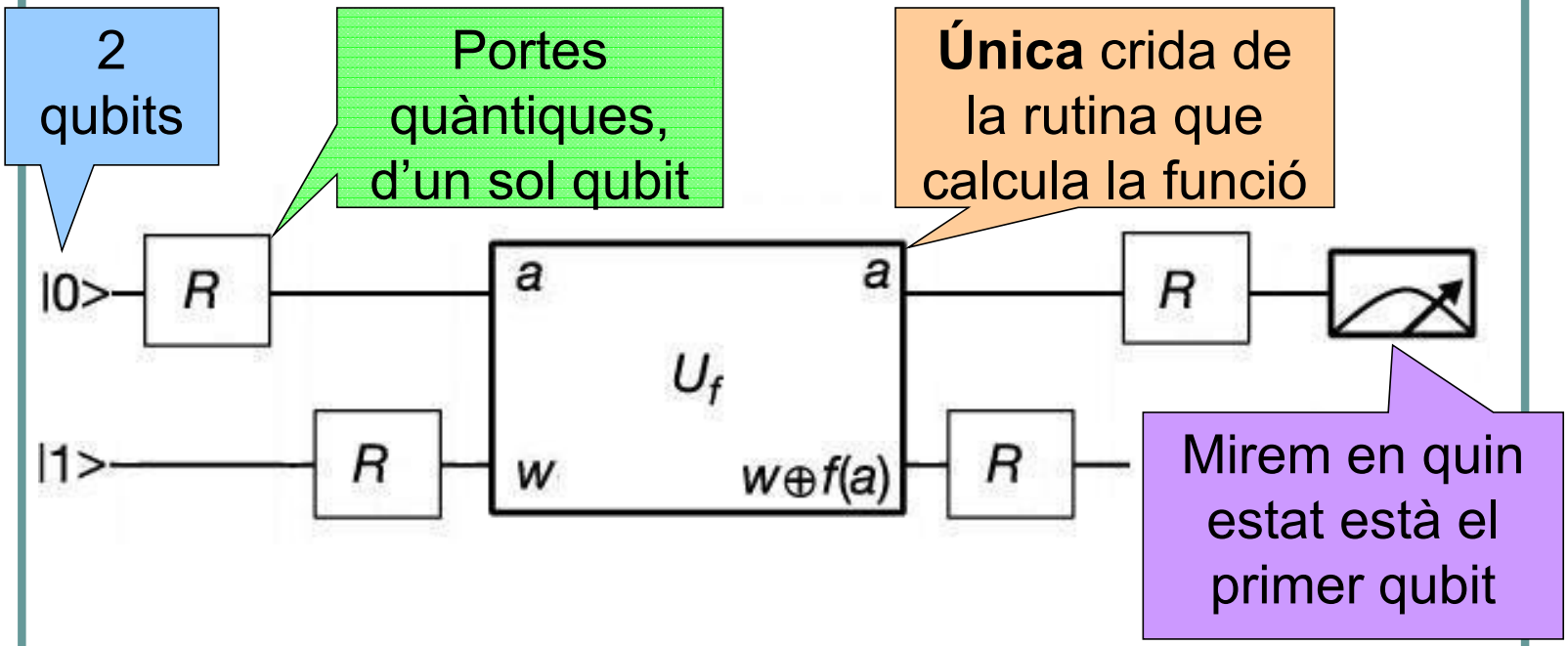
En llenguatge més matemàtic

- Donada una funció binària, podem saber amb **una sola consulta** si és constant?

f(0) = 0	f(1) = 0
f(0) = 1	f(1) = 1
f(0) = 0	f(1) = 1
f(0) = 1	f(1) = 0

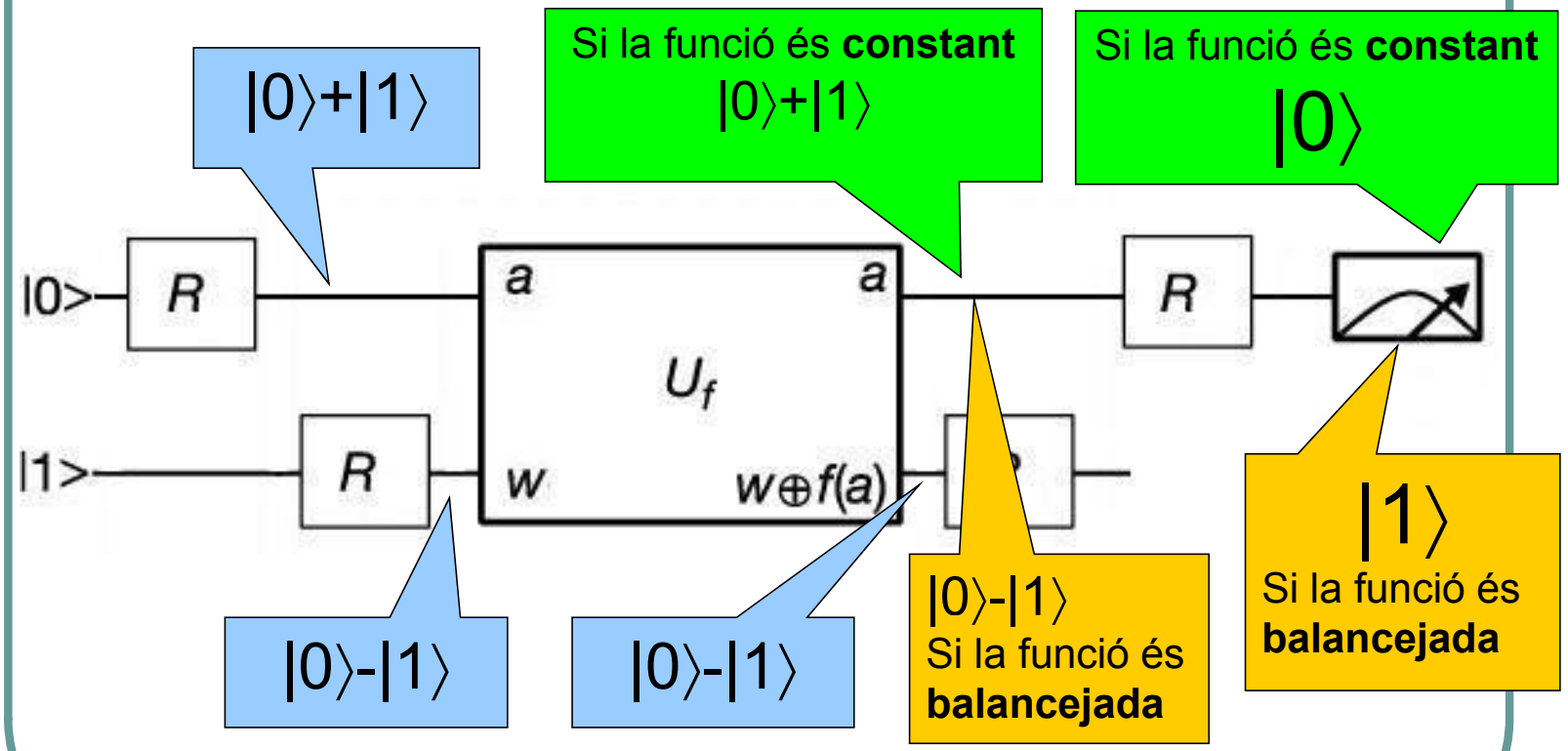
La lògica habitual ens diu que primer haurem de cridar la rutina pel valor 0, després pel valor 1, i comparar el resultat $\Rightarrow$**2** crides

Aquest "ordinador quàntic" ho fa amb una sola crida!

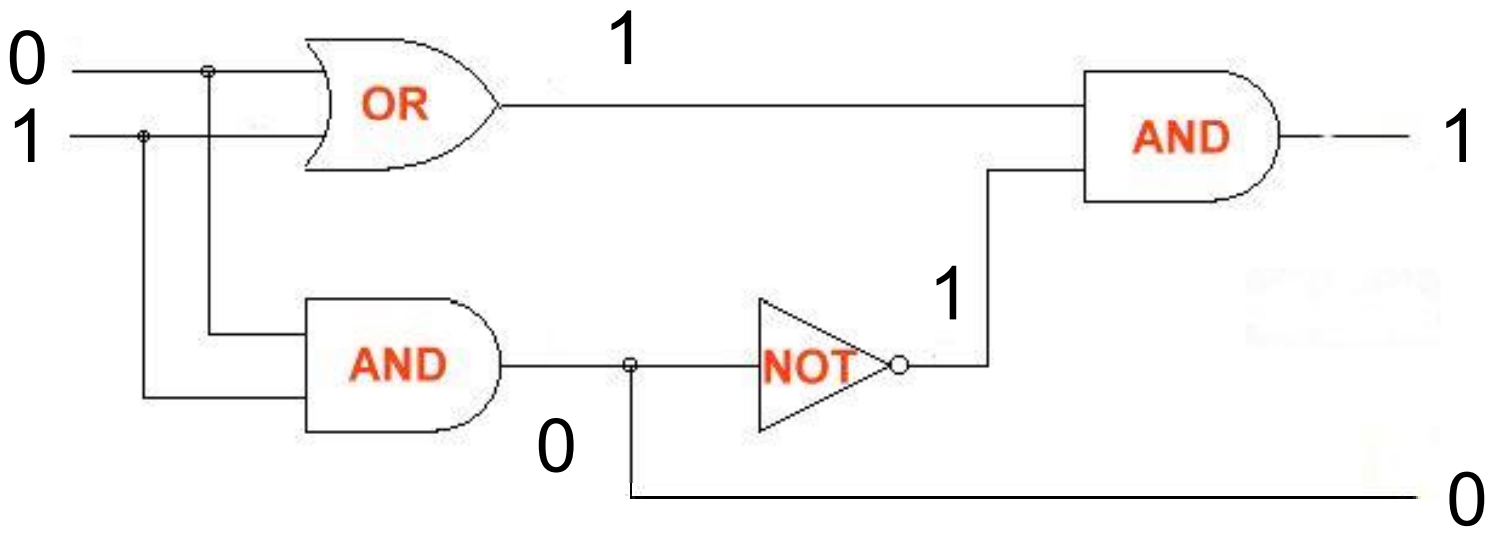


- ✓ Implementat físicament l'any 1998 per primer cop
- ✓ Des de llavors s'ha aconseguit utilitzant diferents "tecnologies" (spins, ions atrapats, …)

El dimoni està en els detalls



Comparem amb un circuit “clàssic”



Aquest canvi és profund

“ La Teoria de la Computació tradicionalment s’ha estudiat…com un tema de Matemàtiques...

…això és un error. Els ordinadors són objectes físics i les computacions processos físics…

…el que els ordinadors poden o no poden fer està sols determinat per les lleis de la Física, i no per les de les Matemàtiques”.

D. Deutsch

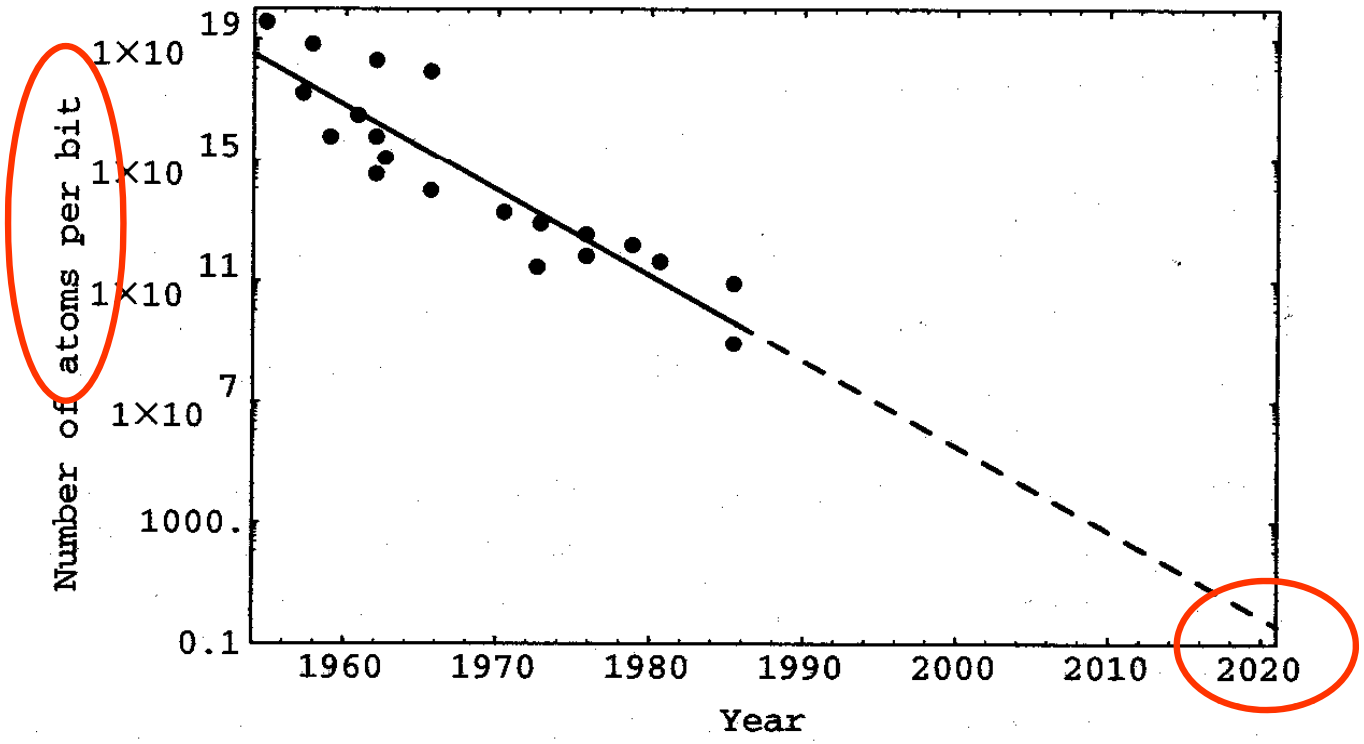
No podríem evitar-ho?

Després de tot l'algorisme de Deutsch no sembla que vagi a canviar el món!

Hi ha, com a mínim, dues raons importants per prendre-s'ho seriosament:

- El procés de miniaturització s'acaba!
- Algorismes quàntics MOLT potents

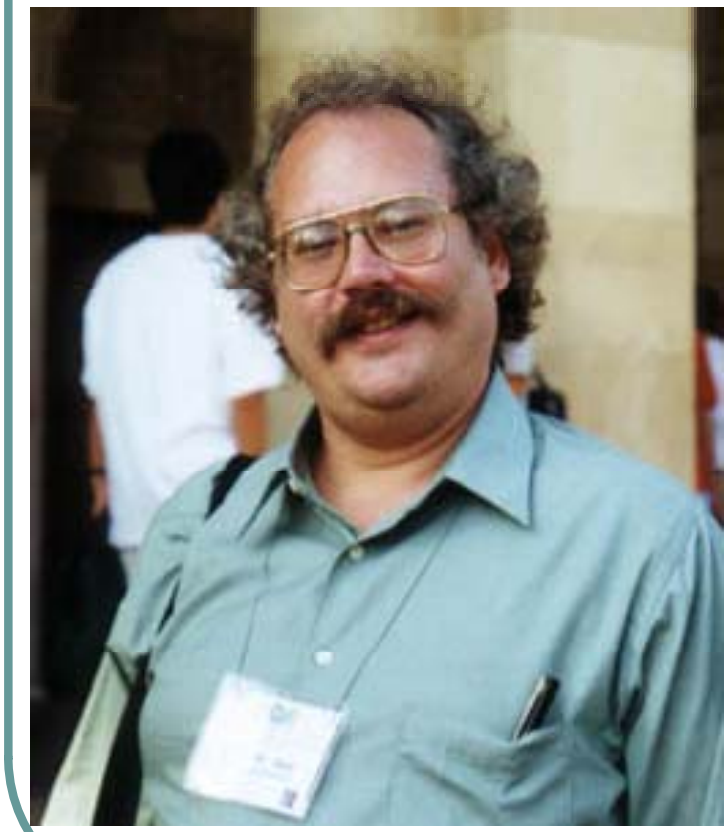
Límit: 1 àtom per bit



Quan això arribi, segurament …

- Els PC “correran” a 40 GHz
- Construir 1 planta de fabricació costarà el 5% del PIB dels USA
- I sobretot …les lleis de la Física Quàntica seran imprescindibles!

1994, any miraculós de la CQ?



- En Peter Shor va descobrir:

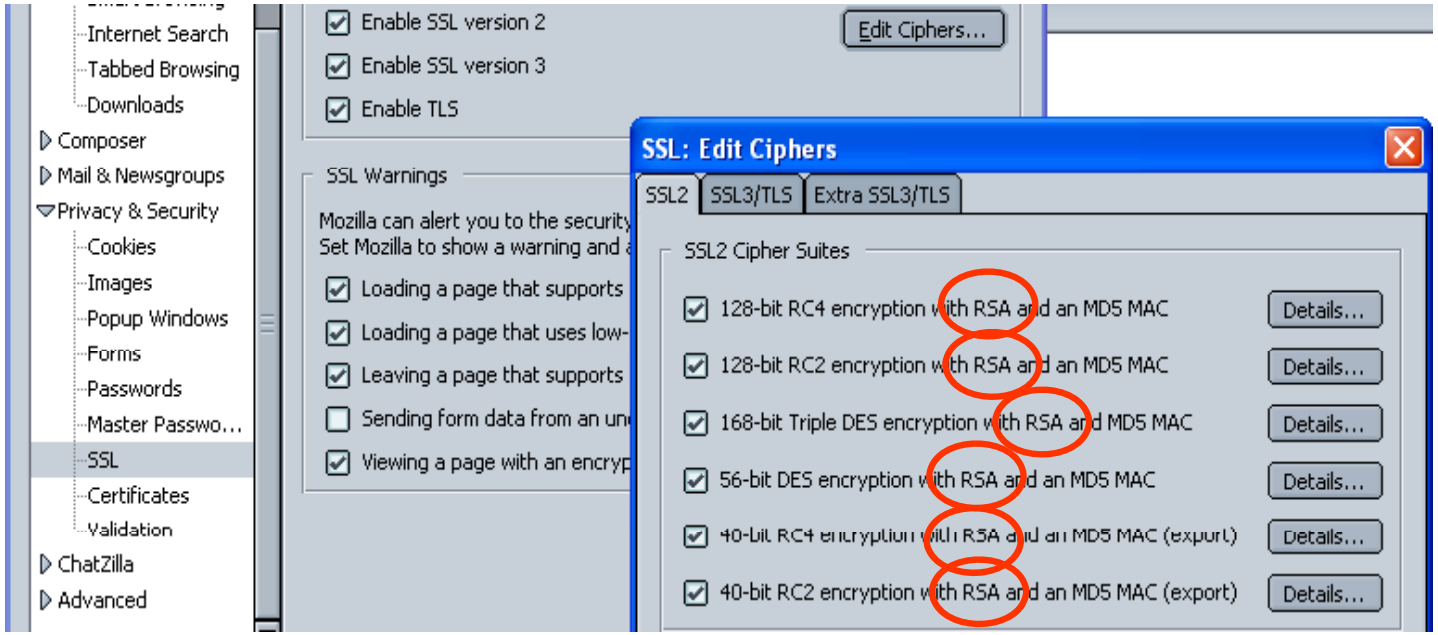
✓ Un algorisme quàntic per trencar RSA fàcilment

✓ Una manera de corregir errors en els qubits.

PREMI NEVANLINNA 1998

~ Premi Nobel de la Informàtica

RSA és per tot arreu!



La clau de volta de RSA

34905295108476509491478496199038 98133417764638493387843990820577

✖

32769132993266709549961988190834 46141317764296799294253979828853 3

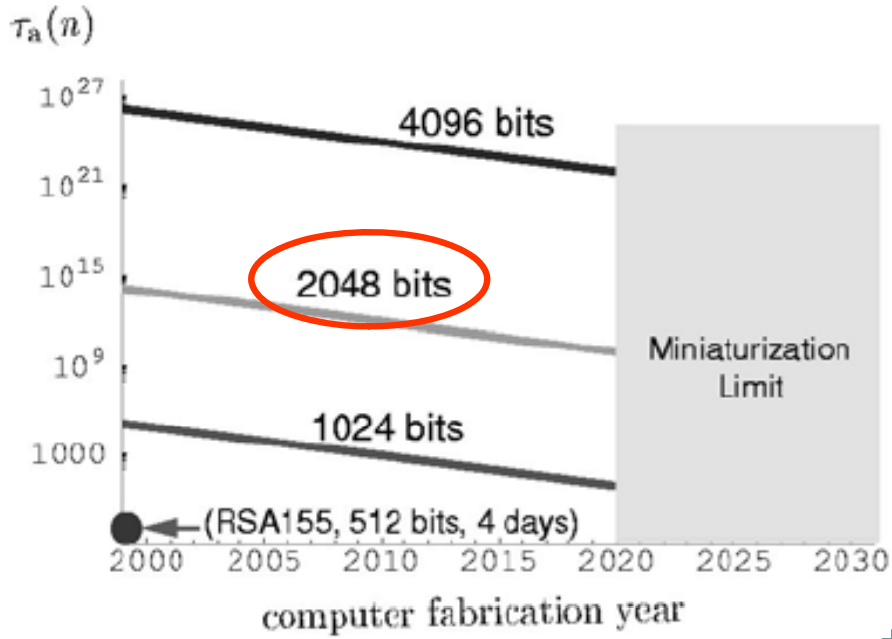
RSA-129 = 14381625757888867669235779976146612010218296721242362562561842935706935245733897830597123563958705058989075147599290026879543541

Es va aconseguir el 1994 amb una xarxa mundial d'ordinadors

Alguns ordres de magnitud

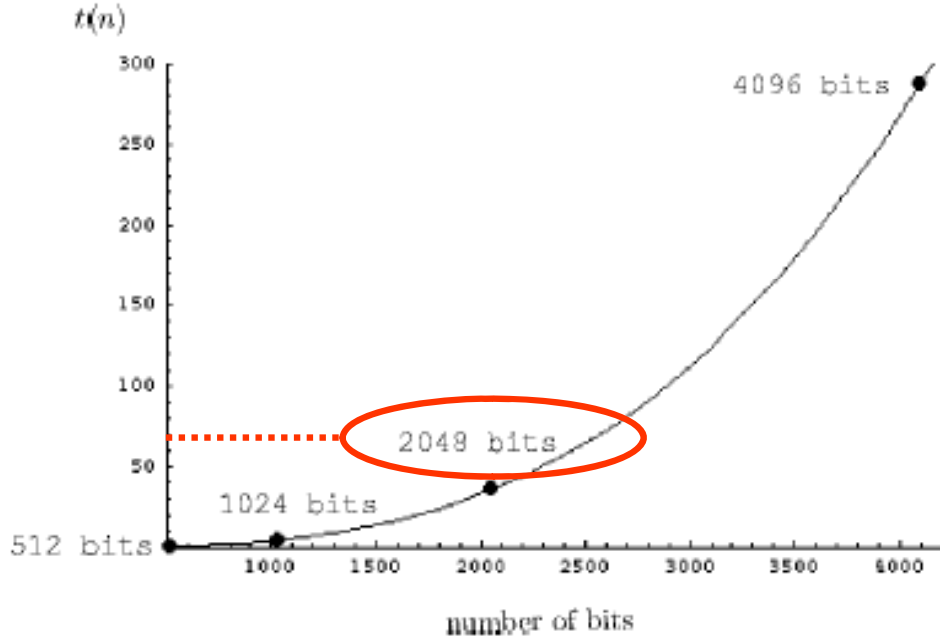
Suposem la potència combinada de 1000 PC i la validesa de la Llei de Moore (temps en anys)

Edat de l'Univers ~10^{11} anys



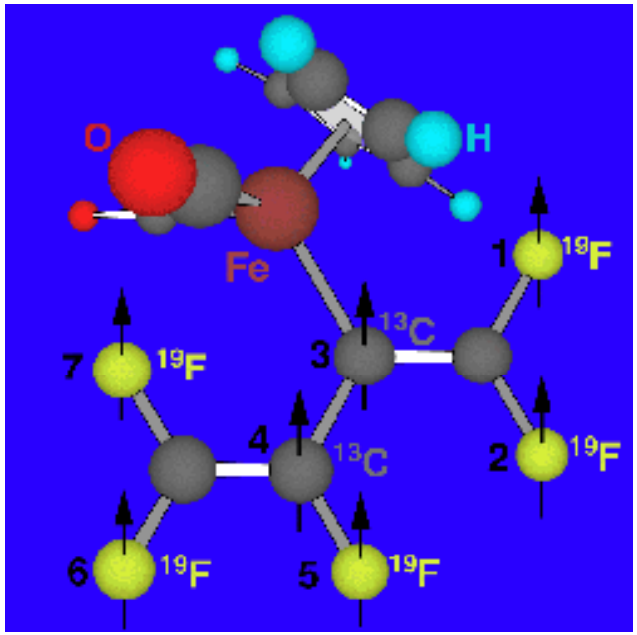
Amb l'algorisme de Shor…

Ordinador quàntic (hipotètic!) a 100 MHz
Temps en minuts!!!



El primer ordinador quàntic!

Al 2001 a IBM es va factoritzar el nombre… **15 !!!**



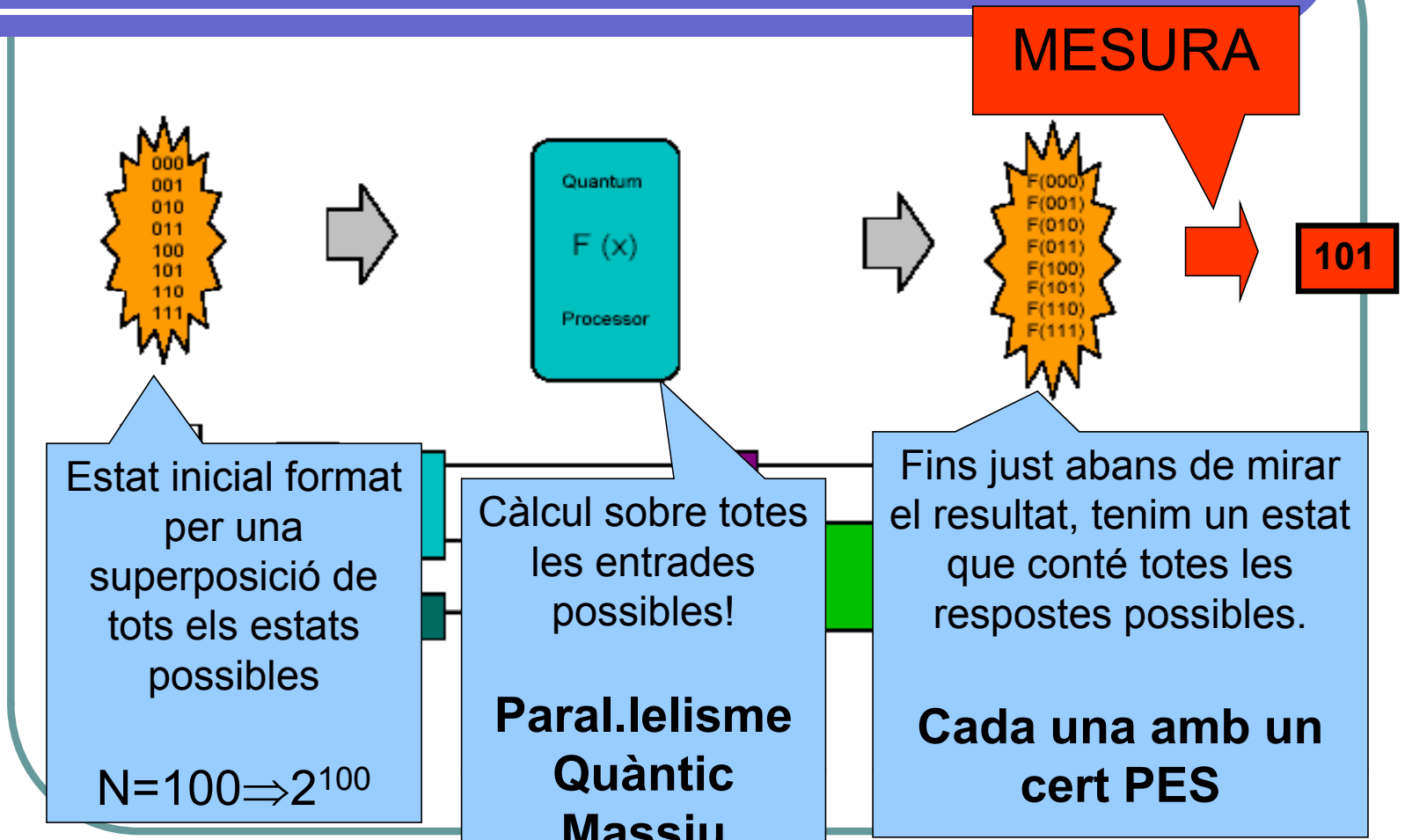
Per factoritzar un nombre de ~400 dígits caldríen ~20,000 qubits

Com funciona l'algorisme de Shor?

Avui això no toca

Teoria de Nombres + Transformada de Fourier Quàntica

Però tots són molt similars



En essència…

- El truc està en dissenyar el conjunt de portes per tal que a la sortida la mesura correspongui a una propietat col.lectiva de les solucions del problema

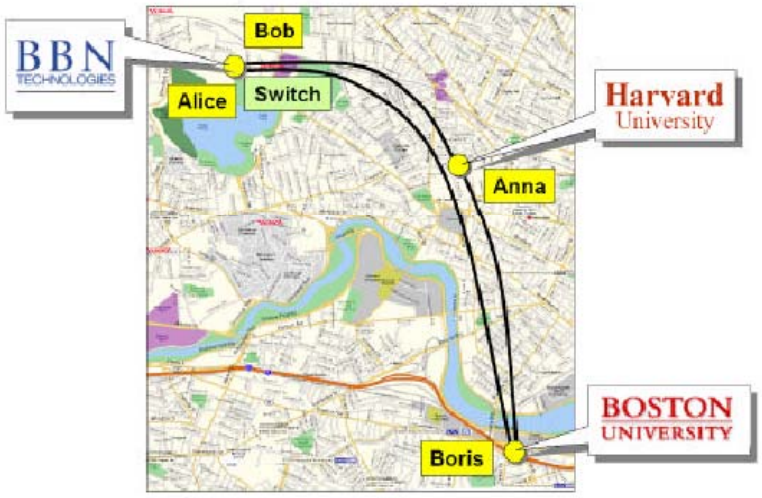
  (amb una certa probabilitat, 1 en el cas de l'algorisme de Deutsch, 0.4 en el de Shor).

- Cada problema necessita el seu circuit (situació similar a la de les calculadores).

La bena abans de la ferida

- La Mecànica Quàntica proporciona la base per Criptografia totalment segura.
- Títol de l'article amb la primera implementació (Bennet et al., 1989): *"The Dawn of a New Era for Quantum Cryptography: The Experimental Prototype Is Working!"*

Ja existexi la primera xarxa!



- DARPA Quantum Network
- Operacional al Juny del 2004
- Link per aire al Juny del 2005

BBN Technologies va ser la companyia que va montar el precursor de l'actual INTERNET a l'any 1969 (ARPANET)

…és tecnologia comercial!

Quantum Key Server

Toshiba's Quantum Key Server delivers digital keys for cryptographic applications on fibre optic based computer networks. Based on quantum cryptography it provides a failsafe method of distributing verifiably secret digital keys, with significant cost and key management advantages.

The system provides world-leading performance. In particular, it allows key distribution over standard telecom fibre links exceeding 100km in length and bit rates sufficient to generate up to 100 256-bit keys per second.

Toshiba's system uses a simple architecture, in which the photons travel from sender to receiver. This is the only design that has been rigorously proven as secure from all types of eavesdropping attack. This ensures that the Toshiba design will be secure not only today, but also in the future.

Toshiba have pioneered active stabilisation technology that allows the system to distribute key material continuously, in even the most challenging operating conditions, without any user intervention. This avoids the need for recalibration of the system due to temperature-induced changes in the fibre lengths. Initiation of the system is also managed automatically, allowing simple turn-key operation.

The system can be used for a wide range of cryptographic applications, eg encryption or authentication of sensitive documents, messages or transactions. A programming interface gives the user access to the key material.

Qubits vs. Bits (fins aquí)

AFIRMACIÓ	BITS	QUBITS
Sols pot ser 0 o 1	SI	NO
Es pot llegir sense afectar el seu valor	SI	NO

Què més?

AFIRMACIÓ	BITS	QUBITS
Llegir-ne un no afecta cap altre	SI	NO
Poden COPIAR-SE	SI	NO

Teorema de No-Clonació

Potser és possible clonar ovelles, però no ho és clonar estats quàntics

Einstein … un altre cop!

- A partir de 1933 Einstein va estar gairebé sol en la seva convicció que la Mecànica Quàntica era una versió incompleta d'una altra teoria en que els efectes quàntics es puguessin explicar en termes més objectius.

Einstein-Podolsky-Rosen (EPR)

Van fer notar que estats com aquest

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

tenen propietats aparentment paradoxals, que actualment s'anomenen

ENTRELLAÇAMENT (**ENTANGLEMENT**)

"Li estires la cua a Nova York, i el cap miola a Los Angeles" A. Einstein

Generem dos qubits en el següent estat

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

Probabilitat del 50% de que mesurem alguna d'aquestes dues configuracions

I ara els separem un de l'altre … tant com vulguem

Mesurem aquest qubit

0

Sabem que quan aquest es mesuri obtindrem també un 0

Acció a distància instantània ?

Es viola el principi relativista segons el qual cap informació pot viatjar més ràpida que la llum?

Einstein no ho pot acceptar !

Segur que la mesura de A ens assegura la mesura de B ?
O ha sigut B qui ha mesurat el seu qubit primer
i ha forçat el resultat de A ?

Com podem garantir qui ha mesurat primer ?

Telefonant !!!

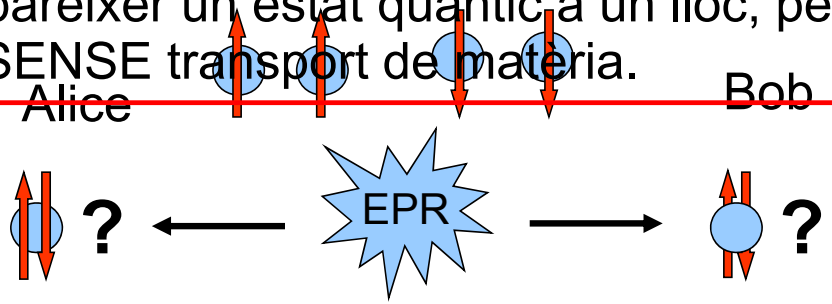
Amb un telèfon normal, amb una velocitat menor que la de la llum.

NO HI HA ACCIÓ A DISTÀNCIA !!!

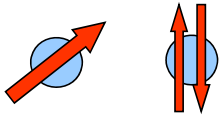
Teletransport

Els estats entrellaçats són la base del teletransport: $|0\rangle|0\rangle + |1\rangle|1\rangle$

Fer desaparèixer un estat quàntic a un lloc, per aparèixer en un altre, SENSE transport de matèria.



C  $a|0\rangle + b|1\rangle$ Qubit general, desconegut

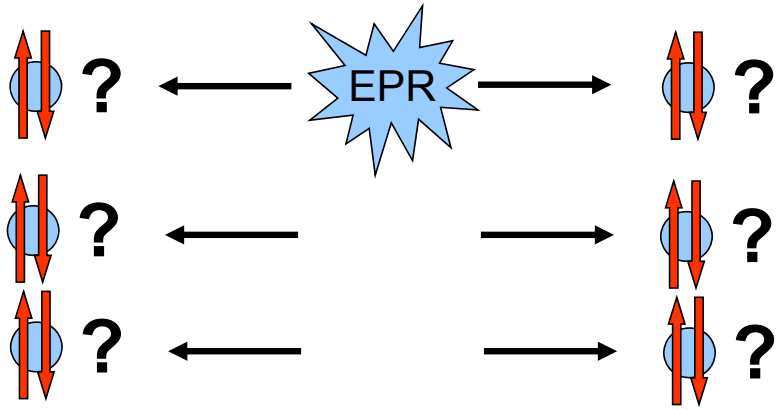
A  + mesura conjunta + resultat + trucada telefònica a B

dient a B com ha de manipular el seu qubit perquè es transformi en C

El qubit inicial C d'Alice queda modificat per la mesura (desapareix) i la manipulació de Bob fa que el seu es transformi en C (apareix) 

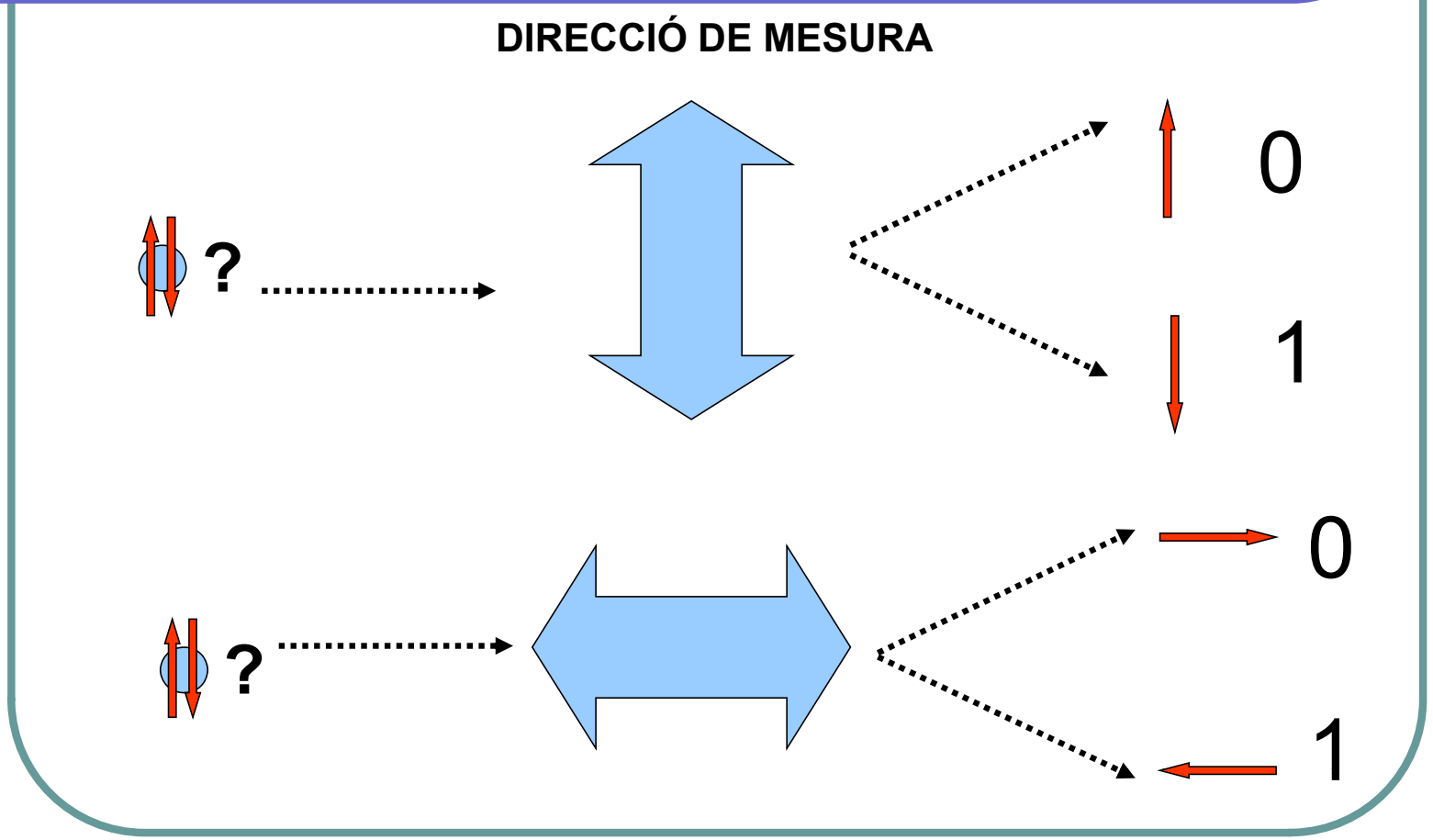
Criptografia Quàntica: Protocol d'Ekert (no és el més popular)

Tenim dues persones que es volen comunicar secretament

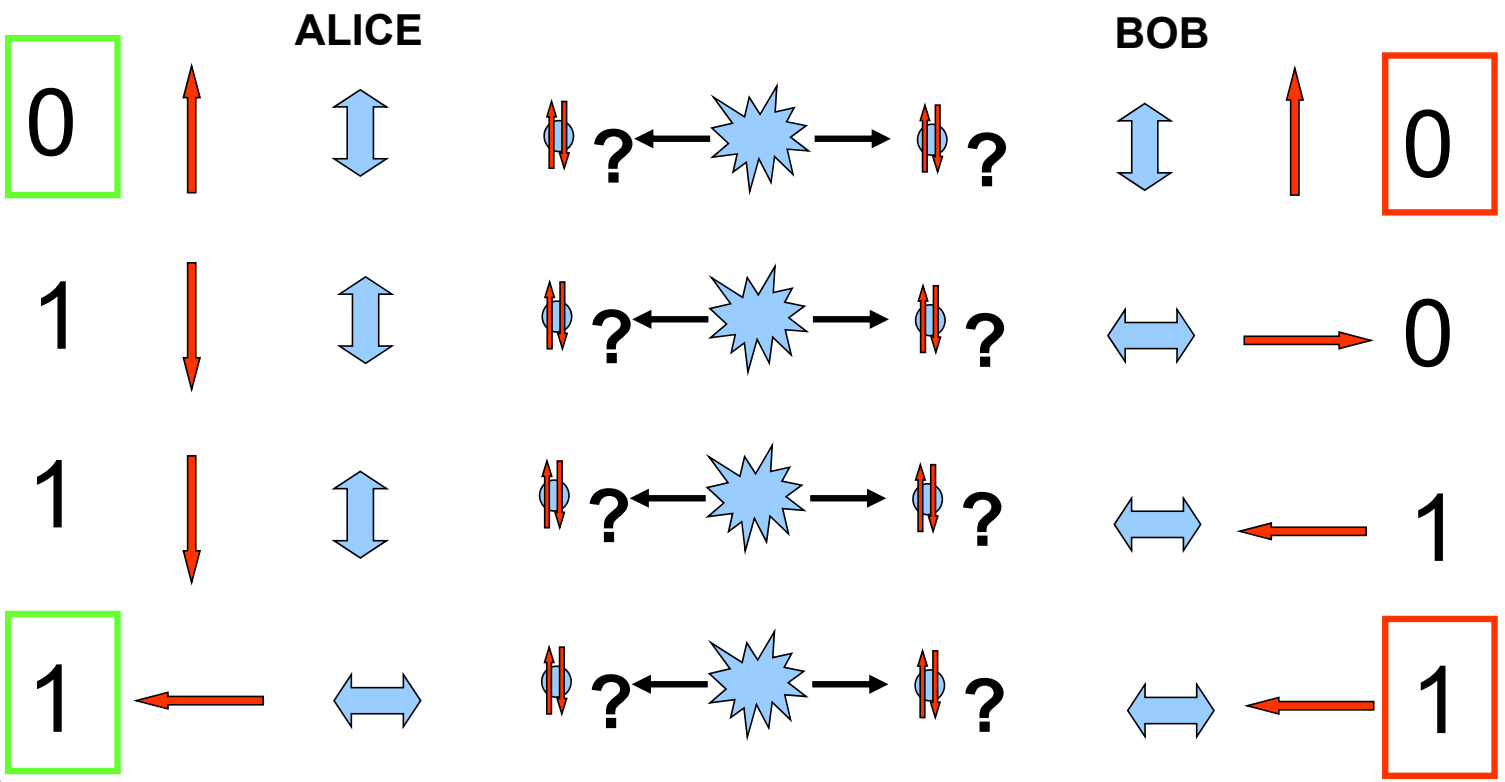


Amb aquests parells generaran una **CLAU**

Poden mesurar en dues direccions



Direccions de mesura al atzar



Anuncien les bases públicament i descarten les no coincidències

CLAU NUMÈRICA: **0 1**

Seguretat

El teorema de No cloning i el Col.lapse en la mesura asseguren que la comunicació és segura:

Eva **no plot** clonar el qubit d'Alice i renviar-lo a Bob

Si Eva mesura en la base correcta i renvia el qubit que ha mesurat, NO serà detectada
En alguns casos mesurarà en la base equivocada:
Degut al col.lapse en la mesura, el qubit que renvia
no serà el que hauria de rebre Bob.
Així, quan Alice i Bob es telefonen, trobaran inconsistències si comproven alguns dels bits que s'envien

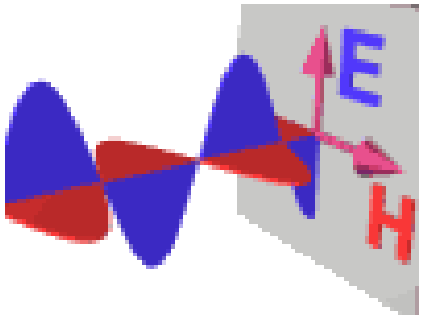
En aquest cas, Alice i Bob descarten continuar l'enviament dels qubits pel canal insegur, i busquen alternatives

Qualsevol espia (Eva) que detecti i espiï la comunicació entre Alice i Bob serà detectada !

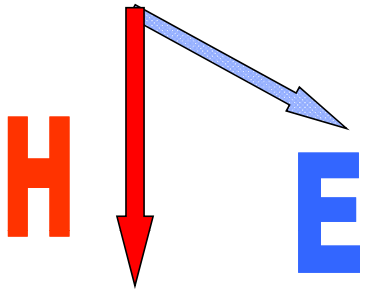
I per acabar … fotons!

Quina mena de qubits s'intercanvien? **FOTONS**

Com es codifiquen el $|0\rangle$ i $|1\rangle$? **POLARITZACIÓ DEL FOTÓ**



$|0\rangle$



$|1\rangle$

CONCLUSIONS

- La FQ ens descriu matemàticament el microcosmos amb una gran precisió
- Ens trobem amb dificultats per entendre-la (a partir dels nostres prejudicis macroscòpics)
- Avui: Àtom, Molècules, Química, Làser, Astrofísica, Nanotecnologia…
- Demà: Les “paradoxes” de la Mecànica Quàntica permeten fer càlculs i transmissió d’informació de formes que fins ara no s’havien imaginat:

  Computació Quàntica, Criptografia Quàntica, Teleportació,...
- Encara no tenim ordinadors quàntics, potser vosaltres podreu contribuir-hi!

I així, el millor títol quin era?

Què ens diu i què no ens diu la FQ

{1/√2 (Què ens diu) + 1/√2 (què no ens diu)} la FQ

I, quan hem fet la “mesura”, l’estat ha col.lapsat donant

Què ens diu la FQ

Si teniu més interès …

- wikipedia.org
- qubit.org
- *“Ultimate Zero and One”,* Williams & Clearwater

- Agraïments:
- Rossend Rey, Núria Ferrer
- I a tots vosaltres per la vostra assistència