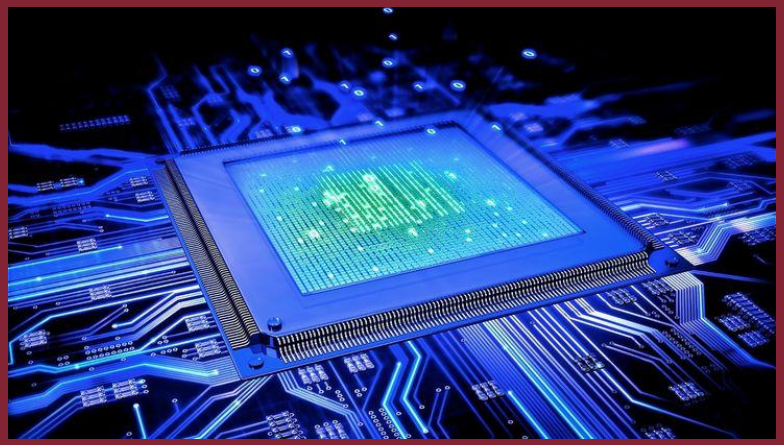
Superare le tecnologie attuali: teletrasporto, crittografia e computazione quantistica

Eugenio Del Re
Dipartimento di Fisica, Università di Roma «La Sapienza»
eugenio.delre@uniroma1.it

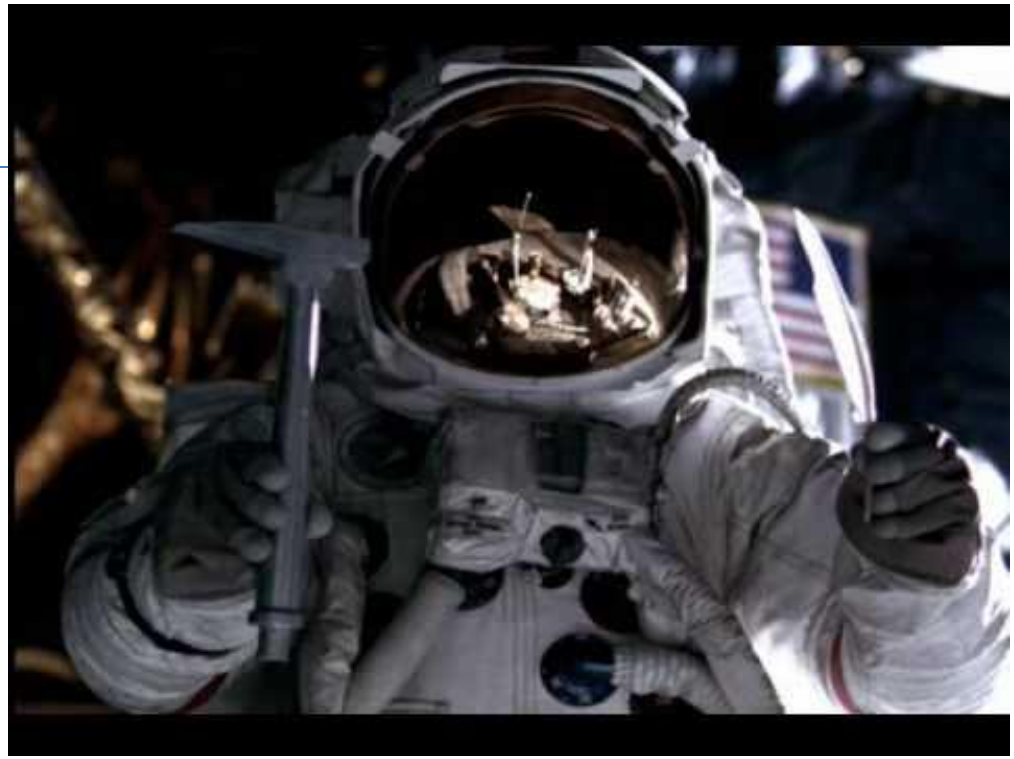


Roma – 27 Gennaio 2017 – Aula Amaldi

Metodo Scientifico

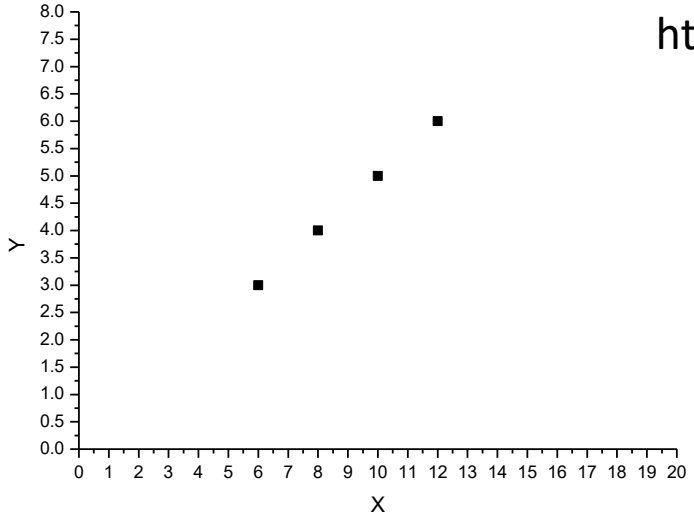
Esperimento & Induzione

Moto universale



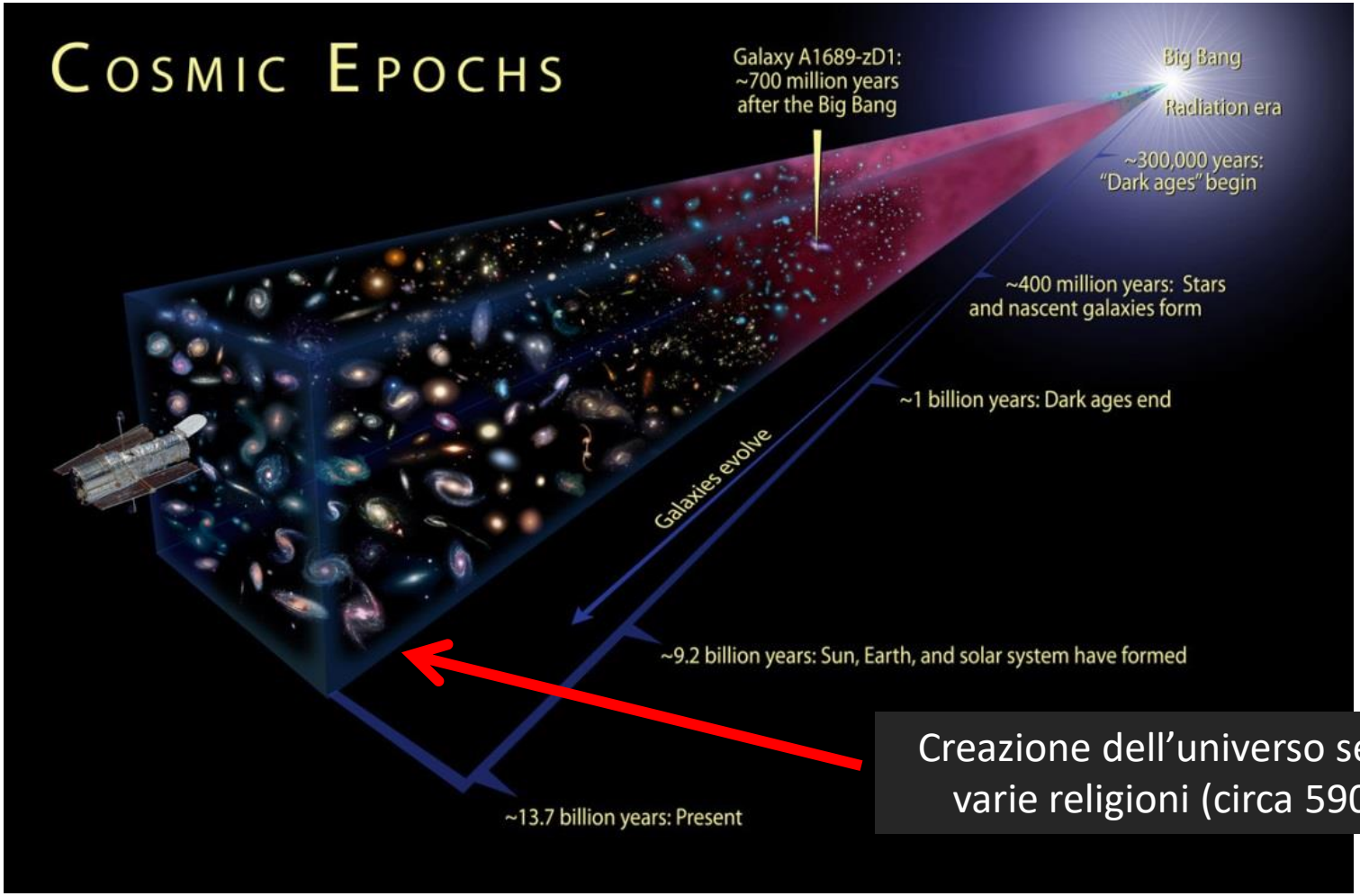
Galileo was right!
https://youtu.be/XtvESpQipcw

x	6	8	10	12	14
y	3	4	5	6	?



Metodo Scientifico

Deduzioni «scientifiche» e «big bang»



Creazione dell'universo secondo varie religioni (circa 5900 fa)

L’atomo: una grande deduzione sbagliata

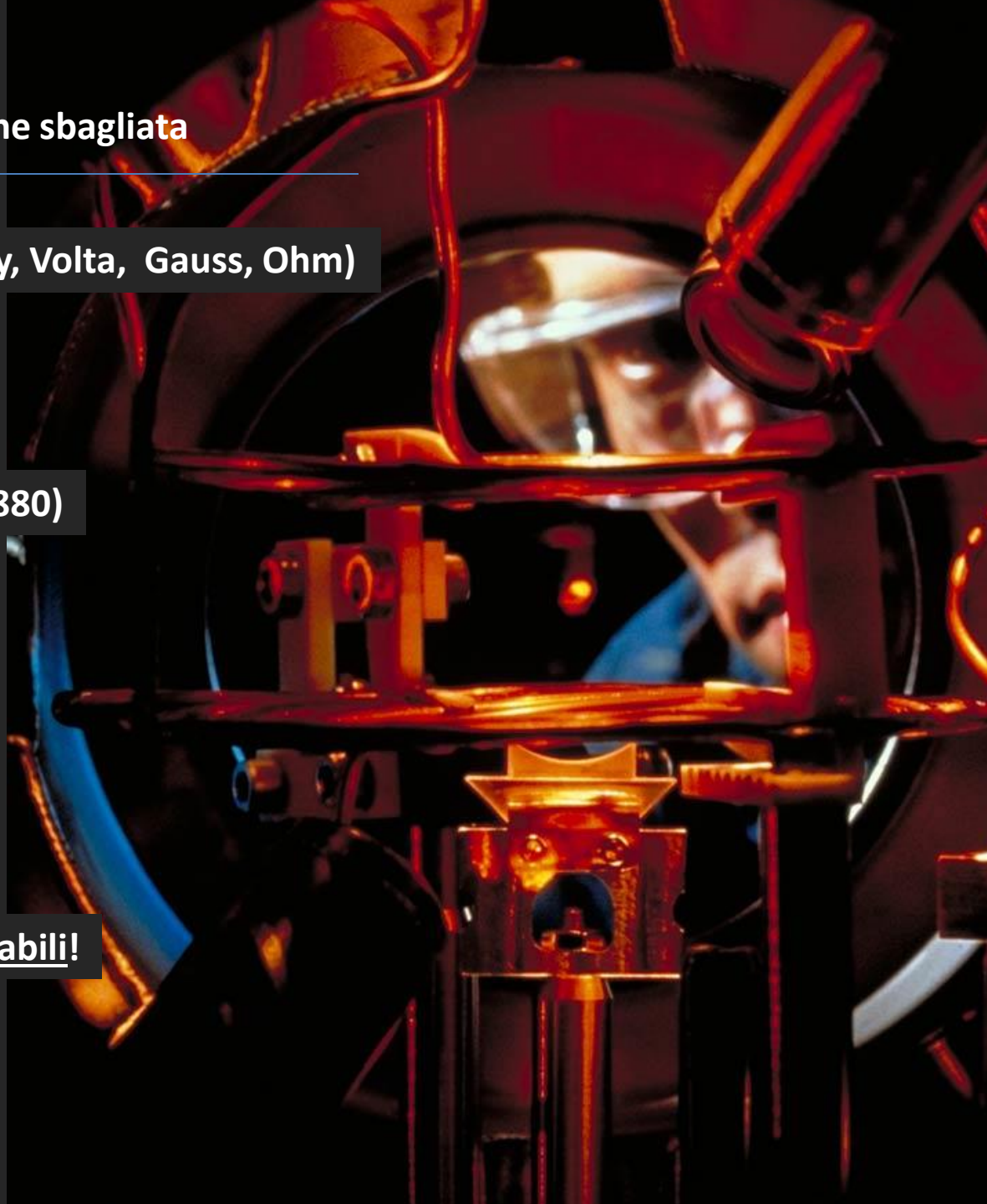
Esperimenti (Galvani, Faraday, Volta, Gauss, Ohm)

Induzione

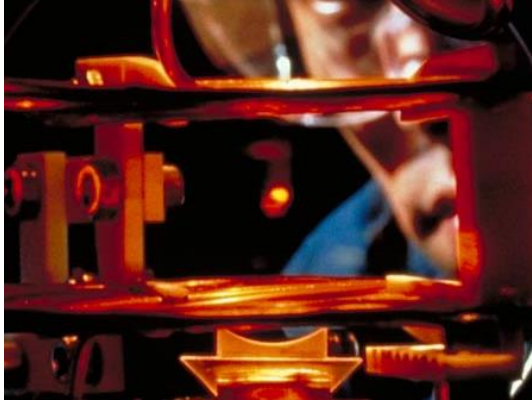
Elettrogmagnetismo (Maxwell - 1880)

Deduzione

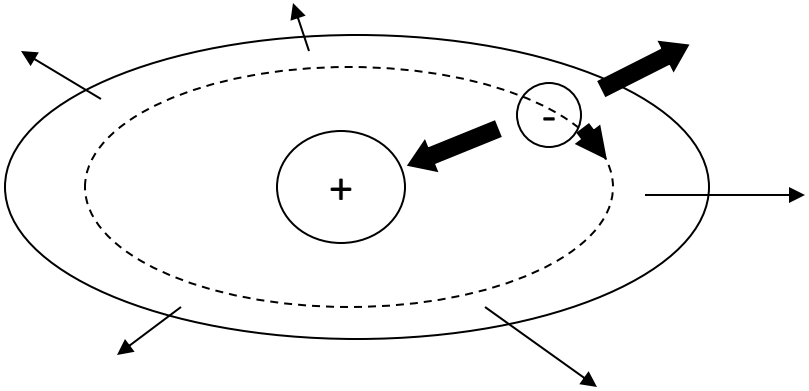
Gli atomi devono essere instabili!



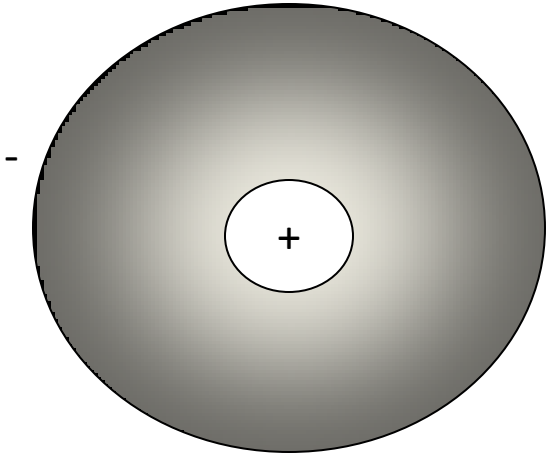
L’atomo: una nuova visione

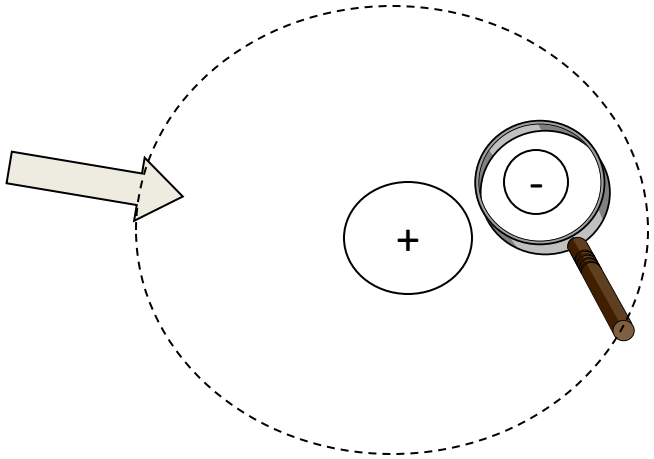


1. Elettroni **negativi** gravitano attorno ad un nucleo **positivo**
2. Per **non cadere** sul nucleo devono avere un **moto** la cui componente centrifuga bilanci l’attrazione elettrica
3. Ma **cariche in moto accelerato emettono** onde elettromagnetiche, e l’atomo dovrebbe rapidamente decadere.



4. Ma **l’atomo è stabile.**
5. Quindi l’atomo **non è fermo e non è in moto**, è *delocalizzato* attorno al nucleo (natura ondulatoria).
6. Ma l’elettrone è sempre **ben localizzato ed indivisibile**.
7. Quando lo osservi, **collassa** in un punto secondo una data distribuzione di probabilità e si localizza (natura corpuscolare).



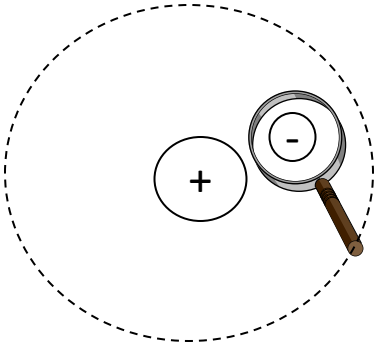


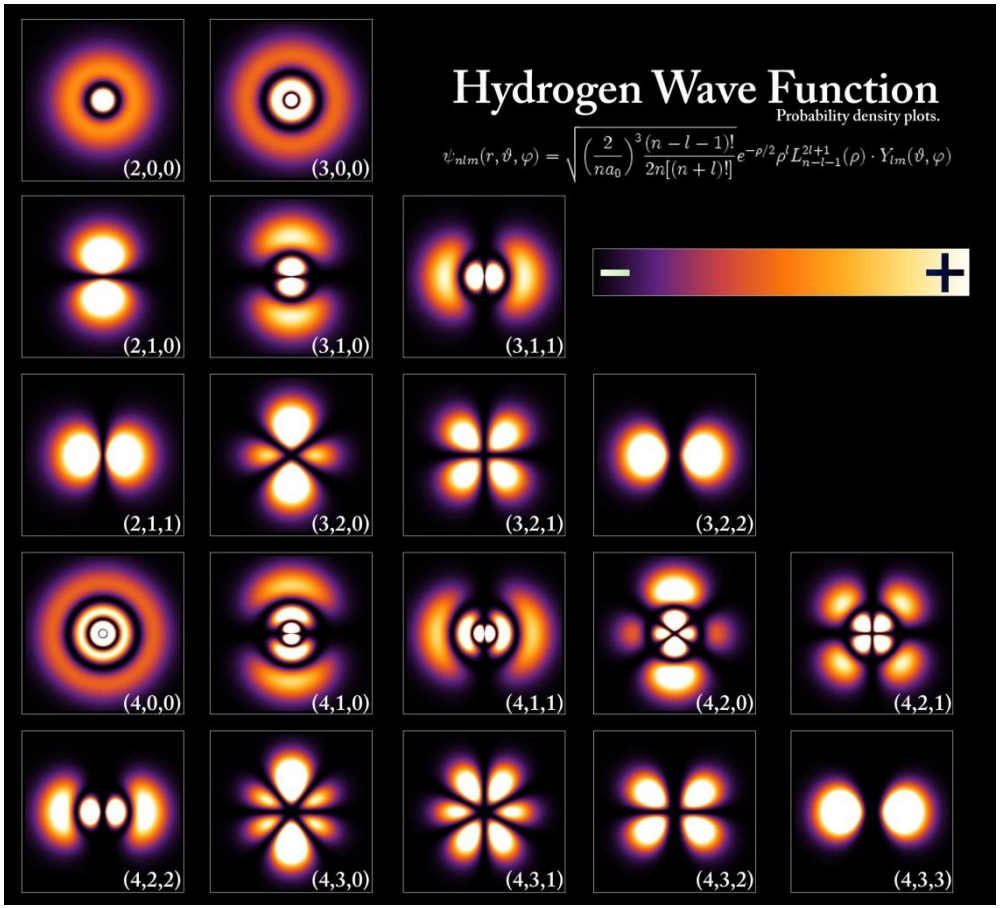
Principio di Indeterminazione

Complementarità onda-particella

Alice nel mondo delle meraviglie…

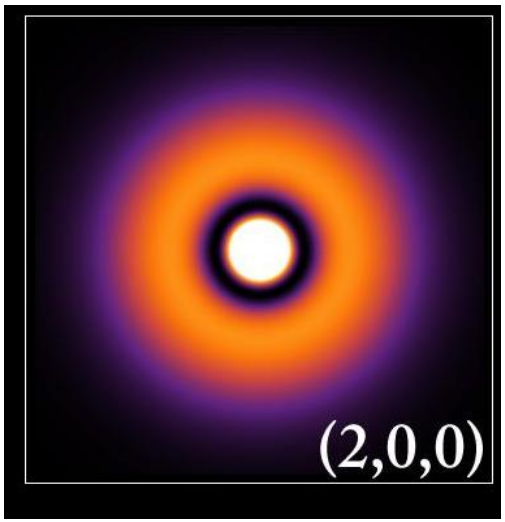
Distribuzioni di probabilità del collasso dell'elettrone nell'atomo di Idrogeno





L'elettrone in "orbita" attorno al nucleo **non segue una traiettoria** formata da una sequenza temporale di posizioni e velocità, ma risulta "fermo" in uno **stato delocalizzato di sovrapposizione di posizioni e velocità** (stato di sovrapposizione microscopica).

Atomo: un **mattoncino** fatto di **indeterminazione**



Δp

(natura ondulatoria)

Indeterminazione nell'impulso ($\boldsymbol{p}=m\boldsymbol{v}$)

Δx

(natura corpuscolare)

Indeterminazione spaziale

$$\Delta x \cdot \Delta p \approx \frac{h}{4\pi}$$

Dualità particella-onda

In generale…

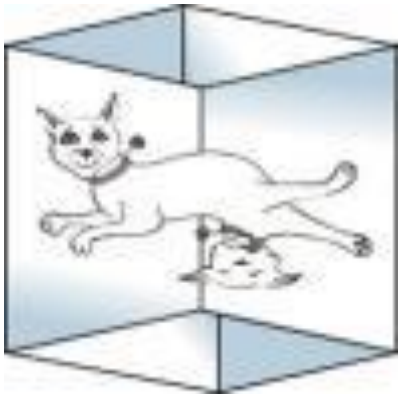
$$\Delta x \cdot \Delta p \geq \frac{h}{4\pi}$$

$$\Delta E \cdot \Delta t \geq \frac{h}{4\pi}$$

Heisenberg (1927)

Braccio operativo della M.Q.: **Principio di Indeterminazione di Heisenberg**

Nulla che si possa disegnare può essere in uno stato di sovrapposizione…

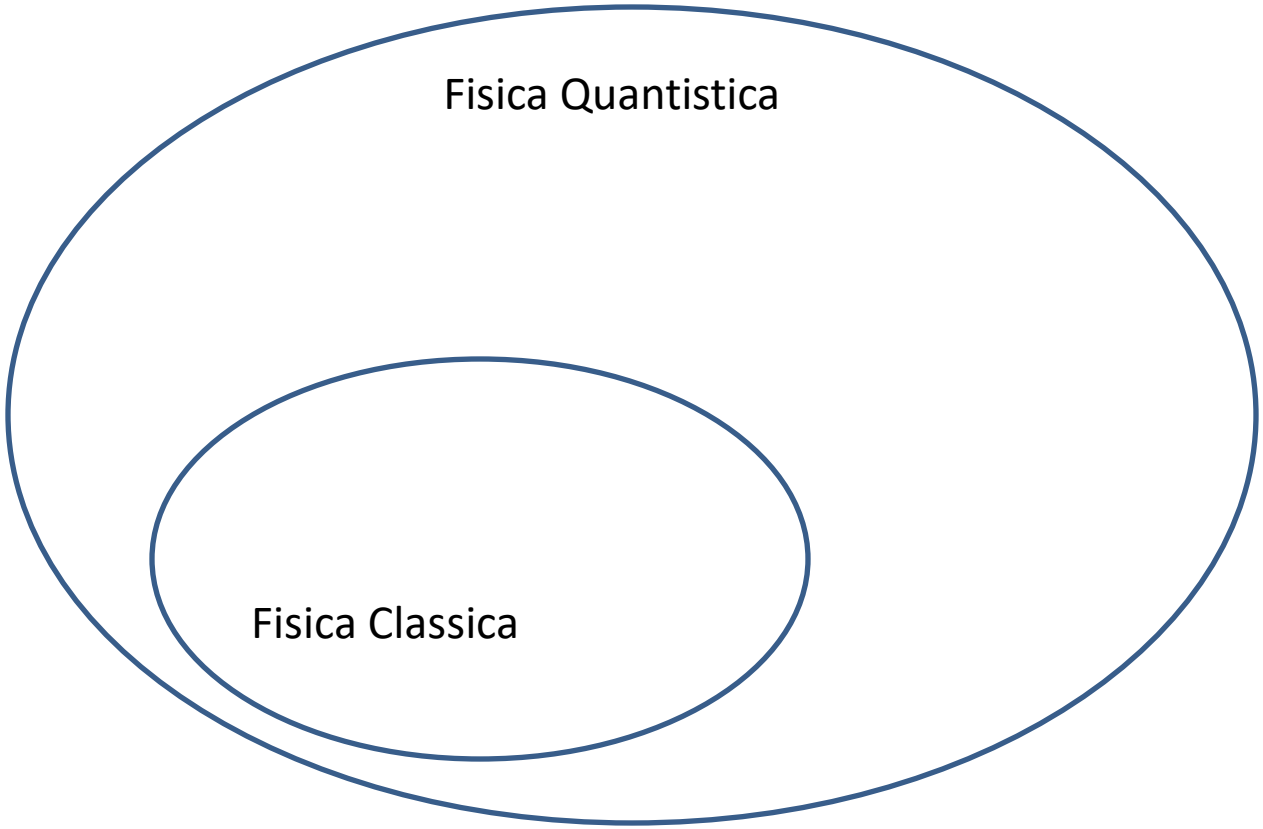


Sovrapposizione

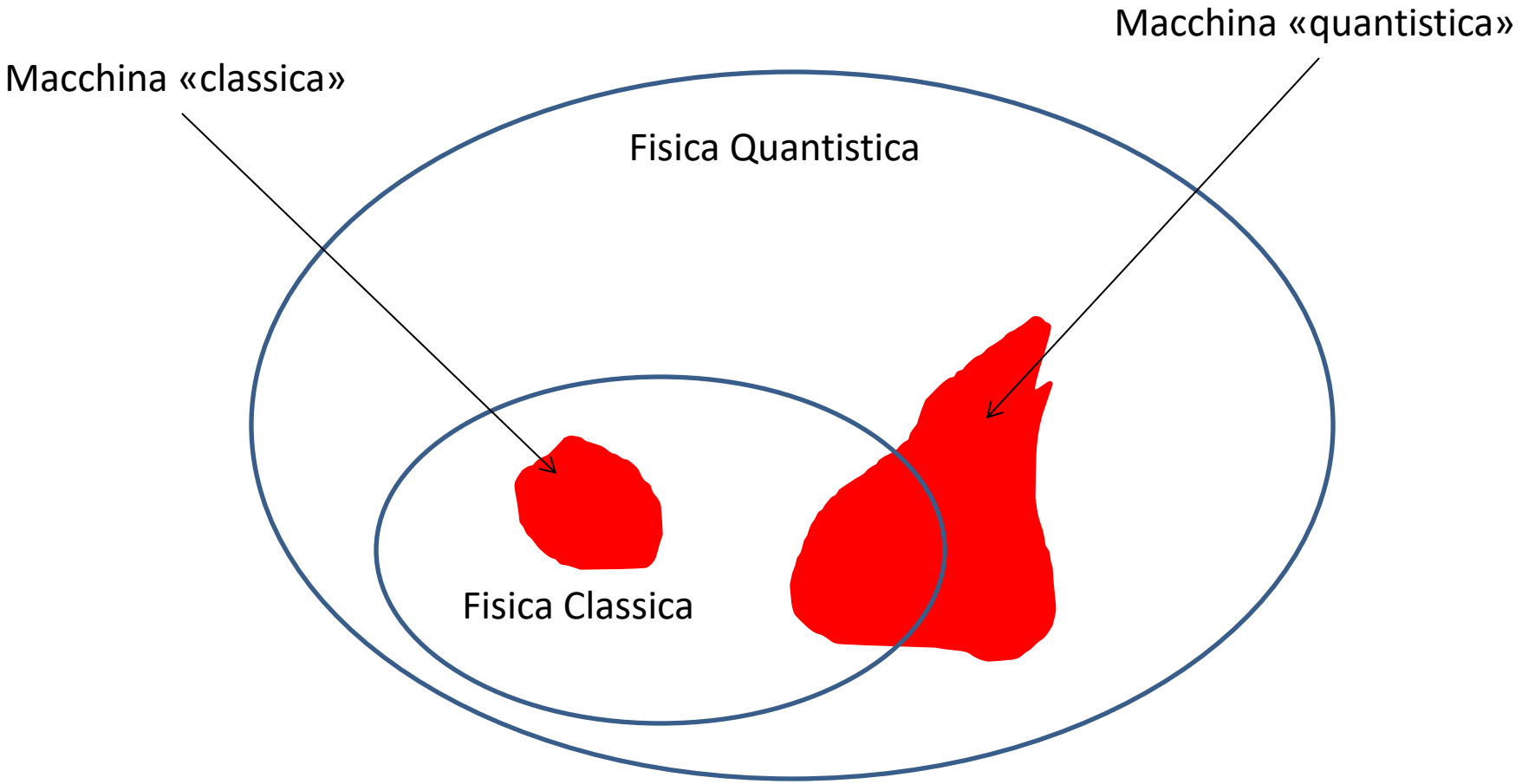
Collasso

neanche

La meccanica quantistica comprende la fisica classica



«Tecnologia quantistica vs tecnologia classica»



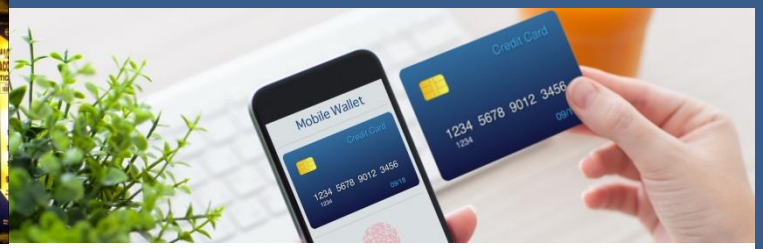
Le macchine quantistiche sono diverse, in certi casi migliori delle macchine classiche.

Possono fare cose che non possono essere fatte dalle macchine «classiche»

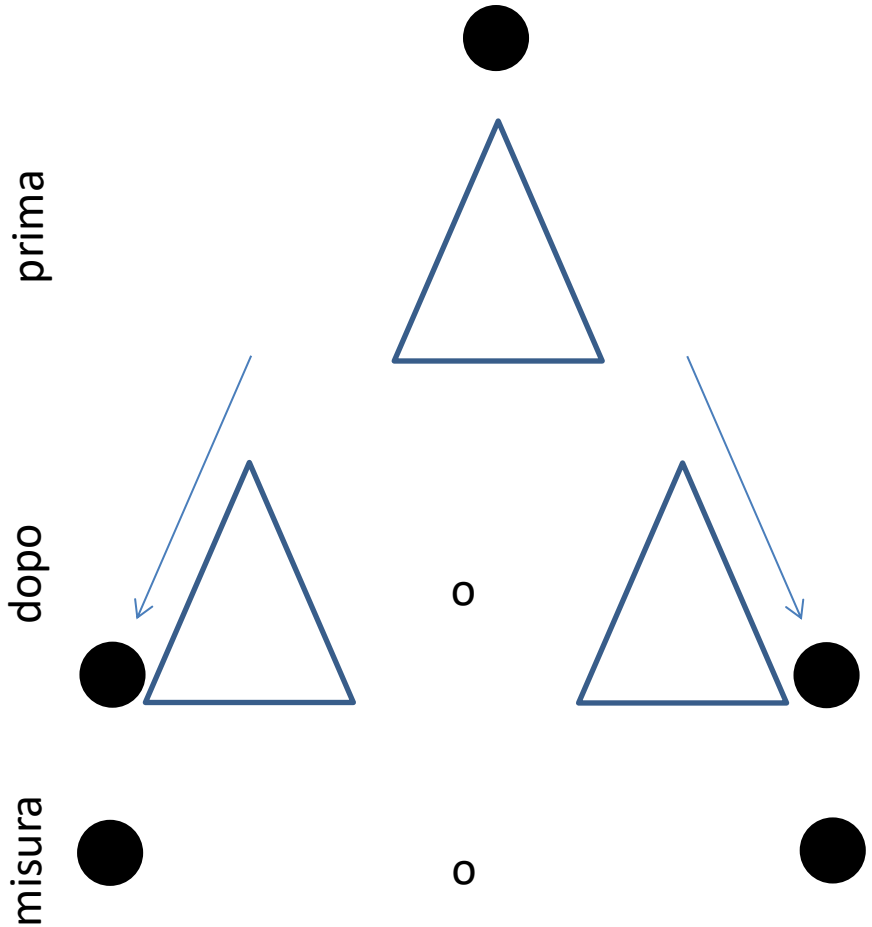
Esempi di tecnologia quantistica

Tecniche classiche	Tecniche quantistiche
Generatori di numeri pseudorandom	Generatori di numeri random
Computer classici	Computer quantistici
Fax	Teletrasporto
Crittografia classica	Crittografia quantistica

Generatore di numeri random

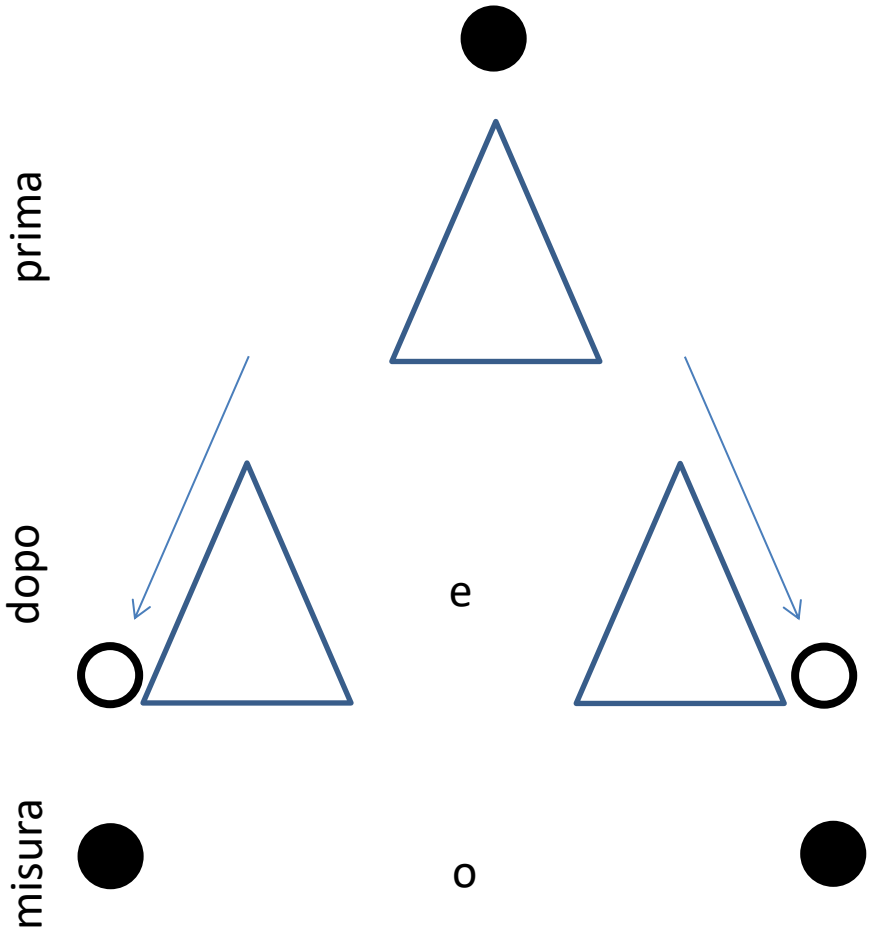


Fisica classica



evento pseudorandom

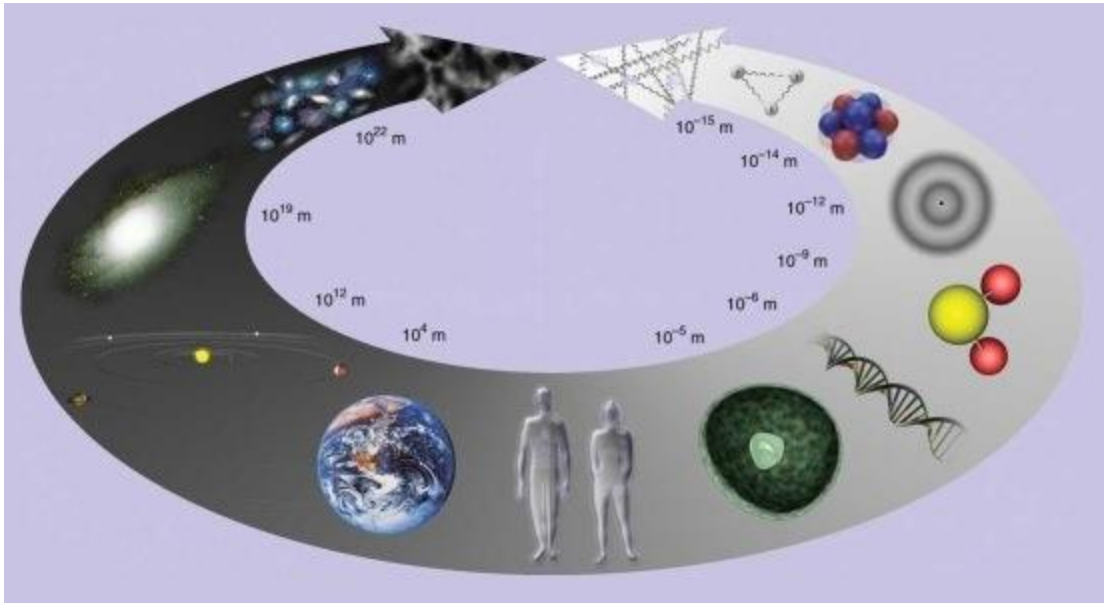
Fisica quantistica



evento random vero

Riproducibilità e dettaglio ultimo

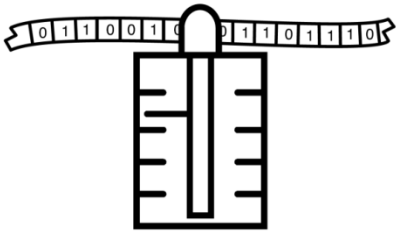
«La Natura non si ripete mai»... (Eraclito, Parmenide, Zenone, Platone, Leibniz ...)



Dovrebbe essere possibile andare nel dettaglio ultimo e arrivare a fenomeni non descrivibili con il metodo scientifico...

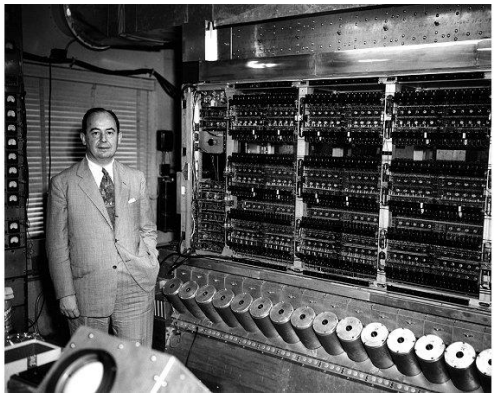
...apparentemente c'è la fisica quantistica!

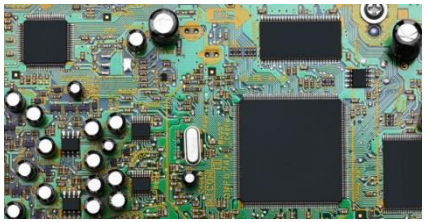
Computer



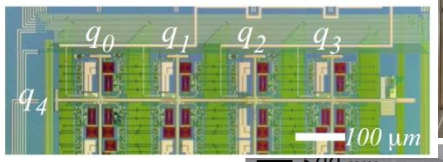
Macchine di Turing

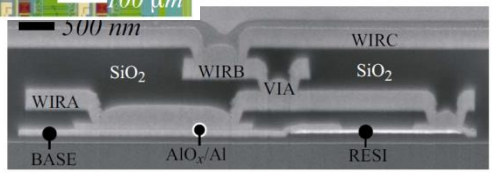
Fisica classica





Fisica quantistica





bit 0
1

qubit |0>
|1>

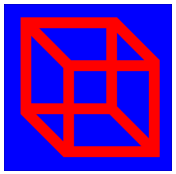
$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

o calcoli 3+2=5
o calcoli 3-2=1

parallelismo calssico

più macchine fanno cose in parallelo

calcoli 3+2=5
e calcoli 3-2=1



parallelismo quantistico

una sola macchina esegue più operazioni allo stesso tempo

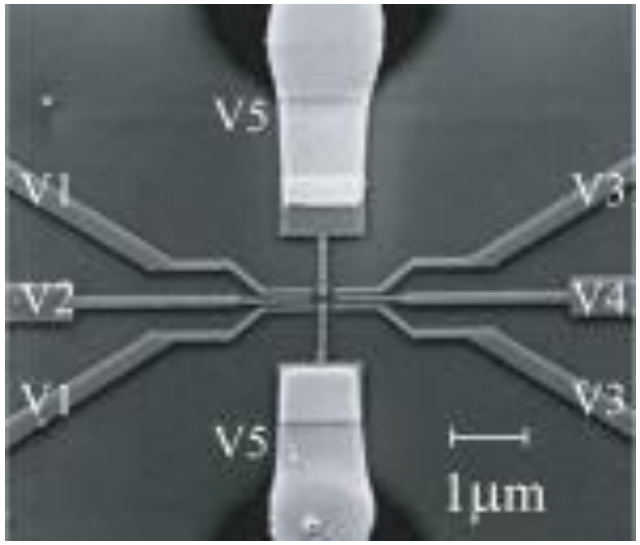
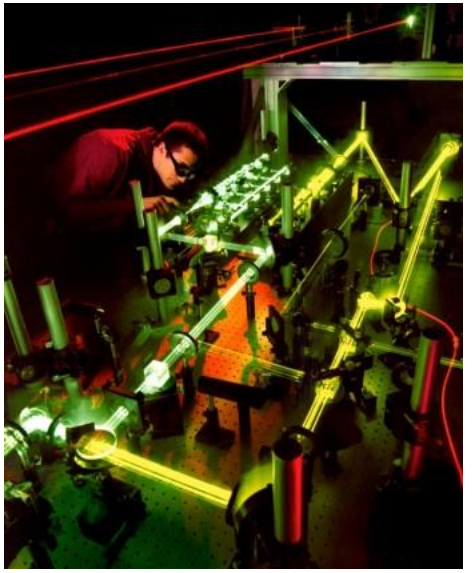


Immagine di una macchina quantistica elettronica (CNOT)

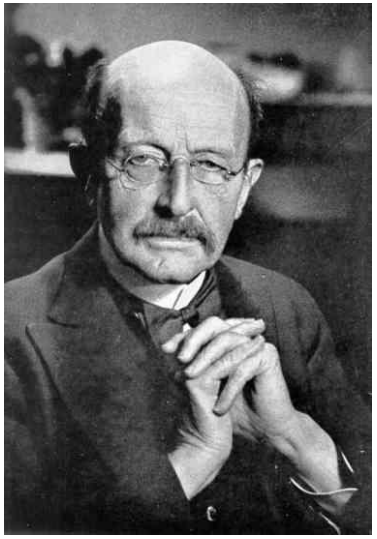


Teletrasportatore fotonico

Einstein vs Bohr & Tecnologia Quantistica

14 Dicembre, 1900

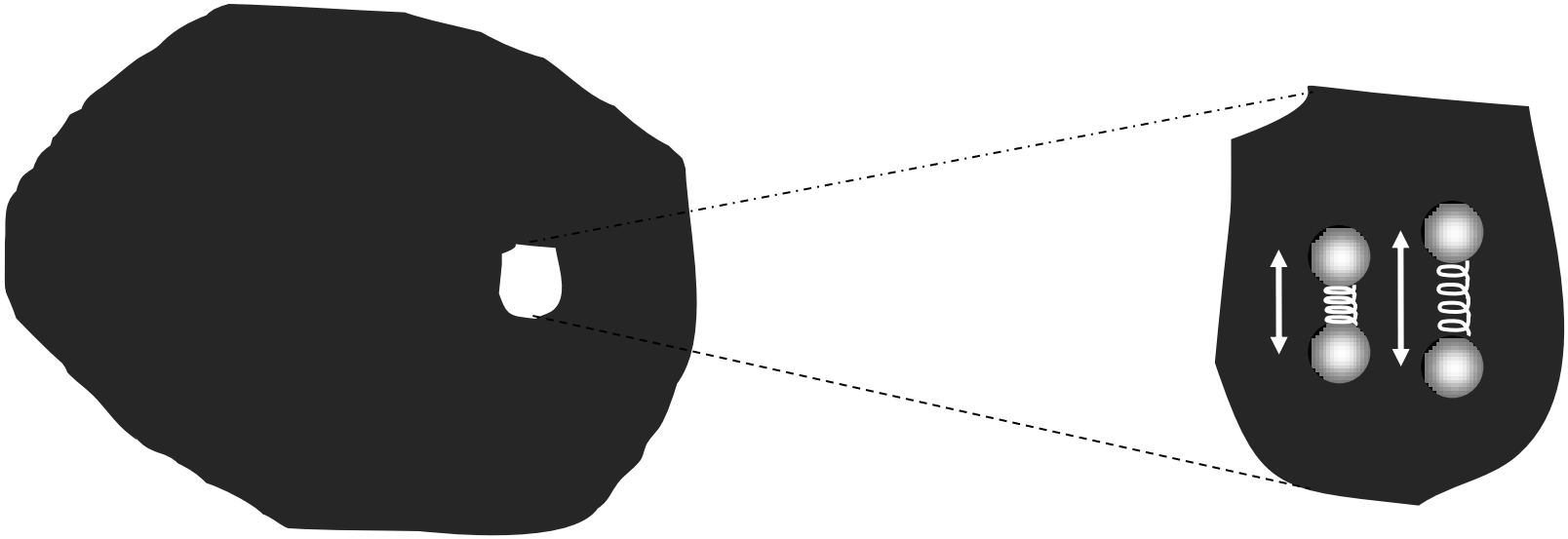
Max Planck



Quantizzazione dell'energia a **livello microscopico** (atomico) per interpretare la radiazione di **Corpo Nero.**

la nascita della Meccanica Quantistica

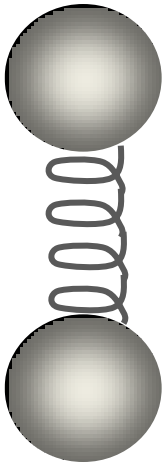
La Quantizzazione

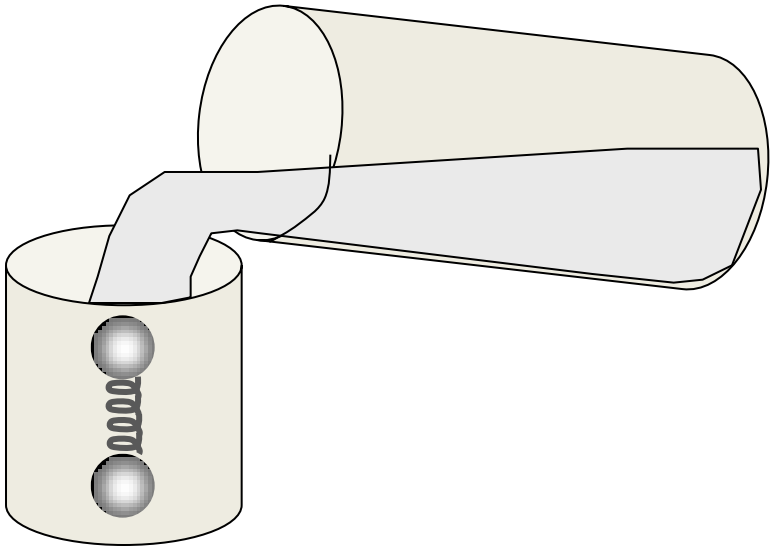


Un **corpo macroscopico** è costituito di **elementi microscopici** simili a degli **oscillatori** (sistema molla + corpo)

La Quantizzazione

Macroscopico

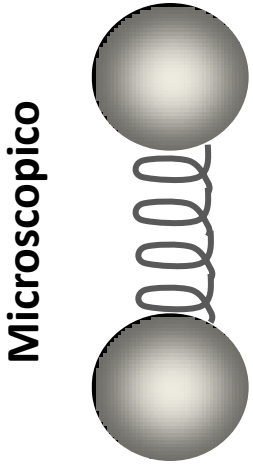


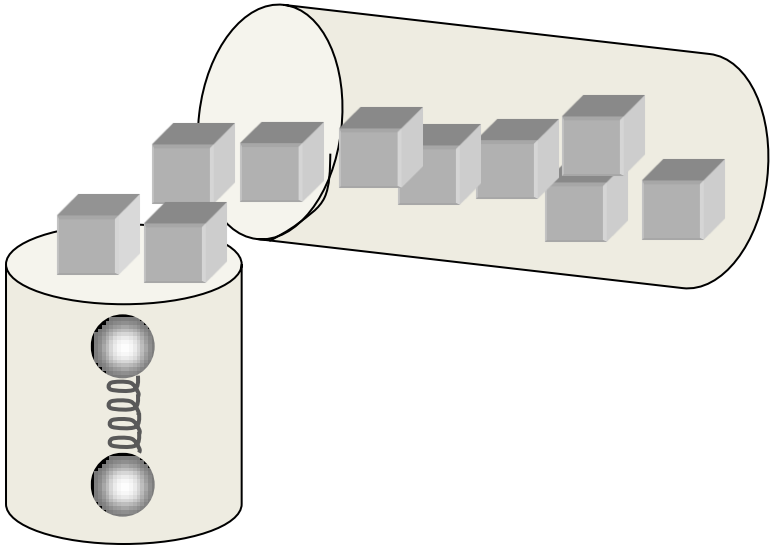


Un **oscillatore macroscopico** può **scambiare** energia in maniera **continua** (come un “fluido”).

La Quantizzazione

Microscopico





Un **oscillatore microscopico** può **scambiare** energia a **pacchetti** o **quanti**.

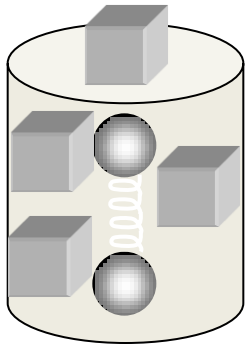
La Quantizzazione

Numero intero

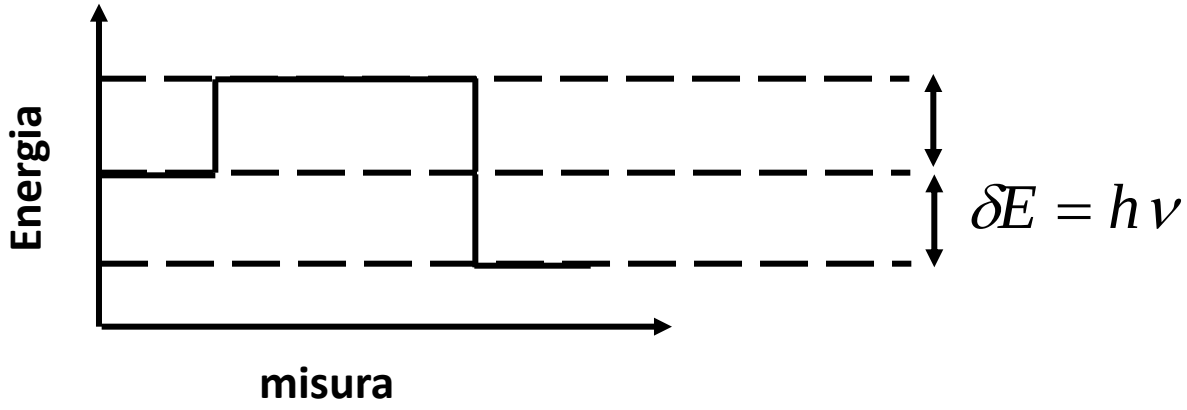
Frequenza di oscillazione

$$E = n \times h\nu$$

Costante di Planck

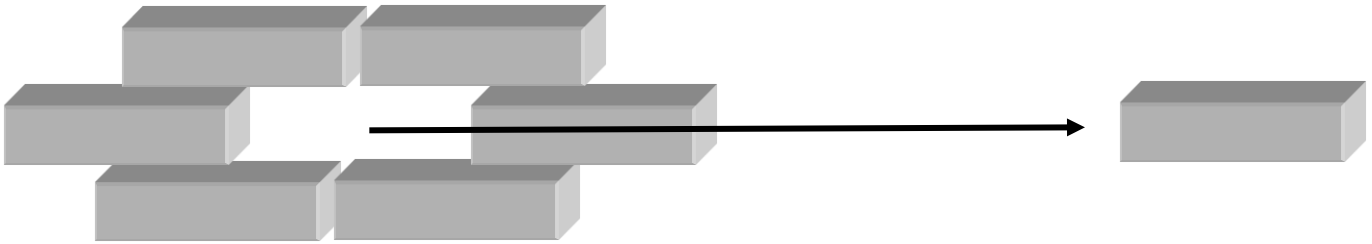


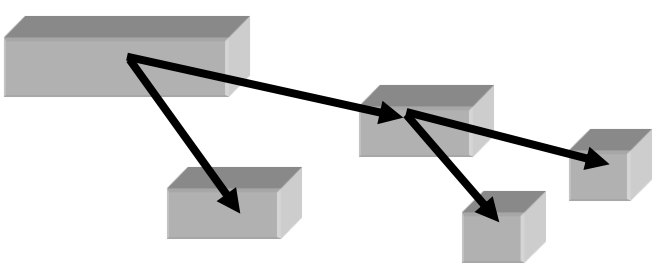
$$\delta E = h\nu$$

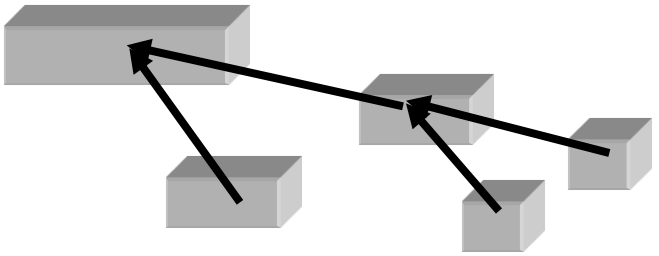


L'energia del sistema microscopico è un **multiplo intero** del **quanto** elementare.

La Quantizzazione “Classica”

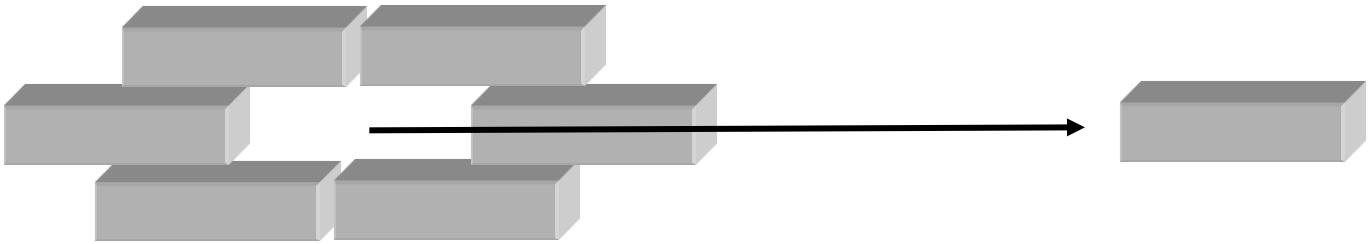


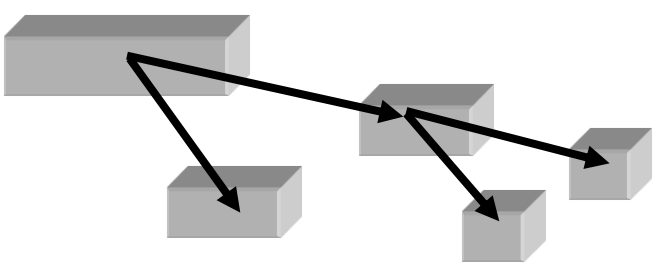


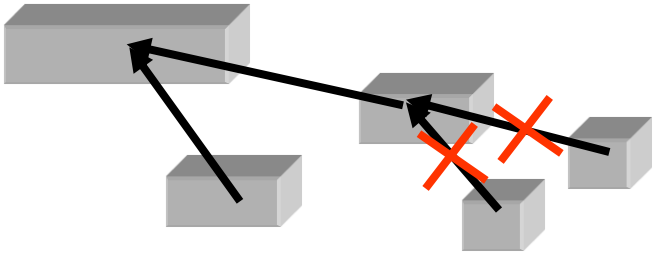


Un sistema macroscopico può avere una struttura “quantizzata”, ma essa è solo uno **schema convenzionale**. In realtà, il mattone può essere **suddiviso** a piacere e ricombinato per riavere il sistema originale.

La Quantizzazione microscopica



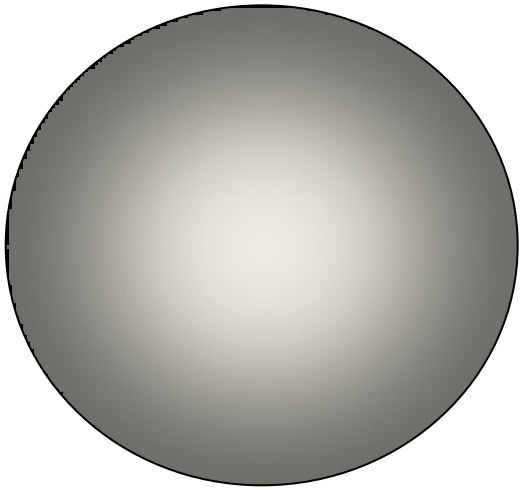




Un sistema **microscopico** non può essere ulteriormente scomposto oltre la sua struttura quantica **senza modificare irreversibilmente** le sue caratteristiche.

Atomo: un **mattoncino** fatto di **indeterminazione**

Bohr (1913)

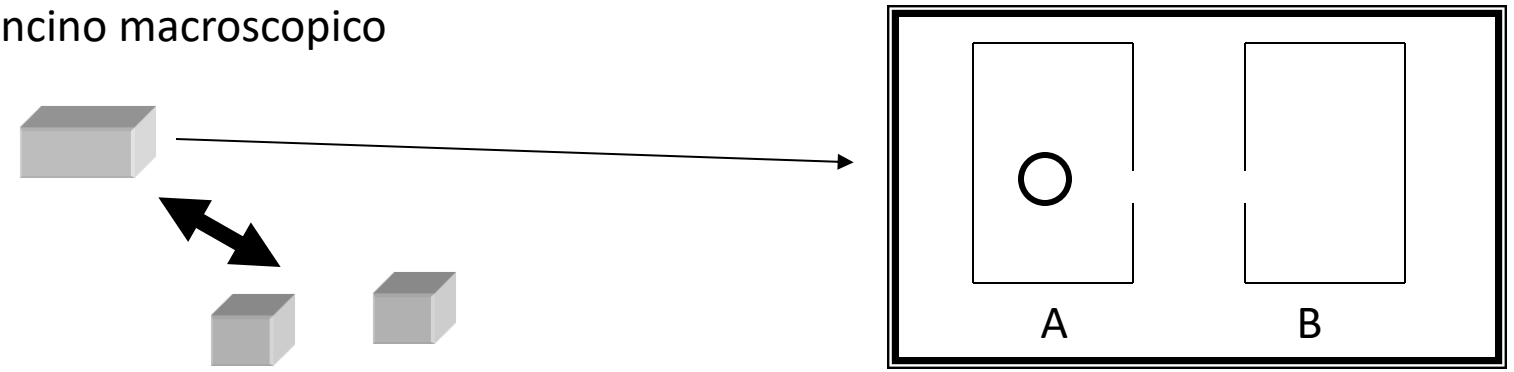


Heisenberg (1927)

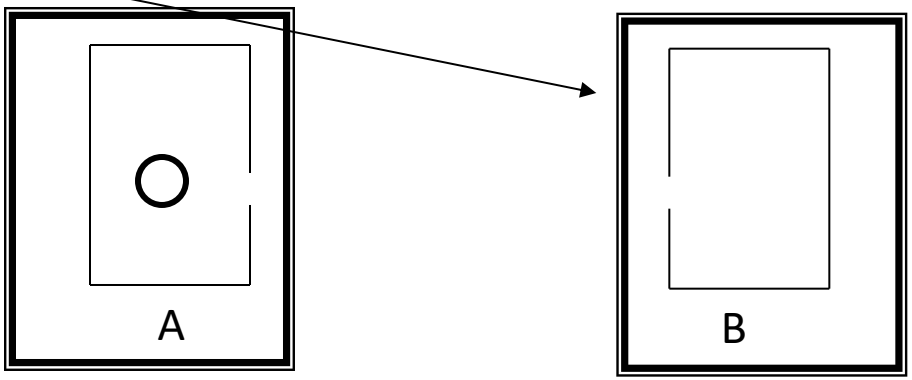
L'elettrone in "orbita" attorno al nucleo **non segue una traiettoria** formata da una sequenza temporale di posizioni e velocità, ma risulta "fermo" in uno **stato delocalizzato di sovrapposizione di posizioni e velocità** (stato di sovrapposizione microscopica).

Il significato della Quantizzazione

Mattoncino macroscopico



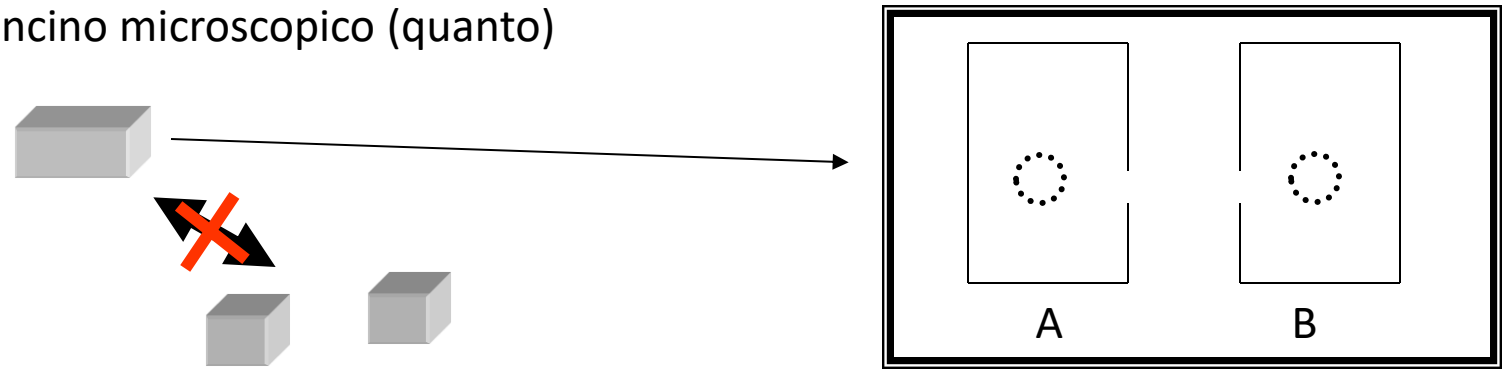
I suoi stati componenti



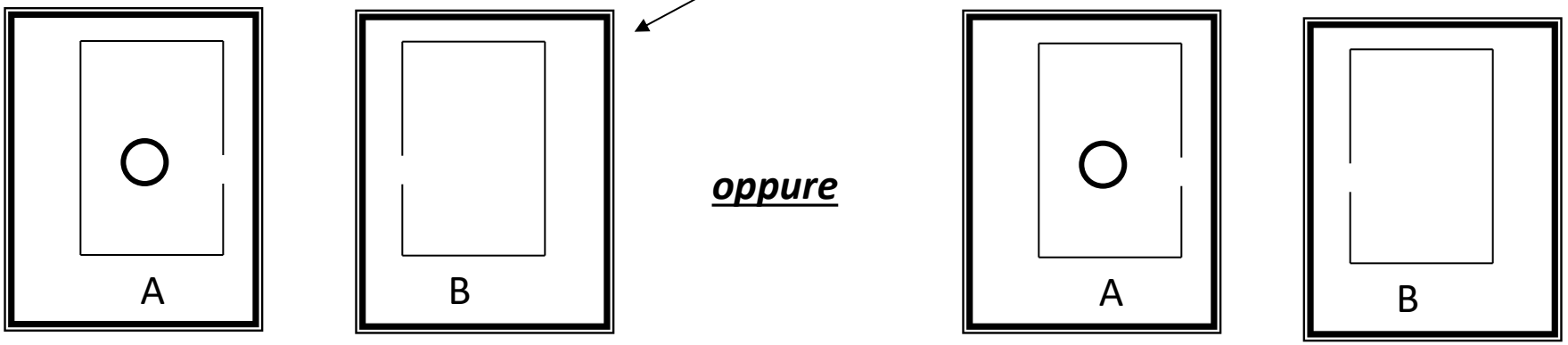
Un mattoncino classico è lo stato di una pallina all'interno di due scatole. Il mattoncino può essere ulteriormente dissezionato nei due mattoncini "la pallina è nella scatola A" e "la pallina non è nella scatola B".

Il significato della Quantizzazione

Mattoncino microscopico (quanto)

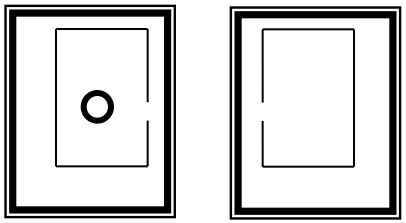


I suoi stati “componenti”

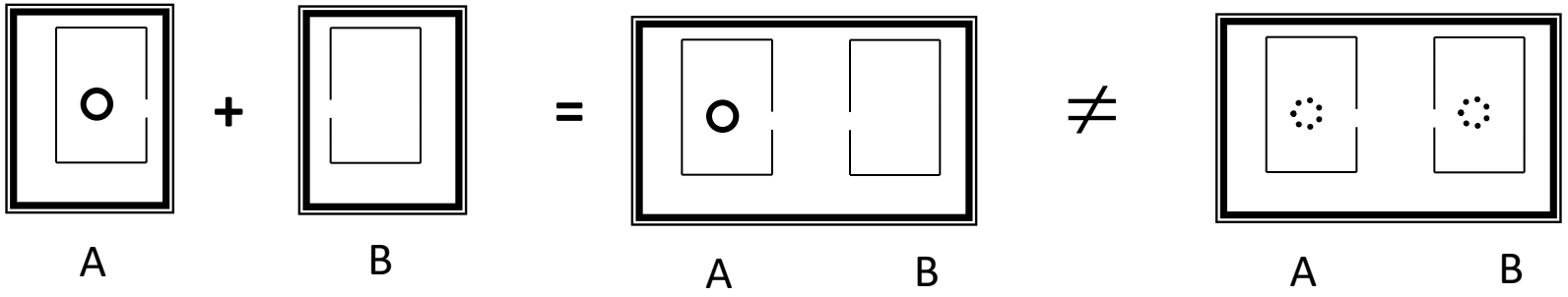


Un mattoncino microscopico (quanto) è lo stato di una particella all’interno di due scatole. Nel dissezionare questo stato, **non si ottiene una struttura univoca**. Il risultato si presenta ***o*** “la pallina è in A e non in B” ***oppure*** “la pallina è in B e non in A”.

Il significato della Quantizzazione



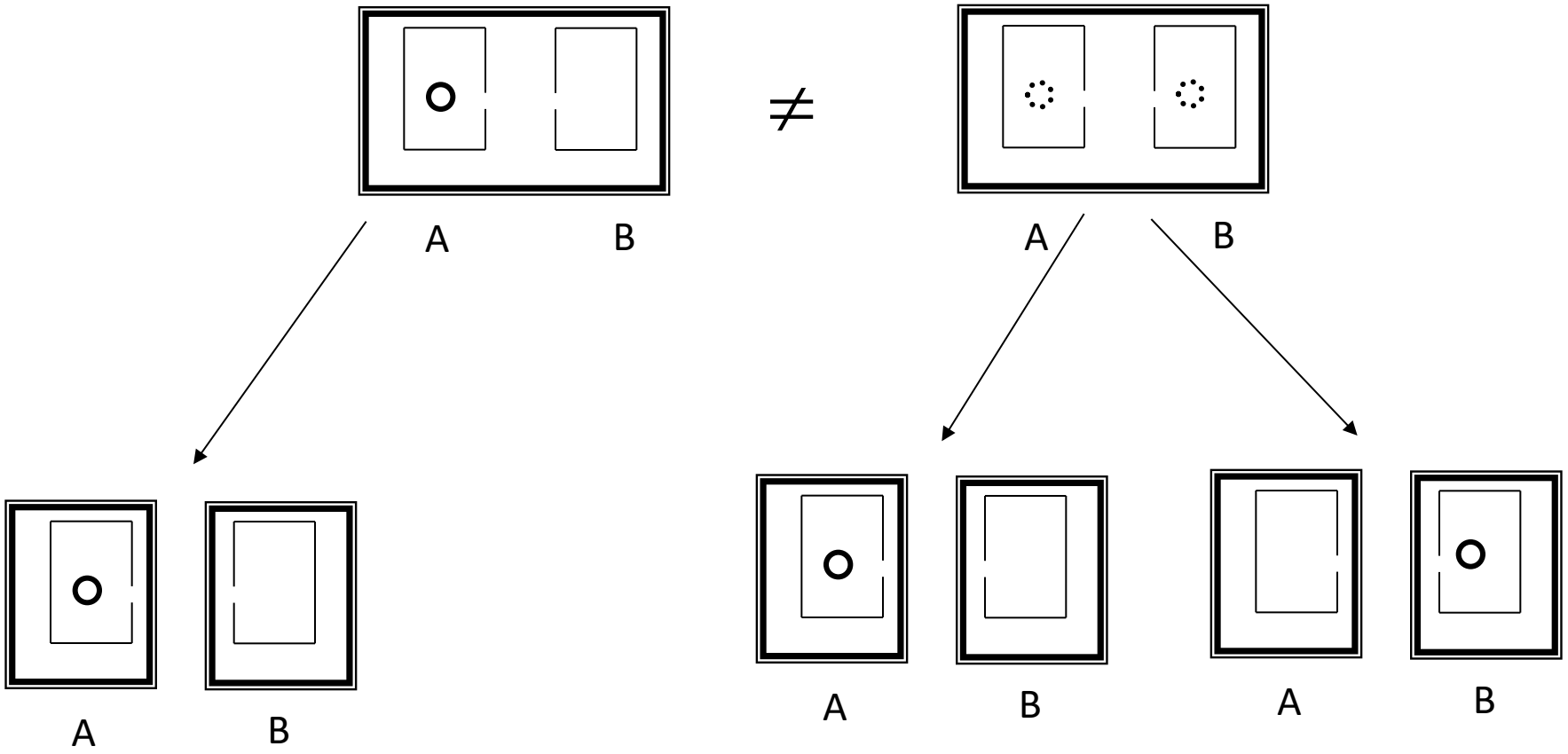
A B



A B A B A B

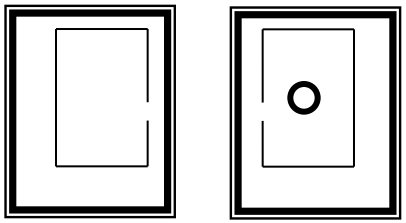
Ora il singolo stato componente **non** può più **riprodurre** lo stato iniziale.

Il significato della Quantizzazione

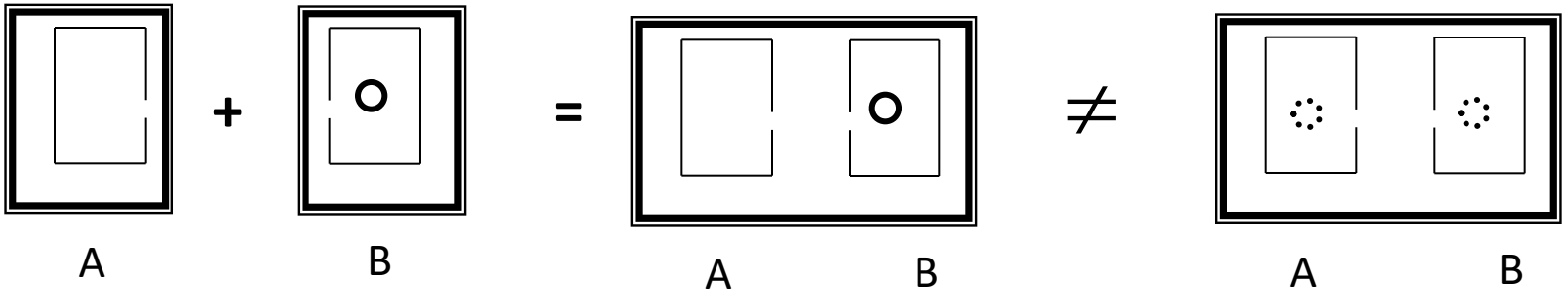


Lo **stato iniziale** conteneva due completamente **diverse e incompatibili** componenti.

Il significato della Quantizzazione



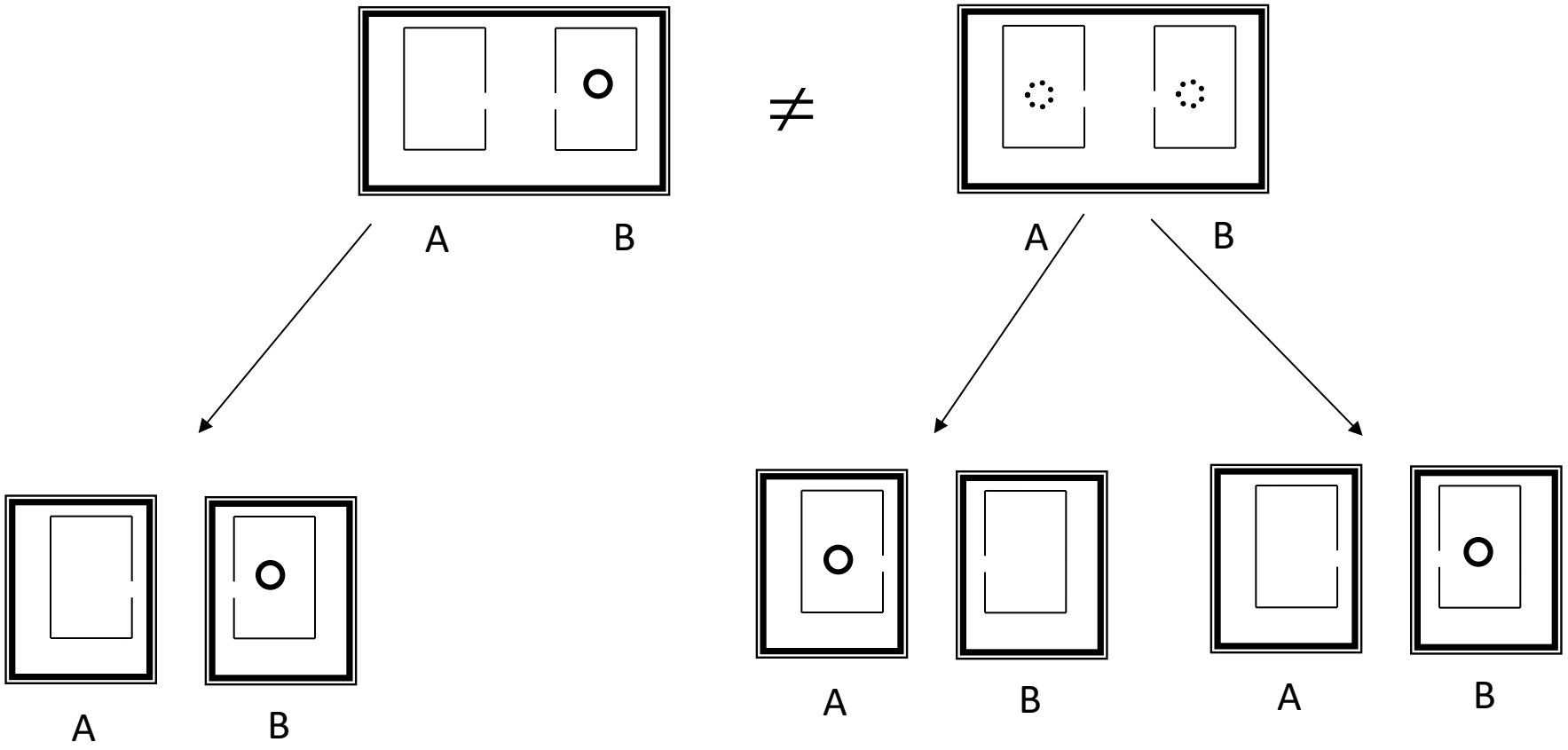
A B



A B A B A B

La stessa cosa vale per la seconda componente.

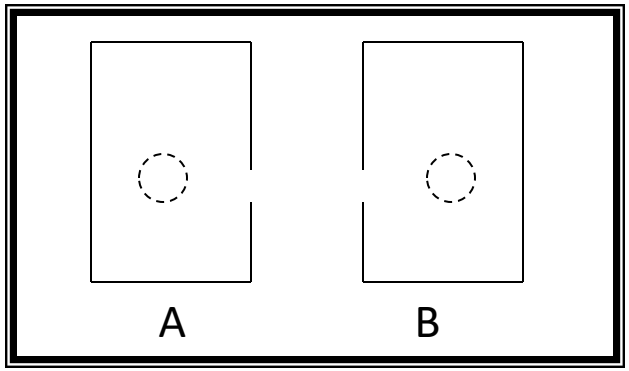
Il significato della Quantizzazione



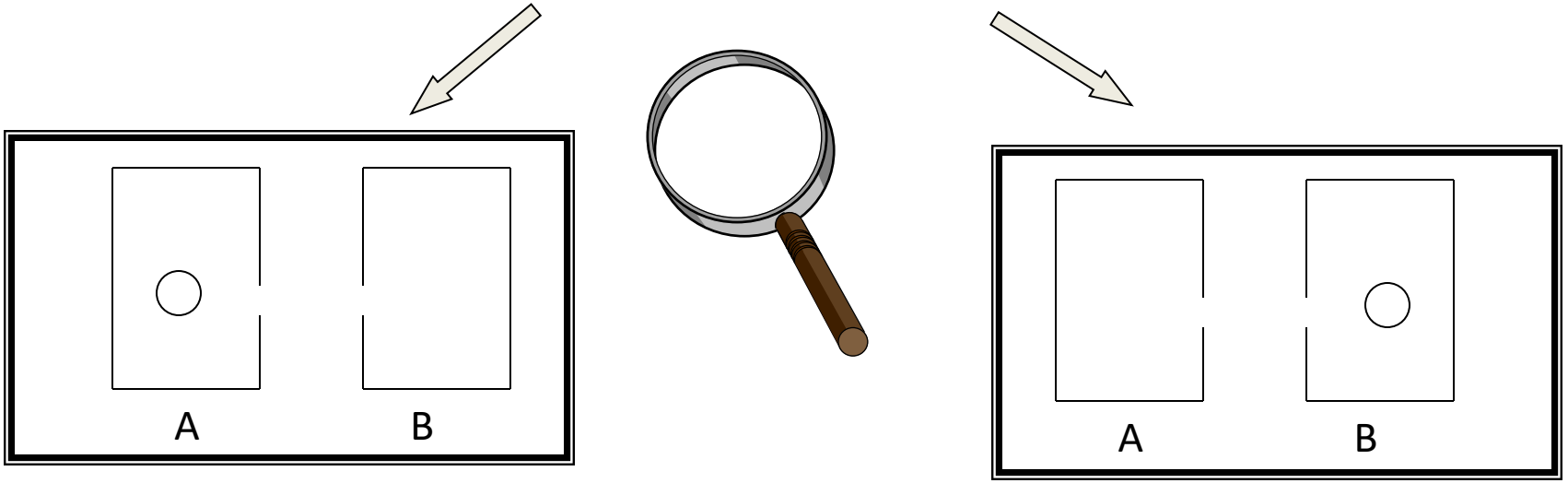
Lo **stato iniziale** conteneva due completamente **diverse e incompatibili** componenti.

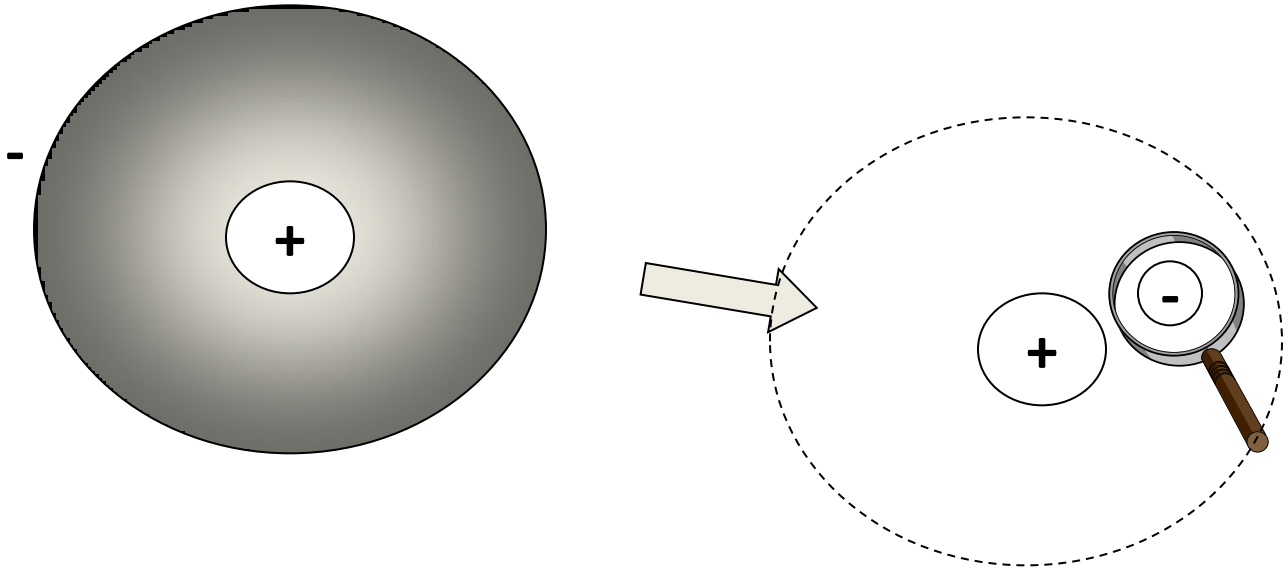
“*Nuova teoria della Meccanica Quantistica*”

Stati di **<u>sovrapposizione</u>** microscopica



<u>Collasso</u> della dello stato di sovrapposizione in conseguenza dell’atto di misurazione (intervento macroscopico)





La base fenomenologica della M.Q.

Spettroscopia

J. Balmer, 1885

Effetto fotoelettrico

A. Einstein, 1905

Stabilità dell'atomo

N. Bohr, 1913

Esperimenti di Franck-Hertz

J. Franck e G. Hertz, 1914

Esperimento di Stern e Gerlach

O. Stern e W. Gerlach, 1922

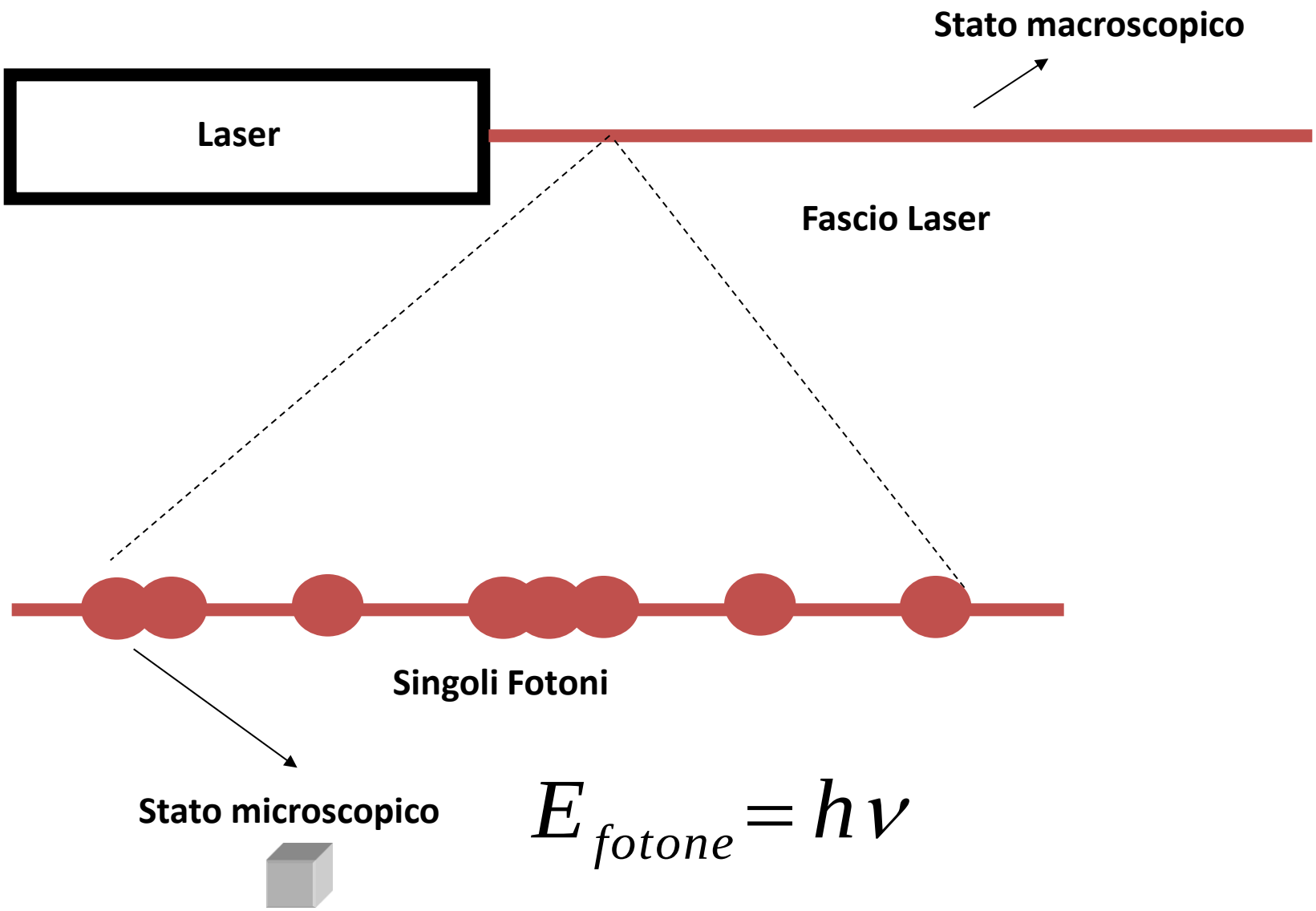
Effetto Compton

A. H. Compton, 1923

Ottica Quantistica: la M.Q. dei fotoni

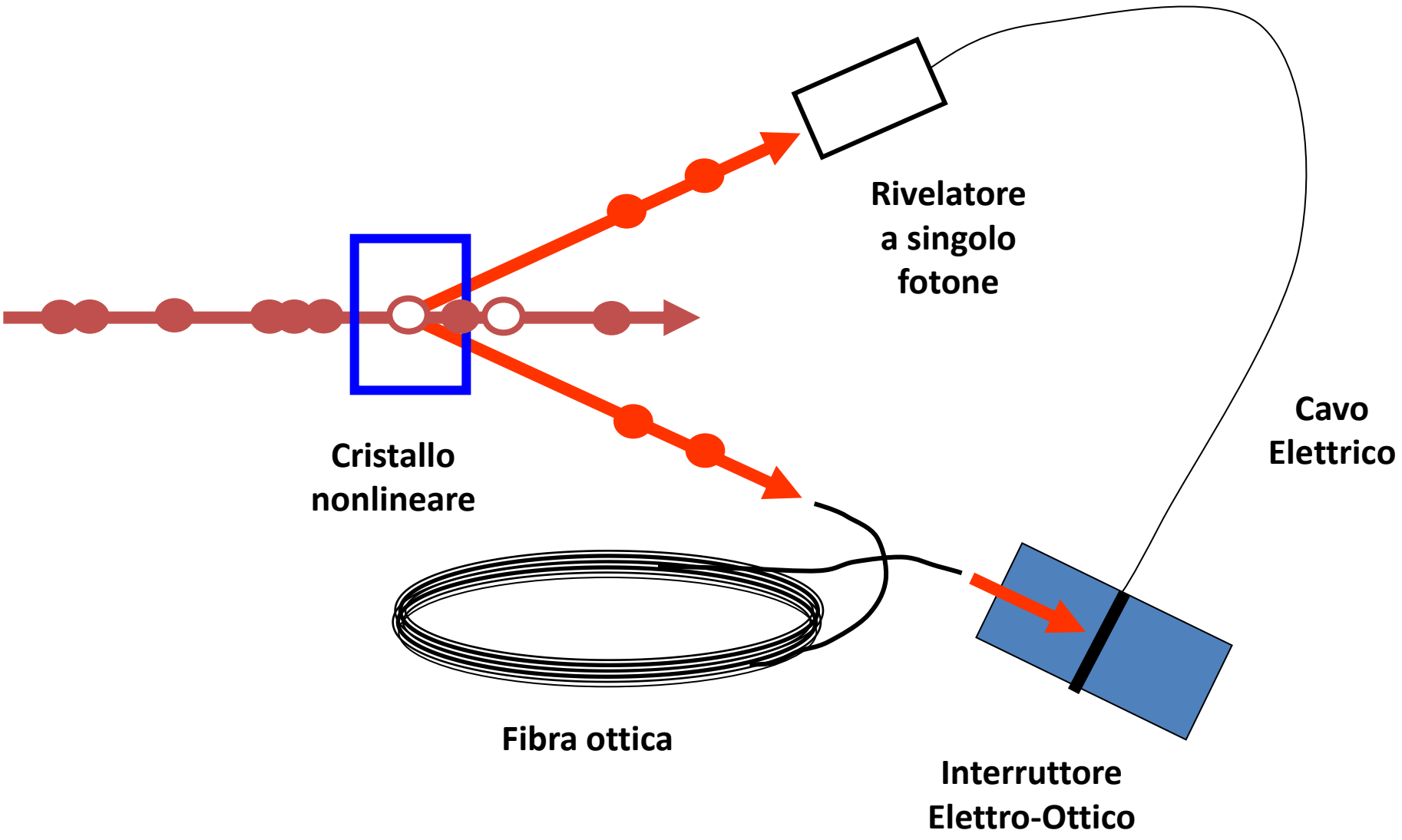
Gli stati macroscopici	**LUCE**
Gli stati microscopici (mattoncini)	**FOTONI**
Sorgenti	**GENERATORI DI SINGOLI FOTONI**
Rivelatori	**RIVELATORI DI SINGOLI FOTONI**
Manipolatori	**STRUMENTAZIONE OTTICA E OPTOELETTRONICA**

La luce e i fotoni

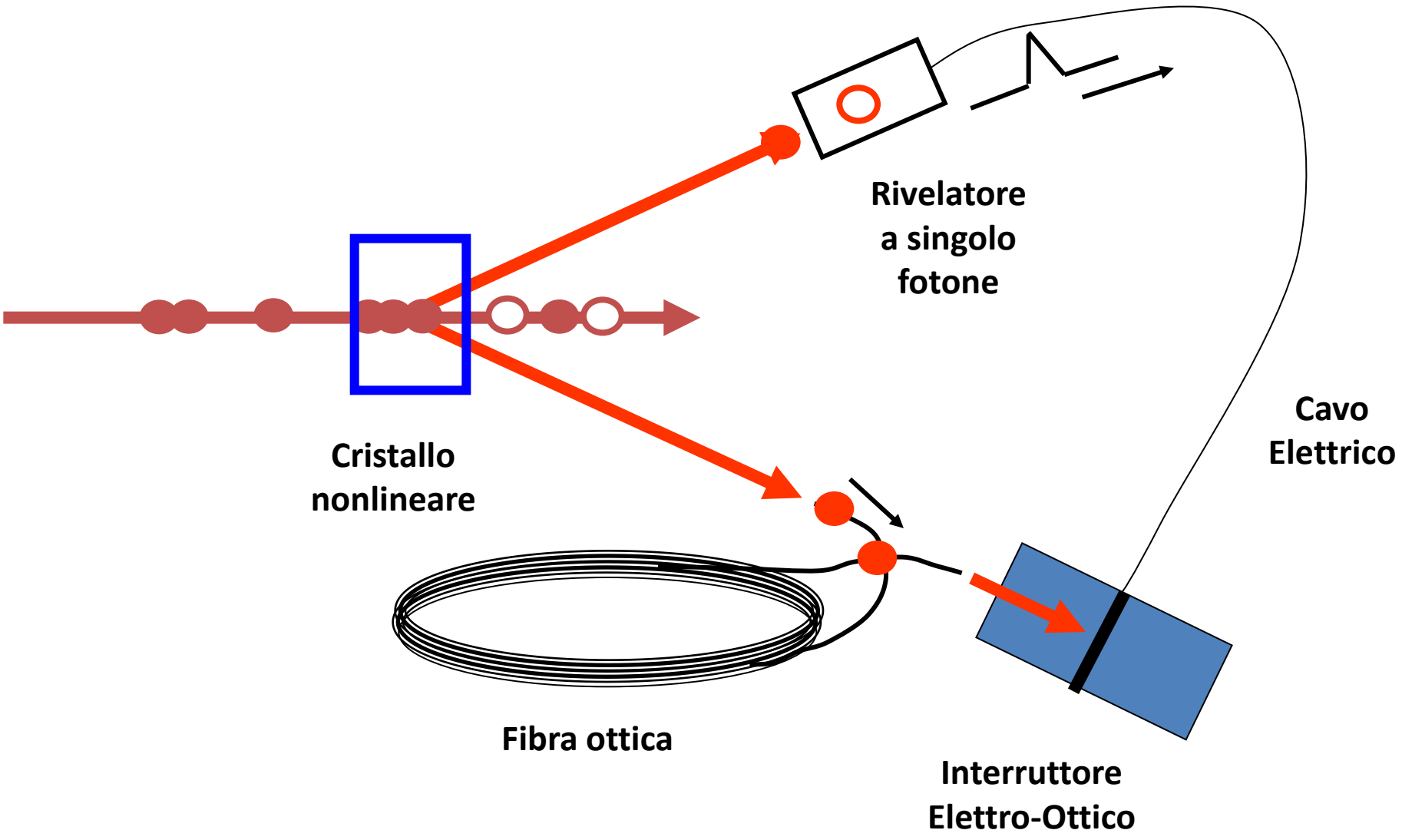


$$E_{fotone} = h\nu$$

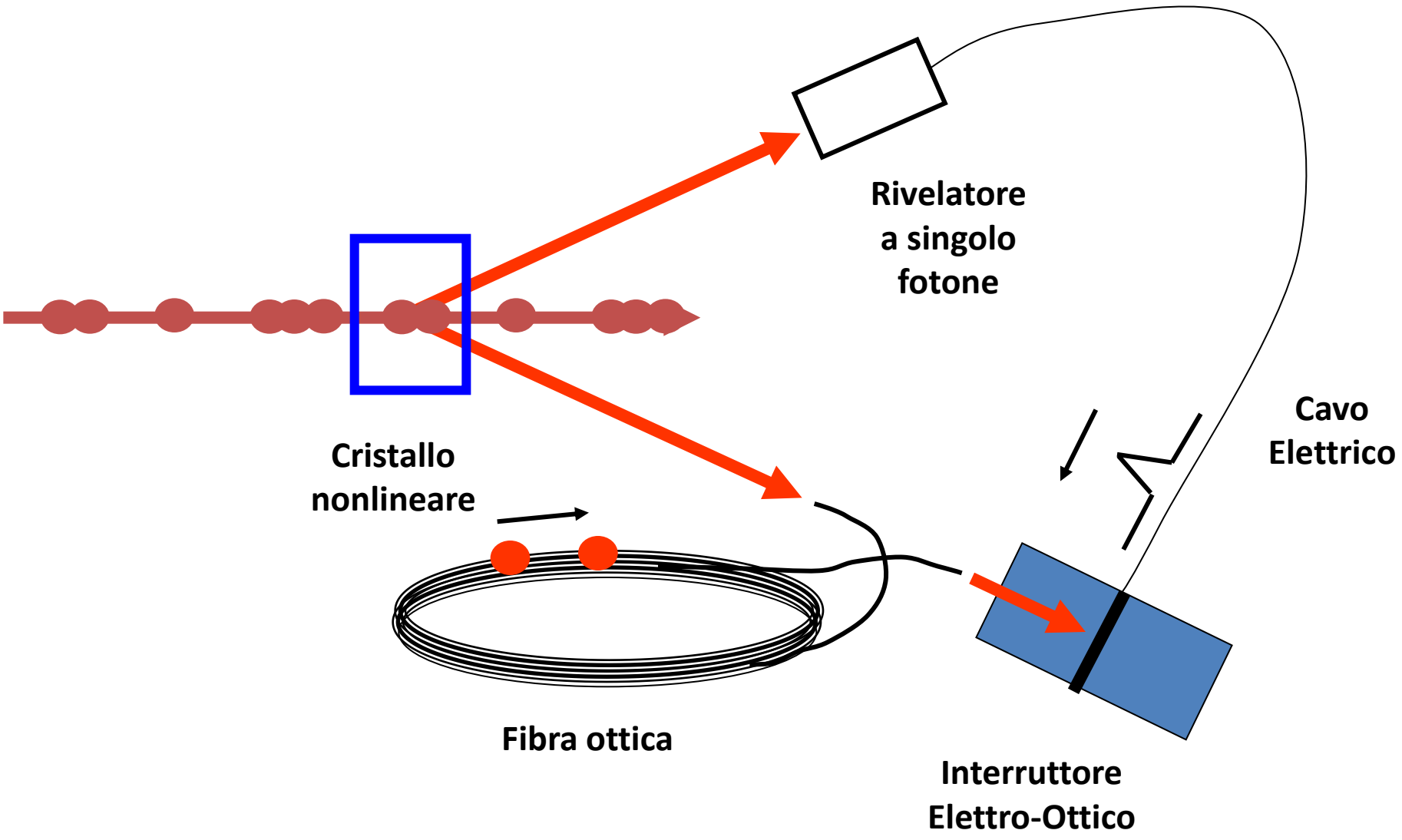
Sorgente di singoli fotoni



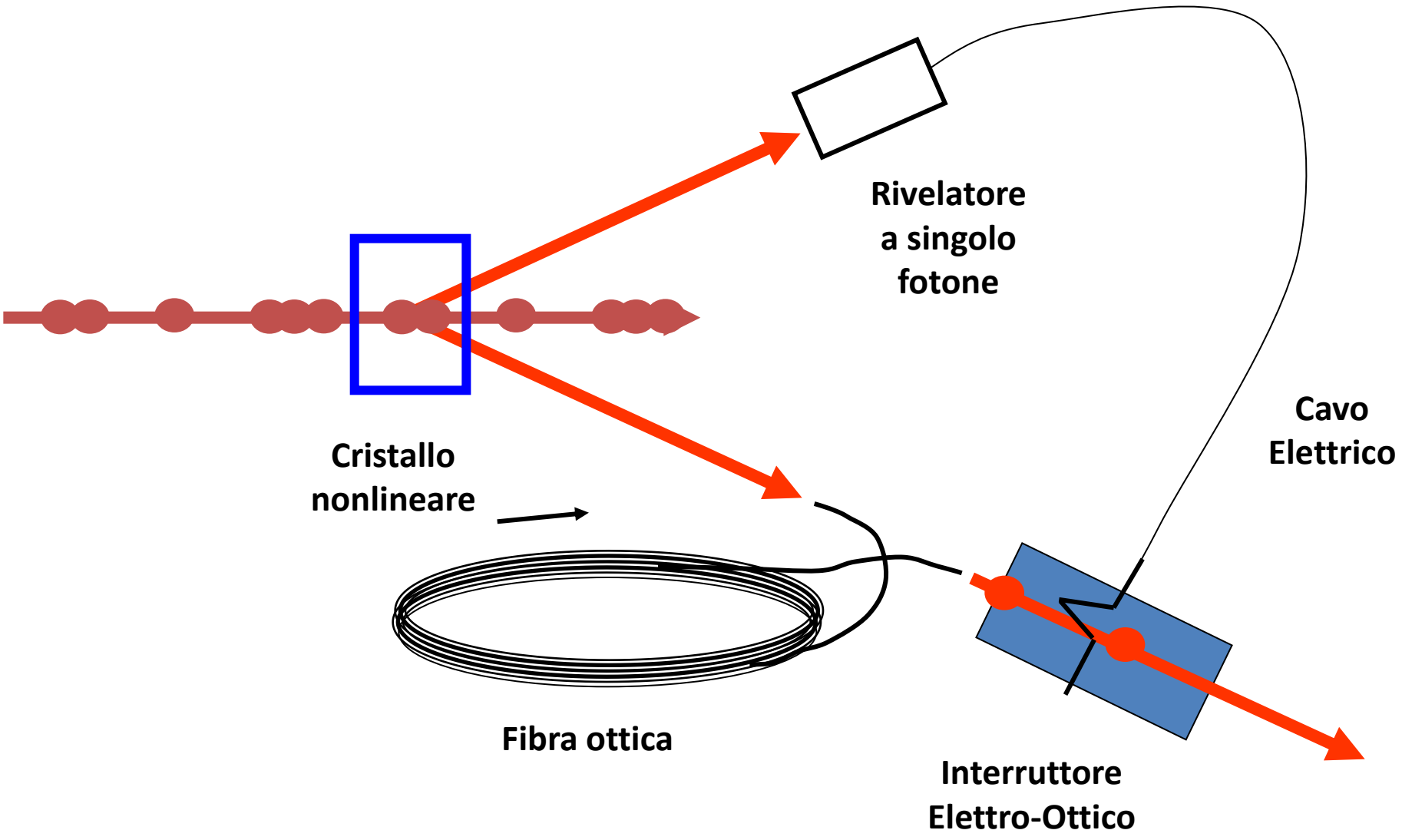
Sorgente di singoli fotoni



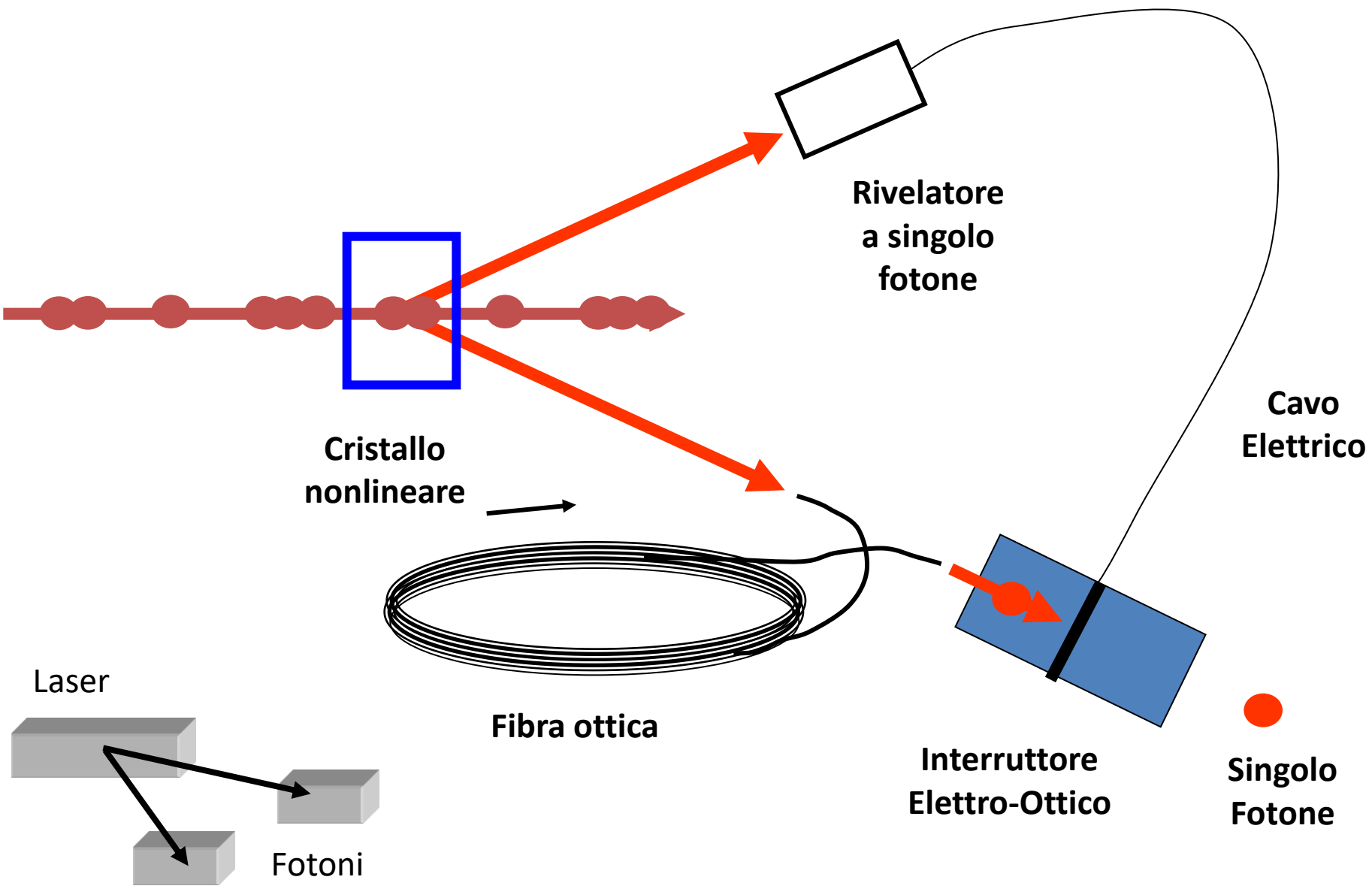
Sorgente di singoli fotoni



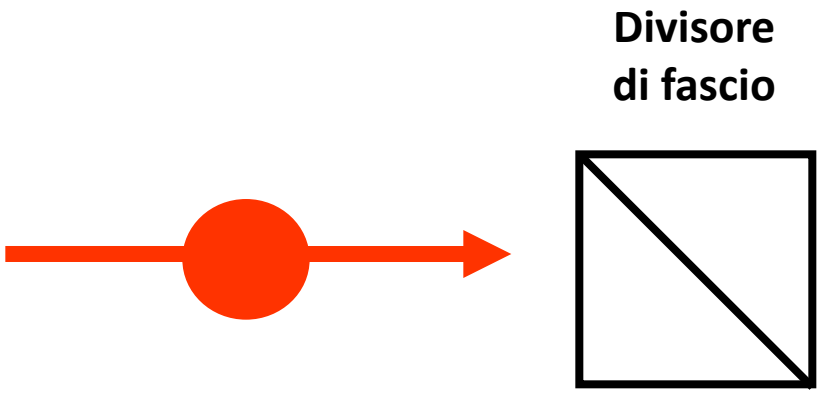
Sorgente di singoli fotoni

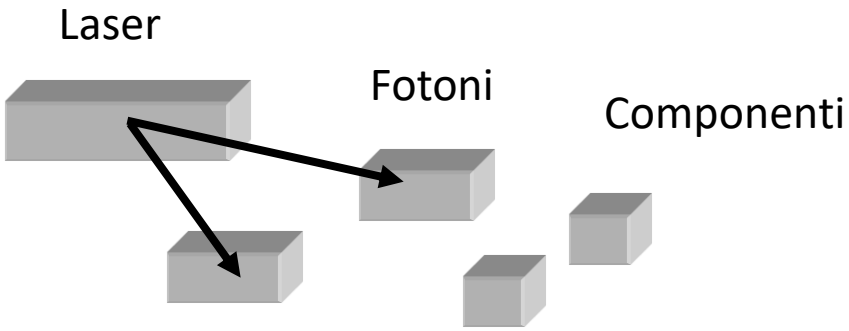


Sorgente di singoli fotoni

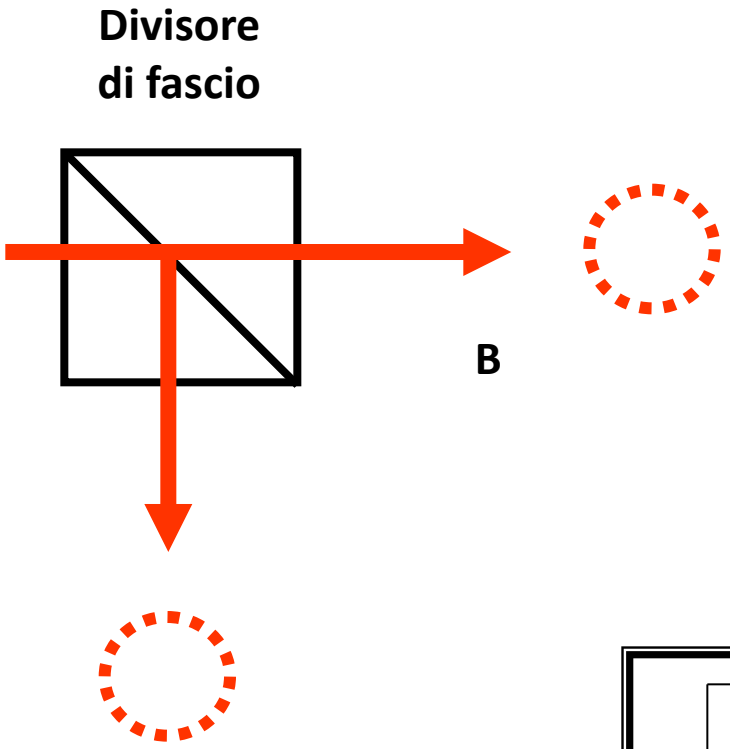


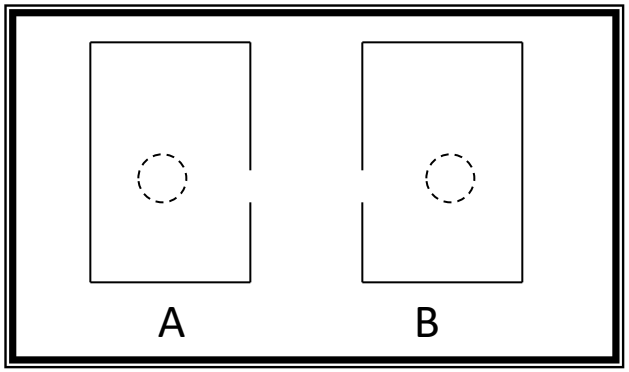
Esperimento di Hanbury-Brown-Twiss

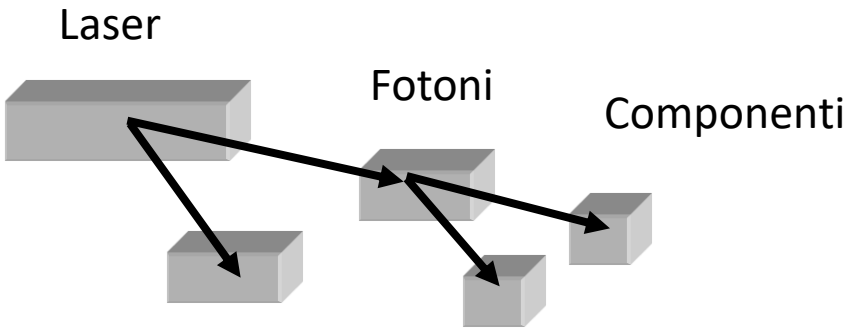




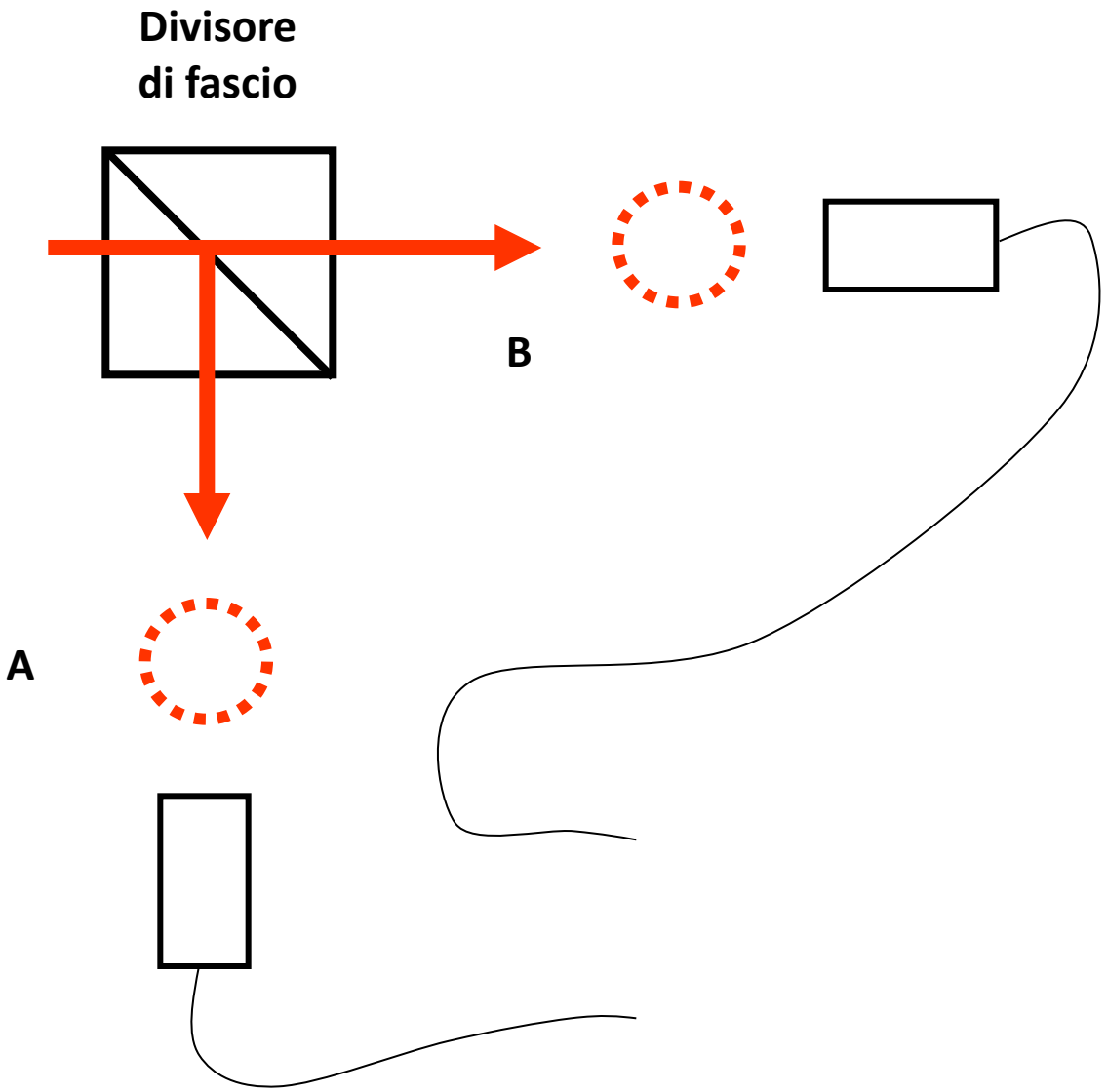
Esperimento di Hanbury-Brown-Twiss



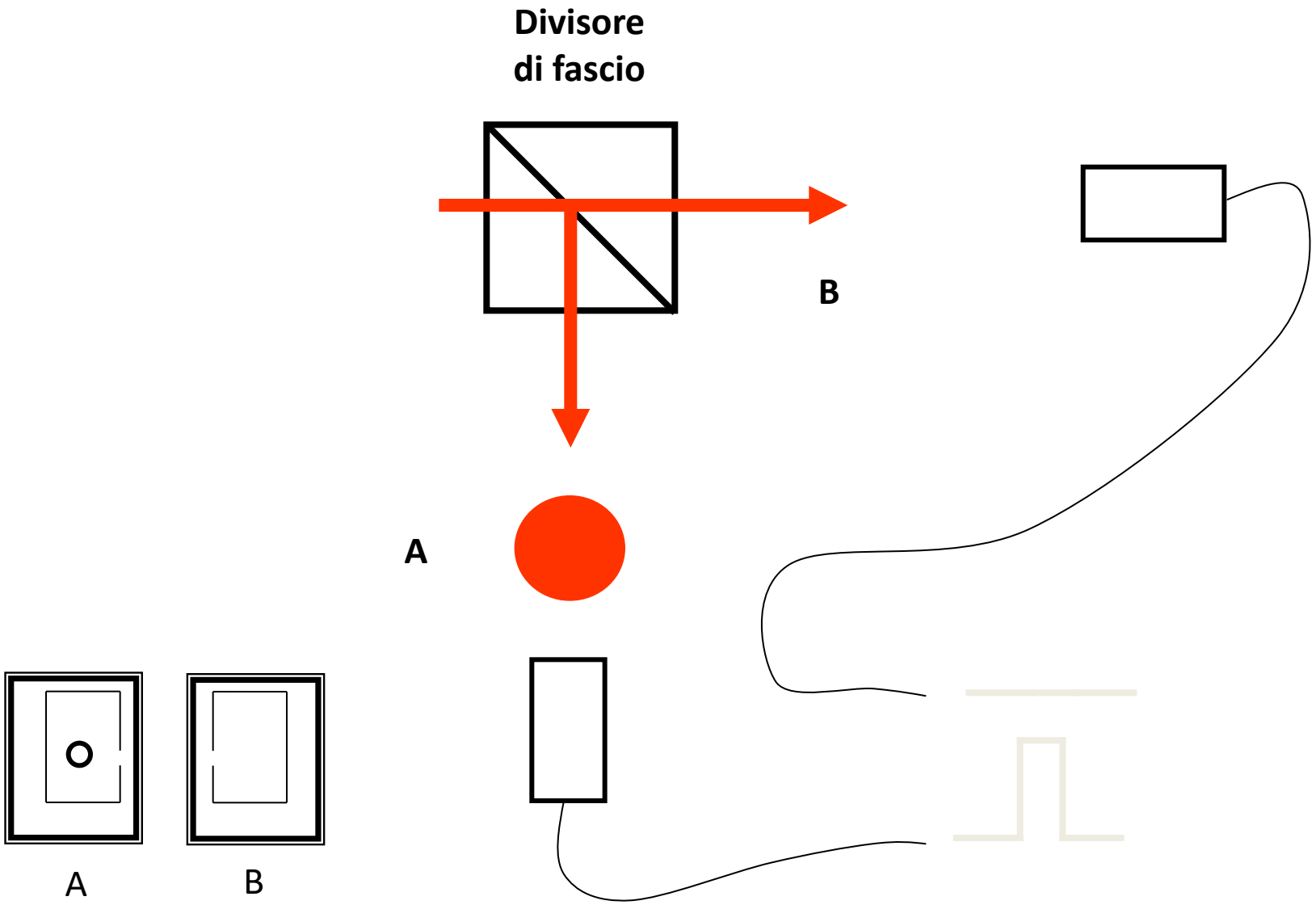




Esperimento di Hanbury-Brown-Twiss

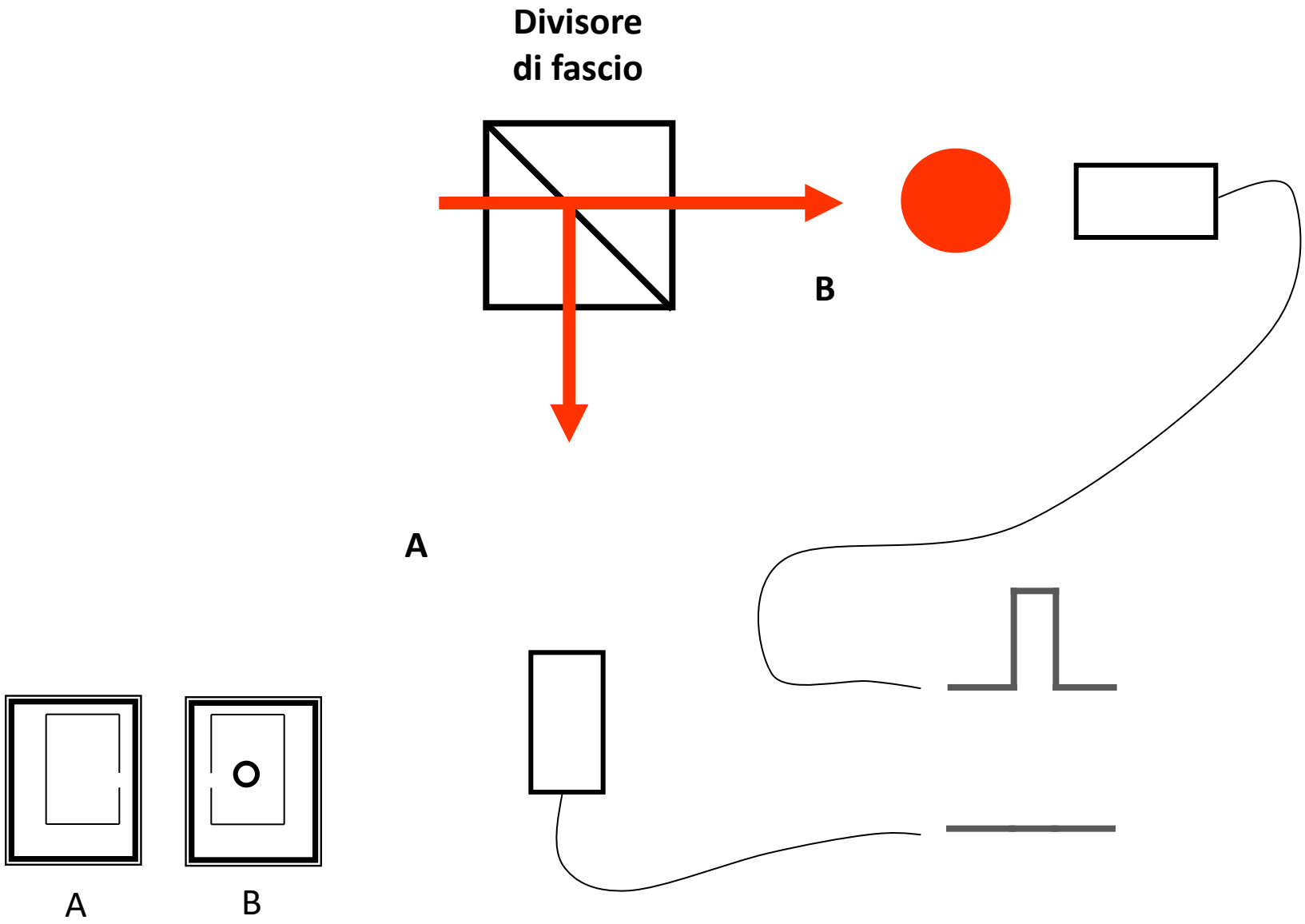


Esperimento di Hanbury-Brown-Twiss



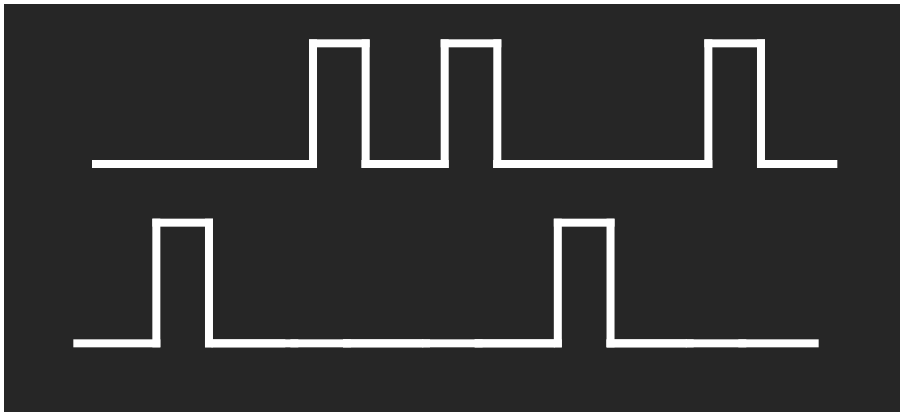
oppure…

Esperimento di Hanbury-Brown-Twiss



B

A



Non si osservano **mai** coincidenze

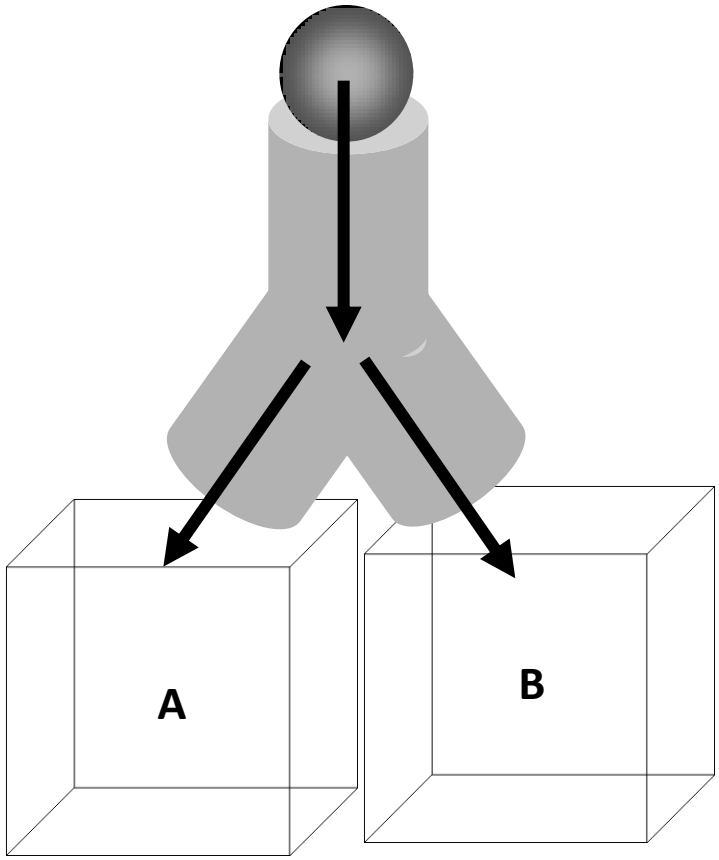
B

A

Sovrapposizione Quantistica vs Probabilità

Anche nel **mondo macroscopico** esistono processi che danno luogo a **due distinti effetti**. Per essi vale una descrizione **statistico-probabilistica.**

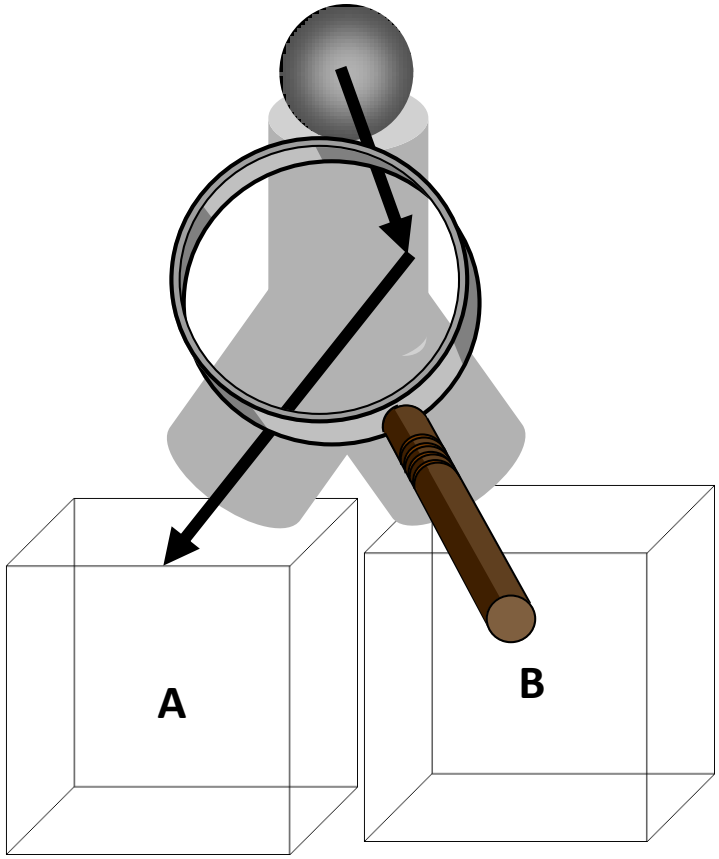
Sovrapposizione Quantistica vs Probabilità



P(A)=1/2
P(B)=1/2

Un oggetto macroscopico può ricadere nello stato A o nello stato B. **Non volendo** osservare tutti i dettagli, utilizziamo una **descrizione statistica**.

Sovrapposizione Quantistica vs Probabilità

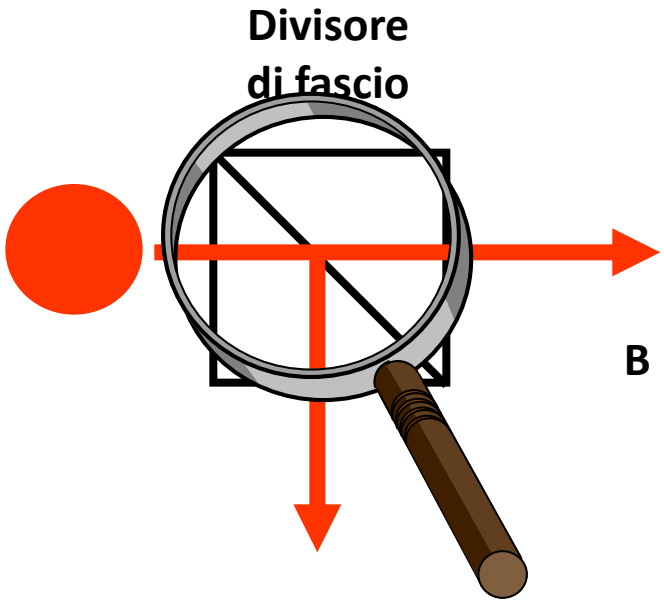


~~P(A)=1/2~~
~~P(B)=1/2~~

Osservando i **dettagli** della dinamica è sempre possibile predire **l'esatta traiettoria** e quindi **rendere inutile** la descrizione statistica.

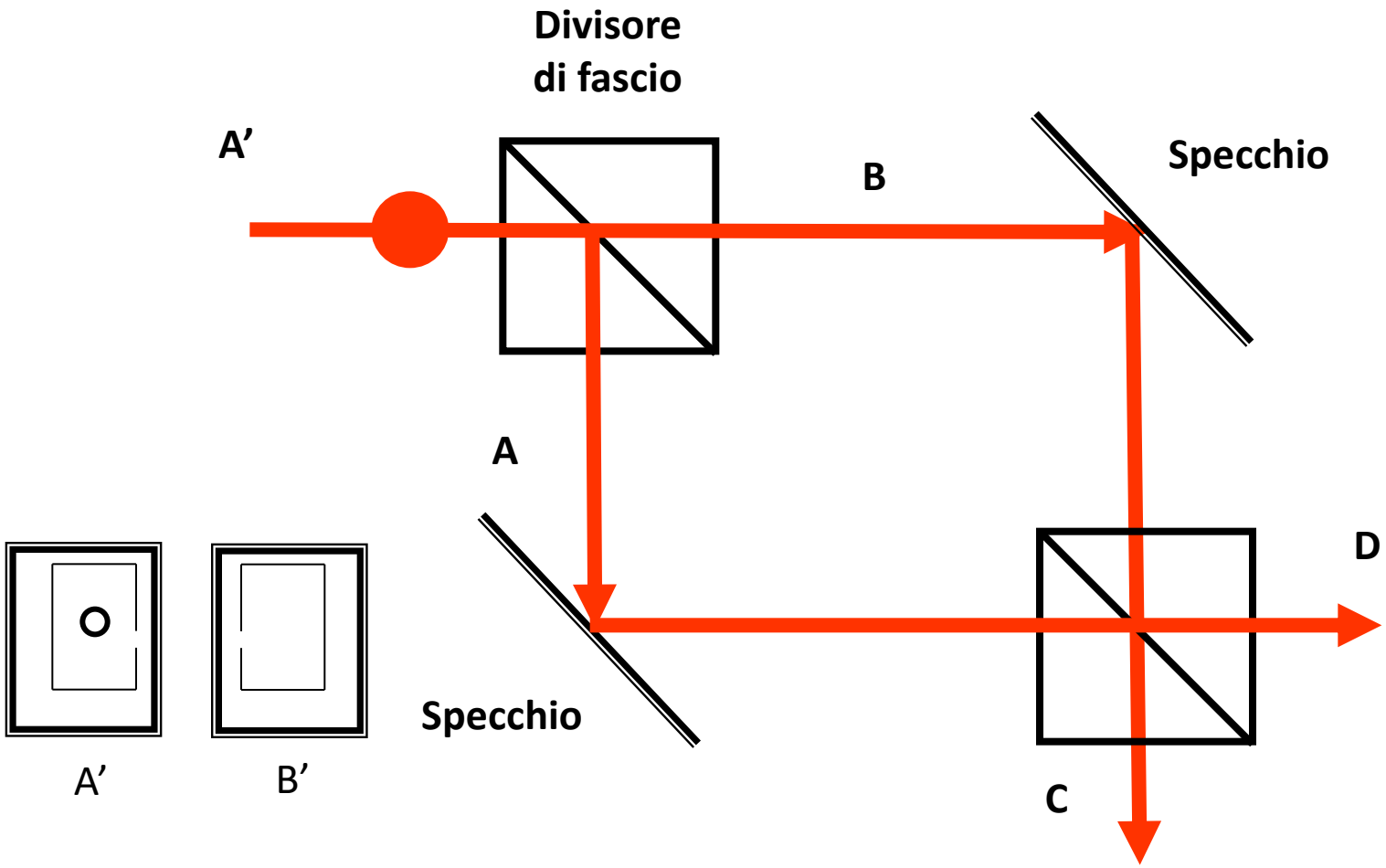
Sovrapposizione Quantistica vs Probabilità

E’ possibile per la dissezione di un quanto?



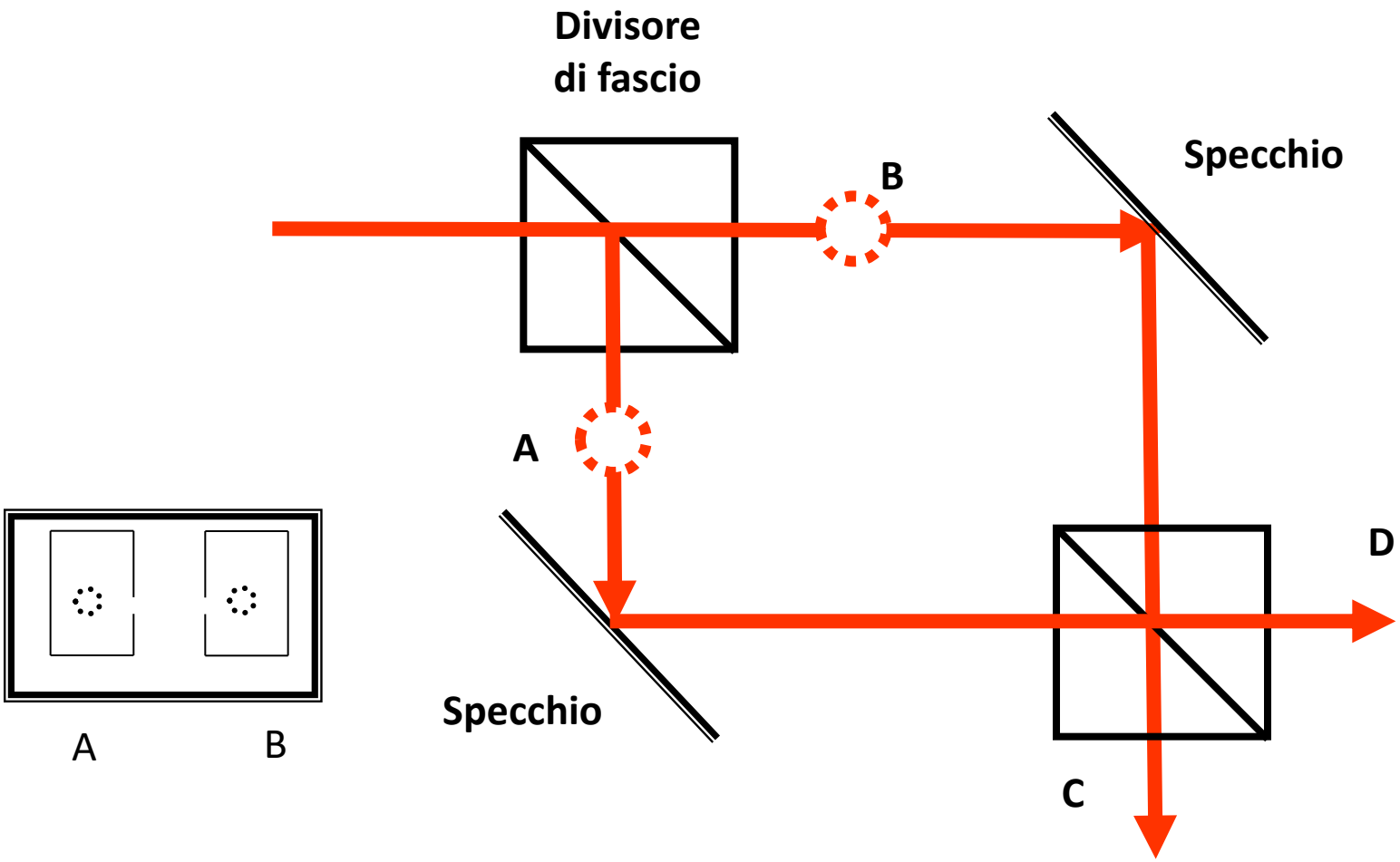
?

Interferometro di Mach-Zehnder



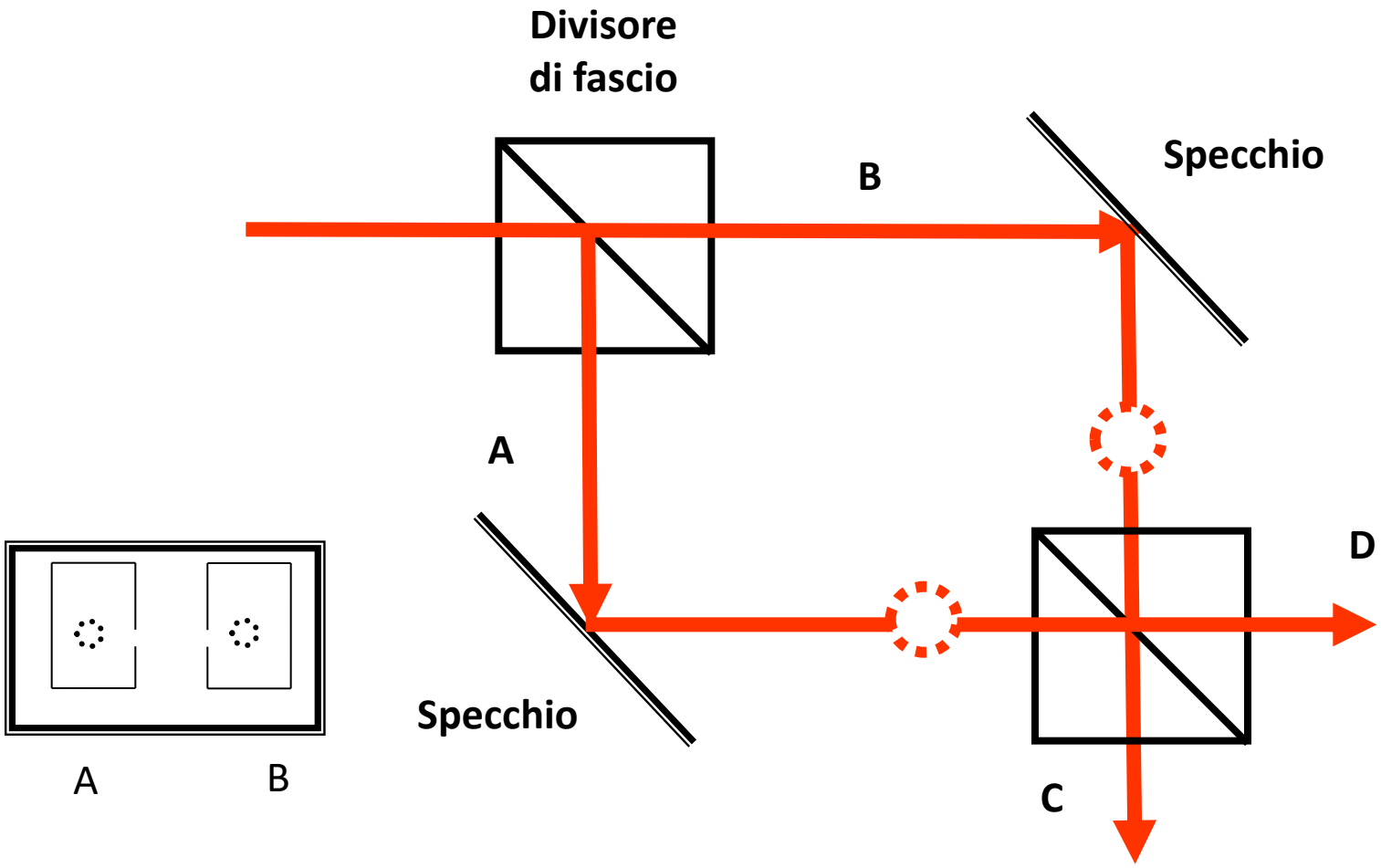
Il fotone può percorrere due diverse traiettorie **A** e **B** per poi **ricombinarsi** su **C** e **D**.

Interferometro di Mach-Zehnder



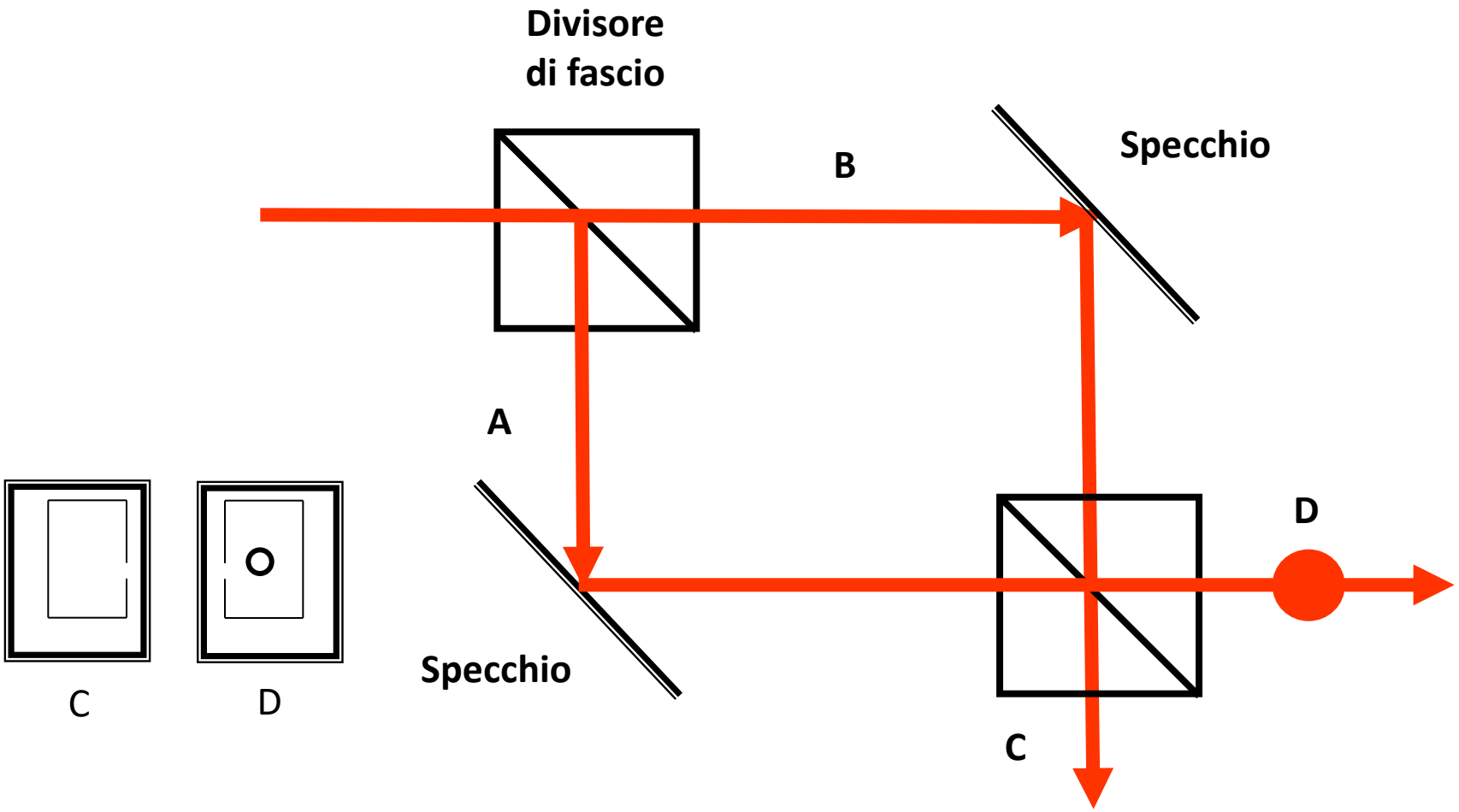
Lo stato fotonico diventa una sovrapposizione dei stati A e B.

Interferometro di Mach-Zehnder



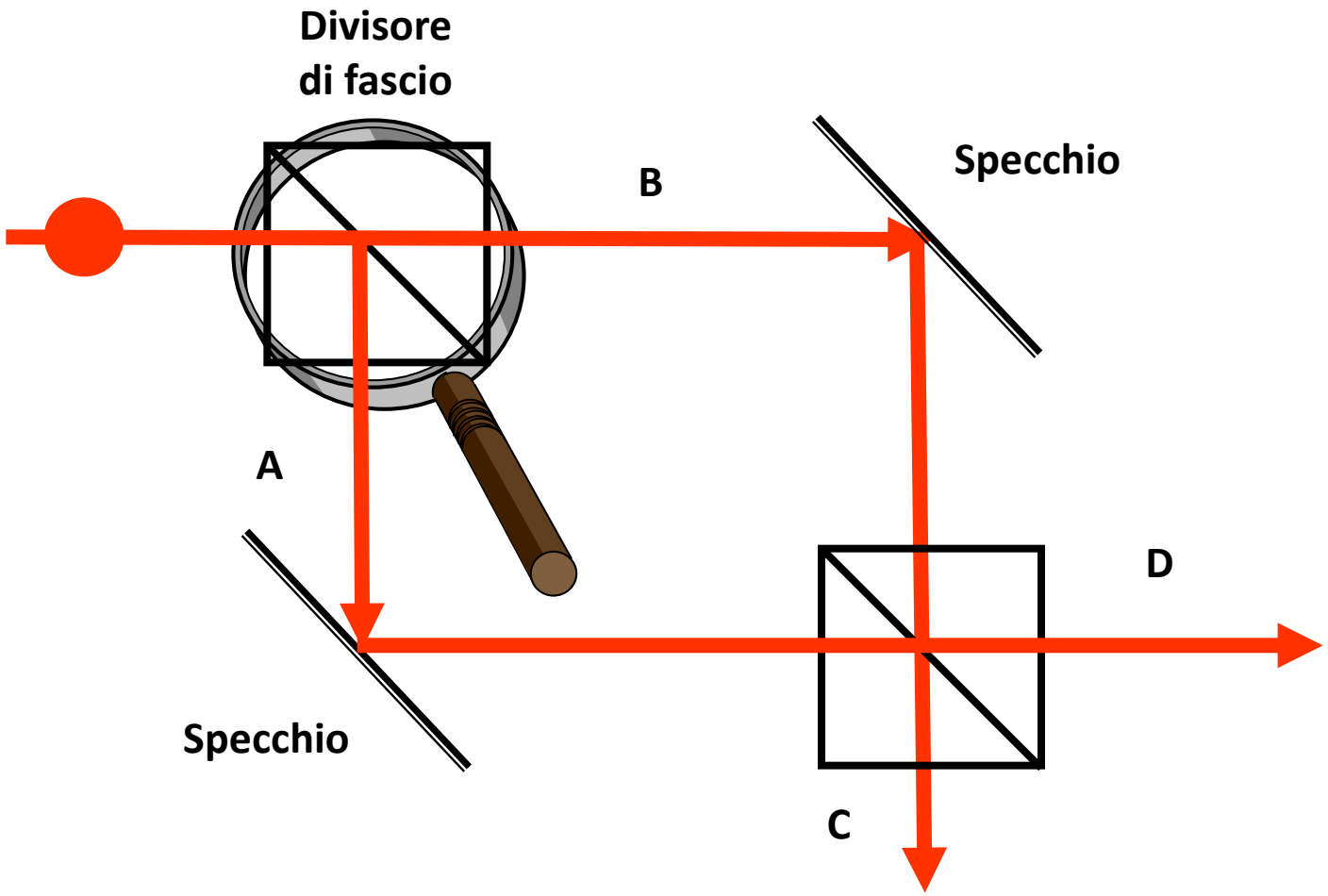
I due stati convergono sul secondo divisore di fascio.

Interferometro di Mach-Zehnder



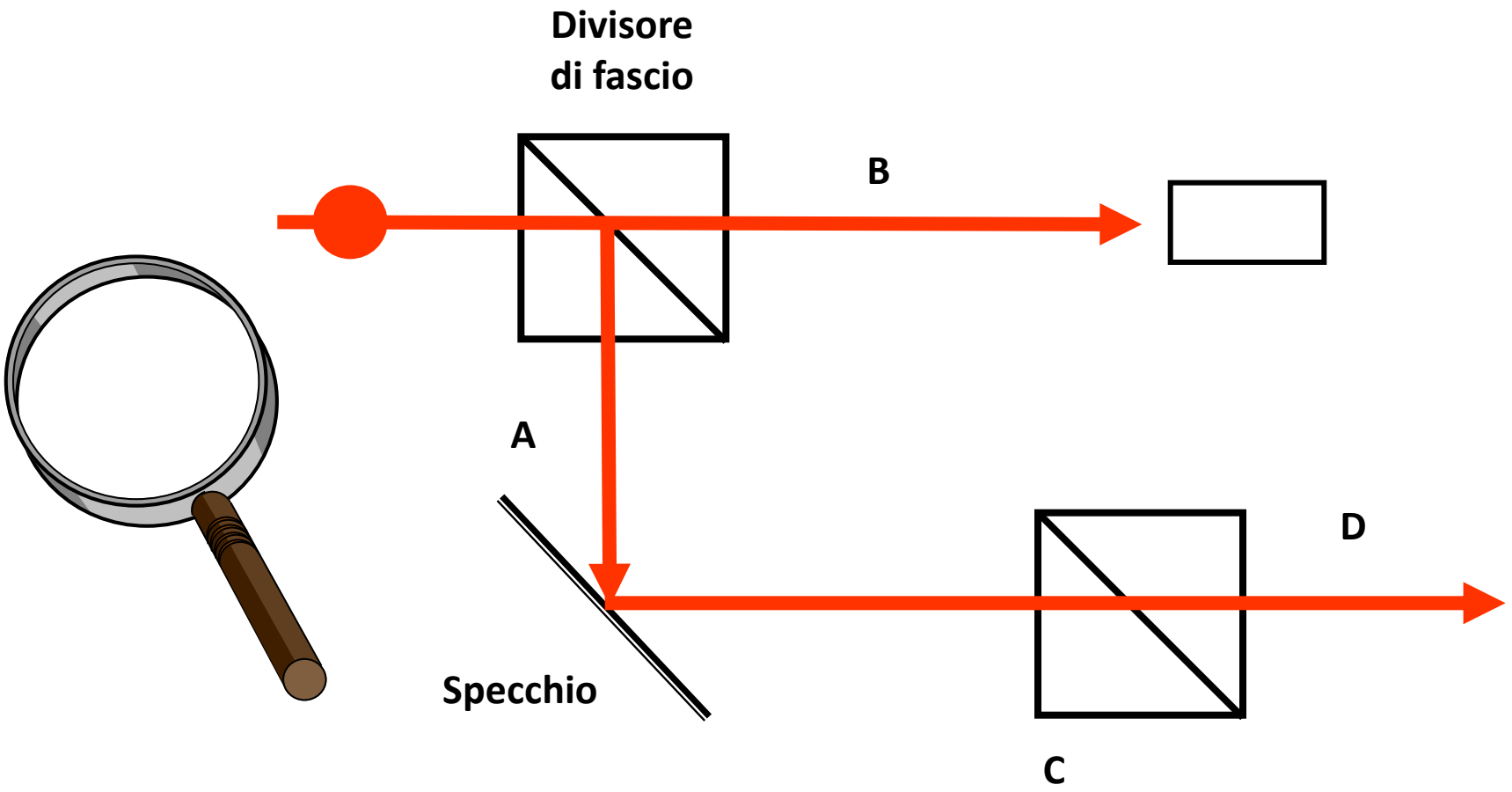
I due cammini A e B interferiscono e costituiscono interferenza costruttiva sullo stato D ed interferenza distruttiva sul canale C. Il fotone esce sempre da D.

Interferometro di Mach-Zehnder



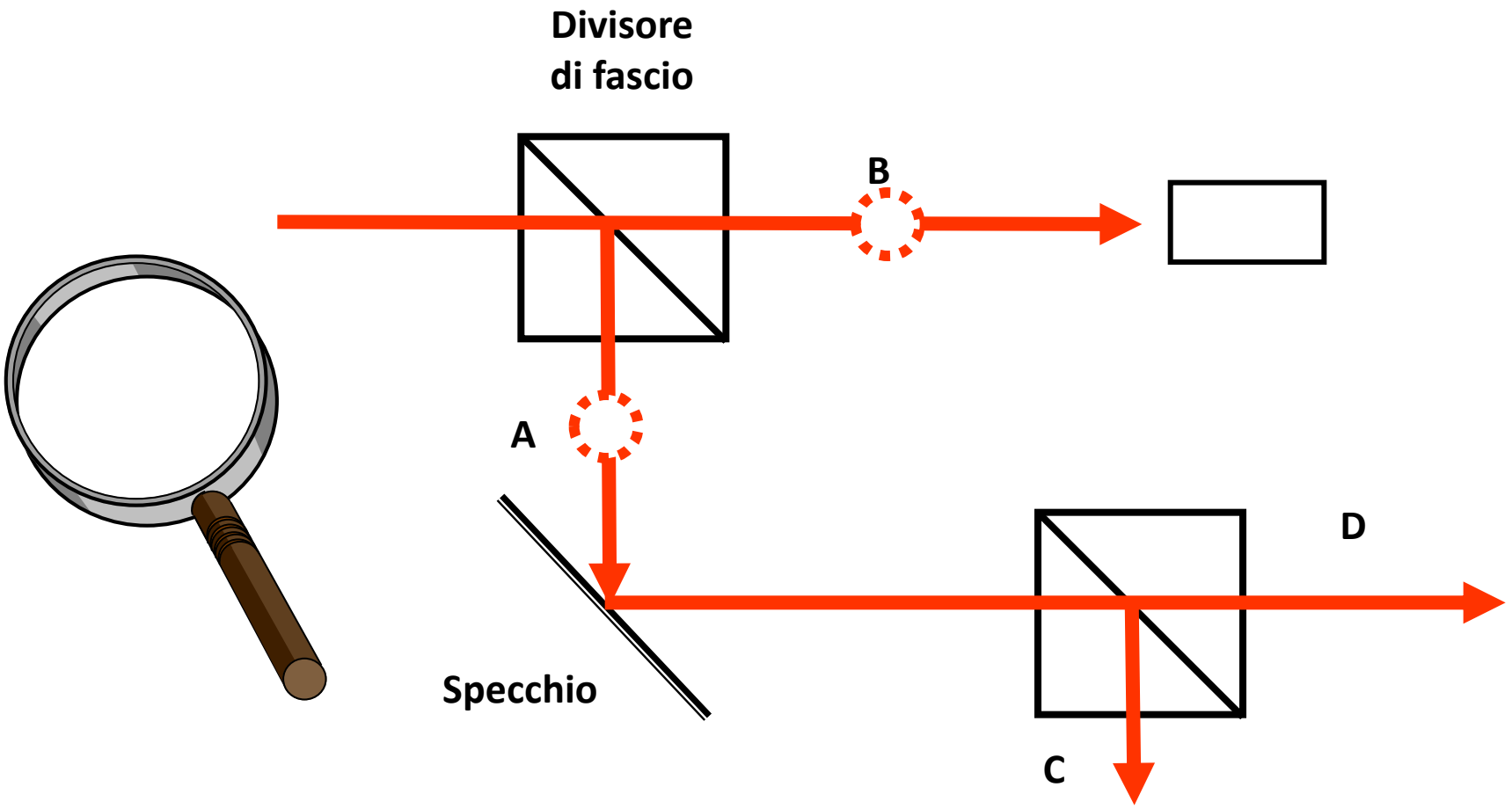
I due cammini A e B interferiscono e costituiscono interferenza costruttiva sullo stato D ed interferenza distruttiva sul canale C. Il fotone esce sempre da D.

Interferometro di Mach-Zehnder



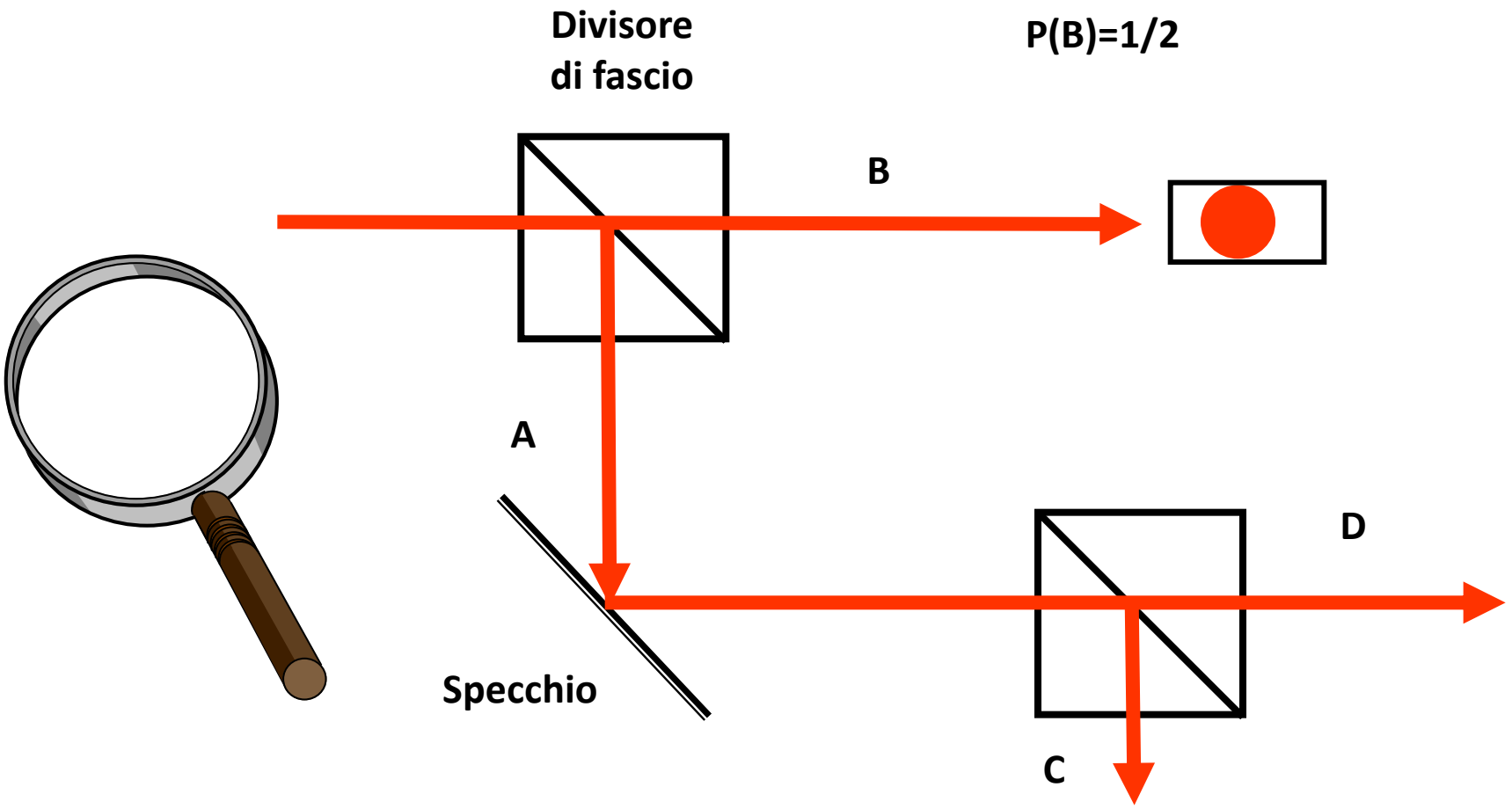
Ispezionare significa al minimo controllare dove va il fotone (esso non può lasciare alcuna traccia).

Interferometro di Mach-Zehnder



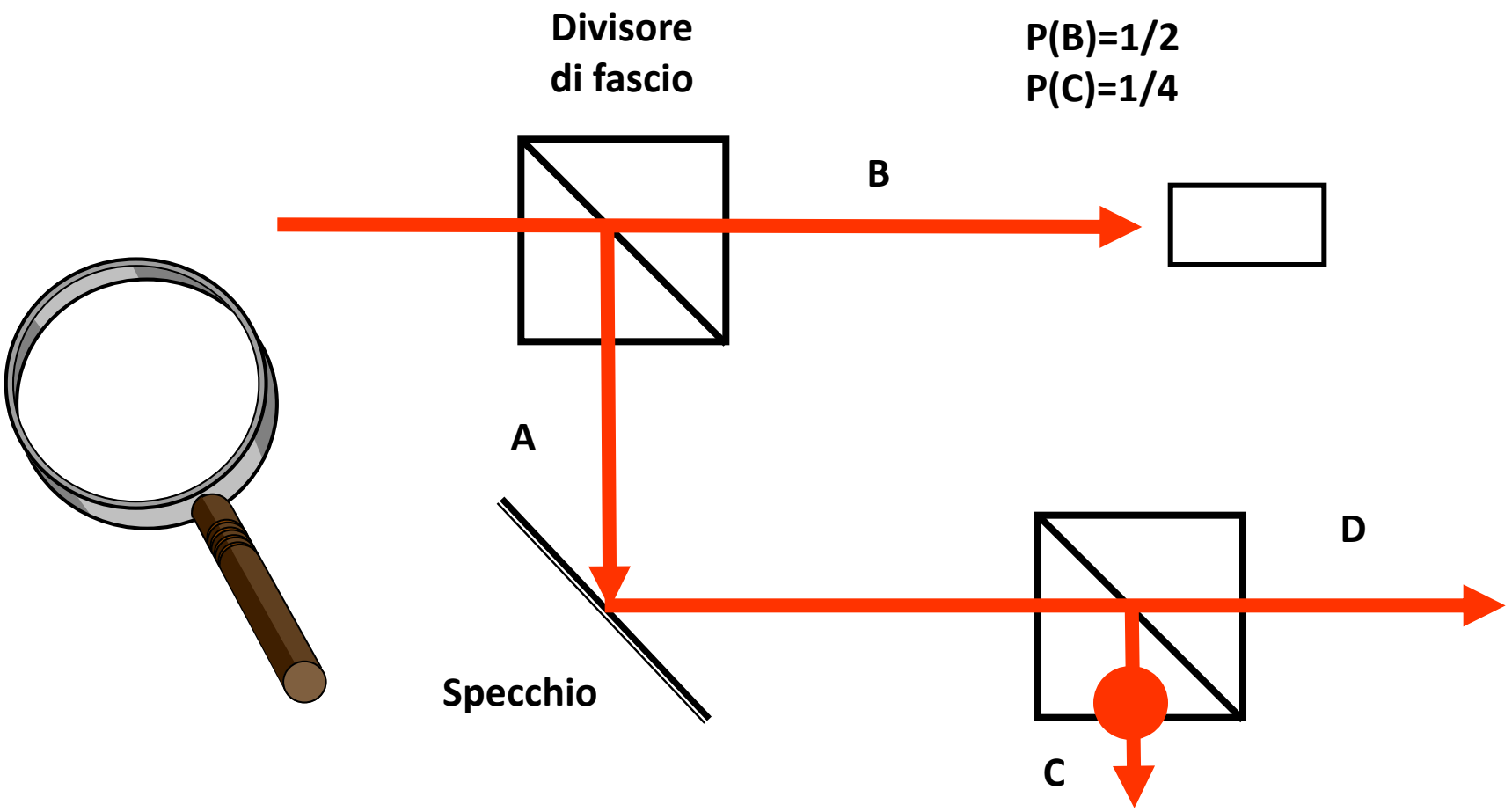
Ispezionare significa al minimo controllare dove va il fotone (esso non può lasciare alcuna traccia).

Interferometro di Mach-Zehnder



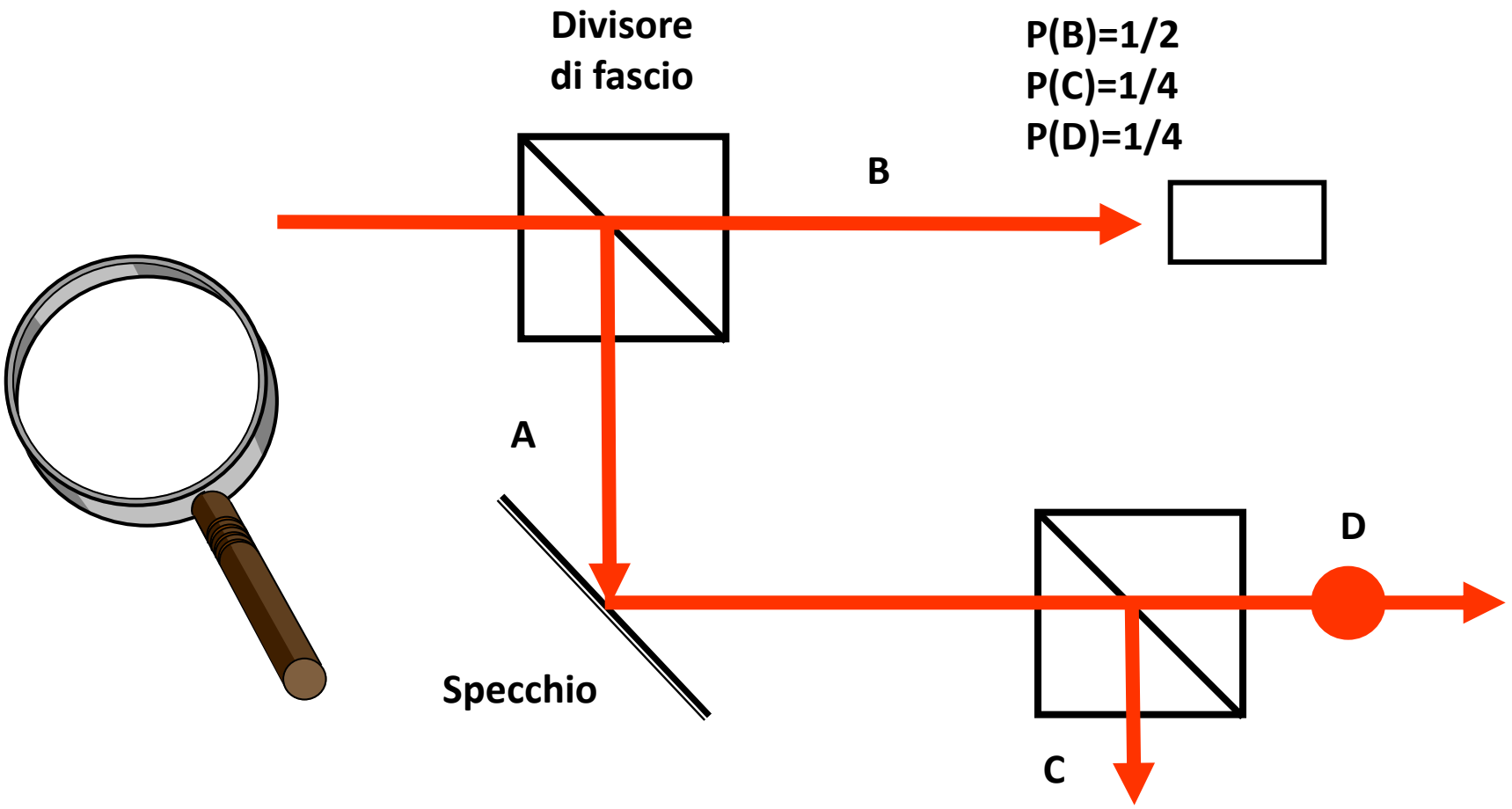
Ispezionare significa al minimo controllare dove va il fotone (esso non può lasciare alcuna traccia).

Interferometro di Mach-Zehnder



Ispezionare significa al minimo controllare dove va il fotone (esso non può lasciare alcuna traccia).

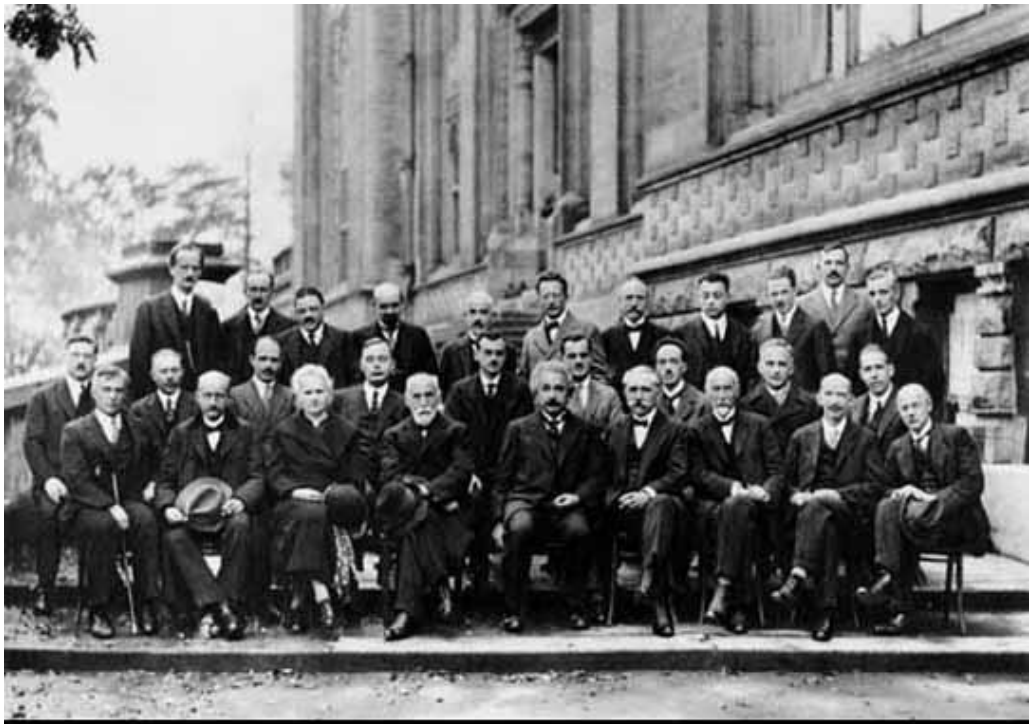
Interferometro di Mach-Zehnder



Il risultato è del tutto diverso dal caso nel quale l'ispezione non avviene. Pertanto, non è possibile alcun tipo di ispezione.

Sovrapposizione Quantistica vs Probabilità

A differenza di un sistema macroscopico classico, la descrizione probabilistica di un esperimento su un singolo quanto **non è una scelta dettata da una mancanza di informazione**, ma da un intrinseca **assenza** di **informazione**.



Scan ©American Institute of Physics

Posizione di A. Einstein

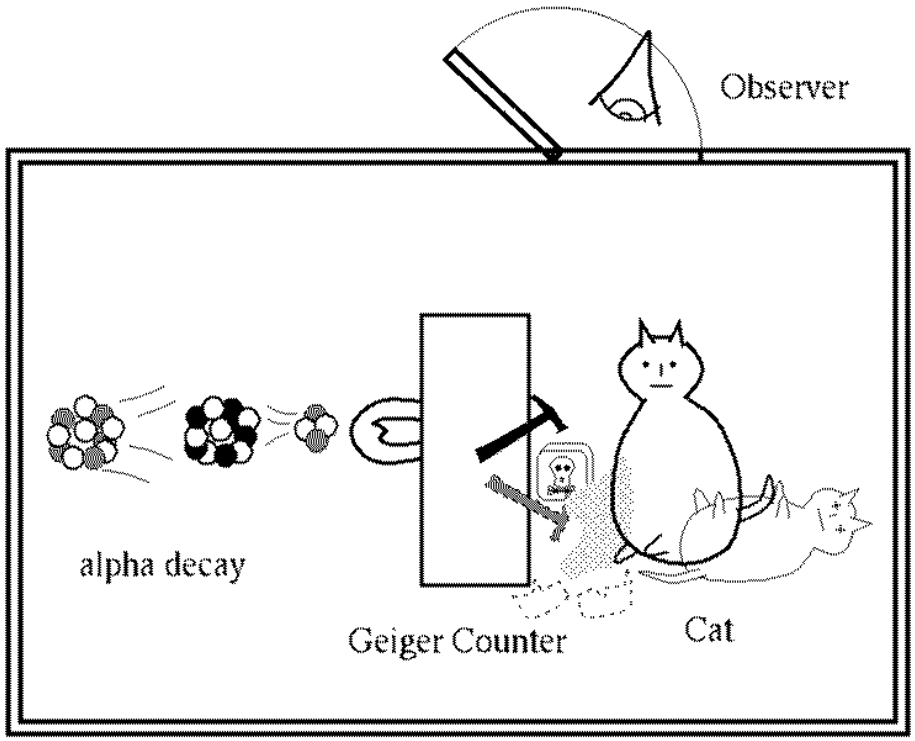
Lorentz:“E’ proprio necessario elevare l’indeterminismo ad un *principio*?”

Einstein:“Che bizarra teoria basata sull’azione a distanza!”

Einstein: “Dovremmo vergognarci, siamo seguaci della regola Gesuitica “Una mano non deve sapere cosa sta facendo l’altra…” ”.
“Caro, o meglio, amato Bohr, non posso rinunciare alla *causalità* ed alla *continuità*.”
“Preferirei essere un calzolaio o meglio un impiegato in una sala d’azzardo che un Fisico.”

Sovrapposizione e collasso sono *paradossali* per Einstein

Schroedinger: aggiunse…



Scopo della tecnologia quantistica…

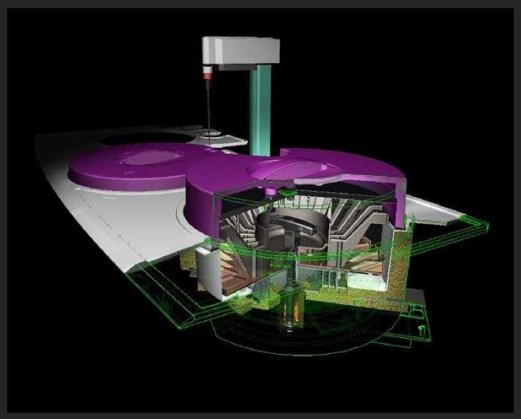
Possiamo ***USARE*** questa “stranezza”, o serve solo a capire qualcosa?

Limite della Fisica

Leggi, grandezze, teorie si devono limitare ad affermazioni che siano sperimentalmente verificabili.

Risultato

La Fisica fornisce sempre tecnologia.



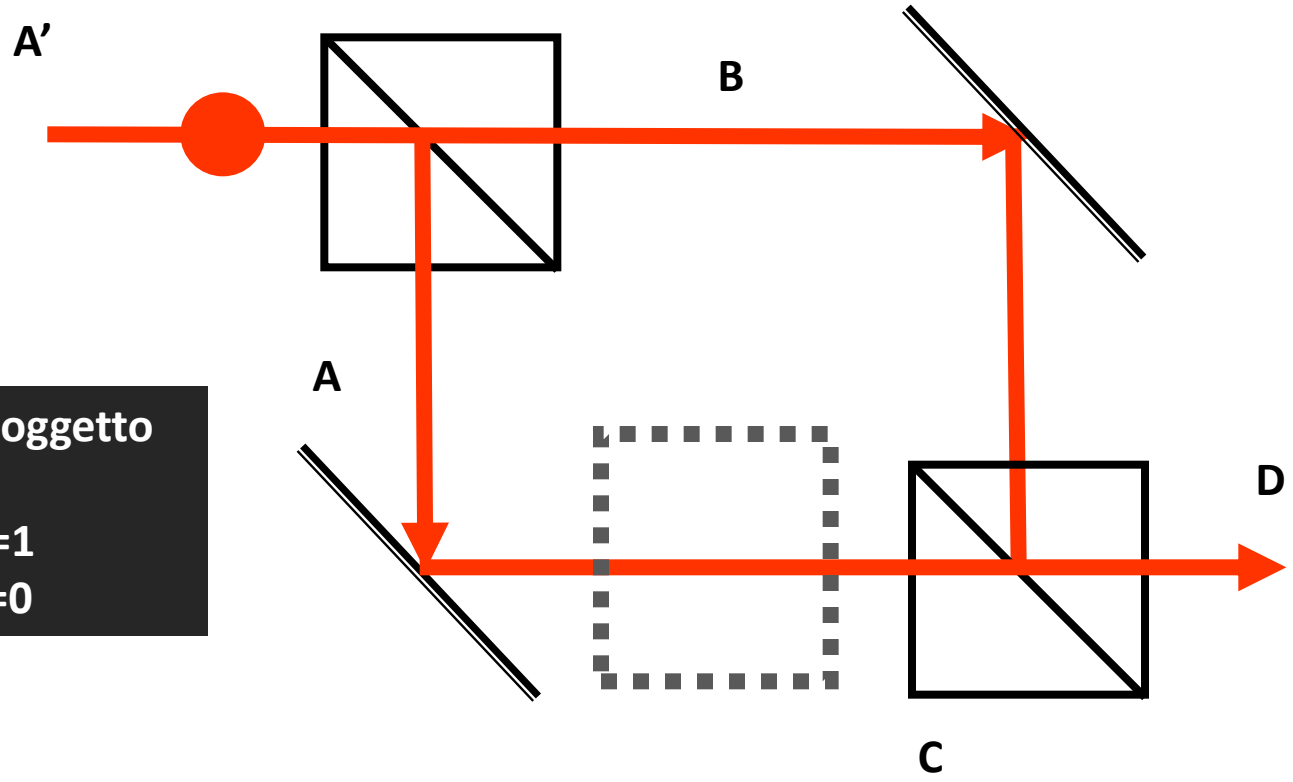
Macchina Classica

Macchina Quantistica

Macchina Complementare di Elitzur e Vaidman

Formulazione – 1993/1994, verifica sperimentale 1995 (De Martini) e 1997 (Zeilinger)

Una macchina capace di **rivelare un oggetto** in una zona dello spazio **senza** che in questa zona penetri **alcuna sonda**.

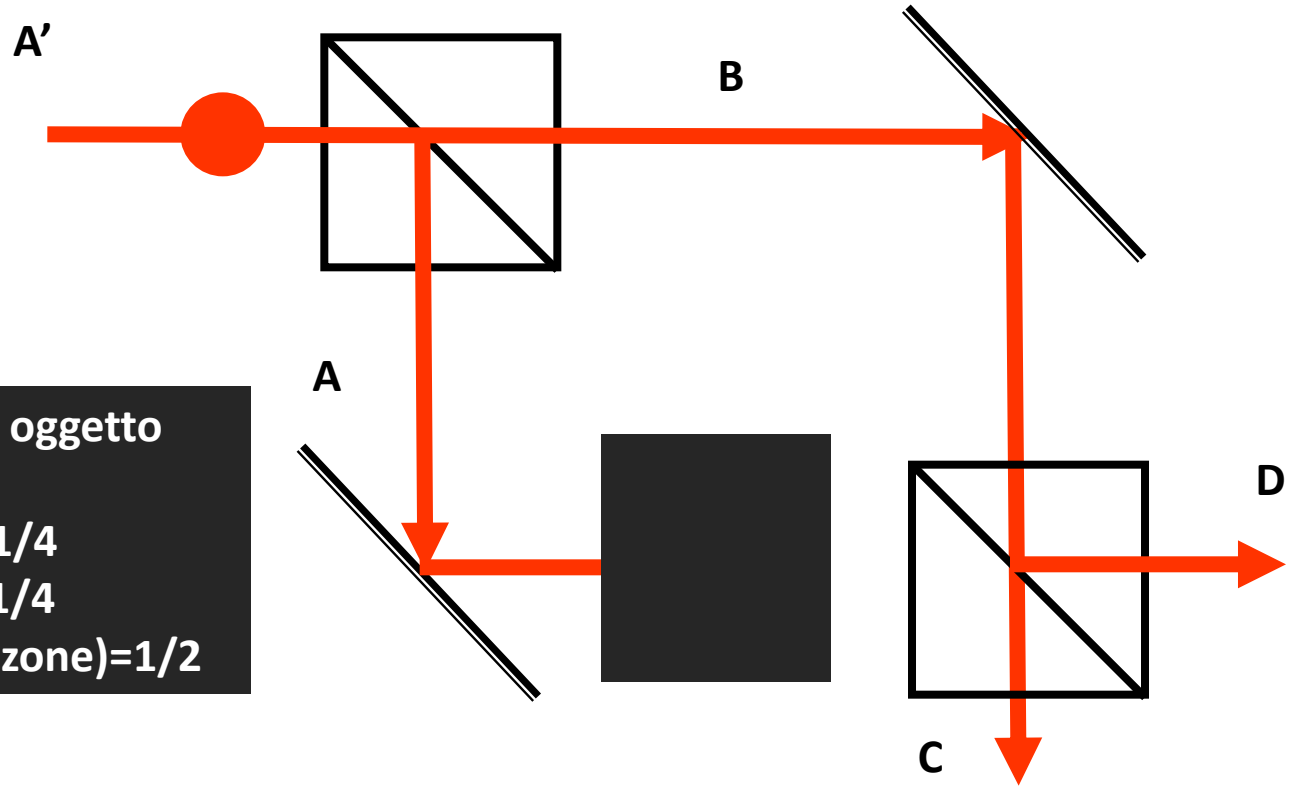


Assenza di oggetto

P(D)=1
P(C)=0

Macchina Complementare di Elitzur e Vaidman

Mentre quando l'oggetto è assente il singolo fotone esce da D, quando è presente, il fotone può anche uscire da C. **Se esce da C rivela la presenza dell'oggetto senza peraltro interagire con esso, essendo uscito e essendo un quanto.**

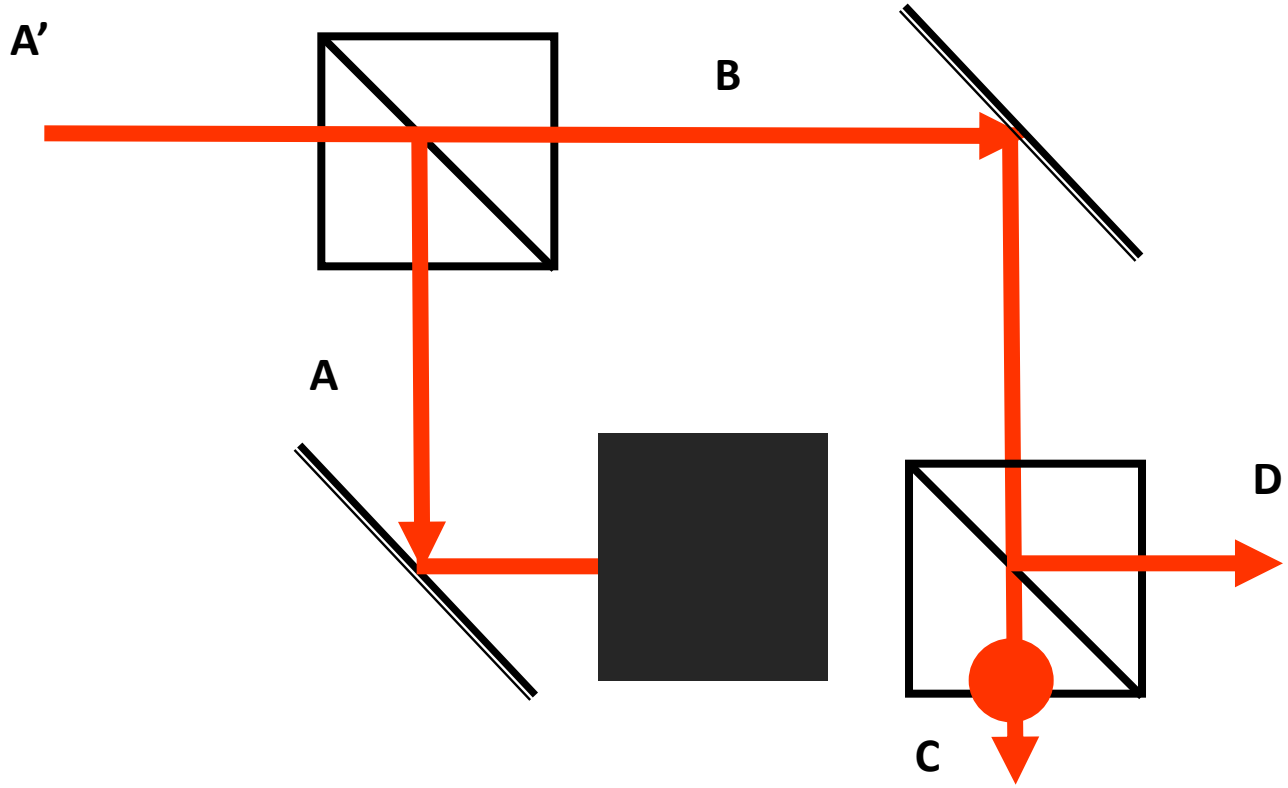


Presenza di oggetto

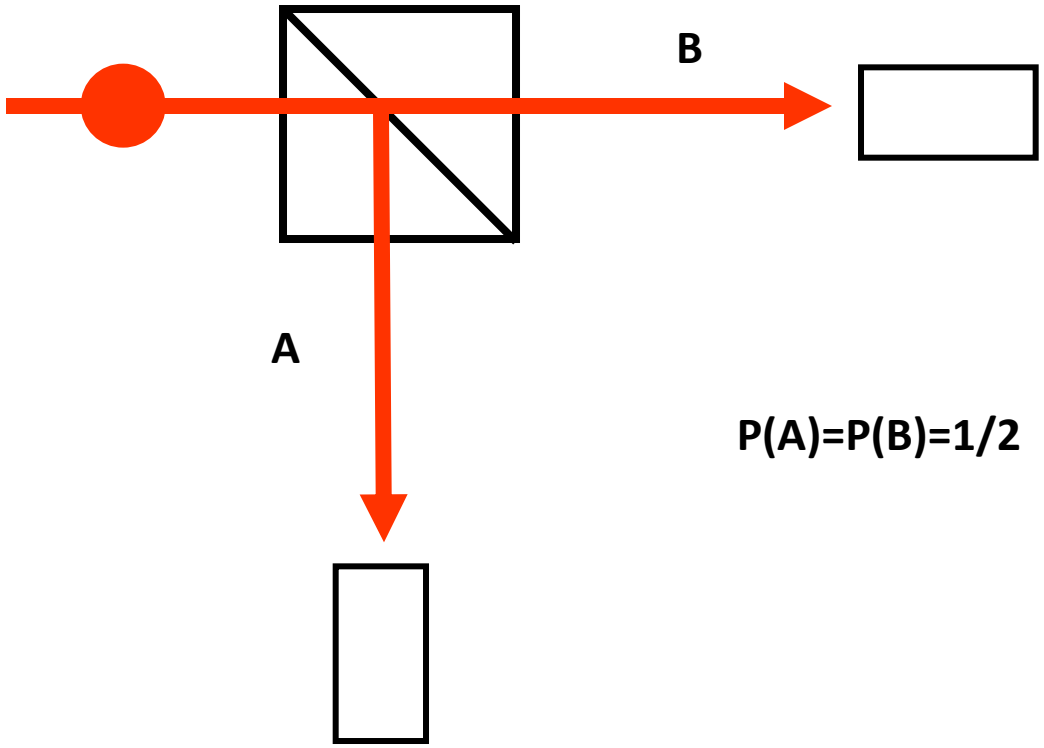
P(D)=1/4
P(C)=1/4
P(A)=P(interazone)=1/2

Macchina Complementare di Elitzur e Vaidman

La macchina funziona da rivelatore di un oggetto senza interazione in ¼ dei casi. Se il fotone esce da D non e' possibile discriminare tra presenza e assenza, ma l'uscita del fotone consente di affermare che se anche ci fosse stato l'oggetto, esso non ha ancora subito interazione, e l'esperimento puo' essere ripetuto (aumentando la probabilità globale di successo a 1/3). Il risultato risulta paradossale per la logica classica macrosopica, ed inaccessibile alle macchine macroscopiche.

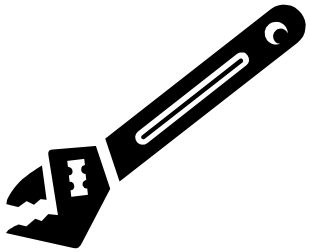


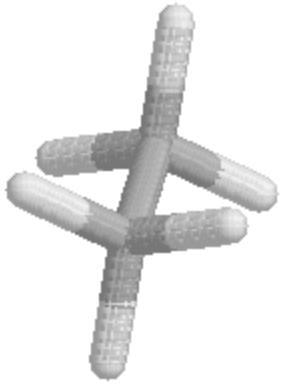
Generatore di numeri random “veri”



P(A)=P(B)=1/2

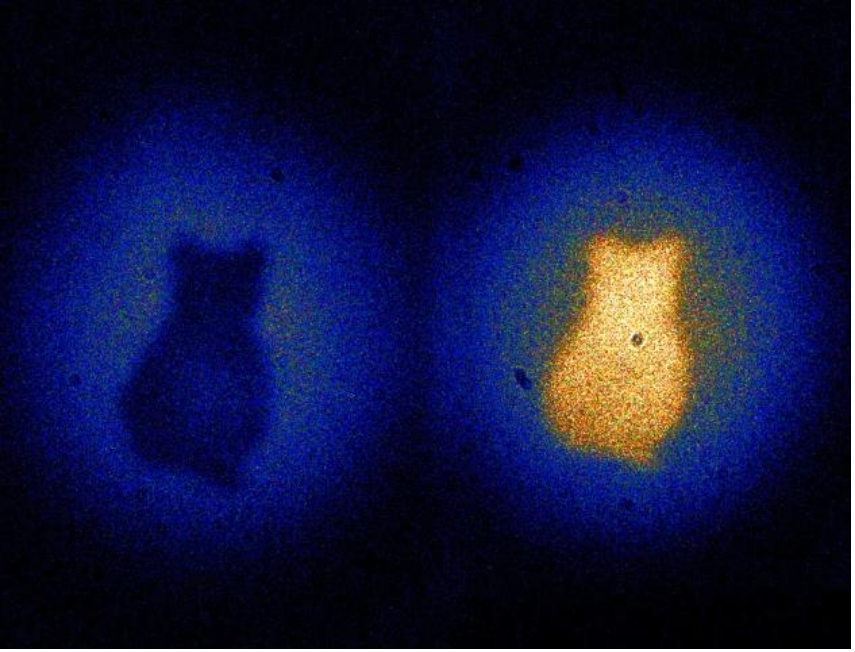
Macchine vs Macchine Quantistiche





Macchina ≠ **Sistema fisico**

Mentre **tutti i sistemi fisici sono quantistici**, le **macchine normali** operano secondo la **logica macroscopica e deterministica**



Macchina *quantistica* o *classica* ?

Probabilità ha qualcosa di **non matematico**

Non riusciamo con un computer, ovvero con la matematica applicata, **a simulare un evento probabilistico**.

E’ strano che riusciamo a capire cosa sia in astratto la probabilita’.

Einstein vs Meccanica Quantistica (1935)

Leggendo un articolo di Popper (1934) sbagliato ("*a gross mistake of which I am ashamed*"), Einstein intuisce che può dimostrare l'*incompletezza* della M.Q. abbandonando la "Scatola Fotonica" (**una sola particella**) in favore dell'utilizzo di ***due particelle microscopiche che hanno avuto una qualche interazione***.

Un quanto… … e un secondo quanto.

Stati ***entangled***.

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)

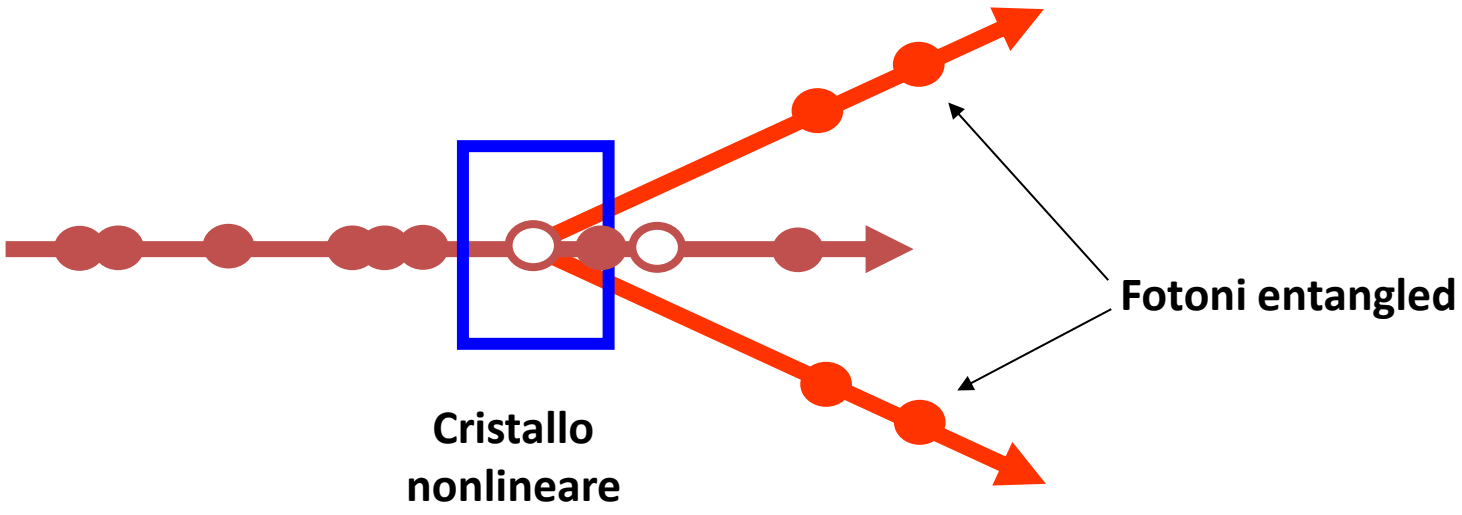
In a complete theory there is an element corresponding to each element of reality. A sufficient condition for the reality of a physical quantity is the possibility of predicting it with certainty, without disturbing the system. In quantum mechanics in the case of two physical quantities described by 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.

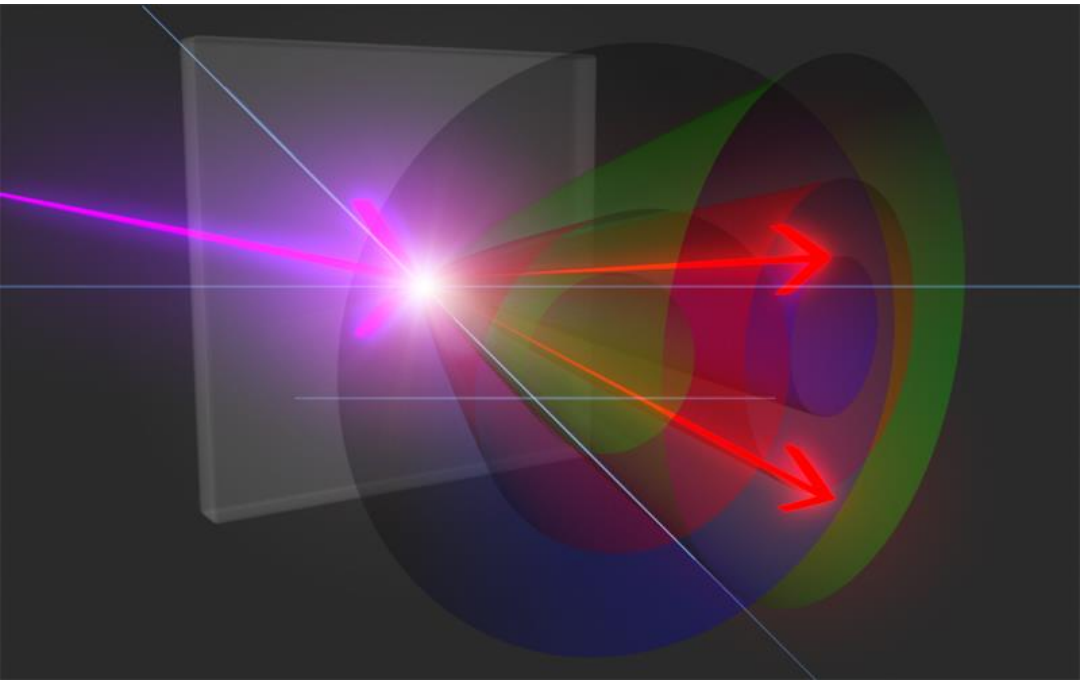
Albert Einstein

Boris Podolsky

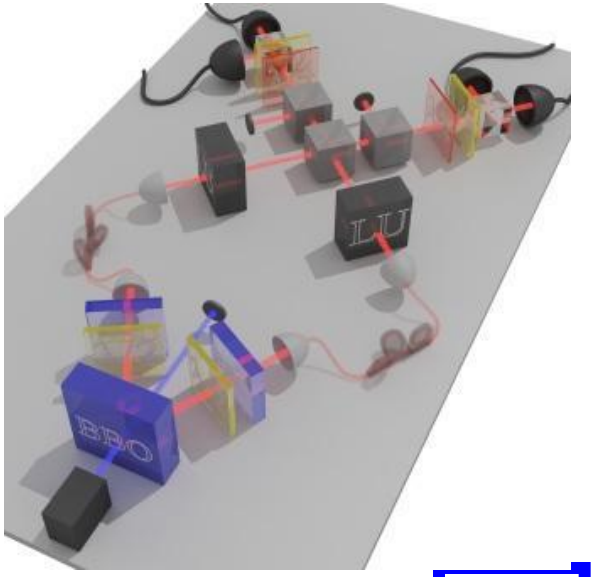
Nathan Rosen

Sorgente di fotoni entangled





Esperimenti di Violazione della Disuguaglianza di Bell



La meccanica quantistica è **valida**, prevede una **azione a distanza superluminale**, che tuttavia **non può essere usata per comunicare**.

Feynman: “Tutto il mistero della M.Q. sta nell’interferometro a singola particella”

Schroedinger: “Il tratto caratteristico della M.Q. è l’entanglement”

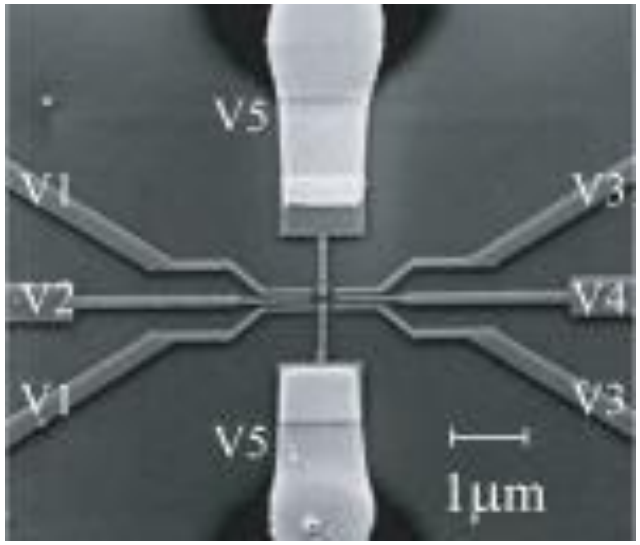
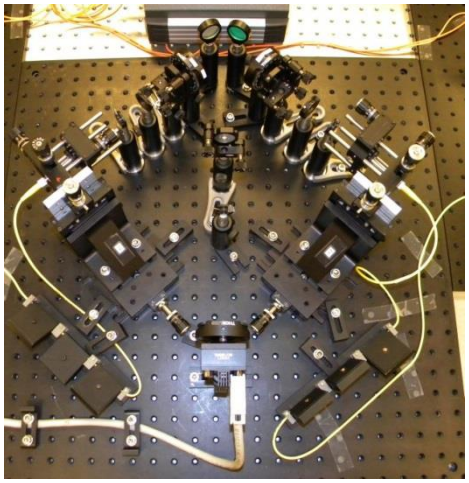
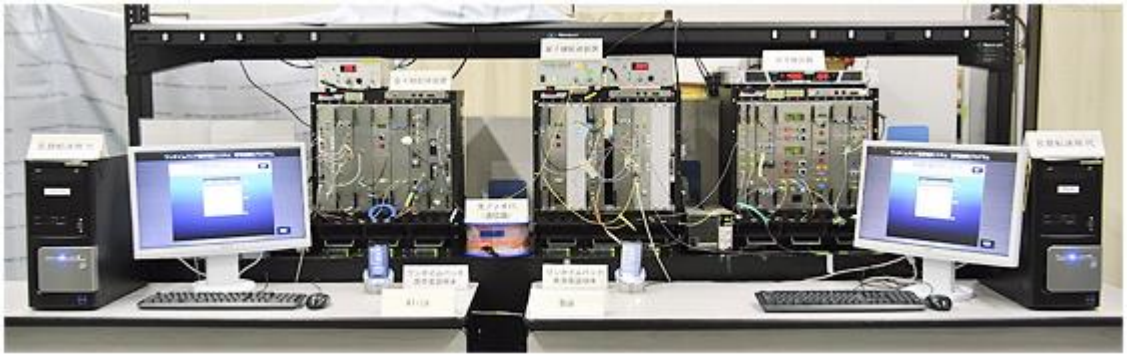


Immagine di una macchina quantistica elettronica (CNOT)



Teletrasportatore fotonico



Macchina crittografica fotonica

Entanglement quale strumento **indispensabile** delle tecnologie moderne

- Crittografia Quantistica (Bennett et al. 1992)
- Teletrasporto Quantistico (Bennett et al. 1993)
- Computazione Quantistica

  (Feynman 1982)

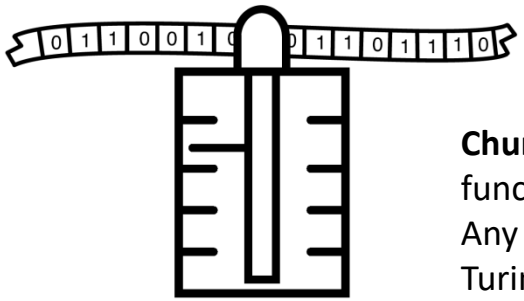
Quantum Computing 1/10

Input → Computation → Output

What can be computed? What system can be realized?!

Information is ***physical***. (Rolf Landauer)

Turing Machine General purpose



Church-Turing thesis: A Turing machine can compute any function computable by a reasonable physical device
Any algorithmic process can be simulated efficiently using a Turing machine.

Quantum Computing 2/10

Computational cost

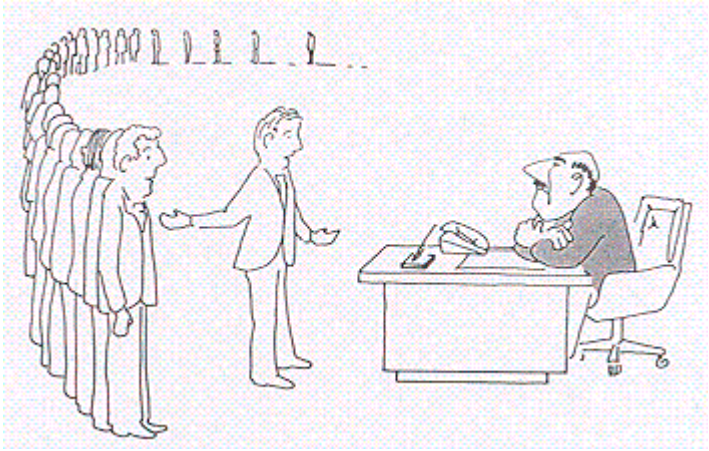
Computational complexity

Resources required (time, space, energy)

n=size of input

Polynomial in ***n***

Easy problems



I can't find an efficient algorithm, but neither can all these other famous people!

Exponential in ***n***

Hard problems

Quantum Computing 3/10

Random computing: TM+random number generator

N bits

Are they 1) all equal; or 2) half «0» and half «1»?

Deterministic: N/2+1 observations

Probabilistic: 100 already gives an error less that ~10^-100

Strong (Modern) Church-Turing thesis: A Probabilistic Turing Machine can simulate any reasonable physical device in polynomial cost.

Quantum Computing 4/10

Analog computers

DNA computer solves NP problems in polynomial time...

...the cost grows exponentially because the number of molecules grows exponentially with the size of the input.

...or exponential precision and noise (no error correction).

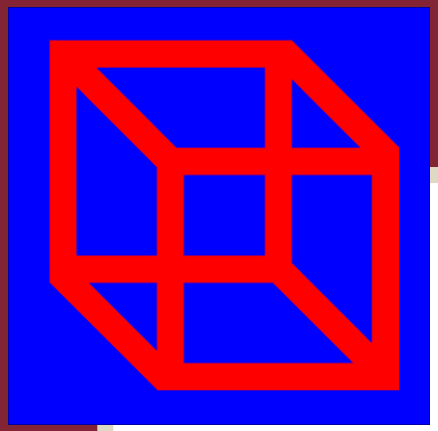
Solution of a 20-Variable 3-SAT Problem on a DNA Computer

Ravinderjit S. Braich,[1] Nickolas Chelyapov,[1] Cliff Johnson,[1] Paul W. K. Rothemund,[2] Leonard Adleman[1]*

A 20-variable instance of the NP-complete three-satisfiability (3-SAT) problem was solved on a simple DNA computer. The unique answer was found after an exhaustive search of more than 1 million (2^{20}) possibilities. This computational problem may be the largest yet solved by nonelectronic means. Problems of this size appear to be beyond the normal range of unaided human computation.

www.sciencemag.org SCIENCE VOL 296 19 APRIL 2002

Quantum Computing 5/10



Quantum Computers

bit 0 1

Computational basis

qubit |+> |0>

|-> |1>

Vector in Hilbert space C^2

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

n qubits $C^2 \otimes C^2 \otimes \cdots \otimes C^2$ 2^n

$$|0\rangle \otimes |0\rangle \otimes \cdots \otimes |0\rangle$$
$$|0\rangle \otimes |0\rangle \otimes \cdots \otimes |1\rangle$$
$$\vdots$$
$$|1\rangle \otimes |1\rangle \otimes \cdots \otimes |1\rangle$$

Quantum Computing 6/10

$$i_1 i_2 ... i_n \longleftrightarrow |i_1\rangle \otimes |i_2\rangle \otimes \cdots \otimes |i_n\rangle \equiv |i_1 .... i_n\rangle$$

$$f : i_1 i_2 ... i_n \longmapsto f(i_1, ... i_n)$$

$$|i_1 i_2 ... i_n\rangle \longmapsto U|i_1 i_2 ... i_n\rangle = |f(i_1, ... i_n)\rangle$$

$$i\hbar \frac{d}{dt}|\Psi(t)\rangle = \mathcal{H}|\Psi(t)\rangle$$

$$|\Psi_f\rangle = \exp\left(-\frac{i}{\hbar}\int \mathcal{H} dt\right)|\Psi_0\rangle = U|\Psi_0\rangle$$

Reversible computation...

Quantum Computing 7/10

Feynman 1982

Quantum system of n particles *seems* exponentially hard to simulate (2^n states).
Quantum computing is looking at this statement in ***reverse***...

Extra resources

$c_0|0\rangle + c_1|1\rangle$ Superposition/Interference

$\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$ Entanglement

Parallelism

Quantum Computing 8/10

Parallelism

(at the same time ***and*** with the same resources)

$$\frac{1}{\sqrt{2^n}} \sum_{i_1,i_2,...,i_n=0}^{1} |i_1, i_2, ..., i_n\rangle$$

$$\frac{1}{\sqrt{2^n}} \sum_{i_1,i_2,...,i_n=0}^{1} |i_1, i_2, ..., i_n\rangle \longmapsto \frac{1}{\sqrt{2^n}} \sum_{i_1,i_2,...,i_n=0}^{1} |f(i_1, i_2, ..., i_n)\rangle$$

2^n

Data

$$f(x) : \{0,1\} \rightarrow \{0,1\}$$

$|x, y\rangle$ U_f

$$|x, y\rangle \rightarrow |x, y \oplus f(x)\rangle$$

Target

Extraction?

Quantum Computing 9/10

Extraction

$$\frac{1}{\sqrt{2^n}} \sum_{i_1,i_2,...,i_n=0}^{1} |i_1, i_2, ..., i_n\rangle \longmapsto \frac{1}{\sqrt{2^n}} \sum_{i_1,i_2,...,i_n=0}^{1} |f(i_1, i_2, ..., i_n)\rangle$$

Collapse of the wavefunction

You need to use interference and restrict outcomes to global properties

Shor's Algorithm 1994: find the prime factors of an integer and solve the discrete logarithm problem

Quantum Fourier Transform $N = 2^n$

$$y_k \equiv \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{2\pi ijk/N} x_j$$

$$|j\rangle \longrightarrow \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{2\pi ijk/2^n} |k\rangle$$

$$N \log(N) = n2^n$$

$$\sum_{j=0}^{2^n-1} x_j |j\rangle \longrightarrow \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} \left[\sum_{j=0}^{2^n-1} e^{2\pi ijk/2^n} x_j \right] |k\rangle = \sum_{k=0}^{2^n-1} y_k |k\rangle$$

$$\log^2(N) = n^2$$

Quantum Computing 10/10

Attacks on Quantum Computing

Decoherence kills it

Threshold theorem (1995)

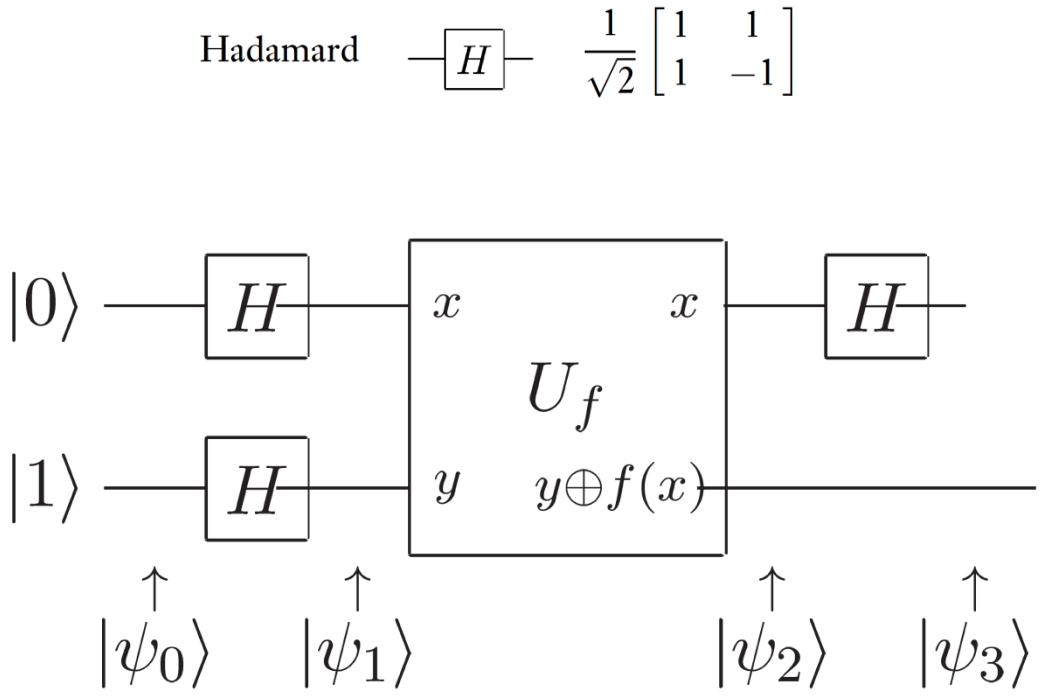
Classical computers can simulate quantum ones

P=NP? Quantum algorithms do not address NP-complete...

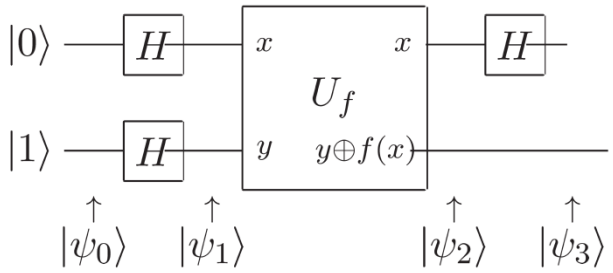
Quantum mechanics is wrong

EPR experiments (1982-)

The Deutsch Algorithm 1/2



The Deutsch Algorithm 2/2



$$|\psi_1\rangle = \left[\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$$

$$|\psi_2\rangle = \begin{cases} \pm\left[\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] & \text{if } f(0) = f(1) \\ \pm\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] & \text{if } f(0) \neq f(1). \end{cases}$$

parallelism

$$|\psi_3\rangle = \begin{cases} \pm|0\rangle\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] & \text{if } f(0) = f(1) \\ \pm|1\rangle\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] & \text{if } f(0) \neq f(1). \end{cases}$$

interference

$$|\psi_3\rangle = \pm|f(0) \oplus f(1)\rangle\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$$

Experimental realizations 1/3

Optical

-Single-photon sources, no photons on demand
-Coherent but no photon-photon interaction

Ion traps

Neutral atom traps

letters to nature

Experimental demonstration of a robust, high-fid… two ion-qubit pl…

might enable faster gate implementation. Here we demonstrate a universal geometric π-phase gate between two beryllium ion-qubits, based on coherent displacements induced by an optical dipole force. The displacements depend on the internal atomic

D. Leibfried*†, B. DeMarco*, V. Meyer*, D. Lucas*‡, M. Barrett*, J. Britton*, W. M. Itano*, B. Jelenković*§, C. Langer*, T. Rosenband*

412

NATURE | VOL 422 | 27 MARCH 2003 | www.nature.com/nature

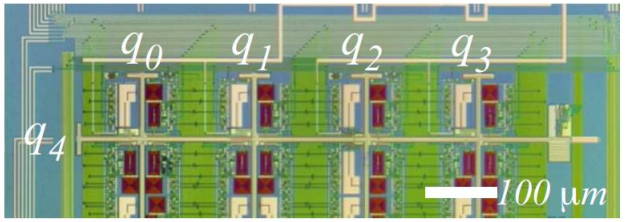
NMR

-Lot's together, no individual control

Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance
Lieven et al. In Nature 414, 883-887 (2001)

Atoms+cavities

Superconducting flux Qubits



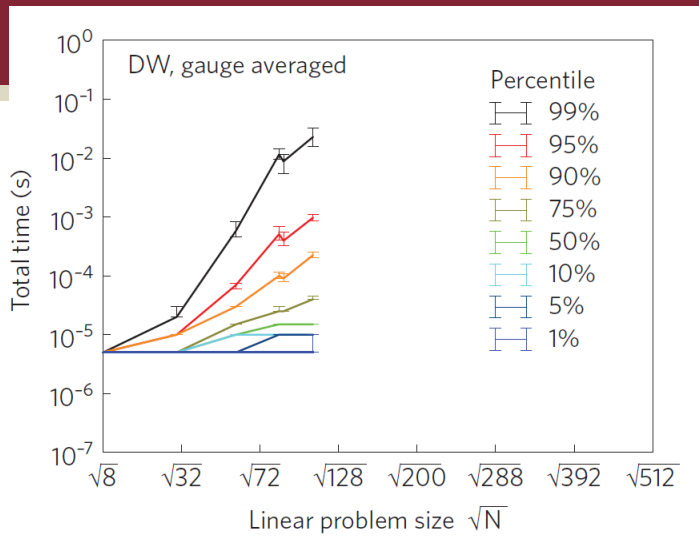
Experimental realizations 2/3

ARTICLES
PUBLISHED ONLINE: 28 FEBRUARY 2014 | DOI: 10.1038/NPHYS2900
nature physics

Evidence for quantum annealing with more than one hundred qubits

Sergio Boixo[1], Troels F. Rønnow[2], Sergei V. Isakov[2], Zhihui Wang[3], David Wecker[4], Daniel A. Lidar[5], John M. Martinis[6] and Matthias Troyer[2]*

Quantum technology is maturing to the point where quantum devices, such as quantum communication systems, quantum random number generators and quantum simulators may be built with capabilities exceeding classical computers. A quantum annealer, in particular, solves optimization problems by evolving a known initial configuration at non-zero temperature towards the ground state of a Hamiltonian encoding a given problem. Here, we present results from tests on a 108 qubit D-Wave One device based on superconducting flux qubits. By studying correlations we find that the device performance is inconsistent with classical annealing or that it is governed by classical spin dynamics. In contrast, we find that the device correlates well with simulated quantum annealing. We find further evidence for quantum annealing in the form of small-gap avoided level crossings characterizing the hard problems. To assess the computational power of the device we compare it against optimized classical algorithms.

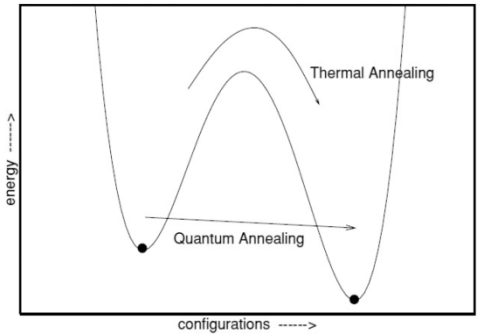


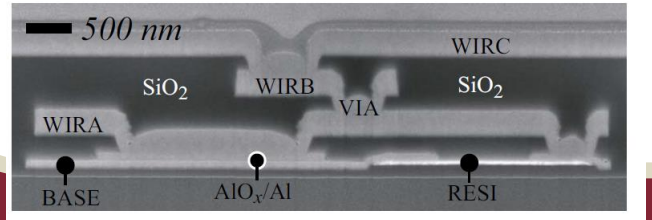
$$H_{\text{Ising}} = -\sum_{i<j} J_{ij}\sigma_i^z\sigma_j^z - \sum_i h_i\sigma_i^z$$

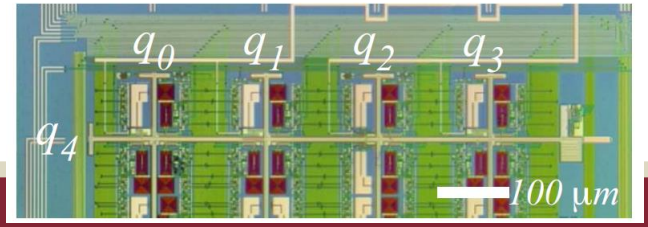
Non-deterministic NP-hard

$$\mathcal{O}(\exp(cN^a))$$

QC: smaller a and c







Experimental realizations 3/3

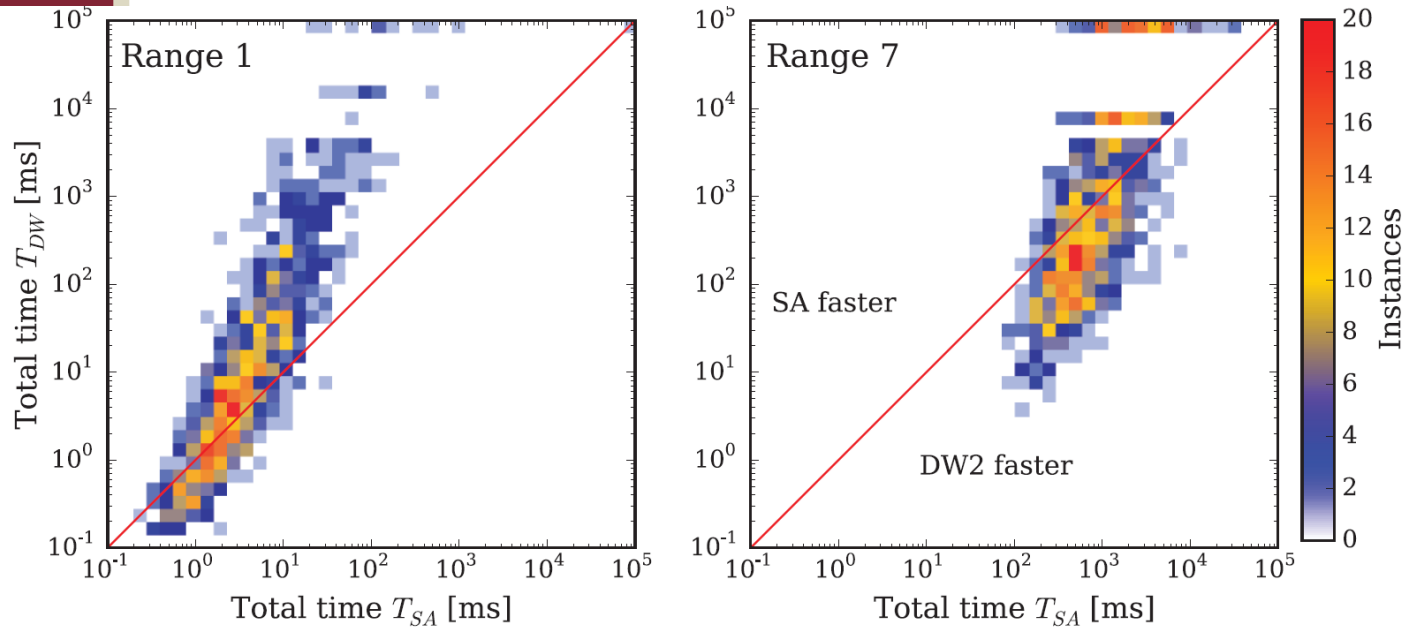
Science
AAAS

Defining and detecting quantum speedup
Troels F. Rønnow *et al.*
Science **345**, 420 (2014);
DOI: 10.1126/science.1252319

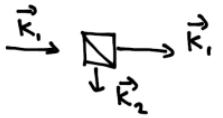
Defining and detecting quantum speedup

Troels F. Rønnow,[1] Zhihui Wang,[2,3] Joshua Job,[3,4] Sergio Boixo,[5,6] Sergei V. Isakov,[7] David Wecker,[8] John M. Martinis,[9] Daniel A. Lidar,[2,3,4,6,10] Matthias Troyer[1]*

The development of small-scale quantum devices raises the question of how to fairly assess and detect quantum speedup. Here, we show how to define and measure quantum speedup and how to avoid pitfalls that might mask or fake such a speedup. We illustrate our discussion with data from tests run on a D-Wave Two device with up to 503 qubits. By using random spin glass instances as a benchmark, we found no evidence of quantum speedup when the entire data set is considered and obtained inconclusive results when comparing subsets of instances on an instance-by-instance basis. Our results do not rule out the possibility of speedup for other classes of problems and illustrate the subtle nature of the quantum speedup question.



Photons and Linear Optics Quantum Computing



$$|\vec{k}_1\rangle \rightarrow \frac{1}{\sqrt{2}}(|\vec{k}_1\rangle + i|\vec{k}_2\rangle)$$

or

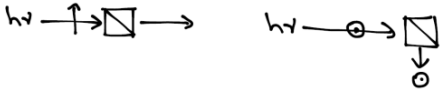
$$|\vec{k}_1\rangle \rightarrow \frac{1}{\sqrt{2}}(|1\rangle_{k_1}|0\rangle_{k_2} + |0\rangle_{k_1}|1\rangle_{k_2})$$

entangled?!

entanglement, interference, superposition....

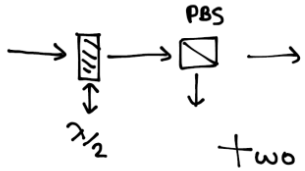
with a single photon – linear optics.

Polarizing Beam-Splitter (PBS)



"1 qubit" is polarization $\leftrightarrow$ data

"1 qubit" is $\vec{k}$ $\leftrightarrow$ target



two degrees of freedom of one single pont.

Dense Coding

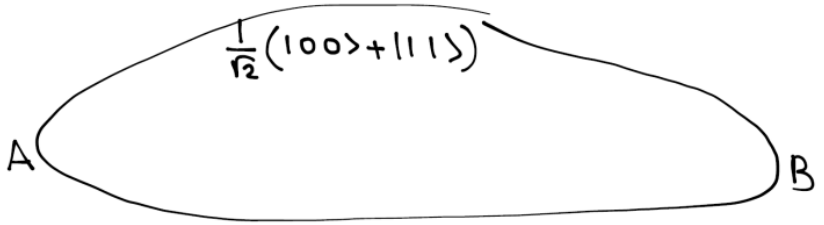
Dense Coding (1992)

How many "bits" can be sent by a single photon?

Alice

Bob

they have never communicated but they share



1) A performs local operations on her particle
2) She sends her particle to Bob

3) Bob measures the state of the two entangled particles

Dense Coding

$I \equiv |0\rangle\langle 0| + |1\rangle\langle 1|$

i) $|0\rangle \to |0\rangle$, $|1\rangle \to |1\rangle$ $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \Rightarrow \frac{00+11}{\sqrt{2}} \longrightarrow \frac{00+11}{\sqrt{2}} = \Phi_+$

or $Y \equiv XZ$ $Z \equiv P(\pi) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{pmatrix}\Big|_{\phi=\pi}$

$|0\rangle \to |1\rangle$, $|1\rangle \to -|0\rangle$ $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \Rightarrow \frac{10-01}{\sqrt{2}} \longrightarrow \frac{10-01}{\sqrt{2}} = \Psi_-$

or $X \equiv |0\rangle\langle 1| + |1\rangle\langle 0|$ (NOT)

$|0\rangle \to |1\rangle$, $|1\rangle \to |0\rangle$ $\Rightarrow \frac{10+01}{\sqrt{2}} = \Psi_+$

or $H \equiv \frac{1}{\sqrt{2}}\left[(|0\rangle + |1\rangle)\langle 0| + (|0\rangle - |1\rangle)\langle 1|\right]$

$|0\rangle \to \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$

$|1\rangle \to \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ $\Rightarrow \frac{00-11}{\sqrt{2}} = \Phi_-$

this is also secure

Bob determines 2 bits from 1 single photon send from Alice!

No cloning

No Cloning (1982)

An unknown quantum state cannot be cloned.

$U(|\alpha\rangle|0\rangle) = |\alpha\rangle|\alpha\rangle$ $\quad U \equiv$ unitary

It must work for any state, hence U ~~α~~

$\Rightarrow U(|\beta\rangle|0\rangle) = |\beta\rangle|\beta\rangle$ for $|\beta\rangle \neq |\alpha\rangle$

If $|\gamma\rangle = \frac{|\alpha\rangle + |\beta\rangle}{\sqrt{2}} \Rightarrow U(|\gamma\rangle|0\rangle) = \frac{1}{\sqrt{2}}(|\alpha\rangle|\alpha\rangle + |\beta\rangle|\beta\rangle) \neq |\gamma\rangle|\gamma\rangle$

Q.E.D.

Quantum Teleportation

Quantum Teleportation (1993)

Can you transmit an unknown state of a qubit without sending it?

A B

$a|+\rangle + b|-\rangle$

$$\frac{|+\rangle_2|+\rangle_3 + |-\rangle_2|-\rangle_3}{\sqrt{2}}$$

$2 \leftarrow \quad \rightarrow 3$

$$|+\rangle_1|+\rangle_2(a|+\rangle_3+b|-\rangle_3)+|+\rangle_1|-\rangle_2(a|-\rangle_3+b|-\rangle_3)+|-\rangle_1|+\rangle_2(a|+\rangle_3-b|-\rangle_3)+$$
$$+|-\rangle_1|-\rangle_2(a|-\rangle_3-b|+\rangle_3)$$

A measures 1,2, sends the bits to B, who knows which unitary operation to enact on 3 to get the original unknown state.

Quantum Key Distribution

Quantum Key Distribution (1984)

A

1) chooses a basis

S_x , S_z

2) encodes a random bit

S_x S_x S_z S_x S_z
\+ + - - +

3) A declares publicly the basis.

B

1) measures a basis

S_x , S_z

2) reads the bits

S_z S_z S_z S_x S_x
× × - - ×

3) Bob informs which slots are OK

4) tampering is checked by publicly comparing a subset of OK slots

SAPIENZA
UNIVERSITÀ DI ROMA