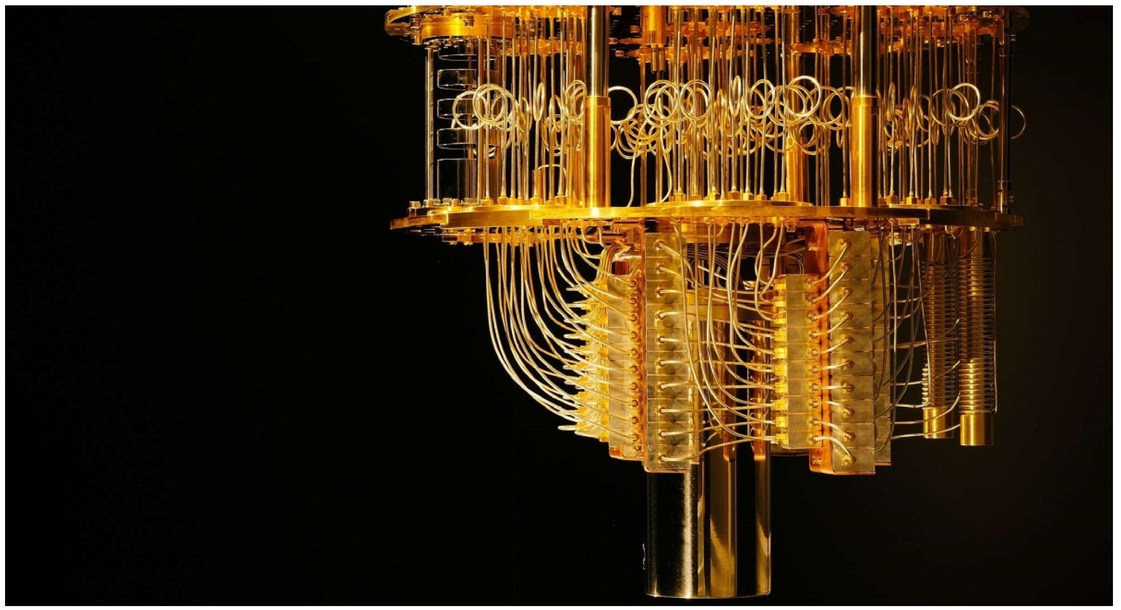
Tecnologie quantistiche

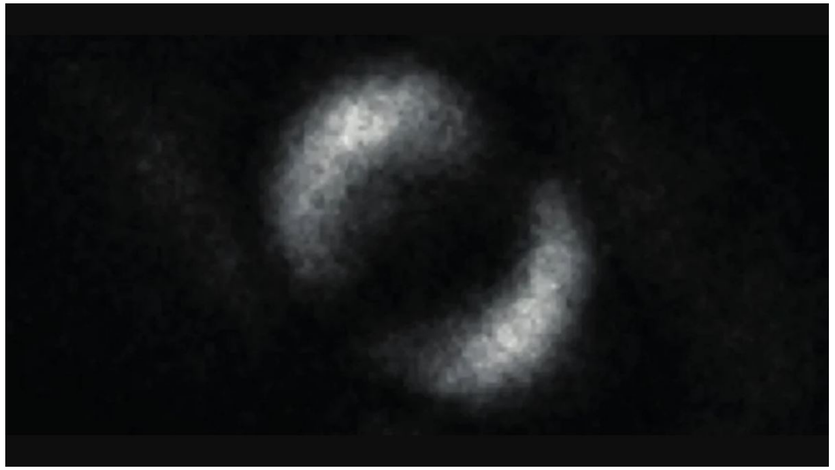
Didattica della fisica quantistica



PLS 2020-2021 - Università degli studi di Pavia - Fisica

Chiara Macchiavello
Lidia Falomo
Massimiliano Malgieri
Claudio Sutrini

Entanglement



"The entanglement is the characteristic trait of Quantum Mechanics, the one that enforces its entire departure from classical line of thoughts." (E. Schroedinger, 1935)

"The deep ways that quantum information differs from classical information involve the properties, implications, and uses of quantum entanglement." (J. Preskill, 2009)

Test telepatici

Alice e Bob si definiscono telepatici e accettano di dimostrarlo sottoponendosi ad un test sotto l'attenta osservazione di due giudici.

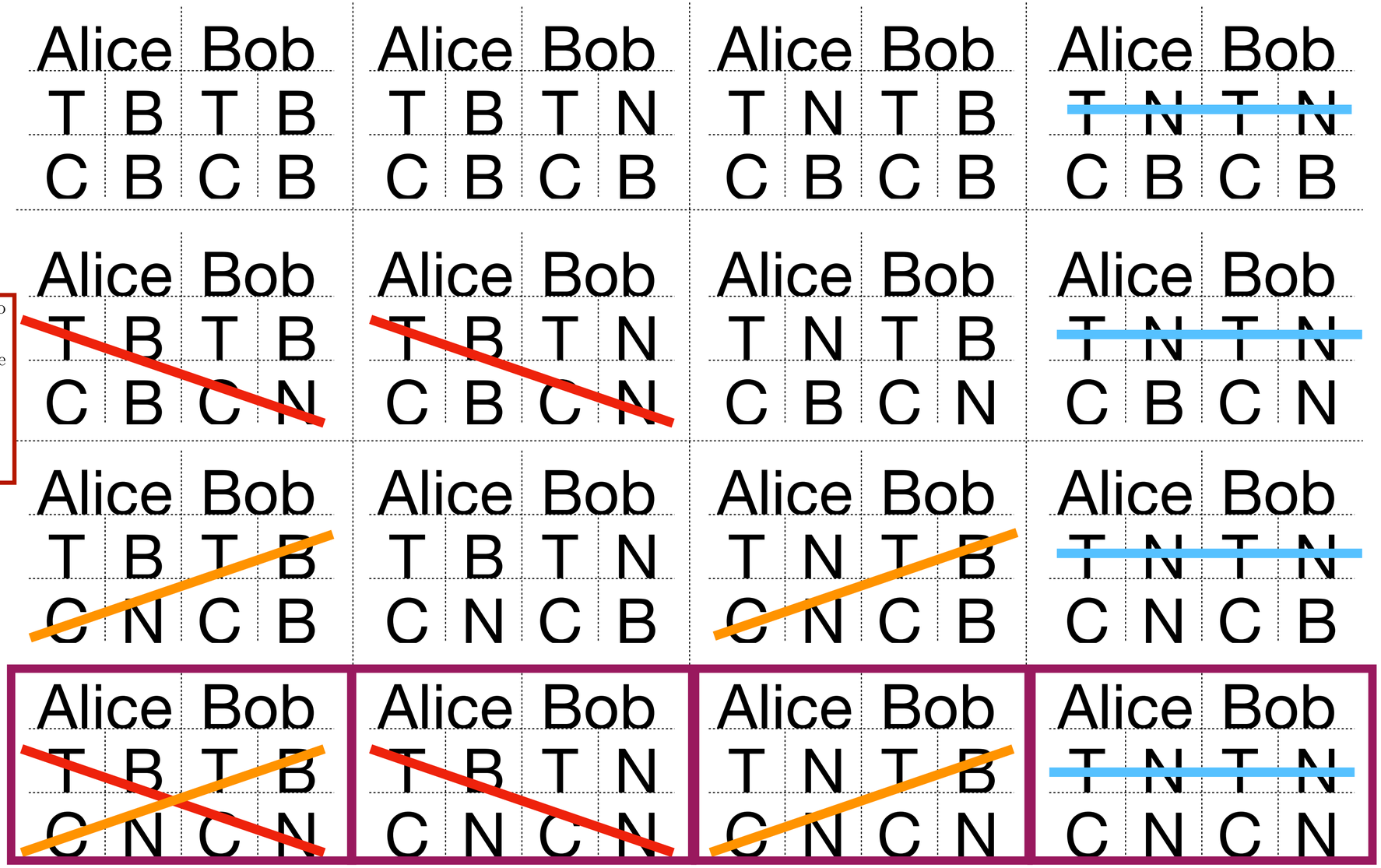
Per prima cosa A e B concordano un insieme di regole insieme ai giudici: le regole sono decise in modo tale che i due possano, secondo l'idea dei giudici, vincere solamente se effettivamente sono telepatici. Una vittoria rappresenterebbe dunque la dimostrazione della loro telepatia; una sconfitta, la dimostrazione del loro inganno.

Protocollo d'intesa:

1. Alice e Bob sono in due camere separate senza possibilità di comunicare in presenza di due arbitri anch'essi impossibilitati a comunicare.
2. Ciascuno degli arbitri lancia una moneta annunciando il risultato: *Testa* o *Croce*.
3. Ciascuno dei due psichici annuncia *Bianco* o *Nero*.
4. Alice e Bob vincono tutte le volte che entrambe le monete sono *Croce* e entrambi rispondono *Nero*.
5. Alice e Bob perdono se una qualsiasi delle loro risposte corrisponde a una delle seguenti accoppiate:
   (a) *Nero-Nero* in risposta a *Testa-Testa*.
   (b) *Nero-Bianco* in risposta a *Croce-Testa*.
   (c) *Bianco-Nero* in risposta a *Testa-Croce*.
6. Se gli psichici vincono almeno 20 volte su 4000 riceveranno un milione di euro

Test telepatici

4. Alice e Bob vincono tutte le volte che entrambe le monete sono *Croce* e entrambi rispondono *Nero*.
5. Alice e Bob perdono se una qualsiasi delle loro risposte corrisponde a una delle seguenti accoppiate:
   (a) *Nero-Nero* in risposta a *Testa-Testa*.
   (b) *Nero-Bianco* in risposta a *Croce-Testa*.
   (c) *Bianco-Nero* in risposta a *Testa-Croce*.



Test telepatici

Protocollo d'intesa:

1. Alice e Bob sono in due camere separate senza possibilità di comunicare in presenza di due arbitri anch'essi impossibilitati a comunicare.
2. Ciascuno degli arbitri lancia una moneta annunciando il risultato: *Testa* o *Croce*.
3. Ciascuno dei due psichici annuncia *Bianco* o *Nero*.
4. Alice e Bob vincono tutte le volte che entrambe le monete sono *Croce* e entrambi rispondono *Nero*.
5. Alice e Bob perdono se una qualsiasi delle loro risposte corrisponde a una delle seguenti accoppiate:
   (a) *Nero-Nero* in risposta a *Testa-Testa*.
   (b) *Nero-Bianco* in risposta a *Croce-Testa*.
   (c) *Bianco-Nero* in risposta a *Testa-Croce*.
6. Se gli psichici vincono almeno 20 volte su 4000 riceveranno un milione di euro

Classicamente, a meno che Alice e Bob non siano davvero telepatici, le probabilità di vincere sono estremamente basse!

Test telepatici

Alice e Bob si presentano ai giudici ciascuno con 4000 scatole dette *MEMORIA* e una detta *HADAMARD.* Nulla nelle regole stabilite lo vieta. I giudici si assicurano in ogni caso che tali scatole non permettano ad Alice e Bob di comunicare. Accertato questo, decidono di far proseguire la sfida.

In realtà ciascuna delle scatole di Alice e Bob contiene una pallina della coppia entangled dello stato

$$|\psi\rangle = \frac{|00\rangle + |01\rangle + |10\rangle}{\sqrt{3}}$$

Vediamo come, sfruttando queste due scatole, potranno vincere la sfida.

In effetti A e B hanno deciso di codificare con 0 il colore *bianco* e con 1 il colore *nero.*

A condizione di mantenere le scatole ben chiuse e isolate, lo stato entangled permane anche se Alice e Bob si allontanano per entrare nelle loro rispettive stanze.

Vediamo ora come agiscono Alice e Bob a seconda dell'esito del lancio della moneta dei giudici.

Test telepatici

Alice-Testa e Bob-Testa Nel caso in cui i due lanci di moneta diano entrambi esito *Testa*, Alice e Bob liberano una pallina ciascuno dalla propria scatola di *MEMORIA* e ne osservano (misurano) il colore.
Dunque osservando lo stato

$$|\psi\rangle = \frac{|00\rangle + |01\rangle + |10\rangle}{\sqrt{3}}$$

esso fornirà una delle seguenti coppie di bit classici

$$0,0 \quad o \quad 0,1 \quad o \quad 1,0$$

ciascuno con probabilità $1/3$. Dunque si potranno presentare i seguenti casi, ciascuno con probabilità $1/3$:

1. Alice osserva B e Bob B
2. Alice osserva B e Bob N
3. Alice osserva N e Bob B

ma in ogni caso mai la combinazione NN, unica non concessa dalle regole.

Al termine del test mostreremo un circuito in grado di realizzare lo stato.

Non possono vincere, ma agendo in questo modo non possono perdere.

4. Alice e Bob vincono tutte le volte che entrambe le monete sono *Croce* e entrambi rispondono *Nero*.
5. Alice e Bob perdono se una qualsiasi delle loro risposte corrisponde a una delle seguenti accoppiate:
   (a) *Nero-Nero* in risposta a *Testa-Testa*.
   (b) *Nero-Bianco* in risposta a *Croce-Testa*.
   (c) *Bianco-Nero* in risposta a *Testa-Croce*.

Test telepatici

4. Alice e Bob vincono tutte le volte che entrambe le monete sono *Croce* e entrambi rispondono *Nero*.
5. Alice e Bob perdono se una qualsiasi delle loro risposte corrisponde a una delle seguenti accoppiate:
   (a) *Nero-Nero* in risposta a *Testa-Testa*.
   (b) *Nero-Bianco* in risposta a *Croce-Testa*.
   (c) *Bianco-Nero* in risposta a *Testa-Croce*.

Alice-Testa e Bob-Croce Analogo

Alice-Croce e Bob-Testa Se nella stanza di Alice il giudice lancia la moneta ed esce *Croce*, Alice usa la scatola *HADAMARD* dopo la scatola *MEMORIA*, Bob osserva semplicemente la sua pallina:

$$|\psi\rangle = \frac{|00\rangle + |01\rangle + |10\rangle}{\sqrt{3}} \xrightarrow{H \otimes I}$$

$$\xrightarrow{H \otimes I} \frac{1}{\sqrt{3}} \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}} \right) |0\rangle + \frac{1}{\sqrt{3}} \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}} \right) |1\rangle + \frac{1}{\sqrt{3}} \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) |0\rangle =$$

$$= \frac{2}{\sqrt{2}\sqrt{3}} |00\rangle + \frac{1}{\sqrt{2}\sqrt{3}} |01\rangle + \frac{1}{\sqrt{2}\sqrt{3}} |11\rangle$$

Non possono vincere, ma agendo in questo modo non possono perdere.

Il ruolo della Hadamard è quello di creare interferenza in modo da annullare l'effetto dello stato $|10\rangle$, proibito dalle regole.

La misura effettuata su questo stato dà:

1. Alice osserva B e Bob B con probabilità $p = 2/3$
2. Alice osserva B e Bob N con probabilità $p = 1/6$
3. Alice osserva N e Bob N con probabilità $p = 1/6$

risposte tutte valide secondo le regole.

Test telepatici

Alice-Croce e Bob-Croce Questo è il caso più interessante perché quello che permette ad Alice e Bob di vincere il premio. In questo caso sia Alice che Bob usano la scatola *HADAMARD* dopo quella *MEMORIA*:

$$|\psi\rangle = \frac{|00\rangle + |01\rangle + |10\rangle}{\sqrt{3}} \xrightarrow{H \otimes H}$$

$$\xrightarrow{H \otimes H} \frac{1}{\sqrt{3}} \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + |1\rangle}{\sqrt{2}} \right) + \frac{1}{\sqrt{3}} \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) +$$

$$+ \frac{1}{\sqrt{3}} \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + |1\rangle}{\sqrt{2}} \right) =$$

$$= \ldots = \frac{3}{2\sqrt{3}} |00\rangle + \frac{1}{2\sqrt{3}} |01\rangle + \frac{1}{2\sqrt{3}} |10\rangle - \frac{1}{2\sqrt{3}} |11\rangle$$

4. Alice e Bob vincono tutte le volte che entrambe le monete sono *Croce* e entrambi rispondono *Nero*.
5. Alice e Bob perdono se una qualsiasi delle loro risposte corrisponde a una delle seguenti accoppiate:
   (a) *Nero-Nero* in risposta a *Testa-Testa*.
   (b) *Nero-Bianco* in risposta a *Croce-Testa*.
   (c) *Bianco-Nero* in risposta a *Testa-Croce*.

Test telepatici

Alice-Croce e Bob-Croce

$$= \ldots = \frac{3}{2\sqrt{3}} |00\rangle + \frac{1}{2\sqrt{3}} |01\rangle + \frac{1}{2\sqrt{3}} |10\rangle - \frac{1}{2\sqrt{3}} |11\rangle$$

Effettuando la misura di questo stato:

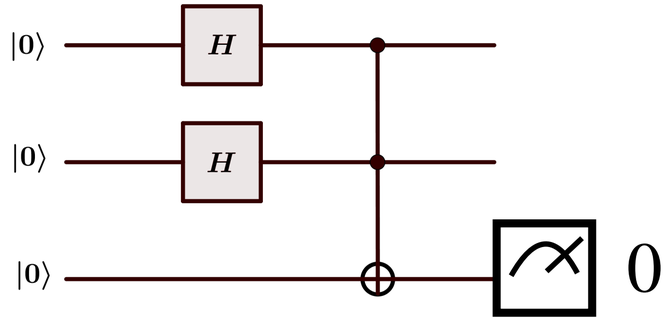
1. Alice osserva B e Bob B con probabilità $p = 9/12$
2. Alice osserva B e Bob N con probabilità $p = 1/12$
3. Alice osserva N e Bob B con probabilità $p = 1/12$
4. Alice osserva N e Bob N con probabilità $p = 1/12$

Siamo proprio nel caso che permette a Alice e Bob di vincere. Nessuna delle combinazioni è vietata dalle regole e l'ultima permette ai due di vincere!!

Alice e Bob telepatici

Test telepatici

Esercizio: dimostrare che al termine del circuito se effettuando una misurazione sul terzo qubit otteniamo 0, allora Alice e Bob avrebbero lo stato entangled condiviso all'inizio del test.



$$|\psi\rangle = \frac{|00\rangle + |01\rangle + |10\rangle}{\sqrt{3}}$$

CHSH game

CHSH game[20] Come nel caso precedente consideriamo Alice e Bob posti in luoghi sufficientemente lontani dello spazio o comunque non in grado di comunicare in modo classico. Immaginiamo sempre che ci siano due giudici uno con Alice e uno con Bob e che anch'essi non possano comunicare, né siano d'accordo in altro modo. Ciascuno dei due giudici lancia una moneta e fornisce l'esito del lancio. Chiameremo x e y gli esiti del lancio della moneta rispettivamente per Alice e per Bob dove ovviamente $x \in \{0, 1\}$ e $y \in \{0, 1\}$. A questo punto anche Alice e Bob dovranno comunicare ai giudici la scelta di un valore tra due possibili; chiameremo tali valori a e b con l'analoga convenzione che $a \in \{0, 1\}$ e $b \in \{0, 1\}$. Alice e Bob vincono se

$$a \oplus b = x \wedge y$$

altrimenti perdono.

CHSH game

Se Alice e Bob giocano classicamente senza la possibilità di scambiarsi informazioni hanno la probabilità massima di vincere pari a $3/4$ ottenuta implementando la seguente la procedura:

1. Bob risponde sempre con $b = 0$
2. Se il giudice di Alice dice $x = 0$ risponde $a = 0$. In questo caso Alice e Bob vincono con probabilità 1.
3. Se il giudice di Alice dice $x = 1$ Alice deve scegliere tra 0 e 1, non sapendo cosa abbia ottenuto il giudice di Bob. In questo caso Alice e Bob vincono con probabilità $1/2$.

Classicamente dunque, la probabilità con cui Alice e Bob vincono è dunque

$$1 \cdot \frac{1}{2} + \frac{1}{2} \cdot \frac{1}{2} = \frac{3}{4} = 75\%$$

x	**y**	$x \wedge y$
0	0	0
0	1	0
1	0	0
1	1	1

a	**b**	$a \oplus b$
0	0	0
0	1	1
1	0	1
1	1	0

La scelta a = b permette di vincere nel 75 % dei casi.

CHSH game

Vediamo ora come Alice e Bob possono aumentare la probabilità di vincere senza comunicare, ma sfruttando le correlazioni non locali degli stati entangled.
Alice e Bob prima di essere allontanati condividono uno stato entangled corrispondente ad uno degli stati di Bell:

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

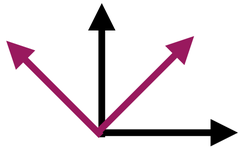
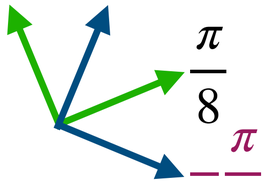
A questo punto ciascuno porta con sé uno dei due qubit che formano lo stato entangled, rispettivamente il primo e il secondo. La procedura adottata da Alice e Bob sarà la seguente:

	Alice	$a \oplus b = x \wedge y$	**Bob**
Input	x		y
Output	a	$Se\ x = y = 1 \longrightarrow a \neq b$ $Altrimenti\ a = b$	b

a e b sono scelti da Alice e Bob in base agli esiti delle misurazioni dello stato $|\psi\rangle$

Scegliendo, ad esempio, a = b = 0 si vince nel 75 % dei casi.

CHSH game

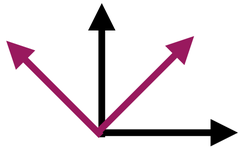
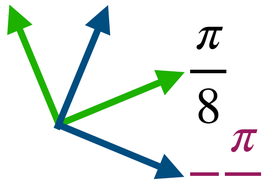
	Alice	Bob
Input	x=0 x=1	y=0 y=1
Basi	 $\{a_0, a_1\}$	 $\{b_0, b_1\}$
Esiti misurazioni nelle due basi	$\{a_{i,0}, a_{i,1}\}$	$\{b_{i,0}, b_{i,1}\}$

x	y
0	0
0	1
1	0
1	1

a	b
$a_{i,0}$	$b_{i,0}$
$a_{i,0}$	$b_{i,1}$
$a_{i,1}$	$b_{i,0}$
$a_{i,1}$	$b_{i,1}$

La condizione che Alice e Bob vincono se a=b si traduce nella probabilità che gli esiti delle misurazioni nelle quattro diverse basi (due per Alice e due per Bob) siano gli stessi per i primi tre casi: $P_{same}(a_{i,k}, b_{j,k})$; diversi nell'ultimo.

CHSH game

	Alice	Bob
Input	x=0 x=1	y=0 y=1
Basi	 $\{a_0, a_1\}$	 $\{b_0, b_1\}$
Esiti misurazioni nelle due basi	$\{a_{i,0}, a_{i,1}\}$	$\{b_{i,0}, b_{i,1}\}$

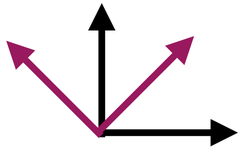
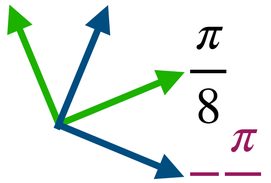
$$|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$ è invariante per rotazioni!!!

La probabilità dipende dall'angolo tra le due basi

Alice misura nella base $\{a_0\}$ e lo stato collassa in una delle due possibilità.
Supponiamo ottenga 0: allora lo stato di Bob collassa in $|00\rangle$

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \xrightarrow{A(a_0)} |00\rangle \xrightarrow{B(b_0)} 0 \text{ con probabilità } cos^2(\pi/8)$$

CHSH game

	Alice	Bob
Input	x=0 x=1	y=0 y=1
Basi	 $\{a_0, a_1\}$	 $\{b_0, b_1\}$
Esiti misurazioni nelle due basi	$\{a_{i,0}, a_{i,1}\}$	$\{b_{i,0}, b_{i,1}\}$

x	y
0	0
0	1
1	0
1	1

a	b
a_0	b_0
a_0	b_1
a_1	b_0
a_1	b_1

$$P = cos^2(\pi/8)$$
$$P = cos^2(\pi/8)$$
$$P = cos^2(\pi/8)$$
$$P = cos^2(3\pi/8) = sin^2(\pi/8)$$

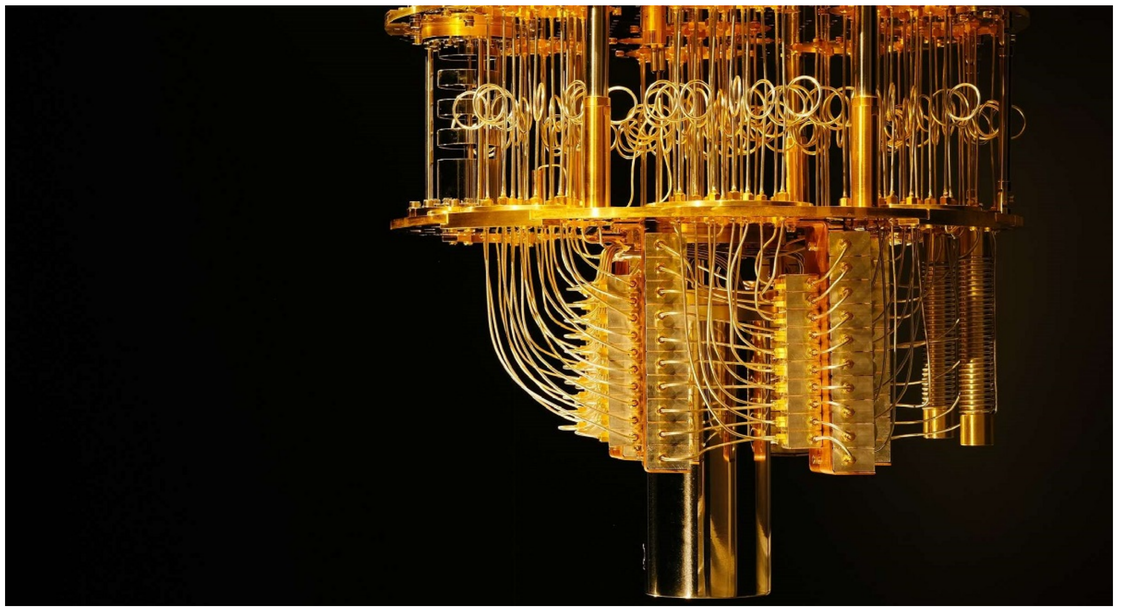
$$P_{same}(a_{i,k}, b_{j,k}) = cos^2(\pi/8) = 85\,\%$$

Teorema di Bell

$$P_{diff} = 1 - sin^2(\pi/8) = cos^2(\pi/8) = 85\,\%$$

Tecnologie quantistiche

Fine...



PLS 2020-2021 - Università degli studi di Pavia - Fisica

Chiara Macchiavello
Lidia Falomo
Massimiliano Malgieri
Claudio Sutrini

Bibliografia

Abramsky https://people.maths.ox.ac.uk/tillmann/SA-CAT17L1.pdf

Benenti, G., Casati, G., Rossini, D., & Strini, G. (2018). Principles of Quantum Computation and Information: A Comprehensive Textbook. World scientific.

Bojić, A. (2013). A new quantum game based on CHSH game. Journal of Information and Organizational Sciences, 37(1), 15-22.

Broadbent, A. L. (2004). Quantum pseudo-telepathy games.

Cleve, R., Hoyer, P., Toner, B., & Watrous, J. (2004, June). Consequences and limits of nonlocal strategies. In *Proceedings. 19th IEEE Annual Conference on Computational Complexity, 2004.* (pp. 236-249). IEEE.

Gharibian http://groups.uni-paderborn.de/fg-qi/courses/CMSC491/notes/Lecture%205%20-%20Non-local%20games.pdf

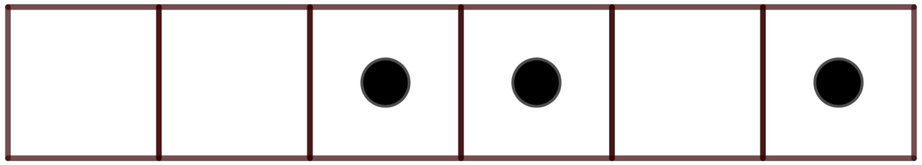
Preskill, J. (1999). Lecture notes for Physics 219: Quantum computation. Caltech Lecture Notes.

T. Rudolph, Quanti, Ed. Adelphi

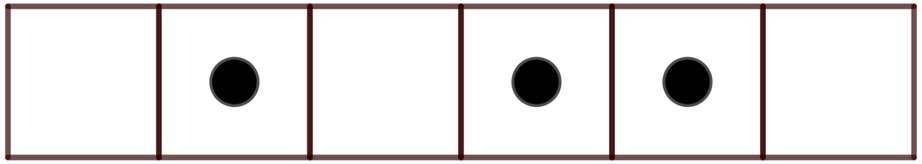
U. Vazirani, https://www.youtube.com/watch?v=DcTPKzco5YE&list=PLnhoxwUZN7-6hB2iWNhLrakuODLaxPTOG&index=16

Abaco e sassi, computer e segnali elettronici

Somma in base 2

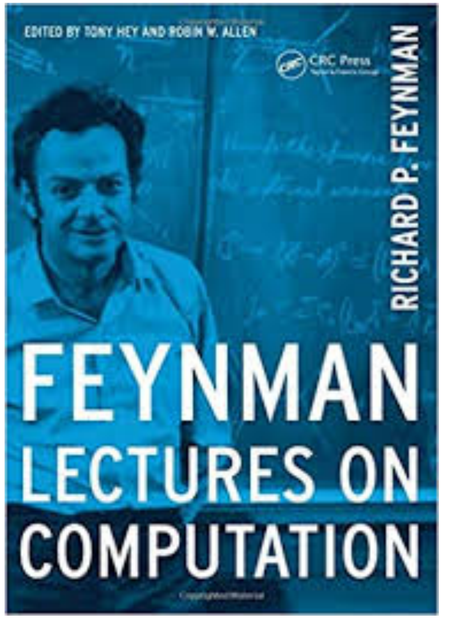


Addendo 1



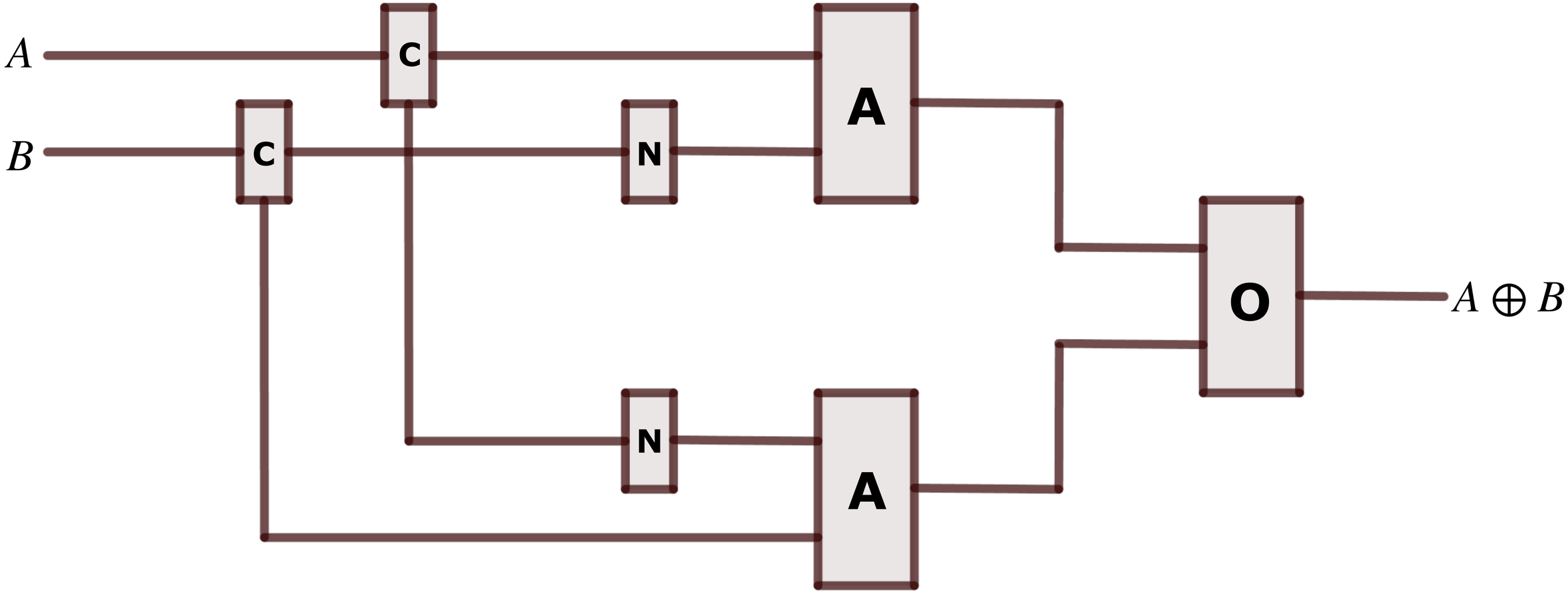
Addendo 2

Vogliamo determinare delle regole pratiche (approccio algoritmico) per poter effettuare la somma in base due con sassolini e strisce.



Tavole di verità e rappresentazioni circuitali

Vediamo ora una possibile rappresentazione circuitale dell'operatore XOR



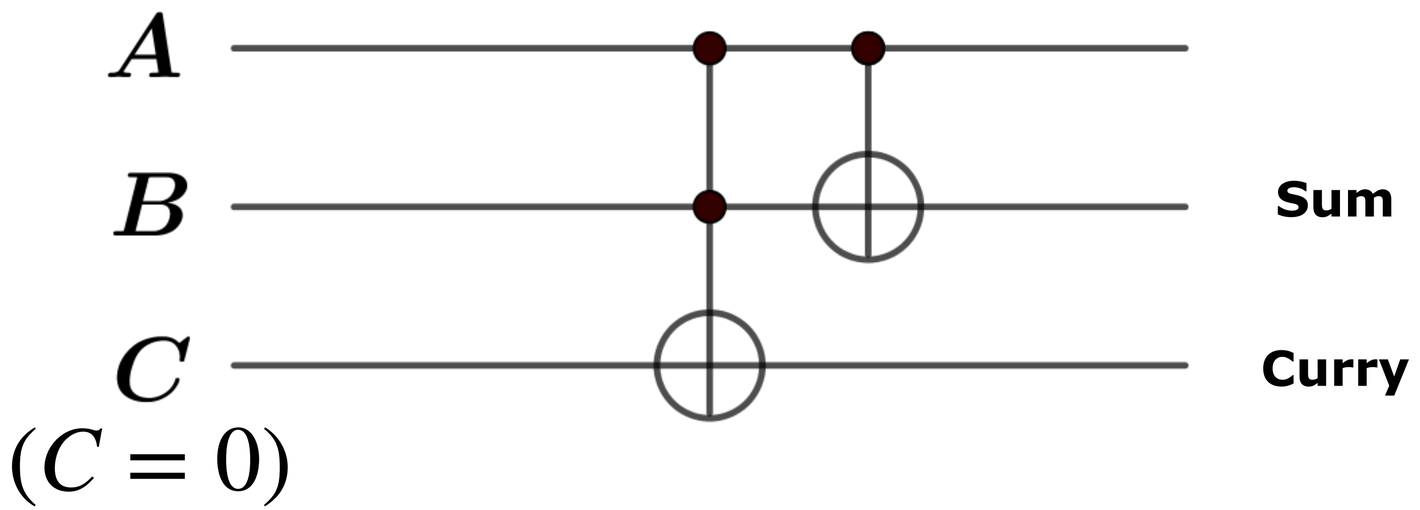
Termodinamica del calcolo

Bennett: "Nel diciannovesimo secolo il calcolo era pensato come un processo mentale, non meccanico. Di conseguenza, la termodinamica del calcolo, se qualcuno si fosse fermato a chiederselo, probabilmente non sarebbe sembrata più urgente come argomento di indagine scientifica della, diciamo, termodinamica dell'amore. Tuttavia, il bisogno di pensare seriamente alla termodinamica dei processi percettivi e mentali è stato imposto alla scienza dal famoso paradosso del demone di Maxwell."

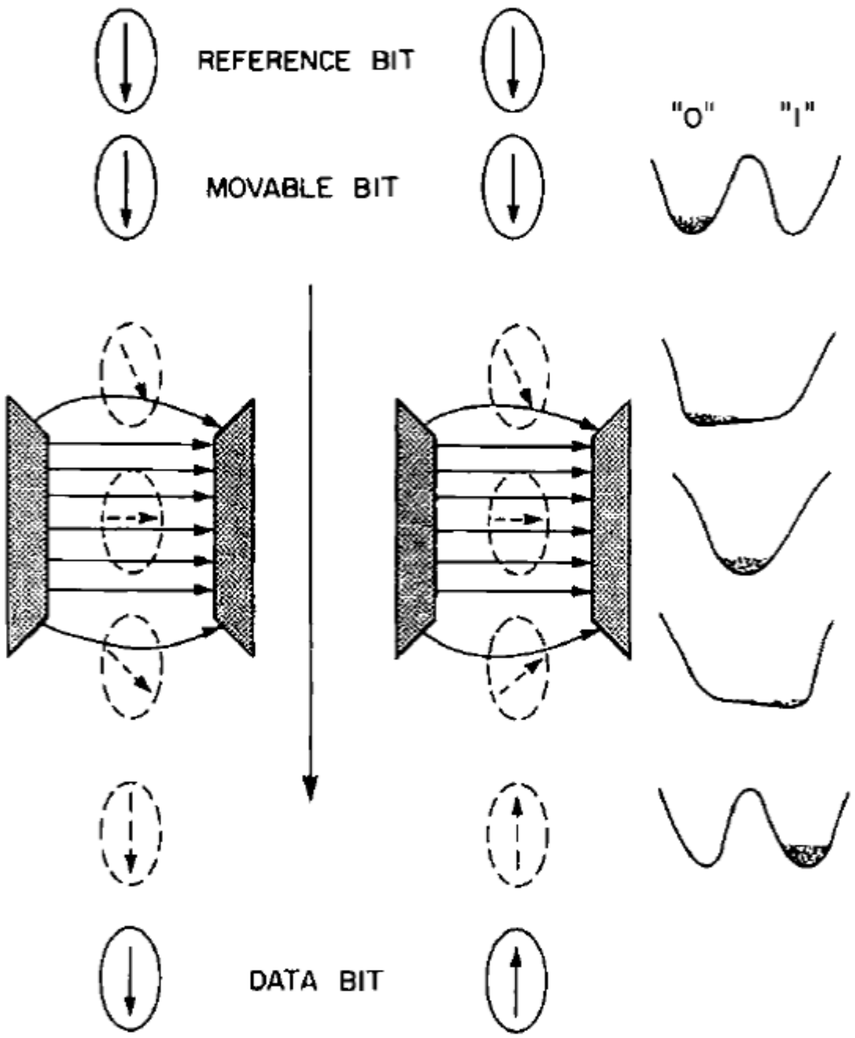
Bennett: "*Una prova della reversibilità termodinamica del calcolo richiede non solo di mostrare che le operazioni logicamente irreversibili possono essere evitate, ma anche di mostrare che, una volta che il calcolo è stato reso nel formato logicamente reversibile, qualche hardware effettivo, o qualche modello teorico fisicamente ragionevole, può eseguire la catena risultante di operazioni logicamente reversibili in modo termodinamicamente reversibile.*"

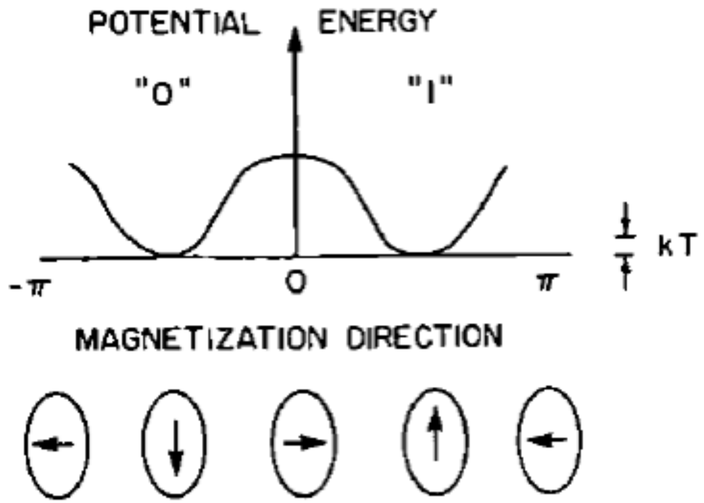
Logica reversibile

Realizzazione circuitale reversibile della somma binaria



Bennett (1982) ha fornito un esempio, utilizzando un sistema microscopico ma più realistico, costituito da un singolo dominio ferromagnetico.





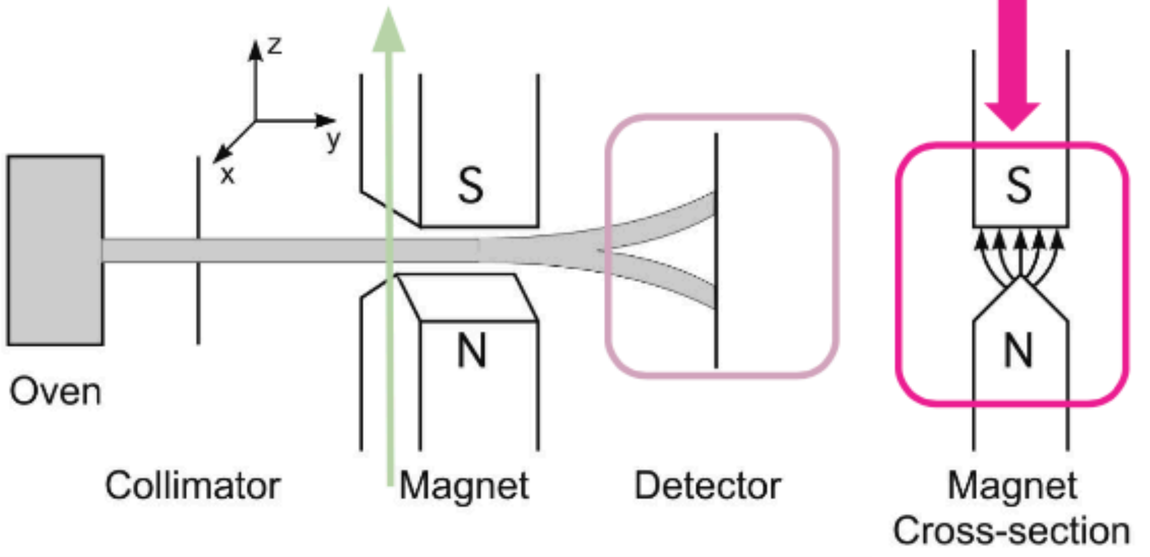
In questo caso il “movable bit” , posto inizialmente a zero, viene fatto passare attraverso un campo magnetico trasverso, che ne rompe la bistabilità portandolo in uno stato instabile, dopodichè avvicinandosi al “data bit” esso viene attirato allo stato ad esso corrispondente.

L'esperimento di Stern - Gerlach (1922)

L'esperimento è stato effettuato con **atomi di Argento** il cui comportamento è identico a quello di un singolo elettrone.

$$1s^2 2s^2 2p^6 3s^2 3p^6 4s^2 3d^{10} 4p^6 4d^{10} 5s^1$$

La sorgente di atomi (forno - oven) genera un fascio con **orientazione casuale** del loro momento magnetico.



Un momento magnetico in un **campo magnetico non uniforme** è soggetto a una forza netta che produce una **deflessione**.

Un momento magnetico (come quello posseduto dall'elettrone) in un **campo magnetico uniforme** è soggetto a un momento torcente che **lo orienta nella direzione del campo.**

Relazione tra $|\uparrow>$ e $|+>$

$$|+> = a\,|\uparrow> + b\,|\downarrow>$$

I pesi ***a*** e ***b*** sono in generale numeri (complessi) che hanno il significato di ampiezze di probabilità di trovare il sistema sullo stato $|\uparrow>$ e $|\downarrow>$

$$P_\uparrow = |a|^2 \text{ e } P_\downarrow = |b|^2$$

$$|a|^2 + |b|^2 = 1 \quad \Rightarrow \quad a = \pm b$$

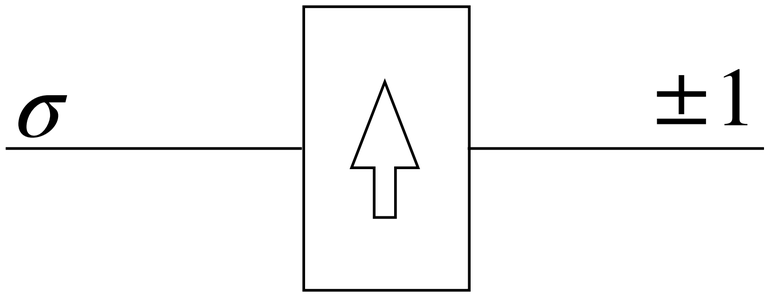
$$P_\uparrow = P_\downarrow$$

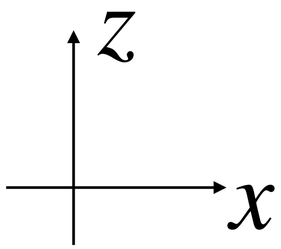
$$|+> = \frac{1}{\sqrt{2}}|\uparrow> + \frac{1}{\sqrt{2}}|\downarrow>$$

$$|-> = \frac{1}{\sqrt{2}}|\uparrow> - \frac{1}{\sqrt{2}}|\downarrow>$$

Dalla logica classica alla **logica quantistica**

Per mostrare che la logica classica non è in grado di modellizzare la fisica quantistica torniamo al concetto di *spin* e sfruttiamo quanto appreso con il dispositivo Stern-Gerlach.





APPROCCIO QUANTISTICO

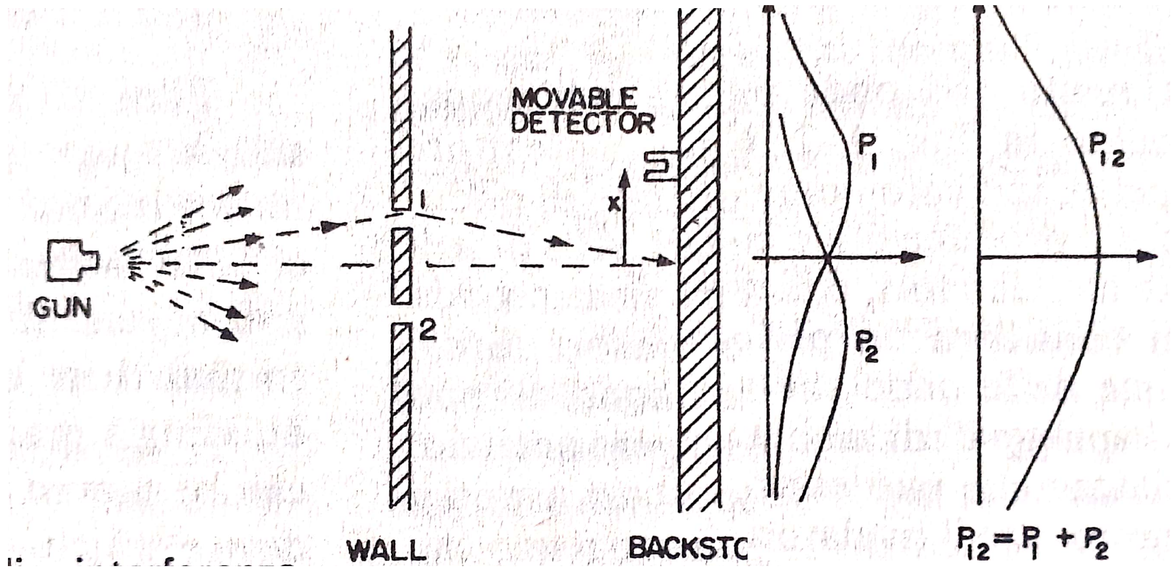
Ipotizziamo che qualcuno o qualcosa (S-G) a noi ignoto abbia preparato segretamente uno *spin* nello stato $|\uparrow\rangle_z$

Proposizione A: "*La componente z dello spin è +1*"
Proposizione B: "*La componente x dello spin è +1*"

Dalla logica classica alla **logica quantistica**

PRINCIPIO DI SOVRAPPOSIZIONE

Probabilità classica ≠ Probabilità quantistica



Ogni famiglia F_S di sottoinsiemi di S è una $\sigma - algebra$ se:

1. $\varnothing \in F_S$
2. $\forall S_A, S_B, \ldots \in F_S\ ,\quad \bigcup A_i \in F_S$
3. Se $S_A \in F_S, allora \overline{S_A} \in F_S$

$\sigma - algebra$

$$p : F_S \longrightarrow [0,1]$$

S **Spazio campionario**
$s \in S$ **Risultato di una prova**
$S_A \subseteq S$ **Evento** (Se $s \in S_A$ si realizza l'evento S_A)

$$p(S_i) \geq 0, \quad p(S) = 1$$

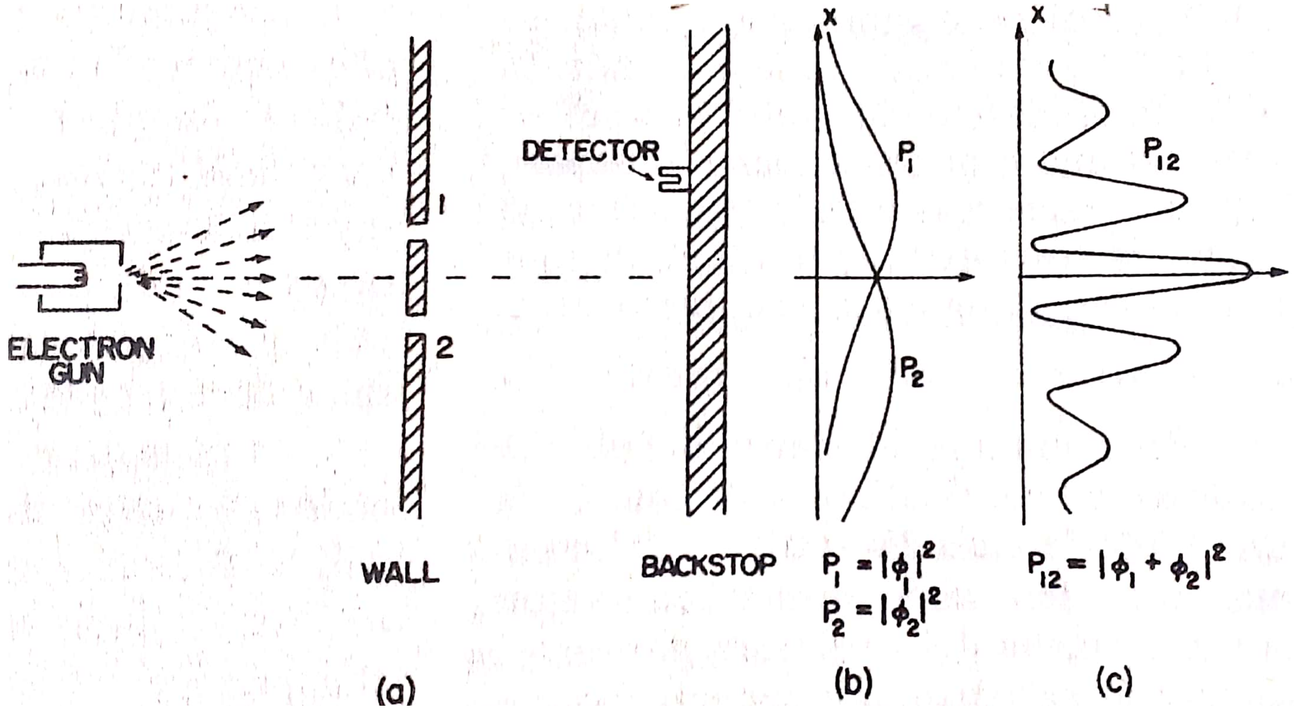
$$p(S_1 \cup S_2 \cup \ldots) = p(S_1) + p(S_2) + \ldots$$

dove $p(S_i)$ è la probabilità che lo stato del sistema sia in S_i e gli eventi S_i sono disgiunti.

Dalla logica classica alla **logica quantistica**

PRINCIPIO DI SOVRAPPOSIZIONE

Probabilità classica ≠ Probabilità quantistica



INTERFERENZA QUANTISTICA

Termine di interferenza

$$p(S_1 \cup S_2) \neq p(S_1) + p(S_2)$$

Un percorso sulla fisica quantistica basato sul metodo dei cammini di Feynman

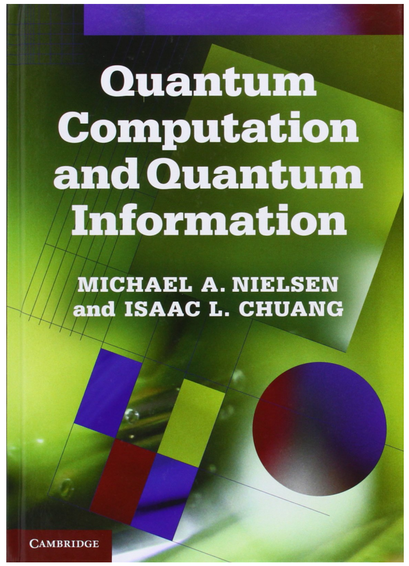
http://www-5.unipv.it/dida-pls/Materiali.htm

Dal bit al qubit

Codifica informazione

Elaborazione informazione

Informazione in uscita



Funzioni booleane
Porte logiche

Stringhe bit

Stringhe bit

$0,1$

$0,1$

$f : \{0,1\}^n \longrightarrow \{0,1\}^m$

Preparazione

Trasformazione

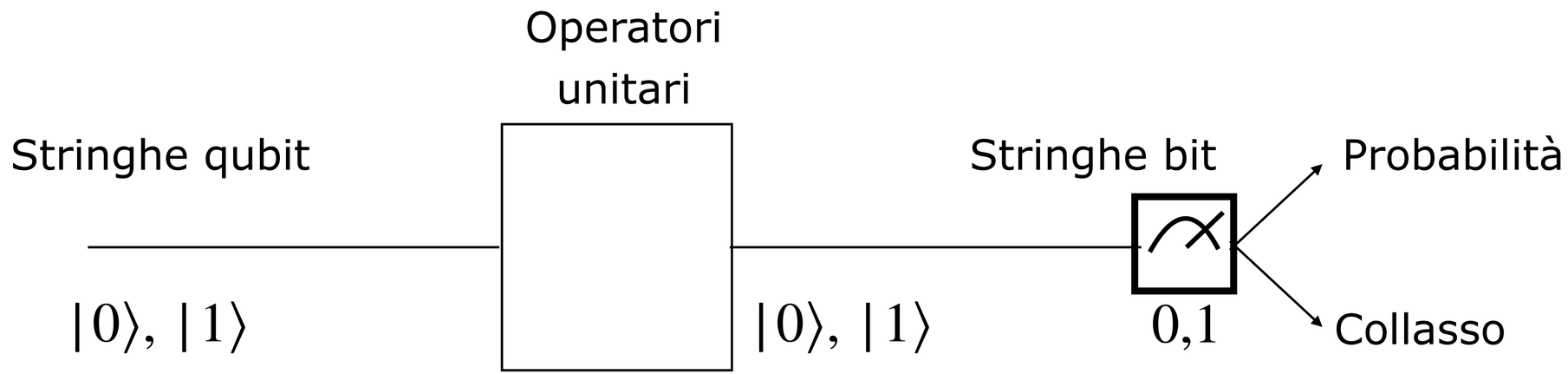
Misurazione

Dal bit **al qubit**

Preparazione

Trasformazione

Misurazione



Codifica
informazione

Elaborazione
informazione

Informazione
in uscita

Strumenti utili

Qubit

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

$$|0\rangle \equiv \begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad |1\rangle \equiv \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

Prodotto scalare

$$|\phi\rangle \cdot |\psi\rangle = \langle\phi|\psi\rangle = \sum_{i=0}^{1} \phi_i^* \psi_i$$

con ϕ^* complesso coniugato

$$|\phi\rangle \cdot |\psi\rangle = \langle\phi|\psi\rangle = [\phi_0^*, \phi_1^*] \begin{bmatrix} \psi_0 \\ \psi_1 \end{bmatrix} = \phi_0^* \psi_0 + \phi_1^* \psi_1$$

Postulati prodotto scalare:

1. $\langle\psi|\phi\rangle = \langle\phi|\psi\rangle^*$
2. $\langle\psi|a\phi + b\chi\rangle = a\langle\psi|\phi\rangle + b\langle\psi|\chi\rangle$
3. $\langle\psi|\psi\rangle \geq 0$

Base

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

$$|\alpha|^2 + |\beta|^2 = 1$$

$$\alpha, \beta \in C$$

$$|\psi\rangle = \alpha \begin{bmatrix} 1 \\ 0 \end{bmatrix} + \beta \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$$

$$|\alpha|^2 = |\langle 0|\psi\rangle|^2 = P_0 \quad |\beta|^2 = |\langle 1|\psi\rangle|^2 = P_1 \text{ (o)}$$

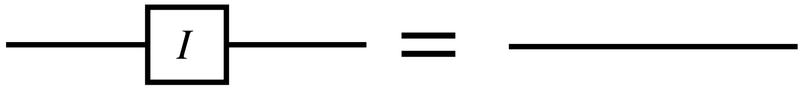
P_0, P_1 sono rispettivamente la probabilità di far collassare lo stato $|\psi\rangle$ in $|0\rangle$ e in $|1\rangle$ (valori ± 1 della misura).

Strumenti utili

Identità:

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

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \qquad |\psi\rangle \longmapsto |\psi\rangle$$



Not (X):

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

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \qquad \alpha|0\rangle + \beta|1\rangle \longmapsto \alpha|1\rangle + \beta|0\rangle$$

Hadamard

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

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \qquad \alpha|0\rangle + \beta|1\rangle \longmapsto \alpha|+\rangle + \beta|-\rangle$$

Phase flip (Z):

$\|0\rangle$	$\|0\rangle$
$\|1\rangle$	$-\|1\rangle$

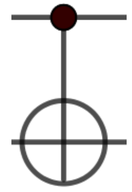
$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \qquad \alpha|0\rangle \pm \beta|1\rangle \longmapsto \alpha|0\rangle \mp \beta|1\rangle$$

$$|+\rangle \xmapsto{Z} |-\rangle$$
$$|-\rangle \xmapsto{Z} |+\rangle$$

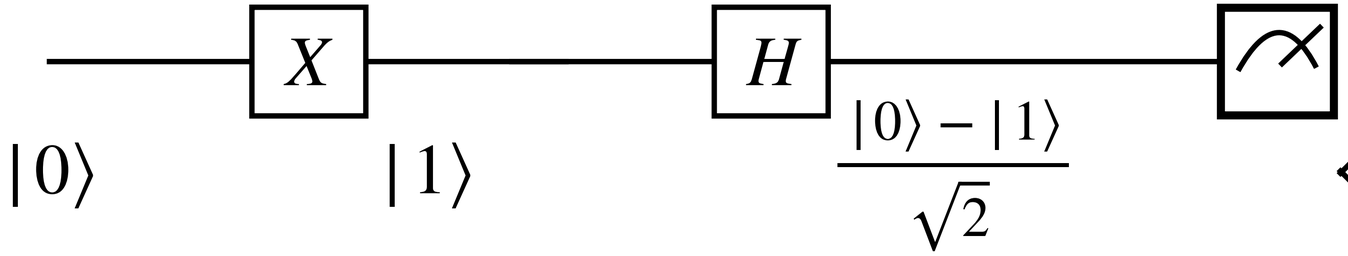
CNOT:

$\|00\rangle$	$\|00\rangle$
$\|01\rangle$	$\|01\rangle$
$\|10\rangle$	$\|11\rangle$
$\|11\rangle$	$\|10\rangle$

$$CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \qquad |x\rangle|y\rangle \longmapsto |x\rangle|x \oplus y\rangle$$



Circuiti



Autovalore Autostato

50 % 1, $|0\rangle$ → 0

COLLASSO

50% − 1, $|1\rangle$ → 1

Bits

$$\begin{bmatrix} 1 \\ 0 \end{bmatrix} \xrightarrow{X} \begin{bmatrix} 0 \\ 1 \end{bmatrix} \xrightarrow{H} \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix} := |\psi\rangle$$

$$|\langle 0|\psi\rangle|^2 = 0.5$$

$$|\langle 1|\psi\rangle|^2 = 0.5$$

$$X \quad \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

$$H \quad \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

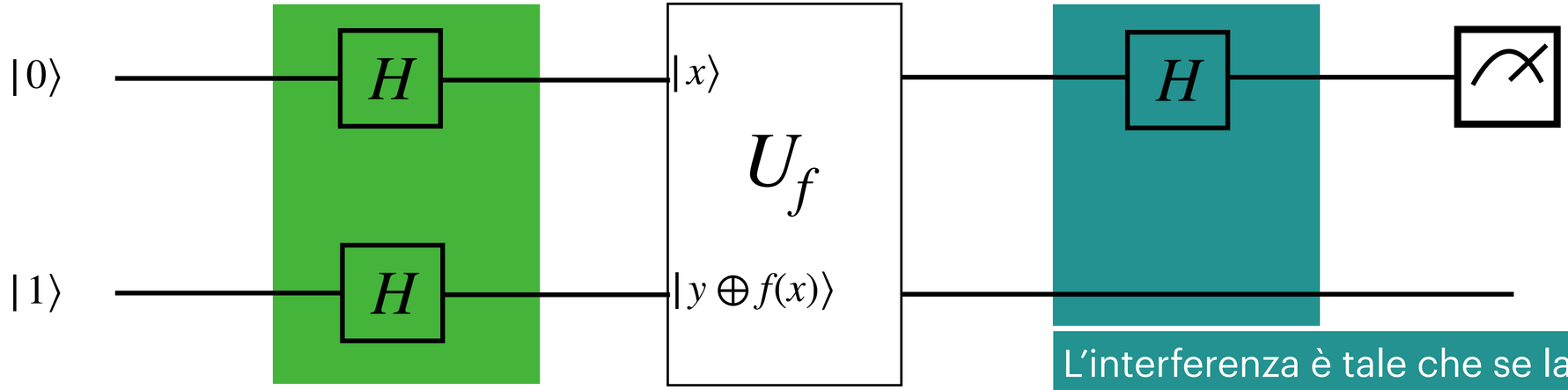
$$P_0 = |\langle 0|\psi\rangle|^2 = \left| [1,0] \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix} \right|^2 = 0.5$$

$$P_1 = |\langle 1|\psi\rangle|^2 = \left| [0,1] \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix} \right|^2 = 0.5$$

Algoritmo di Deutsch

La porta di Hadamard permette di generare uno stato che risulta sovrapposizione di tutti quelli che codificano le informazioni

N.B. L'operatore U_f ha potuto agire contemporaneamente su tutti gli stati: parallelismo quantistico.



L'interferenza è tale che se la funzione è costante lo stato è trasformato in $|0\rangle$, altrimenti in $|1\rangle$

Si dimostra quindi che se

f è costante → $P(0) = 1$

f è bilanciata → $P(1) = 1$

Abbiamo implementato f UNA SOLA VOLTA!!!

Algoritmo di Deutsch -Jozsa

Generalizzazione!

RAPINA IN BANCA

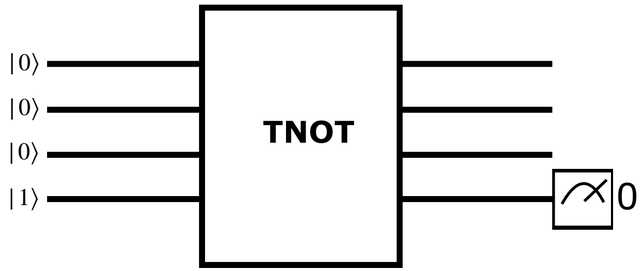
Sei stato assoldato per rapinare una banca celebre per le sue strutture di sicurezza.
La banca è divisa in molti caveaux in ciascuno dei quali ci sono 8 enormi lingotti d'oro.

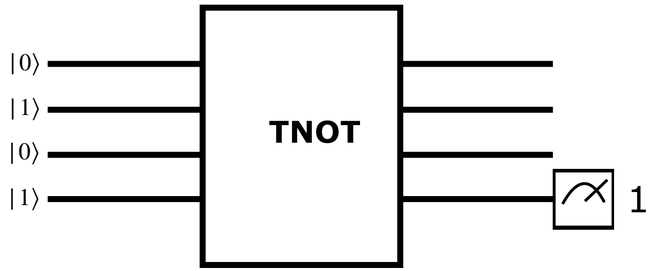
Il capo della banda è venuto a sapere che in ogni stanza o tutti i lingotti sono falsi o metà sono falsi e metà sono veri. Purtroppo la falsità o l'autenticità dei lingotti può essere verificata con apparecchiature troppo sofisticate da poter essere trasportate durante la rapina.
Anche i dipendenti della banca non possono riconoscerne l'autenticità o meno.
Per evitare che una mappa dei lingotti veri possa essere copiata o rubata, il direttore della banca ha deciso di installare un computer (quantistico) in ogni stanza. Ogni lingotto può essere codificato in modo ovvio con dei qubit

Algoritmo di Deutsch - Jozsa

Generalizzazione!

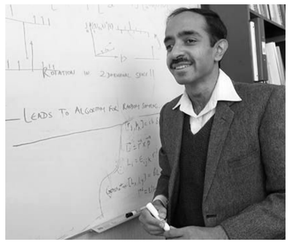
Il computer ha un programma che funziona in questo modo: l'impiegato inserisce su tre registri i qubit corrispondenti al lingotto scelto e su un quarto un qubit $|1\rangle$; se il lingotto è autentico allora al quarto qubit viene applicato un *NOT* altrimenti no. Quindi se l'impiegato vede 0 sullo schermo del computer sa che il lingotto è vero; altrimenti è falso. I primi tre qubit invece riescono esattamente come sono entrati[1].



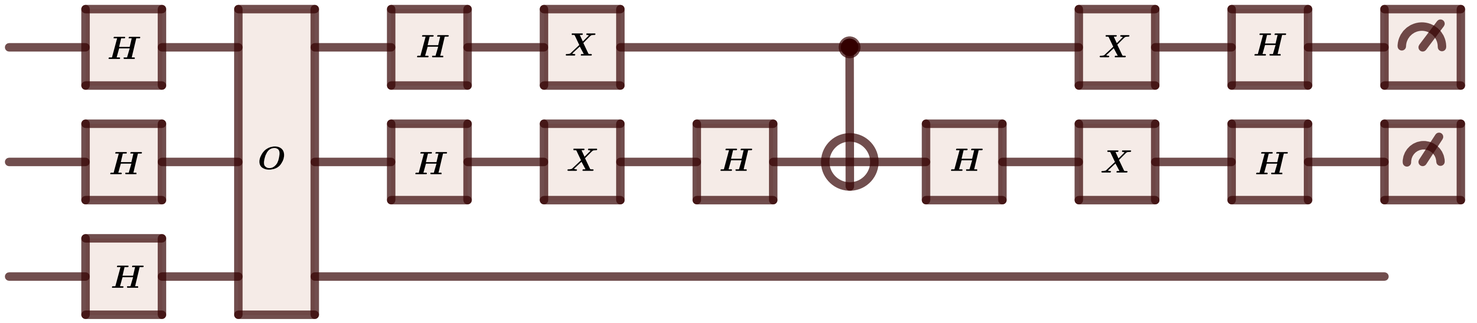


[1] Possiamo inventarci una porta logica di nome TNOT-gate, ossia una TRUE-NOT gate.

Algoritmo di Grover



Lov Grover, 1996



Codifica: 2 bit

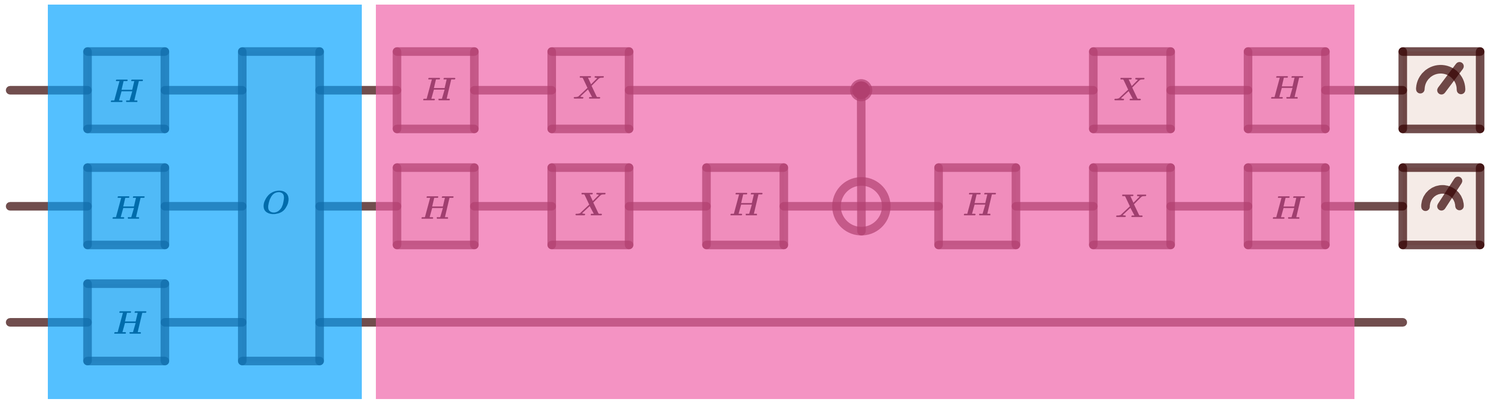
Antonio $\longrightarrow (0,0)$
Carlo $\longrightarrow (0,1)$
Luigi $\longrightarrow (1,0)$
Stefano $\longrightarrow (1,1)$

Codifica: 2 qubit

Antonio $\longrightarrow |0\rangle|0\rangle$
Carlo $\longrightarrow |0\rangle|1\rangle$
Luigi $\longrightarrow |1\rangle|0\rangle$
Stefano $\longrightarrow |1\rangle|1\rangle$

f viene implementata una sola volta

Algoritmo di Grover



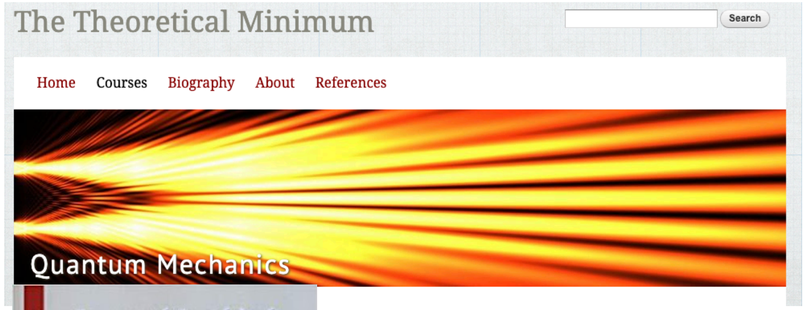
$$|\psi_1\rangle = \left[\frac{1}{2}\left(|0\rangle|0\rangle + |0\rangle|1\rangle - |1\rangle|0\rangle + |1\rangle|1\rangle\right)\right] \xrightarrow{Misura} P(0,0) = P(1,0) = P(0,1) = P(1,1)$$

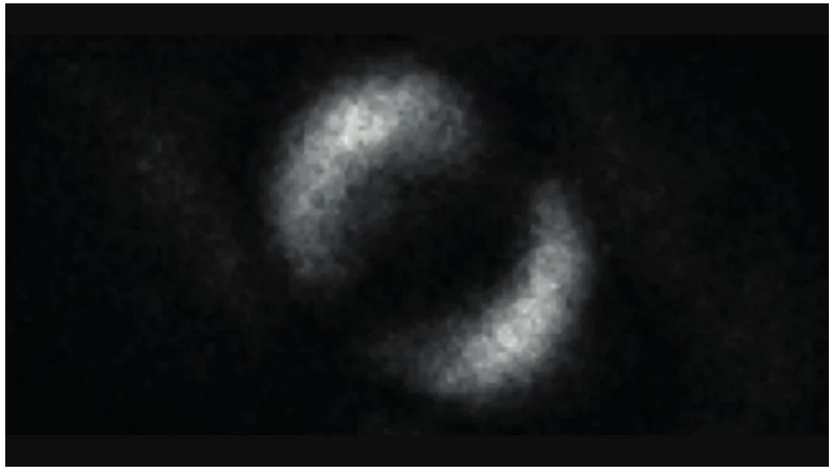
$$|\psi_{fin}\rangle = -|1\rangle|0\rangle \xrightarrow{Misura} P(1,0) = 1$$

Abbiamo implementato f UNA SOLA VOLTA!!!

Possiamo rileggere quanto visto
da un punto di vista geometrico

Entanglement





"The entanglement is the characteristic trait of Quantum Mechanics, the one that enforces its entire departure from classical line of thoughts." (E. Schroedinger, 1935)

"The deep ways that quantum information differs from classical information involve the properties, implications, and uses of quantum entanglement." (J. Preskill, 2009)

Sistemi composti

Il punto di partenza di questa secondo ciclo di incontri è il ruolo dei sistemi composti e la profonda differenza tra il caso classico e quello quantistico

SISTEMI COMPOSTI CLASSICI

$$A = A_1 \times A_2 \times \ldots \times A_n$$

Lo spazio degli stati complessivo è sempre il prodotto di n sottospazi

La conoscenza del sistema composto implica la conoscenza delle sue parti.

L'utilizzo della probabilità è dovuto solo ad ignoranza sul sistema. (Correlazioni classiche)

SISTEMI COMPOSTI QUANTISTICI

$$H = \otimes_{l=1}^{n} H_l$$

In generale non è possibile ottenere un singolo vettore di stato come prodotto di n vettori corrispondenti agli n sottosistemi

La conoscenza del sistema composto non permette la conoscenza delle sue parti.

L'utilizzo della probabilità è intrinseco alla teoria quantistica (Correlazioni quantistiche: non località)

Sistemi composti: il caso classico

$$\langle AB \rangle - \langle A \rangle \langle B \rangle = -1$$

Da un punto di vista probabilistico questo significa che la probabilità non fattorizza.

$$P(a,b) \neq p_A(a) \cdot p_B(b)$$

Se considerassimo invece due coppie di scatole (due eventi indipendenti)

$$\langle AB \rangle - \langle A \rangle \langle B \rangle = 0$$

$$P(a,b) = p_A(a) \cdot p_B(b)$$

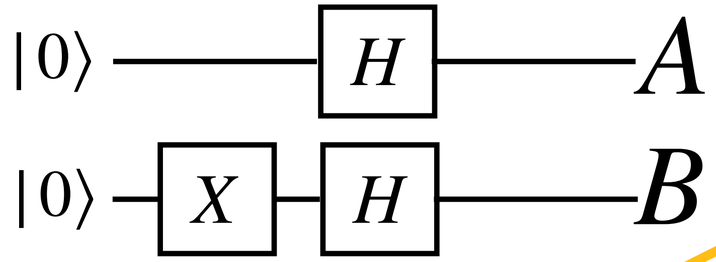
L'utilizzo della probabilità è dovuto al fatto che in origine non sappiamo quale biglia ci sia in ciascuna scatola. Ma in linea di principio potremmo guardare di nascosto senza per questo alterare l'esito delle successive misurazioni.

Se facessimo così potremmo conoscere il sistema composto e questa conoscenza implica, naturalmente, la conoscenza delle sue singole parti. La conoscenza sul sistema completo implica la conoscenza completa sulle singole parti.

Sistemi composti: stati separabili

Analizziamo alcuni stati quantistici

Consideriamo lo stato ottenuto mediante il seguente circuito:



Lo stato prodotto è il risultato di due preparazioni totalmente indipendenti da parte di A e B, in cui ciascuno utilizza il proprio apparato sperimentale per preparare lo stato fisico.

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A + |1\rangle_A) \otimes \frac{1}{\sqrt{2}}(|0\rangle_B - |1\rangle_B)$$

$$\Longleftrightarrow$$

$$|\psi\rangle = \frac{1}{2}(|0\rangle|0\rangle + |1\rangle|0\rangle - |0\rangle|1\rangle - |1\rangle|1\rangle)$$

Definizione: Uno stato $|\psi\rangle$ è detto *stato prodotto* o *separabile* se possiamo trovare due stati $|\phi\rangle_A$, $|\phi\rangle_B$ rispettivamente negli spazi di Alice e Bob tali che

$$|\psi\rangle = |\phi\rangle_A \otimes |\phi\rangle_B$$

Sistemi composti: stati entangled

Gli stati prodotto non sono gli unici che vivono nello spazio composto

$$|\psi\rangle_{AB} = \alpha\gamma|00\rangle + \alpha\delta|01\rangle + \beta\gamma|10\rangle + \beta\delta|11\rangle$$

Più in generale infatti uno stato avrà la forma (combinazione lineare complessa di elementi della base)

$$|\psi\rangle_{AB} = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$$

Con la conseguente condizione di normalizzazione $a^*a + b^*b + c^*c + d^*d = 1$

e una sola fase globale da ignorare → sei parametri reali → Esistono stati non separabili

↓

STATI ENTANGLED

Esistono stati che non possono essere preparati indipendentemente da Alice e da Bob.

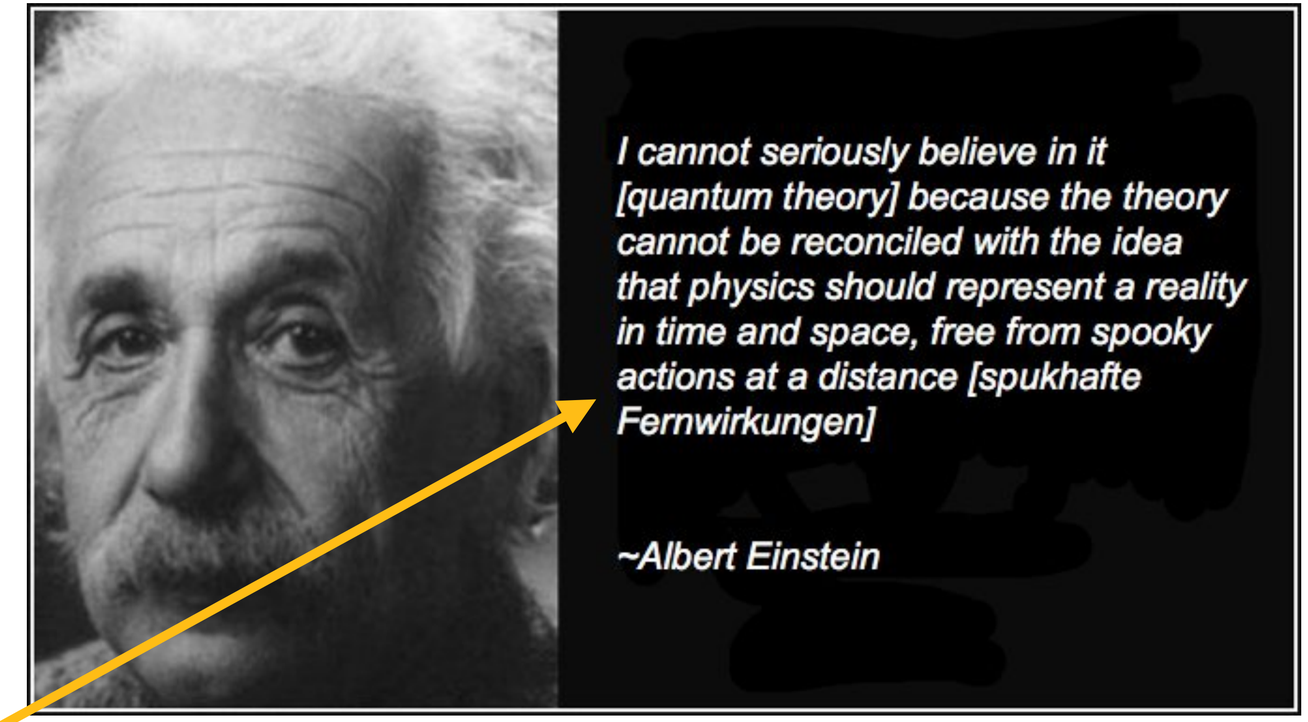
Sistemi composti: stati prodotto e stati entangled

Stati prodotto	Stati max. entangled
Ogni sottosistema è descritto in modo completo. Non esistono correlazioni tra i sottosistemi.	Il sistema composto è conosciuto in modo completo. Nessuna conoscenza sui sottosistemi. Correlazioni.
Vettore di stato: $\|\psi\rangle_{AB} = \alpha\gamma\|00\rangle + \alpha\delta\|01\rangle + \beta\gamma\|10\rangle + \beta\delta\|11\rangle$ **Normalizzazione:** $\alpha^*\alpha + \beta^*\beta = 1 \qquad \gamma^*\gamma + \delta^*\delta = 1$	**Vettore di stato:** $\|\psi\rangle_{AB} = a\|00\rangle + b\|01\rangle + c\|10\rangle + d\|11\rangle \qquad Ex. \quad \|\psi_{11}\rangle = \frac{1}{\sqrt{2}}(\|01\rangle - \|10\rangle)$ **Normalizzazione:** $a^*a + b^*b + c^*c + d^*d = 1$
La probabilità si fattorizza $P(A,B) = P(A)\cdot P(B)$	**La probabilità non si fattorizza** $P(A,B) \neq P(A)\cdot P(B)$
Valori di aspettazione: $\langle X\rangle^2 + \langle Y\rangle^2 + \langle Z\rangle^2 = 1$	**Valori di aspettazione:** $\langle Z\rangle = \langle X\rangle = \langle Y\rangle = 0$ $\langle Z_B Z_A\rangle, \langle X_B X_A\rangle, \langle Y_B Y_A\rangle = \pm 1$
Correlazione: $\langle Z_B Z_A\rangle - \langle Z_B\rangle\langle Z_A\rangle = 0$	**Correlazione:** $\langle \Sigma_B \Sigma_A\rangle - \langle \Sigma_B\rangle\langle \Sigma_A\rangle = \pm 1$

Entanglement: spooky action!

$$\frac{1}{\sqrt{2}}(|\uparrow\rangle_A|\uparrow\rangle_B + |\downarrow\rangle_A|\downarrow\rangle_B) \longrightarrow |\uparrow\rangle_A|\uparrow\rangle_B$$

Possiamo interpretare questo dicendo che dopo la misura effettuata da uno dei due (Alice o Bob non conta) lo stato collassa e, se i due fossero sufficientemente lontani e in modo che uno sia leggermente più distante dell'altro, la prima misurazione avrebbe l'effetto di determinare anche l'esito della seconda, questa volta con assoluta certezza.



Come è possibile che le proprietà di un sistema (possedere oggettivamente la proprietà) possano essere influenzate istantaneamente a distanza?

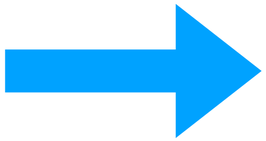
NON LOCALITÀ

Peculiarità correlazioni quantistiche (spin)

Ipotesi:

R (realtà): Se, senza disturbare in alcun modo un sistema è possibile prevedere con certezza il risultato di una misurazione di una osservabile del sistema, allora esiste un elemento di realtà associato all'osservabile in questione, o equivalentemente, il sistema possiede oggettivamente (indipendentemente da qualsiasi osservatore, dal fatto che la misurazione sia effettuata o meno) la relativa proprietà.

LE (Località einsteiniane): Gli elementi di realtà fisica posseduti oggettivamente da un sistema non possono venire influenzati istantaneamente a distanza.

R + LE  L'elettrone 2 aveva prima e indipendentemente dalla misurazione la proprietà spin-down Z e spin-down X.

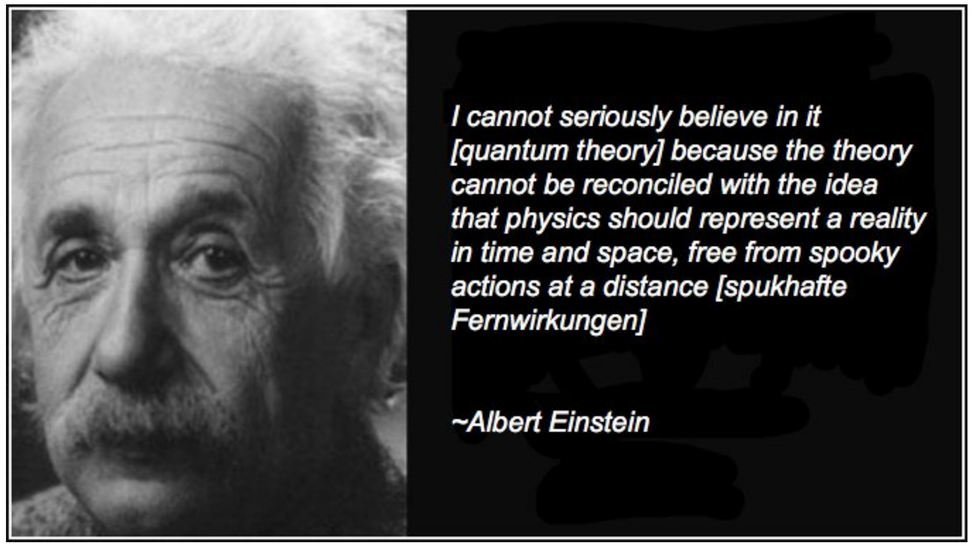
Peculiarità correlazioni quantistiche (spin)

Poiché richieste naturali e ovvie ci hanno portato a concludere che l'elettrone 2 possiede simultaneamente proprietà incompatibili ($[\sigma_{X,2}, \sigma_{Z,2}] \neq 0$) questo significa che, di fatto, anche se non risulta possibile determinare con precisione arbitraria queste proprietà, esse ciò nondimeno devono essere considerate come possedute oggettivamente dal sistema. Ma la MQ nega questa possibilità e lo stato non contiene alcun elemento formale che possa specificare queste proprietà.

La MQ è una teoria basilarmente incompleta, essa non è in grado di descrivere, non lascia spazio per rendere conto di elementi di realtà fisica che si devono riconoscere come posseduti da un sistema fisico.

Analogamente: l'elettrone 2 ha prima della misura, la proprietà spin-down Z. Ma lo stato è invariante per rotazioni e non contiene informazioni su spin-down Z. Ma la teoria asserisce che lo stato rappresenta il massimo dell'informazione possibile. Quindi la teoria è incompleta.

Entanglement: spooky action!



La probabilità in MQ è dello stesso tipo di quella in MC.
Basta aggiungere delle variabili nascoste!

Speranza di Einstein

"…la teoria statistica dei quanti avrebbe, nel quadro della fisica futura, assunto una posizione approssimativamente analoga alla meccanica statistica nel quadro della meccanica classica"

Un decennio dopo la morte di Einstein, John Bell infranse questo sogno: qualsiasi completamento della meccanica quantistica con variabili nascoste sarebbe incompatibile con la causalità relativistica!

Teorema di Bell

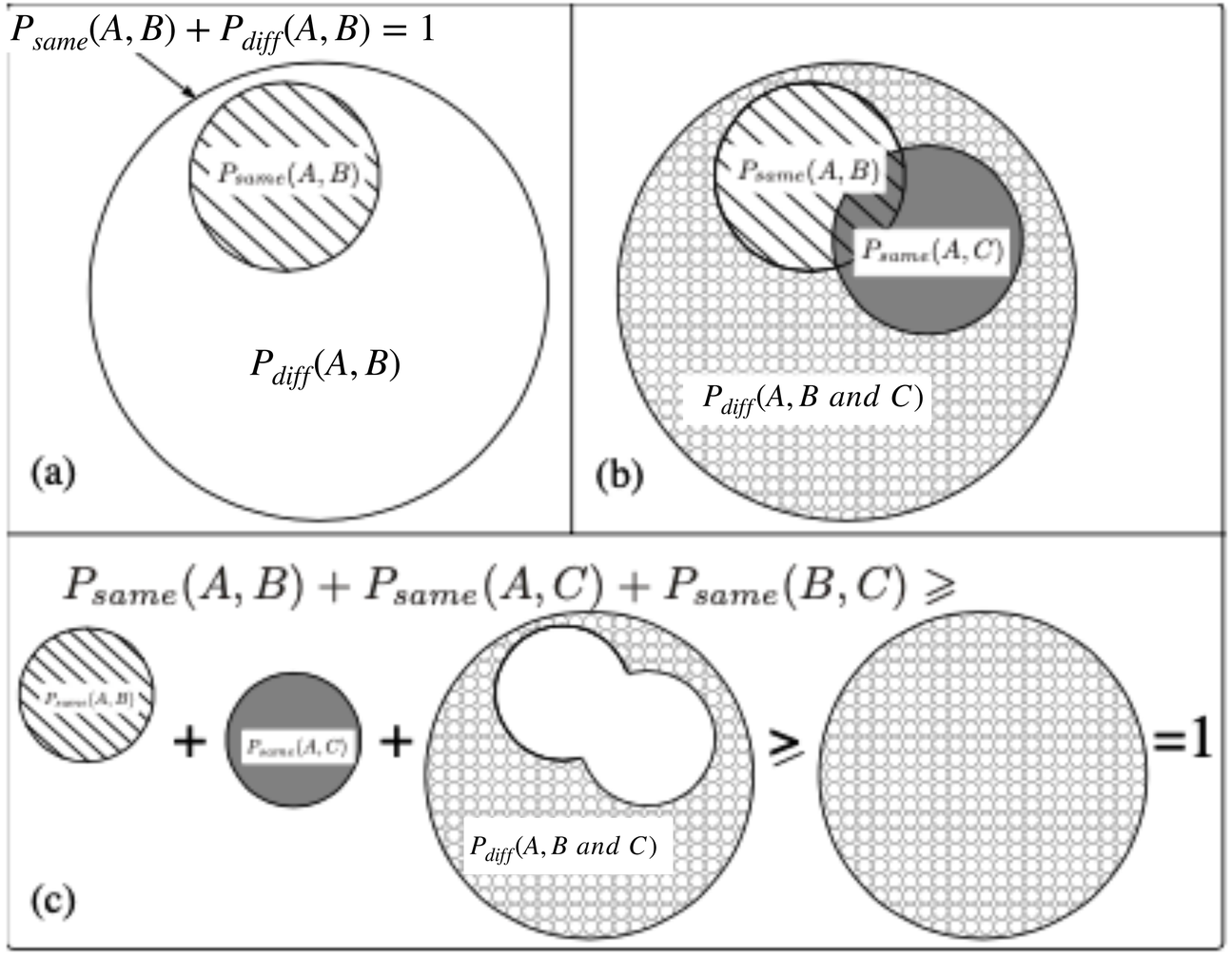
Teorema: la meccanica quantistica non può essere sia locale che controfattuale-definita.

Locale: una teoria in cui i risultati di un esperimento su un sistema sono indipendenti dalle azioni compiute su un sistema diverso che non ha alcuna connessione causale con il primo (località alla Einstein).

Controfattuale-definita: una teoria i cui esperimenti scoprono proprietà preesistenti, in cui ha senso assegnare una proprietà a un sistema (per esempio la posizione di un elettrone) indipendentemente dal fatto che la misurazione di tale proprietà sia stata effettuata.

Per **dimostrare** questo teorema, Bell ha fornito una disuguaglianza (riferita alle correlazioni dei risultati di misura) che è soddisfatta da tutte le teorie che sono sia locali che controfattuali-definite. Ha poi dimostrato che la meccanica quantistica viola questa disuguaglianza, e quindi non può essere locale e controfattuale-definita.

Disuguaglianza di Bell



(a) L'area tratteggiata rappresenta la probabilità che la proprietà A del primo oggetto e B del secondo siano uguali (entrambe 1 o entrambe 0): $P_{same}(A,B)$. L'area bianca rappresenta la probabilità che siano diverse: $P_{diff}(A,B)$. L'intero cerchio ha area 1 $P_{same}(A,B) + P_{diff}(A,B) = 1$.

(b) L'area grigia rappresenta la probabilità che A e C siano uguali, e l'area non grigia rappresenta la probabilità che A e C siano diversi. Se A del primo oggetto è diverso sia da B che da C del secondo (area a bolle), allora B e C del secondo oggetto devono essere uguali. Quindi, la probabilità che B e C siano uguali deve essere maggiore (o uguale) all'area a bolle: poiché B è lo stesso per i due oggetti, $P_{same}(B,C)$ deve essere maggiore (o uguale) all'area a bolle.

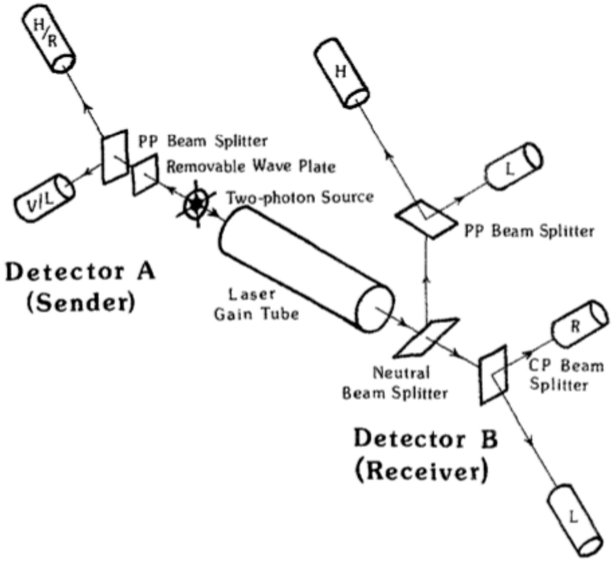
(c) La quantità $P_{same}(A,B) + P_{same}(B,C) + P_{same}(A,C)$ è quindi maggiore (o uguale) alla somma delle aree tratteggiata + grigia + a bolle, che è a sua volta maggiore (o uguale) al cerchio completo di area 1: questo prova la disuguaglianza di Bell.

Entanglement: segnali superluminali?

FLASH[1]—A Superluminal Communicator Based Upon a New Kind of Quantum Measurement

Nick Herbert[2]

Received January 15, 1982 *Foundations of Physics*

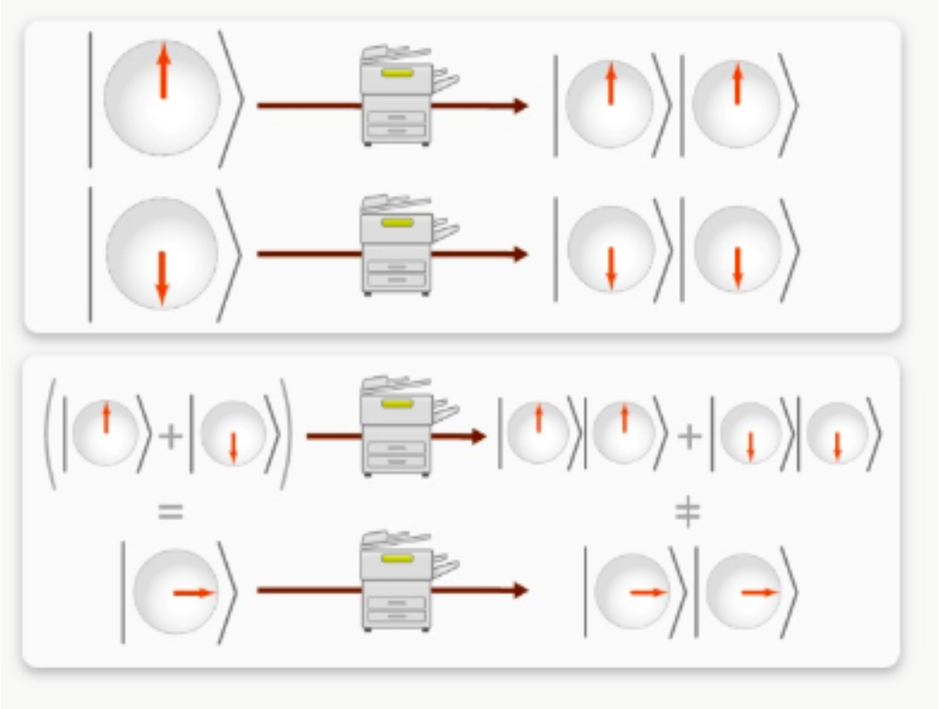


N.B. *Non entriamo nel dettaglio dell'apparato perché ne vedremo una versione semplificata. Rimandiamo comunque alla bibliografia*

…Questo fotone è amplificato dal tubo di amplificazione in N fotoni polarizzati V che sono separati dal beam splitter neutro in due pacchetti di circa N/2 fotoni ciascuno…

È implicito il riferimento alla possibilità di clonare stati!!!

Teorema di non clonazione



Teorema: non è possibile costruire una macchina che operi una trasformazione unitaria e sia in grado di clonare un generico stato di un qubit.

dim: esista una macchina in grado di clonare i qubit $|0\rangle$ e $|1\rangle$

$$U : |0\rangle \longmapsto |0\rangle|0\rangle$$
$$U : |1\rangle \longmapsto |1\rangle|1\rangle$$

allora scelto $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ otteniamo $U|\psi\rangle = |\psi\rangle|\psi\rangle$ da cui

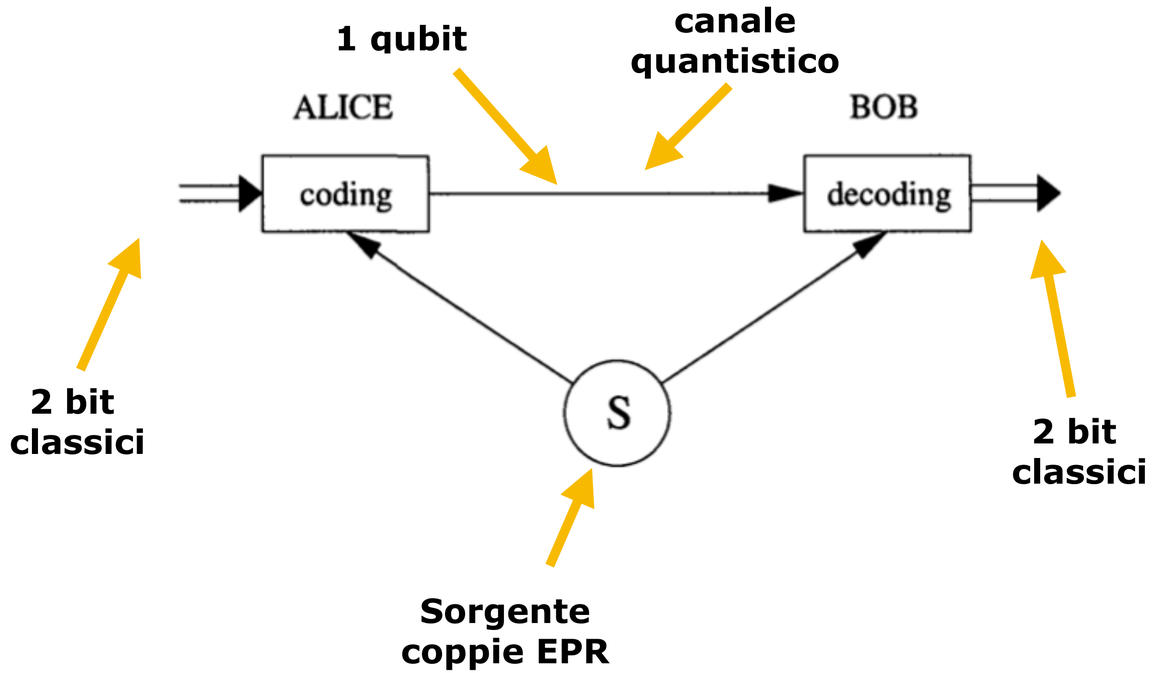
$$U|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$$

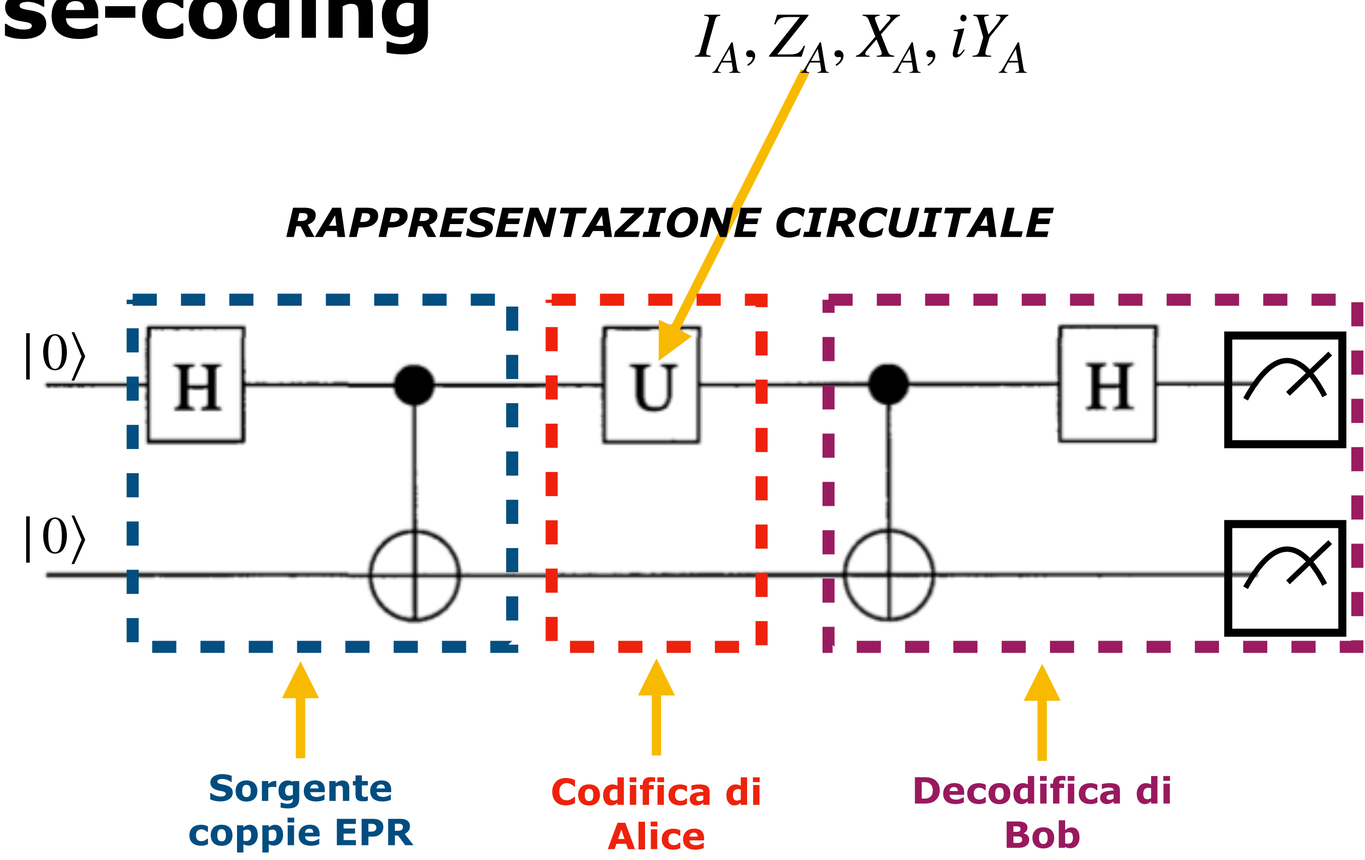
D'altronde per linearità della teoria

$$U|\psi\rangle = U\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \frac{1}{\sqrt{2}}(U|0\rangle + U|1\rangle) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

$\neq$

Dense-coding





Consideriamo una sorgente di coppie EPR che invii ad Alice un qubit e a Bob l'altro della coppia. Alice può codificare i propri due bit classici grazie alla proprietà che uno stato massimamente entangled di Bell può essere trasformato in uno qualsiasi degli altri tre facendo agire localmente una delle quattro matrici di Pauli (Identità compresa). In questo modo Alice può inviare il proprio qubit a Bob il quale a questo punto esegue una misura nella base di Bell e ottiene in questo modo la decodifica dell'informazione inviata da Alice.

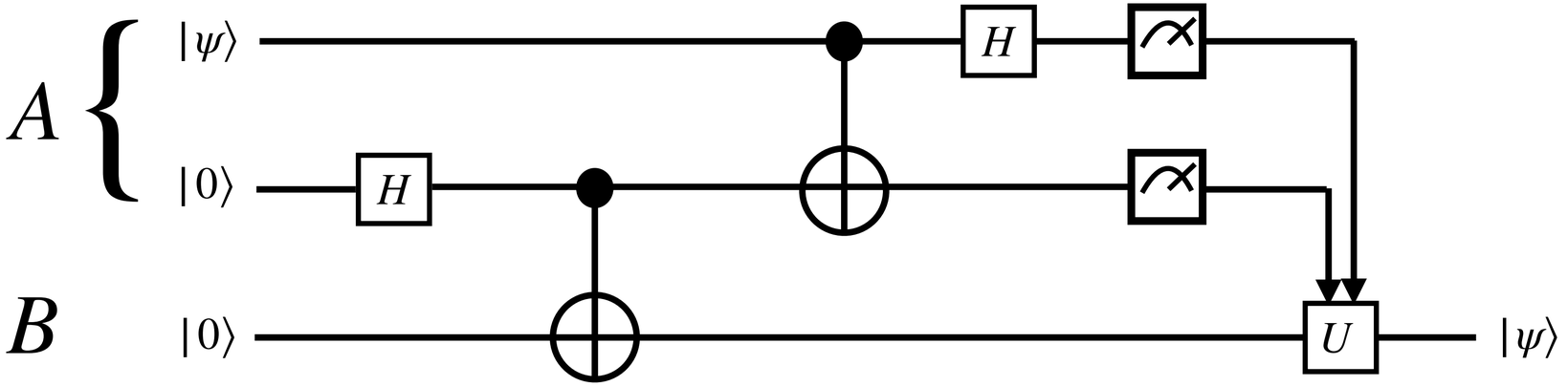
Teletrasporto quantistico

PHYSICAL REVIEW
LETTERS

VOLUME 70 | 29 MARCH 1993 | NUMBER 13

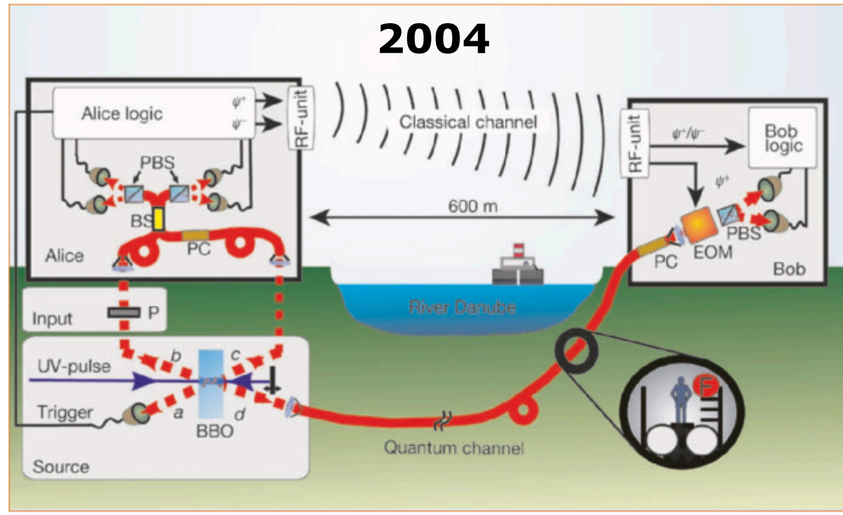
Teleporting an Unknown Quantum State via Dual Classical and Einstein-Podolsky-Rosen Channels

Charles H. Bennett,[1] Gilles Brassard,[2] Claude Crépeau,[2,3]
Richard Jozsa,[2] Asher Peres,[4] and William K. Wootters[5]

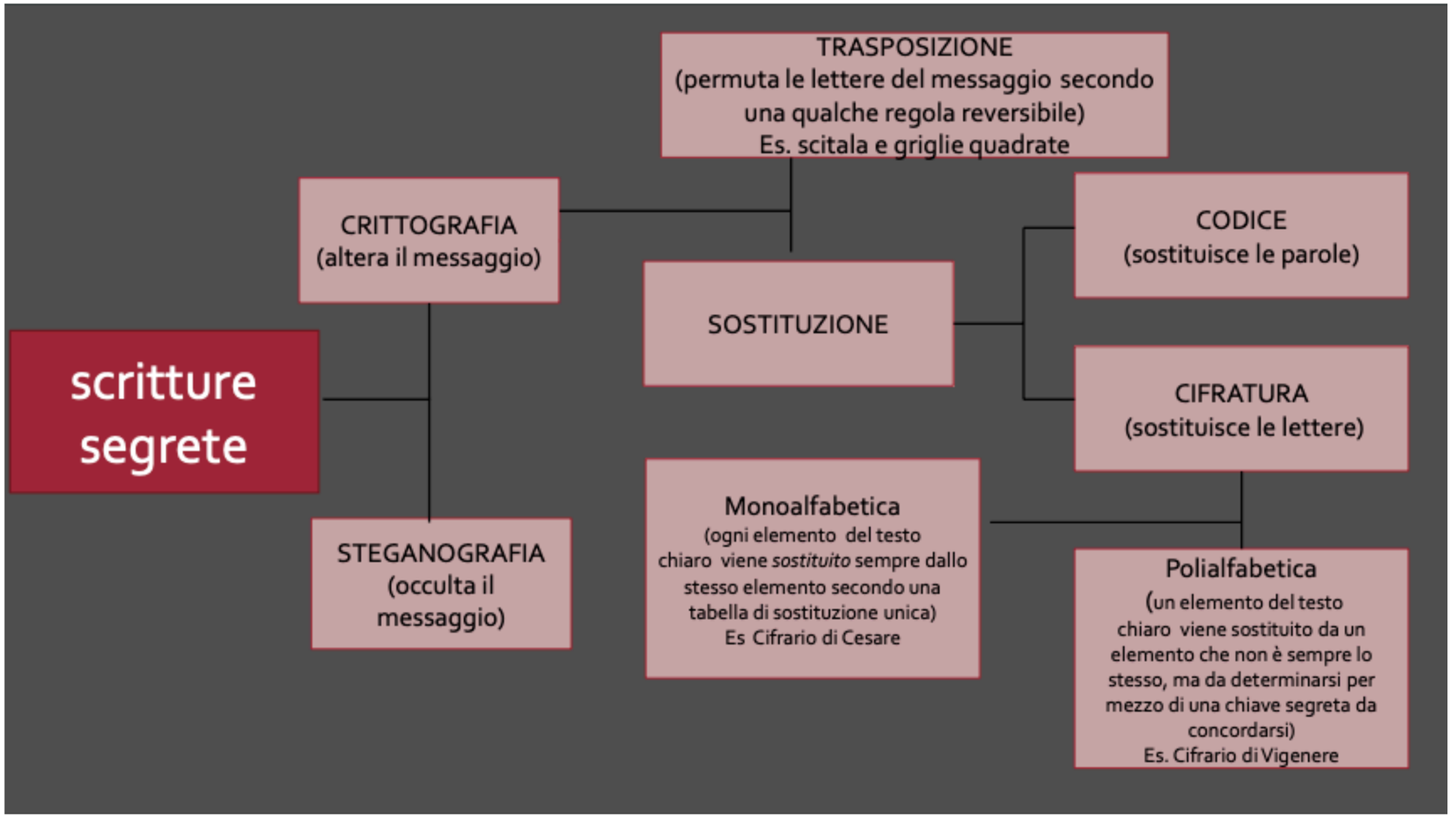


Quantum teleportation across the Danube

A real-world experiment marks a step towards worldwide quantum communication.



Crittografia classica: dall’antichità al Novecento



Crittografia classica: sostituzione monoalfabetica

Vita dei Cesari,
Svetonio (II sec. a.C.)

Cifrario di Cesare

Alfabeto chiaro	a b c d e f g h i l m n o p q r s t u v z
Alfabeto cifrante	D E F G H I L M N O P Q R S T U V Z A B C
Testo chiaro	v e n i, v i d i, v i c i
Testo cifrante	B H Q N, B N G N, B N F N

$A = \{a, b, c, \ldots, z\}$ Alfabeto di *k* caratteri

j *chiave*

$$f : A \longrightarrow A$$
$$i \longmapsto i + j \ (mod\ k)$$

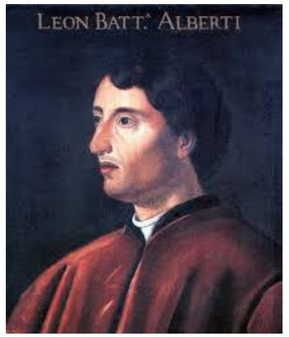
Mittente e destinatario devono possedere la chiave!

Con l'algoritmo di Grover le potremmo testare in pochi minuti!!!

Possiamo immaginare una versione meno semplice da decifrare: sostituzione del tutto generica.
21! possibili chiavi

Crittografia classica: sostituzione polialfabetica

Leon Battista Alberti
XV secolo



Ebbe per primo l'idea di cifrare usando più di un alfabeto, ma non lo fece diventare una tecnica definita.

Blaise de Vigenère
XVI secolo

Chiaro	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
26	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Parola chiave:	M	O	N	T	E	M	O	N	T	E	M	O	N	T	E	M	O	N	T	E	M	O	N	T	E	M	O	N
Testo chiaro:	s	p	o	s	t	a	r	e	t	r	u	p	p	e	s	u	c	i	m	a	e	s	t					
Testo in cifra:	E	D	B	L	X	M	F	R	M	V	G	D	C	X	W	G	Q	V	F	E	Q	G	G					

Rimase inviolato fino a metà Ottocento
(Storia dei crittogrammi di Bale!!!)

Crittografia classica: crittografia con calcolatori

3. La terza, e forse più importante, differenza è che un computer scambia e traspone numeri anziché caratteri alfabetici.

Matematici e scienziati prendono il posto dei linguisti.

Prima della cifratura un messaggio dev'essere convertito in cifre binarie

A	1000001	N	1001110
B	1000010	O	1001111
C	1000011	P	1010000
D	1000100	Q	1010001
E	1000101	R	1010010
F	1000110	S	1010011
G	1000111	T	1010100
H	1001000	U	1010101
I	1001001	V	1010110
J	1001010	W	1010111
K	1001011	X	1011000
L	1001100	Y	1011001
M	1001101	Z	1011010

American Standard Code for Information Interchange (ASCII)

Ciao = 1000011 1001001 1000001 1001111

Crittografia classica: protocollo RSA

Cifratura asimmetrica

! NUMERI PRIMI

Classicamente il miglior algoritmo di fattorizzazione di un numero N in primi richiede un tempo esponenziale: non risolubile!

Chi poteva garantire che non si sarebbe trovato un algoritmo più efficiente?

Shor 1994

Algoritmo quantistico di fattorizzazione troppo complesso per il nostro percorso!

Crittografia quantistica: fotoni

Charles Bennett

Jilles Brassard

Quantum Cryptography

Charles H. Bennett, Gilles Brassard and Artur K. Ekert

1984

Protocollo BB84

Sfortunatamente inviare una chiave privata in modo sicuro è difficile in quanto richiede l'uso di qualche altro schema di crittografia come l'RSA che è teoricamente violabile. In alternativa entrambe le parti possono incontrarsi faccia a faccia per scambiarsi la chiave, ma questo a volte non è fattibile. Fortunatamente la distribuzione quantistica delle chiavi (QKD) propone una soluzione per questo.

Necessità di un protocollo di distribuzione di chiavi quantistico

Vernman Cipher

The Vernman cipher (one time pad) is theoretically unbreakable if implemented correctly. It requires three things:

1. A private key that is shared between both parties
2. That the key be longer than or equal to the size of the message
3. A new key to be used for each message sent

```
      H       E       L       L       O  message
    7 (H)   4 (E)  11 (L)  11 (L)  14 (O) message
+ 23 (X)  12 (M)   2 (C)  10 (K)  11 (L) key
= 30      16      13      21      25     message + key
=  4 (E)  16 (Q)  13 (N)  21 (V)  25 (Z) (message + key) mod 26
       E       Q       N       V       Z  → ciphertext
```

Figure 1: Vernman cipher encryption [1]

In this example the each number in the key is used to move a letter across the alphabet.
Note: the first 'L' in HELLO is changed to 'N' and the second 'L' to 'V' (this makes cryptanalysis difficult)

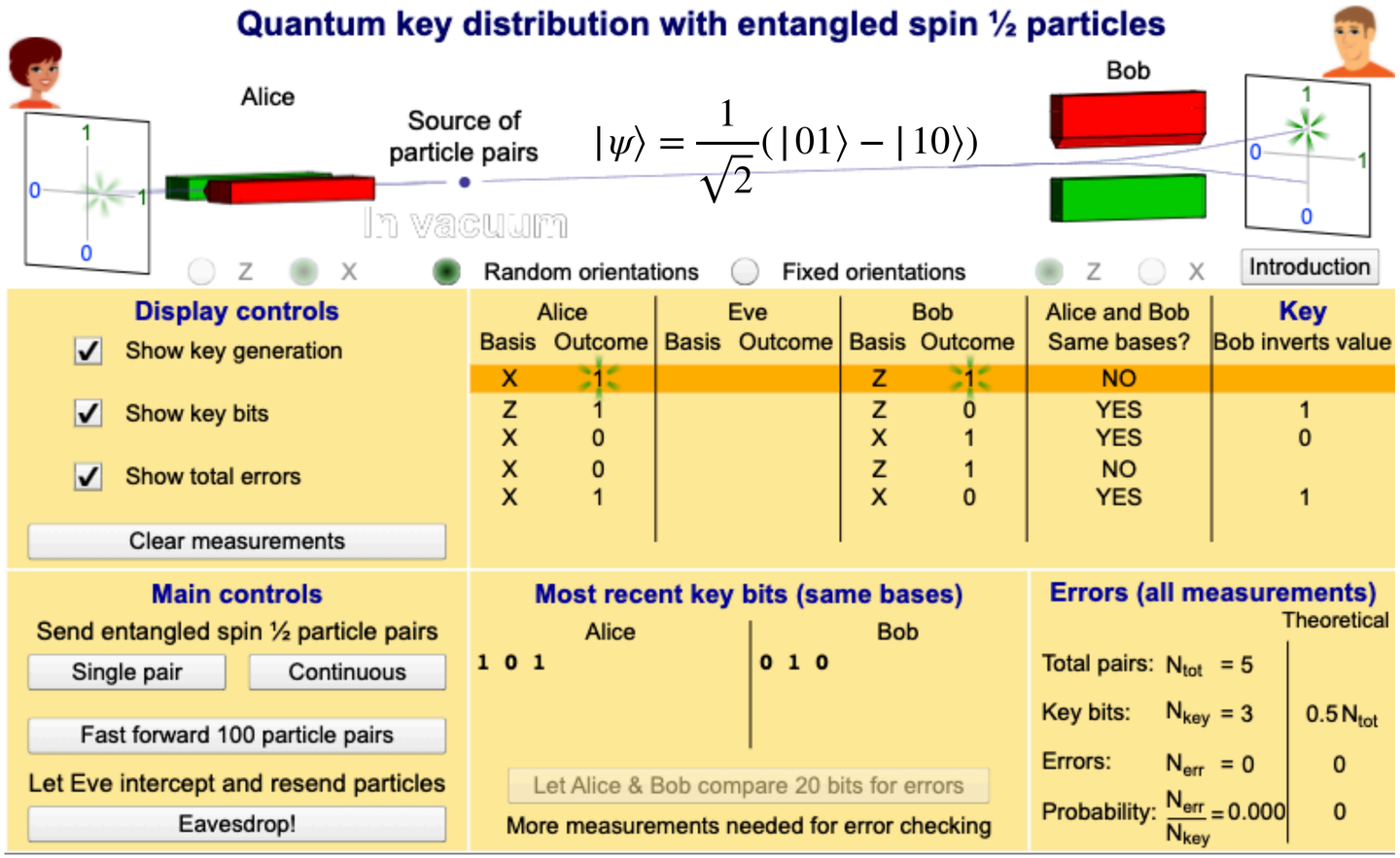
```
       E       Q       N       V       Z  ciphertext
    4 (E)  16 (Q)  13 (N)  21 (V)  25 (Z) ciphertext
-  23 (X)  12 (M)   2 (C)  10 (K)  11 (L) key
= -19       4      11      11      14     ciphertext - key
=   7 (H)   4 (E)  11 (L)  11 (L)  14 (O) ciphertext - key (mod 26)
       H       E       L       L       O  → message
```

Figure 2: Vernman cipher decryption [1]

Unfortunately sending a private key securely is difficult as it requires the use of some other encryption scheme such as RSA which is theoretically crackable. Alternatively both parties can meet face-to-face to exchange the key, but this is sometimes unfeasible. Luckily quantum key distribution (QKD) proposes a solution for this.

Crittografia quantistica: spin

Protocollo BBM92: esercizio



VOLUME 68, NUMBER 5 PHYSICAL REVIEW LETTERS 3 FEBRUARY 1992

Quantum Cryptography without Bell's Theorem

Charles H. Bennett
IBM Research Division, T. J. Watson Research Center, Yorktown Heights, New York 10598

Gilles Brassard
Département IRO, Université de Montréal, CP 6128, succursale "A," Montréal, Québec, Canada H3C 3J7

N. David Mermin
Laboratory of Atomic and Solid State Physics, Cornell University, Ithaca, New York, 14853-2501
(Received 26 September 1991)