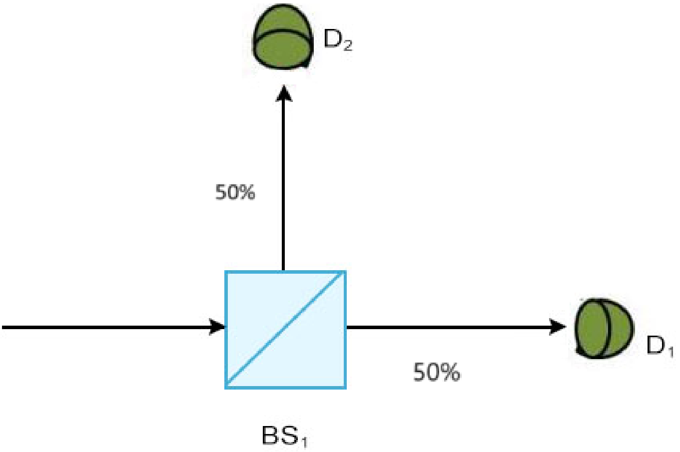
Quantum Computing $|101\rangle$

Alessio Baldelli, PhD Student @ Università Politecnica delle Marche
Gabriele Tedeschi, PhD Student @ Università di Pisa

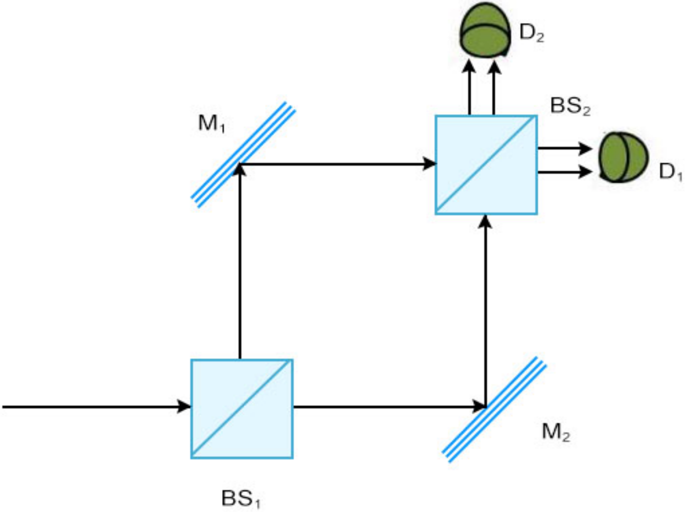
Outline

0. Come nasce la Quantum Theory?
1. Qubits e Sovrapposizione
2. Trasformazioni Invertibili
3. Entanglement

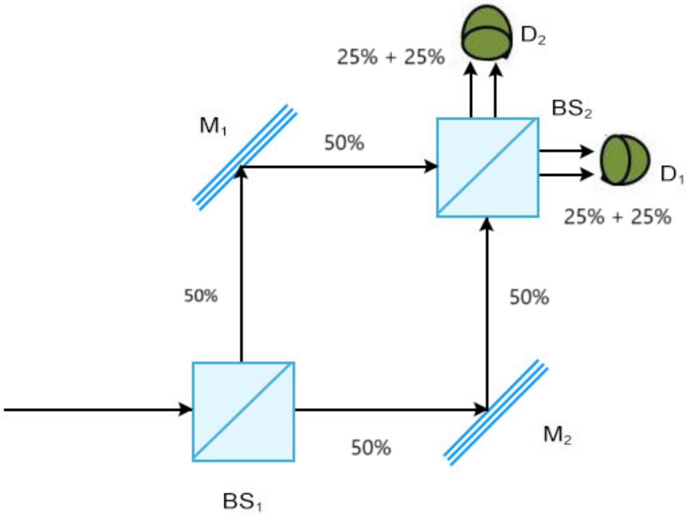
Esperimento nr. 1



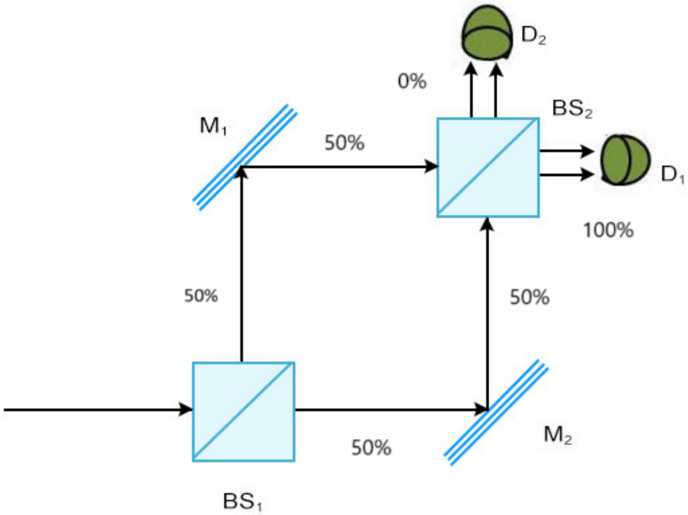
Esperimento nr. 2



Esperimento nr. 2



Esperimento nr. 2



I Qubits

Un qubit è il più piccolo sistema quantistico, ha soltanto due **stati calssici**: $|0\rangle$ e $|1\rangle$. Per esempio, lo spin di una particella, l'energia di un elettrone, la polarizzazione della luce...

I Qubits

Un qubit è il più piccolo sistema quantistico, ha soltanto due **stati calssici**: $|0\rangle$ e $|1\rangle$. Per esempio, lo spin di una particella, l'energia di un elettrone, la polarizzazione della luce...
Un qubit può essere in una **sovrapposizione** di stati:

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \qquad \text{con } \textbf{ampiezze } \alpha, \beta \in \mathbb{C}$$
$$|\alpha|^2 + |\beta|^2 = 1$$

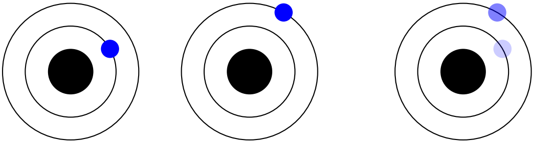
I Qubits

Un qubit è il più piccolo sistema quantistico, ha soltanto due **stati calssici**: $|0\rangle$ e $|1\rangle$. Per esempio, lo spin di una particella, l'energia di un elettrone, la polarizzazione della luce...

Un qubit può essere in una **sovrapposizione** di stati:

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \qquad \text{con } \textbf{ampiezze } \alpha, \beta \in \mathbb{C}$$

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



$|0\rangle$ $\qquad$ $|1\rangle$ $\qquad$ $\sqrt{\frac{1}{4}}\,|0\rangle + \sqrt{\frac{3}{4}}\,|1\rangle$

Misurare un qubit

Quando **osserviamo** un qubit in sovrapposizione, esso **decade** in uno stato classico.
Il qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ **decade**:

Misurare un qubit

Quando **osserviamo** un qubit in sovrapposizione, esso **decade** in uno stato classico.

Il qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ **decade**:

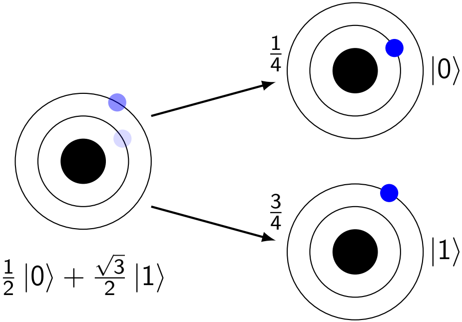
- in $|0\rangle$ con probabilità $|\alpha|^2$
- in $|1\rangle$ con probabilità $|\beta|^2$

Misurare un qubit

Quando **osserviamo** un qubit in sovrapposizione, esso **decade** in uno stato classico.

Il qubit $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ **decade**:

- in $|0\rangle$ con probabilità $|\alpha|^2$
- in $|1\rangle$ con probabilità $|\beta|^2$



Un po' di matematica

Lo stato di un qubit si rappresenta come un vettore $|\psi\rangle$ nello spazio vettoriale $\mathbb{C}^2$.

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \quad |+\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \quad |-\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}$$

Un po' di matematica

Lo stato di un qubit si rappresenta come un vettore $|\psi\rangle$ nello spazio vettoriale $\mathbb{C}^2$.

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \quad |+\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \quad |-\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}$$

Abbiamo anche coefficienti complessi:

$$|i\rangle = \frac{1}{\sqrt{2}} |0\rangle + \frac{1}{\sqrt{2}} i \, |1\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \frac{1}{\sqrt{2}} i \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ i \end{pmatrix}$$

Un po' di matematica

Lo stato di un qubit si rappresenta come un vettore $|\psi\rangle$ nello spazio vettoriale $\mathbb{C}^2$.

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \quad |+\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \quad |-\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}$$

Abbiamo anche coefficienti complessi:

$$|i\rangle = \frac{1}{\sqrt{2}} |0\rangle + \frac{1}{\sqrt{2}} i\, |1\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \frac{1}{\sqrt{2}} i \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ i \end{pmatrix}$$

Il prodotto interno fra 2 vettori si scrive $\langle\psi|\phi\rangle$

$$|\psi\rangle = \alpha\, |0\rangle + \beta\, |1\rangle \qquad |\langle 0|\psi\rangle|^2 = |\alpha|^2$$

Un po' di matematica

Lo stato di un qubit si rappresenta come un vettore $|\psi\rangle$ nello spazio vettoriale $\mathbb{C}^2$.

$$|0\rangle = \begin{pmatrix}1\\0\end{pmatrix} \quad |1\rangle = \begin{pmatrix}0\\1\end{pmatrix} \quad |+\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix} \quad |-\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix}$$

Abbiamo anche coefficienti complessi:

$$|i\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}i\,|1\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\end{pmatrix} + \frac{1}{\sqrt{2}}i\begin{pmatrix}0\\1\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\i\end{pmatrix}$$

Il prodotto interno fra 2 vettori si scrive $\langle\psi|\phi\rangle$

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \qquad |\langle 0|\psi\rangle|^2 = |\alpha|^2$$

Ci limitiamo solo a **vettori con norma unitaria**: $\langle\psi|\psi\rangle = 1$.

Gate Quantistici

Un quantum computer è in grado di applicare delle **trasformazioni**, o **gate**, che cambiano stato del qubit.

Gate Quantistici

Un quantum computer è in grado di applicare delle **trasformazioni**, o **gate**, che cambiano stato del qubit.

Gate di un computer classico:

$$NOT, AND, OR, XOR...$$

Gate Quantistici

Un quantum computer è in grado di applicare delle **trasformazioni**, o **gate**, che cambiano stato del qubit.

Gate di un computer classico:

$$NOT, AND, OR, XOR...$$

Gate di un computer quantistico:

$$X, Z, T, H, CNOT, CCNOT$$

Gate Quantistici – ctd.

X è (quasi) il *NOT classico*: $X\left|0\right\rangle = \left|1\right\rangle,\ X\left|1\right\rangle = \left|0\right\rangle$.

Gate Quantistici – ctd.

X è (quasi) il *NOT classico*: $X|0\rangle = |1\rangle\,,\; X|1\rangle = |0\rangle$.

Quanto vale $X|\psi\rangle$, per una sovrapposizione $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$?

Gate Quantistici – ctd.

X è (quasi) il *NOT classico*: $X\,|0\rangle = |1\rangle\,,\ X\,|1\rangle = |0\rangle$.

Quanto vale $X\,|\psi\rangle$, per una sovrapposizione $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$?

Si può calcolare facilmente per **linearità**!

$$X(\alpha\,|0\rangle + \beta\,|1\rangle) = (\alpha \cdot X\,|0\rangle) + (\beta \cdot X\,|1\rangle) = \beta\,|0\rangle + \alpha\,|1\rangle\,.$$

Il gate X scambia i valori delle ampiezze di probabilità tra $|0\rangle$ e $|1\rangle$.

Gate Quantistici – ctd.

X è (quasi) il *NOT classico*: $X\left|0\right\rangle = \left|1\right\rangle,\ X\left|1\right\rangle = \left|0\right\rangle$.

Quanto vale $X\left|\psi\right\rangle$, per una sovrapposizione $\left|\psi\right\rangle = \alpha\left|0\right\rangle + \beta\left|1\right\rangle$?

Si può calcolare facilmente per **linearità**!

$$X(\alpha\left|0\right\rangle + \beta\left|1\right\rangle) = (\alpha \cdot X\left|0\right\rangle) + (\beta \cdot X\left|1\right\rangle) = \beta\left|0\right\rangle + \alpha\left|1\right\rangle.$$

Il gate X scambia i valori delle ampiezze di probabilità tra $\left|0\right\rangle$ e $\left|1\right\rangle$.

Si noti che:

$$X \circ X = I \qquad X\left|+\right\rangle = \left|+\right\rangle$$

Gate Quantistici – ctd.

H è l'operatore di Hadamard, definito da: $H|0\rangle = |+\rangle$, $H|1\rangle = |-\rangle$

$$H(\alpha|0\rangle + \beta|1\rangle) = \alpha|+\rangle + \beta|-\rangle$$

Si noti che:

- $H \circ H = I$

Gate Quantistici – ctd.

H è l'operatore di Hadamard, definito da: $H\,|0\rangle = |+\rangle\,,\ H\,|1\rangle = |-\rangle$

$$H(\alpha\,|0\rangle + \beta\,|1\rangle) = \alpha\,|+\rangle + \beta\,|-\rangle$$

Si noti che:

- $H \circ H = I$

Z è simile a X, ma per $\{|+\rangle\,, |-\rangle\}$:

$$Z\,|+\rangle = |-\rangle \qquad Z\,|-\rangle = |+\rangle$$

Si noti che:

- $Z \circ Z = I$
- $Z\,|0\rangle = |0\rangle$

Unitarie

Tutti i gate quantistici sono descritti da **trasformazioni unitaria**.

Per un singolo qubit:

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \qquad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \qquad H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

Unitarie

Tutti i gate quantistici sono descritti da **trasformazioni unitaria**.

Per un singolo qubit:

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \qquad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \qquad H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

Cosa sono gli operatori unitari?

Un operatore lineare U si dice *unitario* quando $UU^\dagger = U^\dagger U = I$, dove $U^\dagger$ è il trasposto coniugato di U.

Unitarie

Tutti i gate quantistici sono descritti da **trasformazioni unitaria**.

Per un singolo qubit:

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \qquad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \qquad H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

Cosa sono gli operatori unitari?

Un operatore lineare U si dice *unitario* quando $UU^\dagger = U^\dagger U = I$, dove $U^\dagger$ è il trasposto coniugato di U.

Tutte le trasformazioni unitarie sono **invertibili**.

Paradosso del gatto di Schrödinger

Il paradosso del gatto di Schrödinger è un esperimento mentale ideato nel 1935 da Erwin Schrödinger con lo scopo di illustrare come la meccanica quantistica fornisca risultati paradossali se applicata a un sistema fisico macroscopico.

DIE NATURWISSENSCHAFTEN

23. Jahrgang | 29. November 1935 | Heft 48

Die gegenwärtige Situation in der Quantenmechanik.

Von E. SCHRÖDINGER, Oxford.

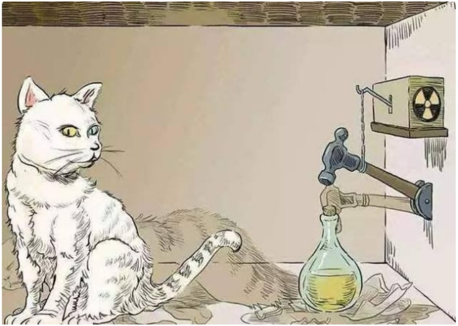
Inhaltsübersicht.

§ 1. Die Physik der Modelle.
§ 2. Die Statistik der Modellvariablen in der Quantenmechanik.
§ 3. Beispiele für Wahrscheinlichkeitsvoraussagen.
§ 4. Kann man der Theorie ideale Gesamtheiten unterlegen?
§ 5. Sind die Variablen wirklich verwaschen?
§ 6. Der bewußte Wechsel des erkenntnistheoretischen Standpunktes.

Gebilde, das sich mit der Zeit verändert, das verschiedene *Zustände* annehmen kann; und wenn ein Zustand durch die nötige Zahl von Bestimmungsstücken bekannt gemacht ist, so sind nicht nur alle anderen Stücke in diesem Augenblick mit gegeben (wie oben am Dreieck erläutert), sondern ganz ebenso alle Stücke, der genaue Zustand, zu jeder bestimmten späteren Zeit; ähnlich wie die Beschaffenheit eines Dreiecks an der Basis seine

Paradosso del gatto di Schrödinger (ctd.)

Il fisico immagina che dentro una scatola ci sia un gatto vivo, una fiala di veleno, un atomo radioattivo e un meccanismo che aziona un martello. Se l'atomo decade spontaneamente, il meccanismo si attiva e rilascia il veleno, uccidendo il gatto.



Sappiamo che l'atomo può decadere o meno con probabilità del 50%.

Paradosso del gatto di Schrödinger (ctd.)

Dunque lo stato dell'atomo si trova in una *sovrapposizione* di due possibili stati:

$$|A\rangle = \frac{1}{\sqrt{2}}(|\text{decaduto}\rangle + |\text{non decaduto}\rangle).$$

Questa condizione, ovviamente, riguarda anche il gatto

$$|G\rangle = \frac{1}{\sqrt{2}}(|\text{morto}\rangle + |\text{vivo}\rangle),$$

almeno fino a quando non si compie un'osservazione, aprendo la scatola.

Paradosso del gatto di Schrödinger (ctd.)

Dunque lo stato dell'atomo si trova in una *sovrapposizione* di due possibili stati:

$$|A\rangle = \frac{1}{\sqrt{2}}(|\text{decaduto}\rangle + |\text{non decaduto}\rangle).$$

Questa condizione, ovviamente, riguarda anche il gatto

$$|G\rangle = \frac{1}{\sqrt{2}}(|\text{morto}\rangle + |\text{vivo}\rangle),$$

almeno fino a quando non si compie un'osservazione, aprendo la scatola.

In effetti però, la teoria quantistica afferma che il sistema "atomo + gatto" sia inevitabilmente correlato, quindi si ha:

$$|A, G\rangle = \frac{1}{\sqrt{2}}(|\text{decaduto, morto}\rangle + |\text{non decaduto, vivo}\rangle).$$

la sovrapposizione di stati riguarda quindi l'intero sistema.

Sistemi quantum composti

Per affrontare problemi complessi abbiamo bisogno di padroneggiare più qubit contemporaneamente...

Sistemi quantum composti

Per affrontare problemi complessi abbiamo bisogno di padroneggiare più qubit contemporaneamente... come fa un quantum computer!

Sistemi quantum composti

Per affrontare problemi complessi abbiamo bisogno di padroneggiare più qubit contemporaneamente... come fa un quantum computer!

Se ci sono due qubit lo spazio di stato è $\mathbb{C}^4$, e i possibili stati validi sono:

$$|\psi\rangle = \alpha\,|00\rangle + \beta\,|01\rangle + \gamma\,|10\rangle + \delta\,|11\rangle\,,$$

$$\text{con } \alpha, \beta, \gamma, \delta \in \mathbb{C} \text{ t.c. } |\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1 \quad \text{e}$$

$$|00\rangle = \begin{pmatrix}1\\0\\0\\0\end{pmatrix} \; |01\rangle = \begin{pmatrix}0\\1\\0\\0\end{pmatrix} \; |10\rangle = \begin{pmatrix}0\\0\\1\\0\end{pmatrix} \; |11\rangle = \begin{pmatrix}0\\0\\0\\1\end{pmatrix}.$$

Prodotto tensore

Due sistemi si **compongono** attraverso il *prodotto tensore*.

Prodotto tensore

Due sistemi si **compongono** attraverso il *prodotto tensore*.

Lo stato di un registro con due qubit, i cui stati sono $|0\rangle$ e $|+\rangle$, è

$$|0\rangle \otimes |+\rangle = \begin{pmatrix} 1\,|+\rangle \\ 0\,|+\rangle \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} \qquad |+\rangle \otimes |+\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1\,|+\rangle \\ 1\,|+\rangle \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}$$

Stati entangled

I sistemi classici composti possono essere sempre descritti dai bit che li compongono . . .

Stati entangled

I sistemi classici composti possono essere sempre descritti dai bit che li compongono . . . È vero anche per i sistemi quantum?

Stati entangled

I sistemi classici composti possono essere sempre descritti dai bit che li compongono ... È vero anche per i sistemi quantum? **No!**
Infatti vale che:

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}.$$

Stati entangled

I sistemi classici composti possono essere sempre descritti dai bit che li compongono ... È vero anche per i sistemi quantum? **No!**
Infatti vale che:

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\\0\\1\end{pmatrix}.$$

Questo è un esempio di stato entangled, poiché non esiste una combinazione di due stati quantum, $|\phi\rangle$ and $|\psi\rangle$, tale che $|\phi\rangle \otimes |\psi\rangle = |\Phi^+\rangle$.

Stati entangled

I sistemi classici composti possono essere sempre descritti dai bit che li compongono ... È vero anche per i sistemi quantum? **No!**
Infatti vale che:

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\\0\\1\end{pmatrix}.$$

Questo è un esempio di stato entangled, poiché non esiste una combinazione di due stati quantum, $|\phi\rangle$ and $|\psi\rangle$, tale che $|\phi\rangle \otimes |\psi\rangle = |\Phi^+\rangle$.

Uno stato quantum che non può essere ottenuto dal prodotto tensore di stati più piccoli è detto *entangled*.

Esempio su circuiti

Una delle unitarie su due qubit è il CNOT:

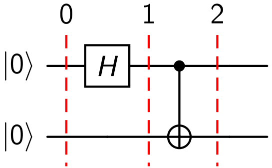
$$CNOT\,|00\rangle = |00\rangle \qquad CNOT\,|01\rangle = |01\rangle$$
$$CNOT\,|10\rangle = |11\rangle \qquad CNOT\,|11\rangle = |10\rangle$$

Esempio su circuiti

Una delle unitarie su due qubit è il CNOT:

$$CNOT\,|00\rangle = |00\rangle \qquad CNOT\,|01\rangle = |01\rangle$$
$$CNOT\,|10\rangle = |11\rangle \qquad CNOT\,|11\rangle = |10\rangle$$

Gli stati entangled possono essere ottenuti attraverso gate unitari:



$$|\psi_0\rangle = |00\rangle$$
$$|\psi_1\rangle = (H \otimes I)\,|00\rangle = |{+}0\rangle$$
$$|\psi_2\rangle = CNOT\,|{+}0\rangle = |\Phi^+\rangle$$

Misure di stati entangled

L'entanglement implica una forte correlazione tra gli stati, per questo il risultato delle misure è fortemente controintuitivo.

Misure di stati entangled

L'entanglement implica una forte correlazione tra gli stati, per questo il risultato delle misure è fortemente controintuitivo.