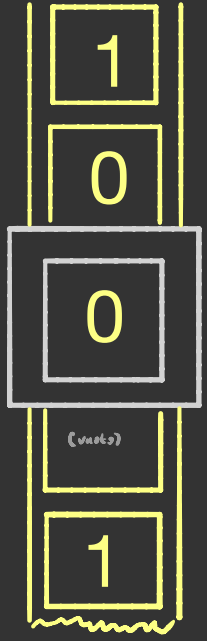
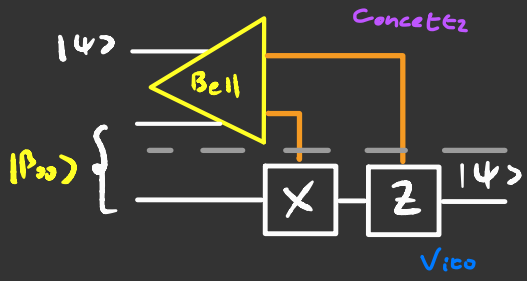
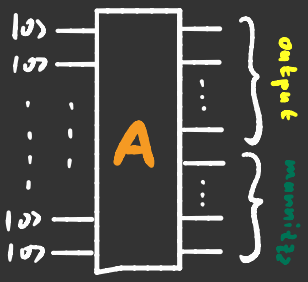
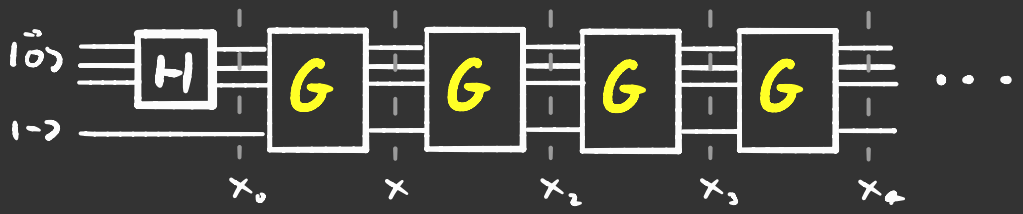
Computazione Quantistica

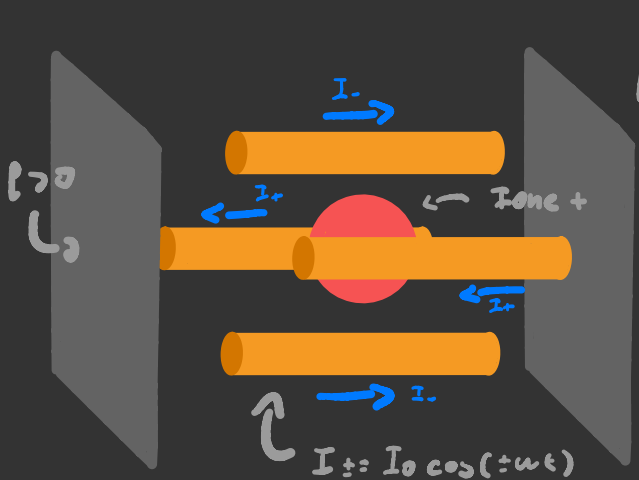
Francesco Sacco A.A. 2019-2020

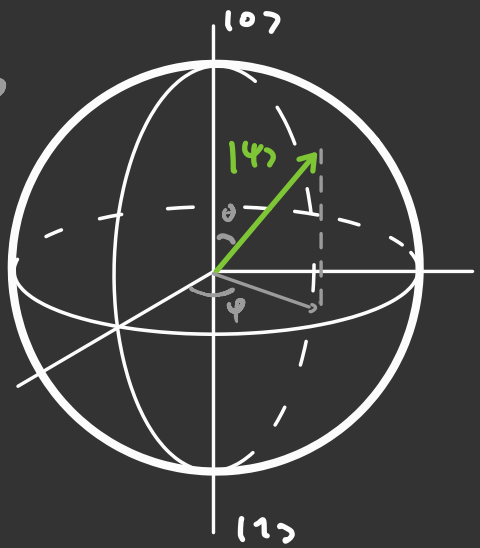








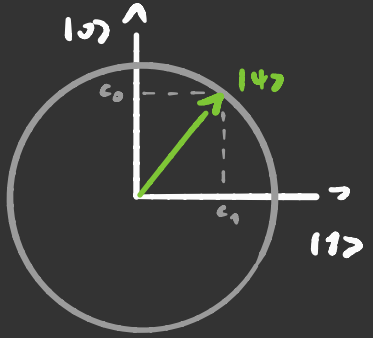




Qbit

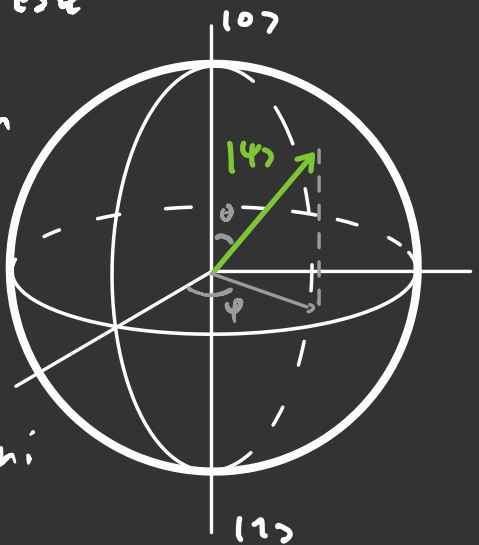
In computazione classica un bit è una variabile che può valere 0 o 1, invece, in computazione quantistica un qbit è una funzione d'onda che appartiene allo span $\{|0\rangle, |1\rangle\}$.
Un generico qbit $|\psi\rangle$ può essere scritto così

$$|\psi\rangle = c_0|0\rangle + c_1|1\rangle = \begin{vmatrix} c_0 \\ c_1 \end{vmatrix} \quad \text{con } |c_0|^2 + |c_1|^2 = 1$$



È possibile rappresentare $|\psi\rangle$ graficamente in due modi.
Il primo è di assegnare a ogni funzione d'onda un asse cartesiano, questo però si limita a rappresentare fedelmente solo funzioni d'onda che hanno $c_0, c_1 \in \mathbb{R}$
L'altro modo è quello di rappresentare sulla sfera di Bloch. Visto che se si manda $|\psi\rangle \to e^{i2}|\psi\rangle$ non cambia niente, io posso scrivere

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\varphi}\operatorname{sen}\left(\frac{\theta}{2}\right)|1\rangle$$

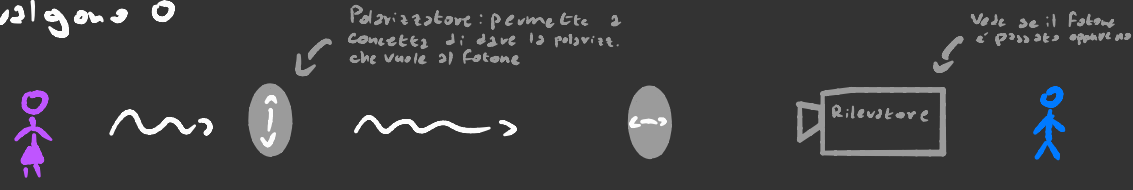


Questo mi permette di rappresentare per bene $|\psi\rangle$ e di rappresentare operatori unitari come rotazioni della sfera.

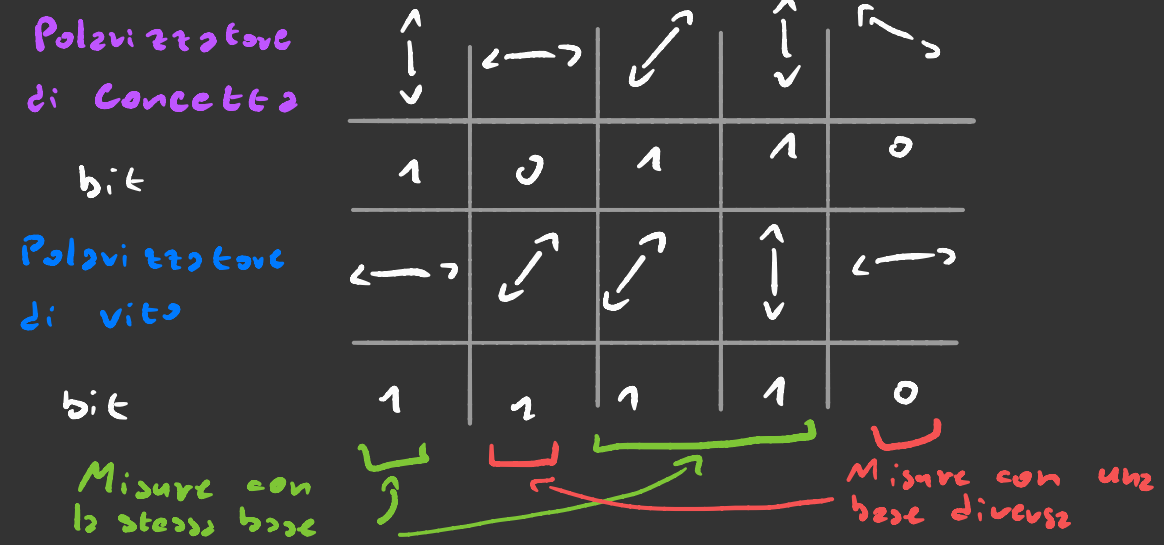
Distribuzione di chiavi Quantistiche

Per comunicare in modo sicuro i dati vanno criptografati e per decodificarli c'è bisogno di una chiave.
Mandare una chiave però è un processo soggetto a vulnerabilità, ma con la meccanica quantistica inviare chiavi può diventare un processo sicuro.
Supponiamo che **Concetta** vuole inviare una chiave a **Vito** e come qbit usano dei Fotoni

Concetta invia a **Vito** alcune volte dei Fotoni polarizzati: così ↕ o così ↔ oppure ↗ o ↘
e ogni volta che ne invia uno si segna com'è polarizzato
I Fotoni polarizzati ↕ e ↗ valgono 1, quelli ↔ e ↘ valgono 0



Alla fine della trasmissione di fotoni Vito annuncia **Pubblicamente** la sequenza di orientazione di filtri che ha usato ma non dice quello che misura il rilevatore.
A questo punto Concetta dice pubblicamente quali basi per la misurazione andavano bene.



Infine Vito manda indietro a Concetta i fotoni misurati con la stessa base, e se combaciano allora i due usano quei bit come chiave.

Ma perché Vito e Concetta devono fare tutta sta mala vita per inviarsi una chiave? Per capirlo dobbiamo vedere che succede se una persona che chiameremo Ateneide cerca di intercettare la chiave.

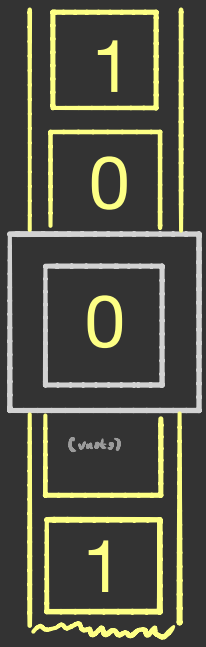
Prendiamo come esempio il terzo bit della sequenza se Ateneide osserva il bit con un polarizzatore messo ↕ e, supponiamo, che gli esca 0 e poi lo invia così come l'ha misurato, ma poi Vito lo misura ↗ e gli torna 0.

Quindi si crea una discrepanza tra quello che Vito e Concetta misurano nonostante usino la stessa base.

In totale queste discrepanze si verificheranno il 25% delle volte.

Concetta allora si rende conto che il messaggio è stato intercettato e blocca tutto.

Macchine di Turing



Una macchina di Turing è una macchina che è composta da un nastro infinito con delle lettere di un alfabeto finito, una testa che è in grado di leggere e muoversi di un passo alla volta a destra o a sinistra.
Inoltre c'è un registro dove sta scritto lo stato e ad ogni stato è associata un' istruzione tipo così:

```
stato 1 7 1

se c'é scritto 0 :
  mettici un 1 ;
  spostati a destra;
  vai allo stato 1 5 ;
Altrimenti:
  vai allo stato 8 8 ;
```

Gli stati fanno le veci del codice di un programma, il nastro fa le veci dell'input e dell'output e la testa è il processore.

Una funzione calcolabile è una funzione che ha un algoritmo che prima o poi finisce. *A dire il vero non esiste una definizione vera e propria di funzione calcolabile*

L'ipotesi di Church-Turing dice che una funzione è calcolabile se è solo se è calcolabile da una macchina di Turing. (Non dimostrata)
Questo non ci dice nulla sull'efficenza della macchina di Turing.

L'efficenza di una funzione è indicato con $O(f(n))$ dove n è il numero di bit dell'input. "O" grande

Un algoritmo è detto efficente se $\exists k$ t.c. $O(f(n)) < O(n^k)$

Nella realtà si è notato che alcuni algoritmi sono più efficienti se la macchina di Turing è dotata di un componente che per ogni operazione scelga un numero a caso (0 o 1), non è chiaro se questo è dovuto al fatto che a nessuno sia venuto in mente come fare la stessa funzione con la macchina di Turing non random.

L'ipotesi forte di Church-Turing dice che Una macchina di Turing probabilistica può calcolare ogni funzione calcolabile efficentemente. (non dimostrata)

Tuttavia sembrerebbe che la meccanica classica non sembra in grado di simulare efficentemente la meccanica quantistica

Ipotesi forte di Church Turing Quantistica

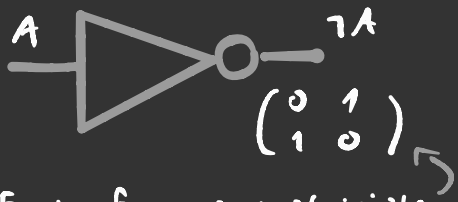
> Una macchina di Turing quantistica può calcolare efficentemente ogni funzione calcolabile

Anche questa non è dimostrata, ma si basa sul fatto che con i computer quantistici è stato possibile risolvere funzioni che si pensava avessero fondamentalmente una complessità esp.

Calcolatori: 2
Porte logiche

I blocchi fondamentali di calcolatori che si usano oggi sono le porte logiche.

Partiamo dalla porta NOT: essa inverte il bit che gli arriva.

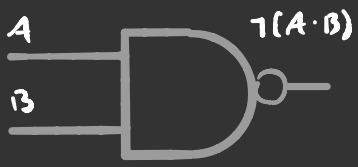


É possibile scrivere l'operazione che fa in forma matriciale

Questa porta é Invertibile, e questa é una cosa buona in computazione quantistica.

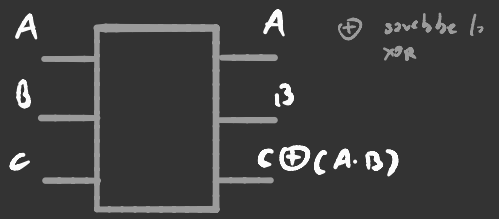
Visto che l'Operatore di evoluzione temporale é unitario, allora ogni porta logica quantistica dev'essere.

Ad esempio la porta logica NAND, che é la più importante dell' elettronica digitale, non può esistere in un computer quantistico così com'é visto che é non invertibile (ha 2 input e un output).



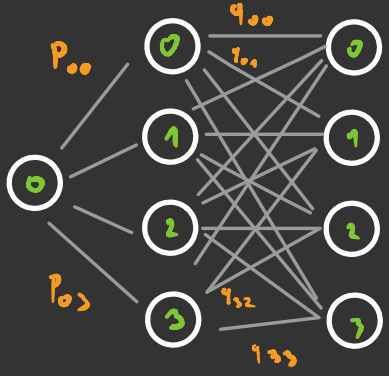
É possibile creare una porta reversibile tale che uno dei suoi output sia (anche) una porta NAND

La porta logica a destra é un esempio di porta reversibile che ha come uno degli output un NAND o un AND a seconda se C vale 1 o 0



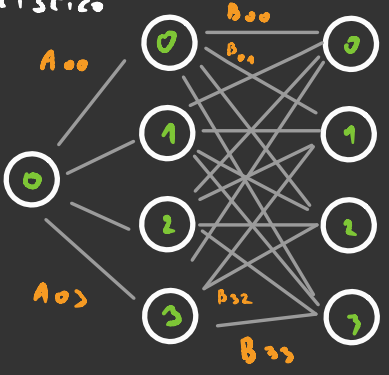
Differenza tra algoritmi Quantistici e Probabilistici

Prendiamo un algoritmo probabilistico che parte da uno stato 0, esso avrà una certa probabilità di finire al primo passo dell'algoritmo a uno stato i uguale a $P_{0i} \geq 0$ al secondo passo ogni stato i-esimo avrà una certa probabilità di finire in uno stato j uguale a $q_{ij} \geq 0$, quindi la probabilità di partire dallo stato iniziale 0 e finire in uno stato finale j è $\sum_i P_{0i} q_{ij}$.



Essendo una somma di termini tutti positivi, l'unico modo per fare zero è che tutti i termini della somma siano nulli.

Se invece prendiamo un algoritmo quantistico dove A e B sono operatori unitari abbiamo che i termini, essendo in $\mathbb{C}$ possono interferire tra di loro, questa è una proprietà estremamente comoda che gli algoritmi probabilistici non hanno.

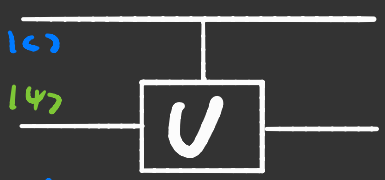


In ogni caso, la probabilità di partire dallo stato 0 e arrivare allo stato j è $|\sum_i A_{0i} B_{ij}|^2 \leq \sum_i |A_{0i}|^2 |B_{ij}|^2$ <

Questa ultima sommatoria è quello che succede se a ogni passo si effettua una misurazione ed è equivalente ad un algoritmo probabilistico

Porte Logiche controllate

Supponiamo di avere 2 qbit $|c\rangle$ e $|\psi\rangle$ e un operatore Unitario U. Il sistema funziona così



$$\begin{cases} \text{Se } |c\rangle = |1\rangle, \text{ allora } |\psi\rangle \to U|\psi\rangle \text{ e } |c\rangle \to |1\rangle \\ \text{se } |c\rangle = |0\rangle, \text{ allora } |\psi\rangle \to |\psi\rangle \text{ e } |c\rangle \to |0\rangle \end{cases}$$

Quindi $|c\rangle$ rimane invariato e fa da "qbit di controllo"

È possibile scrivere l'azione del sistema.

La porta complessiva che agisce sullo stato $|c\rangle|\psi\rangle$ è definita c-U che sta per control-U

Supponiamo che l'operatore U sia una porta NOT, essa ha 2 autostati $|\pm\rangle = \frac{|0\rangle \pm |1\rangle}{\sqrt{2}}$ con autovalori ± 1

$$c\text{-}U|0\rangle|\pm\rangle = |0\rangle|\pm\rangle \qquad c\text{-}U|1\rangle|\pm\rangle = |1\rangle \otimes (U|\pm\rangle) = \pm|1\rangle|\pm\rangle$$

Il fattore $\pm$ però è un fattore che appartiene all'intera Funzione d'onda, quindi è come se anche il bit di controllo viene effetto dall'operazione.

È possibile modificare il bit di controllo come in questo esempio.

$$c\text{-}U|\pm\rangle|-\rangle = c\text{-}U\left[\frac{|0\rangle \pm |1\rangle}{\sqrt{2}}\right]|-\rangle =$$

$$c\text{-}U\frac{|0\rangle|-\rangle}{\sqrt{2}} \pm c\text{-}U\frac{|1\rangle|-\rangle}{\sqrt{2}} = \frac{|0\rangle|-\rangle}{\sqrt{2}} \mp |1\rangle|-\rangle = |\mp\rangle|-\rangle$$

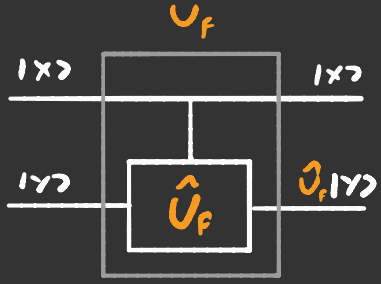
In questo caso è solo il bit di controllo a esser cambiato

L'Algoritmo di Deutsch

Supponiamo di avere una funzione $f: \{0,1\} \to \{0,1\}$ (Non necessariamente Reversibile)

è possibile creare un operatore U_f tale che

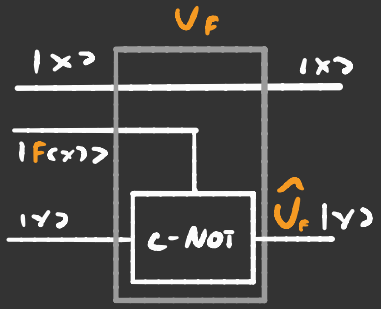
$U_f |x\rangle|y\rangle = |x\rangle|f(x) \oplus y\rangle$.



In questa operazione $y \to \neg y$ se $f(x)=1$ altrimenti viene inviato, quindi questa operazione è equivalente a dare un circuito logico fatto come nella figura 2.

Lavorando con gli stati puri è semplice calcolare quanto vale $f(x)$, adesso vediamo che succede con gli stati misti:

Se prendiamo $y = |-\rangle$, che è un autostato della porta NOT, $U_f|x\rangle|-\rangle = (-1)^{f(x)}|x\rangle|-\rangle$.



Seguendo il ragionamento della pagina di prima, se ad esempio

$|x\rangle = |+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$ $\quad U_f|+\rangle|-\rangle = \left[\frac{(-1)^{f(0)}|0\rangle}{\sqrt{2}} + \frac{(-1)^{f(1)}|1\rangle}{\sqrt{2}}\right]|-\rangle =$

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

Il Fattore di Fase, se si vuole effettuare una misura non serve a niente

$$U_f|+\rangle|-\rangle = \begin{cases} (-1)^{f(0)}|+\rangle|-\rangle & \text{se } f(0)=f(1) \\ (-1)^{f(0)}|-\rangle|-\rangle & \text{se } f(0)\neq f(1) \end{cases}$$

Così facendo con una singola operazione è possibile sapere se f sia pari o dispari

Questa cosa è importante perché in un calcolatore classico ci tocca calcolare sia $f(0)$ che $f(1)$ per vedere se è pari

Insieme Universale di porte quantistiche

Nei calcolatori classici qualunque tipo di circuito può essere espresso in termini di alcune semplici porte logiche. Vogliamo sapere se nei calcolatori quantistici è possibile fare lo stesso.

> Un insieme di porte logiche quantistiche è detto **Universale** se con esse è possibile approssimare arbitrariamente bene qualunque operatore unitario

C'è un teorema che non abbiamo dimostrato che dice che:

> La porta c-NOT con tutte le porte a singolo qbit formano un insieme Universale di porte quantistiche

Questa è un'ottima cosa perché nella realtà queste porte logiche sono perfettamente realizzabili.

Da questo punto in poi cercheremo di fare circuiti quantistici che siano facilmente scrivibili in termini della porta c-NOT e porte a singolo bit.

Una porta a singolo qbit che useremo spesso è quella di Hadamard H e la sua forma algebrica è così

$$H = \begin{vmatrix} 1 & 1 \\ 1 & -1 \end{vmatrix}$$

Algoritmo di Grover

Supponiamo di avere una funzione $f: \{0,1\}^n \to \{0,1\}$ e noi vogliamo trovare per quali valori la funzione faccia 1. Classicamente il modo in cui si risolve il problema è andare a tentativi, ma questo significa che $O(f) = O(2^n)$. Con l'algoritmo di Grover è possibile far sì che $O(f) = O(2^{\frac{n}{2}})$.

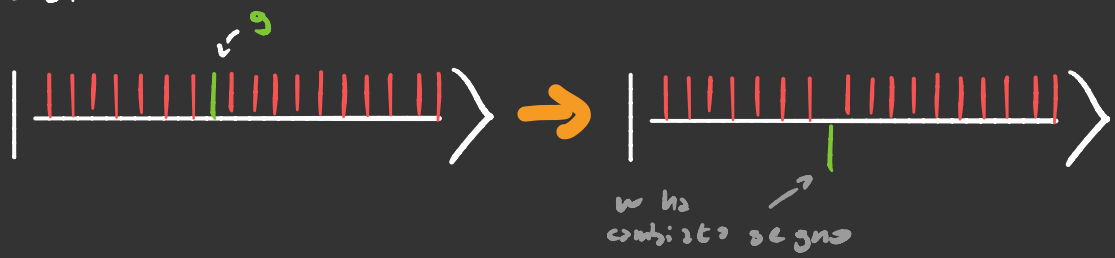
Prendiamo il solito operatore $U_f |x\rangle|b\rangle \to |x\rangle|b \oplus f(x)\rangle$, da ora in poi useremo $|b\rangle = |0\rangle$, e per semplificare sceglieremo una funzione che ha solo un bit $|g\rangle$ tale che $f(g) = 1$.

Parto con $|x\rangle = H^{\otimes n}|0\rangle = \sqrt{\frac{1}{2^n}}|g\rangle + \sqrt{\frac{2^n-1}{2^n}}|s\rangle$

$$\sqrt{\frac{1}{2^n}}|g\rangle + \sqrt{\frac{2^n-1}{2^n}}|s\rangle \left\{ \begin{array}{l} \\ \\ |0\rangle \end{array} \right. \boxed{U_f} \left. \begin{array}{l} \\ \\ \end{array} \right\} \quad \sqrt{\frac{1}{2^n}}|g\rangle|1\rangle + \sqrt{\frac{2^n-1}{2^n}}|s\rangle|0\rangle$$

Così facendo se misurando il bit di controllo esce $|b\rangle = |1\rangle$ allora misurando $|x\rangle$ esce $|x\rangle = |w\rangle$. C'è però il problema che la maggior parte delle volte $|b\rangle = |0\rangle$.

Se come input ci mettiamo $|b\rangle = |-\rangle$ l'operatore U_f inverte il segno della componente di $|x\rangle$ lungo $|w\rangle$ e lascia invariata la componente lungo $|s\rangle$, esso si può rappresentare così



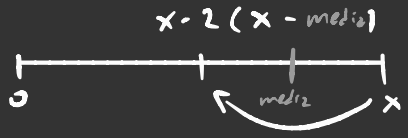
Se si concatena questo con un operatore che inverte rispetto alla media si amplifica la componente lungo $|g\rangle$

Così facendo abbiamo amplificato la componente di $|x\rangle$ lungo $|g\rangle$, per amplificarlo ancora di più basta ripetere l'operazione.

Prima di andare avanti dobbiamo vedere come scrivere in forma operatoriale questa riflessione rispetto alla media.

Per calcolare la media basta proiettare $|x\rangle$ su $|\psi\rangle = H^{\otimes n}|0\rangle$,

Guardando l'immagine a destra si capisce che l'operatore di inversione rispetto alla media è

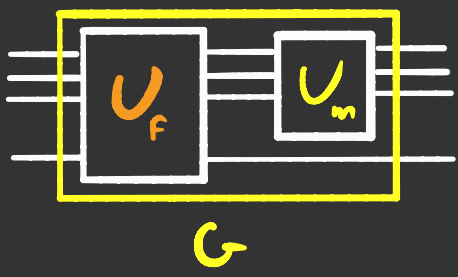


$$U_m = I - 2(I - |\psi\rangle\langle\psi|) = 2|\psi\rangle\langle\psi| - I$$

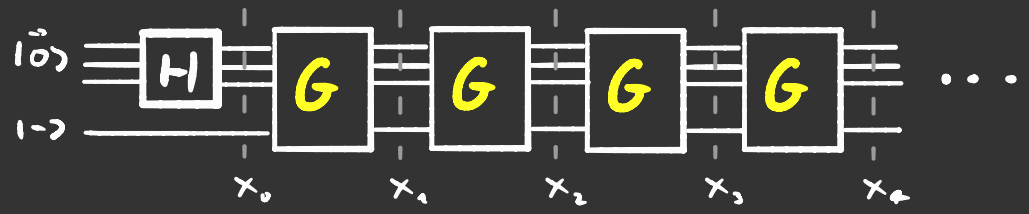
$|\psi\rangle$ rispetto alla base di Hadamard è $|\vec{0}\rangle$, quindi l'operatore di inversione rispetto alla media è scrivibile come

$$U_m = H^{\otimes n}(2|\vec{0}\rangle\langle\vec{0}| - I)H^{\otimes n}$$

Combinando U_f e U_m come a destra un operatore chiamato iteratore di Grover G che più si itera più si amplifica il Pattore moltiplicatore di $|g\rangle$.



OK, tutto bello, ma quante volte devo applicare G?

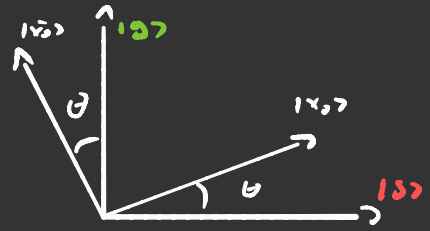


Per farlo vediamo quanto valgono i vettori $|x_i\rangle$, come già detto prima

$$|x_0\rangle = \sqrt{\frac{1}{2^n}}|g\rangle + \sqrt{\frac{2^n-1}{2^n}}|s\rangle \equiv \sin\theta|g\rangle + \cos\theta|s\rangle$$

definisco $\quad |\bar{x}_0\rangle \equiv \cos\theta|g\rangle - \sin\theta|s\rangle$

quindi $\begin{cases} |g\rangle = \sin\theta|x_0\rangle + \cos\theta|\bar{x}_0\rangle \\ |s\rangle = \cos\theta|x_0\rangle - \sin\theta|\bar{x}_0\rangle \end{cases}$



$$U_f|x_0\rangle = -\sin\theta|g\rangle + \cos(\theta)|s\rangle =$$

$$= -\sin^2\theta|x_0\rangle - \sin\theta\cos\theta|\bar{x}_0\rangle + \cos^2\theta|x_0\rangle - \sin\theta\cos\theta|\bar{x}_0\rangle$$

$$= \cos(2\theta)|x_0\rangle - \sin(2\theta)|\bar{x}_0\rangle$$

$$U_m U_f|x_0\rangle = U_m[\cos(2\theta)|x_0\rangle - \sin(2\theta)|\bar{x}_0\rangle] =$$

$$= \cos(2\theta)|x_0\rangle + \sin(2\theta)|\bar{x}_0\rangle =$$

$$= \sin(3\theta)|g\rangle + \cos(3\theta)|s\rangle$$

Questo è un vettore ruotato di 2θ rispetto alla base $|x_0\rangle, |\bar{x}_0\rangle$. Quindi rispetto alla base $|g\rangle, |s\rangle$ è un vettore ruotato di 3θ

Se si va a calcolare

$$(U_m U_f)^n |x_0\rangle = |x_n\rangle = \sin[(2n+1)\theta]|g\rangle + \cos[(2n+1)\theta]|s\rangle$$

Esiste una dimostrazione grafica, ma per ora non ho voglia di disegnare

Programmazione Superdensa

Supponiamo che Concetta vuole inviare due bit a Vito inviandogli solo un qbit, come deve fare?

Definiamo la base di Bell così

$$|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \qquad |\beta_{01}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$

$$|\beta_{10}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \qquad |\beta_{11}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

L'operatore che permette di passare dalla base computazionale a quella canonica è questo

La proprietà cruciale che viene usata in questo algoritmo è come si comporta lo stato di $|\beta_{00}\rangle$ rispetto a questi operatori:

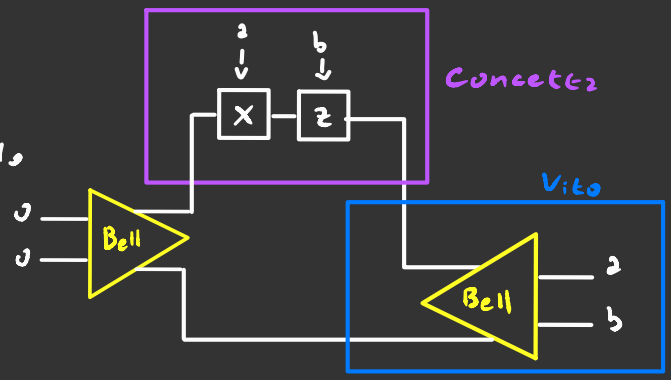
$I \otimes I \, |\beta_{00}\rangle = |\beta_{00}\rangle$ $\qquad X \otimes I \, |\beta_{00}\rangle = |\beta_{01}\rangle$

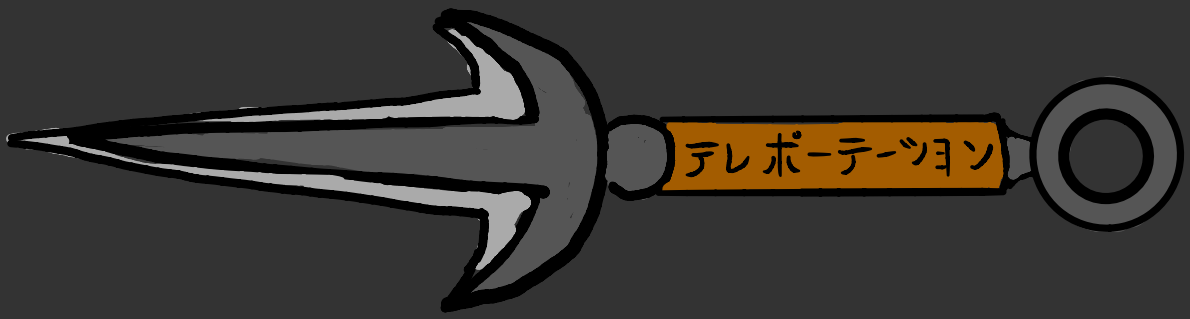
$Z \otimes I \, |\beta_{00}\rangle = |\beta_{10}\rangle$ $\qquad Z \cdot X \otimes I \, |\beta_{00}\rangle = |\beta_{11}\rangle$

$$X = \begin{vmatrix} 0 & 1 \\ 1 & 0 \end{vmatrix} \qquad Z = \begin{vmatrix} 1 & 0 \\ 0 & -1 \end{vmatrix}$$

La cosa importante da notare qua è che questi operatori agiscono solo sul primo qbit della base computazionale.

Quindi se si organizza un circuito come quello in figura è possibile inviare due bit con un singolo qbit

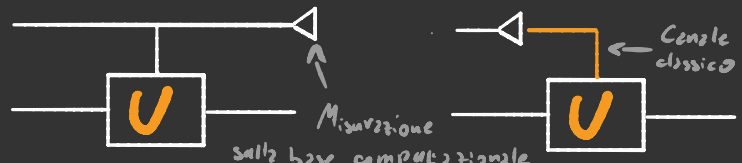




Supponiamo di voler inviare un qbit attraverso linee di trasmissione classiche.

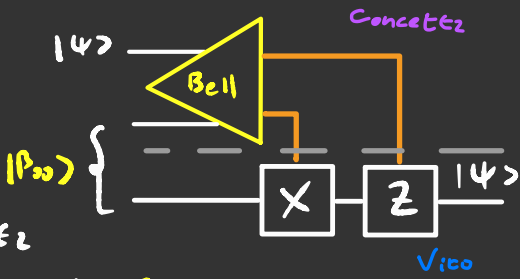
Per capire questo algoritmo bisogna prima sapere 2 cose:

Questi 2 circuiti sono equivalenti.



$$|\psi\rangle|\beta_{00}\rangle$$
$$=$$
$$\frac{1}{2}\left[|\beta_{00}\rangle|\psi\rangle + |\beta_{01}\rangle(X|\psi\rangle) + |\beta_{10}\rangle(Z|\psi\rangle) + |\beta_{11}\rangle(XZ|\psi\rangle)\right]$$

Se si costruisce un circuito come quello a destra è possibile inviare un qbit generico $|\psi\rangle$ con due canali classici ammesso che Concetta e Vito si siano smezzati precedentemente $|\beta_{00}\rangle$.



Per capire bene come funziona bisogna guardare la prima componente della funzione d'onda nella parte bassa dell'equazione gialla. L'operatore di Bell si occupa di prendere $|\beta_{ij}\rangle \to |ij\rangle$ e poi misurarlo facendo collassare la funzione d'onda in $|ij\rangle(X^i Z^j)|\psi\rangle$.

Trasformata di Fourier

Supponiamo di avere uno stato di n qbit così

$$|\psi_n(w)\rangle = \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} e^{2\pi i w y} |y\rangle \quad \text{con } w \in [0,1)$$

e vogliamo scrivere un algoritmo che ci dica quanto vale w.

Intanto scriviamo w come un numero decimale binario

$$w = 0, x_1 x_2 x_3 \ldots = x_1 \cdot 2^{-1} + x_2 \cdot 2^{-2} + x_3 \cdot 2^{-3} + \ldots \qquad x_i \in \{0,1\}$$

Vorremmo vedere se $|\psi(w)\rangle$ è separabile, per fare ciò la proviamo a moltiplicare per una funzione d'onda e vediamo che succede

$$|\theta\rangle|\psi_n(w)\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i\theta}|1\rangle)\frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} e^{2\pi i w y} |y\rangle =$$

$$= \frac{1}{\sqrt{2^{n+1}}}\left[\sum_{y=0}^{2^n-1} e^{2\pi i w y}|0\rangle|y\rangle + \sum_{y=0}^{2^n-1} e^{2\pi i w y + i\theta}|1\rangle|y\rangle\right] =$$

Qui y posso da essere un numero a n bit o anche a $n+1$ bit

$$= \frac{1}{\sqrt{2^{n+1}}}\left[\sum_{y=0}^{2^n-1} e^{2\pi i w y}|y\rangle + \sum_{y=0}^{2^n-1} e^{2\pi i w y + i\theta}|2^n+y\rangle\right] =$$

$$= \frac{1}{\sqrt{2^{n+1}}}\left[\sum_{y=0}^{2^n-1} e^{2\pi i w y}|y\rangle + \sum_{y=0}^{2^n-1} e^{2\pi i w y + i\theta}|2^n+y\rangle\right] =$$

$$= \frac{1}{\sqrt{2^{n+1}}}\left[\sum_{y=0}^{2^n-1} e^{2\pi i w y}|y\rangle + \sum_{y=2^n}^{2^{n+1}-1} e^{2\pi i w (y-2^n) + i\theta}|y\rangle\right] =$$

Per $\theta = 2^{n+1}\pi w$ si ottiene qualcosa di interessante

$$|2^{n+1}\pi w\rangle|\psi_n(w)\rangle = \frac{1}{\sqrt{2^{n+1}}}\left[\sum_{y=0}^{2^n-1} e^{2\pi i w y}|y\rangle + \sum_{y=2^n}^{2^{n+1}-1} e^{2\pi i w y}|y\rangle\right] =$$

$$= \frac{1}{\sqrt{2^{n+1}}} \sum_{y=0}^{2^{n+1}-1} e^{2\pi i w y}|y\rangle = |\psi_{n+1}(w)\rangle$$ Quindi

La produttoria finisce con $n=1$ perché significa che resta solo 1 qbit

$$|\psi_n(w)\rangle = \frac{|0\rangle + e^{i2^n\pi w}|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + e^{i2^{n-1}\pi w}|1\rangle}{\sqrt{2}} \otimes \cdots \otimes \frac{|0\rangle + e^{i2\pi w}|1\rangle}{\sqrt{2}}$$

Adesso che sappiamo qual'é lo stato di ogni qbit di $|\Psi_n(w)\rangle$ cerchiamo di capire come ricavarci w.
Supponiamo che sia w che $|\Psi\rangle$ siano funzioni d'onda a 1 qbit, quindi $w = 0,x$ con $x \in \{0,1\}$ e

$$|\Psi_1(w)\rangle = \frac{|0\rangle + e^{i2\pi w}|1\rangle}{\sqrt{2}} = \begin{cases} |+\rangle \text{ se } w=0,0 \\ |-\rangle \text{ se } w=0,1 \end{cases}$$

Quindi per capire quanto fa w in questo caso ristretto basta fare $|2w\rangle = H|\Psi_1(w)\rangle$. H é la porta di Hadamard

Che succede se w non é esattamente $0,1$ o $0,0$? In quel caso lo stato $|2w\rangle$ diventa una combinazione lineare degli stati $|0\rangle$ e $|1\rangle$.

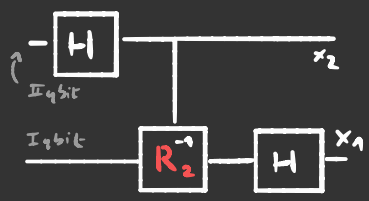
Adesso prendiamo $w = 0, x_1 x_2$ e

$$|\Psi_2(w)\rangle = \frac{|0\rangle + e^{i\pi w}|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + e^{i2\pi w}|1\rangle}{\sqrt{2}} =$$

$$= \frac{|0\rangle + e^{i2\pi x_1,x_2}|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + e^{i2\pi \cdot 0,x_1x_2}|1\rangle}{\sqrt{2}} = \frac{|0\rangle + e^{i2\pi\, 0,x_2}|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + e^{i2\pi \cdot 0,x_1x_2}|1\rangle}{\sqrt{2}} =$$

$$R_n \equiv \begin{vmatrix} 1 & 0 \\ 0 & e^{i\pi 2^{1-n}} \end{vmatrix}$$

Dal secondo qbit si può ricavare x_2 con la porta di Hadamard. Una volta fatto ciò si moltiplica il primo qbit per R_2^{-1} se $x_2 = 1$, quindi il circuito rappresentativo dell'operazione é questo qua a sinistra.

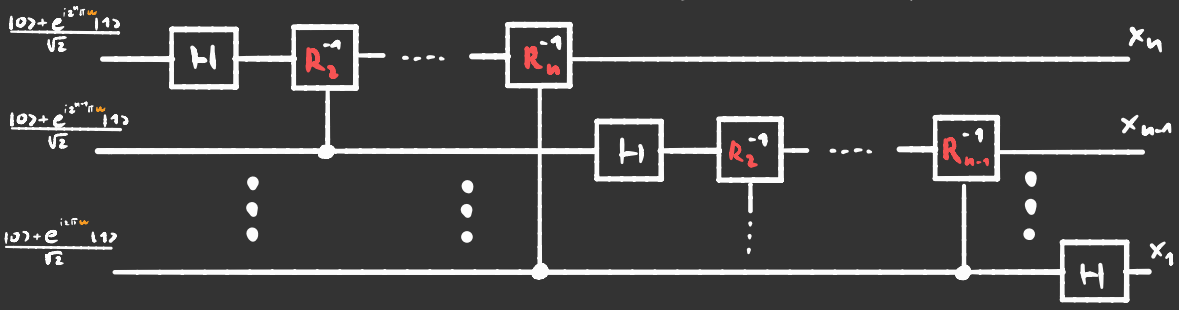


Visto che R_n é una matrice diagonale si può scambiare il bit di controllo con l'altro

Nel caso con n qbit l'algoritmo diventa così per

$w = 0, x_1 x_2 \cdots x_n$

Per avere l'antitrasformata basta leggere il circuito al contrario



Adesso vediamo come usarla per calcolarci la periodicità di uno stato quantistico fatto così

$$|r,b\rangle = \frac{1}{\sqrt{m}} \sum_{z=0}^{m-1} |zr+b\rangle \qquad z,r,b \in \mathbb{N}$$

Noi: ancora non sappiamo bene cosa faccia la trasformata applicata ai vettori della base computazionale, ma l'antitrasformata sì. Qui sotto in grigio ci sono i conti noiosi per calcolarla.

$$QFT^{-1}|r,b\rangle = \frac{1}{\sqrt{m}} \sum_{z=0}^{m-1} QFT^{-1}|zr+b\rangle = \frac{1}{\sqrt{m}} \sum_{z=0}^{m-1} \sum_{y=0}^{2^n-1} \exp\left[i\pi \frac{(zr+b)y}{2^{n-1}}\right]|y\rangle = \frac{1}{\sqrt{m}} \sum_{y=0}^{2^n-1} \sum_{z=0}^{m-1} \exp\left[i\pi \frac{(zr+b)y}{2^{n-1}}\right]|y\rangle$$

$$= \frac{1}{\sqrt{m}} \sum_{y=0}^{2^n-1} \exp\left(i\pi \frac{by}{2^{n-1}}\right)|y\rangle \sum_{z=0}^{m-1} \exp\frac{i\pi zry}{2^{n-1}}$$

La serie geometrica ha la proprietà che $\sum_{z=0}^{m-1} a^z = \frac{1-a^{m-1}}{1-a}$

$$\frac{1-\exp\left[\frac{i\pi ry(m-1)}{2^{n-1}}\right]}{1-\exp\left(\frac{i\pi ry}{2^{n-1}}\right)} = \frac{e^{\frac{i\pi ry(m-1)}{2^{n-1}}}}{e^{\frac{i\pi ry}{2^{n-1}}}} \frac{\operatorname{sen}\left[\frac{\pi ry(m-1)}{2^n}\right]}{\operatorname{sen}\left(\frac{\pi ry}{2^n}\right)} = e^{\frac{i\pi ry m}{2^n}} \frac{\operatorname{sen}\left[\frac{\pi ry(m-1)}{2^n}\right]}{\operatorname{sen}\left(\frac{\pi ry}{2^n}\right)}$$

I valori che dominano sono quelli per cui il denominatore fa 0. Questo avviene se $K = 2^n/r \in \mathbb{N}$ e $y = jK$ con $j \in \mathbb{N}$

$$\frac{\operatorname{sen}\left[\frac{\pi y(m-1)}{K}\right]}{\operatorname{sen}\left(\frac{\pi y}{K}\right)} \simeq (m-1)\delta_{r,jm} \quad \Rightarrow \quad \frac{m-1}{\sqrt{m}} \sum_{y=0}^{2^n-1} \exp\left(i\frac{\pi b}{2^{n-1}} y\right) e^{\frac{2i\pi rjm}{K}} \delta_{r,jm}|y\rangle =$$

$$\frac{m-1}{\sqrt{m}} \sum_{j=0}^{r-1} \exp\left(-\frac{2\pi b}{rK} jK\right) e^{\frac{2i\pi jm}{K}}|jK\rangle = \frac{m-1}{\sqrt{m}} \sum_{j=0}^{r-1} \exp\left[i\pi j \frac{2b}{r}\right]|jK\rangle = \frac{m-1}{\sqrt{m}} \sum_{j=0}^{r-1} \exp\left(i\pi j \frac{rm}{r}\right)|jK\rangle =$$

Il risultato viene un po' diverso da quello che esce dal libro, in teoria dovrebbe venire

$$QFT^{-1}|r,b\rangle = \frac{1}{\sqrt{r}} \sum_{K=0}^{r-1} \exp\left(-2\pi i \frac{b}{r} K\right)|mK\rangle$$

A prima vista sembrerebbe che non si è fatto nulla di utile, dopotutto alla fine è uscita fuori una sovrapposizione di tante funzioni d'onda.

Se misuriamo $QFT^{-1}|r,b\rangle$ ci salterà fuori un multiplo della funzione d'onda, ma se ripetiamo l'operazione più volte possiamo trovare il massimo comune divisore, e quello è la frequenza di $|r,b\rangle$. L'algoritmo per trovare il massimo comune divisore è molto efficiente e si chiama algoritmo di Euclide

L'applicazione più famosa della Trasformata di Fourier quantistica è

L'Algoritmo di Shor

Prima di leggere qua la spiegazione ti consiglio di andare a vedere questo video youtu.be/IvTqbM5Dq4Q

Sia N il numero che vogliamo scomporre $N = a \cdot b$, dove a e b sono numeri primi.

Se riuscissimo a trovare un numero $M = a \cdot c$ che ha un divisore in comune con N il problema sarebbe risolto trovando il massimo comune divisore.

Un teorema della matematica ci viene a salvare, esso dice che:

Siano g e N due numeri senza fattori comuni allora esistono due numeri interi p ed m tali che

$$g^p = m \cdot N - 1 \rightarrow \underbrace{(g^{p/2}+1)}_{\text{multiplo di } a}\underbrace{(g^{p/2}-1)}_{\text{multiplo di } b} = m \cdot N$$

A dire il vero uno dei due coefficienti potrebbe essere un multiplo di N, o potrebbe capitare che p sia dispari. Tuttavia 3/8 delle volte che si sceglie g questi problemi non sussistono.

Adesso però dobbiamo trovare il modo di stimare p.
Sia $|p\rangle$ la funzione d'onda che rappresenta p

$$|x,0\rangle \to |x,g^x\rangle \to |x, \text{resto}(g^x/r)\rangle$$

Devo finire di scriverlo, in ogni caso il video dovrebbe essere più che sufficiente

Mettere i piedi a terra

Finora abbiamo trattato il funzionamento di calcolatori quantistici ideali, quindi adesso vediamo quali limitazioni ci impone il mondo reale.

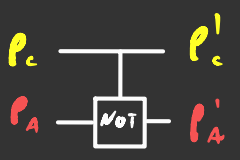
I 7 criterii necessari per costruire un calcolatore quantistico sono detti **Criterii di Di Vincenzo** e dicono che un calcolatore quantistico deve avere

- Un sistema fisico di qbit scalabile
- Lunghi tempi di decoerenza

  Parte difficile
- L'abilità di inizializzare i qbit
- Un insieme universale di porte logiche
- L'abilità di misurare i qbit
- L'abilità di convertire qbit stazionarii (elettroni) in qbit volanti e viceversa (Fotoni)
- L'abilità di trasmettere qbit volanti

  Necessario per comunicare tra più PC

Il principale fattore limitante è l'interazione con l'ambiente esterno, proviamo a modellarlo partendo dal caso più semplice: Sia il calcolatore che l'ambiente sono singolo qbit e modellizziamo l'interazione con una porta c-NOT (Si sarebbe potuto scegliere una porta Entangling qualunque)



Per semplificare ulteriormente supponiamo che l'ambiente si trovi nello stato $|0\rangle$. Avremmo potuto scegliere un qualunque altro stato ma il ragionamento sarebbe stato identico

Visto che all'inizio ρ_c rappresenta uno stato puro abbiamo che $\rho_c = |\psi\rangle\langle\psi| = \begin{vmatrix} |\alpha|^2 & \alpha\beta^* \\ \alpha^*\beta & |\beta|^2 \end{vmatrix}$

La matrice di densità totale $\rho_T = \rho_c \otimes \rho_A =$

$= |\alpha|^2 |00\rangle\langle 00| + \alpha\beta^* |00\rangle\langle 10| + \alpha^*\beta |10\rangle\langle 00| + |\beta|^2 |10\rangle\langle 10|$

Quando si fa passare attraverso la porta c-NOT si ha che $|00\rangle \to |00\rangle$, $|10\rangle \to |11\rangle$ $\langle 10| \to \langle 11|$ e $\langle 00| \to \langle 00|$, quindi

$\rho_T \to$ c-NOT $\cdot \rho_T \cdot$ c-NOT $=$

$= |\alpha|^2 |00\rangle\langle 00| + \alpha\beta^* |00\rangle\langle 11| + \alpha^*\beta |11\rangle\langle 00| + |\beta|^2 |11\rangle\langle 11|$

Noi però non possiamo misurare niente dell'ambiente, quindi effettivamente possiamo lavorare solo con ρ_c, però dopo essere passati dalla porta logica ρ_T non è più separabile quindi ci tocca fare la traccia sugli indici di ρ_A.

Dopo aver fatto l'operazione ci risulta che

$$\rho_c' = Tr_{\rho_A}(\rho_T) = |\alpha|^2 |0\rangle\langle 0| + |\beta|^2 |1\rangle\langle 1|$$

In generale questo non è più uno stato puro, quindi si crea una indeterminazione sullo stato.

Che è diversa dall'indeterminazione tipo quella di Heisemberg che è sulle variabili

Questo tipo di fenomeno è detto **Decoerenza**

Correzione errori

Nei calcolatori classici talvolta un bit può cambiare valore, per evitare questo problema si triplica il numero di bit

output senza errori = 100101 → 111 000 000 111 000 111

output con errori = 000 111 → 101 000 000 011 000 111

Sbagliato → Giusto → 111 000 000 111 000 111

Se non si fosse capito dallo schemino dopo che l'operazione viene conclusa si fa un voto di maggioranza.

C'è comunque la possibilità che 2 numeri saltino, ma calcoliamoci le probabilità.

Sia p la probabilità che un bit generico cambi, allora la probabilità che una sequenza a 3 bit sballi è $p^3 + 3p^2(1-p) = 3p^2 - 2p^3$

p nei calcolatori classici è molto piccolo, quindi p^2 è molto piccolissimo

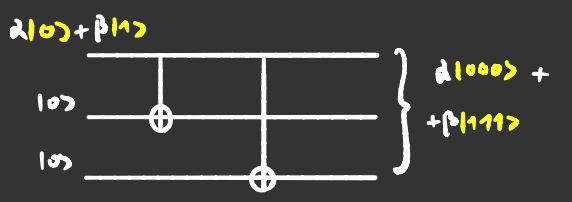
Adesso vediamo il caso **Quantistico**

L'idea è di usare al posto dei qbit $|0\rangle$ e $|1\rangle$ i qbit $|000\rangle$ e $|111\rangle$.

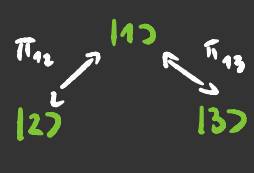
Quello che ci serve per fare la stessa cosa con i qbit è:

- Un modo per mandare $\alpha|0\rangle + \beta|1\rangle$ in $\alpha|000\rangle + \beta|111\rangle$
- Un modo per fare il voto di maggioranza

Il primo punto è facile da fare, basta fare il circuito come quello a destra

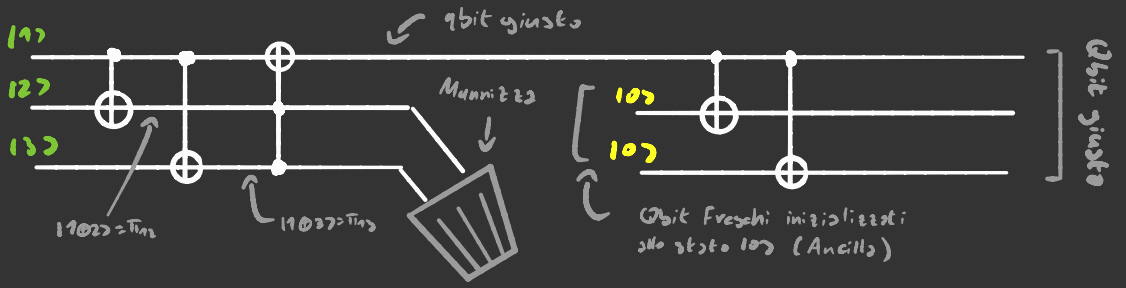


Fare il voto di maggioranza invece è un po' più complicato. Prima di tutto bisogna individuare il qbit sbagliato, sia π_{ij} la parità tra lo stato i e lo stato j che vale 0 se i e j hanno la stessa parità, altrimenti: 1, quindi $\pi_{ij} = i \oplus j$. Possiamo determinare il bit sbagliato così

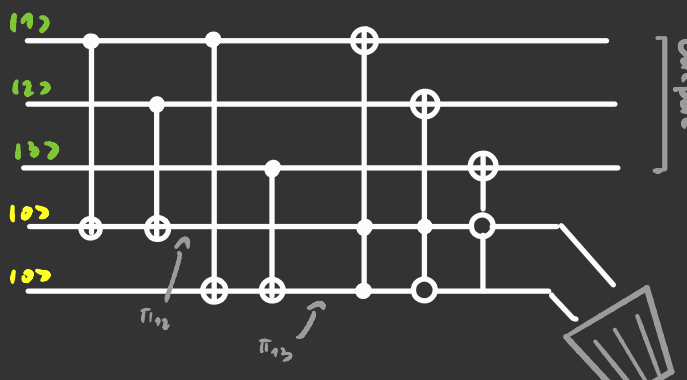


- Il bit |1⟩ è sbagliato se $\pi_{12} = \pi_{13} = 1$
- Il bit |2⟩ è sbagliato se $\pi_{12} = 1$, $\pi_{13} = 0$
- Il bit |3⟩ è sbagliato se $\pi_{12} = 0$, $\pi_{13} = 1$
- Tutti i bit sono giusti se $\pi_{12} = \pi_{13} = 0$

Quindi possiamo dire che il bit corretto è |1⟩ se $\pi_{12} \cdot \pi_{13} = 0$, altrimenti è $X|1\rangle$. Una volta ottenuto il qbit giusto si ri-triplica



Questo procedimento funziona bene solo se si suppone che esso stesso non è soggetto ad errori, per ovviare a ciò basta usare questo circuito



Non mi metto a spiegare sto circuito che ci vuole troppo tempo, però se hai capito il circuito di sopra non dovrebbe essere difficile capirlo

Informazione

Intuitivamente l'informazione é qualcosa di semplice da definire, ad esempio il numero di bit salvati in un calcolatore o il numero di parole in un libro. Poi in fisica uno si puó chiedere quant'é l'informazione in un sistema quantistico.
Per trovare una definizione sensata dell'informazione bisogna partire dall'opposto: l'**Entropia**.

In un sistema termodinamico l'entropia é definita

$$S = k_B \ln \Gamma$$

k_B: Costante di Boltzmann che impongo = 1; Γ: Numero di stati quantistici possibili

Solo che in termodinamica tutti gli stati sono equiprobabili.
É possibile ridefinire l'entropia cosí

$$S \equiv \sum_{\text{stati}} p_i \ln \frac{1}{p_i}$$

p_i: probabilità di stare nello stato i-esimo

Se supponiamo che gli stati sono equiprobabili ci ritroviamo la definizione termodinamica, e se abbiamo uno stato j "certo" $p_i = \delta_{ij}$, allora $S = 0$.

Notiamo che questa definizione di entropia si puó usare per una generica distribuzione di probabilitá

$$S(X) = \sum_x p_x \ln \frac{1}{p_x} \qquad \text{dove} \qquad p_x = \text{Prob}(X = x)$$

Ad esempio se X é la moneta $x \in \{\text{testa}, \text{croce}\}$, quindi $S(\text{Moneta}) = -p_t \ln p_t - p_c \ln p_c$

L'entropia congiunta di 2 variabili casuali X e Y è

$$S(X,Y) = -\sum_{x,y} p_{x,y} \ln p_{x,y}$$

Se le due distribuzioni sono indipendenti abbiamo che

$$S(X,Y) = -\sum_{x,y} p_x p_y \ln(p_x p_y) = -\cancel{\sum_x p_x}^{=1} \sum_y p_y \ln p_y - \cancel{\sum_y p_y}^{=1} \sum_x p_x \ln p_x =$$

$$= S(X) + S(Y)$$

Se invece X e Y non sono indipendenti: uso Bayes

$$S(X,Y) = -\sum_{x,y} p_{x|y}\, p_y (\ln p_{x|y} + \ln p_y) = \qquad p_y = \sum_x p_{x,y}$$

$$= \underbrace{\sum_y p_y \sum_x p_{x|y} \ln p_{x|y}}_{\downarrow} + \cancel{\sum_x p_{x|y}}^{=1} \sum_y p_y \ln p_y$$

$$S(X|Y) + S(Y)$$

Bene, ma che senso ha in pratica $S(X|Y)$?

Prendiamo la seguente distribuzione di probabilità di X e Y, se conosciamo y allora possiamo dire con esattezza il valore di x, quindi intuitivamente $S(X|Y) = 0$.

	$x=0$	$x=1$
$y=0$	0	$\frac{1}{2}$
$y=1$	$\frac{1}{2}$	0

Inoltre sia $S(X,Y)$ che $S(Y)$ hanno 2 esiti equiprobabili, quindi sono entrambi uguali a $-\ln 2$. Se fai i conti è esattamente quello che esce.

Sapere il valore di Y ci da più informazione sul valore che X può ottenere, quindi definisco L'**Informazione**

$$I(X,Y) = S(X) - S(X|Y)$$

Che equivale a dire quanta entropia ho in meno se conosco Y. Da notare che l'informazione è qualcosa di Relativo

Inoltre l'informazione è simmetrica

$$I(X,Y) = S(x) + S(y) - S(x,y) = I(Y,X)$$

Un'altra quantità utile da usare è la **Divergenza di Kullback-Leibler**, siano P_i e Q_i due distribuzioni di

$$D_{KL}(P||Q) = \sum_i P_i \ln\left(\frac{P_i}{Q_i}\right)$$

Essa è un modo per stimare in termini entropici quanto sono diverse due distribuzioni di probabilità

Studiare e aggiungere proprietà fisiche

Matrice di densità

Se vogliamo cambiare base l'entropia va espressa in termini della matrice di densità

$$S = -\mathrm{tr}(\hat{\rho} \ln \hat{\rho}) \qquad \hat{\rho} = \sum_{\text{stati}} p_i |i\rangle\langle i|$$

Se si ci mette nella base diagonale si riottiene la definizione di prima, e visto che la traccia è un invariante sotto cambiamento di base l'entropia così è ben definita.

In meccanica quantistica però c'è una sottigliezza da tenere in conto.

Supponiamo di avere un qbit così $|+\rangle = \frac{|\uparrow\rangle + |\downarrow\rangle}{\sqrt{2}}$

Se lo misuro rispetto alla base $\{|\uparrow\rangle, |\downarrow\rangle\}$ metà delle volte fa $\uparrow$ e metà $\downarrow$. Volendo possiamo dire che

$p_\uparrow = p_\downarrow = \frac{1}{2}$

Questo significa che per l'osservatore che sta nella base $\{|\uparrow\rangle, |\downarrow\rangle\}$ il sistema si comporta come un sistema a entropia $\ln 2$

$$S = -p_\uparrow \ln p_\uparrow - p_\downarrow \ln p_\downarrow = \ln 2$$

Però in teoria lo stato è $|+\rangle$, quindi $S = 0$. Dove sta l'errore?

Questo paradosso si risolve dicendo che l'entropia dipende dalla base, quindi sotto un certo punto di vista, si può dire che l'entropia è soggettiva.

Si può ri-aggiornare la definizione di entropia così:
Sia $\mathcal{B}$ una base dello spazio di Hilbert con cui lavoriamo, allora

$$S(\mathcal{B}) = -\sum_{\psi \in \mathcal{B}} \langle \psi | \hat{\rho} | \psi \rangle \ln \langle \psi | \hat{\rho} | \psi \rangle$$

Questa entropia si chiama **Entropia di Shannon**

Non sono sicuro che sia questo il nome

Prima avevamo visto come calcolare l'entropia di delle distribuzioni di probabilità, adesso sarebbe interessante vedere come fare per degli operatori quantistici.

Sia $\hat{X}$ l'operatore di cui vogliamo calcolarci l'entropia, allora

$$P(X = x) = p_x = |\langle x | \psi \rangle|^2 \quad \text{dove} \quad \hat{X}|x\rangle = x|x\rangle$$

Se invece abbiamo una matrice di densità

Ho supposto che $\hat{X}$ sia non degenere, altrimenti bisogna sommare su tutti gli autostati con lo stesso autovalore

$$p_x = \sum_{\text{somma sugli blah blah}} \langle x | \hat{\rho} | x \rangle$$

E l'entropia di $\hat{X}$ diventa

$$S(\hat{X}) = -\sum_{x \in Sp(\hat{X})} p_x \ln p_x$$

$Sp(\hat{X})$ è lo spettro, quindi gli autovalori

Una cosa interessante da notare è che l'entropia di shannon è uguale all'entropia dell'operatore che effettua la misurazione. Quindi ci sono questi due modi di interpretare l'entropia quantistica

Come costruire un Calcolatore Quantistico

Attenzione! Le tecnologie discusse in questa parte sono ancora agli albori, quindi è più che probabile che tra qualche anno saranno obsolete.

Per iniziare bisogna scegliere un un sistema con livelli energetici ben definiti:

- **Un Atomo** — L'atomo ha tanti livelli energetici, la cosa migiore è sceglierne 2 ben distanziati dagli altri livelli
- **Uno Ione** — Ha le stesse proprietà dell'atomo, ma è anche carico elettricamente, e questo può cornare utile
- **Una Molecola** — Ci sono tanti modi per usare delle molecole come qbit
- **Un Elettrone** — Lo spin dell'elettrone Fornisce un sistema a 2 livelli
- **Un Fotone** — Si può sfruttare la polarizzazione del fotone, è ottimo per trasmettere qbit nella fibra ottica, ma non interagisce con altri fotoni, quindi è difficile fargli fare entanglment
- **Un Superconduttore** — Si usano gli stati di corrente come qbit
- **Quantum dot** — Sono buche di potenziale create artificialmente
- **Eccetera** — Ci sono un sacco di altre idee strambe in sviluppo

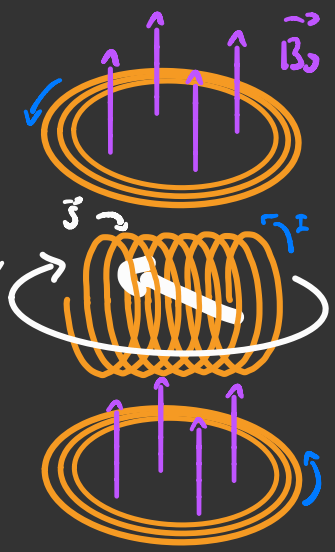
Al momento della stesura di questa pagina il calcolatore quantistico con più qbit ne ha circa 50 ed è basato su una tecnologia a superconduttore

NMR

Nuclear Magnetic Resonance

Cominciamo a studiare un sistema con un qbit caratterizzato da un determinato spin e momento magnetico.

Per manipolare il qbit si usa un apparato fatto come nell'immagine qui a destra



I **solenoidi** di sopra e di sotto servono a creare un campo magnetico $B_0 \hat{z}$.

Il solenoide centrale ruota a una velocità angolare $w\hat{z}$ e crea un campo magnetico $B_1(\hat{x}\cos wt + \hat{y}\sin wt)$. Il dipolo magnetico ha spin $\vec{S}$ e se ne sta fermo al centro dell'apparato. Siano w_0 e w_1 le frequenze di precessione del dipolo nei campi $\vec{B_0}$ e $\vec{B_1}$, allora l'Hamiltoniana del sistema è

$$H = -\frac{\hbar}{2}\left[w_0 \sigma_z + w_1(\sigma_x \cos wt + \sigma_y \sin wt)\right] =$$

$$= -\frac{\hbar}{2}\left[w_0 \sigma_z + w_1\left(\sigma_+ e^{iwt} + \sigma_- e^{-iwt}\right)\right] = -\frac{\hbar}{2}\begin{vmatrix} w_0 & w_1 e^{iwt} \\ w_1 e^{iwt} & -w_0 \end{vmatrix}$$

Per studiare il sistema quantistico ci mettiamo in un "sistema di riferimento rotante" solidale col solenoide centrale $|\Psi\rangle = \exp\left(-\frac{iw\sigma_z t}{2}\right)|\varphi(t)\rangle$

Alternativamente si può usare questa Hamiltoniana

$$\tilde{H} = -\frac{\hbar}{2}\left[(w_0 - w)\sigma_z + w_1 \sigma_x\right]$$

Attenzione, questa Ham. non determina i livelli energetici perché ci troviamo nel sistema di riferimento rotante. I livelli energetici sono gli autovalori di H

Grazie a $\tilde{H}$ se $\omega = \omega_0$ possiamo ruotare la componente dello spin lungo la $\hat{z}$ con l'operatore $-\frac{\hbar}{2}\omega_1 \sigma_x$ così posso fare tutte le operazioni che voglio a singolo qbit.

Adesso riveliamo di cosa è fatto il nostro qbit.

Come qbit usiamo la molecola di Cloroformio (come esempio)

Più precisamente si tengono in considerazione gli spin degli atomi di Carbonio e di Idrogeno. Avendo momenti magnetici diversi essi hanno frequenze di risonanza diverse ω_0^C e ω_0^H.

Visto che abbiamo due atomi ci mettiamo due campi magnetici ruotanti assieme quindi il campo magnetico ruotante esce

$$B_1 = B_1^C(\hat{x}\cos\omega^C t + \hat{y}\,\mathrm{sen}\,\omega^C t) + B_1^H(\hat{x}\cos\omega^H t + \hat{y}\,\mathrm{sen}\,\omega^H t)$$

Le due frequenze sono scelte in modo tale che siano vicine alle frequenze di risonanza del carbonio e dell'idrogeno, quindi possiamo far finta che ogni atomo sia soggetto ad un solo campo magnetico.

L'Hamiltoniana del sistema è

$$H^{CH} = -\frac{\hbar}{2}\left[\omega_0^C \sigma_z^C + \omega_1^C\left(\sigma_+^C e^{i\omega t} + \sigma_-^C e^{-i\omega t}\right)\right] - \quad \leftarrow \text{Hamiltoniana agente sul carbonio}$$

$$-\frac{\hbar}{2}\left[\omega_0^H \sigma_z^H + \omega_1^H\left(\sigma_+^H e^{i\omega t} + \sigma_-^H e^{-i\omega t}\right)\right] + \quad \leftarrow \text{Hamiltoniana agente sull'Idrogeno}$$

$$+ \hbar J \sigma_z^C \sigma_z^H \quad \leftarrow \text{Hamiltoniana d'interazione mediata dagli elettroni di legame, } J \text{ è una costante}$$

Nel sistema di riferimento ruotante l'Hamiltoniana diventa

$$\tilde{H} = \frac{\hbar}{2}\left[(\omega^C - \omega_0^C)\sigma_z^C - \omega_1^C \sigma_x^C + (\omega^H - \omega_0^H)\sigma_z^H - \omega_1^H \sigma_x^H\right] + \hbar J \sigma_z^C \sigma_z^H$$

Ci siamo messi in due sistemi di riferimento ruotanti diversi

Da queste Hamiltoniane si vede che è praticamente impossibile controllare indipendentemente i 2 qbit.

Bisogna considerare che:

- $J \ll \omega_1^H, \omega_1^C$ Il che significa che gli effetti dovuti all'interazione sono lenti
- $|\delta^C| \equiv |\omega^C - \omega_0^C| \ll \omega_1^C$
- $|\delta^H| \equiv |\omega^H - \omega_0^H| \ll \omega_1^H$

$$\tilde{H_I} = \frac{\hbar}{2}\left[\delta^C \sigma_z^C - \omega_1^C \sigma_x^C + \delta^H \sigma_z^H - \omega_1^H \sigma_x^H\right] + \hbar J \sigma_z^C \sigma_z^H$$

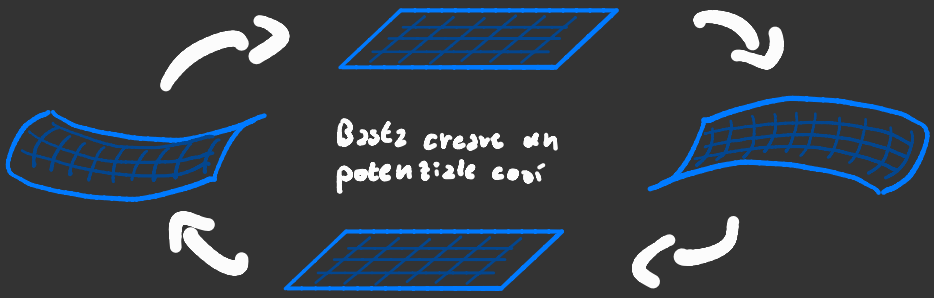
Con questa Hamiltoniana si possono manipolare i singoli qbit agendo sull'intensità e la frequenza dei campi magnetici rotanti.

La parte di interazione dell'Hamiltoniana è un generatore infinitesimo della porta c-NOT.

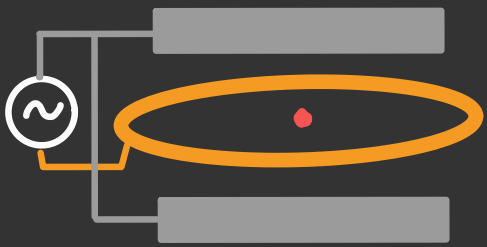
Visto che grazie alle operazioni a singolo qbit e alla porta cNOT è possibile fare qualunque tipo di operazione a 2 qbit.

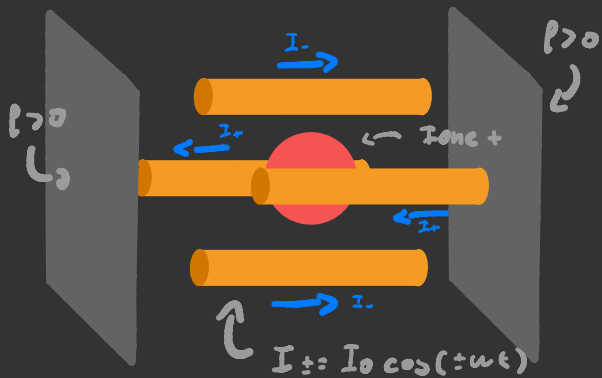
Ioni intrappolati:

Come abbiamo visto l'NMR fa abbastanza schifo, quindi cerchiamo delle alternative, un'idea sarebbe quella di usare diversi ioni sospesi nel vuoto.
Visto che $\nabla \cdot \vec{E} = 0$ non è possibile intrappolare particelle cariche con un campo elettrostatico, ma con un campo elettrico alternato qualcosina si può fare...



Una particella in un potenziale oscillante in questo modo tende ad oscillare attorno a un punto.
Gli oggetti che fanno dei campi così si chiamano trappole di Paul. Ti consiglio di cercarle su youtube che si trovano delle animazioni
Ecco alcuni esempi di trappole di Paul:





Una volta che gli Ioni sono intrappolati possiamo supporre che si trovino in un potenziale equivalente

$$V(x,y,z) = \frac{M}{2}(\omega_x^2 x^2 + \omega_y^2 y^2 + \omega_z^2 z^2)$$

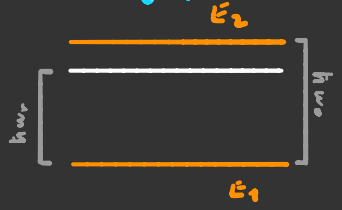
In pratica però c'è spesso una delle omega che è più piccola $\omega_x \ll \omega_y, \omega_z$ quindi possiamo dire che la particella lungo l'asse y e z è bloccata allo stato fondamentale, mentre lungo l'asse x si può muovere un pochino, quindi $V(x) = M\omega_x^2 x^2/2$. Noi però vogliamo usare lo spin come qbit, quindi se aggiungiamo un campo magnetico $\vec{B}_0 = B_0 \hat{z}$ a cui corrisponde una frequenza di risonanza dello spin ω_0

$$H_0 = \frac{p^2}{2m} + \frac{M}{2}\omega_x^2 x^2 - \frac{\hbar\omega_0}{2}\sigma_z = \hbar\omega_x a^\dagger a - \frac{\hbar\omega_0}{2}\sigma_z$$

Noi per poter usare un sistema quantistico regolato da questa Hamiltoniana dobbiamo assicurarci che $K_b T \ll \hbar\omega_x, \hbar\omega_0$. Per raggiungere queste temperature il metodo migliore è il

Raffreddamento Doppler

Supponiamo di avere un sistema a 2 livelli con un gap di energia uguale a $\hbar\omega_0$ immerso in una radiazione isotropa con frequenza ω_r. Se l'atomo si muove contro la radiazione, per effetto doppler la vedrà con una frequenza aumentata, e se la velocità è sufficiente assorbe il fotone, e poi lo emette in una direzione a caso, questo diminuisce la velocità delle particelle e quindi abbassa la temperatura



Manipolazione dei qbit con : LASER

Ora che abbiamo il nostro bel qbit pronto, vediamo come manipolarlo.

Per farlo si usa un campo elettromagnetico oscillante

$$\vec{B}_1(\vec{x},t) = B_1 \cos(K\cdot x - \omega t)\,\hat{z} \qquad \text{con } \vec{K} = K\hat{x}$$

E l'Hamiltoniana d'interazione $H_I = -q\cdot B_I$

$$H_I = -\hbar\omega_1 \sigma_z \cos(Kx-\omega t) = -\frac{\hbar\omega_1}{2}(\sigma_+ + \sigma_-)\left[e^{iKx - i\omega t} + e^{-iKx + i\omega t}\right]$$

Se consideriamo il nostro atomo in $x \simeq 0$ possiamo dire che

$$H_I \simeq -\frac{\hbar\omega_1}{2}(\sigma_+ + \sigma_-)\left[(1-iKx)\,e^{i\omega t} + (1+iKx)\,e^{-i\omega t}\right]$$

che possiamo dividere in

$$H_1 = -\frac{\hbar\omega_1}{2}(\sigma_+ + \sigma_-)\left[e^{i\omega t} + e^{-i\omega t}\right] \qquad H_2 = \frac{i\hbar\omega_1}{2}(\sigma_+ + \sigma_-)Kx\left[e^{i\omega t} - e^{-i\omega t}\right]$$

Possiamo scrivere la seconda Ham. in termini di a e $a^\dagger$ sostituendo $x = (a + a^\dagger)\sqrt{\frac{\hbar}{M\omega_x}}$ e se definisco $\eta = K\sqrt{\frac{\hbar}{M\omega_x}}$ abbiamo che

$$H_2 = \frac{i\hbar\omega_1}{2}\eta\,(\sigma_+ + \sigma_-)(a + a^\dagger)\left[e^{i\omega t} - e^{-i\omega t}\right]$$

Se ci mettiamo nel sistema di riferimento ruotante attorno a z con una frequenza ω_0

$$\sigma_x \to \sigma_x \cos(\omega_0 t) + \sigma_y \operatorname{sen}(\omega_0 t) = \sigma_+ e^{i\omega_0 t} + \sigma_- e^{-i\omega_0 t}$$

Per vedere come trasformano gli operatori di creazione e distruzione sotto rotazioni di un angolo θ bisogna calcolare:

$$R(\theta)\, a\, R^\dagger(\theta) \quad e \quad R(\theta)\, a^\dagger R^\dagger(\theta) = [R(\theta)\, a\, R^\dagger(\theta)]^\dagger$$

dove $R(\theta) = e^{\frac{i}{\hbar}(\vec{\nabla}\wedge\vec{P})_z\,\theta}$

$\frac{i}{\hbar}(rAp)_z = \frac{i}{\hbar}xp_y - yp_x$ visto che $x = (a+a^\dagger)\sqrt{\frac{\hbar}{2m\omega_x}}$ e $p_x = -i(a-a^\dagger)\sqrt{\frac{m\hbar\omega}{2}}$ abbiamo che

$\frac{i}{\hbar}(rAp)_z = (a_x+a_x^\dagger)(a_y-a_y^\dagger)\frac{1}{2}\sqrt{\frac{\omega_y}{\omega_x}} - (a_x-a_x^\dagger)(a_y+a_y^\dagger)\frac{1}{2}\sqrt{\frac{\omega_x}{\omega_y}}$

$[a_x, \frac{i}{\hbar}(rAp)] = (a_x-a_x^\dagger)\frac{1}{2}\sqrt{\frac{\omega_y}{\omega_x}} - (a_x+a_x^\dagger)\sqrt{\frac{\omega_x}{\omega_y}}$

Ricordiamoci che ci mettiamo nel sistema di riferimento rotante perché così ci leviamo dai piedi la sconvenienza della precessione lungo l'asse z

Adesso scriviamo la prima Hamiltoniana nel sistema rotante

$$\tilde{H}_1 = -\frac{\hbar\omega_1}{4}(\sigma_+ e^{i\omega t} + \sigma_- e^{-i\omega t})\left[e^{i\omega t} + e^{-i\omega t}\right] \simeq -\frac{\hbar\omega_1}{4}\left[\sigma_+ e^{i(\omega_0-\omega)t} + \sigma_- e^{-i(\omega_0-\omega)t}\right]$$

All'ultimo ho applicato l'approssimazione d'onda rotante.

Questa Hamiltoniana ci permette di effettuare rotazioni dello spin con l'asse di rotazione nel piano x-y, i livelli energetici relativi al potenziale armonico restano invariati

Adesso vediamo com'è e cosa fa $\tilde{H}_2$

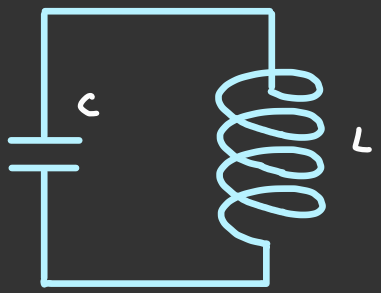
$$\tilde{H}_2 = \frac{\hbar\omega_1}{4}(\sigma_+ e^{i\omega_0 t} + \sigma_- e^{-i\omega_0 t})(a^\dagger e^{i\omega t} + a e^{-i\omega t})\left[e^{i\omega t} + e^{-i\omega t}\right] \simeq$$

$\simeq$ Da finire

Qbit a Superconduttore

I qbit esaminati fin ora sono molto sensibili a perturbazioni esterne, i superconduttori invece sono molto meglio da questo punto di vista. Inoltre è possibile fabbricare un circuito a superconduttore per far sì che vada incontro alle nostre esigenze.

Prima di tutto dobbiamo costruire un circuito che abbia dei livelli energetici. Il circuito qui a destra è un oscillatore LC. Facendo un pò di conti si ottiene l'Hamiltoniana



Flusso che passa attraverso tutto il circuito → Φ

$$H = \frac{\Phi^2}{2L} + \frac{q^2}{2C}$$ ← Carica

Questa Hamiltoniana è equivalente a quella di un oscillatore armonico con frequenza $\omega_0 = \sqrt{LC}$.

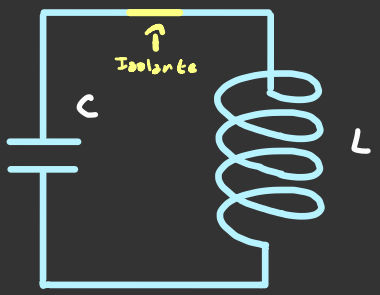
In questo caso lo stato della corrente è quantistica e funge da qbit.

È possibile aggiungere o rimuovere corrente facendo passare un campo alternato dentro all'induttore.

Questo sistema però ha il grosso problema che ha i livelli energetici equispaziati, quindi la stessa forzante che ci fa passare dal primo livello energetico al secondo, ci fa passare dal secondo al terzo, ecc...

Per ovviare a questo problema bisogna inserire una non linearità nel sistema.

Un modo per farlo è creare un pezzo di circuito dove la corrente è costretta a passare per effetto tunnel.



Questo può esser fatto mettendo dell'**isolante** in un pezzo del circuito al posto del **Superconduttore**.

Dal punto di vista circuitale questo elemento viene detto "Giunzione di Josephson" e viene raffigurato così

Io non mi metterò a fare tutti i conti dell'effetto tunnel e mi limiterò a descrivere la giunzione come semplice elemento circuitale.

Il contributo all'Hamiltoniana dovuta alla giunzione è

$$H_J = -J \cos\left(2\pi \frac{\phi}{\phi_0}\right)$$

$$J = \frac{I_0 \phi_0}{2\pi} \qquad \phi_0 = \frac{h}{2e}$$

$$I_0 = \sqrt{\rho_1 \rho_2}\, \frac{2\pi}{h}$$ ← Costante di Tunneling

ρ_1, ρ_2: Densità elettroniche ai capi della giunzione

Per tutti gli effetti pratici possiamo trattare J come una costante e scordarci di cosa è fatta e da dove viene.

A questo punto i livelli energetici non sono più equispaziati e si possono usare i primi due come qbit.