Alma Mater Studiorum · Università di Bologna

Scuola di Scienze
Dipartimento di Fisica e Astronomia
Corso di Laurea in Fisica

Sviluppo di porte logiche quantistiche

Relatore:
Dott. Cristian Degli Esposti Boschi

Presentata da:
Michele Fossati

Anno Accademico 2016/2017

Indice

Sommario

In questo testo tratteremo alcuni punti importanti nel campo della computazione quantistica, analizzando in particolare certi aspetti di fondo della realizzazione delle porte logiche quantistiche.

Dopo una breve introduzione sulla computazione ed alcune caratteristiche particolari, proprie del mondo quantico, da tenere in considerazione nella realizzazione dei QuBit, l'entità in cui viene immagazzinata l'informazione equivalente al bit classico dei computatori, inizieremo la discussione sulla realizzazione delle porte logiche quantistiche.

Tratteremo di come viene descritto un QuBit, dai suoi stati rappresentati tramite operatore di densità, che nel caso di una singola unità si riduce alla cosiddetta sfera di Bloch. Discuteremo di conseguenza sia le porte logiche quantistiche che operano su singolo QuBit che di controllo, specialmente tratteremo l'importanza di poter avere una porta universale equivalente al NAND.

Tutto questo per poi argomentare come sia possibile realizzare una implementazione fisica. Delle varie possibilità tratteremo le trappole ioniche, dove vengono usati gli stati interni della struttura iperfine e dei livelli vibrazionali degli ioni per rappresentare il QuBit. Questo specialmente per la capacità dello stato interno, piuttosto che quello vibrazionale, di avere lunghi periodi di coerenza.

Argomenteremo su come siano possibili realizzare delle porte logiche quantistiche per questa metodologia, con maggior premura riguardo alla C-NOT (Contolled-NOT). Questo a dimostrare che un implementazione di queste porte è possibile ed effettivamente realizzata sperimentalmente.

Concluderemo questa dissertazione con una breve analisi critica della metodologia studiata e una prospettiva su possibili impieghi futuri.

Capitolo 1 Introduzione

Per avere un'idea dei motivi che hanno spinto a ricercare una metodologia atta a realizzare una macchina capace di computazione quantistica, occorre un attimo vedere alcuni aspetti generali della scienza computazionale.

Comprendere cosa si intenda per computazione e le varie risorse che servono per essa, usando classici esempi per fare chiarezza come la macchina di Turing. Analizzando velocemente anche la parte elettronica che vi è dietro.

Approfondiremo descrivendo i problemi decisionali, suddivisi per complessità in problemi P e NP. Se fosse possibile che i problemi P siano in relazione diretta con gli NP e non semplicemente un suo sottogruppo, con menzione in questo caso alla tecnica di riduzione.

Infine si discuteranno sia i famosi criteri di Di Vincenzo i quali, accenniamo ora, descrivono sia le caratteristiche generali che un computer quantistico dovrebbe possedere e sia di come uno dei principali problemi, che si affrontano in questo campo, sia legato ad un fenomeno fisico denominato decoerenza e simile per certi versi al rumore nell'elettronica.

1.1 Metodi di Computazione

Attualmente possiamo definire la computazione come un qualsiasi sistema o algoritmo che viene sfruttato per eseguire dei calcoli. In questa prospettiva un computer non è altro che un sofisticato calcolatore, che può essere programmato per eseguire una serie di operazioni.

Un quesito a tal riguardo venne posto da David Hilbert nel 1928, ipotizzando se fosse possibile l'esistenza di un algoritmo universale, in grado da solo di risolvere qualsiasi problema matematico. Questo quesito chiamato Entscheidungsproblem [01], che si traduce come problema decisionale, venne studiato e contro-intuitivamente la risposta che trovarono ad esso fu negativa.

Ricercatori noti del passato come Alan Turing e Alonzo Church per giungere ad una tale conclusione in questa ricerca diedero la nascita alle teorie fondamentali della scienza computazionale.

La Macchina di Turing

Partiamo con i risultati del matematico Turing, la cui pubblicazione avvenuta nel 1936 esce poco dopo il lavoro di Church e ad essa indipendente, si sviluppa attorno al concetto di una

macchina di computazione ideale nominata Macchina di Turing che ora illustreremo.

Il dispositivo, nella sua forma più generale, viene descritto come costituito da quattro semplici elementi di base: un nastro infinito, che funziona da memoria; una testina che legge/scrive sul nastro, la quale si sposta sul nastro e lavora ovviamente sulla parte in cui la sua testa poggia; uno stato di controllo finito, l'equivalente di un microprocessore che coordina le varie operazioni; infine il programma, non di meno un codice di istruzioni che la macchina deve eseguire.

Più nel dettaglio, ripartiamo col descrivere più nel dettagliatamente questi elementi ripartendo dal nastro. Si tratta da come sì può intuire dall'immagine (Fig. 1) che è un oggetto unidimensionale di lunghezza infinita. Il nastro viene diviso in infinite celle che contengono ciascuna un simbolo, per convenienza si potrebbero scegliere dall'insieme {0,1,-,S} dove per - si intende uno spazio vuoto e per S la cella iniziale.

La testina si muove quindi su questo nastro partendo convenientemente dalla cella S, essa potrà poi muoversi, secondo i comandi datogli dallo stato di controllo, sul nastro. Essa si muoverà di cella in cella, potendo leggere e riscrivere solamente quella che al momento sta puntando.

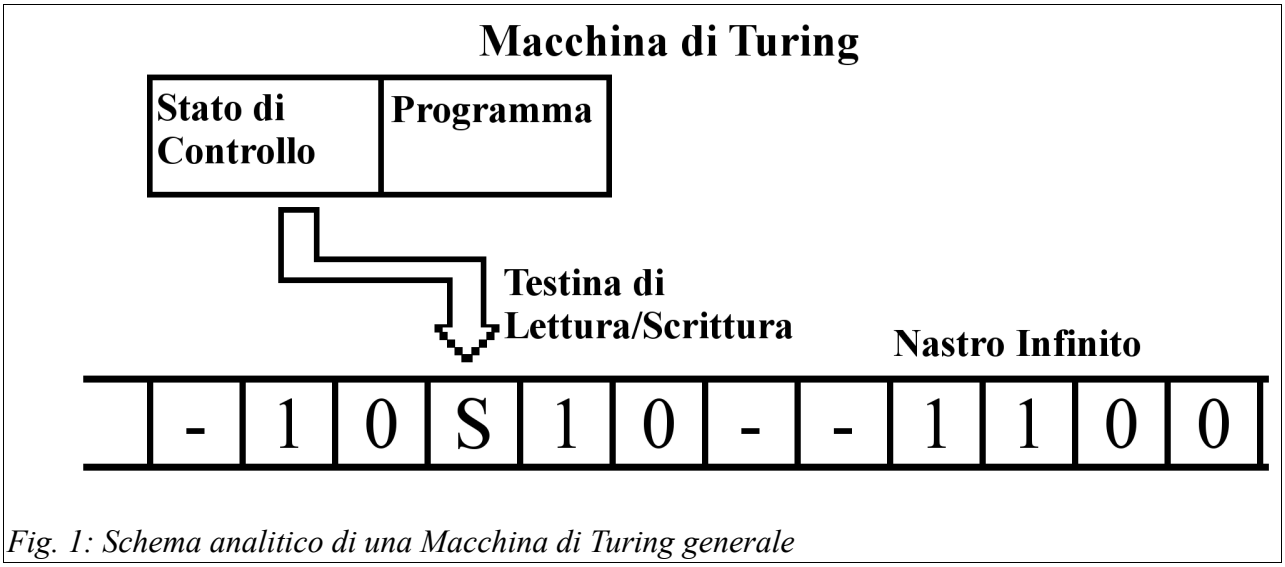


Fig. 1: Schema analitico di una Macchina di Turing generale

Discutendo dello stato finito di controllo, deve avere un numero N finito di stati interni q_1, q_2, …, q_N. Seppur N è una variabile, se preso per valori molto grandi si nota che l'efficienza della macchina non cambia sostanzialmente, permettendoci in questo caso di considerarla una costante senza perdita di generalità. Si possono poi aggiungere due ulteriori stati q_s e q_h, i quali definiscono lo stato di partenza e di arresto della macchina. Possiamo considerare lo stato finito di controllo, come già accennato, alla stregua di un microprocessore il quale imposta le operazioni che deve seguire il dispositivo.

L'ultimo elemento, il programma, è una lista di linee finite nella forma < q, x, q', x', S_C >. Analizzando la linea abbiamo subito q come stato in qui si trova la macchina e x il valore letto dalla testina. La macchina si mette alla ricerca di una linea che inizia per l'appunto con < q, x, *, *, * > da eseguire. In caso non la trovasse lo stato viene cambiato in q_h. Nel caso contrario viene eseguita la linea con i valori corrispondenti. Lo stato interno cambia in q' e la testina scrive il valore di x' sulla cella che sta puntando, poi si sposta di una cella a destra, sinistra o rimane ferma in base se S_C sia di valore +1, -1 o 0.

Una tale macchina è in grado di eseguire una vasta gamma di algoritmi o, per dare un idea più chiara della sua potenzialità, può altresì simulare un moderno computer. In seguito riportiamo a riguardo una tesi formulata in maniera indipendente sia da Church che da Turing, la quale cattura in pieno la nozione di come una macchina di Turing possa computare una funzione potendo utilizzare un algoritmo.

Tesi di Church-Turing: Le classi di funzioni computabili da una macchina di Turing corrispondono esattamente alle classi di funzioni che verrebbero considerate naturalmente come computabili da un algoritmo

Modello circuitale

Questo secondo approccio alla teoria della computazione differisce dalla macchina di Turing per un approccio più realistico al problema, ma rimanendone comunque equivalente.

Un circuito è costituito normalmente da porte logiche e fili elettrici, i primi che eseguono operazioni logiche elementari e i secondi che trasportano l'informazione come corrente elettrica. La mancanza di corrente viene codificata come 0 e la presenza del flusso come 1. Possiamo altresì avere più di un valore all'ingresso al circuito così come più di un valore in uscita. Formalmente potremmo definire un circuito equivalentemente a una trasformazione F: $\{0,1\}_i$ -->$\{0,1\}_u$, dove abbiamo i ingressi e u uscite.

Possiamo intuitivamente progettare così un circuito, conoscendo le trasformazioni che fanno le singole porte logiche, per implementare macchine fisiche che sono in grado di computare delle funzioni similmente ad una macchina d Turing.

Una caratteristica che ci tornerà utile da rivedere è l'impiego di porte logiche universali. Con queste si ha la

Teoremi di De Morgan

$$\overline{A * B} = \overline{A} + \overline{B}$$
$$\overline{A + B} = \overline{A} * \overline{B}$$

Fig. 2:I teoremi di De Morgan portano una relazione negli operatori di coniugazione logica boleana

possibilità di realizzare un intero circuito, qualsiasi esso sia, con l'impiego di un solo tipo di porta di questa categoria. Per l'elettronica classica l'esistenza di porte logiche universali, nel caso specifico le porte NAND e NOR, può essere dimostrata grazie all'utilizzo dei teoremi di De Morgan (Fig. 2).

1.2 Problemi P e NP

La ricerca è l'uso di metodi computazionali per simulare algoritmi sempre via via più complessi porta alla luce nuovi problemi da affrontare. La classe di problemi che andremo a discutere sarà quella dei problemi decisionali, ovvero quei problemi in cui si deve dare un risposta affermativa o negativa. Rappresentabili col formalismo D : I → {False;True} dove: D sta per domanda; I sta per istanza o le informazioni che abbiamo al corrente; False e True sono le due possibili risposte.

Usando degli algoritmi per cercare una risposta a questi quesiti, si incorre sia ad un costo di risorse che di tempo da impiegare. Problemi come la somma di due numeri occupano un tempo polinomiale, dipendente dalla lunghezza N delle stringe in ingresso e dal loro numero totale K per una Macchina di Turing. Sicché un quesito che richieda delle risorse dipendenti da $O(F(N^K))$ viene detto *polinomiale* o P [02].

Esistono poi problemi *non polinomiali deterministici* o NP , di complessità maggiore, che differiscono dai precedenti dal fatto che è più facile verificare che la risposta data sia corretta che ottenere la stessa. Una analogia sarebbe che è più facile verificare che la moltiplicazione di due numeri primi ci dia X, piuttosto che trovare i due numeri primi che moltiplicati ci diano X. Questi problemi impiegano un tempo polinomiale per essere risolti nel caso si utilizzi una Macchina di Turing non deterministica, ovvero che per uno stesso stato iniziale e di lettura esistono più righe di comando che possono essere eseguiti.

Vediamo quindi che P diviene allora un sottogruppo di NP, ma la possibilità che ci siano dei problemi in NP che non possano essere risolti in P rimane tutt'ora aperta. Se si dimostrasse P=NP significherebbe che i problemi decisionali NP hanno una *riduzione* che li porterebbe ad essere trattati come P.

La *riduzione* è un metodo che significa il poter trasformare un problema in un altro equivalente da un punto di vista delle risorse di calcolo, è un concetto alla base della scienza dei computer. In un formalismo più matematico, avendo due linguaggi A e B avremmo che A e riducibile a B solamente se per ogni elemento $x \in A$ esiste un algoritmo R che viene eseguito in un tempo polinomiale da una

Macchina di Turing tale che si ottiene R(x) ϵ B.

Questa ricerca diviene di particolare interesse specialmente per via del grande numero di problemi NP-completi esistenti, definiti come problemi K appartenenti a NP tali che ogni altro problema K' sia riducibile a K. La particolarità è che se si trova una soluzione per risolvere rapidamente, in un tempo polinomiale, un problema di classe NP-completo, si può usare la stessa per risolvere tutti gli stessi NP della stessa classe in tempo polinomiale per via della *riduzione*.

1.3 Criteri di Di Vincenzo

Un calcolatore quantistico possiede delle caratteristiche tecniche ben diverse da un calcolatore classico, pur potendo essere simulati in tempi lunghi da quest'ultimi. Alla base vi è la sostituzione dei più comuni e comprensibili Bit con i QuBit per rappresentare l'informazione.

Per la realizzazione di un calcolatore quantistico devono venir presi in considerazione i criteri di Di Vincenzo [03]. Questi ci permettono di porre delle linee guida generali da seguire, in particolar modo definendo le quattro caratteristiche fondamentali che deve possedere una tale macchina:

1. Deve essere in grado di rappresentare i QuBit;

Bisogna adoperare un metodo per utilizzare le caratteristiche dei fenomeni studiati nella meccanica quantistica, quali sono la sovrapposizione e l'entaglement ad esempio, per rappresentare l'informazione che vogliamo.

2. Capace di realizzare su questi un gruppo di trasformazioni unitarie;

Poter usare dei dispositivi che implementano delle porte quantistiche, come Hadamard o C-NOT, che sono tutte delle trasformazioni unitarie.

3. Preparare uno stato iniziale con sufficiente fiducia;

Essere in grado di preparare lo stato del QuBit in uno specifico stato, che converrebbe essere una configurazione semplice da realizzare. Si deve avere una buona fiducia della sua condizione senza poterlo misurare, poiché pure in questa maniera può essere cambiato.

4. Essere in grado di misurarne il risultato finale;

Dopo tutte le operazioni di calcolo, o meglio le trasformazioni unitarie che verranno svolte sul nostro QuBit, è indispensabile un metodo per riuscire ad ottenere lo stato di quest'ultimo ricavando il valore delle computazioni eseguite.

Si precisa che la velocità in cui si eseguono le varie computazioni sul QuBit, fra quando lo stato

viene inizializzato e poi misurato, deve essere tale che l'informazione non venga persa prima a causa della *decoerenza.* Viene reso possibile così solo un numero finito di operazioni che si possono fare prima di perdere l'informazione, in base alla metodologia adoperata (Tab. 1).

Un ultimo dettaglio da tenere in considerazione, ma comunque importante per un efficiente uso di un calcolatore quantistico è la *scalabilità*. Un processore di tale genere non dovrebbe in questo caso presentare problemi o costi insostenibili all'aumentare del numero di QuBit che vengono adoperati. E' la controparte di quello che avviene nei calcolatori classici, dove si riesce ad aumentare la potenza e la rapidità dei calcoli eseguibili miniaturizzando sempre di più i processori, senza riscontrare perdite di prestazioni. Questo fintanto che non vengano raggiunte delle scale di grandezza fisiche per le quali la miniaturizzazione viene limitata in maniera definitiva.

Sistema adoperato	Td (secondi)	Top (secondi)	Nop
Spin nucleare	10^{-2} - 10^{8}	10^{-3} - 10^{-6}	10^{5} - 10^{14}
Spin elettronico	10^{-3}	10^{-7}	10^{4}
Trappola Ionica (In^{+})	10^{-1}	10^{-14}	10^{13}
Elettrone - Au	10^{-8}	10^{-14}	10^{6}
Elettrone - GaAs	10^{-10}	10^{-13}	10^{3}
Punto Quantico	10^{-6}	10^{-9}	10^{3}
Cavità Ottica	10^{-5}	10^{-14}	10^{9}
Cavità Microonde	10^{0}	10^{-4}	10^{4}

Tab. 1: Confronto dei tempi di decoerenza e dell'esecuzione delle operazioni per differenti sistemi, si faccia caso alla terza colonna per evidenziare il numero di operazioni eseguibili prima che avvenga la decoerenza [02]

1.4 Decoerenza

Un fenomeno da tenere in considerazione, nei procedimenti di realizzazione di un QuBit, è la *decoerenza* [02] accennata poco fa che porta alla perdita dell'informazione. Simile per certi aspetti ha un effetto paragonabile al *rumore* dell'elettronica classica, essa non è correlata ad un disturbo esterno ma dipende molto dalla metodologia impiegata con cui sviluppiamo il QuBit.

Si tratta di un avvenimento probabilistico, che causa una spontanea e inevitabile perdita di informazione. Similmente come un elettrone in uno stato eccitato tende spontaneamente a perdere energia, per tornare allo stato fondamentale. Questo non avverrebbe in un sistema completamente

isolato e si deve a interazioni incontrollate con l'ambiente la cui funzione d'onda non è completamente isolata da quella del sistema.

Si sottolinea che la *decoerenza* rimane comunque un fenomeno quantistico, meglio rappresentabile tramite la *Sfera di Bloch* che è altresì una ottima rappresentazione per un QuBit. Questo fenomeno porta alla perdita dello stato di sovrapposizione fra due stati, divenendo una *miscela statistica*, che può essere descritta dall'operatore di densità.

Un altro caso semplice può essere visionato con la teoria fenomenologica degli A e B di Einstein, una descrizione semi-classica dell'interazione fra materia e radiazione elettromagnetica. Se abbiamo un numero elevato di atomi N nello stato fondamentale e si applica un campo elettromagnetico, si ha una probabilità che N' atomi siano stati portati al primo stato eccitato. In questo caso gli atomi possono ritornare allo stato fondamentale in due maniere, o per *emissione stimolata* sempre tramite la presenza di un campo elettromagnetico o per *emissione spontanea* in maniera indipendente ad altro fattori esterni.

Per l'esempio che ci prefiggiamo prendiamo un campione di un solo atomo, il controllo probabilistico nel suo stato fondamentale o nel primo eccitato, può essere controllato tramite un campo elettromagnetico ma *l'emissione spontanea* fa sì che inevitabilmente ritorna nello stato fondamentale. Così l'informazione in cui lo stato si trovava si perde, similmente a come potremmo perdere l'informazione immagazzinata in un QuBit per un fenomeno di *decoerenza.*

Capitolo 2 Porte Logiche

Dopo aver visto alcune tematiche di base del mondo della computazione, possiamo ora approcciare i temi principali riguardanti la realizzazione e implementazione delle principali porte logiche quantistiche.

Partiremo con le basi, descrivendo quindi come si può rappresentare e vedere un QuBit. Di conseguenza tratteremo sia la sfera di Bloch che la matrice densità e rivedremo come viene la perdita di informazione a causa della decoerenza. In particolare vedremo come lo stato del sistema possieda particolari caratteristiche quando si ha più di un singolo QuBit.

Mostreremo le porte logiche quantistiche e come queste cambino lo stato del QuBit con cui interagiscono. Divideremo la trattazione in porte logiche a singolo QuBit e di controllo, in cui lo stato di un QuBit bersaglio viene cambiato anche in base a quello di altri definiti appunto di controllo.

Un altro fattore interessante che andremo a analizzare e con cui concluderemo il capitolo è l'individuazione di una porta logica universale di tipo quantistico, che costituisce per similitudine al NAND dei circuiti classici.

2.1 Rappresentazione di QuBit

A differenza dei Bit classici, che possono avere solo 0 e 1 come valori, un QuBit può trovarsi in un una sovrapposizione di questi due valori. Questi vengono riscritti nella notazione di Dirac $|0\rangle$ e $|1\rangle$ [02]. Una rappresentazione generale di uno stato che si trova in sovrapposizione è:

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

dove α e β sono numeri complessi il cui modulo quadro ci fornisce la probabilità di trovare il QuBit nello stato $|0\rangle$ per $|\alpha|^2$ e nello stato $|1\rangle$ per $|\beta|^2$. Inoltre devono rispettare l'equazione $|\alpha|^2 + |\beta|^2 = 1$ come condizione che lo stato del QuBit sia normalizzato, rendendo generalmente lo stato del QuBit come un vettore a due dimensioni:

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

Tocca precisare che questo stato di sovrapposizione perdura fino a quando non viene misurato il valore del QuBit, il quale può riportare solo il valore 0 o 1 con la probabilità descritte prima. Prendendo ad esempio:

$$|\psi\rangle = \sqrt{\frac{3}{4}}|0\rangle + \sqrt{\frac{1}{4}}|1\rangle$$

si ottiene come risultato nel 75% dei casi $|0\rangle$ e nel 25% restante $|1\rangle$.

Una rappresentazione migliore per un singolo QuBit la possiamo ottenere per mezzo della *sfera di Bloch* [02] la quale fornisce una descrizione geometrica dei vari valori che si possono ottenere (Fig. 3).

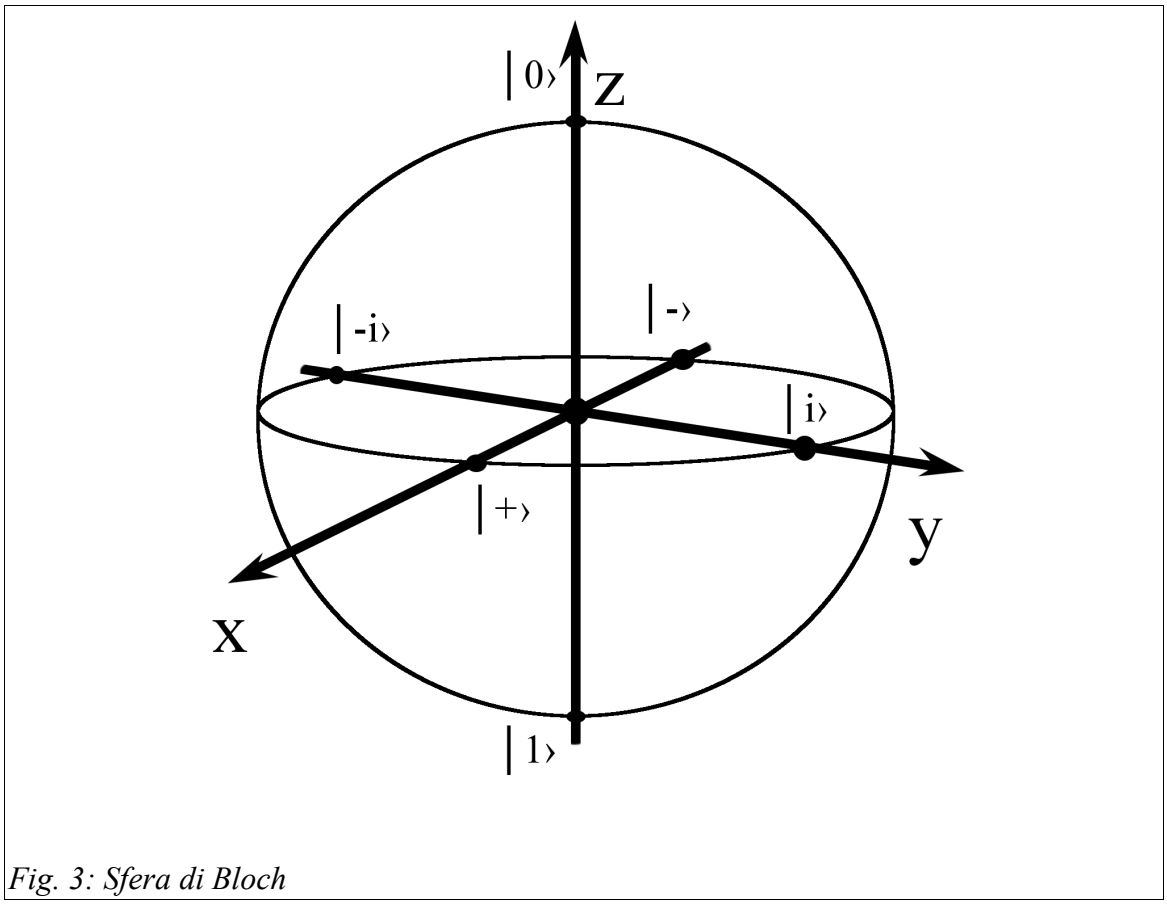


Fig. 3: Sfera di Bloch

Possiamo notare che un qualsiasi punto della superficie della sfera rappresenta un valore unico, dove i valori ai due poli dell'asse $\hat{z}$ sono li stati $|0\rangle$ e $|1\rangle$. Teoricamente un solo QuBit potrebbe immagazzinare una quantità illimitata di informazione in questa maniera, ma ad ogni misurazione la sovrapposizione è costretta a collassare in uno dei due stati principali perdendo tutto

il resto. Lo stato riscritto per indicare un punto sulla sfera diviene:

$$\begin{aligned} |\psi\rangle &= \alpha\,|0\rangle + \beta\,|1\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\varphi}\sin\left(\frac{\theta}{2}\right)|1\rangle \\ &= \cos\left(\frac{\theta}{2}\right)|0\rangle + [\cos(\varphi)+i\sin(\varphi)]\sin\left(\frac{\theta}{2}\right)|1\rangle \end{aligned}$$

con θ e φ numeri reali. Possiamo inoltre indicare il punto sulla sfera tramite vettore di Bloch $\vec{r}$, usando gli stessi parametri θ e φ come gli angoli polari del versore:

$$\vec{r} = \begin{bmatrix} \sin(\theta)\cos(\phi) \\ \sin(\theta)\sin(\phi) \\ \cos(\theta) \end{bmatrix} = \begin{bmatrix} u \\ v \\ w \end{bmatrix}$$

Gli stati $|+\rangle$, $|-\rangle$, $|i\rangle$ e $|-i\rangle$ che sono mostrati in Fig. 3 equivalgono ai ket:

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \quad |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}} \quad |i\rangle = \frac{|0\rangle + i|1\rangle}{\sqrt{2}} \quad |-i\rangle = \frac{|0\rangle - i|1\rangle}{\sqrt{2}}$$

Usiamo il caso più semplice di due QuBit per vedere quali stati si ottengono:

$$|\psi\rangle = \alpha_1|00\rangle + \alpha_2|01\rangle + \alpha_3|10\rangle + \alpha_4|11\rangle$$

qui avremmo nuovamente per la normalizzazione $\sum_i |\alpha_i|^2 = 1$. Avendo N QuBit si avrà una combinazione lineari di 2^N stati finali. Nel caso si misura lo stato di un solo QuBit, ad esempio il primo, la funzione muta come:

$$|\psi_m\rangle = \frac{\alpha_1|00\rangle + \alpha_2|01\rangle}{\sqrt{|\alpha_1|^2 + |\alpha_2|^2}}$$

questo considerando che $|\psi_m\rangle$ sia la stato ottenuto da $|\psi\rangle$ dove il primo QuBit riporta come valore lo stato $|0\rangle$ dalla sua misurazione.

Un particolarità di questa conseguenza emerge studiando degli specifici stati a due QuBit, chiamati *stati di Bell* [02]:

$$|\psi^+\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}} \qquad |\phi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$
$$|\psi^-\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}} \qquad |\phi^-\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}}$$

conoscendo lo stato del ket con cui stiamo lavorando, in queste condizioni prima di misurare in che stato si trova uno solo dei QuBit avremmo il 50% di possibilità di ottenere 0 e il 50% di probabilità di avere 1. L'interesse risiede nel fatto che per come è costruito lo stato composto sapremmo già il valore del secondo QuBit prima di misurarlo, la prima misura influenza anche lo stato non osservato rivelando un correlazione forte fra i due QuBit. Cambiando lo stato di un solo elemento vengono cambiati gli stati di tutti gli altri QuBit.

Abbiamo così mostrato un esempio semplice di come agisce il fenomeno di *entanglement* in sistemi quantistici costituiti da molte parti. Quello che vogliamo realizzare adesso è un sistema che ci permetta di tenere conto degli effetti di correlazione del primo QuBit sul secondo, introducendo una struttura che descrivi solo quest'ultimo.

Per cogliere questo e altri aspetti più generali degli stati quantistici si introduce il concetto di *matrice densità* o *operatore densità* [02], la *sfera di Bloch* è una rappresentazione di questa nel caso specifico si avesse un solo QuBit. Si tratta di un formalismo matematico che ne agevola la visualizzazione degli stati rispetto alla forma vettoriale. Prendendo uno stato vettoriale $|\psi\rangle$ di un numero imprecisato di QuBit, si ricava la matrice densità ρ dal prodotto tensoriale di $|\psi\rangle\langle\psi|$:

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$$

gli stati $|\psi_i\rangle$ vengono detti puri e sono usati per costruire una miscela statistica di pesi p_i, realizzando l'ensemble $\{p_i, |\psi_i\rangle\}$.

Un generico stato puro per un solo QuBit della forma $\alpha|0\rangle + \beta|1\rangle$ verrà così riscritto:

$$\rho = \begin{bmatrix} |\alpha|^2 & \alpha\beta^* \\ \beta\alpha^* & |\beta|^2 \end{bmatrix}$$

se la matrice è espressa nella forma $|0\rangle$ e $|1\rangle$.

Serve precisare che in questo modo non vengono solo rappresentate sovrapposizioni di stati, ma anche miscele statistiche. Se prendiamo uno stato $|\psi\rangle$ che ha il 50% di possibilità di trovarsi in $|\psi_1\rangle = |0\rangle$ e il 50% in $|\psi_2\rangle = |1\rangle$, che non è uno stato di sovrapposizione ma una miscela

statistica poiché non abbiamo ampiezze di probabilità ma distribuzioni classiche di probabilità degli stati scriveremo:

$$\rho = \sum_{i=1}^{2} a_i \left| \psi_i \right\rangle \left\langle \psi_i \right| = \frac{1}{2} \left| 0 \right\rangle \left\langle 0 \right| + \frac{1}{2} \left| 1 \right\rangle \left\langle 1 \right| = \frac{1}{2} \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} + \frac{1}{2} \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$$

$$\rho = \frac{1}{2} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

indicando che lo stato iniziale quantistico non è sempre preparato allo stesso modo ma per la precisione sarà metà delle volte in $\left| 0 \right\rangle$ e metà delle volte in $\left| 1 \right\rangle$. possono comunque venir rappresentati stati puri e in sovrapposizione. Nel caso della formula, le due prime matrici sono stati puri in cui nel primo $\left| 0 \right\rangle$ ha il 100% e nel secondo $\left| 1 \right\rangle$ ha il 100% di probabilità.

L'utilità particolare di usare miscele statistiche deriva specialmente dal fatto che con sistemi composti, dei quali si osserva solo una parte, non è possibile definire una sua sottoparte attraverso un singolo ket, sebbene il tutto si trovi in uno stato definito. Altri fattori sono dovuti alla incertezza sullo stato iniziale preparato in molti modi non identici.

Le caratteristiche che devono possedere tali matrici sono le seguenti:

1. La traccia della matrice deve essere uguale a uno:

$$Tr(\rho) = \sum_i p_i Tr(\left| \psi_i \right\rangle \left\langle \psi_i \right|) = \sum_i p_i = 1$$

   Questo è dovuto alla particolarità in cui gli elementi della diagonale definiscono la probabilità che si ottenga un determinato stato finale, per questo la somma di tutte gli eventi deve essere unitaria.
   La traccia risulta invariante per cambi di base, questa condizione mostra come la probabilità totale di osservazioni di uno stato venga conservata.

2. La matrice deve essere definita positiva:

$$\left\langle \phi \right| \rho \left| \phi \right\rangle = \sum_i p_i \left\langle \phi_i \right| \psi_i \left\rangle \right\langle \psi_i \left| \phi_i \right\rangle = \sum_i p_i \left| \left\langle \phi_i \right| \psi_i \left\rangle \right|^2 \geq 0$$

   Dove $\left| \varphi \right\rangle$ è un generico vettore di stato.

3. La matrice deve essere Hermitiana:

$$\rho = \rho^{\dagger}$$

Possiamo derivare un ulteriore caratteristica dalla traccia che è sempre $Tr(\rho^2) \leq 1$, da cui si ricavano il caso di miscela statistica per un valore minore di 1 e di stato puro per l'uguaglianza. Nel secondo caso si ottiene anche $\rho^2 = \rho$.

Possiamo riscrivere la sfera di Bloch tramite matrice di densità adoperando il vettore di Bloch, la matrice identità I e le *matrici di Pauli*:

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad \sigma_x = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad \sigma_y = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad \sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad \vec{\sigma} = \hat{x}\sigma_x + \hat{y}\sigma_y + \hat{z}\sigma_z$$

$$\rho = \frac{1}{2}(I + \vec{r}\,\vec{\sigma})$$

da qui possiamo vedere che $|\vec{r}|^2 < 1$ per le miscele statistiche e il vettore indica un punto interno alla sfera di Bloch, mentre per $|\vec{r}|^2 = 1$ si ha uno stato puro e il vettore indica un punto della superficie della sfera.

Un particolare che viene spesso frainteso è quello di associare ad un singolo stato la matrice di densità ottenuta. Difatti una stessa può descrivere più miscele statistiche non essendo uniche, ad esempio:

$$\rho = \frac{3}{4}|0\rangle\langle 0| + \frac{1}{4}|1\rangle\langle 1|$$

questo ci potrebbe far concludere che il primo stato ha il 75% di probabilità di avvenire ed il secondo il 25% ma tramite:

$$|a\rangle = \sqrt{\frac{3}{4}}|0\rangle + \sqrt{\frac{1}{4}}|1\rangle \qquad |b\rangle = \sqrt{\frac{3}{4}}|0\rangle - \sqrt{\frac{1}{4}}|1\rangle$$

$$\rho = \frac{1}{2}|a\rangle\langle a| + \frac{1}{2}|b\rangle\langle b| = \frac{3}{4}|0\rangle\langle 0| + \frac{1}{4}|1\rangle\langle 1|$$

possiamo vedere che i valori delle probabilità e i ket associati sono diversi e le matrici non uniche.

Riprendendo l'esempio degli stati in entanglement, si introduce il concetto di *matrice di densità*

ridotta. Tramite questo formalismo, possiamo estrarre da un sistema costituito da molte parti un suo sottoinsieme che tiene in considerazioni queste correlazioni. Considerando un sistema realizzato da un elemento A e B descritto da ρ^{AB}, la matrice di densità ridotta di A si ricava da:

$$\rho^{A}=Tr_{B}(\rho^{AB})$$

$$Tr_{B}(|a_1\rangle\langle a_2| * |b_1\rangle\langle b_2|)=|a_1\rangle\langle a_2|\,Tr(|b_1\rangle\langle b_2|)$$

con a_1 e a_2 due vettori dello stato di A e b_1 e b_2 dello stato di B. Il risultato della traccia parziale $TrB(|b_1\rangle\langle b_2|)=\langle b_2|b_1\rangle$ è uguale al valore della traccia del sistema B.

Usando lo stato di Bell $|\phi^{+}\rangle$ possiamo vedere come opera:

$$\rho=|\phi^{+}\rangle\langle\phi^{+}|=\left(\frac{|00\rangle+|11\rangle}{\sqrt{2}}\right)\left(\frac{\langle 00|+\langle 11|}{\sqrt{2}}\right)=$$
$$\frac{|00\rangle\langle 00|+|00\rangle\langle 11|+|11\rangle\langle 00|+|11\rangle\langle 11|}{2}$$

$$\rho^{1}=Tr_{2}(\rho)=$$
$$\frac{Tr_{2}(|00\rangle\langle 00|)+Tr_{2}(|00\rangle\langle 11|)+Tr_{2}(|11\rangle\langle 00|)+Tr_{2}(|11\rangle\langle 11|)}{2}=$$
$$\frac{|0\rangle\langle 0|\langle 0|0\rangle+|0\rangle\langle 1|\langle 1|0\rangle+|1\rangle\langle 0|\langle 0|1\rangle+|1\rangle\langle 1|\langle 1|1\rangle}{2}=$$
$$\frac{|0\rangle\langle 0|+|1\rangle\langle 1|}{2}=\frac{I}{2}$$

dal quale si è estratto il primo QuBit dalla matrice e il risultato finale risulta essere una miscela statistica.

Se prendiamo il fenomeno della decoerenza in ultima analisi, l'effetto che provoca sulla matrice densità è la rapida scomparsa degli elementi fuori dalla diagonale. Possiamo descrivere la matrice densità che include l'effetto tramite stati correlati tra sistema e ambiente:

$$|\varphi\rangle=|\psi\rangle|R\rangle$$

con $|R\rangle$ contributo della decoerenza dove $|R\rangle\rightarrow|R_0\rangle$, causata dall'interazione di un sistema che si cerca di mantenere isolato con l'ambiente che lo circonda. Si può estrarre la matrice di densità ridotta dello stato $|\psi\rangle$, che tiene in considerazione il contributo di $|R\rangle$, il quale risulta:

$$\rho = \\ |\alpha|^2 |0\rangle |R_0\rangle\langle R_0| \langle 0| + \alpha\beta^* |0\rangle |R_0\rangle\langle R_1| \langle 1| + \\ \alpha^*\beta |1\rangle |R_1\rangle\langle R_0| \langle 0| + |\beta|^2 |1\rangle |R_1\rangle\langle R_1| \langle 1|$$

a questo punto riducendo con la traccia parziale sugli stati $|R_0\rangle$ e $|R_1\rangle$ si ottiene la matrice densità ridotta per il primo QuBit che risulta una matrice 2x2:

$$\rho^A = \begin{bmatrix} |\alpha|^2 & 0 \\ 0 & |\beta|^2 \end{bmatrix}$$

dove i termini fuori diagonali della matrice tendono a scomparire. Per la sfera di Bloch la decoerenza fa si che il modulo del vettore $\vec{r}$ diventi minore di 1.

Il motivo per cui si ha questo fenomeno di decoerenza è, per quanto si cerca di mantenere lo stato del sistema più isolato possibile, che questo è inevitabilmente correlato col sistema esterno.

2.2 Quantum Gates

Le porte logiche che dobbiamo realizzare adesso devono essere tutte trasformazioni unitarie, Possiamo inizialmente dividere le porte logiche in due categorie: porte logiche su singolo QuBit e porte logiche di controllo.

Operazione su Singolo QuBit

Definito il QuBit come vettori di dimensione due dipendente da due parametri a e b complessi, che rispettano la norma $|a|^2 + |b|^2 = 1$, le operazioni su singolo devono di conseguenza conservare questa norma e devono essere matrici 2x2 unitarie. Scritta in forma vettoriale lo stato del QuBit diventa:

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

La prima porta logica che possiamo scrivere inspirandoci alla computazione classica è il NOT. Bisogni quindi per questo trovare una matrice che inverta gli stati in maniera tale che

$\alpha \mid 0 \rangle + \beta \mid 1 \rangle \rightarrow \alpha \mid 1 \rangle + \beta \mid 0 \rangle$. Una possibile soluzione è:

$$X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad \rightarrow \quad X \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \beta \\ \alpha \end{bmatrix}$$

Osservando la porta trovata si nota che è una matrice di Paul. Possiamo derivare altre due porte logiche dalle restanti matrici di Pauli:

$$Y \equiv \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \qquad Z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

La prima porta oltre a scambiare i valori fra di loro come per X cambia le fasi ad entrambi gli stati di un valore $\exp(\pm i\pi/2)$, la seconda porta invece si limita a cambiare in negativo il valore del seconda stato.

$$Y \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} -i\beta \\ i\alpha \end{bmatrix} \qquad Z \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \alpha \\ -\beta \end{bmatrix}$$

si può notare che questi si possono costruire a vicenda a meno di un cambiamento di fase:

$$iY = X * Z = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$

A seguire abbiamo la porta logica Hadamard molto importante per il suo utilizzo:

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

Essa se riceve in ingresso lo stato $\mid 0 \rangle$ ci fa avere in uscita $(\mid 0 \rangle + \mid 1 \rangle)/2$, nel caso invece riceve $\mid 1 \rangle$ ci fornirà $(\mid 0 \rangle - \mid 1 \rangle)/2$. E' possibile formulare la forma in uscita se l'ingresso non è uno stato puro di conseguenza come:

$$H \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} \alpha + \beta \\ \alpha - \beta \end{bmatrix}$$

Possiamo infine notare che nella porta logica Z possiamo leggere il valore di -1 come $\exp(i\theta)$ con $\theta = \pi$. Per diversi valori di θ si ottengono diverse matrici unitarie:

$$\begin{bmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{bmatrix}$$

Alcune computazioni utilizzate usando questa caratteristica sono la porta S o di fase con $\theta = \pi/2$ e la porta T o $\pi/8$ che contrariamente al nome ha una fase di $\theta = \pi/4$:

$$S \equiv \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} \qquad T \equiv \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$$

Riportiamo nell'appendice di questo lavoro un riassunto delle principali porte logiche con una loro rappresentazione grafica convenzionale.

Teorema di decomposizione per singolo QuBit Z-Y: si può mostrare, usando due porte logiche Z e Y, che possiamo realizzare tutte le porte a operazione su singolo QuBit. Considerando U un operatore unitario, esistono allora α, β, γ e δ reali tali che:

$$U = e^{i\alpha} R_z(\beta) R_y(\gamma) R_z(\delta)$$

dove $R_z(\theta)$ e $R_y(\theta)$ sono matrici di rotazioni unitarie generate dalle matrici di Pauli:

$$R_y(\theta) = e^{-i\theta Y/2} = I\cos(\frac{\theta}{2}) - iY\sin(\frac{\theta}{2}) = \begin{bmatrix} \cos(\frac{\theta}{2}) & -\sin(\frac{\theta}{2}) \\ \sin(\frac{\theta}{2}) & \cos(\frac{\theta}{2}) \end{bmatrix}$$

$$R_z(\theta) = e^{-i\theta Z/2} = I\cos(\frac{\theta}{2}) - iZ\sin(\frac{\theta}{2}) = \begin{bmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{bmatrix}$$

Per dimostrare il teorema consideriamo U. Essendo una matrice unitaria le sue righe e colonne sono ortonormali fra di loro, di conseguenza possiamo ricavare dei valori α, β, γ e δ reali che soddisfino:

$$U = \begin{bmatrix} e^{i(\alpha-\beta/2-\delta/2)}\cos(\frac{\gamma}{2}) & -e^{i(\alpha-\beta/2+\delta/2)}\sin(\frac{\gamma}{2}) \\ e^{i(\alpha+\beta/2-\delta/2)}\sin(\frac{\gamma}{2}) & e^{i(\alpha+\beta/2+\delta/2)}\cos(\frac{\gamma}{2}) \end{bmatrix}$$

Possiamo avere una decomposizione X-Y, sostituendo a $R_z(\theta)$ la rotazione $R_x(\theta)$:

$$R_x(\theta) = e^{-i\theta X/2} = I\cos(\frac{\theta}{2}) - iX\sin(\frac{\theta}{2}) = \begin{bmatrix} \cos(\frac{\theta}{2}) & -i\sin(\frac{\theta}{2}) \\ -i\sin(\frac{\theta}{2}) & \cos(\frac{\theta}{2}) \end{bmatrix}$$

Operazione Controllata

Le porte logiche di questo tipo presentano uno o più QuBit di controllo e un bersaglio. La caratteristica è che lo stato del QuBit bersaglio viene cambiato in base allo stato del QuBit controllo. Per queste porte abbiamo come unica restrizione che la nostra matrice deve essere unitaria, quindi $U^{\dagger}U = I$.

Prendendo il caso semplice con due QuBit, lo stato del sistema è rappresentabile da un vettore di dimensione 4. Più precisamente la dimensione generale del vettore è 2^N, con N il numero di QuBit totali di controllo e bersaglio. Una seconda condizione risulta quindi che le matrici unitarie per una determinata computazione a N QuBit devono essere di dimensioni $2^N x 2^N$:

$$|\psi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle = \begin{bmatrix} \alpha \\ \beta \\ \gamma \\ \delta \end{bmatrix}$$

Come per le porte logiche su singolo QuBit vediamo una trasformazione simile al NOT, la porta C-NOT. Questa in base allo stato di controllo può seguire due possibilità, se riceve $|0\rangle$ lo stato bersaglio non viene alterato mentre se riceve $|1\rangle$ il bersaglio subirà una trasformazione come se passasse per una porta quantica *X*:

$$C-NOT \equiv \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \quad \rightarrow \quad C-NOT \begin{bmatrix} \alpha \\ \beta \\ \gamma \\ \delta \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \\ \gamma \\ \delta \end{bmatrix} = \begin{bmatrix} \alpha \\ \beta \\ \delta \\ \gamma \end{bmatrix}$$

Usando questa porta possiamo realizzarne una che scambi gli stati fra i due QuBit chiamata

SWAP, il procedimento sarebbe di usare tre porte logiche C-NOT. Per illustrarlo definiamo:

$$SWAP = C-NOT_{12}\,C-NOT_{21}\,C-NOT_{12}$$

$$SWAP = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

$$SWAP\begin{bmatrix} \alpha \\ \beta \\ \gamma \\ \delta \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}\begin{bmatrix} \alpha \\ \beta \\ \gamma \\ \delta \end{bmatrix} = \begin{bmatrix} \alpha \\ \gamma \\ \beta \\ \delta \end{bmatrix}$$

La porta $C\text{-}NOT_{CB}$ così scritta indica che il QuBit in C è quello usato per il controllo e quello in B è il bersaglio.

E' possibile realizzare due porte logiche quantistiche universali, di cui discuteremo meglio nella sezione successiva, che sono costituite da 3 QuBit e possono avere 8 stati diversi. Le matrici unitarie in questo scenario sono 8x8.

La prima è la porta di Toffoli o CC-NOT ed equivale ad avere un C-NOT con due stati di controllo. Se questi sono in entrambi in $|1\rangle$ viene eseguito un C-NOT sul terzo, altrimenti non succede nulla:

$$Toffoli \equiv \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

La seconda è la porta di Fredkin o C-SWAP. Qui abbiamo uno stato di controllo e due bersagli. Nel caso lo stato di controllo sia $|1\rangle$ i due bersagli eseguono uno SWAP fra di loro, in caso contrario non cambiano:

$$Fredkin \equiv \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Per completezza sono anche interessanti le porte C-Z e C-S. Similmente al C-NOT eseguono la corrispettiva computazione Z o S sullo stato bersaglio solamente se quello di controllo ha in ingresso $|1\rangle$, altrimenti gli stati bersaglio non vengono modificati:

$$C-Z \equiv \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix} \quad \rightarrow \quad C-Z \begin{bmatrix} \alpha \\ \beta \\ \gamma \\ \delta \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \\ \gamma \\ \delta \end{bmatrix} = \begin{bmatrix} \alpha \\ \beta \\ \gamma \\ -\delta \end{bmatrix}$$

$$C-S \equiv \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & i \end{bmatrix} \quad \rightarrow \quad C-S \begin{bmatrix} \alpha \\ \beta \\ \gamma \\ \delta \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & i \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \\ \gamma \\ \delta \end{bmatrix} = \begin{bmatrix} \alpha \\ \beta \\ \gamma \\ i\delta \end{bmatrix}$$

Da osservare che tutte le porte logiche realizzate in questa maniera sono completamente reversibili. Conoscendo lo stato iniziale sappiamo sempre lo stato finale e sapendo lo stato finale possiamo ottenere a ritroso lo stato iniziale perché sono unitarie, quindi invertibili. Questo sempre in linea teorica poiché alla misura lo stato collassa in uno di quelli possibili, con relativa probabilità e quest'ultimo processo è irreversibile in modo non deterministico.

Un altro processo interessante è l'impossibilità di copiare lo stato di un QuBit in un secondo senza conoscerne lo stato. Una tale macchina che sia in grado dato uno stato generico in ingresso $|\psi\rangle$ di usare uno stato $|\phi\rangle$ su cui viene copiato tale che $|\psi\rangle|\phi\rangle \rightarrow |\psi\rangle|\psi\rangle$ dovrebbe dare un risultato analogo per $|\psi'\rangle$ tale da essere $|\psi'\rangle|\phi\rangle \rightarrow |\psi'\rangle|\psi'\rangle$. Guardando il prodotto scalare notiamo $\langle\phi|\phi\rangle = 1$ ma comporterebbe $\langle\psi|\psi'\rangle = 0$ o $\langle\psi|\psi'\rangle = 1$ contraddicendo la richiesta di avere in ingresso uno stato qualsiasi. L'unica possibilità altrimenti rimane trasferire lo stato del primo tramite SWAP al secondo.

2.3 Quantum Gates Universali

Con le porte di Toffoli e Fredkin abbiamo accennato alle porte logiche quantistiche universali. Queste permettono di realizzare qualsiasi circuito elettrico non usando altre porte, anche se vedremmo che questo non è completamente soddisfatto. In un calcolatore quantistico la realizzazione di tale porta universale avviene tramite operazione su singolo QuBit e C-NOT [04].

Tramite teorema di decomposizione, abbiamo visto come tutte le porte su singolo QuBit potevano essere decomposte in matrici di rotazioni. Per ottenere avere d'altro canto delle porte generali su più QuBit occorre usare delle porte di controllo.

Per creare porte di controllo generali su due QuBit, usando il teorema della decomposizioni, è necessario trovare degli operatori A, B e C tali che il loro prodotto ABC = I quando lo stato del bit di controllo è $|0\rangle$, mentre quando lo stato è $|1\rangle$ diventa AXBXC = W. La X è l'operatore singolo NOT e W rappresenta una porta generale. A dimostrazione di queste asserzioni proponiamo un esempio:

$$A = R_z(\alpha) R_y(\gamma/2) \qquad B = R_y(\gamma/2) R_z(\frac{-\alpha+\beta}{2}) \qquad C = R_z(\frac{\beta-\alpha}{2})$$

$$ABC = R_z(\alpha) R_y(\gamma/2) R_y(\gamma/2) R_z(\frac{-\alpha+\beta}{2}) R_z(\frac{\beta-\alpha}{2}) =$$
$$R_z(\alpha) R_z(-\alpha) = I$$

$$AXBXC = R_z(\alpha) R_y(\gamma/2) X R_y(\gamma/2) R_z(\frac{-\alpha+\beta}{2}) X R_z(\frac{\beta-\alpha}{2}) =$$
$$R_z(\alpha) R_y(\gamma/2) R_y(-\gamma/2) R_z(\frac{\alpha+\beta}{2}) R_z(\frac{\beta-\alpha}{2}) =$$
$$R_z(\alpha) R_y(\gamma) R_z(\beta) = W$$

i parametri α, β e γ sono valori reali che possiamo scegliere accuratamente per implementare qualsiasi porta logica controllata W.

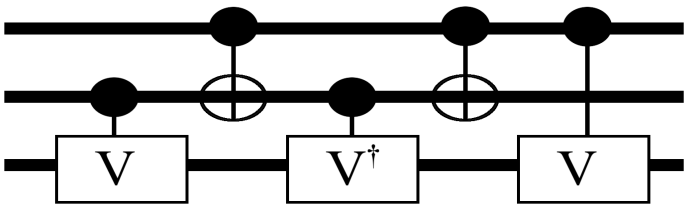
Per particolari porte W è possibile utilizzare solo due A e B tali che possiamo ridurre AB = I e AXB = V:

$$W = R_x(\alpha) R_y(\gamma) R_z(\beta) = \begin{bmatrix} e^{i\alpha}\cos(\delta/2) & \sin(\delta/2) \\ -\sin(\delta/2) & e^{-i\alpha}\cos(\delta/2) \end{bmatrix}$$

$$V = R_x(\alpha) R_y(\gamma) R_z(\beta) X = \begin{bmatrix} \sin(\delta/2) & e^{i\alpha}\cos(\delta/2) \\ e^{-i\alpha}\cos(\delta/2) & -\sin(\delta/2) \end{bmatrix}$$

$$\rightarrow \qquad VX = W$$

Questi operatori V tornano particolarmente utili per poter eseguire computazioni con più QuBit di controllo usando $V^{\dagger}$. In un esempio a tre QuBit:



con $VV^{\dagger} = I$ e $VV = V^2 = U$. Possiamo rapidamente verificare che solamente se i due QuBit di controllo sono nello stato $|1\rangle$ verrà applicato sull'ultimo stato U mentre in tutte le altre circostanze non cambierà poiché subirà una operazione totale uguale a I.

Questo procedimento può essere ampliato per la computazione a N QuBit di controllo, producendo una porta logica (2N+2)x(2N+2). Questo realizza un cambiamento totale U di ordine 2x2 sullo stato finale solamente se tutti i QuBit di controllo sono a $|1\rangle$:

$$U = \begin{bmatrix} u_{00} & u_{01} \\ u_{10} & u_{11} \end{bmatrix} \qquad W_n = \begin{bmatrix} 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & u_{00} & u_{01} \\ 0 & 0 & \cdots & u_{10} & u_{11} \end{bmatrix}$$

In uno stesso circuito N QuBit si possono usare più applicazioni successive di questo gate per poter accoppiare in tutti i modi possibili i diversi QuBit Questo permette di realizzare una qualsiasi porta logica $U(2^{N+1})$.

Capitolo 3 Implementazioni Fisiche

Sono stati realizzati diversi dispositivi in grado di rappresentare un QuBit sempre più accuratamente, accenneremo diverse tecniche che sono state utilizzate ma focalizzeremo l'attenzione principalmente su quelle che si basano su ioni intrappolati. Questo poiché possiedono uno dei migliori rapporti fra il tempo che adoperano per eseguire una singola operazione e quello che deve trascorrere prima che questa si perda a causa della già vista decoerenza. Verranno fornite informazioni sul funzionamento di tali dispositivi, compresi pregi e difetti

Ogni singolo ione come vedremo può essere sfruttato per potervici immagazzinare due QuBit di informazione, uno nello stato interno di spin e l'altro nello stato vibrazionale.

Vedremo rapidamente come deve essere formalizzata l'Hamiltoniana di un tale dispositivo, in particolar modo così da poter studiare dei metodi per implementare le varie porte logiche quantistiche.

Descrivendo un particolare esperimento importante in cui viene realizzata la porta logica *C-NOT* per la prima volta, facendo computare lo stato vibrazionale con quello di spin dello ione.

3.1 Trappole Ioniche

Esistono differenti sistemi che possono essere adoperati per intrappolare un atomo, che hanno caratteristiche diverse in base se bisogna catturare una particella carica o neutra. La scelta migliore riguarda le particelle elettricamente cariche basandoci sulla necessità di avere trappole con buche di potenziale più profonde. Utilizzando tecniche che si basano su particelle neutre rischieremo molto più facilmente di perdere queste ultime, divenendo necessarie più procedure per rendere lo stato stabile.

Un fattore importante da considerare per trappole cariche è il *teorema di Earnshaw.* Questo teorema afferma che oggetti quali cariche puntiformi non possono essere intrappolate da soli potenziali elettrostatici in tre dimensioni, ma sono necessari di conseguenza campi elettrici e magnetici statici o campi elettrici variabili nel tempo. Una semplice dimostrazione riguarda un atomo, se si trova in una posizione di equilibrio è subisce delle perturbazioni esso dovrà ritornare nella sua posizione. Questo è vero solo se le linee del campo di forza puntano tutte nella direzione della posizione di equilibrio facendo si che la divergenza in quel punto sia negativa. Questo non è possibile per la *legge di Gauss*, in uno spazio vuoto le linee di campo elettrico totale hanno sempre

divergenza nulla. Di conseguenza non possono esistere punti di minimo o massimo locale ma si potrebbero riuscire ad avere solamente punti di sella con soli campi elettrostatici.

Le principali trappole per ioni sono le *trappole di Penning* e *trappole di Paul*, per le prime il confinamento è realizzato con un potenziale elettrostatico e un campo magnetico costante mentre per il secondo viene adoperato un quadrupolo variabile nel tempo.

3.2 Apparato fisico

Impiegando gli atomi ionizzati, si adoperano gli stati interni distinguibili per energie diverse a differenti valori di spin e di grado di oscillazione. In particolare se lavoriamo con solo due livelli di un atomo definiamo quello base come $|0\rangle$ e il primo eccitato come $|1\rangle$. Questi due livelli scelti devono inoltre potersi mettere in connessione compatibili fra di loro tramite le regole di selezione.

Il nostro apparato principale è una trappola di Paul realizzata con quattro elettrodi cilindrici posizionati come vertici di un quadrato e usando ioni come in Fig. 4.

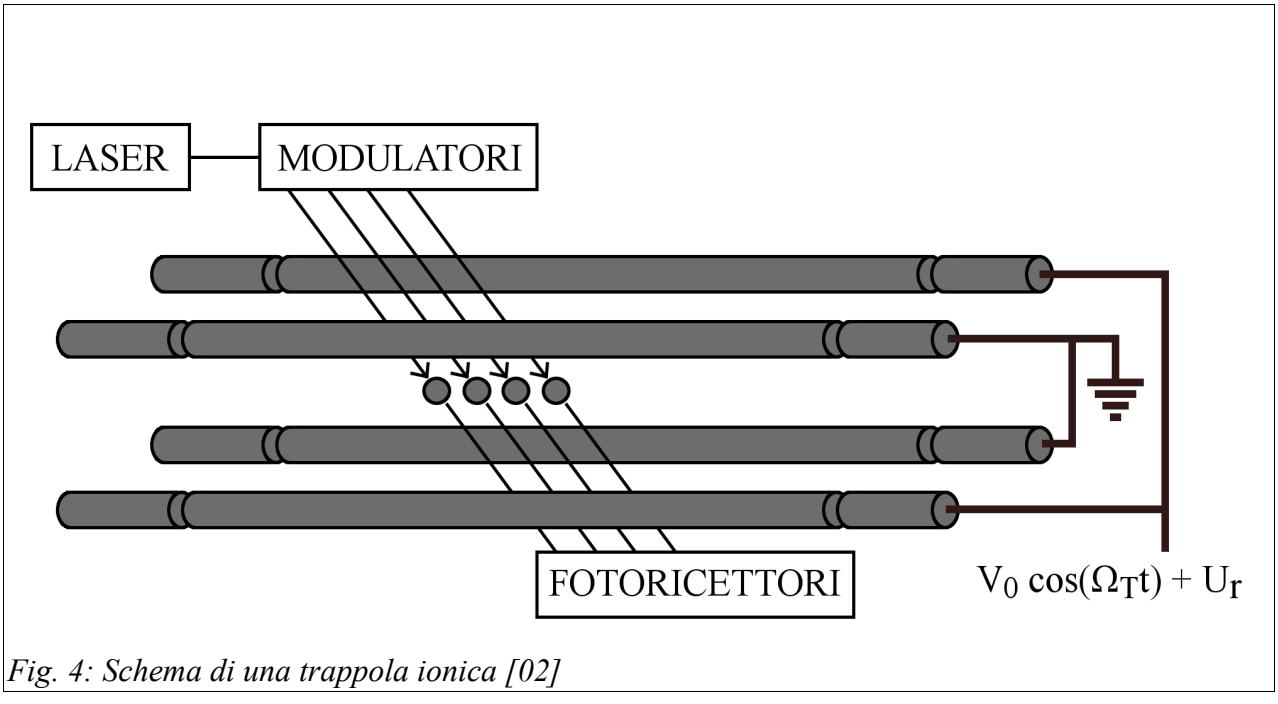


Fig. 4: Schema di una trappola ionica [02]

Alla estremità degli elettrodi è applicato un diverso voltaggio U_0 rispetto al loro centro, così da poter impilare lungo l'asse i diversi ioni per mezzo di un campo statico:

$$\Phi_{dc} = \kappa U_0[\, z^2 - (x^2+y^2)\,]/2$$

lungo l'asse $\hat{z}$ e con k fattore geometrico che dipende dalla posizione reciproca dei vari elettrodi. Ricordando il *teorema di Earnshaw* si realizza un campo elettrico variabile nel tempo, due degli elettrodi a vertici opposti vengono messi a terra mentre i due cilindri restanti vengono posti ad un voltaggio oscillante con i segmenti accoppiati rendendo costante il potenziale che li attraversa. Questo crea un potenziale a radiofrequenza RF:

$$\Phi_{rf} = [\, V_0 \cos(\Omega_T t) + U_r\,]\,[\, 1 + (x^2 - y^2)/R^2\,]/2$$

Unendo i potenziali Φ_{dc} e Φ_{rf} lungo un tempo maggiore dell'inverso di Ω_T, si crea un potenziale armonico lungo gli assi che, combinata con il potenziale di *repulsione coulombiana* degli ioni, ci genera per N ioni la seguente Hamiltoniana:

$$H = \sum_{i=1}^{N} \frac{M}{2}(\omega_x^2 x_i^2 + \omega_y^2 y_i^2 + \omega_z^2 z_i^2 + \frac{|\vec{p}\,|^2}{M^2}) + \sum_{i=1}^{N}\sum_{j>i} \frac{e^2}{4\pi\epsilon_0\,|\vec{r}_i - \vec{r}_j\,|}$$

dove M è la massa di ciascuno ione, non vi è riportato l'indice perché rimane sempre la stessa per ciascuno ione, e con ω_x, ω_y, ›› ω_z per avere le particelle allineate lungo l'asse $\hat{z}$. Aumentando il numero di ioni intrappolati la formula tende a diventare complessa, si rimarrà nel caso di pochi ioni intrappolati linearmente.

Il moto dei nostri atomi diviene quantizzato rendendo il nostro sistema sufficientemente isolato col mondo esterno. In questa situazione i livelli dell'energia sono paragonabili a quelli di un oscillatore armonico $n\hbar\omega_z$. Questi rappresentano l'intera energia vibrazionale della catena di ioni che possiedono a diversi modi di campo, che si muove come se fosse un solo corpo di massa totale NM e non come N singole particelle di massa M. Ogni singolo quanto di modo di energia $\hbar\omega_z$ è equivalente ad una particella definita *fonone*, come il *fotone* è una particella per un quanto di energia del campo elettromagnetico [05].

Il dispositivo viene messo in uno spazio vuoto a bassa pressione, su valori di circa 10^{-8} Pa. Gli ioni intrappolati vengono preparati tramite *raffreddamento Doppler*, si tratta di una tecnica nella quale le particelle sono sotto messe sotto l'effetto di due raggi laser contro propaganti di lunghezza d'onda propriamente prestabilita. Per *effetto Doppler*, gli ioni sentono una forza maggiore verso il fascio contro cui si muovono facendo si che sia presente una forza viscosa. Questa finisce per

rallentarli quando l'energia degli ioni sono paragonabili a:

$$k_b T \approx \hbar \Gamma / 2$$

con Γ il valore della frequenza della transazione usata per raffreddare gli ioni.

Un ultimo parametro importante viene dal criterio di *Lamb-Dicke* in cui le oscillazioni degli ioni devono essere molto piccole rispetto alla lunghezza d'onda della luce incidente. Definiamo il rapporto adimensionale con il valore di:

$$\eta \equiv \frac{2\pi z_0}{\lambda} \qquad z_0 = \sqrt{\hbar / 2\mathrm{NM}\omega}$$

con λ la lunghezza d'onda della luce e z_0 la distanza caratteristica fra due ioni nella trappola di potenziale. Il *criterio di Lamb-Dicke* richiede che $\eta \ll 1$, ma per rendere una trappola ionica efficace nell'eseguire computazioni quantistiche è sufficiente che sia $\eta \approx 1$. Questo permette che singoli ioni possano essere distinti dai raggi differenti e contemporaneamente semplificare il processo di eccitare otticamente il loro moto per eseguire operazioni logiche.

3.3 L'Hamiltoniana del sistema

Lo stato interno nel quale si ritrovano gli ioni, una volta raffreddati a temperature alle quali si possono sfruttare meccanismi quantistici, è ottenuta da una combinazione degli spin elettronici S e nucleari I:

$$F = S + I$$

con F momento angolare totale.

Far interagire gli ioni con un singolo fotone può causare l'aumentare o diminuire di una singola unità il momento angolare totale. Questo però non differenzia fra i valori del momento orbitale, di spin dell'elettrone o dei nucleoni portando a formalizzare di conseguenza una base dove il momento angolare totale sia in grado di definire univocamente le proprietà dello stato. Questo requisito viene soddisfatto prendendo $\left| j, m_j \right\rangle_J$ che sono simultaneamente autostati di J^2 e j_z con autovalori

rispettivamente $j(j + 1)^2$ e m_j.

Vi è inoltre da considerare che una sovrapposizione di diversi stati ha una vita limitata a causa *dell'emissione spontanea*. Questo fenomeno è causato dall'accoppiamento fra l'atomo e il campo elettromagnetico secondo l'interazione di Jaynes-Cummings con in approssimazione di onda rotante si scrive come:

$$H_I = g\left(a^{\dagger}\sigma_{-} + a\,\sigma_{+}\right)$$

con g costante di accoppiamento fra l'atomo e il campo elettromagnetico, le a sono operatori del singolo modo di campo e le σ sono gli operatori di Pauli definiti:

$$\sigma_{\pm} = \frac{X \pm iY}{2}$$

dove X e Y sono gli operatori σ_x e σ_y nello spazio del sistema a due livelli già visti.

E' possibile prendendo uno stato eccitato accoppiato senza fotoni $|0,1\rangle$, nella notazione $|Campo, Atomo\rangle$, ottenere la probabilità di decadimento, applicando l'operatore unitario $U = e^{-iHt}$ di evoluzione temporale per il caso di singolo-fotone e singolo-atomo, che risulta [02]:

$$H = -\begin{bmatrix} \delta & 0 & 0 \\ 0 & \delta & g \\ 0 & g & \delta \end{bmatrix} \qquad p_{decadimento} = \left|\langle 1, 0 \right| U \left| 0, 1 \rangle\right|^2$$

$$p_{decadimento} = g^2 \frac{4\sin^2 1/2(\omega-\omega_0)^2 t}{(\omega-\omega_0)^2}$$

Un atomo situato in uno spazio vuoto interagisce con diversi modi ottici:

$$g^2 = \frac{\omega_0^2}{2\hbar\,\omega\,\epsilon_0 c^2}\left|\langle 0 \right| \vec{\mu} \left| 1 \rangle\right|^2$$

dove $\vec{\mu}$ è l'operatore di dipolo atomico. Integrando rispetto a tutti i modi ottici e derivando rispetto al tempo si scopre la probabilità di decadimento al secondo:

$$\gamma_{radiazione} = \frac{\omega_0^3 \left|\langle 0 \right| \vec{\mu} \left| 1 \rangle\right|^2}{3\,\pi\,\hbar\,\epsilon_0 c^5}$$

nel quale approssimando $\langle 0 \mid \mu \mid 1 \rangle \approx \mu_B \approx 9x10^{-24} J/T$, il noto magnetone di Bhor, e assumendo $\omega_0/2\pi \approx 10\,Ghz$ abbiamo un valore approssimato di $\gamma_{radiazione} \approx 10^{-15} sec^{-1}$. Gli stati interni possono avere conseguentemente un lungo periodo di coerenza, con tempi di vita media sperimentalmente misurati che vanno da una decina di secondi a una decina di ore.

Hamiltoniana

Considerando queste premesse è possibile formalizzare l'Hamiltoniana, usando un sistema di spin a due livelli che interagisce con un campo elettromagnetico come interazione magnetica di dipolo:

$$H_I = -\vec{\mu} \cdot \vec{B}$$

dove il momento di dipolo è proporzionale al all'operatore di spin S tramite l'equazione $\vec{\mu} = \mu_B \cdot \vec{S}$ e il campo magnetico dato equivale a $\vec{B} = B_1 \hat{x} \cos(kz - \omega t + \varphi)$ con B_1 la massima intensità del campo. Useremo per convenienza gli operatori di spin $S_x = X/2$, $S_y = Y/2$ e $S_z = Z/2$.

In aggiunta ci sono anche interazioni con i modi vibrazionali che a loro volta, essendo quantizzati, necessitano di essere descritti da un operatore $z = z_0(a^\dagger + a)$. Gli operatori a innalzano e diminuiscono i modi vibrazionali delle particelle, equivalenti alla creazione e distruzione dei fononi.

Potendo raffreddare una particella vicino al minimo livello di modo vibrazionale, tale che l'oscillazione è piccola confrontata con la lunghezza d'onda della luce incidente, si rispetta il *criterio di Lamb-Dicke*. Definendo poi la frequenza di *Rabi* come $\Omega = \mu_m B_1/2$ e $S_x = (S_+ + S_-)/2$ si ricava la seguente Hamiltoniana di interazione semplificata nel limite di piccole η:

$$H_I = -\vec{\mu} \cdot \vec{B}$$

$$[\frac{\hbar\Omega}{2}(S_+ e^{i(\varphi-\omega t)} + S_- e^{-i(\varphi-\omega t)})]$$
$$+ [i\frac{\eta\hbar\Omega}{2}(S_+ a + S_- a^\dagger + S_+ a^\dagger + S_- a)(e^{i(\varphi-\omega t)} - e^{-i(\varphi-\omega t)})]$$

La prima parte dentro parentesi, dal momento che lo direzione dello spin rimane costante lungo

l'asse $\vec{z}$, viene ricavata *dall'Hamiltoniana di Jaynes-Cummings*. Si tratta di una forma particolare in cui non compaiono gli operatori dei fotoni, questo perché fintanto che B_1 è un forte stato coerente si possono ignorare le sue proprietà quantistiche è considerare un Hamiltoniana che descrive solo l'evoluzione del suo stato atomico interno. In questo caso uno stato coerente del campo non crea un fenomeno di entanglement con l'atomo con cui interagisce.

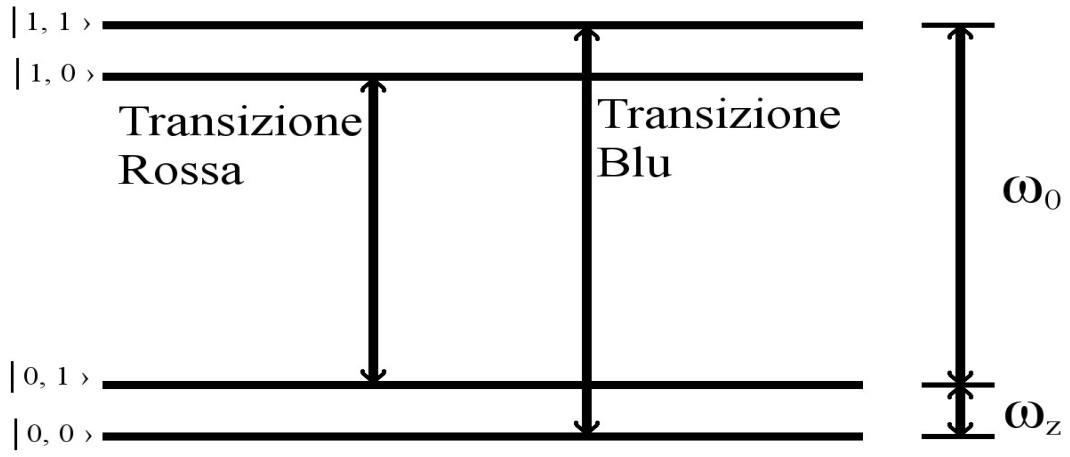


Fig. 5: Transizioni possibili dovute all'accopiamento fra spin e modi vibrazionali, dove gli stati sono definiti | spin, modo vibrazionale ›

La seconda parte compresa fra le parentesi comprende l'accoppiamento fra lo stato di spin dello ione e il suo modo vibrazionale, il campo magnetico osservato dipende dalla sua posizione. I quattro termini con gli operatori *S* e a rappresentano le quattro transizioni possibili conosciute come bande laterali rosse e blu, di cui due sono transizioni di aumento e due di diminuzione del livello (Fig. 5).

Per vedere come mai le bande laterali possono avere solo frequenze di transizione equivalenti a $\omega_0 \pm \omega_z$ usiamo l'Hamiltoniana di una particella libera:

$$H_0 = \hbar \omega_0 S_z + \hbar \omega_z a^\dagger a$$

La quale comporta di conseguenza che l'operatore dello spin e dei modi vibrazionali di evolvere nel tempo come:

$$S_+(t) = S_+ e^{i\omega_0 t} \qquad S_-(t) = S_- e^{-i\omega_0 t}$$
$$a^\dagger(t) = a^\dagger e^{i\omega_z t} \qquad a(t) = a e^{-i\omega_z t}$$

In referenza alla H_0 si ricavano i termini dominanti di $H_I^{'}=e^{iH_0 t/\hbar}H_I e^{-iH_0 t/\hbar}$ nella forma di:

$$H_I^{'}=\begin{cases} i\dfrac{\eta\hbar\Omega}{2}\left(S_+ a^{\dagger}e^{i\varphi}-S_- a\, e^{-i\varphi}\right) & \omega=\omega_0+\omega_z \\ i\dfrac{\eta\hbar\Omega}{2}\left(S_+ a\, e^{i\varphi}-S_- a^{\dagger}e^{-i\varphi}\right) & \omega=\omega_0-\omega_z \end{cases}$$

dove ω è la frequenza del campo magnetico. I termini si valutano a questo punto rispetto a dei tempi lunghi a confronto di $1/(\omega_0+\omega_z)$ per cui si hanno molte oscillazioni che mediano a zero il valore nella prima riga di $H_I^{'}$ rendendola trascurabile, allo stesso tempo $\omega_0-\omega_z$ può essere una differenza nulla o quasi ricavando dal suo inverso un tempo di interazione grande e la seconda riga in questo regime è il processo dominante rispetto a quella della prima.

Un ultimo fattore da tenere in considerazione è che il modello appena proposto riguarda solo una particella e che deve essere ampliato da uno a N particelle, per considerare tutti gli N ioni che si trovano nella trappola. Le modifiche sono semplici assumendo che tutte le particelle condividono un comune centro di modo vibrazionale, la cui energia è molto più bassa di ogni altro modo vibrazionale del sistema. In questa circostanza si cambia solo il valore della frequenza di Rabi da Ω a $\Omega/\sqrt{N}$, dove N è il numero totale delle particelle che si muovono insieme.

3.4 Esperimento C-NOT

Per la computazione quantistica occorre implementare dei metodi che eseguono delle trasformazioni unitarie sugli stati interni degli ioni, come viste nel capitolo precedente sulle porte logiche quantistiche, in maniera tale che possiamo utilizzare i nostri QuBit per operazioni di computazione.

Consideriamo le operazioni sullo stato interno di un singolo QuBit. Applicando un fascio laser coerente di frequenza ω_0 *l'Hamiltoniana* interna di interazione cambia come:

$$H_I^{internal}=\frac{\hbar\Omega}{2}\left(S_+ e^{i\varphi}+S_- e^{-i\varphi}\right)$$

Scegliendo accuratamente φ e la durata dell'interazione permette di operare operazioni di rotazione

$R_x(\theta) = \exp(-i\theta S_x)$ e $R_y(\theta) = \exp(-i\theta S_y)$, che ci permettono di realizzare ogni tipo di operazione di singolo QuBit usando lo spin di un atomo, tramite il teorema di decomposizione X-Y visto. Possiamo denotare le trasformazioni su un j-esimo ione nella nostra trappola come $R_{xj}(\theta)$.

Supponendo ora che con lo spin dell'atomo noi immagazziniamo l'informazione di un QuBit e con i modi vibrazionali un secondo QuBit, si può realizzare un invertitore di fase controllato [06] con trasformazione unitaria:

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$$

Questa tecnica può essere compresa meglio usando un atomo che possiede tre livelli energetici. Un laser di frequenza $\omega_{aus} + \omega_z$ causa la comparsa di transizioni fra gli stati $|2,0\rangle$ e $|1,1\rangle$, facendo prendere all'Hamiltoniana la forma:

$$H'_{aus} = i\frac{\eta\hbar\Omega'}{2}\left(S'_+ a' e^{i\varphi} - S'_- a'^{\dagger} e^{-i\varphi}\right)$$

dove i nuovi operatori S' e a' sono riferite alle transizioni fra gli stati $|2,0\rangle$ e $|1,1\rangle$, assumendo che gli ordini vibrazionali più alti siano inoccupati (Fig. 6). Nessun'altra transazione con questo metodo è eccitata.

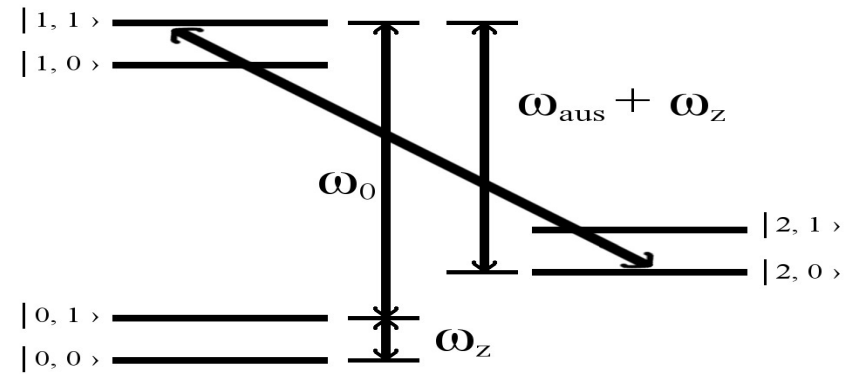


Fig. 6: Configurazione di un atomo che possiede tre livelli energetici nella nostra trappola. Ciacun livello possiede due modi vibrazionali

Applicando il fascio laser per ottenere un impulso di 2π si ha una rotazione $R_x(2\pi)$ sullo spazio

generato dai due stati $|2,0\rangle$ e $|1,1\rangle$ che è equivalante ha una trasformazione unitaria $|1,1\rangle \rightarrow -|1,1\rangle$. Tutti gli altri stati rimangono invariati, specificando che stati indesiderati come $|1,2\rangle$ abbiano probabilità d'ampiezza nulla. Si trova così una porta che chiamiamo $C_j(Z)$ che evidenzia una operazione a Z-Controllata o Controlled-Z.

Prima di passare all'esperimento del C-NOT ci serve predisporre ora solo una metodologia con cui si può scambiare il valore del QuBit memorizzato nello spin con quello dei modi vibrazionali e viceversa. Tramite un laser di frequenza $\omega_0 - \omega_z$ e con una fase tale da permettere una rotazione $R_y(\pi)$ nel spazio generato fra $|0,1\rangle$ e $|1,0\rangle$ si riesce in questa operazione, con una trasformazione unitaria:

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

sugli spazi $|0,0\rangle$, $|0,1\rangle$, $|1,0\rangle$ e $|1,1\rangle$.

Se il nostro stato iniziale fosse $a|0,0\rangle + b|1,0\rangle$ avremmo successivamente allo scambio $a|0,0\rangle + b|0,1\rangle$, rendendo la trasformazione efficace. Denominando $SWAP_j$ questa operazione possiamo denotare la sua inversa come $\overline{SWAP_j}$, realizzata con una rotazione di $R_y(-\pi)$. Questo procedimento però non è perfetto a causa dal segno meno presente nell'elemento $|1,0\rangle\langle 0,1|$, per questo a volte viene richiamata questa procedura come a un operazione di mappatura invece che di scambio.

Esperimento

Usando le tecniche precedentemente menzionate possiamo realizzare diverse porte logiche, ora vediamo in particolare riguardo alla realizzazione della porta logica C-NOT. Questa ci serve in modo particolare per la realizzazione di porte logiche universali poiché come abbaiamo visto ci basterebbe una porta C-NOT e una porta a operazioni su singolo QuBit.

Un metodo per realizzare il C-NOT è con la sequenza di operazioni:

$$C-NOT_{jk} = H_k \; \overline{SWAP}_k \; C_j(Z) \; SWAP_k \; H_k$$

dove definiamo j lo ione di controllo è k lo ione bersaglio. H_k è la già vista porta di Hadamard realizzata qui tramite rotazioni R_x e R_y.

L'esperimento che dimostrò la funzionalità della porta C-NOT si svolse nel 1995 [07] e sfruttò una trappola per ioni con un singolo atomo di $^{9}Be^{+}$. La particella viene trattenuta da una trappola a risonatore coassiale RF. Viene scelto il berillio per la disposizione della sua struttura fine come mostrata da Fig. 7.

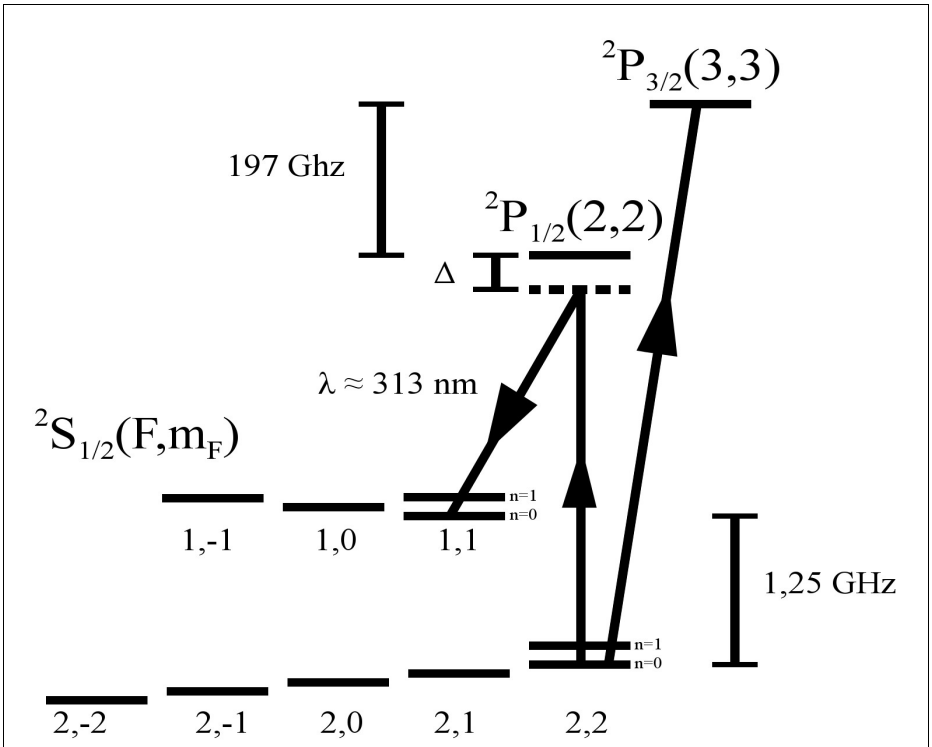


Fig. 7: Livelli energetici del berillio usati nell'esperimento. Gli n=0,1 sono i valori del modo vibrazionale

I livelli energetici interni $^2S_{1/2}(1,1)$ e $^2S_{1/2}(2,2)$ vengono adoperati come lo stato di un QuBit e i modi n=0,1 dei fononi come lo stato di un secondo QuBit. La transizione approssimata di 313 nm fra i due livelli $^2S_{1/2}(1,1)$ e $^2S_{1/2}(2,2)$ viene portata a termine con due laser la cui differenza equivale alla transizione, invece di adoperare un solo laser della lunghezza d'onda desiderata, per semplificare la richiesta di stabilità del fascio laser. Il livello $^2S_{1/2}(2,0)$ è adoperato come stato ausiliario, questo perché applicando un campo magnetico di intensità 0.18 mT i vari livelli energetici degli stati $^2S_{1/2}$ vengono divisi per *effetto Zeeman*.

Lo ione di berillio intrappolato possiede frequenze vibrazionali con valori di $(\omega_x\ ;\ \omega_y\ ;\ \omega_z)/2\pi = (11{,}2\ ;\ 18{,}2\ ;\ 29{,}8)\ Mhz$ e con uno stato fondamentale a $n_x = 0$ che fornisce una funzione d'onda di 7 nm circa. Questo permette di calcolare un parametro di Lamb-Dicke pari a $\eta_x = 0{,}2$. La frequenza di Rabi infine nella transizione in risonanza è $\Omega/2\pi = 140$kHz, nel moto laterale $\eta_x\Omega/2\pi = 30$ kHz e nella transizione ausiliare $\eta_x\Omega'/2\pi = 12$ kHz.

Lo ione viene inizializzato allo stato fondamentale con raffreddamento tramite effetto doppler e bande laterali, portandolo nello stato $|0,0\rangle = |{}^2S_{1/2}(2,2)\rangle |n_x = 0\rangle$ con una probabilità approssimata al 95%. Ora lo stato interno e vibrazionale vengono portati in una delle quattro basi $|0,0\rangle$, $|0,1\rangle$, $|1,0\rangle$ o $|1,1\rangle$ attraverso operazioni di porta logica su singolo QuBit. Subito dopo viene eseguita una operazione di porta C-NOT realizzata tramite tre impulsi che permettono di eseguire i seguenti passaggi:

1 – Lo stato interno del QuBit subisce una rotazione $R_y(\pi/2)$

2 – Si esegue una operazione a Z-Controllata fra i due QuBit

3 – Lo stato interno del QuBit subisce una seconda rotazione $R_y(-\pi/2)$

La lettura dell'output ottenuto viene eseguita tramite due misure, seppur il procedimento è sostanzialmente lo stesso. Per la prima si controlla la fluorescenza dello ione che avviene in presenza di luce polarizzata circolarmente + è applicata per la transizione $^2S_{1/2}(2,2) - {}^2P_{3/2}(3,3)$. Nel caso fossimo nello stato $^2S_{1/2}(1,1)$ non avviene una transizione apprezzabile, così l'intensità della fluorescenza è proporzionale alla probabilità che lo stato interno si trovi in $|0\rangle$. L'efficacia di questo metodo consiste nella ciclicità della transizione, la quale può essere ripetuta anche per più di un centinaio di volte fra $^2S_{1/2}(2,2)$ e $^2P_{3/2}(3,3)$. Come menzionato il primo metodo è identico al primo, quello che cambia è che prima viene eseguito un impulso per realizzare uno SWAP fra lo stato interno e quello vibrazionale.

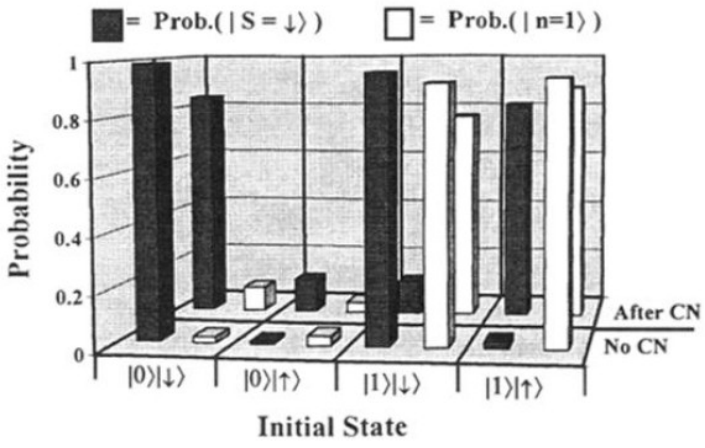


Fig. 8: Risultati dell'eperimento. L'immagine è fedelmente tratta dalla referenza [07]

L'esperimento dimostra che sia i valori classici della tabella della verità del C-NOT vengono

rispettati e sia attraverso stati in sovrapposizione in input e misurati in output con matrici di densità che le trasformazioni unitarie possono essere caratterizzate tramite un processo di *stato tomografico*. Si nota che la porta logica C-NOT, realizzata con questa tecnica, richiede circa 50 microsecondi per eseguire l'operazione è confrontata con il periodo che rimane in coerenza, che varia fra le centinaia e le migliaia di microsecondi, ci garantisce di conseguire la quasi totalità delle computazioni con successo. Fra le cause che portano alla decoerenza del sistema vengono presi in considerazioni l'instabilità del fascio laser, la frequenza e ampiezza di voltaggio di deriva della trappola ionica e le fluttuazioni del campo magnetico esterno.

E' altresì da tenere in considerazione che l'esperimento ha adoperato solo uno ione intrappolato e per una efficiente computazione si dovrebbe poter eseguire l'operazione C-NOT fra differenti ioni.

Attualmente altre tecniche vengono sviluppate per superare questa limitazione e lo stato vibrazionale, a causa della corta durata della sua vita a causa della decoerenza, può venir usato come per immagazzinare valori solo temporaneamente e lasciare stati importanti immagazzinati in struttura più resistente alla decoerenza come lo è lo stato interno.

Aumentare il numero di QuBit è relativamente semplice tramite la trappola di Paul discussa a inizio capitolo, in cui si possono impilare molti ioni linearmente al suo interno.

Vi è da menzionare un esperimento più recente del 2003 [08], usando sempre un trappola di Paul lineare per intrappolare gli atomo, si è riuscito ad implementare una porta C-NOT fra due ioni di $^{40}Ca^{+}$ adoperando come tramite fra i due i fononi.

3.5 Altri esempi

Attualmente esistono comunque altri sistemi per realizzare i QuBit che riproponiamo per completezza descrivendo brevemente le loro qualità principali.

Singolo Fotone, viene adoperato un fotone che si propaga in due cavità ottiche

Lo stato del QuBit è rappresentato da un singolo fotone fra due stati $|01\rangle$ e $|10\rangle$ tramite polarizzazione.

Le trasformazioni lineari vengono eseguite con *spostamenti di fase*, *separatori di fascio* e materiali che producono l'effetto *Kerr non-lineari*. Questo è un fenomeno in cui un mezzo ha un

indice di rifrazione proporzionale all'intensità della luce che lo attraversa, usato con la propagazione di due fasci di uguale densità fa sì che entrambi i raggi subiscano un cambiamento di fase maggiore rispetto al fascio singolo.

Lo stato iniziale si ottiene creando un fotone e il valori vengono acquisiti tramite fotorecettori.

Cavità-QED, viene adoperato un atomo con un elevato numero di elettroni posto all'interno di una cavità ottica. Può interagire diverse volte con i fotoni presenti nella cavità prima che questi ne escano.

La rappresentazione del QuBit è la stessa del metodo per *Singolo Fotone,* quasi come per le trasformazioni unitarie con gli *spostamenti di fase* e i *separatori di fascio*. Queste ultime si differenziano per la sola sostituzione dei *Kerr di media non-lineari* con la *cavità QED,* realizzata tramite una *cavità di Fabry-Perot* contenente alcuni atomi.

Nuovamente lo stato iniziale è preparato producendo un singolo fotone e misurato tramite fotorecettori.

Risonanza magnetica nucleare, dove al posto di avere ioni intrappolati vengono utilizzate delle molecole.

Qui lo stato del QuBit è rappresentato dallo spin dei nuclei atomici.

Le trasformazioni unitarie avvengono tramite l'uso di impulsi di campi magnetici applicati agli spin in presenza di un forte campo magnetico, dove l'accoppiamento fra gli spin e assicurato dai legami chimici fra gli atomi.

Lo stato iniziale viene creato polarizzando gli spin in un forte campo magnetico e i valori in lettura ottenuti grazie alle tensioni di correnti indotte create dai momenti magnetici.

Si accenna inoltre al progetto della D-Wave [09] in cui realizzano un simulatore quantistico, non un calcolatore, che sfrutta processi adiabatici [10] grazie a gas refrigeranti che portano a temperature prossime i 0,015 K. Il sistema così costituto da array di giunzioni di Josephson è in grado di adoperare gli effetti superconduttivi che, con tecniche di microelettronica, si possono interagire su grande scala.

Da notare che il consumo di energia di questo sistema dipende quasi esclusivamente da processi di raffreddamento, permettendo così che all'aumentare della potenza di calcolo il consumo di energia richiesto non aumenta significativamente, rispetto a quanto avviene invece con i supercomputer attuali.

Conclusioni e prospettive

La computazione quantistica, come abbiamo notato, si differenzia dalla computazione classica perché l'ente che adoperiamo per memorizzare l'informazione non è più limitato a due stati ma ad un'ampiezza di probabilità fra questi, da non confondere con la probabilità statistica, quindi in linea di principio per ogni QuBit abbiamo l'informazione codificabile in coefficienti complessi e la possibilità di operare linearmente su una combinazione lineare in modo “parallelo”.

Realizzando porte logiche quantistiche con questi stati possiamo riottenere gli stessi risultati dei computatori classici ma, in alcuni casi particolari di problemi, possiamo sfruttare la natura quantistica per ottenere risultati in tempi drasticamente più ridotti e affrontare così problemi, di tipo NP, che sarebbero inattaccabili con calcolatori classici. Con il vantaggio che, essendo queste porte universali, si può concettualmente realizzare qualsiasi combinazione di porte nei circuiti, disegnando quindi appositi algoritmi che godono appieno delle caratteristiche quantistiche.

Il problema principale alla computazione quantistica rimarrà la decoerenza, i cui effetti non possono che aumentare sul nostro sistema all'incrementare del numero di QuBit che usiamo. In questo campo non si può che cercare di isolare al meglio i nostri stati dall'ambiente e cercare elementi che hanno una lunga coerenza. Tuttavia non abbiamo qua menzionato strategie esistenti per tentare di lavorare in “sottospazi” schermati dalla decoerenza [11].

L'uso della trappola di Paul per catturare un numero elevato di ioni linearmente è una ottima dimostrazione di come questi dispositivi siano effettivamente realizzabili e al contempo scalabili, considerando anche che lo spin degli ioni dura molto a lungo prima di subire gli effetti di decoerenza e i fononi hanno una vita media lunga da poter essere usati come tramite per far computare gli stati di due ioni fra di loro.

Questo può non essere che uno dei primi passi verso la realizzazione di un calcolatore quantistico. Una macchina di grande interesse non solo per la velocità ed efficienza di calcolo raggiungibile in certe situazioni, ma anche per la simulazione di diversi sistemi fisici quantistici difficili da indagare, tramite altri sistemi più trattabili decritti dalle medesime equazioni.

I valori rappresentabili da Bit classici sono per forza approssimati per loro natura avendo solo un finito numero di stati possibili. Per un QuBit è diverso potendosi questo trovare in una ampiezza di valori che può considerarsi infinita a meno di restrizioni fisiche. Sebbene lo stato finale può essere solo di due valori comunque, a causa della perdita di informazione per la misura che fa collassare la funzione d'onda, si possono cercare algoritmi che computano interamente su sovrapposizioni lineari per cui fornirci solo nell'ultimo passaggio di uscita due possibili valori per

ogni QuBit, interpretabili come risposte ultime ai problemi decisionali trattati.

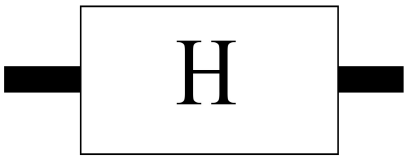
Attualmente i supercomputer più potenti non arrivano a competere per potenza di calcolo col cervello umano. Lo studio della computazione quantistica potrebbe essere validamente impiegato in futuro, ponendo le basi per la realizzazione di simulatori di alcuni processi del cervello umano, dal momento che questo stesso nostro calcolatore naturale basa la sua stessa esistenza sulle leggi della fisica quantistica.

Appendice

A – Schemi grafici delle porte logiche quantistiche

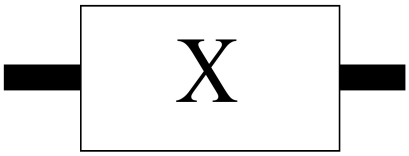
Qua riportiamo la rappresentazione delle porte logiche quantistiche e loro rappresentazione convenzionale nei circuiti. Si rammentano anche le espressioni matriciali 2x2 e 4x4 nella base computazionale $|0\rangle$ e $|1\rangle$.

Porta di Hadamard



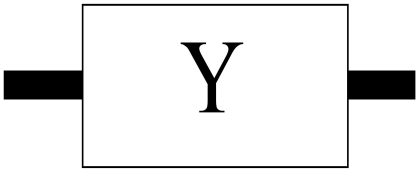
$$H \equiv \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix}$$

Porta di Pauli-X (NOT)



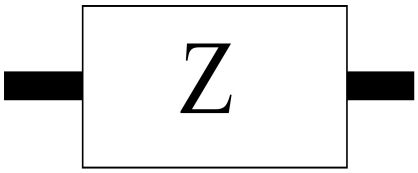
$$X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

Porta di Pauli-Y



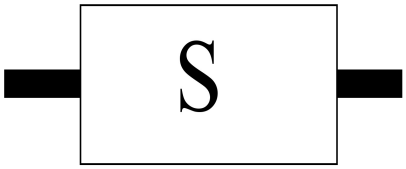
$$Y \equiv \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

Porta di Pauli-Z



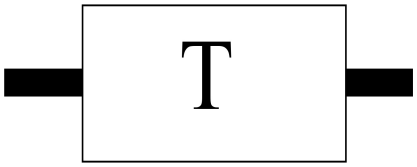
$$Z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

Porta di Fase (S)



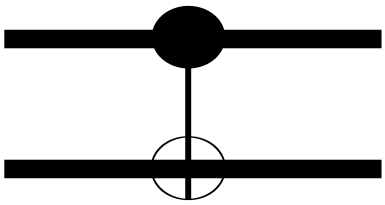
$$S \equiv \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$$

Porta di π/8 (T)



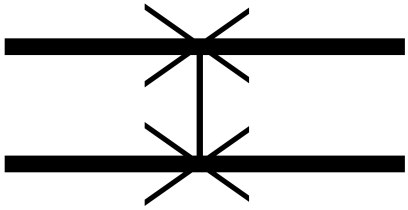
$$H \equiv \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$$

Porta di Not Controllato (C-NOT)



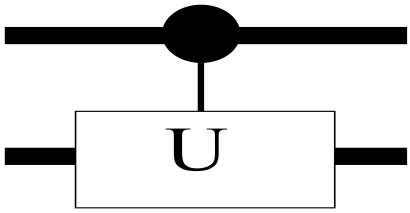
$$C-NOT \equiv \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

Porta di Scambio (SWAP)



$$SWAP \equiv \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Porta Controllata Unitaria (S)



$$C-U \equiv \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & u_{00} & u_{01} \\ 0 & 0 & u_{10} & u_{11} \end{bmatrix}$$

Bibliografia

[01] Proceedings of the London Mathematical Society; Ser. 2, Vol. 42; A. M. Turing; On Computable Numbers, with an application to the Entscheidungsproblem; 12 novembre 1936.

[02] Mihael A. Nielsen, and Isaac L. Chuang; Quantum Computation and Quantum Information; Cambridge University Press.

[03] International Journal of Theoretical Physics; Vol. 21; Richard P. Feynman; Simulating Physics with Computers; 7 maggio 1981

[04] Phisical Rewiev Letters; Vol. 52, Numero 5; Adriano Barenco, Charles H. Bennett, Richard Cleve, David P. DiVincenzo, Norman Margolus, Peter Shor, Tycho Sleator, John A. Smolin, and Harald Weinfurter; Elementary gates for quantum computation; 22 marzo 1995.

[05] Robert Eisberg, Robert Resnick; Quantum Physics of atoms, molecules, solids, nuclei and particles; John Wiley & Sons, Inc.

[06] Journal Of Optics B: Quantum And Semiclassical Optics; S371–S383; P. J. Lee, K. A. Brickman, L. Deslauriers, P. C. Haljan, L. M. Duan, and C. Monroe; Phase control of trapped ion quantum gates; Institute Of Physics Publishing; 21 September 2005.

[07] Physical Rewiev Letters; Vol. 75, Numero 25; C. Monroe, D. M. Meekhof, B. E. King, W. M. Itano, and D. J. Wineland; Demonstration of a Fundamental Quantum Logic Gate; 18 dicembre 1995.

[08] Nature; Vol. 422; Ferdinand Schmidt-Kaler, Hartmut Häffner, Mark Riebe, Stephan Gulde, Gavin P. T. Lancaster, Thomas Deuschle, Christoph Becher, Christian F. Roos, Jürgen Eschner, and Rainer Blatt; Realization of the Cirac–Zoller controlled-NOT quantum gate; Nature Publishing Group; 27 marzo 2003.

[09] D-Wave Systems Inc.; The D-Wave 2000Q™ System | D-Wave Systems; https://www.dwavesys.com/d-wave-two-system;

[10] arXiv:1611.04471v1; [qquant-ph]; Tameem Albash, and Daniel A. Lidar; Adiabatic Quantum Computing; 14 novembre 2016.

[11] Physical Rewiev Letters; Vol. 82; D. A. Lidar, I. L. Chuang, and K. B. Whaley; Decoherence-Free Subspace for Quantum Computation; 21 settembre 1998.