

ALMA MATER STUDIORUM · UNIVERSITÀ DI BOLOGNA

---

Scuola di Scienze  
Corso di Laurea in Fisica

# Applicazioni e implementazioni della computazione quantistica

Relatore:  
Prof. Fabio Ortolani

Presentata da:  
Alex Baroncini

Sessione II  
Anno Accademico 2014/2015

# Indice

<b>1</b>	<b>Introduzione</b>	<b>5</b>
1.1	I computer classici . . . . .	5
1.2	Verso i computer quantistici . . . . .	6
<b>2</b>	<b>Computazione quantistica</b>	<b>8</b>
2.1	Bit quantistici . . . . .	8
2.1.1	Qubit singoli . . . . .	8
2.1.2	Qubit multipli . . . . .	9
2.2	Porte quantistiche . . . . .	10
2.2.1	Porte a qubit singoli . . . . .	10
2.2.2	Porte a qubit multipli . . . . .	12
2.3	Circuiti quantistici . . . . .	14
2.3.1	Proprietà e misura . . . . .	14
2.3.2	Circuito di scambio . . . . .	14
2.3.3	Creare stati di Bell . . . . .	15
2.3.4	Teletrasporto quantistico . . . . .	16
<b>3</b>	<b>Applicazioni</b>	<b>18</b>
3.1	Algoritmi quantistici . . . . .	18
3.1.1	Computazione classica su un computer quantistico . . . . .	18
3.1.2	Parallelismo quantistico . . . . .	20
3.1.3	Algoritmo di Deutsch . . . . .	21
3.1.4	Algoritmo di Deutsch-Jozsa . . . . .	23
3.2	Classi di algoritmi e problemi . . . . .	24
3.2.1	Algoritmi basati sulla trasformata di Fourier . . . . .	24
3.2.2	Algoritmi di ricerca . . . . .	25
3.2.3	Simulazione quantistica . . . . .	25
3.2.4	Crittografia quantistica . . . . .	26
3.3	Visione d'insieme . . . . .	27

<b>4</b>	<b>Implementazioni</b>	<b>28</b>
4.1	Condizioni per la realizzazione . . . . .	28
4.2	Oscillatori armonici . . . . .	29
4.2.1	Apparato fisico . . . . .	29
4.2.2	Hamiltoniana . . . . .	30
4.2.3	Computazione quantistica . . . . .	31
4.2.4	Problematiche . . . . .	31
4.3	Fotoni ottici . . . . .	32
4.3.1	Apparato fisico . . . . .	32
4.3.2	Computazione quantistica . . . . .	33
4.3.3	Problematiche . . . . .	36
4.4	Trappole ioniche . . . . .	36
4.4.1	Apparato fisico . . . . .	37
4.4.2	Hamiltoniana . . . . .	39
4.4.3	Computazione quantistica . . . . .	39
4.4.4	Problematiche . . . . .	42
4.5	Altri modelli e risultati recenti . . . . .	42
4.6	Conclusioni . . . . .	43

# Sommario

Questa tesi introduce le basi della teoria della computazione quantistica, partendo da un approccio teorico-matematico al concetto di qubit per arrivare alla schematizzazione di alcuni circuiti per algoritmi quantistici, analizzando la differenza tra le porte logiche classiche e la loro versione quantistica.

Segue poi una lista descrittiva di possibili applicazioni dei computer quantistici, divise per categorie, e i loro vantaggi rispetto ai computer classici. Tra le applicazioni rientrano la crittografia quantistica, gli algoritmi di fattorizzazione e del logaritmo discreto di Shor, il teletrasporto di informazione quantistica e molte altre.

La parte più corposa della tesi riguarda le possibili implementazioni, ovvero come realizzare praticamente un computer quantistico rendendo entità fisiche i qubit. Di queste implementazioni vengono analizzati i vari aspetti necessari alla computazione quantistica, ovvero la creazione di stati iniziali, la misura di stati finali e le trasformazioni unitarie che rappresentano le porte logiche quantistiche. Infine vengono elencate le varie problematiche del modello preso in considerazione.

Infine vengono citati alcuni esperimenti e modelli recenti che potrebbero vedere una realizzazione su scala industriale nei prossimi anni.

# Capitolo 1

## Introduzione

### 1.1 I computer classici

L'idea moderna di computer è dovuta al grande matematico Alan Turing. Nel 1936 ha pubblicato un articolo nel quale ha sviluppato in dettaglio una nozione astratta di quello che noi oggi chiamiamo computer programmabile, un modello per la computazione in grado di eseguire algoritmi chiamato *macchina di Turing* [1], in suo onore.

Turing ha anche dimostrato che esiste una *macchina di Turing universale* che può essere usata per simulare le evoluzioni di qualsiasi macchina di Turing. Come conseguenza, se c'è un algoritmo che può essere eseguito su un qualsiasi hardware (per esempio un computer moderno), allora c'è un algoritmo equivalente per una macchina di Turing universale che esegue lo stesso esatto compito dell'algoritmo sul computer.

Per capire meglio i vantaggi della computazione quantistica, è necessario introdurre il concetto di *'efficienza'* di un algoritmo. Questo concetto, espresso in termini matematici precisi nella *teoria della complessità computazionale*[2], può essere riassunto brevemente come segue: un algoritmo è efficiente se il tempo di esecuzione è una funzione polinomiale rispetto alla grandezza del problema risolto (o lunghezza dell'input); un algoritmo è inefficiente se il tempo di esecuzione è superiore al polinomiale (tipicamente esponenziale).

Alla fine degli anni '60 e all'inizio degli anni '70 sembrava che la macchina di Turing fosse un modello computazionale potente almeno quanto un qualsiasi altro modello computazionale, vale a dire che un problema che aveva una soluzione efficiente in un qualche modello generico poteva essere risolto efficientemente anche su una macchina di Turing che simulava quel modello. Questa osservazione diventò famosa come *tesi di Church-Turing*:

*”Un qualsiasi processo algoritmico può essere simulato efficientemente usando una macchina di Turing.”*

La potenza degli hardware aumentò ad un ritmo incredibile da allora. Nel 1965 Gordon Moore codificò questa crescita nella celebre *legge di Moore*:

*”La complessità di un microcircuito, misurata ad esempio tramite il numero di transistor per chip, raddoppia ogni 18 mesi.”* [3]

Questa legge tuttavia non sarà valida per sempre. La fabbricazione di componenti tecnologici sempre più piccoli infatti ha già cominciato a riscontrare problemi dovuti alla dimensione: gli effetti quantistici interferiscono sempre di più man mano che i componenti si rimpiccioliscono. Eventualmente ci sarà un punto oltre il quale non sarà possibile trascurare questi effetti (per esempio l'effetto tunnel quantistico diventerebbe troppo rilevante).

## 1.2 Verso i computer quantistici

Alla fine degli anni '70, con il fiorire degli algoritmi probabilistici (ovvero non deterministici, con elementi intrinsecamente casuali), si cominciarono ad avere dubbi sulla validità della tesi di Church-Turing. Sembrava che alcuni problemi potessero essere risolti efficientemente solo con una macchina di Turing probabilistica. Cominciò la ricerca di un modello computazionale in grado di simulare efficientemente qualsiasi altro modello computazionale con certezza.

Nel 1985 David Deutsch ipotizzò che, essendo in definitiva le leggi della fisica quelle della meccanica quantistica, si potesse usare un dispositivo basato sui principi della meccanica quantistica per simulare efficientemente un sistema fisico arbitrario. Questa idea portò alla concezione odierna di computer quantistici. Rimane tuttavia un problema aperto dei giorni nostri determinare se un computer quantistico universale sia effettivamente in grado di simulare un sistema fisico arbitrario. Deutsch diede anche un semplice esempio di come un computer quantistico fosse in grado di risolvere efficientemente problemi che non hanno soluzioni efficienti conosciute su computer classici, intesi come macchine di Turing probabilistiche.

I primi passi effettuati da Deutsch culminarono nel 1994 con la dimostrazione di Peter Shor che la ricerca dei fattori primi di un intero e il calcolo dei logaritmi interi, due problemi fondamentali che si ritiene ancora oggi non abbiano soluzione efficiente su un computer classico, possono essere risolti efficientemente su un computer quantistico [4]. Un'altra evidenza della potenza dei computer quantistici si ebbe nel 1995 quando Lov Grover dimostrò che anche la ricerca in uno spazio non strutturato poteva essere velocizzata su un computer quantistico [5]. Sebbene il guadagno di velocità non fosse

comparabile con gli algoritmi di Shor, la vasta applicabilità delle metodologie di ricerca portò molto interesse verso l'algoritmo di Grover.

Questi vantaggi essenziali dei computer quantistici sui computer classici sono così rilevanti che molti ricercatori presumono che nessun progresso nel campo della computazione classica, per quanto grande esso sia, riuscirà a colmare la differenza di potenza tra un computer classico e un computer quantistico. Tuttavia, non è così semplice sfruttare questa incredibile potenza. Per risolvere problemi efficientemente su computer quantistici, o almeno più velocemente che sui computer classici, occorre infatti ideare degli algoritmi quantistici efficienti. Ciò è reso difficile dal fatto che l'intuizione umana è basata sul mondo classico, e non sugli effetti quantistici. Inoltre non basta realizzare un algoritmo quantistico: esso deve essere anche migliore di qualsiasi algoritmo classico equivalente già esistente. La sfida maggiore per la computazione quantistica è quindi trovare soluzioni a problemi di reale importanza risolvibili in maniera notevolmente vantaggiosa dai computer quantistici rispetto ai computer classici.

# Capitolo 2

## Computazione quantistica

### 2.1 Bit quantistici

#### 2.1.1 Qubit singoli

Così come il bit è un concetto fondamentale per la computazione classica, il bit quantistico (o *qubit* in breve) è il concetto alla base della computazione quantistica. Prima di vedere come realizzare fisicamente dei sistemi che rappresentino queste entità, conviene trattare i qubit come degli oggetti matematici astratti. In questo modo è possibile sviluppare una teoria che non è vincolata al modo in cui vengono realizzati.

Un bit classico può essere solo in due stati: 0 o 1. Un qubit invece si trova in una combinazione lineare (o sovrapposizione) di due stati fondamentali (o stati della base computazionale), chiamati  $|0\rangle$  e  $|1\rangle$ . Questi stati formano una base ortonormale per questo spazio vettoriale. Un qubit sarà quindi in uno stato generico

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \quad (2.1)$$

dove  $\alpha$  e  $\beta$  sono dei numeri complessi che descrivono la probabilità di ottenere gli stati  $|0\rangle$  e  $|1\rangle$ . Per essere più precisi, quando misuriamo lo stato di un qubit, otteniamo 0 con probabilità  $|\alpha|^2$  oppure 1 con probabilità  $|\beta|^2$ . In generale possiamo quindi pensare allo stato di un qubit come un vettore unitario in uno spazio vettoriale complesso bidimensionale. Un esempio di stato importante è lo stato  $|+\rangle$ , definito come

$$|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle. \quad (2.2)$$

Questo stato, quando misurato, restituisce il valore 0 o il valore 1 con la stessa probabilità: 50%.



Visto che vale sempre  $|\alpha|^2 + |\beta|^2 = 1$ , possiamo riscrivere lo stato di un qubit nel seguente modo (a meno di un fattore di fase):

$$|\psi\rangle = \cos \frac{\theta}{2} |0\rangle + e^{i\varphi} \sin \frac{\theta}{2} |1\rangle . \quad (2.3)$$

I numeri  $\theta$  e  $\varphi$  individuano un punto sulla sfera tridimensionale di raggio unitario, spesso chiamata *sfera di Bloch* (vedi Figura 2.1), che risulta un utile mezzo per rappresentare lo stato di un qubit singolo.

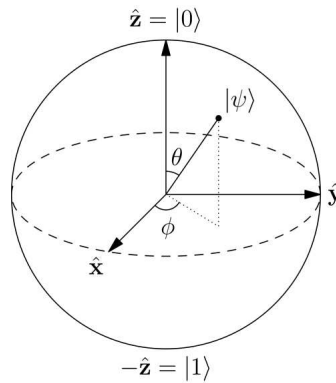


Figura 2.1: Stato  $|\psi\rangle$  generico di un qubit sulla sfera di Bloch.

Molte operazioni sul singolo qubit possono essere viste come trasformazioni sulla sfera di Bloch. Sebbene lo stato di un qubit possa essere un qualsiasi punto della superficie della sfera, è bene ricordare che una misura dello stato darà sempre e solo 0 o 1, facendo collassare la sovrapposizione degli stati nel risultato ottenuto. Ovvero se la misura dà risultato 0, il qubit si troverà nello stato  $|0\rangle$ . Se invece la misura dà risultato 1, il qubit si troverà nello stato  $|1\rangle$ .

Da una singola misura è possibile quindi ottenere solamente un bit di informazione. Tuttavia, c'è un'informazione nascosta nelle variabili  $\alpha$  e  $\beta$  che viene conservata fintanto che non avvengono misure. Questa informazione cresce esponenzialmente con il numero di qubit che consideriamo, ed è alla base della potenza della meccanica quantistica come mezzo computazionale.

### 2.1.2 Qubit multipli

Un sistema di due qubit ha quattro stati fondamentali, scrivibili come  $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ . In generale lo stato di una coppia di qubit sarà una sovrapposizione di questi quattro stati:

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle , \quad (2.4)$$

in cui i moduli delle ampiezze al quadrato indicano la probabilità di ottenere il corrispondente stato, e quindi la loro somma è normalizzata a 1:  $|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1$ . In un sistema di due qubit possiamo anche misurare lo stato di un singolo qubit. Per esempio se misuriamo solo il primo qubit otteniamo 0 con probabilità  $|\alpha_{00}|^2 + |\alpha_{01}|^2$ , e otteniamo 1 con la probabilità  $|\alpha_{10}|^2 + |\alpha_{11}|^2$ . Nel caso in cui ottenessimo uno 0, lo stato del sistema diventerebbe

$$|\psi'\rangle = \frac{\alpha_{00}|00\rangle + \alpha_{01}|01\rangle}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}}, \quad (2.5)$$

dove il fattore al denominatore è dovuto alla ri-normalizzazione, in modo che i coefficienti siano ancora normalizzati a 1.

Uno stato particolare molto importante nei sistemi a due qubit è lo *stato di Bell*, o *coppia EPR*:

$$|\varphi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}. \quad (2.6)$$

La proprietà interessante di questo stato è che i due qubit sono *correlati*. Misurando il primo qubit si ottiene 0 con probabilità 1/2, e lo stato del sistema dopo la misura diventa  $|\varphi'\rangle = |00\rangle$ , oppure si ottiene 1 con probabilità 1/2, e lo stato del sistema diventa  $|\varphi'\rangle = |11\rangle$ . Come ovvia conseguenza, la misura del secondo qubit restituirà sempre un risultato uguale a quella del primo qubit, in entrambi i casi. Bell dimostrò che questa correlazione viene mantenuta se si effettuano alcune operazioni sulla coppia EPR, prima della misurazione dei qubit.

Se in generale consideriamo un sistema di  $n$  qubit, avremo  $2^n$  ampiezze per gli stati fondamentali. Per  $n = 500$  questo numero è più grande del numero stimato di atomi nell'universo, quindi nessun computer classico potrebbe contenere così tante informazioni. La cosa impressionante è che, sebbene sia un sistema relativamente piccolo di qubit (basti pensare a quanti pochi sono 500 bit), il numero di variabili in gioco è enorme, e la Natura effettua i suoi calcoli su tutte queste variabili mentre il sistema evolve. Uno degli obiettivi della computazione quantistica è sfruttare questa incredibile potenza di calcolo a nostro vantaggio.

## 2.2 Porte quantistiche

### 2.2.1 Porte a qubit singoli

Nei computer classici abbiamo delle porte logiche, che manipolano le informazioni nei circuiti. Per un bit singolo, abbiamo solo due porte possibili: l'identità, che mantiene lo stato del bit, e la porta NOT, che inverte lo stato del bit (se prima era 0 diventa 1 e viceversa). Come si potrebbe realizzare una porta NOT che agisca sui qubit?

Per esempio, potrebbe scambiare lo stato  $|0\rangle$  con lo stato  $|1\rangle$ . Però cosa succederebbe alla sovrapposizione degli stati? A causa delle proprietà della meccanica quantistica, tutte le porte quantistiche devono essere lineari [6]. Ciò significa che se avevamo lo stato iniziale  $\alpha|0\rangle + \beta|1\rangle$ , lo stato ottenuto dalla porta NOT sarà  $\alpha|1\rangle + \beta|0\rangle$ .

Un modo comodo di rappresentare le porte quantistiche è dato dalle matrici. Se per esempio definiamo la porta NOT come la matrice

$$X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad (2.7)$$

e scriviamo lo stato quantistico  $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$  come il vettore colonna

$$|\psi\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}, \quad (2.8)$$

allora l'azione della porta NOT può essere scritta come

$$|\psi'\rangle = X \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \beta \\ \alpha \end{bmatrix}. \quad (2.9)$$

Se pensiamo alle porte quantistiche su un singolo qubit come a matrici 2x2, viene spontaneo chiedersi se qualsiasi matrice 2x2 possa essere una porta quantistica. La risposta è che solo le matrici unitarie, a causa della condizione di normalizzazione, possono essere porte quantistiche. Tuttavia non ci sono altre restrizioni. Questo significa che, al contrario del caso classico in cui c'è una sola porta a bit singolo non banale (ovvero la porta NOT), nel caso quantistico ci sono molte porte a qubit singolo non banali. Due di notevole importanza sono la porta  $Z$

$$Z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \quad (2.10)$$

e la porta *Hadamard*

$$H \equiv \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}. \quad (2.11)$$

La porta  $Z$  lascia invariato lo stato  $|0\rangle$  e inverte il segno dello stato  $|1\rangle$ . Per visualizzare l'azione della porta  $H$ , invece, conviene utilizzare la sfera di Bloch. Come si vede in Figura 2.2, la porta Hadamard è rappresentata da una rotazione attorno all'asse  $\hat{y}$  di  $90^\circ$  seguita da una rotazione attorno all'asse  $\hat{x}$  di  $180^\circ$ .

L'azione delle porte  $X$ ,  $Z$  e  $H$  è riassunta nella Figura 2.3, dove è mostrata anche la porta NOT classica. Sebbene ci siano infinite matrici 2x2 unitarie, è possibile costruire

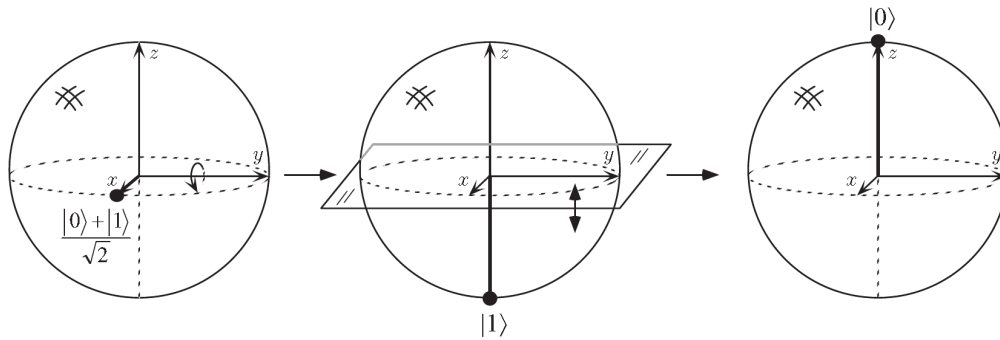


Figura 2.2: Azione della porta Hadamard sullo stato  $(|0\rangle + |1\rangle)/\sqrt{2}$ .

una qualsiasi porta a qubit singolo con un numero finito di porte quantistiche. Qualsiasi matrice unitaria  $2 \times 2$  si può infatti decomporre come

$$U = e^{i\alpha} \begin{bmatrix} e^{-i\beta/2} & 0 \\ 0 & e^{i\beta/2} \end{bmatrix} \begin{bmatrix} \cos \frac{\gamma}{2} & -\sin \frac{\gamma}{2} \\ \sin \frac{\gamma}{2} & \cos \frac{\gamma}{2} \end{bmatrix}. \quad (2.12)$$

Il primo termine è un fattore di fase, la prima matrice rappresenta una rotazione attorno all'asse  $\hat{z}$  e la seconda matrice è una rotazione attorno all'asse  $\hat{y}$ . Questo significa che, se si riescono a implementare le rotazioni attorno a suddetti assi, è possibile realizzare qualsiasi porta a qubit singolo. Prima di poter creare porte a qubit multipli arbitrarie, abbiamo bisogno di introdurre una porta a qubit multipli fondamentale: la porta CNOT.

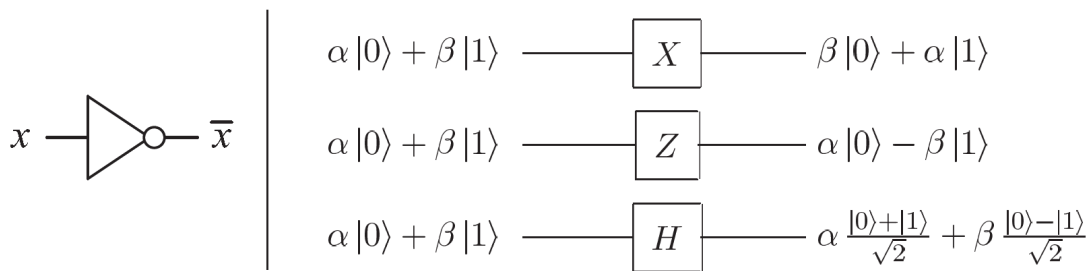


Figura 2.3: Porte a bit singolo (sinistra) e qubit singolo (destra).

### 2.2.2 Porte a qubit multipli

Un importante risultato teorico della computazione classica è che qualsiasi funzione su un insieme di bit può essere eseguita da sole porte NAND, che vengono quindi chiamate porte universali. L'analogo quantistico di una porta universale è il *NOT controllato*,

o CNOT. Questa porta ha due qubit in ingresso: uno di controllo e uno bersaglio, rispettivamente. Se il qubit di controllo è 0, il qubit bersaglio non viene cambiato. Se il qubit di controllo è 1, il qubit bersaglio viene invertito. Come è possibile vedere in Figura 2.4, l'azione di una porta CNOT generalizza una classica porta XOR, in quanto lo stato iniziale  $|A, B\rangle$  diventa lo stato finale  $|A, B \oplus A\rangle$ , dove  $\oplus$  è la somma a modulo 2 rappresentata dalla classica porta XOR e  $A, B$  sono i due qubit di valore 0 o 1.

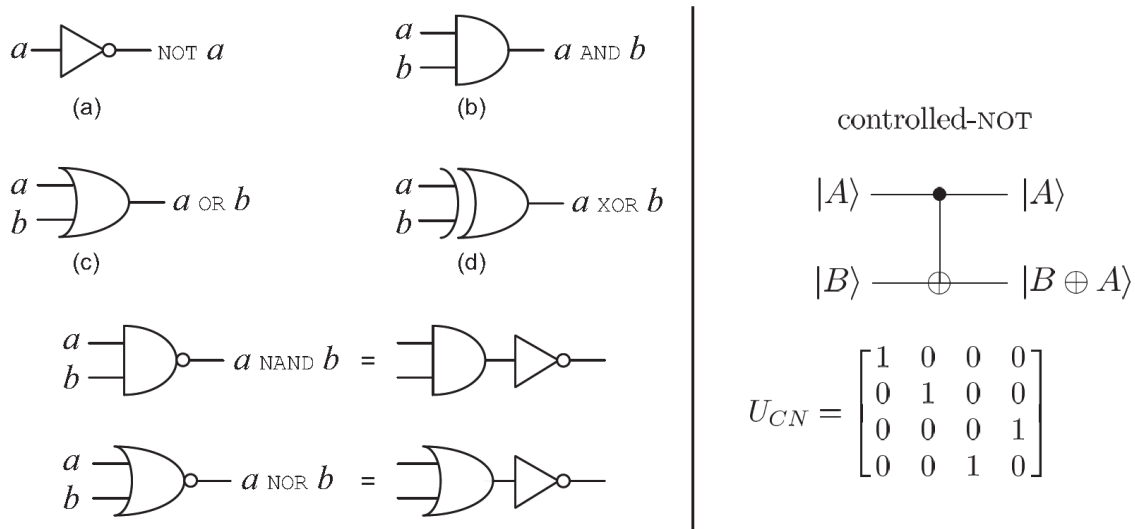


Figura 2.4: Porte classiche a bit multipli (sinistra). Circuito e rappresentazione matriciale della porta quantistica CNOT (destra).

Visto che le trasformazioni unitarie sono invertibili, con inverse unitarie, tutte le porte quantistiche sono invertibili. D'altro canto, le porte classiche XOR e NAND non sono invertibili, in quanto non è possibile risalire agli input partendo dall'output. Quindi non è possibile generalizzare le porte classiche a bit multipli con porte quantistiche a qubit multipli, come invece era possibile con il NOT.

Si può tuttavia dimostrare che, così come si può usare una porta NAND come porta universale per i circuiti classici, usando unicamente porte quantistiche CNOT e porte a qubit singoli è possibile ottenere l'equivalente di qualsiasi porta a qubit multipli. Ciò rende la porta CNOT la porta quantistica universale [7].

## 2.3 Circuiti quantistici

### 2.3.1 Proprietà e misura

Analogamente ai circuiti classici, anche i circuiti quantistici sono rappresentati da porte e fili che collegano le varie porte. Tuttavia un filo (o una linea) in un circuito quantistico non corrisponde necessariamente a un filo fisico reale: potrebbe rappresentare il passaggio del tempo, o la posizione di un fotone che si muove nello spazio.

Ci sono alcune cose permesse nei circuiti classici ma vietate in quelli quantistici. I circuiti sono aciclici, cioè non è permesso il feedback da una parte del circuito a un'altra parte. Far convergere più fili in un unico punto (*FANIN*) è un'operazione non invertibile e quindi vietata. Per il *teorema di no-cloning quantistico* non è possibile copiare lo stato di un qubit (a meno che esso sia 0 o 1), e quindi diramare un filo (*FANOUT*) è vietato.

L'operazione di misura di un qubit è rappresentata in Figura 2.5. Come già visto, questa operazione converte un qubit  $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$  in un bit classico  $M$  (simboleggiato dalla doppia linea). Il risultato è 0 con probabilità  $|\alpha|^2$  e 1 con probabilità  $|\beta|^2$ .

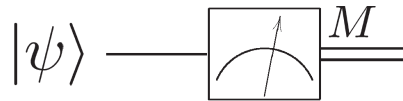


Figura 2.5: Simbolo del circuito quantistico di misura di un qubit.

### 2.3.2 Circuito di scambio

Un circuito semplice ma utile è il circuito di scambio. Dati due qubit, ciò che fa è semplicemente scambiarli di posto. Per realizzarlo sono necessarie tre porte CNOT, come mostrato in Figura 2.6. Per verificare che il circuito scambi effettivamente i qubit, basta eseguire le somme a modulo 2:

$$\begin{aligned}
 |a, b\rangle &\rightarrow |a, a \oplus b\rangle \\
 &\rightarrow |a \oplus (a \oplus b), a \oplus b\rangle = |b, a \oplus b\rangle \quad . \\
 &\rightarrow |b, (a \oplus b) \oplus b\rangle = |b, a\rangle
 \end{aligned}
 \tag{2.13}$$

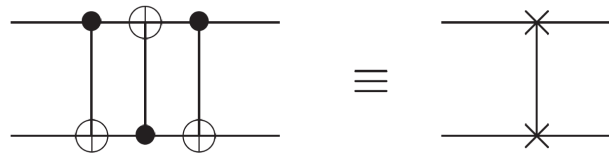


Figura 2.6: Simbolo del circuito quantistico di scambio di due qubit.

### 2.3.3 Creare stati di Bell

Un altro circuito utile è formato da una porta Hadamard seguita da una porta CNOT, come mostrato in Figura 2.7. Questo circuito trasforma i quattro stati fondamentali del sistema a due qubit in degli stati di Bell:

$$|\beta_{00}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} \tag{2.14}$$

$$|\beta_{01}\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}} \tag{2.15}$$

$$|\beta_{10}\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}} \tag{2.16}$$

$$|\beta_{11}\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}} \tag{2.17}$$

In	Out
$ 00\rangle$	$( 00\rangle +  11\rangle)/\sqrt{2} \equiv  \beta_{00}\rangle$
$ 01\rangle$	$( 01\rangle +  10\rangle)/\sqrt{2} \equiv  \beta_{01}\rangle$
$ 10\rangle$	$( 00\rangle -  11\rangle)/\sqrt{2} \equiv  \beta_{10}\rangle$
$ 11\rangle$	$( 01\rangle -  10\rangle)/\sqrt{2} \equiv  \beta_{11}\rangle$

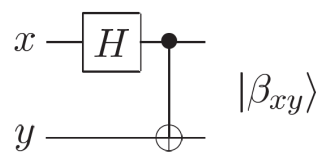


Figura 2.7: Tabella di verità e simbolo del circuito quantistico per creare stati di Bell.

Per fare un esempio, consideriamo lo stato  $|00\rangle$ . La porta Hadamard lo trasforma nello stato  $(|0\rangle + |1\rangle)|0\rangle/\sqrt{2}$ , cioè porta il primo qubit in una sovrapposizione dei due stati fondamentali. Poi agisce come ingresso di controllo per il CNOT, che inverte il secondo bit solo se il primo è 1. Il risultato sarà quindi  $(|00\rangle + |11\rangle)/\sqrt{2}$ . Gli stati di Bell, come già visto in precedenza, sono molto particolari in quanto i due qubit del sistema sono correlati (o *entangled*).

### 2.3.4 Teletrasporto quantistico

Per il teorema di no-cloning quantistico [8], copiare lo stato di un qubit è vietato (a meno che esso sia 0 o 1). Tuttavia, nulla impedisce di teletrasportare il qubit a qualsiasi distanza, anche senza un canale di comunicazione quantistico.

Consideriamo due persone fittizie, Alice e Bob. Insieme si sono trovati e hanno creato uno stato di Bell (o coppia EPR). In seguito si sono separati, prendendo ognuno uno dei due qubit entangled. Una volta a grande distanza, l'obiettivo di Alice è trasmettere un nuovo qubit  $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ , in uno stato sconosciuto, a Bob. Per farlo però, può usare solo canali di comunicazione classici (ovvero può spedire solo dei bit). Intuitivamente, sembrerebbe una missione impossibile. Ma grazie ai qubit entangled non lo è.

Il circuito è mostrato in Figura 2.8. Alice crea un sistema con il nuovo qubit e il suo qubit della coppia EPR. Lo stato iniziale del sistema è

$$|\psi_0\rangle = |\psi\rangle|\beta_{00}\rangle = \frac{1}{\sqrt{2}} [\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|00\rangle + |11\rangle)] , \quad (2.18)$$

dove i primi due qubit (a sinistra) sono di Alice e il terzo è di Bob. Alice manda i suoi due qubit in una porta CNOT, ottenendo

$$|\psi_1\rangle = \frac{1}{\sqrt{2}} [\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|10\rangle + |01\rangle)] . \quad (2.19)$$

Alice manda poi il suo primo qubit in una porta Hadamard, ottenendo

$$|\psi_2\rangle = \frac{1}{\sqrt{2}} [\alpha(|0\rangle + |1\rangle)(|00\rangle + |11\rangle) + \beta(|0\rangle - |1\rangle)(|10\rangle + |01\rangle)] . \quad (2.20)$$

Se raccogliamo i qubit di Alice, possiamo riscrivere l'equazione come

$$\begin{aligned} |\psi_2\rangle = & \frac{1}{\sqrt{2}} [|00\rangle(\alpha|0\rangle + \beta|1\rangle) + |01\rangle(\alpha|1\rangle + \beta|0\rangle) + \\ & + |10\rangle(\alpha|0\rangle - \beta|1\rangle) + |11\rangle(\alpha|1\rangle - \beta|0\rangle)] . \end{aligned} \quad (2.21)$$

A questo punto, Alice misura i suoi due qubit e manda il risultato a Bob. A seconda del risultato ottenuto, il sistema si troverà in uno di questi quattro stati:

$$00 \mapsto |\psi_3(00)\rangle = [\alpha|0\rangle + \beta|1\rangle] \quad (2.22)$$

$$01 \mapsto |\psi_3(01)\rangle = [\alpha|1\rangle + \beta|0\rangle] \quad (2.23)$$

$$10 \mapsto |\psi_3(10)\rangle = [\alpha|0\rangle - \beta|1\rangle] \quad (2.24)$$

$$11 \mapsto |\psi_3(11)\rangle = [\alpha|1\rangle - \beta|0\rangle]. \quad (2.25)$$



Per recuperare lo stato  $|\psi\rangle$  Bob deve applicare una porta quantistica che dipende dal risultato spedito da Alice. Se il risultato è 00, Bob non deve applicare nulla. Se il risultato è 01, Bob deve applicare una porta  $X$ . Se il risultato è 10, Bob deve applicare una porta  $Z$ . Se il risultato è 11, Bob deve applicare una porta  $X$  e poi una porta  $Z$ . Per riassumere, Bob deve applicare una porta  $Z^{M_1} X^{M_2}$  (dove  $M_1$  e  $M_2$  sono i due bit inviati da Alice, e come nel prodotto matriciale viene applicato prima il termine sulla destra).

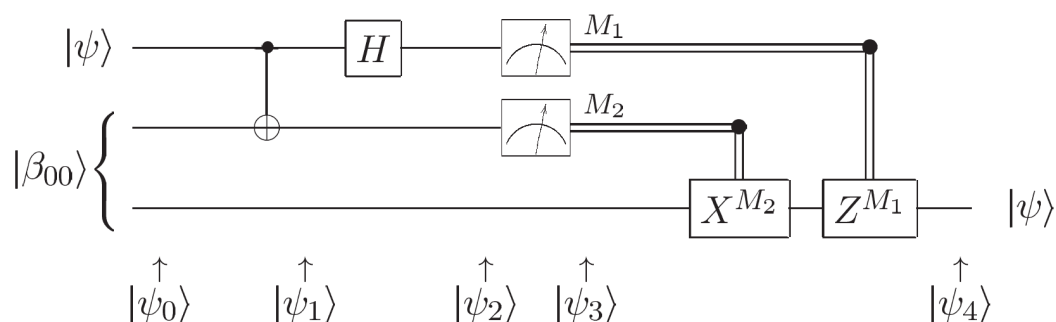


Figura 2.8: Circuito quantistico per il teletrasporto di un qubit. Le prime due linee rappresentano i qubit di Alice, mentre la terza il qubit di Bob.

Sembrerebbe che il teletrasporto quantistico permetta di comunicare a velocità superiore della luce, in disaccordo con la relatività ristretta. Tuttavia così non è: perché Bob possa recuperare una qualsiasi informazione, infatti, è necessario che Alice gli trasmetta dei dati su un canale classico. Visto che non è possibile trasmettere bit a velocità superluminale, la relatività ristretta non viene violata.

Un'altra legge che sembra essere infranta è il teorema di no-cloning, in quanto sembrerebbe che il qubit recuperato da Bob sia una copia di quello iniziale. Tuttavia anche ciò è falso, in quanto il qubit finale sarà l'unico nello stato  $|\psi\rangle$ , perché il qubit iniziale è stato misurato ed è quindi in uno stato fondamentale  $|0\rangle$  o  $|1\rangle$ .

Il teletrasporto quantistico ha varie applicazioni, soprattutto nella computazione quantistica, in quanto permette di creare porte quantistiche che resistano al rumore ed è strettamente collegato con le proprietà dei codici di correzione degli errori di trasmissione.

# Capitolo 3

## Applicazioni

### 3.1 Algoritmi quantistici

#### 3.1.1 Computazione classica su un computer quantistico

In precedenza abbiamo mostrato come fosse impossibile simulare direttamente le porte logiche classiche, che sono perlopiù non invertibili (per esempio la porta NAND) con porte quantistiche, necessariamente invertibili. Tuttavia è possibile rimpiazzare un qualsiasi circuito classico con un circuito equivalente contenente solamente elementi invertibili, usando la *porta Toffoli*. Come mostrato in Figura 3.1, questa porta ha in ingresso tre bit: due di controllo, che non vengono modificati dalla porta, e uno bersaglio, che viene invertito solo se entrambi i bit di controllo sono 1, altrimenti viene lasciato invariato. Questa particolare porta è invertibile, e ha come inversa sé stessa.

Inputs			Outputs		
$a$	$b$	$c$	$a'$	$b'$	$c'$
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0

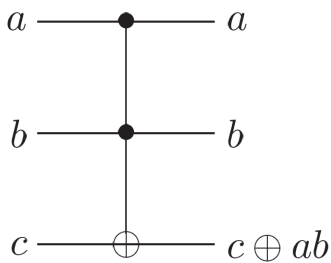


Figura 3.1: Tabella di verità e circuito classico della porta Toffoli.

Come mostrato in Figura 3.2, questa porta può essere usata per simulare una porta NAND, e quindi mediante porte Toffoli è possibile costruire un circuito equivalente a qualsiasi circuito classico (grazie all'universalità della porta NAND).

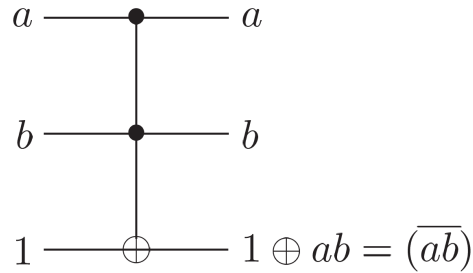


Figura 3.2: Circuito classico equivalente a una porta NAND usando una porta Toffoli.

Non è difficile poi generalizzare la porta Toffoli, essendo essa invertibile, nel caso quantistico. La matrice corrispondente può essere scritta come

$$U = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}. \quad (3.1)$$

Ciò che questa matrice fa è semplicemente invertire il terzo qubit se entrambi i primi due sono nello stato  $|1\rangle$ . Quindi, per esempio, lo stato  $|110\rangle$  verrebbe trasformato nello stato  $|111\rangle$ . Così come la porta Toffoli classica, la porta Toffoli quantistica può essere usata per simulare le porte classiche invertibili, assicurando di poter simulare qualsiasi circuito classico su un computer quantistico.

Si noti tuttavia che la porta Toffoli quantistica non è una porta universale per la computazione quantistica, in quanto è comunque necessaria almeno una porta a qubit singolo che crei uno stato a coefficienti reali non banale (analogamente al caso della porta CNOT). Per esempio, se si vuole generare un bit casuale su un computer quantistico, è sufficiente preparare un qubit nello stato  $|0\rangle$  e applicargli una porta Hadamard. Come già visto, il risultato della misura dello stato dopo la porta sarà 0 o 1 con la stessa probabilità  $1/2$ .

### 3.1.2 Parallelismo quantistico

Il *parallelismo quantistico* è una caratteristica fondamentale di molti algoritmi quantistici. Fondamentalmente consente ai computer quantistici di valutare una funzione  $f(x)$  per più valori diversi di  $x$  contemporaneamente. Consideriamo una funzione  $f(x) : 0, 1 \rightarrow 0, 1$  che ha come dominio e codominio un bit; un sistema di due qubit nello stato  $|x, y\rangle$ , e un circuito di porte quantistiche che trasforma questo stato nello stato  $|x, y \oplus f(x)\rangle$ . Chiamiamo questa trasformazione  $U_f$ . Se  $y = 0$ , chiaramente lo stato finale del secondo qubit sarà il valore  $f(x)$ . Non ci interessiamo a come sia strutturata la trasformazione  $U_f$ , ci basta sapere che è possibile dimostrare che dato un circuito classico che valuta  $f$  c'è un circuito quantistico capace di valutare con efficienza comparabile  $U_f$  (infatti basta rendere il circuito che valuta  $f$  invertibile e "tradurlo" in un circuito quantistico).

Se come stato di ingresso scegliamo  $x = |+\rangle$  (ottenibile usando una porta Hadamard sullo stato  $|0\rangle$ ) e  $y = |0\rangle$ , come mostrato in Figura 3.3, l'uscita sarà nello stato notevole

$$\frac{|0, f(0)\rangle + |1, f(1)\rangle}{\sqrt{2}}, \quad (3.2)$$

che contiene informazioni sia su  $f(0)$  che su  $f(1)$ .

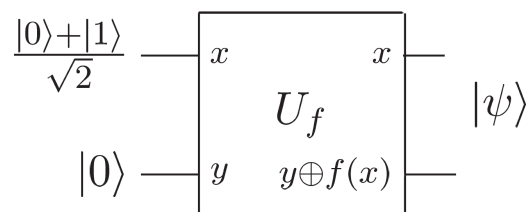


Figura 3.3: Circuito quantistico per valutare  $f(0)$  e  $f(1)$  contemporaneamente.

A differenza del parallelismo classico, dove più circuiti per calcolare  $f(x)$  sono eseguiti contemporaneamente, in questo caso un unico circuito viene impiegato per valutare la funzione per diversi valori di  $x$ , sfruttando la sovrapposizione degli stati tipicamente quantistica.

Questa procedura può essere generalizzata per funzionare su un numero arbitrario di bit, tramite un'operazione conosciuta come *trasformata di Walsh-Hadamard*, che consiste semplicemente in  $n$  porte Hadamard che agiscono parallelamente su  $n$  qubit. Formalmente indichiamo la trasformata di Walsh-Hadamard come  $H^{\otimes n}$ , dove  $\otimes$  è letto "tensore". Questa operazione produce in maniera estremamente efficiente una sovrapposizione di  $2^n$  stati usando solamente  $n$  porte. Se tutti i qubit sono nello stato iniziale  $|0\rangle$ , il risultato della trasformata sarà

$$H^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_x |x\rangle, \quad (3.3)$$

dove la somma avviene su tutti i possibili valori di  $x$ , insieme degli  $n$  qubit. Per esempio nel caso  $n = 2$  avremo

$$H^{\otimes 2} = \frac{|00\rangle + |01\rangle + |10\rangle + |11\rangle}{2}. \quad (3.4)$$

La valutazione quantistica parallela di una funzione  $f(x)$  con  $n$  bit di dominio e un bit di codominio può quindi essere effettuata in questa maniera: si preparano  $n + 1$  qubit nello stato  $|0\rangle^{\otimes n}|0\rangle$ ; si esegue una trasformata di Walsh-Hadamard sui primi  $n$  qubit; si applica la trasformazione  $U_f$ . Ciò produce lo stato

$$\frac{1}{\sqrt{2^n}} \sum_x |x\rangle |f(x)\rangle. \quad (3.5)$$

Si noti come il parallelismo quantistico non consente di valutare direttamente tutti i valori degli stati sovrapposti, in quanto una misura dello stato finale restituirebbe  $f(x)$  per un valore casuale di  $x$ , impedendo ulteriori misure. Anche un computer classico può fare ciò con semplicità. Tuttavia grazie alla computazione quantistica è possibile estrarre informazioni sul valore di  $f(x)$  per più  $x$  diversi contemporaneamente (altrimenti il parallelismo quantistico sarebbe inutile), ma per fare ciò sono necessari alcuni algoritmi.

### 3.1.3 Algoritmo di Deutsch

Una semplice modifica al circuito in Figura 3.3 mostra come, sfruttando la proprietà quantistica dell'*interferenza*, sia possibile determinare alcune informazioni più velocemente di qualsiasi computer classico. Il circuito che implementa l'algoritmo di Deutsch è mostrato in Figura 3.4. Prepariamo il primo qubit nello stato  $|+\rangle$  mandando lo stato  $|0\rangle$  attraverso una porta Hadamard. Prepariamo il secondo qubit nello stato  $|-\rangle \equiv (|0\rangle - |1\rangle)/\sqrt{2}$  mandando lo stato  $|1\rangle$  attraverso un'altra porta Hadamard.

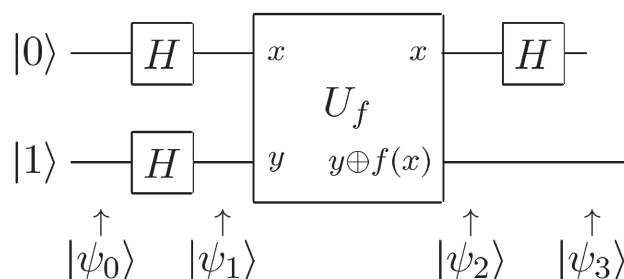


Figura 3.4: Circuito quantistico che implementa l'algoritmo di Deutsch.

Lo stato iniziale

$$|\psi_0\rangle = |01\rangle \quad (3.6)$$

passa attraverso due porte Hadamard e diventa

$$|\psi_1\rangle = \left[ \frac{|0\rangle + |1\rangle}{\sqrt{2}} \right] \left[ \frac{|0\rangle - |1\rangle}{\sqrt{2}} \right]. \quad (3.7)$$

Qualche semplice calcolo mostra che applicando  $U_f$  allo stato  $|x\rangle(|0\rangle - |1\rangle)/\sqrt{2}$  otteniamo lo stato  $(-1)^{f(x)}|x\rangle(|0\rangle - |1\rangle)/\sqrt{2}$ . Quindi  $U_f$  applicata allo stato  $|\psi_1\rangle$  restituisce

$$|\psi_2\rangle = \begin{cases} \pm \left[ \frac{|0\rangle + |1\rangle}{\sqrt{2}} \right] \left[ \frac{|0\rangle - |1\rangle}{\sqrt{2}} \right] & \text{se } f(0) = f(1) \\ \pm \left[ \frac{|0\rangle - |1\rangle}{\sqrt{2}} \right] \left[ \frac{|0\rangle - |1\rangle}{\sqrt{2}} \right] & \text{se } f(0) \neq f(1). \end{cases} \quad (3.8)$$

Infine applicando una porta Hadamard sul primo qubit otteniamo

$$|\psi_3\rangle = \begin{cases} \pm|0\rangle \left[ \frac{|0\rangle - |1\rangle}{\sqrt{2}} \right] & \text{se } f(0) = f(1) \\ \pm|1\rangle \left[ \frac{|0\rangle - |1\rangle}{\sqrt{2}} \right] & \text{se } f(0) \neq f(1). \end{cases} \quad (3.9)$$

Visto che  $f(0) \oplus f(1)$  è 0 se  $f(0) = f(1)$  e 1 altrimenti, possiamo riscrivere il risultato come

$$|\psi_3\rangle = \pm|f(0) \oplus f(1)\rangle \left[ \frac{|0\rangle - |1\rangle}{\sqrt{2}} \right]. \quad (3.10)$$

Quindi misurando il primo qubit possiamo determinare  $f(0) \oplus f(1)$ . Questo circuito, quindi, con una sola valutazione di  $f(x)$ , restituisce una proprietà globale (in questo caso  $f(0) \oplus f(1)$ ) della funzione. Un qualsiasi circuito classico richiederebbe almeno due valutazioni di  $f(x)$  per ottenere lo stesso risultato, risultando quindi ovviamente più lento.

Questo algoritmo mette anche in evidenza la differenza tra parallelismo quantistico e algoritmi probabilistici classici. Sebbene sia possibile fare un circuito classico che valuti o  $f(0)$  o  $f(1)$  con la stessa probabilità, le alternative si escludono mutuamente. Invece nel caso quantistico le due possibilità interferiscono tra di loro, permettendo di determinare, con un'opportuna trasformazione, una proprietà globale della funzione con una sola valutazione. Come in questo caso, la potenzialità alla base degli algoritmi quantistici va sfruttata applicando le giuste funzioni e le giuste trasformazioni, per ottenere risultati più efficienti di quelli ottenibili tramite circuiti classici.

### 3.1.4 Algoritmo di Deutsch-Jozsa

L'algoritmo di Deutsch è un caso particolare semplificato di un algoritmo quantistico più generale chiamato *algoritmo di Deutsch-Jozsa*. La sua applicazione permette di risolvere il cosiddetto *problema di Deutsch*, che può essere descritto nel modo seguente.

Alice sceglie un numero  $x$  da 0 a  $2^n - 1$  e lo manda per lettera a Bob, che per ipotesi si trova lontano da Alice. Bob calcola una qualche funzione  $f(x)$  e spedisce il risultato a Alice. Questa funzione può restituire solo 0 o 1, e inoltre Bob premette che può essere solo di due tipi: o è costante per tutti i valori di  $x$ , oppure è bilanciata (cioè è 0 per esattamente la metà degli  $x$  possibili e 1 per l'altra metà). L'obiettivo di Alice è determinare il tipo di funzione scelto da Bob nel minor numero di comunicazioni possibile.

Nel caso classico, Alice può spedire solo un valore di  $x$  (quindi  $n$  bit) alla volta. Quindi nel caso peggiore Alice dovrebbe scrivere a Bob  $2^{n-1} + 1$  volte prima di poter essere sicura che la funzione non sia costante (e quindi sia bilanciata). Se invece Alice potesse spedire dei qubit, e Bob potesse eseguire la trasformazione unitaria  $U_f$  per calcolare il valore di  $f(x)$ , allora Alice potrebbe determinare il tipo della funzione con certezza in un'unica comunicazione, sfruttando l'algoritmo di Deutsch-Jozsa (mostrato in Figura 3.5).

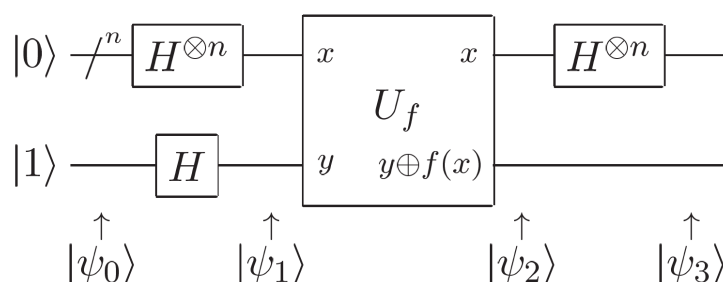


Figura 3.5: Circuito quantistico che implementa l'algoritmo di Deutsch-Jozsa. Il filo con  $f^n$  sopra rappresenta  $n$  qubit.

Alice ha  $n$  qubit per la "domanda", e un qubit per la "risposta". Il sistema viene preparato nello stato

$$|\psi_0\rangle = |0\rangle^{\otimes n} |1\rangle. \quad (3.11)$$

Dopo aver applicato la trasformata di Walsh-Hadamard sui suoi  $n$  qubit e la porta Hadamard sul qubit per Bob, il sistema si trova nello stato

$$|\psi_1\rangle = \sum_{x \in \{0,1\}^n} \frac{|x\rangle}{\sqrt{2^n}} \left[ \frac{|0\rangle - |1\rangle}{\sqrt{2}} \right]. \quad (3.12)$$

In seguito la funzione  $f$  è valutata da Bob tramite la trasformazione  $U_f$ , risultando nello stato

$$|\psi_2\rangle = \sum_x \frac{(-1)^{f(x)}|x\rangle}{\sqrt{2^n}} \left[ \frac{|0\rangle - |1\rangle}{\sqrt{2}} \right]. \quad (3.13)$$

Per calcolare la trasformata di Walsh-Hadamard sugli  $n$  qubit di Alice conviene prima vedere l'azione della trasformata su uno stato generico  $|x\rangle$  di  $n$  qubit. Ricordando l'equazione (3.3), abbiamo

$$H^{\otimes n}|x\rangle = \frac{\sum_z (-1)^{x \cdot z} |z\rangle}{\sqrt{2^n}}, \quad (3.14)$$

dove  $x \cdot z$  indica il prodotto scalare modulo 2. Quindi avremo

$$|\psi_3\rangle = \sum_z \sum_x \frac{(-1)^{x \cdot z + f(x)} |z\rangle}{2^n} \left[ \frac{|0\rangle - |1\rangle}{\sqrt{2}} \right]. \quad (3.15)$$

Osserviamo che l'ampiezza dello stato  $|0\rangle^{\otimes n}$  è  $\sum_x (-1)^{f(x)}/2^n$ . Se  $f$  è costante e uguale a 0 per tutti gli  $x$ , l'ampiezza per  $|0\rangle^{\otimes n}$  sarà +1. Se  $f$  è costante e uguale a 1, l'ampiezza sarà -1. Essendo  $|\psi_3\rangle$  di lunghezza unitaria, ne segue che tutte le altre ampiezze devono essere 0, quindi misurando i suoi qubit Alice otterrà tutti 0. Se  $f$  è bilanciata i contributi positivi e negativi all'ampiezza di  $|0\rangle^{\otimes n}$  si cancellano a vicenda risultando in un'ampiezza nulla, quindi Alice misurerà almeno un qubit diverso da 0 nei suoi  $n$  qubit.

Riassumendo, se Alice misura tutti 0 la funzione è costante, altrimenti è bilanciata. Diversamente dal caso classico, in cui il problema ha una soluzione deterministica che dipende esponenzialmente dal numero di bit, nel caso quantistico il problema ha una soluzione che richiede un'unica esecuzione, consentendo quindi un vantaggio di velocità (*speedup*) esponenziale rispetto al caso classico. Si noti tuttavia che non ci sono applicazioni conosciute dell'algoritmo di Deutsch-Jozsa.

## 3.2 Classi di algoritmi e problemi

### 3.2.1 Algoritmi basati sulla trasformata di Fourier

La trasformata discreta di Fourier trasforma una successione  $x_0, \dots, x_{N-1}$  di  $N$  numeri complessi in una successione  $y_0, \dots, y_{N-1}$  di numeri complessi definita come

$$y_k \equiv \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{2\pi i j k / N} x_j. \quad (3.16)$$

Questa trasformata ha moltissime applicazioni in vari campi scientifici, in quanto la versione trasformata di un problema è spesso più facile (o risolvibile) dell'originale. É



stata anche elaborata una teoria matematica avanzata su una versione generalizzata delle trasformate di Fourier. La trasformata di Walsh-Hadamard, usata nell'algoritmo di Deutsch-Jozsa, rientra in questa classe di trasformate di Fourier generalizzate.

Quanto velocemente è possibile applicare una trasformata di Fourier? Nel caso classico occorrono circa  $n2^n$  passaggi per trasformare  $2^n$  numeri. Nel caso quantistico, invece, ne occorrono solamente  $n^2$ , cioè si ha uno speedup esponenziale. Tuttavia, questa trasformata quantistica viene applicata sulle ampiezze "nascoste" degli stati quantistici, e quindi non è direttamente misurabile. Possiamo quindi effettuare alcune operazioni sulle  $2^n$  ampiezze trasformate degli  $n$  qubit più velocemente di quanto sia possibile su un qualsiasi computer classico; occorre però ingegnarsi per riuscire a recuperare informazioni sui risultati di questi calcoli. Anche per questo sfruttare appieno la potenza dei computer quantistici non è affatto semplice, in quanto la trasformata di Fourier ha moltissime applicazioni utili.

Estremamente importanti, in questo gruppo, sono gli algoritmi quantistici di Shor per la fattorizzazione di numeri interi e per il problema del logaritmo discreto, che garantiscono una soluzione efficiente (cioè di tipo polinomiale rispetto all'input), mentre si crede che non ci siano soluzioni efficienti con algoritmi classici.

### 3.2.2 Algoritmi di ricerca

Una classe completamente differente di algoritmi, inizialmente descritta da Grover, è quella degli algoritmi di ricerca quantistici, che risolvono il seguente problema: dato uno spazio di ricerca di dimensione  $N$ , e senza conoscenza a priori della struttura dell'informazione contenuta in esso, si vuole trovare un elemento in quello spazio con una proprietà conosciuta. Classicamente la soluzione di questo problema richiede approssimativamente  $N$  operazioni, mentre la versione quantistica ne richiede solamente  $\sqrt{N}$ . Lo speedup in questo caso è solamente quadratico, e non esponenziale, ma è comunque di grande interesse in quanto l'applicabilità è più vasta degli algoritmi basati sulla trasformata di Fourier.

### 3.2.3 Simulazione quantistica

La simulazione di sistemi quantistici è un'ovvia candidata come applicazione per i computer quantistici, anche a causa della difficoltà in questo ambito dei computer classici. In generale memorizzare lo stato quantistico di un sistema con  $n$  componenti richiede qualcosa dell'ordine di  $c^n$  bit di memoria su un computer classico, dove  $c$  è una costante che dipende dai dettagli e dalla precisione voluta nella simulazione. Per effettuare la simulazione su un computer quantistico invece servono solamente  $kn$  qubit, dove  $k$  è di

nuovo una costante dipendente dai dettagli del sistema simulato. Questo significa ovviamente che i computer quantistici possono simulare efficientemente sistemi meccanici quantistici che si crede non sia possibile simulare efficientemente su computer classici.

### 3.2.4 Crittografia quantistica

Il problema crittografico più diffuso è la trasmissione di messaggi segreti. Ci sono due persone, Alice e Bob, che vogliono comunicarsi un messaggio segreto. Si possono distinguere due categorie di sistemi crittografici:

**Chiave privata:** Alice usa una chiave che conosce solo lei (può essere qualsiasi cosa, per esempio un numero binario) per codificare l'informazione che vuole spedire a Bob. Alice deve poi spedire l'informazione codificata e la sua chiave a Bob (o comunque Bob deve conoscere la chiave in qualche modo), che può decifrare il messaggio ricevuto. Il problema più ovvio di questo sistema è che comunicare segretamente la chiave è analogo a comunicare segretamente il messaggio: se qualcuno riesce a "spiare" la conversazione e ottenere la chiave, riuscirà a decodificare il messaggio.

**Chiave pubblica:** Bob rende disponibile a tutti una chiave, detta appunto pubblica. Alice usa questa chiave per codificare il messaggio che vuole spedire a Bob. Il metodo di codifica è scelto in modo che sia estremamente difficile decifrare il messaggio avendo a disposizione solamente la chiave pubblica. Bob, invece, ha una chiave segreta che conosce unicamente lui e che insieme alla chiave pubblica rende semplice la decodifica. Il sistema crittografico più diffuso al giorno d'oggi è l'RSA (dai cognomi dei suoi inventori Rivest, Shamir e Adleman)[9], e sfrutta una chiave pubblica.

Una delle prime scoperte nel campo della computazione quantistica era il suo possibile utilizzo per distribuire le chiavi private. Questa procedura, nota come *crittografia quantistica*, si basa sul principio che l'osservazione di un sistema quantistico ne altera lo stato, solitamente facendo collassare la funzione d'onda. Quindi se qualcuno tentasse di spiare la comunicazione della chiave tra Alice e Bob, loro potrebbero notare il disturbo o l'interferenza e capire che la trasmissione non è sicura, scegliendo quindi di spedire un'altra chiave, magari su un altro canale. Dal primo protocollo di Wiesner degli anni '60, rielaborato poi nel 1984 da Bennett e Brassard, sono stati proposti e progettati numerose versioni di crittografia quantistica, e al giorno d'oggi siamo al punto in cui potrebbero avere qualche applicazione reale su piccola scala [10].

La computazione quantistica può essere usata per trasmettere chiavi private in modo sicuro, ma non solo. Il punto di forza della sicurezza dei sistemi a chiave pubblica è la difficoltà (o la potenza computazionale richiesta) nel decifrare un messaggio conoscendo

solamente la chiave pubblica e non quella segreta. Per esempio, invertire la crittografia del sistema RSA è un problema strettamente collegato alla fattorizzazione dei numeri interi, che si crede non abbia soluzione efficiente su un computer classico. Tuttavia, l'algoritmo quantistico di Shor per la fattorizzazione è efficiente su un computer quantistico, in quanto richiede un tempo polinomiale anziché esponenziale. Questo vantaggio di velocità potrebbe plausibilmente essere usato per invalidare il sistema RSA. Anche altri sistemi crittografici, basati per esempio sul problema del logaritmo discreto, potrebbero perdere la loro sicurezza a causa degli algoritmi quantistici. Questa particolare applicazione degli algoritmi quantistici ha indubbiamente suscitato molto interesse verso la computazione quantistica.

### 3.3 Visione d'insieme

Molte applicazioni su piccola scala della computazione quantistica sono già ben conosciute. Tra di esse molto importanti sono la *tomografia di stato quantistico* e la *tomografia di processo quantistico*, o QPT [11]. La prima è un metodo per determinare lo stato quantistico di un sistema. Per fare ciò occorre preparare varie copie dello stesso stato quantistico che vengono poi misurate in maniere differenti per ricostruire una descrizione completa dello stato. La seconda invece, più ambiziosa ma strettamente collegata, è una procedura per caratterizzare completamente la dinamica di un sistema quantistico. La QPT, oltre ad ovvie applicazioni nel campo della computazione quantistica, potrebbe essere usata come strumento diagnostico in molti campi scientifici e tecnologici dove gli effetti quantistici sono rilevanti.

Applicazioni nel campo della comunicazione comprendono la crittografia quantistica, per trasmettere chiavi private in sicurezza, e il teletrasporto quantistico, per trasmettere stati quantistici tra nodi distanti di una rete di computer evitando il rumore.

Una delle applicazioni su media scala più promettenti è la simulazione quantistica. Potrebbe essere di grande utilità nello studio del design e delle proprietà di nuove molecole, simulando molti degli strumenti utilizzati in laboratorio tramite appositi software, rendendo il processo più veloce ed economico. In passato sono già state effettuate delle prove di questi calcoli per aiutare a inventare nuove molecole, ma i computer classici si sono dimostrati troppo poco potenti per simulare in maniera utile dei sistemi quantistici.

Le applicazioni a larga scala comprendono invece la fattorizzazione di grandi numeri interi e il problema dei logaritmi discreti, anche se in realtà sarebbero più rilevanti i risvolti negativi (in quanto come già visto potrebbero essere usate per violare la sicurezza dei sistemi crittografici esistenti) che l'effettiva applicabilità a lungo termine. Di grande utilità, sempre a larga scala, è invece la ricerca quantistica, che potrebbe essere usata in vari campi scientifici e tecnologici.

# Capitolo 4

## Implementazioni

### 4.1 Condizioni per la realizzazione

Un computer quantistico deve essere ben isolato per mantenere le sue proprietà quantistiche, ma allo stesso tempo i suoi qubit devono essere accessibili così che possano essere manipolati per eseguire dei calcoli e leggere i risultati. Un'implementazione realistica deve trovare il giusto equilibrio tra questi aspetti. Un concetto fondamentale per capire la validità di un particolare computer quantistico è il *rumore quantistico*, a volte chiamato *decoerenza*. Con questa nozione si indicano tutti i processi che disturbano o corrompono l'evoluzione voluta del sistema, o che comunque causano perdita di informazione quantistica del sistema.

I quattro requisiti fondamentali per la computazione quantistica sono:

**Rappresentazione digitale dell'informazione quantistica:** L'insieme degli stati accessibili deve essere finito. Variabili continue, come per esempio la posizione di una particella su una linea, non sono generalmente buone rappresentazioni di stati quantistici. Infatti conviene solitamente avere delle simmetrie che vincolano la dimensione dello spazio, per ridurre la decoerenza. Per esempio una particella con spin  $1/2$  vive in uno spazio di Hilbert dato dallo span dei due stati  $|\uparrow\rangle$  e  $|\downarrow\rangle$ , e quindi è un qubit praticamente ideale quando ben isolata.

**Esecuzione di trasformazioni unitarie:** I sistemi quantistici chiusi evolvono come descritto dalla loro hamiltoniana, ma per effettuare calcoli arbitrari bisogna essere in grado di controllare l'hamiltoniana per effettuare una selezione arbitraria di trasformazioni da una famiglia universale di trasformazioni arbitrarie. Visto che ogni trasformazione unitaria può essere composta da operazioni a qubit singolo e porte CNOT, la realizzazione di questi due tipi di porte è l'obiettivo primario.

**Preparazione di stati iniziali affidabili:** Ovviamente non ha senso poter effettuare qualsiasi calcolo si voglia se non si possono decidere gli input del circuito. Tuttavia è sufficiente essere in grado di preparare (ripetutamente) solo uno specifico stato quantistico con grande precisione, in quanto una trasformazione unitaria può poi trasformarlo in uno stato di input a piacere.

**Misura del risultato in uscita:** Si può pensare alla misurazione come al processo di accoppiamento di uno o più sistemi quantistici con un sistema classico in modo che, dopo un certo intervallo di tempo, lo stato dei qubit sia indicato dallo stato del sistema classico. Le misure di proiezione (dette "forti"), che fanno collassare la funzione d'onda del sistema e restituiscono un segnale relativamente grande, sono spesso difficili da implementare. Tuttavia è possibile sfruttare misure "deboli", eseguite continuamente, compiendo i calcoli in un tempo minore dell'accoppiamento per la misura, e usando grandi *ensemble* di computer quantistici. Per fare ciò bisogna però modificare gli algoritmi per funzionare con i valori medi misurati degli ensemble.

## 4.2 Oscillatori armonici

Consideriamo un semplice oscillatore armonico, e vediamo perché non è un buon candidato per la computazione quantistica.

### 4.2.1 Apparato fisico

Un esempio di un oscillatore armonico semplice è una particella in una buca di potenziale parabolica,  $V(x) = m\omega^2 x^2/2$ . Nel caso classico potrebbe essere una massa attaccata a una molla, che oscilla trasferendo l'energia potenziale della molla in energia cinetica della massa e viceversa. In questo caso l'energia del sistema è un parametro continuo. Nel caso quantistico l'energia può assumere solo un numero discreto di valori. Per esempio per una radiazione elettromagnetica intrappolata in una cavità l'energia può essere solo un multiplo di  $\hbar\omega$ , dove  $\omega$  è la frequenza della radiazione.

L'insieme discreto degli autostati dell'energia di un oscillatore armonico semplice può essere etichettato come  $|n\rangle$ , dove  $n = 0, 1, \dots, \infty$ . Per rappresentare i qubit si sceglie un sottoinsieme finito di questi stati. Questi qubit avranno un tempo di vita determinato da parametri fisici come per esempio la qualità della cavità (che può essere aumentata rendendo più riflettenti le superfici interne). Per applicare trasformazioni unitarie sarà sufficiente lasciar evolvere il sistema nel tempo.

### 4.2.2 Hamiltoniana

L'hamiltoniana per una particella in potenziale parabolico unidimensionale è

$$H = \frac{p^2}{2m} + \frac{1}{2}m\omega^2 x^2, \quad (4.1)$$

dove  $p$  è l'operatore quantità di moto della particella,  $m$  è la sua massa,  $x$  è l'operatore posizione e  $\omega$  dipende dalla buca di potenziale. Questa formula si può riscrivere come

$$H = \hbar\omega \left( a^\dagger a + \frac{1}{2} \right), \quad (4.2)$$

dove  $a^\dagger$  e  $a$  sono, rispettivamente, gli operatori di creazione e distruzione, che nel caso dell'oscillatore armonico sono dati da

$$a = \frac{1}{\sqrt{2m\hbar\omega}}(m\omega x + ip) \quad (4.3)$$

$$a^\dagger = \frac{1}{\sqrt{2m\hbar\omega}}(m\omega x - ip). \quad (4.4)$$

Gli autostati  $|n\rangle$  di  $H$  hanno le proprietà

$$a^\dagger a |n\rangle = n |n\rangle \quad (4.5)$$

$$a^\dagger |n\rangle = \sqrt{n+1} |n+1\rangle \quad (4.6)$$

$$a |n\rangle = \sqrt{n} |n-1\rangle. \quad (4.7)$$

Risolvendo l'equazione di Schrödinger indipendente dal tempo si ottiene lo spettro degli autovalori dell'energia

$$H |n\rangle = \hbar \left( n + \frac{1}{2} \right) |n\rangle. \quad (4.8)$$

Risolvendo poi l'equazione di Schrödinger generale si trova che lo stato  $|\psi(0)\rangle = \sum_n c_n(0) |n\rangle$  evolve nel tempo nello stato

$$|\psi(t)\rangle = e^{-iHt/\hbar} |\psi(0)\rangle = \sum_n c_n e^{-in\omega t} |n\rangle. \quad (4.9)$$

Per questo caso di implementazione trascuriamo il problema della preparazione dello stato iniziale e della misura dello stato finale.

### 4.2.3 Computazione quantistica

Scegliamo di codificare una coppia di qubit mappandoli nel seguente modo:

$$\begin{aligned}
 |00\rangle_L &= |0\rangle \\
 |01\rangle_L &= |2\rangle \\
 |10\rangle_L &= (|4\rangle + |1\rangle)/\sqrt{2} \\
 |11\rangle_L &= (|4\rangle - |1\rangle)/\sqrt{2},
 \end{aligned}
 \tag{4.10}$$

dove il pedice  $L$  indica lo stato "logico" dei qubit. Prepariamo il sistema a  $t = 0$  in uno stato appartenente allo span di questi stati della base computazionale, e lo evolviamo al tempo  $t = \pi/\hbar\omega$ . Ciò equivale a trasformare gli autovalori dell'energia nel seguente modo:

$$|n\rangle \rightarrow e^{-i\pi a^\dagger a} |n\rangle = (-1)^n |n\rangle. \tag{4.11}$$

In questo modo, gli stati  $|0\rangle$ ,  $|2\rangle$  e  $|4\rangle$  rimangono invariati, mentre  $|1\rangle \rightarrow -|1\rangle$ . Come risultato, è come se i due qubit fossero passati attraverso una porta CNOT.

In generale una condizione necessaria e sufficiente per un sistema fisico per essere in grado di eseguire una trasformazione unitaria  $U$  è che l'operatore evoluzione temporale del sistema,  $T = e^{-iHt}$ , definito dall'hamiltoniana  $H$ , abbia lo stesso spettro di  $U$ . L'hamiltoniana di un oscillatore armonico può essere perturbata per realizzare praticamente qualsiasi spettro di autovalori, ed un qualsiasi numero di qubit potrebbe essere rappresentato mappandolo negli infiniti autostati del sistema.

### 4.2.4 Problematiche

Ci sono molti inconvenienti in questo modello computazionale, rendendolo inadatto per la computazione quantistica. Non sempre è possibile conoscere lo spettro degli autovalori di un operatore unitario, anche se si conosce il modo di realizzarlo con porte quantistiche. Infatti per molti problemi risolti dagli algoritmi quantistici, conoscere gli autovalori è analogo a conoscere la soluzione del problema. Un altro problema è che non sarebbe possibile eseguire calcoli in sequenza, in quanto la combinazione di due trasformazioni unitarie risulta generalmente in una nuova trasformazione con autovalori sconosciuti. Infine usando un solo oscillatore armonico semplice viene meno la rappresentazione digitale dell'informazione quantistica. Uno spazio di Hilbert di  $2^n$  dimensioni mappato nello spazio degli stati di un singolo oscillatore armonico richiederebbe stati di energia  $2^n \hbar\omega$ . Se lo stesso spazio di Hilbert fosse ottenuto sfruttando  $n$  sistemi a due livelli, l'energia massima richiesta sarebbe  $n\hbar\omega$ .

## 4.3 Fotoni ottici

I fotoni possono essere trasportati per grandi distanze in fibre ottiche e manipolare fasci di fotoni è relativamente semplice. Inoltre reagiscono poco tra di loro e sono soggetti all'interferenza, fenomeno tipicamente quantistico, rendendoli dei buoni candidati per un modello computazionale quantistico.

### 4.3.1 Apparato fisico

Come abbiamo visto nel caso dell'oscillatore armonico, l'energia della radiazione elettromagnetica intrappolata in una cavità è quantizzata in termini di  $\hbar\omega$ . Ognuno di questi quanti è un fotone. Consideriamo due cavità, di energia totale  $\hbar\omega$ , e mappiamo lo stato di un qubit a seconda se il fotone sia in una cavità ( $|01\rangle$ ) oppure nell'altra ( $|10\rangle$ ). La sovrapposizione dei due stati viene scritta come  $c_0|01\rangle + c_1|10\rangle$ . Questa rappresentazione viene chiamata *dual-rail*.

Un modo per generare fotoni singoli in laboratorio è attenuare l'output di un laser. Gli stati emessi da un laser sono detti stati coerenti, definiti come

$$|\alpha\rangle = e^{-|\alpha|^2/2} \sum_{n=0}^{\infty} \frac{a^n}{\sqrt{n!}} |n\rangle, \quad (4.12)$$

dove  $|n\rangle$  indica l'autostato dell'energia di  $n$  fotoni. Per ottenere un singolo fotone, prendiamo per esempio  $\alpha = \sqrt{0.1}$ , e abbiamo lo stato  $\sqrt{0.90}|0\rangle + \sqrt{0.09}|1\rangle + \sqrt{0.002}|2\rangle + \dots$ . Si nota immediatamente dai coefficienti che con questo stato avremo zero fotoni il 90% delle volte, un fotone il 9% delle volte e più fotoni l'1% delle volte. I fotoni singoli possono essere rilevati con alta efficienza per un grande intervallo di lunghezze d'onda, sfruttando varie tecnologie. Una delle caratteristiche dei rilevatori di maggior importanza in questo caso è la capacità di determinare con alta probabilità se zero o un fotone esistono in un determinato modo spaziale (che può essere per esempio la direzione di polarizzazione della luce). Per la rappresentazione dual-rail, ciò si traduce in una misura proiettiva sulla base computazionale.

Tre dispositivi già ben conosciuti per manipolare i fotoni sono gli specchi, gli sfasatori (phase shifter) e i divisori di fascio (beam splitter). Gli specchi riflettono i fotoni cambiandone la direzione di propagazione spaziale, solitamente con perdite dell'ordine del 0.01%. Gli sfasatori sono semplicemente dei blocchi di mezzi trasparenti con indice di rifrazione  $n$  diverso da quello del vuoto  $n_0$ . Un fotone che si propaga in un mezzo del genere per una lunghezza  $L$  subisce uno sfasamento di  $e^{ikL}$ , dove  $k = n\omega/c$ . Quindi, rispetto a un fotone che percorre la stessa distanza nel vuoto, ci sarà una differenza di fase di  $e^{i(n-n_0)L\omega/c}$ .



I divisori di fascio sono solitamente dei pezzi di vetro parzialmente argentati, che riflettono una frazione  $R$  del fascio e ne trasmettono la restante  $1 - R$ . In laboratorio possono essere realizzati collegando due prismi con un sottile strato metallico. Viene definito l'angolo  $\theta$  del divisore come  $\cos \theta = R$ . Questo angolo parametrizza la quantità di luce riflessa, e non l'orientazione spaziale del divisore. I divisori di fascio sono descritti dalle equazioni

$$a_{out} = a_{in} \cos \theta + b_{in} \sin \theta \quad (4.13)$$

$$b_{out} = -a_{in} \sin \theta + b_{in} \cos \theta, \quad (4.14)$$

dove  $a$  e  $b$  rappresentano, nel caso classico, i campi elettromagnetici della radiazione.

Infine un altro componente fondamentale, parte dell'ottica non lineare, sono i mezzi Kerr. In questi materiali l'indice di rifrazione è proporzionale all'intensità  $I$  della luce che li attraversa, un effetto ottico conosciuto come effetto Kerr:

$$n(I) = n + n_2 I. \quad (4.15)$$

Sperimentalmente, il comportamento rilevante di questi mezzi è che quando due fasci di luce di stessa intensità sono propagati parallelamente in un mezzo Kerr, ogni fascio subisce uno sfasamento di  $e^{in_2 I L \omega / c}$  rispetto al caso di un fascio singolo. Sarebbe comodo se la lunghezza  $L$  potesse essere arbitraria, ma sfortunatamente i mezzi Kerr sono solitamente molto assorbenti o diffondono la luce fuori dal modo spaziale desiderato.

### 4.3.2 Computazione quantistica

Le trasformazioni unitarie possono essere applicate all'informazione quantistica codificata nella rappresentazione dual-rail usando sfasatori, divisori di fascio e mezzi Kerr. L'evoluzione temporale della radiazione elettromagnetica in una cavità è descritta dall'oscillatore armonico:  $|0\rangle$  è lo stato del vuoto,  $|1\rangle = a^\dagger |0\rangle$  è lo stato con un singolo fotone, e in generale

$$|n\rangle = \frac{a^{\dagger n}}{\sqrt{n!}} |0\rangle \quad (4.16)$$

è lo stato con  $n$  fotoni, dove  $a^\dagger$  è l'operatore di creazione del modo spaziale. L'evoluzione in spazio libero è descritta dall'hamiltoniana  $H = \hbar \omega a^\dagger a$  e applicando l'equazione (4.9) vediamo l'evoluzione temporale

$$|\psi\rangle = c_0 |0\rangle + c_1 |1\rangle \rightarrow |\psi(t)\rangle = c_0 |0\rangle + c_1 e^{-i\omega t} |1\rangle. \quad (4.17)$$

La rappresentazione dual-rail è conveniente perché l'evoluzione temporale libera cambia  $|\varphi\rangle = c_0 |01\rangle + c_1 |10\rangle$  solo di un fattore di fase globale, che non è misurabile.

**Sfasatori:** Uno sfasatore  $P$  agisce come una normale evoluzione temporale, ma con una velocità diversa, e solo sui modi spaziali che lo attraversano. Ciò è dovuto al fatto che la luce rallenta quando attraversa un mezzo, in particolare ci vuole  $\Delta \equiv (n - n_0)L/c$  tempo in più per propagarsi in un mezzo lungo  $L$  con indice di rifrazione  $n$  rispetto al vuoto. L'azione di  $P$  sullo stato del vuoto è nulla:  $P|0\rangle = |0\rangle$ , su un fotone singolo invece  $P|1\rangle = e^{i\Delta}|1\rangle$ . Nel caso della rappresentazione dual-rail, usare uno sfasatore su un modo spaziale ritarda l'evoluzione della sua fase rispetto a un modo spaziale che percorre la stessa distanza ma non attraversa lo sfasatore. La trasformazione che avviene è quindi

$$c_0|01\rangle + c_1|10\rangle \rightarrow c_0e^{-i\Delta/2}|01\rangle + c_1e^{i\Delta/2}|10\rangle, \quad (4.18)$$

(a meno di un fattore di fase globale irrilevante), che è semplicemente una rotazione attorno all'asse  $\hat{z}$

$$R_z(\Delta) = e^{-iZ\Delta/2}, \quad (4.19)$$

dove abbiamo  $|0\rangle_L = |01\rangle$  e  $|1\rangle_L = |10\rangle$  (il pedice  $L$  indica lo stato logico).  $Z$  è il solito operatore già visto, che equivale a una rotazione di  $\pi$  attorno all'asse  $\hat{z}$  sulla sfera di Bloch. Si può quindi pensare a  $P$  come risultato dell'evoluzione dovuta all'hamiltoniana  $H_{sf} = (n_0 - n)Z$ , con

$$P = e^{-iH_{sf}L/c}. \quad (4.20)$$

**Divisori di fascio:** Nel caso quantistico i divisori agiscono su due modi, che descriviamo con gli operatori di distruzione (creazione)  $a$  ( $a^\dagger$ ) e  $b$  ( $b^\dagger$ ). In questo caso l'hamiltoniana è

$$H_{df} = i\theta(ab^\dagger - a^\dagger b), \quad (4.21)$$

e il divisore esegue la trasformazione unitaria

$$B = e^{\theta(a^\dagger b - ab^\dagger)}. \quad (4.22)$$

La trasformazione applicata a  $a$  e  $b$  è scrivibile come

$$BaB^\dagger = a \cos \theta + b \sin \theta \quad (4.23)$$

$$BbB^\dagger = -a \sin \theta + b \cos \theta \quad (4.24)$$

In termini di porte logiche quantistiche, notiamo che  $B|00\rangle = |00\rangle$ , quindi se non c'è nessun fotone in ingresso in nessuno dei due modi, non ci sono fotoni in uscita. Quando c'è un fotone in ingresso nel modo  $a$ , ricordando che  $|1\rangle = a^\dagger|0\rangle$ , abbiamo

$$B|01\rangle = Ba^\dagger|00\rangle = Ba^\dagger B^\dagger B|00\rangle = (a^\dagger \cos \theta + b^\dagger \sin \theta)|00\rangle = \cos \theta|01\rangle + \sin \theta|10\rangle. \quad (4.25)$$

Analogamente  $B|10\rangle = \cos \theta|10\rangle - \sin \theta|01\rangle$ . Quindi, sulla varietà degli stati computazionali  $|0\rangle_L$  e  $|1\rangle_L$  possiamo scrivere

$$B = \begin{bmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{bmatrix} = e^{i\theta Y}, \quad (4.26)$$

che rappresenta una rotazione attorno all'asse  $\hat{y}$  sulla sfera di Bloch. L'operatore  $Y$  esegue una rotazione di  $\pi$  attorno all'asse  $\hat{y}$ , analogamente all'azione degli altri operatori di Pauli  $Z$  e  $X$  per gli omonimi assi, e può essere scritto come

$$Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}. \quad (4.27)$$

Come già visto in precedenza, qualsiasi porta a qubit singolo può essere generata da una rotazione attorno all'asse  $\hat{z}$  e da una rotazione attorno all'asse  $\hat{y}$ . Nel caso del fotone ottico, quindi, con sfasatori e divisori di fascio si possono realizzare tutte le porte a qubit singolo.

**Mezzi Kerr:** L'effetto più importante di questi mezzi è la modulazione di fase incrociata che crea su due modi di luce. Classicamente questo effetto è descritto dall'equazione (4.15), mentre quantisticamente è descritto dall'hamiltoniana

$$H_{\text{mk}} = -\chi a^\dagger a b^\dagger b, \quad (4.28)$$

dove  $a$  e  $b$  sono i due modi della luce che si propaga nel mezzo. Per un cristallo di lunghezza  $L$  abbiamo la trasformazione unitaria

$$K = e^{i\chi L a^\dagger a b^\dagger b}. \quad (4.29)$$

In queste equazioni  $\chi$  è un coefficiente collegato con  $n_2$  e con il coefficiente di suscettibilità non lineare del terzo ordine solitamente denotato con  $\chi^{(3)}$ . Grazie a questi mezzi è possibile realizzare una porta CNOT. Per gli stati di fotone singolo, si ha

$$K|00\rangle = |00\rangle \quad (4.30)$$

$$K|01\rangle = |01\rangle \quad (4.31)$$

$$K|10\rangle = |10\rangle \quad (4.32)$$

$$K|11\rangle = e^{i\chi L}|11\rangle. \quad (4.33)$$

Scegliendo  $L$  in modo che  $\chi L = \pi$ , si avrà  $K|11\rangle = -|11\rangle$ . Consideriamo ora due stati dual-rail, cioè quattro modi spaziali di luce. Questi stati appartengono allo spazio dato dallo span dei quattro stati  $|e_{00}\rangle = |1001\rangle$ ,  $|e_{01}\rangle = |1010\rangle$ ,  $|e_{10}\rangle = |0101\rangle$  e  $|e_{11}\rangle = |0110\rangle$  della base, dove abbiamo invertito la prima coppia di modi rispetto all'ordine solito, per convenienza. Fisicamente ciò si ottiene semplicemente con uno specchio. Se applichiamo un mezzo Kerr ai due modi centrali, vediamo che  $K|e_i\rangle = |e_i\rangle$  per tutti gli  $i$  a parte 11, per il quale abbiamo  $K|e_{11}\rangle = -|e_{11}\rangle$ . Ciò è utile, perché il CNOT è fattorizzabile come

$$\underbrace{\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}}_{U_{\text{CNOT}}} = \underbrace{\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{bmatrix}}_{I \otimes H} \underbrace{\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}}_K \underbrace{\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{bmatrix}}_{I \otimes H} \quad (4.34)$$

dove  $H$  è la porta Hadamard per un qubit singolo e  $K$  è la trasformazione Kerr appena vista. Quindi, usando sfasatori, divisori di fascio e mezzi Kerr è possibile creare qualsiasi porta quantistica, anche a più qubit, sfruttando l'universalità della porta CNOT insieme alle porte a qubit singolo.

### 4.3.3 Problematiche

I fotoni sono relativamente semplici da creare e da misurare, e grazie a sfasatori e divisori di fascio è possibile creare porte a qubit singolo senza troppi problemi. Purtroppo, però, i mezzi Kerr non lineari disponibili sono molto deboli (cioè  $\chi$  è molto piccolo), e quindi non riescono a creare una modulazione di fase incrociata di  $\pi$ , perché dovrebbero essere lunghi  $L = \pi/\chi$ , ma sono molto assorbenti e i fotoni singoli non riescono ad attraversarli. Ciò è un problema intrinseco dei mezzi Kerr: visto che l'indice di rifrazione non lineare è solitamente ottenuto usando un mezzo normale vicino ad una risonanza ottica, c'è sempre un assorbimento dovuto alla non linearità. Nel caso migliore, è stato stimato teoricamente che circa 50 fotoni (in media) verrebbero assorbiti prima di riuscire a ottenere un fotone con modulazione di fase  $\pi$ , rendendo questo modello molto svantaggioso quando si tratta di porte a più qubit.

Sebbene i fotoni ottici non siano quindi molto adatti alla computazione quantistica a più qubit, la comunicazione ottica è un'applicazione molto importante, grazie ai notevoli risparmi di energia rispetto alla comunicazione classica. I qubit ottici potrebbero quindi tornare utili nella trasmissione di informazione quantistica, come per esempio nel caso della crittografia quantistica, piuttosto che nella computazione vera e propria.

## 4.4 Trappole ioniche

Gli spin di elettroni e nuclei sono potenzialmente una buona rappresentazione dei qubit. Purtroppo la differenza di energia tra i vari stati con diverso spin è molto bassa rispetto per esempio all'energia cinetica degli atomi a temperatura ambiente, rendendo questi stati difficili da osservare e manipolare. Tuttavia è possibile creare un ambiente adatto ai nostri scopi, per esempio isolando in trappole elettromagnetiche un piccolo numero di atomi e raffreddandoli in modo che la loro energia cinetica sia molto inferiore al contributo dello spin. Per cambiare gli stati dei nuclei si può poi usare della luce monocromatica con una particolare lunghezza d'onda.

### 4.4.1 Apparato fisico

L'apparato sperimentale principale è costituito da una trappola elettromagnetica formata da quattro elettrodi cilindrici, come mostrato in Figura 4.1.

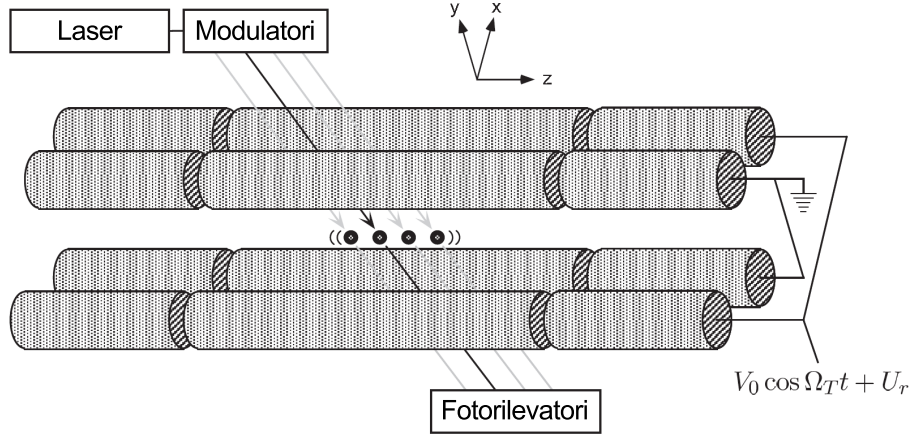


Figura 4.1: Disegno non in scala di una trappola ionica con quattro ioni. L'apparato è solitamente contenuto in vuoto ultra alto ( $\approx 10^{-8}$  Pa).

I segmenti alle estremità, diversamente dal segmento centrale, sono caricati a un potenziale  $U_0$  in modo che gli ioni siano confinati dal potenziale statico

$$\Phi_{\text{dc}} = kU_0 \frac{z^2 - (x^2 + y^2)}{2} \quad (4.35)$$

lungo l'asse  $\hat{z}$  ( $k$  è un fattore geometrico). Tuttavia il teorema di Earnshaw [12] afferma che una carica elettrica non può essere confinata in tre dimensioni usando solamente potenziali statici. Quindi per riuscire nel confinamento, due elettrodi sono posti a massa, e gli altri due sono sottoposti a un potenziale oscillante che crea un potenziale a radiofrequenza (RF)

$$\Phi_{\text{rf}} = \frac{V_0 \cos \Omega_T t + U_r}{2} \left( 1 + \frac{x^2 - y^2}{R^2} \right), \quad (4.36)$$

dove  $R$  è un fattore geometrico. I segmenti degli elettrodi sono connessi tra di loro capacitivamente in modo che il potenziale RF sia costante tra di loro. I due potenziali  $\Phi_{\text{dc}}$  e  $\Phi_{\text{rf}}$  creano, in media su  $\Omega_T$ , un potenziale armonico in  $x$ ,  $y$  e  $z$ . Insieme alla repulsione coulombiana tra gli  $N$  ioni otteniamo quindi l'hamiltoniana

$$H = \sum_{i=1}^N \left[ \frac{M}{2} \left( w_x^2 x_i^2 + w_y^2 y_i^2 + w_z^2 z_i^2 + \frac{|\vec{p}_i|^2}{M^2} \right) + \sum_{j>i} \frac{e^2}{4\pi\epsilon_0 |\vec{r}_i - \vec{r}_j|} \right], \quad (4.37)$$

dove  $M$  è la massa di ogni ione, e tipicamente  $w_x, w_y \gg w_z$  per costruzione, in modo che gli ioni siano allineati lungo l'asse  $\hat{z}$ .

Il moto degli ioni confinati elettromagneticamente diviene quantizzato quando è sufficientemente "isolato". Come abbiamo visto, l'energia dei livelli di un oscillatore armonico è egualmente spaziata in unità di  $\hbar\omega_z$ . Nel regime della trappola ionica che ci interessa, questi autostati dell'energia rappresentano i vari modi vibrazionali dell'intera catena lineare di ioni, che si comporta come un unico corpo di massa  $NM$ . Questi modi sono chiamati solitamente *modi del centro di massa*. Ogni quanto  $\hbar\omega_z$  di energia vibrazionale viene chiamato *fonone*, e può essere visto come una particella analoga al fotone.

Per essere valida, questa descrizione ha dei criteri da rispettare. L'accoppiamento con l'ambiente deve essere sufficientemente piccolo in modo che la termalizzazione non renda casuale lo stato del sistema (facendolo comportare in modo classico). I campi elettrici e magnetici fluttuanti nelle vicinanze della trappola agiscono sugli ioni, causando transizioni casuali tra gli autostati dell'energia. Tecnicamente questi rumori di sottofondo sono quasi inevitabili, ma possono essere controllati abbastanza bene in modo che non riscaldino o sfasino gli ioni eccessivamente almeno per la durata dell'esperimento. Man mano che i processi aumentano la casualità, le proprietà quantistiche dello stato degli ioni sono perse, e il loro comportamento viene descritto dalla statistica classica.

Un altro fattore importante è la temperatura degli ioni: devono essere abbastanza freddi perché valga l'approssimazione armonica monodimensionale, in quanto il vero potenziale è non-quadratico per posizioni troppo distanti dal centro della trappola. Se ciò non valesse, le transizioni a stati di energia superiore non avverrebbero tramite assorbimento di fononi del centro di massa. Per raggiungere il limite necessario  $k_B T \ll \hbar\omega_z$ , dove  $T$  è la temperatura collegata all'energia cinetica degli ioni, si usano principalmente due metodi: il raffreddamento Doppler, basato appunto sull'effetto Doppler, seguito dal raffreddamento a bande laterali.

Infine bisogna soddisfare il *criterio di Lamb-Dicke*, ovvero la larghezza dell'oscillazione degli ioni nella trappola di potenziale deve essere piccola rispetto alla lunghezza d'onda della luce incidente (luce usata per modificare o leggere lo stato degli ioni). Ciò permette ai singoli ioni di essere risolti (cioè distinti) da raggi laser diversi senza rendere troppo difficile eccitare otticamente gli stati per eseguire operazioni logiche. Questo criterio è quantificato dal parametro di Lamb-Dicke

$$\eta \equiv kz_0 = \frac{2\pi}{\lambda} \sqrt{\frac{\hbar}{2NM\omega}}, \quad \eta \ll 1, \quad (4.38)$$

dove  $k$  è il numero d'onda e  $z_0$  è una scala di lunghezza caratteristica della distanza tra gli ioni nella trappola.

### 4.4.2 Hamiltoniana

Consideriamo un sistema di spin a due livelli che interagisce con un campo elettromagnetico. L'hamiltoniana sarà

$$H_I = -\vec{\mu} \cdot \vec{B} , \quad (4.39)$$

dove  $\vec{\mu} = \mu_m \vec{S} = -g\mu_b \vec{S}/\hbar$  è il momento di dipolo di spin ( $\mu_b$  è il magnetone di Bohr e  $g$  è il fattore di Landè). Il campo magnetico è  $\vec{B} = B_1 \hat{x} \cos(kz - \omega t + \varphi)$ , dove  $B_1$  rappresenta l'intensità del campo. Gli operatori di spin sono  $S_x = X/2$ ,  $S_y = Y/2$  e  $S_z = Z/2$ , dove  $X$ ,  $Y$  e  $Z$  sono gli operatori di Pauli già visti in precedenza.

Oltre all'interazione elettromagnetica, ci sono interazioni con i modi vibrazionali. Il sistema è confinato spazialmente da un potenziale armonico con scala di energia  $\hbar\omega_z$ , quindi la sua posizione è quantizzata e possiamo descriverla con un operatore  $z = z_0(a^\dagger + a)$  dove  $a^\dagger$  e  $a$  rappresentano gli operatori di creazione e distruzione dei fononi (cioè gli operatori di alzamento e abbassamento dei modi vibrazionali).

Assumiamo che la particella sia raffreddata fino al modo vibrazionale più basso, in modo che il parametro di Lamb-Dicke  $\eta \equiv kz_0$  sia piccolo. Definendo la *frequenza di Rabi* [13] dello spin come

$$\Omega = \frac{\mu_m B_1}{2\hbar} , \quad (4.40)$$

e sapendo che  $S_x = (S_+ + S_-)/2$ , dove  $S_+$  e  $S_-$  sono gli operatori di creazione e distruzione dello spin, è possibile ricavare l'hamiltoniana nell'approssimazione  $\eta$  piccolo:

$$H_I \approx \left[ \frac{\hbar\Omega}{2} (S_+ e^{i(\varphi-\omega t)} + S_- e^{-i(\varphi-\omega t)}) \right] + \left[ i \frac{\eta\hbar\Omega}{2} \{S_+ a + S_- a^\dagger + S_+ a^\dagger + S_- a\} (e^{i(\varphi-\omega t)} - e^{-i(\varphi-\omega t)}) \right] . \quad (4.41)$$

La prima parentesi è dovuta all'*hamiltoniana di Jaynes-Cummings* [14], che descrive l'interazione tra il sistema di spin a due livelli e la radiazione elettromagnetica. La seconda parentesi descrive invece l'accoppiamento dello stato cinetico dello ione con il suo stato di spin. I quattro termini nelle parentesi graffe corrispondono a quattro transizioni (due su e due giù) note come *bande cinetiche rosse e blu*, mostrate in Figura 4.2.

### 4.4.3 Computazione quantistica

**Operazioni a qubit singolo:** Applicando un campo elettromagnetico con frequenza  $\omega_0$  il termine interno al sistema dell'hamiltoniana diventa

$$H_I^{\text{interna}} = \frac{\hbar\Omega}{2} (S_+ e^{i\varphi} + S_- e^{-i\varphi}) . \quad (4.42)$$

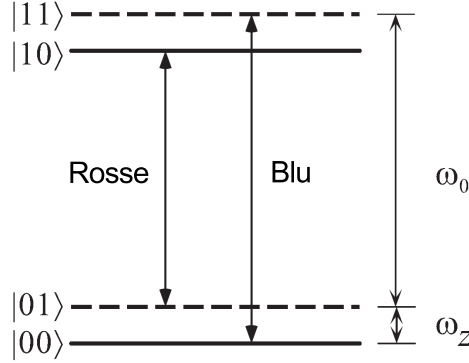


Figura 4.2: Livelli energetici dello ione intrappolato che mostrano le transizioni cinetiche "rosse e blu", che corrispondono alla creazione o distruzione di un singolo fonone. Gli stati sono etichettati come  $|n, m\rangle$  dove  $n$  rappresenta lo stato di spin e  $m$  è il numero di fononi.

Scegliendo opportunamente  $\varphi$  e la durata dell'interazione, ciò permette di eseguire le operazioni di rotazione

$$R_{xj}(\theta) = e^{-i\theta S_x} \quad \text{e} \quad R_{yj}(\theta) = e^{-i\theta S_y} , \quad (4.43)$$

dove il pedice  $j$  indica il  $j$ -esimo ione. Come già visto in precedenza, grazie a queste due rotazioni è possibile eseguire qualsiasi operazione a qubit singolo.

**Invertitore di fase controllato:** Consideriamo ora un qubit mappandolo nello stato dello spin e un altro qubit mappandolo negli stati  $|0\rangle$  o  $|1\rangle$  del fonone. In questo caso, è possibile eseguire un'inversione di fase controllata (ovvero una porta Z controllata), con la trasformazione unitaria

$$C_j(Z) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix} . \quad (4.44)$$

Per vedere come eseguire questa trasformazione, presupponiamo che l'atomo abbia un terzo livello energetico, come mostrato in Figura 4.3. Questo livello non è fisicamente necessario, ma rende la spiegazione concettualmente più semplice. Impostiamo la frequenza di un laser a  $\omega_{\text{aux}} + \omega_z$ , per indurre transizioni tra gli stati  $|20\rangle$  e  $|11\rangle$ , rappresentate da  $S'_+$  e  $S'_-$ . Il termine dell'hamiltoniana di questa interazione è

$$H_{\text{aux}} = i \frac{\eta \hbar \Omega'}{2} (S'_+ e^{i\varphi} + S'_- e^{-i\varphi}) . \quad (4.45)$$

Applichiamo il laser con fase e durata tali da causare un impulso di  $2\pi$ , cioè una rotazione  $R_x(2\pi)$  nel sottospazio generato dallo span di  $|20\rangle$  e  $|11\rangle$ , che è semplicemente la



trasformazione unitaria  $|11\rangle \rightarrow -|11\rangle$ . A causa della selettività della frequenza, nessuna altra transizione si verifica, e quindi gli altri stati rimangono invariati, realizzando la trasformazione di fase  $C_j(Z)$  voluta.

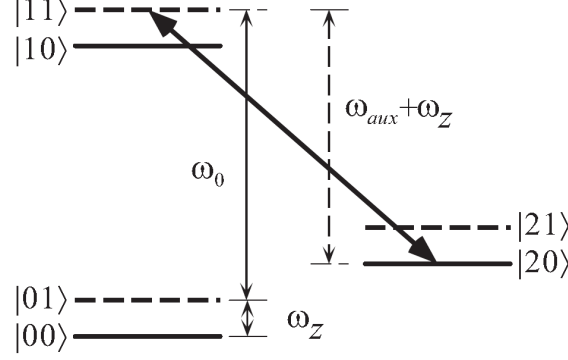


Figura 4.3: Livelli energetici di uno ione a tre livelli. Gli stati sono etichettati come  $|n, m\rangle$  dove  $n$  rappresenta lo stato dell'atomo e  $m$  è il numero di fononi.

**Porta di scambio:** Infine, per realizzare una porta CNOT, è necessaria una porta che scambi lo stato del qubit legato allo spin dell'atomo con quello del qubit legato al fonone. Ciò si può fare semplicemente impostando un laser alla frequenza  $\omega_0 - \omega_z$  e utilizzando la fase giusta; il risultato sarà una rotazione  $R_y(\pi)$  sul sottospazio generato dallo span di  $|01\rangle$  e  $|10\rangle$ , corrispondente alla trasformazione unitaria

$$\text{SWAP}_j = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}. \quad (4.46)$$

Il pedice  $j$  indica, come nel caso delle altre porte, che la trasformazione viene eseguita sullo ione  $j$ -esimo. L'operazione inversa, che corrisponde a una rotazione  $R_y(-\pi)$ , è chiamata  $\overline{\text{SWAP}}_j$ .

**Porta CNOT:** Usando due ioni si può creare una porta CNOT utilizzando le porte appena viste, implementando un circuito che realizzi la trasformazione:

$$\text{CNOT}_{jk} = H_k \overline{\text{SWAP}}_k C_j(Z) \text{SWAP}_k H_k, \quad (4.47)$$

dove  $j$  rappresenta lo ione di controllo e  $k$  lo ione bersaglio della porta. L'ordine è quello matriciale (quindi gli operatori vengono applicati da destra a sinistra).

#### 4.4.4 Problematiche

Tra gli svantaggi di questo modello rientrano tutte le difficoltà viste nel creare gli stati iniziali, che bisogna mantenere coerenti almeno per la durata dell'esperimento. Bisogna raffreddare gli ioni a temperature bassissime, e sebbene ci siano tecniche per fare ciò (il raffreddamento Doppler seguito dal raffreddamento a bande laterali [15]), sono comunque poco pratiche da realizzare. Bisogna inoltre evitare rumori di fondo da campi elettromagnetici nelle vicinanze, che rendono breve la vita dei fononi del centro di massa degli ioni.

Nel 1995 è stato eseguito un esperimento al National Institute of Standards and Technology, situato a Boulder, in Colorado [16]. In questo esperimento sono state sfruttate le trappole ioniche per realizzare con successo una porta CNOT. Purtroppo in questo caso la porta non servirebbe per la computazione quantistica, in quanto è stata creata usando un solo ione (quindi usando delle trasformazioni diverse da quelle appena viste), mentre in generale per poter eseguire dei calcoli sono necessari almeno due ioni.

Tuttavia nulla vieta di aumentare il numero di ioni del sistema, in questo modello di implementazione, se non difficoltà di ordine tecnologico, e quindi presumibilmente risolvibili in futuro.

### 4.5 Altri modelli e risultati recenti

Durante gli anni sono state proposte moltissime implementazioni possibili per la computazione quantistica. Per esempio sfruttando la risonanza magnetica nucleare di molecole in soluzione, i circuiti superconduttori, alcune particolari imperfezioni nei diamanti, i condensati di Bose-Einstein o la risonanza paramagnetica elettronica nel fullere. Tuttavia molti di questi modelli, seppur funzionino bene per pochi qubit, incontrano vari problemi tecnici quando si cerca di aumentare il numero di qubit del sistema.

Uno dei risultati recenti più importanti è stato pubblicato su Nature a ottobre del 2015 [17]. In questo articolo, scritto nel novembre 2014, viene proposta l'implementazione di un qubit nello spin di un elettrone singolo associato a un transistor. Questa implementazione sfrutta componenti tecnologici già molto ben conosciuti, ovvero i transistor CMOS al silicio, semplicemente associando un unico elettrone ad ogni transistor. Usando due qubit implementati in questo modo sono state create porte CNOT ed è stato dimostrato che era possibile "eseguire" oltre 100 porte in un tempo di coerenza dei due qubit di  $8\mu s$ , un tempo sufficientemente grande per rendere il sistema *scalabile*, ovvero valido per creare un computer quantistico con un grande numero di qubit. Lo spin degli elettroni (e quindi lo stato dei qubit) può essere manipolato semplicemente applicando tensioni diverse ai *gate* dei transistor, che indirizzano anche i vari qubit, rendendo il sistema sufficientemente accessibile.

L'enorme esperienza nel campo dell'ingegneria dei transistor potrebbe quindi essere sfruttata (sebbene occorra un riadattamento per i circuiti quantistici) a vantaggio di questo modello, rendendo l'idea di un computer quantistico accessibile molto più concreta e realistica. Lo stesso Dzurak, uno dei fisici coinvolti nell'esperimento, stima che sarebbe possibile realizzare un chip con decine o addirittura centinaia di qubit di questo tipo entro i prossimi anni, con opportuni investimenti in questo campo di ricerca.

## 4.6 Conclusioni

La computazione quantistica potrebbe essere il prossimo grande passo nella storia del progresso tecnologico, un passo che potrebbe rivoluzionare la nostra vita di tutti i giorni, proprio come i computer classici hanno già fatto. I computer quantistici probabilmente non potranno sostituire completamente la loro controparte classica, in quanto gli algoritmi quantistici sono indirizzati per la maggior parte verso una categoria particolare di problemi, ovvero quelli che vengono ritenuti senza soluzione efficiente su computer classici. Probabilmente i computer del futuro saranno dotati sia di bit che di qubit, sfruttando i vantaggi di entrambi per rimediare ai propri svantaggi.

Infinite applicazioni aspettano solamente di essere scoperte, e i campi possibili spaziano dalla fisica quantistica alla chimica, passando per la medicina e l'economia. Purtroppo inventare algoritmi quantistici è tutt'altro che semplice, e i problemi tecnici dei vari modelli che cercano di implementare i qubit sono degli ostacoli notevoli, ma sperabilmente superabili.

La strada è ancora lunga, e siamo appena agli inizi.

# Bibliografia

- [1] Alan Turing. On computable numbers, with an application to the Entscheidungsproblem. *Proc. London Math. Soc.*, 42:230–265, 1936.
- [2] Mikhail J. Atallah. *Algorithms and Theory of Computation Handbook*. CRC Press, 1999.
- [3] Gordon Moore. Cramming more components onto integrated circuits. *Electronics Magazine*, 1965.
- [4] Peter Shor. Algorithms for quantum computation: Discrete log and factoring. *Proceedings of the 35th Annual Symposium on the Foundations of Computer Science*, 1994.
- [5] Lov K. Grover. A fast quantum mechanical algorithm for database search. *Proceedings, 28th Annual ACM Symposium on the Theory of Computing*, 1996.
- [6] Paul Dirac. *I principi della meccanica quantistica*. Bollati Boringhieri, 1971.
- [7] Monroe; Meekhof; King; Itano; Wineland. Physical review letters 75(25):4714-4717, 1995.
- [8] Wootters; Zurek. A single quantum cannot be cloned. *Nature*, 299, 1982.
- [9] Rivest; Shamir; Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21, 1978.
- [10] T. Lunghi; J. Kaniewski; F. Bussi eres; R. Houlmann; M. Tomamichel; A. Kent; N. Gisin; S. Wehner; H. Zbinden. Physical review letters 111, 180504, 2013.
- [11] M. Mohseni; A.T. Rezakhani; D.A. Lidar. Quantum Process Tomography: resource analysis of different strategies. *Phys. Rev. A*, 77, 032322, 2008.
- [12] Samuel Earnshaw. On the nature of the molecular forces which regulate the constitution of the luminiferous ether. *Trans. Camb. Phil. Soc.*, 7, 1842.

- [13] H. Yokoyama; K. Ujihara. *Spontaneous emission and laser oscillation in microcavities*. Boca Raton: CRC Press, 1995.
- [14] E.T. Jaynes. Comparison of quantum and semiclassical radiation theories with application to the beam maser. *Proc. IEEE*, 51, 1963.
- [15] V. Vuletić; H.W. Chan; A.T. Black. Three-dimensional cavity Doppler cooling and cavity sideband cooling by coherent scattering. *Physical Review A*, 64, 033405, 2001.
- [16] Monroe; Meekhof; King; Itano; Wineland. Demonstration of a fundamental quantum logic gate. *Physical Review Letters*, 75, 4714, 1995.
- [17] Veldhorst; Yang; Hwang; Huang; Dehollain; Muhonen; Simmons; Laucht; Hudson; Itoh; Morello; Dzurak. A two-qubit logic gate in silicon. *Nature*, 526, 2015.
- [18] M.A. Nielsen; I.L. Chuang. *Quantum computation and quantum information*. Cambridge, 2000.
- [19] John Preskill. Lecture notes for physics 229: Quantum information and computation, 1998.

# Ringraziamenti

Colgo quest'occasione per ringraziare il mio relatore Fabio Ortolani per le idee e il supporto ricevuti durante la stesura della tesi; tutto il corpo didattico della facoltà di Fisica e tutto il personale universitario in generale per aver reso possibili questi tre anni di insegnamento.

Ringrazio i miei genitori Romana e Lelio, mia sorella Sara e tutti i membri della mia famiglia per tutto il bene e l'amore che mi danno tutti i giorni.

Ringrazio tutti i miei amici per avermi fatto divertire in questi anni, e in particolare i miei compagni nelle campagne di Pathfinder. Un grazie speciale a Valentina per i momenti indimenticabili che mi ha donato, e a mio cugino Filippo che è come un fratello per me.

Ringrazio anche i miei colleghi stretti Michele, Serena, Elisa e Massimo per avermi fatto compagnia (e passato gli appunti) in questi tre anni insieme.

Infine vorrei ringraziare la Fisica, che mi meraviglia continuamente e stuzzica la mia curiosità tutti i giorni.