Indice

CAPITOLO 1

Prefazione

Informatica quantistica è forse la novità più entusiasmante dopo la produzione dei primi calcolatori universali da quando il modello di Alan Turing è stato concretamente implementato in una macchina elettronica.

Lo sviluppo e la ricerca dell'intelligenza artificiale, e in generale della scienza della computazione, hanno condotto gli sforzi della ricerca a cercare soluzioni sempre più ottimizzate per rispondere alle grandi domande provenienti sia dal mondo accademico che dalle esigenze della società, la quale ha visto nella potenza del calcolo informatico una possibile soluzione ai diversi problemi concreti. Per esempio, la possibilità di prevedere la

forma presa da una sequenza amminoacidi, cioè di prevedere la forma di una proteina, può fare risparmiare interi decenni nella ricerca di una molecola contro una determinata patologia.
Purtroppo questo tipo di calcoli si è rivelato spesso computazionalmente troppo costoso anche per le macchine più sofisticate di cui disponiamo in questo terzo decennio nel terzo millennio. L'informatica quantistica, col suo parallelismo intrinseco, promette nuove soluzioni a vecchi problemi e, sebbene si sia già dimostrato che alcune classi di problemi non potranno essere particolarmente migliorate da questo nuovo paradigma di calcolo, è vero che la computazione quantistica potrebbe rivelarsi assolutamente innovativa per tutti quei calcoli che sono intrinsecamente quantistici.

Questo testo è preliminare allo studio della computazione quantistica. Il concetto di qubit è assolutamente alla base dell'informatica e della computazione quantistica e senza comprendere questo non è possibile comprendere il significato di parallelismo ed entanglement, pertanto questo libro è indicato a tutti coloro che intendono iniziare questo percorso, specie se

autodidatti, e lo vogliono fare nel modo migliore possibile.

CAPITOLO 2

Introduzione: dai bits ai qu-bits

L'innovazione tecnologia ha dominato e continua a dominare lo scenario sociale ormai da due secoli. Se nell'Ottocento è stata la meccanica la regina della scena, il Novecento e questi primi due decenni del terzo millennio vedono l'elettronica e l'informatica come dominatrice incontrastata.

L'idea di costruire un calcolatore universale, capace di eseguire qualsiasi algoritmo[8] conduce rapidamente alla nascita e all'evoluzione della teoria informatica che formalizza il concetto di informazione trattandone la produzione, la trasformazione e la

ricezione[7]. Turing e Shannon sono fra in principali protagonisti di questa epopea, ma altre personalità, come ad esempio Von Neumann, giocano ruoli cruciali che a volte rimangono nell'ombra. Ciò non di meno è stata proprio da queste zone d'ombra che una evoluzione impensata dell'informatica ha preso vita portando poi alla nascita della computazione quantistica.

L'elemento chiave delle teoria dell'informazione di Shannon è lo stesso che si trova nella teoria della computazione di Turing, cioè l'idea di un alfabeto che codifica l'informazione. Nei trattati teorici l'alfabeto può essere un qualsiasi insieme di simboli, nella implementazione concreta c'è bisogno di identificare dei simboli che non prevedano capacità cognitive per essere riconosciuti. Uno dei primi ad affrontare questo problema sul piano pratico e proprio Von Neumann che, nel suo report *First Draft of a Report on EDVAC*, propone di usare un sistema digitale binario (bit) per la codifica dell'alfabeto.

La realizzazione di una memoria formata di bit è una sfida sia scientifica che tecnologica. Aver ridotto l'alfabeto a due soli simboli ha semplificato il problema dal punto di vista concettuale e ha permesso di pensare i circuiti dell'EDVAC in termini di porte logiche e quindi di progettare fattivamente il centro

computazionale del computer, ma ancora non ha risolto il problema di come memorizzare i simboli alfabetici, cioè lo 0 e l'1, per poterli leggere e scrivere durante la computazione. Una delle prime soluzioni efficienti a questa sfida è stata la memoria basata su nuclei magnetici. Oggi, nel 2021, siamo abituati a comprare a cifre ridotte banchi di memoria da diversi giga bytes che occupano pochi centimetri quadrati, per questo calarsi nel problema della realizzazione dei primi sistemi di memoria a bit può essere difficile, ma è molto utile perché ci proietta in una realtà analoga a quella vissuta dai progettisti dei primi computer. Infatti, lo stesso problema che questi hanno vissuto lo stanno vivendo oggi i progettisti dei computer quantistici che si trovano ad affrontare sfide ritenute letteralmente impossibili, come ad esempio la realizzazione di un gate CNot di tipo fotonico.

Le prime memorie a bit erano basate sull'isteresi magnetica di un toroide (anello) di ferrite in cui può instaurarsi una magnetizzazione permanente.

Dallo studio del magnetismo è noto che la magnetizzazione di un nucleo toroidale di ferrite segue un certo ciclo di istere-

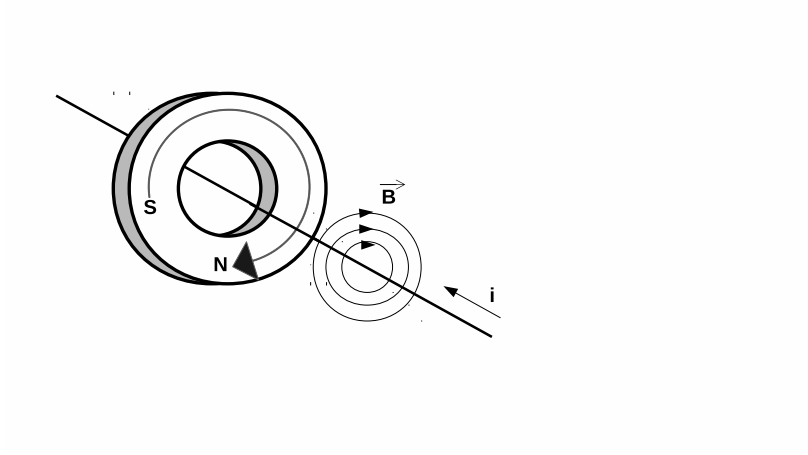

Figura 2.1: La figura mostra un nucleo di ferrite attraversato da un filo conduttore in cui è presente una corrente elettrica textbfi.

si, cioè conserva memoria della magnetizzazione. In pratica è possibile indurre una magnetizzazione permanente nel nucleo facendo passare una corrente elettrica per un filo che lo attraversa (vedi figura 2.1). Il fatto interessante è che la magnetizzazione indotta permane anche se la corrente elettrica cessa di fluire.

L'idea alla base di questo tipo di memoria è quindi quella di associare i due possibili valori del bit, cioè 0 ed 1, al verso di magnetizzazione all'interno del toroide, ottenibili variando il verso della corrente elettrica che induce la magnetizzazione, co-

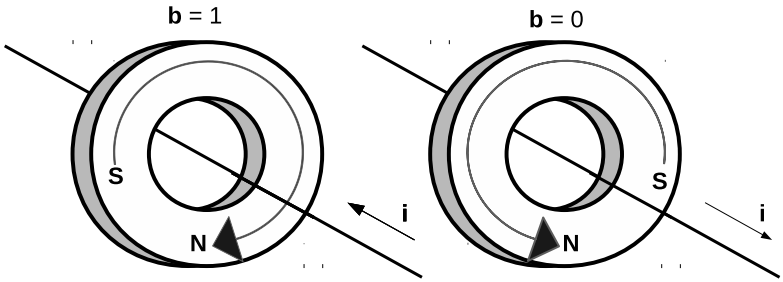

Figura 2.2: La figura mostra un nucleo di ferrite in cui è presente un campo magnetico indicato da una freccia. Nella figura a sinistra il campo magnetico è diretto in senso orario rispetto all'osservatore, mentre in quella a destra in senso antiorario. In questo schema si assume per convenzione che al senso orario sia associato il valore binario 1 (b=1), mentre a quello antiorario il valore 0 (b=0).

me mostrato in figura 2.2.

Una volta stabilita la relazione tra lo stato fisico del bit e il suo valore logico, si pone il problema di come controllare lo stato fisico per poi controllare di conseguenza il valore logico.

Nel caso delle memorie a nuclei di ferro, il campo magnetico nel toroide è controllabile per mezzo di due linee elettriche. In linea di principio basterebbe una linea elettrica per ogni bit, però questo comporterebbe che il numero di linee elettriche (fili) dovrebbe essere uguale al numero di bit, quindi per esempio

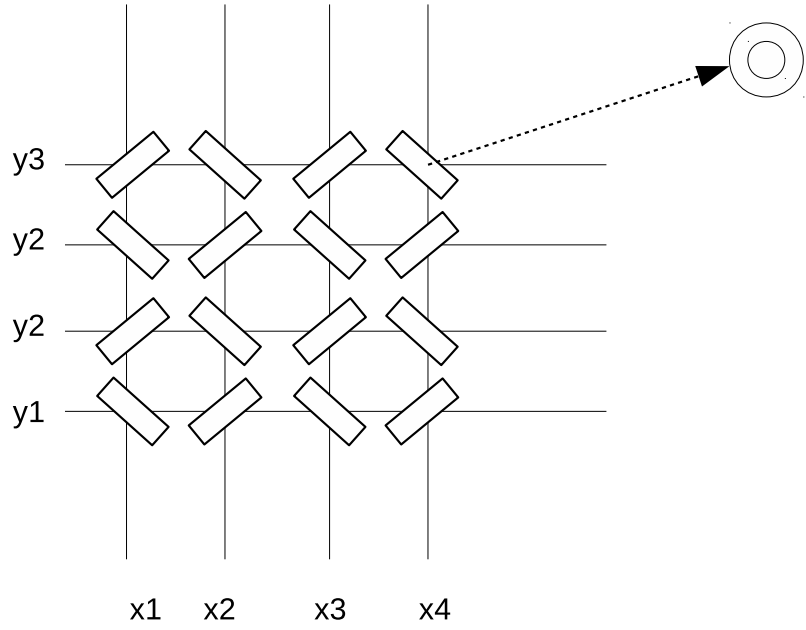

Figura 2.3: La figura mostra una schiera (array) di bits realizzati come nuclei di ferrite. Ogni bit è attraversato da due linee di corrente indicate con x e y.

ci vorrebbero 1000 fili elettrici per gestire un Kbits (chilo bit) di memoria. La soluzione alternativa, che fu realmente adottata, è quella di usare due fili per ogni bit, ma disponendo i bit in modo che un intera linea condivida lo stesso filo (vedi figura 2.3). Per modificare il valore di un bit si devono attivare simultaneamente le due linee x e y che lo attraversano, in questo modo il

campo magnetico dovuto alla corrente elettrica sarà sufficientemente intenso da modificare la magnetizzazione già presente nel relativo nucleo magnetico. Tutti gli altri nuclei magnetici presenti sulle due linee rimangono invece inalterati, perché il campo magnetico dovuto ad un singolo filo non è sufficiente a modificare la magnetizzazione del nucleo di ferrite (vedi figura 2.4).

Il vantaggio di questa tecnica è che il numero dei fili necessari al controllo dei bits di memoria scala in ragione di 2 volte la radice quadrata del numero totale di bit, quindi per esempio, sono sufficienti meno di 70 fili per controllare il kbits dell'esempio precedente. Questa breve introduzione al principio di funzionamento di una *antica* memoria digitale dovrebbe continuare spiegando il funzionamento della lettura del bit. Se è vero che l'opportuna l'attivazione delle linee x e y induce il bit ad un cambiamento di stato da 0 ad 1 e da 1 a 0, non è però stato spiegato come *leggere* il valore memorizzato. Senza entrare troppo nel dettaglio è sufficiente introdurre nel nostro schema un nuovo filo, detto filo di *sense*, questo filo attraversa tutti i bits presenti nella memoria (vedi figura 2.5) Per leggere il valore del bit si impostano i valori di corrente nelle due linee x

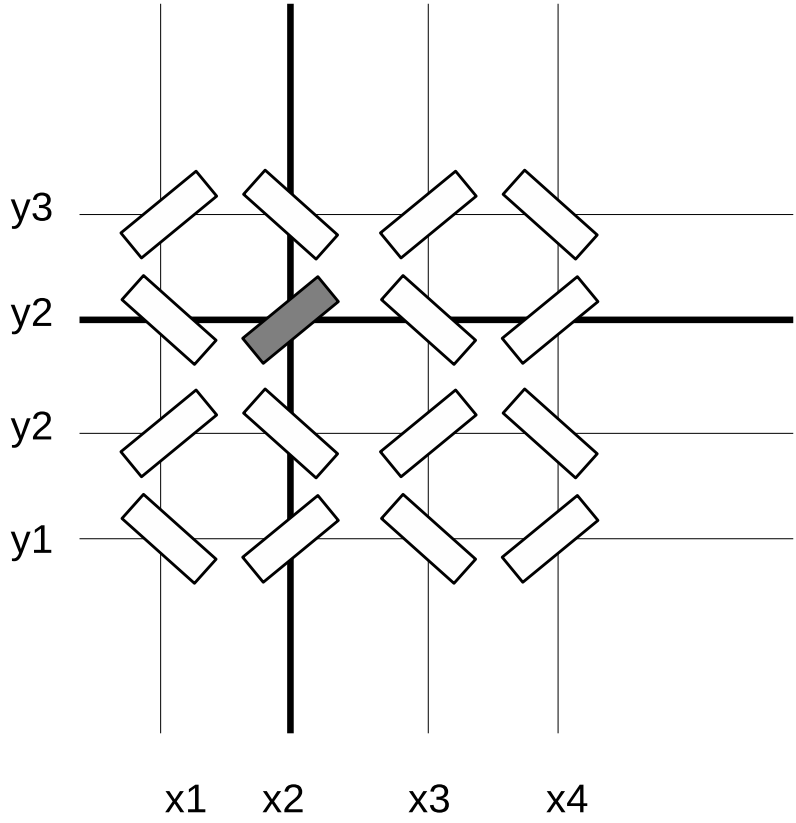

Figura 2.4: La figura mostra le linee $x1$ e $y1$ percorse da corrente e la conseguente selezione del bit che si trova in corrispondenza del loro punto di incrocio.

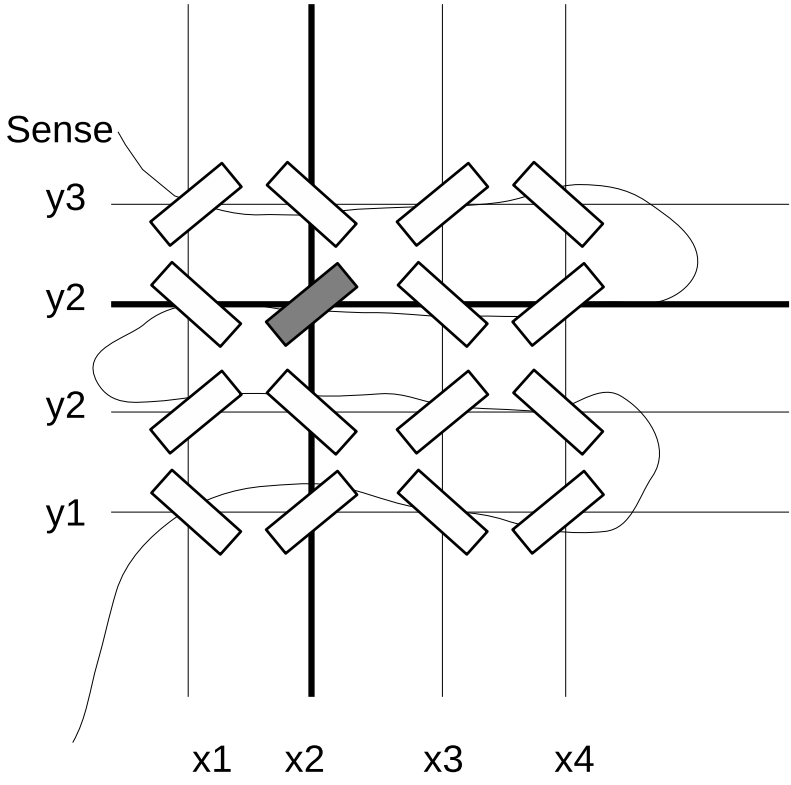

Figura 2.5: La figura mostra la linea di sense attraversare tutti i bits della memoria.

e y che lo incrociano in modo da magnetizzare il nucleo sullo 0. Se il bit corrispondente è già nello stato 0, allora non cambia nulla della sua magnetizzazione, se invece il bit è nello stato 1, la variazione del campo magnetico nel nucleo induce una corrente nel filo di *sense* che viene rilevata e quindi permette di conoscere il valore memorizzato, cioè 1. Quindi, se dopo l'operazione di misura non si misura alcuna corrente significa che nel bit era (e rimane) memorizzato uno 0, se invece si misura una corrente allora nel bit era memorizzato un 1, ma l'operazione di lettura lo ha portato a 0, quindi bisognerà ripristinare il suo valore.

L'analisi dettagliata del funzionamento della memoria digitale ha messo in evidenza la relazione tra il concetto di bit logico e la sua implementazione fisica.
L'aspetto più notevole delle memorie a nucleo magnetico è che esse sfruttano un caratteristica fisica implicitamente *discreta* e *binaria*, cioè il senso, orario o antiorario, di magnetizzazione del bit.
I qubit sfruttano una idea simile. Essi sono basati su sistemi il cui stato fisico è completamente definibile usando una combi-

nazione di due soli stati base che possiamo chiamare $|0\rangle$ e $|1\rangle$. I due stati $|0\rangle$ e $|1\rangle$ sono ben separati e distinguibili quindi, in questo senso, sono analoghi ai due versi di magnetizzazione dei bit classici visti poche righe sopra. La differenza tra i qubit e i bit classici è che mentre i bit possono trovarsi selettivamente in uno o nell'altro stato, i qubit possono essere in una sovrapposizione dei due stati fisici.

La sovrapposizione di stati fisici è un concetto assai diverso dalla scomposizione dei vettori lungo le coordinate e i due non vanno confusi. Questo concetto è alla base nell'attuale computazione quantistica ed è ciò che permette il *parallelismo intrinseco* di questo paradigma computazionale.

È bene sapere che i vantaggi della computazione quantistica non sono ancora del tutto chiari e la ricerca in questa affascinante disciplina è solo all'inizio.

Il percorso che sta per iniziare è ricco di elementi interessanti che per molti lettori risulteranno assolutamente nuovi. Per apprezzare a pieno i concetti che verranno via via incontrati, è però necessario un bagaglio di matematica che spesso non viene fornito nelle scuole superiori. Per questo motivo, si chiede

al lettore di armarsi di pazienza, di carta e di penna e di completare lo studio degli elementi di matematica presentati nella prima sezione del testo. Questi gli permetteranno di affrontare il proseguo con serenità e consapevolezza.

Buona lettura.

Parte I

Concetti matematici

Introduzione

Per comprendere e usare la computazione quantistica è necessaria un po' di matematica, ma questa non è in complicata in sé, infatti si riduce ad addizioni, moltiplicazioni ed una base di nozioni di trigonometria elementare, operazioni e concetti che normalmente vengono apprese alle scuole superiori. A queste nozioni si devono aggiungere l'algebra dei numeri complessi e un minimo di algebra delle matrici.

Visto che questi ultimi argomenti non vengono di norma trattati alle scuole secondarie, questi concetti e il loro utilizzo, sono illustrati nella prima parte di questo libro.

CAPITOLO 3

I numeri complessi

3.1 Cosa sono i numeri complessi

Quando si pensa ad un numero si pensa ad una quantità: ad esempio il numero 1 esprime la quantità di satelliti naturali posseduti dalla Terra, mentre il numero π esprime il rapporto tra la lunghezza della circonferenza ed il suo diametro.
Le proprietà delle operazioni algebriche sono definite in modo formale, ma sono generalmente intuitive. Se si pensa alle proprietà delle potenze o dei radicali, queste possono essere comprese in modo semplice e diretto facendo qualche esempio numerico. Per esempio per convincersi della validità della regola

del quadrato di un binomio si puó fare una prova numerica:

$$(1+2)^2 = 1^2 + 2^2 + 2 \times 1 \times 2 = 1 + 4 + 4 = 9$$

risultato che avremmo ottenuto anche eseguendo prima la somma tra parentesi:

$$(1+2)^2 = (3)^2 = 9$$

È naturale trovare assurdo che il quadrato di un numero possa essere negativo: cioè che esista un numero i per cui valga la proprietà seguente:

$$i \times i = i^2 = -1$$

se un numero siffatto esistesse, diremmo che esso **non** è reale.

L'unità immaginaria Se rinunciamo al principio di *realtà*, ovviamente tutto diventa possibile. Per esempio diventa possibile introdurre delle regole algebriche *consistenti*[1] che prevedano anche l'esistenza del numero i il cui quadrato è -1.

Il numero$i$ è detto *unità immaginaria*

[1] Regole consistenti significa che sono coerenti con dei postulati che possono anche non aver corrispondenza nella realtà. Supporre che per due punti passi una sola rette ci porta a considerazioni consistenti, anche se il concetto di punto è astratto e non esiste nella realtà. Supporre invece che un numero sia divisibile per zero non ci porta a considerazioni consistenti.

Definiamo un nuovo tipo di numero che chiameremo *complesso*. Questo è composto dalla somma di una parte reale ed una parte immaginaria, per esempio:

$$z = 3 + i \times 5$$

è il numero complesso z che ha parte reale uguale a 3 e parte immaginaria uguale a 5. D'ora in avanti eviteremo di usare il simbolo della moltiplicazione, e scriveremo più semplicemente: $z = 3 + i5$.

Corrispondenza reali e complessi Un numero complesso può avere parte immaginaria uguale a zero. Per esempio consideriamo il numero:

$$z = 3 + i0$$

Il coefficiente che moltiplica l'unità immaginaria i è uguale a 0, quindi diremo che z ha parte immaginaria pari a 0 mentre la parte reale è uguale a 3. Tra il numero complesso $3 + i0$ e il numero reale 3 esiste quindi una corrispondenza biunivoca. Questa corrispondenza vale per tutti i numeri complessi con parte immaginaria nulla (cioè pari a 0), per essi esiste una corrispondenza biunivoca con i numeri reali.

La corrispondenza tra i numeri complessi che hanno parte immaginaria nulla ha conseguenze di tipo pratico ed operativo, cioè i numeri complessi con parte immaginaria nulla, possono essere: sommati, sottratti, moltiplicati ecc. come se fossero numeri reali.

3.2 Perchè vengono introdotti nella matematica i numeri complessi

Per capire il perchè questi numeri vengono introdotti, consideriamo la seguente equazione algebrica:

$$x + 2x = -3$$

Nel membro di sinistra compare un monomio in x di primo grado, mentre a destra compare il numero *reale* -3. L'equazione ha una soluzione reale $x = 1$. Si consideri ora l'equazione

$$x^4 - 3x^2 + 2 = 0$$

che ha quattro soluzioni reali distinte: 1, -1, 2 e -2.
In generale ci si aspetta che esistano tante soluzioni quanto è il grado dell'equazione. Si consideri però l'equazione seguente:

$$x^2 = -1$$

ovviamente questa equazione non ha soluzione, perché il quadrato di qualsiasi numero reale è sempre una quantità positiva. L'equazione ha però soluzione se si rinuncia a cercarla tra i numeri reali e la si cerca tra i numeri complessi. La soluzione dell'equazione è infatti il numero complesso $z = 0 + i$, cioè l'unità immaginaria.
Senza pretesa di rigore, si può pensare che i numeri complessi siano stati introdotti in modo che una equazione algebrica di grado n abbia sempre almeno una o più soluzioni, sebbene queste saranno di tipo complesso anziché reale.

3.3 Come si rappresentano i numeri complessi

Ci sono due modi comuni per rappresentare i numeri complessi, questi sono la forma algebrica e quella trigonometrica o esponenziale. I due modi sono equiavalenti e da una rappresentazione è sempre possibile passare all'altra.

3.3.1 Forma algebrica

La forma algebrica consiste nello scrivere ogni numero complesso come la somma tra una parte reale e una immaginaria:

$$z = a + ib$$

dove a è la parte reale e b è il coefficiente reale della parte immaginaria.

Norma, modulo e complesso coniugato nella forma algebrica

Una volta data una forma ai numeri complessi possiamo definirne delle proprietà che saranno utili nel calcolo. La prima è la norma. Per un numero $z = a + ib$ questa è definita come la somma dei quadrati della parte reale e del coefficiente della parte complessa: $a^2 + b^2$. La norma è sempre un numero reale positivo.
La radice quadrata della norma: $\sqrt{a^2 + b^2}$ è invece detta essere il modulo del numero complesso z. Anch'esso è un numero reale, sempre positivo.

Dato un numero complesso $z = a + ib$ definiamo il suo comples-

so coniugato come il numero che ha parte reale a e coefficiente complesso $-b$. Per esempio il complesso coniugato di $4 + i5$ è $4-i5$, oppure il complesso coniugato di $12-i9$ è il numero $12+i9$. Il complesso coniugato di z si scrive $\bar{z}$ o come spesso faremo z^*.

3.3.2 Forma esponenziale e trigonometrica

I numeri complessi possono essere rappresentati anche in un'altra forma detta *forma trigonometrica* dei numeri complessi.
In forma trigonometrica scriviamo z come

$$z = \rho \cos\theta + i\rho \sin\theta$$

dove ρ è un coefficiente reale detto modulo. In forma esponenziale lo scriviamo come il prodotto di ρ per un esponenziale complesso:

$$z = \rho e^{i\theta}$$

. La forma trigonometrica e quella esponenziale sono concretamente la stessa cosa e vengono trattate nel seguito come un'unica forma.
Dal momento che uno stesso numero complesso può essere espresso sia in forma trigonometrica che in forma algebrica, si capisce che deve esistere una relazione tra i parametri a e b

della rappresentazione algebrica e i parametri ρ e θ della rappresentazione trigonometrica. Per comprendere tale differenza possiamo aiutarci rappresentando il numero complesso z in un piano. Dal momento che esso é definito in forma algebrica attraverso i due numeri reali a e b, possiamo associarlo al punto del piano di coordinate (a, b), come mostrato in figura 3.1. Chiameremo allora x asse reale, e y asse immaginario. Come si vede in figura 3.2, lo stesso punto può essere indicato con un vettore (freccia) di lunghezza ρ e angolo $theta$ preso rispetto all'asse delle x. Le coordinate (a, b) possono essere calcolate rispetto a (ρ, θ) come segue:

$$\begin{aligned} a &= \rho \cos\theta \\ b &= \rho \sin\theta \end{aligned} \tag{3.1}$$

Dalle equazioni 3.1 si deduce anche la relazione inversa, infatti dividendo b per a si ottiene:

$$\frac{b}{a} = \frac{\rho \sin\theta}{\rho \cos\theta} = \tan\theta \tag{3.2}$$

e quindi:

$$\theta = \arctan(\frac{b}{a}) \tag{3.3}$$

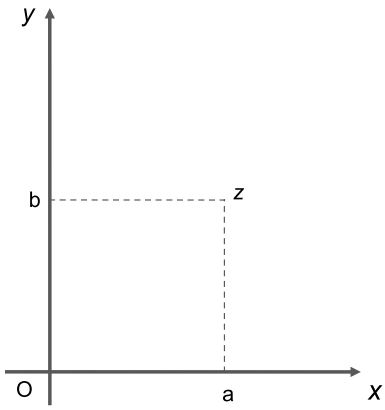

Figura 3.1: Rappresentazione del numero complesso $z = a+ib$ nel piano cartesiano.

Il modulo ρ del vettore è ottenuto sommando i quadrati dei coefficienti reali a e b:

$$\rho = \rho \sin^2 \theta + \rho \cos^2 \theta \tag{3.4}$$

Un numero complesso può quindi essere espresso equivalentemente nelle due forme algebrica o trigonometrica, anche se, come già accennato, nella meccanica quantistica e nell'informatica quantistica si predilige l'uso della seconda perchè meglio permette di evidenziare l'angolo θ.

.

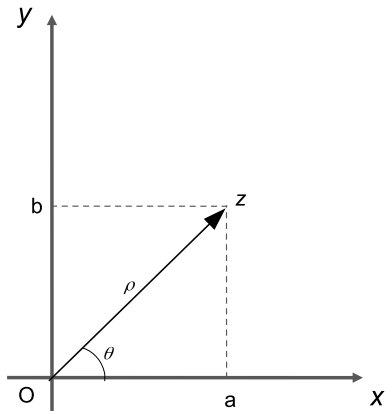

Figura 3.2: In figura sono indicati il modulo ρ e l'angolo θ del raggio vettore tracciato dall'origine O al punto z.

Norma, modulo e complesso coniugato nella forma trigonometrica

Nella rappresentazione trigonometrica, il modulo è ρ stesso, mentre la norma è semplicemente ρ^2. Il complesso coniugato di $z = \rho e^{i\theta}$ è il numero $z^* = \rho e^{-i\theta}$ ottenuto cambiando il segno dell'esponente.

La rappresentazione trigonometrica rende chiaro che il complesso coniugato di z, rappresenta il numero complesso z^* ottenuto per simmetria rispetto l'asse delle x, come mostrato in figura 3.3 È inoltre facilmente dimostrabile che il prodotto di

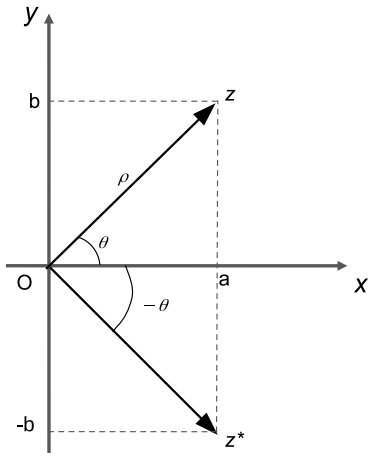

Figura 3.3: Il numero complesso z^* si ottiene per simmetria rispetto l'asse reale x.

un numero complesso per il suo complesso coniugato risulta essere la sua norma, infatti si ha:

$$zz^* = \rho e^{i\theta} \rho e^{-i\theta} = \rho^2 e^0 = \rho^2$$

3.4 I numeri complessi nell' informatica quantistica

L'informatica quantistica è un nuovo modello di computazione che sta affiancando il modello sviluppato da Alan Turing che è

alla base della ben nota informatica convenzionale.

Il modello di Turing (macchina di Turing MdT) consiste in un nastro suddiviso in celle che scorrono sotto ad una testina. Un programma consiste in una sequenza di simboli scritti sopra il nastro in corrispondenza delle celle. In base al contenuto della cella presente soto la testina, questa può ignorare la cella sottostante, oppure modificarne il simbolo contenuto, cancellandolo o rimpiazzandolo con un simbolo diverso.

Ogni calcolo riconducibile ad una funzione sui numeri naturali può essere eseguito con una macchina di Turing[2]. Per ogni istruzione, l'operazione concreta da compiere dipende dallo stato q in cui si trova la macchina e da quanto la macchina legge sotto la testina. La lettura del simbolo sotto la testina e dello stato q sono operazioni deterministiche, cioè si dà per scontato che il nastro non deteriori e che una volta impostato, lo stato non vari purché questo non sia richiesto da una istruzione.

Sebbene questo principio possa sembrare ovvio, non lo è nel mondo quantistico, dove le informazioni, come ad esempio i simboli scritti sul nastro, possono essere in sovrapposizione e

[2]Per una definizione rigorosa vedi:

https://en.wikipedia.org/wiki/Church%E2%80%93Turing_thesis

acquisire un valore determinato soltanto a seguito di una lettura.

Da questo si può intuire che l'idea secondo la quale ogni modello di calcolo sia riconducibile ad una macchina di Turing è sconfessata nel mondo quantistico, cioè per i fenomeni fisici che richiedono di essere spiegati con la meccanica quantistica. In pratica, la macchina di Turing si basa su un principio, assai intuibile e ben condiviso, cioè che i simboli, una volta scritti sul nastro, tali rimangano finché non vengono cancellati o sostituiti da un nuovi simboli. Questo principio è assolutamente normale nel mondo classico al quale siamo abituati. Per esempio quando scriviamo sopra un quaderno, nel momento in cui andiamo a leggere, ritroviamo esattamente ciò che abbiamo scritto. Ovviamente è possibile che intervengano agenti come l'usura a modificarne il contenuto. La normale usura di un quaderno può essere corretta ricopiando periodicamente il contenuto del quaderno su un altro quaderno. Questo è per esempio il lavoro che facevano i frati amanuensi nei conventi riscrivendo i codici Miniati, ma è anche la normale attività di un computer che fa manutenzione alla propria memoria.

Quindi, con le debite considerazioni fatte per la necessità della

manutenzione, rimane il fatto che ciò che è stato scritto corrisponde esattamente a ciò che verrà letto. Questo principio, che come abbiamo detto è assolutamente scontato nel mondo classico, non lo ritroviamo invece nel mondo quantistico. Per una ipotetica macchina di Turing quantistica, la testina scriverebbe un'informazione codificata in una sovrapposizione di stati fisici, ma nel momento in cui decidesse di leggere quanto ha scritto troverebbe in modo esclusivo o l'uno o l'altro stato. Quindi, in generale, ciò che scrive non corrisponde con ciò che legge. Questa violazione dei principi base su cui si basa la macchina di Turing è l'incipit per capire che la computazione classica ha in sé una breccia e quindi esiste la possibilità di esplorare oltre ad essa.

Concettualmente, nell'informatica quantistica l'insieme Q dei possibili stati in cui si può trovare la macchina, viene rappresentato da uno spazio di Hilbert su campo complesso. Per questo motivo, i numeri complessi giocano un ruolo chiave per la comprensione effettiva dell'informatica quantistica.

3.5 Esercizi

3.5.1 Esercizi risolti

- Esercizio 1: Scrivere il numero complesso z di parte reale 1 e parte immaginaria -1.

  In forma algebrica, z è scritto come: $z = 1 - i$ dove il coefficiente 1 è omesso. Lo stesso numero può essere scritto in forma trigonometrica una volta calcolati ρ e θ. Viste le equazioni 3.3 e 3.4. Si ha:

  $$\theta = \arctan\left(\frac{-1}{1}\right) = -\pi/4$$

  e

  $$\rho = \sqrt{1^2 + (-1)^2} = \sqrt{2}$$

  quindi z può essere scritto come $z = \sqrt{2}(\cos(-\pi/4) + i\sin(-\pi/4))$ o in forma esponenziale: $z = \sqrt{2}e^{-i\pi/4}$

- Esercizio 2: calcolare il complesso coniugato di $z = 1 - i$.

  Applicando direttamente la 3.5 al risultato dell'esercizio 1, si ottiene: $z^* = \sqrt{2}e^{i\pi/4}$.

3.5.2 Esercizi proposti

- Esercizio 1: si scriva l'insieme dei numeri complessi che hanno modulo ρ uguale ad 1. Che luogo geometrico individuano nel piano?

- Esercizio 2: Si scriva l'insieme dei numeri complessi che hanno argomento θ uguale a $\pi/4$. Che luogo geometrico individuano nel piano?

CAPITOLO 4

Matrici e vettori di elementi complessi

I vettori vengono introdotti nello studio delle materie scientifiche per rappresentare delle grandezze fisiche non scalari, come ad esempio la posizione di un punto nello spazio o la velocità di un corpo. Tali grandezze necessitano di specificare la direzione e il verso, per questo una semplice quantità scalare non è sufficiente. Per esempio, se si vuole indicare la posizione di un oggetto all'interno di una abitazione é possibile farlo scegliendo un angolo dell'abitazione come origine e una freccia che partendo da tale origine raggiunga con la punta l'oggetto in questione.

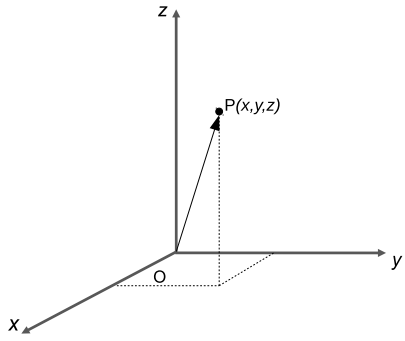

Figura 4.1: Il punto ***P*** *ha coordinate* (x, y, z) *misurate rispetto all'origine O.*

Siffatta freccia prende il nome di vettore. In matematica un vettore dello spazio viene rappresentato con una terna di numeri che corrispondono anche ad uno specifico punto. Per esempio in figura 4.1 viene indicato un punto **P** di coordinate (x, y, z). Tale terna costituisce un vettore. È importante notare che esiste una differenza tra un punto ed un vettore, infatti un punto è una unità geometrica che non cambia mai, anche se per esempio ruotiamo il piano cartesiano. La terna di coordinate x, y, z invece cambia per le rotazioni del sistema stesso.

4.1 Vettori

Se il punto **P** si trova nello spazio fisico, cioè lo stesso spazio in cui viviamo e ci spostiamo, allora le variabili x, y e z hanno valori reali, cioè non sono numeri complessi. Con uno sforzo di astrazione (assai comune in matematica) possiamo pensare al vettore solo in termini della terna di coordinate x, y e z rinunciando ad immaginarlo nello spazio. In questo modo un vettore è semplicemente l'insieme di tre variabili che assumono valore nel campo R dei numeri reali. Detto questo, nulla impedisce di considerare anche una terna di variabili che anzichè assumere valori nel campo $\mathbb{R}$, assume valori nel campo $\mathbb{C}$ dei numeri complessi. Per esempio possiamo considerare il vettore **z** di componenti complesse z_1, z_2 e z_3. Diversamente da **P** non riusciamo ad immaginare tale vettore, ma per esso valgono le stesse proprietà matematiche che valgono per i vettori con componenti reali.

Per i vettori complessi valgono alcune semplici proprietà che vediamo di seguito in modo informale.

Se **z** e **w** sono due vettori complessi, anche **z+ w** è un vettore complesso. Dato **z** esiste un vettore **z'** tale che $\mathbf{z} + \mathbf{z'} = 0$ dove 0 è l'elemento neutro additivo. Preso arbitrariamente $\lambda \in \mathbb{C}$ si ha $\lambda(\mathbf{z} + \mathbf{w}) = \lambda\mathbf{z} + \lambda\mathbf{w}$.

Come vedremo nel prossimo capitolo, un qubit è un vettore complesso di dimensione 2, quindi anzichè considerare una terna di numeri complessi, considereremo d'ora in avanti coppie di numeri complessi.

4.1.1 Prodotto scalare tra vettori complessi

Il prodotto scalare tra due vettori complessi **z** e **w** si può scrivere come segue: $\mathbf{z} \cdot \mathbf{w}$ e si calcola come la somma dei prodotti delle componenti coniugate di **z** per le componenti di **w**:

$$\mathbf{z} \cdot \mathbf{w} = \sum_i z_i^* w_i \tag{4.1}$$

Consideriamo ad esempio il vettore **z** dato da:

$$\mathbf{z} = \begin{bmatrix} 1+i \\ \\ 2+i \end{bmatrix}$$

e il vettore $\mathbf{w}$ definito come:

$$\mathbf{w} = \begin{bmatrix} 2+2i \\ 4+2i \end{bmatrix}$$

I due vettori hanno due componenti, quindi si dice che appartengono a $\mathbb{C}^2$. Seguendo la definizione data in 4.1, si ha che il loro prodotto scalare è calcolato come:

$$\begin{aligned} \mathbf{z} \cdot \mathbf{w} &= (1+i)^*(2+2i) + (2+i)^*(4+2i) = \\ &= (1-i)(2+2i) + (2-i)(4+2i) = \\ &= 2(1-i)(1+1i) + 2(2-i)(2+i) = \\ &= 2(1-i^2) + 2(4-i^2) = 14 + i0 \end{aligned}$$

4.2 Matrici

Una matrice è una tabella di numeri avente un dato numero di righe ed un dato numero di colonne.

$$\mathbf{A} = \begin{bmatrix} 1 & 2 & 1 \\ 0.1 & 1.1 & 2.8 \\ 1 & 0 & 1 \\ 2 & 21 & 12.9 \end{bmatrix} \tag{4.2}$$

La matrice mostrata in 4.2 ha 4 righe e 3 colonne. Ogni matrice è identificata dalla coppia $n \times m$ di righe e colonne, la 4.2 è

una matrice 4×3. Alle matrici si assegna un nome, per esempio **A**. I numeri nelle celle della matrice sono detti elementi della matrice e si indicano con una lettera e due indici, per esempio $a_{i,j}$ è l'elemento di riga i e colonna j della matrice **A**.

Quanto visto per i vettori vale anche per le matrici, cioè è possibile che una matrice abbia elementi complessi come la seguente:

$$\sigma_{\mathbf{y}} = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \tag{4.3}$$

Le matrici sono un elemento caratteristico della meccanica quantistica, che un tempo era anche detta *meccanica delle matrici*. Il motivo è che nella meccanica quantistica le variabili dinamiche, come ad esempio il momento angolare, sono rappresentate da operatori matematici tensoriali e vengono comunemente trattate operando algebricamente sulle loro componenti, che appunto costituiscono una matrice.

4.2.1 Matrice trasposta coniugata

Nella sezione dedicata alla computazione quantistica, faremo molto uso della matrice **trasposta coniugata** o **matrice ag-**

giunta, cioè una matrice che si ottiene da un'altra trasformandone gli elementi. Presa una matrice **M**, si indica la sua trasposta coniugata usando il simbolo *dagger*(†) come segue: $\mathbf{M}^{\dagger}$. Come suggerisce il nome, la matrice trasposta coniugata è ottenuta per mezzo di due diverse trasformazione: la trasposizione e la coniugazione.

Matrice trasposta La trasposizione di una matrice dà come risultato una nuova matrice. La matrice ottenuta si indica solitamente apponendo la lettera T in altro a destra della matrice originale. Ad esempio la trasposta della matrice **M** si indica come: $\mathbf{M}^{T}$. La matrice $\mathbf{M}^{T}$ è ottenuta dagli stessi elementi della matrice **M** ma scambiando tra loro le righe e le colonne, in modo che tra le due matrici esista la seguente relazione:

$$n_{i,j} = m_{j,i}$$

dove con $n_{i,j}$ si sono indicati gli elementi della matrice $\mathbf{M}^{T}$, mentre con $m_{i,j}$ quelli della matrice **M**. Un esempio di trasposizione è mostrato qui di seguito:

$$\begin{bmatrix} 1 & i \\ 0 & 2 \end{bmatrix}^{T} = \begin{bmatrix} 1 & 0 \\ i & 2 \end{bmatrix}$$

Come si vede gli elementi giacenti sulla diagonale non vengono modificati dalla trasposizione, mentre si scambiano tra loro i due elementi sulla diagonale secondaria.

Matrice coniugata Questa seconda operazione consiste nel calcolare il complesso coniugato di ognuno degli elementi della matrice, quindi costruire una seconda matrice, coniugata alla prima, in cui gli elementi corrispondono ai coniugati della prima. Per ogni elemento vale la seguente:

$$n_{i,j} = m^*_{i,j}$$

dove con $n_{i,j}$ si sono indicati gli elementi della matrice $\mathbf{M}^*$, mentre con $m_{i,j}$ quelli della matrice $\mathbf{M}$. Un esempio di coniugazione è mostrato qui di seguito:

$$\begin{bmatrix} 1 & i \\ 0 & 2 \end{bmatrix}^* = \begin{bmatrix} 1 & -i \\ 0 & 2 \end{bmatrix}$$

Matrice trasposta coniugata Come già suggerisce il nome, la matrice trasposta coniugata, si ottiene applicando prima la trasposizione poi la coniugazione (l'ordine non importa). Tornando quindi ai due esempi visti prima si ha:

$$n_{i,j} = m^*_{j,i}$$

dove si noti che per gli elementi vengono scambiati gli indici e operata la coniugazione. Nell'esempio seguente vediamo l'operazione di trasposta coniugazione applicata alla matrice

$$\begin{bmatrix} 1 & i \\ 0 & 2 \end{bmatrix}^{\dagger} = \begin{bmatrix} 1 & 0 \\ -i & 2 \end{bmatrix}$$

4.2.2 Prodotto tra matrice e vettore

Ora che è stato definito il prodotto scalare è immediato generalizzarlo al prodotto di una matrice per un vettore.
Data la matrice **M** e il vettore **z**, entrambi a componenti complessi, definiamo il loro prodotto $\mathbf{w} = \mathbf{Mz}$ come:

$$w_i = \sum_j m_{i,j} z_j \tag{4.4}$$

4.2.3 Prodotto tensoriale tra matrici

Le grandezze fisiche della meccanica quantistica sono spesso rappresentate sotto forma di matrici i cui elementi rappresentano le componenti di un tensore. Le operazioni che vengono eseguite sui qubits sono operazioni tensoriali che in pratica si riducono al prodotto di matrici per vettori. Per costruire un algoritmo quantistico, è necessario anche saper moltiplicare in

forma tensoriale due matrici tra loro. Questo prodotto, detto appunto *prodotto tensoriale* ed indicato con il simbolo $\otimes$ è l'argomento di questo paragrafo. La trattazione completa di questo argomento non è necessaria ai fini della programmazione quantistica, ma è necessario conoscere le regole per eseguire il prodotto tensoriale tra matrici che di seguito vengono spiegate. Per una trattazione più completa, si veda [3] degli stessi autori.

Si considerino le due seguenti matrici 2×2:

$$\mathbf{A} = \begin{bmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{bmatrix}$$

$$\mathbf{B} = \begin{bmatrix} b_{1,1} & b_{1,2} \\ b_{2,1} & b_{2,2} \end{bmatrix}$$

Il loro prodotto tensoriale $\mathbf{A} \otimes \mathbf{B}$ è dato dall'espressione seguente:

$$\mathbf{A} \otimes \mathbf{B} = \begin{bmatrix} a_{1,1} \begin{bmatrix} b_{1,1} & b_{1,2} \\ b_{2,1} & b_{2,2} \end{bmatrix} & a_{1,2} \begin{bmatrix} b_{1,1} & b_{1,2} \\ b_{2,1} & b_{2,2} \end{bmatrix} \\ a_{2,1} \begin{bmatrix} b_{1,1} & b_{1,2} \\ b_{2,1} & b_{2,2} \end{bmatrix} & a_{2,2} \begin{bmatrix} b_{1,1} & b_{1,2} \\ b_{2,1} & b_{2,2} \end{bmatrix} \end{bmatrix} \tag{4.5}$$

Come si vede, il risultato è una matrice 4×4 dove l'intera matrice B viene moltiplicata per ognuno dei singoli elementi della matrice A.

4.3 Esercizi

4.3.1 Esercizi risolti

- Esercizio 1: Calcolare il prodotto scalare tra i due vettori $\mathbf{z} = (0 + j, 1 + j)$ e $\mathbf{w} = (2 + 2j, 1 + 0j)$

  In questo esercizio i due vettori non vengono rappresentati come matrici colonne, ma ne vengono elencate le componenti tra parentesi. Questa è una pratica comune che non deve confondere. Anzitutto vediamo che il complesso coniugato di $\mathbf{z}$ è dato da $\mathbf{z}^* = (0 - j, 1 - j)$. Il prodotto scalare

tra i due vettori è quindi dato da:

$$\mathbf{z} \cdot \mathbf{w} = \sum_{i=1}^{2} z_i^* w_i$$
$$= (-j)(2+2j) + (1-j)(1) =$$
$$= -2j - 2 + 1 - j = -1 - 3j$$

- Esercizio 2: Calcolare il prodotto tra la matrice

$$\sigma_y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

e il vettore

$$\mathbf{w} = \begin{bmatrix} 1 \\ i \end{bmatrix}$$

Procediamo come indicato dalla 4.4, calcolando le due componenti w_1 e w_2 L'elemento complesso w_1 è dato dalla somma $0 \times 1 + (-i) \times i = 0 + 1 = 1$, mentre w_2 è dato dalla somma $i \times 1 + 0 \times i = i$. Quindi il risultato w del prodotto è:

$$\mathbf{w} = \begin{bmatrix} 1 \\ i \end{bmatrix}$$

- Esercizio 3: Calcolare il prodotto tensoriale tra la matrice I e la matrice σ_y.

La matrice $\mathbf{I}$ è l'identità, cioè l'elemento neutro rispetto al prodotto matriciale, per le matrici 2×2 ed è data dalla seguente espressione:

$$\mathbf{I} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

mentre la matrice σ_y è data dalla seguente:

$$\sigma_y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

Il prodotto tensoriale $\mathbf{I} \otimes \sigma_\mathbf{y}$ si calcola applicando direttamente la 4.6 come:

$$\mathbf{I} \otimes \sigma_y = \begin{bmatrix} 1 \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} & 0 \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \\ 0 \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} & 1 \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \end{bmatrix} \tag{4.6}$$

Eseguendo ora esplicitamente i conti, si ottiene:

$$\mathbf{I} \otimes \sigma_y = \begin{bmatrix} 0 & -i & 0 & 0 \\ i & 0 & 0 & 0 \\ 0 & 0 & 0 & -i \\ 0 & 0 & i & 0 \end{bmatrix} \tag{4.7}$$

4.3.2 Esercizi proposti

- Esercizio 1: Usando la notazione trigonometrica e il piano complesso, si individui, se esiste, la relazione che deve esistere tra due numeri complessi, affinchéè il loro prodotto sia nullo.

- Esercizio 2: Si calcoli il prodotto tensoriale $\sigma_y \otimes \sigma_y$.

Parte II

Fondamenti

CAPITOLO 5

Il qubit

In questo capitolo utilizzeremo la matematica sviluppata nei capitoli precedenti per formulare il bit quantistico, detto appunto qubit, e poterlo quindi concettualizzare. Prima di ciò faremo un rapido excursus nella formulazione del bit classico necessario per confrontare bits e qubits e capirne le differenze.

5.1 La codifica binaria

In questo paragrafo viene introdotto il concetto di informazione binaria anche detta *bit*, concetto che si evolverà in quello di informazione binaria quantistica o *qubit*.

Rappresentazione dei numeri in base 2 I numeri che usiamo per quantificare le grandezze, per esempio: cento pecore, dieci clienti, duecentotrenta euro e via dicendo, sono espressi in linguaggio matematico per mezzo di un sistema di cifre. Per esempio i tre esempi appena scritti possono essere riformulati nel sistema decimale come: 100 pecore, 10 clienti e 230 euro. Il sistema decimale è formato da dieci cifre {0,1,2,3,4,5,6,7,8,9} e da un regola posizionale che stabilisce come interpretare ciascuna cifra. Per esempio il numero 123 deve essere inteso come: $3 \times 1 + 2 \times 10 + 1 \times 100$, o analogamente come: $3 \times 10^0 + 2 \times 10^1 + 1 \times 10^2$. In pratica ogni cifra del numero deve essere intesa come il coefficiente di una potenza di dieci. In simboli possiamo scrivere questo:

$$D_n D_{n-1} D_{n-2} ... D_2 D_1 D_0 = \tag{5.1}$$

$$D_n \times 10^n + D_{n-1} \times 10^{n-1} + D_{n-2} \times 10^{n-2} + \tag{5.2}$$

$$... + D_2 \times 10^2 + D_1 \times 10^1 + D_0 \times 10^0 \tag{5.3}$$

dove il simbolo D_n rappresenta il coefficiente della potenza ennesima. Con una codifica simile è possibile rappresentare anche i numeri relativi ed i numeri in virgola mobile.

È immediato verificare che il sistema di cifre adottato non influenza la capacità di rappresentare i numeri. Ad esempio, tutti i numeri rappresentabili con il sistema decimale, possono essere rappresentati anche usando due sole cifre, per esempio $\{0,1\}$. Un sistema che usa solo due cifre è detto binario. Per convincerci vediamo che lo stesso numero 123 può essere espresso in binario come segue:

$$123 = 1 \times 2^6 + 1 \times 2^5 + 1 \times 2^4 + 1 \times 2^3 + 0 \times 2^2 + 1 \times 2^1 + 1 \times 2^0$$

che rappresenta la cifra binaria:

$$1111011$$

In simboli possiamo riscrivere la 5.3 come segue:

$$B_n B_{n-1} B_{n-2} ... B_2 B_1 B_0 = \tag{5.4}$$

$$B_n \times 2^n + B_{n-1} \times 2^{n-1} + B_{n-2} \times 2^{n-2} + \tag{5.5}$$

$$... + B_2 \times 2^2 + B_1 \times 2^1 + B_0 \times 2^0 \tag{5.6}$$

5.2 Il concetto di bit classico

I coefficienti B_n introdotti nella 5.6 sono detti bit e possono assumere solo i valori 0 o 1. Un bit é l'unità minima di informazione presente in un sistema di computazione digitale binario,

cioè un classico computer elettronico.
La maggior parte dei computer, non memorizza i bits singolarmente, ma in gruppi di 8 detti bytes. Si dice infatti che 8 bits formano un byte. Le dimensioni delle memorie usate per l'immagazzinamento dei dati sono normalmente espresse in termini di bytes e non di bits.

I bits però entrano in due modi nell'informatica classica, infatti da un lato, i dati vengono memorizzati nei sistemi informatici come detto sopra, dall'altro i dati vengono anche processati, cioè vengono usati come operandi di operazioni matematiche e logiche. Sebbene si parli sempre di bit, la differenza di dimensioni tra questi due aspetti è impressionante. Infatti mentre un comune computer da tavolo nel 2020 ha a disposizione una memoria di magazzino (storage memory) di molti miliardi di bytes, e quindi di bits, lo stesso computer processa al più 64 bit simultaneamente. Per questo è importante separare logicamente il concetto di *bit di memoria* da quello di *bit di processo*.
Probabilmente questa separazione potrebbe risultare nuova, ma è molto utile nell'approcciarsi alla computazione quantistica, infatti i qubit, cioè i bit quantistici, di cui tratteremo nel

proseguo del testo, si riferiscono principalmente alla seconda classe di bit, cioè ai bit di processo.

5.3 Il concetto di bit quantistico

L'interesse e il successo dell'informatica quantistica nascono nelle proprietà intrinseche del qubit. Se tanti informatici hanno deciso di confrontarsi con il difficile campo della meccanica quantistica, è stato per poter sfruttare appieno le potenzialità computazionali di questo cugino del bit.

Come vedremo, un qubit può essere anche ridotto ad un bit classico e comportarsi esattamente come questo. Questa caratteristica è importante per capire anzitutto che una macchina di Turing (MdT) può essere realizzata anche con tecnologie quantistiche. Quando però si realizza una MdT classica usando i qubits, non si sta sfruttando il vero valore computazionale dei qubits stessi, ma li si sta utilizzando come bits classici. Quando un qubit "è libero" di comportarsi "quantisticamente' allora i due concetti, bit e qubit, sono completamente diversi, tale libertà porta alla costruzione di vere MdT quantistiche, cioè basate sui principi di computazione quantistica.

5.3.1 Formulazione vettoriale del qubit

Un qubit è un vettore complesso di dimensione due. Per esempio, detto $\mathbf{q}$ un qubit, si ha:

$$\mathbf{q} = \begin{bmatrix} q_1 \\ \\ q_2 \end{bmatrix} \tag{5.7}$$

dove q_1 e q_2 sono due numeri complessi.
Non tutti i vettori complessi di dimensione 2 sono però dei qubit, infatti deve valere la seguente relazione tra le componenti del vettore

$$\mathbf{q} \cdot \mathbf{q} \equiv |q_1|^2 + |q_2|^2 = 1 \tag{5.8}$$

affinché questo sia un qubit.

Alcuni vettori complessi rappresentano lo stesso qubit, cioè vettori complessi diversi possono rappresentare lo stesso qubit. In termini matematici possiamo dire che la relazione che associa il sottoinsieme di vettori di $\mathbb{C}^2$ che hanno modulo 1 ai qubit non è iniettiva. Questo non deve indurre in confusione né preoccupare, infatti come vediamo subito, il criterio per sapere se due vettori complessi rappresentano lo stesso qubit è molto

semplice.

Se un qubit è dato dal vettore complesso **q**:

$$\mathbf{q} = \begin{bmatrix} q_1 \\ \\ q_2 \end{bmatrix}$$

allora ogni altro vettore complesso ottenuto moltiplicando **q** per un numero complesso $z = \rho e^{i\theta}$ con $\rho = 1$ rappresenta lo stesso qubit **q**. Possiamo rappresentare matematicamente questa relazione come segue:

$$\mathbf{q} \sim e^{i\theta}\mathbf{q} \tag{5.9}$$

Come si nota, nella relazione 5.9 è stato omesso il modulo ρ del coefficiente complesso che moltiplica **q**, questo perché come scritto sopra, questa relazione vale solo se $\rho = 1$, quindi può essere omesso nella formula.

In sintesi un qubit è un vettore complesso appartenente a $\mathbb{C}^2$ il quale (il vettore complesso) **deve** soddisfare la relazione 5.8 e per il quale **vale** la relazione 5.9. É importante notare che mentre la prima relazione è restrittiva, cioè restringe l'insieme dei vettori complessi che rappresentano un qubit, la seconda relazione esprime semplicemente una proprietà, che come vedremo

tornerà molto utile nel momento in cui vorremo rappresentare graficamente i qubits.

5.3.2 Implementazione fisica del qubit

Nel paragrafo precedente abbiamo definito il qubit in termini matematici, in questo paragrafo invece vediamo come è possibile realizzarlo nella realtà rimanendo aderenti alla sua definizione formale. Questo è un passaggio molto importante perché ci mostra in che modo sia possibile costruire una macchina computazionale basata sui qubits, esattamente come è stato fatto con gli attuali calcolatori classici che si basano sui bits classici.
Un qubit è per sua natura un *oggetto* quantistico, cioè il suo *comportamento* non può essere descritto correttamente usando la fisica classica. Questo è un tema molto delicato che facilmente trae in confusione i non addetti ai lavori, per questo è bene chiarilo.

La fisica classica è stata formulata tra la fine del 1600 e la fine del 1800. In quegli anni gli studiosi riuscirono a creare modelli e teorie della maggior parte dei fenomeni che erano osser-

vabili ad occhio nudo o con semplici microscopi ottici. Furono anni d'oro per la scienza che però lasciavano ancora alcune domande senza risposta, in particolare non era chiaro cosa fosse la materia. Essa veniva descritta in termini di massa e di carica elettrica, ma la sua natura intima sfuggiva alla capacità di osservazioni degli strumenti allora disponibili. Le idee della fisica e la loro formulazione matematica realizzavano un mondo a sé, parallelo a quello *reale*. Tale mondo permetteva di prevedere con certezza l'evoluzione nel tempo sia di esperimenti che di alcuni sistemi naturali. Per esempio era possibile prevedere con *precisione arbitraria*[1] il tempo di caduta di un grave da un'altezza nota (esperimento), oppure misurare la distanza del fondale marino usando un eco sonora (sistema naturale). Questo mondo *fisico* era basato su alcune idee che sembravano ovvie ma presto risultarono un fardello da abbandonare. La prima e più importante era che la materia potesse essere descritta in termini di punti materiali ognuno dei quali aveva una precisa posizione e velocità ad ogni istante di tempo.

[1] Cioè con la possibilità di aumentare indefinitamente la precisione delle misure aumentando lo sforzo nella produzione degli strumenti di misura e la cura posta nell'operazione stessa di misura.

La fisica quantistica portò scompiglio nel mondo classico che ormai sperava di aver raggiunto l'acme della disciplina e di poter riposare sugli allori. La volontà di conoscere cosa nascondesse la natura microscopica della materia portò gli uomini e le donne di scienza a pensare nuovi esperimenti che mettessero in luce gli aspetti ancora nascosti. I risultati non mancarono e andarono letteralmente fuori dalle aspettative degli sperimentatori, tanto che per poterli spiegare in modo coerente furono abbandonate le basi stesse della meccanica classica. In particolare si dovette rinunciare all'idea di punto materiale in quanto la meccanica quantistica, che prese il posto della meccanica classica, non permette la conoscenza simultanea della posizione e della velocità delle particelle.

Nella meccanica quantistica la teoria viene formulata in modo nuovo rispetto a quella classica, infatti la fisica quantistica incorpora nella teoria stessa anche il concetto di misura. Come ebbe a notare il fisico Heisenberg: *Science no longer is in the position of observer of nature, but rather recognizes itself as part of the interplay between man and nature. The scientific method ... changes and transforms its object: the procedure can no longer keep its distance from the object*

In pratica mentre nella meccanica classica si assume che esista una *realtà oggettiva* che può essere misurata e descritta, e che i metodi e gli strumenti di misura influenzino tale realtà solo nel limite in cui le misure saranno precise, nella meccanica quantistica il processo di misura è intrinseco nella teoria, tanto che i sistemi fisici che si vogliono descrivere vengono formulati nei termini degli strumenti di misura usati per gli esperimenti. Questo discorso, un po' complicato, ci conduce finalmente ad introdurre la descrizione della realizzazione pratica e sperimentale di un qubit per mezzo della polarizzazione della luce.

I fotoni sono i quanti elementari che descrivono il campo elettromagnetico, cioè la *grana fine* in cui si possono formulare le equazioni che descrivono la interazione dell'energia elettromagnetica con la materia. Un esempio semplice di interazione tra campo elettromagnetico e materia si trova nella fotografia digitale. Le immagini digitali sono infatti composte contando il numero di fotoni che incidono sulla pellicola elettronica, cioè quella parte della camera elettronica sensibile alla luce che viene tecnicamente chiamata rivelatore. Questo è una placchetta divisa in quadratini, come un foglio a quadretti, ma che hanno di lato alcuni micron (milionesimi di metro) e noti con il nome

di *pixel*. La luce entra nella camera attraverso l'obiettivo che è formato da una lente che ha il compito di far convergere i raggi verso il rivelatore. Quelli che comunemente chiamiamo raggi, sono in realtà descritti da onde elettromagnetiche nella teoria classica e da fotoni nella teoria quantistica[2]. I fotoni sono assorbiti dal rivelatore e la loro energia libera una certa quantità di carica elettrica che rimane immagazzinata nei pixel. Dopo l'acquisizione dell'immagine (scatto della foto), la carica elettrica di ogni pixel viene letta e memorizzata in un file che verrà poi usato per creare l'immagine in uno dei formati standard.
I fotoni sono quindi presenti nella realtà e nella tecnologia che viene usata comunemente. Come vedremo ora, una delle caratteristiche dei fotoni può essere considerata un qubit, quindi i fotoni possono essere usati per implementare concretamente i qubits.
I fotoni hanno una precisa frequenza e una precisa polarizzazione. La frequenza determina per esempio il colore della luce: i diversi colori che percepisce l'occhio sono eccitati dalla fre-

[2]La luce è ancora trattata come composta da raggi nella disciplina dell'ottica geometrica, cioè in quei casi in cui la lunghezza d'onda della luce stessa è molto piccola rispetto agli strumenti ottici con cui interagisce, per esempio le lenti ottiche.

quenza dei fotoni che incidono sulla retina. La polarizzazione è invece la direzione in cui oscilla il campo elettrico trasportato dal fotone stesso. Sebbene questa sia la definizione fisica corretta, in questo contesto non siamo interessati a questo tipo di definizione, ma ad una definizione che sia esprimibile nei termini in cui possiamo misurare la polarizzazione stessa, infatti, come abbiamo scritto poco sopra, la meccanica quantistica è formulata tenendo conto della misura con cui si determina sperimentalmente una certa proprietà.

La polarizzazione è ben comprensibile dopo aver osservato, o come in questo caso letto, alcuni esperimenti che richiedono un apparato sperimentale abbastanza semplice. Come abbiamo scritto nel paragrafo precedente, nella teoria quantistica la luce visibile è descritta in termini di fotoni. In questo paragrafo descriviamo un esperimento semplice il cui risultato è spiegabile per mezzo della polarizzazione dei fotoni che costituiscono un fascio di luce.

Si prepari una sorgente luminosa, ad esempio una luce di un led, e la si fissi ad un sostegno, poi si prepari uno schermo, come ad esempio un cartoncino bianco e lo si ponga ad una certa distanza dalla sorgente. A questo punto si prenda un fil-

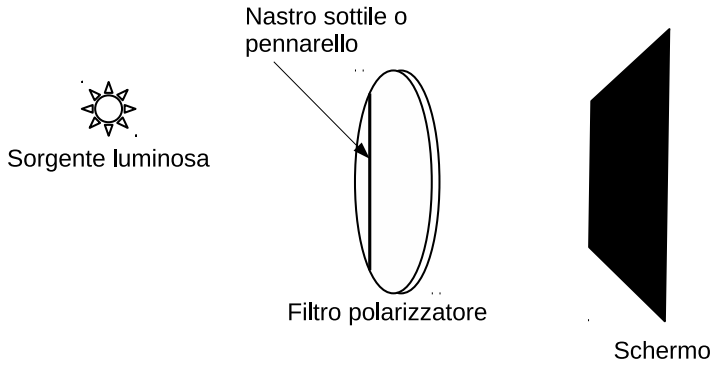

Figura 5.1: La figura mostra il materiale necessario per eseguire l'esperimento. Sono presenti una sorgente luminosa, un filtro polaroid e uno schermo in cartoncino.

tro polarizzatore ad alta trasmissibilità e lo si tagli in modo da ottenerne due che chiameremo filtro **A** e filtro **B**. Questo tipo di filtro è un prodotto facilmente reperibile e dal costo trascurabile (per esempio le lenti in plastica degli occhiali usati per il cinema 3D). Si proceda accendendo il led in modo da illuminare lo schermo. Si noti a sentimento l'intensità della luce proiettata. Poi si frapponga il filtro **A** tra il led e lo schermo e si noterà che l'intensità della luce cala. Uno schema dell'esperimento fin qui condotto è rappresentato in figura 5.2

Si proceda quindi ruotando il filtro attorno all'asse che unisce idealmente il led allo schermo per notare che questa rotazione

non produce alcun effetto sulla intensità della luce trasmessa allo schermo.
Si proceda ora con una penna o un pezzetto di nastro adesivo a tracciare un segmento lungo il filtro che indicherà una direzione, ma non importa completarlo con una freccia in uno dei due versi, basta una linea che indichi la direzione.

Si prenda quindi il filtro **B** e lo si frapponga tra il filtro **A** e lo schermo in modo che i due filtri risultino circa su piani paralleli. Cosa si nota? Ci sono due possibilità:

- L'intensità cala di poco o per nulla
- l'intensità cala molto

Nella prima ipotesi si ruoti lentamente il filtro **B** mantenendolo parallelo al primo. Dopo al più 90 gradi di rotazione ci si accorgerà che l'intensità della luce trasmessa sullo schermo cala fino a scomparire del tutto.
Anche nella seconda ipotesi si ruoti il filtro **B** fino a che la luce non raggiunge più lo schermo.
Poi, indipendentemente da quale delle ipotesi si è verificata, dalla posizione raggiunta si ruoti in senso orario il filtro **B** di

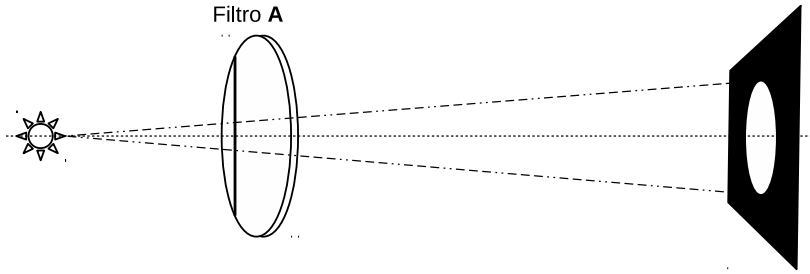

*Figura 5.2: Il filtro **A** è interposto tra la sorgente luminosa e lo schermo. La luce emessa dalla sorgente è parzialmente attenuata dal filtro polarizzante.*

90 gradi, si noterà che la luce raggiunge un massimo di intensità, come mostrato in figura 5.3.

Come fatto per l'altro filtro si tracci un segmento sul filtro **B** in modo che sia parallelo a quello tracciato sul filtro **A**.

Ora si proceda ancora a ruotare il filtro **B** di altri 90 gradi sempre in senso orario e ci si accorgerà che di nuovo la luce è completamente schermata dal sistema di filtri.

Prima di trarre delle conclusioni si ripeta l'esperimento ruotando in senso anti orario anziché orario. Come si avrà modo di notare il risultato non cambia.

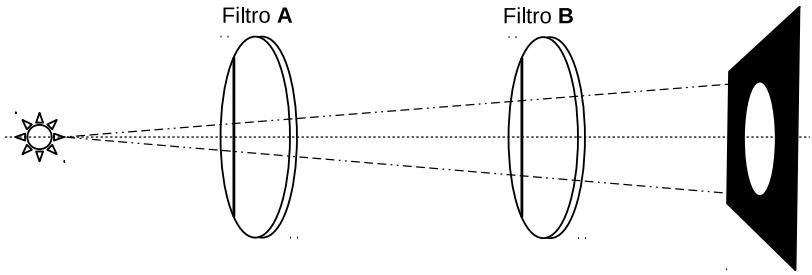

*Figura 5.3: Il filtro **B** è orientato come il filtro **A** ed interposto tra questo e lo schermo. La luce emessa dalla sorgente è trasmessa senza attenuazione dal secondo filtro polarizzante.*

Come possiamo interpretare questo risultato? Sappiamo che l'intensità della luce è proporzionale al numero dei fotoni che raggiunge lo schermo, quindi se l'intensità viene diminuita dalla presenza del primo filtro significa che esso ha fermato parte dei fotoni, quindi questi hanno una proprietà che può essere misurata dal filtro. La rotazione del filtro non influenza l'intensità dei fotoni trasmessi: questo è un fatto importante ma ancora non sappiamo come interpretarlo.

Se anziché schermare la luce con un solo filtro se ne usano due, abbiamo visto che l'intensità della luce trasmessa dipende dall'angolo di cui il secondo filtro è ruotato rispetto al primo. Fatto importante, l'effetto schermo dei due filtri combinati non

dipende dall'angolo assoluto del sistema formato dai due filtri, infatti abbiamo visto che possiamo ruotare il primo filtro a piacere senza modificare la trasmissione, ma solo dall'angolo relativo tra i due.
I risultati che abbiamo ottenuto ci suggeriscono che i fotoni abbiano una proprietà, che chiamiamo *polarizzazione*, che entra in gioco quando questi incontrano il filtro e che sicuramente diventa cruciale quando ci sono due filtri consecutivi, in questi caso la proprietà è chiaramente legata alla direzione.
Per fissare le idee possiamo assegnare una proprietà anche al filtro e chiamarla asse di polarizzazione. Abbiamo visto che nel caso della luce led, la direzione dell'asse di polarizzazione non ha importanza in sé, infatti l'intensità della luce trasmessa è indipendente dalla rotazione del filtro, ma assume importanza se vengono inseriti due filtri, in tal caso infatti, se i due filtri hanno asse perpendicolare (sfasato di 90 gradi) essi agiscono in modo da fermare la maggior parte dei fotoni, nel caso di filtri perfetti, essi fermeranno tutti i fotoni.

Un secondo esperimento ci può aiutare a chiarirci le idee. Ricaviamo da uno dei due filtri un terzo filtro che indichiamo come filtro **C**. Ruotiamo i due filtri **A** e **B** in modo che la pro-

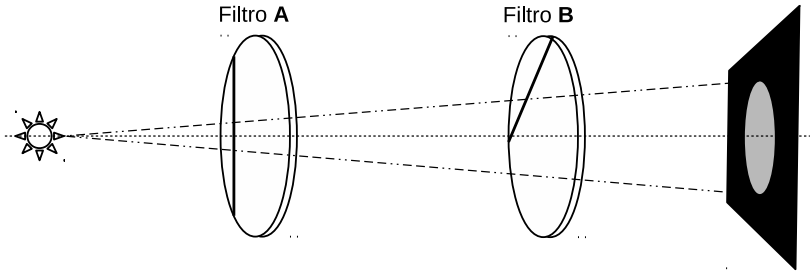

*Figura 5.4: Il filtro **B** è ruotato di 45 gradi rispetto al filtro **A**. La luce emessa dalla sorgente è parzialmente trasmessa dal secondo filtro polarizzante.*

iezione della luce sullo schermo sia minima o nulla. A questo punto inseriamo il terzo filtro **C** tra i due. Cosa si nota? Sono possibili due scenari:

- L'intensità della luce sullo schermo torna come se ci fosse solo un filtro
- l'intensità rimane minima o nulla

L'eventualità più probabile è di ritrovarsi nel primo scenario descritto sopra, ma se capita il secondo, si ruoti il filtro **C** di circa 90 gradi e, in questo modo, ci si porterà nel caso del primo scenario.

Come fatto in precedenza si tracci un segmento (o un pezzetto

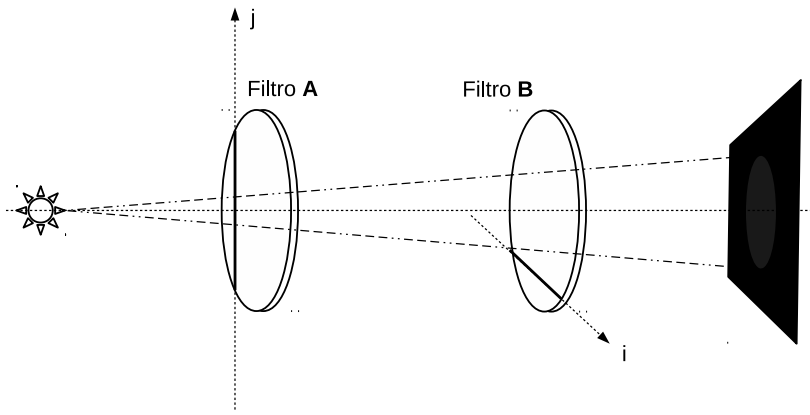

*Figura 5.5: Il filtro **B** è ruotato di 90 gradi rispetto al filtro **A**. La luce emessa dalla sorgente è completamente fermata dal secondo filtro polarizzante.*

di nastro adesivo) sul filtro **C** con una inclinazione di circa 45 gradi.

Il risultato descritto nel primo scenario dovrebbe sorprenderci. Infatti dal primo esperimento abbiamo capito che l'azione combinata dei due filtri opportunamente ruotati blocca completamente (o quasi) la trasmissione dei fotoni. È quindi naturale chiedersi perché l'inserimento del terzo filtro annulla l'azione combinata dei primi due. Potrà sorprendere, ma non c'è interesse a rispondere a questa domanda. Infatti in realtà non è possibile dare un risposta che porti più informazione di

quella che abbiamo già ottenuto: **questo è l'approccio della meccanica quantistica**.

Forse si potrebbe rimanere un po' spiazzati, ma se aggiungiamo un po' della matematica vista nel capitolo precedente le cose potrebbero migliorare. Anzitutto facciamo un piccolo atto di fiducia e passiamo dall'esperimento qui descritto ad uno analogo ma che richiede delle condizioni sperimentali più complesse. L'idea è semplice anche se complessa nella sua realizzazione pratica. Si tratta infatti di diminuire moltissimo l'intensità del fascio luminoso tanto da poter essere sicuri che dalla sorgente luminosa venga emesso un fotone alla volta ad intervalli di tempo regolari. Quindi niente che stravolga alla radice l'esperimento fin qui condotto, ma che ci permetta di fare delle considerazioni specifiche sul singolo fotone e non sul comportamento statistico che vediamo quando ne usiamo un intero fascio.

Poniamo quindi un solo filtro tra la sorgente di fotoni e lo schermo e iniziamo a *sparare* un fotone per volta. Quello che vedremo è che in conseguenza di ogni *colpo* sullo schermo arriva un impulso luminoso, oppure nulla, non arriva mai mezzo fotone. Questa è una realtà sperimentale difficilmente misurabile con

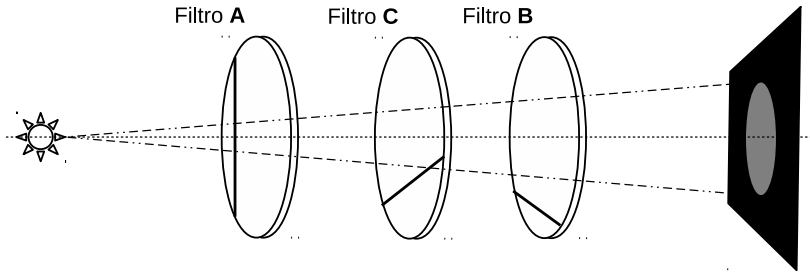

*Figura 5.6: Il filtro **C** a 45 gradi è interposto tra il filtro **A** e il **B** sfasati tra loro di 90 gradi. Parte del fascio luminoso raggiunge lo schermo.*

mezzi casalinghi, ma già dimostrata da Einstein nel 1905 e per la quale ebbe il premio Nobel[5].

L'esperimento può essere descritto come segue. Al momento dell'emissione del fotone, la sua polarizzazione si trova in uno stato non noto che decidiamo di indicare come segue:

$$\begin{bmatrix} \psi_1 \\ \psi_2 \end{bmatrix} \tag{5.10}$$

Nell'espressione 5.10 è facile riconoscere il formalismo usato per rappresentare i vettori, infatti come vederemo è proprio quello che vogliamo fare, però per il momento la 5.10 può essere pensata semplicemente come un modo per indicare uno stato fisico attraverso un simbolo distintivo.

Quando il fotone attraversa il filtro **A** non sappiamo cosa succede nel dettaglio, però se il fotone produce luce sullo schermo sappiamo che non è stato fermato dal filtro, se invece non vediamo nulla allora sappiamo che il fotone è stato arrestato dal filtro.

Indichiamo la direzione del primo filtro (**A**) con la lettera $\hat{j}$. Prendiamo il filtro **B** e posizioniamolo in modo che la sua direzione (indicata dal segmento tracciato su di esso) sia ora perpendicolare alla direzione del primo (vedi figura 5.5): chiamiamo questa direzione $\hat{i}$.

Ora che entrambi i filtri sono posizionati torniamo a sparare fotoni contro lo schermo. Cosa rileviamo? Nulla, nessun fotone raggiunge lo schermo. Questo non deve sorprenderci perché avevamo avuto lo stesso risultato nell'esperimento realmente condotto in casa. Ora però possiamo asserire una cosa, che un fotone se è passato per il filtro in posizione $\hat{j}$ si trova in uno stato particolare che **sicuramente** gli impedirà di passare per il secondo filtro posto in direzione $\hat{i}$. Chiamiamo lo stato di questo fotone $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$.

A questo punto è importante notare che questo ragionamento

è indipendente dalla rotazione del primo filtro rispetto all'asse centrale. L'unica cosa che determina la condizione per cui nessun fotone raggiunge lo schermo è che le due direzioni $\hat{j}$ e $\hat{i}$ siano l'una perpendicolare all'altra. Quindi possiamo dire che lo stato

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

è lo stato che posseggono i fotoni uscenti dal primo filtro e visto che abbiamo indicato la direzione del filtro **A** con $\hat{j}$, associamo alla direzione $\hat{j}$ lo stato

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

Ripetiamo l'esperimento togliendo il filtro **A** e lasciando solo il **B**. Come nel caso precedente notiamo che solo la metà dei fotoni raggiunge lo schermo. Se poi inseriamo il filtro **A** tra il **B** e lo schermo (quindi in pratica scambiamo i due filtri) e li ruotiamo in modo che assumano le due direzioni $\hat{j}$ e $\hat{i}$ (cioè perpendicolari l'uno all'altro), vedremo che nessun fotone raggiunge più lo schermo. Con questa osservazione possiamo asserire con sicurezza che dopo aver attraversato il filtro **B** (cioè quello che prima era il secondo filtro ma ora è il primo) il fotone si trova

in uno stato preciso, che **non** possiamo chiamare

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

perché questo è lo stato che coincide con quello dei fotoni che attraversano il filtro in direzione $\hat{j}$. Quindi chiameremo lo stato dei fotoni uscenti da **B**:

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

Abbiamo stabilito qualcosa di molto importante: per descrivere completamente lo stato di polarizzazione di un fotone ci bastano due stati di base:

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

e

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

Questi vanno riferiti alla direzione reale che hanno i segmenti tracciati sui nostri filtri, ma indipendentemente dalla direzione di questi, finché fra di loro esiste uno sfasamento di 90 gradi, queste due direzioni possono essere considerate la base per lo stato di ogni fotone.

Abbiamo detto tutto? Ancora no, infatti, se così fosse, avremo che lo stato di polarizzazione sarebbe in sé equivalente ad un bit classico, ma come vederemo esso è molto più generale e coincide esattamente con i qubit che abbiamo descritto in termini matematici come vettori complessi dello spazio $\mathbb{C}^2$.

Il risultato *chiave* che ancora dobbiamo incorporare nella teoria riguarda il comportamento della luce quando viene inserito il terzo filtro. Ripetiamo questo esperimento nelle nuove condizioni sperimentali, in cui viene emesso un solo fotone per volta.

Posizioniamo quindi i due filtri l'uno perpendicolare all'altro aiutandoci con il segno tracciato su di essi. In questa condizione vediamo che nessun fotone raggiunge lo schermo, quindi possiamo stabilire che se un fotone si trova nello stato:

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

non può passare un filtro nella direzione $\hat{j}$, mentre se si trova nello stato

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

non può passare un filtro nella direzione $\hat{i}$. Visto questo inseriamo il terzo filtro tra i due, mantenendo la sua direzione a 45 gradi rispetto alle altre due. Con nostra sorpresa noteremo che una frazione dei fotoni emessi ricomincia a raggiungere lo schermo.

Ragioniamo ora sul risultato ottenuto. Sappiamo che dopo aver attraversato il filtro $\hat{j}$ la polarizzazione del fotone è nello stato

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

, poi sappiamo che se la polarizzazione è nello stato

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

il fotone non può attraversare il filtro $\hat{i}$, ma visto che alcuni fotoni lo fanno, dobbiamo per forza giungere alla conclusione che il filtro obliquo abbia modificato lo stato di polarizzazione. A questo punto potremmo pensare che il filtro obliquo abbia qualche proprietà particolare, ma sappiamo che non è così perché lo abbiamo ottenuto da uno degli altri due filtri, inoltre possiamo fare un esperimento, e sostituire il filtro obliquo a uno degli altri due e accorgerci che il risultato non cambia.

L'unica considerazione che possiamo trarre è che dopo aver at-

traversato il filtro di mezzo, i fotoni che arrivano dal primo filtro non siano più nello stato

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

perché altrimenti non passerebbero l'ultimo filtro. A questo punto possiamo pensare che esista un terzo stato che indicheremo con

$$\begin{bmatrix} \psi_1 \\ \psi_2 \end{bmatrix}$$

in cui si trovano i fotoni dopo aver attraversato il filtro di mezzo. Per i ragionamenti visti sopra però questo stato deve corrispondere con lo stato

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

se poniamo il filtro di mezzo avanti agli altri due, e allo stato

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

se lo poniamo dopo i due. La cosa si complica ancora se proviamo a lasciarlo tra i due ma a ruotarlo in modo che la sua direzione coincida con uno di essi, come si potrebbe notare, di nuovo nessun fotone raggiunge lo schermo.

La risposta della meccanica quantistica è che dopo aver attraversato lo schermo mediano, il fotone si trova in una combinazione dei due stati

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

e

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

data dalla seguente espressione:

$$\psi = 1/\sqrt{2} \begin{bmatrix} 1 \\ 0 \end{bmatrix} + 1/\sqrt{2} \begin{bmatrix} 0 \\ 1 \end{bmatrix} \tag{5.11}$$

Questa espressione corrisponde esattamente alla definizione di qubit data in equazione 5.8, infatti si ha:

$$\psi \cdot \psi = \left(\frac{1}{\sqrt{2}}\right)^2 + \left(\frac{1}{\sqrt{2}}\right)^2 \tag{5.12}$$

cioè la somma delle probabilità relative ai due stati è pari ad uno, il che significa che il qubit, una volta misurato, sarà trovato in uno o nell'altro stato, e non ci sono possibilità alternative. È chiaro che lo stato ψ in cui si trova la polarizzazione dei fotoni che hanno attraversato il primo e il secondo filtro può dipendere solo dall'angolo relativo tra esso ed il filtro successivo e non dal terzo filtro che deve ancora essere attraversato. Facciamo

quindi una prova e rimuoviamo il terzo filtro. Ora sul piano ci sono solo due filtri, il secondo ruotato di 45 gradi rispetto al primo. Sosteniamo a ragione che lo stato dei fotoni che escono dal secondo filtro sia

$$\psi \cdot \psi = \left(\frac{1}{\sqrt{2}}\right)^2 + \left(\frac{1}{\sqrt{2}}\right)^2 \tag{5.13}$$

Ora possiamo provare a modificare l'angolo, che per chiarezza chiameremo θ, del filtro obliquo e noteremo che approssimandosi all'allineamento con il primo filtro il numero dei fotoni che raggiunge lo schermo aumenta come il coseno dell'angolo che i due filtri formano, o come il seno dell'angolo che il secondo filtro forma con la direzione perpendicolare a quella del primo filtro.

Decidiamo allora di generalizzare la 5.12 incorporando questa informazione:

$$\psi = \sin(\theta) \begin{bmatrix} 0 \\ \\ 1 \end{bmatrix} \tag{5.14}$$

Ora l'equazione 5.14 non è ancora completa, infatti se lo stato di un fotone uscente dal filtro obliquo fosse espresso solo dalla componente $\sin(\theta) \begin{bmatrix} 0 \\ \\ 1 \end{bmatrix}$ non si spiegherebbe perché aggiungendo il terzo filtro polarizzato perpendicolarmente al primo si continua ad osservare l'arrivo di fotoni sullo schermo visto che i

fotoni nello stato $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$ sono completamente fermati dal filtro in posizione $\hat{i}$.

Per spiegare anche questo fenomeno completiamo la 5.14 aggiungendo un termine:

$$\psi = \cos(\theta) \begin{bmatrix} 1 \\ 0 \end{bmatrix} + \sin(\theta) \begin{bmatrix} 0 \\ 1 \end{bmatrix} \tag{5.15}$$

L'espressione 5.15 è finalmente quello che volevamo ottenere. Questa è l'espressione che rappresenta correttamente la realtà sperimentale perché descrive correttamente i risultati che si osservano nella realtà. L'espressione 5.15 ha due caratteristiche che vogliamo notare:

- Lo stato delle polarizzazione è un vettore di dimensione due, perché qualsiasi possibile stato può essere espresso come combinazione lineare di due vettori tra loro ortogonali

- Lo stato di polarizzazione è un qubit perché il suo modulo quadro è sempre uguale ad uno

Nel paragrafo che segue notiamo una terza caratteristica anche essa molto importante.

Il significato fisico che possiamo associare alla ψ è vincolato agli esperimenti che possiamo condurre sullo stato di polarizzazione del fotone stesso. Come abbiamo visto possiamo solo esprimere la probabilità che esso passi o non passi per il polarizzatore e si è visto che detta probabilità è calcolabile come il modulo quadro di ψ. Se due vettori ψ e ψ' hanno lo stesso modulo quadro allora esprimono la stessa probabilità che il fotone passi per un polarizzatore e perciò contengono la stessa informazione fisica e quindi, in questa ipotesi, si avrebbe che i due vettori sono *fisicamente* equivalenti.
Se si prova a moltiplicare le componenti di ψ per uno stesso numero complesso $z = e^{i\theta}$ si ottiene un nuovo vettore ψ'. Con i passaggi che seguono, dimostra facilmente che il valore del modulo quadro di ψ' è lo stesso di ψ:

$$|\psi'|^2 = |e^{i\theta}\psi|^2 = (e^{i\theta}\psi) \cdot (e^{i\theta}\psi) = (e^{i\theta}e^{-i\theta})\psi \cdot \psi = \psi \cdot \psi = |\psi|^2$$

Quindi lo stato fisico rappresentato da ψ soddisfa la 5.8 e per esso vale la 5.9. In pratica abbiamo dimostrato che lo stato di polarizzazione di un fotone è un qubit.

Abbiamo detto tutto? Abbiamo dimostrato che la polarizzazione è un vettore di dimensione due, ma per le argomentazioni che abbiamo usato, è sufficiente usare un vettore reale, quindi costruito su $\mathbb{R}^2$. Esistono però altri tipi di filtri, che non possono essere ricondotti a quelli usati negli esperimenti che anche essi producono effetti analoghi a quelli che abbiamo osservato. Con ragionamenti analoghi a quelli fin qui condotti, si conclude che qualsiasi stato di polarizzazione può essere espresso come:

$$\psi = \beta \begin{bmatrix} 1 \\ 0 \end{bmatrix} + \alpha \begin{bmatrix} 0 \\ 1 \end{bmatrix} \tag{5.16}$$

dove α e β sono dei numeri complessi.

Con la 5.16 abbiamo visto che esiste almeno un modo di implementare il qubit come stato quantistico di un sistema fisico. Ne esistono altri, che sfruttano altri sistemi fisici, come ad esempio lo *spin* di atomi artificiali.

Il risultato qui raggiunto è molto importante perché ora abbiamo chiarito cosa sia un qubit in senso astratto e come questo può essere realizzato nella pratica. Con questo nuovo armamentario possiamo continuare lo studio.

5.3.3 Relazione tra qubits e bits classici

Come abbiamo visto nel paragrafo 3.1, esiste una corrispondenza tra i numeri reali e i numeri complessi, infatti il sottoinsieme dei complessi che ha parte immaginaria nulla può essere posto in corrispondenza biunivoca con i numeri reali.
Forti di questa corrispondenza vogliamo stabilire una relazione tra due possibili *valori* di un qubit quantistico e i due possibili valori, 0 e 1, ammessi per un bit classico.
In realtà, essendo un qubit un vettore, non si può definirne il valore, ma si parla piuttosto del suo stato che comprende entrambi i valori delle sue componenti q_1 e q_2. Diremo, per fare un esempio che illustri il concetto di stati, che il vettore seguente:

$$\begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix} \tag{5.17}$$

è in uno stato diverso dal vettore:

$$\begin{bmatrix} \sin(\pi/6) \\ \cos(\pi/6) \end{bmatrix} \tag{5.18}$$

Quindi, quello che vogliamo fare è scegliere due tra gli infiniti stati in cui può trovarsi un qubit per associarli ai due soli valori, 0 ed 1, che può assumere un bit. Come si può capire,

questa scelta ha una componente di arbitrarietà e per questo è necessario stabilire una convenzione che è la seguente:

$$\begin{bmatrix} 1+0i \\ 0+0i \end{bmatrix} \equiv 0 \tag{5.19}$$

$$\begin{bmatrix} 0+0i \\ 1+0j \end{bmatrix} \equiv 1 \tag{5.20}$$

La 5.20 stabilisce due corrispondenze: una per il bit 0 e una per il bit 1. Le due componenti dei vettori mostrati nella definizione 5.20 sono numeri complessi la cui parte immaginaria è nulla, ma è stata comunque espressa per chiarire la natura complessa dei qubit, che in generale potrà stare in stati diversi dallo 0 e dall'1.

5.4 Principio di sovrapposizione degli stati

Nel paragrafo precedente abbiamo visto come lo stato di un vettore complesso puó essere usato per rappresentare un qubit, e che è possibile scegliere due specifici stati per ricreare un'analogia classica con i valori 0 ed 1 possibili per un bit.

In questo paragrafo vediamo che gli stati possibili per un qubit sono infiniti e non limitati a due come quelli di un bit.

Qubit senza relazione classica Consideriamo il vettore $\mathbf{q}$ definito come segue:

$$\mathbf{q} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} \tag{5.21}$$

Esso è diverso dai due qubit definiti in 5.20, quindi non corrisponde nè al bit 1 nè al bit 0. D'altra parte è immediato verificare che esso può essere scritto come la *combinazione lineare* dei due vettori definiti in 5.20.

Per combinazione lineare di due vettori $\mathbf{w}$ e $\mathbf{z}$ si intende la somma $\alpha\mathbf{w} + \beta\mathbf{z}$ dove α e β appartengono al campo su cui sono definiti i vettori, quindi in questo caso ai numeri complessi.

Detto questo, il vettore 5.21 può essere scritto come segue:

$$\frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \end{bmatrix} + \frac{1}{\sqrt{2}} \begin{bmatrix} 0 \\ 1 \end{bmatrix} \tag{5.22}$$

Nel membro di destra dell'espressione 5.22 è immediato riconoscere i due qubit definiti in 5.20, quindi come preannunciato, abbiamo riscritto il vettore $\mathbf{q}$ come combinazione lineare di loro due.

Il qubit $\mathbf{q}$ non corrisponde nè al bit classico 0 né al bit classico

1, quindi non ha corrispondenza classica. Si è appena visto però che esso può essere scritto come la somma dei due qubit che invece hanno una corrispondenza classica. Questo vale per ogni qubit, quindi: è sempre possibile scrivere un qubit come la somma di due qubit con corrispondenza classica.

D'ora in avanti, chiameremo **qubits di base** i due qubits scelti per avere una corrispondenza classica. Un esempio di qubits di base è stato dato in 5.20, ma in generale qualsiasi coppia di vettori complessi a due componenti che siano ortonormali, cioè che abbiano modulo uguale ad 1 e che siano perpendicolari tra loro, può essere scelta come coppia di base.

Con questo, abbiamo introdotto il **principio di sovrapposizione** degli stati.

5.5 Sovrapposizione degli stati per un qubit

Un qubit può trovarsi in una combinazione lineare dei qubits di base, quindi trovarsi simultaneamente in entrambi gli stati

base.

Da un punto di vista puramente matematico questa affermazione equivale a dire che il numero sette è in realtà una combinazione lineare del numero 3 e del numero 4, che sebbene possa essere una osservazione interessante, non aggiunge nulla di nuovo all'utilità del numero 7.

La sovrapposizione degli stati per il qubit ha invece una natura fisica che si manifesta nel momento in cui si procede con la *misura* del qubit. L'argomento della misura è molto importante, per questo aspettiamo a trattarlo dopo aver introdotto il formalismo *bra-ket* che ci permetterà nel proseguo del testo di usare espressioni matematiche più semplici e concise.

5.6 Formalismo Bra e Ket

I qubits sono anche rappresentati e trattati usando un formalismo diverso da quello matriciale visto in precedenza. In pratica si tratta di assegnare un simbolo (più semplice *ndr*) ad ognuno dei qubit di base, in modo che si possa scrivere qualsiasi altro qubit come combinazione lineare di questi due simboli. Il

qubit:

$$\begin{bmatrix} 1 \\ 0 \end{bmatrix} \tag{5.23}$$

viene rappresentato con il simbolo $|0\rangle$, mentre il qubit:

$$\begin{bmatrix} 0 \\ 1 \end{bmatrix} \tag{5.24}$$

viene rappresentato con il simbolo $|1\rangle$.

La notazione appena vista è detta a *ket* ed è stata usata per primo nella meccanica quantistica dal fisico P.A.M. Dirac[1] perchè, molto comoda per esprimere formulazioni complesse su una singola riga, del resto essa è del tutto equivalente alla formulazione matriciale.

5.6.1 Prodotto scalare tra bra e ket

Nel paragrafo 4.1.1 è stato definito il prodotto scalare tra vettori complessi, in questo paragrafo viene definito l'analogo per i *bra* e i *ket*. In generale, ogni qubit **q** viene rappresentato con un *ket*, ad esempio $|q\rangle$. Se però si vuole rappresentare il prodotto scalare tra il qubit **q** e un altro vettore complesso **z**, allora si scrive $\langle z|q\rangle$. Il simbolo $\langle z|$ indica un *bra*, cioè il trasposto coniu-

gato del vettore **z**.

Usando la notazione appena introdotto possiamo scrivere:

$$\frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix} \equiv \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \tag{5.25}$$

In generale, qualsiasi qubit potrà sempre essere scritto come: $\alpha|0\rangle + \beta|1\rangle$ con la condizione vista sopra che $|\alpha|^2 + |\beta|^2 = 1$.

5.6.2 Prodotto tensoriale tra ket e bra

L'argomento che viene trattato in questo paragrafo è presentato qui in modo diretto ed informale, ma sufficiente ad acquisire gli strumenti necessari per la computazione quantistica[3].

Poco sopra abbiamo introdotto il formalismo dei bra e dei ket e abbiamo definito il prodotto scalare tra bra e ket come $\langle\psi|\phi\rangle$, in questo paragrafo estendiamo tale formalismo definendo anche il prodotto tensoriale tra ket e bra $|\psi\rangle\langle\phi|$, ottenuto in modo *pratico* scambiando l'ordine in cui compaiono il bra e i ket rispetto al prodotto scalare.

Prendiamo ad esempio il ket $|0\rangle$ e il corrispondente bra $\langle 0|$ e il

[3]Una trattazione più formale può essere trovata in *Informatica quantistica*[3]

loro prodotto tensoriale *ket per bra* : $|0\rangle\langle 0|$.

L'elemento trovato: $|0\rangle\langle 0|$ corrisponde alla matrice

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \tag{5.26}$$

ed è detto essere un *operatore*.

Osserviamo l'effetto che ha l'operatore $|0\rangle\langle 0|$ sul ket $|0\rangle$

$$|0\rangle\langle 0|0\rangle = |0\rangle$$

In maniera simile possiamo costruire altri operatori, ad esempio prendendo il ket $|0\rangle$ e il bra $\langle 1|$ otteniamo $|0\rangle\langle 1|$ che corrisponde alla matrice

$$\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \tag{5.27}$$

Continuando possiamo costruire l'operatore $|1\rangle\langle 0|$ che corrisponde alla matrice

$$\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \tag{5.28}$$

e infine anche $|1\rangle\langle 1|$ che corrisponde alla matrice

$$\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \tag{5.29}$$

5.6.3 Gli operatori

Azione degli operatori sui ket

Si chiamano operatori perché operano sui ket trasformandoli in *nuovi* ket, esattamente come fanno le matrici sui vettori. Si è visto che ad ogni operatore è associata una matrice, perciò studiando l'azione di una matrice sui vettori di base $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$ e $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$, si può calcolare l'azione dell'operatore sui corrispondenti ket di base $|0\rangle$ ed $|1\rangle$. In generale, però, la notazione in bra e ket degli operatori è ancora più semplice da capire se si tiene conto delle regole seguenti. Per il ket $|0\rangle$:

$$\begin{aligned} |0\rangle\langle 0|0\rangle &= |0\rangle \\ |0\rangle\langle 1|0\rangle &= 0 \\ |1\rangle\langle 0|0\rangle &= |1\rangle \\ |1\rangle\langle 1|0\rangle &= 0 \end{aligned} \tag{5.30}$$

e per il ket $|1\rangle$

$$
\begin{aligned}
|0\rangle\langle 0|1\rangle &= 0 \\
|0\rangle\langle 1|1\rangle &= |0\rangle \\
|1\rangle\langle 0|1\rangle &= 0 \\
|1\rangle\langle 1|1\rangle &= |1\rangle
\end{aligned}
\tag{5.31}
$$

Le 5.30 e le 5.31 non sono né definizioni né regole arbitrarie, ma derivano direttamente dagli *alter ego* matriciali dei bra, dei ket e degli operatori. Comunque spesso nel calcolo risulta molto più semplice riferirsi ad esse piuttosto che eseguire i calcoli matriciali.

Somma di operatori

Gli operatori possono essere moltiplicati per un generico numero complesso, così ad esempio è possibile definire l'operatore $\mathbf{A}$ moltiplicando il numero complesso λ per l'operatore $|0\rangle\langle 0|$ come segue:

$$\mathbf{A} = \lambda|0\rangle\langle 0| \tag{5.32}$$

e l'azione di $\mathbf{A}$ sul ket $|0\rangle$ come:

$$\mathbf{A}|0\rangle = \lambda|0\rangle\langle 0|0\rangle = \lambda|0\rangle \tag{5.33}$$

É possibile anche definire l'azione di $\mathbf{A}$ su un generico ket $\alpha|0\rangle + \beta|1\rangle$ come:

$$\mathbf{A}(\alpha|0\rangle + \beta|1\rangle) = \mathbf{A}\alpha|0\rangle + \mathbf{A}\alpha|1\rangle = \lambda\alpha|0\rangle\langle 0|0\rangle + \lambda\beta|0\rangle\langle 0|1\rangle = \lambda\alpha|0\rangle \tag{5.34}$$

dove il risultato è stato ottenuto usando le 5.30 e le 5.31.
Gli operatori possono essere anche sommati tra loro. Per esempio si consideri l'operatore $\mathbf{B}$ ottenuto moltiplicando il numero complesso γ per l'operatore $|1\rangle\langle 1|$

$$\mathbf{B} = \gamma|1\rangle\langle 1| \tag{5.35}$$

e l'operatore $\mathbf{A}$ definito precedentemente. É possibile definire il nuovo operatore $\mathbf{C}$ dato dalla somma di $\mathbf{A}$ e $\mathbf{B}$ come segue:

$$\mathbf{C} = \mathbf{A} + \mathbf{B} = \lambda|0\rangle\langle 0| + \gamma|1\rangle\langle 1| \tag{5.36}$$

L'azione di $\mathbf{C}$ su un generico ket $\alpha|0\rangle + \beta|1\rangle$ si ottiene applicando le 5.30 e le 5.31 come segue:

$$
\begin{aligned}
(\mathbf{C})(\alpha|0\rangle + \beta|1\rangle) = \alpha\mathbf{C}|0\rangle + \beta\mathbf{C}|1\rangle = \\
= \alpha(\mathbf{A}+\mathbf{B})|0\rangle + \beta(\mathbf{A}+\mathbf{B})|1\rangle = \\
\alpha(\lambda|0\rangle\langle 0| + \gamma|1\rangle\langle 1|)|0\rangle + \beta(\lambda|0\rangle\langle 0| + \gamma|1\rangle\langle 1|)|1\rangle = \\
\alpha\lambda|0\rangle + \beta\gamma|1\rangle
\end{aligned}
\tag{5.37}
$$

Le operazioni quantistiche sui qubits sono descritte per mezzo di operatori, per questo motivo è molto importante dedicare il giusto tempo ad esercitarsi provando varie combinazioni come quella descritta in 5.36.

Operatore aggiunto

Nel paragrafo 4.2.1 è stata definita l'operazione che permette di passare da una matrice alla relativa matrice trasposta coniugata (o aggiunta). La stessa operazione è definita per gli operatori, anche se per essi si usa solo il termine **operatore aggiunto**. La procedura per passare da un operatore $\mathbf{O}$ al suo aggiunto $\mathbf{O}^*$ è del tutto corrispondente a quanto visto per le matrici, si tratta di scambiare riga e colonna, che in questo caso saranno bra e ket, e di eseguire la coniugazione del coefficiente dell'elemento dell'operatore. Vediamo subito un esempio

chiarificatore. Consideriamo l'operatore:

$$\mathbf{O} = i|0\rangle\langle 1| + |1\rangle\langle 0|$$

si ha che l'aggiunto $\mathbf{O}^*$ di $\mathbf{O}$ è dato dalla espressione seguente:

$$\mathbf{O}^* = -i|1\rangle\langle 0| + |0\rangle\langle 1|$$

Si noti che per l'operatore aggiunto si usa spesso il simbolo $*$, ma è corretto anche l'uso del dagger $\dagger$.

Prodotto tensoriale tra operatori

Nel paragrafo 4.2.3 è stato definito il prodotto tensoriale tra matrici. Dopo quanto si è visto sulla relazione tra matrici ed operatori, è naturale aspettarsi di poterlo applicare agli operatori in modo del tutto analogo usando il formalismo dei bra e dei ket. Riprendiamo quindi l'esempio del prodotto tensoriale tra le matrici $\mathbf{I}$ e $\sigma_\mathbf{y}$ dato dalla seguente:

$$\mathbf{I}\otimes\sigma_y = \begin{bmatrix} 1\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} & 0\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \\ 0\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} & 1\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \end{bmatrix} = \begin{bmatrix} 0 & -i & 0 & 0 \\ i & 0 & 0 & 0 \\ 0 & 0 & 0 & -i \\ 0 & 0 & i & 0 \end{bmatrix} \tag{5.38}$$

Vediamo anzitutto che sia la matrice $\mathbf{I}$ che la matrice $\sigma_\mathbf{y}$ possono essere scritte in forma di bra e ket come segue:

$$\mathbf{I} = |0\rangle\langle 0| + |1\rangle\langle 1|$$
$$\sigma_\mathbf{y} = -i|0\rangle\langle 1| + i|1\rangle\langle 0| \tag{5.39}$$

dove si ricorda che la lettera i indica l'unità immaginaria dei numeri complessi.
Il prodotto tensoriale tra la matrice $\mathbf{I}$ e la matrice $\sigma_\mathbf{y}$ si ottiene calcolando il prodotto tensoriale tra i singoli addendi della matrice e sfruttando la proprietà distributiva del prodotto rispetto all'addizione. Scriviamo quindi il prodotto tra le due matrici come segue:

$$\mathbf{I} \otimes \sigma_\mathbf{y} = (|0\rangle\langle 0| + |1\rangle\langle 1|) \otimes (-i|0\rangle\langle 1| + i|1\rangle\langle 0|) \tag{5.40}$$

e sfruttiamo la proprietà distributiva del prodotto per scrivere:

$$\mathbf{I} \otimes \sigma_\mathbf{y} = (|0\rangle\langle 0| + |1\rangle\langle 1|) \otimes (-i|0\rangle\langle 1| + i|1\rangle\langle 0|) =$$
$$-i|0\rangle\langle 0| \otimes |0\rangle\langle 1| + i|0\rangle\langle 0| \otimes |1\rangle\langle 0| - i|1\rangle\langle 1| \otimes |0\rangle\langle 1| + i|1\rangle\langle 1| \otimes |1\rangle\langle 0| \tag{5.41}$$

La 5.41 mostra in totale quattro termini non nulli (diversi da zero), esattamente lo stesso numero dei termini non nulli presenti nella 5.38. I termini diversi da zero nella 5.38 sono: l'$m_{1,2}$,

$m_{2,1}$, $m_{3,4}$ e il $m_{4,3}$, dove si è indicato con $m_{i,j}$ il termine $i-$esimo e $j-$esimo della matrice.

Tra i termini della 5.41 e quelli della 5.38 esiste ovviamente la corrispondenza biunivoca riportata di seguito:

$$|0\rangle\langle 0| \otimes |0\rangle\langle 1| \leftrightarrow m_{1,2}$$

$$|0\rangle\langle 0| \otimes |1\rangle\langle 0| \leftrightarrow m_{2,1}$$

$$|1\rangle\langle 1| \otimes |0\rangle\langle 1| \leftrightarrow m_{3,4}$$

$$|1\rangle\langle 1| \otimes |1\rangle\langle 0| \leftrightarrow m_{4,3}$$

La notazione appena sviluppata può rivelarsi pesante, così viene naturale cercare una forma alternativa per rappresentare questi elementi. Una convenzione ampiamente usata è di

accorpare i ket insieme ai ket e i bra insieme ai bra come segue:

$$
\begin{aligned}
&|0\rangle\langle 0| \otimes |0\rangle\langle 0| \leftrightarrow m_{1,1} \leftrightarrow |00\rangle\langle 00| \\
&|0\rangle\langle 0| \otimes |0\rangle\langle 1| \leftrightarrow m_{1,2} \leftrightarrow |00\rangle\langle 01| \\
&|0\rangle\langle 1| \otimes |0\rangle\langle 0| \leftrightarrow m_{1,3} \leftrightarrow |00\rangle\langle 10| \\
&|0\rangle\langle 1| \otimes |0\rangle\langle 1| \leftrightarrow m_{1,4} \leftrightarrow |00\rangle\langle 11| \\
&|0\rangle\langle 0| \otimes |1\rangle\langle 0| \leftrightarrow m_{2,1} \leftrightarrow |01\rangle\langle 00| \\
&|0\rangle\langle 0| \otimes |1\rangle\langle 1| \leftrightarrow m_{2,2} \leftrightarrow |01\rangle\langle 01| \\
&|0\rangle\langle 1| \otimes |1\rangle\langle 0| \leftrightarrow m_{2,3} \leftrightarrow |01\rangle\langle 10| \\
&|0\rangle\langle 1| \otimes |1\rangle\langle 1| \leftrightarrow m_{2,4} \leftrightarrow |01\rangle\langle 11| \\
&|1\rangle\langle 0| \otimes |0\rangle\langle 0| \leftrightarrow m_{3,1} \leftrightarrow |10\rangle\langle 00| \\
&|1\rangle\langle 0| \otimes |0\rangle\langle 1| \leftrightarrow m_{3,2} \leftrightarrow |10\rangle\langle 01| \\
&|1\rangle\langle 1| \otimes |0\rangle\langle 0| \leftrightarrow m_{3,3} \leftrightarrow |10\rangle\langle 10| \\
&|1\rangle\langle 1| \otimes |0\rangle\langle 1| \leftrightarrow m_{3,4} \leftrightarrow |10\rangle\langle 11| \\
&|1\rangle\langle 0| \otimes |1\rangle\langle 0| \leftrightarrow m_{4,1} \leftrightarrow |11\rangle\langle 00| \\
&|1\rangle\langle 0| \otimes |1\rangle\langle 1| \leftrightarrow m_{4,2} \leftrightarrow |11\rangle\langle 01| \\
&|1\rangle\langle 1| \otimes |1\rangle\langle 0| \leftrightarrow m_{4,3} \leftrightarrow |11\rangle\langle 10| \\
&|1\rangle\langle 1| \otimes |1\rangle\langle 1| \leftrightarrow m_{4,4} \leftrightarrow |11\rangle\langle 11|
\end{aligned}
\tag{5.42}
$$

Usando le relazioni 5.42 possiamo riscrivere l'operatore

$$\mathbf{I} \otimes \sigma_{\mathbf{y}}$$

in forma compatta come mostrato dalla seguente:

$$\mathbf{I} \otimes \sigma_{\mathbf{y}} = -i|00\rangle\langle 01| + i|01\rangle\langle 00| - i|10\rangle\langle 11| + i|11\rangle\langle 10| \qquad (5.43)$$

Faremo uso di questa notazione dopo aver introdotto la *sfera di Bloch* e le trasformazioni unitarie dei qubits.

5.7 Misure di bits e misure di qubits

5.7.1 Misura di un bit

Anche un singolo bit può essere molto utile. Per esempio nel linguaggio assembly (cioè nel linguaggio più vicino alla sequenza di 1 e 0 compresa da un computer), si esegue la lettura di un singolo bit per verificare se una espressione relazionale è vera o falsa. Ad esempio se vogliamo confrontare il contenuto di due registri e sapere quale è il più grande possiamo usare l'istruzione di confronto e poi il salto condizionato che si basa sul valore di un bit di flag. Confrontare i valori presenti in due registri è quindi una operazione che richiede la lettura di un bit. La lettura di bits è una operazione comune in quasi tutti i linguaggi

di programmazione[4] Nell'informatica classica si è soliti riferirsi all'operazione di lettura di un bit e non a quella di misura. Il termine lettura però è solo un'astrazione dell'operazione concreta eseguita dal computer che dal punto di vista fisico esegue in pratica una misura. Se ciò può suonare strano, si consideri che la misura non viene eseguita da un essere umano, ma dall'elettronica del computer che provvede a trasformare una grandezza fisica in un'altra più utile alla computazione. Per esempio se la memoria in questione è basata sul principio di condensazione della carica elettrica (vedi figura 5.7), allora la misura consiste nel trasformare la carica elettrica presente nel condensatore all'indirizzo hardware del bit b_n in un valore di tensione elettrica processabile dalla CPU del computer. Tale misura avviene attivando simultaneamente due linee elettriche dette *worldline* e *bitline* che permettono al condensatore di scaricare la carica immagazzinata tra le armature generando una piccolissima corrente elettrica. Tale corrente viene amplificata e trasformata in un segnale di tensione logico, tipicamente tra

[4]Nelle architetture degli elaboratori elettronici convenzionali, i valori dei bits vengono letti e modificati in otteti (i bytes), ma per semplificare la discussione, nel seguito del paragrafo, ragioneremo in termini di scrittura e lettura di singoli bits classici.

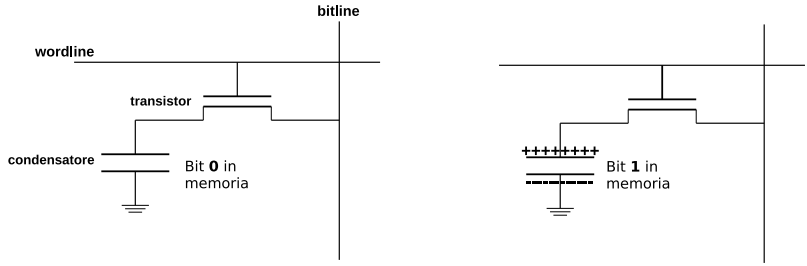

Figura 5.7: La figura mostra lo schema circuitale per la memorizzazione e la lettura di un bit. La figura di sinistra presenta il condensatore scarico, quindi il bit 0, mentre in quella di destra si vedono sulle due armature del condensatore i segni + e - ad indicare l'accumolo di carica elettrica e quindi il bit 1.

gli 0 e i 5 Volt. Se il condensatore è carico allora il bit è nello stato 1 altrimenti è nello stato 0.

Nella computazione classica, non c'è differenza tra lo stato di un bit ed il risultato dell'operazione di lettura di tale bit. Si supponga che il bit b_n della memoria sia posto nello stato 1 durante una operazione di scrittura, in questo caso si è certi che una successiva lettura dello stesso bit dovrà dare come risultato il valore 1. È possibile che a causa di *errori hardware* il bit cambi il proprio valore e quindi che la lettura dia il valore 0 anziché l'1. Questa eventualità, che comunque è prevista e

corretta dai computer stessi, rappresenta un errore di funzionamento: la regola è che ciò che viene letto corrisponde a ciò che è stato scritto. Ogni deviazione da questo rappresenta un errore.

Come vedremo ora, questa regola non si applica alla misura dei qubits.

5.7.2 Misura di un qubit

I concetti di lettura e misura di un qubit sono presenti anche nell'informatica quantistica, ma mentre in quella classica si predilige il termine *lettura* in quella quantistica si predilige *misura* perché la teoria quantistica è formulata attorno al concetto stesso di misura.

La misura di un qubit dipende dalla tecnologia con cui esso è stato realizzato. Il caso più semplice da illustrare è quello della tecnologia fotonica, cioè la tecnologia che impiega i quanti elementari del campo elettromagnetico come qubits. I fotoni hanno una proprietà detta polarizzazione che è descritta da un vettore complesso di dimensione due[3] e quindi ha le caratteristiche viste nel capitolo precedente per rappresentare il qubit. I computer quantistici di tipo fotonico, usano i fotoni come

qubits e ne trasformano lo stato per mezzo di operatori logici detti *quantum gates*. Durante la computazione di un programma quantistico i qubits possono dover essere letti, come accade nella computazione classica, e questo significa dover misurare lo stato di polarizzazione del fotone associato. Questa misura si può implementare utilizzando un *polarizzatore lineare* e un *rivelatore*. Lo schema sperimentale per eseguire la misura della polarizzazione di un fotone è riportato in figura 5.8. Il polarizzatore lineare è uno strumento che ha la caratteristica di lasciare passare solo i fotoni la cui polarizzazione ha la stessa direzione del suo asse di polarizzazione, mentre gli altri vengono assorbiti al suo interno. Il polarizzatore può quindi essere usato per filtrare i fotoni che abbiano una specifica polarizzazione.

I fotoni che sono trasmessi attraverso il polarizzatore raggiungono il rivelatore. Questo è uno strumento che ha il compito di generare un segnale *trattabile*, cioè rilevabile da un normale amplificatore, quando viene attraversato da un fotone. Un tipico esempio di rivelatore è lo *scintillatore*.

Rivelare la presenza di un fotone non è una cosa semplice perché non ha né carica elettrica né massa inerziale. Per rivelarlo è necessario sfruttare la sua natura di *mediatore*, infatti il fotone trasporta l'energia del campo elettromagnetico a particelle come l'elettrone che invece hanno carica e massa. Il fotone può essere assorbito e la sua energia viene acquisita dal sistema che lo assorbe. Per esempio lo scintillatore è formato da un cristallo che assorbe facilmente il fotone e produce altri fotoni secondari a più bassa energia. Questi ultimi, a causa della loro energia minore, si trasmettono liberamente dentro al cristallo stesso. Il cristallo è normalmente accoppiato ad un fotocatodo che assorbe i fotoni secondari ed emette elettroni. Questi vengono raccolti ed accelerati in un tubo a vuoto innescando un effetto a cascata che amplifica la corrente elettronica prodotta dal fotocatodo. In questo modo è possibile rilevare la presenza di un fotone e quindi conoscerne la polarizzazione che aveva al momento della rivelazione.

Quello che abbiamo descritto è quindi un sistema per misurare un qubit, in figura 5.9 è presentata una schematizzazione del sistema di misura.

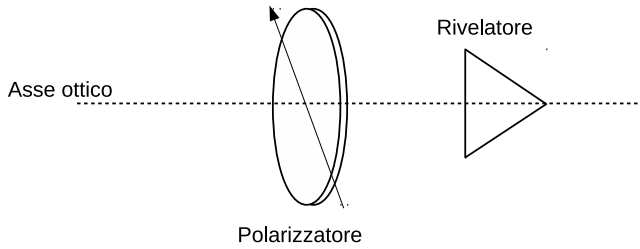

Figura 5.8: La figura mostra lo schema concettuale per la lettura di un qubit. I qubit si propagano lungo l'asse ottico sotto forma di fotoni, lo stato del qubit corrisponde allo stato del fotone. Quando il fotone raggiunge il polarizzatore, il suo stato deve assumere uno fra i due possibili stati base 0 oppure 1. Se la polarizzazione assunta dal fotone coincide con la direzione del polarizzatore il fotone lo attraversa e viene assorbito dal rivelatore che ne rivela quindi la polarizzazione.

Assi di polarizzazione e base del qubit Come si è capito dal paragrafo 5.3.2 lo stato di un qubit deve essere sempre espresso rispetto ad una coppia di stati fisici, per esempio i due stati corrispondenti alla polarizzazione parallela all'asse $\hat{i}$ e quella parallela all'asse $\hat{j}$. In termini matematici diremo che questi definiscono una base completa di vettori o ket per rappresentare ogni possibile stato fisico del qubit.

Gli stati base del qubit dipendono da come si realizza fisicamente il qubits stesso, nel caso del fotone, è necessario sce-

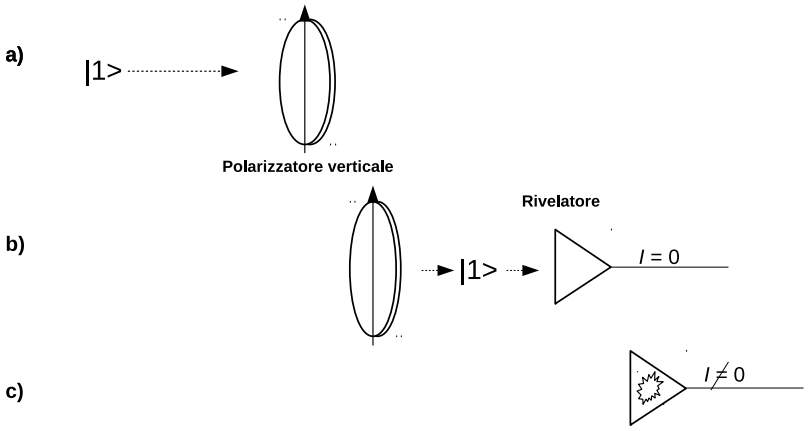

Figura 5.9: La figura mostra la misura di un qubit nello stato 1 per mezzo di un polarizzatore lineare diretto lungo la verticale ed un rivelatore a scintillazione. a) Il qubit raggiunge il polarizzatore, b) il qubit passa attraverso il polarizzatore, c) il fotone viene assorbito dallo scintillatore

gliere due stati di polarizzazione come base. Dal momento che i qubits al termine della computazione vengono misurati per mezzo di strumenti come una coppia di polarizzatori con assi reciprocamente perpendicolari o un polarizzatore a due vie (per esempio un *beam splitter*), è naturale scegliere come stati di base i due assi dei polarizzatori.

Cosa cambia tra le due misure? Nei due paragrafi precedenti si è visto che entrambe le letture di un bit classico e di un

qubit sono misure di quantità fisiche, eppure l'una misura un *sistema classico*, l'altra un sistema quantistico e in questa differenza si trova la ragion d'essere della meccanica quantistica. La differenza tra i due tipi di misura è che il risultato della prima misura dipende solo dallo stato fisico in cui si trova il bit (classico) all'istante in cui viene misurato, mentre il risultato della misura quantistica dipende sempre dallo stato in cui si trova il qubit all'istante della misura, ma solo in modo probabilistico. Sembra strano? Si lo è, è sembrato talmente strano che anche fisici della levatura di Albert Einstein[4] non hanno mai completamente abbracciato la teoria quantistica.

Facciamo un esempio: supponiamo che un bit sia nello stato 1 quindi, con riferimento alla figura 5.7, sappiamo che sulle facce del condensatore è presente una carica elettrica. Nel momento un cui il bit viene misurato siamo assolutamente sicuri che la chiusura del circuito permetterà al condensatore di scaricarsi e quindi a noi di ottenere la misura 1 del bit. Si presti solo attenzione che quando scriviamo *assolutamente sicuri*, intendiamo dire che siamo sicuri della legge fisica che porterà inevitabilmente il condensatore a scaricarsi ma, nonostante

questa sicurezza, potrebbero intervenire dei fattori accidentali, come imperfezioni dell'hardware, campi elettrici esterni ecc.., a rendere *aleatoria* questa sicurezza. Per ora tralasciamo questa aleatorietà e supponiamo di avere un hardware perfetto e di essere sufficientemente isolati da fattori esterni che potrebbero compromettere la misura. In tali condizioni, siamo sicuri del risultato della misura. Questo è un assunto fondamentale, su cui si basa l'intera formulazione della MdT classica.
Supponiamo ora che un qubit si trovi nello stato $|\psi\rangle = \frac{1}{\sqrt{2}}|1\rangle + |0\rangle$ e di volerlo misurare usando un polarizzatore orientato parallelamente alla direzione di polarizzazione dello stato $|1\rangle >$. In questo caso non possiamo essere sicuri del risultato della misura, infatti è possibile sia che il qubit venga misurato nello stato $|1\rangle$ che nello stato $|0\rangle$, questo si distingue fortemente dalla misura classica in cui il risultato è certo.

Classico e quantistico possono sembrare due mondi separati, ma non è esattamente così. Il mondo classico, cioè il mondo di cui abbiamo maggior esperienza è comunque un sistema quantistico, cioè soggetto alle leggi della meccanica quantistica, ma è un mondo talmente *ingarbugliato* e ricco di interconnessioni tra le parti che lo costituiscono, che gli effetti quantistici

non sono visibili. Immaginiamo di avere tra le mani un morbido lenzuolo di seta, a noi apparirà liscio e omogeneo, in pratica non avvertiremo la struttura della sua trama, ma ad un acaro che ci vive dentro apparirà come un ambiente complesso ricco di strutture in cui cercare cibo e nascondersi da altri acari. In modo simile appare a noi la meccanica quantistica, se vivessimo su scala atomica, avremmo a che fare tutti i giorni con le sue leggi, ma vivendo su una scala amplificata di decine di miliardi di volte, questi effetti diventano trascurabili e quello che sperimentiamo è un *effetto medio* simile a quello che sperimentiamo passando la mano sulla seta: la struttura della seta esiste, ma con la mano percepiamo una apparente continuità data dalla media delle imperfezioni stesse.

Dove finisce la validità dell'approssimazione classica? In fisica c'è una quantità chiamata *azione* che può essere calcolata per ogni sistema dinamico. L'azione è talmente importante che tutto l'apparato della fisica teorica classica e relativistica può essere derivato da un principio che richiede che i sistemi dinamici evolvano nel tempo in modo che l'azione abbia sempre il valore minimo possibile. La trattazione quantistica diventa *imprescindibile* quando il valore dell'azione è molto piccolo.

Cosa è piccolo e cosa è grande dipende però dalla scala che si sta usando, nel caso in questione si ha un valore preciso noto come *costante di Planck* che ha il valore di circa 6.6×10^{-34} J·s (Jaul per secondo) e si indica con la lettera h. Se l'azione di un sistema è paragonabile alla costante di Planck allora questo deve essere trattato in termini quantistici.

Il problema di distinguere a priori quando un sistema possa essere considerato classico fu trattato in dettaglio dal fisico PAM Dirac, uno dei padri fondatori della meccanica quantistica[1]. Dalla sua trattazione, che richiede studi specifici di teoria dei campi per essere compresa nei dettagli, emerge che quando l'azione è molto maggiore di h gli effetti quantistici si sovrappongono con interferenza distruttiva e quello che rimane è l'effetto medio, appunto la meccanica classica.

5.7.3 Misura quantistica

Nella sezione precedente abbiamo chiarito cosa sia un qubit e come esso possa essere misurato, d'altra parte abbiamo anche scritto che il risultato di una misura non è sempre prevedibile. In questo paragrafo vediamo che esiste una legge che permette

di conoscere la probabilità del risultato di una misura di un qubit.

La legge è molto semplice. Consideriamo un qubit rappresentato dallo stato $|\psi\rangle$ dato da:

$$|\psi\rangle \equiv \alpha|0\rangle + \beta|1\rangle \tag{5.44}$$

il risultato di una misura eseguita come spiegato nel paragrafo precedente ha probabilità data da α^2 di risultare lo stato $|0\rangle$ e β^2 di risultare lo stato $|1\rangle$. Siccome ad ogni esperimento troveremo sempre che lo stato è esclusivamente $|0\rangle$ oppure $|1\rangle$ è chiaro che la somma delle probabilità dei due eventi deve dare la certezza, quindi in formule abbiamo $\alpha^2 + \beta^2 = 1$, come già formulata nella 5.8.

Questo aspetto aleatorio della meccanica quantistica è alquanto particolare e si distacca dall'idea di fisica deterministica che normalmente si forma alle scuole secondarie ed era stata protagonista nei secoli dell'illuminismo. Va anzitutto notato che la fisica rimane deterministica, infatti il calcolo della probabilità con cui si verificherà l'uno o l'altra ipotesi è assolutamente certo, quello che non è certo a priori è in quale stato si troverà il qubit dopo una misura.

Questo schema aleatorio ammette però una eccezione. Infatti se il qubit si trova in un autostato, cioè in uno stato perfettamente corrispondente alla direzione di uno dei due polarizzatori che verrà usato per rivelarlo, allora la sua misura è certa. Per esempio se il qubit si trova nello stato $|0\rangle$ e viene rivelato da un polarizzatore in direzione $\hat{i}$ allora esso verrà sicuramente misurato come uno $|0\rangle$. Questo ci da la possibilità di usare i qubits sempre in stati corrispondenti agli autostati per replicare completamente il comportamento della computazione classica.

5.8 Esercizi

5.8.1 Esercizi risolti

- Esercizio 1: La figura 5.10 mostra un apparato per il rivelamento di fotoni. L'apparato è composto da una sorgente di fotoni polarizzati, un filtro polaroid e uno scintillatore.
  I fotoni sono polarizzati con un angolo di 30 gradi rispetto l'asse di polarizzazione.
  Calcolare il *valore atteso* di scintillazioni a fronte di 100 spari di fotoni (tutti con la stessa polarizzazione).

  Lo stato di polarizzazione $|\psi\rangle$ dei fotoni uscenti dalla sor-

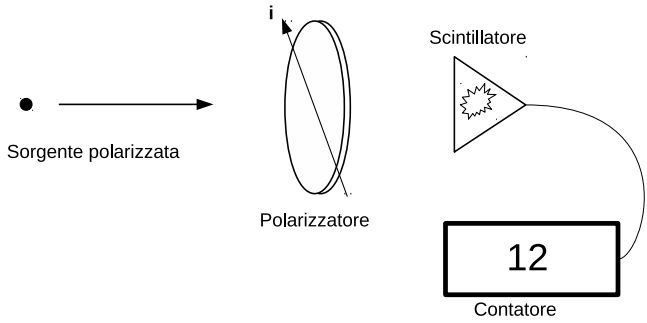

Figura 5.10: In figura è rappresentato il setup sperimentale per l'emissione e il conteggio di fotoni

gente può essere scritto come:

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

Il valore di α è dato dal seno dell'angolo che la direzione di polarizzazione forma con l'asse $\hat{i}$, quindi $\alpha = \sin(\pi/6)$ mentre quello di β è dato dal coseno: $\beta = \cos(\pi/6)$. Ogni fotone che attraversa il polarizzatore ha probabilità $p = \alpha^2$ di essere trasmesso e raggiungere lo scintillatore e probabilità $p = \beta^2$. Il valore atteso di conteggi è allora dato dal numero di spari per la probabilità che ogni sparo raggiunga lo scintillatore, quindi i conteggi c sono dati da: $c = 100 \times \cos(\pi/6) = 75$

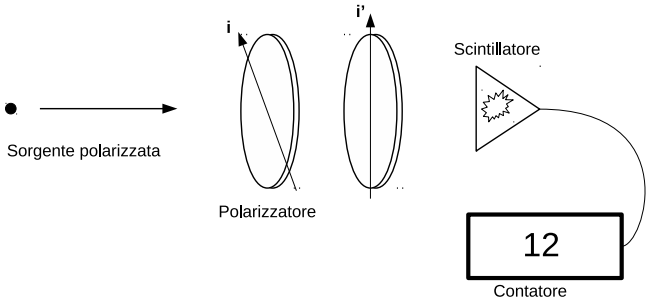

Figura 5.11: In figura è repparesentato lo stesso setup di figura 5.10 con l'aggiunta di un secondo polarizzatore.

- Esercizio 2: La figura 5.11 mostra un apparato per il rivelamento di fotoni simile a quello usato nell'esercizio precedente. L'apparato è composto da una sorgente di fotoni polarizzati, due filtri polaroid sfasati di 45 gradi l'uno rispetto all'altro e uno scintillatore.
  I fotoni sono polarizzati con un angolo di 30 gradi rispetto l'asse di polarizzazione.
  Calcolare il *valore atteso* di scintillazioni a fronte di 100 spari di fotoni (tutti con la stessa polarizzazione).

  Come per l'esercizio precedete, lo stato di polarizzazione $|\psi\rangle$ dei fotoni uscenti dalla sorgente può essere scritto

come:

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

Il valore di α è dato dal seno dell'angolo che la direzione di polarizzazione forma con l'asse $\hat{i}$, quindi $\alpha = \sin(\pi/6)$ mentre quello di β è dato dal coseno: $\beta = \cos(\pi/6)$. Ogni fotone che attraversa il polarizzatore ha probabilità $p = \alpha^2$ di essere trasmesso e raggiungere lo scintillatore e probabilità $p = \beta^2$. Il valore atteso di fotoni che raggiungeranno il secondo polarizzatore è dato dal numero di spari per la probabilità che ogni sparo superi il primo polarizzatore, quindi i fotoni s sul secondo polarizzatore sono dati da: $s = 100 \times \cos(\pi/6) = 75$.

I fotoni uscenti dal primo scintillatore sono tutti nello stato $|0\rangle$ riferito alla direzione dell'asse $\hat{i}$. Dal momento che l'asse di polarizzazione $\hat{i}'$ del secondo polarizzatore è ruotato di 45 gradi ($\pi/4$) rispetto ad $\hat{i}$, possiamo scrivere che lo stato $|\psi\rangle$ dei fotoni uscenti dal primo polarizzatore può essere scritto come

$$|\psi\rangle = \cos(\pi/4)|0\rangle + \cos(\pi/4)|1\rangle$$

dove ora lo stato $|0\rangle$ è espresso rispetto alla direzione $\hat{i}'$ e

non più alla direzione $\hat{i}$.

La probabilità dei fotoni di attraversare il secondo polarizzatore è allora data da: $p = \cos(\pi/4)^2 = 1/2$. Visto che s fotoni raggiungono il secondo polarizzatore, si avrà che il numero di conteggi atteso è dato da $c = 100 \times \cos(\pi/6) \times \cos(\pi/4)^2 = 37$

5.8.2 Esercizio proposto

- Esercizio: Progettare un sistema sperimentale composto da una sorgente di fotoni polarizzati, tre filtri polarizzatori, uno scintillatore ed un contatore, in modo che il valore atteso di conteggi sia un decimo del numero di fotoni emessi.

CAPITOLO 6

Sfera di Bloch

Rappresentare un bit è facile, infatti basta pensare a uno dei due possibili valori che esso può assumere che sono esclusivamente 0 ed 1. La semplicità con cui è possibile costruire le tabelle di verità delle funzioni logiche deriva anche da questa immediatezza dei bits. I qubits invece sono quantità complesse e quindi più sfuggenti all'intuizione. Un valido aiuto per manipolarli e prendere confidenza è quello di poterli rappresentare in modo visivo. Il metodo comunemente usato è quello noto come sfera di Bloch. Avere confidenza con i qubits e poterli immaginare semplifica molto l'attività di progettazione e analisi dei circuiti quantistici, infatti essi sono composti da *quantum*

gates cioè matrici (più correttamente tensori[3]) che operano delle rotazioni e altre trasformazioni di simmetria, nello spazio complesso dei qubits. In pratica ogni trasformazione di un qubit può essere vista come una trasformazione (i.e. rotazione, riflessione...) che avviene nello spazio complesso $\mathbb{C}^2$ e non nello spazio ordinario $\mathbb{R}^3$. Come si è visto nel primo capitolo, un vettore dello spazio $\mathbb{C}^2$ è descritto da due componenti complesse, quindi quattro numeri reali, quindi la rappresentazione grafica di un vettore complesso richiede una rappresentazione in quattro dimensioni (4D) che ovviamente non può essere rappresentata graficamente neanche usando le regole della prospettiva. A differenza di un generico vettore complesso, i qubits devono sottostare alla regola di *unitarietà* che impone un vincolo sul loro modulo (vedi paragrafo 5.3), quindi i veri gradi di libertà in cui può muoversi un qubit non sono quattro ma tre. Questo permette di rappresentare i qubit in uno spazio 3D e quindi di rappresentarli in 2D usando le regole della prospettiva.
La sfera di Bloch è un modo diretto e chiaro per rappresentare i qubit in 3D.

In figura 6.1 è rappresentata la sfera di Bloch o *Bloch spehere*.

Si tratta di un sistema costituito da un terna di assi perpendicolari tra loro ed una sfera il cui centro geometrico coincide con l'origine O degli assi.

Diversamente dalla ordinaria terna di assi cartesiani $Oxyz$ però, gli assi della sfera di Bloch non rappresentano le direzioni indipendenti che esistono nello spazio fisico (i.e. altezza, larghezza e profondità dello spazio).

Questo punto è molto importante e deve essere analizzato con cura. Infatti, come è stato scritto ad inizio capitolo, le trasformazioni *unitarie* che preservano il modulo del qubit sono analoghe a rotazioni nello spazio cartesiano 3D. Il termine esatto che descrivere la relazione tra le prime e le seconde non è *analogia* bensì *omomorfismo suriettivo* che significa che tutte le rotazioni nello spazio $\mathbb{R}^3$ sono trasformazioni unitarie in $\mathbb{C}^2$ ma che esistono alcune trasformazioni di $\mathbb{C}^2$ che non hanno un analogo tra le rotazioni in $\mathbb{R}^3$. Affronteremo questo problema nel prossimo paragrafo, mentre qui è importante notare che l'omomorfismo esistente tra le trasformazioni non è limitato allo spazio *fisico*, ma in generale ad uno spazio a tre dimensioni reali, quindi possiamo costruire la sfera di Bloch in $\mathbb{R}^3$ anche se gli assi non sono i consueti x, y e z ma quelli indicati in figura

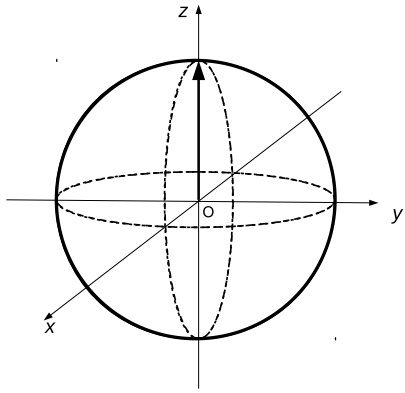

Figura 6.1: La sfera di Bloch.

6.1.

6.1 Rappresentazione di un qubit nella sfera

6.1.1 Proiezione del qubit sul piano complesso

In questa sezione vediamo il procedimento matematico che si deve seguire per rappresentare un qubit sulla sfera di Bloch. É giusto avvertire che questo potrebbe risultare un po' complicato, ma vale la pena seguirne i passaggi senza troppo timore, infatti poi nella pratica le cose si semplificano.

Ricordiamo che la forma generale in cui possiamo scrivere un singolo qubit è la seguente:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \tag{6.1}$$

I coefficienti α e β sono numeri complessi ognuno dei quali è formato da una coppia di numeri reali (componente reale e componente immaginari) e quindi il qubit è identificato da due coppie di numeri reali. La relazione 5.8 aggiunge un vincolo (o relazione) tra questi quattro numeri e quindi elimina un grado di libertà, quindi un qubit è identificato da tre soli valori. Alla relazione 5.8 va aggiunta la 5.9 che si è visto discendere direttamente dalla natura fisica del qubit. Infatti, uno stato quantistico non cambia se viene moltiplicato per un numero complesso che abbia modulo 1, quindi il qubit $|\psi\rangle$ è equivalente al qubit $e^{i\theta}|\psi\rangle$ dove il coefficiente $e^{i\theta}$ è appunto un numero complesso espresso in forma esponenziale e di modulo 1. Questo non è propriamente un vincolo che abbassa il numero dei gradi di libertà, però ci permette di introdurre il parametro complesso

$a = s + it$ come segue[1]:

$$a = \frac{\alpha}{\beta} \tag{6.2}$$

quindi, s rappresenta la parte reale di $a = \frac{\alpha}{\beta}$ mentre t la parte immaginaria.

Definito a possiamo definire i coefficienti α e β rispetto ad a come:

$$\alpha = \frac{1}{\sqrt{1 + |a|^2}} \text{ e } \beta = \frac{a}{\sqrt{1 + |a|^2}} \tag{6.3}$$

in pratica la 6.3 definisce la trasformazione inversa della 6.2.

Le trasformazioni definite in 6.2 e 6.3 rappresentano una proiezione da $\mathbb{C}^2$ a $\mathbb{C}^1$, infatti vediamo che i vettori complessi di dimensione 2 definiti in 6.1 sono mappati dal vettore complesso a di dimensione 1. La trasformazione 6.2 però non è definita quando $\alpha = 0$ e $\beta = 1$, quindi, come accennato ad inizio sezione, esiste un elemento che non è mappato. Per completare la mappatura si aggiunge *artificiosamente* un elemento al piano complesso che viene indicato con il simbolo ∞ e si fa corrispondere al vettore complesso di componenti (0,1), quindi al ket $|1\rangle$.

Riassumendo, in questo paragrafo sono state definite delle tra-

[1] In termini fisici e matematici, si dice che lo spazio degli stati del qubit è ridotto a CP^1 che è lo spazio proiettivo per i vettori complessi di dimensione due.

sformazioni matematiche che permettono di mappare i qubit che *vivono* nello spazio $\mathbb{C}^2$ nello spazio $\mathbb{C}$ più il punto ∞. Questo risultato è molto importante in quanto lo spazio $\mathbb{C}$ ha due dimensioni reali, in pratica ogni elemento di $\mathbb{C}$ ha una corrispondenza in $\mathbb{R}^2$ e gli elementi di $\mathbb{R}^2$ possono essere messi in corrispondenza con i punti della superficie di una sfera per mezzo della *proiezione stereografica* che definiamo ora.
Prima di procedere con il procedimento di proiezione, vediamo come le 6.2 e 6.3 mappano alcuni qubits notevoli:

- $|0\rangle \to 0 + 0i$

  Dimostrazione: Il ket $|0\rangle$ corrisponde al vettore complesso di componenti $\alpha = 1$ e $\beta = 0$. Dalle 6.2 otteniamo $a = \frac{\beta}{\alpha} = \frac{0}{1} = 0 + 0i$ quindi $s = 0$ e $t = 0$.

- $|1\rangle \to \infty$

  Dimostrazione: Il ket $|1\rangle$ corrisponde al vettore complesso di componenti $\alpha = 0$ e $\beta = 1$. Dalle 6.2 otteniamo $a = \frac{\beta}{\alpha} = \frac{1}{0}$ che non è definito in matematica. Quindi associamo *artificiosamente* l'elemento ∞ al ket $|1\rangle$.

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

  Dimostrazione: Il ket $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ corrisponde al vettore

complesso di componenti $\alpha = \frac{1}{\sqrt{2}}$ e $\beta = \frac{1}{\sqrt{2}}$. Dalle 6.2 otteniamo $a = \frac{\beta}{\alpha} = \frac{\frac{1}{\sqrt{2}}}{\frac{1}{\sqrt{2}}} = 1 + 0i$ quindi $s = 1$ e $t = 0$.

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

  Dimostrazione: Il ket $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ corrisponde al vettore complesso di componenti $\alpha = \frac{1}{\sqrt{2}}$ e $\beta = -\frac{1}{\sqrt{2}}$. Dalle 6.2 otteniamo $a = \frac{\beta}{\alpha} = \frac{\frac{1}{\sqrt{2}}}{-\frac{1}{\sqrt{2}}} = -1 + 0i$ quindi $s = -1$ e $t = 0$.

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

  Dimostrazione: Il ket $\frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)$ corrisponde al vettore complesso di componenti $\alpha = \frac{1}{\sqrt{2}}$ e $\beta = \frac{i}{\sqrt{2}}$. Dalle 6.2 otteniamo $a = \frac{\beta}{\alpha} = \frac{\frac{i}{\sqrt{2}}}{\frac{1}{\sqrt{2}}} = 0 + i$ quindi $s = 0$ e $t = 1$.

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

  Dimostrazione: Il ket $\frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)$ corrisponde al vettore complesso di componenti $\alpha = \frac{1}{\sqrt{2}}$ e $\beta = \frac{-i}{\sqrt{2}}$. Dalle 6.2 otteniamo $a = \frac{\beta}{\alpha} = \frac{\frac{-i}{\sqrt{2}}}{\frac{1}{\sqrt{2}}} = 0 - i$ quindi $s = 0$ e $t = -1$.

6.1.2 Proiezione stereografica

Con le 6.2 e 6.3 si è definita una trasformazione che associa un qubit ad un numero complesso $a \in \mathbb{C}$. In quest'ultima espressione, scrivendo esplicitamente che a appartiene ($\in$) a $\mathbb{C}$ si è voluto ribadire che il numero a è complesso quindi ha una parte

reale ed una immaginaria che possiamo scrivere come:

$$a = s + it$$

dove s è la parte reale e t è il coefficiente complesso (non si sono usate α e β per non fare confusione con l'espressione 6.2).
Introduciamo ora tre nuove relazioni definite come segue:

$$\begin{aligned} x &= \frac{2s}{s^2 + t^2 + 1} \\ y &= \frac{2t}{s^2 + t^2 + 1} \\ z &= \frac{1 - s^2 - t^2}{s^2 + t^2 + 1} \end{aligned} \tag{6.4}$$

Le 6.4 definiscono una mappa tra il numero complesso a e la terna di numeri reali x, y e z. La terna x, y, z può essere pensata come le tre componenti cartesiane di un punto nello spazio, quindi, con questa idea nella mente, possiamo pensare le 6.4 come una mappa tra il piano complesso e lo spazio cartesiano.
Le 6.4 hanno però una proprietà molto importante, infatti se si prova a sommare i quadrati delle tre componenti cartesiane si trova che la loro somma è sempre uguale all'unità (1) indipendentemente dai valori di s e t, come dimostriamo di seguito.
Per dimostrare che $x^2 + y^2 + z^2 = 1$ prendiamo le definizioni di

x, y, z date nella 6.4 e le eleviamo al quadrato come segue:

$$\begin{aligned} x^2 &= \frac{4s^2}{(s^2+t^2+1)^2} \\ y^2 &= \frac{4t^2}{(s^2+t^2+1)^2} \\ z^2 &= \frac{(1-s^2-t^2)^2}{(s^2+t^2+1)^2} = \frac{1+2s^2t^2-2s^2-2t^2+s^4+t^4}{(s^2+t^2+1)^2} \end{aligned} \tag{6.5}$$

quindi le sommiamo:

$$\begin{aligned} x^2+y^2+z^2 &= \frac{4s^2+4t^2+1+2s^2t^2-2s^2-2t^2+s^4+t^4}{(s^2+t^2+1)^2} = \\ &= \frac{2s^2+2t^2+1+2s^2t^2+s^4+t^4}{(s^2+t^2+1)^2} = \\ &= \frac{(s^2+t^2+1)^2}{(s^2+t^2+1)^2} = 1 \end{aligned} \tag{6.6}$$

Quanto dimostrato ci dice che la mappa creata porta i punti del piano complesso $\mathbb{C}$ sulla superficie di una sfera S^2, quindi riassumendo dall'inizio, è possibile mappare i qubit sulla superficie di una sfera, questa è appunto detta *sfera di Bloch*.

Vediamo qualche esempio di qubit rappresentato sulla sfera di Bloch. Consideriamo innanzi tutto gli stessi stati visti nell'esempio sopra, calcoliamo le coordinate cartesiane x, y e

z e mappiamole sulla sfera di Bloch usando un raggio vettore che dall'origine degli assi conduca verso il punto avente le coordinate individuate.

- Il primo qubit che mappiamo sulla sfera è descritto dal ket $|0\rangle$ (fig. 6.2). Questo come si è visto nell'esempio sopra corrisponde, secondo le 6.3, al numero complesso $a = 0 + 0i$ quindi si ha: $s = 0$ e $t = 0$ che sostituiti nelle 6.4 danno:

$$\begin{aligned} x &= \frac{0}{0^2 + 0^2 + 1} = 0 \\ y &= \frac{0}{0^2 + 0^2 + 1} = 0 \\ z &= \frac{1 - 0^2 - 0^2}{0^2 + 0^2 + 1} = 1 \end{aligned} \tag{6.7}$$

  D'ora in avanti lasceremo il ket $|0\rangle$ in corrispondenza del verso positivo dell'asse delle z.

- In questo secondo esempio vediamo il ket $|1\rangle$ (fig. 6.3). Questo, come si è discusso nel paragrafo precedente, non può essere mappato usando le 6.3 in quanto richiede di dividere il numero 1 per 0, cosa non definita in matematica. Abbiamo visto che il vettore $|1\rangle$ viene associato *artificialmente* all'elemento ∞, questo risolve mezzo problema, però ancora non ci permette di mappare tale vettore sulla

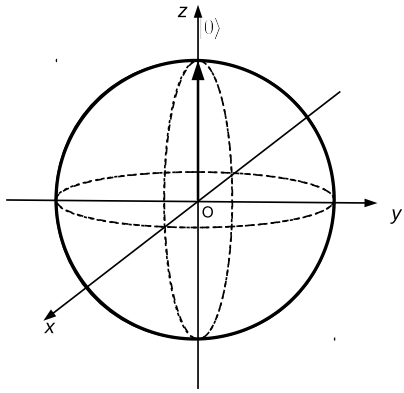

Figura 6.2: Il raggio vettore rappresenta il qubit $|0\rangle$ sulla sfera di Bloch.

sfera in quanto non sappiamo come mappare l'elemento ∞ su di essa.

Per mappare il qubit $|1\rangle$ è necessario eseguire un passaggio al limite. In pratica calcolando le 6.4 scegliendo $t = 1$ e s molto vicino allo 0 si vede che esse assumono un valore sempre più prossimo alla terna (0,0,-1) e si dice che al limite per s che tende a 0 esse valgono esattamente (0,0,-1). Il lettore che non abbia praticità con il calcolo infinitesimale può accettare questo come un dato di fatto senza perdita di generalità dell'intera discussione.

D'ora in avanti lasceremo il ket $|1\rangle$ in corrispondenza del

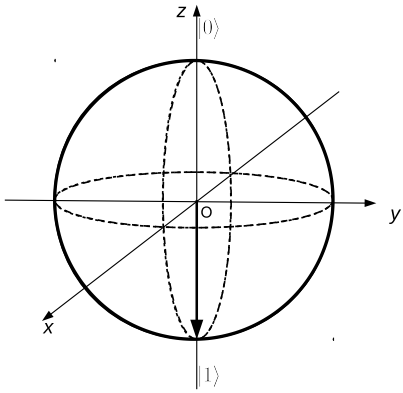

Figura 6.3: Il raggio vettore rappresenta il qubit $|1\rangle$ sulla sfera di Bloch.

verso negativo dell'asse delle z.

- Procediamo con gli esempi mappando il ket $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ sulla sfera di Bloch (fig. 6.4). Questo corrisponde al numero complesso $1 + i0$, quindi $s = 1$ e $t = 0$. Secondo le 6.3 si ha:

$$\begin{aligned} x &= \frac{1}{1^2 + 0^2 + 1} = 1 \\ y &= \frac{0}{1^2 + 0^2 + 1} = 0 \\ z &= \frac{1 - 1^2 - 0^2}{1^2 + 0^2 + 1} = 0 \end{aligned} \tag{6.8}$$

quindi al ket $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ corrisponde la terna (1,0,0).

Il qubit $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ è normalmente indicato anche con il seguente ket $|+\rangle$, mentre il qubit $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ viene comu-

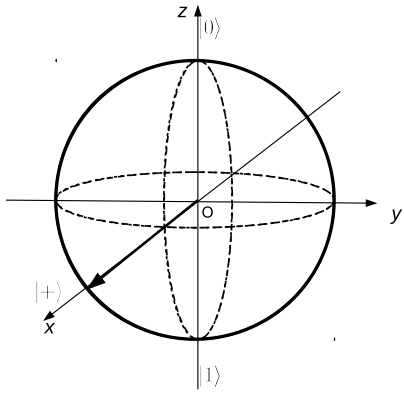

Figura 6.4: Il raggio vettore rappresenta il qubit $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ *sulla sfera di Bloch.*

nemente indicato con $|-\rangle$, è quindi bene imparare questa associazione:

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

D'ora in avanti lasceremo il ket $|+\rangle$ in corrispondenza del verso positivo dell'asse delle x.

- Il ket $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, quindi il ket $|-\rangle$, corrisponde al numero complesso $-1+i0$, quindi $s = -1$ e $t = 0$ (fig. 6.5). Secondo

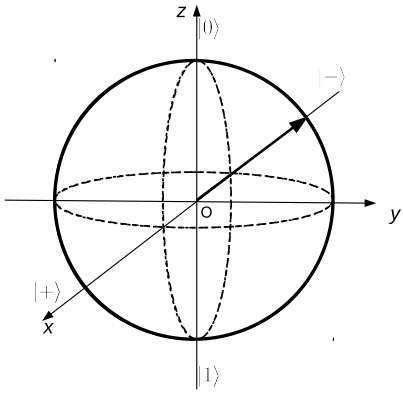

Figura 6.5: Il raggio vettore rappresenta il qubit $|-\rangle$ sulla sfera di Bloch.

le 6.3 si ha:

$$
\begin{aligned}
x &= \frac{-1}{(-1)^2+0^2+1} = -1 \\
y &= \frac{0}{(-1)^2+0^2+1} = 0 \\
z &= \frac{1-(-1)^2-0^2}{(-1)^2+0^2+1} = 0
\end{aligned}
\tag{6.9}
$$

quindi al ket $|-\rangle$ corrisponde alla terna (-1,0,0).

- Il ket $\frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)$ corrisponde al numero complesso $0+i$,

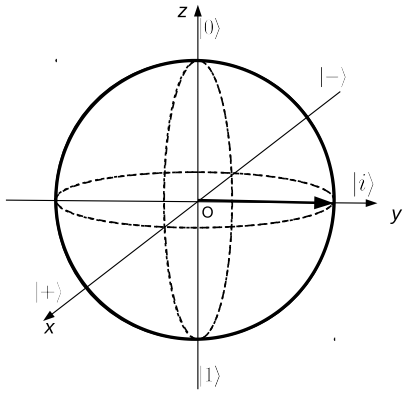

Figura 6.6: Il raggio vettore rappresenta il qubit $|i\rangle$ sulla sfera di Bloch.

quindi $s = 0$ e $t = 1$ (fig. 6.6). Secondo le 6.3 si ha:

$$\begin{aligned} x &= \frac{0}{(0)^2 + 0^2 + 1} = 0 \\ y &= \frac{2}{0^2 + 1^2 + 1} = 1 \\ z &= \frac{1 - (-0)^2 - 1^2}{(0^2 + 1^2 + 1} = 0 \end{aligned} \tag{6.10}$$

quindi al ket $\frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)$ corrisponde la terna (0,1,0).

Il qubit $\frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)$ è normalmente indicato anche con il seguente ket $|i\rangle$, mentre il qubit $\frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)$ viene comunemente indicato con $|-i\rangle$, è quindi bene imparare questa associazione:

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

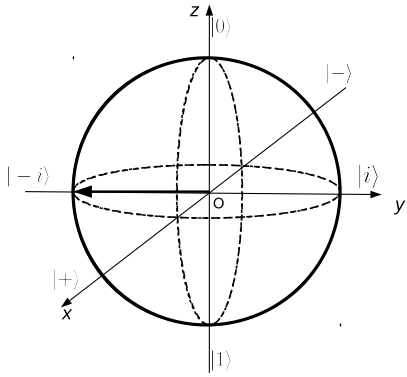

Figura 6.7: Il raggio vettore rappresenta il qubit $|-i\rangle$ sulla sfera di Bloch.

– $\frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle) \equiv |-i\rangle$

D'ora in avanti lasceremo il ket $|i\rangle$ in corrispondenza del verso positivo dell'asse delle y.

- Il ket $\frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)$ corrisponde al numero complesso $0-i$, quindi $s = 0$ e $t = -1$ (fig. 6.7). Secondo le 6.3 si ha:

$$
\begin{aligned}
x &= \frac{0}{(0)^2 + 0^2 + 1} = 0 \\
y &= \frac{-2}{0^2 + (-1)^2 + 1} = -1 \\
z &= \frac{1 - (-0)^2 - (-1)^2}{(0^2 + (-1)^2 + 1} = 0
\end{aligned}
\qquad (6.11)
$$

quindi al ket $|-i\rangle$ corrisponde la terna (0,-1,0).

Il qubit $\frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)$ è normalmente indicato anche con il seguente ket $|i\rangle$, mentre il qubit $\frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)$ viene comunemente indicato con $|-i\rangle$, è quindi bene imparare questa associazione:

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

D'ora in avanti lasceremo il ket $|-i\rangle$ in corrispondenza del verso negativo dell'asse delle y.

6.2 Coordinate sferiche del qubit

Nella sezione precedente abbiamo visto come si possono creare delle trasformazioni matematiche che mappano un qubit nelle coordinate cartesiane di punti che stanno su una superficie sferica di raggio pari ad uno.

Come si è accennato, le operazioni *informatiche* su un qubit equivalgono a rotazioni del qubit rappresentato nella sfera di Bloch. Ogni rotazione è sempre riferita ad un asse e viene parametrizzata attraverso un angolo. Per fare un esempio, le ruote dell'automobile ruotano rispetto al semiasse e ad ogni giro completo corrisponde un angolo di 360 gradi, cioè 2π.

In questo paragrafo individuiamo un metodo per rappresentare i qubits sulla sfera di Bloch in modo che essi siano espressi rispetto agli angoli che formano con gli assi anziché rispetto alle coordinate cartesiane, in questo modo sarà più semplice mettere in relazione le trasformazioni del qubit nello spazio complesso $\mathbb{C}^2$ con le rotazioni nello spazio $\mathbb{R}^3$.

In questa sezione introduciamo quindi il sistema delle *Coordinate sferiche*. In figura 4.1 abbiamo visto che un punto dello spazio può essere rappresentato per mezzo di una terna di coordinate calcolate come la sua proiezione rispetto a tre assi tra loro perpendicolari. Questo modo di rappresentare un punto è detto rappresentazione cartesiana. Lo stesso punto può essere rappresentato anche in un diverso sistema che anziché sfruttare la proiezione del punto rispetto ad una terna di assi, sfrutta l'idea più intuitiva di raggio vettore.

Come per gli assi cartesiani anche questa idea, una volta capita, risulta semplice ed intuitiva. Come per il sistema cartesiano, si parte da una terna di assi perpendicolari che si incontrano in un punto che chiamiamo origine e indicheremo con la lettera O. Dall'origine si traccia un segmento conducendolo fino al punto di interesse che chiameremo P. La lunghezza del

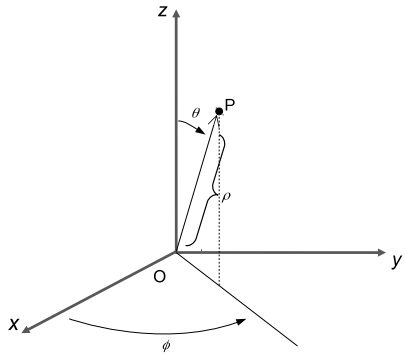

Figura 6.8: Il punto $\mathbf{P}$ *ha coordinate* (ρ, ϕ, θ).

segmento, misurata sempre positiva, da O a P è detta essere il raggio o modulo e si indica con la lettera greca ρ. L'angolo che il raggio forma con l'asse z viene chiamato con la lettera θ, mentre l'angolo che la proiezione del raggio sul piano xy forma con l'asse delle x viene chiamato ϕ. Il sistema descritto è rappresentato in figura 6.8.[2]

Il punto P, che può essere pensato come un *vero punto* nello spazio, può quindi essere mappato usando due diversi sistemi di coordinate: quello cartesiano e quello sferico.

[2]Alcuni testi usano una notazione dei due angoli invertita rispetto a questo. Ovviamente non 'è nessuno specifico significato nella scelta della notazione, ma si ponga attenzione nel caso si debbano confrontare delle formule.

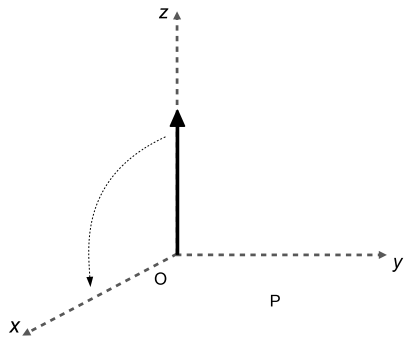

Figura 6.9: Il punto ***P*** *ha coordinate* $(1, \pi/2, \pi/4)$.

6.2.1 Rappresentazione di un punto

Vediamo come tracciare un punto nello spazio usando le coordinate sferiche. Questo esercizio è assolutamente propedeutico al tracciamento dei qubits nella sfera di Bloch. Si consideri, a titolo di esempio, il punto dato dalle coordinate $\rho = 1$, $\theta = \pi/2$ e $\phi = \pi/4$. Esso può esser costruito graficamente come rappresentato in figura 6.11 e come si vede esso coincide con il punto di coordinate cartesiane ($1/\sqrt{2}$,$1/\sqrt{2}$,0). Per ottenere il punto, si può partire dalla situazione raffigurata in figura 6.9 in cui il raggio vettore di modulo $\rho = 1$ è posizionato lungo l'asse delle z. Da quella posizione lo si ruota di 90 gradi ($\pi/2$) verso l'asse delle x fino a farlo appoggiare sull'asse stesso (vedi figura 6.10).

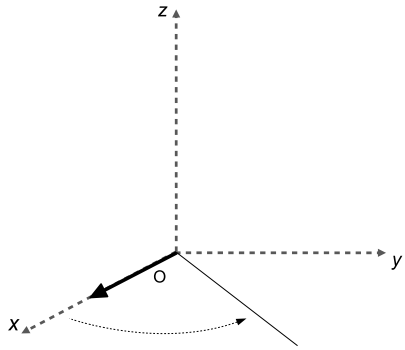

Figura 6.10: Il punto $\mathbf{P}$ *ha coordinate* $(1, \pi/2, \pi/4)$.

Segue poi una seconda rotazione di 45 gradi ($\pi/4$) nel piano xy, quindi attorno all'asse z, come mostrato in figura 6.10, che porta il raggio vettore nella posizione voluta (vedi figura 6.11).

6.2.2 Trasformazione delle coordinate

Nel paragrafo precedente si è visto un esempio intuitivo della relazione tra le tre coordinate ρ, θ e ϕ e le coordinate cartesiane. In questa sezione vediamo che esistono delle specifiche regole di trasformazione che permettono di passare da un sistema (di coordinate) all'altro.

Si consideri il punto P rappresentato in figura 6.12. Le relazioni tre le sue componenti cartesiane x, y e z e le sue coordinate

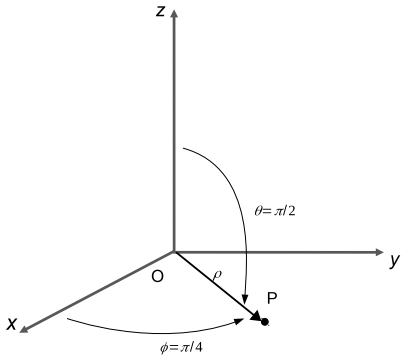

Figura 6.11: Il punto $\boldsymbol{P}$ *ha coordinate* $(1, \pi/2, \pi/4)$.

sferiche sono date dalle seguenti:

$$\begin{aligned} x &= \rho \sin\theta \cos\phi \\ y &= \rho \sin\sin\phi \\ z &= \rho \cos\theta \end{aligned} \tag{6.12}$$

Per comprendere come si giunge a tali relazioni conviene esaminare anzi tutto la terza di esse: $z = \rho\cos\theta$. Come si vede chiaramente in figura 6.12, la proiezione del raggio vettore che conduce dall'origine a P è esattamente il cateto del triangolo che giace sull'asse delle z che misura esattamente $\rho\cos\theta$. Per comprendere le altre due relazioni, conviene calcolare anche la lunghezza del secondo cateto che corrisponde a $\rho\sin\theta$ (vedi figura 6.12). Ora si consideri di proiettare detto cateto sul piano

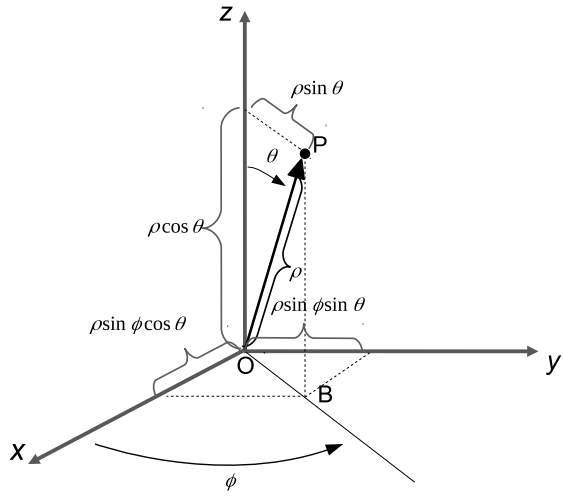

Figura 6.12: Le componenti cartesiane del punto ***P*** *sono espresse rispetto agli angoli* θ *e* ϕ*.*

xy quindi nel punto indicato come B in figura. Costruendo ora un triangolo rettangolo che abbia un vertice in O, uno in B e il terzo sull'asse x (come indicato in figura), si vede che l'ipotenusa OB ha lunghezza $\rho \sin\theta$, mentre il cateto sull'asse delle x è dato dal prodotto dell'ipotenusa per il coseno dell'angolo che essa forma con l'asse delle x, quindi $\cos\phi$, da cui si ha che il cateto è uguale $\rho \sin\theta \cos\phi$. Con la stessa costruzione si vede che il secondo cateto è dato da $\rho \sin\theta \sin\phi$.

Trasformazioni inverse Le relazioni 6.12 definiscono le trasformazioni dal sistema di coordinate sferiche a quello cartesiano. È naturale aspettarsi che sia possibile anche fare il procedimento inverso, quindi calcolare le coordinate sferiche ρ, θ e ϕ quando siano note quelle cartesiane. Tali relazioni *inverse* sono date dalle seguenti:

$$\begin{aligned} \rho &= \sqrt{x^2 + y^2 + z^2} \\ \theta &= \arccos\left(\frac{z}{\rho}\right) \\ \phi &= \arctan\left(\frac{y}{x}\right) \end{aligned} \tag{6.13}$$

Nella prossima sezione sfrutteremo il formalismo fin qui introdotto per comprendere a fondo la natura delle trasformazioni dei qubit da parte dei *quantum gates*, cioè gli operatori quantistici che agiscono sui qubits in modo analogo a come le porte logiche agiscono sui bits.

Parte III

Computazione quantistica elementare

CAPITOLO 7

Trasformazione dei qubits

Cosa fa un computer classico? In cosa consiste la computazione? Se proviamo a guardare al computer come ad una *black box*, cioè come ad una scatola che esegue un lavoro, ma di cui non conosciamo il principio di funzionamento, vediamo che un computer è una macchina che accetta un input binario e restituisce un output binario (vedi figura 7.1).

Lo scopo della computazione è quindi quello di trasformare il valore che hanno i bits di ingresso in quello che devono avere i bits di uscita. Questa affermazione diventa molto più significativa se consideriamo un sistema il cui numero di bits di ingresso coincide esattamente con il numero di bits di usci-

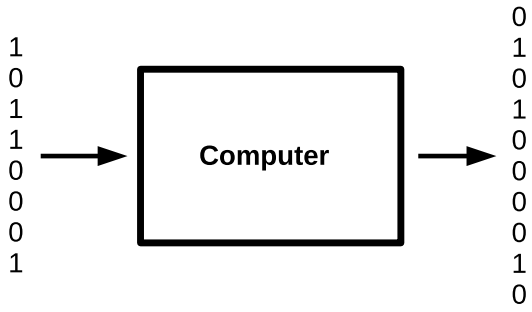

Figura 7.1: Un computer può essere visto come una scatola nera (black box) che accetta un input in formato binario e restituisce un output in formato binario.

ta. In questa ipotesi è immediato pensare alla computazione come ad un processo che agisce su ogni bit. Questo ragionamento, può essere esteso anche al caso in cui il risultato di una elaborazione dipenda non solo dalla configurazione di bits presentata in input, ma anche dalle configurazioni che l'hanno preceduta.

Questo esercizio mentale ci aiuta ad entrare nella logica della computazione quantistica in cui accade esattamente questo. Al contrario dei bits, che in ogni processo elettronico vengono distrutti e ricreati, i qubits mantengono la loro identità durante la computazione e vengono eventualmente distrutti solo all'atto

della loro misura. Questo significa che l'intero processo di computazione è in realtà un processo di trasformazione dei qubits. Per questo il primo passo per comprendere la computazione quantistica consiste esattamente nel prendere confidenza con le trasformazioni dei qubits.

7.1 Operatore X

La prima trasformazione che analizziamo è la trasformazione che porta un qubit dallo stato $|0\rangle$ allo stato $|1\rangle$, quindi una trasformazione con un analogo classico noto.

Questa trasformazione classicamente coincide con l'operazione NOT che può essere scritta come $1 - b$ dove b rappresenta il valore del bit. Se il bit vale 0, allora si ha che $1 - 0 = 1$ quindi b passa da 0 ad 1, mentre se $b = 1$ si ha che $1 - 1 = 0$ e quindi b passa da 1 a 0.

Come si vede da figura 7.4, la trasformazione che porta un qubit da $|0\rangle$ ad $|1\rangle$ è una rotazione di 180 gradi (π) attorno all'asse $|+\rangle$, cioè l'asse delle x. Come è facile immaginare, non è possibile trasformare un qubit agendo sulla sfera di Bloch, che è solo una rappresentazione comoda e chiara del suo stato, ma

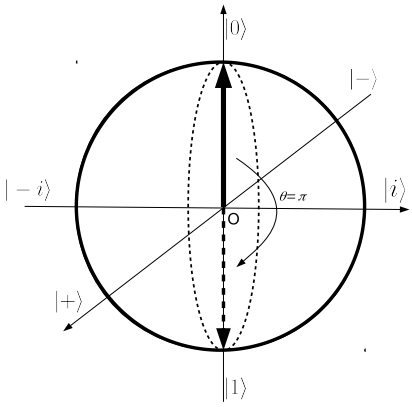

Figura 7.2: Il qubit $|0\rangle$ viene ruotato di 180 gradi (π) attorno all'asse $|+\rangle$. La posizione iniziale del qubit viene indicata con una freccia continua mentre quella finale con una freccia tratteggiata.

bisogna agire sul sistema fisico attraverso il quale è stato implementato il qubit. Se il qubit è implementato come il vettore di polarizzazione di un fotone, allora è necessario agire fisicamente su di esso, con uno strumento ottico, in modo che al termine della trasformazione lo stato di polarizzazione sia passato da $|0\rangle$ allo stato $|1\rangle$.

Le trasformazioni fisiche che agiscono a livello quantistico sono rappresentabili per mezzo di matrici complesse, cioè le matrici studiate nella sezione 4.2.

Nel paragrafo 5.3 si è visto che i qubit debbono rispettare il vin-

colo di unitarietà del modulo, cioè devono avere modulo quadro uguale ad 1. Le trasformazioni fisiche quantistiche devono preservare l'unitarietà del modulo dei qubits.

Ricaviamo la matrice complessa che trasforma il qubit da $|0\rangle$ allo stato $|1\rangle$. Vediamo che la matrice presente nel seguente prodotto

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \tag{7.1}$$

corrisponde esattamente alla matrice che stiamo cercando, infatti trasforma il vettore complesso $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$

nel vettore complesso $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$

esattamente come richiesto.

Con pochi calcoli è facile verificare che la 7.1 continua a valere anche se moltiplichiamo il vettore $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$ per una fase $e^{i\theta}$, quindi la trasformazione 7.1 trasforma qubits in qubits. Vista la sua importanza, diamo un nome a questa trasformazione, e la chiamiamo σ_x. Per ora abbiamo dimostrato che essa manda il qubit $|0\rangle$ nel qubit $|1\rangle$, e facilmente ci si può convincere del viceversa,

infatti:

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \tag{7.2}$$

In sintesi si è visto che la rotazione del qubit nella sfera di Bloch dallo stato $|0\rangle$ allo stato $|1\rangle$ corrisponde alla trasformazione 7.1 nello spazio complesso $\mathbb{C}^2$ operata per mezzo della matrice

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

.

La matrice σ_x è la forma *matriciale* di una trasformazione fisica. Tale trasformazione può essere espressa come un operatore secondo la espressione seguente:

$$\mathbf{X} = |1\rangle\langle 0| + |0\rangle\langle 1| \tag{7.3}$$

Analizzando la figura 7.4 si può capire che le rotazioni attorno all'asse delle x hanno una caratteristica importante: esse trasformano ket *reali* in ket reali. In pratica, se un ket ha coefficienti reali, o meglio coefficienti complessi con parte immaginaria nulla, una trasformazione operata da σ_x preserverà questa sua caratteristica.

Dopo aver visto come generare una rotazione di π è naturale chiedersi come generare una rotazione per un generico angolo

θ, ma a questo risponderemo dopo aver introdotto le due matrici σ_y e σ_z e i corrispettivi operatori **Y** e **Z** ed aver valutato la loro operazione di trasformazione sui qubit.

Prima di procedere, manca ancora una osservazione. Abbiamo visto che l'azione dell'operatore σ_x *nega* gli stati di base $|0\rangle$ e $|1\rangle$, ma non abbiamo analizzato il suo effetto su un generico qubit $|\psi\rangle$, per farlo consideriamo un qubit nello stato $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. Possiamo valutare l'azione di σ_x sul qubit $|\psi\rangle$ come è stato visto nella 5.34:

$$\sigma_{\mathbf{x}}(\alpha|0\rangle + \beta|1\rangle) = \sigma_{\mathbf{x}}\alpha|0\rangle + \sigma_{\mathbf{x}}\alpha|1\rangle = \tag{7.4}$$

$$\alpha|1\rangle + \beta|0\rangle \tag{7.5}$$

Come si vede il risultato della 7.5 non può essere interpretato come l'equivalente dell'operazione NOT. L'analogia tra i gates quantistici come σ_x e gli operatori logici dell'informatica classica ha valore solo fintanto che si operi con qubits che si trovino negli stati $|0\rangle$ o $|1\rangle$, ma cessa di esistere quando si consideri una sovrapposizione di essi. Questo non deve sorprendere, perché se così non fosse, allora tra la computazione classica e quella quantistica ci sarebbe una totale analogia e la seconda avrebbe poco senso di esistere visto che si rivela assai più laboriosa

della sua controparte classica.

In estrema sintesi, abbiamo visto che la computazione quantistica è un processo fisico che trasforma i qubits. Il primo passo nello studio della computazione quantistica è quindi lo studio delle trasformazioni che agiscono su un singolo qubit, quella appena vista è la prima di esse, nel proseguo di questa sezione ne introdurremo altre due, denominate σ_y e σ_z.

7.2 Operatore Z

La seconda trasformazione che vogliamo analizzare è rappresentata dall'operatore **Z** definito come segue:

$$\mathbf{Z} = |0\rangle\langle 0| - |1\rangle\langle 1| \tag{7.6}$$

Si ricava facilmente che all'operatore **Z** è associata la matrice σ_z:

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

Come abbiamo fatto con l'operatore **X**, valutiamo l'azione

dell'operatore **Z** sui ket di base. Vediamo subito che:

$$\begin{aligned} \mathbf{Z}|0\rangle &= |0\rangle \\ \mathbf{Z}|1\rangle &= -|1\rangle \end{aligned} \tag{7.7}$$

I due stati di base $|0\rangle$ e $|1\rangle$ si dicono autostati di **Z** perché l'operatore non li trasforma, ma si limita a moltiplicarli per un numero complesso detto *autovalore* dell'autostato. L'autovalore di $|0\rangle$ è quindi il numero complesso $1 + 0i$, mentre quello di $|0\rangle$ è il numero complesso $-1 + 0i$.

L'azione dell'operatore **Z** diventa più chiara se si analizza rispetto allo stato $|+\rangle$. Si ha infatti che:

$$\begin{aligned} \mathbf{Z}|+\rangle &= |-\rangle \\ \mathbf{Z}|-\rangle &= |+\rangle \end{aligned} \tag{7.8}$$

come si può facilmente verificare ricordando che $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ e $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, quindi:

$$\begin{aligned} \mathbf{Z}|+\rangle &= (|0\rangle\langle 0| - |1\rangle\langle 1|)\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = |-\rangle \\ \mathbf{Z}|-\rangle &= (|0\rangle\langle 0| - |1\rangle\langle 1|)\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = |+\rangle \end{aligned} \tag{7.9}$$

Dalle 7.8 si vede l'analogia dell'azione dell'operatore **X** con l'operatore **Z**. Il primo infatti trasforma il qubit in modo che sulla

sfera di Bloch tale trasformazione corrisponda ad una rotazione di π rispetto all'asse X, il secondo, invece, lo trasforma in modo che un qubit inizialmente disposto lungo l'asse x positivo, quindi nello stato $|+\rangle$ venga ruotato di π attorno all'asse x e si trovi lungo l'asse x negativo, cioè lo stato $|-\rangle$.
É facile dimostrare che l'operatore **Z** trasforma anche lo stato $|i\rangle$ nello stato $|-i\rangle$ e viceversa, infatti si ha:

$$\begin{aligned} \mathbf{Z}|i\rangle &= |-i\rangle \\ \mathbf{Z}|-i\rangle &= |i\rangle \end{aligned} \tag{7.10}$$

come si può facilmente verificare ricordando che $|i\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)$ e $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)$, quindi:

$$\begin{aligned} \mathbf{Z}|+\rangle &= (|0\rangle\langle 0| - |1\rangle\langle 1|)\frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle) = |-i\rangle \\ \mathbf{Z}|-\rangle &= (|0\rangle\langle 0| - |1\rangle\langle 1|)\frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle) = |i\rangle \end{aligned} \tag{7.11}$$

7.3 Operatore Y

La terza trasformazione che analizziamo è data dall'operatore **Y** definito come segue:

$$\mathbf{Y} = |0\rangle\langle 1| - |1\rangle\langle 0| \tag{7.12}$$

Si ricava facilmente che l'operatore **Y** è **proporzionale** alla matrice σ_y:

$$\sigma_y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

La differenza tra l'operatore **Y** e la matrice σ_y è che il primo ha coefficienti reali mentre la seconda ha coefficienti puramente immaginari. Alcuni autori non fanno questa distinzione e definiscono **Y** come segue:

$$\mathbf{Y} = i|0\rangle\langle 0| - i|1\rangle\langle 0|$$

in questo non c'è nulla di sbagliato, l'importante è prestare attenzione alla scelta compiuta. Comunque la scelta adottata in questo testo sembra essere quella maggiormente usata nei testi che si stanno occupando di informatica quantistica, mentre la seconda scelta è un eredità (corretta) della fisica. In ogni caso, la cosa importante è sapere bene cosa si sta facendo per evitare di incorrere in errori grossolani.

L'operatore **Y** può essere ottenuto dal prodotto dei due operatori **X** e **Z**, infatti è facile verificare la seguente relazione:

$$\mathbf{XZ} = \mathbf{Y} \tag{7.13}$$

Il prodotto tra operatori in generale non è commutativo (può esserlo per precisi operatori ma non per altri) e la relazione 7.13 vale solo nel preciso ordine in cui è scritta. In questo caso particolare il prodotto è *anti* commutativo e vale anche la seguente:

$$\mathbf{ZX} = -\mathbf{Y} \tag{7.14}$$

Questa considerazione potrebbe apparire poco importante, in realtà è fondamentale perché gli operatori che vengono introdotti in questa sezione sono i *quantum gates* che rappresentano gli analoghi delle porte logiche usate nei circuito logici alla base della computazione classica. Scambiare l'ordine in qui essi operano equivarrebbe quindi ad un importante errore di programmazione.

Come abbiamo fatto con l'operatore **X**, valutiamo l'azione dell'operatore **Z** sui ket di base. Vediamo subito che:

$$\begin{aligned} \mathbf{Z}|0\rangle &= |0\rangle \\ \mathbf{Z}|1\rangle &= -|1\rangle \end{aligned} \tag{7.15}$$

7.4 Operatore I

L'ultima trasformazione che rimane da analizzare è la trasformazione identità, rappresentata dall'operatore **I** come segue:

$$\mathbf{I} = |0\rangle\langle 0| + |1\rangle\langle 1|$$

che è associata alla matrice identità

$$\mathbf{I} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

L'azione di **I** è di lasciare immutati i ket su cui agisce, infatti si ha che preso un generico qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, l'azione di **I** è data da:

$$\begin{aligned} \mathbf{I}|\psi\rangle = (|0\rangle\langle 0| + |1\rangle\langle 1|)(\alpha|0\rangle + \beta|1\rangle) = \\ = \alpha|0\rangle + \beta|1\rangle \end{aligned} \tag{7.16}$$

che quindi trasforma $|\psi\rangle$ in sé stesso.

Serve a qualcosa una trasformazione *identità*? A prima vista può sembrare di no, ma in realtà essa è fondamentale per rappresentare qualsiasi trasformazione *continua*, cioè che trasformi un qubit in un qubit *infinitesimalmente* differente da quello di partenza.

7.5 Trasformazioni arbitrarie

Nelle sezioni precedenti è stato introdotto il qubit e la sua differenza rispetto al bit e si è visto come rappresentarlo sulla sfera di Bloch. Si è visto inoltre che esiste una relazione tra tre trasformazioni nello spazio $\mathbb{C}^2$ (e nello spazio dei ket) con tre specifiche rotazioni di un raggio vettore sulla sfera di Bloch.
La computazione quantistica consiste nella trasformazione dello stato dei qubits, pertanto è naturale chiedersi come acquisire il pieno controllo sull'intera sfera di Bloch e non solo su sei delle infinite orientazioni che il qubit può assumere su di essa.
A questa importante domanda daremo una risposta ora, costruendo tutte le trasformazioni possibili per un qubit e valutando le relative rotazioni sulla sfera di Bloch.

7.5.1 Rotazioni attorno all'asse y

Nei paragrafi precedenti abbiamo visto che possiamo costruire degli operatori sommandone altri tra loro. Consideriamo allora l'operatore $\mathbf{R}_Y(\delta\zeta) = \mathbf{I} - \delta\zeta\mathbf{Y}$ che in forma matriciale può essere

scritto come

$$\mathbf{I} - \delta\zeta\mathbf{Y} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} - \begin{bmatrix} 0 & \delta\zeta \\ -\delta\zeta & 0 \end{bmatrix} \tag{7.17}$$

L'espressione 7.23 rappresenta un generatore di trasformazioni, in pratica si ha che preso per esempio un qubit nello stato iniziale $|0\rangle$, e applicando l'operatore $\mathbf{R}_\theta$ si ottiene:

$$\mathbf{R}_Y(\zeta)|0\rangle = \mathbf{I} - \delta\zeta\mathbf{Y}|0\rangle = \\ |0\rangle + \delta\zeta|1\rangle \tag{7.18}$$

che corrisponde ad una rotazione infinitesima del qubit $|0\rangle$ attorno all'asse y sulla sfera di Bloch.

Questo punto non è affatto semplice da capire e necessita di ulteriori chiarimenti. Proseguiamo quindi per gradi e abbandoniamo per un attimo la rappresentazione del qubit sulla sfera di Bloch per vederlo ancora rappresentato su di un piano.

Si supponga di formare un piano in cui i due assi sono rispettivamente dati dai ket $|0\rangle$ e $|1\rangle$ come riportato in figura 7.3 e che sia perpendicolare all'asse dell'y. Si consideri ora il qubit $|\psi\rangle$ che si trovi inizialmente nello stato $|0\rangle$ e si consideri di ruotarlo in senso antiorario di un angolo $\delta\zeta$. Come si vede in figura 7.3, la variazione dello stato del qubit è pari al prodotto dell'angolo

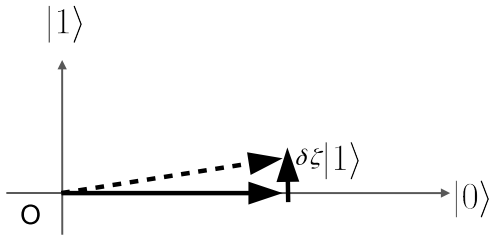

Figura 7.3: Il qubit nello stato $|0\rangle$ è ruotato di un angolo infinitesimo $\delta\zeta$ rispetto all'asse perpendicolare al piano.

infinitesimo $\delta\zeta$ per il ket $|1\rangle$, quindi dopo la rotazione il qubit $|\psi\rangle$ si troverà nello stato $|0\rangle + \delta\zeta|1\rangle$, cioè esattamente nello stato prodotto dall'operatore $\mathbf{R}_Y(\delta\zeta)$. In questo senso vediamo che l'operatore $\mathbf{R}_Y(\delta\zeta)$ ha prodotto una rotazione infinitesima del qubit attorno all'asse y. L'espressione di $\mathbf{R}_Y$ per una rotazione di un angolo finito ζ è la seguente:

$$\mathbf{R}_Y(\zeta) = \begin{bmatrix} \cos\zeta & -\sin\zeta \\ \sin\zeta & \cos\zeta \end{bmatrix} \tag{7.19}$$

Si noti che il motivo per cui abbiamo potuto rappresentare la rotazione attorno all'asse y su di un piano, anziché dover usare la sfera di Bloch, è che l'operatore $\mathbf{R}_Y$ trasforma qubits a componenti reali in qubits a componenti reali. In altre parole se un qubit $|\psi\rangle$ è inizialmente descritto dalla relazione $|\psi\rangle = a|0\rangle + b|1\rangle$ con a e b reali, cioè con componente immaginaria nulla,

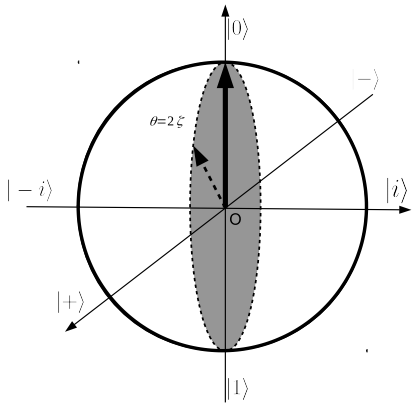

Figura 7.4: Il qubit $|0\rangle$ viene ruotato di θ attorno all'asse $|i\rangle$. La posizione iniziale del qubit viene indicata con una freccia continua mentre quella finale con una freccia tratteggiata.

una rotazione attorno all'asse y ad opera l'operatore $\mathbf{R}_Y$ non modifica questa proprietà e trasforma $|\psi\rangle$ in $|\psi\rangle' = a'|0\rangle + b'|1\rangle$ a' e b' ancora reali.

Ora è interessante notare questa stessa proprietà sulla sfera di Bloch. Come mostrato in figura 7.4, una rotazione di un angolo ζ di un qubit che sia inizialmente allineato all'asse $|0\rangle$ ad opera d $\mathbf{R}_Y$ produce una trasformazione che lo mantiene sempre sul piano zx. In pratica genera una rotazione attorno all'asse y individuato sulla sfera di Bloch dalla direzione $|i\rangle$.

Rotazione da $|0\rangle$ a $|+\rangle$

Vediamo ora come trasformare un qubit inizialmente nello stato $|0\rangle$ in un qubit nello stato $|+\rangle$.

Facciamo riferimento ancora alla figura 7.4 e immaginiamo come passare dallo stato iniziale a quello voluto. È facile dedurre che sia necessaria una rotazione di 90 gradi ($\pi/2$) attorno all'asse $|i\rangle$, cioè l'asse z dell'ordinario piano cartesiano. Abbiamo visto che le rotazioni attorno a detto asse sono operate dell'operatore $\mathbf{R}_Y(\zeta)$, quindi ci aspettiamo che debba esistere un valore dell'angolo ζ tale per cui si abbia:

$$\mathbf{R}_Y(\zeta)|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \tag{7.20}$$

Risolvere la 7.21 rispetto a ζ è immediato se si considera la forma bra/ket dell'operatore di rotazione data da:

$$\mathbf{R}_Y(\zeta) = \cos\zeta|0\rangle\langle 0| - \sin\zeta|0\rangle\langle 1| + \sin\zeta|0\rangle\langle 0| + \cos\zeta|1\rangle\langle 1|$$

applicando $\mathbf{R}_Y(\zeta)$ al qubit nello stato $|0\rangle$ si ha:

$$\begin{aligned}\mathbf{R}_Y(\zeta)|0\rangle = (\cos\zeta|0\rangle\langle 0| - \sin\zeta|0\rangle\langle 1| + \sin\zeta|0\rangle\langle 0| + \cos\zeta|1\rangle\langle 1|)|0\rangle = \\ = \cos\zeta|0\rangle + \sin\zeta|0\rangle\end{aligned} \tag{7.21}$$

Il problema è quindi ridotto a trovare un valore di ζ tale per cui si abbia:

$$\cos\zeta|0\rangle + \sin\zeta|0\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|0\rangle$$

che è banalmente soddisfatto dalla soluzione $\zeta = \pi/4$, cioè 45 gradi. La rotazione di $\pi/4$ rispetto a ζ corrisponde però ad una rotazione doppia ($pi/2$) sulla sfera di Bloch (vedi figura 7.5) quindi si ha l'importante relazione

$$\theta = 2\zeta \tag{7.22}$$

cioè l'angolo di rotazione nello spazio della sfera di Bloch è il doppio dell'angolo di cui vengono realmente ruotati i qubits.

Rotazione da $|0\rangle$ a $|1\rangle$

I passaggi presentati nel paragrafo precedente ci hanno mostrato chiaramente che le rotazioni sulla sfera di Bloch possono essere ottenute attraverso l'azione di operatori che agiscono sui qubit. Tutti gli operatori fin qui mostrati hanno una importante proprietà, cioè il loro prodotto con il proprio trasposto coniugato è uguale alla identità, tali operatori sono detti **unitari**.
Gli operatori unitari sono molto importanti perché rappresentano delle operazioni fisiche che possono essere compiute realmente, quindi non sono solo *oggetti matematici*. L'operatore

$\mathbf{R}_Y(\zeta)$, ad esempio, può essere realmente realizzato per un computer quantistico che usi i fotoni per implementare i qubits. Esso può quindi essere usato realmente per trasformare un qubit da $|0\rangle$ a $|1\rangle$.

Osservando la figura 7.5 si vede che dopo aver ruotato dallo stato $|0\rangle$ allo stato $|+\rangle$, per raggiungere lo stato $|1\rangle$ è necessaria un'altra rotazione di 90 gradi sulla sfera di Bloch, e quindi di 45 gradi rispetto all'angolo ζ, in totale una rotazione di 180 gradi (π) sulla sfera di Bloch. Questa rotazione può essere ottenuta operando con l'operatore $\mathbf{R}_Y(\pi/2)$ sullo stato $|0\rangle$. Si noti però che può essere ottenuta anche operando con l'operatore $\mathbf{R}_Y(\pi/4)$ sullo stato $|+\rangle$.

É importante sottolineare che i qubits che stanno sul piano xz, o più propriamente il piano individuato dalle direzioni $|0\rangle$ e $|+\rangle$, hanno solo componenti reali, non complessi, come si deduce anche graficamente dal fatto che un qubit che giace in tale piano ha componente immaginaria nulla. Ogni rotazione operata da $\mathbf{R}_Y(\zeta)$ su un qubit che sia già su tale piano, ruoterà tale qubit sempre all'interno di tale piano, senza quindi portarlo fuori da esso.

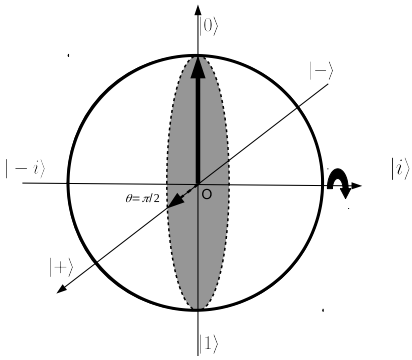

Figura 7.5: Il qubit $|0\rangle$ viene ruotato di $\pi/2$ attorno all'asse $|i\rangle$ fino a raggiungere l'asse $|+\rangle$. La posizione iniziale del qubit viene indicata con una freccia continua mentre quella finale con una freccia tratteggiata.

Perché tanta enfasi su questo aspetto? La computazione quantistica è la scienza di trasformare i qubit per ottenere informazioni. La piena consapevolezza dell'azione di ogni operatore sui qubits è pertanto fondamentale se si vuole acquisire il controllo sulla computazione, in pratica imparare l'azione degli operatori quantistici (quantum gates) equivale ad imparare il funzionamento dei codici macchina su una architettura computazionale classica.

7.5.2 Rotazioni attorno all'asse z

In questo paragrafo continuiamo ad esplorare le rotazioni del qubit sulla sfera di Bloch, provando a ruotare attorno alla direzione z cioè quella individuata dal ket $|0\rangle$ sulla sfera di Bloch. L'operatore di rotazione $\mathbf{R}_Z(\zeta)$ è costruito in modo analogo all'operatore $\mathbf{R}_Y(\zeta)$ cioè partendo da un generatore di rotazioni infinitesime, che in forma matriciale possiamo scrivere come:

$$\mathbf{I} - i\delta\zeta\mathbf{Z} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} - \begin{bmatrix} i\delta\zeta & 0 \\ 0 & -i\delta\zeta \end{bmatrix} \tag{7.23}$$

La forma matriciale finita dell'operatore $\mathbf{R}_Z(\zeta)$ è la seguente:

$$\mathbf{R}_Z(\zeta) = \begin{bmatrix} \cos\zeta - i\sin\zeta & 0 \\ 0 & \cos\zeta + i\sin\zeta \end{bmatrix} \tag{7.24}$$

La forma dell'operatore nel formalismo bra/ket è data dalla seguente:

$$\begin{aligned} \mathbf{R}_Z(\zeta) = \\ \cos\zeta\mathbf{I} + i\sin\zeta\mathbf{Z} = \\ (\cos\zeta - i\sin\zeta)|0\rangle\langle 0| + (\cos\zeta + i\sin\zeta)|1\rangle\langle 1| \end{aligned} \tag{7.25}$$

Vediamo l'azione dell'operatore $\mathbf{R}_Z(\zeta)$ su alcuni qubits. Partiamo anzitutto dallo stato $|0\rangle$. La direzione di un qubit che si trovi

in detto stato, quindi giacente lungo l'asse z, non viene alterata dall'azione dell'operatore, si ha infatti:

$$\begin{aligned} \mathbf{R}_Z(\zeta)|0\rangle = \\ ((\cos\zeta - i\sin\zeta)|0\rangle\langle 0| + (\cos\zeta + i\sin\zeta)|1\rangle\langle 1|)\,|0\rangle = \\ (\cos\zeta - i\sin\zeta)|0\rangle \end{aligned} \tag{7.26}$$

La 7.26 ci dice che quando un qubit si trova nello stato $|0\rangle$ allora si trova in un autostato di $\mathbf{R}_Z$. In effetti questo è abbastanza intuitivo, si pensi ad esempio di porre una matita in verticale e di ruotarla attorno al proprio asse di simmetria (in altre parole attorno alla mina) è chiaro che la direzione della matita non cambia. Nello stesso modo, il qubit che si trovi nella direzione $|0\rangle$ non cambia direzione per una rotazione attorno all'asse z.
Ancora più interessante è analizzare l'azione di $\mathbf{R}_Z$ sul qubit $|+\rangle$. Tornando alla figura 7.5 ci aspettiamo che una rotazione di 90 gradi attorno all'asse z (direzione $|0\rangle$) porti il qubit nella direzione $|i\rangle$, cioè allineato con l'asse delle y.
I qubits che giacciono al di fuori del piano xz hanno per costruzione la parte complessa diversa da zero, in particolare ci aspettiamo questo da un qubit allineato alla direzione $|i\rangle$. Per verificare il risultato della rotazione applichiamo l'operatore $\mathbf{R}_Z$

al qubit $|+\rangle$ in modo analogo a quanto fatto in 7.26:

$$\mathbf{R}_Z(\zeta)|+\rangle = ((\cos\zeta - i\sin\zeta)|0\rangle\langle 0| + (\cos\zeta + i\sin\zeta)|1\rangle\langle 1|)\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \frac{1}{\sqrt{2}}((\cos\zeta - i\sin\zeta)|0\rangle + (\cos\zeta + i\sin\zeta)|1\rangle) \quad (7.27)$$

Dalla 7.27 ci si aspetta che l'azione di una rotazione di 90 gradi (ϕ) produca lo stato $|i\rangle$, quindi che per un certo ζ, si abbia:

$$\frac{1}{\sqrt{2}}((\cos\zeta - i\sin\zeta)|0\rangle + (\cos\zeta + i\sin\zeta)|1\rangle) = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle) \quad (7.28)$$

Per verificare che la 7.28 sia la soluzione che ci aspettiamo di trovare riscriviamo il membro di sinistra attraverso la notazione esponenziale (modulo e fase). Si ha che il termine $\cos\zeta + i\sin\zeta$ assume la forma $e^{i\zeta}$, mentre il termine $\cos\zeta - i\sin\zeta$ assume la forma $e^{-i\zeta}$, in questo modo la 7.28 può essere riscritta come:

$$\frac{1}{\sqrt{2}}\left(e^{-i\zeta}|0\rangle + e^{i\zeta}|1\rangle\right) = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle) \quad (7.29)$$

Raccogliendo il termine $e^{-i\zeta}$ nella 7.28, si ottiene

$$\frac{1}{\sqrt{2}}e^{-i\zeta}\left(|0\rangle + e^{2i\zeta}|1\rangle\right) = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle) \quad (7.30)$$

Il termine $e^{-i\zeta}$ raccolto nella 7.30 è un numero complesso di modulo uno, quindi rappresenta un fattore di fase ininfluente. Il termine $e^{2i\zeta}$ moltiplica solo il ket $|1\rangle$ quindi non può essere

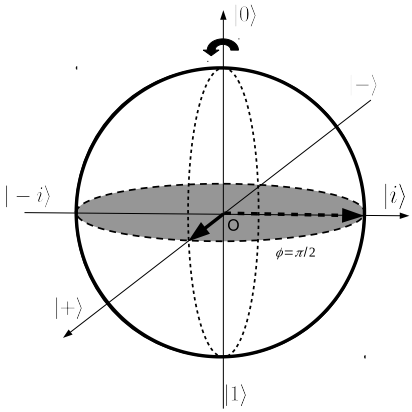

Figura 7.6: Il qubit $|+\rangle$ viene ruotato di $\pi/2$ attorno all'asse $|0\rangle$ fino a raggiungere l'asse $|i\rangle$. La posizione iniziale del qubit viene indicata con una freccia continua mentre quella finale con una freccia tratteggiata.

ignorato. Quando ζ vale $\pi/4$, il termine $e^{2i\zeta}$ assume il valore i, quindi la rotazione $\mathbf{R}_Z(\pi/4)$ trasforma un qubit dallo stato $|+\rangle$ allo stato $|i\rangle$.

In questo paragrafo abbiamo visto che la rotazione attorno all'asse z porta un qubit che inizialmente non ha componenti complesse in un qubit con componenti complesse. Sarebbe molto interessante discutere questo aspetto anche dal punto di vista della fisica, infatti esiste una importante differenza tra gli stati di polarizzazione dei fotoni che hanno solo componenti reali rispetto a quelli che hanno componenti complesse. I pri-

mi, detti a polarizzazione lineare, sono caratterizzati dal vettore campo elettrico che ha una direzione fissa nello spazio, mentre varia nel tempo la sua intensità. Per i secondi, detti a polarizzazione ellittica, il vettore campo elettrico ruota nello spazio in un piano perpendicolare alla direzione di propagazione.
I collegamenti tra la fisica quantistica e l'informatica quantistica sono ovviamente tanti, il lettore che si trovi incuriosito, è invitato ad approfondirli su testi dedicati alla meccanica quantistica come il [1] o il [2]
Dopo questa piccola parentesi sulla fisica che sta alla base degli stati dei qubits, vediamo la terza rotazione, quella attorno all'asse x.

7.5.3 Rotazioni attorno all'asse x

La terza rotazione che rimane da esaminare è quella relativa all'asse delle x, quindi alla direzione $|+\rangle$ sulla sfera di Bloch. L'operatore di rotazione infinitesima può essere scritto in forma matriciale come:

$$\mathbf{I} - i\delta\zeta\mathbf{X} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} - \begin{bmatrix} 0 & \delta\zeta \\ \delta\zeta & 0 \end{bmatrix} \tag{7.31}$$

All'espressione 7.31 corrisponde la forma matriciale finita:

$$\mathbf{R}_X(\zeta) = \begin{bmatrix} \cos\zeta & -i\sin\zeta \\ -i\sin\zeta & \cos\zeta \end{bmatrix} \tag{7.32}$$

che si differenzia dalla 7.19 per la componente immaginaria degli elementi sulla diagonale secondaria e per il segno omogeneo per tutti gli elementi.

$$\mathbf{R}_X(\zeta) = (\cos\zeta|0\rangle\langle 0| - i\sin\zeta|0\rangle\langle 1| - i\sin\zeta|0\rangle\langle 0| + \cos\zeta|1\rangle\langle 1|) \tag{7.33}$$

$$\mathbf{R}_X(\zeta) = \mathbf{I} - i\delta\zeta\mathbf{X}|0\rangle =$$

L'operatore $\mathbf{R}_X(\zeta)$ genera le rotazioni del qubit attorno all'asse x cioè la direzione $|+\rangle$. Per valutare la sua azione consideriamo sempre un qubit nello stato $|0\rangle$ e valutiamo la sua trasformazione per mezzo dell'operatore:

$$\mathbf{R}_X(\zeta)|0\rangle = (\cos\zeta|0\rangle\langle 0| - i\sin\zeta|0\rangle\langle 1| - i\sin\zeta|0\rangle\langle 0| + \cos\zeta|1\rangle\langle 1|)|0\rangle = \cos\zeta|0\rangle - i\sin\zeta|0\rangle \tag{7.34}$$

Dalla 7.34 è immediato verificare che una rotazione di $\zeta = -\pi/4$ porta lo stato $|0\rangle$ esattamente nello stato $|i\rangle$, definito appunto

come $\frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)$.

Si è visto che partendo dallo stato $|0\rangle$ si può raggiungere lo stato $|i\rangle$ attraverso una rotazione attorno all'asse x oppure due rotazioni successive, una attorno all'asse y poi una attorno all'asse z. Questo ci porta giustamente a dedurre che anche dal punto di vista computazionale, l'azione congiunta dei due operatori $\mathbf{R}_y$ e $\mathbf{R}_Z$ debba essere equivalente a quella dell'operatore $\mathbf{R}_X(\zeta)$. In formule questo significa che deve essere vera la seguente relazione:

$$\mathbf{R}_X(\pi/4) = \mathbf{R}_Z(\pi/4)\mathbf{R}_Y(\pi/4) \tag{7.35}$$

che può essere facilmente verificata già dalla forma matriciale delle σ_x, σ_y e σ_z.

7.6 Esercizio proposto

- Esercizio: Partendo dallo stato $|+\rangle$ ruotare il qubit in modo che la sua direzione coincida con quella della bisettrice del piano yz.

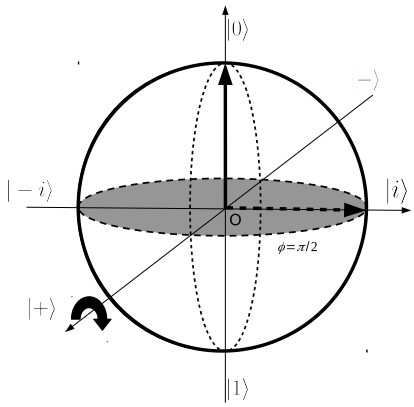

Figura 7.7: Il qubit $|0\rangle$ viene ruotato di $\pi/2$ attorno all'asse $|+\rangle$ fino a raggiungere l'asse $|i\rangle$. La posizione iniziale del qubit viene indicata con una freccia continua mentre quella finale con una freccia tratteggiata.

CAPITOLO 8

Circuiti quantistici

Cosa sia un qubit e come esso sia trasformato tra tutti i suoi possibili stati è stato ampiamente discusso nei capitoli precedenti. Il qubit è alla base dell'informatica quantistica e della computazione quantistica basata sul concetto di *circuito*. Ogni algoritmo classico che viene eseguito su una MdT può essere anche visto e implementato come un circuito logico, per esempio una circuiteria elettronica dedicata. Ogni circuito logico classico può essere trasformato in un circuito quantistico che anziché operare sui bits opera sui qubits.

Gli operatori che trasformano i qubits sono detti *quantum gates* la loro caratteristica principale è che presentano un nume-

ro di ingressi uguale al numero di uscite. Questa caratteristica è alla base del principio di reversibilità della computazione quantistica[3]. Qualsiasi circuito quantistico può essere implementato usando un insieme di quantum gates che operano su un singolo qubit, come quelli descritti nel capitolo precedente, e due quantum gates che operano su due qubits.

Nel paragrafo 4.2.3 e presto nel 8.2 è mostrato come combinare tra loro le matrici e gli operatori per mezzo del prodotto tensoriale. In questa sezione vedremo che i quantum gates che operano su più qubits sono ottenuti proprio in questo modo, cioè come prodotto tensoriale tra due operatori. Ovviamente il prodotto tensoriale è il mezzo matematico, o più in generale il mezzo formale, attraverso il quale si esprime l'azione di dispositivi fisici reali che implementano detti quantum gates. La realizzazione tecnologica di questi dipende dalla grandezza fisica scelta per implementare i qubits. In questo libro abbiamo sempre pensato ai qubits implementati nei termini della polarizzazione dei fotoni. Continuando quindi con questa scelta, vediamo che l'esempio più semplice di un quantum gates è dato un dispositivo ottico chiamato *beam splitter* che consiste in due prismi triangolari incollati tra loro. Il beam splitter è un

esempio soprattutto didattico, ma allo stato attuale della ricerca (2021) sembra possibile realizzare dei quantum gates che possono essere integrati in circuiti di silicio.
Indipendentemente dalla soluzione tecnologica con cui i quantum gates sono realizzati è fondamentale conoscerne la rappresentazione formale e l'azione sui qubits.
Scrivere un algoritmo quantistico significa progettare un circuito. Nel prossimo paragrafo vedremo come rappresentare graficamente un circuito quantistico in termini di quantum gates. Inizieremo prima con un semplicissimo circuito ad un solo qubit per poi passare a circuiti a due qubits.

8.1 Circuiti elementari

L'informatica quantistica è assai complicata, inutile negarlo, affrontarla solo in termini di formule matematiche la rende ancora più complessa, ma può aiutare l'uso di schemi grafici che ha almeno due aspetti positivi: da un lato semplifica la visualizzazione dei processi a cui vanno incontro i qubits, dall'altro avvicina la progettazione dell'algoritmo al dispositivo hardware che lo implementerà.

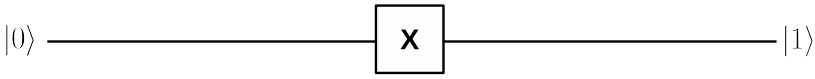

Figura 8.1: La figura mostra lo schema circuitale di un singolo qubit (q_0) trasformato dal gate X. Il qubit entra nel circuito nello stato $q_0 = |0\rangle$ e esce nello stato $|1\rangle$.

Il circuito più semplice è costituito da un singolo qubit il cui stato viene trasformato dall'operatore X. Il qubit q_0 è rappresentato con una linea retta, mentre l'operatore X con un quadrato (*box*) posto sulla linea stessa (figura 8.1).

Se si decide di inserire in input un qubit che sia nello stato $|0\rangle$ o nello stato $|1\rangle$, allora questo circuito rappresenta una algoritmo classico molto semplice che ha come unico effetto quello di *negare* il valore logico attribuito al qubit.

È importante notare che se siamo sicuri che lo stato iniziale del qubit sia $|0\rangle$, allora siamo sicuri al cento per cento (a meno di errori hardware al momento non eliminabili[1]) che il qubit emergerà dal gate nello stato $|1\rangle$. Quindi in questo primo esempio, il gate quantistico ha un effetto completamente prevedibile.

[1] Il problema degli errori hardware esiste anche nella computazione classica, ma allo stato attuale della tecnologia essi vengono corretti in percentuale vicinissima al cento per cento.

Nonostante lo stato di uscita del qubit sia in questo caso ben noto, per poterlo conoscere è necessario misurarlo. Il concetto di misura è stato affrontato nel paragrafo 5.7 vedremo ora come una misura viene inserita simbolicamente in un circuito.

Anzitutto è bene chiarire che il risultato di una misura è un'informazione classica, quindi viene memorizzata in un bit, per questo un circuito quantistico che necessiti di una o più misure deve prevedere anche delle linee di bit classici. Queste vengono rappresentate in maniera analoga alle linee quantistiche, ma per convezione si assegna normalmente un nome che inizia con la C, per esempio c_1 che ne evidenzia il carattere classico. Si noti che l'indice del bit classico ha continuato la numerazione del numero totale di bit, includendo l'indice 0 del qubit. Queste sono convenzioni, non universali, ma che stanno iniziando ad affermarsi. È comunque possibile che esse varino nel tempo, l'importante è avere la consapevolezza delle quantità che si sta trattando, della natura classica o quantistica e dell'azione degli strumenti di trasformazione o di misura che si stanno usando.

Per indicare che il qubit viene misurato è necessario inserire il simbolo di misura sulla linea quantistica che si desidera misu-

rare e collegarlo alla linea classica corrispondente al bit in cui si vuole memorizzare il risultato. Lo schema appena descritto è riportato in figura 8.2.

Il semplice algoritmo quantistico appena descritto, può essere anche implementato in un linguaggio apposito detto $QASM$, cioè *quantum assembly*:

```
OPENQASM 2.0;
include "qelib1.inc";

qreg q[1];
creg c[1];

x q[0];
measure q[0] -> c[0];
```

Il codice riportato si riferisce alla versione OPENQSM attualmente adottata dall'IBM. Le prime due istruzioni dichiarano un array di qubits e uno di bits classici, entrambi gli array di dimensione 1. La sintassi ricorda molto il linguaggio C. Segue poi l'azione dell'operatore X sul qubit q_0 e la sua misura memorizzata nel bit c_0.

Per quanto l'idea di programmare una macchina quantistica

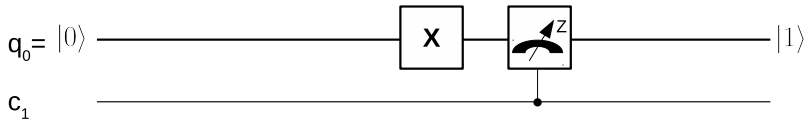

Figura 8.2: La figura mostra lo schema circuitale di un singolo qubit trasformato dal gate X. Successivamente al gate è posto un misuratore del bit il cui valore viene memorizzato sulla linea classica c_1.

risulti suggestiva è importante sapere che al momento non esistono MdT universali quantistiche, quindi più che programmare si tratta di configurare dei circuiti quantistici.

Il significato dell'algoritmo si complica se invece di inserire uno dei due precedenti valori, prepariamo il qubit in un generico stato $q_0 = \alpha|0\rangle + \beta|0\rangle$.
Per continuare l'analisi, vediamo la situazione da un punto di vista sperimentale. Per poter affermare a ragion veduta che il qubit si trova al suo ingresso nel circuito nello stato $|0\rangle$ è possibile porre un polarizzatore di fronte all'ingresso del circuito, in questo modo si può essere sicuri che il qubit entri solo se si trova nello stato desiderato. A questo punto siamo esattamente nella situazione descritta in figura 8.1.

Per ottenere il qubit nello stato $q_0 = \alpha|0\rangle + \beta|0\rangle$ è necessario

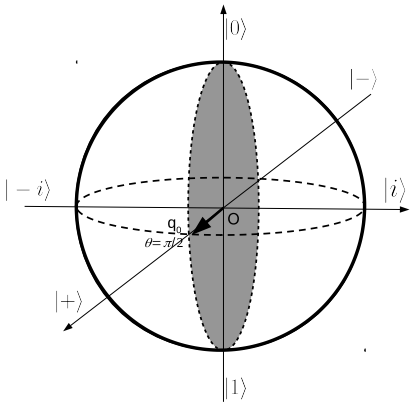

Figura 8.3: La figura mostra il qubit q_0 con coordinate polari $\theta = \pi/4, \phi = 0$.

inserire un nuovo gate che ruoti il qubit nella sfera di Bloch. Supponiamo quindi di volere che il qubit q_0, prima di essere misurati sia trasformato in $q_0 = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|0\rangle$ come indicato in figura 8.3. Per ottenere il qubit nello stato voluto lo si deve trasformare con l'operatore $\mathbf{R}_Y(\pi/4)$. Questo è rappresentato sempre con un quadrato etichettato dal simbolo RY e parametrizzato con $\theta = \pi/2$, come mostrato in figura 8.4. Si noti come l'angolo con cui viene parametrizzata la rotazione sia θ e si riferisca alla sfera di Bloch e non ζ relativo alla rotazione nello spazio complesso. La domanda che ci si pone ora è quale sia il valore del bit c_1 dopo la misura. La risposta, coerente con la

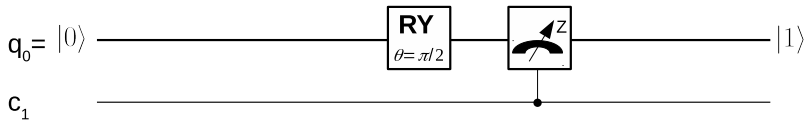

Figura 8.4: La figura mostra lo schema circuitale di un singolo qubit trasformato dal gate X. Successivamente al gate è posto il gate RY parametrizzato con $\theta = \pi/2$ misuratore del bit il cui valore viene memorizzato sulla linea classica c_1.

meccanica quantistica, è che il risultato può essere sia 1 che 0. Cosa significa? Facciamo un esempio: supponiamo di far entrare un singolo qubit nel circuito quindi di leggere il valore di c_1. É possibile leggere il valore 0, ma è anche possibile leggere il valore 1: o uno o l'altro, ma entrambi possibili. Questa aleatorietà si traduce nel fatto che se eseguissimo cento misure, troveremo circa cinquanta volte il valore 1 e circa cinquanta volte il valore 0.

Con questo esempio si è entrati concretamente nel così detto *quantum parallelism*, cioè la caratteristica peculiare per cui un algoritmo quantistico può valutare più stati simultaneamente. Nel caso in questione il parallelismo creato non ha alcuna utilità, ma esso è rappresentativo della possibilità di preparare degli stati che siano la sovrapposizione di stati di base come

lo stato $|0\rangle$ e lo stato $|1\rangle$. Vedremo un esempio concreto, anche se puramente didattico, di questo tipo di algoritmi alla fine del capitolo.

8.2 Circuiti a due qubits

I circuiti visti nella sezione precedente hanno mostrato parte del formalismo usato per descrivere gli algoritmi quantistici e sono serviti per rompere il ghiaccio. L'idea di dover usare una trasformazione unitaria per ottenere una *applicazione* informatica non è del tutto intuitiva, ma giunti qui ci si sentesicuramente più a proprio agio rispetto a prima.

Per procedere aumentando la complessità degli algoritmi bisogna operare su almeno due qubits. In figura 8.5 è rappresentato un circuito che prevede due qubits. Similmente alla terminologia usata per il linguaggio assembly, che descrive molto da vicino l'architettura del computer, anche nel linguaggio QASM ci si riferisce all'insieme di qubits e bits come a registri. Nel circuito in questione si dirà che è presente un registro di due qubits.

Nel circuito sono presenti il gate I, che implementa l'operatore

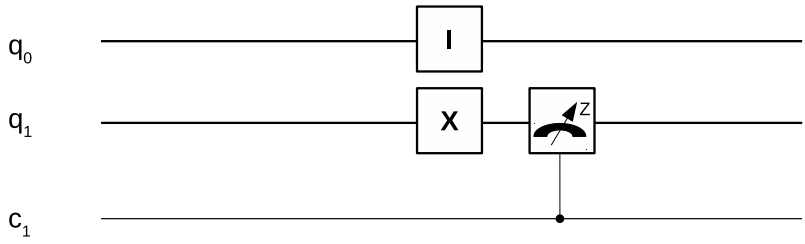

Figura 8.5: La figura mostra lo schema circuitale con un registro di 2 qubits e uno di un solo bit classico.

di identità incontrato nel capitolo 6, e il gate X. Come si vede graficamente, essi sono intesi agire sul singolo qubit che li intercetta, quindi il circuito di figura 8.5 è in realtà semplicemente la somma di due circuiti indipendenti.

Per creare un vero circuito a due qubit è necessario pensare ad un sistema fisico che esegua su di essi una trasformazione che dipende dallo stato di entrambi. Se guardiamo di nuovo al circuito 8.5, ci accorgiamo che la trasformazione operata dal gate **I** sul qubit q_0 è indipendente dal valore di q_1, e lo stesso vale per il gate **X**. Quello che vogliamo ottenere è invece un gate in cui il valore di uscita di q_0 e q_1 sia funzione della combinazione con cui si presentano i due qubits al loro ingresso. In termini

matematici vogliamo che:

$$q_0 \leftarrow f_0(q_0, q_1)$$
$$q_1 \leftarrow f_1(q_0, q_1) \tag{8.1}$$

Per realizzare questo tipo di trasformazione, dobbiamo ricordare quanto fatto nel paragrafo dove abbiamo definito il prodotto tensoriale tra operatori. Consideriamo allora ancora i due gates **I** e **X** e calcoliamo il loro prodotto tensoriale rispettivamente con gli operatori $|0\rangle\langle 0|$ e $|1\rangle\langle 1|$ e la somma tra i termini ottenuti $|0\rangle\langle 0| \otimes \mathbf{I} + |1\rangle\langle 1| \otimes \mathbf{X}$:

$$|0\rangle\langle 0| \otimes \mathbf{I} + |1\rangle\langle 1| \otimes \mathbf{X} =$$
$$= (|0\rangle\langle 0|) \otimes (|0\rangle\langle 0| + |1\rangle\langle 1|) + (|1\rangle\langle 1|) \otimes (|0\rangle\langle 1| + |1\rangle\langle 0|) \tag{8.2}$$

che usando le 5.42 può essere scritta nella forma compatta:

$$|0\rangle\langle 0| \otimes \mathbf{I} + |1\rangle\langle 1| \otimes \mathbf{X} = |00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 11| + |11\rangle\langle 10| \tag{8.3}$$

La 8.1 può essere scritta anche in forma vettoriale come:

$$\begin{bmatrix} q_0 \\ q_1 \end{bmatrix} \leftarrow \begin{bmatrix} f_0(q_0, q_1) \\ f_0(q_0, q_1) \end{bmatrix} \begin{bmatrix} q_0 \\ q_1 \end{bmatrix} \tag{8.4}$$

Dove, nella 8.4 , i due qubits q_0 e q_1 sono racchiusi in un unico vettore a quattro componenti e, allo stesso modo, le componenti

f_0 e f_1 del gate sono rappresentate come una matrice che opera sul vettore a quattro componenti.

Il vettore $\begin{bmatrix} q_0 \\ q_1 \end{bmatrix}$ deve poter essere scritto anche nel formalismo bra/ket, quindi, come è stato fatto con le 5.42 bisogna fare per gli stati base che descrivono due qubit. Per convenzione, e per

coerenza con le 5.42 si hanno le seguenti relazioni:

$$
\begin{aligned}
|0\rangle \otimes |0\rangle \leftrightarrow |00\rangle \leftrightarrow & \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} \\
|0\rangle \otimes |1\rangle \leftrightarrow |01\rangle \leftrightarrow & \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} \\
|1\rangle \otimes |0\rangle \leftrightarrow |10\rangle \leftrightarrow & \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} \\
|1\rangle \otimes |1\rangle \leftrightarrow |11\rangle \leftrightarrow & \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}
\end{aligned} \tag{8.5}
$$

È utile dare una rappresentazione matriciale anche dell'opera-

tore $\mathbf{I} \otimes \mathbf{X}$ che si ricava facilmente essere data da:

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \tag{8.6}$$

8.2.1 Controlled NOT

Qubits in stati fondamentali

L'operatore appena definito è un gate molto importante a cui è assegnato il nome di *Controlled Not* o CNOT, o ancora Cnot, perché il suo comportamento, quando al suo ingresso vengono presentati due qubits nella base standard ($|0\rangle$ oppure $|1\rangle$), è di agire come un not sul secondo qubit, ma solo nel caso in qui il primo sia nello stato $|1\rangle$, altrimenti agisce come una identità.
In pratica possiamo rappresentare l'azione del CNOT sui due qubit usando una tabella di verità costruita con quattro colonne. Usiamo le prime due colonne per rappresentare i valori *logici* associati ai qubits di ingresso che chiameremo I_0 e I_1 rispettivamente e le seconde due per i valori logici dei qubit dopo la trasformazione, che indicheremo come O_0 e O_1.
Deve essere chiaro che l'associazione tra valori logici e stato del

I_0	I_1	O_0	O_1
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0

Tabella 8.1: ***Tabella di verità CNOT*** *Le colonne I_0 e I_1 rappresentano i valori logici assegnati a due qubits con le regole $|0\rangle \rightarrow 0$ e $|1\rangle \rightarrow 1$. Le colonne O_0 e O_1 rappresentano i valori logici dei due stessi qubits dopo aver attraversato il gate CNOT.*

qubit è possibile solo quando un qubit si trovi in uno degli stati di base, come in questo esempio (vedi il paragrafo 5.3.3).

Il circuito quantistico che implementa la tabelle 8.1 può essere implementato in QASM come segue:

```
OPENQASM 2.0;
include "qelib1.inc";
```

```
qreg q[2];
creg c[1];

// Configurazione 0 0
reset q[0];
reset q[1];

// Configurazione 0 1
//x q[1];

// Configurazione 1 0
//x q[0];

// Configurazione 1 1
//x q[0];
//x q[1];

cx q[0],q[1];
measure q[1] -> c[0];
measure q[0] -> c[0];
```

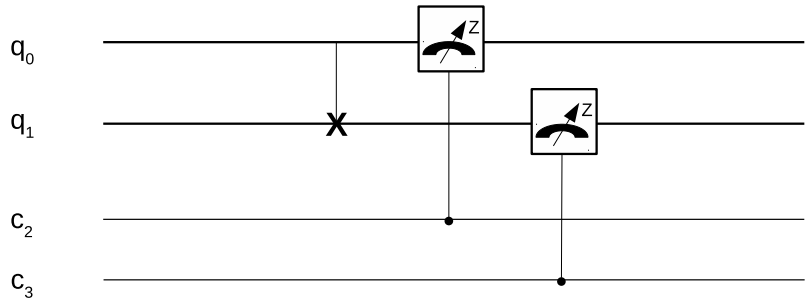

Figura 8.6: La figura mostra lo schema circuitale di due qubit che interagiscono in un gate CNOT.

Osservando la tabella 8.1 si vede che la variabile logica Q_0 dipende solo dalla variabile logica I_0 mentre la variabile logica O_1 dipende da entrambe I_0 ed I_1, in particolare si ha che $O_1 = I_0 \text{XOR} I_1$. Questa relazione vale solo se i qubits sono negli stati base $|0\rangle$ e $|1\rangle$.

Il gate CNOT implementa il controllo di un qubit su un secondo qubit e permette insieme al gate X di implementare qualsiasi funzione logica booleana.

A livello grafico viene rappresentato come una X posta sul qubit controllato e collegata al qubit controllore, come mostrato in figura 8.6

Prima di chiudere questo paragrafo è bene notare che nel-

la computazione quantistica stanno incominciando a nascere alcune convenzioni non scontate e non ovvie. Una tra questa è la scelta adottata anche da IBM di far corrispondere l'indice i+esimo del qubit q_i alla sua posizione in un ket di stato ponendo q_0 destra e numerando con indice crescente verso sinistra, così ad esempio la coppia di qubits $q_0 = |0\rangle$ e $q_1 = |1\rangle$ si riferisce al ket $|10\rangle$ e non $|01\rangle$.

Ovviamente è solo una questione di notazione. ma è meglio tenerla presente per non confondersi quando si comincino ad approcciare i sistemi di computazione. In questo testo **non** stiamo seguendo questa convenzione e poniamo il qubit q_0 come il primo qubit a sinistra.

Qubits in sovrapposizione di stati

Si è visto che i gates quantistici possono produrre trasformazioni sui qubits che dipendono dallo loro combinazione di stati, per esempio si è visto che il CNOT ha una tabella di verità analoga a quella della porta logica XOR. Quello che ancora non si è analizzato è cosa succede quando un gate come il CNOT opera su qubits che non si trovino in stati di base, ma in una sovrapposizione di stati. Questa condizione è importantissima

in quanto segna la vera differenza tra la computazione classica quella quantistica. Come si è potuto intuire dal paragrafo precedente (vedi anche [3]) i gates quantistici possono essere usati per produrre qualsiasi circuito logico classico, quindi la computazione quantistica può riprodurre quella classica. Gran parte dell'interesse verso la computazione quantistica risiede, però, nella sua intrinseca differenza rispetto alla classica e non nella sua analogia con essa.

La caratteristica peculiare della computazione quantistica è che un gates può operare in parallelo su più configurazioni di qubits.

Si consideri il circuito rappresentato in figura 8.6 e si consideri di preparare il qubit q_0 nello stato $q_0 = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ cioè lo stato $q_0 = |+\rangle$, mentre il secondo qubit, cioè q_1 si trovi nello stato $q_1 = |0\rangle$. Quale sarà il risultato della computazione? Per saperlo non resta che applicare il gates allo stato dei due qubits e vederne il risultato. Per farlo abbiamo sia l'opzione *matriciale* che è quella relativa al formalismo bra/ket degli operatori. Seguiamo la seconda.

Lo stato di ingresso che descrive due qubits è dato dal prodotto

tensoriale dei due stati:

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) \tag{8.7}$$

L'azione del gate CNOT su di esso è data da:

$$(|00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 11| + |11\rangle\langle 10|)\frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) = \\ = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \tag{8.8}$$

Il risultato della 8.8 è la sovrapposizione dei due stati $|00\rangle$ e $|11\rangle$, normalizzata dal fattore $\frac{1}{\sqrt{2}}$. In pratica con un'unica operazione informatica si sono potute valutare due possibili combinazioni degli stati di input e produrre la sovrapposizione degli stati di output. Questo potrebbe far pensare che procedendo in questo modo possa scalare la complessità temporale degli algoritmi. Sebbene questo non sia falso, è anche vero che non è sempre possibile sfruttare i risultati della computazione, infatti, per conoscere la combinazione di stati in cui termina un circuito quantistico è necessario eseguire diverse esecuzioni del circuito e diverse misure perché, come si è visto, il risultato di una misura è sempre un autostato dell'operatore, cioè uno dei ket di base.

Tornando al risultato della esecuzione del circuito calcolato in 8.8, non è possibile eseguire una misura che dia come risultato

$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Quello che è possibile è eseguire cento misure, delle quali circa un mezzo darà come risultato $|00\rangle$ e il restate darà come risultato $|11\rangle$.

Il parallelismo quantistico è alla base di algoritmi quantistici che non hanno un analogo classico, come ad esempio l'algoritmo di Shor e quello di Grover, che sfruttano il parallelismo quantistico in modo che non ha analogo classico, ed è in questo che essi si avvantaggiano rispetto ai corrispondenti classici.

8.2.2 Sistema di gates universale

È stato anticipato che qualsiasi circuito quantistico può essere realizzato usando gates che operano su soli due qubits. Questo non significa che qualsiasi algoritmo possa essere implementato usando soli due qubits, di qubits ne possono servire tanti, ma è sufficiente che i gates presenti ne trasformino due alla volta, lo stesso che succede nell'elettronica digitale. Per quanti bits vengano impiegati da un processore, le porte logiche operano sempre su due bits classici alla volta.

Gates S e T

Costruiamo due operatori unitari a partire dall'operatore **Z** questi sono il gates **S** e il gates **T**.

La forma matriciale di **S** è la seguente:

$$\mathbf{S} = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/2} \end{bmatrix}$$

mentre quella nel formalismo bra/ket è data da:

$$\mathbf{S} = |0\rangle\langle 0| + i|1\rangle\langle 1| \tag{8.9}$$

(Si ricordi che $e^{i\pi/2} = i$.)

Il gate S rappresenta un operatore unitario, infatti si ha:

$$\mathbf{S}\mathbf{S}^* = (|0\rangle\langle 0| + i|1\rangle\langle 1|)(|0\rangle\langle 0| - i|1\rangle\langle 1|) = |0\rangle\langle 0| + |1\rangle\langle 1|$$

La forma matriciale di **T** è invece la la seguente:

$$\mathbf{T} = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$$

mentre quella nel formalismo bra/ket è data da:

$$\mathbf{T} = |0\rangle\langle 0| + e^{i\pi/4}|1\rangle\langle 1| \tag{8.10}$$

Il gate S rappresenta un operatore unitario, infatti si ha:

$$\mathbf{T}\mathbf{T}^* = (|0\rangle\langle 0| + e^{i\pi/4}|1\rangle\langle 1|)(|0\rangle\langle 0| + e^{-i\pi/4}|1\rangle\langle 1|) = |0\rangle\langle 0| + |1\rangle\langle 1|$$

Gates H

Il gate H è costruito a partire dall'operatore **H** di Hadamard. La forma matriciale di **H** è la seguente:

$$\mathbf{S} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

mentre quella nel formalismo bra/ket è data da:

$$\mathbf{H} = \frac{1}{\sqrt{2}}(|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| - |1\rangle\langle 1|) \tag{8.11}$$

Il gate H rappresenta un operatore unitario, infatti si ha:

$$\mathbf{H}\mathbf{H}^* = \frac{1}{\sqrt{2}}(|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| - |1\rangle\langle 1|)\frac{1}{\sqrt{2}}(|0\rangle\langle 0| + \tag{8.12}$$

$$+|0\rangle\langle 1| + |1\rangle\langle 0| - |1\rangle\langle 1|) =$$

$$(|0\rangle\langle 0| + |1\rangle\langle 1|) \tag{8.13}$$

I gates presentati e quelli che si possono ottenere con gli operatori visti fin'ora sono un insieme universale e da essi è possibile ottenere qualsiasi funzione logica.

Gates AND e NOT

Un insieme ben nota di gates universali sono il gate AND e il NOT, per provare l'universalità dei gate fin qui presentati prove-

remo quindi che con essi è possibile definire il gate quantistico AND che, insieme al gate X già incontrato costituirà una base noto di gate universali.

La tavola di verità della porta logica AND è mostrata nella tabella seguente:

x	y	x AND y
0	0	0
0	1	0
1	0	0
1	1	1

Come si vede, per il valore 0 del risultato x AND y corrispondono tre differenti configurazioni dei valori di input. Questo significa che il semplice risultato di una operazione AND non è sufficiente a conoscere il valore iniziale dei bits che l'hanno prodotto, ma solo a sapere che i due bit non erano entrambi ad 1.

Questa constatazione è sufficiente a farci dedurre che nessun gate quantistico che usi solo due qubits può implementare tale funzione, infatti si è visto che le operazioni quantistiche sono

implementate da operatori unitari i quali ammettono sempre un inverso, quindi è sempre possibile ricavare lo stato dei qubit di ingresso conoscendo lo stato dei qubit di uscita.
L'unico modo per ottenere una computazione analoga ad una porta AND è quella di usare tre qubits. Due qubits rimarranno inalterati dalla computazione, mentre il terzo assumerà il valore della funzione logica AND. Il circuito ricercato è rappresentato in figura 8.7. La tavola di verità del gate quantistico AND si ottiene direttamente da quella del gate classico:

q_0	q_1	q_2	q_0	q_1	q_0 AND q_1
Ingressi			Uscite		
0	0	0	0	0	0
0	1	0	0	1	0
1	0	0	1	0	0
1	1	0	1	1	1

La definizione del circuito presentato in figura 8.7 rappresenta il cuore della computazione quantistica: progettare trasformazioni unitarie e pensare a come usarle. Ogni trasformazione unitaria può essere decomposta in trasformazioni unitarie elementari, per questo per progettare un algoritmo quantistico non è necessario inventare nuovi gates, ma è sufficiente

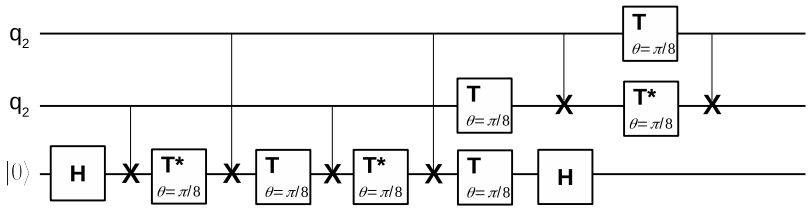

Figura 8.7: La figura mostra lo schema circuitale con un registro di 3 qubits che implementa la porta AND.

usare i gates di base già esistenti.

8.3 Esercizo risolto

- Esercizio: Creare un circuito quantistico che scambi tra loro gli stati di due qubits.

  Soluzione: La tavola di verità del circuito che vogliamo ottenere è mostrata nella tabella seguente:

q_0	q_1	q_0	q_1
Ingressi		Uscite	
0	0	0	0
0	1	1	0
1	0	0	1
1	1	1	1

Dobbiamo ora pensare ad una trasformazione, o ad una serie di trasformazioni che implementi la tabella 8.3. Indichiamo con la lettera **G** il gate che trasforma due qubits come voluto. Dalla tavola di verità è immediato ricavare la sua forma, infatti procedendo una riga alla volta, vediamo che la prima chiede che se i due qubits si trovano all'ingresso del circuito nello stato iniziale $|00\rangle$ allora si devono trovare nello stesso stato all'uscita, quindi troviamo la prima parte della definizione di **G**:

$$\mathbf{G} = |00\rangle\langle 00| + ... \tag{8.14}$$

perché in questo modo risulta che:

$$\mathbf{G}|00\rangle = |00\rangle\langle 00|00\rangle = |00\rangle \tag{8.15}$$

La seconda riga della tabella richiede che allo stato di ingresso $|01\rangle$ corrisponda lo stato di uscita $|10\rangle$, questo si ottiene semplicemente aggiungendo l'elemento $|01\rangle\langle 10|$ all'operatore **G** come segue:

$$\mathbf{G} = |00\rangle\langle 00| + |01\rangle\langle 10| + ... \tag{8.16}$$

Continuando con questo procedimento, cioè analizzando una riga per volta della tabella di verità, otteniamo alla

fine la seguente espressione per **G**:

$$\mathbf{G} = |00\rangle\langle 00| + |01\rangle\langle 10| + |10\rangle\langle 01| + |11\rangle\langle 11| \tag{8.17}$$

L'operatore **G** è il *programma* quantistico che volevamo realizzare. L'intuizione logica ci porta a pensare che il programma realizzato sia corretto e realizzabile, cioè sia una trasformazione unitaria nel senso in cui le trasformazioni unitarie sono state definite nel paragrafo 6. In pratica, per essere sicuri che **G** sia un programma quantistico corretto, dobbiamo verificare che sia verificata la condizione di unitarietà:

$$\mathbf{G}^*\mathbf{G} = \mathbf{I} \tag{8.18}$$

Per farlo vediamo che l'operatore $\mathbf{G}^*$ è ottenuto da **G** scambiando semplicemente i bra con i ket:

$$\mathbf{G}^* = |00\rangle\langle 00| + |10\rangle\langle 01| + |01\rangle\langle 10| + |11\rangle\langle 11| \tag{8.19}$$

Il prodotto $\mathbf{G}^*\mathbf{G}$ è quindi dato da:

$$\begin{aligned}\mathbf{G}^*\mathbf{G} = &(|00\rangle\langle 00| + |10\rangle\langle 01| + |01\rangle\langle 10| + |11\rangle\langle 11|) \\ &(|00\rangle\langle 00| + |01\rangle\langle 10| + |10\rangle\langle 01| + |11\rangle\langle 11|) = \\ = &|00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 10| + |11\rangle\langle 11| = \mathbf{I}\end{aligned} \tag{8.20}$$

Con questo calcolo è stato dimostrato che il programma è corretto e può essere quindi implementato come programma quantistico. A questo punto l'esercizio sarebbe già completato, se solo avessimo a disposizione un gate che implementa la trasformazione di questo operatore... invece per esso non è presente un gate, allora va ottenuto attraverso altri gates. Come vediamo dai seguenti passaggi possiamo ottenere il gate voluto come il prodotto di tre Cnot:

$$\begin{aligned} &|00\rangle\langle 00| + |10\rangle\langle 01| + |01\rangle\langle 10| + |11\rangle\langle 11| = \\ &= (|00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 11| + |11\rangle\langle 10|) \\ &\quad (|01\rangle\langle 11| + |11\rangle\langle 01| + |00\rangle\langle 00| + |10\rangle\langle 10|) \\ &\quad (|00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 11| + |11\rangle\langle 10|) \end{aligned} \tag{8.21}$$

Il primo Cnot rappresenta il controllo di un qubit sul secondo qubit. Il secondo agisce sempre sui due qubits ma questi si scambiano di ruolo ed è il secondo qubit a controllare il primo. Infine nel terzo abbiamo di nuovo il primo qubit che controlla il secondo (vedi figura 8.8)

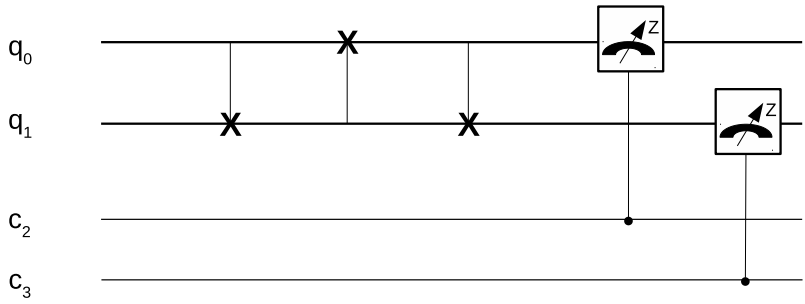

Figura 8.8: La figura mostra lo schema circuitale del programma swap che scambia tra loro il valore dei qubits q_0 e q_1 se questi si trovano in uno degli stati base.

8.4 Qubits in stato entangled

Una caratteristica peculiare dei qubits è che essi possono presentarsi in uno stato particolare in cui la misura di uno determina la misura dell'altro.

Da bambini capita di dover prendere decisioni sul gioco da fare, per esempio all'interno di una piccola comitiva il capo propone di giocare a calcio. Alcuni sono d'accordo, altri sono in disaccordo, e Marco dice: *Io gioco solo se gioca Luca* indicando l'amico del cuore.

Dal punto di vista dell'organizzatore del gioco, si presenta una

situazione particolare, egli dispone di una parte di dati certi, e di altri dati incerti ma condizionati. Perché dati incerti? Perché egli non ha ancora chiesto a Luca cosa intenda fare, ma sa che la sua risposta porterà o a due nuove adesioni alla sua proposta, oppure a due defezioni.

Le decisioni di Marco e Luca sono *entangled*.

Ora però lasciamo Luca, Marco e gli altri amici ai loro giochi e torniamo ad occuparci di giochi da grandi. Consideriamo il seguente stato di due qubits:

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|11\rangle + |00\rangle) \tag{8.22}$$

La 8.22 descrive lo stato in cui si trovano due qubits e come si vede si stratta di una sovrapposizione degli stati base $|00\rangle$ e $|11\rangle$. Come si è visto nel paragrafo 5.7.3 il risultato della misura di un qubit è probabilistico. Se si provasse ad eseguire la misura del primo qubit, il qubit q_0, si avrebbe la metà delle probabilità di trovarlo nello stato $|1q_1\rangle$ e metà di trovarlo nello stato $|0q_1\rangle$. Cosa dire della misura di q_1?

Analizzando con attenzione la 8.22 si vede che dopo aver misurato q_0, lo stato di q_1 è determinato e non più probabilistico, esattamente come dopo aver chiesto a Luca se gli sta bene giocare a calcio, lo stato di Marco è determinato e non più proba-

bilistico. Infatti vediamo che i due qubits sono nella sovrapposizione di stati $\frac{1}{\sqrt{2}}(|11\rangle + |00\rangle)$. Lo stato in cui $q_0 = |1\rangle$ e $q_1 = |0\rangle$ corrisponderebbe allo stato $|10\rangle$ ma come si vede questo non è presente nella 8.22 quindi ha probabilità zero di essere trovato alla fine di una misura.

Come si è visto da questo semplice esempio, esistono degli stati in cui i qubits sono *aggrovigliati*, un po' come due fili che si intreccino e per scioglierne uno sia necessario sciogliere anche l'altro. Gli stati entangled sono semplici da produrre. Si supponga infatti di avere un circuito composto da due qubits, il qubits q_0 e il qubits q_1. Sia il primo nello stato $|+\rangle$ e il secondo nello stato $|0\rangle$. Si mandino i due qubit al gate Cnot: quello che si ottiene è esattamente lo stato mostrato in 8.22.

Il meccanismo dell'entanglement fu inizialmente considerato un punto debole della teoria quantistica, infatti il fisico Albert Einstein propose un paradosso, noto come il paradosso EPR, per il quale l'esistenza dell'entanglement avrebbe contraddetto la stessa teoria della relatività.

Oggi l'entanglement è considerato un aspetto cruciale della computazione quantistica, infatti gli stati di qubits entangled so-

no alla base del teletrasporto quantistico, del principio di non clonazione e del dense coding[3] elementi fondamentali della computazione quantistica avanzata.

CAPITOLO 9

Conclusioni

Informatica classica, quella di A. Turing ed E. Shannon per intenderci, si basa sul concetto di bit. I bits sono l'alfabeto del nastro di Turing e sono i simboli usati per lo scambio di messaggi di Shannon.

Comprende l'informatica: trasmettere trasformare e ricevere informazioni, significa comprendere Cosa significa trasmettere trasformare e ricevere bits. L'uso dei linguaggi di alto livello ha sicuramente semplificato la programmazione permettendo di astrarsi dai veri problemi informatici concentrandosi solo sugli aspetti algoritmici. Sebbene questo sia assolutamente naturale, è chiaro che la programmazione svincolata dal proprio alfa-

beto ha poco a che fare con l'informatica mentre ha sicuramente a che fare con la logica matematica e con la computazione in generale.

Sorge una domanda, può valere lo stesso nell' informatica quantistica? Potrebbe aver senso pensare ad una informatica quantistica di alto livello svincolata dal concetto di qubit?

La risposta sembra essere un no. L'informatica quantistica è intrinsecamente collegata al suo alfabeto. Il vantaggio che si potrà trarre dal informatica quantistica è basato sul parallelismo intrinseco di questo paradigma computazionale, quindi alla sovrapposizione degli stati per un qubit.

Questo testo ha fornito gli elementi fondamentali che sono necessari a chi vuole intraprendere un percorso in questa disciplina e vuole capire a fondo questo nuovo paradigma computazionale.

Bibliografia

[1] PAM Dirca, The Lagrangian in Quantum Mechanics. Physikalische Zeitschift der Sowjetunion (1933)

[2] Laundau, L., Lifsits, E. Meccanica quantistica, teoria non relativistica. Editori riuniti university press.

[3] Sisini, F. Sisini, V Informatica quantistica: introduzione con esempi in linguaggio C. Scuola Sisini (2020).

[4] A. Einstein, B. Podolsky, and N. Rosen. Can Quantum-Mechanical Description of Physical Reality Be Considered Complete? Phys. Rev. 47 (1935)

[5] Über einen die Erzeugung und Verwandlung des Lichtes betreffenden heuristischen Gesichttspunkt ("On a Heuristic Viewpoint Concerning the Production and Transformation of Light"). Annalen der Physik, 4 (1905)

[6] Heisenberg W.K. (1958), Physics and philosophy, New York Harper and Row. (Original published in 1955: Das Naturbild der heutigen Physik). Italiano: H.W.K. Natura e fisica moderna, Garzanti, 1960, pagg. 24 e 25.

[7] Shannon E. A Mathematical Theory of Communication, Bell System Technical Journal (1948)

[8] Turing, A.M. On Computable Numbers, with an Application to the Entscheidungsproblem, Proceedings of the London Mathematical Society (1937).

Indice analitico