

Francesco e Valentina Sisini

Informatica Quantistica

Introduzione con esempi in linguaggio C

Prima edizione

Edizioni: i Sisini Pazzi, 2020

Proprietà intellettuale di Francesco Sisini, 20

Edizione: I Sisini Pazzi

*Questo testo è dedicato a Carlo Ferrario (1949-2015),
relatore della mia tesi di Laurea.*

*Per la sua lucidità di pensiero e chiarezza espositiva è stato
un punto di riferimento per diverse generazioni di studenti
e studentesse che si sono formati presso l'università degli
studi di Ferrara.*

*Per negligenza, non l'ho ringraziato allora. Lo faccio
adesso.*

Francesco

Scuola Sisini ringrazia calorosamente Lauro Galtarossa per
la rilettura, non specializzata ma condotta in forma
amichevole, del testo.

Ai nostri lettori

Scuola Sisini è una piccola casa di produzione di testi e giochi realizzati con lo scopo di divulgare argomenti complessi.

Esiste una forbice tra richiesta ed offerta di conoscenza: da un lato articoli scientifici destinati solo ad un pubblico iper specialistico, dall'altro la divulgazione nozionistica di contenuti affascinanti, descritti però qualitativamente.

Tra questi due estremi si inserisce il metodo di divulgazione di Scuola Sisini che, attraverso un percorso ragionato, porta ad uscire dalla propria zona di comfort per far propri gli strumenti e le basi che permettono poi di approfondire autonomamente gli argomenti di interesse.

Indice

Introduzione	7
Come è organizzato questo libro	
A chi è rivolto questo testo?	
Convenzioni tipografiche	
Pagina web del libro	
Premessa	12
1. Punto di partenza	13
1.1 Mondo classico e mondo quantistico: la doppia fenditura	
1.2 Si deve imparare la meccanica quantistica per comprendere la computazione quantistica?	
1.3 Simulare la fisica sul computer: si può fare Mr. Feynman?	
2. Dai bits classici ai qubits quantistici	25
2.1 I bits nell'informatica classica	
2.2 Proprietà dei bits	
2.3 I qubits	
3. Principi della meccanica quantistica	46
3.1 Formulazione matematica del principio di sovrapposizione	
3.2 Stato e probabilità	
3.3 Spazi vettoriali e prodotti tensoriali: capire l'entanglement	
3.4 Vettori bra e ket	
3.5 Osservabili fisiche	
4. I calcoli dei computer, consumano energia?	69
4.1 Entropia	
4.2 Termodinamica della computazione irreversibile	
4.3 Termodinamica della computazione reversibile	
4.4 Componenti circuitali per la computazione reversibile	
4.5 Circuiti reversibili	
5. Gates quantistici	91

5.1 Il NOT come gate quantistico	
5.2 Matrici di Pauli	
5.3 Il gate H	
5.4 Il gate CNOT	
5.5 Altri gates a due qubits	
6. Computazione quantistica senza corrispondenza classica	
6.1 Teorema di non clonazione	105
6.2 Dense coding	
6.3 Teletrasporto	
7. Esercizi in linguaggio C	118
7.1 Libreria libSSQ	
7.2 Esercizi	
7.3 Soluzioni	
Conclusioni	151
Come approfondire gli argomenti	
Risposte alle domande	153
Bibliografia e riferimenti	154
Altre pubblicazioni di Scuola Sisini	

Introduzione

L'informatica quantistica si è impegnata in una promessa importante: usare i processi della fisica quantistica per codificare, elaborare e trasmettere informazioni.

Rispetto alle tecnologie informatiche *classiche*, la scienza quantistica propone tre importanti novità non previste nella *fisica/informatica classica* perché basate sul concetto quantistico di sovrapposizione degli stati ed in particolare su quello di entanglement:

- principio di non clonazione
- teletrasporto quantistico (dell'informazione)
- dense coding (codificazione a maggior densità)

La sfida è duplice: da un lato creare un sistema di trasmissione delle informazioni sicuro e a prova di qualsiasi intrusione, dall'altro scrivere algoritmi che risolvano problemi che attualmente richiedono anni di computazioni anche ai super computer di ultima generazione.

Da sola, la promessa di questi risultati è già sufficiente a far *entusiasmare* le grosse compagnie informatiche del momento e a spingerle ad investire ingenti capitali. Ma l'aspetto realmente affascinante della computazione quantistica, che per tanti darà finalmente un senso allo studio della termodinamica compiuto alle scuole superiori o all'università, è che essa è reversibile e, in linea di principio, è eco sostenibile: potrebbe non consumare energia.

Come è organizzato questo libro

Questo testo propone un percorso figurato attraverso idee, concetti, nozioni e dimostrazioni. Raggiungere la fine del percorso è senz'altro importante, ma non bisogna trascurare il valore del percorso in sé che ha l'obiettivo di creare

collegamenti e connessioni tra argomenti diversi che qui si fondono in un filo conduttore che porta infine alla capacità di comprendere, e poi di padroneggiare, la nuova scienza informatica che da più di quarant'anni busca alle porte e che per ora è stata accessibile solo a pochi.

Per stimolare l'interesse, la curiosità e facilitare la comprensione, anche intuitiva, di questo argomento ancora nuovo, il percorso proposto non sarà sempre lineare, ma arricchito di esempi e anticipazioni che hanno lo scopo di introdurre gradualmente gli argomenti lasciando il tempo necessario affinché essi siano assimilati prima di venire trattati con gli strumenti formali necessari. Si potranno quindi incontrare concetti e termini che vengono inizialmente solo accennati per essere poi ripresi e sviluppati nel seguito del testo.

Questo testo è nato per essere letto in modo completo ed, essendo un'introduzione, predilige la scorrevolezza della lettura allo sviluppo esaustivo degli argomenti trattati.

- Nel capitolo 1 vengono introdotte le prime idee della meccanica quantistica e si percorre rapidamente lo sviluppo del pensiero che ha portato all'ipotesi di poter costruire un computer quantistico.
- Nel capitolo 2 si introducono in modo *informale* i concetti di qubits e di sovrapposizione degli stati. Scopo del capitolo è portare l'attenzione sui veri obiettivi del libro creando l'interesse per proseguirne la lettura e superare il capitolo 3.
- Il capitolo 3 è il più complesso dell'intero testo, ma, dopo averlo compreso, si avranno tutti gli strumenti per capire l'informatica quantistica ad ogni livello. Qui vengono introdotti i principi base della meccanica quantistica necessari per comprendere a pieno il senso del resto della lettura. I principi vengono trattati anche matematicamente.

Si raccomanda la lettura dell'intero capitolo.

- La relazione tra reversibilità della computazione e la meccanica quantistica è trattata nel capitolo 4. Questo capitolo rappresenta il cuore dell'argomento e, senza eccedere nei formalismi matematici, presenta un aspetto affascinante delle tecnologie quantistiche emergenti.
- Nel capitolo 5 vengono presentati i gates quantistici. Si concretizzano i concetti visti nel capitolo 3 in componenti circuitali che sono capaci di trasformare lo stato dei qubits da 1 a 0 e da 0 ad 1, analogamente a quanto fanno le porte logiche (logics gates) con i bits *classici*.
- Il principio di non clonazione, il teletrasporto e il dense coding sono presentati e spiegati in dettaglio nel capitolo 6. Fondamenti su cui si basa la potenzialità dell'informatica quantistica, capiti i quali, saranno acquisiti gli strumenti intellettuali per entrare consapevolmente nello studio e nella pratica della computazione quantistica.
- Nel capitolo 7 vengono proposti una serie di esercizi da eseguire per fissare le idee sui concetti appresi. Questi sono esercizi di programmazione in linguaggio C che per essere svolti richiedono di aver compreso le nozioni presentate nei capitoli precedenti.

Al termine del capitolo sono presentate le soluzioni dei problemi proposti.

A chi è rivolto questo testo?

Questo libro può essere letto in chiavi diverse a seconda della propria preparazione di base.

Completamente digiuno di fisica e di informatica

Lo yoga ci insegna che il primo movimento della respirazione deve essere l'espirazione, perché nei polmoni serve spazio prima di inspirare nuovo ossigeno. Quindi, se vi trovate nella

situazione di non sapere nulla, non disperate, perché allora c'è posto per il nuovo.

Sazio di informatica ma digiuno di meccanica quantistica

Se la teoria di Shannon e il concetto di entropia dell'informazione sono già note, la loro applicazione nell'ambito quantistico sarà frutto di sorpresa e soddisfazione. In questo caso potrete apprezzare come concetti già noti possono essere rivisitati in un'ottica completamente nuova.

Sazio di fisica ma digiuno di informatica

È difficile completare il corso di studi in fisica senza aver scritto qualche riga di codice, ma si sa che la programmazione è solo una piccola fetta dell'informatica e quindi non disperate perché troverete nel testo le informazioni essenziali per applicare le vostre conoscenze di meccanica quantistica alla teoria informatica e, dove il testo deve glissare, troverete i giusti riferimenti per completare lo studio in modo indipendente.

Esperto di fisica e di informatica

La fisica e l'informatica si sono trovate già a stretto contatto nei primi anni '40. Ora, di nuovo, è la fisica che ha la responsabilità di guidare lo sviluppo tecnologico fino a rendere l'informatica quantistica una realtà ingegnerizzata. Questo testo ha l'ambizione di fornire una prima guida introduttiva per mettere in relazione la meccanica quantistica e la teoria dell'informazione.

Convenzioni tipografiche

Nel testo sono inseriti dei **Box** che contengono degli approfondimenti sull'argomento trattato nel paragrafo. I box

sono segnalati dalla scritta **Box**, incorniciati e con lo sfondo giallo.

Nel testo si è fatto uso del **grassetto** per evidenziare i termini chiave in una frase e del *corsivo* per le parole che hanno un significato specifico nel contesto del discorso.

Per esempio:

La meccanica quantistica inserisce all'interno della teoria anche il concetto di **misura**. Si deve notare che anche la teoria classica prevedeva le misure sperimentali...

Per programmare un computer *classico* è necessario prendere confidenza con la tecnologia: tastiera, monitor, editor ecc., e apprendere il concetto di *linguaggio formale* con il quale è possibile descrivere un algoritmo.

Pagina web del libro

Sul sito <https://pumar.it> è presente la pagina web del libro (<https://pumar.it/libroQuantistica.php>)

Sulla pagina si possono trovare diversi link di interesse e il link con gli **errata corrige** che emergeranno nel corso del tempo.

Sono state programmate una serie di revisioni del testo con scadenza mensile, gli eventuali errori rilevati saranno riportati e corretti. I codici C presentati nel capitolo 7 sono disponibili all'indirizzo:

<https://github.com/francescosisini/LIBRO-Informatica-Quantistica>

Gli argomenti sono inoltre trattati sul canale di ScuolaSisini: <https://www.youtube.com/channel/UCDwLlFqa0xZ71PEOdHA0aSQ>

Premessa

Questo testo è una prima introduzione ai concetti e ai principi dell'informatica quantistica. Qui sono presentati e spiegati tutti gli strumenti matematici, fisici e informatici necessari per una comprensione completa e consapevole. Il testo è auto consistente e, per una prima lettura, non richiede l'ausilio di altri testi specifici. Per mettere in pratica i concetti presentati alla fine del libro sono inseriti in un capitolo apposito degli esercizi di programmazione in linguaggio C. Il capitolo può essere saltato senza pregiudicare la comprensione del resto.

1. Punto di partenza

La fisica è una scienza impegnativa perché non si accontenta di risposte verosimili, ma pretende una continua verifica sperimentale di ogni affermazione che viene fatta in suo nome. Nonostante questo obiettivo è ironico sapere che ogni teoria è probabilmente falsa, e quelle che crediamo vere, sono in attesa di essere dimostrate false o appunto *falsificate*.

Con questo, si deve rinunciare al proposito di studiarle? No certo, perché le teorie della fisica, entro certi limiti, funzionano. Nel XX secolo è stato dimostrato che la teoria della gravitazione universale è falsa, ciò nonostante, essa è ancora molto utile per numerosi calcoli di balistica spaziale e per i conti più *grossolani* di astronomia del sistema solare.

La teoria di Newton sulla gravitazione è stata sostituita da quella di Einstein della relatività generale. Negli ultimi decenni però anche quest'ultima ha dato segni di cedimento e in futuro potrebbe essere messa in discussione.

Le leggi che la fisica identifica come leggi fondamentali costituiscono la *meccanica* del nostro universo.

Il primo incontro *scolastico* che si ha con la meccanica è la *cinematica*. Questa descrive le relazioni tra posizione e velocità di un *punto materiale*. Il concetto di punto materiale è un concetto *classico* che parte dall'idea che la materia possa essere pensata in modo analogo alla geometria euclidea, dove i solidi hanno superficie e volume definiti, ma sono costituiti da insiemi di punti ognuno dei quali ha dimensione nulla.

Allo stesso modo il punto materiale ha dimensione nulla, ma ad esso è associata una massa.

Lo stato del punto materiale è completamente descritto quando sono definite le sue tre coordinate spaziali x , y e z e le tre componenti cartesiane della sua velocità: v_x , v_y e v_z .

La posizione e la velocità del punto materiale possono variare con il tempo e per questo si specifica che sia le coordinate che

la velocità sono funzioni di quest'ultimo: $x(t)$, $y(t)$ e $z(t)$ e $v_x(t)$, $v_y(t)$ e $v_z(t)$.

La meccanica quantistica trova il suo primo **disaccordo** con la meccanica classica già qui: secondo la meccanica quantistica non è possibile che ad un dato istante di tempo, per una particella, si conoscano **esattamente** la sua posizione e la sua velocità. Questo è noto come *principio di indeterminazione di Heisenberg*.

Come è stato chiarito all'inizio del paragrafo, la meccanica quantistica si discosta notevolmente dalla meccanica classica, ma non è definibile senza di essa.

Nella meccanica classica un sistema fisico si ritiene completamente definito quando siano note tutte le posizioni dei punti che lo compongono, tutte le velocità e le eventuali forze che stanno agendo. Ovviamente non può essere lo stesso per un sistema quanto-meccanico, visto che queste grandezze non possono essere note simultaneamente con precisione arbitraria. La meccanica quantistica inserisce all'interno della teoria anche il concetto di **misura**. Si deve notare che anche la teoria classica prevedeva le misure sperimentali, anzi queste fanno parte del metodo sperimentale con cui la teoria è stata costruita, ma nella meccanica classica tali misure sono intese come esterne alla teoria.

La differenza tra i due approcci è che nel *classico* il processo di misura è visto come un'azione necessaria all'osservatore dell'esperimento per conoscere empiricamente il valore di una grandezza che sta osservando, ma che detta grandezza abbia un ben dato valore indipendente dal processo di misura. Nel *quantistico* invece, secondo l'interpretazione della scuola di Copenaghen, le grandezze fisiche di un dato sistema non hanno sempre valori definiti, ma li assumono nel momento stesso in cui accade un evento *speciale*, come appunto una misura.

A questo proposito è d'obbligo chiarire subito per evitare malintesi. Il concetto di **misura** in meccanica quantistica non prevede la presenza di un essere intelligente: con misura si intende (per esempio) l'interazione di un sistema molto piccolo, cioè di dimensioni atomiche, sub-atomiche o particellare con un sistema classico, cioè di grande massa. Non si pensi che grande massa significhi la massa di un edificio, basta prendere venti grammi di acqua per avere (circa) un numero di Avogadro (6×10^{23}) di molecole, quindi il concetto di grande massa va rapportato alla scala atomica (Landau, 1947; Bohr 1928).

Questo aspetto della teoria è difficile da capire perché si scontra contro l'esperienza quotidiana che per l'appunto è un'esperienza *classica* della fisica.

Domanda n. 1 Il principio di indeterminazione di Heisemberg riguarda:

- a. L'impossibilità di misurare simultaneamente e con precisione arbitraria la posizione e la quantità di moto di una particella
- b. L'impossibilità di predire correttamente l'evoluzione dello stato di un sistema fisico

1.1 Mondo classico e mondo quantistico: la doppia fenditura

Se lasciamo cadere un oggetto dalla mano, durante la sua caduta, siamo convinti che esso abbia una posizione ed una velocità ben definite.

Non importa se lo stiamo osservando o meno: secondo il senso comune l'oggetto si trova sempre in uno stato fisico ben definito.

Le cose stanno diversamente secondo la meccanica quantistica

(Tonomura, 1989). Per fare un esempio familiare, consideriamo un vecchio televisore a tubi catodici e proviamo a seguire il percorso di un elettrone che fuoriesce dal catodo. Supponiamo di porre tra il catodo e lo schermo televisivo una targhetta in metallo con due fenditure vicine, in modo che se l'elettrone non azzecca una delle due venga fermato dalla targhetta.

Dopo aver acceso la TV, vederemo comparire dei puntini luminosi sullo schermo secondo una data disposizione, e penseremo:

*ogni puntino sullo schermo corrisponde ad un elettrone
che è riuscito ad attraversare una fenditura*

Nel nostro pensiero, ch  segue l'intuizione classica, un elettrone che   riuscito a passare deve aver attraversato l'una o l'altra fenditura della targhetta.

Secondo la meccanica quantistica, invece, le cose non sono andate esattamente cos .

Se durante il moto dell'elettrone non   stato condotto alcun esperimento per misurare la sua posizione, allora non si pu  dire se l'elettrone abbia seguito una specifica traiettoria e neanche se sia passato dall'una o dall'altra fenditura, ma si pu  dire solo che:

se   arrivato sullo schermo, allora   passato per l'una e/o per l'altra fenditura.

A prima vista questa considerazione pu  sembrare priva di interesse pratico, quasi un sofisma, ma dal 1980 in avanti ha assunto un ruolo chiave nella tecnologia futura, cio  da quando il fisico Richard Feynman ha pensato che la meccanica quantistica poteva essere la base per la costruzione di un nuovo modello di calcolo, differente da quello sviluppato da Alan Turing (Feynman, 1982).

Questo aspetto della natura   chiamato **principio di sovrapposizione degli stati**.

Da esso discendono un teorema e due importanti applicazioni dell'informatica quantistica: il teorema del **no cloning principle** e le due applicazioni **dense coding** e **quantum teleportation**, che saranno discusse dettagliatamente più avanti nel testo.

1.2 Si deve imparare la meccanica quantistica per comprendere la computazione quantistica?

Per comprendere la meccanica quantistica servono almeno tre anni di studio: uno dedicato alle basi matematiche, partendo dal calcolo differenziale in una sola dimensione e sul campo dei numeri reali, per arrivare al calcolo sul campo dei numeri complessi; uno dedicato allo studio della meccanica hamiltoniana ed uno alla meccanica quantistica, teoria non relativistica e teoria relativistica.

Questo studio **non può** essere condotto dopo cena come passatempo, ma deve impegnare il giorno intero.

Per fortuna si possono comprendere i principi dell'informatica quantistica e la base del funzionamento di un computer quantistico anche senza conoscere tutta la meccanica quantistica.

La situazione presente non è diversa dallo scenario in cui furono presentati i primi computer nel secolo scorso.

Le prime macchine erano la sintesi perfetta dello stato dell'arte della logica matematica e dell'elettronica, che allora era una scienza su cui avevano competenza solo i fisici perché i corsi di ingegneria elettronica ancora non esistevano.

Negli anni '50 del XX secolo per spiegare il funzionamento di un computer era necessario un fisico esperto e per scrivere un programma serviva comunque un matematico o un ingegnere.

Il concetto di memoria volatile era assolutamente nuovo e si basava su tecnologie al limite del realizzabile, per cui era difficile separare l'idea astratta di **automa** dalla sua concreta

realizzazione.

Come risultato di questo scenario la programmazione di un computer appariva possibile solo ad esperti fisici, matematici ed ingegneri.

Anche senza correre troppo indietro negli anni, basta pensare al film "War Games" di John Badham (1983). Il film racconta la storia di un giovane hacker che si trova ad affrontare un'intelligenza artificiale che scambia la guerra mondiale per un gioco di strategia.

È interessante notare che il programma di intelligenza artificiale venga presentato come il frutto del lavoro di un unico scienziato: Stephen Falken.

L'idea dello *scienziato* capace da solo di realizzare *un mostro* come quello del dottor Frankenstein, era un retaggio della prima informatica degli anni '50.

Dalla visione di un'informatica lontana ed *aliena* si è passati in pochi decenni a linguaggi di programmazione come *scratch* pensati per introdurre la programmazione già dalle scuole elementari.

Oggi è possibile formare un programmatore in pochi mesi senza che egli conosca nulla di elettronica.

Per programmare un computer classico è necessario prendere confidenza con la tecnologia: tastiera, monitor, editor ecc., e apprendere il concetto di *linguaggio formale* con il quale è possibile descrivere un algoritmo, anche senza sapere come funziona effettivamente un computer.

Quanto appena detto per la programmazione di computer classici, vale anche per i computer quantistici. Se si conosce la meccanica quantistica si può capire a fondo come funzionino la loro tecnologia, ma la comprensione approfondita di questa non è necessaria per formulare un algoritmo quantistico.

Il messaggio quindi è il seguente: con un certo sforzo, chiunque si applichi, può comprendere e applicare la computazione

quantistica e, se studierà in modo completo la meccanica quantistica, comprenderà anche come funziona un computer quantistico.

Non mi sembra nulla di diverso dallo scenario attuale.

In questo testo svilupperemo diversi esempi di programmi che simuleranno alcuni aspetti di un computer quantistico. Va da sé che la simulazione non potrà riprodurre le prestazioni in termini di velocità.

Domanda n. 2 Quali sono i tre aspetti peculiari della informatica quantistica di cui si è accennato?:

- a. Dense coding, quantum teleportation, indeterminazione degli stati
- b. Dense coding, quantum teleportation, no cloning principle
- c. Dense coding, no cloning principle, sovrapposizione degli stati

1.3 Simulare la fisica sul computer: si può fare Mr. Feynman?

Il titolo di questo paragrafo nasce dalla parafrasi del titolo del libro "Sta scherzando Mr. Feynman?" di Ralph Leighton, amico di Feynman, che raccolse diversi aneddoti sullo scienziato.

Richard Feynman era un fisico con una ricca carriera accademica che aveva lavorato con J. von Neumann a metà degli anni '40 e vide nascere i primi computer *classici*.

L'idea di un modello di computazione basato sulla meccanica quantistica risale almeno al 1980, proprio per opera di Feynman, che presentò la sua idea nel 1981 con un articolo intitolato *Simulating physics with computers*, pubblicato sulla rivista International Journal of Theoretical Physics, nel quale

poneva una domanda precisa:

È possibile simulare la fisica quantistica usando un computer?

Nell'articolo, Feynman spiegava le ragioni per cui i computer classici erano adatti a simulare la fisica classica, ma non la fisica quantistica.

È interessante notare l'influenza che von Neumann deve avere avuto sull'allora giovane Feynman, nell'articolo, infatti, Feynman si riferisce ai computer sempre in termini di automi cellulari, idea nata appunto dalla mente di von Neumann mentre cercava di progettare un modello di automa che potesse *auto riprodursi*.

L'argomentazione usata da Feynman, di seguito esposta, è importante perché ci introduce direttamente ai principi di meccanica quantistica che ci sono necessari per sviluppare il resto del testo, in modo particolare al principio di *località* della fisica classica.

La fisica classica è locale

La fisica classica è una *teoria locale*, cioè: l'interazione tra due *entità fisiche* avviene solo quando sono a diretto contatto.

Questa affermazione potrebbe sembrare in contrasto con i fenomeni elettromagnetici ed elettrostatici: pensiamo per esempio a due punti materiali che esercitano l'uno sull'altro una forza coulombiana.

In realtà anche l'elettromagnetismo è una teoria locale e infatti l'azione a distanza tra due cariche è dovuta al *campo di forze* indotto da ogni carica che agisce sull'altra carica, quindi l'azione su ogni carica è comunque sempre **locale** e quindi dipende solo dal valore del campo nel punto in cui si trova la carica.

Per chiarire bene il proprio punto di vista Feynman fece riferimento al modello computazionale dell'**automa cellulare**.

A differenza della più nota *architettura di von Neumann*, dovuta naturalmente a von Neumann, l'automa cellulare ha la caratteristica che ogni bit cambia il proprio valore in base al valore che hanno i bit adiacenti, quindi l'*interazione è locale*. In realtà anche i computer odierni che si basano sull'architettura di von Neumann sono *locali*, ma nell'automa cellulare questa *località* è resa più evidente, e per questo Feynman preferì riferirsi ad essa.

Box: Modello di calcolo dell'automa cellulare

Questo modello è stato introdotto da von Neumann che, studiando i primi modelli di intelligenza artificiale nel campo informatico, pensò all'automa cellulare per realizzare una forma di automa che potesse auto riprodursi.

La particolarità dell'automa cellulare è che la computazione avviene in modo *parallelo* e puntuale o, appunto, **locale**. L'automa infatti consiste in:

- Una stringa formata di bit che possono essere nello stato 0 oppure 1. Ogni bit è detto cella.
- Una regola che stabilisce come ogni cella cambi di stato in base al valore delle celle vicine.

Il sistema di calcolo è molto semplice. All'istante $t = 0$ l'automa si trova in una certa configurazione iniziale. All'istante $t = 1$, per ogni cella, si valutano i due bit a destra e a sinistra della cella e, in base alla regola stabilita, si assegna il nuovo valore del bit per la configurazione dell'automa a $t = 1$.

Si ripete la procedura per i t successivi.

Per fare un esempio di si consideri la seguente configurazione:

- Configurazione iniziale: 11011011
- Regola:
 - 111 \rightarrow 0
 - 110 \rightarrow 1
 - 101 \rightarrow 1
 - 100 \rightarrow 0
 - 011 \rightarrow 1
 - 010 \rightarrow 1
 - 001 \rightarrow 1
 - 000 \rightarrow 0

La computazione dei primi 4 passi è rappresentata nella tabella seguente.

$t = 0$	(1)	1	1	0	1	1	0	1	1	(1)
$t = 1$	(0)	0	1	1	1	1	1	1	0	(0)
$t = 2$	(0)	1	1	0	0	0	0	1	0	(1)
$t = 3$	(1)	1	1	0	0	0	1	1	1	(1)

I bit fra parentesi sono usati per il *padding*, cioè per poter racchiudere tra due celle anche le celle dei bordi. In questo esempio il padding è ottenuto per *circolarità*: in pratica è come se la stringa di bit si chiudesse su sé stessa. Cambiando le regole è possibile definire diversi tipi di automi che possono anche essere definiti su una griglia a due dimensioni. Quello qui mostrato è noto con il nome di **Rule 110**: un automa Turing completo che in

linea di principio può essere usato per eseguire un qualsiasi programma che può essere eseguito su un calcolatore ordinario.

Tornando al punto, Feynman illustra come sfruttando la *località* del computer sia possibile **simulare** la fisica classica ma, al contrario, **non** sia possibile simulare la fisica regolata dalla meccanica quantistica.

Sia chiaro che in un computer classico può essere eseguita l'evoluzione di un sistema quantistico: se si conosce la dinamica di un sistema quantistico, cioè le equazioni che descrivono la sua evoluzione nel tempo (l'analogo delle leggi orarie delle coordinate nella fisica classica), è assolutamente possibile **emularlo**, ma non simularlo, perché la meccanica quantistica non è locale. Questo argomento è molto complesso e può dar luogo a fraintendimenti, infatti la non-località della meccanica quantistica non significa che per essa sia ammessa un'azione a distanza, ma che sia possibile riscontrare una correlazione tra misure sperimentali che non è spiegabile da nessuna teoria locale. La non località della meccanica quantistica è legata al concetto di entanglement che viene discusso nei prossimi capitoli.

È importante avere presente questo argomento perché è stato uno delle motivazioni principali che ha spinto Feynman e altri insieme e dopo di lui ad indagare la possibilità di realizzare una macchina quantistica che permettesse di simulare la fisica quantistica come i computer ordinari permettono di simulare la fisica classica.

Domanda n. 3 In base al principio di *località* della fisica classica, come si spiegano i fenomeni elettrostatici?:

- a. Si spiegano con la presenza di fotoni virtuali, quindi con la meccanica quantistica
- b. Inserendo il campo elettrico come una entità fisica
- c. Sono una eccezione alla teoria

2. Dai bits *classici* ai qubits quantistici

In questo capitolo vengono esposti i principi della meccanica quantistica che devono essere appresi e *digeriti* per continuare con successo la lettura del testo.

Invece di formulare i principi e i postulati con l'ambizione di descrivere l'intero mondo fisico, verranno formulati con l'obiettivo di descrivere ciò che serve a comprendere la computazione quantistica.

In questo capitolo introdurremo questi concetti in modo informale, cercando di abituarci alle nuove idee che devono essere apprese. Nel capitolo successivo daremo una visione più formale e compatta degli stessi concetti.

2.1 I bits nell'informatica classica

Un bit è l'unità di informazione usata in informatica classica. Un bit può assumere solo due valori: l'1 e lo 0. Usando più bit si possono rappresentare delle informazioni complesse, per esempio il numero decimale 11 può essere rappresentato in forma binaria come la sequenza di bit 1011 che sviluppata sulle potenze del due risulta esattamente il numero decimale 11 (i.e. $1 \times 2^0 + 1 \times 2^1 + 0 \times 2^2 + 1 \times 2^3 = 1 + 2 + 8$).

Un bit può essere *realizzato* con diverse tecnologie. In generale si tratta di creare un **sistema fisico** che ammetta due possibili **stati** di equilibrio. Chiameremo questo sistema: **sistema fisico classico** dove l'aggettivo classico si riferisce alla possibilità di descrivere la fisica del sistema usando le leggi della meccanica classica (Newton, per intenderci).

Per esempio si può pensare ad un bit realizzato da una matita in cui il valore 0 è associato allo **stato** in cui la matita è in posizione verticale, e il valore 1 allo **stato** in cui la matita è in orizzontale.

Lo stato *verticale* della matita può essere espresso

matematicamente indicando con θ l'angolo tra la matita e il piano (per esempio il piano del tavolo). Se θ è uguale a $\frac{\pi}{2}$ allora il bit è 0, se θ è zero allora il bit è 1.

In pratica possiamo associare il valore *binario* del bit allo stato θ del sistema fisico che, nel caso in questione, è una semplice matita.

Ci sono diversi altri modi per realizzare un bit, per esempio usando un interruttore collegato ad una luce led, e associando alla luce accesa il valore 1 e alla luce spenta lo 0.

Ovviamente per condensare molti giga bits in uno spazio limitato non si possono usare matite o led, ma si usano altre tecnologie come quelle presenti nei moderni calcolatori.

2.2 Proprietà dei bits

In questo paragrafo ci soffermiamo su alcune osservazioni che possono sembrare ovvie, ma che acquisiranno interesse nel momento in cui le confronteremo con osservazioni analoghe compiute sui **qubit** cioè i bit quantistici.

Per semplicità continuiamo a considerare i bit identificati dallo stato θ della matita, ma la considerazione che trarremo valgono in generale per qualsiasi tecnologia *classica* che si possa usare per realizzarli.

Relazione tra lo stato di un bit e il suo valore

Lo stato di un *bit-matita* è sempre perfettamente determinato.

La matita può stare solo nello stato $\theta = \frac{\pi}{2}$ o nello stato $\theta = 0$ e, a causa della forza di gravità, non è possibile che si trovi in equilibrio uno stato intermedio.

Per conoscere il valore del bit è sufficiente conoscere il suo angolo rispetto al piano.

Se un osservatore, sulla Terra, si trovasse ruotato rispetto al piano di un angolo α vedrebbe il *bit-matita* formare un angolo

diverso dai due angoli possibili appena definiti: dal punto di vista dell'osservatore, infatti, la matita si troverebbe ad uno dei due angoli $\frac{\pi}{2} + \alpha$ o $0 + \alpha$.

Questa rotazione non impedirebbe di ricondurre la posizione del *bit-matita* al corretto valore del bit, infatti, l'osservatore saprebbe di essere ruotato perché potrebbe verificarlo con un esperimento legato alla forza gravitazionale: per esempio osservando la direzione in cui gli oggetti cadono a terra. In tal modo potrebbe sempre ricondurre la propria misurazione dell'angolo formato dalla matita nel suo sistema di riferimento, con l'angolo θ usato per definire lo stato della matita.

Quindi, per i bit *classici*, possiamo affermare che:

Lo stato di un bit è associato sempre ad uno ed un solo valore: 0 oppure 1.

Modifica dello stato di un bit

Lo stato di un *bit-matita* può essere modificato solo in seguito ad una azione volontaria che lo porti dallo stato $\theta = 0$ a $\theta = \frac{\pi}{2}$ oppure da $\theta = \frac{\pi}{2}$ a $\theta = 0$.

Domanda n. 4 In linea di principio, per un computer *classico*, il risultato della lettura di un bit dalla memoria è prevedibile?:

- a. Sì, fatta eccezione per possibili problemi hardware del dispositivo
- b. No, è un fenomeno probabilistico
- c. Sì, ma solo se si è eseguita una copia di back-up

Copia dello stato di un bit

Lo stato di un bit è sempre noto ed è possibile eseguirne una

copia senza modificare l'originale.

Questa caratteristica permette molte operazioni utili come la copia di un documento da condividere o da inviare per email, e altrettante delicate o rischiose dal punto di vista della sicurezza informatica come per esempio un intruso che può leggere un messaggio scambiato tra due soggetti comunicanti senza che loro se ne accorgano intercettando la comunicazione e copiandone il contenuto bit a bit, senza compromettere il messaggio trasmesso.

Stato di più bits

Il bit è l'unità minima di informazione dell'informatica (discreta). Per rappresentare delle grandezze complesse, come ad esempio per codificare un alfabeto o le cifre decimali, un singolo bit non è sufficiente e quindi se ne devono usare un certo insieme in cui ogni bit a seconda della sua posizione abbia un significato preciso, come visto nell'esempio della trasformazione della sequenza binaria 1101 nel numero decimale 11.

Consideriamo per esempio un insieme di otto *bit-matite* (byte) disposti alcuni nello stato $\theta = 0$ e altri nello stato $\theta = \frac{\pi}{2}$.

Per riferirci in modo chiaro allo stato di ognuna delle matite useremo l'indice i . Ad esempio scrivendo θ_0 indicheremo lo stato della prima matita, mentre scrivendo θ_7 quello dell'ottava.

Usando queste otto matite creiamo un nuovo sistema fisico che ammette 2^8 configurazioni diverse e che corrispondono ad una precisa sequenza dei valori θ_i .

Per esempio lo stato $(\pi/2 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ \pi/2)$ corrisponde ai bits $(0 \ 1 \ 1 \ 1 \ 1 \ 1 \ 1 \ 0)$.

La corrispondenza individuata è di natura biunivoca e quindi alle 256 diverse configurazioni corrispondono esattamente 256 diverse informazioni codificate dagli otto bits, non di più e non di meno.

Abbiamo portato volutamente l'attenzione sulla relazione tra l'unità di informazione (1 e 0) e il concetto di sistema fisico classico, perché nel prossimo paragrafo riprendiamo questa relazione, applicandola però al concetto di sistema fisico **quantistico**.

2.3 I qubits

Ci chiediamo ora se esiste una differenza tra sistemi fisici classici e sistemi quantistici.

A rigor di logica dovremmo dire che la teoria quantistica è considerata la meccanica che regola ogni sistema fisico esistente, quindi esistono solo sistemi quantistici.

In realtà è prassi indicare come quantistici solo quei sistemi che non possono essere spiegati con sufficiente accuratezza dalla meccanica classica.

Per esempio, per descrivere il classico moto di una palla di cannone, lanciata ad un angolo θ di inclinazione, non abbiamo bisogno della meccanica quantistica, e chiamiamo un sistema siffatto *classico*.

Chiamiamo quindi sistemi quantistici quei sistemi fisici che richiedono la meccanica quantistica per essere descritti correttamente.

Sistemi come gli atomi e le particelle elementari hanno sempre natura quantistica, ma anche certi sistemi *macroscopici*, normalmente non presenti in natura sulla Terra, ma ottenuti per via artificiale, possono essere sistemi quantistici se il loro comportamento non è descrivibile dalla fisica classica e richiede l'uso della meccanica quantistica.

Realizzare un esperimento per misurare un sistema quantistico non è semplice come realizzarlo per un sistema classico.

Gli esperimenti per acquisire delle misure classiche, come ad esempio la posizione di un oggetto o il tempo di percorrenza di

un carrello lungo un binario, sono facilmente realizzabili, e per questo fanno parte del bagaglio di studio ed esperienza che si acquisisce già frequentando la scuola.

Per questo il concetto di **stato** introdotto con l'esempio della matita è diretto ed intuitivo, in quanto rientra nelle esperienze di tutti.

Il bit è una associazione tra uno stato fisico classico e uno dei due valori numerici 0 e 1.

Analogamente, il qubit è un'associazione tra uno stato fisico quantistico e uno dei due valori numerici 0 e 1. La differenza esistente tra stato fisico classico e quello quantistico è ciò che determina la differenza tra l'informatica classica e quella quantistica.

Il concetto di **stato** che definiremo per i sistemi fisici quantistici non è invece altrettanto intuitivo di quello classico perché, nella vita comune, mancano le occasioni per familiarizzare con esperimenti di misura quantistica.

Per definire i qubits, nel seguito di questo capitolo, introdurremo le particelle chiamate **fotoni** perché useremo la misura del loro stato fisico associandogli il valore binario 0 o 1.

Domanda n. 5 Cosa si intende con sistema quantistico?:

- a. Un sistema di dimensioni atomiche, cioè paragonabili a quelle degli atomi
- b. Qualsiasi sistema, anche macroscopico, che *richieda* di essere descritto con le leggi della meccanica quantistica, come ad esempio certi sistemi macroscopici a temperature prossime agli 0 gradi Kelvin
- c. Un sistema che non può essere misurato con strumenti classici

I fotoni: le particelle del campo elettromagnetico

I fotoni vengono introdotti in fisica teorica in seguito ad un procedimento matematico noto come *seconda quantizzazione*.

La prima quantizzazione è un procedimento con cui si ottiene la descrizione quantistica a partire dalla descrizione classica di un sistema fisico. La prima quantizzazione è applicata per descrivere le particelle come ad esempio l'elettrone, il positrone, ecc.

La seconda quantizzazione si applica invece alle entità fisiche note come *campi*: ad esempio il campo elettromagnetico. Dal procedimento matematico di quantizzazione, descritto per esempio da Dirac (Dirac, 1957), si individuano delle soluzioni matematiche che hanno una interpretazione fisica molto interessante.

Ogni *onda piana* del campo elettromagnetico, può essere vista come un insieme di particelle prive di massa ma con energia, quantità di moto e polarizzazione definite. Queste particelle sono dette **fotoni**. La fisica sperimentale aveva evidenziato già dall'inizio del XX secolo la natura *quantizzata* dello scambio di energia tra atomi e campo elettromagnetico: Einstein ricevette il premio Nobel proprio per aver descritto in modo efficace il meccanismo con cui il campo elettromagnetico estrae gli elettroni dagli atomi cedendo energia in quantità discreta e non continua come invece ci si sarebbe aspettato dalla natura continua del campo elettromagnetico. Questa quantità discreta di energia è associabile all'energia rilasciata da un fotone assorbito dall'atomo: il noto *effetto fotoelettrico*.

Per questo motivo i fotoni, che sono stati ottenuti come procedura matematica dal campo elettromagnetico, hanno guadagnato rapidamente *credibilità* come particelle, e oggi si tende a considerarli *reali* tanto quanto gli elettroni, i protoni, ecc.

Come è fatto un fotone se non ha massa?

Non c'è una risposta scientifica a questa domanda perché la meccanica quantistica rinuncia alla descrizione *pittorica* di particelle e campi e si limita a descrivere ciò che succede nel corso di un esperimento senza aggiungere elementi non misurabili dalla teoria, e quindi, in meccanica quantistica, un fotone è *in sé la descrizione* di come il campo elettromagnetico si propaga ed interagisce con gli altri elementi fisici come elettroni, positroni, ecc., a prescindere da cosa esso possa essere veramente.

Viene la tentazione di immaginare i fotoni come piccole particelle che trasportano l'energia elettromagnetica viaggiando alla velocità della luce.

È importante precisare che ai fini della comprensione della informatica quantistica, figurarsi il fotone non è necessariao, anzi potrebbe risultare controproducente.

Purtroppo la meccanica quantistica non è una teoria intuitiva e i tentativi di renderla tale possono creare confusione.

Stato di un fotone

Il qubit è associato allo stato di un sistema quantistico. Ci sono diversi possibili sistemi fisici che possono essere usati per realizzare i qubits ma, il fotone è sicuramente il più semplice da capire e, probabilmente, quello candidato ad essere più usato per le realizzazione tecnologiche integrate in sistemi di dimensioni ridotte. La caratteristica del fotone è che può essere usato sia come qubit per la computazione, sia come qubit per la trasmissione di dati. Cosa più complessa quando i qubit sono realizzati come stati di sistemi aventi massa che non possono essere trasmessi da un punto all'altro senza movimento di materia.

Un fotone trasporta energia, non ha massa e *viaggia* alla

velocità della luce nel vuoto. Oltre a queste proprietà ne ha un'altra, ereditata dal campo elettromagnetico, molto importante perché è quella che useremo per stabilire il suo **stato**, la direzione di oscillazione del campo elettrico, cioè la **polarizzazione**.

Per capire cosa sia la polarizzazione del fotone è istruttivo partire dalle onde elettromagnetiche descritte nella teoria classica. Cosa sono le onde elettromagnetiche?

Un esempio di fenomeno fisico descritto da onde elettromagnetiche è la luce visibile. L'occhio animale vede grazie all'interazione di una certa *gamma* di onde elettromagnetiche con i neuroni presenti nella retina dell'occhio. La luce è quindi descritta da onde elettromagnetiche e può essere polarizzata.

Vediamo ora due esempi in cui si presentano degli effetti dovuti alla polarizzazione della luce.

È esperienza comune che osservando il cielo si vedano le stelle brillare, mentre la Luna e i pianeti visibili, appaiano più opachi e non brillanti. Questo fenomeno è dovuto alla riflessione della luce, che riflettendo sulla superficie di questi astri rimane polarizzata.

Un altro fenomeno simile, dovuto alla polarizzazione, si osserva indossando un paio di occhiali con filtro polaroid. Questi occhiali sono in grado di eliminare i riflessi perché permettono solo alla luce polarizzata lungo una certa direzione di attraversarli.

La polarizzazione della luce è la direzione che ha il campo elettrico dell'onda elettromagnetica.

Per un'onda elettromagnetica piana, tale direzione si modifica seguendo una legge precisa del tempo, per esempio ruotando con velocità costante. Nel caso più semplice si mantiene costante, e in questo caso si parla di **polarizzazione lineare**.

La polarizzazione della particella fotone discende direttamente dalla polarizzazione delle onde elettromagnetiche.

La particella fotone eredita, dalle onde elettromagnetiche della fisica classica, la direzione di propagazione e la polarizzazione, mentre la sua energia è legata alla frequenza ω di oscillazione del campo elettrico (uguale a quella del magnetico) dalla relazione $\mathbf{E} = h\omega$, dove h è una costante detta di Planck.

Negli esempi da qui in avanti, fotoni saranno le nostre *matite quantistiche*, che come i *bit-matita* saranno usati per definire il valore dei **qubits**

La polarizzazione di un fotone è descritta usando due soli stati, esattamente come è per la matita. Nel caso classico della matita abbiamo visto che i due stati sono definiti come $\theta = \frac{\pi}{2}$ e $\theta = 0$, per i fotoni useremo una notazione diversa, indicheremo i due stati come $|0\rangle$ e $|1\rangle$

Domanda n. 6 Cosa lega le onde elettromagnetiche piane dell'elettrodinamica classica ai *fotoni* della teoria quantistica?:

- a. I fotoni hanno la stessa polarizzazione e direzione di propagazione delle corrispondenti onde elettromagnetiche
- b. Ogni fotone ha la stessa intensità del campo elettrico e magnetico dell'onda elettromagnetica
- c. Il fotone è un fenomeno ottico, mentre le onde elettromagnetiche hanno natura elettrica e magnetica

Fotoni e qubit

In questo paragrafo vediamo di concretizzare maggiormente il concetto di qubit e di capire come realizzarlo usando un sistema fisico quantistico.

Abbiamo visto che, in un sistema classico, i due possibili stati della matita sono un esempio di bit, similmente:

lo spazio di tutti i possibili stati in cui può trovarsi la polarizzazione di un fotone, è un esempio di qubit.

La relazione tra i due stati, verticale e orizzontale, di una matita e i due valori 0 e 1 del bit è chiara. Presa una matita, il valore del bit associato ad essa è ottenuto misurando l'angolo che la matita forma rispetto ad un certo piano. Una volta stabilita la convenzione che la matita verticale significa 0 e orizzontale significa 1, non è possibile alcun fraintendimento tra diversi possibili soggetti che effettuano misure sulle matite, perché la direzione verticale è definita usando una direzione preferenziale, cioè quella in cui agisce la forza di gravità.

Per i fotoni invece non abbiamo un fenomeno importante come la gravità per definire una direzione preferenziale perché la loro polarizzazione non ne è influenzata.

Tra qubits e bits c'è una importante analogia: entrambi sono associati a sistemi fisici caratterizzati da due soli stati, nel seguito vedremo però che ci sono anche delle differenze molto importanti dovute al diverso significato attribuito alla parola *stato* nella fisica classica e in quella quantistica.

Nella storiella che segue vediamo come utilizzare lo stato quantico della polarizzazione di un fotone per associarvi un qubit cioè l'analogo quantistico del bit che possiamo chiamare scherzosamente *bit-fotone*. Questa serve a dare una visione

d'insieme dei concetti presentati fin'ora ed è necessaria per avvicinarsi con gradualità allo studio della meccanica quantistica che viene approfondito nel capitolo 3.

Il signor Rossi e il signor Ferrari: una classica storia di bits

Il signor Rossi è una persona a modo abituata a non distinguersi troppo dagli altri. Il mattino quando arriva al lavoro, dispone le sue matite per formare un codice binario che verrà letto pochi minuti dopo dal signor Ferrari, suo collega.

Al contrario di Rossi, Ferrari è un tipo eccentrico e ama farsi notare, per questo invece di camminare come fanno tutti gli altri, gira attaccato a due pertiche mantenendo una posizione obliqua rispetto al suolo. Ama vedere il mondo da un altro punto di vista.

Quando il mattino si reca presso la scrivania del signor Rossi per leggere i bit delle sue matite, non si lascia confondere dal proprio punto di vista perché sa che deve giudicare lo stato dei bit a partire dalla direzione in cui penzola la sua cravatta!

Il signor Magri e il signor Fabbri: una storia di qubits

Il signor Magri produce molti dati tutti i giorni, e non avendo modo di registrarli tutti in un archivio, deve inviarli a chi ne ha bisogno: il signor Fabbri, poi eliminarli. Il signor Magri abita lontano dal signor Fabbri. Ogni mattina si assicura di preparare un dispositivo polarizzatore per trasmettere dei fotoni polarizzati al signor Fabbri.

Il signor Magri è una persona scrupolosa e prepara i fotoni in modo che essi vengano prodotti con polarizzazione verticale $|0\rangle$ oppure orizzontale $|1\rangle$.

Con polarizzazione verticale ($|0\rangle$), egli intende un fotone che attraversi (senza essere fermato) un filtro *polaroid* con asse di

polarizzazione disposto verticalmente, cioè nella direzione in cui agisce la gravità, mentre con polarizzazione orizzontale ($|1\rangle$) un fotone che attraversi un polaroid con asse orizzontale. Egli chiama l'insieme formato da $|1\rangle$ e $|0\rangle$ **base standard** per la polarizzazione dei fotoni.

Il primo incidente: dati recuperabili

Il signor Fabbri ogni mattina attende i fotoni del signor Magri, con i quali egli deve comunicargli informazioni importanti. Egli sa che i fotoni possono avere solo due possibili polarizzazioni però ha frainteso l'accordo con il signor Magri, e ha sistemato gli assi di polarizzazione dei suoi polaroid in modo errato, infatti li ha invertiti tra di loro, scambiando in questo modo i fotoni con polarizzazione $|1\rangle$ con quelli a polarizzazione $|0\rangle$ e di conseguenza i qubit a 1 con i qubit a 0.

Un giorno per puro caso, il signor Fabbri e il signor Magri si sentono al telefono e ne approfittano per discutere dei dati che il signor Magri ha appena inviato al signor Fabbri e che non ha ancora cancellato. I due si rendono conto che qualcosa non va, e presto si accorgono che tutti i valori dei qubit sono diversi.

Il signor Fabbri ha l'archivio con tutti i dati trasmessi dall'inizio dal sig Magri e questi lo tranquillizza dicendogli che sarà sufficiente trasformare tutti i qubit che sono a 0 al valore 1 e quelli che sono ad 1 al valore 0.

Il secondo incidente: dati non recuperabili

Dopo altre due settimane di trasmissione dei dati secondo la stessa procedura, il signor Fabbri si accorge che inavvertitamente ha ruotato di 45 gradi entrambi gli assi dei polarizzatori. Nonostante questo disallineamento il suo sistema ha sempre funzionato, continuando a registrare i due possibili valori 0 o 1.

Per sua fortuna, il signor Fabbri, riesce a risalire al momento dell'*incidente* che capisce essere avvenuto durante le pulizie del suo laboratorio.

Forte della esperienza già avuta dal primo incidente, egli ripone fiducia nell'esistenza di una legge fisica o informatica che permetta di risalire ai valori corretti dei qubit partendo dai valori registrati con i polarizzatori ruotati di 45 gradi.

Egli però non conosce questa legge e si rivolge al signor Magri scoprendo suo malgrado che neanche lui la conosce, ma di nuovo ha tenuto copia dei dati trasmessi.

Da un confronto degli ultimi dati trasmessi con quelli ricevuti, si accorge che non c'è correlazione, infatti i fotoni trasmessi come $|1\rangle$ sono stati ricevuti a volte come $|1\rangle$ e altre come $|0\rangle$ in modo apparentemente casuale e con la stessa frequenza di casi. Il signor Magri e il signor Fabbri capiscono che non c'è modo di risalire ai dati corretti partendo dai dati registrati.

È finita bene anche questa volta grazie alla scrupolosità del signor Magri che aveva conservato per qualche giorno in più i dati. Però i due si sono accorti che il loro sistema di trasmissione dei dati nasconde qualcosa di particolare.

Un'osservazione interessante

Il signor Fabbri è molto amareggiato e si auto accusa di negligenza. Il signor Magri invece è rimasto colpito dall'accaduto, e decide di sperimentarlo ulteriormente. Chiede allora al signor Fabbri di ruotare volontariamente i due polaroid, ma di un angolo di soli 30 gradi. Ciò fatto, egli trasmette un serie di fotoni di cui archivia il valore per confrontarli con quelli ricevuti dal signor Fabbri.

Dal confronto segue un risultato inaspettato: questa volta esiste una relazione tra i qubit ricevuti e quelli inviati, però è solo una relazione statistica: i qubit ricevuti sono per il 75% dei casi corretti, e per il restante 25% errati.

I signori Magri, Fabbri, Rossi e Ferrari si incontrano

I quattro signori Magri, Fabbri, Rossi e Ferrari si incontrano e si raccontano le relative esperienze. Essi comprendono che l'utilizzo della posizione delle matite per rappresentare i bit è assai diverso dall'utilizzo della polarizzazione dei fotoni.

Il signor Magri vuole provare a capire cosa sta succedendo con i fotoni e prova ad impostare una serie di ragionamenti partendo da quanto ha osservato fin'ora:

- un fotone verticale ($|0\rangle$) passa per un polaroid polarizzato in modo verticale
- un fotone orizzontale ($|1\rangle$) passa per un polaroid polarizzato in modo orizzontale
- un fotone verticale è fermato da un polaroid orizzontale
- un fotone orizzontale è fermato da un polaroid verticale

Desidera esprimere il fatto che un fotone polarizzato verticalmente ha il 50% di probabilità di passare attraverso un polaroid inclinato di 45 gradi, come ha capito dal secondo incidente occorso.

Sapendo che nell'universo non esiste una direzione preferenziale, pensa che, l'effetto di un fotone, a polarizzazione verticale su un polaroid obliquo, debba essere lo stesso di un fotone a polarizzazione obliqua su un polaroid verticale. In pratica, decide di ruotare la polarizzazione del fotone rispetto l'asse del polaroid anziché fare il contrario: perché la cosa importante è l'angolo fra i due e non l'angolo rispetto la verticale, visto che la polarizzazione non è influenzata dalla gravità (come visto nel paragrafo precedente).

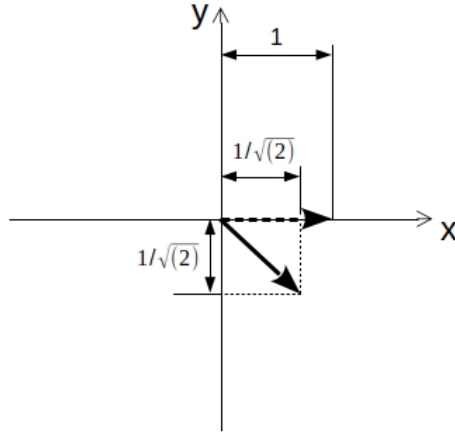


Fig.1 Il vettore ha lunghezza unitaria. Dopo la rotazione di 45 gradi, le sue componenti cartesiane misurano entrambe $\frac{1}{\sqrt{2}}$.

Per scrivere i due stati del fotone rispetto al polaroid ruotato egli si figura di dover ruotare nel piano cartesiano un segmento di lunghezza unitaria con centro nell'origine e associa all'asse x lo stato $|0\rangle$ e all'asse y lo stato $|1\rangle$ e scrive la rotazione di 45 gradi in senso orario dello stato $|0\rangle$ di polarizzazione del fotone come:

$$\left(\frac{1}{\sqrt{2}} \right) (|0\rangle - |1\rangle)$$

e quella della rotazione di 45 gradi in senso orario dello stato $|1\rangle$ del fotone come:

$$\left(\frac{1}{\sqrt{2}} \right) (|0\rangle + |1\rangle)$$

Il signor Magri postula che la probabilità p che un fotone polarizzato a 45 gradi lungo la diagonale secondaria (come in figura) passi attraverso un polaroid ad asse verticale è data da:

$$\mathbf{p} = \left(\frac{1}{\sqrt{2}} \right)^2 = \frac{1}{2}$$

Il signor Magri non sa spiegarsi il perché, però capisce che c'è una relazione tra la radice di 2 trovata nella rotazione della polarizzazione del fotone e la probabilità del 50% (appunto $\frac{1}{2}$) misurata sperimentalmente, ma essendo un informatico non è interessato alla polarizzazione dei fotoni in sé, ciò che sta catturando la sua attenzione è, invece, la relazione che hanno i qubit con lo stato di polarizzazione dei fotoni ed è questo che lui vuole studiare.

Prima di continuare i suoi studi capisce che le espressioni trovate sono importanti e decide di assegnare dei simboli agli stati da esse individuati. Sceglie i due simboli $|0'\rangle$ e $|1'\rangle$ e li definisce come segue:

$$|0'\rangle = \left(\frac{1}{\sqrt{2}} \right) (|0\rangle - |1\rangle)$$

e

$$|1'\rangle = \left(\frac{1}{\sqrt{2}} \right) (|0\rangle + |1\rangle)$$

Si accorge quindi che può riscrivere gli stati $|0\rangle$ e $|1\rangle$ usando gli stati $|0'\rangle$ e $|1'\rangle$. Infatti:

$$|0\rangle = \left(\frac{1}{\sqrt{2}} \right) (|0'\rangle + |1'\rangle)$$

e

$$|1\rangle = \left(\frac{1}{\sqrt{2}} \right) (|0'\rangle - |1'\rangle)$$

Il signor Magri capisce che i qubit possono essere rappresentati anche attraverso questi due stati e che quindi questi due stati sono una base per rappresentare i qubit. Il signor Magri ha quindi intuito un concetto importante:

lo stato di polarizzazione di un fotone è esprimibile rispetto ad una base formata da due stati separati e indipendenti

ed esso può anche non coincidere con nessuno dei due stati di base, come gli è successo quando i fotoni con polarizzazione obliqua incidevano sui polaroid ad assi verticale ed orizzontale.

Il signor Magri ha capito un'altra cosa molto importante:

se la polarizzazione del fotone è parallela uno degli assi dei polaroid, allora il risultato della misura è certo, altrimenti, se la polarizzazione del fotone giace su una retta non parallela a nessuno dei due assi, allora il risultato è solo probabilistico.

Differenze tra bits e qubits

La storia del signor Magri e del signor Fabbri, ci ha aperto gli occhi sulle differenze tra bits e qubits.

Entrambi sfruttano lo stato di un sistema fisico per identificare un coppia di valori (1 e 0) e questa è la loro **analogia**. La **differenza** è che per i primi c'è una corrispondenza *biunivoca* tra lo stato e il valore del bit, mentre per i secondi c'è una corrispondenza biunivoca tra la *misura* dello stato e il valore del qubit.

Nel caso classico, lo stato della matita identifica univocamente il valore del bit (verticale 0, orizzontale 1), nel caso dei quantistici stati diversi possono portare probabilisticamente allo stesso valore del bit, quindi non si può stabilire una corrispondenza biunivoca tranne nei casi in cui lo stato di polarizzazione coincide con uno degli assi dei polaroid.

La misura dello stato di polarizzazione, invece, porta sempre ad un risultato che può essere solo uno tra i due possibili e quindi esiste una relazione biunivoca tra la misura dello stato e il valore del qubit.

Questa differenza è molto importante ed è ciò che caratterizza l'informatica quantistica rispetto a quella classica. Quando si sarà finito di leggere il libro, si torni su questo punto fintanto che non risulti completamente chiaro.

Perché questa differenza?

Nella fisica classica, non c'è differenza tra lo stato di un sistema e la sua misura.

Ripensando all'esempio delle matite si può immaginare di adottare la stessa convenzione a bordo di una **stazione spaziale** orbitante. In quel contesto le matite possono assumere angoli arbitrari rispetto al riferimento della stazione quindi, sebbene una coppia di assi rimanga un valido sistema per definirne lo stato, si potrebbe obiettare che analogamente a quanto accade nella meccanica quantistica, se una matita non è allineata lungo uno dei due assi, il suo stato è in una sovrapposizione di stati.

Questo non è falso, ma c'è una differenza importante e sostanziale con il concetto di stato quantistico. Dal punto di vista classico, anche se sulla stazione spaziale la matita può assumere una qualsiasi angolazione rispetto agli assi, rimane una relazione biunivoca tra stato e misura:

la misura dell'angolo che la matita forma con un dato asse può essere eseguita con precisione arbitraria senza modificare lo stato della matita.

Anche su una stazione spaziale si potrebbero quindi usare i *bit-matita* adottando la semplice convenzione che l'angolo da 0 a 45 gradi rappresenti il bit 1 mentre l'angolo da 45 a 90 rappresenti il bit 0.

Per i sistemi quantistici invece:

la relazione tra lo stato del sistema e il risultato della misura ha natura probabilistica

Come abbiamo visto, quando si misura lo stato di polarizzazione di un fotone si possono ottenere solo due valori distinti. Prima della misura, il fotone può essere in un infinità di stati diversi tra loro. Il processo di misura *obbliga* il fotone ad assumere uno dei due stati che per questo sono detti *stati di base*.

Questo aspetto della meccanica quantistica è difficile da digerire ed in effetti esistono anche interpretazioni diverse da questa, detta *interpretazione di Copenaghen*, che offrono una visione alternativa. Quella di Copenaghen è comunque l'interpretazione più diffusa e per questo è detta essere *ortodossa*.

Stato fisico del fotone e valore del qubit

Alcuni testi potrebbero tendere ad unificare il concetto di qubit con quello di stato fisico quantistico della polarizzazione del fotone. Indipendentemente dal modo in cui lo si vuole trattare formalmente, è sempre importante tenere a mente la distinzione esistente tra lo stato fisico prima e dopo l'esecuzione di una misura.

Ora che abbiamo introdotto il concetto di stato quantistico dobbiamo chiarire bene qual'è la relazione **tra stato fisico e**

valore del qubit.

Dato un fotone, si è visto che, ad esso è associato un qubit legato al suo stato di polarizzazione che possiamo indicare con la lettera ψ o con il simbolo $|\psi\rangle$ come ha fatto il signor Magri.

Dal concetto di bit, ci aspettiamo che al qubit sia associato un valore binario, o lo zero oppure l'uno.

Il valore binario associato al qubit non è il suo stato $|\psi\rangle$ in sé, quindi ci chiediamo in che forma sia ad esso legato.

Per determinare il valore di un qubit è necessario sempre compiere una **misura**, nel caso in questione una misura della sua polarizzazione.

La misura *obbliga* lo stato (o funzione d'onda) ψ a *collassare* in uno dei due stati che rappresentano la base scelta per eseguire la misura stessa.

Supponendo di aver eseguito la misura rispetto ai due assi dei polaroid, dopo la misura, lo stato $|\psi'\rangle$ del fotone potrà essere:

- $|\psi'\rangle = |0\rangle$ oppure
- $|\psi'\rangle = |1\rangle$

e questo **determina** il valore del qubit ad essere rispettivamente 0 oppure 1.

Domanda n. 7 La principale differenza tra i *bit-matita* e i *bit-fotoni* è che:

- a. Per i primi c'è una relazione deterministica tra il loro stato e la misura del loro valore, mentre per i secondi no
- b. I *bit-matita*, sebbene non efficienti, sono implementabili realmente, i secondi sono solo un ipotesi teorica
- c. Non mostrano differenze e per questo è possibile realizzare concretamente dispositivi che sfruttano la meccanica quantistica per la computazione

3. Principi della meccanica quantistica

In questo capitolo si pongono le basi canoniche per comprendere i principi della meccanica quantistica. I concetti presentati in modo informale e discorsivo nel capitolo precedente, sono qui ripresi dall'inizio e sviluppati fin dove necessario agli obiettivi del testo.

Per comprendere ed *accettare* la formulazione della meccanica quantistica, così come si presenta oggi, è importante partire dalla visione di chi l'ha concretamente formulata, cioè P.A.M Dirac (Dirac, 1957).

Agli orecchi di chi non è un fisico di professione, questo potrebbe sembrare strano: *in fondo si tratta di formule che o sono giuste o sono sbagliate!*

Non è così perché la fisica è la risposta alle domande che ci si pone e la sua forma dipende dalle domande stesse e dal modo in cui queste sono state poste.

Per questo studiare le risposte della fisica, senza conoscere il pensiero di chi l'ha formulata, può essere molto complesso, specialmente se la formulazione non è intuitiva, come appunto il caso della meccanica quantistica.

Dirac scrive che l'obiettivo principale della fisica non è quello di fornire una raffigurazione della natura, ma di fornire le leggi che governano i fenomeni conosciuti e che possono guidare alla scoperta di fenomeni nuovi.

Si noti che Dirac scrive esattamente:

...the main object of physical science is not the provision of picture,...

evidenziando la **non necessità** di raffigurarsi il mondo quantistico.

Dirac aveva un buon motivo per sostenere questo pensiero visto che si era assunto la responsabilità di stravolgere la visione che

la fisica aveva avuto fino ai primi anni '20.

Il XX secolo era cominciato con diverse *novità* interessanti per la fisica e la formulazione delle leggi dell'elettromagnetismo aveva aperto le porte a nuove frontiere dello studio e della ricerca. All'inizio del secolo Rutherford ipotizza il modello planetario per gli atomi, de Broglie ipotizza la dualità onda corpuscolo, Planck ipotizza il quanto di azione che diverrà la base per la meccanica quantistica ed Einstein spiega l'effetto fotoelettrico basandosi sull'idea di fotone.

I fisici e le scoperte sarebbero molti di più, ma ci accontentiamo di questi appena citati perché ci servono solo per giungere ad altri due: Schrodinger e Heisenberg che furono tra i primi a comprendere che le scoperte e le teorie che avevano salutato il nuovo secolo non potevano trovare una collocazione nel *vecchio* paradigma classico newtoniano e che un nuovo paradigma doveva essere formulato.

Lo fecero entrambi, ognuno a modo suo. Il primo formulò la **meccanica ondulatoria** e il secondo la **meccanica matriciale**.

La prima era più semplice, perché parlava una lingua più conosciuta ai fisici ed ebbe maggior successo iniziale, ma la seconda si rivelò più semplice nel proseguo perché era complessa per trattare i problemi semplici, ma semplice per i problemi difficili. Fu raccolta da Dirac e divenne la **meccanica quantistica**.

Questa breve introduzione ha avuto lo scopo di preparare il lettore digiuno di meccanica quantistica a quanto seguirà, perché la meccanica quantistica può essere apprezzata più facilmente se si comprende a fondo che nasce dal pensiero di altri esseri umani, non è vera o falsa, è una teoria, un modo di pensare e di sperimentare, che si sta rivelando molto utile, tanto quanto lo è stata la meccanica newtoniana prima di lei.

Domanda n. 8 Chi è considerato il *padre* della meccanica ondulatoria?

- a. Dirac
- b. Schrodinger
- c. Heisenberg

3.1 Formulazione matematica del principio di sovrapposizione

Dobbiamo ora addentrarci nei dettagli della teoria quantistica. Nella trattazione che segue si è cercato di estrapolare solo il necessario della teoria ai fini dell'introduzione all'informatica quantistica, attenendosi però rigorosamente al testo di Dirac da cui nasce la principale linea di interpretazione della meccanica quantistica, quella detta della *Scuola di Copenhagen*.

Il lettore sia rassicurato: non è necessario comprendere tutto e perfettamente, ma piuttosto sia determinato a leggere questi capitoli per intero, in modo da non trovarsi sprovveduto nei capitoli dedicati all'informatica dove i concetti e le idee qui esposte troveranno applicazione.

Non si saltino poi le domande e ci si fermi a ragionarci sopra, consultando nel caso le risposte in fondo al testo.

Stato fisico

Consideriamo un sistema atomico composto di corpi (puntiformi) ognuno con una specifica massa, carica elettrica, ecc. I corpi interagiscono tra loro attraendosi o respingendosi secondo certe leggi della fisica.

Ci saranno vari possibili moti per ognuno di questi corpi che saranno in accordo con le leggi della fisica. Seguendo Dirac, chiameremo ognuno di questi possibili moti *stato* del sistema.