

# Introduzione al quantum computing

Il quantum computing è stato un campo di ricerca sempre più vigoroso e fonte di clamore negli ultimi anni. Utilizzando la fisica quantistica per eseguire calcoli in nuovi e straordinari modi, i computer quantistici possono avere un impatto sulla società, e pertanto questo è un momento entusiasmante per scoprire e imparare a programmare i computer quantistici e applicare risorse quantistiche alla soluzione di problemi importanti.

Con tutto il rumore sui vantaggi offerti dal quantum computing, tuttavia, è facile perdere di vista la reale portata di tali vantaggi. Abbiamo alcuni interessanti precedenti storici di ciò che può accadere quando le promesse di una tecnologia superano la realtà. Negli anni Settanta, il machine learning e l'intelligenza artificiale hanno sofferto di finanziamenti drasticamente ridotti, poiché l'attenzione dei media e l'entusiasmo per l'intelligenza artificiale aveva superato i risultati; questo periodo sarebbe stato poi chiamato "l'inverno dell'AI". Allo stesso modo, le società basate su Internet hanno affrontato lo stesso pericolo quando hanno cercato di superare il fallimento delle dot-com.

Un modo di procedere consiste nel comprendere in modo critico le promesse del quantum computing, come funzionano i computer quantistici e anche, semplicemente, che cos'è e non è il quantum computing. In questo capitolo, vi aiutiamo a sviluppare tali conoscenze, in modo che possiate mettervi a scrivere i vostri programmi quantistici, con l'aiuto del libro.

Ma, a parte tutto questo, la verità è che è davvero fantastico conoscere un modello di elaborazione

## In questo capitolo

- **Perché il quantum computing è importante?**
- **Che cos'è un computer quantistico?**
- **Come utilizzeremo i computer quantistici**
- **Che cos'è un programma?**
- **Riepilogo**

interamente nuovo! Mentre leggerete questo libro, scoprirete come funzionano i computer quantistici, programmando simulazioni che potrete eseguire anche su un computer portatile. Queste simulazioni vi mostreranno molti elementi essenziali del modo in cui ci aspettiamo che sia la vera programmazione quantistica, quando sarà disponibile il relativo hardware commerciale. Questo libro è rivolto a chi abbia qualche esperienza di programmazione di base e algebra lineare, ma nessuna conoscenza preliminare di fisica quantistica o computer science. Se avete già una certa familiarità con i concetti quantistici, potete saltare alle Parti 2 e 3, dove entreremo più in dettaglio nelle attività di programmazione e negli algoritmi quantistici.

## Perché il quantum computing è importante?

La tecnologia informatica sta avanzando a un ritmo davvero sbalorditivo. Solo tre decenni fa, il processore 80486 consentiva agli utenti di eseguire 50 MIPS (milioni di istruzioni al secondo). Oggi, anche piccoli computer come il Raspberry Pi possono raggiungere i 5.000 MIPS, mentre i sistemi desktop possono facilmente raggiungere i 50.000–300.000 MIPS. Quando abbiamo un problema di eccezionale difficoltà computazionale, una strategia molto ragionevole per risolverlo potrebbe essere, semplicemente, aspettare la prossima generazione di processori, per semplificarsi la vita, scaricare video in streaming più velocemente e avere giochi più vivaci.

Per molti problemi a cui teniamo, tuttavia, non siamo così fortunati. Potremmo sperare che avendo una CPU due volte più veloce potremo risolvere problemi due volte più complessi, ma come accade sempre nella vita, “di più è anche diverso”. Supponiamo di dover ordinare un elenco di 10 milioni di numeri e di scoprire che l’operazione richiede circa 1 secondo. Successivamente, se vorremo ordinare un elenco di 1 miliardo di numeri in 1 secondo, avremo bisogno di una CPU 130 volte più veloce, non solo 100 volte. In alcuni tipi di problemi, la situazione è anche peggiore: per alcuni problemi grafici, passare da 10 milioni a 1 miliardo di punti richiederebbe 13.000 volte più tempo.

Problemi del tutto differenti, come il controllo del traffico in una città e la previsione delle reazioni chimiche, diventano sempre più complessi, *molto* rapidamente, aumentando la scala. Se il quantum computing consistesse nel creare un computer 1.000 volte più veloce, potremmo a malapena intaccare le grandi sfide che intendiamo risolvere. Fortunatamente, i computer quantistici sono *molto* più interessanti. Ci aspettiamo che i computer quantistici saranno molto più *lenti* dei computer classici, ma che le risorse necessarie per risolvere molti problemi *varieranno di scala* in modo diverso, in modo tale che, guardando ai giusti tipi di problemi, possiamo andare oltre al “di più è diverso”. Allo stesso tempo, i computer quantistici non sono una bacchetta magica: alcuni problemi rimarranno difficili. Per esempio, sebbene sia probabile che i computer quantistici possano aiutarci immensamente nella previsione delle reazioni chimiche, potrebbero non essere di grande aiuto con altri problemi difficili.

Scoprire esattamente in quali problemi possiamo ottenere un reale vantaggio e sviluppare algoritmi quantistici per risolverli è stato un grande obiettivo della ricerca sul quantum computing. Finora, è stato molto difficile valutare gli approcci quantistici in questo modo, poiché ciò richiede una grande abilità matematica, necessaria per scrivere gli algoritmi quantistici e per comprendere tutte le sottigliezze della meccanica quantistica.

Tuttavia, dal momento in cui l'industria ha iniziato a sviluppare piattaforme in grado di aiutare a connettere gli sviluppatori al quantum computing, questa situazione ha iniziato a cambiare. Utilizzando il Quantum Development Kit Microsoft, possiamo astrarre la maggior parte delle complessità matematiche del quantum computing e iniziare a *comprendere* e *utilizzare* effettivamente i computer quantistici. Gli strumenti e le tecniche insegnati in questo libro consentono agli sviluppatori di esplorare e comprendere come sarà lo “scrivere programmi” per questa nuova piattaforma hardware.

In altre parole, il quantum computing non scomparirà, quindi è davvero molto importante capire a quali problemi possiamo applicarlo! Indipendentemente dal fatto che si verifichi una “rivoluzione” quantistica, il quantum computing ha preso pesantemente in considerazione – e continuerà a farlo – le decisioni su come sviluppare le risorse di calcolo nei prossimi decenni. Decisioni come le seguenti sono fortemente influenzate dal quantum computing:

- Che cosa si intende per “ipotesi ragionevoli” nella sicurezza delle informazioni?
- Quali competenze sono utili nei corsi di laurea?
- Come possiamo valutare il mercato delle soluzioni informatiche?

Coloro, fra noi, che lavorano in settori tecnologici o a essi correlati, si trovano sempre più spesso a prendere decisioni di questo tipo o a fornire input per tali decisioni. Abbiamo la responsabilità di capire che cos'è il quantum computing e, cosa forse più importante, che cosa non è. In questo modo saremo preparati al meglio per intensificare gli sforzi e contribuire a queste nuove decisioni.

A parte questo, un altro motivo per cui il quantum computing è un argomento così affascinante è che è allo stesso tempo così simile e così diverso dalla computer science classica. Comprendere sia le somiglianze sia le differenze tra la computer science classica e quella quantistica ci aiuta a capire che cosa è fondamentale in tutta la computer science, in generale. Il calcolo, sia classico sia quantistico, deriva da diverse descrizioni delle leggi fisiche, così che la comprensione del calcolo potrà aiutarci a comprendere l'universo in un modo nuovo.

Ciò che è assolutamente fondamentale, tuttavia, è che non esiste una ragione giusta o addirittura migliore per essere interessati al quantum computing. Qualunque cosa vi abbia avvicinato alla ricerca o alle applicazioni del quantum computing, imparerete qualcosa di interessante, lungo il percorso.

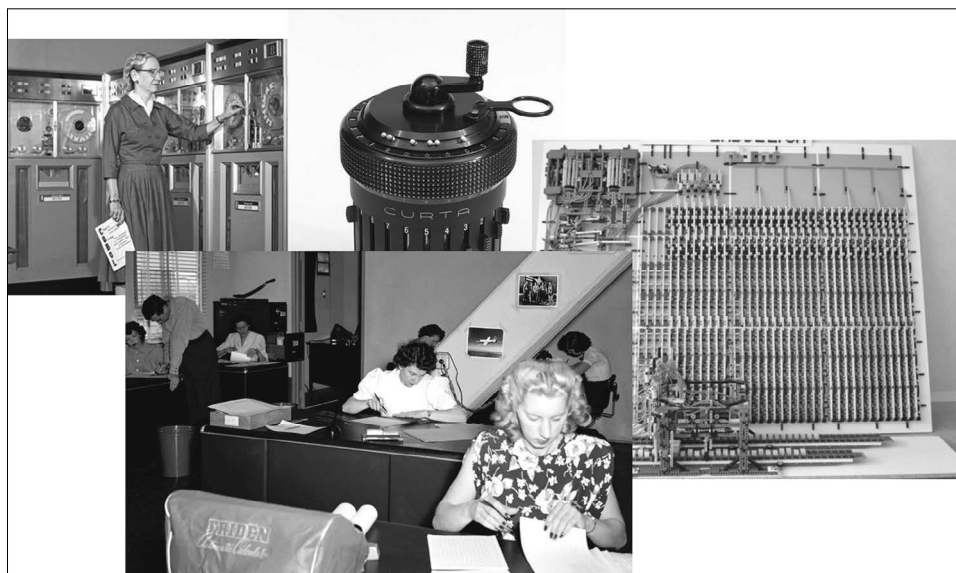
## Che cos'è un computer quantistico?

Cerchiamo di scoprire che cosa rende “quantistico” un computer. Per introdurre questa discussione, parliamo brevemente del significato del termine *computer*.

### DEFINIZIONE

Un *computer* è un dispositivo che prende dei dati in input ed esegue qualche tipo di operazione su quei dati.

Ci sono molti esempi di quello che abbiamo appena chiamato *computer*, come potete vedere nella Figura 1.1.



**Figura 1.1** Diversi esempi di diversi tipi di computer, incluso il mainframe UNIVAC del contrammiraglio Hopper, una stanza di “computer umani” che lavorano per risolvere i dati di volo, un calcolatore meccanico e una macchina di Turing basata su LEGO. Ogni computer può essere descritto dallo stesso modello matematico: telefoni cellulari, laptop e server. Fonti: foto di “computer umani” della NASA. Foto della macchina di Turing LEGO di Proiet Rubens, utilizzata sotto CC BY 3.0 (<https://creativecommons.org/licenses/by/3.0>).

Tutti questi elementi hanno in comune il fatto che possiamo modellarli con la fisica classica, cioè in termini di leggi del moto di Newton, gravità newtoniana ed elettromagnetismo.

Questo ci aiuterà a distinguere i tipi di computer cui siamo abituati (per esempio laptop, telefoni, tostapane, case, automobili e pacemaker) dai computer che stiamo trattando in questo libro. Per distinguerli, chiameremo i computer che possono essere descritti impiegando la fisica classica con il nome *computer classici*. Un aspetto interessante di questa scelta è che se sostituiamo il termine *fisica classica* con *fisica quantistica*, abbiamo un’ottima definizione di che cosa sia un computer quantistico.

#### DEFINIZIONE

Un *computer quantistico* è un dispositivo che prende dei dati in input ed esegue qualche tipo di operazione su quei dati con un processo che può essere descritto solo impiegando la fisica quantistica.

In altre parole, la distinzione tra computer classici e computer quantistici è esattamente quella tra fisica classica e fisica quantistica. Ne parleremo più avanti nel libro, ma la differenza principale è di scala: la nostra esperienza quotidiana riguarda in gran parte oggetti aventi dimensioni e temperature tali per cui gli effetti quantistici, pur esistenti, in generale non agiscono molto. Anche se la meccanica quantistica funziona anche alla scala degli oggetti di uso quotidiano, come le tazzine del caffè, i sacchi di farina e le mazze da baseball, possiamo fare un ottimo lavoro nel descrivere le interazioni fra questi oggetti impiegando solo la fisica classica.

### Approfondimento: che cosa è successo alla relatività?

La fisica quantistica si applica a oggetti molto piccoli e molto freddi o ben isolati. Allo stesso modo, un altro ramo della fisica, la *relatività*, descrive oggetti che sono abbastanza grandi da consentire alla gravità di svolgere un ruolo importante o che si muovono molto velocemente, quasi alla velocità della luce. Molti computer si basano su effetti relativistici; infatti, i satelliti di posizionamento globale dipendono in modo critico dalla relatività. Finora abbiamo confrontato principalmente la fisica classica e quella quantistica, quindi... perché parlare di relatività?

Come vedremo, tutto il calcolo implementato utilizzando effetti relativistici può essere descritto utilizzando modelli di calcolo puramente classici, come le macchine di Turing. Al contrario, il quantum computing non può essere descritto come un calcolo classico più veloce, ma richiede un diverso modello matematico. Non è ancora stato proposto per un "computer gravitazionale" che usi la relatività allo stesso modo, quindi possiamo tranquillamente mettere da parte la relatività, in questo libro.

Se ci concentriamo su una scala molto più piccola, in cui è necessaria la meccanica quantistica per descrivere i nostri sistemi, il quantum computing è l'arte di utilizzare dispositivi piccoli e ben isolati per trasformare i dati in modi che non possono essere descritti in termini di pura fisica classica. Un modo per costruire dispositivi quantistici consiste nell'usare piccoli computer classici come i processori di segnali digitali (DSP) per controllare le proprietà di materiali esotici.

### Fisica e quantum computing

I materiali esotici utilizzati per costruire computer quantistici hanno nomi che possono anche spaventare, come *superconduttori* e *isolanti topologici*. Possiamo però alleggerire questa preoccupazione pensando a come impariamo a comprendere e utilizzare i computer classici.

Possiamo programmare i computer classici senza sapere che cosa sia un semiconduttore. Allo stesso modo, la fisica in base alla quale costruiamo i computer quantistici è un argomento affascinante, ma è non è necessario conoscerla per imparare a programmare e impiegare i dispositivi quantistici.

I dispositivi quantistici possono differire da quelli classici per i dettagli del modo in cui vengono controllati, ma alla fine tutti i dispositivi quantistici sono controllati e gestiti da computer classici e da un'elettronica di controllo. Dopotutto, siamo interessati a dati classici, quindi, alla fine, deve esistere un'interfaccia fra mondo classico e mondo quantistico.

#### NOTA

Molti dispositivi quantistici devono essere mantenuti molto freddi e ben isolati, poiché possono essere estremamente sensibili al rumore.

Se applichiamo operazioni quantistiche su un hardware classico embedded, possiamo manipolare e trasformare dati quantistici. La potenza del quantum computing deriva

quindi da una scelta attenta di quali operazioni applicare, al fine di attuare una trasformazione utile che risolva il problema in questione.

## Come utilizzeremo i computer quantistici?



**Figura 1.2** Modi in cui vorremmo poter utilizzare i computer quantistici. Fumetto utilizzato con il permesso di xkcd.com.

È importante comprendere sia le potenzialità sia i limiti dei computer quantistici, soprattutto dato il clamore che circonda il quantum computing. Molti degli equivoci alla base di questo clamore derivano dall'extrapolazione di analogie ben oltre il punto in cui perdono senso: tutte le analogie hanno i loro limiti e il quantum computing non sfugge alla regola. Simulare il modo in cui un programma quantistico agisce nella pratica può essere un ottimo modo per sottoporre a test e perfezionare la comprensione fornita dalle analogie. Tuttavia, in questo libro utilizzeremo ancora varie analogie, in quanto possono aiutare a fornire idee su come funziona il quantum computing.

### SUGGERIMENTO

Se avete letto descrizioni dei nuovi risultati nel quantum computing che dicono qualcosa come "Possiamo teletrasportare gatti che esistono contemporaneamente in due posti utilizzando la potenza di infiniti universi paralleli che collaborano, tutti insieme, per curare il cancro", allora avete toccato con mano il pericolo di eseguire estrapolazioni ben lontano da dove le analogie possono essere utili.

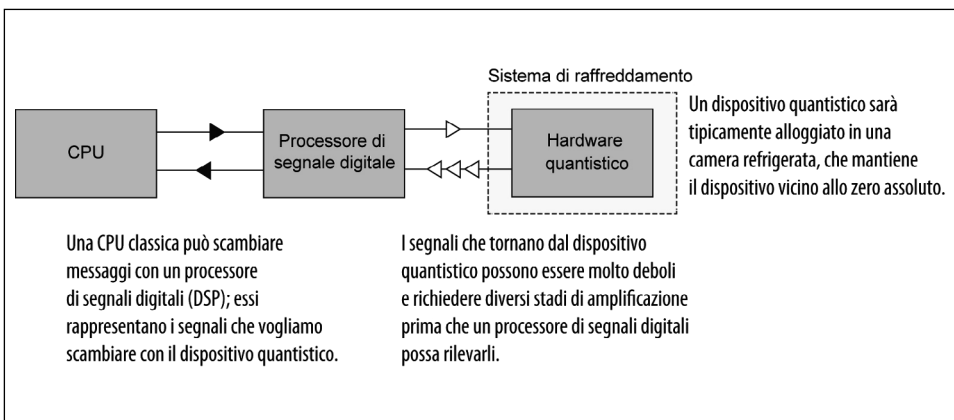
Un punto di confusione particolarmente comune riguardo al quantum computing riguarda il modo in cui gli utenti useranno i computer quantistici. Come società, siamo arrivati a capire che cos'è un *computer*: qualcosa che potete usare per eseguire applicazioni web, scrivere documenti ed eseguire simulazioni. In effetti, i computer classici svolgono talmente tante attività nella nostra vita che non sempre è facile capire che cosa sia e non sia un computer. Cory Doctorow ha compiuto questa osservazione notando che "La tua automobile è un computer in cui ti siedi" (DrupalCon Amsterdam 2014, [www.youtube.com/watch?v=iaf3512r3jE](http://www.youtube.com/watch?v=iaf3512r3jE)).

I computer quantistici, al contrario, probabilmente saranno molto più specializzati: ci aspettiamo che i computer quantistici siano inutili per alcune attività. Un ottimo modello per il modo in cui il quantum computing si adatterà ai nostri problemi di elaborazione classici sono le GPU. Le GPU sono dispositivi hardware specializzati, progettati per velocizzare determinati tipi di calcoli come il disegno grafico, le attività di machine learning e qualsiasi cosa sia facilmente parallelizzabile. Certamente vorrete avere una GPU per quelle attività specifiche, ma probabilmente non vorrete usarla per tutto, poiché abbiamo CPU molto più flessibili per le attività generali, come il controllo della posta elettronica. I computer quantistici saranno esattamente la stessa cosa: saranno ottimi per accelerare determinati tipi di attività, ma non saranno appropriati per un uso più generale.

#### NOTA

La programmazione di un computer quantistico prevede alcune limitazioni, quindi sarà preferibile impiegare computer classici quando non è possibile trovare un determinato vantaggio con quelli quantistici.

La computer science classica sarà ancora in circolazione e sarà il modo con cui comunicheremo e interagiranno fra noi, ma sarà affiancata da hardware quantistico. Anche per far sì che le risorse classiche si interfaccino con i dispositivi quantistici, nella maggior parte dei casi avremo anche bisogno di un processore di segnale da digitale ad analogico, come illustrato nella Figura 1.3.



**Figura 1.3** Un esempio del modo in cui un dispositivo quantistico potrebbe interagire con un computer classico attraverso l'uso di un processore di segnali digitali (DSP). Il DSP invia segnali a bassa potenza al dispositivo quantistico e amplifica i segnali a bassissima potenza che tornano dal dispositivo.

Inoltre, la fisica quantistica descrive entità esistenti su scale molto piccole (sia per dimensioni sia per energia) e ben isolate dall'ambiente circostante. Questo pone alcune forti limitazioni agli ambienti in cui possiamo collocare un computer quantistico. Una possibile soluzione consiste nel mantenere i dispositivi quantistici in apparecchi criogenici, spesso vicino a zero assoluto ( $-273,15^{\circ}\text{C}$ ). Mentre questo può non rappresentare

un problema in un data center, la manutenzione di un refrigeratore a diluizione non è davvero sensata in un computer desktop, tanto meno in un laptop o in un telefono cellulare. Per questo motivo, i computer quantistici verranno probabilmente utilizzati a lungo attraverso il cloud, almeno per un bel po' di tempo dopo che saranno disponibili per la prima volta in commercio.

L'utilizzo di computer quantistici come servizio cloud somiglia ad altri progressi nell'hardware di calcolo specializzato. Centralizzando le risorse di calcolo più costose nei data center, è possibile esplorare modelli di elaborazione che sarebbero difficili da distribuire in utilizzo locale, se non per gli utenti più grandi.

- Hardware di gioco specializzato (PlayStation Now, Xbox One).
- Cluster di elaborazione a latenza estremamente bassa e ad alte prestazioni (per esempio Infiniband) per problemi scientifici.
- Enormi cluster di GPU.
- Hardware riprogrammabile (per esempio Catapult/Brainwave).
- Cluster di unità di elaborazione tensoriale (TPU).
- Archiviazione a elevata permanenza e latenza (per esempio Amazon Glacier).

In futuro, i servizi cloud come Azure Quantum (<https://azure.com/quantum>) renderanno disponibile la potenza del quantum computing più o meno allo stesso modo.

Proprio come le connessioni Internet ad alta velocità e ad alta disponibilità hanno reso il cloud computing accessibile a un gran numero di utenti, saremo in grado di utilizzare computer quantistici da una sdraio in spiaggia o da un caffè, grazie al WiFi, o anche da un treno, mentre ammiriamo maestose catene montuose, in lontananza.

## Che cosa possono fare i computer quantistici?

Come programmatori quantistici, se abbiamo un determinato problema, *come facciamo a sapere che ha senso risolverlo con un computer quantistico?*

Stiamo ancora scoprendo la portata esatta di ciò di cui sono capaci i computer quantistici, e quindi non abbiamo ancora regole concrete per rispondere a questa domanda. Finora, abbiamo trovato alcuni esempi di problemi in cui i computer quantistici offrono vantaggi significativi rispetto agli approcci classici più noti. In tutti i casi, tutti gli algoritmi quantistici che sono stati sviluppati per risolvere questi problemi sfruttano gli effetti quantistici per ottenere tali vantaggi, motivo per cui si parla di un *vantaggio quantistico*. Ecco due esempi di algoritmi quantistici.

- L'algoritmo di Grover (discusso nel Capitolo 11) esegue ricerche in una lista di  $N$  elementi in  $\sqrt{N}$  passaggi.
- L'algoritmo di Shor (Capitolo 12) calcola rapidamente numeri interi di grandi dimensioni, come quelli utilizzati dalla crittografia per proteggere i dati privati.

Ne vedremo molti altri in questo libro, ma gli algoritmi di Grover e Shor sono buoni esempi di come lavorano gli algoritmi quantistici: ognuno di essi impiega effetti quantistici per separare le risposte corrette dei problemi computazionali dalle soluzioni non valide. Un modo per realizzare un vantaggio quantistico consiste nel trovare modi per sfruttare gli effetti quantistici per separare le soluzioni corrette da quelle errate nei problemi classici.



## Quali sono i vantaggi quantistici?

Gli algoritmi di Grover e Shor illustrano due tipi distinti di vantaggi quantistici. La fattorizzazione di numeri interi potrebbe essere più semplice di quanto sospettiamo. Sono molti ad aver tentato di scomporre rapidamente i numeri interi, e non ci sono riusciti, ma ciò non significa che possiamo *dimostrare* che la fattorizzazione sia difficile. D'altra parte, possiamo dimostrare che l'algoritmo di Grover è più veloce di *qualsiasi* algoritmo classico; il problema è che utilizza un diverso tipo di input. Trovare un vantaggio *dimostrabile* per un problema pratico è un'area di ricerca attiva nel quantum computing. Detto questo, i computer quantistici possono essere strumenti potenti per risolvere i problemi, anche se non possiamo dimostrare che verrà mai trovato un algoritmo classico migliore. Dopotutto, l'algoritmo di Shor sfida le ipotesi che sono alla base di molte applicazioni di sicurezza delle informazioni: è necessaria una dimostrazione matematica solo perché non abbiamo ancora costruito un computer quantistico abbastanza grande da eseguire l'algoritmo di Shor.

I computer quantistici offrono vantaggi significativi anche per la simulazione delle proprietà dei sistemi quantistici, con applicazioni nei campi della chimica quantistica e della scienza dei materiali. Per esempio, i computer quantistici potrebbero rendere molto più facile lo studio delle energie dello stato fondamentale dei sistemi chimici. Queste energie dello stato fondamentale forniscono quindi informazioni su tassi di reazione, configurazioni degli elettroni, proprietà termodinamiche e altre proprietà di grande interesse per la chimica.

Lungo la strada per lo sviluppo di queste applicazioni, abbiamo anche intravisto vantaggi significativi nelle tecnologie derivate, come la distribuzione quantistica delle chiavi e la metrologia quantistica, alcuni dei quali saranno esaminati nei prossimi capitoli. Nell'imparare a controllare e comprendere i dispositivi quantistici per scopi di calcolo, abbiamo anche appreso tecniche preziose per l'imaging, la stima dei parametri, la sicurezza e altro ancora. Sebbene queste non siano applicazioni di quantum computing in senso stretto, sono molto utili per mostrare i valori del *ragionamento* in termini di calcolo quantistico. Naturalmente, diventa molto più facile scoprire nuove applicazioni dei computer quantistici quando abbiamo una comprensione concreta di come funzionano gli algoritmi quantistici e di come costruire nuovi algoritmi a partire dai principi di base. Da quel punto di vista, la programmazione quantistica è un'ottima risorsa per imparare a scoprire applicazioni interamente nuove.

## Che cosa non possono fare i computer quantistici?

Come altre forme di hardware specializzato, i computer quantistici non sono “buoni per tutto”. Per alcuni problemi, i computer classici saranno, semplicemente, più adatti al compito. Nello sviluppo di applicazioni per dispositivi quantistici, è utile parlare di quali attività e problemi non rientrano nell'ambito del quantum computing.

La “versione breve” è che non abbiamo regole rigide per decidere rapidamente quali attività sono più adatte ai computer classici e quali possono trarre vantaggio dai computer quantistici. Per esempio, i requisiti di archiviazione e larghezza di banda per le applicazioni in stile big data sono molto difficili da mappare su dispositivi quantistici,

dove potremmo avere a disposizione un sistema quantistico relativamente piccolo. Gli attuali computer quantistici possono registrare solo input di poche decine di bit e questa limitazione diventerà più rilevante man mano che i dispositivi quantistici verranno utilizzati per compiti sempre più impegnativi. Sebbene ci aspettiamo di costruire in futuro sistemi quantistici molto più grandi di quanto possiamo ora, i computer classici saranno probabilmente sempre preferibili per quei problemi la cui risoluzione richiede grandi quantità di input/output.

Allo stesso modo, le applicazioni di machine learning che dipendono fortemente dall'accesso casuale a grandi serie di input classici sono concettualmente difficili da risolvere con il quantum computing. Detto questo, *potrebbero* esserci altre applicazioni di machine learning che si mappano in modo molto più naturale sul quantum computing. Gli sforzi di ricerca per trovare i modi migliori per applicare le risorse quantistiche a risolvere attività di machine learning sono ancora in corso. In generale, i problemi che hanno piccoli dati di input e output ma richiedono grandi quantità di calcolo per passare dall'input all'output sono buoni candidati per i computer quantistici.

Alla luce di queste sfide, si potrebbe essere tentati di concludere che i computer quantistici eccellono sempre in compiti che hanno piccoli input e output ma molto calcolo intenso per passare dall'uno all'altro. Concetti come il *parallelismo quantistico* sono ampiamente presenti nei media e talvolta i computer quantistici sono persino descritti come se utilizzassero universi paralleli per i loro calcoli.

#### NOTA

Il concetto di "universi paralleli" è un ottimo esempio di analogia che può aiutare a rendere comprensibili i concetti quantistici, ma che può anche portare a vere sciocchezze, se portata al suo estremo. A volte può essere utile pensare che le diverse parti di un calcolo quantistico si trovino in "universi" differenti, che non possono influenzarsi a vicenda, ma questa descrizione non aiuta a pensare ad alcuni degli effetti che tratteremo in questo libro, come l'interferenza. Se portata troppo lontano, l'analogia degli universi paralleli porta a pensare al quantum computing in modi che sono più vicini a un episodio particolarmente intrigante e divertente di una serie di fantascienza come *Star Trek* che alla realtà.

Ciò che questo non riesce a comunicare, tuttavia, è che non sempre è ovvio capire come utilizzare gli effetti quantistici per estrarre risposte utili da un dispositivo quantistico, anche se lo stato del dispositivo quantistico sembra contenere l'output desiderato. Per esempio, un modo per fattorizzare un intero  $N$  utilizzando un computer classico è elencare ogni fattore *potenziale* e verificare se è effettivamente un fattore o meno:

1. Esegui l'assegnamento  $i = 2$ .
2. Verifica se il resto di  $N / i$  è 0.
  - In tal caso, restituisci che  $i$  è un fattore di  $N$ .
  - In caso contrario, incrementa  $i$  e ripeti il ciclo.

Possiamo accelerare questo algoritmo classico utilizzando una grande quantità di computer classici, uno per ogni fattore potenziale che vogliamo provare. Cioè, questo problema può essere facilmente parallelizzato. Un computer quantistico può provare ogni fattore potenziale all'interno dello stesso dispositivo, ma, a quanto pare, questo non è ancora sufficiente per fattorizzare gli interi più velocemente dell'approccio classico. Se utilizziamo questo approccio su un computer quantistico, l'output sarà uno dei potenziali

fattori scelti a caso. I fattori effettivamente corretti si verificheranno con probabilità di circa  $1 / \sqrt{N}$ , un risultato non migliore dell'algoritmo classico.

Come vedremo nel Capitolo 12, però, possiamo usare altri effetti quantistici per fattorizzare i numeri interi con un computer quantistico più velocemente rispetto ai più noti algoritmi classici. Gran parte del lavoro pesante svolto dall'algoritmo di Shor consiste nell'assicurarsi che la probabilità di misurare un fattore corretto alla fine sia molto maggiore della probabilità di misurare un fattore errato. Cancellare le risposte errate in questo modo è il punto in cui entra in gioco gran parte dell'arte della programmazione quantistica; è non è facile o addirittura nemmeno possibile farlo per tutti i problemi che potremmo voler risolvere.

Per capire più concretamente che cosa possono e non possono fare i computer quantistici e come fare cose interessanti con i computer quantistici nonostante queste sfide, è utile adottare un approccio più concreto. Quindi, cerchiamo di prendere in considerazione ciò che un programma quantistico *effettivamente* è, in modo da poter iniziare a scrivere i nostri programmi.

## Che cos'è un programma?

In tutto il libro, troveremo spesso utile spiegare un concetto quantistico riesaminando prima l'analogo concetto classico. In particolare, facciamo un passo indietro ed esaminiamo che cos'è un programma classico.

### DEFINIZIONE

Un *programma* è una sequenza di istruzioni che può essere interpretata da un computer classico per eseguire il compito desiderato. I moduli fiscali, le indicazioni stradali, le ricette e gli script Python sono tutti esempi di programmi.

Possiamo scrivere programmi classici per suddividere un'ampia varietà di compiti per consentirne l'interpretazione da parte di tutti i tipi di computer. La Figura 1.4 mostra alcuni esempi di programmi.

Vediamo l'aspetto di un semplice programma "hello world" in Python:

```
>>> def hello():
...     print ("Hello, world!")
...
>>> hello()
Hello, world!
```

Nella sua forma più elementare, questo programma può essere considerato come una sequenza di istruzioni fornite all'interprete Python, che quindi lo esegue un'istruzione per volta per ottenere qualche effetto, in questo caso, mostrare un messaggio sullo schermo. Il programma è quindi una descrizione di un'attività che viene poi *interpretata* da Python e, a sua volta, dalla CPU per raggiungere l'obiettivo. Questa interazione tra la descrizione e l'interpretazione spinge a chiamare Python, C e altri strumenti di programmazione simili con il nome di *linguaggi*, enfatizzando la programmazione è il modo in cui comunichiamo con i nostri computer.

The figure displays three examples of classic programs, each with a unique interface and a sequence of instructions to be interpreted by a user.

- Form 1040 (2017):** A tax form with various sections like "Tax and Credits", "Standard Deduction", and "Total boxes". It contains numerous checkboxes and numerical fields for tax calculations.
- Navigation App:** A map interface showing a route from "Living Computers: Museum + Labs, 221" to "Pioneer Square". It includes options like "Leave now" and "Send directions to your phone", along with estimated travel times and distances for different routes.
- Biscotti allo zucchero:** A recipe card for "Biscotti allo zucchero" (Sugar Cookies). It lists ingredients (1 1/2 cups butter, 1 1/2 cups sugar, 1 egg, 1 tsp vanilla, 1/2 tsp almond extract, 2 1/2 cups flour, 1 tsp baking soda, 1 tsp cream of tartar, 1 Hershey's Kisses) and provides step-by-step instructions for preparation and baking.

**Figura 1.4** Esempi di programmi classici. Moduli fiscali, indicazioni stradali e ricette sono tutti esempi in cui una sequenza di istruzioni deve essere interpretata da quel “calcolatore” classico, che è una persona. Possono sembrare programmi molto diversi, ma ognuno di essi utilizza un elenco di passaggi per comunicare una procedura.

Nell’esempio dell’utilizzo di Python per mostrare “Hello, world!” stiamo effettivamente comunicando con Guido van Rossum, il progettista fondatore del linguaggio Python. Guido, a sua volta, comunica in pratica per nostro conto con i progettisti del sistema operativo che stiamo utilizzando. Questi progettisti a loro volta comunicano per nostro conto con Intel, AMD, ARM o qualsiasi altra azienda abbia progettato la CPU che stiamo utilizzando e così via.

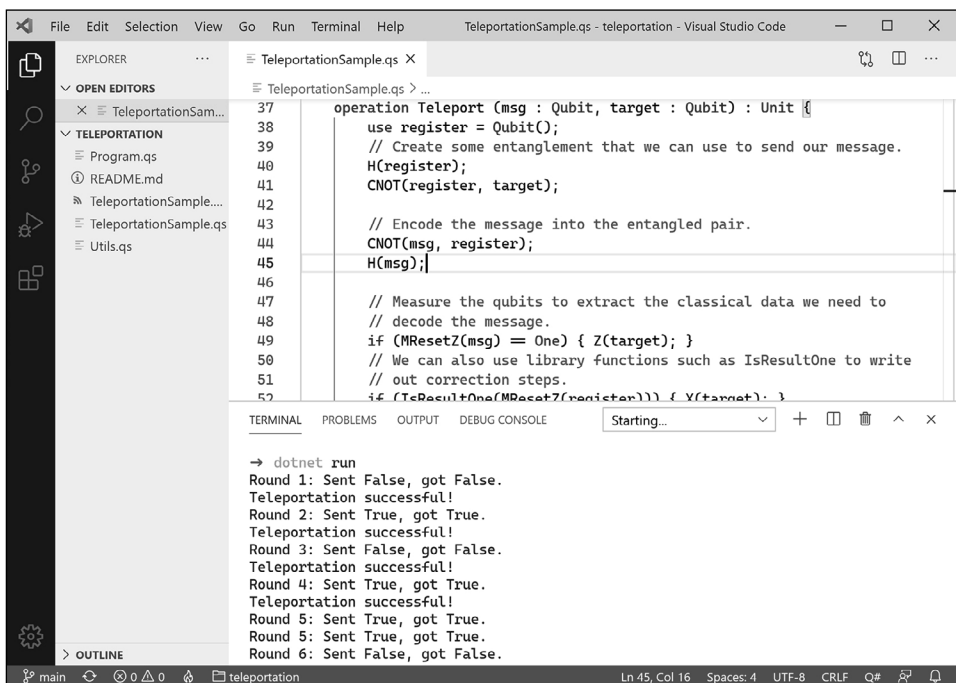
## Che cos’è un programma quantistico?

Come i programmi classici, i programmi quantistici sono costituiti da sequenze di istruzioni che vengono interpretate dai computer classici per eseguire un determinato compito. La differenza, tuttavia, è che in un programma quantistico, il compito che desideriamo svolgere viene svolto da un sistema quantistico.

Di conseguenza, anche le istruzioni utilizzate nei programmi classici e quantistici differiscono. Un programma classico può descrivere un’attività come il caricamento da Internet

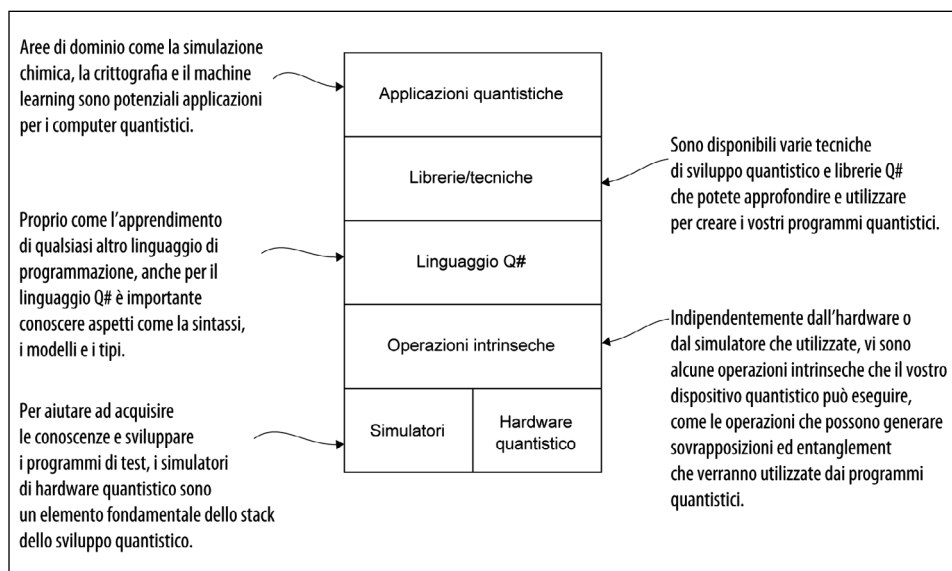
di alcune immagini di gatti in termini di istruzioni per uno stack di rete e alla fine in termini di istruzioni assembler, come `mov`. Al contrario, linguaggi quantistici come Q# consentono ai programmatori di esprimere compiti quantistici in termini di istruzioni come `M` (misura). Quando vengono eseguiti utilizzando hardware quantistico, questi programmi possono chiedere a un elaboratore di segnali digitali di inviare microonde, onde radio o laser a un dispositivo quantistico e di amplificare poi i segnali che escono dal dispositivo.

Nel resto di questo libro, vedremo molti esempi dei tipi di compiti che un programma quantistico deve risolvere o, quanto meno, affrontare, e scopriremo quali tipi di strumenti classici possiamo impiegare per agevolare la programmazione quantistica. La Figura 1.5 mostra un esempio di scrittura di un programma quantistico in Visual Studio Code, un classico ambiente di sviluppo integrato (IDE).



**Figura 1.5** Scrittura di un programma quantistico con Quantum Development Kit e Visual Studio Code. Esamineremo il contenuto di questo programma nel Capitolo 7, ma già a questo livello noterete certamente la similitudine con altri progetti software sui quali potreste aver lavorato.

Capitolo per capitolo svilupperemo i concetti di cui abbiamo bisogno per poter scrivere programmi quantistici; la Figura 1.6 mostra una tabella di marcia. Nel prossimo capitolo, scopriremo gli elementi di base che compongono un computer quantistico e li utilizzeremo per scrivere il nostro primo programma quantistico.



**Figura 1.6** Questo libro sviluppa i concetti di cui abbiamo bisogno per scrivere programmi quantistici. La Parte I offre descrizioni di basso livello dei simulatori e delle operazioni intrinseche (l'API hardware) tramite la costruzione di un simulatore in Python. La Parte II esamina il linguaggio Q# e le tecniche di sviluppo quantistico che ci aiuteranno a sviluppare le nostre applicazioni. La Parte III mostra alcune applicazioni note di quantum computing e le sfide e opportunità che ci offre questa nuova tecnologia.

## Riepilogo

- Il quantum computing è importante perché i computer quantistici ci consentiranno, potenzialmente, di risolvere problemi troppo difficili per i computer convenzionali.
- I computer quantistici possono fornire vantaggi rispetto ai computer classici per alcune classi di problemi, come la fattorizzazione di grandi numeri.
- I computer quantistici sono dispositivi che utilizzano la fisica quantistica per elaborare i dati.
- I programmi sono sequenze di istruzioni che possono essere interpretate da un computer classico per eseguire determinate attività.
- I programmi quantistici sono programmi che eseguono calcoli inviando istruzioni a dispositivi quantistici.