Alberto Palazzi

Informatica Quantistica per Programmatori e Investitori

il glifo ***ebooks***

ISBN: 9788897527534

Indice

1. Introduzione

Una spiegazione per programmatori e investitori

Perché questo libro si rivolga insieme a programmatori e investitori, si capirà pienamente dopo averlo letto. Preliminarmente, diciamo che riguardo al computer quantistico ci sono due domande:

1) quando si riuscirà a costruirne uno efficiente?

2) quali problemi potrà risolvere?

I libri sull'informatica quantistica che sono stati scritti contengono nozioni di carattere diverso: parlano con maggiore o minore dettaglio dei principi fisici (quantistici) che governano i fenomeni subatomici, espongono la matematica necessaria per lo studio della fisica quantistica (algebra lineare), e infine trattano l'informatica quantistica. In questo libro i lettori non troveranno alcuna nozione riguardante i principi fisici, e riguardo alla matematica troveranno solo la parte applicata necessaria all'informatica quantistica, che consiste di algoritmi per operazioni aritmetiche su vettori e matrici di numeri complessi. Poi su questa base i lettori troveranno la descrizione dei gate quantistici e degli algoritmi quantistici più celebri, con implementazione in linguaggio C. Il computer quantistico sarà descritto come una black box hardware che è in grado di trasformare un dato input in un dato output, come accade sempre nei testi di informatica, nei quali le nozioni riguardanti l'elettronica dei semiconduttori sottostante ai calcoli sono solo accennate e potrebbero anche essere completamente omesse.

Perciò, questo libro non ha alcuna risposta per la domanda 1. Se mai e quando si riuscirà a costruire un computer quantistico efficiente, è domanda tale che richiede una completa conoscenza ed esperienza della fisica quantistica per poter azzardare una risposta.

Invece, leggendo questo libro i lettori si ritroveranno in possesso di una risposta precisa alla seconda domanda: se questa notte il diavolo, come nelle favole, costruisse un computer quantistico perfettamente efficiente e stabile, e capace di gestire una matrice di qubit di dimensioni considerevoli, il giorno dopo per quali scopi potremmo utilizzarlo? Va detto subito che la particolarità dello hardware quantistico sarà quella di eseguire in un solo atto, un solo cambiamento di stato della macchina, certe operazioni su matrici che gli odierni computer basati sul principio della macchina di Turing devono eseguire mediante l'iterazione di numerosi cicli innestati l'uno dentro l'altro, e quindi con tempi di esecuzione considerevoli, e per certi problemi con tempi talmente espansi da non consentire

soluzioni tecnicamente utili. Eseguendo con un solo mutamento di stato trasformazioni dell'input corrispondenti a un certo numero (idealmente molto grande) di cicli di un computer classico, si legge e si sente dire che il computer quantistico sarà in grado di tagliare drasticamente il tempo di esecuzione per operazioni di cifratura e crittografia, e per il ritrovamento di soluzioni a problemi di alta complessità come quelli di logistica, ottimizzazione, schedulazione, ricerca operativa ecc.

Come ciò possa avvenire, può essere compreso mediante l'emulazione degli algoritmi quantistici mediante il computer classico disponibile oggi, anche se ovviamente l'emulazione non avrà alcuna utilità pratica perché l'emulazione di un algoritmo quantistico senza lo hardware quantistico richiederà sempre risorse di calcolo maggiori di quelle richieste per eseguire il corrispondente algoritmo non quantistico. Cioè, supponiamo di dover eseguire una trasformazione di una matrice che il computer quantistico eseguirà in un solo mutamento di stato della macchina. Supponiamo che quella stessa trasformazione mediante un algoritmo realizzabile su un computer classico richieda la ripetizione di, poniamo, mille o un milione di cicli. Bene, se provassimo a ottenere lo stesso risultato con un algoritmo classico che emula un algoritmo quantistico, come vedremo e come è immaginabile, avremo bisogno di un numero di cicli molto maggiore dei mille o del milione dell'algoritmo classico, e avremo anche bisogno di allocare una quantità di memoria molto maggiore. Vedremo nel seguito, per esempio, come l'emulazione su computer classico dell'algoritmo di Shor per la ricerca dei fattori di un numero sia enormemente meno efficiente di qualsiasi elementare algoritmo per la ricerca dei fattori primi.

Questo libro è scritto per *programmatori* perché per leggerlo è necessario soltanto possedere le nozioni basilari comuni di informatica (gate logici, diagrammi di flusso, linguaggi di programmazione). Gli esempi sono scritti in linguaggio C nel modo più piano e senza uso di costrutti che non siano elementari, sicché chiunque sappia leggere un qualsiasi linguaggio di programmazione potrà capirlo. Lo scopo del libro è quello di condurre il lettore a comprendere la logica degli algoritmi quantistici descritti nel capitolo 6, e perciò tutto quanto esposto nei capitoli da 2 a 5 è enormemente semplificato e ridotto al minimo indispensabile: la scelta deliberata è stata quella di dare al lettore solo le premesse necessarie per comprendere il flusso logico e i calcoli degli algoritmi quantistici, che si suppone sia l'obiettivo del lettore, e per questa ragione i capitoli precedenti quello dedicato agli algoritmi quantistici

contengono solo le informazioni che sono condizione necessaria alla comprensione.

È importante mettere bene a fuoco che la conoscenza della parte puramente informatica degli algoritmi quantistici non è soggetta a nessuna limitazione per il fatto di prescindere completamente dalle caratteristiche fisiche dello hardware. La riprova sta nel fatto che leggendo questo libro il lettore potrà implementare ed eseguire gli algoritmi quantistici sul proprio PC ottenendo i risultati previsti dalla teoria: quindi la conoscenza degli algoritmi quantistici sarà tanto completa da permetterne l'applicazione e la verifica. Ciò riprova anche che gli algoritmi quantistici in se stessi non richiedono lo hardware quantistico, così come la CPU di un computer teoricamente si potrebbe costruire con mezzi meccanici anziché sfruttando proprietà elettroniche: ma se ne otterrebbe una macchina troppo lenta per essere utile a qualcosa, esattamente come accade emulando gli algoritmi quantistici con il computer classico oggi esistente.

Poiché questo libro consente a chi abbia le cognizioni di un *programmatore* di capire esattamente a cosa potrebbe servire un computer quantistico, una volta costruito, esso risolve almeno metà del problema che si pongono gli *investitori* nel momento di valutare se e quanto sia opportuno rischiare investendo sullo sviluppo dell'informatica quantistica. Perciò gli investitori (investitori privati, consulenti, gestori di fondi di investimento, gestori di fondi di finanziamento delle iniziative tecnologiche ecc.), se non posseggono personalmente i prerequisiti necessari per capire questo libro, potrebbero servirsene incaricando qualche esperto di informatica di loro fiducia di leggerlo, capirlo e fare relazione riguardo al risultato.

Bibliografia e verifica

Questo libro è una presentazione semplificata della teoria esposta con completezza in due trattazioni fondamentali, che sono:

- Nielsen, Michael & Chuang, Isaac L., *Quantum Computation and Quantum Information*, Cambridge University Press, 2000 e 2010
- Yanofsky, Noson S. & Mannucci, Mirco A., *Quantum Computing for Computer Scientists*, Cambridge University Press, 2008.

Tutto quanto nel seguito verrà asserito in maniera descrittiva e come dato di fatto, senza dimostrazioni e senza citazioni, può essere verificato e approfondito mediante lo studio di questi due volumi, che il lettore che abbia assimilato questo libro probabilmente troverà più agevole di quanto non sembri a prima vista.

La circostanza che siamo ormai nel 2020 è poco importante: questi due libri espongono la base teorica della materia in un modo che è consolidato, e nei dieci e più anni che sono passati non si è realizzato altro che qualche progresso nella costruzione dei prototipi dello hardware. Questo è confermato dalla lettura di un'altra trattazione molto recente, più semplice e tuttavia rigorosa:

- Bernhardt, Chris, *Quantum Computation for Everyone*, The MIT Press, 2019

la quale discute i gate quantistici e i cinque algoritmi fondamentali (accennando solo a quello di Shor) esattamente nello stesso modo dei trattati precedenti, né contiene alcunché di nuovo dal punto di vista dello sviluppo del software.

Rispetto a questi trattati, la nostra trattazione manca completamente sia della parte fisica sia delle dimostrazioni delle proprietà numeriche su cui si fondano gli algoritmi quantistici, ed è orientata a favorire la comprensione concreta degli algoritmi mediante l'implementazione; tuttavia lo stato delle cose e le potenzialità del computer quantistico che vengono messi in luce dalla nostra trattazione corrispondono esattamente alle conclusioni che chiunque può trarre dalla lettura attenta di quei libri più complessi e completi. I lettori quindi sono caldamente invitati a usare questo libro per prendere confidenza con la materia, e poi a studiare la materia in maniera più astratta e rigorosa nei trattati citati, i quali a chi assimila questo libro non appariranno più così complessi come accade a chi si accosta per la prima volta a questi argomenti. Il primo libro da leggere è quello di Bernhardt del 2019, che per molti lettori avrà un rigore teorico più che soddisfacente, e fornisce anche una minima introduzione alla fisica sottostante al funzionamento dello hardware.

Non siamo a conoscenza di opere semplificate e divulgative utili: i libri più semplici che abbiamo consultato sono tutti costruiti in modo troppo generico per consentire alcuna comprensione della materia. E in particolare sconsigliamo i lettori di partire dai linguaggi di programmazione quantistici, che come punto di partenza sono incomprensibili, mentre per il lettore che abbia compreso gli algoritmi quantistici fondamentali sono una conseguenza ovvia ed estremamente semplice. Comunque, per una trattazione più semplice e aggiornata orientata ai linguaggi di programmazione, si può consultare:

- Radovanovic Aleksandar, *Quantum Computing Illustrated*, qpi-book, 2020.

Progetto QcNooq e download del codice sorgente

Il codice degli esempi di programmazione che viene citato nel libro contiene solo le istruzioni necessarie per la comprensione degli algoritmi. Consigliamo di leggere attentamente il libro una prima volta senza preoccuparsi di eseguire il codice: se non si comprende ciò che si legge nel libro, il codice sorgente non sarà di aiuto.

Chi volesse potrebbe implementare la propria emulazione dei cinque algoritmi usando il solo codice citato nel libro, e aggiungendo le istruzioni necessarie per l'output e la verifica dei risultati. Comunque, tutto il codice sorgente è disponibile in Visual C per Windows. Il progetto si chiama *QcNooq* ed è descritto in Appendice, con le istruzioni per l'uso in ambiente Windows e in altri ambienti.

Informazioni pratiche

Questo libro è disponibile in ebook su molti ebook store e anche in formato cartaceo su Amazon. Il formato è stato progettato in modo da rendere il libro leggibile anche sul piccolo schermo di un ebook reader, ma con inevitabili limitazioni, per cui qualche lettore preferirà il formato cartaceo.

Notazione

Il simbolo ► richiama l'attenzione su fatto che le linee successive contengono una definizione da ricordare.

Talvolta nel corso del testo vi sono note e chiarimenti accessori, o parti che possono essere lette rapidamente da chi già conosca i dettagli discussi: queste parti del testo sono in corpo tipografico leggermente più piccolo.

La notazione dei frammenti di codice sorgente è quella del linguaggio C, di cui sono usati i costrutti più semplici e simili a quelli di ogni altro linguaggio, che si assumono conosciuti dal lettore. Comunque qualche spiegazione è aggiunta per chiarire ciò che non è del tutto ovvio. Poiché il linguaggio C è usato correntemente nelle parti discorsive del testo, quando per leggibilità ciò è opportuno i nomi lunghi di variabili sono sottolineato come in questo esempio: "il risultato si legge nella variabile mresult".

Gli indici di vettori e matrici nel corso del testo vengono indicati nel modo più semplice dato il contesto, quindi con pedici quando li si guarda dal punto di vista matematico, e con la notazione del C quando si fa riferimento all'implementazione. Così per un vettore di numeri reali potremo avere la notazione v_n oppure: double v[N], e per un suo elemento v_j nel primo caso e v[j] nel secondo.

Per i circuiti quantistici si userà la notazione usata generalmente da tutti i testi, e la introdurremo al momento opportuno.

2. Numeri complessi

2.1 Aritmetica dei numeri complessi

Probabilmente tutti i lettori di questo libro ricordano le nozioni basilari che riguardano i numeri complessi. Qui richiamiamo solo quelle che saranno utilizzate nell'implementazione del codice per emulare gli algoritmi quantistici; lo studio della fisica quantistica e dello hardware del computer quantistico invece richiederebbe il ripasso completo, a cominciare dalla rappresentazione geometrica dei numeri complessi in coordinate polari.

……. fine dell'anteprima

Quarta di copertina

Questo libro si rivolge a chi conosce semplicemente le nozioni basilari della programmazione di un computer. Non richiede alcuna nozione di fisica e consente di comprendere con totale esattezza e nel modo più semplice l'uso che si potrebbe fare di un computer quantistico spiegando passo dopo passo come si può scrivere il software di emulazione del suo funzionamento. L'usuale espressione che un qubit "è un oggetto che può stare simultaneamente in entrambi gli stati binari 0 e 1" perderà tutto l'alone di mistero che la circonda, e i lettori ne comprenderanno esattamente il significato e le implicazioni per l'uso informatico senza necessità di alcuna cognizione di fisica. Il libro descrive il computer quantistico trattandolo dal punto di vista strettamente informatico, semplicemente come una macchina che è in grado di trasformare un dato input in un dato output utilizzando qualsiasi principio fisico adeguato per funzionare, e così consente di acquisire familiarità completa con i gate quantistici e con gli algoritmi quantistici più celebri. L'unica condizione è che i lettori abbiano dimestichezza con qualche linguaggio di programmazione e con i concetti basilari dell'informatica classica: coloro che hanno queste cognizioni seguiranno senza difficoltà la descrizione degli algoritmi quantistici e comprenderanno il funzionamento dell'emulazione che è implementata nel libro, che sarà anche piacevole eseguire e verificare con il proprio PC.

La conoscenza che si acquisisce con questo libro è di vitale importanza per gli *investitori* perché consente loro di giudicare in autonomia sul rischio dell'investimento in questa tecnologia. Esso è stato scritto per *programmatori* perché la conoscenza dell'informatica di base è utile per capire esattamente a cosa potrebbe servire un computer quantistico, una volta costruito. Ma questa comprensione è indispensabile anche per gli *investitori* che devono valutare se e quanto sia opportuno rischiare investendo sullo sviluppo dell'informatica quantistica. Perciò anche gli *investitori* (investitori privati, consulenti, gestori di fondi di finanziamento delle iniziative tecnologiche ecc.) che vogliano decidere l'allocazione di risorse nel quantum computing con piena cognizione della posta in gioco, devono conoscere questo libro, e se non posseggono personalmente i prerequisiti necessari potranno servirsene incaricando qualche esperto di informatica di loro fiducia di leggerlo, capirlo e fare relazione riguardo al risultato.

Alberto Palazzi

Studioso di storia e filosofia della scienza e progettista di algoritmi informatici per la soluzione di problemi di complessità superiore, l'autore di questo libro è membro del team di consulenza *QcNooq* (www.zonabit.it/qcnooq), la cui missione è fornire agli investitori la chiarezza di vedute necessaria per decidere in materia di investimenti nel quantum computing.