Praktični pristup

Naučite kvantno računarstvo uz Python i Q#

Sarah Kaiser
Cassandra Granade

kompjuter biblioteka

MANNING

Naučite kvantno računarstvo uz Python i Q#

Praktični pristup

Kvantni računari predstavljaju radikalan skok u brzini i računarskoj moći. Poboljšane naučne simulacije i nove granice u kriptografiji koje su nemoguće sa klasičnim računarstvom uskoro bi mogle biti dostupne. Microsoftov Quantum Development Kit i Q# jezik pružaju nam alate za eksperimentisanje sa kvantnim računarstvom bez poznavanja napredne matematike ili teorijske fizike.

Knjiga **Naučite kvantno računarstvo uz Python i Q#** predstavlja kvantno računarstvo iz praktične perspektive. Koristite Python za izgradnju sopstvenog kvantnog simulatora i iskoristite prednosti Microsoftovih alata otvorenog koda za fino podešavanje kvantnih algoritama.Autori objašnjavaju složenu matematiku i teoriju kroz priče, vizuelne prikaze i igre. Naučićete da primenite kvantno računarstvo na aplikacije iz stvarnog sveta, kao što su slanje tajnih poruka i rešavanje hemijskih problema.

Šta ćete pronaći u knjizi

- Osnovna mehanika kvantnih računara
- Simulacija kubita u jeziku Python
- Istraživanje kvantnih algoritama pomoću jezika Q#
- Primena kvantnog računarstva na hemiju, aritmetiku i podatke

Za programere softvera. Nije potrebno prethodno iskustvo u kvantnom računarstvu.

Dr Sarah Kaiser radi u neprofitnoj organizaciji Unitary Fund, koja podržava kvantni ekosistem otvorenog koda, a stručnjak je za izgradnju kvantne tehnologije u laboratoriji.

Dr Cassandra Granade radi u grupi Quantum Systems u Microsoftu, i stručnjak je za karakterizaciju kvantnih uređaja.

„Kvantno računarstvo je sledeća velika stvar i dešava se sada. Ova knjiga će vam trebati da započnete igru."

— Clive Harber
Distorted Thinking Ltd.

„Odlična uvodna knjiga o kvantnom računarstvu."

—Dimitri Denisjonok, Fyld

„Praktičan vodič za učenje o kvantnom računarstvu koji će vas pokrenuti za kratko vreme."

— Thomas Heiman,
TechnoGems

„Odličan uvod u kvantno računarstvo sa odličnim aplikacijama!"

—William E. Wheeler,
TekSystems

ISBN: 978-86-7310-581-9

kompjuter biblioteka
osnovana 1986.
www.kombib.rs

MANNING

Naučite kvantno računarstvo uz Python i Q#

SARAH KAISER
CHRISTOPHER GRANADE

MANNING

kompjuter biblioteka

Izdavač:
kompjuter biblioteka

Obalskih radnika 4a, Beograd

Tel: 011/2520272

e-mail: kombib@gmail.com

internet: www.kombib.rs

Urednik: Mihailo J. Šolajić

Za izdavača, direktor:
Mihailo J. Šolajić

Autor: Sarah Kaiser
Christopher Granade

Prevod: Slavica Prudkov

Lektura: Nemanja Lukić

Slog: Zvonko Aleksić

Znak Kompjuter biblioteke:
Miloš Milosavljević

Štampa: „Pekograf“, Zemun

Tiraž: 500

Godina izdanja: 2022.

Broj knjige: 558

Izdanje: Prvo

ISBN: 978-86-7310-581-9

Learn Quantum Computing with
Python and Q#
Sarah Kaiser
Christopher Granade
©2021 by Manning Publications Co.
9781617296130

©2021 by Manning Publications Co. All rights reserved. No part of this book may be reproduced or transmitted in any form or by means, electronic or mechanical, including photocopying, recording or by any information storage retrieval system, without permission from the Publisher.
Autorizovani prevod sa engleskog jezika edicije u izdanju by Manning Publications Co. All rights reserved.

Sva prava zadržana. Nije dozvoljeno da nijedan deo ove knjige bude reprodukovan ili snimljen na bilo koji način ili bilo kojim sredstvom, elektronskim ili mehaničkim, uključujući fotokopiranje, snimanje ili drugi sistem presnimavanja informacija, bez dozvole izdavača.

Zaštitni znaci
Kompjuter Biblioteka i „Manning Publications Co.” su pokušali da u ovoj knjizi razgraniče sve zaštitne oznake od opisnih termina, prateći stil isticanja oznaka velikim slovima.
Autor i izdavač su učinili velike napore u pripremi ove knjige, čiji je sadržaj zasnovan na poslednjem (dostupnom) izdanju softvera. Delovi rukopisa su možda zasnovani na predizdanju softvera dobijenog od strane proizvođača. Autor i izdavač ne daju nikakve garancije u pogledu kompletnosti ili tačnosti navoda iz ove knjige, niti prihvataju ikakvu odgovornost za performanse ili gubitke, odnosno oštećenja nastala kao direktna ili indirektna posledica korišćenja informacija iz ove knjige.

PREDGOVOR

Tokom većeg dela svoje istorije, kvantno računarstvo je bilo polje za fizičare - možda nekoliko njih ima sklonost za kompjuterske nauke, ali ne obavezno. Popularni udžbenik Quantum Computation and Quantum Information, autora Majkla A. Nielsena i Isaka L. Čuanga, i dalje je standardni udžbenik, a napisala su ga dva kvantna fizičara. Naravno, kompjuterski naučnici su oduvek bili tu, ali neki teoretičari ono malo koda što su napisali nose kao orden časti. Ovo je kvantni svet - ja, Kajzer i Granade postali smo punoletni. Lako sam mogao da stisnem pesnicu i viknem novoj grupi učenika: „Kad sam bio vaših godina, nismo pisali kod – gušili smo se u prašini od krede!"

Upoznao sam Chrisa Granadea dok smo bili studenti. Tada smo pisali članke za akademske časopise o fizici, koji su sadržali linije koda i bili smo odbijani jer „to nije fizika". Ali nas to nije obeshrabrilo. I sada, mnogo godina kasnije, ova knjiga za mene predstavlja konačnu potvrdu! Ovo je knjiga koja vas uči svemu što ćete ikada poželeti da znate o kvantnom računarstvu, bez uplitanja fizike – mada, ako zaista želite da znate vezu sa fizikom, Kaiser i Granade nude i to ☺? Tu su i emotikoni ☺!

Od tada sam prešao dug put i mnogo dugujem Granadeu, kao i polju kvantnog računarstva, jer je pokazao mnogima od nas da između „kvantnog" i „računarstva" postoji mnogo više od samih teorema i dokaza. Kajzer me je, takođe, naučio više nego što sam mislio da je potrebno softverskom inženjeru u razvoju kvantne tehnologije. Kaiser i Granade su svoju stručnost pretvorili u reči i linije koda tako da svi mogu imati koristi od toga, pa i ja.

Iako je cilj bio da se napravi „ne-udžbenik", ova knjiga bi svakako mogla da se koristi kao takva na univerzitetskom predavanju kao uvod u premeštanje kvantnog računarstva sa odseka za fiziku u odsek računarstva. Postoji ogromno i rastuće interesovanje za kvantno računarstvo, koje ne dolazi iz oblasti fizike – programeri softvera, operativni menadžeri i finansijski rukovodioci žele da znaju šta je kvantno računarstvo i kako da ga primene. Prošli su dani kvantnog računarstva kao čisto akademske aktivnosti. Ova knjiga služi potrebama rastuće kvantne zajednice.

Iako sam aludirao na sve manji udeo fizičara u oblasti kvantnog računarstva, ne želim da ih odbacim. Iako sam se nekada protivio razvoju softvera, ova knjiga je zaista za svakoga—posebno za one koji su već uključeni u ovu oblast i žele da nauče više o softverskoj strani kvantnog računarstva u poznatom okruženju.

Uključite svoj omiljeni uređivač koda i pripremite se za štampanje („Zdravo kvantni svete!").

Dr CHRIS FERRIE
Vanredni profesor, Centar za kvantni softver i informacije
Sidnej, NSW, Australija

UVOD

Kvantno računarstvo je naša “stvar” već više od 20 godina i vrlo rado koristimo to iskustvo da pomognemo da što više ljudi prigrli kvantne tehnologije. Zajedno smo završili doktorske studije, dok su nas mučila istraživačka pitanja, takmičenja u igrama reči i društvenim igrama, što nam je pomoglo da pomerimo granice mogućnosti kubita. Uglavnom, to je značilo razvoj novog softvera i alata koji će nama i našim timovima pomoći da radimo bolje istraživanje, što je bio odličan most između „kvantnog“ i „računarskog“ dela predmeta. Međutim, dok smo razvijali različite softverske projekte, morali smo da podučavamo i informišemo naše kolege programere na čemu radimo. Stalno smo se pitali, „Zašto ne postoji dobra knjiga za kvantno računarstvo koja je tehnička, ali ne i udžbenik?“ Rezultat je pred vama.

Napisali smo knjigu tako da bude dostupna programerima, umesto da je pišemo u stilu udžbenika koji je tipičan za druge knjige o kvantnom računarstvu. Kada smo sami učili kvantno računarstvo, bilo je veoma uzbudljivo, ali i pomalo zastrašujuće. To ne mora da bude tako, jer mnogo toga što teme kvantnog računarstva čini zbunjujućim je način na koji su one predstavljene, a ne sadržaj.

Nažalost, kvantno računarstvo se često opisuje kao „čudno“, „sablasno“ ili nerazumljivo, a istina je da je kvantno računarstvo postalo prilično dobro shvaćeno tokom svoje 35-godišnje istorije. Korišćenjem kombinacije razvoja softvera i matematike možete da izgradite osnovne koncepte koji su vam potrebni da biste razumeli kvantno računarstvo i istražili ovu sjajnu novu oblast.

Naš cilj je da vam ovom knjigom pomognemo da naučite osnove o tehnologiji i opremite se alatima koje možete da koristite za izgradnju kvantnih rešenja u budućnosti. Fokusiramo se na praktično iskustvo u razvoju koda za kvantno računarstvo. U prvom delu, izgradićete sopstveni simulator kvantnog uređaja u Python jeziku; u drugom delu, naučićete da primenite svoje nove veštine u pisanju kvantnih aplikacija pomoću jezika Q# i Quantum Development Kit paketa; a u trećem delu naučićete da implementirate algoritam koji faktoriše cele brojeve eksponencijalno brže od najpoznatijeg konvencionalnog algoritma - i u potpunosti vi to radite, a ovo je vaše kvantno putovanje.

Uključili smo puno praktičnih primena, ali istina je da se tada i vi priključujete! Kvantno računarstvo je na vrhuncu od kog idemo napred i potreban nam je most između ogromne količine podataka o tome šta kvantni računari mogu, a šta ne mogu da urade i problema koje ljudi treba da reše. Izgradnja tog mosta vodi nas od kvantnih algoritama koji omogućavaju istraživanje do kvantnih algoritama koji mogu uticati na celo društvo. Možete pomoći u izgradnji tog mosta. Dobrodošli na vaše kvantno putovanje; mi smo tu da vam putovanje učinimo zabavnim!

PRIZNANJA

Na početku nismo znali u šta se upuštamo sa ovom knjigom; sve što smo znali je da mora da postoji resurs kao što je ovaj. Pisanje knjige nam je dalo ogromnu priliku da usavršimo i razvijemo svoje veštine u objašnjavanju i podučavanju sadržaja koji nam je bio poznat. Svi ljudi sa kojima smo radili u Mening izdavačkoj kući bili su divni — Deirdre Hiam, urednik produkcije; Tiffani Tailor, editor; Katie Tennant, lektor i Ivan Martinović, recenzent — i oni su nam pomogli da budemo sigurni da je ovo najbolja knjiga za naše čitaoce.

Zahvaljujemo Oliviji Di Mateo i Krisu Feriju na vrednim povratnim informacijama i beleškama, koje su nam pomogle da naša objašnjenja budu tačna i jasna.

Takođe zahvaljujemo svim recenzentima rukopisa koji su ga pregledali u različitim fazama razvoja i čije su promišljene povratne informacije učinile ovu knjigu mnogo boljom: Alain Couniot, Clive Harber, David Raymond, Debmalya Jash, Dimitri Denisjonok, Domingo Salazar, Emmanuel Medina Lopez , Geoff Clark, Havier, Karthikeyarajan Rajendran, Krzysztof Kamiczek, Kumar Unnikrishnan, Paskuale Zirpoli, Patrick Regan, Paul Otto, Raffaella Ventaglio, Ronald Tischliar, Sander Zegveld, Steve Sussman, Tom Heiman, Tuan A. Tran, Walter Alexander Mata Lopez i William E. Wheeler.

Zahvaljujemo svim pretplatnicima Manning Early Access Programa (MEAP) koji su pomogli da se pronađu bagovi, greške u kucanju i da se poboljšaju objašnjenja. Mnogi ljudi su takođe dali povratne informacije prijavljivanjem problema na našem primeru koda: zahvaljujemo im!

Želeli bismo da zahvalimo mnogim sjajnim ustanovama širom oblasti Sijetla (posebno Caffe Ladro, Miir, Milstead & Co. i Downpour Coffee Bar) gde smo pili kafu za kafom i živahno pričali o kubitima, kao i divnim ljudima iz Fremont Brewinga, koji su uvek bili tu kada bi nam trebalo piće. Uvek je bio dobrodošao prekid kada bi nas slučajni prolaznik pitao o tome na čemu radimo!

Takođe bismo želeli da zahvalimo talentovanim članovima tima Quantum Systems u Microsoftu što rade na tome da programerima pruže najbolje moguće alate za uključivanje u kvantno računarstvo. Posebno zahvaljujemo Betini Hajm što radi na tome da Q# postane neverovatan jezik, a ona je takođe i dobar prijatelj.

Na kraju, zahvaljujemo našem nemačkom ovčaru, Čuviju, koji nam je pružao preko potrebne smetnje i izgovore za pauze.

SARAH KAISER

Moja porodica je uvek bila uz mene i zahvaljujem im na svom strpljenju i ohrabrivanju dok sam radila na ovom projektu. Želela bih da zahvalim svom terapeutu bez kojeg ova knjiga nikada ne bi nastala. Najviše od svega želim da zahvalim svom koautoru i partneru, Krisu. Bili su uz mene i uvek me hrabrili i inspirisali da uradim ono što su znali da mogu.

CHRIS GRANADE

Ova knjiga ne bi bila moguća bez neverovatne ljubavi i podrške mog partnera i koautora, dr Sare Kajzer. Zajedno smo prošli mnogo i postigli više nego što sam ikad sanjao. Naša zajednička priča je uvek bila o stvaranju bolje, bezbednije i inkluzivnije kvantne zajednice, a ova knjiga je sjajna prilika da napravimo još jedan korak na tom putu. Sara, hvala ti što si ovo omogućila.

Ovo ne bi bilo moguće ni bez podrške moje porodice i prijatelja. Hvala vam što ste bili uz mene, bilo da delite fotografije slatkih štenaca, saosećate zbog najnovijih naslova ili se pridružujete kasnonoćnom posmatranju meteora u Animal Crossingu. Na kraju, takođe zahvaljujem fantastičnoj onlajn zajednici na koju sam se godinama oslanjao da mi pomogne da razumem svet iz mnogih, novih perspektiva.

O OVOJ KNJIZI

Dobrodošli u Naučite kvantno računarstvo uz Python i Q#! Ova knjiga će vas uvesti u svet kvantnog računarstva pomoću Pythona kao početne tačke, nadograđujući se na rešenja napisana u jeziku Q#, programskom jeziku specifičnom za domen, koji je razvio Microsoft. Za podučavanje o kvantnom računarstvu i konceptima razvoja koristimo pristup zasnovan na primerima i igrama, koji vam omogućavaju da odmah počnete da pišete kod.

DUBOKO RONJENJE: U REDU JE RONITI S MASKOM!

Kvantno računarstvo je bogata interdisciplinarna oblast proučavanja, koja okuplja ideje iz programiranja, fizike, matematike, inženjerstva i računarstva. S vremena na vreme, odvojićemo trenutak da ukažemo na to kako kvantno računarstvo koristi ideje iz ovih drugih oblasti da bismo koncepte o kojima učimo stavili u taj bogatiji kontekst.
Iako je cilj ovih odstupanja da izazovu radoznalost i dalja istraživanja, ona su po prirodi tangencijalna. Uz ovu knjigu dobićete sve što vam je potrebno za uživanje u kvantnom programiranju u Python i Q# jezicima bez obzira na to da li uranjate i u druge oblasti. Duboko ronjenje bez maske može biti zabavno i prosvetljujuće, ali ako to ne želite, i to je u redu; savršeno je u redu i ronjenje s maskom.

Ko bi trebalo da čita ovu knjigu

Ova knjiga je namenjena ljudima koji su zainteresovani za kvantno računarstvo i koji imaju malo ili nimalo iskustva sa kvantnom mehanikom, ali imaju znanje o programiranju. Dok učite da pišete kvantne simulatore u jeziku Python i kvantne programe u jeziku Q#, specijalizovanom jeziku kompanije Microsoft za kvantno računarstvo, koristimo tradicionalne ideje i tehnike programiranja da vam pomognemo. Opšte razumevanje koncepta programiranja, kao što su petlje, funkcije i dodeljivanje promenljivih, biće od pomoći.

Slično tome, koristimo neke matematičke koncepte iz linearne algebre, kao što su vektori i matrice, da nam pomognu da opišemo kvantne koncepte; ako ste upoznati sa kompjuterskom grafikom ili mašinskim učenjem, mnogi koncepti su slični. Mi koristimo Python da bismo usput pregledali najvažnije matematičke koncepte, ali će poznavanje linearne algebre biti od pomoći.

Kako je ova knjiga organizovana: mapa puta

Ovaj tekst ima za cilj da vam omogući da počnete da istražujete i koristite praktične alate za kvantno računarstvo. Knjiga je podeljena na tri dela koji se nadovezuju jedan na drugi:

- U prvom delu pažljivo predstavljamo koncepte potrebne za opisivanje kubita, osnovne jedinice kvantnog računara. U ovom delu je opisano kako da simulirate kubite u jeziku Python, što olakšava pisanje jednostavnih kvantnih programa.
- U drugom delu opisano je kako da koristite Quantum Development Kit i Q# programski jezik za sastavljanje kubita i pokretanje kvantnih algoritama koji se razlikuju od svih poznatih klasičnih algoritama.
- U trećem delu primenjujemo alate i metode iz prethodna dva dela da biste naučili kako se kvantni računari mogu primeniti na probleme u stvarnom svetu, kao što je simulacija hemijskih svojstava.

Tu su i četiri dodatka. Dodatak A sadrži sva uputstva za instalaciju i podešavanje alata koje koristimo u knjizi. Dodatak B sadrži brze reference sa kvantnim pojmovnikom, podsetnicima za notaciju i isečcima koda koji mogu biti od pomoći dok napredujete kroz knjigu. Dodatak C predstavlja podsetnik linearne algebre, a dodatak D je duboko uranjanje u jedan od algoritama koje ćete implementirati.

O kodu

Sav kod koji je upotrebljen u ovoj knjizi možete naći na adresi https://github.com/crazy4pi314/learn-qc-with-python-and-qsharp. Kompletna uputstva za instalaciju su dostupna u skladištu za ovu knjigu i u dodatku A.

Primeri iz knjige takođe mogu da budu pokrenuti online bez instaliranja, korišćenjem servisa mybinder.org. Da biste počeli rad otvorite stranicu https://bit.ly/qsharp-book-binder.

Forum za diskusiju liveBook

Kupovinom knjige Naučite kvantno računarstvo uz Python i Q# dobijate besplatan pristup privatnom veb forumu koji vodi Manning Publications, gde možete da komentarišete knjigu, postavljate tehnička pitanja i dobijate pomoć od autora i drugih korisnika. Da biste pristupili forumu, otvorite stranicu https://livebook.manning.com/#!/book/learn-quantum-computing-with-python-and-q-sharp/discussion. Takođe, možete saznati više o Meningovim forumima i pravilima ponašanja na stranici https://livebook.manning.com/#!/discussion.

Meningova posvećenost čitaocima ogleda se u potrebi da se obezbedi mesto gde se može održavati smislen dijalog između pojedinaca i između čitalaca i autora. Ovde se ne radi o obavezi autora za učešće u forumu, njihov doprinos forumu ostaje dobrovoljan (i neplaćen). Predlažemo da pokušate da im postavite neka izazovna pitanja! Forum i arhiva prethodnih diskusija biće dostupni sa veb stranice izdavača sve dok je knjiga u štampi.

Drugi onlajn resursi

Kada počnete svoje putovanje u kvantno računarstvo čitanjem ove knjige i radom na datim primerima koda, sledeći resursi vam mogu biti od pomoći:

- Dokumentacija za Quantum Development Kit (https://docs.microsoft.com/azure/quantum/) — Konceptualna dokumentacija i potpuna referenca za sve o jeziku Q#, uključujući izmene i dodatke od štampanja ove knjige
- Primeri za Quantum Development Kit (https://github.com/microsoft/quantum) – Kompletni primeri za korišćenje jezika Q#, kako samostalno tako i sa host programima u jezicima Python i .NET, koji pokrivaju širok spektar različitih aplikacija
- QuTiP.org (http://qutip.org) – Potpun korisnički vodič za QuTiP paket koji smo koristili u ovoj knjizi kao pomoć za matematičke zadatke

Postoje i neke sjajne zajednice za stručnjake za kvantno računarstvo, kao i za početnike. Pridruživanje zajednici kvantnog razvoja, kao što su sledeće, može pomoći u rešavanju pitanja koja imate na tom putu, a takođe će vam omogućiti da pomognete drugima na njihovim putovanjima:

- qsharp.community (https://qsharp.community)—Zajednica Q# korisnika i programera, zajedno sa sobama za ćaskanje, blogovima i repozitorijumima projekata
- Quantum Computing Stack Exchange (https://quantumcomputing.stackekchange.com/) — Odlično mesto za traženje odgovora na pitanja o kvantnom računarstvu, uključujući sva pitanja u vezi sa jezikom Q# koja možda imate
- Women in Quantum Computing and Applications (https://wiqca.dev) — Inkluzivna zajednica za ljude svih polova o kvantnom računarstvu i za ljude koji to omogućavaju
- Quantum Open Source Foundation (https://qosf.org/) — Zajednica koja podržava razvoj i standardizaciju otvorenih alata za kvantno računarstvo
- UnitaryFund (https://unitary.fund/) — neprofitna organizacija koja radi na stvaranju ekosistema kvantne tehnologije koji je koristan većini ljudi

Više od toga

Kvantno računarstvo je fascinantna nova oblast koja nudi nove načine razmišljanja o računarstvu i nove alate za rešavanje teških problema. Ova knjiga vam može pomoći da počnete rad sa kvantnim računarstvom kako biste mogli da nastavite da ga istražujete i učite. Ipak, ova knjiga nije udžbenik i nije namenjena da vas pripremi za istraživanje kvantnog računarstva. Kao i kod klasičnih algoritama, razvoj novih kvantnih algoritama je matematička umetnost kao i bilo šta drugo; dok se u ovoj knjizi dotičemo matematike i koristimo je za objašnjenje algoritama, dostupni su razni udžbenici koji vam mogu pomoći da nadogradite ideje koje opisujemo.

Kada pročitate ovu knjigu i počnete da koristite kvantno računarstvo, pa poželite da nastavite svoje putovanje u fiziku ili matematiku, predlažemo vam jedan od sledećih resursa:

- The Complexity Zoo (https://complexityzoo.net/Complexity_Zoo)
- The Quantum Algorithm Zoo (http://quantumalgorithmzoo.org)

- Complexity Theory: A Modern Approach autora Sanjeeva Arora i Boaza Baraka (Cambridge University Press, 2009)
- Quantum Computing: A Gentle Introduction autora Eleanore G. Rieffel i Volfganga H. Polaka (MIT Press, 2011.)
- Quantum Computing since Democritus autora Skota Aaronsona (Cambridge University Press, 2013)
- Quantum Computation and Quantum Information autora Majkla A. Nielsena i Isaaca L. Chuanga (Cambridge University Press, 2000)
- Quantum Processes Systems, and Information autora Benjamina Schumachera i Majkla Vestmorelanda (Cambridge University Press, 2010)

O AUTORIMA

SARAH KAISER završila je doktorat iz fizike (kvantne informacije) na Institutu za kvantno računarstvo Univerziteta Vaterlo. Veći deo svoje karijere provela je razvijajući novi kvantni hardver u laboratoriji, od izgradnje satelita do hakovanja hardvera za kvantne kriptografije. Objašnjenje onoga što je tako uzbudljivo u vezi s kvantnim računarstvom je njena strast, i voli da kreira nove demonstracije i alate koji će pomoći razvoju kvantne zajednice. Kada nije za svojom mehaničkom tastaturom, voli vožnju kajakom i pisanje knjiga o nauci za sve uzraste.

CHRIS GRANADE završio je doktorat iz fizike (kvantne informacije) na Institutu za kvantno računarstvo Univerziteta Vaterlo i sada radi u timu za kvantne sisteme u Microsoftu. Oni rade na razvoju standardnih biblioteka za Q# i eksperti su za statističku karakterizaciju kvantnih uređaja iz klasičnih podataka. Kris je takođe pomogao Skotu Aronsonu da pripremi svoja predavanja kao knjigu, Quantum Computing Since Democritus (Cambridge University Press, 2013).

O ILUSTRACIJI NASLOVNE STRANICE

Figura na naslovnoj strani knjige *Naučite kvantno računarstvo uz Python i Q#* ima natpis „Hongroise“, ili Mađarica. Ilustracija je preuzeta iz knjige kolekcija kostima iz raznih zemalja autora Žaka Grasea de Sen Sovera (1757–1810), pod nazivom Costumes de Differents Pays, objavljene u Francuskoj 1797. godine. Svaka ilustracija je fino nacrtana i ručno obojena. Bogat izbor kolekcije Grasseta de Saint-Sauveura nas živo podseća na to koliko su gradovi i regioni sveta bili kulturno odvojeni pre samo 200 godina.

Izolovani jedni od drugih, ljudi su govorili različitim dijalektima i jezicima. Na ulicama ili na selu bilo je lako prepoznati gde žive i šta je njihov zanat ili položaj, samo po njihovoj odeći. Način na koji se oblačimo se od tada promenio, a raznolikost regiona, tako bogata u to vreme, je nestala. Sada je teško razlikovati stanovnike različitih kontinenata, a kamoli različitih gradova, regiona ili zemalja. Možda smo zamenili kulturnu raznolikost za raznovrsniji lični život - svakako za raznovrsniji tehnološki život koji se veoma brzo razvija.

U vreme kada je teško razlikovati jednu kompjutersku knjigu od druge, Mening slavi inventivnost i inicijativu kompjuterskog poslovanja koricama knjiga zasnovanim na bogatoj raznolikosti regionalnog života od pre dva veka, koji su oživele Graset de Sen-Sauveurove slike.

DEO 1

POČETAK RADA U OBLASTI KVANTNOG RAČUNARSTVA

U ovom delu knjige vam pomažemo da postavite pozornicu za ostatak našeg kvantnog putovanja. U prvom poglavlju dobijamo više konteksta o kvantnom računarstvu, pristupu učenju kvantnog računarstva u ovoj knjizi i možemo očekivati da ćemo stečeno znanje koristiti za primenu veština koje učimo. U poglavlju 2 počinjemo pisanje koda razvijajući kvantni simulator u jeziku Python. Zatim, koristimo simulator da programiramo kvantni generator slučajnih brojeva. Zatim, u poglavlju 3, proširujemo simulator na programiranje kriptografskih aplikacija kvantne tehnologije, kao što je BB84 kvantni protokol za razmenu ključeva. U 4. poglavlju koristimo nelokalne igre da bismo učili o uplitanju i još jednom proširili simulator tako da podrži više kubita. U poglavlju 5 učimo kako da koristimo novi Python paket da bismo pomogli u implementaciji kvantnih strategija za igranje nelokalnih igara iz poglavlja 4. Konačno, u poglavlju 6, poslednji put proširujemo simulator dodavanjem novih kvantnih operacija tako da možemo da simuliramo tehnike, kao što je kvantna teleportacija (eng. quantum teleportation) i vežbamo pomeranje podataka u našim kvantnim uređajima.

1 PREDSTAVLJANJE KVANTNOG RAČUNARSTVA

Ovim poglavljem obuhvaćene su sledeće teme:

- Zašto su ljudi uzbuđeni zbog kvantnog računarstva
- -Šta je kvantni računar
- -Šta kvantni računar može, a šta ne može
- -Kakav je odnos kvantnih računara i klasičnog programiranja

Kvantno računarstvo je sve popularnija oblast istraživanja u poslednjih nekoliko godina. Korišćenjem kvantne fizike za obavljanje izračunavanja na nove i divne načine, *kvantni računari (eng. quantum computers)* mogu da utiču na društvo, čineći ga uzbudljivim tako da ćete poželeti da se uključite i naučite da programirate kvantne računare i primenjujete kvantne resurse za rešavanje važnih problema.

Međutim, u svoj toj priči o prednostima koje nudi kvantno računarstvo, lako je izgubiti iz vida *pravi* obim tih prednosti. Imamo zanimljiv istorijski presedan za ono što se može dogoditi kada obećanja o tehnologiji nadmaše stvarnost. Tokom 1970-ih godina, mašinsko učenje i veštačka inteligencija su patili od dramatično smanjenog finansiranja, pošto su pompa i uzbuđenje oko veštačke inteligencije nadmašili njene rezultate; to je kasnije nazvano „AI zima“. Slično tome, internet kompanije su se suočile sa istom opasnošću kada su pokušavale da prevaziđu krah dot-com-a.

Jedan od načina napretka je da se kritički shvati obećanje koje nudi kvantno računarstvo, kako funkcionišu kvantni računari i šta jeste, a šta nije, u domenu kvantnog računarstva. U ovom poglavlju vam pomažemo da razvijete to razumevanje da biste mogli da steknete praksu i da napišete sopstvene kvantne programe, u ostatku knjige.

Ipak, zaista je super učiti o potpuno novom računarskom modelu! Dok budete čitali ovu knjigu, naučićete kako kvantni računari funkcionišu tako što ćete programirati simulacije koje danas možete da pokrenete na svom laptopu. Ove simulacije će pokazati mnoge bitne elemente onoga što očekujemo da će biti stvarno komercijalno kvantno programiranje dok se na internetu pojavljuje koristan komercijalni hardver. Ova knjiga je namenjena ljudima koji imaju osnovno iskustvo u programiranju i linearnoj algebri, ali nemaju prethodno znanje o kvantnoj fizici ili računarstvu. Ako ste upoznati sa kvantnim pitanjima, možete preći na delove 2 i 3, gde prelazima na kvantno programiranje i algoritme.

1.1 Zašto je kvantno računarstvo važno?

Računarska tehnologija napreduje zaista zapanjujućim tempom. Pre tri decenije, 80486 procesor je omogućio korisnicima da izvrše 50 MIPS (milion instrukcija u sekundi). Danas mali računari kao što je Raspberry Pi mogu dostići 5.000 MIPS, dok desktop procesori lako mogu dostići 50.000 do 300.000 MIPS. Ako imamo izuzetno težak računarski problem koji želimo da rešimo, veoma razumna strategija je da jednostavno sačekamo sledeću generaciju procesora da nam olakša život, da naši video snimci budu brži, a naše igre šarenije.

Međutim, za mnoge probleme do kojih nam je stalo, nismo te sreće. Možda se nadamo da će nam duplo brži CPU omogućiti da rešimo dvostuko teže probleme, ali kao i sa toliko toga u životu, „više je drugačije“. Pretpostavimo da sortiramo listu od 10 miliona brojeva i otkrivamo da je za to potrebno oko 1 sekunde. Kasnije, ako želimo da sortiramo listu od 1 milijarde brojeva za 1 sekundu, biće nam potreban CPU koji je 130 puta brži, a ne samo 100 puta. Kada rešavamo neke vrste problema, to postaje još gore: za neke grafičke probleme, prelazak sa 10 miliona na milijardu tačaka bi trajao 13.000 puta duže.

Problemi koji su veoma različiti, kao što su usmeravanje saobraćaja u gradu i predviđanje hemijskih reakcija, mnogo brže postaju sve teži. Da je kvantno računarstvo u stvari stvaranje računara koji radi 1000 puta brže, jedva bismo nešto postigli u zastrašujućim izazovima koje želimo da rešimo. Na sreću, kvantni računari su *mnogo* zanimljiviji. Očekujemo da će kvantni računari biti mnogo *sporiji* nego klasični računari, ali da će se resursi potrebni za rešavanje mnogih problema *skalirati* drugačije, tako da ako pogledamo prave vrste problema, možemo probiti shvatanje „više je drugačije“. U isto vreme, kvantni računari nisu magični metak — neki problemi će ostati teški. Na primer, iako je verovatno da nam kvantni računari mogu izuzetno pomoći u predviđanju hemijskih reakcija, oni možda neće biti od velike pomoći kod drugih teških problema.

Istraživanje o kojim tačno problemima možemo dobiti takvu prednost i razvoj kvantnih algoritama za to bio je glavni fokus istraživanja kvantnog računarstva. Do sada je bilo veoma teško proceniti kvantne pristupe na ovaj način, jer je to zahtevalo opsežne matematičke veštine za pisanje kvantnih algoritama i razumevanje svih suptilnosti kvantne mehanike.

Međutim, kako je industrija počela da razvija platforme koje pomažu programerima da se povežu sa kvantnim računarstvom, ova situacija je počela da se menja. Koristeći ceo Microsoftov Quantum Development Kit možemo da apstrahujemo većinu matematičke složenosti kvantnog računarstva i da počnemo zapravo da *razumemo* i *koristimo* kvantne računare. Alati i tehnike o kojima ćete učiti u ovoj knjizi omogućavaju programerima da istraže i razumeju kakvo će zapravo biti pisanje programa za ovu novu hardversku platformu.

Drugačije rečeno, kvantno računarstvo ne nestaje, tako da je razumevanje koje probleme možemo rešiti njime zaista veoma važno! Nezavisno od toga da li će se kvantna „revolucija" desiti, kvantno računarstvo je uticalo – i nastaviće da utiče – u velikoj meri na odluke o tome kako razvijati računarske resurse u narednih nekoliko decenija. Kvantno računarstvo utiče u velikoj meri na sledeće odluke:

- Koje su pretpostavke razumne u informacionoj bezbednosti?
- Koje veštine su korisne u studijskim programima?
- Kako možemo da procenimo tržište računarskih rešenja?

Mi koji radimo u tehnologiji ili srodnim oblastima, sve više moramo da donosimo takve odluke ili da dajemo doprinos za njih. Imamo odgovornost da razumemo šta je kvantno računarstvo i, što je možda još važnije, šta nije. Na taj način ćemo biti najbolje pripremljeni da se uključimo i doprinesemo ovim novim naporima i odlukama.

Još jedan razlog zašto je kvantno računarstvo tako fascinantna tema je to što je i slično klasičnom računarstvu i veoma različito od njega. Razumevanje sličnosti i razlika između klasičnog i kvantnog računarstva pomaže nam da razumemo šta je fundamentalno u računarstvu uopšte. I klasično i kvantno računarstvo proizilaze iz različitih opisa fizičkih zakona, tako da nam razumevanje proračuna može pomoći da razumemo univerzum na nov način.

Međutim, ono što je apsolutno važno je da ne postoji nijedan pravi ili čak najbolji razlog da budete zainteresovani za kvantno računarstvo. Šta god da vas dovede do istraživanja ili primene kvantnog računarstva, usput ćete naučiti nešto zanimljivo.

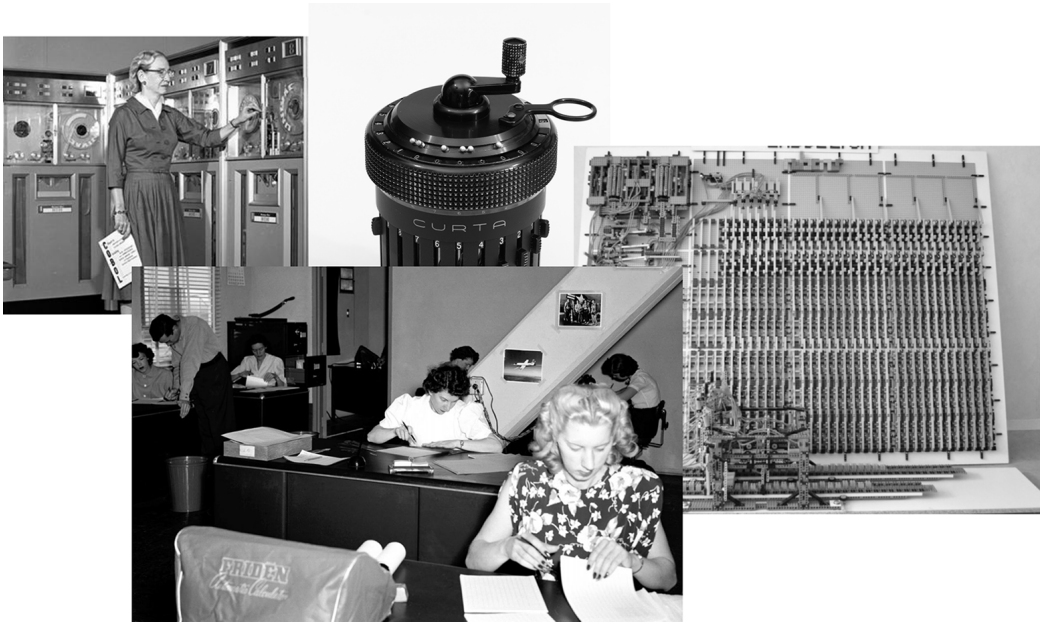
1.2 Šta je kvantni računar?

Hajde da razgovaramo malo o tome šta zapravo čini kvantni računar. Da bismo olakšali ovu diskusiju, ukratko ćemo govoriti o tome šta znači pojam *računar*.

DEFINICIJA *Računar* je uređaj koji koristi podatke kao ulaz i vrši neku vrstu operacija na tim podacima.

Postoji mnogo primera onoga što smo nazivali *računar*; pogledajte sliku 1.1 za neke primere.

Svima njima je zajedničko to što možemo da ih modelujemo pomoću klasične fizike – odnosno, u smislu Njutnovih zakona kretanja, Njutnove gravitacije i elektromagnetizma.



Slika 1.1 Nekoliko primera različitih vrsta računara, uključujući UNIVAC mainframe kojim upravlja Rear Admiral Hopper, prostoriju „ljudskih računara" koji rade na rešavanju proračuna leta, mehanički kalkulator i LEGO-baziranu Tjuringovu mašinu. Svaki računar možemo opisati istim matematičkim modelom kao i računare kao što su mobilni telefoni, laptopovi i serveri. Izvori: Fotografija „ljudskih kompjutera" od NASA-e. Fotografija LEGO Tjuringove mašine od Projet Rubensa, koja se koristi pod CC By 3.0 (https://creativecommons.org/licenses/by/3.0/).

Ovo će nam pomoći da razlikujemo vrste računara na koje smo navikli (npr. laptopove, telefone, mašine za hleb, kuće, automobile i pejsmejkere) i računare o kojima učimo u ovoj knjizi. Da bismo ih razlikovali, računare koji se mogu opisati pomoću klasične fizike nazvaćemo *klasični računari*. Ono što je dobro u vezi sa tim je da ako zamenimo termin *klasična fizika* terminom *kvantna fizika*, imamo sjajnu definiciju šta je kvantni računar!

DEFINICIJA *Kvantni računarje* uređaj koji koristi podatke kao ulaz i vrši neku vrstu operacija na tim podacima procesom koji može da bude opisan samo pomoću kvantne fizike.

Drugačije rečeno, razlika između klasičnih i kvantnih računara je upravo razlika između klasične i kvantne fizike. O tome ćemo detaljnije govoriti kasnije u knjizi. Ali primarna razlika je u razmerama: naše svakodnevno iskustvo se uglavnom odnosi na objekte koji su dovoljno veliki i dovoljno vrući da, iako kvantni efekti i dalje postoje, u proseku ne rade mnogo. Dok kvantna mehanika funkcioniše čak i na nivou svakodnevnih predmeta kao što su šolje za kafu, kese brašna i bejzbol palice, ispostavilo se da možemo vrlo dobro da opišemo kako ovi objekti komuniciraju međusobno korišćenjem samo klasične fizike.

Detaljnije: Šta se desilo sa relativnošću?

Kvantna fizika se primenjuje na objekte koji su veoma mali i veoma hladni ili dobro izolovani. Slično, druga grana fizike je relativnost (eng. relativity) i opisuje objekte koji su dovoljno veliki da gravitacija igra važnu ulogu ili koji se kreću veoma brzo — blizu brzini svetlosti. Mnogi računari se oslanjaju na relativističke efekte; zaista, globalni sateliti za pozicioniranje zavise od relativnosti. Do sada smo prvenstveno upoređivali klasičnu i kvantnu fiziku, pa šta je sa relativnošću?

Kako se ispostavilo, sva računanja koja su implementirana korišćenjem relativističkih efekata mogu se opisati i korišćenjem čisto klasičnih modela računarstva, kao što su Tjuringove mašine. Nasuprot tome, kvantno računanje ne možemo opisati kao brže klasično računanje, već to zahteva drugačiji matematički model. Još uvek nije bilo predloga za „gravitacioni kompjuter" koji koristi relativnost na isti način, tako da možemo sa sigurnošću da ostavimo relativnost po strani u ovoj knjizi.

Ako se fokusiramo na mnogo manji obim gde je kvantna mehanika potrebna da opišemo naše sisteme, onda je kvantno računarstvo umetnost korišćenja malih, dobro izolovanih uređaja za korisnu transformaciju podataka na načine koji ne mogu da budu opisani samo terminima klasične fizike. Jedan od načina za kreiranje kvantnih uređaja je korišćenje malih klasičnih računara kao što su digitalni procesori signala (digital signal processor - DSP) za kontrolu svojstava egzotičnih materijala.

Fizika i kvantno računarstvo

Egzotični materijali koji se koriste za izgradnju kvantnih računara imaju nazive koji mogu zvučati zastrašujuće, kao što su *superprovodnici (eng. superconductor)* i *topološki izolatori (eng. topological insulator)*. Međutim, možemo se utešiti time kako učimo da razumemo i koristimo klasične računare.

Možemo da programiramo klasične računare, a da ne znamo šta je poluprovodnik. Slično tome, fizika koja stoji iza toga kako gradimo kvantne računare je fascinantna tema, ali nije potrebna da bismo učili da programiramo i koristimo kvantne uređaje.

Kvantni uređaji se mogu razlikovati u detaljima načina na koji se kontrolišu, ali na kraju svi kvantni uređaji se kontrolišu i čitaju pomoću klasičnih računara i neke vrste kontrolne elektronike. Na kraju krajeva, nas zanimaju klasični podaci, tako da na kraju mora da postoji interfejs sa klasičnim svetom.

NAPOMENA Većina kvantnih uređaja mora da se čuva na veoma hladnom i dobro izolovanom mestu, jer mogu da budu izuzetno osetljivi na buku.

Primenom kvantnih operacija korišćenjem ugrađenog klasičnog hardvera, možemo da manipulišemo i transformišemo kvantne podatke. Moć kvantnog računarstva tada dolazi iz pažljivog odabira operacija koje će se primeniti da bi se implementirala korisna transformacija koja rešava dati problem.

1.3 Kako ćemo koristiti kvantne računare?

Slika 1.2 Načini na koje bismo želeli da koristimo kvantne računare. Strip se koristi uz dozvolu sajtaxkcd.com.

Važno je razumeti i potencijal i ograničenja kvantnih računara, posebno s obzirom na uzbuđenje oko kvantnog računanja. Mnogi nesporazumi koji su u osnovi ove pompe potiču od ekstrapolacije analogija izvan onoga gde one imaju smisla – sve analogije imaju svoje granice, a kvantno računarstvo se po tome ne razlikuje. Simulacija kako kvantni program deluje u praksi može biti odličan način da se pomogne u testiranju i poboljšanju razumevanja koje pružaju analogije. Bez obzira na to, i dalje ćemo koristiti analogije u ovoj knjizi, jer one mogu pomoći u pružanju intuicije o tome kako funkcioniše kvantno računanje.

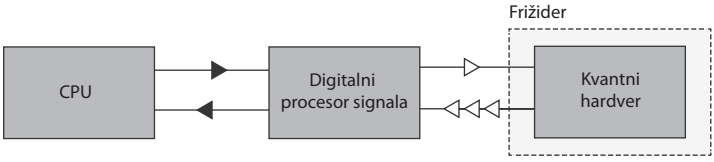
SAVET Ako ste ikada videli opise novih rezultata u kvantnom računarstvu koji glase kao „Možemo teleportovati mačke koje se nalaze na dva mesta istovremeno koristeći moć beskonačnog broja paralelnih univerzuma koji svi zajedno rade na lečenju raka“, onda ste videli opasnost od ekstrapolacije predaleko od mesta gde su analogije korisne.

Jedna posebno uobičajena tačka konfuzije u vezi sa kvantnim računarstvom je kako će korisnici koristiti kvantne računare. Kao društvo, shvatili smo šta je *računar*: nešto što možete da koristite za pokretanje veb aplikacija, pisanje dokumenata i pokretanje simulacija. U stvari, klasični računari rade toliko različitih stvari u našem životu da ne primećujemo uvek šta jeste, a šta nije računar. Cory Doctorow je otkrio to primetivši da je „Vaš auto računar u kome sedite“ (DrupalCon Amsterdam 2014 keynote, www.youtube.com/watch?v=iaf3Sl2r3jE).

Međutim, kvantni računari će verovatno biti više namenski – očekujemo da će kvantni računari biti besmisleni za neke zadatke. Odličan model za to kako će se kvantno računarstvo uklopiti u naš postojeći klasični računarski stek su GPU-ovi. GPU-ovi su specijalizovani hardverski uređaji dizajnirani da ubrzaju određene vrste proračuna kao što su grafičko crtanje, zadaci mašinskog učenja i bilo šta što se lako paralelizuje. Želite GPU za te specifične zadatke, ali verovatno ne želite da ga koristite za sve, jer imamo mnogo fleksibilnije procesore za opšte zadatke, kao što je provera e-pošte. Kvantni računari će biti potpuno isti: biće dobri u ubrzavanju određenih vrsta zadataka, ali neće biti prikladni za široku upotrebu.

NAPOMENA Programiranje kvantnog računara dolazi sa određenim ograničenjima, tako da će klasični računari biti poželjniji kada ne postoji određena kvantna prednost.

Klasično računarstvo će i dalje postojati i biće primaran način na koji komuniciramo jedni sa drugima, kao i sa našim kvantnim hardverom. Čak i da bi se klasični računarski resursi povezivali sa kvantnim uređajima, u većini slučajeva biće nam potreban i digitalno-analogni procesor signala, kao što je prikazano na slici 1.3.



Slika 1.3 Primer načina na koji kvantni uređaj može da stupi u interakciju sa klasičnim računarom pomoću digitalnog procesora signala (DSP). DSP šalje signale male snage u kvantni uređaj i pojačava slabe signale koji se vraćaju u uređaj.

Štaviše, kvantna fizika opisuje stvari u veoma malim razmerama (i veličine i energiju) koje su dobro izolovane od svog okruženja. Ovo postavlja neka teška ograničenja na okruženja u kojima možemo da pokrenemo kvantni računar. Jedno moguće rešenje je da se kvantni uređaji drže u kriogenim frižiderima, često blizu apsolutnih 0 K (–459,67°F ili –273,15°C). Iako to nije problem sprovesti u data centru, održavanje frižidera za razhlađivanje nije nešto što ima smisla na desktopu, a još manje na laptopu ili mobilnom telefonu. Iz tog razloga, kvantni računari će se verovatno koristiti kroz cloud, barem neko vreme nakon što postanu komercijalno dostupni.

Korišćenje kvantnih računara kao cloud servisa liči na druge napretke u specijalizovanom računarskom hardveru. Centralizacijom egzotičnih računarskih resursa, kao što su sledeći, u centrima podataka, moguće je istražiti računarske modele koje je teško primeniti na lokalnom nivou za sve osim najvećih korisnika:

- Specijalizovan hardver za igre (PlayStation Now, Xbox One)
- Klasteri računara visokih performansi (npr. Infiniband) sa izuzetno malim kašnjenjem za naučne probleme
- Masivni GPU klasteri
- Reprogramabilni hardver (npr. Catapult/Brainwave)

- Klasteri Tensor processing unit (TPU)
- Arhivsko skladištenje visoke performanse sa velikim kašnjenjem (npr. Amazon Glacier)

Ubuduće, cloud servisi kao što je Azure Quantum (https://azure.com/quantum) učiniće moć kvantnog računarstva dostupnom na skoro isti način.

Baš kao što su internet veze velike brzine i velike dostupnosti učinile cloud računarstvo dostupnim velikom broju korisnika, moći ćemo da koristimo kvantne računare udobno smešteni na omiljenoj plaži ili kafiću sa dobrom WiFi konekcijom ili čak u vozu dok uživamo u pogledu na veličanstvene planinske lance u daljini.

1.3.1 Šta mogu da urade kvantni računari?

Kao kvantni programeri, ako imamo određeni problem, *kako znamo da ima smisla to rešavati kvantnim računarom*?

Još uvek učimo o tome za šta su kvantni računari sposobni, i stoga još uvek nemamo nikakva konkretna pravila za odgovor na ovo pitanje. Do sada smo pronašli neke primere problema u kojima kvantni računari nude značajne prednosti u odnosu na najpoznatije klasične pristupe. U svakom slučaju, kvantni algoritmi, za koje je utvrđeno da rešavaju ove probleme, koriste kvantne efekte da bi postigli prednosti, koje ponekad nazivamo *kvantna prednost (eng. quantum advantage)*. Slede dva korisna kvantna algoritma:

- Groverov algoritam (opisan u poglavlju 11) pretražuje listu N stavki u $\sqrt{N}$ koracima.
- Šorov algoritam (poglavlje 12) brzo faktoriše velike cele brojeve, kao što su oni koje koristi kriptografija za zaštitu privatnih podataka.

Videćemo još nekoliko algoritama u ovoj knjizi, ali Groverov i Šorov primer su dobri primeri kako funkcionišu kvantni algoritmi: svaki koristi kvantne efekte da odvoji tačne odgovore na računarske probleme od nevažećih rešenja. Jedan od načina da se ostvari kvantna prednost je pronalaženje načina korišćenja kvantnih efekata za razdvajanje tačnih i netačnih rešenja klasičnih problema.

Koje su kvantne prednosti?

Groverov i Šorov algoritam ilustruju dve različite vrste kvantnih prednosti. Faktorisanje celih brojeva na klasičan način bi moglo da bude jednostavnije nego što pretpostavljamo. Mnogi ljudi su se veoma trudili da brzo faktorišu cele brojeve i nisu uspeli u tome, ali to ne znači da možemo da dokažemo da je faktorisanje teško. S druge strane, možemo dokazati da je Groverov algoritam brži od bilo kog klasičnog algoritma; caka je u tome što koristi drugačiju vrstu ulaza.

Pronalaženje *dokazane* prednost za praktičan problem je aktivna oblast istraživanja u kvantnom računarstvu. Međutim, kvantni računari mogu da budu moćan alat za rešavanje problema, čak i ako ne možemo da dokažemo da nikada neće postojati bolji klasičan algoritam. Na kraju krajeva, Šorov algoritam dovodi u pitanje pretpostavke koje leže u osnovi velikog dela informacione bezbednosti — matematički dokaz je neophodan samo zato što još uvek nismo izgradili kvantni računar dovoljno veliki da pokrene Šorov algoritam.

Kvantni računari takođe nude značajne prednosti za simulaciju svojstava kvantnih sistema, omogućavanjem primene za kvantnu hemiju i nauku o materijalima. Na primer, kvantni računari bi mogli da olakšaju učenje o energijama osnovnog stanja hemijskih sistema. Ove energije osnovnog stanja zatim pružaju uvid u brzine reakcije, elektronske konfiguracije, termodinamička svojstva i druga svojstva od ogromnog interesa za hemiju.

Na putu ka razvoju ovih aplikacija, takođe smo videli značajne prednosti u spin-off tehnologijama kao što su kvantna distribucija ključeva i kvantna metrologija, od kojih ćemo neke videti u narednih nekoliko poglavlja. Učeći da kontrolišemo i razumemo kvantne uređaje u svrhu računarstva, takođe smo naučili vredne tehnike za snimanje slika, procenu parametara, bezbednost i još mnogo toga. Iako ovo nisu aplikacije za kvantno računarstvo u strogom smislu, one su veoma vredne za *razmišljanja* u smislu kvantnog proračuna.

Naravno, nove primene kvantnih računara mnogo je lakše otkriti kada imamo konkretno razumevanje funkcionisanja kvantnih algoritama i načina izgradnje novih algoritama na osnovu osnovnih principa. Iz te perspektive, kvantno programiranje je odličan resurs za učenje načina otkrivanja potpuno nove primene.

1.3.2 Šta ne mogu kvantni računari?

Kao i drugi oblici specijalizovanog računarskog hardvera, kvantni računari neće biti dobri u svemu. Za neke probleme, klasični računari će jednostavno biti bolje prilagođeni zadatku. U razvoju aplikacija za kvantne uređaje, korisno je primetiti koji zadaci ili problemi su van okvira kvantnog računarstva.

Kratka verzija je da nemamo nikakva čvrsta i brza pravila da brzo odlučimo koji zadaci se najbolje izvršavaju na klasičnim računarima, a koji zadaci mogu da iskoriste prednosti kvantnih računara. Na primer, zahtevi za skladištenje i propusni opseg za aplikacije Big Data stila veoma je teško mapirati na kvantne uređaje, gde možda imamo samo relativno mali kvantni sistem. Trenutni kvantni računari mogu da snimaju samo ulaze od najviše nekoliko desetina bitova, a ovo ograničenje će postati relevantnije kako se kvantni uređaji budu koristili za zahtevnije zadatke. Iako očekujemo da ćemo na kraju izgraditi mnogo veće kvantne sisteme nego što možemo sada, klasični računari će verovatno uvek biti poželjniji za probleme koji zahtevaju velike količine ulaza/izlaza za rešavanje.

Slično tome, aplikacije za mašinsko učenje koje u velikoj meri zavise od slučajnog pristupa velikim skupovima klasičnih ulaza su konceptualno teško rešive kvantnim računarstvom. Na primer, *možda* postoje druge aplikacije za mašinsko učenje koje se mapiraju mnogo prirodnije na kvantne proračune. Istraživački napori da se pronađu najbolji načini za primenu kvantnih

resursa za rešavanje zadataka mašinskog učenja su još uvek u toku. Generalno, problemi koji imaju male količine ulaznih i izlaznih podataka, ali zahtevaju velike količine proračuna da bi prešli od ulaza do izlaza, dobri su kandidati za kvantne računare.

Uzimajući u obzir ove izazove, moglo bi biti primamljivo zaključiti da su kvantni računari *uvek* izvrsni u zadacima koji imaju male ulaze i izlaze, ali između njih postoje veoma intenzivni proračuni. Pojmovi kao što je *kvantni paralelizam (eng. quantum parallelism),* su popularni u medijima, a kvantni računari se ponekad čak opisuju kao da koriste paralelne univerzume za računanje.

NAPOMENA Koncept „paralelnih univerzuma" je odličan primer analogije koja može pomoći da kvantni koncepti budu razumljivi, ali može dovesti do besmislica kada se dovede do krajnosti. Ponekad može biti korisno razmišljati o različitim delovima kvantnog proračuna kao da se nalaze u različitim univerzumima koji ne mogu da utiču jedni na druge, ali ovaj opis otežava razmišljanje o nekim efektima koje ćemo naučiti u ovoj knjizi, kao što je smetnja. Kada se ode predaleko, analogija paralelnog univerzuma takođe omogućava razmišljanje o kvantnom računarstvu na načine koji su bliži zabavnoj epizodi naučno-fantastične emisije *Zvezdane staze,* nego stvarnosti.

Međutim, što ovo ne može da prenese je da nije uvek očigledno kako koristiti kvantne efekte za izvlačenje korisnih odgovora iz kvantnog uređaja, čak i ako se čini da stanje kvantnog uređaja sadrži željeni izlaz. Na primer, jedan od načina za faktorisanje celog broja N korišćenjem klasičnog računara je da navedete svaki *potencijalni* faktor i proverite da li je to zapravo faktor ili ne:

1. Ako je $i = 2$.
2. Proverite da li je ostatak od N / i nula.
   - Ako jeste, vratite da je i faktor N.
   - Ako ne, povećajte i i ponovite proračun.

Ovaj klasični algoritam možemo ubrzati korišćenjem velikog broja različitih klasičnih računara, po jedan za svaki potencijalni faktor koji želimo da isprobamo. Odnosno, ovaj problem se lako može paralelizovati. Kvantni računar može da isproba svaki potencijalni faktor unutar istog uređaja, ali kako se ispostavilo, to *ipak* nije dovoljno za faktorisanje celih brojeva brže od klasičnog pristupa. Ako koristimo ovaj pristup na kvantnom računaru, izlaz će biti jedan od nasumično odabranih potencijalnih faktora. Stvarni tačni faktori će se pojaviti sa verovatnoćom oko $1/\sqrt{N}$, što nije ništa bolje od klasičnog algoritma.

Međutim, kao što ćemo videti u poglavlju 12, možemo koristiti druge kvantne efekte za faktorisanje celih brojeva pomoću kvantnog računara brže od najpoznatijih klasičnih algoritama za faktorisanje. Veliki deo teškog zadatka koji obavlja Šorov algoritam je da se uveri da je verovatnoća merenja tačnog faktora na kraju mnogo veća od verovatnoće merenja pogrešnog faktora. Poništavanje netačnih odgovora na ovaj način je ono u što se rešava kvantnim programiranjem; to nije lako, ili čak moguće, uraditi za sve probleme koje bismo možda želeli da rešimo.

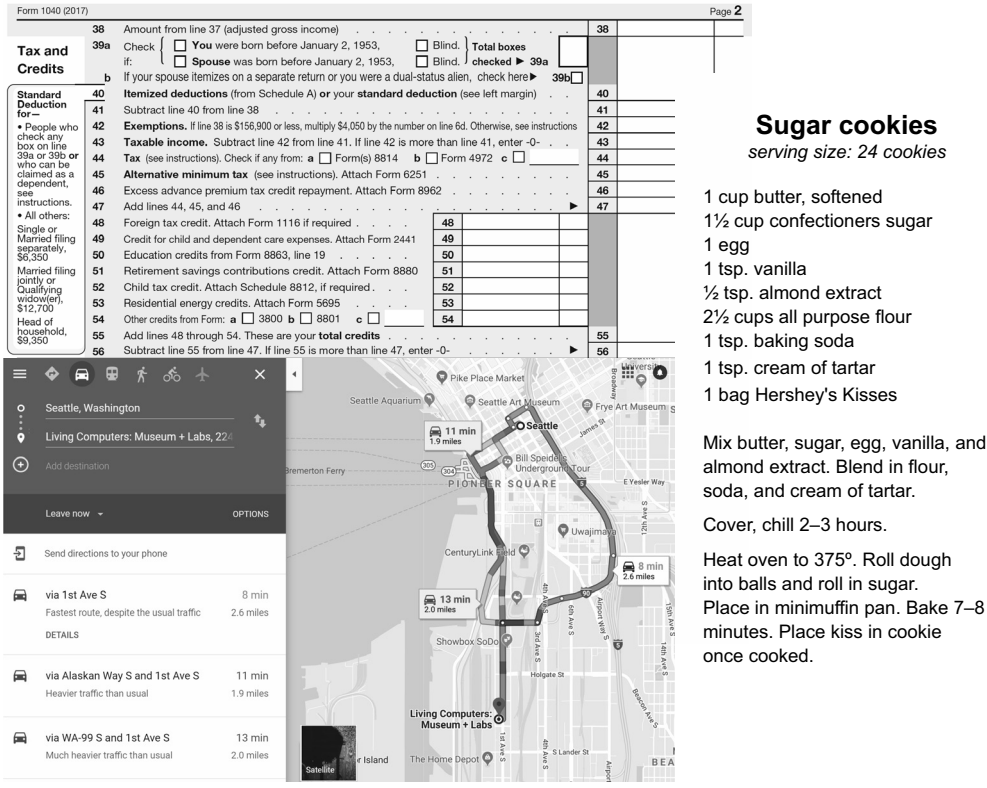
Da bismo konkretnije razumeli šta kvantni računari mogu, a šta ne, i kako da uradite sjajne stvari sa kvantnim računarima uprkos ovim izazovima, korisno je zauzeti konkretniji pristup. Dakle, razmotrimo šta je uopšte kvantni program, da bismo mogli da počnemo da pišemo svoje.

1.4 Šta je program?

U ovoj knjizi često ćemo smatrati korisnim da objasnimo kvantni koncept tako što ćemo prvo ponovo ispitati analogni klasičan koncept. Konkretno, vratimo se korak unazad i ispitajmo šta je klasičan program.

DEFINICIJA *Program* je niz instrukcija koje klasičan računar može da protumači za obavljanje željenog zadatka. Poreski obrasci, uputstva za vožnju, recepti i Python skriptovi su primeri programa.

Možemo da pišemo klasične programe za razdvajanje širokog spektra različitih zadataka za interpretaciju na svim vrstama računara. Pogledajte sliku 1.4 za neke primere programa.



Slika 1.4 Primeri klasičnih programa. Poreski obrasci, uputstva na mapi i recepti su primeri u kojima se niz uputstava tumači klasičnim računarom kao što je osoba. Oni mogu izgledati veoma različito, ali svaki koristi listu koraka za saopštavanje postupka.

Pogledajmo kako bi jednostavan „hello, world“ program mogao da izgleda u Python jeziku:

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

U svom najosnovnijem obliku, ovaj program možemo da posmatramo kao niz instrukcija datih Python *interpreteru*, koji zatim izvršava svaku instrukciju redom da bi postigao neki efekat—u ovom slučaju, to je štampanje poruke na ekranu. Odnosno, program je *opis* zadatka koji Python jezik zatim *tumači* a zatim ga tumači i CPU da bismo postigli svoj cilj. Ova interakcija između opisa i interpretacije motiviše pozivanje jezika Python, C i drugih sličnih programskih alata *jezika*, naglašavajući da je programiranje način na koji komuniciramo sa našim računarima.

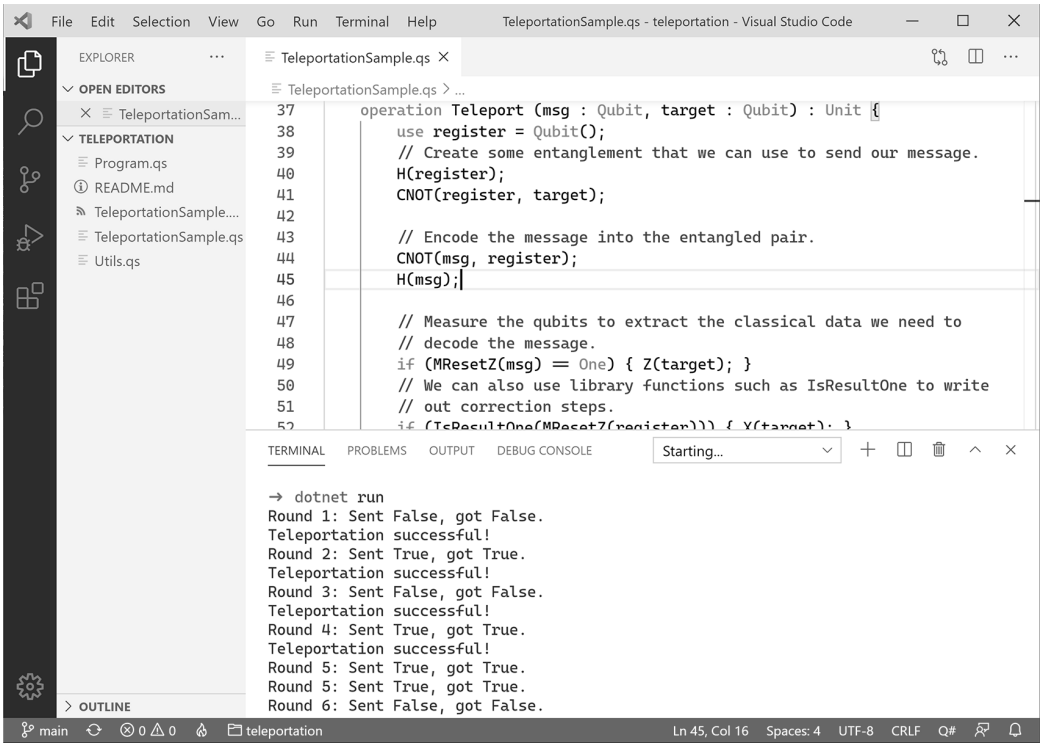
U primeru korišćenja jezika Python za štampanje „Hello, world!“ mi efikasno komuniciramo sa Gvidom van Rosumom, osnivačem jezika Python. Gvido tada efikasno komunicira u naše ime sa dizajnerima operativnog sistema koji koristimo. Ovi dizajneri zauzvrat komuniciraju u naše ime sa Intelom, AMD-om, ARM-om ili bilo kojom kompanijom koja je dizajnirala CPU koji koristimo, i tako dalje.

1.4.1 Šta je kvantni program?

Kao i klasični programi, kvantni programi se sastoje od nizova instrukcija koje tumače klasični računari da bi izvršili određeni zadatak. Međutim, razlika je to što u kvantnom programu zadatak koji želimo da izvršimo uključuje kontrolu kvantnog sistema za izvršavanje proračuna.

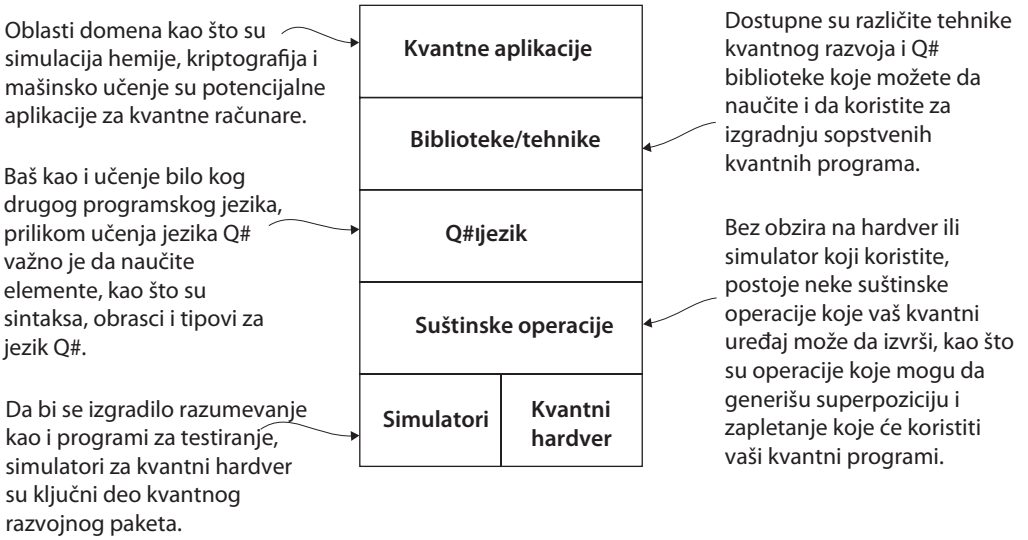
Kao rezultat toga, instrukcije koje se koriste u klasičnim i kvantnim programima se takođe razlikuju. Klasični program može opisati zadatak kao što je učitavanje nekih slika mačaka sa interneta u smislu uputstava za mrežni stek i na kraju u smislu uputstava za sklapanje kao što je mov (pomak). Nasuprot tome, kvantni jezici poput Q# dozvoljavaju programerima da izraze kvantne zadatke u smislu instrukcija kao što je M (mera). Kada se pokreću pomoću kvantnog hardvera, ovi programi mogu da upute procesoru digitalnih signala da šalje mikrotalase, radio talase ili lasere u kvantni uređaj i pojačava signale koji izlaze iz uređaja.

U ostatku ove knjige videćemo mnoge primere zadataka sa čijim se rešavanjem suočava kvantni program, i saznaćemo koje vrste klasičnih alata možemo da koristimo da olakšamo kvantno programiranje. Na primer, na slici 1.5 prikazan je primer pisanja kvantnog programa u razvojnom okruženju Visual Studio Code, koji je klasično integrisano razvojno okruženje (IDE).



Slika 1.5 Pisanje kvantnog programa pomoću Quantum Development Kit paketa i razvojnog okruženja Visual Studio Code. Doći ćemo do sadržaja ovog programa u poglavlju 7, ali možete da vidite da izgleda slično drugim softverskim projektima na kojima ste možda radili.

Izgradićemo koncepte koji su nam potrebni za pisanje kvantnih programa, poglavlje po poglavlje; na slici 1.6 prikazana je mapa puta. U sledećem poglavlju učićemo o osnovnim gradivnim blokovima koji čine kvantni računar i koristićemo ih za pisanje našeg prvog kvantnog programa.



Slika 1.6 U ovoj knjizi gradimo koncepte koji su nam potrebni za pisanje kvantnih programa. Počinjemo u prvom delu sa opisima simulatora i suštinskih operacija nižeg nivoa (mislimo na hardverski API) izgradnjom sopstvenog simulatora u Python jeziku. U drugom delu ispitujemo Q# jezik i kvantne razvojne tehnike koje će nam pomoći da razvijemo sopstvene aplikacije. U trećem delu prikazujemo neke poznate aplikacije za kvantno računarstvo i izazove i mogućnosti koje imamo sa ovom tehnologijom koja napreduje.

Rezime

- Kvantno računarstvo je važno jer će nam kvantni računari potencijalno omogućiti da rešimo probleme koje je preteško rešiti konvencionalnim računarima.
- Kvantni računari mogu pružiti prednosti u odnosu na klasične računare za neke vrste problema, kao što je faktorisanje velikih brojeva.
- Kvantni računari su uređaji koji koriste kvantnu fiziku za obradu podataka.
- Programi su nizovi instrukcija koje klasični računar može protumačiti za obavljanje zadataka.
- Kvantni programi su programi koji obavljaju računanje slanjem instrukcija kvantnim uređajima.