Predgovor

Napredak računarske tehnike od pionirskih dana do današnjeg nivoa razvoja ne može se posmatrati a da ne izazove divljenje. Međutim, napredak hardvera, softvera i računarskih algoritama nije bio usklađen. Iako impresivan, razvoj hardvera nije uvek išao u korak sa rastućim zahtevima naučnih i komercijalnih aplikacija. Ilustrativan primer je oblast mašinskog učenja. Mnogi teorijski koncepti i metode mašinskog učenja su bili poznati već šezdesetih i sedamdesetih godina dvadesetog veka, ali praktična upotreba mašinskog učenja morala je da sačeka da razvoj hardvera dostigne nivo potreban za njihovu implementaciju. Protekle su decenije dok je hardver dostigao nivo koji je omogućio računarima da postanu neodvojivi deo moderne civilizacije.

Danas se pojavljuju novi izazovi i otvara niz novih primena, na primer, veštačka inteligencija i obrada velikih podataka, gde tradicionalni, fon Nojmanov koncept računarstva više nije primeren rastućim zahtevima. Uz to, postoji cela klasa problema, kao što su NP-teški problemi koji se, osim za male instance, na savremenim računarima ne mogu rešiti u realnom vremenu. Kao prelazno rešenje, primenjuju se različite heurističke metode koje daju približne rezultate. Kontradiktorno, računarske komunikacije i zaštita podataka se oslanjaju upravo na nemogućnost današnjih računara da dešifruju savremene kriptografske algoritme.

Postalo je očigledno da je za dalji razvoj računarstva potreban novi, inovativni, model. Traženi model nudi upravo kvantno računarstvo. Koristeći kvantnu mehaniku kao osnovu, kvantno računarstvo potpuno menja koncept obrade podataka, od reprezentacije i procesiranja do njihove interpretacije. Koristeći superpoziciju i činjenicu da kvantno stanje nije određeno do trenutka dekoherencije, kvantnomehanički pristup omogućava modeliranje izuzetno kompleksnih sistema. Mnogi od problema koji se efektno ne mogu rešiti današnjim računarima u principu mogu biti rešeni primenom kvantnih računara.

Ipak, jedna od sličnosti tradicionalnog i kvantnog računarstva je to što razvoj hardvera i softvera nije usklađen. Praktični, inženjerski problemi u razvoju su izuzetno veliki, ali napredak je vidljiv i nema sumnje da će ubrzani napori uroditi plodom. Sa druge strane, teorijske osnove kvantnog računarstva su dobro poznate. Određen broj algoritama je već razvijen, dok je dalji razvoj predmet intenzivnog istraživanja. Napredak na ovom polju se ipak ne odvija očekivanom brzinom. Zbog razlike između principa rada i algoritama kvantnog i tradicionalnog računarstva, stečeno znanje i iskustvo na klasičnim sistemima ima ograničenu primenu.

Knjiga „Kvantno računarstvo" dr Aleksandra Radovanovića predstavlja jedinstven poduhvat u kome se oblast kvantnog računarstva tretira sveobuhvatno. Na jasan način se objašnjavaju koncepcijske razlike između tradicionalnog i kvantnog računarstva kao i oblasti njihove primene. Počevši od pregleda osnovnih matematičkih pojmova potrebnih za razumevanje izloženog materijala, sadržaj uključuje teorijske osnove kvantnog računarstva, osnovne elemente i principe implementacije kvantnih kola, sve do analize važnijih algoritama. Knjiga takođe

sadrži i poglavlje o osnovama kvantnih komunikacija kao i poglavlje o kvantnom mašinskom učenju, kao oblastima od posebnog interesa.

Već letimičan pregled postojeće literature iz ove oblasti, većinom na engleskom jeziku, ukazuje na činjenicu da su koncepti kvantnog računarstva većinom izloženi na način koji je pre namenjen teorijskim fizičarima, nego stručnjacima iz oblasti računarstva. Ova knjiga menja tu perspektivu. Autor uspeva da ovu veoma kompleksnu materiju izloži na način koji nije suvoparan, čemu svakako doprinose i kratki istorijski osvrti na pojedine epizode iz razvoja kvantne mehanike i kvantnog računarstva. Način izlaganja i dostupnost materijala u knjizi su njena najveća vrednost. Svi potrebni pojmovi se uvode bez nepotrebnih komplikacija, ali ipak dovoljno rigorozno.

Iako je knjiga pre svega namenjena studentima kvantnog računarstva, ona takođe može da bude od velike koristi i svima onima koji su zainteresovani da uđu u ovu kompleksnu, ali uzbudljivu materiju.

Dr Boris Janković

Reč autora

Kvantno računarstvo je dinamična oblast koja donosi značajne promene u našem razumevanju računara i načina obrade informacija. Osim što predstavlja izazov, kvantno računarstvo je izuzetno inspirativno, jer nas suočava sa konceptima koji premašuju granice intuicije klasičnog računarstva.

Ova je knjiga nastala sa ciljem da pruži temeljno razumevanje osnovnih principa kvantnog računarstva, kvantnih programskih jezika, kvantnih algoritama i praktične primene kvantnih računara. Knjiga je namenjena kako studentima računarskih nauka tako i svima onima koje interesuje ova zanimljiva i dinamična oblast.

Želeo bih da izrazim zahvalnost profesorki dr Bojani Dimić Surla, dekanu Računarskog fakulteta Univerziteta Union u Beogradu, na podršci prilikom pisanja i objavljivanja ove knjige. Takođe se zahvaljujem recenzentima dr Borisu Jankoviću i dr Đorđu Tomaševiću. Njihovi komentari, sugestije i stručni uvidi pomogli su unapređenju kvaliteta teksta koji je pred vama.

Dr Aleksandar Radovanović

Sadržaj

GLAVA 1: UVOD 1

1.1. Kratka istorija kvantnog računarstva 1
1.2. Elementi kvantnog računarstva 2
1.2.1. Neformalni uvod u principe kvantne mehanike 4
1.2.2. Histogram – dizanje vela slučajnosti 8
1.3. Binarni brojni sistem 9
1.3.1. Big-endian / little-endian 11

GLAVA 2: MATEMATIČKE OSNOVE KVANTNOG RAČUNARSTVA 13

2.1. Korisne matematičke konstante i funkcije 14
2.2. Kompleksni brojevi 18
2.2.1. Kompleksni brojevi na jediničnom krugu 21
2.2.2. n-ti koreni jedinice 21
2.3. Elementi matrične algebre 24
2.3.1. Matrica 24
2.3.2. Operacije sa matricama 25
2.3.3. Paulijeve matrice 33
2.4. Vektori i vektorski prostori 34
2.4.1. Operacije nad vektorima 35
2.4.2. Vektorski prostor 39
2.4.3. Vektori baze 42
2.5. Linearne transformacije 44
2.5.1. Rotacija vektora 46
2.5.2. Sopstvene vrednosti i sopstveni vektori 48
2.6. Dirakova bra-ket notacija 50
2.7. Operatori 55
2.7.1. Projekcije i projekcioni operatori 56
2.7.2. Osobine ermitskih operatora 59
2.8. Bulova algebra 61
2.8.1. Forme Bulovih izraza 64
2.9. Modularna aritmetika 65

GLAVA 3: KUBIT 69

3.1. Model kubita 70
3.1.1. Blohova sfera 72
3.2. Bornovo pravilo 76
3.2.1. Očekivana vrednost 79
3.2.2. Projektivno merenje 81
3.3. Praktična primena Bornovog pravila 86
3.4. Registri 87
3.4.1. Merenje registra 89
3.5. Matrica gustine 91
3.6. Vizualizacija kubita 95
3.6.1. Stubičasti dijagrami 95
3.6.2. Fazni disk 96
3.6.3. Q sfera 97
3.7. Nekoliko postulata i teorema kvantne mehanike 98
3.7.1. Teoreme o zabrani kopiranja i zabrani brisanja kvantnog stanja 100

GLAVA 4: ELEMENTARNA KVANTNA KOLA 104
4.1. Kvantna kola 105
4.1.1. Programski jezici namenjeni kvantnim računarima 108
4.2. Dizajn elementarnih kvantnih kola 112
4.2.1. Konstrukcija operatora 115
4.3. Jednokubitna elementarna kvantna kola 119
4.4. Dvokubitna elementarna kvantna kola 132
4.4.1. Elementarna kola sa inverznom kontrolom 139
4.5. Trokubitna elementarna kvantna kola 142
4.6. Operacije i kola posebne namene 144
4.7. Teoreme o kvantnim kolima 146
4.7.1. Teorema Z-Y dekompozicije 146
4.7.2. Dekompozicija $C2U$ kvantnih kola 150
4.7.3. Dekompozicija CnU kvantnih kola 151

GLAVA 5: ELEMENTI KVANTNIH ALGORITAMA 153
5.1. Kvantna superpozicija i kvantna interferencija 153
5.1.2. Kvantna interferencija 155
5.2. Kvantna spletenost 157
5.2.1. Belova stanja 160
5.2.2. CHSH nejednakost 163
5.2.3. CHSH igra 167
5.2.4. Neka ograničenja u primeni kvantne spletenosti 169
5.2.5. GHZ stanja 169
5.3. Kvantna aritmetika 170
5.3.1. Kvantno sabiranje 170
5.4. Evaluacija funkcije 173
5.5. Prenos faze 176
5.6. Kvantna Furijeova transformacija 178
5.6.1. Matematičke osnove 179
5.6.2. Konstrukcija KFT kola 185
5.7. Očitavanje/merenje kubita 192
5.7.1. Paulijeva merenja 192
5.7.2. Merenje Belovih stanja 196
5.7.3. Remzijevo kolo 197
5.8. Implicitno i odloženo merenje 199
5.9. Kvantna procena faze 199
5.10. Kvantni orakl 205
5.10.1. Binarni orakl 206
5.10.2. Fazni orakl 207

GLAVA 6: KVANTNI ALGORITMI 210
6.1. Dojčov algoritam 212
6.1.1. Analiza Dojčovog algoritma primenom faznog orakla 216
6.1.2. Dojč – Džoza algoritam 217
6.2. Bernstin–Vazirani algoritam 221
6.3. Sajmonov algoritam 224
6.4. Groverov algoritam 228
6.4.1. Analiza Groverovog algoritma 229
6.4.2. Geometrijska interpretacija Groverovog algoritma 238

6.4.3. Praktična implementacija Groverovog algoritma za $N = 4$ 242
6.4.4. Problem zadovoljivosti (SAT problem) 246
6.5. Šorov algoritam 247
6.5.1. Uvodni matematički koncepti 247
6.5.2. Skica Šorovog algoritma 251
6.5.3. Nalaženje perioda modularne eksponencijalne funkcije 253
6.5.4. Složenost Šorovog algoritma 257

GLAVA 7: KVANTNA KRIPTOGRAFIJA I KVANTNE KOMUNIKACIJE 259

7.1. Viznerovo kodiranje i kvantni novac 260
7.1.1. Viznerovo kodiranje 260
7.1.2. Viznerov kvantni novac 261
7.2. BB84 protokol 264
7.3. B92 protokol 267
7.4. E91 protokol 269
7.5. Gusto kodiranje 272
7.6. Kvantna teleportacija 275
7.6.1. Razmena spletenosti 281
7.7. Kvantna ispravka grešaka 282
7.7.1. Modeliranje kvantnih grešaka 284
7.7.2. Ispravka grešaka inverzije kubita 285
7.7.3. Ispravka grešaka inverzije faze 288
7.7.4. Šorov kod 289

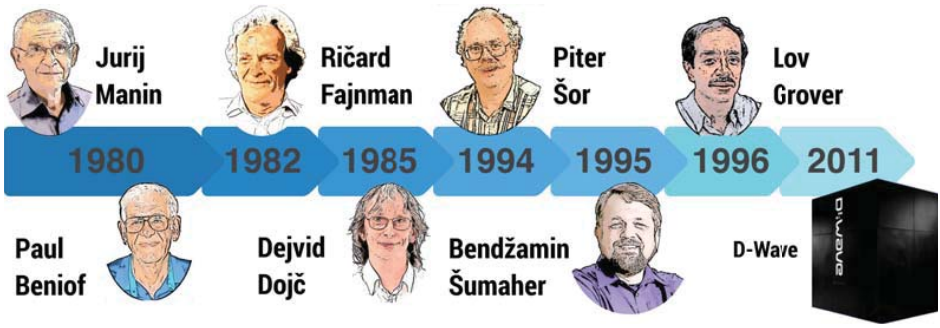
GLAVA 8: UVOD U KVANTNO MAŠINSKO UČENJE 290

8.1. Tipovi mašinskog učenja 290
8.2. Varijaciona/parametarizovana kvantna kola 293
8.2.1. Kodiranje podataka 295
8.2.2. Varijaciona kvantna kola 298
8.2.3. Merenje 301
8.2.4. Obuka modela 302
8.3. Generativno kvantno mašinsko učenje 305
8.3.1. Kvantna generativna suparnička mreža (qGAN) 305
8.3.2. Kvantne Bolcmanove mašine (QBM) 308

BIBLIOGRAFIJA 311

1.1. Kratka istorija kvantnog računarstva

Kvantno računarstvo je multidisciplinarna oblast koja obuhvata aspekte računarskih nauka, kvantne mehanike i matematike. Kvantna mehanika je grana fizike koja objašnjava pojave na atomskom i subatomskom nivou. Reč „kvant" (lat. *quantum*: količina) odnosi se na diskretne jedinice energije, naelektrisanja, materije ili neke druge fizičke veličine. Kvantni svet je okarakterisan neobičnim pojavama, kao što je postojanje objekta na dva mesta istovremeno ili prisustvo tajanstvene veze koja drži objekte u savršenoj korelaciji bez obzira na njihovu međusobnu udaljenost. Nobelovac Ričard Fajnman kaže: „Mislim da mirno mogu da kažem da niko ne razume kvantnu mehaniku". Fizičar Verner Hajzenberg pravi razliku između razumevanja i opisivanja: „Kvantna teorija nam pruža upečatljivu ilustraciju činjenice da možemo u potpunosti razumeti vezu iako o njoj možemo govoriti samo u slikama i parabolama". Ovakvo, pre svega matematičko razumevanje kvantne mehanike omogućilo je pronalazak i razvoj lasera, poluprovodnika, tranzistora, mikroprocesora i konačno, kvantnih računara.



Slika 1-1. Kratka istorija razvoja kvantnog računarstva od teorijskih ideja do prvog komercijalnog računara.

Istorija kvantnog računarstva počinje 1980-tih godina sa pojavom prvih ideja o primeni kvantne mehanike u svrhu mašinskog računanja (Slika 1-1). Nuklearni hemičar Paul Beniof i matematičar Jurij Manin 1980. godine nezavisno iznose ideju o direktnoj primeni zakona kvantne mehanike u računarstvu. Dve godine kasnije, 1982., fizičar Ričard Fajnman predlaže „univerzalni kvantni simulator". Fizičar Dejvid Dojč, koji se danas smatra ocem kvantnog računarstva, 1985. godine teorijski razvija model kvantnog procesiranja i opisuje budući univerzalni kvantni računar.

Početkom sledeće decenije, 1992. godine, dva američka fizičara, Bendžamin Šumaher i Vilijam Vuters u neobaveznom razgovoru smišljaju termin „kubit" (eng.

qubit) kojim nazivaju osnovnu jedinicu kvantnih podataka – kvantni bit. Peter Šor 1994. godine objavljuje algoritam za faktorizaciju celih brojeva, a 1996. godine Lov Grover opisuje algoritam za pretragu nesortirane baze podataka.

Krajem 90-tih godina prošlog veka intenzivira se i rad na razvoju hardvera. Grupa istraživača sa Univerziteta britanske Kolumbije u Kanadi 1999. godine osniva kompaniju za kvantne računare pod imenom „D-Wave ". Nešto više od decenije kasnije, 2011. godine, kompanija predstavlja računar D-Wave One. Iako u istoriju ulazi kao prvi komercijalni kvantni računar, ovaj se računar ne smatra univerzalnim računarom jer je bio u mogućnosti da rešava samo izvesnu klasu problema. Prvi kvantni računar opšte namene lansira američka kompanija IBM 2016. godine. U to vreme, preko veb platforme Quantum Experience, IBM pruža priliku korisnicima širom sveta da eksperimentišu sa kvantnim procesorima. Programi se grafički konstruišu ili pišu na IBM-ovom Open Quantum Assembly Language (Open QASM) jeziku, ili na Pajton programskom jeziku uz korišćenje Qiskit SDK (Quantum Information Software Kit) kompleta za razvoj softvera. U godinama koje slede pojavljuju se sve bolji i brži kvantni procesori, garantujući budućnost kvantnih računara.

1.2. Elementi kvantnog računarstva

Kvantno računarstvo je multidisciplinarna nauka koja spaja elemente računarske nauke, kvantne mehanike i matematike sa svrhom unapređenja teorije računarstva i sa praktičnim ciljem rešavanja računarskih problema. Kao računska mašina, kvantni računar je tip računara koji direktno koristi principe kvantne mehanike za izvršavanje računskih operacija.

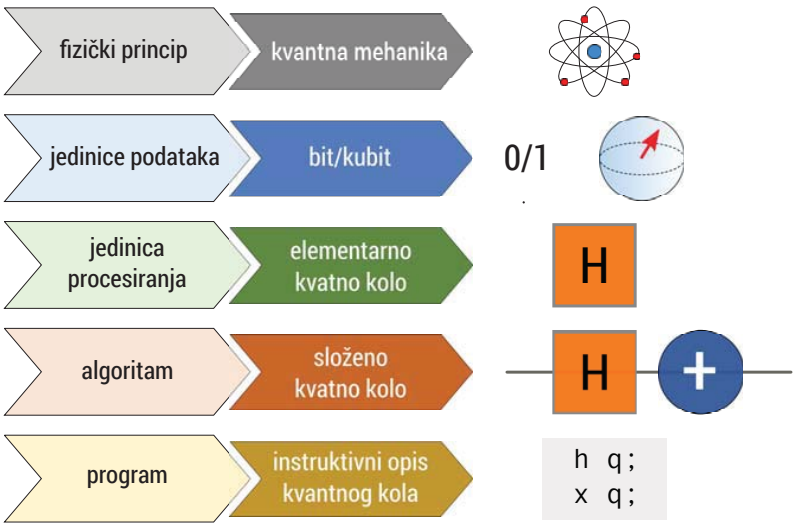
Slika 1-2 prikazuje apstraktan, hijerarhijski model kvantnog računara.

- Na fizičkom nivou, kvantni računar koristi principe kvante mehanike za predstavljanje i obradu podataka.
- Osnovne jedinice podataka u kvantom računarstvu su klasični bit i **kvantni bit** ili **kubit**. Klasični bit može biti u jedom od dva stanja predstavljena ciframa 0 i 1, dok se kubit može nalaziti u beskonačno mnogo stanja predstavljenih vektorom, koji rotira unutar sfere jediničnog poluprečnika.
- Osnovna jedinica kvantnog procesiranja je elementarno kvantno kolo ili kvantna kapija [1]. Elementarno kvantno kolo menja stanje kubita što odgovara rotaciji vektora unutar sfere.
- Kvantni algoritam se prikazuje u obliku dijagrama koji se naziva kvantno kolo. Kvantno kolo prikazuje sekvencu elementarnih kvantnih kola koja izvode niz transformacija kroz koje kubit prolazi u toku izvršavanja

[1] Reč „kapija" je stranog porekla, pa se neće koristiti u ovoj knjizi.

programa. Iako izraz „kvantno kolo” sugeriše hardverski dijagram, kolo predstavlja dijagram toka programa.

- Kvantni program je instruktivni opis kvantnog kola na nekom od programskih jezika koje podržavaju programiranje kvantnog računara.



Slika 1-2. Apstraktan, hijerarhijski model kvantnog računara.

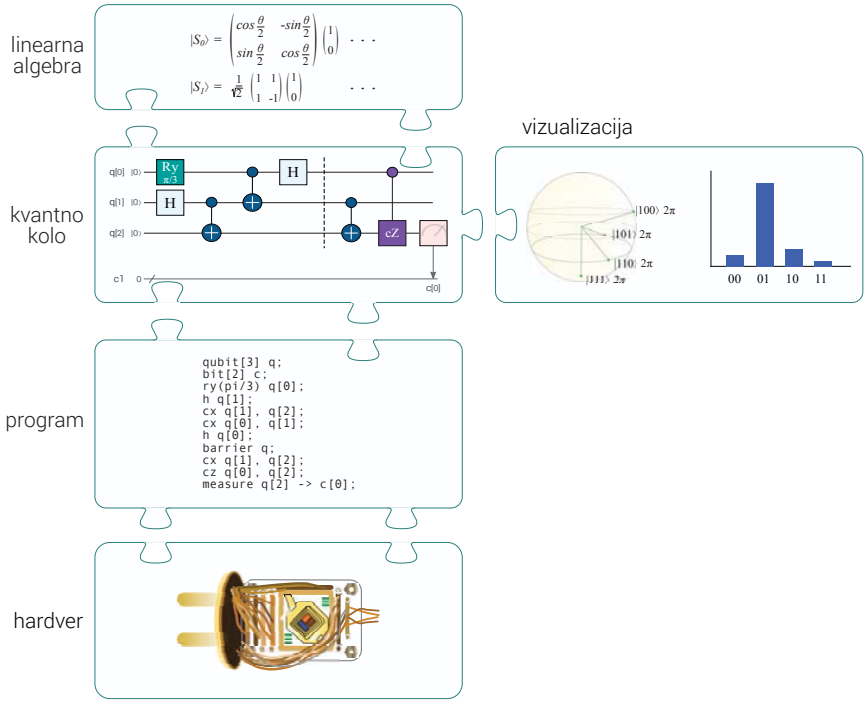
Slika 1-3 ilustruje opšti programski model kvantnog računara.

- Matematičku osnovu kvantnog računarstva čini linearna algebra, posebno matrični račun.
- Matematički model algoritma se vizualizuje u obliku kvantnog kola.
- Tekstualni opis kvantnog kola preko instrukcija kvantnog programskog jezika čini izvorni kôd programa.
- Izvorni kôd se zatim prevodi u mašinske instrukcije koje se izvršavaju na kvantom procesoru.
- Vizualizacija je važna komponenta kvantnog računarstva, počevši od vizualizacije kubita, preko stanja kvantnog kola sve do vizualizacije rezultata.

Model sa slike diktira izvesne razlike u razvoju programa za kvantni računar u poređenju sa razvojem programa za klasičan računar. U opštim crtama, razvoj programa za kvantni računar sastoji se od sledećih koraka:

1. Definicija problema koji se rešava.
2. Formulisanje problema u okviru linearne algebre.
3. Dizajn rešenja u matrično-vektorskom obliku.

4. Dizajn kvantnog kola kao implementacije matričnih operatora.
5. Prevod kvantnog kola u programski kôd.
6. Integracija sa klasičnim programskim okruženjem.
7. Testiranje, optimizacija i otklanjanje grešaka na simulatoru.
8. Testiranje na kvantnom hardveru.
9. Proizvodna verzija.



Slika 1-3. Programski model kvantnog računara.

1.2.1. Neformalni uvod u principe kvantne mehanike

Na fizičkom nivou obrade podataka, kvantni računari koriste principe kvantne mehanike. To su pre svega, princip superpozicije, interferencije, spletenosti i princip kvantnog merenja. Ovi su principi primenljivi samo na kvantne objekte, odnosno na objekte koji podležu zakonima kvantne mehanike i ne mogu se primeniti na objekte iz našeg makro-sveta. Kvantni objekti koji nose informaciju u kvantnim računarima – kubiti, izvode sa kao superprovodna elektronska kola, atomi (joni) ili fotoni. Kao uvodnu metaforu za kubit koristićemo „kvantni novčić" sa stranama 0 i 1.

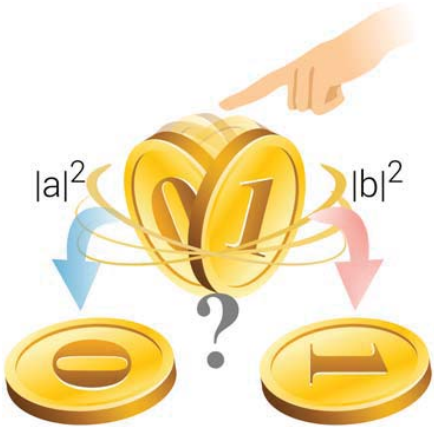
Princip kvantne superpozicije kaže da kvantni objekat koji može zauzimati jedno od nekoliko mogućih stanja, takođe može zauzimati sva ova stanja istovremeno. Ova se kombinacija takozvanih baznih stanja naziva superpozicija. Naš kubit-novčić može u kvantom svetu zauzimati bazno stanje 0, bazno stanje 1, ili oba stanja istovremeno; i 0 i 1 (Slika 1-4). U svakodnevici klasične mehanike postojanje novčića u superpoziciji je samo privid, dok se u svetu kvantne mehanike stanje superpozicije smatra realnim stanjem.



Slika 1-4. Kvantni kubit–novčić u baznom stanju 0, baznom stanju 1 i u superpoziciji baznih stanja (i 0 i 1).

Superpoziciju nije moguće direktno osmotriti tako da se u cilju dobijanja informacije o kvantnom objektu vrši njegovo merenje odgovarajućim mernim instrumentom.

Princip kvantnog merenja kaže da merenje stanja kvantnog objekta u superpoziciji dovodi do kolapsa, ili redukcije superpozicije u jedno od mogućih baznih stanja (Slika 1-5). Dodirivanjem kvantnog novčića kao na slici, narušava se superpozicija i novčić pada ili na stranu 0 ili na stranu 1. Jednom izmereni kubit-novčić zadržava bazno stanje i ponovno merenje daje isti rezultat.

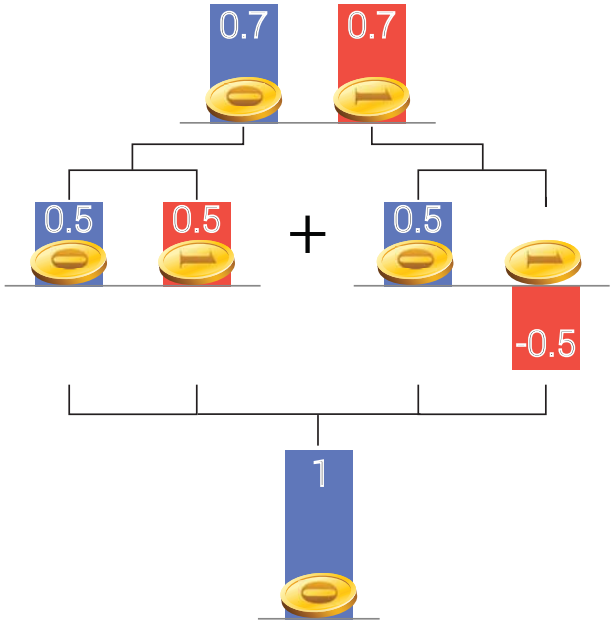


Slika 1-5. Merenje kubit–novčića. Dodirivanjem novčića superpozicija se narušava i novčić pada ili na stranu 0 ili na stranu 1. Na koju će stranu pasti, zavisi od kvadrata „težina "a i b svake od strana.

Ako je novčić pravičan, verovatnoća svakog od ishoda je 50%. Postavlja se pitanje da li je moguće predvideti na koju će stranu pasti novčić koji nije pravičan? Neka je a težina koja vuče novčić na stranu 0, i neka je b težina koja vuče novčić na stranu 1. U svakodnevnom svetu klasične mehanike za očekivati je da će novčić za većom verovatnoćom pasti na težu stranu, a sa manjom verovatnoćom na lakšu stranu.

Slično je i očekivanje u kvantnom svetu, ali uz razliku da je svaka od dve verovatnoća precizno definisana kao kvadrat „težine" svake od strana. Verovatnoća da novčić padne na stranu 0 je jednaka $|a|^2$, a verovatnoća da novčić padne na stranu 1 je jednaka $|b|^2$. Veličine a i b se u kvantnoj mehanici nazivaju amplitude verovatnoća.

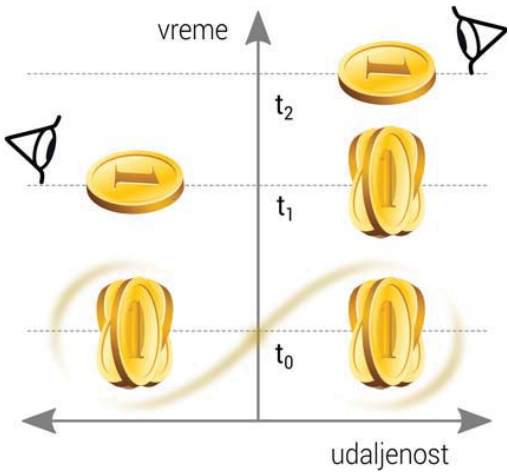
Amplituda verovatnoće je (kompleksan) broj koji se definiše kao broj čiji kvadrat daje verovatnoću ishoda kvantnog merenja. Kako će novčić eventualno pasti na jednu od strana, uzimajući u obzir da je verovatnoća sigurnog događaja 1, može se reći da je $|a|^2 + |b|^2 = 1$. Ovaj se uslov naziva **uslov normalizacije**. Posledica po kvantno računarstvo je da merenje, kubita u jednakoj superpoziciji daje slučajan rezultat. Da se ovo ne bi dogodilo, zadatak kvantnog softvera je da maksimizuje amplitudu ciljnog i minimizuje amplitudu neželjenog rezultata. Ovo se postiže metodom poznatom kao kvantna interferencija.



Slika 1-6. Primer kvantne interferencije. Kubit-novčić se stavlja u jednaku superpoziciju, a zatim se svaka od komponenti opet stavlja u superpoziciju. U novonastalom stanju dolazi do kvantne interferencije u kojoj se pozitivne amplitude istog stanja sabiraju, a negativne poništavaju, osiguravajući ishod 0.

Kvantna interferencija je pojava međusobnog uticaja kvantnih objekata pa čak i objekta sa samim sobom, u kome se amplitude verovatnoća sabiraju ili oduzimaju. Slika 1-6 prikazuje kubit-novčić u superpoziciji sa jednakim amplitudama verovatnoća od po ~ 0.7 predstavljenih stubičastim grafikonom. Ako se svaka komponenta superpozicije stavi opet u superpoziciju dobijaju se četiri komponente sa amplitudama verovatnoća od po 0.5, sa tim što je jedna od amplituda negativna. Amplitude verovatnoća su se smanjile jer u svakom trenutku zbir njihovih kvadrata mora biti 1. U novonastaloj superpoziciji dolazi do kvantne interferencije kubita sa samim sobom, odnosno do sabiranja amplituda pridruženih istom stanju. Amplitude stanja 0 se sabiraju, dok se amplitude stanja 1 poništavanju osiguravajući da će kubit-novčić sigurno pasti na stranu 0.

Kvantna spletenost je princip koji omogućava da dva ili više kvantna objekata postoje u stanju visoke korelacije. Neka su dva kubita-novčića u superpoziciji spletena u sinhronu rotaciju vremenskom trenutku t_0. U trenutku t_1 posmatrač dodiruje levi novčić koji slučajno pada na stranu 1. Nešto kasnije, drugi posmatrač dodiruje desni novčić koji takođe pada na stranu 1. Isti ishod nije rezultat slučajnosti. Kvantna spletenost garantuje da će rezultati merenja prvog novčića odrediti rezultat merenja drugog novčića bez obzira na prostornu i vremensku udaljenost. Ovaj fenomen je Ajnštajn nazivao „sablasno delovanje na daljinu". Iako još uvek ne postoji teorijsko objašnjenje, kvantna spletenost je tehnički lako izvodljiva i rutinski se koristi u kvantnim računarima i u svrhu kvantnih komunikacija.



Slika 1-7. Dva kubita–novčića spletena u sinhronoj rotaciji. Kvantna spletenost garantuje da će oba novčića izmerena u vremenima t_1 i t_2, uvek dati isti rezultat (u ovom slučaju 1).

Za kvantni sistem koji pokazuje svojstva superpozicije i spletenosti se kaže da je u stanju **kvantne koherencije** (lat. *cohaerēre*: zajedništvo). Dužina trajanja

koherencije je jedna od važnih mera u kvantnom računarstvu jer je kvantno procesiranje podataka moguće samo tokom vremena u kome su kubiti u ovom stanju. Nesavršenost izolacije kvantnog sistema od uticaja okolne sredine, na primer elektromagnetnih i toplotnih zračenja, proces manipulacije kubita i kvantno merenje dovodi do gubitka kvantne koherencije. Gubitak kvantne koherencije ili **kvantna dekoherencija** je prelazak sistema iz kvantnog stanja u stanje koje se podvrgava zakonima klasične fizike.

1.2.2. Histogram – dizanje vela slučajnosti

Pojedinačno gledajući, čini se da su rezultati kvantnog merenja slučajni. Ipak, primenom jednostavne statističke metode mogu se naći verovatnoće svakog od mogućih ishoda.

Statistika definiše pojam verovatnoće kao meru očekivanja da će se neki događaj desiti. Verovatnoća se izražava brojem između 0 i 1, gde 0 označava nemoguć, a 1 siguran događaj. Verovatnoća se može izraziti i u procentima tako što se ovaj broj pomnoži sa 100.

Za procenu eksperimentalnih rezultata, u ovom slučaju kvantnog merenja, koristi se mera koja se zove relativna učestalost. **Relativna učestalost**, ili **relativna frekvencija** posmatranog ishoda nekog eksperimenta definiše se kao količnik broja pojavljivanja tog ishoda i ukupnog broja svih ishoda eksperimenta.

$$relativna\ učestalost\ = \frac{broj\ pojavljivanja\ posmatranog\ ishoda}{broj\ svih\ ishoda}$$

Relativne učestalosti se grafički prikazuju histogramom. Histogram je stubičasti dijagram na čijoj se horizontalnoj osi nalaze klase mogućih ishoda a na vertikalnoj relativne učestalosti. Visina svakog stupca odgovara relativnoj učestalosti odgovarajuće klase.

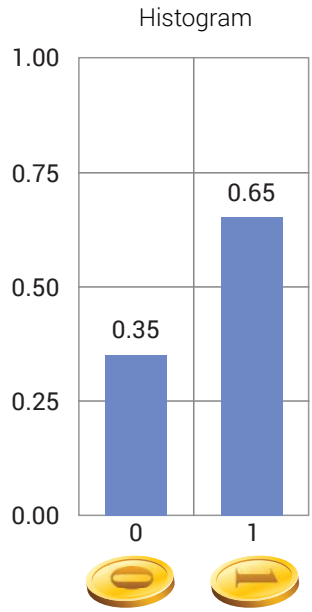
Neka je na primer, novčić bačen 100 puta pri čemu je 35 puta izašla nula i 65 puta izašla jedinica. Relativne učestalosti ovih ishoda su:

$$RF(0) = \frac{35}{100} = 0.35 \quad RF(1) = \frac{65}{100} = 0.65$$

Slika 1-8 prikazuje histogram dobijenih eksperimentalnih rezultata. Histogram pokazuje da novčić nije pravičan, jer je verovatnoća dobijanja jedinice veća od verovatnoće dobijanja nule. Iz podataka i iz histograma se takođe vidi da zbir verovatnoća iznosi 1.

Eksperimentalni rezultati

ishod	n	RF=n/100
0	35	0.35
1	65	0.65
zbir	100	1



Slika 1-8. Eksperimentalno utvrđivanje pravičnosti novčića. Novčić je bačen 100 puta: 35 puta je dobijen ishod 0, a 65 puta ishod 1. Rezultati uneti u tabelu i grafički prikazani histogramom pokazuju da novčić nije pravičan jer češće pada na jedinicu.

Slično, rezultat merenja kubita i, generalno, rezultat rada kvantnog programa je nepredvidljiv ali se iz histograma može videti distribucija rezultata. Sama distribucija može predstavljati rezultat proračuna, na primer, verovatnoća meteoroloških padavina. Ako se zahteva precizan odgovor, najčešći rezultat se može (uz određenu verovatnoću) smatrati tačnim. Ovo je razlog zašto se kvantno računarstvo često naziva i probabilističko računarstvo (eng. *probability*: verovatnoća).

1.3. Binarni brojni sistem

Iako kvantni računari koriste kvantno mehaničke principe u toku obrade podataka, izlazne rezultate daju u binarnoj formi. Stoga je poznavanje binarnog sistema, ne samo od teorijskog, nego i od praktičnog značaja.

Kao i decimalni sistem, binarni sistem je pozicioni brojni sistem. Pozicioni brojni sistem je sistem za predstavljanje brojeva uređenim skupom numeričkih simbola (cifara) u kome vrednost numeričkog simbola zavisi od njegove pozicije.