Moderni računari i njihove karakteristike - Kvantno računarstvo

Sreten Kovačević 446/22

[Uvod 2](#_Toc164461528)

[Kvantno računarstvo 2](#_Toc164461529)

[Teorijska osnova 2](#_Toc164461530)

[Arhitektura 4](#_Toc164461531)

[Algoritmi 5](#_Toc164461532)

[Potencijal 7](#_Toc164461533)

[Ograničenja 7](#_Toc164461534)

[Zaključak 8](#_Toc164461535)

[Literatura 8](#_Toc164461536)

# 

# Uvod

Moderni programabilni računari mogu se, na osnovu tehnologije koju koriste, grupisati u sledeće generacije:

1. I generacija računara (kraj 1930-ih do kraja 1950-ih) - vakumske cevi i magnetni doboši
2. II generacija računara (kraj 1950-ih do polovine 1960-ih) - tranzistori umesto vakumskih cevi
3. III generacija računara (polovina 1960-ih do polovine 1970-ih) - integrisana kola smeštena na mikročipovima
4. IV generacija računara (polovina 1970-ih do danas) - visoko integrisana (VLSI - *very large scale integrated*) kola sa hiljade kola smeštenih na jedan silicijumski čip (mikrokontroler)
5. V generacija računara (danas pa nadalje) - ultra-visoko integrisana (ULSI - *ultra large scale integrated*) kola, paralelizacija

Peta generacija računara predstavlja revolucionarni korak u razvoju tehnologije, kombinujući napredne karakteristike kao što su veštačka inteligencija, paralelno procesiranje, i korišćenje optičkih vlakana. Ovi računari su sposobni za veliku računarsku moć i brzinu zahvaljujući tehnologiji ultra-visoke integracije (ULSI) kola, što ih čini pouzdanim, efikasnim i manje zahtevnim za održavanje. Pored toga, implementacija veštačke inteligencije omogućava interakciju sa korisnicima putem različitih modaliteta kao što su znakovni jezik, slike i grafikoni, dok se paralelno procesiranje i superprovodnička tehnologija koriste za unapređenje performansi. Očekuje se da će pete generacije računara doneti revolucionarne promene u svakodnevnom životu, transformišući ih u lične asistente sposobne za automatsko obavljanje raznih zadataka, dok će razvoj veštačke inteligencije otvoriti vrata za nove mogućnosti, poput razumevanja i odgovaranja na prirodni govor i razvoj sveprisutnih AI sistema.

Kvantno računarstvo se ističe kao jedno od područja koje može doživeti najznačajniju revoluciju u okviru pete generacije računara. Od ove nove tehnologije se očekuje da omogući efikasniju obradu velikih količina podataka, što će biti ključno za napredak veštačke inteligencije, ali i raznih drugih oblasti. U nastavku, istražićemo osnovne koncepte kvantnog računarstva kako bismo bolje razumeli njegovu ulogu u budućnosti računarske tehnologije.

# Kvantno računarstvo

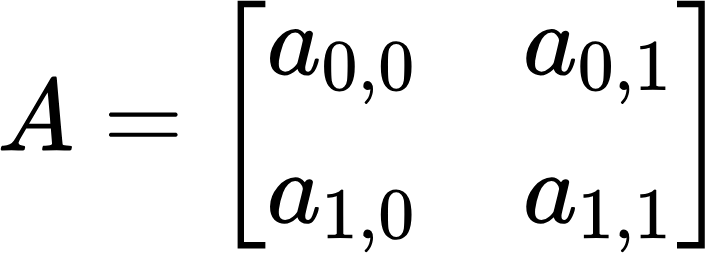
## Teorijska osnova

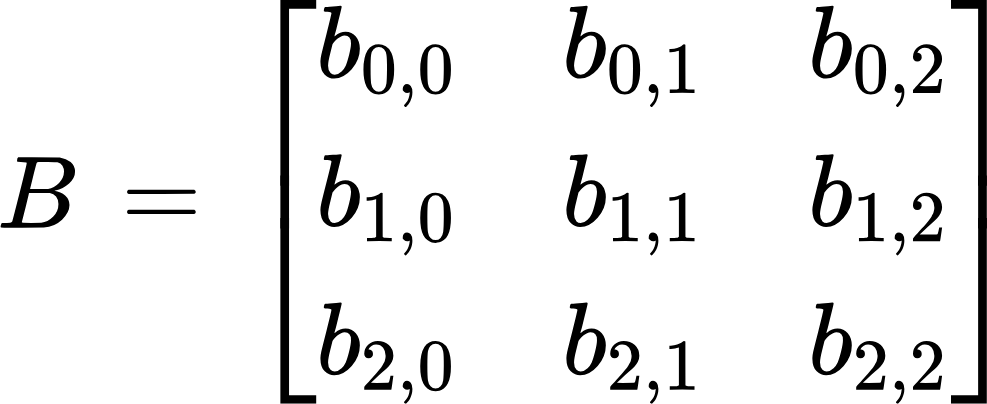
Pre samog definisanja karakteristika kvantnih računara, potrebno je da se spoznamo određene teorijske osnove na kojima počivaju kvantni računari.

**Probabilistički sistem** je matematički sistem, koji skup mogućih stanja definiše na osnovu verovatnoće svakog od stanja. Posmatrajmo primer 27 klikera, koji se mogu nalaziti na 6 različitih pozicija. Tradicionalni, deterministički sistem, mogao bi da opiše jedno stanje na sledeći način , gde svaki element niza odgovara broju klikera na odgovarajućoj poziciji. Probabilistički pristup ovom stanju dao bi sledeći opis , gde svaka pozicija odgovara verovatnoći da se na tom mestu nalazi kliker. Možemo primetiti da je zbir svih elemenata u probabilističkom stanju jednak 1, a da je svaki element realan broj iz opsega .

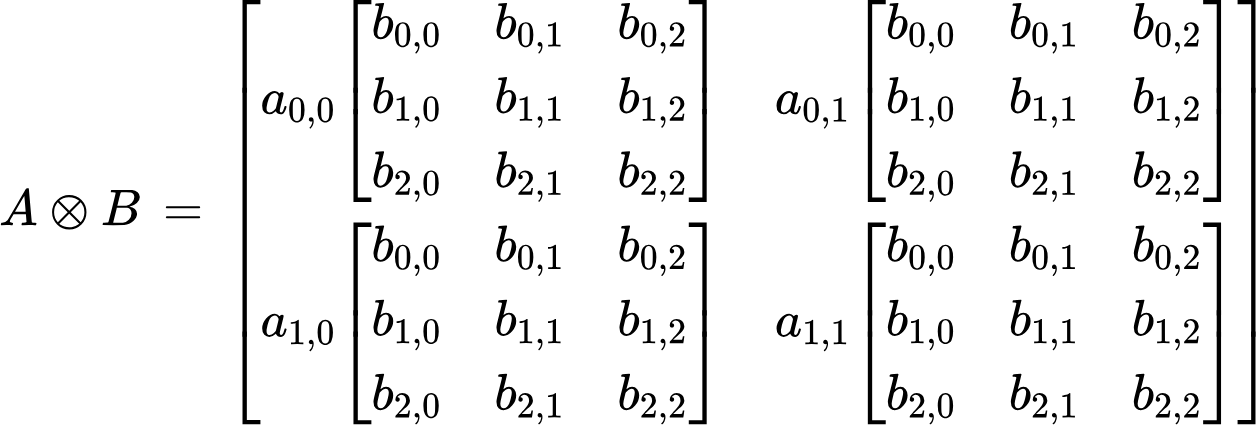
**Kvantni sistem** je modifikacija probabilističkog sistema takva da je prilagođen kvantnoj mehanici. Kako se kvantna mehanika zasniva na kompleksnim brojevima, tako se prethodno stanje može zapisati pomoću kompleksnih brojeva, uz određene dodatke. Umesto da se stanje predstavlja realnim brojem između 0 i 1, gde je zbir svih stanja jednak 1, stanje ćemo predstaviti kompleksnim brojevima za koje važi da je i . Stanje iz prethodnog primera bi se u kvantnom sistemu moglo predstaviti sa . Razlog iz kog se verovatnoće predstavljaju na ovaj način je zanimljivo svojstvo kompleksnih brojeva, po kom sabiranjem verovatnoća ne dobijamo nužno veći broj, kako je to sa verovatnoćama predstavljenim pomoću realnih brojeva.

**Spoljašnji (tenzorski) proizvod**, u oznaci , definisaćemo za vektore i matrice na primerima. Prvo, neka su data dva vektora, i , onda je . Slično, ukoliko su date matrice:





onda važi



Možemo zaključiti da, ukoliko spoljašnjim proizvodom množimo elemente iz i , onda je dimenzija proizvoda iz .

**Superpozicija** je ključni koncept u kvantnoj mehanici koji se odnosi na svojstvo kvantnih sistema da budu u više stanja istovremeno. Drugim rečima, kvantni sistem može biti u superpoziciji između dva ili više mogućih stanja, pri čemu nije u jednom precizno definisanom stanju sve dok ne bude izmeren. Umesto toga, pre merenja, sistem postoji u svim mogućim stanjima sa različitim verovatnoćama. Nakon merenja, superpozicija se “urušava”, a sistem prelazi u jedno od mogućih stanja.

Superpozicija se može jednostavno objasniti pomoću misaonog eksperimenta Šredingerove mačke. Dok ne otvorimo kutiju, ne možemo znati da li je mačka mrtva ili živa.

**Kvantno zaplitanje** (engl. *entanglement*) je fenomen u kvantnoj mehanici gde se dva ili više kvantnih objekata, poput čestica ili fotona, međusobno povezuju na način koji ne može biti opisan zakonima fizike. Kada se dva kvantna objekta nađu u stanju zaplitanja, njihova svojstva postaju međusobno zavisna i povezana, bez obzira na udaljenost između njih.

## Arhitektura

Može se reći da je svaki računar kvantni. Tranzistori i kola funkcionišu po principima kvnatnih efekata. Ipak, tradicionalni računari se oslanjaju na Bulovu algebru i kao osnovnu jedinicu funkcionisanja imaju bitove, koji mogu imati vrednost 0 ili 1. Dakle, tradicionalni računari zanemaruju kvantne efekte pri svom radu. Sa druge strane, kvantni računari pokušavaju u potpunosti da iskoriste prednosti koje kvantni efekti pružaju.

Bit nije dovoljan da bi se opisao kvantni svet. U te svrhe, koristi se **kvantni bit** (kjubit), koji predstavlja opis dvodimenzionalnog kvantnog sistema. Može se zapisati kao , gde predstavlja verovatnoću stanja 0, a predstavlja verovatnoću stanja 1, predstavljene u kvantnom modelu.

Ukoliko uopštimo sve ovo, zapravo se i tradicionalni bit može posmatrati kao kjubit, samo što u trenutku merenja gubi svojstvo superpozicije, te je verovatnoća njegove vrednosti ili .

Kao što tradicionalni računari nisu mašine od jednog bita, tako ni kvantni računari nisu mašine jednog kjubita. Posmatrajmo bajt u tradicionalnim računarima, on se sastoji od 8 bitova. Predstavimo svaki bit kao kjubit, gde je bit 0 predstavljen pomoću kjubita , a bit 1 pomoću . Tada bajt možemo predstaviti sledećom formulom , čiji je rezultat , te pomoću bajta možemo predstaviti različitih vrednosti. Posmatrajmo sada taj bajt iz ugla kvantnog računara. Iz ugla superpozicije, grupa od 8 kjubita (kjubajt) u svakom trenutku može imati bilo koju od mogućih 256 vrednosti, sa nekom verovatnoćom predstavljenom pomoću kompleksnog broja.To znači da je za predstavljanje stanja jednog kjubajta neophodno čuvati 256 kompleksnih brojeva. Tako bi, za predstavljanje stanja računara sa 64-kjubitnim registrom bilo neophodno zapisati kompleksnih brojeva. Ova eksponencijalna eksplozija je velika prepreka sa kojom se današnja tehnologija suočava.

Radi lakšeg zapisa, uvedimo i **Dirakovu notaciju**, takođe poznatu i kao *bra-ket* notaciju. Za predstavljanje vrednosti kjubita u superpoziciji koristi se *ket* notacija, i to za predstavljanje stanja 0 superpozicije i predstavlja stanje 1 superpozicije. Oba ova stanja predstavljaju superpozicije u kojima su verovatnoće oba ishoda iste. Razlika je što je u stanju 1 superpozicije faza obrnuta. Algoritmi kjubite često postavljaju u jedno od ova dva stanja na samom početku izvršavanja.

Kada pričamo o arhitekturi kvantnih računara, potrebno je pomenuti i takozvane kjubitne kapije (engl. *Quantum Gates*), koje omogućavaju manipulaciju kjubitima, slično kao što logička kola omogućavaju manipulaciju bitovima. Korisno je napomenuti da se ova kola često oslanjaju i na efekat kvantnog zaplitanja. Ipak, u ovom tekstu se nećemo posebno baviti njima, ali će biti pominjana prilikom definisanja algoritama, kada će u kratkim crtama biti objašenjni njihovi efekti, bez ulaska u složene zakone njihovog funkcionisanja..

## Algoritmi

Da bi bolje razumeli potencijal kvantnog računara, potrebno je da se upoznamo sa nekim algoritmima koji su već osmišljeni, a koji se odnose na neke opšte poznate probleme u našem okruženju. Takođe, uporedićemo ih sa algoritmima koji se koriste u tradicionalnom računarstvu.

Počnimo od jednostavnog problema, pretrage imenika. U opštem slučaju, da bi pronašli unos koji nam je neophodan potrebno nam je operacija, gde je broj unosa u imeniku. Tačnije, to je slučaj sa tradicionalnim računarima. U kvantnom računarstvu, **Groverov algoritam pretrage** omogućava pronalazak unosa u tom imeniku sa vremenskom složenošću i prostornom . Pretpostavimo da je stepen broja dva i da imenik sadrži sve moguće vrednosti (nema duplikata).

U nastavku je dat pseudo-kod ovog algoritma:

1. Inicijalizuj kjubite u stanje
2. Primeni operaciju
3. Ponovi puta:
   1. Primeni operaciju fazne inverzije
   2. Primeni operaciju inverzije oko proseka
4. Izmeri vrednosti kjubita

kjubitna Hadamardova kapija, koja kjubit iz početnog stanja prebacuje u stanje . Rezultat ove operacije je da će kjubit biti u stanju superpozicije sa amplitudom vrednosti . je kapija identiteta, a matrica dimenzije , u kojoj je svaki element vrednosti . je matrica dimenzije , koja je uopštenje funkcije , gde je traženi unos.

Operacija fazne inverzije će promeniti fazu samo elementu koji tražimo, dok će operacija inverzije oko proseka dodatno promeniti verovatnoće u superpoziciji kako bi željeni ishod bio što verovatniji. Nakon iteracija vrednosti kjubita će sadržati traženi unos.  
Pogledajmo sada korak po korak primenu ovog algoritma na jednostavnom primeru sa 3 kjubita (), gde tražimo vrednost 101. Svaka tabela predstavlja međustanje po koracima algoritma, a vrednosti u tabeli predstavljaju verovatnoću stanja 3 kvantno zapletena kjubita:

1.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 000 | 001 | 010 | 011 | 100 | 101 | 110 | 111 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

2.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 000 | 001 | 010 | 011 | 100 | 101 | 110 | 111 |
|  |  |  |  |  |  |  |  |

3a.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 000 | 001 | 010 | 011 | 100 | 101 | 110 | 111 |
|  |  |  |  |  |  |  |  |

3b.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 000 | 001 | 010 | 011 | 100 | 101 | 110 | 111 |
|  |  |  |  |  |  |  |  |

3a.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 000 | 001 | 010 | 011 | 100 | 101 | 110 | 111 |
|  |  |  |  |  |  |  |  |

3b.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 000 | 001 | 010 | 011 | 100 | 101 | 110 | 111 |
|  |  |  |  |  |  |  |  |

Ukoliko Izračunamo verovatnoću da se dogodi 101, dobićemo , a izvršenje i treće iteracije bi dovelo do verovatnoće od 100%, što smo i želeli da postignemo.

Još jedan algoritam koji privlači mnogo pažnje u svetu kvantnog računarstva je **Šorov algoritam faktorizacije**. Neka je dat broj , za koji važi da je i neka je . U nastavku je pseudo-kod Šorovog algoritma za faktorizaciju:

1. Utvrditi da li je prost broj ili stepen prostog broja (u polinomijalnom vremenu); Ukoliko jeste, završi izvršavanje
2. Nasumično izaberi broj . Euklidovim algoritmom odrediti ; Ukoliko je rezultat , završi izvršavanje
3. Pronađi **periodu** pomoću sledećeg kvantnog kola:
   1. Primeni operaciju
   2. Primeniti operaciju
   3. Primeniti operaciju inverzne kvantne Furijeove transformacije
4. Ako je parno ili važi , vrati se na korak 2
5. Euklidovim algoritmom odrediti i . Vratiti bar jedno netrivijalno rešenje

Perioda je takav broj za koji važi i neka je funkcija takva funkcija da vraća 1 ukoliko je perioda, a 0 u suprotnom. Takođe, neka je matrica koja je uopštenje ove funkcije. Zbog kompleksnosti, nećemo se udubljivati u detalje funkcionisanja matrične operacije i operacije inverzne kvantne Furijeove transformacije, napomenimo samo da su to operacije koje su jednostavne za kvantni računar.

Vremenska složenost Šorovog algoritma je , dok je složenost najoptimalnijeg algoritma tradicionalnog računarstva , gde je neka konstanta. Dakle, umesto eksponencijalnog, imamo polinomijalan algoritam.

## Potencijal

Na osnovu primera algoritama koje smo videli, možemo pričati o potencijalu koji kvantno računarstvo donosi. Neke od oblasti računarstva na koje se očekuje da će kvantno računarstvo imati najveći uticaj su veštačka inteligencija i kriptografija.

Ako pričamo o veštačkoj inteligenciji, prva asocijacija je treniranje modela na ogromnim količinama podataka. Kako kvantni računari omogućavaju laku paralelizaciju nad podacima, benefit pri učenju bi mogli biti ogromni. Primena veštačke inteligencije na kvantnim računarima omogućila bi naučnicima da u kratkom vremenu obrade mnogo veću količinu podataka, što smo videli na primeru Groverovog algoritma. Ovakav pristup bi potencijalno mnogo da dovede do spoznaje novih materijala za razne svrhe (lekovi, električne baterije, đubrivo…). Ovakav uticaj na industriju mogao bi doneti nezamislive promene u tehnološkom razvoju u mnogim poljima.

Tradicionalna kriptografija počiva na složenosti operacije faktorizacije broja. Kao što smo videli, složenost tog algoritma u tradicionalnom računarstvu je eksponencijalna. RSA enkripcija na kojoj se zasniva većina današnjih transakcija oslanja se na ovaj problem. Javni ključ je ogroman broj koji je proizvod dva prosta broja čija je razlika takođe velika. Ta dva broja su privatni ključevi. Ukoliko bi faktorizacija bila lako rešiv problem, onda bi i bezbednost ovakvih algoritama bila narušena i na osnovu javnog ključa bi se lako pronašli. Iako na osnovu ovoga deluje da kvantno računarstvo znači i kraj bezbednosti, ipak ono donosi i nove sisteme zaštite, kao što je **Kvantna distribucija ključeva**. Oslanjajući se na kvantne zakone, kao što je stanje superpozicije, moguće je primetiti i mešanje sa strane. Preciznije, postoje mogućnosti detektovanja da neko treće lice pokušava da presretne komunikaciju i izmeri stanje kjubita. Takođe, postoje mehanizmi da takvo neželjeno čitanje učini podatke beskorisnim.

Osim ovih, kvantno računarstvo može doneti velike promene na mnogim druim poljima. Tako, na primer, očekuje se da će moć kvantnih računara značajno olakšati rešavanje problema trgovačkog putnika, koji zadaje glavobolje stručnjacima mnogih oblasti današnjeg sveta.

## Ograničenja

Nakon što smo videli šta nam kvantno računarstvo sve može doneti, neophodno je da razumemo i koje su to tehničke poteškoće sa kojima se naučnici susreću pri razvoju ove tehnologije. Prva i osnovna je izbor čestice koja bi se koristila za kjubit, neke od opcija su fotoni i elektroni.

Ono što treba uzeti u obzir je da su kjubiti izrazito osetljivi na spoljne efekte, koji mogu promeniti njihovo stanje, a samim tim i krajnji rezultat izračunavanja. Vreme koje kjubit može provesti u stanju superpozicije, odolevajući spoljnim efektima nazivamo **vremenom koherencije**. Današnji kvantni računari imaju vreme koherencije reda veličina 100 mikrosekundi. Kako se svaka kvantna operacija izvršava za 50 nanosekundi, svi poznati algoritmi su i dalje praktično neupotrebljivi.

Da bi izolovali kjubite, naučnici koriste principe frižidera ili vakuumskih cevi. Ideja frižidera je da se smanjenjem temperature smanji kinetička energija, a samim tim i efekat spoljnih čestica na kjubite. Da bi se to postiglo, potrebno je temperaturu držati što bliže apsolutnoj nuli (). Kako je temperatura u međuzvezdanom prostoru oko , jasno je koliko je ovo izazovan zadatak.

Još jedno bitno ograničenje sa kojim se naučnici susreću je i mala razlika u energetskoj vrednosti između stanja 0 i 1 kjubita. U zavsnosti od čestice koja se koristi ta razlika je u rasponu od 10 do 24 džula. To čini određivanje stanja u kom se kjubit nalazi izrazito teškim.

# Zaključak

Sva navedena ograničenja sa kojima se susreće razvoj kvantnog računarstva ukazuje da su potrebne posebne laboratorija i velike količine novca kako bi se izradila jedna ovakva mašina. U skladu sa tim, najveći doprinos ovoj oblasti donose univerzitetski razvojni centri, specijalizovani za kvantno računarstvo, potpomognuti industrijskim gigantima kakvi su *Google*, *IBM*, *NASA* i drugi.

Na primer, *IBM* je pre nekoliko godina putem *cloud*-a učinio svoju verziju kvantnog računara javno dostupnim za sve zainteresovane. Iako je ovaj servis počeo sa pružanjem usluge kvantnog računara koji sadrži svega 5 kjubita, vremenom je rastao i danas pruža sistem sa preko 100 kjubita. To i dalje nije dovoljno za obavljanje nekih složenijih izračunavanja, ali daje mogućnost entuzijastima i naučnicima širom sveta da se uključe i lakše prate razvoj tehnologije.

Sa druge strane, *NASA* i *Google* su pokrenuli saradnju sa firmom *D-Wave*, koja se bavi isključivo kvantnim računarstvom i, po informacijama koje su javno dostupne, trenutno imaju računar koji podržava preko 5000 kjubita. Ova firma je od prvog dana svog rada uvela revoluciju u razvoj kvantnih računara pružajući javnosti redovne izveštaje o svom napretku. Na taj način, pogurali su i konkurentne i na neki način otpočeli trku u razvoju kvantnih računara.

Iako su izazovi sa kojima se tehnologija kvantnih računara susreće veoma ozbiljni i deluju i nepremostivi, resursi i posvećenost firmi koje ulažu u njihov razvoj obećavaju brz napredak. Ukoliko bi tehnologija postala dovoljno stabilna za primenu na nekim od gorućih problema sa kojima se susreće čovečanstvo, to bi dovelo do proboja na mnogim poljima, uključujući i druge koje su u fokusu pete generacije računara.

# Literatura

1. Programiranje 1 - Filip Marić, Predrag Janičić [p1-b5.pdf (bg.ac.rs)](https://poincare.matf.bg.ac.rs/~predrag.janicic/books/p1-b5.pdf)
2. [Fifth Generation of Computers - GeeksforGeeks](https://www.geeksforgeeks.org/fifth-generation-of-computers/)
3. [Characteristics of Fifth Generation Computers (unacademy.com)](https://unacademy.com/content/bank-exam/study-material/computer-knowledge/characteristics-of-fifth-generation-computers/)
4. [Uvod u kvantno računarstvo — oblast u koju ulažu svi ozbiljni igrači (startit.rs)](https://startit.rs/kvantno-racunarstvo-101-ulaganja-d-wave-iqc/)
5. Quantum Computing for Computer Scientists - Noson S. Yanofsky, Mirco A. Mannucci [CNYT/Quantum Computing for Computer Scientists by Noson S. Yanofsky, Mirco A. Mannucci (z-lib.org).pdf at master · Ersocaut/CNYT · GitHub](https://github.com/Ersocaut/CNYT/blob/master/Quantum%20Computing%20for%20Computer%20Scientists%20by%20Noson%20S.%20Yanofsky%2C%20Mirco%20A.%20Mannucci%20(z-lib.org).pdf)
6. [Arhitektura kvantne mašine | PULSE Magazin](https://pulse.rs/kvantni-kompjuter/)
7. [IBM Quantum Computing](https://www.ibm.com/quantum)
8. [D-Wave Systems | The Practical Quantum Computing Company (dwavesys.com)](https://www.dwavesys.com/)