# O mogućnostima kvantno-mehaničkih računara

*SVETOMIR I. SIMONOVIĆ*, Akademija tehničkih strukovnih studija Beograd, Beograd

*Pregledni rad*
*UDC: 004.38:621.373.8*
*DOI: 10.5937/tehnika2203337S*

*U radu se analiziraju teoretske mogučnosti kvantno-mehaničkih modela računara u odnosu na klasične modele računara u smislu, njihove univerzalnosti, domena primene, efikanosti u rešavanju problema i njihove tehnološke izvodljivosti. Izloženi su koncepti determinističke Turingove mašine, probabilističke Turingove mašine i kvantno-mehaničke Turingove mašine. Objašnjen je pojam osnovne jedinice informacija u kvantno-mehaničkom modelu računara - kubita i prikazana reprezentacija kubita putem Blochove sfere. Objašnjena je upotreba Dirakove braket notacije za opis stanja kvantno-mehaničkog sistema i u toj notaciji data jednačina stanja jedne ćelije kvantno-mehaničke Turingove mašine. Posebno su razmatrane posledice kvantnog paralelizma, kvantne interferencije i kolapsa talasne funkcije na mogućnosti kvantno-mehaničkih modela računara. Prikazan je međusobni odnos klasa problema koji se mogu efikasno rešiti kvantno-mehaničkihm modelom, odnosno klasičnim modelom računara.*

**Ključne reči:** *kvantni paralelizam, kvantna interferencija, kolaps talasne funkcije*

## 1. UVOD

Mogucnosti kvantno-mehaničkih računara su usko povezane sa mogućnošću pronalaženja klasa problema koje kvantno-mehanički računari mogu efikasno da reše, teškoćama u otkrivanju efikasnih kvantno-mehaničkih algoritama, mogućnostima efikasne simulacije kvantno-mehaničkih sistema i tehnološka izvodljivost kvantno-mehaničkih računara koji mogu da nadmaše klasične računare u rešavanju važnih računarskih zadataka, [1].

Za razmatranje mogućnosti kvantno-mehanickih modela racunara ovom radu koristiće se kriterijumi, univerzalnosti, oblasti primene, efikasnosti i tehnoloških mogućnosti izrade kvantno-mehaničkih modela računara.

Univerzalnost daje odgovor na pitanje da li jedan model računske mašine može efikasno simulirati druge modele računskih mašina.

Domen primene daje odgovor na pitanje koje probleme dati model računara može da reši.

Efikasnost govori u kojoj meri se povećava potreba za memorijskim i vremenskim resursima računara sa povećanjem veličine problema.

Za potrebe ovoga rada uvode se i sledeći pojmovi:

Računar je fizički uređaj koji podržava obradu informacija tako što izvršava algoritme, [2]**.**

Računarski algoritam je precizno definisana procedura realizovana konačnim skupom instrukcija koja izvršava određeni računarski zadatak u konačnom vremenu, [3].

Kvantno-mehanickih model racunara je rezultat korišćenja fizičke realnosti o kojoj govori kvantno-mehanička teorija da bi se obavili zadaci koji su ranije smatrani nemogućim ili neizvodljivim na klasičnim računarima, [2].

Problem odlučivanja je problem čija rešenja mogu biti isključivo odgovori „da“ ili „ne“.

Ako se sa T(n) označi vreme, ili ekvivalentan broj koraka potrebnih da se reši problem ulazne dužine n, i ako se za bilo koju vrednost n mogu naći pozitivni brojevi k i p takvi da je $T(n) \leq kn^p$ , kaže se da se predmetni problem može rešiti za polinomijalno vreme, [4]**.**

Ako se mogu naći pozitivan broj k i broj c>1 takvi da je je $T(n) > kc^n$ za svako n, kaže se da je za rešavanje predmetnog problema potrebno eksponencijalno vreme,[4].

n označava veličinu problema,[4].

Adresa autora: Svetomir Simonović, Akademija tehničkih strukovnih studija Beograd, Katarine Ambrozić br. 3

e-mail: svetomir.simonovic@visokatehnicka.edu.rs

Rad primljen: 01.03.2022.

Rad prihvaćen: 15.06.2022.

Problemi koji se mogu rešiti za polinomijalno vreme se smatraju lakima, a predmetni algoritmi efikasnima. Problemi koji za svoje rešavanje zahtevaju eksponencijalno vreme smatraju se teškima, a predmetni algoritmi neefikasnima.

Pod zajedničkim osobinama funkcija podrazumevaju se srednja vrednost, medijana, period funkcije i sl.

## 2. TURINGOVE MAŠINE

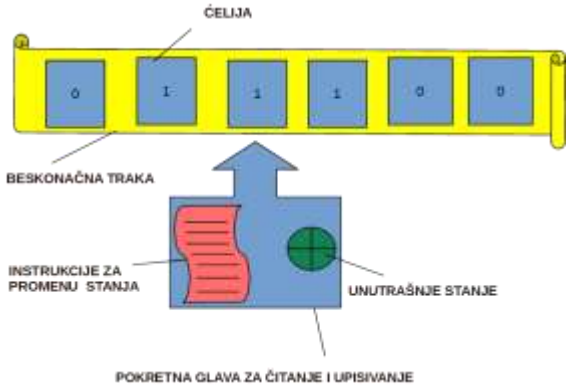
Najuticajniji model računara je koncipiran 1936. godine od strane Alana Turinga i nazvan je Turingova mašina, [5].

Turingova mašina je apstraktni koncepti računanja koji pruža preciznu matematičku formulaciju intuitivnog pojma algoritma,[1].

Turingova mašina (TM) je idealizovan matematički model računara koji se može iskoristiti za razumevanja granica sposobnosti računara, [6].

Opšta ideja koja stoji iza koncepta Turingove mašine je da ona obavlja računarske operacije onako kako bi to čovek uradio: čovek koji računa je sposoban da u svom mozgu čuva samo ograničenu količinu informacija ali ima na raspolaganju neograničen broj listova za operacije čitanja i pisanja ograničenog broja simbola na osnovu ograičenog broja pravila razmišljanja, [1]

Deterministička Turingova mašina je model računara koji se sastoji od konačnog skupa internih stanja, beskonačne trake podeljene u ćelije u koje se pomoću pokretne glave mogu upisivati i iz njih čitati simboli konačne azbuke, kao i funkcije prelaza (instrukcija za promenu stanja) koja na osnovu trenutnog internog stanja i simbola koji je trenutno pročitala glava jednoznačno specifikuje buduće stanje (slika 1), [2].




*Slika 1- Deterministička Turingova mašina*

Ako Turingova mašina sa trake pročita symbol S dok se nalazi u internom stanju G, ona će symbol S zameniti simbolom $S^1$, promeniti svoje interno stanje u stanje $G^1$ i pomeriti glavu u prvcu d (levo ili desno) za jedan korak. Turingova mašina je potpuno određena konačnim skupom tranzicionih pravila

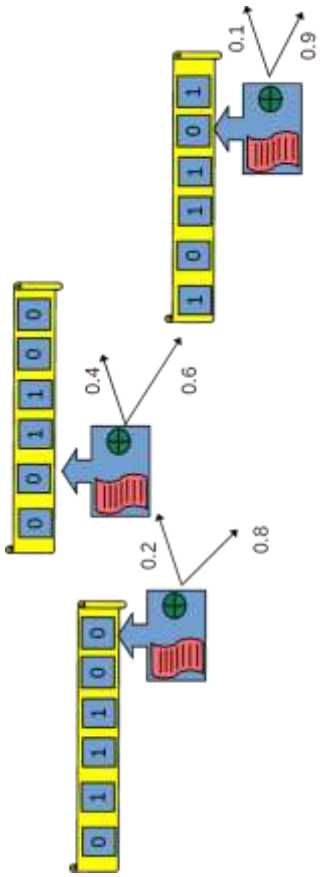
$$(S,G) \rightarrow (S^1, G^1, d)$$

gde je stanje Turingove mašine uređena dvojka (S,G). Jedno od internih stanja Turingove mašine je stanje "STOP", [7].

U početku je traka postavljena u standardizovano početno stanje, na primer takvo da su sve ćelije popunjene nulama osim onih koji sadrže program i početne podatke. Posle toga traka služi kao pomoćno sredstvo za zapisivanje međurezultata i eventualno, konačnog rezultata, [8].

Probabilistička Turingova mašina (PTM) ima sposobnost da napravi izbor između više narednih -ređenom stanju, kada pročita određeni simbol, ima samo jedno naredno stanje na raspolaganju, probabilistička Turingova mašina ima mogućnost da pređe u jedno od dva nareda stanja koje joj stoje na raspolaganju. U koje će naredno stanje probabilistička Turingova mašina preći zavisi od raspodele verovatnoća narednih stanja koje su joj na raspolaganju, kako je prikazano na slici 2.

Mnogi problemi koji zahtevaju dugo vreme da se reše na determinističkoj Turingovoj mašini često se mogu rešiti vrlo brzo na probabilističkoj Turingovoj mašini, [8**]**.

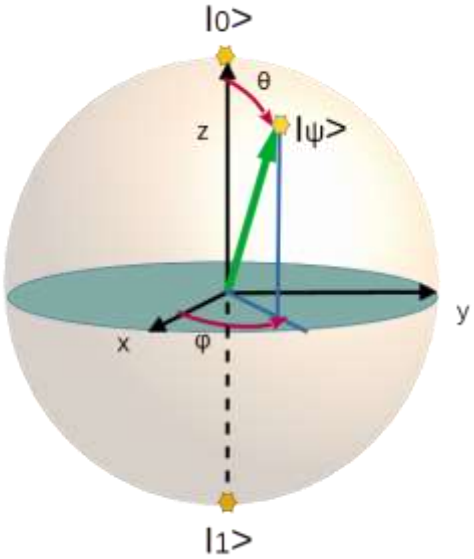



*Slika 2 - Probabilistička Turingova mašina*

Danas je poznato da Turingov model računanja ima nedostatke u smislu da je pod implicitnim

uticajem klasične fizike, zbog toga što „potpuna specifikacija njegovog stanja u svakom momentu odgovara skupu brojeva koji su u principu svi merljivi. Međutim, prema kvantnoj teoriji ne postoji fizički sistem sa takvim osobinama“,[9]. Kako gustina integralnih kola postaje sve veća, njihovo ponašanje potpada pod sve veći uticaj kvantno-mehaničkih fenomena. Ovi kvantno-mehanički fenomeni ograničavaju primenu klasičnog kompjuterskog hardvera, ali bi mogli da se iskoristite za stvaranje nove koncepcije računanja, što je dovelo do stvaranja koncepta kvantno-mehaničke Turingove mašine. Kod kvantno-mehaničke Turingove mašine (KTM) se operacije čitanja, pisanja i pomeranja obavljaju putem kvantno-mehaničkih interakcija i kod nje se „traka“ može nalaziti u stanjima koja se ne mogu opisati pojmovima klasične fizike. Posebno, dok kod klasične Turingove mašine ćelije „trake“ mogu sadržavati isključivo nule, jedinice ili biti prazne, kod kvantno-mehaničke Turingove mašine čelija može sadržavati istovremeno i nulu i jedinicu (kvantno-mehanička superpozicija). Otuda, kvantno-mehanička Turingova mašina ima mogućnost da istovremeno enkodira mnogo varijanti ulaznih podataka na istu „traku“ i da obavi operaciju računanja na svim ovim inputima istovremeno, i to za vreme koje je potrebno da se obavi jedna računska operacija na klasičan način (kvantni paralelizam) [9].

Ideja da elementarna jedinica informacije u ćelijama KTM pretstavlja mešavinu (superpoziciju) klasičnih jedinica informacija 0 i 1 (kubit) može se predstaviti putem jediničnog vektora koji definiše sferu, kako je prikazano na slici 3 (Blochova sfera). Pravac vektora „pravo naviše“ pretstavlja klasičnu 0, a „pravo naniže“ pretstavlja klasično 1. Ugao ovog vektora prema vertikalnoj osi pretstavlja meru odnosa 0 prema 1u kubitu.




*Slika 3 - Blochova sfera*

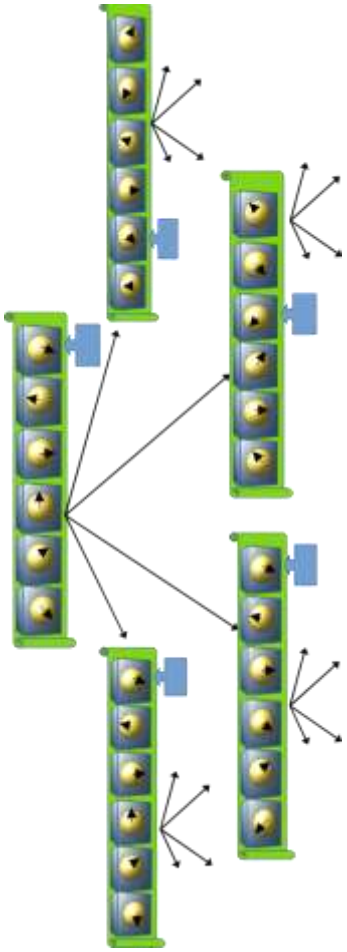
Kubit se može smatrati za reprezentaciju čistog Hilbertovog prostora stanja dvonivoinog kvantno-mehaničkog sistema, čija su elementarna stanja |0> i |1>, i koji se opisuje putem Dirakove “bra-ket” notacije kao složeno stanje (kvantno-mehaničko stanje jedne ćelije KTM)

$$|\psi> = \alpha\,|0> + \beta\,|1> \qquad (1)$$

gde su α i β kompleksni brojevi koji zadovoljavaju jednačinu $|\alpha|^2+|\beta|^2=1$; tako da merenje rezultuje stanjem |0> sa verovatnoćom $|\alpha|^2$ ili stanjem |1> sa verovatnoćom $|\beta|^2$. Formalno, kubit se pretstavlja u standardnoj ortonormalnoj bazi kao $\alpha|0> + \beta\,|1>$, pri čemu su bazni vektori.

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad i \qquad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

KTM se može opisati kao kvantno-mehanička generalizacija probabilističke Turingove mašine (PTM), kako je prikazano na slici 4.



*Slika 4- Kvantno-mehanička Turingova mašina*

Ako se traka PTM inicijalizuje i PTM pusti da radi tokom nekog vremena t bez nadgledanja njenog stanja, tada je stanje mašine određeno raspodelom verovatnoća prelaska u sva stanja koja se mogu doseći iz tog početnog stanja. Isto tako, ako se KTM

startuje od nekog početnog stanja i pusti da radi neko vreme t bez nadgledanja, tada je njeno stanje u momentu t opisano superpozicijom svih mogućih stanja koja mogu biti dosegnuta u momentu t. Ključna razlika je da se kod PTM ostvaruje samo jedna trajektorija prelaza a kod KTM se istovremeno ostvaruju sve moguće trajektorije prelaza pri čemu je rezultujuća superpozicija stanja rezultat zbira svih trajektorija koje se mogu ostvariti u vremenu t, kako je prikazano na slici 4. Pri tome strelice na slici 4 ne reprezentuju verovatnoće prelaza u naredno stanje nego amplitude verovatnoća iz kojih se mogu izvesti odgovarajuće verovatnoće [8, 9].

## 3. UNIVERZALNOST KVANTNO-MEHANIČKIH MODELA RAČUNARA

Koncept univerzalizma u računarskoj nauci počeo je da se razvija kada su Alan Turing, Alonso Church i Emil Post nezavisno stvorili, naizgled razlčite, matematičke modele procesa računanja, sa ciljem da budu slobodni od bilo kakve pretpostavke o njihovoj fizičkoj implementaciji, [5, 10, 11].

Post je ove modele identifikovao putem opštih rekurzivnih funkcija, Church ih je identifikovao takozvanim λ- definabilnim funkcijama a Turing ih je identifikovao klasom funkcija koje se mogu sračunati hipotetičnim postupkom računanja nazvanim Turingova mašina,[8].

Church je dokazao da su svi ovi modeli računanja međusobno ekvivalentni i predložio sledeći princip: „Svaki proces koji je po svojoj prirodi efektivan (algoritmički) definiše matematičku funkciju koja pripada specifičnoj, dobro definisanoj klasi, poznatoj pod različitim nazivima kao rekurzivna, λ- definibilna ili Turingovom mašinom sračunljiva klasa funkcija“, [12].

U svom seminalnom radu, [5], Turing je pokazao da postoji univerzalna Turingova mašina koja može simulirati bilo koju drugu Turingovu mašinu. Turing je, dalje, tvrdio da univerzalna Turingova mašina u potpunosti opisuje algoritamski postupak izvšavanja proizvoljnog računskog zadatka, ili u Turingovoj formulaciji: „Bilo koja funkcija koja bi se prirodno mogla smatrati za sračunljivu može se sračunati univerzalnom Turingovom mašinom“. Ova pretpostavka poznata je pod nazivom Church-Turingova teza.

Drugim rečima, ako se neki algoritam može izvršiti na bilo kakvom hardveru, tada postoji ekvivalentni algoritam za univerzalnu Turingovu mašinu koja će izvršavajući taj algoritam obaviti potpuno isti zadatak kao algoritam na predmetnom hardveru. Ovom tvrdnjom se uspostavlja ekvivalencija između fizičkog pojma klase algoritama koji se mogu izvršiti na nekom fizičkom uređaju sa rigoroznim matematičkim pojmom univerzalne Turingove mašine, [13].

U modernoj verziji Church-Turingova teza glasi: „Bilo koja funkcija koja bi se prirodno mogla smatrati za sračunljivu može se efikasno sračunati univerzalnom Turingovom mašinom“, [14].

Godine 1982. Richard Feynman je postavio pitanje da li se kvantna fizika može efikasno simulirati na klasičnim računarima? Istovremeno je dao dobre razloge za negativan odgovor, naime da ne izgleda moguće da klasična Turingova mašina može simulirati izvesne procese kvantne fizike a da ne dođe do eksponencijalnog usporenja u računanju. Šta više, spekulisao je sa idejom da bi se taj problem mogao rešiti postizanjem da računari rade na principima kvantne mehanike, [15], drugim rečima da bi kvantni računari mogli biti eksponencijalno brži u odnosu na klasične i biti prvi smisleni modeli računara koji se ne bi pokoravali modernoj verziji Church-Turingove teze. Međutim, iako je Feynman dao nekoliko primera u kojima jedan kvantni system simulira drugi, nije konkluzivno dokazao mogućnost postojanja „univerzalnog kvantnog simulatora“, [8].

Očigledna diskrepancija između Feynman-ovih zapažanja i Church-Turing-ove teze je navela Deutcha da 1985. predloži reformulaciju Church-Turingove teze u pojmove fizike: „Svaki fizički sistem koji se može realizovati konačnim sredstvima može se savršeno simulirati putem univerzalnog modela računske mašine koja radi na bazi upotrebe konačnih sredstava“, [9]. Ova teza može samo onda biti kompatibilna sa Feynman-ovim zapažanjima o efikasnosti simuliranja kvantnih sistema kada se model univerzalnog računara sam zasnuje na kvantnoj mehanici, [8].

Elaborirajući Feymanove ideje, Deutch je 1985. takođe pokazao da postoji univerzalna KTM, međutim njegov model univerzalne KTM imao je nedostatak da je simulaciju drugih KTM obavljao za eksponencijalno vreme,[16]. Ovaj problem su prevazišli Bernstein i Vazirani 1993. [17], i Yao 1993, [18], tako što su pokazali da postoji univerzalna KTM koja može simulirati druge KTM za polinomijalno vreme.

## 4. DOMEN PRIMENE KVANTNO-MEHANIČKIH MODELA RAČUNARA

Teorija domena primene daje odgovor na pitanje koje probleme dati model računara može rešitii (ili na koja pitanja može odgovoriti) u konačnom intervalu vremena. Ukoliko ne postoji algoritam (model računara) koji garantuje dobijanje datog odgovora u konačnom intervalu vremena kaže se da je taj odgovor nesračunljiv na predmetnom modelu računara, odnosno da nije u njegovom domenu primene.

Deutchov rad, [9], doveo je do finalne modifikacije Church-Turingove teze, tako da glasi: „Kvantna Turingova mašina može efikasno simulirati bilo koji realistični model računanja“, [19], što znači da kvantni računari mogu raditi najmanje sve ono što mogu klasični računari.

Takođe je za određivanje oblasti primene kvantno-mehaničkih modela računara relevantan Gödelov odgovor na Hilbertov problem odlučivanja (Entscheidungsproblem) kojim je postavljeno pitanje da li postoji algoritam pomoću kojeg se može proveriti istinitost proizvoljne matematičke tvrdnje, [8]. Godine 1930. Kurt Gödel je dokazao teoremu u kojoj se navodi da u bilo kom formalnom sistemu postoje tvrdnje matematičke prirode o čijoj se istinitosti ne može odlučiti, što znači da se ni afirmacije ni negacije tih tvrdnji ne mogu dokazati upotrebom aksioma i pravila predmetnog formalnog sistema, [20].

Kako fizika daje matematički model prirode, ona u suštini predstavlja formalni system pa navedena teorema takođe postavlja ograničenje za mogućnosti primene računara. To jest, uzevši u obzir da su računari zasnovan na fizici i da simuliraju fizičke sisteme, oni ne mogu odgovoriti na sva aritmetička pitanja, [1].

Moguće je izreći i specifičnije tvrdnje u vezi domena primene kvantno-mehaničkih modela računara. Prvi rad u ovoj oblasti dao je David Deutsch govoreći o kvantnim Turingovim mašinama. Deutsch je tvrdio da kvantno-mehanički modeli računara mogu sračunati izvesne veličine, kao što su pravi slučajni brojevi, koje nisu sračunljive bilo kojom determinističkom Turingovom mašinom. Klasična deterministička Turingova mašina može sračunavati isključivo funkcije, odnosno matematičke procedure koje daju jedinstvene, ponovljive odgovore. Međutim, postoje izvesni računski zadaci koji se ne mogu izvršiti evaluacijom nijedne funkcije. Na primer, ne postoji funkcija koja generiše prave slučajne brojeve. Sledi da klasična Turingova mašina može samo simulirati generisanje slučajnih brojeva, [9].

U istom radu Deutch uvodi ideju „kvantnog paralelizma“. Kvantni paralelizam se odnosi na to da se vrši samo jedna evaluacija funkcije na osnovu mešavine ili „superpozicije“ svih mogućih ulaza u funkciju, da bi se dobila superpozicija izlaza. Na taj način svi izlazi se sračunavaju za vreme koje je potrebno da se na klasičan način sračuna samo jedan izlaz. Međutim, ne mogu se dobiti svi ovi izlazi eksplicitno zbog toga što merenje izvršeno na izlaznom superponiranom stanju daje samo jedan rezultat, ali moguće je dobiti izvesne zajedničke osobine svih izlaza funkcije bez potrebe dobijanja bilo kakvog eksplicitnog izlaza [8].

Godine 1991. Richard Jozsa je dao matematičku karakterizaciju klase funkcija (tj. funkcija zajedničkih osobina) koje su sračunljive putem kvantnog paralelizma, [21]. On je otkrio da ako je f neka funkcija koja uzima celobrojne argumente u rasponu 1 do m i vraća binarnu vrednost, i ako funkcija neke zajedničke osobine izlaza funkcije f, uzima m binarnih vrednosti izlaza funkcije f i vraća jednu binarnu vrednost, tada je samo frakcija

$$\frac{2^{2^m}-2^{m+1}}{2^{2^m}}$$

svih mogućih funkcija zajedničkih osobina sračunljiva putem kvantnog paralelizma. Zbog toga sam kvantni paralelizam nije dovoljan da odgovori na sva pitanja koja se mogu postaviti u vezi zajedničkih osobina funkcija, [8].

Naravno, uvek se može klasična TM simulirati na KTM da bi se sračunala neka zajednička osobina ali to ne bi bilo racionalno jer takva kalkulacija ne bi bila efikasnija na kvantnom računaru nego na klasičnom. Međutim, sposobnost KTM da simulira TM znači da klasa funckija sračunljvih na KTM sadrži klasu funkcija sračunljivih na klasičnoj TM, [8].

Za razliku od lanca dokaza koji je proverljiv i opipljiv kod TM, kod KTM, zbog kvantne interferencije koja može nastati pri paralelnom računanju, potvrda o istinitosti neke tvrdnje može se dobiti bez postojanja načina da se izvrši uvid u sve računske operacije koje su dovele do potvrđivanja predmetne tvrdnje. Otuda, kod KTM, sposobnost da se nešto dokaže i sposobnost da se taj dokaz obrazloži su sasvim različiti pojmovi. Šta više, ako bi se pokušao izvršiti uvid u KTM u toku izvođenja nekog dokaza, da bi se dobile neke informacije o stanju dokazivanja u tom momentu, to bi nepopravljvo pokvarilo budući tok dokazivanja zbog kolapsa talasne funkcije, [8].

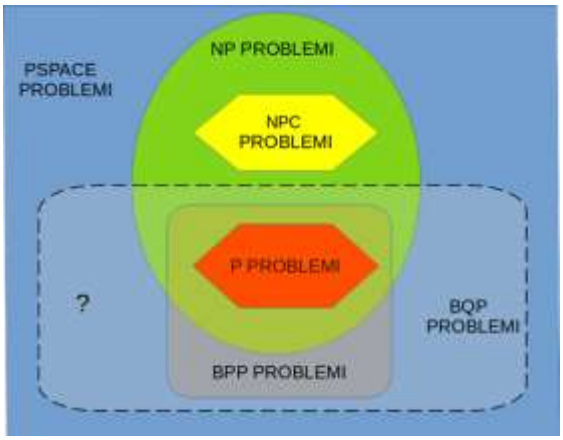
## 5. EFIKASNOST KVANTNO-MEHANIČKIH MODELA RAČUNARA

Deutsch, [9], je pokazao da kvantni paralelizam omogućava izvršavanje eksponencijalnog broja evaluacija neke funkcije za vreme za koje se obavlja samo jedna evaluacija na klasičan način. Međutim, pri tome kolaps talasne funkcije koji nastaje pri ekstrakciji informacija onemogućava da se ekstrahuje više od jednog rezultata evaluacije eksplicitno, a u procesu ekstrakcije se informacije o svim drugim rezultata evaluacije nepovratno gube.

Na taj način efikasnost nije bolja nego da se koristila klasična TM, odnosno, što se evaluacije funkcija tiče, kvantno-mehanički model računara nije bolji od modela klasičnog računara, [9].

U odgovoru na pitanje da li je moguće da kvantno-mehanički računar efikasno rešava računske probleme koji se ne mogu efikasno rešiti na klasičnim računarima sačinjeno je više kvantno-mehaničkih algoritama koji su potvrdili tu mogućnost, [22, 23, 24, 25, 26, …].

Do danas postoji samo nekoliko kvantno-mehaničkih algoritama od kojih se, uglavnom, jedni oslanjaju na Shorovu verziju Furijeove transformacije, a drugi na Groverov algoritam kvantno-mehaničkog pretraživanja, [13].




*Slika 5 - Pretpostavljeni odnos između različitih klasa efikasno sračunljivih računarskih problema*

Na slici 5. grafički su prikazani pretpostaljeni odnosi između različitih klasa računarskih problema koji se mogu rešiti efikasno klasičnim ili kvantno-mehaničkim algoritmima, [2].

Problemi klase PSPACE su problemi koji se mogu rešiti na malom računaru, ali pri tome nije neophodno da dužina vremena računanja bude mala. U klasi P nalaze se problem koji se mogu rešiti klasičnim algoritmima za polinomijalno vreme. U klasi NP nalaze se problem čija se rešenja mogu verifikovati klasičnim algoritmima za polinomijalno vreme, [19].

U klasi NPC nalaze se problemi na koje se mogu svesti svi NP problemi za polinomijalno vreme, [1].

U BPP klasi problema nalaze se problemi za koje postoji klasični algoritam koji daje ispravan odgovor sa verovatnoćom uspeha od najmanje 1/3. U BPQ klasi problema nalaze se problemi za koje postoji kvantni algoritmi koji daju ispravan odgovor sa verovatnoćom uspeha od najmanje 1/3, [14].

Zna se da je $P \subseteq BPP \subseteq BQP \subseteq SPACE$ *i* $P \subseteq NP \subseteq PSACE$. Do danas nije dokazana striktnost nijedne od inkluzija skiciranih na slici 5. Široko se veruje da $P \neq NP$ *i* $NP \neq PSPACE$. Očekuje se da je $BPP \neq BQP$, [2].

Gde se klasa BPQ tačno nalazi u odnosu na klase P, NP i PSPACE je do sada nepoznato. Ono što je poznato je da kvantni računari sve probleme u klasi P rešavaju efikasno i da ne mogu efikasno rešavati problem van klase PSPACE, pa klasa BPQ mora obuhvatati klasu P i biti sadržana u klasi PSPACE, kako je prikazano na slici 5, [13].

## 6. TEHNOLOŠKA IZVODLJIVOST

Umesto kao KTM, kvantni računari se iz praktičnih razloga razmatraju putem modela kvantnih kola, što je ekvivalentno, [18]. Kvantna kola se sastoje od „žica“ (kubita) i elementarnih „kvantnih kapija“ (unitarnih operacija nad jednim ili dva kubita). Iako je za neke računske probleme kvantni računar moćniji od klasičnog, još uvek je potrebno 50-1000 kubita i od 1.000 do 1.000.000 kvantnih kapija da se obave zadaci nedostupni klasičnim računarima (tačan broj zavisi od kvantnog algoritma), [1]. Za razbijanje konvencionalne enkripcije potrebno je oko 1.000.000 kubita, [28]. Isto tako potrebna je sposobnost kontrole evolucije velikog broja kubita za vreme potrebno da se ostvari veliki broj kvantnih kapija, a da pri tome ne dođe do dekoherencije. Takođe je radi korekcije grešaka potebno ostvariti dodatnih 1000 do 10000 kvantnih kapija, [1]. Ovi zahtevi su još daleko od ispunjenja, [28], pa se postavlja pitanje: da li je moguće napraviti kvantni računar koji će nadmašiti klasični računar u važnim računskim zadacima? I, ako jeste, kada će to biti moguće, [1]?

## 7. ZAKLJUČAK

Klasična Turingova mašina je antropocentrični model računanja, zasnovan na klasičnoj fizici, za koji su dati argumenti da je neefikasan pri simulaciji nekih kvantno-mehaničkih pojava. Mogu postojati problemi koji se ne mogu rešiti kvantno-mehaničkim modelom računanja zbog formalnosti kvantno-mehaničke teorije.

Zbog kvantnog paralelizma i interferencije, primenom kvantno-mehaničkog modela računanja je moguće dokazati istinitosti nekih tvrdnji i bez izvođenja dokaza. Kvantno-mehanički model računanja nema prednosti u odnosu na klasični model računanja kada je reč o eksplicitnom sračunavanju funkcija.

Pokazano je da postoje računarski problemi koji nisu evaluacije funkcija, za koje je moguće dizajnirati kvantno-mehaničke algoritme koji se izvršavaju za polinomijalno vreme, a za koji se ne može dokazati da postoje klasični algoritmi kojima se ti problemi rešavaju za polinomijalno vreme. Takođe, pokazano je da postoje računarski problemi koji ne spadaju u evaluaciju funkcija i koji se ne mogu rešiti kvantno-mehaničkim algoritmima, kao i da postoje problem koji se mogu rešiti isključivo kvantno-mehaničkim algoritmima.

Postoji samo nekoliko efikasnih kvantno-mehaničkih algoritama, [4].

Ne postoji dokaz da kvantno-mehanička Turingova mašina može efikasno simulirati sve fizičke sisteme. Na primer, u budućnosti bi se možda mogli pokazati adekvatniji modeli računara zasnovani na teoriji kvantnog polja, teoriji struna, kvantne gravitacije, [13]**,** ili mehanike jedinstvenog polja (unified field mechanic), [27].

I dalje postoji neizvesnost oko praktičnog izvođenja kvantnog računara, [5, 28].

LITERATURA


[1] Benenti G, Casati G, Strini G. *Principles of quantum computation and information*, World Scientific Publishing Co. Pte. Ltd. London, 2004.

[2] Kaye P. R, Laflamme R, Mosca M. *An Introduction to Quantum Computing*, Oxford University Press, New York, 2007.

[3] Tomašević M. V. *Strukture podataka*, Elektrotehnički fakultet Univerziteta u Beogradu, Beograd, 2000.

[4] Bernhardt C. *Quantum computing for everyone*, The MIT Press, Cambridge, Massachusetts, 2019.

[5] Turing A. On Computable Numbers with an Application to the Entscheidungsproblem, In *Proceedings of the London Mathematical Society*, Vol. 42, pp. 230-265, 1936.

[6] Hopcroft J. Turing Machines, *Scientific American*, May, pp. 86-98,1984.

[7] Stolze J, Suter D. *Quantum Computing A Short Course from Theory to Experimen*t, WILEY-VCH GmbH & Co. KGaA, Weinheim,2004.

[8] Williams C. P, Clearwater SH. *Explorations in quantum computing*, Springer-Verlag, New York, 1998.

[9] Deutsch D. Quantum Theory, the Church-Turing Principle, and the Universal Quantum Computer, In *Proceedings of the Royal Society of London*, Vol. A400, pp. 97-117, 1985.

[10]Church A. The Calculi of Lambda-Conversion, *Annals of Mathematics Studies*, No. 6, Princeton University Press,1941.

[11]Post E. Recursively Enumerable Sets of Positive Integers and their Decision Problems, *Bulletin of the American Mathematical Society*, Vol. 50, pp. 284-316, 1944.

[12] Shapiro S. (ed.). Church's Thesis, in: *Encyclopedia of Artificial Intelligence*, pp. 99-100, John Wiley & Sons, New York, 1990.

[13]Nielsen M, Chuang I. *Quantum Computation and Quantum Information*. Cambridge University Press, New York, 2010.

[14]Lanzagorta M, Uhlmann J. *Quantum Computer Science*, Morgan & Claypool, 2009. DOI 10.2200/S00-159ED1V01Y200810QMC002

[15]Feynman R. Simulating Physics with Computers, *International Journal of Theoretical Physics*, Vol. 21, Nos. 6/7, pp.

[16]Gruska J. *Quantum Computing*, McGraw-Hill, London, 1999.

[17]Bernstein E, Vazirani U. *Quantum Complexity Theory*, SIAM Journal on Computing, Vol. 5, No. 26, pp.1411–1473, 1997.

[18]Yao A. C. Quantum circuit complexity. In Proc. *34th Ann. IEEE Symp. on Foundations of Computer Science*, Computer Society Press, Los Alamitos, CA, USA, pp.352 –361, 1993.

[19]Pathak A. *Quantum Computation and Quantum Communication*, Taylor & Francis Group, Boca Raton, USA, 2014.

[20]Godel K. Uber formal unentscheidbare Satze der Printipia Mathematica und verwandter Systeme I, *Monatshefte fur Mathematik und Physik*, Vol. 38, pp. 173-98, 1931.

[21]Jozsa R. Characterizing Classes of Functions Computable by Quantum Parallelism, In *Proceedings of the Royal Society of London*, Vol. 1435, pp. 563-574, 1991.

[22]Deutsch D, Jozsa R. Rapid Solution of Problems by Quantum Computation, In *Proceedings of the Royal Society of London*, Vol. 439A, pp. 553-558, 1992.

[23]Berthiaume A, Brassard G. Oracle Quantum Computing, *Journal of Modern Optics*, Vol. 41, No. 12, pp. 2521-2535, 1994.

[24] Shor P. Algorithms for Quantum Computation: Discrete Logarithms and Factoring, in Proc. *35th Annual Symposium on Foundations of Computer Science*, Los Alamitos, CA, pp. 124- 134, 1994.

[25]Simon D. On the Power of Quantum Computation, *SIAM Journal on Computing*, Vol. 26, No. 5, pp. 1474–1483, 1997.

[26]Grover L. A Fast Quantum Mechanical Algorithm for Database Search, in Proc. *28th Annual ACM Symposium on the Theory of Computing*, Philadelphia, Pennsylvania, USA, pp. 212-219, 22–24 May 1996.

[27] Amoroso R. L. *Universal quantum computing: supervening decoherence - surmounting uncertainty*. World Scientific, Hackensack, 2017.

[28] Gibney E. Underdog tech makes gains in quantum computer race, *Nature*, No. 587, pp. 342-343, 2020.

## SUMMARY

ON CAPABILITIES OF QUANTUM-MECHANICAL COMPUTER MODELS

*The work includes the analyses of the theoretical capabilities of quantum-mechanical versus classical computer models in terms of their universality, their application domain, their efficacy in solving the problems and their technological feasibility. The concepts of deterministic Turing machine, probabilistic Turing machine and quantum-mechanical Turing machine are exposed. The concept of basic information unit of quantum-mechanical computer model- qubit is introduced and the qubit is represented through the use of Bloch sphere. The use of Dirac`s bra-ket notation in description of quantum-mechanical state is explained, and the notation is used to form state equation of a quantum-mechanical Turing machine cell. Especially, consequences of quantum parallelism, quantum interference and wave function collapse are studied in respect to capabilities of quantum-mechanical computer models. The interrelationship between classes of problems that can be efficiently solved by quantum mechanical and/or classical computer models is displayed.*

**Key Words:** *Quantum parallelism, Quantum interference, Wave function collapse*