NASTAVNO-NAUČNOM VEĆU ELEKTROTEHNIČKOG FAKULTETA U BEOGRADU

Na sednici Komisije za studije II stepena Elektrotehničkog fakulteta u Beogradu od 08.06.2021. godine, imenovani smo u Komisiju za pregled i odbranu master rada Nenada Popovića, dipl. inž. elektrotehnike, pod nazivom „Optimizacija i primena testova primalnosti na kvantnim računarima“. Posle analiziranja podnetog materijala Nastavno-naučnom veću podnosimo sledeći

I Z V E Š T A J

1. Biografski podaci o kandidatu

Dipl. inž. Nenad Popović rođen je 24.05.1991. godine u Šapcu. Završio je osnovnu školu "Cvetin Brkić" u Glušcima kao vukovac. Upisao je Matematičku gimnaziju u Beogradu 2006. godine, i završio je kao vukovac. Elektrotehnički fakultet u Beogradu upisao je 2010. godine. Diplomirao je na odseku za Softversko inženjerstvo 2019. godine sa prosečnom ocenom 9,27. Diplomski rad odbranio je u septembru 2019. godine sa ocenom 10. Diplomske akademske – master studije na Elektrotehničkom fakultetu u Beogradu, na Modulu za primenjenu matematiku, upisao je u oktobru 2019. godine.

2. Predmet, cilj i metodologija istraživanja

Predmet rada predstavlja razmatranje primene kvantnog računarstva na testove primalnosti. Cilj rada je prikaz mogućih kvantnih optimizacija nekih poznatih testova primalnosti, kao što su Fermaov test, Miler-Rabin test i AKS test. Pored toga, razmotriće se neki aspekti mogućih primena testova primalnosti na kvantnim računarima, poput generisanja velikih prostih brojeva, procene vrednosti funkcije raspodele prostih brojeva, procene gustine prostih brojeva blizanaca... Moguće primene se realizuju u programskom jeziku *Python* kroz frejmvork *Qiskit*, u okruženju *PyCharm*. Određeni broj eksperimenata vezanih za moguće primene biće izvršavan i na javno dostupnim *IBM*-ovim kvantnim računarima. Rezultati eksperimenata su probabilistički, i dati u formi histograma.

3. Sadržaj i rezultati

Master rad Popović Nenada podeljen je u pet poglavlja i napisan na 133 strane. Rad sadrži 47 slika i 6 tabela. U radu je priložen spisak korišćene literature.

U prvom poglavlju detaljno je predstavljen model kvantnog računarstva kao apstrakcija realnih kvantnih sistema, dat kroz poznati jezik linearne algebre. Predstavljen je matematički opis kubita kao vektora sa specifičnim svojstvima i notacijom. Opisan je skup kvantnih izračunavanja koje je moguće vršiti nad kubitima, a koja su u formi unitarnih operatora. Ilustrovana je operacija merenja, kao i njena probabilistička priroda. Na kraju, predstavljeno je trenutno stanje tehnologije kvantnih računara.

Drugo poglavlje predstavlja osvrt na najznačajnije kvantne algoritme. Opisana je kvantna Furijeova transformacija kao ključna komponenta brojnih algoritama. Predstavljena je operacija procene faze sopstvenih vrednosti unitarnih operatora koja koristi upravo kvantnu Furijeovu transformaciju. Ova operacija kasnije je generalizovana u kvantnom postupku pronalaženja reda po modulu, što se dalje generalizuje u Šorov algoritam faktorizacije. Detaljno je opisan Groverov algoritam pretrage nestrukturiranih skupova podataka. Predstavljen je i postupak kvantnog brojanja koji omogućava procenu broja rešenja koje neki problem može imati u datom prostoru pretrage.

U trećem poglavlju uvedeni su testovi primalnosti kao teorijski značajan skup algoritama u kriptografiji i primenjenoj matematici. Prvi prikazan test je najjednostavniji, test deljenjem gde se proveravaju svi delioci manji od $\sqrt{N}$. Sledeći test je ponovljeni Fermaov test koji se oslanja se na malu Fermaovu teoremu. Slede dva slična testa bazirana na poznavanju faktorizacije $N-1$, Lukaov i Poklingtonov test. Miler-Rabin test je dat zbog svoje praktične važnosti, i predstavlja uopštenje Fermaovog testa. Konačno, izložen je teorijski značajan AKS test koji je dokazao da je moguće vršiti determinističko testiranje primalnosti u polinomijalnom vremenu.

Četvrto poglavlje predstavlja neke potencijalne optimizacije algoritama iz prethodnog poglavlja na kvantnim računarima. Test deljenjem optimizovan je korišćenjem kvantnog brojanja. Za Fermaov i Miler-Rabin test nisu ostvarena značajna poboljšanja, osim u specifičnim slučajevima, ponovo korišćenjem kvantnog brojanja. Lukaov test optimizovan je korišćenjem Šorovog algoritma. Predstavljen je i test koji su kreirali Donis-Vela i Garsija-Eskartin, optimizovan specifično kvantnim pronalaženjem reda po modulu, čime se dobija novi, najefikasniji test primalnosti. Konačno, AKS test je detaljno optimizovan po koracima, čime je smanjen polinomijalni stepen složenosti.

U petom poglavlju, prikazane su moguće praktične upotrebe testova primalnosti, kroz eksperimente na kvantnim simulatorima, kao i na realnom kvantnom hardveru. Umesto realnih testova primalnosti, korišćena su jednostavnija kola sa istim efektom, zbog trenutnih ograničenja kako klasičnih, tako i kvantnih računara. Eksperimentalno je demonstriran mogući metod kreiranja velikih prostih brojeva sa kvadratnim ubrzanjem u poređenju sa klasičnim metodom. Takođe, prema algoritmu kvantnog brojanja, prikazane su implementacije i eksperimentalni rezultati za procenu vrednosti funkcije raspodele prostih brojeva, kao i funkcije raspodele prostih brojeva blizanaca, sa potencijalnom primenom za enormne vrednosti van domašaja klasičnih računara.

4. Zaključak i predlog

Kandidat Nenad Popović je u svom master radu predstavio detaljan prikaz kvantnog računarstva kao grane računarstva u povoju. Na primeru testova primalnosti, demonstrirao je neke moguće prednosti kvantnih računara u njihovoj optimizaciji. Pored toga, kreirao je eksperimente u formi programa napisanih u frejmvorku *Qiskit* koji demonstriraju praktičnu i inovativnu upotrebu testova primalnosti na kvantnim računarima, ukoliko oni postignu zadovoljavajuće uslove dimenzije ulaza i stabilnosti. Rezultati ovog rada doprinose popularizaciji inovativne grane kvantnog računarstva kroz predstavljene algoritme i implementirane programe, koji se jednostavno modifikuju za praktičnu upotrebu na budućem kvantnom hardveru.

Na osnovu izloženog, Komisija predlaže Nastavno-naučnom veću Elektrotehničkog fakulteta u Beogradu da rad Nenada Popovića pod naslovom „Optimizacija i primena testova primalnosti na kvantnim računarima" prihvati kao master rad i kandidatu odobri javnu usmenu odbranu.

U Beogradu, 28.06.2021.

Članovi komisije:

Branko Malešević

dr Branko Malešević, Redovni profesor

M. Rašajski

dr Marija Rašajski, Redovni profesor

Bojana Mihailović

dr Bojana Mihailović, Docent