UNIVERZITET CRNE GORE

PRIRODNO-MATEMATIČKI FAKULTET, PODGORICA

Vijeću Prirodno-matematičkog fakulteta Univerziteta Crne Gore

Predmet. Izvještaj komisije o pregledu i ocjeni master rada Balše Asanovića

Vijeće Prirodno-matematičkog fakulteta na sjednici održanoj 9.7.2024. godine, donijelo je Odluku o imenovanju mentora i komisije za ocjenu master rada pod nazivom "Algoritmi faktorizacije velikih brojeva u Rust-u" kandidata Balše Asanovića u sastavu:

1. dr Milenko Mosurović, redovni profesor PMF-a, mentor
2. dr Savo Tomović, redovni profesor PMF-a, član
3. dr Sanja Jančić Rašović, redovni profesor PMF-a, član.

Kandidat Balša Asanović je dana 31.3.2025. godine predao rukopis rada na uvid javnosti i ocjenu. Nakon uvida u podneseni materijal, a u vezi sa članom 22 Pravila studiranja na master studijama, podnosimo sledeći

IZVJEŠTAJ

Master rad pod nazivom"Algoritmi faktorizacije velikih brojeva u Rust-u" kandidata Balše Asanovića je oblast računarskih nauka, a uže oblasti su složenost algoritama i algoritmi u teoriji brojeva. Rad je napisan na 78 strana kucanog teksta. Sastoji se iz pet glava, zaključka i literature sa trideset jednom bibliografskom jedinicom. Svaka glava je podijeljena na više poglavlja u kojima se obrađuje jedna logička cjelina.

Prva glava je uvodnog karaktera. U njoj se navodi istorijski značaj i važnost faktorizacije, kao i pregled osnovnih algoritama faktorizacije. Pored toga ukazuje se na pogodnosti i prednosti koje pruža upotreba programskog jezika Rust za implementaciju algoritama faktorizacije.

Druga glava se odnosi na pregled matematičkih koncepata koji su osnova za algoritme faktorizacije. U ovoj glavi se daje i detaljan opis nekih od algoritama faktorizacije: Fermaova metoda, Polardov ro algoritam, Kvadratno sito i GNFS.

U trećoj glavi se daje pregled nekih kriptografskih metoda i veza kriptografije i faktorizacije velikih brojeva. Opisuje se RSA algoritam koji je osnova moderne kriptografije

sa javnim ključem, a čija sigurnost je usko povezana sa mogućnostima faktorizacije velikih brojeva.

Četvrta glava je posvećena programskom jeziku Rust. Rust je relativno noviji programski jezik koji je zbog nekoliko ključnih prednosti u odnosu na druge programske jezike stekao popularnost. Otuda se u okviru četvrte glave opisuju i analiziraju prednosti i novine koje donosi Rust, poput bezbjednosti memorije, konkurentnost, optimizacija performansi i sl.

U petoj glavi je opisan praktični dio rada tj. implementacija algoritama faktorizacije u programskom jeziku Rust kao i prikaz i analiza postignutih rezultata. Implementacija je poslužila za procjenu efikasnosti i upotrebljivosti različitih metoda za faktorizaciju, kako bi se u realnim uslovima testirala njihova vremenska složenost, korišćenje resursa, kao i mogućnosti koje Rust nudi za ovaj tip problema. Implementirani algoritmi uključuju Probnu podjelu (Trial Division), Fermaovu metodu, Polardovu ro metodu i Kvadratno sito (Quadratic Sieve). Izbor ovih algoritama pruža širok spektar pristupa metodama faktorizacije, od osnovnih do složenijih, te je omogućio uporednu analizu u pogledu performansi i optimizacija. Najvažniji djelovi koda su prikazani u okviru ovog poglavlja, dok se cjelokupan kod može naći na Github-u.

Počev još od antičkog doba matematičari su proučavali proste brojeve i faktorizaciju brojeva. Sem važnog teorijskog značaja u matematici faktorizacija postaje jedan od ključnih praktičnih problema u polju kriptografije pojavom RSA algoritma. Naime RSA algoritam je kriptografski algoritam sa javnim ključem, koji se intezivno koristi, a čija bezbednost se oslanja na još uvijek „teškoj" faktorizaciji velikih brojeva. Otuda se i u računarskim naukama intezivno proučavaju algoritmi faktorizacije velikih brojeva. O tome koliko je problem izazovan govori i činjenica da je još uvjek otvoreno pitanje kojoj klasi složenosti pripada zadatak faktorizacije na klasičnom računaru. Takođe, pojava Šortovog algoritma za faktorizaciju, koji pripada polinomijalnoj klasi na kvantnom računaru, uticala je na značajna ulaganja u kvantne tehnologije. Nažalost kvantni računari su na takvom stupnju razvoja da i dalje ne omogućavaju praktičnu primjenu Šortovog algoritma. Otuda je od ključnog značaja analiza i implementacija algoritama faktorizacije velikih brojeva na klasičnim računarima, što je i tema ovoga rada.

Postavljeni istraživački ciljevi su usmjereni ka dubljem razumijevanju i unapređenju algoritama faktorizacije, kao i njihovoj implementaciji u programskom jeziku Rust. Otuda su osnovni ciljevi master rada: 1) Analiza i razumijevanje ključnih algoritama faktorizacije, 2) Primjena u kriptografiji i teoriji brojeva, 3) Implementacija u Rust programskom jeziku, 4) Optimizacija i poboljšanje algoritama.

Kako bi se ostvarili postavljeni ciljevi i dali odgovore na istraživačka pitanja korišćene su različite metode. Osnovna metoda je matematička analiza problema. Naime s matematičkog aspekta razmatrane su teorijske osnove algoritama, uključujući i dokaze korektnosti algoritama. S druge strane, s računarskog aspekta analizira se vremenska složenost kao i samo vrijeme izvršavanja implementiranih algoritama. Otuda je korišćena komparativna analiza za upoređivanje različitih algoritama u zavisnosti od veličine i osobina brojeva koji se faktorišu. Korišćenjem ove metode indentifikovani su najprikladniji algoritmi za brojeve sa određenim svojstvima. Ključni izazovi u implementaciji ovih algoritama leže u potrebi upravljanja

ogromnim količinama podataka, kompleksnoj linearnoj algebri i optimizaciji performansi na nivou memorije i procesora. Implementacijom u Rust-u, prevaziđeni su mnogi od ovih izazova koristeći prednosti jezika kao što su stroga bezbjednost memorije, programiranje niskog nivoa, visoke performanse kompajliranja i drugo.

Rezultat ovoga rada je i softver, razvijen u programskom jeziku Rust, za faktorizaciju velikih brojeva što omogućava njihovu praktičnu primjenu i dalje analize i optimizacije. Doprinos rada je i u detaljnoj analizi i praktičnoj demonstraciji kako odabir savremenog programskog jezika kao što je Rust može značajno unaprijediti efikasnost i praktičnost algoritama za faktorizaciju. Pored toga master rad se može koristiti i u edukativne svrhe za istraživanje algoritama faktorizacije velikih brojeva.

ZAKLJUČAK

Nakon pregledanog master rada komisija konstatuje da rad zadovoljava sve uslove propisane Pravilima studiranja na master studijama. Kandidat je pokazao da odlično poznaje naučnu problematiku, kao i da posjeduje značajan nivo istraživačkih sposobnosti. Stoga, komisija pozetivno ocjenjuje master rad pod nazivom „Algoritmi faktorizacije velikih brojeva u Rust-u", kandidata Balše Asanovića.

Komisija predlaže Vijeću Prirodno-matematičkog fakulteta da rad pod naslovom „Algoritmi faktorizacije velikih brojeva u Rust-u", kandidata Balše Asanovića prihvati kao master rad i odobri njegovu javnu odbranu.

U Podgorici, 27.5.2025. godine

Komisija

dr Milenko Mosurović, redovni profesor PMF-a, mentor

Mosurović

dr Savo Tomović, redovni profesor PMF-a, član

dr Sanja Jančić Rašović, redovni profesor PMF-a, član

Sanja Jančić Rašović