Наставно-научном већу
Математичког факултета
Универзитета у Београду

Одлуком Наставно-научног већа Математичког факултета у Универзитета у Београду, донетом на 294. Седници, која је одржана 07.05.2010. године, именовани смо у комисију за преглед и оцену рукописа **„Аутоматско генерисање и проверавање услова исправности програма“** који је предат као докторска дисертација **мр Милене М. Вујошевић Јаничић**, дипломираног математичара. Након прегледа рукописа, подносимо следећи

Извештај

1. Биографија кандидата

Милена Вујошевић Јаничић рођена је 3. јуна 1980. године у Београду, где је завршила основну школу Иван Горан Ковачић и Математичку гимназију. Студије на смеру Рачунарство и информатика на Математичком факултету у Београду уписала је 1999. године. Током студија имала је две стручне праксе, на универзитету државе Ајова (САД) и на Политехничком универзитету у Хонг Конгу (Кина). Била је добитник стипендије Краљевског дома Карађорђевића, стипендије Владе Србије, стипендије краљевине Норвешке и стипендије Републичке фондације за развој научног и уметничког подмлатка. Дипломирала је 2004. године са просечном оценом 9.86 (од 10.00) и уписала магистарске студије на истом смеру. Исте године била је изабрана у звање асистента-приправника на Математичком факултету. Магистарски рад под називом „Аутоматско откривање прекорачења бафера у програмском језику C” одбранила је 2008. године. Изабрана је у звање асистента на Математичком факултету 2009. године. Током досадашњег рада на Математичком факулету држала је вежбе из шест предмета. Бави се истраживањима у области верификације софтвера, пре свега у подобласти аутоматског откривање грешака техникама симболичког извршавања и проверавања модела, као и применама верификацијских техника у образовању. Учествовала је у раду више међународних радионица и летњих школа и боравила је у истраживачкој

посети универзитету EPFL у Лозани (Швајцарска). Објавила је радове на водећим међународним форумима из области верификације софтвера.

2. Проблем и садржај тезе

Рукопис кандидата мр Милене М. Вујошевић Јаничић под називом „Аутоматско генерисање и проверавање услова исправности програма“ (у даљем тексту рукопис) састоји се из: резимеа на српском и енглеском језику, предговора, садржаја, шест глава, литературе, додатка, биографије аутора и три изјаве. Рукопис има 163 стране, 181 библиографску јединицу и у оквиру тога 6 самоцитата.

У рукопису се разматра проблем аутоматског испитивања исправности софтвера. Испитивање исправности софтвера један је од кључних проблема у развоју софтвера. Грешке у софтверу коштају светску економију милијарде долара годишње, а могу имати и материјално немерљиве последице. У рукопису је представљен нови верификацијски систем LAV за аутоматско проналажење грешака и проверавање услова исправности у императивним програмским језицима. Приказана је имплементација и експериментална евалуација система, као и примена система у унапређивању аутоматске евалуације студентских програма.

У уводу је истакнут значај верификације софтвера, наведена је мотивација и истакнут је циљ израде тезе. Описани су основни доприноси тезе, као и организација тезе.

У другој глави укратко су описани појмови и технике који се користе у остатку рукописа: општи приступи верификацији софтвера, најчешће коришћене теорије за моделовање понашања и услова исправности програма, решавачи који се за ове теорије користе и међујезици који се користе за трансформацију и анализу програма.

У трећој глави описан је систем LAV за статичку анализу, генерисање и проверу услова исправности императивних програма. Систем обавља комуникацију са другим системима ради трансформисања кода у форму која је погодна за анализу и ради добијања информација о ваљаности генерисаних формула. Систем обухвата моделовање понашања програма, конструкцију услова исправности програма, трансформисање конструисаних услова у формуле одговарајућих теорија, испитивање ваљаности формула у оквиру изабране теорије и генерисање одговарајућег извештаја за корисника.

Четврта глава садржи опис реализације предложеног система и његове перформансе. Систем LAV имплементиран је у програмском језику C++, отвореног је кода и јавно је доступан. Имплементација, без интерфејса ка решавачима и помоћних класа за рад са дељеним изразима, садржи око 10 000 линија кода. LAV анализира програме на језику ниског нивоа LLVM, а

развијан је првенствено за анализу програма добијених трансформацијом од програма написаних у програмском језику C. У оквиру алата LAV постоји подршка за рад са неколико SMT решавача (Boolector, MathSAT, Yices и Z3). Експериментални резултати на релевантном корпусу C програма, који служе за утврђивање могућности верификацијских алата, показују да је представљен алат упоредив са постојећим сродним алатима. Такође, експерименталне резултати показују предност предложеног компактног моделовања путања кроз програм у односу на симболичко извршавање, посебно за програме у којима постоји велики број могућих путања.

У петој глави разматра се примена система LAV. Акцент је на провери програма које развијају студенти у оквиру уводних курсева програмирања. У овој глави, детаљно се описују доприноси примене верификацијског алата у аутоматској евалуацији студентских радова. Верификацијски алат може да помогне студентима указујући на грешке у програму у ситуацијама када наставник није у близини (што је најчешће случај), док за наставнике верификацијски алат може да буде користан за аутоматско оцењивање студентских радова.

Шеста глава садржи закључке и дискусију о могућим правцима даљих истраживања. Даља истраживања укључују унапређивање прецизности моделовања и ефикасности самог система, унапређивање имплементације алата, као и развој одговарајућег окружења за аутоматску евалуацију студентских програма.

У додатку А детаљно је описана употреба система LAV: представљен је поступак инсталације система, начини коришћења и излаз који систем генерише.

3. Полазне претпоставке

Постоје разнородни приступи статичкој аутоматској верификацији програма. Ови приступи се разликују по ефикасности и прецизности, а њихова практична примена зависи од програмског језика и врсте грешака које имају за циљ да открију. Приликом израде тезе, пошло се од претпоставке да је могуће креирати практично употребљиви, хибридни систем за верификацију и аутоматско откривање грешака у софтверу процедуралних програмских језика, који је у стању да превазиђе неке од слабости појединачних, широко коришћених, метода које комбинује (симболичко извршавање и проверавање ограничених модела).

4. Научни методи који су коришћени у раду на тези

Систем за верификацију софтвера предложен у овој тези заснован је на општем методу статичке верификације програма. Овај метод представља испитивање исправности програма без његовог извршавања, анализом кода. У оквиру овог метода, за моделовање понашања програма коришћени су методи проверавања ограничених модела и симболичког извршавања. У имплементирању предложеног система, коришћени су стандардни методи развоја објектно-оријентисаног софтвера.

5. Остварени научни допринос истраживања

У наставку текста набројани су основни доприноси тезе.

1. Развијен је систем LAV који на нов начин комбинује постојеће технике верификације и који уводи новине у моделовање контроле тока програма. Систем се заснива на анализи кода ниског нивоа, па га је могуће применити на различите процедуралне програмске језике.

2. Развијена је имплементација предложеног система. Имплементација предложеног система, алат LAV, отвореног је кода и јавно је доступна.

3. Експериментални резултати поређења имплементације система и сродних алата показују да је предложени систем упоредив по ефикасности са постојећим сродним техникама, као и да је примењив на класу програма који су ван домашаја техника симболичког извршавања. Развијен систем, имплементација и експериментална евалуација представљени су на водећој конфернецији из области верификације софтвера: ,,Verified Software: Theories, Tools, and Experiments''.

4. Алат LAV успешно је примењен у домену универзитетког образовања. Овом применом показано је да у студентским радовима постоји велики број грешака које верификацијски алат може ефикасно да пронађе, да верификацијски алати могу да допринесу проналажењу грешака које су ван домашаја техника које се тренутно доминантно користе у овом контексту, као и да верификацијски алат може значајно да унапреди аутоматску евалуацију студентских радова. Ови резултати објављени су у часопису категорије M21 ,,Information and Software Technologies''.

6. Главне референце које су генерисане у току рада на тези

Један део резултата тезе већ је објављен у часопису са SCI листе категорије M21, зборницима водећих међународних конференција, као и у часописима од националног значаја, док је други део у припреми за објављивање. Поред тога, резултати тезе су излагани на 4 међународне радионице, као и на семинару током посете аутора универзитету EPFL у Лозани у Швајцарској.

Листа референци (у свима радовима је аутор тезе први аутор):

[1] Milena Vujošević Janičić. Ensuring Safe Usage of Buffers in Programming Language C. In Proceedings of ICSOFT 2008 --- Third International Conference on Software and Data Technologies, Volume PL/DPS/KE, pages 29--36, 2008.

[2] Milena Vujošević Janičić, Dušan Tošić. The Role of Programming Paradigms in the First Programming Courses. The Teaching of Mathematics, Issue XI_2, pages 63-83, 2008.

[3] Milena Vujošević Janičić, Filip Marić, Dušan Tošić. Using Simplex Method in Verifying Software Safety. Yugoslav Journal of Operations Research, Volume 19, no 1, pages 133–148, June 2009.

[4] Milena Vujošević-Janičić, Viktor Kuncak: Development and Evaluation of LAV: an SMT-Based Error Finding Platform. Verified Software: Theories, Tools, Experiments. Lecture Notes in Computer Science, Volume 7152, pages 98–113, Springer 2012.

[5] Milena Vujošević-Janičić, Mladne Nikolić, Dušan Tošić, Viktor Kuncak: Software Verification and Graph Similarity for Automated Evaluation of Students' Assignments. Information and Software Technology, 55(6):1004 – 1016, Elsevier 2013.

Поред наведених радова, кандидат има 6 радова (један у часопису са SCI листе, а остали у зборницима са конференција) који су индиректно везани за резултате тезе.

7. Закључак

У рукопису: **„Аутоматско генерисање и проверавање услова исправности програма“** кандидат мр Милена М. Вујошевић Јаничић је на нов и оригиналан начин темељно обрадила проблематику аутоматског откривања грешака у софтверу. Осмишљен је нови верификацијски систем, реализована је његова имплементација, експериментално је потврђена ефикасност предложеног система, а систем је и успешно примењен за проналажење грешака у студентским програмима. Значај ове тезе је и у томе што она (по нашим сазнањима) садржи прве резултате у нашој земљи, као и први научни текст на српском језику из области аутоматске верификације софтвера, области која је све важнија у савременом свету.

С обзиром на изложено, може се констатовати да су испуњени главни циљеви наведени приликом предлагања теме. Сматрамо да научно истраживање приказано у овом раду даје значајан допринос решавању проблема верификације и аутоматског откривања грешака у софтверу. Стога предлажемо Наставно-научном већу да поменути рукопис прихвати као докторску дисертацију и одреди комисију за јавну одбрану.

Београд, 28.8.2013.

Чланови комисије:

др Душан Тошић
редовни професор
Математички факултет у Београду

[redacted]
др Виктор Кунчак
ванредни професор
EPFL, Лозана, Швајцарска

др Филип Марић
доцент
Математички факултет у Београду