

УНИВЕРЗИТЕТ У БЕОГРАДУ
МАТЕМАТИЧКИ ФАКУЛТЕТ

Катедри за рачунарство и информатику

Пријава теме за израду докторске дисертације

Молим да ми одобрите израду докторске дисертације под насловом *„Формализација различитих модела геометрије и примене у верификацији аутоматских доказивача теорема”*.
Тему предлажем у договору са ментором др Филипом Марићем.

Подносилац пријаве

Данијела Симић

Ментор:
др Филип Марић

Београд, новембар 2015.

**Наставно-научном већу Математичког факултета
Универзитета у Београду**

**Пријава теме за израду докторске тезе
кандидата Данијеле Симић (девојачко Петровић):**

**Формализација раличитих модела геометрије и примене у формализацији
аутоматских доказивача теорема**

1 Подаци о кандидату

1.1 Биографија

Данијела Симић је рођена 26.09.1986. године у Ваљеву. Основну школу Жикица Јовановић Шпанац завршила је као ђак генерације и вуковац. Потом је уписала Ваљевску гимназију, коју је такође завршила као ђак генерације и вуковац. Током школовања учествовала је на бројним такмичењима при чему се посебно истичу резултати и награде са републичких и савезних такмичења из физике и програмирања. Године 2005. уписала је Математички факултет, универзитета у Београду, смер Рачунарство и Информатика. Студије је завршила 2009. године са просечном оценом 9.86. Исте године уписала је докторске студије на смеру Информатика. Положила је све испите на докторским студијама са просечном оценом 10.

Запослена је на Математичком факултету, Универзитета у Београду од 2009. године и држала је вежбе из следећих предмета:

- Програмирање 1
- Програмирање 2
- Увод у организацију рачунара
- Вештачка интелигенција

1.2 Списак научних радова

Објављени радови

- Filip Marić, Ivan Petrović, Danijela Petrović, Predrag Janičić: *Formalization and Implementation of Algebraic Methods in Geometry*. Electronic Proceedings in Theoretical Computer Science 79, pp. 63–81.
- Filip Marić, Danijela Petrović: *Formalizing Complex Plane Geometry*. Annals of Mathematics and Artificial Intelligence, November 2014
- Danijela Simić: *Using Small-Step Refinement for Algorithm Verification in Computer Science Education*. Accepted for publication in The International Journal for Technology in Mathematics Education, Volume 22, Number 4 (December 2015)

Саопштења на научним скуповима

- Danijela Petrović, Filip Marić: *Formalizing Analytic Geometries*. Automated Deduction in Geometry 2012, Edinburgh, UK, 2012.
- Danijela Petrović: *Using Small-Step Refinement for Algorithm Verification in Computer Science Education*. ThEdu'14

1.3 Конференције и летње школе

- Automated Deduction in Geometry, Automated Deduction in Geometry 2012, Единбург, Велика Британија, 17.09. – 19.09.2012.
- European Summer School in Logic, Language and Information, Љубљана, Словенија, 01.08. – 12.08.2011
- Више пута презентовала и учествовала у организацији радионица ARGO групе

2 Преглед области тезе и постојећих резултата

2.1 Формално доказивање теорема геометрије

У класичној математици постоји много различитих геометријских теорија. Такође, различита су и гледишта шта се сматра стандардном (Еуклидском) геометријом. Понекад, геометрија се дефинише као независна формална теорија, а понекад као специфични модел. Наравно, везе између различитих заснивања геометрије су јаке. На пример, показује се да Декартова равна представља модел формалних, аксиоматских теорија геометрије.

Традиционална Еуклидска (синетичка) геометрија је још од античке Грчке заснована често на малом скупу основних појмова (на пример, тачке, праве, релације између, релације подударности итд.) и на скупу аксиома које имплицитно дефинишу ове основне појмове. Иако су Еуклидови „Елементи” један од најутицајнијих радова из математике, у савременом схватању они не пружају довољно прецизан геометријски систем јер често користе имплицитне претпоставке настале због погрешне интуиције или погрешног позивања на слике. Ове празнине су утицале на појаву других аксиоматских система чији је циљ био да дају формалну аксиоматизацију Еуклидове геометрије. Најважнији су Хилбертов систем аксиома, систем аксиома Тарског, као и Авигадов систем аксиома који представља савремену реформулацију оригиналног Еуклидовог система.

Хилбертов систем се састоји из три основна појма (тачка, права и равна), 6 предиката и 20 аксиома подељених по групама. Хилберт није желео ништа да остави интуицији. Овакав приступ је повећао ниво ригорозности не само у геометрији, него у целој математици.

Систем Тарског је мањи, састоји се од једног основног појма (тачка), 2 предиката и 11 аксиома и његова основна предност у односу на Хилбертов систем је у његовој једноставности. Са друге стране, систем Тарског уводи појам праве као скупове тачака што доста отежава резонување јер захтева да се у доказима користи теорија скупова.

Једно од најзначајнијих открића у математици, које датира из XVII века, јесте Декартово откриће координатног система и оно је омогућило да се алгебарским изразима представе геометријске фигуре. То је довело до рада на новој математичкој области која је названа аналитичка геометрија.

Иако се појам сферне геометрије појавио још у старој Грчкој, озбиљније истраживање неевклидске геометрије је започето 1829. године са радом Лобачевског. Ипак, са интензивнијим истраживањем неевклидских геометрија се почело тек после пола века. Оно што је највише утицало на ову промену јесте откриће комплексних бројева крајем XVIII века. Комплексни бројеви су представљали значајану алатку за истраживање особина објеката у различитим геометријама. Заменом Декартове координатне равни комплексном равни добијају се једноставније формуле које описују геометријске објекте. Након Гаусове теорије о закривљеним површинама и Римановог рада о многострукостима, геометрија Лобачевског добија на значају. Ипак, највећи утицај има рад Белтрамија који показује да дводимензионална неевклидска геометрија је ништа друго до изучавање одговарајуће површи константне негативне кривине. Уводи и појам пројективног диска модела који је касније популаризован од стране Клајна. Поинкаре посматра модел полуравни који су предложили Лиувил и Белтрами и пре свега изучава изометрије хиперболичке равни које чувају оријентацију. Данас се те трансформацију најчешће називају Мебијусове трансформације.

- David Hilbert. *Grundlagen der Geometrie*. Leipzig, B.G. Teubner, 1903.
- W. Schwabhäuser, W. Szmielew, and A. Tarski. *Metamathematische Methoden in der Geometrie*. Springer-Verlag, 1983.
- Tristan Needham. *Visual Complex Analysis*. Oxford University Press, 1998.
- Hans Schwerdtfeger. *Geometry of Complex Numbers*. Dover Books on Mathematics. Dover Publications, 1979.

2.2 Интерактивно доказивање теорема уз помоћ рачунара

Потреба за ригорозним заснивањем математике постоји веома дуго и са развојем математике повећавао се и степен ригорозности. Међу наукама, математика се издваја својим прецизним језиком и јасним правилима за изношење аргумената. Ова чињеница омогућава да се математички докази моделују као формална аксиоматска извођења. Још у седамнаестом веку, постојала је идеја да мора постајати формалан језик којим би се могла записати математичка тврђења и систем правила извођења теорема. Један од најзначајних напретка у математици почетком двадесетог века био је у открићу да се математички аргументи могу представити у формалним аксиоматским системима на такав начин да њихова исправност се може једноставно испитати коришћењем једноставних механичких правила. Генерално, математика се могла формализовати коришћењем аксиоматске теорије скупова и теорије типова. Математички доказ је ригорозан ако може бити записан у логици првог реда као низ закључака који су изведени применом дефинисаних правила из аксиоматске теорије скупова.

Често, механички проверени докази попуњавају празнине које постоје у дефиницијама и доказима и упућују на дубљу анализу теме која се изучава. У историји математике постоји пуно контроверзи око исправности математичких аргумената. Године 1935. Лекат је објавио књигу о грешкама које су до 1900. године направили познати математичари. Поред грешака, често се дешавало да математичари нису умели да одреде да ли је неки доказ исправан или не и дешавало се да се у потпуности верује да је доказ тачан ако га је објавио познати математичар, као Гаус или Коши, и њихови докази нису подлежали дубљој критици. У деведнаестом веку докази постају све комплекснији и математичари почињу да све више

истичу важност ригорозности доказа. Математичари се свакодневно сусрећу са прескоченим корацима у доказима, са непрецизним дефиницијама, са хипотезама и претпоставкама које недостају. Понекад грешке у доказима не буду примећене јако дуго. На пример, први доказ теореме о обојивости графа са четири боје је имао грешку која је уочена тек десет година касније. Грешке је углавном лако исправити, али има случајева када је то јако тешко. На пример, 1980. године објављено је да је завршена класификација простих коначних група, али је примећено да постоји пропуст у једној од класа и исправка тог пропуста објављена је тек 2001. године, а доказ је имао 1221 страну. Додатно, често се дешава да се одређени делови доказа никада не покажу, често уз реченицу „специјалан случај се тривијално показује” при чему се дешава да за тај специјалан случај тврђење не важи или га није тривијално показати. Поред овога, понекад је потребно много времена да би се неки доказ проверио. На пример, доказ Томаса Хејлса Кеplerове хипотезе има 300 страна и 12 рецензената је провело четири године анализирајући доказа и закључили су само да су 99% сигурни да је доказ исправан.

Многи научници су сматрали да потпуна формализација математике је недостижни идеал. Са појавом рачунара настала је могућност генерисања машински проверивих доказа. Тако су се појавили системи за доказивање теорема уз помоћ рачунара и они су или потпуно аутоматски или интерактивни.

Многи системи за доказивање теорема се заснивају на интеракцији корисника и рачунара. Системи који се заснивају на логикама вишег реда су полуаутоматски и у процесу формалног доказивања теорема од стране корисника (често програмер и/или математичар) помажу тако што контролишу исправност доказа и, колико је то могуће, проналазе аутоматске доказе. Ови *интерактивни доказивачи* се називају и *асистенти за доказивање теорема*. Данас постоји много интерактивних доказивача: Isabelle, Isabelle/HOL, Coq, HOL Light, PVS и други. Посебно се истичу Isabelle/HOL и Coq као системи са већим бројем корисника који су током година развили велики скуп библиотека са формално доказаним теоријама које је могуће даље надограђивати. Асистенти за доказивање теорема се користе у различитим областима. Пре свега, истиче се примена у образовању. Поред тога, могу се користити и за формалну верификацију рачунарских програма. Помажу развој и продубљивање математичког знања.

У последњих десет година направљени су значајни резултати у формализацији математике коришћењем интерактивних доказивача. Формално је доказана Брауерова теорема фиксне тачке, основна теорема алгебре, Гodelова теорема некомплетности, реална анализа и многи други велики фрагменти математике. У најзначајније постигнуте резултате до данас могу се убројати формализација теореме о простим бројевима коју је урадио Цереми Авигад, затим формални доказ о обојивости графа са четири боје. Важно је поменути и пројекат Flyspeck који је покрену Томас Хејлс да би могао формално да докаже Кеplerову хипотезу. У оквиру овог пројекта формално је показано много математичких тврђења и он има велику базу математичког знања која може да послужи у неким новим формализацијама. Поред формализације математике, коришћењем асистената за доказивање теорема рађена је и верификација софтвера. Значајан резултат је CompCert, формално верификован компилатор и L4, формално верификован оперативни систем.

Постоји велики број формализација фрагмената различитих геометрија у оквиру интерактивних доказивача теорема. Делови Хилберове књиге „Основи геометрије” су формализовани у Isabelle-у и Coq-у. У оквиру система Coq је формализована геометрија Тарског, конструктивна геометрија, пројективна геометрија, геометрија лењира и шестара и друге.

Неки од најзначајних радова из формализације геометрије су:

- Laura Meikle and Jacques Fleuriot. *Formalizing Hilberts Grundlagen in Isabelle/Isar*. In Theorem Proving in Higher Order Logics, volume 2758 of Lecture Notes in Computer Science. Springer, 2003.
- Phil Scott. *Mechanising Hilberts Foundations of Geometry in Isabelle*. Master's thesis, University of Edinburgh, 2008.
- Julien Narboux. *Mechanical Theorem Proving in Tarski's Geometry*. In Automated Deduction in Geometry, volume 4869 of Lecture Notes in Computer Science. Springer, 2007.
- Gilles Kahn. *Constructive geometry according to Jan von Plato*. Coq contribution, Coq V5.10, 1995.
- Frédérique Guillhot. *Formalisation en Coq et visualisation d'un cours de géométrie pour le lycée*. Technique et Science Informatiques, 24(9), 2005.
- Nicolas Magaud, Julien Narboux, and Pascal Schreck. *Formalizing Projective Plane geometry in Coq*. In Automated Deduction in Geometry, volume 6301 of Lecture Notes in Computer Science. Springer, 2011.
- Stojanović, Sana, Vesna Pavlović, and Predrag Janičić. *A coherent logic based geometry theorem prover capable of producing formal and readable proofs*. Automated Deduction in Geometry. Springer Berlin Heidelberg, 2011. 201-220.

Формализација система Тарски за неевклидске геометрије (Клајн-Белтрами модел) урађена је у раду:

- Timothy James McKenzie Makarios. *A mechanical verification of the independence of Tarski's Euclidean axiom*. Master's thesis, Victoria University of Wellington, 2012.

Формализација комплексне анализе може се видети у радовима:

- Robert Milewski. *Fundamental theorem of algebra*. Formalized Mathematics, 9(3), 2001.
- Herman Geuvers, Freek Wiedijk, and Jan Zwanenburg. *A Constructive Proof of the Fundamental Theorem of Algebra without Using the Rationals*. In Types for Proofs and Programs, volume 2277 of Lecture Notes in Computer Science. Springer, 2002.

2.3 Аутоматско доказивање теорема

Системи који омогућавају потпуно аутоматску конструкцију доказа најчешће користе технике резолуције, презаписивања и процедуре одлучивања за одређене уже теорије (на пример, SAT или SMT решаваче). Иако је систем за потпуно аутоматско доказивање теорема важан подухват, постоје, за сада, мале реалне могућности да такав систем заиста доказује компликована математичка твђења.

Један од првих аутоматских доказивача теорема био је аутоматски доказивач за геометрију. Интересовање за аутоматско доказивање у геометрији постоји још одавно, од времена Тарског. Он је развио алгебарску методу за Еуклидску геометрију, али је та метода била неупотребљива за компликованије теореме. Ипак, највећи напредак је направљен тек средином XX-ог века када је Ву предложио своју алгебарску методу за доказивање теорема у Еуклидској геометрији.

Његова метода је могла да докаже и веома комплексне теореме. Још једна алгебарска метода која се развила у исто време је метода Гребнерових база. Ови методи имају аналитички приступ у доказивању и заснивају се на репрезентацији тачака коришћењем координата. Модерни доказивачи теорема који се заснивају на овим методима су коришћени да се докажу стотине нетривијалних теорема. Ипак, велика мана ових система је што производе доказе који нису читљиви. Деведесетих година XX-ог века постојало је више покушаја да се овај проблем реши и развијене су нове методе засноване на аксиоматизацији синтетичке геометрије – метода површина, метода пуног угла. Ипак, њихова главна мана је што су далеко мање ефикасни у односу на алгебарске методе.

Примена система за аутоматско доказивање теорема у геометрији је велика. Пре свега ови системи се могу користити у образовању. Поред тога користе се у начним областима као што су роботика, биологија, препознавање слика и друге.

Значајни радови из ове области су:

- Wen-Tsiün Wu. *On the decision problem and the mechanization of theorem proving in elementary geometry*. Scientia Sinica , 21:157–179, 1978
- Deepak Kapur. *Using Gröbner bases to reason about geometry problems*. Journal of Symbolic Computation, 2(4):399–408, 1986
- Shang-Ching Chou, Xiao-Shan Gao, and Jing-Zhong Zhang. *Machine Proofs in Geometry*. World Scientific, Singapore, 1994

3 Релевантност области тезе

Истраживачке области које покрива теза су релевантне и актуелне. На овој проблематици тренутно ради велики број истраживачких група широм света и постоји одређени број часописа и конференција специјализованих за ове истраживачке области.

Интерактивно доказивање теорема, између осталог, изучава се на следећим универзитетима и истраживачким центрима:

Катедра за логику и верификацију Техничког универзитета у Минхену, Немачка (Chair for Logic and Verification, Institut für Informatik, Technische Universität München). У овој групи развија се интерактивни доказивач теорема Isabelle/HOL. Вођа групе је професор Тобијас Нипков (Tobias Nipkow), а њени најистакнутији бивши чланови су и Макаријус Венцел (Makarius Wenzel) и Јасмин Бланшет (Jasmin Blanchette).

Рачунарска лабораторија Универзитета у Кембриџу, Велика Британија (Computer Laboratory, Faculty of Computer Science and Technology, University of Cambridge). У оквиру лабораторије водећи истраживач у области аутоматског резоновања је Лоренс Полсон (Lawrence Paulson), оригинални аутор интерактивног доказивача теорема Isabelle/HOL као и аутоматског доказивача за елементарне функције MetiTarski и аутор значајних формализација математике и рачунарства, укључујући и Геделове теореме непотпуности, као и верификацију сигурносних протокола.

Пројекат πr^2 француског националног института за рачунарство и примењену математику (INRIA Project-Team πr^2 , Institut national de recherche en informatique et en automatique). У оквиру овог пројекта током претходних 30 година велики тим истраживача развио је интерактивни доказивач Coq који је заснован на рачуну конструкција који су још 1984. године формулисали Тјери Кокан (Thierry Coquand) и Жерар Хует (G  rard Huet). Један од главних истраживача који ради на развоју система Coq данас је Иго Ерблен (Hugo Herbelin).

Заједнички истраживачки центар компаније Microsoft и института INRIA (Microsoft Research - INRIA, Joint centre). Тим предводи Жорж Гонтије (Georges Gonthier) који је први формално доказао теорему о обојивости графова помоћу 4 боје. Тим је успешно спровео неколико веома крупних формализацијских подухвата, од којих је најзначајнији формални доказ Фејт-Томпсонове теореме.

Интерактивно и аутоматско доказивање теорема у геометрији се, између осталог, изучава и на следећим универзитетима и истраживачким центрима:

Одсек за електротехнику и рачунарство Универзитета Вичита, Канзас, САД (Electrical Engineering and Computer Science, Wichita State University) Два најзначајнија истраживача на пољу аутоматског резонувања у геометрији који су радили на овом одсеку су Шанг Чинг Чоу (Shang Ching Chou) који је аутор неколико уџбеника о механичком доказивању теорема геометрије и Шијао Шан Гао (Xiao-Shan Gao). Најзначајнији геометријски софтверски пакети које су они развили су Mathematics Mechanization Platform, MMP и Geometry Expert.

Тим за рачунарску графику и геометрију Универзитета у Стразбуру, Француска (IGG,   quipe Informatique G  om  trique et Grafique, Universit   de Strasbourg). Тим се бави интерактивним доказивањем теорема геометрије и њихови најзначајнији резултати укључују формализацију значајних фрагмената геометрије Тарског, као пројективне геометрије. Поред тога, чланови тима се баве и аутоматски решавањем конструктивних проблема и проблемом решавања геометријских ограничења. Водећи чланови тима који се баве овим темама су Паскал Шрек (Pascal Schreck) и Жилијен Нарбу (Julien Narboux).

Центар за интелигентне системе и њихове примене, Универзитет у Единбургу, Велика Британија (Centre for Intelligent Systems and their Applications, The University of Edinburgh). У оквиру овог центра раде истраживачи (на пример, Жак Флорио (Jacques Fleuriot), Стивен Обуа (Steven Obua), Фил Скот (Phil Scott)) који се баве аутоматским и интерактивним доказивањем теорема геометрије и нестандартне анализе. Један од њихових најзначајнијих резултата је формализација значајних делова Хилбертових „Основа геометрије”.

Истраживачки институт за симболичко израчунавање и Одсек за математичко образовање, Универзитет Јохан Кеплер, Линц, Аустрија (Research Institute for Symbolic Computation (RISC) и Department of Mathematical Education, Johannes Kepler University, Linz). Оснивач института RISC је Бруно Бухбергер (Bruno Buchberger), отац технике Гребнерових база која има изузетно велике примене како у геометрији тако и у многим другим областима математике. У оквиру одсека за математичко образовање развија се систем за

динамичку геометрију GeoGebra укључујући и његову интеграцију са аутоматским доказивачима геометријских теорема.

Најзначајније конференције у области интерактивног доказивања теорема и аутоматског и интерактивног доказивања теорема у геометрију су следеће:

1. **Interactive Theorem Proving**, ITP,
2. **Automated Deduction in Geometry**,)ADG,
3. **Conferences on Intelligent Computer Mathematics**, CICM,
4. **Conference on Certified Programs and Proofs**, CPP,
5. **Conferences on Automated Deduction**, CADE.

Најзначајнији часописи у којима се објављују радови из области тезе су следећи:

1. **Journal of Automated Reasoning**, JAR (if: 0,881),
2. **Logical Methods in Computer Science**, LMCS (if: 0,443),
3. **Annals of Mathematics and Artificial Intelligence**, AMAI (if: 0,691),
4. **Computational Geometry**, CG (if: 0,480),
5. **Mathematical Structures in Computer Science**, MSCS (if: 0,449)
6. **Journal of Formalized Reasoning**, JFR

4 Циљеви тезе

4.1 Формализација аналитичке геометрије Декартове равни

Синтетичка геометрија се обично изучава ригорозно, као пример ригорозног аксиоматског извођења. Са друге стране, аналитичка геометрија се углавном изучава неформално. Често се ова два приступа представљају независно и веза између њих се ретко показује потпуно прецизно. Циљ тезе је да повеже ове празнине.

Први циљ је да се формализује аналитичка геометрија тј. Декартова раван у оквиру система за интерактивно доказивање теорема. Циљ је представити добро изграђену формализацију Декартове геометрије равни у оквиру система Isabelle/HOL. Потом ће бити дато неколико различитих дефиниција Декартове координатне равни и показати да су све дефиниције еквивалентне. Дефиниције ће бити преузете из стандарних уџбеника. Међутим, да би их исказали у формалном окружењу асистента за доказивање теорема, потребно је подићи ниво ригорозности (на пример, праве је могуће дефинисати као класе еквиваленције тројки коефицијената у односу на релацију пропорционалности, на скупу свих не-нула тројки, док класични уџбеници аналитичке геометрије овакве појмове користе само имплицитно). Биће и формално показано да Декартова координатна раван задовољава све аксиоме Тарског и већину аксиома Хилберта (укључујући и аксиому непрекидности).

Чињеница да је аналитичка геометрија модел синтетичке геометрије се често подразумева као једна једноставна чињеница. Наш циљ је да формално покажемо ову чињеницу и анализирамо колико су докази заиста једноставни. Такође, циљ је извести неке закључке из доказа, на пример, да ли постоји нека техника која је најпогоднија за коришћење у доказима јер омогућава упрошћавање доказа или је боље све доказе изводити директним приступом. Важно питање које се поставља је и коришћење реалних бројева у доказима. Наиме, питање је да ли је могуће за доказе користити било које нумеричко поље или је заиста неопходно заиста користити поље реалних бројева и својства која у њему важе.

4.2 Формализација геометрије комплексне равни

Постоји јако пуно радова и књига које описују геометрију комплексне равни. Циљ тезе је да представи потпуно развијену теорију проширене комплексне равни, њених објеката (правих и кругова) и њених трансформација (Мебијусове трансформације). Иако је већина појмова већ описана у различитим књигама, циљ тезе је да споји бројне приступе у један униформни приступ у коме ће бити коришћен јединствен и прецизан језик за описивање појмова. Наиме, чак и у оквиру исте књиге дешава се да аутори користе исти назив за различите појмове. Поред тога, циљ је анализирати и формално показати све случајеве који често остану недовољно истражени јер их више различитих аутора сматра тривијалним.

Прво ће бити анализирана и формално представљена проширена комплексна раван (комплексна раван која садржи тачку бесконачно), као и хомогене координате комплексне тачке. У оквиру комплексне равни биће дефинисани различити појмови и анализирана њихова својства, као што су аритметичке операције, размера и дворамера, метрика, група Мебијусових трансформација и њихово деловање на проширену комплексну раван, потом неке важне подгрупе Мебијусових трансформација (као што су аутоморфизми диска, Еуклидске сличности), уопштена права и њена веза са правима и круговима, Риманова сфера, дејство Мебијусових трансформација на уопштене праве, јединственост уопштене праве, типови уопштене праве и кардиналост скупа уопштене праве, оријентисане уопштене праве, угао и очување угла након дејства Мебијусових трансформација или инверзије итд.

Природно се намећу два приступа формализацији: геометријски и алгебарски, као и питање да ли избор приступа утиче на ефикасност формалног доказивања. У раду ће бити детаљно дискутовани односи између два наведена приступа у формализацији као и њихове предности и мане. Биће анализирани технике које се користе у доказима, као и могућност коришћења аутоматизације. Такође, посматраћемо да ли је доказе лакше извести у моделу Риманове сфере или у моделу хомогених координата.

4.3 Формализација Поинкареовог диск модела

Циљ тезе је и да се формализује Поинкарев диск модел. Иако постоји много радова који упућују да би формализација Поинкареовог диск модела могла бити тривијална, до сада нисмо пронашли ни један рад, нити књигу који садрже доказ да Поинкареов модел заиста представља модел синтетичке геометрије представљен у довољно прецизном облику да би се могао формализовати у оквиру интерактивног доказивача. На пример, једна од потешкоћа је, на пример, како погодније дефинисати релацију „између” за три тачке Поинкареове диск равни, на начин који омогућава да се једноставно покаже да у моделу важи Пашова аксиома. Иако једна од основних релација, њену потпуно прецизну дефиницију нисмо пронашли до сада,

барем не у истакнутој литератури из ове области. Потом, циљ је анализирати како Мебијусове трансформације утичу на релацију „између” и доказати да Поинкареов диск модел је модел геометрије Лобачевског.

4.4 Формална анализа алгебарских метода и разматрање њихове примене на проблеме у стереометрији

Већина система за доказивање теорема са аналитичким (тј. алгебарским) приступом се користи као софтвер којем се верује иако они обично нису формално верификовани. Да би се повећала њихова поузданост потребно их је повезати са модерним интерактивним доказивачима теорема и то је могуће учинити на два начина – њиховом имплементацијом у оквиру интерактивног доказивача теорема и показивањем њихове исправности или коришћењем интерактивних доказивача да провере њихова тврђења. Неколико корака у овом правцу је већ направљено.

Циљ тезе је да допуни ова истраживања и да понуди формално верификован систем за аутоматско доказивање у геометрији који користи метод Гребнерових база или Вуову методу, при чему би значајан део верификације био заснован на мета-теорији тј. на показаним везама између аналитичке и синтетичке геометрије.

Поред овога циљ је направити систем за доказивање тврђења у стереометрији. Први корак је представити стереометријске објекте и тврђења у одговарајућем облику коришћењем полинома. Потом је циљ направити софтвер који би омогућио запис геометријских објеката и тврђења у једноставном облику који је разумљив човеку, а потом превођење тог записа у систем полинома на који би била примењена Вуова метода. Даљи циљ је примена система на решавање различитих задатака из уџбеника за средње школе и факултет и задатака са математичких такмичења, као и анализа ефикасности оваквог приступа.

5 Прелиминарни садржај тезе

Теза ће се састојати из 4 велике целине подељене на мање делове при чему се неки од делова могу мењати у зависности од тока истраживања:

1. *Увод.* У овом поглављу биће описани основни појмови и главни циљеви тезе.
2. *Интерактивни доказивачи теорема.* Биће описани софтверски системи за интерактивно формално доказивање теорема са нагласком на систему Isabelle/HOL који ће бити коришћен у раду.
3. *Различити приступи и тренутни резултати у формализацији геометрије.*
 - 3.1. *Аутоматско доказивање у геометрији.* Ово поглавље ће представити различите приступе у овој области и биће наведени најзначајнији резултати.
 - 3.2. *Интерактивно доказивање у геометрији.* Биће представљени различити приступи у интерактивном доказивању у геометрији и биће истакнути сви значајни резултати из стално растућег скупа нових радова и истраживања.
4. *Формализација аналитичке геометрије.*

- 4.1. *Модел аксиоматског система Тарског.* Биће описана формализација аналитичке геометрије у аксиоматском систему Тарског. Биће представљене дефиниције појмова и докази аксиома Тарског у аналитичкој геометрији.
- 4.2. *Модел аксиоматског система Хилберта.* Биће представљене дефиниције појмова и докази аксиома Хилберта у аналитичкој геометрији.
5. *Формализација хиперболичке геометрије.*
 - 5.1. *Формализација геометрије комплексне равни.* Биће приказана формализација многих појмова комплексне геометрије: Мебијусове трансформације, круг, права, угао итд. У оквиру овог поглавља биће анализирани различити приступи у формализацији.
 - 5.2. *Формализација Поинкареовог диск модела.* У овом поглављу биће анализиране аксиоме Тарског у Поинкареовом диск моделу.
6. *Формална анализа алгебарских метода и разматрање њихове примене на проблеме у стереометрији*
 - 6.1. *Формална анализа алгебарских метода у систему Isabelle/HOL.* Ово поглавље је посвећено анализи полинома којима се представљају геометријске конструкције и тврђења у оквиру система Isabelle/HOL.
 - 6.2. *Примена алгебарских метода на проблеме у стереометрији.* Биће анализирана примена алгебарских метода на задатке из стереометрије.

6 Досадашњи резултати кандидата

Формализација аналитичке геометрије је завршена. Показано је да је она модел за две аксиоматски засноване геометрије, геометрије Тарског и геометрије Хилберта. Ови резултати су приказани у раду:

- Petrović, Danijela, and Filip Marić. *Formalizing Analytic Geometries*. Paper presented at ADG 2012: The 9th International Workshop on Automated Deduction in Geometry, held on September 17–19, 2012 at the University of Edinburgh.

Поред овог рада, урађена је и формализација геометрије комплексне равни. Дефинисани су основни појмови и показане су многе особине Мебијусових трансформација. Такође, истражено је како Мебијусове трансформације утичу на објекте комплексне равни, као што су права, круг, угао, оријентација. Резултати овог истраживања приказани су у раду:

- Marić, Filip, and Danijela Petrović. *Formalizing complex plane geometry*. *Annals of Mathematics and Artificial Intelligence*: 1-38.

7 Podaci o mentoru

Ime i prezime: Filip Marić

Zvanje: docent

Spisak radova koji kvalifikuju mentora za vođenje doktorske disertacije:

1. Filip Marić, Danijela Petrović: Formalizing Complex Plane Geometry. *Annals of Mathematics and Artificial Intelligence*, Springer, 74(3), 2015, doi: 10.1007/s10472-014-9436-4, ISSN:1012-2443, IF 0.744 (5 year).
2. Filip Marić, Predrag Janičić: Formalization of Abstract State Transition Systems for SAT, *Logical Methods in Computer Science*, 7(3), 2011, doi: 10.2168/LMCS-7 (3:19) 2011, ISSN: 1860-5974, IF 0.497 (5 year).
3. Filip Marić: Verification of a Modern SAT Solver by Shallow Embedding into Isabelle/HOL, *Theoretical Computer Science*, 411(50), pp. 4333–4356, 2010, doi: 10.1016/j.tcs.2010.09.014, ISSN: 0304-3975, IF 0.652 (5 year).
4. Filip Marić, Predrag Janičić: Formal Correctness Proof for DPLL Procedure, *Informatica*, 21(1), pp. 57–78, 2010, ISSN 0868-4952, IF 0.852 (5 year).
5. Filip Marić: Formalization and Implementation of Modern SAT Solvers, *Journal of Automated Reasoning*, 43(1), pp. 81–119, Springer, 2009, DOI: 10.1007/s10817-009-9127-8, ISSN: 0168-7433, IF 0.987 (5 year).