УНИВЕРЗИТЕТ У БЕОГРАДУ
МАТЕМАТИЧКИ ФАКУЛТЕТ

Данијела Симић

ФОРМАЛИЗАЦИЈА РАЗЛИЧИТИХ МОДЕЛА ГЕОМЕТРИЈЕ И ПРИМЕНЕ У ВЕРИФИКАЦИЈИ АУТОМАТСКИХ ДОКАЗИВАЧА ТЕОРЕМА

докторска дисертација

Београд, 2015.

UNIVERSITY OF BELGRADE
FACULTY OF MATHEMATICS

Danijela Simić

•••

Doctoral Dissertation

Belgrade, 2015.

Ментор:

др Филип Марић, доцент
Универзитет у Београду, Математички факултет

Чланови комисије:

***др Ана Анић, ванредни професор
University of Disneyland, Недођија

***др Лаза Лазић, доцент
Универзитет у Београду, Математички факултет

Датум одбране: _____

родитељима, Милијани и Драгану Петровићу

Наслов дисертације: Формализација различитих модела геометрије и примене у верификацији аутоматских доказивача теорема

Резиме: Овде иде апстракт.

Кључне речи: ****

Научна област: рачунарство

Ужа научна област: ***

УДК број: 004.415.5(043.3)

Dissertation title: ...

Abstract: Here it goes.

Keywords: *****

Research area: computer science

Research sub-area: ****

UDC number: 004.415.5(043.3)

Садржај

Глава 1

Увод

1.1 Мотивација и циљ тезе

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, може се показати да Декартова раван представља модел формалних теорија геометрије.

Традиционална Еукидска (синетичка) геометрија је још од античке Грчке заснована на често малом скупу основних појмова (на пример, тачке, праве, основних геометријских релација попут инциденције, подударности итд.) и на скупу аксиома које имплицитно дефинишу ове основне појмове. Иако су Еуклидови „Елементи" један од најутицајних радова из математике, поставило се озбиљно питање да ли систем аксиома, теорема и лема којима се геометрија описује заиста прецизан. Испоставило се да су нађене грешке у доказима, а и да су неки докази били непотпуни јер су имали имплицитне претпоставке настале због погрешне интуиције или погрешног позивања на слике (дијаграме). Ове празнине су утицале на појаву других аксиоматских система чији је циљ био да дају формалну, прецизнију аксиоматизацију Еуклидове геометрије. Најважнији су Хилбертов систем аксиома, систем аксиома Тарског.

Хилбертов систем уводи три основна појма (тачка, права и раван), 6 релација и 20 аксиома подељених по групама. Хилберт је желео да направи систем који је прецинији од Еуклидовог, у коме ништа није остављено интуицији. Овакав приступ је повећао ниво ригорозности не само у геометрији,

него у другим областима математике.

Систем Тарског је мањи, уводи један основни појам (тачка), 2 релације 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 скупа тачака што доста отежава резоновање 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*.

У математичком образовању у средњим школама и на факултетима често се демонстрирају оба приступа у геометрији (аналитички и синтетички). Ипак, док се синтетички приступ предаје као ригорозан систем (са намером да се демонстрира формалан, аксиоматски приступ изградње математичких теорија), аналитичка геометрија се показује много мање формално. Такође, ова два приступа се уводе независно, и везе између њих се ретко формално показује у оквиру стандарог наставног плана.

Иако се појам сферне геометрије појавио још у старој Грчкој, озбиљније истраживање нееуклидских геометрија (сферне, хиперболичке и др.) је започето 1829. године са радом Лобачевског. Ипак, са њиховим интензивнијим истраживањем се почело тек пола века касније. 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 нееуклидска геометрија није ништа друго до изучавање унутрашње геометрије неке површи константне негативне кривине. Хиперболичка геометрија се изучава кроз многе њене моделе. Уводи се појам пројективног диск модела који Клајн касније популаризује. Поинкаре посматра полуравански модел који су предложили Лиувил и Белтрами и пре свега изучава изометрије хиперболичке равни које чувају оријентацију. Данас се те трансформацију и у ширем контексту, у оквиру Мебијусове трансформације.

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 аргументвања, тј. доказима. Ова чињеница омогућава да се тачност математичких тврђења аргументују формалним аксиоматским извођењима, тј. доказима. Још у седамнаестом веку, постојала је идеја да мора постајати неки општи језик којим би се могла записати математичка тврђења и општи систем правила за извођење. Један од најзначајних напретка у математици почетком двадесетог века било је у открићу да се математички аргументи могу представити у формалним аксиоматским системима на такав начин да се њихова исправност може једноставно испитати коришћењем једноставних механичких правила. Генерално, математика се могла формализовати коришћењем аксиоматске теорије скупова, теорије типова, логике вишег реда и слично. Математички доказ је ригорозан ако може бити записан у некој формалној логици као низ закључака који су изведени применом јасно дефинисаних правила.

Често, механички проверени докази попуњавају празнине које постоје у дефиницијама и доказима и упућују на дубљу анализу теме која се изучава. У историји математематике постоји пуно контроверзи око исправности математичких доказа. 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 подлегали дубљој критици. У девентанестом 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. Иако је грешке углавном лако исправити, има случајева када је то јако тешко. На пример, 1980. године објављено је да је завршена класификација једноставних коначних група, али је примећено да постоји пропуст у једној од класа и исправка тог пропуста обајвљења је тек 2001. године, а доказ је имао 1221 страну. Додатно, често се дешава да

се одређени делови доказа никада не прикажу, често уз реченицу „специјалан случај се тривијално доказује" 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 Кеплерове хипотезе коју је саставио Томас Хејлс има 300 страна и 12 рецензената су провели четири године у анализи доказа и коначно су написали да су 99% сигурни да је доказ исправан.

Многи научници су сматрали да је потпуна формализација математике недостижни идеал. Са појавом рачунара настала је могућност генерисања машински проверивих доказа. Тако су се појавили системи за формално доказивање теорема. Постоје системи који омогућавају потпуно аутоматску конструкцију доказа и они користе технике попут SAT решавача, технике презаписивања, резолуцију, алгебарске доказиваче. Иако је изградња систем за потпуно аутоматско доказивање теорема важан подухват, постоје, за сада, мале реалне могућности да се направи систем који заиста аутоматски доказује компликована математичка тврђења.

Зато је посебан акценат на системима који се заснивају на интеракцији корисника и рачунара. Такви системи 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 великим 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 могу се користити за формалну верификацију рачунарских програма. Поред тога, значајна примена је и у образовању. Помажу развој и продубљивање математичког знања.

Интересовање за аутоматско доказивање у геометрији постоји још одавно. Један од првих аутоматских доказивача теорема уопште био је аутоматски доказивач за геометрију. Тарски је развио алгебарску методу за доказивање теорема Еуклидске геометрије, али је она била неупотребљива за комликоване теореме. Највећи напредак је направљен тек средином XX-ог века када је Ву предложио своју алгебарску методу за доказивање теорема у Еуклидској

геометрији. Његовом методом могле су се доказати и веома комплексне теореме. Још једна алгебарска метода која се развила у исто време је метода Гребнерових база. Ови методи имају алгебарски, тј. аналитички приступ у доказивању и заснивају се на репрезентацији тачака коришћењем координата. Модерни доказивачи теорема који се заснивају на овим методама могу да докажу стотине нетривијалних теорема. Ипак, велика мана ових система је што не производе класичне доказе, већ само пропратне аргументе 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. Већина система са аналитичким приступом за доказивање теорема се користи као софтвер којем се верује иако 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 њихове сертификате. Неколико корака у овом правцу је већ направљено [8, **?**].

Примена система за аутоматско доказивање теорема у геометрији је велика, на пример могу користити у образовању. Поред тога користе се у научним областима као што су роботика, биологија, препознавање слика и друге.

1.2 Доприноси тезе

Овај рад покушава да премости неколико празнина за које мислимо да тренутно постоје у формализацији геометрије.

Због своје важности, геометрија комплексних бројева је добро описана у литератури. Постоје многи уџбеници који описују ову област са много детаља (током нашег рада, ми смо интезивно користили уџбенике које су писали Needham [**?**] и Schwerdtfeger [**?**]). Такође, постоји велики избор материјала за ову област (слајдова, белешки, приручника) који су доступни на вебу. Ипак, ми нисмо упознати да постоји формализација ове области, и у овом раду, ми представљамо наше поптпуно формално, механички проверено представљање геометрије комплексне равни које је, према нашем сазнању, прво такве врсте.

Додано, ми сматрамо да једнако (или чак више) од коначног резултата је важно искуство које смо стекли приликом различитих покушаја да достигнемо коначни циљ. Наиме, постоји много различитих начина како је област изложена у литератури. Поредећи, на пример, Needham [?] и Schwerdtfeger [?], представљају два врло различита начина приказивања исте приче — један приступ је више геометријски оријентисан, док је други више алгебарски оријентисан. Наше искуство показује да избор правог приступа је важан корак у остваривању циља да формализација буде изводљива у оквиру асистенат за доказивање теорема — и показало да што је више приступ алгебарски оријентисан, то је формализација једноставнија, лепша, флексибилнија и више робусна.

У оквиру рада на докторској тези, формализована је аналитичка геометрија Декартове равни, геометрија комплексне равни, дат је део формализације Поинкареовог диск модела, дата је формална анализа алгебарских метода и систем за аутоматско доказивање у стереометрији. У наставку текста набројани су основи доприноси тезе:

- Формализована је аналитичка геометрија тј. Декартова раван у оквиру система за интерактивно доказивање теорема. Представљена је добро изграђена формализација Декартове геометрије равни у оквиру система Isabelle/HOL. Дато је неколико различитих дефиниција Декартове координатне равни и показано је да су све дефиниције еквивалентне. Дефиниције су преузете из стандарних уџбеника, али је подигнут ниво ригорозности. На пример, у текстовима се обично не помињу конструкције као што су релација еквиваленције и класа еквиваленције које ће морати да буду уведене у формалним дефиницијама. Формално је показано да Декартова координатна раван задовољава све аксиоме Тарског и већину аксиома Хилберта (укључујући и аксиому непрекидности). Аанализирани су докази и упоређено који од два система аксиома је лакши за формализацију. Наш циљ је да формално покажемо да је аналитичка геометрија модел синтетичке геометрије и анализирамо колико су докази заиста једноставни.

- Коначни резултат нашег рада је добро развијена теорија проширене комплексне равни (дата као комплексан пројективни простор, али и као Риманова сфера), њени објекти (кругови и праве) и њене трансформације

(Мебијусове трансформације). Може да служи као веома важан блок за изградњу будућих формалних модела различитих геометрија (нпр, наша мотивација за овај рад је била управо у покушају да се формализује Поинкареов диск модел хиперболичке геометрије). Већина концепата које смо формализовали већ је описана у литератури (иако је постојало пуно детаља које смо морали да измислимо јер их нисмо нашли у литератури који смо разматрали). Ипак, наш рад је захтевао обједињавање различитих извора у једану јединствену, формалну репрезентацију и пребацивање у један јединствен језик имајући на уму да је првобитно било описано на много различитих начина. На пример, чак и у оквиру истог уџбеника, без икаквог формалног оправдања, аутори често лако прелазе из једне поставке у другу (рецимо, из обичне комплексне равни у проширену комплексну раван), прелазе између геометријског и алгебарског представљања, често користе многе недоказане, нетривијалне чињенице (посматрајући их као део математичког "фолклора") и др. Један од наших најзначајнијих доприноса је управо расветљавање ових непрецизности и креирање униформног, јасног и самосталног материјала.

- Извршена је формализација осам аксиома Тарког у оквиру Поинкареовог диск модела. Дата је дефиниција релације између и показана су нека њена основна својства у оквиру Поинкареовог диск модела.

- 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. 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 геометрисјких 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 или метода Гребнерових база. Даљи циљ је примена система на решавање различитих задатака из уџбеника за средње школе и факултете и задатака са математичких такмичења, као и анализа ефикасности оваквог приступа.

1.3 Организација тезе

Литература

[1] Francisco Botana, Markus Hohenwarter, Predrag Janičić, Zoltán Kovács, Ivan Petrović, Tomás Recio, and Simon Weitzhofer. Automated theorem proving in geogebra: Current achievements. *Journal of Automated Reasoning*, 55(1):39–59, 2015.

[2] XueFeng Chen and DingKang Wang. The projection of quasi variety and its application on geometric theorem proving and formula deduction. In *International Workshop on Automated Deduction in Geometry*, pages 21–30. Springer, 2002.

[3] Shang-Ching Chou. *Mechanical geometry theorem proving*, volume 41. Springer Science & Business Media, 1988.

[4] Shang-Ching Chou, Xiao-Shan Gao, and Jing-Zhong Zhang. *Machine proofs in geometry: Automated production of readable proofs for geometry theorems*, volume 6. World Scientific, 1994.

[5] Shang-Ching Chou, William F Schelter, and Jin-Gen Yang. Characteristic sets and gröbner bases in geometry theorem proving. *Resolution of equations in algebraic structures*, 2:33–91, 1987.

[6] David Cox, John Little, and Donal O'shea. *Ideals, varieties, and algorithms*, volume 3. Springer, 1992.

[7] Xiao-Shan Gao and Shang-Ching Chou. Computations with parametric equations. In *Proceedings of the 1991 international symposium on Symbolic and algebraic computation*, pages 122–127. ACM, 1991.

[8] Jean-David Génevaux, Julien Narboux, and Pascal Schreck. Formalization of wu's simple method in coq. In *Certified Programs and Proofs*, pages 71–86. Springer, 2011.

[9] John Harrison. Without loss of generality. In *Theorem Proving in Higher Order Logics*, pages 43–59. Springer, 2009.

[10] Predrag Janicic. Zbirka zadataka iz geometrije. *Skripta Internacional, Beograd,*, 1997.

[11] Bernhard Kutzler and Sabine Stifter. On the application of buchberger's algorithm to automated geometry theorem proving. *Journal of Symbolic Computation*, 2(4):389–397, 1986.

[12] NJ Lord. A method for vector proofs in geometry. *Mathematics Magazine*, 58(2):84–89, 1985.

[13] Changpeng Shao, Hongbo Li, and Lei Huang. Challenging theorem provers with mathematical olympiad problems in solid geometry. *Mathematics in Computer Science*, 10(1):75–96, 2016.

[14] Christian Sternagel and René Thiemann. Executable multivariate polynomials. 2013.

[15] Sabine Stifter. Geometry theorem proving in vector spaces by means of gröbner bases. In *Proceedings of the 1993 international symposium on Symbolic and algebraic computation*, pages 301–310. ACM, 1993.

[16] Dongming Wang. Decomposing polynomial systems into simple systems. *Journal of Symbolic Computation*, 25(3):295–314, 1998.

[17] Wenjun Wu and Xiaoshan Gao. Mathematics mechanization and applications after thirty years. *Frontiers of Computer Science in China*, 1(1):1–8, 2007.

Биографија аутора

Ovde pisem svoju biografiju.

Прилог 1.

Изјава о ауторству

Потписани-а _____

број индекса _____

Изјављујем

да је докторска дисертација под насловом

_____

_____

- резултат сопственог истраживачког рада,
- да предложена дисертација у целини ни у деловима није била предложена за добијање било које дипломе према студијским програмима других високошколских установа,
- да су резултати коректно наведени и
- да нисам кршио/ла ауторска права и користио интелектуалну својину других лица.

Потпис докторанда

У Београду, _____

_____

Прилог 2.

Изјава о истоветности штампане и електронске верзије докторског рада

Име и презиме аутора _____

Број индекса _____

Студијски програм _____

Наслов рада _____

Ментор _____

Потписани/а _____

Изјављујем да је штампана верзија мог докторског рада истоветна електронској верзији коју сам предао/ла за објављивање на порталу **Дигиталног репозиторијума Универзитета у Београду.**

Дозвољавам да се објаве моји лични подаци везани за добијање академског звања доктора наука, као што су име и презиме, година и место рођења и датум одбране рада.

Ови лични подаци могу се објавити на мрежним страницама дигиталне библиотеке, у електронском каталогу и у публикацијама Универзитета у Београду.

Потпис докторанда

У Београду, _____

_____

Прилог 3.

Изјава о коришћењу

Овлашћујем Универзитетску библиотеку „Светозар Марковић“ да у Дигитални репозиторијум Универзитета у Београду унесе моју докторску дисертацију под насловом:

_____

_____

која је моје ауторско дело.

Дисертацију са свим прилозима предао/ла сам у електронском формату погодном за трајно архивирање.

Моју докторску дисертацију похрањену у Дигитални репозиторијум Универзитета у Београду могу да користе сви који поштују одредбе садржане у одабраном типу лиценце Креативне заједнице (Creative Commons) за коју сам се одлучио/ла.

1. Ауторство

2. Ауторство - некомерцијално

3. Ауторство – некомерцијално – без прераде

4. Ауторство – некомерцијално – делити под истим условима

5. Ауторство – без прераде

6. Ауторство – делити под истим условима

(Молимо да заокружите само једну од шест понуђених лиценци, кратак опис лиценци дат је на полеђини листа).

Потпис докторанда

У Београду, _____

_____