[SmallCapsFont=CMU Serif, SmallCapsFeatures=Language=Default,Letters=SmallCaps]

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: _____

коме ћу ја, морам навести целу фамилију

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

Различити приступи и тренутни резултати у формализацији геометрије

У последњих десет година направљени су значајни резултати у формализацији математике коришћењем интерактивних доказивача. У овом поглављу навешћемо неке најзначајније и најновије радове у формализацији геометрије.

Прво, осврнућемо се и на пар радова из формализације математике који су важни и због своје улоге у формализацији геометрије (бројни резултати су коришћени као познате чињенице приликом формализације геометрије), али и због свеукупног значаја и утицаја на формализацију и интерактивно доказивање теорема.

1.1 Важни резултати и пројекти у области интерактивног доказивања теорема

Формално су доказане Брауерова теорема фиксне тачке [38], основна теорема алгебре [55, 28], Геделова теорема непотпуности [67], многе теореме реална анализа [37, 21]. У најзначајније постигнуте резултате до данас могу се убројати и формализација теореме о простим бројевима [4], затим формални доказ о обојивости графа са четири боје [29].

Важно је поменути и актуелне пројеката великих размера чији циљ обухвата формализацију великих делова математике и у којима учествују многи

научници. У оквиру пројеката чији руководилац је (фра. Georges Gonthier) је успешно формално доказана *Feit-Thompson теорема* (која се још и назива теорема непарног поретка) [30]. Формализација је рађена уз помоћ асистента за доказивање теорема Coq и језика за доказе SSreflect [31]. Ова теорема је била веома важан корак у *класификацији коначних једноставних група*. Оригинални доказ на папиру је заузимао 225 страна, док формализација има 150000 линија кода, 4000 дефиниција и 13000 лема и теорема. Да би могли да формализују ову теорему, аутори су морали да формализују и бројна тврђења и својства линеарне алгебре, теорије коначних група, Galois theory, and representation theory. Наилазили су на бројне празнине и грешке, од којих неке није било лако исправити и допунити.

Други важан пројекат је пројекат *Flyspeck* [35] који је покренуо Томас Хејлс да би могао формално да докаже Кеплерову хипотезу. У оквиру овог пројекта формално је показано много математичких тврђења, направљена је велика база 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 [47, 48], формално верификован компилатор за програмски језик C и L4 [45, 44], формално верификован оперативни систем.

1.2 Интерактивно доказивање у геометрији

Интерактивно доказивање у Хилберовој геометрији

Постоји велики број формализација фрагмената различитих геометрија у оквиру интерактивних доказивача теорема. Први покушај да се формализује *прва група Хилбертових аксиома и њихових последица* је био у оквиру асистената за доказивање теорема Coq, у интуиционистичком окружењу [22]. Следећи покушај је био у систему Isabelle/Isar и ову формализацију су радили Meikle и Флориот [54]. Аутори оповргавају уобичајено мишљење да су Хилбертови докази мање интуитивни, а више ригорозни. Важан закључак је да је Хилберт користио бројне претпоставке које у формализацији са рачунаром нису могле да буду направљене и стога су морале да буду формално верификоване и оправдане. Наставак ове формализације, пратећи Хилберто-

ву књигу „Основи геометрије" [39], урадио је Скот у оквиру своје мастер тезе [65].

У раду [62] је *предложен минималан скуп Хилбертових аксиома* и за модел је коришћена теорија скупова. Изведена су и формално показана основна својства и тврђења у овом моделу.

Интерактивно доказивање у геометрији Тарског

Велике делове геометрије Тарског [64] је формализовао Нарбу у систему Coq [56]. Бројна геометријска својства су изведена, доказано је више облика Пашове аксиоме, показана су бројна својства релације подударности и релације између. Рад се завршава доказом о постојању средишње тачке сегмента.

У оквиру своје мастер тезе Тимоти Макариос је показао *независност аксиоме паралелености* [51]. За доказивање је изабрао аксиоматски систем Тарског зато што је тај систем категоричан. Да би могао да покаже независност прво је формализовао аксиоме Тарског у оквиру система Isabelle. Онда је формализовао и Клајн Белтрами модел (енг. Klein-Beltrami model) нееуклидске геометрије Тарског и показао је да је ово модел за све аксиоме Тарског осим за аксиому паралелности, односно Еуклидову аксиому. На тај начин је показао да је ова аксиома независна од осталих аксиома Тарског за планарну геометрију. За неке аксиоме Тарског су у литератури недостајали докази да Клајн-Белтрами модел задовољава аксиому или су докази били некомплетни, па је рад попунио ове празнине. Као део рада, дефинисана је реална пројективна раван у систему Isabelle/HOL и показане су неке њене карактеристике.

Формализацију еквиваленције између различитих верзија *Еуклидовог петог постулата* дали су Пјер ? (фра. Pierre Boutry), Џулијен Нарбу (фра. Julien Narboux) и Паскал Шрек (фра. Pascal Schreck) [10]. Овај постулат је посебно значајан јер је било много покушаја да се он докаже. Наиме, иако је пети постулат Еуклид записао као аксиому, веома рано је настала идеја да би он могао да се изведе из прва четири постулата. Бројни покушаји да се постулат докаже су били погрешни јер су се у доказима често користиле претпоставке које нису биле доказане. Аутори су у раду показали да су 10 различитих тврђења еквивалентни Еуклидовом петом постулату. Такође, они су у раду разматрали како избор различитих верзија Еуклидовог постулата утиче на проблем одлучивања у геометријским доказима.

У раду [12] аутори су формализовали *првих дванаест поглавља књиге „Математички методи у геометрији"* [64] и на основу доказаних својстава су механички успели да докажу да се аксиоме Хилберта могу извести из аксиома Тарског. Габријел Браун (фра. Gabriel Braun) и Џулијен Нарбу (фра. Julien Narboux) су формализовали синтетички доказ Папусове теореме у геометрији Тарског [13]. Ова теорема је веома важна за *конструкцију координатне равни и представља један од важних корака у успостављању везе између аналитичке и синтетичке геометрије.* Ова веза је посебно важна јер омогућава коришћење алгебарског приступа у аутоматском закључивању у геометрији. Поред појмова који су дати у књизи, аутори су дали и формализацију вектора, квадрилитерала, паралелограма, пројекције, оријентације праве и других. Наставак овог рада и коначни производ вишегодишњег пројекта приказан је у раду [9]. Аутори су завршили формализацију књиге „Математички методи у геометрији" и у овом раду су показали како су формализвали последња три поглавља. Ову формализацију су искористили да *геометријски дефинишу аритметичке операције и доказали су да ове операције чине уређено поље. Потом су увели Декартову координатну раван и показали су својства основних геометријских релација. Ови резултати су веома важни јер оправдавају коришћење алгебарских метода за доказивање у геометрији.* Аутори то и демонстрирају у раду тако што користе метод Гребнерових база да покажу теорему о девет тачака на кругу.

Интерактивно доказивање у неколико различитих геометрија

Магауд, Нарбу и Шрек су урадили још једну формализацију коришћењем Coq-а и то за *геометрију пројективне равни* [49, 50]. Показана су нека основна својства и доказан је принцип дуалности за пројективну геометрију. Коначно, доказана је конзистенција аксиома у три модела, од којих су неки коначни, а неки бесконачни. На крају аутори дискутују о дегенеративним случајевима и да би се са њима изборили користе рангове и монотоност.

Kahn је формализовао *вон Платову конструктивну геометрију* такође у систему Coq [69, 42].

Потом, Guilhot користећи Coq *повезује Софтвер за интерактивну геометрију (СИГ) и формално доказивање* у намери да олакша учење Еуклидске

геометрије у средњој школи [34]. Pham, Bertot and Narboux су предложили и неколико унапређења [58]. Прво је да се елиминишу сувишне аксиоме коришћењем вектора. Они су додали четири аксиоме да опишу векторе и још три аксиоме да дефинишу Еуклидску раван и увели су додатне дефиниције да би описали геометријске концепте. Коришћењем ових аксиома и дефиниција, геометријска својства су лако доказана. Друго унапређење је коришћење методе површина за аутоматско доказивање теорема. Да би се формално оправдало коришћење методе површина, морала је да се конструише Декартова координатна раван коришћењем геометријских својстава која су раније доказана.

Duprat формализује *геометрију лењира и шестара* [23]. Авигад нуди још једну аксиоматизацију Еуклидске геометрије [3]. Он полази од чињенице да Еуклидска геометрија описује природније геометријска тврђења него новије аксиоматизације геометрије. Он сматра да посматрање слике, односно дијаграма, није пуно мана као што многи мисле. У намери да ово докаже, уводи систем E у коме су основни објекти тачке и праве. Аксиоме се користе да опишу својства дијаграма на основу којих се може закључивати. Аутори такође илуструју логички оквир у коме се могу изводити докази. У раду су презеновани неки докази геометријских својстава, као и доказ еквивалентности између система Тарског за геометрију лењира и шестара и система E. Дегенеративни случајеви су избегнути коришћењем претпоставки и стога се само доказује централни случај.

Као део пројекта Flyspeck, Харисон је развио веома богату теорију (која укључује алгебру, топологију и анализу) *Еуклидског n-димензионог простора* $\mathbb{R}^n$ у доказивачу теорема HOL Light [36, 38].

Показани су и различити резултати из *комплексне анализе* у оквиру доказивача теорема. Милевски је доказао основу теорему алгебре у систему Мизар [55], Geuvers et al. је показао исту теорему у систему Coq [28], а Харисон је имплементирао комплексну елиминацију квантификтора за логику вишег реда и то је користио у разним формализацијама, укључујући и формализације геометрије.

Ревизија формализације

У раду [2] приказује се начин како би могла да се изврши *ревизија формализације*. Наиме, аутори сматрају да иако формализација даје стриктан

и прецизан приступ математици, и даље су могуће неке грешке. Једна од грешака која се често спомиње је да се формализовано тврђење разликује од тврђења за које је рађена формализација или од тврђења за које мислимо да је показано. Ова грешка може настати због лоших дефиниција које се могу провлачити кроз целу формализацију и тако утицати на крајњи исход формализације. Поред ових грешака, аутори истичу и неке недостатке најпопуларнијих доказивача теорема, а међу недостацима се посебно истиче комплексност система који се користи и који може бити место потенцијаним грешкама у самом доказивачу. Њихов приступ ревизији се своди на неколико корака, при чему није циљ проверавати сваку линију комплетне формализације, већ завршно стање формализације. Такође, предлажу да ако је формализација рађена у једном језику, да се ревизија ради у другом (или у више других) језика и дају пример неколико алатки које врше превођење из једног језика у други. Коначно, дају пример како је могуће извршити ревизију над делом Flyspeck пројекта.

1.3 Аутоматско доказивање у геометрији

У раду [16] смо нашли веома детељан историјски опис развоја аутоматских доказивача до почетка овог века, као и детаљан опис различитих приступа у аутоматском доказивању у геометрији и нешто од тих идеја је приказано у овом поглављу.

Коришћење вештачке интелигенције. Један од првих радова у области аутоматског доказивања у геометрији је рад Gelernter [26], који је користио методе вештачке интелигенције, и његов приступ се заснивао на прављењу доказа сличних онима које пише човек. Сличан приступ имали су Wos и његови сарадници [53] и они су користили резолуцијски доказивач за доказивање у геометрији Тарског. Ипак, ови приступи нису били веома ефикасни. Новији рад који такође користи методе вештачке интелигенције је систем Geometrix [33].

Рани развој алгебарских метода за аутоматско доказивање у геометрији

Вуов метод и метод Гребнерових база. Највећи напредак у аутоматском доказивању теорема у геометрији направио је Ву. Он је ограничио скуп проблема које посматра и посматрао само оне проблеме са једнакостима на које је могао да примени моћан метод који је могао да докаже и компликована тврђења. Овај метод је представио у оквиру свог рада [75] 1978. године. Како је овим методом показано 130 тврђења [15], он постаје све популарнији. Бројни аутори су овај метод имплементирали и унапређивали разним хеуристикама [25, 66, 43]. Убрзо, постаје јасно да се Вуов приступ могао извести из Ritt рада [63], па се често овај метод још назива и *Ву–Рит метод*.

Успех овог метода утицао је на развој нових метода. Један од успешних је *Бухбергеров алгоритам* [14], који се заснива на методи Гребнерових база и може се применити на исту класу проблема као и Вуов метод.

Главна мана ова два метода је што се са њима *не могу доказивати неједнакости*. За решавање проблема са неједнакостима Ву је предложио метод који се заснива на проналажењу минималне или максималне вредности полиномијалне функције под одређеним условима [72]. Поред доказивања у елементарној геометрији, Ву је представио и *метод за доказивање у диференцијалној геометрији* [71]. Постоје и проширења која омогућавају да се *метод користи и за хиперболичку геоемтрију* [76].

Метод површина и његова проширења. Сви набројани методи преводе геометријско тврђење у једначине коришћењем координата тачака које се посматрају, а потом се примењују алгебарске технике на ове једначине. Ови доказивачи дају одговор „да" или „не", али не дају никакву информацију о извођењу која би била разумљива човеку и слична доказима у школским уџбеницима. Постоје бројни покушаји да се направе доказивачи који би поред доказивања уједно производили *читљиве доказе*. Један од најзначајнијих је *метод површина* [17]. Овај метод користи геометријске инваријанте као што су површина, размера, Питагорина разлика и слично. Главна предност овог доказивача је што сваки корак у доказивању има јасно геометријско значење. Додатно, експерименти су показали да су докази коришћењем метода површина краћи. Метод је могуће проширити тако да је могуће радити и са неједнакостима.

Аутори су такође представили и *метод пуног угла* [19]. У експреминетима је примећено да се метод површина веома добро понаша за конструктивне теореме у афиној геометрији. Са друге стране, метод пуног угла је погодан за проблеме у којима има много кругова и углова и за овакве проблеме чешће производи краће доказе него што је то случај са методом површина. Као што и само име сугерише овај метод као геометријску инваријанту посматра пун угао.

Исти аутори су у раду [18] представили могућност *проширења методе површина на проблеме у стереометрији*. Хипотезе се задају конструктивно, а закључци су полиномијалне једначине неколико геометријских величина, као што су запремина, размера сегмената, размера површина и Питагорине разлике. Главна идеја овог метода је да елиминише тачке из закључка геометријског тврђења коришћењем основних својстава запремине. Поред овог, није нам познато да постоји још радова који се баве аутоматским доказивањем у стереометрији.

Иако је метод површина описан још деведесетих година прошлог века, до скора нису детаљно описана имплементациона питања, али ни испитана оправданост коришћења самог метода. У раду [41] аутори управо скрећу пажњу на ове проблеме. Они *веома детаљно описују метод, и формално доказују у систему Coq важне дефиниције и леме које омогућавају коришћење метода*. Детаљно описују и нека важна имплементациона питања јер метод површина, иако је једноставан за разумевање, је тежак за имплементацију јер постоји много детаља на које треба обратити пажњу.

Различити системи за аутоматско доказивање у геометрији

Wang је у раду [70] описао систем *GEOTHER* који може послужити за аутоматско доказивање теорема у геометрији. За развој система користи Maple. Геометријска тврђења репрезентује коришћењем предикатске спецификације, а те спецификације је могуће аутоматски превести на тврђења записана на енглеском или кинеском, или на алгебарске једнакости или на логичке формуле. На основу спецификација могуће је конструисати и дијаграме које је потом могуће мењати коришћењем миша. Оно што је посебно интересантно је што је у систему имплементирано више аутоматских доказивача теорема. Импле-

метиран је доказивач заснован на Вуовој методи. Потом доказивач заснован на методи Kutzler–Stifter и доказивач заснован на методи Kapur (оба метода су заносвана на идејама методе Гребнерових база). Имплеметирани су још и методи засновани на нула декомпозицији и обичној диференцијалној нула декомпозицији. Доказивачи су упоређивани над више различитих теорема, а Вуов метод се за већину тврђења показао као ефикаснији.

Значајно је поменути и систем *Geometry Expert* [20] који има имплементиран Вуов метод, метод Гребнерових база, метод вектора, метод пуног угла и метод површина. Посебно је интересантно његово проширење, систем *Java Geometry Expert* [77]. Ова алатка је занимљива јер поред аутоматског доказивања теорема нуди и визуалну, динамичку репрезентацију доказа. Производи серију визуелних ефеката за презентацију доказа и у својој бази садржи преко шест стотина примера.

Систем *Geometry Explorer* [73] производи читљиве доказе о својствима конструисаних објеката коришћењем метода пуног угла.

Важно је поменути и систем *Discover* [8] за аутоматско откривање у Еуклидској геометрији, који користи алгебарски софтвер CoCoA [1] и Mathematica [74].

Значајан је и систем *GCLC* [40] који омогућава запис конструкције и тврђења и превођење истих у различите формате (рецимо, у формат .tkz који је значајан јер је погодан за уметање слика у TeX документ). Овај систем је посебно значајан јер има интегрисана три доказивача теорема, Вуов метод, метод Гребнерових база и метод површина.

Нешто другачији приступ у односу на поменуте системе има систем *Cinderella* [46] који примењује разне произвољне провере дате конструкције. Ово је систем који није симболички, ни динамички већ користи пробабилистичке методе да провери да ли је дата претпопставка највероватније теорема.

Полуаутоматски системи за доказивање теорема у геометрији Рад [68] демонстрира коришћење *синтетичког доказивача за доказивање теорема у геометрији Тарског*. Пре свега је интересантно то што је повезано интерактивно и аутоматско доказивање, што значи да су сви аутоматски генерисани докази уједно и формално верификовани. Систем поред доказивања теорема генерише и машински проверене, читљиве доказе који су веома слични доказима из уџбеника. Користе кохерентну логику, део логике првог реда

као основну логику система. Примењују резолуцијски доказивач, доказивач теорема у кохерентној логици, и XML алатке за конхерентну логику који им омогућавају да доказе трансформишу у машински провериве доказе и у доказе разумљиве човеку. Систем примењују на доказивање тврђења из првог дела књиге „Математички методи у геометрији" [64] и успешно, потпуно аутоматски доказају 37% теорема.

Сличан приступ је описан у раду [5] у коме се описује *полуаутоматски приступ за доказивање у геометрији Тарског*. Аутори су посматрали више група доказа, од којих су неки краћи од 40 корака, потом доказе који су између 40 и 100 корака и који се сматрају тежим за човека и коначно доказе дуже од 100 корака који најчешће представљају теме докторских радова. За доказивање користе доказивач OTTER, који је и раније коришћен за доказивање теорема [61]. Један од циљева је била и анализа утицаја хардверског напретка, али и нових техника за аутоматско доказивање у геометрији на успешност аутоматских доказивача. Потпуно механички је изведена већина кратких доказа. Испрва за дугачке доказе није било могуће добити механичке доказе, и аутори су коришћењем доказа из књиге конструисали формалне доказе. Потом су применили нову технику, где су доказивачу прослеђивали све потребне аксиоме и претходно доказана тврђења, као и неке кораке доказа и систем је успевао да нађе механичке доказе за тврђења која су се доказивала у више од 100 корака.

Коришћење аутоматски доказивача теорема за решавање проблема у геометрији и примена у образовању

Интензивно поље истраживања није само аутоматско доказивање него и коришћење аутоматских доказивача за решавање проблема у геометрији.

У раду [52] аутори се баве *проблемом конструкције помоћу лењира и шестара*. У овом раду, фокус је на проблему конструкције троугла где су дате тачке и услови који за њих морају да важе. Приликом проналажења конструкције пролази се кроз све четири фазе, аутоматски се проналазе кораци конструкције, као и доказ исправности који се даје у облику који је читљив човеку. Додатно, користе се алгебарски методи за аутоматско доказивање да ли је могуће извршити конструкцију или није могуће извршити конструкцију,

што је посебно интересантно јер постоје много познатих проблема за које није могуће показати њихову неконструктивност.

Веома широко распрострањени у образовању су *динамички геометријски алати*. Коришћењем тог софтвера корисник лако може креирати и мењати геометријске конструкције. Конструкција обично започиње задавањем тачака или неких објеката (праве, кругови), а онда се креирају зависне тачке и објекти. Потом, почетна конфигурација се може мењати и може се посматрати како мењање почетних положаја утиче на крајњи резултат. На тај начин могуће је тестирати претпоставке, рецимо, да ли су три тачке увек колинеарне без обзира на конфигурацију. Како је могуће само тестирање, али не и доказивање, нови правци у развоју оваквог софтвера су управо у додавању аутоматских доказивача у оквиру динамичке геометријске алатке. Најпознатији динамичко геометријски софтвер је GeoGebra и користи се у многим земљама, укључујући и Србију, као помоћно наставно средство.

Алгоритам који је проширење метода Гребнерових база и који се заснива на анализи система са параметрима се користи у раду [6] ради *проналажења хипотеза које морају да важе (поред претпоставки које су већ дате) да би дато тврђење било могуће извести*. Систем је имплементиран тако да се може користити у оквиру система GeoGebra. Значајно је што систем симболички одређује геометријско место тачака и потом показује валидност геометријског тврђења. Посебно је значајно и то што се у процесу одређивања геометријског места тачака, нотирају и ирелевантне тачке (најчеће су то у питању дегенерисани случајеви) и избацују из разматрања.

Поред поменутог, значајан *додатак систему GeoGebra је аутоматски доказивач заснован на Вуовој методи* [7]. Поред могућности доказивања, систем може да идентификује „интересантна" својства дате конструкције, односно да аутоматски одреди неке релације између констрисаних објеката.

Формализација алгебарских метода за аутоматско доказивање

Поред формализације геометријских тврђења многи истраживачи су покушали да формализују аутоматско доказивање у геометрији.

Grégoire, Pottier and Théry комбинују модификовану верзију *Бухбергеровог алгоритма* и неке технике рефлексије да би добили ефективну процедуру која

аутоматски производи формални доказ теорема у геометрији [32].

Génevaux, Narboux and Schreck су формализовали *упрошћен Вуов метод* у систему Coq [27]. Њихов приступ се базира на верификацији сертификата које генерише програм за упрошћен Вуов метод писан у Ocaml.

Fuchs and Théry су формализовали алгебру Grassmann-Cayley систему Coq [24]. Други део рада, који је интересантнији са аспекта наше формализације, представља *примену алгебре на геометрију инциденције*. Тачке, праве и њихови односи су дефинисани у форми алгебарских операција. Коришћењем ових дефиниција, теореме Pappus и Desargues су интерактивно доказане у систему Coq. Коначно, аутори описују аутоматизацију у систему Coq за доказивање теорема у геометрији коришћем ове алгебре. Мане овог приступа су у томе што је могуће показати само она тврђења где се доказује колинеарност међу тачкама и што се разматрају само недегенерисани случајеви.

Програме за *одређивање Гребнерове базе*, F4 и GB, презентује Pottier [59] и упоређује их са gbcoq [60]. Он предлаже решење са сертификатима и ово скраћује време које је потребно за израчунавања, тако да gbcoq, иако направљен у систему Coq, постаје упоредив са друга два програма. Примена Гребнерових база на алгебру, геометрију и аритметику је приказана кроз три примера.

Веома интересентан је рад који су представили Gabriel Braun и Julien Narboux и који се бави *проналажењем специјалних тачака троугла и доказивањем својстава које те тачке задовољавају* [57]. Наиме, под руководством Clark Kimberling направљена је електронска енциклопедија важних тачака троугла у којој се тренутно налазе дефиниције о више од 7000 тачака, као и својства које те тачке задовољавају. Ипак, ова својства често немају доказ или је доказ задат неформално. Како се у енциклопедији налази веома велики број тачака и њихових својстава, било би прилично напорно ручно преписивати и доказивати сва та својства. Gabriel Braun и Julien Narboux су у оквиру система Coq дефинисали аутоматске мотоде за дефинисање тачака и аутоматске методе за доказивање њихових својстава. Веома важну улогу имају геометријске трансформације које помажу и у налажењу тачака и у доказивању одговарајућих лема.

Pierre Boutry, Julien Narboux и Pascal Schreck су у Coq-у *формализовали и имлементирали рефлексивну тактику за аутоматско генерисање доказа о инциденцији* [11]. Тврђења о инциденцији се често јављају у формалним доказима разних геометријских тврђења, али су у доказима који су записа-

ни на папиру често изостављена јер често не доприносе разумевању доказа. Ипак, приликом формалне верификације у оквиру асистента за доказивање теорема, леме и докази о инциденцији морају бити записани. Аутори су представили генеричку тактику која је примењива на било коју теорију чији је циљ да аутоматски докаже та ситна тврђења. Уједно, ово је један од низа корака да се формални доказ приближи доказима из уџбеника у којима се често изостављају „очигледна" тврђења.

Литература

[1] J Abbott, A Bigatti, and G Lagorio. Cocoa-5: A system for doing computations in commutative algebra (2014).

[2] Mark Adams. Proof auditing formalised mathematics. *Journal of Formalized Reasoning*, 2016.

[3] Jeremy Avigad, Edward Dean, and John Mumma. A formal system for euclid's elements. *The Review of Symbolic Logic*, 2(04):700–768, 2009.

[4] Jeremy Avigad, Kevin Donnelly, David Gray, and Paul Raff. A formally verified proof of the prime number theorem. *ACM Transactions on Computational Logic (TOCL)*, 9(1):2, 2007.

[5] Michael Beeson and Larry Wos. Finding proofs in tarskian geometry. *to appear, The Journal of Automated Reasoning*, 2016.

[6] Francisco Botana and Miguel A Abánades. Automatic deduction in (dynamic) geometry: Loci computation. *Computational Geometry*, 47(1):75–89, 2014.

[7] 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.

[8] Francisco Botana and José L Valcarce. A dynamic–symbolic interface for geometric theorem discovery. *Computers & Education*, 38(1):21–35, 2002.

[9] Pierre Boutry, Gabriel Braun, and Julien Narboux. From tarski to descartes: Formalization of the arithmetization of euclidean geometry. In *SCSS 2016 The 7th International Symposium on Symbolic Computation in Software Science*, 2016.

[10] Pierre Boutry, Julien Narboux, and Pascal Schreck. Parallel postulates and decidability of intersection of lines: a mechanized study within tarski's system of geometry. 2015.

[11] Pierre Boutry, Julien Narboux, and Pascal Schreck. A reflexive tactic for automated generation of proofs of incidence to an affine variety. 2015.

[12] Gabriel Braun and Julien Narboux. From tarski to hilbert. In *Automated Deduction in Geometry*, pages 89–109. Springer, 2012.

[13] Gabriel Braun and Julien Narboux. A synthetic proof of pappus' theorem in tarski's geometry. 2015.

[14] Bruno Buchberger. Bruno buchberger's phd thesis 1965: An algorithm for finding the basis elements of the residue class ring of a zero dimensional polynomial ideal. *Journal of symbolic computation*, 41(3):475–511, 2006.

[15] Shang-Ching Chou. Proving elementary geometry theorems using wu's algorithm. Master's thesis, University of Texas at Austin, 1984.

[16] Shang-Ching Chou and Xiao-Shan Gao. Automated reasoning in geometry. *Handbook of automated reasoning*, 1:707–749, 2001.

[17] Shang-Ching Chou, Xiao-Shan Gao, and Jing-Zhong Zhang. Automated production of traditional proofs for constructive geometry theorems. In *Logic in Computer Science, 1993. LICS'93., Proceedings of Eighth Annual IEEE Symposium on*, pages 48–56. IEEE, 1993.

[18] Shang-Ching Chou, Xiao-Shan Gao, and Jing-Zhong Zhang. Automated production of traditional proofs in solid geometry. *Journal of Automated Reasoning*, 14(2):257–291, 1995.

[19] Shang-Ching Chou, Xiao-Shan Gao, and Jing-Zhong Zhang. Automated generation of readable proofs with geometric invariants. *Journal of Automated Reasoning*, 17(3):325–347, 1996.

[20] Shang-Ching Chou, Xiao-Shan Gao, and Jing-Zhong Zhang. An introduction to geometry expert. In *Automated Deduction—Cade-13*, pages 235–239. Springer, 1996.

[21] Luís Cruz-Filipe. A constructive formalization of the fundamental theorem of calculus. In *Types for Proofs and Programs*, pages 108–126. Springer, 2002.

[22] Christophe Dehlinger, Jean-François Dufourd, and Pascal Schreck. Higher-order intuitionistic formalization and proofs in hilbert's elementary geometry. In *Automated Deduction in Geometry*, pages 306–323. Springer, 2001.

[23] Jean Duprat. Une axiomatique de la géométrie plane en coq. *Actes des JFLA*, pages 123–136, 2008.

[24] Laurent Fuchs and Laurent Théry. A formalization of grassmann-cayley algebra in coq and its application to theorem proving in projective geometry. In *Automated Deduction in Geometry*, pages 51–67. Springer, 2011.

[25] Xiaoshan Gao. Transcendental functions and mechanical theorem proving in elementary geometries. *Journal of Automated Reasoning*, 6(4):403–417, 1990.

[26] Herbert Gelernter. Realization of a geometry theorem proving machine. In *IFIP Congress*, pages 273–281, 1959.

[27] 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.

[28] 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*, pages 96–111. Springer, 2000.

[29] Georges Gonthier. Formal proof–the four-color theorem. *Notices of the AMS*, 55(11):1382–1393, 2008.

[30] Georges Gonthier, Andrea Asperti, Jeremy Avigad, Yves Bertot, Cyril Cohen, François Garillot, Stéphane Le Roux, Assia Mahboubi, Russell O'Connor, Sidi Ould Biha, et al. A machine-checked proof of the odd order theorem. In *Interactive Theorem Proving*, pages 163–179. Springer, 2013.

[31] Georges Gonthier, Assia Mahboubi, and Enrico Tassi. *A small scale reflection extension for the Coq system*. PhD thesis, Inria Saclay Ile de France, 2014.

[32] Benjamin Grégoire, Loïc Pottier, and Laurent Théry. Proof certificates for algebra and their application to automatic geometry theorem proving. In *Automated Deduction in Geometry*, pages 42–59. Springer, 2011.

[33] Jérémie Gressier. Geometrix iv. `http://geometrix.free.fr/`, 2013.

[34] Frédérique Guilhot. Formalisation en coq et visualisation d'un cours de géométrie pour le lycée. *Technique et Science informatiques*, 24(9):1113–1138, 2005.

[35] Thomas C Hales. Introduction to the flyspeck project. In *Dagstuhl Seminar Proceedings*. Schloss Dagstuhl-Leibniz-Zentrum für Informatik, 2006.

[36] John Harrison. A hol theory of euclidean space. In *Theorem proving in higher order logics*, pages 114–129. Springer, 2005.

[37] John Harrison. *Theorem proving with the real numbers*. Springer Science & Business Media, 2012.

[38] John Harrison. The hol light theory of euclidean space. *Journal of Automated Reasoning*, 50(2):173–190, 2013.

[39] David Hilbert. *Grundlagen der geometrie*. Springer-Verlag, 2013.

[40] Predrag Janičić. Geometry constructions language. *Journal of Automated Reasoning*, 44(1-2):3–24, 2010.

[41] Predrag Janičić, Julien Narboux, and Pedro Quaresma. The area method. *Journal of Automated Reasoning*, 48(4):489–532, 2012.

[42] Gilles Kahn. Constructive geometry according to jan von plato. *Coq contribution. Coq*, 5:10, 1995.

[43] Deepak Kapur and Hoi K Wan. Refutational proofs of geometry theorems via characteristic set computation. In *Proceedings of the international symposium on Symbolic and algebraic computation*, pages 277–284. ACM, 1990.

[44] Gerwin Klein, June Andronick, Kevin Elphinstone, Toby Murray, Thomas Sewell, Rafal Kolanski, and Gernot Heiser. Comprehensive formal verification of an os microkernel. *ACM Transactions on Computer Systems (TOCS)*, 32(1):2, 2014.

[45] Gerwin Klein, Kevin Elphinstone, Gernot Heiser, June Andronick, David Cock, Philip Derrin, Dhammika Elkaduwe, Kai Engelhardt, Rafal Kolanski, Michael Norrish, et al. sel4: Formal verification of an os kernel. In *Proceedings of the ACM SIGOPS 22nd symposium on Operating systems principles*, pages 207–220. ACM, 2009.

[46] Ulrich Kortenkamp and Jürgen Richter-Gebert. Using automatic theorem proving to improve the usability of geometry software. In *Proceedings of MathUI*, volume 2004, 2004.

[47] Xavier Leroy. Formal verification of a realistic compiler. *Communications of the ACM*, 52(7):107–115, 2009.

[48] Xavier Leroy. A formally verified compiler back-end. *Journal of Automated Reasoning*, 43(4):363–446, 2009.

[49] Nicolas Magaud, Julien Narboux, and Pascal Schreck. Formalizing projective plane geometry in coq. In *Automated Deduction in Geometry*, pages 141–162. Springer, 2011.

[50] Nicolas Magaud, Julien Narboux, and Pascal Schreck. A case study in formalizing projective geometry in coq: Desargues theorem. *Computational Geometry*, 45(8):406–424, 2012.

[51] Timothy James McKenzie Makarios. A mechanical verification of the independence of tarski's euclidean axiom. 2012.

[52] Vesna Marinković, Predrag Janičić, and Pascal Schreck. Computer theorem proving for verifiable solving of geometric construction problems. In *Automated Deduction in Geometry*, pages 72–93. Springer, 2014.

[53] John D McCharen, Ross A Overbeek, and LAWRENCE T WOS. Problems and experiments for and with automated theorem-proving programs. In *The Collected Works of Larry Wos: (In 2 Volumes) Volume I: Exploring the Power of Automated Reasoning Volume II: Applying Automated Reasoning to Puzzles, Problems, and Open Questions*, pages 166–196. 2000.

[54] Laura I Meikle and Jacques D Fleuriot. Formalizing hilbert's grundlagen in isabelle/isar. In *Theorem proving in higher order logics*, pages 319–334. Springer, 2003.

[55] Robert Milewski. Fundamental theorem of algebra1. 2001.

[56] Julien Narboux. Mechanical theorem proving in tarski's geometry. In *Automated Deduction in Geometry*, pages 139–156. Springer, 2007.

[57] Julien Narboux and David Braun. Towards a certified version of the encyclopedia of triangle centers. 2015.

[58] Tuan-Minh Pham, Yves Bertot, and Julien Narboux. A coq-based library for interactive and automated theorem proving in plane geometry. In *Computational Science and Its Applications-ICCSA 2011*, pages 368–383. Springer, 2011.

[59] Loic Pottier. Connecting gr\„ obner bases programs with coq to do proofs in algebra, geometry and arithmetics. *arXiv preprint arXiv:1007.3615*, 2010.

[60] Loic Pottier. Connecting gr\" obner bases programs with coq to do proofs in algebra, geometry and arithmetics. *arXiv preprint arXiv:1007.3615*, 2010.

[61] Art Quaife. *Automated development of fundamental mathematical theories*. JSTOR, 1992.

[62] William Richter. A minimal version of hilbert's axioms for plane geometry.

[63] Joseph Fels Ritt. *Differential algebra*, volume 33. American Mathematical Soc., 1950.

[64] Wolfram Schwabhäuser, Wanda Szmielew, and Alfred Tarski. *Metamathematische methoden in der geometrie*. Springer-Verlag, 2013.

[65] Phil Scott. Mechanising hilbert's foundations of geometry in isabelle. *Master's thesis, University of Edinburgh*, 2008.

[66] WANG DONG-MING HU SEN. A mechanical proving system for constructible theorems in elementary geometry. 1987.

[67] Natarajan Shankar. *Metamathematics, machines and Gödel's proof*. Number 38. Cambridge University Press, 1997.

[68] Sana Stojanović Đurđević, Julien Narboux, and Predrag Janičić. Automated generation of machine verifiable and readable proofs: A case study of tarski's

geometry. *Annals of Mathematics and Artificial Intelligence*, 74(3-4):249–269, 2015.

[69] Jan von Plato. The axioms of constructive geometry. *Annals of pure and applied logic*, 76(2):169–200, 1995.

[70] Dongming Wang. Geother 1.1: Handling and proving geometric theorems automatically. In *Automated Deduction in Geometry*, pages 194–215. Springer, 2002.

[71] Wu Wen-Tsun. Mechanical theorem proving of differential geometries and some of its applications in mechanics. *Journal of Automated Reasoning*, 7(2):171–191, 1991.

[72] Wu Wen-Tsun. On a finiteness theorem about optimization problems. Technical report, 1992.

[73] Sean Wilson and Jacques D Fleuriot. Combining dynamic geometry, automated geometry theorem proving and diagrammatic proofs. In *Workshop on User Interfaces for Theorem Provers (UITP)*, 2005.

[74] Inc Wolfram Research. Mathematica, 2008.

[75] Wen-tsün Wu. On the decision problem and the mechanization of theorem-proving in elementary geometry. *Scientia Sinica*, 21(2):159–172, 1978.

[76] L Yang, X Gao, S Chou, and Z Zhang. Automated proving and discovering of theorems in non-euclidean geometries. *Proceedings of Automated Deduction in Geometry (ADG98), Lecture Notes in Artificial Intelligence*, 1360:171–188, 1998.

[77] Zheng Ye, Shang-Ching Chou, and Xiao-Shan Gao. An introduction to java geometry expert. In *Automated Deduction in Geometry*, pages 189–195. Springer, 2008.

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, _____

_____