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

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

1.1 Увод

У Еуклидској геометрији објекти и релације међу њима могу бити изражени коришћењем полинома. Додатно, свака геометријска конструкција може бити изражена скупом полинома, а свако геометријско тврђење може бити доказано коришћењем алгебарских метода као што су Гребнерове базе или Вуов метод над скупом полинома. Описаћемо имплементацију алгоритма у систему *Isabelle/HOL* који као улазне податке прихвата термове који описују геометријску конструкцију и враћа одговарајући скуп полинома. Даљи циљ је примена метода Гребнерових база у оквиру система *Isabelle/HOL* над генерисаним полиномима у намери да се докаже исправност конструкције и тврђења.

Главна идеја је да се поже аутоматско и формално доказивање у геометрији. И даље не постоји јединствен, нити верификован алгоритам који трансформише геометријску конструкцију у скуп полинома. Обично, транслација у полиноме се ради ад-хок методама и не постоји формална веза између добијених полинома и датих геометријских објеката. Са формално верификованим методом транслације овај проблем би био решен и у оквиру ове тезе биће представљени кораци у том правцу.

1.2 Алгебарски методи у геометрији

Транслација геометријских тврђења у алгебарску форму

Алгебарски методи се користе у аутоматском доказивању у геометрији за теореме конструктивног типа, тј. претпоставке о геометријским објектима које су добијене током геометријске конструкције. Уводе (симболичке) координате за геометријске објекте (тачке, и понекад праве) који се јављају у конструкцији и геометријске конструкције и тврђења изражавају као алгебарске једначине у којима се јављају уведене координате. Потом користе алгебарске технике да покажу да тврђење следи из конструкције.

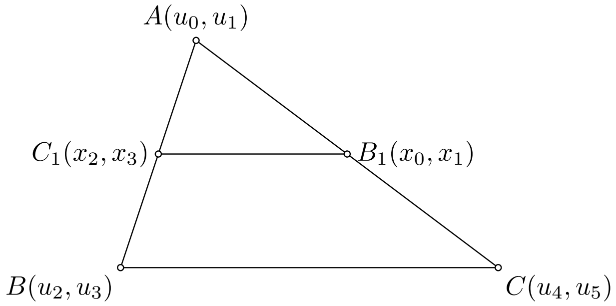
Пре него што је могуће применити алгебарске методе, геометријско тврђење мора бити записано у алгебарској форми, као скуп полиномијалних једнакости (односно полинома), при чему се претпоставља да су све полиномијалне једнакости облика $f(x) = 0$. Стандардна процедура за алгебризацију уводи нове симболичке промељиве за координате тачке и уводи (полиномијане) једнакости који карактеришу сваки конструктивни корак и свако тврђење које је потребно показати. Иако је могуће и за праве које се појављују у конструкцији увести непознате коефицијенте као симболичке промењиве, стандардна процедура избегава такав приступ и користи само тачке (а праве су имплицитно задате). Свака конструкција почиње скупом слободних тачака и током конструкције се уводе зависне тачке. У неким случајевима је могуће зависне тачке бирати са неким степеном слободе (на пример, избор произвољне тачке на датој прави).

Свака тачка добија координате које су репрезентоване симболичким промењивима. Најчеће се слободне промењиве означавају са u_i $(i = 0, 1, 2, \ldots)$, а зависне промењиве се означавају са x_i $(i = 0, 1, 2, \ldots)$. Ако је тачка зависна, онда ће све њене координате бити зависне промењиве. Ако је тачка слободна, онда су њене координате такође слободне. Ако је тачка зависна, али са неким степеном слободе, онда једна координата у дводимензионалном случају или две координате у тродимензионом случају координате могу бити слободне. Ипак, која координата је зависна, а која слободна није тривијално питање и захтева посебну пажњу. На пример, у Декартовој координатној равни, ако је тачка произвољна тачка праве l, једна од координата може бити слободна, а једна зависна и може бити израчуната на основу ограничења која важе за праву. Ипак, ако је права l паралелна са x-осом, онда y координата тачке A не може бити слободна. Слично, ако је l паралелно са y-осом онда x координата тачке A не може бити слободна.

Геометријска ограничења која важе за тачке могу се формулисати у виду алгебарских ограничења над координатама тачке (тј. као полиномијалне једначине над уведеним симболичким координатама). На пример, претпоставимо да симболичке координате за тачку A су (a^x, a^y), за тачку B су (b^x, b^y), а за тачку C су (c^x, c^y). Чињеница да је тачка A средишња тачка интервала BC одговара алгебарским условима $2 \cdot a^x = b^x + c^x$ и $2 \cdot a^y = b^y + c^y$. Услов да су тачке A, B и C колинеарне одговара алгебарском услову $(a^x - b^x)(b^y - c^y) = (a^y - b^y)(b^x - c^x)$. Слични услови се могу формулисати и за друге основне геометријске релације (паралелне праве, нормалне праве, симетрала сегмента итд.).

Примери

***Пример* 1.2.1.** *Дат је троугао ABC, и нека је B_1 средишња тачка сегмента AC, C_1 нека је средишња тачка интервала AB. Показати да је средња линија B_1C_1 паралелна страници троугла BC.*



Слика 1.1: Теорема о средњој линији троугла

Основна идеја је поставити горњу фигуру у координатну раван, те је стога први корак поставити координате за свако теме троугла. Тачке A,

B и C су слободне тачке, те им додељујемо координате $A(u_0, u_1)$, $B(u_2, u_3)$ и $C(u_4, u_5)$. Тачке B_1 и C_1 су зависне, те им додељујемо координате $B_1(x_0, x_1)$ и $C_1(x_2, x_3)$. Како је B_1 средишња тачка сегмента AC, важи

$$2 \cdot x_0 - u_0 - u_4 = 0$$

$$2 \cdot x_1 - u_1 - u_5 = 0$$

Полином са леве страна прве једначине означићемо са f_1, а полином са леве стране друге једначине означићемо са f_2.

Тачка C_1 је средишња тачка сегмента AB, па важи:

$$2 \cdot x_2 - u_0 - u_2 = 0$$

$$2 \cdot x_3 - u_1 - u_3 = 0$$

Полином са леве страна прве једначине означићемо са f_3, а полином са леве стране друге једначине означићемо са f_4.

Са ове четири једначине дат је опис конструкције. Кажемо да полиноми f_1, f_2, f_3 и f_4 припадају скупу–конструкције.

Потребно је показати да је BC паралелно са B_1C_1, односно, записано полиномима, потребно је да важи:

$$(x_2 - x_0)(u_5 - u_3) - (x_3 - x_1)(u_4 - u_2) = 0$$

Полином са леве стране једначине означићемо са g и то је полином тврђења (припада скупу–тврђења).

Потребно је показати да свака n-торка која анулира полиноме конструкције, такође анулира и полиноме тврђења, тј. потребно је показати да

$$\begin{aligned}\forall\ u_0\ u_1\ u_2\ u_3\ u_4\ u_5\ x_0\ x_1\ x_2\quad & x_3 \in \mathbb{R}.\ 2 \cdot x_0 - u_0 - u_4 = 0 \wedge 2 \cdot x_1 - u_1 - u_5 = 0 \\ & \wedge\ 2 \cdot x_2 - u_0 - u_2 = 0 \wedge 2 \cdot x_3 - u_1 - u_3 = 0 \\ & \Longrightarrow (x_2 - x_0)(u_5 - u_3) - (x_3 - x_1)(u_4 - u_2) = 0\end{aligned}$$

Приметимо да у претходном примеру услов да је ABC троугао није преведен у услов да су тачке A, B и C међусобно различите. Додатно, услов да је B_1C_1 паралелно са BC је дато условом једначином $(x_2 - x_0)(u_5 - u_3) - (x_3 - x_1)(u_4 - u_2) = 0$. Са друге стране, ова алгебарска једначина је једнака једном слабијем услову, наиме услову: $B \equiv C$ или $B_1 \equiv C_1$ или B_1C_1 паралелно са

BC. Преведено у геометријски запис, тврђење које је доказано алгебарском методом је следеће:

Нека је B_1 средишња тачка сегмента AC и C_1 нека је средишња тачка интервала AB. Онда је B_1C_1 паралелно са BC или је B идентично тачки C или је тачка B_1 идентична тачки C_1.

Како $B_1 \not\equiv C_1$ следи из $B \not\equiv C$, претходно тврђење је еквивалетно са:

Нека су B и C две различите тачке. Нека је B_1 средишња тачка сегмента AC и C_1 нека је средишња тачка интервала AB. Онда је сегмент B_1C_1 паралелан са BC.

Овај пример показује да транслације геометријског тврђења у алгебарски запис и обратно захтева да се обрати пажња на многе детаље. У већини система, хипотеза облика $AB||CD$ се обично записује једначином облика $(b^x - a^x)(d^y - c^y) = (d^x - c^x)(b^y - a^y)$, чак се ова једначина користи као дефиниција за $AB||CD$. Ипак, овакав приступ, раскида везу са синтетичком геометријом.

У зависности од конструкције и тврђења може бити пуно полинома који припадају скупу–конструкције или скупу–тврђења. Ова два скупа су веома важна за метод Гребнерових база (или за Вуов метод) и касније биће детаљније појашњена њихова улога.

Може се показати да је већина геометријских својстава инваријантна у односу на изометријске трансформације [8, 9]. Ако су P_1 и P_2 две слободне тачке, увек постоји изометрија (прецизније, композиција транслације и ротације) која слика P_1 у тачку $(0, 0)$ (тј. у координатни почетак), а тачку P_2 у тачку на x-оси (или у тачку на y-оси). Зато се без губитка на општости може претпоставити да слободна тачка има координате $(0, 0)$, док друга тачка има координате $(u_0, 0)$ или $(0, u_0)$ (иако су оба избора коректна, у неким случајевима избор може утицати на ефикасност, или, у случају једноставног Вуовог метода, избор може утицати на могућност доказивања). Примена овог закључка може значајно утицати на обим посла који има алгебарска метода. Уз то, постоје хеуристике (са циљем да побољшају ефикасност) за избор која од слободних тачака је најпогоднија за ове специјалне координате.

***Пример* 1.2.2.** *Без губитка на општости у Примеру 1.2.1, тачкама B C могу бити додељене координате $B(0, 0)$ и $C(u_4, 0)$. Тада се алгебарско тврђење које треба доказати своди на:*

$\forall\ u_0\ u_1\ u_4\ x_0\ x_1\ x_2\ x_3 \in \mathbb{R}.\ \ 2 \cdot x_0 - u_0 - u_4 = 0 \land 2 \cdot x_1 - u_1 = 0$

$$\begin{aligned}&\wedge\ 2\cdot x_2 - u_0 = 0 \wedge 2\cdot x_3 - u_1 = 0\\ &\Longrightarrow (x_2 - x_0)\cdot 0 - (x_3 - x_1)\cdot u_4 = 0\end{aligned}$$

што тривијално следи (x_3—$x_1 = 0$ следи из $2\cdot x_1 - u_1 = 0$ и $2\cdot x_3 - u_1 = 0$).

Алгебарски алгоритми

Када се геометријско тврђење преведе у алгебарску форму, могуће је применити алгебарски метод за доказивање теорема. Алгебарски доказивачи теорема користе специфичан алгоритам над системом полинома. Ако су $f_1,\ldots,f_k$ полиноми скупа–конструкције, а $g_1,\ldots,g_l$ полиноми који су добијени из тврђења, онда провера претпоставке се своди на проверу да ли је за свако g_i испуњено:

$$\forall v_1,\ldots,v_n \in \mathbb{R} \bigwedge_{i=1}^{k} f_i(v_1,\ldots,v_n) = 0 \Longrightarrow g_i(v_1,\ldots,v_n) = 0$$

Тарски је приметио да се коришћењем елиминације квантификатора за релане бројеве може доћи до доказа. Али у пракси, тешко је доказати нетривијална математичка тврђења на овај начин јер су и софистицирани алгоритми за елиминацију реалних квантификатора прилично неефикасни. Зато се примењује другачији приступ. Главна идеја, коју је предложио Ву 1978. године је да велики број геометријских тврђења, које се формулишу као универзална алгебарска тврђења у терминима координата, су такође тачна и за комплексне вредности координата. Уместо проверавања полинома над реалним бројевима, користи се поље комплексних бројева и посматра се следећа претпоставка [1]:

$$\forall v_1,\ldots,v_n \in \mathbb{C} \bigwedge_{i=1}^{k} f_i(v_1,\ldots,v_n) = 0 \Longrightarrow g_i(v_1,\ldots,v_n) = 0 \qquad (1.1)$$

Ово је тачно ако g припада идеалу $I = \langle f_1,\ldots f_k\rangle$ који је генерисан над полиномима f_i $(i = 1,\ldots k)$, тј. када постоји цео број r и полиноми $h_1,\ldots h_l$ такви да $g_i^r = \sum_{i=1}^{k} h_i f_i$. Хилбертова (Nullstellensatz) теорема тврди да ако је поље алгебарски затворено (а $\mathbb{C}$ јесте) онда је обрнуто такође тачно.

---

[1] Наравно, постоји проблем некомплетности метода (у односу на геометрију) јер у неким случајевима тврђење важи у $\mathbb{R}$, али метод не успева да докаже због контрапримера који важе у $\mathbb{C}$.

Два најзнаајнија алгебарска метода користе врсту Еуклидског дељења да провере исправност претпоставке дате у 1.1. Бухбергеров алгоритам трансформише полазни скуп у *Гребнерову базу* у којој алгоритам дељења се може ефикасно употребити, а Вуов метод користи *псеудо–дељење* које на неки начин имитира Еуклидско дељење.

Вуов метод

Главна операција над полиномима у Вуовом методу је псеудо–дељење које када се примени на два полинома $p(v_1, \ldots, v_n)$ и $q(v_1, \ldots, v_n)$ производи декомпозицију

$$c^r \, p = tq + r$$

при чему је $c(v_1, \ldots, v_{n-1})$ водећи коефицијент у полиному q уз промењљиву v_n, r је број ненула коефицијената полинома p, $t(v_1, \ldots, v_n)$ је псеудо–количник, $r(v_1, \ldots, v_n)$ је псеудо–остатак, степен v_n у r је мањи него у q. Како важи $r = c^r \, p - tq$, јасно је да r припада идеалу генерисаном над полиномима p и q.

Први корак (једноставног) Вуовог метода [3] користи псеудо–дељење да трансформише конструисани систем полинома $(\bigwedge_{i=1}^{k} f_i)$ у троугаону форму, тј. у систем једначина у коме свака наредна једначина у систему уводи тачно једну нову зависну промењљиву. Након тога, коначни остатак се рачуна псеудо–дељењем полинома тврђења (g_i) са сваким полиномом троугаоног система.

Вуов метод у свом најједноставнијем облику омогућава израчунавање полинома $c, h_1, \ldots, h_k$ и r таквих да важи

$$cg_i = \sum_{i=1}^{k} h_i f_i + r$$

Ако је коначни остатак r једнак нули, онда се сматра да је претпоставка доказана. Једноставан Вуов метод није комплетан (у алгебарском смислу). Комплекснија и комплетна верзија метода користи растуће ланце који се разматрају у оквиру Рит-Вуовог принципа.

Припадност иделу, Гребнерове базе, пример примене Гребнеровог метода на конкретан проблем

У овом одељку су дате основне дефиниције и теореме које представљају математичку основу за овај рад. Прва дефиниција је дефиниција проблема који треба решити. Друга дефиниција дефинише Гребнерове базе, алатку која даје одговор на проблем припадности идеалу. Коначно, дата је и теорема која спаја ове две дефиниције.

Дефиниција 1.2.1 (Припадност идеалу)**.** За дате $f, f_1, \ldots, f_k \in K[X_1, \ldots, X_n]$ где су $f, f_1, \ldots, f_k$ полиноми, а $K[X_1, \ldots, X_n]$ је прстен полинома над K, и $\langle f_1, \ldots f_k \rangle$ је идеал генерисан са $f_1, \ldots f_k$, $f \in \langle f_1, \ldots f_k \rangle$ је задовољено.

Дефиниција 1.2.2. Нека $I = \langle f_1, \ldots, f_n \rangle$ је идеал генерисан коначним скупом полинома. G је **Гребенерова база** идеала I ако и само ако мултиваријантно дељење (означено са $\rightarrow_G$) било ког полинома у идеалу I са G даје 0.

***Теорема* 1.2.1.** *Проблем $f \in I$ је еквивалентан $f \overset{*}{\rightarrow}_G 0$.*

Оно што је заправо речено овом теоремом је да ако постоји скуп полинома конструкције и ако су сви полиноми једнаки нули, онда је могуће одредити Гребнерову базу за овај скуп и ако је могуће показати (коришћем полинома Гребнерове базе) да су сви полиноми тврђења једнаки нули онда је геометријско тврђење тачно. За израчунавање Гребнерове базе користи се *Бухбергеров алгоритам* који се лако може имплементирати. Данас постоје многе хеуристике које омогућавају да израчувања буду бржа, али ми ћемо га представити у његовој основном облику:

Дефиниција 1.2.3. S-полином над полиномима f_i и f_j, означен са $S(f_i, f_j)$ се израчунава на следећи начин:

1) $m = GCD(H(f_i), H(f_j))$

2) $m = m_i * H(f_i)$ при чему је $H(f_i)$ водећи моном у f_i

3) $m = m_j * H(f_j)$ при чему је $H(f_j)$ водећи моном у f_j

4) $S(f_i, f_j) = m_i * f_i - m_j * f_j$

За скуп полинома $\{f_i, ..., f_j\}$ Бухбергеров алгоритам се састоји из следећих корака:

1) S-полином се одређује за свака два полинома из скупа чији водећи мономи нису узајамно прости и новодобијени полиноми се додају у скуп.

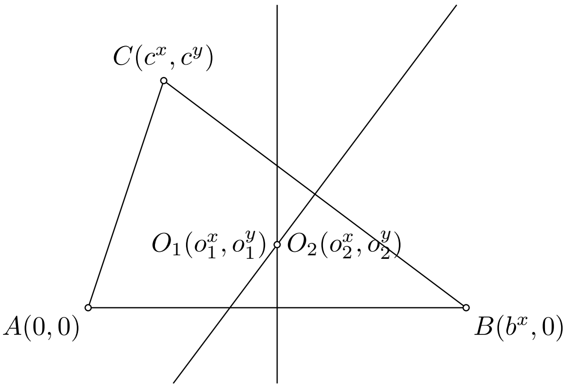
2) Понавља се први корак док год има полинома који могу бити додати.

Метод Гребнерових база је већ имплементиран у систему Isabelle/HOL и може се користити на следећи начин:

lemma "$[\![-2 \cdot u_1 + x_1 + x_2 =$ (0::real); $-2 \cdot v_1 + y_1 + y_2$ = $0]\!] \Longrightarrow$
$x_1 \cdot v_1 - x_1 \cdot y_2 + u_1 \cdot y_2 - v_1 \cdot x_2 - y_1 \cdot u_1 + y_1 \cdot x_2 = 0$"
by algebra

при чему је метод Гребнерових база позван са `by algebra`.

***Пример* 1.2.3.** *Показати да се симетрале страница троугла секу у једној тачки.*



Слика 1.2: Теорема о симетралама страница троугла

Основна идеја је да се горња фигура постави у координатну раван, а потом да се хипотезе теореме интерпретирају као тврђења у аналитичкој, а не синтетичкој, геометрији. То значи да је први корак поставити координате троугла тако што поставимо тачку A у координатни почетак, односно $A = (0,0)$. *Потом, можемо одабрати да су координате тачке* $B = (b^x, 0)$, *а тачке* $C = (c^x, c^y)$ *(тврђење је потребно показати за било које координате тачака, али се лако може показати да је могуће било које координате транслирати у ове које су специјално одабране и олакшавају даља израчунавања). Тачке A, B и C су слободне и њихове координате би могли означити са* u_i $(i = 1, 2, 3)$, али да би лакше пратили ознаке у овом примеру, означили смо их другачије. Сада се геометријска конструкција транслира у скуп полинома.

Прво записујемо хипотезу да се симетрале страница AB и BC секу у тачки $O_1 = (o_1^x, o_1^y)$. Како су симетрале потпуно одређене тачкама A, B, C и O_1, добијају се следеће једначине:

$$f_1 : \qquad o_1^x - \tfrac{b^x}{2} = 0$$

$$f_2 : \qquad \tfrac{b^x - c^x}{c^y} \cdot o_1^x - o_1^y + \tfrac{c^{y2} - b^{x2} + c^{x2}}{2 \cdot c^y} = 0$$

Сада посматрамо другу хипотезу – симетрале страница AB и AC се секу у тачки $O_2 = (o_2^x, o_2^y)$. Добијамо две нове једначине:

$$f_1' : \qquad o_2^x - \tfrac{b^x}{2} = 0$$

$$f_3 : \qquad \tfrac{c^x}{c^y} \cdot o_2^x + o_2^y - \tfrac{c^y}{2} - \tfrac{c^{x2}}{2 \cdot c^y} = 0$$

Значи, имамо скуп полинома:

$$G = \{f_1, f_2, f_1', f_3\}$$

Са овим полиномима је заправо описана конструкција. Сада је потребно показати да важи $O_1 = O_2$, тј. $(o_1^x, o_1^y) = (o_2^x, o_2^y)$. То значи да је потребно одредити Гребнерову базу G' скупа G и циљ је доказати $o_1^x - o_2^x \to_{G'} = 0$ и $o_1^y - o_2^y \to_{G'} = 0$. Са ова два полинома (лева страна датих једначина) дати су полиноми тврђења.

У намери да се израчуна Гребнерова база скупа G користи се Бухбергеров алгоритам и добијени резултат је:

$$\begin{aligned} G' = & \{f_1, f_2, f_3, f_4, f_5, f_6\} = \{o_1^x - \frac{b^x}{2}, \quad o_2^x - \frac{b^x}{2}, \\ & \frac{b^x - c^x}{c^y} \cdot o_1^x - o_1^y + \frac{c^{y2} - b^{x2} + c^{x2}}{2 \cdot c^y}, \quad \frac{c^x}{c^y} \cdot o_2^x + o_2^y - \frac{c^y}{2} - \frac{c^{x2}}{2 \cdot c^y}, \\ & -o_1^y + \frac{c^y}{2} + \frac{c^{x2}}{2 \cdot c^y} - \frac{c^x \cdot b^x}{2 \cdot c^y}, \quad o_2^y - \frac{c^y}{2} - \frac{c^{x2}}{2 \cdot c^y} + \frac{c^x \cdot c}{2 \cdot c^y}\} \end{aligned}$$

Коришћењем овог скупа, $o_1^x - o_2^x \overset{*}{\to}_{G'} 0$ се лако може показати. Заиста,

$$o_1^x - o_2^x \quad \to_{f_1} \quad -o_2^x + \frac{b^x}{2} \quad \to_{f_3} \quad -o_2^x + \frac{b^x}{2} + o_2^x - \frac{b^x}{2} = 0 \; .$$

Слично се може показати $o_1^y - o_2^y \overset{*}{\to}_{G'} 0$,

$$o_1^y - o_2^y \quad \to_{f_5} \quad -o_2^y + \frac{c^y}{2} + \frac{c^{x2}}{2c^y} - \frac{c^x b^x}{2c^y} \quad \to_{f_6}$$

$$\to_{f_6} \quad -o_2^y + \frac{c^y}{2} + \frac{c^{x2}}{2c^y} - \frac{c^x b^x}{2c^y} + o_2^y - \frac{c^y}{2} - \frac{c^{x2}}{2c^y} - \frac{c^x b^x}{2c^y} = 0 \; .$$

1.3 Формална анализа алгебарских метода у систему Isabelle/HOL

Репрезентација геометријских конструкција коришћењем термова

Прво, било је потребно представити геометријску конструкцију на одговарајући начин тако да се лако може аутоматски обрадити, тј. да се може користити у оквиру нашег алгоритма. Зато су геометријске конструкције репрезентоване термовима. Тренутно, постоје два типа објеката – тачке и праве. Додатно, геометријска тврђења су репрезентована коришћењем термова. У систему Isabelle/HOL одговарајући типови се дефинишу на следећи начин:

```
datatype
    point = Point id | Intersect line line | Center point point
and line = Line point point | Bisector point point
       | Normal line point | Parallel line point
and statement = IsIncident point line
       | IsEqualp point point | IsEquall line line
       | IsParallel line line | IsNormal line line
       | IsCongruent point point point point
       | IsBisector line point point
```

Као што можемо видети, тачка може бити дата својим идентификатором или може бити конструисана као пресек две праве или као средиште дужи одређене двема тачкама. Слично, права може бити конструисана као права која је одређена двема тачкама или као симетрала датог сегмента итд. Такође, постоје и различита тврђења. На пример, `IsIncident point line` означава тврђење да тачка припада прави, а `IsEqualp point point` означава да су две тачке једнаке.

***Пример* 1.3.1.** *Терм `IsIncident (Point 1) (Line (Point 1) (Point 2))` означава тврђење да тачка припада прави која је одређена са том тачком и још једном датом тачком.*

***Пример* 1.3.2.** *Терм*

```
let c = Bisector (Point A) (Point B);
    b = Bisector (Point A) (Point C);
    a = Bisector (Point B) (Point C);
    O1 = Intersect a b;
    O2 = Intersect a c in
    IsEqualp O1 O2
```

је пример који је описан раније – симетрале страница се секу у једној тачки.

Синтетичким термовима који служе за репрезентацију геометријских тврђења може бити дата различита семантика интерпретирањем у различитим моделима геометрије (на пример, Декартова координатна раван, геометрија Хилберта, геометрија Тарског). Коришћењем система модула у систему Isabelle/HOL (**`locales`**) избегава се понављање дефиниција. Зато је дефинисан модуо `AbstractGeometry` који садржи примитивне релације (на пример, релацију инциденције, релацију између, релацију подударно) и дефинише њихова својства. Изведени концепти се могу дефинисати једино у оквиру овог локала. На пример, изведени појам колинеарност се своди на примитиван појам инциденције — кажемо да су три тачке колинеарне акко постоји права којој припадају све три тачке. Различите геометрије могу интерпретирати овај модуо и (апстрактне) дефиниције изведених појмова се пренесе у те геометрије.

Сематика термова (у апстрактној геометрији) је дата функцијама `point_interp`, `line_interp` и `statement_interp` чији улазни подаци (редом) су `point`, `line` и `statement`, а повратна вредност су редом (апстрактна) тачка, (апстрактна) права или вредност Boolean. Како је апстрактна интерпретација термова јединствено одређена само ако су слободне тачке фиксне, све ове функције имају и додатни аргумент — функцију која мапира индексе слободних тачака у тачке.

Тврђења се интерпретирају коришћењем примитивних релација апстрактне геометрије, док се конструкције своде на примитивне релације коришћењем Хилбертовог ε оператора (**`SOME`** у систему Isabelle/HOL). На пример:

```
statement_interp (Incident p l) fp =
   incident (point_interp p fp) (line_interp l fp)
point_interp (Intersection l1 l2) fp =
   (SOME P. incident P (line_interp l1 fp)
            ∧ incident P (line_interp l2 fp))
```

Тврђење (записано термом) је исправно у (апстрактној) геометрији ако је тачно за све интерпретације (за било који избор слободних тачака).

```
definition (in AbstractGeometry) valid :: "statement_term => bool"
where
   "valid stmt = (ALL fp. statement_interp stmt fp)"
```

Сви појмови се подижу на ниво конкретног геометријског модела (на пример, Декартова координатна раван, геометрија Хилберта, геометрија Тарског) када се покаже да су интерпретација модула `AbstractGeometry`.

Након што је дефинисана репрезентација геометријских конструкција коришћењем термова, следећи корак је транслирати термове у скупове полинома тако да се на њих може применити метод Гребнерових база или Вуов метод.

Кратак опис алгоритма за транслацију термова у полиноме

Алгоритам се користи да трансформише репрезентацију геометријске конструкције и тврђења из записа коришћењем термова у одговарајуће полиноме. Алгоритам је рекурзиван и његовом применом се добијају два скупа. Први скуп је скуп полинома који репрезентују геометријску конструкцију и зато се зове *скуп–конструкција*. Други скуп је скуп полинома који репрезентују тврђења и њега зовемо *скуп–тврђења*. Метод Гребнерових база се заснива на показивању да сваки полином из скупа–тврђења се може свести на нула коришћењем Гребнерове базе скупа–конструкција.

Алгоритам рекурзивно обрађује дати терм и за сваки непознати објекат уводи нове координате. Такође, истовремено, додају се нови полиноми у одговарајуће скупове који се заснивају на идентитетима аналитичке геометрије. У сваком тренутку чувају се подаци о тренутном стању, односно о симобиличким координатама које су до тог тренутка уведене (што су заправо подтермови полазног терма самог тврђења).

Као пример, показаћемо кораке алгоритма за тврђење `IsIncident point_t line_t` при чему `point_t` и `line_t` могу бити произвољни, комплексни термови за тачку и праву. Кораци су следећи:

- додају се нове променљиве x_0 и y_0. Ове променљиве су непознате координате за тачку O која је дата термом `point_t` — $O(x_0, y_0)$
- додају се променљиве a_0, b_0, и c_0 које представљају непознате коефицијенте за праву p која је дата термом `line_t` — $p = a_0 \cdot x + b_0 \cdot y + c_0$.
- позива се функција `point_poly(point_t,` x_0`,` y_0`)` која конструише полиноме који спајају променљиве x_0 и y_0 са термом `point_t`.
- позива се функција `line_poly(line_t,` a_0`,` b_0`)` која конструише полиноме који спајају променљиве a_0, b_0 и c_0 са термом `line_t`.
- додаје се полином $a_0 \cdot x_0 + b_0 \cdot y_0 + c_0$ у скуп–тврђења.

Као илустрација у наставку се може видети део кода у систему Isabelle/HOL који имплементира овај корак транслације.

```
algbrize (IsIncident p l) ==
   "let x = point_id_x 0; y = point_id_y 0;
        a = line_id_a 0; b = line_id_b 0; c = line_id_c 0;
        (s', pp) = point_poly p x y (| maxp = 0, maxl = 0 |);
        (_, lp) = line_poly l a b s' in
    (sup pp lp,
    Fset.Set[poly_of (PSum [PMult[PVar a, PVar x],
                            PMult[PVar b, PVar y]])])"
```

За репрезентацију полинома коришћена је Isabelle/HOL теорија *Executable Multivariate Polynomials* [14].

Као што се може приметити постоје две нове функције `point_poly` и `line_poly` које имају два аргумента — термове и две променљиве. Ове функције су узајамно рекурзивне и користе се да се одреде полиноми скупа–конструкција. Демонстрираћемо како функционишу на следећем примеру примеру — `Intersect line1_t line2_t`. Као и раније, термови `line1_t` и `line2_t` репрезентују линије и могу бити произвољно комплексни. Терм примера репрезентује тачку и потребно је одредити полиноме који одређују ту тачку. Кораци алгоритма у овом примеру су следећи:

- додајемо променљиве a_1 и b_1 који су коефицијенти праве ($p = a_1 \cdot x + b_1 \cdot y + 1$) која је дата термом `line1_t`
- додајемо променљиве a_2 і b_2 који су коефицијенти праве ($p = a_2 \cdot x + b_2 \cdot y + 1$) која је дата термом `line2_t`
- позива се функција `line_poly(line_t,` a_1`,` b_1`)`
- позива се функција `line_poly(line_t,` a_2`,` b_2`)`
- додају се полиноми $x \cdot (b_2 \cdot a_1 - a_2 \cdot b_1) - b_1 + b_2$ и $y \cdot (b_2 \cdot a_1 - a_2 \cdot b_1) - (a_2 - a_1)$ у скуп–конструкције.

Ови полиноми су добијени коришћењем геометријских једнакости тако да дато геометријско својство важи.

Доказивање исправности

Главна идеја је да се аутоматски метод за доказивање теорема у геометрији формално верификује. То значи да је главни део нашег рада да се докаже исправност алгоритма транслације. У намери да се то уради, биће коришћена аналитичка геометрија као веза између синтетичке геометрије и алгебре. Потребно је показати да све што се покаже коришћењем алгебарских метода такође важи у свим моделима синететичке геометрије. Са друге стране, још је потребно показати да је аналитичка геометрија модел синтетичке геометрије и још даље, да су сви модели изоморфни, тј. да све што важи у нашем моделу такође важи и у другим моделима.

Формализацију везе између синтетичке и аналитичке геометрије, односно, доказ да је аналитичка геометрија модел геометрије Тарског и геометрије Хилберта смо показали и дискутовали раније, у поглављу **??**.

Веза између аналитичке геометрије и алгебре. Централна теорема коју смо формално показали је да ако су сви полиноми тврђења нула кад год су и полиноми конструкције нула (тј. ако сви полиноми тврђења припадају идеалу генерисаном над полиномима конструкције), онда је тврђење исправно у аналитичкој геометрији. Односно, ако је неко тврђење доказано методом Гребнерових база оно заиста важи и у аналитичкој геометрији. Записано у терминима математичке формуле:

$$(\forall(u,x))(\forall g \in G)((\forall f \in F.f(u,x)=0) \Rightarrow g(u,x)=0) \Rightarrow \text{геометријско тврђење}$$

при чему је $F(u,x)$ скуп–конструкције, а $G(u,x)$ је скуп–тврђења. Када кажемо *геометријско тврђење* мислимо на тврђење у аналитичкој геометрији јер су алгебарски методи повезани са аналитичком геометријом. Први део је показати да важи $(\forall f \in F)(\forall(u,x))f(u,x)=0$. Други део је показати да ако је показано $(\forall g \in G)(\forall f \in F.f(u,x)=0) \Rightarrow g(u,x)=0)$ онда геометријско тврђење важи у аналитичкој геометрији.

Запис овог тврђења у систему Isabelle/HOL је:

```
theorem "let (cp, sp) = algebrize term in
(ALL ass. ((ALL p : cp. eval_poly ass p = 0) ⟶
           (ALL p : sp. eval_poly ass p = 0)) ⟶
        AnalyticGeometry.valid s)"
```

Доказ се изводи коришћењем индукције у систему Isabelle/HOL. Посматрајмо следећи пример:

`In (Center (Point 0) (Point 1)) (Line (Point 0) (Point 1))`

`Point 0` `Point 1` добијају фиксне координате (p_0^x, p_0^y) и (p_1^x, p_1^y). Потом `Center (Point 0) (Point 1)` добија координате (x_1, y_1) и оне су зависне промењљиве и зависе од `Point 0` и `Point 1`. На исти начин додељујемо координате (a_1, b_1, c_1) за `Line (Point 0) (Point 1)` (a_1, b_1, c_1) (то су опет зависне промењљиве које зависе од већ датих тачака `Point 0` и `Point 1`). За доказ исправности потребно је показати да важи:

$$\begin{aligned} 2x_1 &= p_0^x + p_1^x \qquad & a_1(p_1^x p_0^y - p_1^y p_0^x) - c_1(p_1^y - p_0^y) &= 0 \\ 2y_1 &= p_0^y + p_1^y \qquad & b_1(p_1^x p_0^y - p_1^y p_0^x) + c_1(p_1^x - p_0^x) &= 0 \\ &\text{закључак је дат у форми једначине:} & a_1x_1 + b_1y_1 + c_1 &= 0 \end{aligned}$$

Ово се лако показује коришћењем идентита у аналитичкој геометрији.

Закључци и даљи рад

Алгоритам се може оптимизовати и могуће је додати још геометријских објеката (кругови, елипсе итд.) и геометријских тврђења. Цео алгоритам је потребно повежати са већ постојаћим формализованим методом Гребнерових база у систему Isabelle/HOL.

Како имплементација генерисања полинома није везана ни за један конкрета метод, могуће је користити генерисане полиноме и за друге алгебарске методе, као што је Вуов метод.

1.4 Примена алгебарских метода на проблеме у стереометрији

Последњих неколико година, рачунари и технологија се интезивно користе и мењају начин како се предаје геометрија. Динамички геометријски системи као што су *GeoGebra* [2], *Cinderella* [3], *Geometer's Sketchpad* [4], *Cabri* [5], *Eukleides* [6] се данас често користе у свим нивоима образовања. Студенти користе овакве системе да би изводили геометријске конструкције и дијаграме које могу да мењају променом слободних тачака. Такви динамички дијаграми су бољи него статичке слике јер померање слободних тачака може да пружи додатни увид у проблем и да открије дегенеративне случајеве и да помогне студентима да утврде да ли је нешто тачно ако и само ако је неки специјални размештај тачака задат (на пример, неко својство може бити тачно само ако је нека тачка између неке друге две тачке, а нетачно је ако то није случај, неко својство може бити тачно само за оштре, али не и за тупе углове, итд.).

Интезивним мењањем дијаграма померајући слободне тачке, студент мое-же бити прилично сигуран да ли је својство тачно у општем случају (тј. тачно у готово свим случајевима, осим у малој групи дегенеративних случајева), али ипак, то не можемо сматрати доказом и овакав приступ је подложан грешкама. Зато, у скорије време, динамички геометријски системи су проширени аутоматским системима за доказивање, који аутоматски могу доказати твр-

---

[2] `https://www.geogebra.org/`

[3] `https://www.cinderella.de/tiki-index.php`

[4] `http://www.dynamicgeometry.com/`

[5] `http://www.cabri.com/`

[6] `http://www.eukleides.org/`

ђење о конструисаним објектима [1]. Такви системи су најчешће алгебарски (операције се изводе над симболичким координатама геометријских објеката).

Можда још значајна употреба динамичког геометријског софтвера може бити за тродимензионални простор у коме је често тешко голим оком одредити неко својство. Ово је најчешће стога што се тродимензиони простор посматрата као дводимензиона пројекција, па самим тим мере и односи нису у складу са стварним дијаграмом.Неки системи су почели да развијају подршку за тродимензионе конструкције. У најновијој верзији система *Geogebra* развијена је подршка за динамичку тродимензионалну геометрију и графику [7]. Могуће је креирати и интерактивно мењати тродимензионалне објекте као што су тачке, праве, полигони, сфере, као и тродимензионе цртеже функција. Ипак, овај систем не подржава доказивање тврђења о тродимензионалним објектима.

Такође, постоји и додатак за систем *Cinderella*, *Cindy3D* [8]. Могуће је цртати објекте коришћењем команди и формула које их описују.

Већина истраживања како у динамичким геометријским системима, као и у аитоматским доказивачима теорема је посвећена само дводимензионалној Еуглидској геометрији (планарној геометрији). Иако постоји неколико покушаја да се примене алгебарски доказивачи теорема на тродимензионалну Еуклидску простору геометријуу (стереометрију), ми нисмо нашли да постоји детаљни опис ових метода, нити јавно доступних аутоматских доказивача за стереометрију. У овом раду ми истражујемо и поредимо пар приступа како се алгебарски доказивачи засновани на Вуовој методи и методи Гребнерових база могу применити на проблеме из стереометрије. Нудимо један систем за стереометрију који може да доказује тврђења о својствима конструисаних објеката. Такође, анализирамо корпус проблема из стереометрије и оцењујемо коришћене методе . Дискутујемо о изазовима и могућим применама у пољу предавања геометрије.

Аутоматско доказивање у стереометрији – досадашњи резултати. Чоу (кин. *hang-Ching Chou*) и сарадници су представили метод запремине за решавање проблема у стереометрији [4]. То је полу–алгебарски метод који је проширење методе површине за стереометрију. Хипотезе се могу конструк-

---

[7] `https://wiki.geogebra.org/en/3D_Graphics_View`

[8] `http://gagern.github.io/Cindy3D/`

тивно представити, а закључци су полиномијалне једначине које садрже неколико геометријских величина, као што су запременима, однос дужи, однос површина и Питагорине разлике. Кључна идеја метода је да елиминише тачке из закључка геометријског тврђења коришћењем неколико основних својстава запремине.

Главна мотивација за наш рад потекла је из интересантног рада који представља неколико примера алгебарског доказивања у стереометрији [13]. У раду се посматрају задаци из стереометрије са Олимпијских такмичења из математике. Они у раду представљају три различита проблема и дају полиноме које су извели на папиру и који описују посматране проблеме. Коришћењем ова три примера они показују да алгебарски методи се могу користити за доказивање у стереометрији. За сваки пример користили су три различита метода, метод карактеристичног скупа [17, 16, 7, 2], метод Гребнерових база [6, 11, 15, 5] и метод вектора [12]. Методи се пореде и закључак је да метод вектора даје бољи геометријски доказ, али формуле могу бити дуге и незгодне за манипулацију и израчунавање. Ипак, они не нуде неки систематичан начин како се геометријска тврђења могу представити полиномима.

Према нашем досадашњем знању, не постоје радови који описују начин примене Вуове методе или методе Гребнерових база на проблеме из стереометрије.

Алгебризација геометријских релација у стереометрији

Да би могли да применимо алгебарске методе прво се мора омогућити репрезентација различитих геометријских релација између објеката у стереометрији коришћењем полиномиалних једнакости над њиовим координатама. У овом поглављу даћемо примере како се то може учинити за најчешће релације међу објектима.

Постоји више приступа за запис релација као полиномијалних једнакости и прво питање које се поставља је који објекти у тродимензионом простору се сматрају као основни. У првом приступу за који смо се одлучили, сви објекти су дефинисани коришћењем тачака (на пример, праве се дефинишу преко две различите тачке, равни се дефинишу преко три различите, неколинеарне тачке итд.). Једине променљиве које се користе у свим полиномима су координате тачака. У другом пристипу, све врсте објекта се представљају коришћењем њихових сопствених координата (на пример, права се дефинише координатама једне своје тачке и координатама вектора правца, а раван се дефинише помоћу коефицијената једначине равни – координате вектора нормале на раван и њена удаљеност од координатног почетка). Полиноми укључују све ове координатне променљиве. Показаћемо како енкодирати релације коришћењем оба приступа и поредићемо њихову ефикасност.

Основни појмови коришћени у конструкцији полинома

Већина релација се изражава коришћењем истог скупа појмова које ћемо овде увести.

Сваки објекат је представњен неком n–торком параметара (а видећемо да то могу бити и симболичке и нумеричке вредности).

Тачке имају три параметра, означена са $([\_]^x, [\_]^y, [\_]^z)$ који репрезентују њене координате. Свака тачка је задата или својим симболичким или нумеричким координатама. За сваку новоуведену тачку се додељују нове симболичке координате.

Праве се представљају различито у зависности од коришћеног приступа. У првом приступу, права је задата са две различите тачке и са шесторком која представља координате тих тачака. За праву p, прва тачка ће бити означена са p_A, а друга тачка ће бити означена са p_B.

У другом приступу, права је дата датом тачком A и датим вектором v. Вектор праве p ће бити означен са $\overrightarrow{p_v}$, а тачка праве p ће бити означена са p_A. Зато, као и у првом приступу, права ће и у другом приступу имати шест параметара који су означени са $([\_]^{v_x}, [\_]^{v_y}, [\_]^{v_z}, [\_]^{A_x}, [\_]^{A_y}, [\_]^{A_z})$, који репрезентују праву дату једначином:

$$x = k \cdot [\_]^{v_x} + [\_]^{A_x} \quad y = k \cdot [\_]^{A_y} + [\_]^{A_y} \quad z = k \cdot [\_]^{v_z} + [\_]^{A_z}.$$

У претходној једначини, k означава размеру праве, али ова информација се не чува међу параметрима праве (а то је поменута шесторка). У неким полиномима ће бити потребно користити параметар размере праве, али ће се посматрати као нова симболлична променљива.

Равни се такође могу различито представити у зависности од коришћеног приступа. У првом приступу, раван се задаје са три неколинеарне тачке, односно са деветорком њихових координата. Прва тачка равни π ће бити означена са π_A, друга тачка ће бити означена са π_B, а трећа тачка ће бити означена са π_C.

У другом приступу, равни су одређене нормалним вектором v и додатним параметром d (померај у односу на координатни почеак). Вектор равни π ће бити означен са $\overrightarrow{\pi_v}$, а слободан параметар равни ће бити означен са. Стога ће раван имати само четири параметра, означена са $([\_]^{v_x}, [\_]^{v_y}, [\_]^{v_z}, [\_]^{d})$, који репрезентују раван дату следећом једначином:

$$[\_]^{v_x} \cdot x + [\_]^{v_y} \cdot y + [\_]^{v_z} \cdot z + [\_]^{d} = 0.$$

Вектор одређен двема тачкама $A = (a^x, a^y, a^z)$ и $B = (b^x, b^y, b^z)$ је $\overrightarrow{AB} = (b^x - a^x, b^y - a^y, b^z - a^z)$. Стандардни појамови скаларног производа, векторског производа и мешовитог производа се могу применити над векторима. Скаларни производ вектора $v = (v^x, v^y, v^z)$ и $u = (u^x, u^y, u^z)$ је $v \cdot u = v^x \cdot u^x + v^y \cdot u^y + v^z \cdot u^z$, њихов векторски производ је одређен матрицом:

$$v \times u = \begin{vmatrix} \overrightarrow{i} & \overrightarrow{j} & \overrightarrow{k} \\ v^x & v^y & v^z \\ u^x & u^y & u^z \end{vmatrix},$$

а мешовити производ са вектором $w = (w^x, w^y, w^z)$ је једнак $v \cdot (u \times w)$, и одређен је матрицом:

$$\begin{vmatrix} v^x & v^y & v^z \\ u^x & u^y & u^z \\ w^x & w^y & w^z \end{vmatrix}.$$

Репрезентовање релација између геометријских објеката

У овом поглављу су дати полиноми који аритметички описују релације над конструисаним објектима (на пример, две тачке су једнаке, две линије су паралелене, две равни су ортогоналне). Свака релација уводи полиномијална ограничења над координатама објеката који учествују у релацији и у зависности од приступа могу бити различити.

Улазни параметри дате релације су параметри свих објеката који су укључени у ту релацију. На пример, за релацију `congruent` $A\ B\ C\ D$ улаз су четири тачке, A, B, C, and D, односно њихове симболичке координате: (a^x, a^y, a^z), (b^x, b^y, b^z), (c^x, c^y, c^z) и (d^x, d^y, d^z).

▷ `congruent` $A\ B\ C\ D$

Опис: Два сегмента, AB и CD су конгруентна.

Полиноми:
$\overrightarrow{AB} \cdot \overrightarrow{AB} = \overrightarrow{CD} \cdot \overrightarrow{CD}$.

Приметимо да из претходног израза можемо добити полиномијалну једнаккост $poly = 0$, при чему је

$$poly = (a^x - b^x)^2 + (a^y - b^y)^2 + (a^z - b^z)^2 - \\ (c^x - d^x)^2 - (c^y - d^y)^2 - (c^z - d^z)^2$$

Објашњење: Квадрати растојања између A и B мора бити једнако квадрату растојања између C и D.

▷ `segments_in_ratio` $A\ B\ C\ D\ m\ n$

Опис: Дужина сегмента AB и CD су у датом односу $\frac{m}{n}$, тј. $\frac{|AB|}{|CD|} = \frac{m}{n}$.

Полиноми:
$n^2 \cdot \overrightarrow{AB} \cdot \overrightarrow{AB} = m^2 \cdot \overrightarrow{CD} \cdot \overrightarrow{CD}$.

Објашњење: Квадрати растојања између A и B и између C и D морају бити у односу $\frac{m^2}{n^2}$. Приметимо да се ово своди на конгруентност када је $m = n$.

▷ `is_midpoint` $M\ A\ B$

Опис: Проверава да ли је тачка M средња тачка сегмента одређеног са тачкама A и B.

Полиноми: $\overrightarrow{MA} = \overrightarrow{MB}$. Приметимо да ова једнакост даје три различита полинома $poly_1 = 0$, $poly_2 = 0$, $poly_3 = 0$:

$$poly_1 = 2m^x - a^x - b^x$$
$$poly_2 = 2m^y - a^y - b^y$$
$$poly_3 = 2m^z - a^z - b^z$$

▷ `point_segment_ratio` $M\ A\ B\ p\ q$

Опис: Проверава да ли тачка M дели сегмент одређен тачкама A и B у односу одређеним са p и q, тј. $\frac{|MA|}{|MB|} = \frac{p}{q}$.

Полиноми: Изводе се три полинома из: $q \cdot \overrightarrow{MA} = p \cdot \overrightarrow{MB}$.

Објашњење: Приметимо да `is_midpoint` M A B може такође бити записнао коришћењем овог правила, на следећи начин `point_segment_ratio` M A B 1 1.

- ▷ `equal_points` A B

  Опис: Проверава да ли две тачке A и B имају исте координате.

  Полиноми: Изводе се три полинома из израза $\overrightarrow{AB} = 0$.

- ▷ `translate_z` A O q

  Опис: Проверава да ли је тачка O једнака тачки која се добија транслирањем тачке point A за вектор $(0, 0, q)$.

  Полиноми: Полиному су изведени из $\overrightarrow{AO} = (0, 0, q)$

- ▷ `orthogonal_4points` A B C D

  Опис: Проверава да ли права одређена са тачкама A и B је ортогонална на праву одређену са тачкама C и D.

  Полиноми: $\overrightarrow{AB} \cdot \overrightarrow{CD} = 0$

- ▷ `orthogonal_lines` p q

  Опис: Две праве, p и q су ортогоналне.

  Полиноми: Ако је коришћен први приступ, онда су праве задате тачкама (p_A, p_B) и (q_A, q_B), па се то своди на претходни случај и полином је $\overrightarrow{p_Ap_B} \cdot \overrightarrow{q_Aq_B} = 0$. Ако се користи други приступ, као улаз задат је вектор правца правих и полином је $\overrightarrow{p_v} \cdot \overrightarrow{q_v} = 0$.

- ▷ `incident` A p

  Опис: Проверава да ли тачка A припада прави p.

  Полиноми: Ако је коришћен први приступ, онда се изводе три полинома из једнакости $\overrightarrow{p_Ap_B} \times \overrightarrow{Ap_A} = 0$. Ако је коришћен други приступ, онда се изводе три полинома из једнакости $\overrightarrow{p_v} \times \overrightarrow{Ap_A} = 0$.

- ▷ `parallel_lines` p q

  Опис: Проверава да ли су две праве, p и q паралелне.

  Полиноми: Изводе се три полинома из $\overrightarrow{p_Ap_B} \times \overrightarrow{q_Aq_B}$ или из $\overrightarrow{p_v} \times \overrightarrow{q_v}$ у зависности од приступа.

▷ `parallel_planes` α β

Опис: Проверава да ли две равни α и β су паралелне.

Полиноми: Ако се користи други приступ, изводе се три полинома из $\overrightarrow{\alpha_v} \times \overrightarrow{\beta_v} = 0$.

Ако се користи први приступ изводе се полиноми из једнакости:

$$\overrightarrow{\beta_A\beta_B} \cdot \overrightarrow{\alpha_A\alpha_C} \times \overrightarrow{\alpha_B\alpha_A} = 0$$

$$\overrightarrow{\beta_A\beta_C} \cdot \overrightarrow{\alpha_A\alpha_C} \times \overrightarrow{\alpha_A\alpha_B} = 0$$

▷ `orthogonal_planes` α β

Опис: Проверава да ли су две равни, α и β ортогоналне.

Полиноми: Ако се користи први приступ полином се изводи из: $(\overrightarrow{\alpha_A\alpha_B} \times \overrightarrow{\alpha_A\alpha_B}) \cdot (\overrightarrow{\beta_A\beta_B} \times \overrightarrow{\beta_A\beta_B}) = 0$.

Ако се користи други приступ, полином се изводи из: $\overrightarrow{\alpha_v} \cdot \overrightarrow{\beta_v} = 0$.

▷ `point_in_plane` A π

Опис: Проверава да ли тачка A припада равни π.

Полиноми: Ако је коришћен први приступ, онда се полином добија из:

$$\overrightarrow{\pi_A A} \cdot (\overrightarrow{\pi_A\pi_B} \times \overrightarrow{\pi_A\pi_C}) = 0.$$

Ако је коришћен други приступ, полином се добија из једнакости: $\overrightarrow{\pi_v} \cdot \overrightarrow{A} + \pi^d = 0$.

▷ `parallel_line_plane` p α

Опис: Проверава да ли су права p и раван α паралелни.

Полиноми: Ако је коришћен први приступ, једнакост је: $\overrightarrow{p_Ap_B} \cdot (\overrightarrow{\alpha_A\alpha_B \times \alpha_A\alpha_C}) = 0$.

Ако је коришћен други приступ, полином се добија из једнакости: $\overrightarrow{p_v} \cdot \overrightarrow{\alpha_v} = 0$.

Примедба: Ова релација важи и у случају када права припада равни.

▷ `orthogonal_line_plane` p α

Опис: Проверава да ли су права p и раван α ортогонални.

Полиноми: Ако је коришћен први приступ, полиноми се изводе из две једнакости: $\overrightarrow{p_A p_B} \cdot \overrightarrow{\alpha_A \alpha_B} = 0$ and $\overrightarrow{p_A p_B} \cdot \overrightarrow{\alpha_A \alpha_C} = 0$.

Ако је коришћен други приступ, три полинома се изводе из једнакости: $\overrightarrow{p_v} \times \overrightarrow{\alpha_v} = 0$.

▷ `equal_angles` $A\ O\ B\ C\ K\ D$

Опис: Проверава да ли су два угла $\angle AOB$ и $\angle CKD$ једнаки.

Полиноми: Ова релација се може изразити коришћењем тригонометрије. Ипак, треба имати на уму да коришћењем тригонометрије, услов је ослабљен јер се пореде косинуси углова, а као што је познато, косинус тупог угла и косинус оштрог угла могу бити исти, а углови (јасно) нису једнаки. Полиноми се изводе из

$$\cos^2 \angle AOB = \cos^2 \angle CKD.$$

А косинус угла се може одредити на следећи начин:

$$\cos^2 \angle AOB = \frac{(\overrightarrow{AO} \cdot \overrightarrow{BO})^2}{|AO|^2 |BO|^2}$$

при чему је $|AO|^2 = \overrightarrow{AO} \cdot \overrightarrow{AO}$. Једнакост за $\cos^2 \angle CKD$ је слична. Коначно, након неколико једноставних алгебарских операција, полином релације се може извести из једнакости

$$(\overrightarrow{AO} \cdot \overrightarrow{BO})^2 |CK|^2 |DK|^2 = (\overrightarrow{CK} \cdot \overrightarrow{DK})^2 |AO|^2 |BO|^2.$$

Ипак, као што ћемо видети у наредном поглављу, овако задат полином је веома комплексан и било је потребно раставити га на једноставније да би могао ефикасно да се користи у доказивачима теорема.

Тела. Тела се задају коришћењем релација које важе за њихова темена и за њихове странице. Одлучили смо да подржимо само она тела која се налазе у неком *канонском* положају — на пример, при дефинисању коцке, једно теме се налази у координатном почетку, а друга три темена се налазе на координатним осама (x–оси, y–оси и z–оси). Ипак, овакав приступ има мане. На пример, није могуће задати више од једне коцке коришћењем елементарне наредбе за задавање коцке. Темена других коцки на слици које нису у канонском положају морају се задати коришћењем релација које смо представили изнад. Ипак, са друге стране, у геометријским проблемима која се сусрећу у збиркама најчешће постоји само једно слободно тело, и без губитка на општости се може претпоставити да је оно у канонском положају. Када се у тексту задатка уводе друга тела, она су обично зависна у односу на већ задато слободно тело, па су њихова темена у некој релацији са већ датим објектима. Зато, могућност задавања само канонских објеката за већину задатака није представљао проблем.

▷ `make_cube` $A\ B\ C\ D\ A_1\ B_1\ C_1\ D_1$

Опис: Коцка у канонској позицији, са дужином странице једнакој 1.

Објекти и параметри: Тачке $A(0,0,0)$, $B(1,0,0)$, $C(1,1,0)$, $D(0,1,0)$, $A_1(0,0,1)$, $B_1(1,0,1)$, $C_1(1,1,1)$ и $D(0,1,1)$.

Полиноми: Не генеришу се полинома. No polynomials are generated.

Објашњење: Како је коцка у канонској позицији, не уводе се нове симболичке променљиве.

▷ `make_tetrahedron` $A\ B\ C\ D$

Опис: Тетраедар у канонској позицији.

Објекти и параметри: Темена тетраедра имају координате the coordinates $A(0,0,0)$, $B(1,0,0)$, $C(c^x, c^y, 0)$ и $D(c^x, d^y, d^z)$, при чему се уводе четири нова параметра.

Полиноми:
$$\begin{aligned} poly_1 &= 2 \cdot c^x - 1 \\ poly_2 &= 2 \cdot c^{y2} - 3 \\ poly_3 &= 3 \cdot d^y - c^y \\ poly_4 &= 3 \cdot d^{z2} - 2 \end{aligned}$$

Објашњење: $c^x = \frac{1}{2}$, $c^y = \frac{\sqrt{3}}{2}$, $d^y = \frac{\sqrt{3}}{6} = \frac{c^y}{3}$, $d^z = \frac{\sqrt{2}}{\sqrt{3}}$. Приметимо да сви објекти имају или симболичке или бројевне параметре. Коефицијенти полинома морају увек бити цели бројеви, па се ирационалне вредности (као и разломци) морају увести коришћењем полинома.

▷ `make_pyramid_4side` $A\ B\ C\ D\ S$

Опис: Правилна пирамида у канонској позицији – основа пирамиде је јединични квадрат у xOy равни, висина пирамиде није фиксирана, а стране пирамиде се једнаке дужине.

Објекти и параметри: Тачке $A(0,0,0)$, $B(1,0,0)$, $C(1,1,0)$, $D(0,1,0)$ и $S(s^x, s^y, s^z)$, са три нове симболичке променљиве s^x, s^y и s^z.

Полиноми: $poly_1 = 2 \cdot s^x - 1$

$poly_2 = 2 \cdot s^y - 1$

Објашњење: Пројекција врха пирамиде је $(s^x, s^y, 0)$ и она лежи у центру јединичног квадрата, тако да $s^x = s^y = \frac{1}{2}$. Приметимо да s^z није ограничено.

▷ `make_square` $A\ B\ C\ D$

Опис: Задаје се квадрат у канонској позицији, односно квадрат у равни xOy, чије једно теме је у координатном почетку, а друга два темена на координатним осама и дужина странице је једнака 1.

Објекти и параметри: Тачке $A(0,0,0)$, $B(1,0,0)$, $C(1,1,0)$, $D(0,1,0)$.

Полиноми: Не креирају се нови полиноми.

▷ `equilateral_triangle` $A\ B\ C$

Опис: Једнакостранични троугао у канонској позицији – налази се у xOy равни, једна тачка је у координатном почетку, а друга тачка је на x–оси.

Објекти и параметри: Тачке $A(0,0,0)$, $B(1,0,0)$, $C(c^x, c^y, 0)$, са два нова параметра c^x и c^y.

Полиноми: $poly_1 = 2 \cdot c^x - 1$

$poly_2 = 4 \cdot c^y - 3$

▷ `regular_hexagon` $A_1\ A_2\ A_3\ A_4\ A_5\ A_6$

Опис: Правилни шестраедар у канонској позицји – налази се у xOy равни, једна тачка је у координатном почетку, а друга тачка је на x–оси.

Објекти и парамерти: Тачке $A_1(0,0,0)$, $A_2(1,0,0)$, $A_3(a_3^x, a_3^y, 0)$, $A_4(1, a_4^y, 0)$, $A_5(0, a_4^y, 0)$ и $A_6(a_6^x, a_3^y, 0)$, са четири нова параметра a_3^x, a_3^y, a_4^y, и a_6^x.

Полиноми: $poly_1 = 2 \cdot a_3^x - 3$

$poly_2 = 4(a_3^y)^2 - 3$

$poly_3 = a_4^y - 3$

$poly_4 = 2a_6^x - 1$

Упрошћавање полинома

Да би могли да тестирамо предлођену алгебризацију геометријских релација користили смо две алатке, *GeoProver* и *Mathematica*, метод Гребнерових база. Први проблем на који смо наишли је временско и просторно огранчење које се дешавало у бројним ситуацијама због комплексности скупа полинома. Разлог за ово је велики број промењљивих и велики број полинома који су у процесу алгебризације креирани. Треба имати на уму да су полиноми у стереометрији доста комплекснији од одговарајучих полинома у планараног геометрији. Зато, морали смо да упростимо скуп добијених полинома.

Користили смо приступ о ком смо раније доста писали – Харисонов приступ без губитка на општости [?] тако што смо бирали погодни координатни систем јер избор координатног система може значајно да смањи комплексност полинома.

За три независоно задате тачке, A, B и C, могуће је изабрати њихове координате на такабв начин да је $A(0, 0, 0)$ у координатном почетку, $B(0, 0, b^z)$ се налази на z–оси, а $C(0, c^y, c^z)$ лежи у yOz равни. Са овим избором координата, број пшромењљивих је смањен за шест, а одоговарајуће нуле значајно поједностављују полиноме. Овај приступ је често коришћен у алгебарским методима. Не утиче на општост тврђења и оправданост коришћења овог приступа је у чињеници да транслације и ротације могу бити коришћење да трансформишу тачке у њихове канонске позиције. Транслације и ротације су изометрије што значи да чувају растојање, али и бројне геометријске релације као што је инциденција, ортогоналност, паралелност, величину угла и друге.

Без примене овог метода, чак и најједноставнија тврђења не могу бити доказана. Избором погодних координата значајно се повећава једноставност система полинома и тиме алгебарски доказивачи су знатно ефикаснији. Даље, може се десити да су неки полиноми вишак јер постану једнаки 0 и онда је само потребно избрисати их из система. Додатно, неки полиноми постану полиноми који имају само једну промењљиву на неки степен (имају само један моном) и ти полиноми исто могу бити избрисани, а одговарајућа променљива се може поставити на нула.

Поред поменутог, треба још имати на уму да доказивач *GeoProver* не може да трансформише систем полинома који садржи једнакост $0 = 0$ у тријагонални систем. Са друге страна, метод Гребнерових база имплементиран у систему *Mathematica* није има проблема приликом доказивања уколико су се у систему налазили полиноми $0 = 0$ или $koeff \cdot x_i^s = 0$.

Раније смо већ видели како се погодно могу задати тела. О томе смо писали у одељку 1.4 и управо избор да тела ставимо у канонски положај значајно утиче на упрошћавање полинома.

Надаље, применили смо још један метод за слимплификацију и то у случају када имамо полиноме облика $koeff \cdot x_i - koeff \cdot x_j = 0$ или $koeff \cdot x_i + koeff \cdot x_j = 0$. Ако без губитка на општости претпоставимо да $j < i$, заменимо свако појављивање x_i са x_j у првом случају, односно свако појављивање x_i са $-x_j$, онда можемо и поменуте полиноме избриати из система. Овим се смањује и број полинома и број променљивих.

Један од најкомплекснијих полинома који се могу добити током агребизације је полином који се добија од релације „једнаки углови”. Приликом доказивања тврђења о једнакости углова, доказивач *GeoProver* је достигао просторни лимит већ након неколико корака. Са друге стране, метод Гребнерових база из система *Mathematica* је радио пар сати након чега смо решили да прекинемо доказивање (а нисмо добили одговор да ли је тврђење тачно). Потом је полином за једнакост углова подељен у више мањих, једноставнијих полинома:

$$\begin{aligned}
scalar_1 &= \overrightarrow{AO} \cdot \overrightarrow{BO} \\
scalar_2 &= \overrightarrow{CK} \cdot \overrightarrow{DK} \\
dist_{CK} &= |CK| \\
dist_{DK} &= |DK| \\
dist_{AO} &= |AO| \\
dist_{BO} &= |BO| \\
poly &= \quad scalar_1 * scalar_1 * dist_{CK} * dist_{DK} \\
&\quad\; - scalar_2 * scalar_2 * dist_{AO} * dist_{BO}
\end{aligned}$$

Иако смо овим повећали скуп полинома, оба доказивача нису имала проблема приликом дојказивања истог тврђења и оба су доказивање завршили у кратком временском периоду, око једне секунде.

Додатно подешавање полинома за Вуов метод

Наијинтересантнији пример пример приликом задавања релација које задовољава тачка је случај пресека правих. У тродимезионом простору немају све праве пресек, неке су паралелне, али неке могу бити и мимоилазне. Погледајмо релацију и полиноме које она генерише.

`intersection_lines` A l_1 l_2

Опис: Тачка A је пресек две дате праве l_1 и l_2.

Улаз: Две дате праве l_1 и l_2 задате својим параметрима (посматрамо само други приступ, слична ситуација је и у првом приступу) $l_1(l_1^{v_x}, l_1^{v_y}, l_1^{v_z}, l_1^{p_x}, l_1^{p_y}, l_1^{p_z})$ и $l_2(l_2^{v_x}, l_2^{v_y}, l_2^{v_z}, l_2^{p_x} l_2^{p_y}, l_2^{p_z})$.

Нови објекти и параметри: Тачка A са симболичким координатама (a^x, a^y, a^z). Параметри k_1 и k_2 који редом представљају размере правих l_1 и l_2.

Полиноми: Полиноми се генеришу коришћењем правла: `intersection_lines` A l_1 $l_2 =$ `incident` A l_1 и `incident` A l_2

Полиноми:
$$\begin{aligned}
poly_1 &= a^x - k_1 \cdot l_1^{v_x} - l_1^{p_x}\\
poly_2 &= a^y - k_1 \cdot l_1^{v_y} - l_1^{p_y}\\
poly_3 &= a^z - k_1 \cdot l_1^{v_z} - l_1^{p_z}\\
poly_4 &= a^x - k_2 \cdot l_2^{v_x} - l_2^{p_x}\\
poly_5 &= a^y - k_2 \cdot l_2^{v_y} - l_2^{p_y}\\
poly_6 &= a^z - k_2 \cdot l_2^{v_z} - l_2^{p_z}
\end{aligned}$$

Објашњење: Како тачка A припада обема правама l_1 (која је дата тачком point $\overrightarrow{l_1^p}$ и вектором $\overrightarrow{l_1^v}$) и l_2 (дата тачком $\overrightarrow{l_2^p}$ и вектором $\overrightarrow{l_2^v}$), онда тачка A мора да задовољи њихове параметарске једначине, односно, мора да важи $\overrightarrow{A} = \overrightarrow{l_1^p} + k_1 \cdot \overrightarrow{l_1^v}$ и $\overrightarrow{A} = \overrightarrow{l_2^p} + k_2 \cdot \overrightarrow{l_2^v}$.

Оно што је важно је да ови полиноми користе две нове променљиве k_1 и k_2 које редом представљају размере правих l_1 и l_2. То значи да је укупан број нових променљивих пет, а постоји шест полинома које ова релација генерише. Ако су свих шест полинома укључени у скуп полинома, онда није могуће одредити еквивалентни троугаони систем јер има више полинома него непознатих променљивих. Довољно је пет полинома да би се одредило решење система, односно вредности свих параметара, а преостали, шести полином је у функцији оправдавања решења. Односно, уколико су тачке мимоилазне, за израчунате вредности шести полином неће бити једнак нули, иако су остали полиноми једнаки нули. Било који од задатих шест полинома може бити искључен из система, али мора бити проверен коришћењем доказивача да ли је и он нула (ако није, онда тврђење у општем случају не важи).

Ипак, у зависности од систем, треба бити пажљив приликом избора који полином избацити из скупа полинома. На пример, нека је $(1, 1, 0)$ вектор праве l_1, а тачка која јој припада је $(0, 0, 0)$ и нека је $(0, 0, 1)$ вектор праве l_2, а права садржи тачку $(1, 1, 1)$. Тада, систем добијених полинома је:

$$
\begin{aligned}
\textit{Polynomials: } poly_1 &= a^x - k_1\\
poly_2 &= a^y - k_1\\
poly_3 &= a^z\\
poly_4 &= a^x - 1\\
poly_5 &= a^y - 1\\
poly_6 &= a^z - k_2 - 1
\end{aligned}
$$

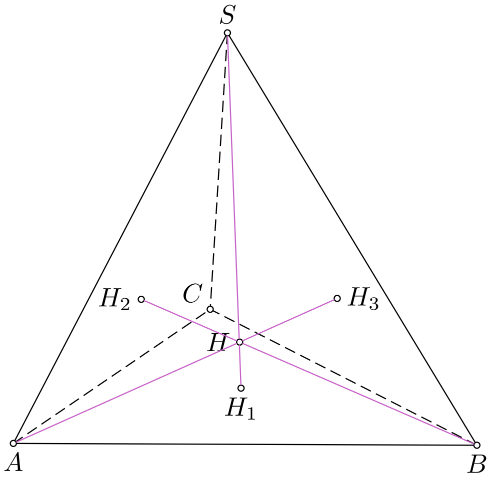
Као што се може приметити, једини полином који има промењљиву k_2 је последњи полином. Зато, последњи полином се не сме избацити из скупа полинома, а могуће решење је избацити полином $poly_5$. Иако се све сличне специфичне ситуације могу лако детектовати, имплементација избора који полином избацити, а које полиноме задржати је прилично незгодна јер је потребно много *if–else* испитивања.

Сличан проблем је и код релације `intersection_4points` $M\ A\ B\ C\ D$ и на истоветан начин се и овај проблем решава.

Експерименти

У овом поглављу ћемо представити резултате тестирања алгебраизације коришћењем система *GeoProver* и Гребнерових база имплементираних у систему *Mathematica*. Применили смо методе на двадесет и пет проблема из збирке задатака „?” [], на три задатка из „Збирке задатака из геометрије” [10] и на проблем једнакости углова представљен у раду о примени аутоматских доказивача на проблеме са Олимпијада из математике [13].

Пример нормала тетраедра. *Нека је $ABCS$ тетраедар и нека су h_a, h_b, h_c и h_s редом висине из темена тетраедра A, B, C и S на одговарајуће* *наспрамне странице и нека је H пресек h_a и h_b. Тада H припада и висинама h_s и h_c.*



Тврђење се може записати на следећи начин:

`make_tetrahedron` A B C S

`plane_points` α_1 A B C
`plane_points` α_2 B C S
`plane_points` α_3 A C S
`plane_points` α_4 A B S

`line_orth_plane` h_1 α_1 S
`line_orth_plane` h_2 α_2 A
`line_orth_plane` h_3 α_3 B
`line_orth_plane` h_4 α_4 C

`intersection_lines` H_1 h_1 h_2
`intersection_lines` H_2 h_2 h_3
`intersection_lines` H_3 h_2 h_4

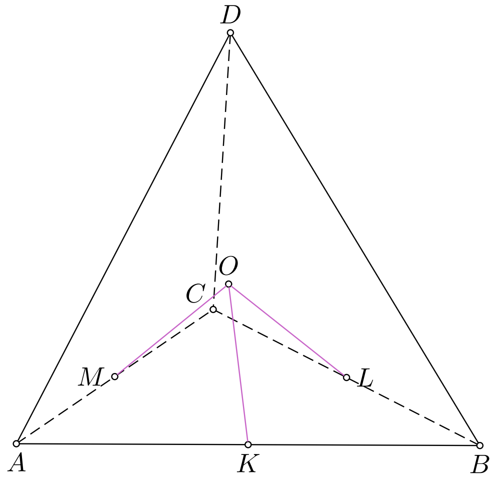
`equal_points` H_1 H_2
`equal_points` H_1 H_3

Како је тетраедар у канонском положају према самој конструкцији, координате тачака су $A(0,0,0)$, $B(0,0,1)$, $C(x_1,x_2,0)$ и $S(x_3,x_4,x_5)$ при чему су x_1, x_2, x_3, x_4 и x_5 зависне променљиве и налазе се у полиномима који описују тетраедар (погледати у ранијем поглављу полиноме за тетраедар 1.4).

Када се изврши алгебраизација коришћењем другог приступа, добија се 38 полинома који описују релације међу објектима, 6 полинома за које треба показати да су једнаки нули (односно ти полиноми су полиноми који изражавају својство да се висине секу у једној тачки) и 41 променљива. Потом иде поступак симплификације и анализе добијених полинома. Број полинома који описују релације се смањи на 29, а и број променљивих се смањи на 29. Број полинома за које треба показати да су нула је 9. Може бити чудно да се број полинома за које треба показати да су нула увећао, али то увећање се добија због пресека правих. Наиме, тачке H_1, H_2 и H_3 (за које треба показати да су једна иста тачка) се добијају као пресек правих, односно одговарајућих висина. Како за пресек правих треба показати да оне нису мимоилазне, већ да се заиста и секу, за један или више полинома пресека је потребно показати да они под датим условима су такође нула. О овом проблему је говорено раније 1.4. Полиноми добијени након симплификације су знантно краћи и најчеће се састоје од само два монома (у почетном скупу су били знатно комплекснији и у просеку су се састојали од 7 монома). Оба алгебарска доказивача (*GeoProver* и метод Гребнерових база имплементираних у систему *Mathematica*) су били успешни у показивању да су свих девет полинома једнаки нули. Просечно време потребно за доказ у систему *GeoProver* је 0.0862 секунде.

Када се изврши алгебраизација коришћењем првог приступа, добија се 34 полинома који описују релације међу објектима, 6 полинома за које треба показати да су једнаки нули и 33 променљиве. Након симплификације добија се 22 полинома који описују релације међу објектима, 9 полинома за које треба показати да су једнаки нули (исти разлог као и у другом приступу) и 25 различитих променљивих. Полиноми су за нијансу комплекснији него у првом приступу и у просеку имају 4 монома. Оба алгебарска доказивача (*GeoProver* и метод Гребнерових база имплементираних у систему *Mathematica*) су били успешни у показивању да су свих девет полинома једнаки нули. Просечно време потребно за доказ у систему *GeoProver* је 0.1132 секунде.

Пример једнаки углови. *Нека је $ABCD$ тетраедар и нека је тачка O центар описаног круга тетраедра $ABCD$. Нека су тачке K, L и M редом средине страница AB, BC и CA. Показати да је $\angle KOL = \angle LOM = \angle MOK$.*



Тврђење се може записати на следећи начин:

`make_tetrahedron` $A\ B\ C\ D$

`line_orth_plane_4points` $l_1\ A\ B\ C\ D$
`line_orth_plane_4points` $l_2\ A\ C\ D\ B$

`intersection_lines` $O\ l_1\ l_2$

`midpoint` $K\ A\ B$
`midpoint` $L\ B\ C$
`midpoint` $M\ C\ A$

`equal_angles` $K\ O\ L\ L\ O\ M$

Као и у претходном примеру тетраедар је у канонском положају према самој конструкцији, координате тачака су $A(0,0,0)$, $B(0,0,1)$, $C(x_1,x_2,0)$ и $S(x_3,x_4,x_5)$ при чему су x_1, x_2, x_3, x_4 и x_5 зависне променљиве и налазе се у полиномима који описују тетраедар (погледати у ранијем поглављу полиноме за тетраедар 1.4).

Коришћењем првог приступа добија се 31 полином који представља релације међу објектима, 1 полином за који је потребно показати да је једнак нули и 36 променљивих. Након симплификације, добија се 4 полинома за које треба показати да су једнаки нули (3 полинома сслуже као провера да ли се праве заиста секу, а један полином служи за проверу углова), 24 који описују релације међу објектима и 18 различитих променљивих. Међу добијеним полинома, 15 полинома је прилично једноставно и састоје се од два монома. Ипак, преостали полиноми су комплексни и састоје се у просеку од осам монома. Метод Гребнерових база имплементираних у систему *Mathematica*) су били успешни у показивању да су свих девет полинома једнаки нули. Систем *GeoProver* није био успешан и након 0.481 секунде пријавио је грешку да је досегао предвиђени меморијски лимит због полинома који има 3339 монома (енг. *Space limit exceeded in pseudo division. Obtained polynomial with 3339 terms*). Просечно време потребно за доказ да су полиноми који проверавају да ли има пресека једнаки нули је у систему *GeoProver* је 0.377 секунду.

Коришћењем другог приступа, број добијених полинома је 28 и један полином за који је потребно показати да је нула, број променљивих је 32. Након сређивања и анализе полинома пресека добија се 24 полинома и два полинома за које је потребно показати да су нула и 24 различите променљиве. У овом приступу 18 полинома је било једноставно и састојало се из два монома, док је преосталих 6 полинома комплексније и састоје се у просеку од 8 монома. Оба алгебарска доказивача (*GeoProver* и метод Гребнерових база имплементираних у систему *Mathematica*) су били успешни у показивању да су свих девет полинома једнаки нули. Време потребно за доказ да је полином који проверава да ли има пресека једнак нули је у систему *GeoProver* једнака 0.081 секунду, а време за доказ да је полином који проверава једнакост углова једнак нули у систему *GeoProver* је 0.835 секунде.

Оно што се може приметити након ова два једноставна примера је да први пруступ генерише мање променљивих, али да други приступ генерише једноставније полиноме. Како ће се показати даљим тестирањем, коришћеним алгебарским доказивачима више одговара када су полиноми једноставнији и зато су били успешнији када је коришћен други приступ.

Резултати методе Гребнерових база имплементираних у систему *Mathematica*. Метод Гребнерових база када је коришћен први приступ над 29 проблема је био успешан 23 пута и није доказао тврђења након 5 минута за 6 посматраних проблема.

Када је коришћен метод Гребнерових база али када је алгебризација рађена другим приступом, метод Гребнерових база је био успешан у свих 29 посматраних проблема.

Резултати система *GeoProver*. Систем *GeoProver* када је коришћен први приступ је био успешан само 13 пута. У различитим проблемима долазило је до различитих грешака због којих није успешно доказ завшен: достигнут је временски лимит (енг. *Time limit reached.*), достигнут је меморијски лимит (енг. *Space limit reached.*) или се догодила генерална грешка (енг. *General error occured.*). Последња грешка означава да доказивач није био у могућности да направи троугаони систем једначина. То, на даље значи да је потребно додатно истражити ову ситуацију и потенцијално изменити улазне полиноме да би се ова грешка избегла. Ипак, за сада нисмо у могућности да овакво понашење спречимо јер ако се током тријангулације појави полином $0 = 0$ доказивач ће пријавити грешку. У почетном систему је лако могуће регистровати да ли такав полином постоји, али није лако могуће одредити да ли ће се у процесу тријангулације такав полином створити јер је потребно испитати односе међу датим променљивима и задатим полиномима, што је доста комплексно питање.

Коришћењем другог приступа у алгебризацији, систем *GeoProver* је био нешто успешнији, од 29 посматраних проблема, систем је био успешан 22 пута. Грешке због којих није успео да заврши доказе су: времески лимит је досегнут или се догодила генерална грешка.

Закључак

Поступак алгебризације објеката и релација у стереометрији је могуће учинити на више начина и ми смо у овом раду представили два приступа.

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, __________________________

____