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

Формализација аналитичке геометрије

1.1 Увод

Синтетичка геометрија се обично изучава ригорозно, као пример ригорозног аксиоматског извођења. Са друге стране, аналитичка геометрија се углавном изучава неформално. Често се ова два приступа представљају независно и веза између њих се ретко показује. Овај рад покушава да премост и више празнина за које мислимо да тренутно постоје у формализацији геометрије.

1. Прво, наш циљ је да формализујемо аналитичку геометрију, тј. Декартову раван у оквиру интерактивног доказивача теорема, са ригорозним приступом, али веома блиско стандарном средњошколском образовању. Представићемо добро изграђену формализацију Декартове геометрије равни у оквиру система Isabelle/HOL.

2. Намеравамо да покажемо да су различите дефиниције основних појмова аналитичке геометрије које можемо видети у литератури заправо еквивалентне, и да заправо представљају јединствен апстрактни ентитет – Декартову раван. Дефиниције ћемо преузети из стандардних уџбеника.

3. Намеравамо да покажемо да стандарна геометрија координатне равни представља модел аксиоматског система Тарског. Наиме, показаћемо да Декартова координатна раван задовољава све аксиоме Тарског.

4. Показаћемо да Декартова координатна раван задовољава већину аксиома Хилберта.

5. Потом, намеравамо да анализирамо доказе и да упоредимо који од два система аксиома је лакши за формализацију.

Поред тога што су многе теореме формализоване и доказане у оквиру система Isabelle/HOL, ми такође дискутујемо и наше искуство у примени различитих техника за поједностављење доказа. Најзначајнија техника је „без губитка на општости” (“бгно”), која прати приступ Харисона [?], а формална оправданост овог приступа је постигнута коришћењем различитих изометријских трансформација.

1.2 Формализација геометрије Декартове равни

Када се формализује теорија, мора се одлучити који појмови ће бити основни, а који појмови ће бити дефинисани помоћу тих основних појмова. Циљ наше формализације аналитичке геометрије је да успостави везу са синтетичком геометријом, па зато има исте основне појмове који су дати у синтетичком приступу. Свака геометрија има класу објеката који се називају *тачке*. Неке геометрије (на пример, Хилбертова) има и додатни скуп објеката који се наизвају *праве*, док неке геометрије (на пример, геометрија Тарског) уопште не разматра праве. У неким геометријама, праве су дефинисани појам, и оне су дефинисане као скуп тачака. Ово подразумева рад са теоријом скупова, а многе аксиоматизације желе то да избегну. У нашој формализацији аналитичке геометрије, ми ћемо дефинисати и тачке и праве јер желимо да омогућимо анализу и геометрије Тарског и геометрије Хилберта. Основна релација која спаја тачке и праве је релације *инциденције*, која неформално означава да права садржи тачку (или дуално да се тачка налази на прави). Други примитивни појмови (у већини аксиоматских система) су релација *између* (која дефише редослед колинеарних тачака) и релација *конгруенције*.

Важно је напоменути да у аналитичкој геометрији многи појмови су често дати у облику дефиниција, а заправно ти појмови су изведени појмови у синтетичкој геометрији. На пример, у књигама за средњу школу дефише се да су праве нормалне ако је производ њихових праваца -1. Ипак, ово нарушава везу са синтетичком геометријом (где је нормалност изведени појам) јер би оваква карактеризација требало да буде доказана као теорема, а не узета као дефиниција.

Тачке у аналитичкој геометрији.

Тачка у реалној координатној равни је одређена са својим x и y координатама. Зато, тачке су парови реалних бројева ($\mathbb{R}^2$), што се може лако формализовати у Isabelle/HOL систему са **type_synonym** point^{ag} $=$ $"real \times real"$.

Редослед тачака.

Редослед (колинерних) тачака се дефинише коришћењем релације *између*. Ово је релација која има три аргумента, $\mathcal{B}(A, B, C)$ означава да су тачке A, B, и C колинеране и да је тачка B између тачака A и C. Ипак, неке аксиоматизације (на пример, аксиоматизација Тарског) дозвољава случај када је тачка B једнака тачки A или тачки C. Рећи ћемо да је релација између *инклузивна*, док неке друге аксиоматизације (на пример, Хилбертова аксиоматизација) не дозвољавају једнакост тачака и тада кажемо да је релација између *ексклузивна*. У првом случају, тачке A, B и C задовољавају релацију између ако постоји реалан број $0 \leq k \leq 1$ такав да $\overrightarrow{AB} = k \cdot \overrightarrow{AC}$. Желимо да избегенемо експлицитно коришћење вектора јер су они чешће изведени, а ређе примитиван појам у синтетичкој геометрији, тако да релацију између формализујемо у Isabelle/HOL систему на следећи начин:

definition "$\mathcal{B}_T^{ag}\ (xa, ya)\ (xb, yb)\ (xc, yc) \longleftrightarrow$
$(\exists (k :: real).\ 0 \leq k \ \wedge\ k \leq 1\ \wedge$
$(xb - xa) = k \cdot (xc - xa)\ \wedge\ (yb - ya) = k \cdot (yc - ya))$"

Ако захтевамо да тачке A, B и C буду различите, она мора да важи $0 < k < 1$, и релацију ћемо означавати са $\mathcal{B}_H^{ag}$.

Конгруенција.

Релација конгрунеције дефинише се на паровима тачака. Неформално, $AB \cong_t CD$ означава да је сегмент AB конгруентан сегменту CD. Стандардна метрика у $\mathbb{R}^2$ дефинише да растојање међу тачкама $A(x_A, y_A)$, $B(x_B, y_B)$ је $d(A, B) = \sqrt{(x_B - x_A)^2 + (y_B - y_A)^2}$. Квадратно растојање се дефинише као $d_{ag}^2\ A\ B = (x_B - x_A)^2 + (y_B - y_A)^2$. Тачке A и B су конгруентне тачкама C и D ако и само ако $d_{ag}^2\ A\ B = d_{ag}^2\ C\ D$. У Isabelle/HOL систему ово се може формализовати на следећи начин:

definition "$d_{ag}^2\ (x_1, y_1)\ (x_2, y_2) = (x_2 - x_1) \cdot (x_2 - x_1) + (y_2 - y_1) \cdot (y_2 - y_1)$"
definition "$A_1 B_1 \cong^{ag} A_2 B_2 \longleftrightarrow d_{ag}^2\ A_1\ B_1 = d_{ag}^2\ A_2\ B_2$"

Права и инциденција.

Једначина праве. Праве у Декартовој координатној равни се обично представљају једначинама облика $Ax + By + C = 0$, па тако тројка $(A, B, C) \in \mathbb{R}^3$ означава праву. Ипак, тројке у којима је $A = 0$ и $B = 0$ морају бити изузете јер не представљају исправну једначину праве. Такође, једначине $Ax+By+C = 0$ и $kAx + kBy + kC = 0$, за реално $k \neq 0$, означавају исту праву. Зато права не може бити дефинисана коришћењем само једне једначине, већ права мора бити дефинисана као класа једначина које имају пропорционалне коефициенте. Формализација у систему Isabelle/HOL се састоји из неколико корака. Прво, дефинише се домен валидних тројки који су коефициенти једначине.

typedef line_coeffs^{ag} =
"$\{((A :: real), (B :: real), (C :: real)).\ A \neq 0 \vee B \neq 0\}$"

Када је овај тип дефинисан, функција Rep_line_coeffs ($\lfloor\_\rfloor_{R3}$) конвертује апстрактне вредности овог типа у њихове конкретне репрезентације (тројке реалних бројева), а функција Abs_line_coeffs ($\lceil\_\rceil^{R3}$) конвертује (валидне) тројке у вредности које припадају овом типу.

Две тројке су еквиваленте ако и само ако су пропорционалне.

definition "$l_1 \approx^{ag} l_2 \longleftrightarrow$
$(\exists\ A_1\, B_1\, C_1\, A_2\, B_2\, C_2.$
$\lfloor l_1\rfloor_{R3} = (A_1, B_1, C_1))\ \wedge\ \lfloor l_2\rfloor_{R3} = (A_2, B_2, C_2)\ \wedge$
$(\exists k.\ k \neq 0\ \wedge\ A_2 = k \cdot A_1\ \wedge\ B_2 = k \cdot B_1\ \wedge\ C_2 = k \cdot C_1))$"

Потом је показано да је ово релација еквиваленције. Дефиниција за тип праве користи подршку за количничке типове и количничке дефиниције. Значи права (тип line^{ag}) се дефинише коришћењем quotient_type команде као класа еквиваленције над релацијом $\approx^{ag}$.

Да би избегли коришћење теорије скупова, геометријске аксиоматизације које експлицитно разматрају праве користе релацију инциденције. Ако се користи претходна дефиниција за праву, онда проверавање инциденције се своди на израчунавање да ли тачка (x, y) задовољава једначину праве $A \cdot x + B \cdot y + C = 0$, за неке коефицијенте A, B, и C који су представници класе.

definition "ag_in_h $(x, y)\ l \longleftrightarrow$
$(\exists\ A\ B\ C.\ \lfloor l \rfloor_{R3} = (A,\ B,\ C) \wedge (A \cdot x + B \cdot y + C = 0))$"

Ипак, да би показали да је релација заснована на представницима класе добро заснована, мора бити показано да ако се изаберу други представници класе, рецимо A', B', и C' (који су пропорционални са A, B, и C), онда $A' \cdot x + B' \cdot y + C = 0$. Зато, у нашој Isabelle/HOL формализацији, ми користимо пакет који подржава рад са количничким типовима (quotient package). Онда $A \in_H^{ag} l$ се дефинише коришћењем **quotient_definition** која се заснива на релацији ag_in_h. Лема добре дефинисаности је

lemma
shows "$l \approx l' \Longrightarrow$ ag_in_h $P\ l =$ ag_in_h $P\ l'$"

Афина дефиниција. У афиној геометрији, права се дефинише помоћу фиксне тачке и вектора. Као и тачка, вектор такође може бити записан као пар реалних бројева на следећи начин: **type_synonym** vec^{ag} = $''real \times real''$. Вектори дефинисани на овај начин чине векторски простор (са природно дефинисаним векторским збиром и скаларним производом). Тачке и вектори се могу сабирати као $(x, y) + (v_x, v_y) = (x + v_x, y + v_y)$. Зато, права се записује као тачка и вектор који је различит од нуле:

typedef line_point_vec^{ag} ="$(p ::\mathrm{point}^{ag}, v ::\mathrm{vec}^{ag}).\ v \neq (0, 0)\}$"

Ипак, различите тачке и вектори могу заправо одређивати једну те исту праву, па конструкција са количничким типом опет мора бити коришћена.

definition "$l_1 \approx^{ag} l_2 \longleftrightarrow (\exists\, p_1\, v_1\, p_2\, v_2.$
$\lfloor l_1 \rfloor_{R3} = (p_1, v_1) \wedge \lfloor l_2 \rfloor_{R3} = (p_2, v_2) \wedge$
$(\exists km.\ v_1 = k \cdot v_2 \wedge p_2 = p_1 + m \cdot v_1))$"

Показује се да је ово заиста релација еквиваленције. Онда се тип праве (line^{ag}) дефинише коришћењем команде quotient_type, као класа еквиваленције над релацијом $\approx^{ag}$.

У овом случају, након што се покаже добра дефинисаност, инциденција се дефинише на начин који можете видети у наставку (поново се уопштава подизање на виши ниво) коришћењем количничког пакета.

definiton "ag_in_h $p\, l \longleftrightarrow (\exists\, p_0\, v_0.\ \lfloor l \rfloor_{R3} = (p_0, v_0) \wedge (\exists k.\ p = p_0 + k \cdot v_0))$"

Још једна могућа дефиниција праве је класа еквиваленције парова различитих тачака. Ми нисмо формализовали овај приступ јер је тривиално изоморфан са афином дефиницијом (разлика тачака је вектор који се појављује у афиној дефиницији).

Изометрије

У синтетичкој геометрији изометрије се уводе коришћењем дефиниције. Рефлексије могу прве да се дефинишу, а онда се друге изометрије могу дефинисати као композиција рефлексија. Ипак, у нашој формализацији, изометрије се користе само као помоћно средство да упросте наше доказе (што ће бити додатно појашњено у одељку 1.3). Зато ми нисмо били заинтересовани да дефинишемо изометрије као примитивне појмове (као што су тачке и конгруенција) него смо представили аналитичке дефиниције и доказали својства која су потребна за касније доказе.

Транслација је дефинисана преко датог вектора (који није експлицитно дефининсан, већ је представљен као пар реалних бројева). Формална дефиниција у Isabelle/HOL систему је једноставна.

definiton "transp^{ag} $(v_1, v_2)\ (x_1, x_2) = (v_1 + x_1, v_2 + x_2)$"

Ротација је параметризована за реални параметар α (који представља угао ротације), а ми само посматрамо ротације око координатног почетка (остале ротације могу се добити као композиција транслације и ротације око координатног почетка). Користимо основна правила тригонометрије да би добили следећу формалну дефиницију у систему Isabelle/HOL.

definition "$\mathtt{rotp}^{ag}\ \ \alpha\ \ (x, y) = ((\cos\alpha)\cdot x - (\sin\alpha)\cdot y, (\sin\alpha)\cdot x + (\cos\alpha)\cdot y)$"

Такође, централна симетрија се лако дефинише коришћењем координата тачаке:

definiton "$\mathtt{symp}^{ag}\ \ (x, y)\ \ = (-x, -y)$"

Важна особина свих изометрија је својство инваријантности, тј. оне чувају основне релације (као што су између и конгруенција).

lemma "$\mathcal{B}_T^{ag}\ \ A\ \ B\ \ C \longleftrightarrow \mathcal{B}_T^{ag}\ \ (\mathtt{transp}^{ag}\ \ v\ \ A)\ \ (\mathtt{transp}^{ag}\ \ v\ \ B)\ \ (\mathtt{transp}^{ag}\ \ v\ \ C)$"
lemma "$AB \cong^{ag} CD \longleftrightarrow$
$(\mathtt{transp}^{ag}\ \ v\ \ A)(\mathtt{transp}^{ag}\ \ v\ \ B) \cong^{ag} (\mathtt{transp}^{ag}\ \ v\ \ C)(\mathtt{transp}^{ag}\ \ v\ \ D)$"
lemma "$\mathcal{B}_T^{ag}\ \ A\ \ B\ \ C \longleftrightarrow \mathcal{B}_T^{ag}\ \ (\mathtt{rotp}^{ag}\ \ \alpha\ \ A)\ \ (\mathtt{rotp}^{ag}\ \ \alpha\ \ B)\ \ (\mathtt{rotp}^{ag}\ \ \alpha\ \ C)$"
lemma "$AB \cong^{ag} CD \longleftrightarrow$
$(\mathtt{rotp}^{ag}\ \ \alpha\ \ A)(\mathtt{rotp}^{ag}\ \ \alpha\ \ B) \cong^{ag} (\mathtt{rotp}^{ag}\ \ \alpha\ \ C)(\mathtt{rotp}^{ag}\ \ \alpha\ \ D)$"
lemma "$\mathcal{B}_T^{ag}\ \ A\ \ B\ \ C \longleftrightarrow \mathcal{B}_T^{ag}\ \ (\mathtt{symp}^{ag}\ \ A\ )\ \ (\mathtt{symp}^{ag}\ \ B\ )\ \ (\mathtt{symp}^{ag}\ \ C\ )$"
lemma "$AB \cong^{ag} CD \longleftrightarrow (\mathtt{symp}^{ag}\ \ A\ )(\mathtt{symp}^{ag}\ \ B\ ) \cong^{ag} (\mathtt{symp}^{ag}\ \ C\ )(\mathtt{symp}^{ag}\ \ D\ )$"

Изометрије се пре свега користе да трансформишу тачку у њену канонску позицију (обично померањем на y-осу). Следеће леме показује да је то могуће учинити.

lemma "$\exists v.\ \mathtt{transp}^{ag}\ \ v\ \ P = (0, 0)$"
lemma "$\exists \alpha.\ \mathtt{rotp}^{ag}\ \ \alpha\ \ P = (0, p)$"
lemma "$\mathcal{B}_T^{ag}\ \ (0, 0)\ \ P_1\ \ P_2 \longrightarrow$
$\exists \alpha\ \ p_1\ \ p_2.\ \mathtt{rotp}^{ag}\ \ \alpha\ \ P_1 = (0, p_1)\ \wedge\ \mathtt{rotp}^{ag}\ \ \alpha\ \ P_2 = (0, p_2)$"

Изометријске трансформације праве се дефинишу коришћењем изометријских трансформација над тачкама (права се трансформише тако што се трансформишу две њене произвољне тачке).

1.3 Коришћење изометријских трансформација

Једна од најважнијих техника која је коришћења за упрошћавање формализације ослањала се на коришћење изометријских трансформација. Ми ћемо покушати да представимо мотивациони разлог за примену изометрија на следећем, једноставном примеру.

Циљ је да покажемо да у нашем моделу, ако $\mathcal{B}_T^{ag}\ A\ X\ B$ и $\mathcal{B}_T^{ag}\ A\ B\ Y$ онда важи $\mathcal{B}_T^{ag}\ X\ B\ Y$. Чак и на овом једноставном примеру, ако применимо директан доказ, без коришћења изометријских трансформација, алгебарски рачун постаје превише комплексан.

Нека важи $A = (x_A, y_A)$, $B = (x_B, y_B)$, и $X = (x_X, y_X)$. Како $\mathcal{B}_T^{ag}\ A\ X\ B$ важи, постоји реалан број k_1, $0 \leq k_1 \leq 1$, такав да $(x_X - x_A) = k_1 \cdot (x_B - x_A)$, и $(y_X - y_A) = k_1 \cdot (y_B - y_A)$. Слично, како $\mathcal{B}_T^{ag}\ A\ B\ Y$ важи, постоји реалан број k_2, $0 \leq k_2 \leq 1$, такав да $(x_B - x_A) = k_2 \cdot (x_Y - x_A)$, и $(y_B - y_A) = k_2 \cdot (y_Y - y_A)$. Онда, може се дефинисати реалан број k са $(k_2 - k_2 \cdot k_1)/(1 - k_2 \cdot k_1)$. Ако $X \neq B$, онда коришћењем комплексних алгебарских трансформација, може се показати да $0 \leq k \leq 1$, и да $(x_B - x_X) = k \cdot (x_Y - x_X)$, и $(y_B - y_X) = k \cdot (y_Y - y_X)$, и зато $\mathcal{B}_T^{ag}\ X\ B\ Y$ важи. Дегенерисани случај $X = B$ тривијално важи.

Ипак, ако применимо изометријске трансформације, онда можемо предспоставити да $A = (0, 0)$, $B = (0, y_B)$, и $X = (0, y_X)$, и да $0 \leq y_X \leq y_B$. Случај када је $y_B = 0$ тривијално важи. У супротном, $x_Y = 0$ и $0 \leq y_B \leq y_Y$. Зато, $y_X \leq y_B \leq y_Y$, и тврђење важи. Приметимо да у овом случају нису биле потребне велике алгебарске трансформације и доказ се ослања на једноставне особине транзитивности релације $\leq$.

Поредећи претходна два доказа, можемо да видимо како примена изометријских трансформација значајно упрошћава потребна израчунавања и скраћује доказе.

Како је ова техника доста коришћена у нашој формализацији, важно је продискутовати који је најбољи начин да се формулишу одговарајуће леме које оправдавају употребу ове технике и покушати што више аутоматизовати коришћење ове технике. Ми смо применили приступ који је предложио Харисон [?].

Својство P је инваријантно под трансформацијом t акко на њега не утиче трансформација тачака на коју је примењена трансформација t.

definiton "inv $P\ t \longleftrightarrow (\forall\ A\ B\ C.\ P\ A\ B\ C \longleftrightarrow P\ (tA)\ (tB)\ (tC))$"

Тада, следећа лема се може користити да сведемо тврђење које важи за било које тачке које су колинеарне на тврђење за које разматрамо само тачке на y-оси (можемо изабрати и x-осу уколико нам тако више одговара).

lemma
  assumes "$\forall\ y_B\ y_C.\ 0 \leq y_B\ \wedge\ y_B \leq y_C \longrightarrow P\ (0,0)\ (0,y_B)\ (0,y_C)$"
  "$\forall v.$ inv P (transp^{ag} v)" "$\forall \alpha.$ inv P (rotp^{ag} α)"
  "inv P (symp^{ag})"
  shows "$\forall A\, B\, C.\ \mathcal{B}_T^{ag}\ A\ B\ C \longrightarrow\ P\ A\ B\ C$"

Доказ да је неко тврђење инваријантно у односу на изометријску трансформацију највише се ослања на леме које показују да су релација између и релација конгруенције инваријантне у односу на изометријске трансформације.

1.4 Модел аксиоматског система Тарског

Наш циљ у овом поглављу је да докажемо да наше дефиниције Декартове координатне равни задовољавају све аксиоме геометрије Тарског[?]. Основни појмови у геометрији Тарског су само три појма - тачке, (инклузивна) релација између (означена са $\mathcal{B}_t(A, B, C)$) и релација конгруенције (коју означавамо са $AB \cong_t CD$). У геометрији Тарског праве нису експлицитно дефинисане и колинеарност се дефинише коришћењем релације између

definition "$\mathcal{C}_t(A, B, C) \longleftrightarrow \mathcal{B}_t(A, B, C) \vee \mathcal{B}_t(B, C, A) \vee \mathcal{B}_t(C, A, B)$"

Аксиоме конгруенције.

Прве три аксиоме Тарског представљају основна својства конгруенције.

lemma „$AB \cong_t BA$"
lemma „$AB \cong_t CC \longrightarrow\ A = B$"
lemma „$AB \cong_t CD \wedge\ AB \cong_t EF\ \longrightarrow CD \cong_t EF$"

Желимо да докажемо да наша релација $\cong^{ag}$ задовољава својства релације $\cong_t$ која је апстрактно задана са претходним аксиомама (тј. да дате аксиоме важе у нашем моделу Декартове координатне равни). У нашој формализацији, аксиоме геометрије Тарског су формулисане коришћењем локала (`locale` [?], и показано је да координатна раван представља интерпретацију тог дефинисаног локала. Како је ово техничка страна формализације у Isabelle/HOL систему, ми је нећемо овде дискутовати у више детаља (погледати одељак ??). На пример, за прву аксиому, доказ се своди на показивање тврђења $AB \cong^{ag} BA$. Докази су праволинијски и готово аутоматски (поједностављивањем након развијања дефиниција).

Аксиоме распореда.

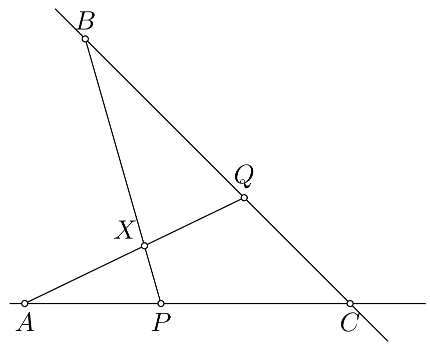
Идентитет у релацији између. Прва аксиома (инклузивне) релације између даје једно њено једноставно својство и, за наш модел, доказује се готово аутоматски.

`lemma` "$\mathcal{B}_t(A, B, A) \longrightarrow A = B$"

Пашова аксиома. Следећа аксиома је Пашова аксиома:

`lemma` "$\mathcal{B}_t(A, P, C) \wedge \mathcal{B}_t(B, Q, C) \longrightarrow (\exists X.\ (\mathcal{B}_t(P, X, B) \wedge \mathcal{B}_t(Q, X, A)))$"

Под претпоставком да су све тачке које се помињу у аксиоми различите и да нису све тачке колинеарне, слика која одговара аксиоми је:



Пре него што дамо доказ да у нашем моделу Декартове координатне равни важи ова аксиома, желимо да продискутујемо нека питања која се односе на геометрију Тарског и која су се показала важа за свеукупну организацију нашег доказа. Последња верзија аксиоматског система Тарског је направљена да буде минимална (садржи само 11 аксиома), и централне аксиоме које описују релацију између су идентитет релације између и Пашова аксиома. У формализацији геометрије Тарског ([?]) сва остала елементарна својства ове релације се изводе из ове две аксиоме. На пример, да би се извела симетричност релације између (и.е., $\mathcal{B}_t(A, B, C) \longrightarrow \mathcal{B}_t(C, B, A)$), Пашова аксиома се примењује на тројке ABC и BCC и тада се добија тачка X тако да важи $\mathcal{B}_t(C, X, A)$ и $\mathcal{B}_t(B, X, B)$, и онда према првој аксиоми, $X = B$ и $\mathcal{B}_t(C, B, A)$. Ипак, према нашем искуству, у намери да покажемо да је наша Декартова координатна раван је модел аксиома Тарског (поготово за Пашову аксиому), потребно је да већ имамо показане неке њене последице (као што су симетричност и транзитивност). Још да додамо, да су раније варијанте аксиоматског система Тарског имале више аксиома, а ова својства су управо била нека од тих додатних аксиома. Такође, својство симетрије је једноставније својство него Пашова аксиома (на пример, оно укључује само тачке које леже на прави, док у аксиоми Паша имамо тачке које леже у равни и не морају бити колинеране). Додатно, претходни доказ користи веома супстилна својства која зависе од тога како је Пашова аксиома формулисана. На пример, ако се у њеном закључку користи $\mathcal{B}_t(B, X, P)$ и $\mathcal{B}_t(A, X, Q)$ уместо $\mathcal{B}_t(P, X, B)$ и $\mathcal{B}_t(Q, X, A)$, онда доказ не може да се изведе. Зато, ми смо одлучили да би добар приступ био да директно покажемо да нека елементарна својства (као што су симетрија и транзитивност) релације између важе у моделу, а онда да користимо ове чињенице у доказу много комплексније Пашове аксиоме.

lemma "$\mathcal{B}_T^{ag}\ A\ A\ B$"
lemma "$\mathcal{B}_T^{ag}\ A\ B\ C \longrightarrow \mathcal{B}_T^{ag}\ C\ B\ A$"
lemma "$\mathcal{B}_T^{ag}\ A\ X\ B\ \wedge\ \mathcal{B}_T^{ag}\ A\ B\ Y \longrightarrow \mathcal{B}_T^{ag}\ X\ B\ Y$"
lemma "$\mathcal{B}_T^{ag}\ A\ X\ B\ \wedge\ \mathcal{B}_T^{ag}\ A\ B\ Y \longrightarrow \mathcal{B}_T^{ag}\ A\ X\ Y$"

Пре него што наставимо са доказом да наша Декартова координатна раван у потпуности задовољава Пашову аксиому, потребно је анализирати неколико дегенерисани случајева. Прва група дегенерисаних случајева настаје када су неке од тачака у конструкцији једнаке. На пример, $\mathcal{B}_t(A, P, C)$ дозвољава да $A = P = C$, или $A = P \neq C$, или $A \neq P = C$ или $A \neq P \neq C$. Директан приступ би био да се сваки од ових случајева посебно анализира. Међутим, бољи приступ је да се пажљиво анализира претпоставка и да се одреди који од случајева су суштински различити. Испоставља се да су само два различита случаја битна. Ако је $P = C$, онда је Q тражена тачка. Ако је $Q = C$, онда је P тражена тачка. Следећа група дегенерисаних случајева настаје када су све тачке колинеарне. У овом случају важи, или $\mathcal{B}_t(A, B, C)$ или $\mathcal{B}_t(B, A, C)$ или $\mathcal{B}_t(B, C, A)$. У првом случају B је тражена тачка, у другом случају A је тражена тачка, а у трећем случају P је тражена тачка.

Приметимо да сви дегенерисани случајеви Пашове аксиоме се директно доказују коришћењем елементарних својстава и да у овим случајевима није било потребно користити координатна израчунавања. Ово сугерише да су дегенерисани случајеви Пашове аксиоме еквивалентни коњукцији датих својстава. Додатно, ово сугерише да ако се промени аксиоматизација Тарског тако да укључује ова елементарна својства, онда се Пашова аксиома може ослабити тако да садржи само централни случај неколинеарних, различитих тачака.

Коначно, остаје да се покаже централни случај. У том случају, коришћене су алгебарске трансформације да се израчунају координате тачке X и да се покаже претпоставка. Да би се упростио доказ, коришћене су изометрије, као што је описано у одељку 1.3. Почетна конфигурација је трансформисана тако да A постаје координатни почетак, односно $(0, 0)$, да $P = (0, y_P)$ и $C = (0, y_C)$ леже на позитивном делу y-осе. Нека је $B = (x_B, y_B)$, $Q = (x_Q, y_Q)$ и $X = (x_X, y_X)$. Како $\mathcal{B}_t(A, P, C)$ важи, постоји реалан број k_3, $0 \leq k_3 \leq 1$, такав да $y_P = k_3 \cdot y_C$. Слично, како $\mathcal{B}_t(B, Q, C)$ важи, постоји реалан број k_4, $0 \leq k_4 \leq 1$, такав да $(x_B - x_A) = k_2 \cdot (x_Y - x_A)$, и $x_Q - x_B = -k_4 * x_B$ и $y_Q - y_B = k_4 * (y_C - y_B)$. Онда, можемо дефинисати реалан број $k_1 = \frac{k_3 \cdot (1-k_4)}{k_4 + k_3 - k_3 \cdot k_4}$. Како за A, P и C важи $A \neq P \neq C$ и тачке нису колинеарне (јер посматрамо само централни, недегенерисани случај), онда, коришћењем директних алгебарских израчунавања, може бити показано да $0 \leq k_1 \leq 1$, и да $x_X = k_1 \cdot x_B$, и $y_X - y_P = k_1 \cdot (y_B - y_P)$, и зато $\mathcal{B}_t(P, X, B)$ важи. Слично, можемо дефинисати реалан број $k_2 = \frac{k_4 \cdot (1-k_3)}{k_4 + k_3 - k_3 \cdot k_4}$ и показати да $0 \leq k_2 \leq 1$ и да важи следеће: $x_X - x_Q = -k_2 \cdot x_Q$ и $y_X - y_Q = -k_2 \cdot y_Q$ и према томе $\mathcal{B}_t(Q, X, A)$ важи. Из ова два закључка ми смо одредили тачку X.

Аксиома ниже димензије. Следећа аксиома каже да постоје 3 неколинеарне тачке. Зато сваки модел ових аксиома мора имати димензију већу од 1.

`lemma` "$\exists\ A\ B\ C.\ \neg\ \mathcal{C}_t(A, B, C)$"

У нашој Декартовој равни тривијално важи (нпр. $(0, 0)$, $(0, 1)$, и $(1, 0)$ су неколинеране).

Аксиома (схема) континуитета. Аксиома континуитета Тарског је у ствари конструкција Дедекиндовог пресека. Интуитивно, ако су све тачке скупа тачака са једне стране у односу на тачаке које припадају другом скупу тачака, онда постоји тачка која је између та два скупа. Оргинална Тарски аксиоматизација је дефинисана у оквиру логике првог реда и скупови нису екплицитно познати у оквиру формализације Тарског. Зато, уместо да користи скупове тачака, Тарски користи предикате логике првог реда, ϕ и ψ.

$$(\exists a.\ \forall x.\ \forall y.\ \phi\ x \wedge \psi\ y \longrightarrow \mathcal{B}_t(a, x, y)) \longrightarrow (\exists b.\ \forall x.\ \forall y.\ \phi\ x \wedge \psi\ y \longrightarrow \mathcal{B}_t(x, b, y))$$

Ипак, формулација ове леме у оквиру логике вишег реда система Isabelle/HOL не ограничава предикате ϕ и ψ да буду предикати логике првог реда. Зато, строго гледано, наша формализација аксиоматског система Тарског у оквиру система Isabelle/HOL даје другачију геометрију у односу на оргиналну геометрију Тарског.

lemma
  assumes "$\exists a.\ \forall x.\ \forall y.\ \phi\ \ x \wedge \psi\ \ y \longrightarrow \mathcal{B}_T^{ag}\ \ a\ \ x\ \ y$"
  shows "$\exists b.\ \forall x.\ \forall y.\ \phi\ \ x \wedge \psi\ \ y \longrightarrow \mathcal{B}_T^{ag}\ \ x\ \ b\ \ y$"

Међутим, испоставља се да је могуће показати да Декартова координатна раван такође задовољава строжију варијанту аксиоме (без ограничавања да предикати ϕ и ψ су предикати логике првог реда). Ако је један скуп празан, тврђење тривијално важи. Ако скупови имају заједничку тачку, онда је та тачка уједно и тражена тачка. У другим случајевим, примењујемо изометријске трансформације тако да све тачке из оба скупа леже на позитивном делу y-осе. Онда, доказ тврђења се своди на доказивање следећег:

lemma
  assumes
  "$P = \{x.\ \ x \geq 0 \wedge \phi(0, x)\}$" "$Q = \{y.\ \ y \geq 0 \wedge \psi(0, y)\}$"
  "$\neg(\exists b.\ \ b \in P \wedge b \in Q)$" "$\exists x_0.\ \ x_0 \in P$" "$\exists y_0.\ \ y_0 \in Q$"
  "$\forall x \in P.\ \ \forall y \in Q.\ \ \mathcal{B}_T^{ag}\ \ (0, 0)\ \ (0, x)\ \ (0, y)$"
  shows
  "$\exists b.\ \ \forall x \in P.\ \ \forall y \in Q.\ \ \mathcal{B}_T^{ag}\ \ (0, x)\ \ (0, b)\ \ (0, y)$"

Доказивање овога захтева коришћење нетривијалних особина реалних бројева, пре свега, њихову потпуност. Потпуност реалних бројева у систему Isabelle/HOL је формализована следећом теоремом (супремум, особина најмање горње границе):

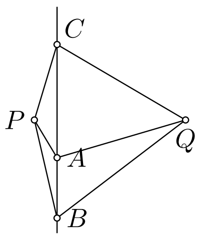
lemma "$(\exists x.\ x \in P) \wedge (\exists y.\ \forall x \in P.\ x < y) \longrightarrow$
$\exists S.\ (\forall y.\ (\exists x \in P.\ y < x) \leftrightarrow y < S)$"

Скуп P задовољава својство супремума. Заиста, како, по претпоставци, P и Q немају заједнички елемент, а из претпоставке следи да $\forall x \in P. \forall y \in Q. x < y$, тако да је било који елемент из Q горња граница за P. По претпоставци, P и Q су непразни, тако да постоји елемент b такав да $\forall x \in P.\ x \leq b$ и $\forall y \in Q.\ b \leq y$, тако да теорема важи.

Аксиоме подударности и распореда.

Аксиома горње димензије. Три тачке које су на истом одстојању од две различите тачке леже на истој прави. Зато, сваки модел ових аксиома мора имати димензију мању од 3.

lemma "$AP \cong_t AQ\ \wedge\ BP \cong_t BQ\ \wedge\ CP \cong_t CQ\ \wedge\ P \neq Q\ \ \longrightarrow \mathcal{C}_t(A, B, C)$"



Ово тврђење је било лако показати анализом различитих случајева и коришћењем алгебарских трансформација. Није било потребно користити изометријске трансформације.

Аксиома конструкције сегмента.

lemma "$\exists E.\ \mathcal{B}_t(A, B, E)\ \ \wedge\ \ BE \cong_t CD$"

Доказ да наш модел Декартове координатне равни задовољава ову аксиму је једноставан и почиње трансформацијом тачака тако да тачка A постаје координатни почетак, а тачка B лежи на позитивном делу y-осе. Онда $A = (0,0)$ и $B = (0,b)$, $b \geq 0$. Нека $d = \sqrt{d_{ag}^2\ C\ D}$. Онда $E = (0, b+d)$.

Аксиома пет сегмената.

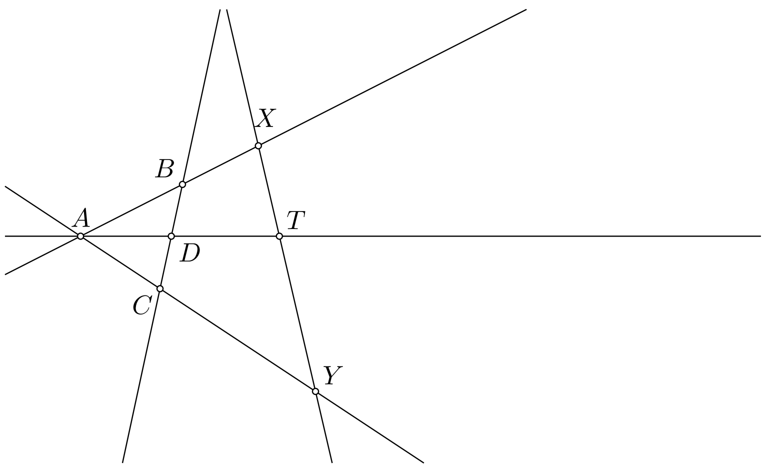
lemma "$AB \cong_t A'B' \wedge BC \cong_t B'C' \wedge AD \cong_t A'D' \wedge BD \cong_t B'D' \wedge$
$\mathcal{B}_t(A,B,C) \wedge \mathcal{B}_t(A',B',C') \wedge A \neq B \longrightarrow CD \cong_t C'D'$"

Доказ да наш модел задовољава ову аксиому је прилично директан, али захтева компликована израчунавања. Да би упростили доказ, тачке A, B и C су трансформисане тако да леже на позитивном делу y-осе. Како су у израчунавањима потребни квадратни корени, није било могуће користити аутоматизацију као у претходним доказима и многи ситни кораци су морали бити исписани ручно.

Еуклидова аксиома.

lemma "$\mathcal{B}_t(A,D,T) \wedge \mathcal{B}_t(B,D,C) \wedge A \neq D \longrightarrow$
$(\exists XY.\ (\mathcal{B}_t(A,B,X) \wedge \mathcal{B}_t(A,C,Y) \wedge \mathcal{B}_t(X,T,Y)))$"

Одговарајућа слика када су све тачке различите:



У доказу овог тврђења коришћене су изометријске трансформације. Тачке A, D и T су пресликане редом у тачке $(0,0)$, $(d,0)$ и $(t,0)$, односно у тачке на y-оси. Потом су анализирани дегенерисани случајеви, односно случајеви када су неке од тачака једнаке или када су све тачке колинарне. У дегенерисаним случајевима, одређивање тачака X и Y није представљало потешкоћу јер углавном су оне неке од датих тачака, односно неке од тачака A, B, C, D или T. Рецимо, уколико су тачке колинеарне и ако важи $\mathcal{B}_t(A, C, T)$, онда је тачка X заправо тачка B, а тачка Y је тачка T.

Доказивање уопштеног случаја захтева доста алгебарских израчунавања. Пре свега, потребно је одредити координате тачака X и Y, а потом на основу тих координата одредити три коефицијента који представљају однос међу тачакама, односно, први коефицијент представља однос међу тачкама A, B и X, други међу тачкама A, C и Y, а трећи међу тачкама X, T и Y. Да би показали да ове тачке заиста задовољавају релацију $\mathcal{B}_T^{ag}$, потребно је показати да сваки од три одређена коефицента се налази у интервалу $[0, 1]$, односно $0 \leq k_i \leq 1$, при чему $i = 1, 2, 3$. Иако је доказ ове чињенице директан, потребно је доста израчунавањи, а због знака $\leq$ није могуће користити аутоматизацију већ је морало да се доста корака показује ручно.

1.5 Геометрија Хилберта

Циљ у овом одељку је да покажемо да наше дефиниције Декартовог координатног система задовољавају аксиоме Хилбертове геометрије. Основни објекти у Хилбертовој планарној геомертрији су тачке, праве, релација између (означена са $\mathcal{B}_h(A, B, C)$) и релација конгруенције (означена са $AB \cong_h C$).

У оргиналној Хилбертовој аксиоматизацији [?] неке претпоставке се имплицитно подразумевају у односу на контекст у коме су дате. На пример, ако је речено *"постоје две тачке"*, то увек значи постоје две различите тачке. Без ове претпоставке нека тврђења не важе (нпр. релација између не важи ако су тачке једнаке).

Аксиоме инциденције

Прве две аксиоме су формализоване коришћењем само једног тврђења.

lemma "$A \neq B \longrightarrow \exists!\ l.\ A \in_h l \wedge B \in_h l$"

Последња аксиома ове групе је формализована коришћењем два одвојена тврђења.

`lemma` "$\exists AB.\ A \neq B \ \wedge\ A \in_h l \ \wedge\ B \in_h l$"
`lemma` "$\exists ABC.\ \neg\ \mathcal{C}_h(A, B, C)$"

Релација колинераности $\mathcal{C}_h$ (која је коришћена у претходној дефиницији) се дефинише на следећи начин:

`definition` "$\mathcal{C}_h(A, B, C) \longleftrightarrow \exists l.\ A \in_h l \ \ \wedge\ \ B \in_h l \ \ \wedge\ \ C \in_h l.$"

Наравно, ми желимо да покажемо да наше дефиниције у Декартовој координатној равни задовољавају ове аксиоме. На пример, ово значи да ми треба да покажемо:

`lemma` „$A \neq B \longrightarrow \exists l.\ A \in_H^{ag} l \wedge B \in_H^{ag} l.$"

Докази ових лема су тривијални и углавном су добијени развијањем дефиниција и онда коришћењем аутоматског доказивања (коришћењем методе Гребнерових база).

Аксиоме поретка

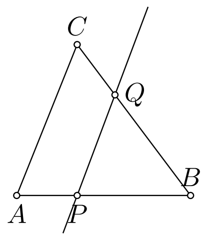
Аксиоме поретка описују својства (ексклузивне) релације између.

`lemma` "$\mathcal{B}_h(A, B, C) \longrightarrow A \neq B \ \wedge\ A \neq C \ \wedge\ B \neq C \ \wedge\ \mathcal{C}_h(A, B, C) \ \wedge\ \mathcal{B}_h(C, B, A)$"
`lemma` "$A \neq C \longrightarrow \exists B.\ \mathcal{B}_h(A, C, B)$"
`lemma` "$A \in_h l \ \wedge\ B \in_h l \ \wedge\ C \in_h l \ \wedge\ A \neq B \ \wedge\ B \neq C \ \wedge\ A \neq C \longrightarrow$
$(\mathcal{B}_h(A, B, C) \ \ \wedge\ \ \neg\mathcal{B}_h(B, C, A) \ \ \wedge\ \ \neg\mathcal{B}_h(C, A, B)) \ \vee$
$(\neg\mathcal{B}_h(A, B, C) \ \ \wedge\ \ \mathcal{B}_h(B, C, A) \ \ \wedge\ \ \neg\mathcal{B}_h(C, A, B)) \ \vee$
$(\neg\mathcal{B}_h(A, B, C) \ \ \wedge\ \ \neg\mathcal{B}_h(B, C, A) \ \ \wedge\ \ \mathcal{B}_h(C, A, B))$"

Докази да релације $\cong^{ag}$, $\in_H^{ag}$, и $\mathcal{B}_H^{ag}$ задовољавају ове аксиоме су једноставни и углавном су изведени одвијањем дефиниција и коришћењем аутоматизације.

Пашова аксиома.

`lemma` "$A \neq B \ \wedge\ B \neq C \ \wedge\ C \neq A \ \wedge\ \mathcal{B}_h(A, P, B) \wedge$
$P \in_h l \ \wedge\ \neg C \in_h l \ \wedge\ \neg A \in_h l \ \wedge\ \neg B \in_h lh \ \ \longrightarrow$
$\exists Q.\ (\mathcal{B}_h(A, Q, C) \ \ \wedge\ \ Q \in_h l) \ \ \vee\ \ (\mathcal{B}_h(B, Q, C) \ \ \wedge\ \ Q \in_h l)$"



У оргиналној Пашовој аксиоми постоји још једна претпоставка – тачке A, B и C нису колинеарне, тако да је аксиома формулисана само за централни, недегенерисани случај. Ипак, у нашем моделу тврђење тривијално важи ако оне јесу колинеарне, тако да смо ми показали да наш модел задовољава и централни случај и дегенерисани случај када су тачке колинеарне. Приметимо да због својстава Хилбертове релације између, претпоставка да су тачке различите не може бити изостављена.

Доказ користи стандардне технике. Прво, користе се изометријске трансформације да транслирају тачке на y-оси, тако да $A = (0, 0)$, $B = (x_B, 0)$ и $P = (x_P, 0)$. Нека је $C = (x_C, y_C)$ и $\lfloor l \rfloor_{R3} = (l_A, l_B, l_C)$. У зависности у којим сегементима тражена тачка се налази, имамо два велика различита случаја. Коришћењем својства $\mathcal{B}_h(A, P, B)$ показује се да важи $l_A \cdot y_B \neq 0$ и онда можемо одредити два коефицијента $k_1 = \frac{-l_C}{l_A \cdot y_B}$ и $k_2 = \frac{l_A \cdot y_B + l_C}{l_A \cdot y_B}$. Даље, показује се да важи $0 < k_1 < 1$ или $0 < k_2 < 1$. Коришћењем $0 < k_1 < 1$, тачка $Q = (x_Q, y_Q)$ је одређена са $x_Q = k_1 \cdot x_C$ и $y_Q = k_1 \cdot y_C$, па зато $\mathcal{B}_h(A, Q, C)$ важи. У другом случају, када друго својство важи, тачка $Q = (x_q, y_q)$ је одређена са $x_Q = k_2 \cdot (x_C - x_B) + x_B$ и $y_Q = k_2 \cdot y_C$, па зато $\mathcal{B}_t(B, Q, C)$ важи.

Аксиоме конгруенције

Прва аксиома конгруенције омогућава конструисање конгруентних сегмената на датој прави. У Хилбертовој књизи „Основи геометрије” [?] аксиома се формулише на следећи начин: *„Ако су A и B две тачке на прави a, а A' је тачка на истој или другој прави a' онда је увек могуће одредити тачку B' на датој страни праве a' у односу на тачку A' такву да је сегмент AB конгруентан сегменту $A'B'$.”* Ипак, у нашој формализацији део *„на датој страни”* је промењен и уместо једне одређене су две тачке (приметимо да је ово имплицитно и речено у оргиналној аксиоми).

lemma "$A \neq B \wedge A \in_h l \wedge B \in_h l \wedge A' \in_h l' \longrightarrow$
$\exists B'\,C'.\ B' \in_h l' \wedge C' \in_h l' \wedge \mathcal{B}_h(C', A', B') \wedge AB \cong_h A'B' \wedge AB \cong_h A'C'$"

Доказ да ова аксиома важи у нашем моделу Декартове координатне равни, почиње са изометријским трансформацијама тако да A' постаје $(0,0)$ и l' постаје x-оса. Тада је прилично једноставно одредити две тачке на x-оси тако што одредимо координате ових тачака користећи услов да d_{ag}^2 између њих и тачке A' је исто као и d_{ag}^2 A B.

Следеће две аксиоме су директно показане одвијањем одговарајућих дефиниција и применом алгебарских трансформација и метода Гребнерових база.

lemma "$AB \cong_h A'B' \wedge AB \cong_h A''B'' \longrightarrow A'B' \cong_h A''B''$"
lemma "$\mathcal{B}_h(A,B,C) \wedge \mathcal{B}_h(A',B',C') \wedge AB \cong_h A'B' \wedge BC \cong_h B'C' \longrightarrow AC \cong_h A'C'$"

Следеће три аксиоме у Хилбертовој аксиоматизацији су о појму угла, а ми још нисмо разматрали угао у нашој формализацији.

Аксиома паралелности

lemma "$\neg P \in_h l \longrightarrow \exists!\, l'.\ P \in_h l' \wedge \neg(\exists\ P_1.\ P_1 \in_h l \wedge P_1 \in_h l')$"

Доказ ове аксиоме састоји се из два дела. Прво је показано да таква права постоји а потом да је она јединствена. Доказивање постојања је учињено одређивањем коефицијената тражене праве. Нека је $P = (x_P, y_P)$ и $\lfloor l \rfloor_{R3} = (l_A, l_B, l_C)$. Онда су коефицијенти тражене праве $(l_A, l_B, -l_A \cdot x_P - l_B \cdot y_P)$. У другом делу доказа, полази се од претпоставке да постоје две праве које задовољавају услов $P \in_h l' \wedge \neg(\exists\ P_1.\ P_1 \in_h l \wedge P_1 \in_h l')$. У доказу је показано да су њихови коефицијенти пропорционални па су самим тим и праве једнаке.

Аксиоме непрекидности

Архимедова аксиома. Нека је A_1 нека тачка на прави између случано изабраних тачака A и B. Нека су тачке $A_2, A_3, A_4, \ldots$ такве да A_1 лежи између тачке A и A_2, A_2 између A_1 и A_3, A_3 између A_2 и A_4 итд. Додатно, нека су сегменти $AA_1, A_1A_2, A_2A_3, A_3A_4, \ldots$ једнаки међусобно. Онда, у овој серији тачака, увек постоји тачка A_n таква да B лежи између A и A_n.

Прилично је тешко репрезентовати серију тачака на начин како је то задато у аксиоми и наше решење је било да користимо листу. Прво, дефинишемо листу такву да су сваке четири узастопне тачке конгруентне, а за сваке три узастопне тачке важи релација између.

definition

"congruentl $l \longrightarrow$ length $l \geq 3 \;\wedge$
$\quad \forall i.\ 0 \leq i \;\wedge\; i+2 <$ length $l \longrightarrow$
$\quad (l\ !\ i)(l\ !\ (i+1)) \cong_h (l\ !\ (i+1))(l\ !\ (i+2)) \;\wedge$
$\quad \mathcal{B}_h((l\ !\ i),(l\ !\ (i+1)),(l\ !\ (i+2)))$"

Са оваквом дефиницијом, аксиома је мало трансформисана, али и даље са истим значењем, и она каже да постоји листа тачака са својствима која су горе поменута таква да за барем једну тачку A' из дате листе важи $\mathcal{B}_t(A, B, A')$. У Isabelle/HOL систему ово је формализовано на следећи начин:

lemma "$\mathcal{B}_h(A, A_1, B) \;\longrightarrow$
$(\exists l.$ congruentl $(A\ \#\ A1\ \#\ l) \;\wedge\; (\exists i.\ \mathcal{B}_h(A, B, (l\ !\ i))))$"

Главна идеја овог доказа је у тврђењима $d_{ag}^2\ A\ A' > d_{ag}^2\ A\ B$ и $d_{ag}^2\ A\ A' = t \cdot d_{ag}^2\ A\ A_1$. Зато, у првом делу доказа одредимо t такво да $t \cdot d_{ag}^2\ A\ A_1 > d_{ag}^2\ A\ B$ важи. Ово се постиже применом Архимедовог правила за реалне бројеве. Даље, показано је да постоји листа l таква да congruentl l важи, да је та листа дужа од t, и таква да су њена прва два елемента A и A_1. Ово је урађено индукцијом по параметру t. База индукције, када је $t = 0$ тривијално важи. У индукционом кораку, листа је проширена са једном тачком таквом да важи релација конгруенције за њу и последње три тачке листе и да важи релација између за последња два елемента листе и додату тачку. Коришћењем ових услова, координате нове тачке се лако одређују алгебарским израчунавањима. Када је једном конструисана, листа задовољава услове аксиоме, што се лако показује у последњим корацима доказа. У доказу се користе неке додатне леме које углавном служе да се опишу својства листе која задовољава услов congruentl l.

1.6 Завршна разматрања

У овом раду ми смо представили добро изграђену формализацију Декартове геометрије равни у оквиру система Isabelle/HOL. Дато је неколико различитих дефиниција Декартове координатне равни и показано је да су све дефиниције еквивалентне. Дефиниције су преузете из стандарних уџбеника. Међутим, да би их исказали у формалном окружењу асистента за доказивање теорема, било је потребно подићи ниво ригорозности. На пример, када дефинишемо праве преко једначина, неки уџбеници помињу да различите једначине репрезентују исту праву ако су њихови коефицијенти "пропорционални", док неки други уџбеници често ово важно тврђење и не наведу. У текстовима се обично не помињу конструкције као што су релација еквиваленције и класа еквиваленције које су у основи наше формалне дефиниције.

Формално је показаано да Декартова коордната раван задовољава све аксиоме Тарског и већину аксиома Хилберта (укључујући и аксиому непрекидности). Доказ да наша Декартова координатна раван задовољава све аксиоме Хилберта је тема за наредни рад јер смо констатовали да формулација аксиоме комплетности и аксиома у којима се помиње изведени појам угла су проблематичне.

Наше искуство је да је доказивање да наш модел задовољава једноставне Хилбертове аксиоме лакше него показивање да модел задовољава аксиоме Тарског. Разлог за ово највише лежи у дефиницији релације између. Наиме, Тарски дозвољава да тачке које су у релацији између буду једнаке. Ово је разлог за постојање бројих дегенерисаних случајева који морају да се анализирају посебно што додатно усложњава расуђивање и доказе. Међутим, Хилбертове аксиоме су формулисане коришћем неких изведених појмова (нпр. углова) што представља проблем за нашу формализацију.

Чињеница да је аналитичка геометрија модел синететичке геометрије се често подразумева као једна једноставна чињеница. Ипак, наше искуство показује да, иако концептуално једноставан, доказ ове чињенице захтева прилично комплексна израчунавања и веома је захтеван за формализацију. Испоставља се да је најважнија техника коришћена да се упросте докази "без губитка на општости" и коришћење изометријских трансформација. На пример, прво смо покушали да докажемо централни случај Пашове аксиоме без примене изометријских трансформација. Иако би требало да буде могуће извести такав доказ, израчунавања која су се појавила су била толико комплексна да ми нисмо успели да завршимо доказ. После примене изометријских трансформација, израчунавања су и даље била нетривијална, али ипак, ми смо успели да завршимо овај доказ. Треба имати на уму да смо морали да се често користимо ручним израчунавањима јер чак и моћна тактика која се заснива на Гребенеровим базама није успела да аутоматски упрости алгебарске изразе. Из овог експеримента са Пашовом аксиомом, закључили смо колики је значај изометријских трансформација и следећа тврђења нисмо ни покушавали да доказујемо директно.

Наша формализација аналитичке геометрије се заснива на аксиомама реалних бројева и у многим доказима су коришћена својства реалних бројева. Многа својства важе за било које нумеричко поље (и тактика заснована на Гребенеровим базама је такође била успешна и у том случају). Међутим, да би доказали аксиому непрекидности користили смо својство супремума, које не важи у произвољном пољу. У нашем даљем раду, волели бисмо да изградимо аналитичку геометрију без коришћења аксиома реланих бројева, тј. да дефинишемо аналитичку геометрију у оквиру аксиоматизације Тарског или Хилберта. Заједно са овим радом, то би омогућило дубљу анализу неких теоријских својстава модела геометрије. На пример, желимо да покажемо категоричност и система аксиома Тарског и система аксиома Хилберта (и да покажемо да су сви модели изоморфни и еквивалентни Декартовој координатној равни).

Литература

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, __________________________

____