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 [3], 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 "B_T^ag (xa, ya) (xb, yb) (xc, yc) ⟷
  (∃(k :: real). 0 ≤ k ∧ k ≤ 1 ∧
    (xb − xa) = k · (xc − xa) ∧ (yb − ya) = k · (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 $d^2_{ag}\ A\ B = (x_B - x_A)^2 + (y_B - y_A)^2$. Тачке A и B су конгруентне тачкама C и D ако и само ако $d^2_{ag}\ A\ B = d^2_{ag}\ C\ D$. У Isabelle/HOL систему ово се може формализовати на следећи начин:

definition "$d^2_{ag}\ (x_1, y_1)\ (x_2, y_2) = (x_2 - x_1) \cdot (x_2 - x_1) + (y_2 - y_1) \cdot (y_2 - y_1)$"
definition "$A_1B_1 \cong^{ag} A_2B_2 \longleftrightarrow d^2_{ag}\ A_1\ B_1 = d^2_{ag}\ A_2\ B_2$"

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 коефицијенте. Формализација у систему Isabelle/HOL се састоји из неколико корака. Прво, дефинише се домен валидних тројки који су коефицијенти 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 $\texttt{line}^{ag}$) 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 ⟷
  (∃ A B C. ⌊l⌋_R3 = (A, B, C) ∧ (A · x + B · 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 $A \in^{ag}_{H} l$ се дефинише коришћењем **`quotient_definition`** која се заснива на релацији `ag_in_h`. Лема добре дефинисаности је

```
lemma
  shows "l ≈ l' ⟹ 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`** $\texttt{vec}^{ag} = \text{"}real \times real\text{"}$. 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 ::point^ag, v ::vec^ag). v ≠ (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 ($\texttt{line}^{ag}$) 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 "$\texttt{transp}^{ag}\ (v_1, v_2)\ (x_1, x_2) = (v_1 + x_1, v_2 + x_2)$"

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

Такође, централна симетрија се лако дефинише коришћењем координата тачаке:

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

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

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

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

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 [3].

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[9]. 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` [1], 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.

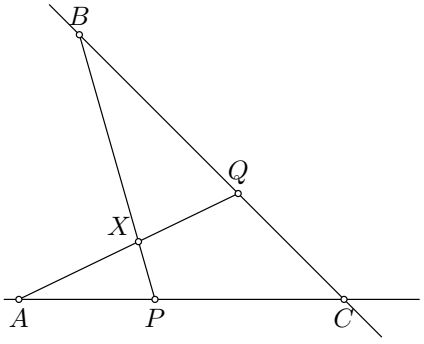
Идентитет у релацији између. Прва аксиома (инсклузивне) релације између даје једно њено једноставно својство и, за наш модел, доказује се готово аутоматски.

`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 ([7]) 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 "$\mathcal{B}^{ag}_T\ A\ A\ B$"
lemma "$\mathcal{B}^{ag}_T\ A\ B\ C \longrightarrow \mathcal{B}^{ag}_T\ C\ B\ A$"
lemma "$\mathcal{B}^{ag}_T\ A\ X\ B\ \wedge\ \mathcal{B}^{ag}_T\ A\ B\ Y \longrightarrow \mathcal{B}^{ag}_T\ X\ B\ Y$"
lemma "$\mathcal{B}^{ag}_T\ A\ X\ B\ \wedge\ \mathcal{B}^{ag}_T\ A\ B\ Y \longrightarrow \mathcal{B}^{ag}_T\ A\ X\ Y$"

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):

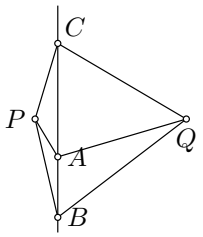
lemma "$(\exists x.\ x \in P) \wedge (\exists y.\ \forall x \in P.\ x < y) \longrightarrow$
$\exists S.\ (\forall y.\ (\exists x \in P.\ y < x) \leftrightarrow y < S)$"

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.

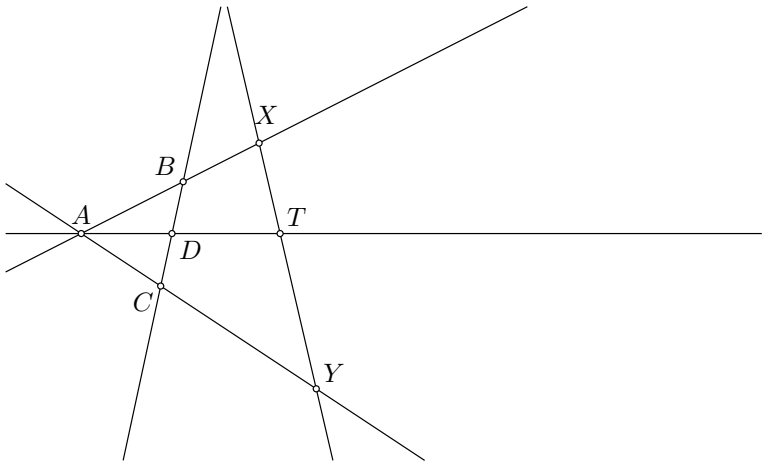
`lemma` "$AB \cong_t A'B' \wedge BC \cong_t B'C' \wedge AD \cong_t A'D' \wedge BD \cong_t B'D' \wedge$
$\mathcal{B}_t(A, B, C) \wedge \mathcal{B}_t(A', B', C') \wedge A \neq B \longrightarrow CD \cong_t C'D'$"

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 коефициента 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 [4] 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 колинеарности $\mathcal{C}_h$ (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 „$A \neq B \longrightarrow \exists l.\ A \in^{ag}_H l \wedge B \in^{ag}_H l$."

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

Аксиоме поретка

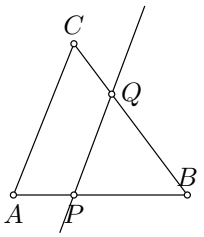
Аксиоме поретка описују својства (ексклузивне) релације између.

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 $\cong^{ag}$, $\in^{ag}_H$, и $\mathcal{B}^{ag}_H$ 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 правој. У Хилбертовој књизи „Основи геометрије” [4] аксиома се формулише на следећи начин: *„Ако су A и B две тачке на правој a, а A' је тачка на истој или другој правој 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^2_{ag} између њих и тачке A' је исто као и $d^2_{ag}\ A\ B$.

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

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 координатна 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).

Глава 2

Формализација хиперболичке геометрије

2.1 Увод

Постоји јако пуно радова и књига које описују геометрију комплексне равни, а у овом поглављу ми ћемо представити резултате наше формализације. Постоји више циљева које смо желели да остваримо.

1. Формализовати теорију проширене комплексне равни (комплексна раван која садржи тачку бесконачно) и њених објеката (правих и кругова) и њених трансформација (Мебијусове трансформације).

2. Спојити бројне приступе које можемо срести у препорученој литератури у један униформни приступ у коме ће бити коришћен јединствен и прецизан језик за описивање појмова

3. Анализирати и формално показати све случајеве који често остану недовољно истражени јер их више различитих аутора сматра тривијалним.

4. Природно се намећу два приступа формализацији: геометријски (рецимо приступ који предлаже Needham [8]) и алгебарски (приступ који можемо видети у раду Schwerdtfeger [10]), као и питање да ли избор приступа утиче на ефикасност формалног доказивања. У раду ће бити детаљно дискутовани односи између два наведена приступа у формализацији као и њихове предности и мане.

5. Биће анализиране технике које се користе у доказима, као и могућност коришћења аутоматизације.

6. Посматраћемо да ли је доказе лакше извести у моделу Риманове сфере или у моделу хомогених координата.

У овој тези, ради сажетости, ми ћемо представити само основне резултате наше формализације — најважније дефиниције и тврђења. Овај рад садржи само кратку рекапитулацију оригиналног формалног извођења и многа својства која су формално доказана неће бити презентована у овом раду. Додано, ни један доказ неће бити показан или описан, а све је доступно у оквиру званичне Isabelle/HOL документације [1].

2.2 Формализација геометрије комплексне равни

Неки основни појмови

Комплексни бројеви. Иако у систему Isabelle/HOL постоји основна подршка за комплексне бројеве, то није било довољно за наше потребе, па смо морали да направимо додатни напор и да ову теорију проширимо. Многе леме које смо показали су углавном веома техничке и нису интересантне за виши ниво формализације коју описујемо и зато их нећемо спомињати у овом тексту (нпр. `lemma "arg` i `=` $pi/2$`"` или `lemma "`$|z|^2$ `= Re (`z `* cnj` z`)"`). Једна од најзначајнијих дефиниција је дефиниција функције за канонизацију угла $\lfloor \_ \rfloor$, која узима у обзир 2π периодичност синуса и косинуса и мапира сваки угао у његову каноничну вредносту која лежи у оквиру интервала $(-\pi, \pi]$. Са овом функцијом, на пример, мултипликативна својства функције `arg` могу се лако изразити и доказати.

`lemma "`$z_1 * z_2 \neq 0 \Longrightarrow$ `arg(`$z_1 * z_2$`) = ⌊arg` z_1 `+ arg` z_2`⌋"`

Како се комплексни бројеви често третирају и као вектори, увођење скаларног производа између два комплексна броја (што је дефинисано као $\langle z_1, z_2 \rangle =$

[1] Isabell документи у којима су теорије и докази доступни се налазе на адреси `http://argo.matf.bg.ac.rs/formalizations/`

$(z_1 * \texttt{cnj}\ z_2 + z_2 * \texttt{cnj}\ z_1)/2)$ се показало веома корисно за сажето приказивање неких услова.

Линеарна алгебра. Следећа важна теорија за даљу формализацију је теорија линеарне алгебре $\mathbb{C}^2$. Представљање вектора и матрица различитих димензија у логици вишег реда представља изазов, због недостатка зависних типова [2], али у нашој формализацији треба само да разматрамо просторе коначне димензије $\mathbb{C}^2$ и у неким ситуацијама $\mathbb{R}^3$, тако да је наш задатак био једноставнији. Комплексни вектори се дефинишу са `type_synonym C2_vec = complex × complex`. Слично, комплексне матрице (`C2_mat`) се дефинишу као четворка комплексних бројева (матрица $\begin{pmatrix} A & B \\ C & D \end{pmatrix}$ репрезентована је са (A, B, C, D)). Скаларно множење вектора означавамо са $*_{sv}$, а скаларно множење са матрицом означавамо са $*_{sm}$. Скаларни производ два вектора означен је са $*_{vv}$, производ вектора и матрице је означено са $*_{vm}$, производ матрице и вектора је означено са $*_{mv}$, а производ две матрице са $*_{mm}$. Нула матрица је означена са `mat_zero`, јединична матрица је означена са `eye`, нула вектор је означен са `vec_zero`, детерминанта матрице је означена са `mat_det`, њен траг (сума елемената на главној дијагонали) са `mat_trace`, инверзна матрица са `mat_inv`, транспонована матрица са `mat_transpose`, коњугација сваког елемента вектора са `vec_cnj`, коњугација сваког елемента матрице са `mat_cnj`, итд. Уведени су многи стандарни појмови линеарне алгебре. На пример, сопствене вредности су дефинисане и карактеризоване на следећи начин:

```
definition eigenval :: "C2_mat ⇒ complex ⇒ bool" where
  "eigenval k A ⟷ (∃v. v ≠ vec_zero ∧ A *mv v = k *sv v)"
lemma "eigenval k H ⟷ k^2 - mat_trace H * k + mat_det H = 0"
```

Адјунгована матрица је транспонована коњугована матрица. *Хермитеове* матрице су оне које су једнаке својој адјунгованој матрици, док су *унитарне* матрице оне чији инверз је једнак њиховој адјунгованој матрици.

```
definition mat_adj where "mat_adj H = mat_cnj (mat_transpose H)"
definition hermitean where "hermitean H ⟷ mat_adj H = H"
definition unitary where "unitary M ⟷ mat_adj M *mm M = eye"
```

Други основни појмови који су потребни у овом раду ће бити уведени у даљем тексту, а читалац може пронаћи више информација у нашем оригиналном документу.

Главни резултати

Проширена комплексна раван

Веома важан корак у развоју гометрије комплексне равни је проширена комплексна раван која има један додатни елемент у односу на комплексну раван $\mathbb{C}$ (који се третира као тачка бесконачно). Проширену комплексну раван ћемо означити са $\overline{\mathbb{C}}$. Постоји више различитих приступа [8, 10] за дефинисање $\overline{\mathbb{C}}$. Најпривлачнији начин са становишта израчунавања је приступ који се базира на хомогеним координатама, а најпривлачнији приступ визуелно је заснован на стереографској пројекцији Риманове сфере.

Хомогене координате

Проширена комплексна раван $\overline{\mathbb{C}}$ се идентификује са комплексном пројективном линијом (једнодимензиони пројективни простор над комплексним пољем, понекад означаван са CP^1). Свака тачка $\overline{\mathbb{C}}$ је репрезентована паром комплексних хомогених координата (од којих нису оба једнака нули), а два пара хомогених координата представљају исту тачку у $\overline{\mathbb{C}}$ акко су они пропорционални са неким ненула комплексним фактором. Формализација овог својства у систему Isabelle/HOL се ослања на lifting/transfer пакет за колинички тип [6] и састоји се из три фазе [2]. Прво се уводи тип за пар комплексних бројева који је различит од нуле (и који се истовремено посматра и као ненула комплексни вектор).

```
typedef C2_vec≠0 = „{v::C2_vec. v ≠ vec_zero}"
```

Одавде добијамо функцију за репрезентацију `Rep_C2_vec`$_{\neq 0}$ (коју ћемо означити са $\lfloor \_ \rfloor_{C2}$) која враћа (ненула) пар комплексних бројева за сваки дати

[2] Једна од фаза може бити прескочена ако би се користио lifting/transfer пакет за парцијални колинички тип. Ову могућност ми нисмо користили у нашој формализацији због неких проблема који су постојали у ранијим верзијама количничког пакета. У међувремену, сви проблеми су исправљени, али наша формализације је у том тренутку већ увелико била развијена и било би заиста мнотоно све мењати од почетка.

елемент помоћног типа $\texttt{C2\_vec}_{\neq 0}$ и враћа функцију за абстракцију $\texttt{Abs\_C2\_vec}_{\neq 0}$ (коју ћемо ми означити са $\lceil \_ \rceil^{C2}$) која враћа $\texttt{C2\_vec}_{\neq 0}$ елемент за сваки дати не-нула пар комплексних бројева. Друго, кажемо да су два елемента типа $\texttt{C2\_vec}_{\neq 0}$ еквивалентна акко су њихове репрезентације пропорционалне.

```
definition ≈C2 :: "C2_vec≠0 ⇒ C2_vec≠0 ⇒ bool" where
  "z1 ≈C2 z2 ⟷ (∃ (k::complex). k ≠ 0 ∧ ⌊z2⌋C2 = k *sv ⌊z1⌋C2)"
```

Прилично је лако показати да $\approx_{C2}$ је релација еквиваленције. Коначно, тип комплексних бројева проширене комплексне равни дат хомогеним координатама се дефинише као класа еквиваленције релације $\approx_{C2}$ и уводи се преко наредног количничког типа.

```
quotient_type complexhc = C2_vec≠0 / ≈C2
```

Да сумирамо, на најнижем нивоу репрезентације постоји тип комплексних бројева, на следећем нивоу је тип ненула комплексних 2×2 вектора (који се представљају претходним типом), а на највишем нивоу је количнички тип који има класу еквивалеције — рад са овим количничким типом (његовом репрезетацијом и апстракцијом) се ради у позадини, коришћењем пакета lifting/transfer [6]. Ова три нивоа апстракције могу на математичаре деловати збуњујуће, али они су неопходни у формалном окружењу где сваки објекат мора имати јединствени тип (на пример, често се узима да је $(1, i)$ истовремено пар комплексних бројева и ненула комплексни вектор, али у нашој формализацији $(1, i)$ је пар комплексних бројева, док је $\lceil (1, i) \rceil^{C2}$ ненула комплексни вектор).

Обични и бесконачни бројеви. Сваки обични комплексни број може бити конвероване у проширени комплексни број.

```
definition of_complex_rep :: "complex ⇒ C2_vec≠0" where
  of_complex_rep z = ⌈(z, 1)⌉C2
lift_definition of_complex :: "complex ⇒ complexhc" is
  of_complex_rep
```

Тачка бесконачности се дефинише на следећи начин:

```
definition inf_hc_rep :: C2_vec≠0 where inf_hc_rep = ⌈(1, 0)⌉^C2
lift_definition ∞hc :: "complexhc" is inf_hc_rep
```

Лако се показује да су сви проширени комплексни бројеви или ∞_{hc} (акко је њихова друга координата једнака нули) или се могу добити конвертовањем обичних комплексних бројева (акко њихова друга координата није нула).

```
lemma "z = ∞hc ∨ (∃ x. z = of_complex x)"
```

Нотација 0_{hc}, 1_{hc} и i_{hc} се користи да означи комплексне бројеве 0, 1, и i у проширеној комплексној равни (у хомогеним координатама).

Аритметичке операције. Аритметичке операције обичних комплексних бројева могу бити проширене тако да се могу применити у проширеној комплексној равани.

На најнижем, репрезентативном нивоу, сабирање (z_1, z_2) и (w_1, w_2) се дефинише као $(z_1 * w_2 + w_1 * z_2, z_2 * w_2)$, тј.

```
definition plus_hc_rep :: "C2_vec≠0 ⇒ C2_vec≠0 ⇒ C2_vec≠0"
  where "plus_hc_rep z w = (let (z1, z2) = ⌊z⌋C2; (w1, w2) = ⌊w⌋C2
                            in ⌈(z1 * w2 + w1 * z2, z2 * w2)⌉^C2)"
```

Овим се добија ненула пар хомогених координата осим ако су и z_2 и w_2 нула (у супротном, добија се лоше дефинисани елемент $\lceil(0,0)\rceil^{C2}$)[3]. Дефиниција је подигнута на ниво количничког типа:

```
lift_definition +hc :: "complexhc ⇒ complexhc ⇒ complexhc" is
  plus_hc_rep
```

Ова дефиниција генерише следећи обавезан услов који треба показати $[\![z \approx_{C2} z'; w \approx_{C2} w']\!] \Longrightarrow z +_{hc} w \approx_{C2} z' +_{hc} w'$, а он се лако доказује анализом случајева да ли су z_2 и w_2 оба једнака нули. Приметимо да због HOL захтева да све функције буду тоталне, ми не можемо дефинисати функцију само за добро дефинисане случајеве, и у доказу морамо да посматрамо и лоше дефинисане случајеве.

[3]Све функције (укључујући и апстрактну функцију $\lceil\_\rceil^{C2}$) у HOL су тоталне. Ипак, све леме о тој функцији које су доказане, садрже један додатни услов, а то је да њихов аргумент није $(0,0)$. Зато, не постоји разлог да резонујемо о вредности $\lceil(0,0)\rceil^{C2}$ и може се сматрати као лоше дефинисана вредност.

Даље, показује се да ова операција проширује уобичајено сабирање комплексних бројева (операцију + у $\mathbb{C}$).

```
lemma "of_complex z +hc of_complex w = of_complex (z + w)"
```

Сума обичних комплексних бројева и ∞_{hc} је ∞_{hc} (ипак, $\infty_{hc} +_{hc} \infty_{hc}$ је лоше дефинсана).

```
lemma "of_complex z +hc ∞hc = ∞hc"
lemma "∞hc +hc of_complex z = ∞hc"
```

Операција $+_{hc}$ је асоцијативна и комутативна, али ∞_{hc} нема инверзни елемент, што прекида лепа алгебарска својства операције + на $\mathbb{C}$.

Друге аритметичке операције су такође проширене. На најнижем, репрезентативном нивоу, унарни минус (z_1, z_2) је $(-z_1, z_2)$, производ (z_1, z_2) и (w_1, w_2) је $(z_1 * z_2, w_1 * w_2)$, а реципрочна вредност (z_1, z_2) је (z_2, z_1) – ове операције су онда подигнуте на апстрактни количнички тип што производи операције означене са $\texttt{uminus}_{hc}$, $*_{hc}$, и $\texttt{recip}_{hc}$. Одузимање (означено са $-_{hc}$) је дефинисано коришћењем $+_{hc}$ и $\texttt{uminus}_{hc}$, а дељење (означено са $:_{hc}$) се дефинише коришћењем $*_{hc}$ и $\texttt{recip}_{hc}$. Као и у случају сабирања, показано је да све ове операције одговарају обичним операцијама коначне комплексне равни (нпр. `lemma "uminus`$_{hc}$ `(of_complex` z`) = of_complex` $(-z)$`"`). Следеће леме показују понашање ових операција када се у њима појављује и тачка бесконачно (приметмо да изрази $0_{hc} *_{hc} \infty_{hc}$, $\infty_{hc} *_{hc} 0_{hc}$, $0_{hc} :_{hc} 0_{hc}$, и $\infty_{hc} :_{hc} \infty_{hc}$ су лоше дефинисани).

```
lemma "uminushc ∞hc = ∞hc"
lemma "recip_hc ∞hc = 0hc" "recip_hc 0hc = ∞hc"
lemma "z ≠ 0hc ⟹ z *hc ∞hc = ∞hc  ∧  ∞hc *hc z = ∞hc"
lemma "z ≠ 0hc ⟹ z :hc ∞hc = 0hc"
lemma "z ≠ ∞hc ⟹ ∞hc :hc z = ∞hc"
```

Такође, проширен је и комплексни коњугат (на репрезентативном типу (z_1, z_2) је мапирано на $(\overline{z_1}, \overline{z_2})$), што даје операцију $\texttt{cnj}_{hc}$. Веома важна операција у комплексној геометрији је *инверзија у односу на јединични круг*:

```
definition inversion_hc :: "complex_hc ⇒ complex_hc" where
  "inversion_hc = cnj_hc ∘ recip_hc"
```

Основне особине инверзије се лако доказују.

lemma "$\texttt{inversion}_{hc} \circ \texttt{inversion}_{hc} = id$"
lemma "$\texttt{inversion}_{hc}\ 0_{hc} = \infty_{hc}$" "$\texttt{inversion}_{hc}\ \infty_{hc} = 0_{hc}$"

Размера и дворазмера. Размера и дворазмера су веома важни појмови у пројективној геометрији и у проширеној комплексној равни (дворазмера се карактерише као инваријанта Мебијусових трансформација – основних трансформација у $\overline{\mathbb{C}}$, и могуће је дефинисати праве коришћењем размера и круга коришћењем дворазмере).

Размера тачака z, v и w се обично дефинише као $\frac{z-v}{z-w}$. Наша дефиниција уводи хомогене координате.

definition ratio_rep **where** "ratio_rep z v w =
  (**let** $(z_1, z_2) = \lfloor z \rfloor_{C2}$; $(v_1, v_2) = \lfloor v \rfloor_{C2}$; $(w_1, w_2) = \lfloor w \rfloor_{C2}$
    in $\lceil((z_1 * v_2 - v_1 * z_2) * w_2, (z_1 * w_2 - w_1 * z_2) * v_2)\rceil^{C2}$)"
lift_definition ratio ::
  "$\texttt{complex}_{hc} \Rightarrow \texttt{complex}_{hc} \Rightarrow \texttt{complex}_{hc} \Rightarrow \texttt{complex}_{hc}$" **is** ratio_rep

Приметимо да је ово добро дефинисано у свим случајевима осим када важи $z = w = v$ или $z = v = \infty_{hc}$ или $z = w = \infty_{hc}$ или $v = w = \infty_{hc}$ (ипак, у доказима код подизања на количнички тип ови лоше дефинисани случајеви такође морају бити анализирани). Додатно, оригинална размера разлика је дефинисана у свим случајевима осим када $z = w = v$ или $z = \infty_{hc}$ или $v = w = \infty_{hc}$, тако да наша дефиниција у хомогеним координатама природно проширује оригиналну дефиницију. Следеће леме показују понашање размере у свим добро дефинисаним случајевима (одговара оригиналној размери разлика кад год је она дефинисана).

lemma "$[\![z \neq v \vee z \neq w;\ z \neq \infty_{hc};\ v \neq \infty_{hc} \vee w \neq \infty_{hc}]\!] \Longrightarrow$
  $\texttt{ratio}\ z\ v\ w = (z -_{hc} v) :_{hc} (z -_{hc} w)$"
lemma "$[\![v \neq \infty_{hc};\ w \neq \infty_{hc}]\!] \Longrightarrow \texttt{ratio}\ \infty_{hc}\ v\ w = 1_{hc}$"
lemma "$[\![z \neq \infty_{hc};\ w \neq \infty_{hc}]\!] \Longrightarrow \texttt{ratio}\ z\ \infty_{hc}\ w = \infty_{hc}$"
lemma "$[\![z \neq \infty_{hc};\ v \neq \infty_{hc}]\!] \Longrightarrow \texttt{ratio}\ z\ v\ \infty_{hc} = 0_{hc}$"

Последње две леме су последице прве леме. Такође, приметимо да размера не може бити дефинисана на природан начин у случају када су барем две тачке бесконачно (тако да функција размере остане непрекидна по свим својим параметрима).

Дворазмера је дефинисана над 4 тачке (z, u, v, w), обично као $\frac{(z-u)(v-w)}{(z-w)(v-u)}$. Поново, ми је дефинишемо користећи хомогене координате.

```
definition cross_ratio_rep where "cross_ratio_rep z u v w =
  (let (z₁, z₂) = ⌊z⌋_C2; (u₁, u₂) = ⌊u⌋_C2;
       (v₁, v₂) = ⌊v⌋_C2; (w₁, w₂) = ⌊w⌋_C2 in
  ⌈(z₁ * u₂ − u₁ * z₂) * (v₁ * w₂ − w₁ * v₂), (z₁ * w₂ − w₁ * z₂) * (v₁ * u₂ − u₁ * v₂))⌉^C2"
lift_definition cross_ratio :: "complex_hc ⇒ complex_hc ⇒
  complex_hc ⇒ complex_hc ⇒ complex_hc" is cross_ratio_rep
```

Ово је добро дефинисано у свим случајевима осим када $z = u = w$ или $z = v = w$ или $z = u = v$ или $u = v = w$ (приметимо да бесконачне вредности за z, u, v или w су дозвољене, што није случај у оригиналној формулацији разломка). Нека основна својства дворазмере су дата следећим лемама.

```
lemma "⟦(z ≠ u ∧ v ≠ w) ∨ (z ≠ w ∧ u ≠ v); z ≠ ∞_hc; u ≠ ∞_hc; v ≠ ∞_hc  w ≠ ∞_hc⟧
   ⟹ cross_ratio z u v w = ((z −_hc u) *_hc (v−_hc) :_hc ((z −_hc w) *_hc (v −_hc u))"
lemma "cross_ratio z 0_hc 1_hc ∞_hc = z"
lemma "⟦ z₁ ≠ z₂; z₁ ≠ z₃ ⟧ ⟹ cross_ratio z₁ z₁ z₂ z₃ = 0_hc"
lemma "⟦ z₂ ≠ z₁; z₂ ≠ z₃ ⟧ ⟹ cross_ratio z₂ z₁ z₂ z₃ = 1_hc"
lemma "⟦ z₃ ≠ z₁; z₃ ≠ z₂ ⟧ ⟹ cross_ratio z₃ z₁ z₂ z₃ = ∞_hc"
```

Риманова сфера и стереографска пројекција

Проширена комплексна раван се може идентификовати са Римановом (јединичном) сфером коришћењем стереографске пројекције [8, 10]. Сфера се пројектује из свог северног пола N на xOy раван (коју означавамо са $\mathbb{C}$). Ова пројекција успоставља бијективно пресликавање sp између $\Sigma \setminus N$ и коначне комплексне равни $\mathbb{C}$. Тачка бесконачно је дефинисана као слика од N.

У Isabelle/HOL систему, сфера Σ је дефинисана као нови тип.

```
typedef riemann_sphere = "{(x, y, z)::R3_vec.  x² + y² + z² = 1}"
```

Као и раније, ово дефинише функцију `Rep_riemann_sphere` (која је означена са $\lfloor\_\rfloor_{R3}$) и функцију `Abs_riemann_sphere` (која је означена са $\lceil\_\rceil^{R3}$) која повезује тачке апстрактног типа (`riemann_sphere`) и тачке репрезантативног типа (тројке реалних бројева). Стереографска пројекција се уводи на следећи начин:

```
definition stereographic_rep :: "riemann_sphere ⇒ C2_vec_{≠0}" where
  "stereographic_rep M =
    (let (x, y, z) = ⌊M⌋_R3
      in if (x, y, z) ≠ (0, 0, 1) then ⌈(x + i * y, 1 − z)⌉^C2
      else ⌈(1, 0)⌉^C2)"
lift_definition stereographic :: "riemann_sphere ⇒ complex_hc" is
  stereographic_rep
```

За све тачке, ово је добро дефинисано (вектор $(x + i * y, 1 - z)$ је ненула јер $(x, y, z) \neq (0, 0, 1)$, и $(1, 0)$ је очито ненула).

Инверзна стереорафска пројекција се дефинише на следећи начин.

```
definition inv_stereographic_rep :: "C2_vec_{≠0} ⇒ riemann_sphere"
where
   "inv_stereographic_rep z =
       (let (z1, z2) = ⌊z⌋_C2
         in if z2 = 0 then ⌈(0, 0, 1)⌉^R3
            else let z = z1/z2; XY = (2*z)/cor (1+|z|^2);
            Z = (|z|^2-1)/(1+|z|^2)
                  in ⌈(Re XY, Im XY, Z)⌉^R3)"
lift_definition inv_stereographic :: "complex_hc ⇒ riemann_sphere" is
   inv_stereographic_rep
```

За све тачке, ово је добро дефинисано (сума квадрата три координате је 1 у оба случаја, па се може применити функција `Abs_riemann_sphere`).

Веза између две функције је дата следећим лемама.

```
lemma "stereographic ∘ inv_stereographic = id"
lemma "inv_stereographic ∘ stereographic = id"
lemma "bij stereographic" "bij inv_stereographic"
```

Докази нису тешки, али захтевају формализацију врло незгодних израчунавања.

Тетивно растојање. Риманова сфера може бити метрички простор. Најчешћи начин да се уведе метрички простор је коришћењем *тетивне метрике* – растојање између две тачке на сфери је дужина тетиве која их спаја.

```
definition dist_rs :: "riemann_sphere ⇒ riemann_sphere ⇒ real" where
  "dist_rs M_1 M_2 = (let (x_1, y_1, z_1) = ⌊M_1⌋_R3; (x_1, y_1, z_1) = ⌊M_2⌋_R3
                      in norm (x_1 - x_2, y_1 - y_2, z_1 - z_2))"
```

Функција `norm` је уграђена функција и у овом случају она рачуна Еуклидску векторску норму. Коришћењем (сада већ познате) чињенице да $\mathbb{R}^3$ је метрички простор (са функцијом растојања $\lambda\ x\ y.\ norm(x - y)$), није било тешко показати да је тип `riemann_sphere` опремљен са $\texttt{dist}_{rs}$ метрички простор, тј. да је он инстанца локала `metric_space`. Иако је дефинисана на сфери, тетивна метрика има своју репрезентацију и у равни.

```
lemma assumes
 "stereographic M_1 = of_complex m_1"
 "stereographic M_2 = of_complex m_2"
 shows "dist_rs M_1 M_2 = 2*|m_1-m_2| / (sqrt (1+|m_1|^2)*sqrt (1+|m_2|^2))"
lemma assumes
 "stereographic M_1 = ∞_hs"
 "stereographic M_2 = of_complex m"
 shows "dist_rs M_1 M_2 = 2 / sqrt (1+|m|^2)"
lemma assumes
 "stereographic M_1 = of_complex m"
 "stereographic M_2 = ∞_hs"
 shows "dist_rs M_1 M_2 = 2 / sqrt (1+|m|^2)"
lemma assumes "stereographic M_1 = ∞_hs" "stereographic M_2 = ∞_hs"
 shows "dist_rs M_1 M_2 = 0"
```

Ове леме праве разлику између коначних и бесконачних тачака, али се ова анализа случаја може избећи коришћењем хомогених координата.

```
definition "⟪z, w⟫ = (vec_cnj ⌊z⌋_C2) *_vv (⌊w⌋_C2)"
```

```
definition "⟪z⟫ = sqrt (Re ⟪z, z⟫)"
definition "dist_hc_rep = 2*sqrt(1 - |⟪z, w⟫|² / (⟪z⟫² * ⟪w⟫²))"
lift_definition dist_hc :: "complex_hc ⇒ complex_hc ⇒ real" is
  dist_hc_rep
lemma "dist_rs M1 M2 = dist_hc (stereographic M1) (stereographic M2)"
```

Понекад, ова форма се зове Fubini-Study метрика.

Тип $\texttt{complex}_{hc}$ опремљен са $\texttt{dist}_{hc}$ метриком је такође инстанца локала `metric_space`. Ово тривијално следи из последње леме која је повезује са метричким простором на Римановој сфери. Постоје и директни докази ове чињенице (нпр. Hille [5] даје директан доказ захваљујући Shizuo Kakutani, али доказ је некомплетан јер занемарује могућност да једна тачка буде бесконачно), а ми смо и те директне доказе формализовали[4]. Испоставило се да је нека својства лакше показати на Римановој сфери коришћењем функције $\texttt{dist}_{rs}$ (нпр. неједнакост троугла), али нека својста је било лакше показати у пројекцији коришћењем функције $\texttt{dist}_{hc}$ (нпр. да је метрички простор савршен, тј. да нема изолованих тачака), што показује значај постојања различитих модела за исти концепт.

Коришћењем тетивне метрике у проширеној комплексној равни, и Еуклидске метрике на сфери у $\mathbb{R}^3$, показано је да су стереографска пројекција и инверзна стереографска пројекција непрекидне.

```
lemma "continuous_on UNIV stereographic"
      "continuous_on UNIV inv_stereographic"
```

Приметимо да у претходној леми, метрика је имплицитна (у систему Isabelle/HOL претпоставља се да коришћена метрика је управо она метрика која је коришћена да се покаже да је дати тип инстанца локала `metric_space`).

Мебијусове трансформације

Мебијусове трансформације (које се још називају и холоморфна пресликавања, ленеарна фракциона трансформација или билинеарна пресликавања) су основне трансформације проширене комплексне равни. У нашој формализацији оне су уведене алгебарски. Свака трансформација је представљена

[4]Наша формализација је започета без анализирања Риманове сфере, тако да смо у почетку једино и могли користити директне доказе, али у неком тренутку увели смо појам Риманове сфере и то је помогло да се многи докази упросте, укључујући и овај.

регуларном (несингуларном, недегенерисаном) 2×2 матрицом која ленеарно делује на хомогене координате. Како пропорционалне хомогене координате представљају исту тачку у $\overline{\mathbb{C}}$, тако и пропорционалне матрице представљају исту Мебијусову трансформацију. Поново, формализација се састоји из три корака коришћењем lifting/transfer пакета. Прво, уводи се тип регуларних матрица.

```
typedef C2_mat_reg = "{M :: C2_mat. mat_det M ≠ 0}"
```

Функција репрезентације `Rep_C2_mat_reg` ће бити означена са $\lfloor \_ \rfloor_M$, а апстрактна функција `Abs_C2_mat_reg` ће бити означена са $\lceil \_ \rceil^M$. Регуларне матрице формирају групу у односу на множење и она се често назива *генерална линеарна група* и означава се са $GL(2, \mathbb{C})$. У неким случајевима се разматра само њена подгрупа, *специјална линерана група*, означена са $SL(2, \mathbb{C})$, која садржи само оне матрице чија је детерминанта једнака 1.

Мебијусова група. Кажемо да су две регуларне матрице еквивалентне ако су њихове репрезентације пропорционалне.

```
definition ≈M :: "C2_mat_reg ⇒ C2_mat_reg ⇒ bool" where
  "M1 ≈M M2 ⟷ (∃ (k::complex). k ≠ 0 ∧ ⌊M2⌋M = k *sm ⌊M1⌋M)"
```

Лако се показује да је ова релација заправо релација еквиваленције. Елементи Мебијусове групе се уводе као класа еквиваленције над овом релацијом.

```
quotient_type mobius = C2_mat_reg / ≈M
```

Понекад ћемо користити помоћни конструктор `mk_mobius` који враћа елемент Мебијусове групе (класу еквиваленције) за дата 4 комплексна параметра (што има смисла само када је одговарајућа матрица регуларна).

Мебијисови елементи формирају групу над композицијом. Ова група се назива *пројективна генерална линерна група* и означена је са $PGL(2, \mathbb{C})$. Поново, могу се разматрати само они елементи *специјалне пројективне групе* $SGL(2, \mathbb{C})$ чија детерминанта је једнака 1. Композиција Мебијусових елемената се постиже множењем матрица које их репрезентују.

```
definition mobius_comp_rep :: "C2_mat_reg ⇒ C2_mat_reg ⇒ C2_mat_reg"
   where "moebius_comp_rep M1 M2 = ⌈⌊M1⌋M *mm ⌊M2⌋M⌉M"
```

```
lift_definition mobius_comp :: "mobius ⇒ mobius ⇒ mobius" is
  mobius_comp_rep
```

Слично, инверзна Мебијусова трансформација се добија инверзијом матрице која је представља.

```
definition mobius_inv_rep :: "C2_mat_reg ⇒ C2_mat_reg" where
  "mobius_inv_rep M = ⌈mat_inv ⌊M⌋_M⌉^M"
lift_definition mobius_inv :: "mobius ⇒ mobius" is "mobius_inv_rep"
```

Коначно, Мебијусова трансформација која је идентитет је представљена јединичном матрицом.

```
definition mobius_id_rep :: "C2_mat_reg" where
  "mobius_id_rep = ⌈eye⌉^M"
lift_definition mobius_id :: "mobius" is mobius_id_rep
```

Све ове дефиниције увек уводе добро дефинисане објекте (јер је производ регуларних матрица регуларна матрица, а инверз регуларне матрице је такође регуларна матрица). Обавезни услови да би се дефиниција могла подићи (нпр. $M_1 \approx_M M_2 \implies$ `mobius_inv_rep` $M_1 \approx_M$ `mobius_inv_rep` M_2) се лако доказују. Онда, показује се да је тип `mobius` заједно са овим операцијама инстанца локала `group_add` који је већ уграђен у систем Isabelle/HOL. Зато, ми ћемо понекад означавати `mobius_comp` са $+$, `mobius_inv` са унарним $-$, и `mobius_id` са 0.

Дејство Мебијусове групе. Мебијусове трансформације су дате као дејство Мебијусове групе на тачке проширене комплексне равни (које су дате у хомогеним координатама).

```
definition mobius_pt_rep :: "C2_mat_reg ⇒ C2_vec_{≠0} ⇒ C2_vec_{≠0}"
  where "moebius_pt_rep M z = ⌈⌊M⌋_M *_mv ⌊z⌋_C2⌉^C2"
lift_definition mobius_pt :: "mobius ⇒ complex_hc ⇒ complex_hc" is
  mobius_pt_rep
```

Како производ регуларне матрице и ненула вектора је увек ненула вектор, резултат је увек добро дефинисан. Подизање дефиниција генерише обавезан

услов $[\![M \approx_M M';\ z \approx_{C2} z']\!] \Longrightarrow$ `mobius_pt_rep` $M\ z \approx_{C2}$ `mobius_pt_rep` $M'\ z'$ који се прилично лако показује.

Када се узима у обзир дејство групе на проширену комплексну раван, онда се може видети да операције групе заиста одговарају композицији пресликавања, инверзном пресликавању и идентичном пресликавању.

```
lemma "mobius_pt (mobius_comp M1 M2) =
                 (mobius_pt M1) ∘ (mobius_pt M2)"
lemma "mobius_pt (mobius_inv M) = inv (mobius_pt M)"
lemma "mobius_pt (mobius_id) = id"
```

Дејство је транзитивно (јер је увек бијективно пресликавање).

```
lemma "bij (mobius_pt M)"
```

У класичној литератури Мебијусове трансформације се обично представљају у форми $\frac{az+b}{cz+d}$, и наредна лема заиста оправдава и овакав запис (али у њој разликујемо специјалан случај када је z тачка бесконачно).

```
lemma assumes "mat_det (a, b, c, d) ≠ 0"
      shows "moebius_pt (mk_mobius a b c d) z =
                 (if z ≠ ∞hc then
                       ((of_complex a) *hc z +hc (of_complex b)) :hc
                       ((of_complex c) *hc z +hc (of_complex d))
                 else (of_complex a) :hc (of_complex c))"
```

Произвољна трансформација у $\overline{\mathbb{C}}$ ће бити звана Мебијусовом трансформацијом акко је она дејство неког елемента Мебијусове групе.

```
definition is_mobius :: "(complexhc ⇒ complexhc) ⇒ bool" where
  "is_mobius f ⟷ (∃ M. f = mobius_pt M)"
```

Приметимо да већина до сада изнетих резултата зависи од чињенице да је матрица репрезентације Мебијусове трансформације регуларна – у супротном, дејство би било дегенерисано и целу раван $\overline{\mathbb{C}}$ би сликало у једну тачку.

Неке специјалне Мебијусове трансформације. Многе трансформације са којима се сусрећемо у геометрији су заправо специјална врста Мебијусових трансформација. Веома важна погрупа је група *Еуклидских сличности* (које

се још називају и *интегралне трансформације*). Оне су одређене са два комплексна параметра (и представљају Мебијусову трансформацију када први од та два параметра није нула).

```
definition similarity :: "complex ⇒ complex ⇒ mobius" where
  "similarity a b = mk_mobius a b 0 1"
```

Сличности формирају групу (која се понекад назива и *параболичка група*).

```
lemma "⟦a ≠ 0; c ≠ 0⟧ ⟹
  mobius_comp (similarity a b) (similarity c d) =
  similarity (a * c) (a * d + b)"
lemma "a ≠ 0 ⟹
  mobius_inv (similarity a b) = similarity (1/a) (-b/a)"
lemma "id_mobius = similarity 1 0"
```

Њихово дејство је линеарна трансформација у $\mathbb{C}$, а свака линеарна трансформација у $\mathbb{C}$ која није константна је дејство елемента групе Еуклидских сличности.

```
lemma "a ≠ 0 ⟹ mobius_pt (similarity a b) =
                (λ z. (of_complex a) *hc z +hc (of_complex b))"
```

Еуклидске сличности су једини елементи Мебијусове групе такви да је тачка ∞_{hc} фиксна тачка.

```
lemma "mobius_pt M ∞hc = ∞hc ⟷
    (∃ a b. a ≠ 0 ∧ M = similarity a b)"
```

Ако су и тачка ∞_{hc} и тачка 0_{hc} фиксне, онда је то сличност са коефицијентима $a \neq 0$ и $b = 0$, а дејство је облика `λ z. (of_complex a) *hc z`.

```
lemma "mobius_pt M ∞hc = ∞hc ∧ mobius_pt M 0hc = 0hc ⟷
  (∃ a. a ≠ 0 ∧ M = similarity a 0)"
```

Еуклидске сличности укључују танслацију, ротацију и дилатацију и свака Еуклидска сличност се може добити композијом ова три пресликавања.

```
definition "translation v = similarity 1 v"
definition "rotation φ    = similarity (cis φ) 0"
definition "dilatation k  = similarity (cor k) 0"
lemma "a ≠ 0 ⟹ similarity a b =
   (translation b) + (rotation (arg a)) + (dilatation |a|)"
```

Реципрочна вредност $(1_{hc} :_{hc} z)$ је такође Мебијусова трансформација.

```
definition "reciprocation = mk_mobius (1, 0, 0, 1)"
lemma "recip_hc = mobius_pt reciprocation"
```

Са друге стране, инверзија није Мебијусова трансформација (то је основни пример такозваних анти-Мебијусових трансформација, или антихоломорфне функције).

Веома важна чињеница је да се свака Мебијусова трансформација може добити композицијом Еуклидских сличности и реципрочне функције. Један од начина како се ово може постићи дат је следећом лемом (када је $c = 0$ је случај Еуклидских сличности и ово је раније већ анализирано).

```
lemma assumes "c ≠ 0" and "a * d - b * c ≠ 0"
shows "mk_mobius a b c d =
       translation (a/c) + rotation_dilatation ((b*c - a*d)/(c*c)) +
       reciprocal + translation (d/c)"
```

Декомпозиција је коришћена у многим доказима. Наиме, да би показали да свака Мебијусова трансформација има неко својство, довољно је показати да реципрочна функција и Еуклидске сличности заадовољавају то својство и да композиција чува то својство (обично, најтеже је показати у случају реципрочне функције, а остала два корака буду углавном много једноставнија).

```
lemma assumes "⋀ v.  P (translation v)" "⋀ α.  P (rotation α)"
  "⋀ k.  P (dilatation k)" "P (reciprocation)"
  "⋀ M1 M2. ⟦ P M1; P M2 ⟧ ⟹ P (M1 + M2)"
  shows "P M"
```

Дворазмера као Мебијусова трансформација. За било које три фиксне тачке z_1, z_2 и z_3, `cross_ratio` z z_1 z_2 z_3 се може посматрати као функција једне промењиве z. Следећа лема гарантује да је ова функција Мебијусова трансформација и да према особина дворазмере она слика z_1 у 0_{hc}, z_2 у 1_{hc} и z_3 у ∞_{hc}.

```
lemma "⟦ z1 ≠ z2; z1 ≠ z3; z2 ≠ z3 ⟧ ⟹
  is_mobius (λ z. cross_ratio z z1 z2 z3)"
```

Доказавши ово тврђење, дворазмера се може користити да се покаже да постоји Мебијусова трансформација која слика било које три различите тачке редом у 0_{hc}, 1_{hc} и ∞_{hc}. Како Мебијусове трансформације чине групу, једноставна последица овога је да постоји Мебијусова трансформација која слика било које три различите тачке у било које три различите тачке.

```
lemma "⟦ z1 ≠ z2; z1 ≠ z3; z2 ≠ z3 ⟧ ⟹ (∃ M. mobius_pt M z1 = 0hc ∧
  mobius_pt M z2 = 1hc ∧ mobius_pt M z3 = ∞hc)"
```

Следећа лема има веома важну примену у даљем развоју теорије јер омогућава закључивање „без губитка на општости (бгно)" [3]. Наиме, ако Мебијусова трансформација чува неко својство, онда уместо три произвољне тачке може се посматрати само случај специјалних тачака 0_{hc}, 1_{hc}, и ∞_{hc}.

```
lemma assumes "P 0hc 1hc ∞hc" "z1 ≠ z2" "z1 ≠ z3" "z2 ≠ z3"
  "⋀ M u v w. P u v w ⟹
            P (mobius_pt M u) (mobius_pt M b) (mobius_pt M c)"
  shows "P z1 z2 z3"
```

Једна од првих примена „бгно" резоновања за Мебијусове трансформације је у анализи фиксних тачака Мебијусових трансформација. Лако се показује да једино идентично пресликавање има фиксне тачке 0_{hc}, 1_{hc}, и ∞_{hc}. Такође важи да ако Мебијусова трансформација M има три различите фиксне тачке, онда је она идентитет, али директан доказ овога се заснива на чињеници да 2×2 матрица има највише два независна сопствена вектора, а овакво закључивање се лако може избећи коришћењем „бгно" резоновања (како било које три тачке можемо сликати редом у 0_{hc}, 1_{hc}, и ∞_{hc} неким пресликавањем M', а онда пресликавање $M' + M - M'$ има ове три тачке фиксне па мора бити једнако 0).

```
lemma "⟦ mobius_pt M 0hs = 0hs; mobius_pt M 1hs = 1hs;
  mobius_pt M ∞hs = ∞hs ⟧ ⟹ M = id_mobius"
lemma "⟦ mobius_pt M z1 = z1; mobius_pt M z2 = z2;
  mobius_pt M z3 = z3; z1 ≠ z2; z1 ≠ z3; z2 ≠ z3 ⟧ ⟹ M = id_mobius"
```

Последица овога је да постоји јединствена Мебијусова трансформација која слика три различите тачке у друге три различите тачке (већ је показано да такво пресликавање постоји, а ако би постојала два таква пресликавања онда би њихова разлика морала имати три фиксне тачке, што значи да би била идентитет).

```
lemma "⟦z1 ≠ z2; z1 ≠ z3; z2 ≠ z3; w1 ≠ w2; w1 ≠ w3; w2 ≠ w3⟧ ⟹ ∃! M.
 mobius_pt M z1 = w1 ∧ mobius_pt M z2 = w2 ∧ mobius_pt M z3 = w3"
```

Мебијусове трансформације чувају дворазмеру. Поново, директан доказ би био компликован, па је формализован елегантан индиректни доказ (у основи, разлика $\lambda z.$ `cross_ratio` z z_1 z_2 z_3 и M слика $(M\ z_1)$ у 0_{hc}, $(M\ z_2)$ у 1_{hc}, и $(M\ z_3)$ у ∞_{hc}, па зато мора бити једнака $\lambda z.$ `cross_ratio` z `(`$M\ z_1$`) (`$M\ z_2$`) (`$M\ z_3$`)`, и тврђење следи замењујући $(M\ z)$ са z).

```
lemma "⟦z1 ≠ z2; z1 ≠ z3; z2 ≠ z3⟧ ⟹
    cross_ratio z z1 z2 z3 =
    cross_ratio (mobius_pt M z) (mobius_pt M z1)
                (mobius_pt M z2) (mobius_pt M z3)"
```

Кругоправа

Веома важно својство проширене комплексне равни је могућност да праве и кругове посматрамо униформно. Основни објекат је *уопштен круг* или скраћено *кругоправа*. У нашој формализацији ми смо пратили приступ који је описао Schwerdtfeger [10] и представили смо кругоправе Хермитским, ненула 2×2 матрицама. У оригиналној формулацији, матрица $\begin{pmatrix} A & B \\ C & D \end{pmatrix}$ одговара једначини $A * z *$ `cnj` $z + B *$ `cnj` $z + C * z + D = 0$, где је $C =$ `cnj` B и A и D су реални (јер је матрица Хермитска). Кључно је да ова једначина представља праву када је $A = 0$, а иначе круг.

Поново, наша формализација се састоји из три корака. Прво, уведен је тип Хермитских, ненула матрица.

```
definition is_C2_mat_herm :: "C2_mat ⇒ bool" where
  "is_C2_mat_herm H ⟷ hermitean H ∧ H ≠ mat_zero"
typedef C2_mat_herm = "{H :: C2_mat. is_C2_mat_herm H}"
```

Функција репрезентације `Rep_C2_mat_herm` ће бити означена са $\lfloor\_\rfloor_H$, а апстрактна функција `Abs_C2_mat_herm` ће бити означена са $\lceil\_\rceil^H$. Имајући на уму интерпретацију у форми једначине, јасно је да поново пропорационалне матрице би требало сматрати еквивалентним. Овог пута, фактор пропорционалности матрица је реалан ненула број.

```
definition ≈cm :: "C2_mat_herm ⇒ C2_mat_herm ⇒ bool" where
  "H1 ≈cm H2 ⟷ (∃ (k::real). k ≠ 0 ∧ ⌊H2⌋H = cor k *sm ⌊H1⌋H)"
```

Лако се показује да је ово релација еквиваленције, а кругоправе се дефинишу коришћењем количничке конструкције као класа еквиваленције.

```
quotient_type circline = C2_mat_herm / ≈cm
```

Помоћни конструктор `mk_circline` даје кругоправу (класу еквиваленције) за дата четири комплексна броја A, B, C и D (под претпоставком да они формирају Хермитску, ненула матрицу).

Свака кругоправа одређује одговарајући скуп тачака. Поново, опис који је дат у хомогеним координатама је нешто бољи него оригинални опис који је дат за обичне комплексне бројеве. Тачка са хомогеним координатама (z_1, z_2) ће припадати скупу тачака кругоправе акко $A * z_1 * \texttt{cnj}\, z_1 + B * \texttt{cnj}\, z_1 * z_2 + C * z_1 * \texttt{cnj}\, z_2 + D * z_2 * \texttt{cnj}\, z_2 = 0$. Приметимо да је ово квадратна форма која је одређена вектором хомогених координата и Хермитском матрицом. Зато, скуп тачака на датој кругоправи се формализује на следећи начин (поред дефиниције кругоправе на овом месту дајемо и дефиниције билинеарне и квадратне форме које су уведене у нашој основној теорији линеарне алгебре).

```
definition "bilinear_form H z1 z2 = (vec_cnj z1) *vm H *vv z2"
definition "quad_form H z = bilinear_form H z z"
definition on_circline_rep :: "C2_mat_herm ⇒ C2_vec≠0 ⇒ bool" where
  "on_circline_rep H z ⟷ quad_form ⌊H⌋H ⌊z⌋C2 = 0"
lift_definition on_circline :: "circline ⇒ complexhc ⇒ bool" is
  on_circline_rep
```

```
definition circline_set :: "complex_hc set" where
  "circline_set H = {z. on_circline H z}"
```

Подизање дефиниције `on_circline` ствара услове $[\![H_1 \approx_{cm} H_2;\ z_1 \approx_{C2} z_2]\!] \Longrightarrow$ `on_circline_rep` $H_1\ z_1 \longleftrightarrow$ `on_circline_rep` $H_2\ z_2$ који се лако доказују.

Неке специјалне кругоправе. Међу свим кругоправама најзначајније су јединични круг, x-оса и имагинарни јединични круг.

```
definition "unit_circle_rep = ⌈(1, 0, 0, −1)⌉^H"
lift_definition unit_circle :: "circline" is unit_circle_rep
definition "x_axis_rep = ⌈(0, i, −i, 0)⌉^H"
lift_definition x_axis :: "circline" is x_axis_rep
definition "imag_unit_circle_rep = ⌈(1, 0, 0, 1)⌉^H"
lift_definition imag_unit_circle :: "circline" is
    imag_unit_circle_rep
```

Лако се показују нека основна својства ових кругоправих. На пример:

```
lemma "0_hc ∈ circline_set x_axis" "1_hc ∈ circline_set x_axis"
      "∞_hc ∈ circline_set x_axis"
```

Повезаност са правама и круговима у обичној Еуклидској равни. У проширеној комплексној равни не постоји разлика између појма праве и појма круга. Ипак, праве могу бити дефнисане као оне кругоправе код којих матрице имају коефицијент $A = 0$, или, еквивалентно као оне кругоправе које садрже тачку ∞_{hc}.

```
definition is_line_rep where
  "is_line_rep H ⟷ (let (A, B, C, D) = ⌊H⌋_H in A = 0)"
lift_definition is_line :: "circline ⇒ bool" is is_line_rep
definition is_circle_rep where
  "is_circle_rep H ⟷ (let (A, B, C, D) = ⌊H⌋_H in A ≠ 0)"
lift_definition is_circle :: "circline ⇒ bool" is is_circle_rep
lemma "is_line H ⟷ ¬ is_circle H" "is_line H ∨ is_circle H"
lemma "is_line H ⟷ ∞_hc ∈ circline_set H"
      "is_circle H ⟷ ∞_hc ∉ circline_set H"
```

Сваки Еуклидски круг и Еуклидкса права (у обичној комплексној равни, коришћењем стандардне, Еуклидске метрике) може бити представљена коришћењем кругоправе.

```
definition mk_circle_rep μ r = ⌈(1, −μ, −cnj μ, |μ|² − (cor r)²)⌉ᴴ
lift_definition mk_circle :: "complex ⇒ real ⇒ circline" is
  mk_circle_rep
lemma "r ≥ 0 ⟹ circline_set (mk_circle μ r) =
                    of_complex ` {z. |z − μ| = r}"
definition mk_line_rep where "mk_line_rep z₁ z₂ =
  (let B = i * (z₂ − z₁) in ⌈(0, B, cnj B, −(B * cnj z₁ + cnj B * z₁)⌉ᴴ)"
lift_definition mk_line :: "complex ⇒ complex ⇒ circline" is
  mk_line_rep
lemma "z₁ ≠ z₂ ⟹ circline_set (mk_line z₁ z₂) - {∞ₕc} =
                     of_complex ` {z. collinear z₁ z₂ z}"
```

Супротно такође важи, скуп тачака који су одређени кругоправом је увек или Еуклидски круг или Еуклидска права. Следећа функција одређује параметре круга или параметре праве (центар и полупречник у случају круга или две различите тачке у случају праве) за дату кругоправу.

```
definition euclidean_circle_rep where "euclidean_circle_rep H =
  (let (A, B, C, D) = ⌊H⌋ᴴ
    in (−B/A, sqrt(Re ((B * C − A * D)/(A * A)))))"
lift_definition euclidean_circle :: "circline ⇒ complex × real" is
  euclidean_circle_rep
definition euclidean_line_rep where "euclidean_line_rep H =
  (let (A, B, C, D) = ⌊H⌋ᴴ;
       z₁ = −(D * B)/(2 * B * C);
       z₂ = z₁ + i * sgn (if arg B > 0 then −B else B)
    in (z₁, z₂))"
lift_definition euclidean_line :: "circline ⇒ complex × complex" is
  euclidean_line_rep
```

Приметимо да нормални вектор праве је вектор који је ортогоналан на коефицијент B — у дефиницији друге тачке вектор B мора бити нормализован у намери да би могли да подигнемо дефиницију (тако да су добијене тачке исте

за сваку матрицу која репрезентује исту кругоправу). Ово даје нешто већи израз $z_2 = z_1 + i * B$.

Додатно, кардиналност скупа тачака кругоправе зависи од знака израза $\mathtt{Re}((B*C - A*D)/(A*A))$. Зато, кругоправе могу бити класификоване у три категорије у зависности од знака детерминанте (који је увек реалан број, јер је матрица Хермитска).

```
definition circline_type_rep where
  "circline_type_rep H = sgn (Re (mat_det (⌊H⌋_H)))"
lift_definition circline_type :: "circline ⇒ real" is
  circline_type_rep
```

Обавезан услов $H \approx_{cm} H' \Longrightarrow$ `circline_type_rep` H = `circline_type_rep` H' се лако показује, јер `Re (mat_det (`k $*_{sm}$ H`)) = (Re` k`)`^{2} `* Re (mat_det` H`)` важи за све Хермитске матрице H и за све k са имагинарним делом 0.

Сада постаје јасно да скуп тачака на датој кругоправи је празан акко је тип кругоправе позитиван (ове кругоправе се зову *имагинарне кругоправе*), да садржи само једну тачку акко је тип кругоправе једнак нули (оне се зову *тачка кругоправе*) и да је бесконачан акко је тип негативан (оне се зову *реалне кругоправе*). Оно што је било изненађујуће је да се испоставило да је веома тешко формално показати ово тврђење и било га је могуће показати само када је формализовано дејство Мебијуса на кругоправе што је омогућило да се користи „бгно" резоновање. Приметимо да не постоје имагинарне праве јер кад је $A = 0$, онда `mat_det` $H \geq 0$.

Коначно, веза између реалних кругоправих и Еуклидских правих и кругова се може успоставити.

```
lemma
  assumes "is_circle H" "(μ, r) = euclidean_circle H"
  shows "circline_set H = of_complex ` {z. |z − μ| = r}"
lemma
  assumes "is_line H" "(z₁, z₂) = euclidean_line H"
          "circline_type H < 0"
  shows
  "circline_set H - {∞_hc} = of_complex ` {z. collinear z₁ z₂ z}"
```

Приметимо да прва лема такође важи за имагинарни и тачка круг јер су оба скупа празна. Ипак, друга лема једино важи за реалне праве јер у случају тачка праве важи да $z_1 = z_2$, па је леви скуп празан, а десни је универзални скуп.

Кругоправе на Римановој сфери. Кругоправе у равни одговарају круговима на Римановој сфери, и ми смо формално показали ову везу. Сваки круг у тродимензионом простору се може добити као пресек сфере и равни. Успоставили смо један-на-један пресликавање између кругова на Римановој сфери и равни у простору. Приметимо и да није неопходно да раван сече сферу и тада ћемо рећи да она дефинише јединствен имагинаран круг. Веза између равни у простору и кругоправих у проширеној комплексној равни је описао Schwerdtfeger [10]. Ипак, аутор није приметио да за једну специјалну кругоправу (она чија репрезентативна матрица је јединична матрица) не постоји раван у $\mathbb{R}^3$ која јој одговара — и да би могли да имамо такву раван, потребно је да уместо посматрања равни у $\mathbb{R}^3$, узмемо у обзир тродимензионални пројективни простор и коначну хипераван. Зато, ми дефинишемо раван на следећи начин (опет у три корака).

typedef R4_vec$_{\neq 0}$ = "{(a, b, c, d) :: R4_vec. $(a, b, c, d) \neq$ vec_zero}"

Приметимо да у $\mathbb{R}^3$, један од бројева a, b, или c ће бити различит од 0. Ипак, наша дефиниција дозвољава постојање равни $(0, 0, 0, d)$ која лежи у бесконачности. Функција репрезентације ће бити означена са $\lfloor \_ \rfloor_{R4}$, а апстрактна функција ће бити означена са $\lceil \_ \rceil^{R4}$. Поново, две равни су еквивалентне акко су пропорционалне (овог пута за неки ненула реални фактор).

definition $\approx_{R4}$ :: "R4_vec$_{\neq 0}$ $\Rightarrow$ R4_vec$_{\neq 0}$ $\Rightarrow$ bool" **where**
"$\alpha_1 \approx_{R4} \alpha_2 \longleftrightarrow (\exists k.\ k \neq 0 \wedge \lfloor \alpha_2 \rfloor_{R4} = k * \lfloor \alpha_1 \rfloor_{R4})$"

Коначно, равни (кругови који су у њима су добијени пресеком са Римановом сфером) се дефинишу као класа еквиваленције ове релације.

quotient_type plane = R4_vec$_{\neq 0}$ / $\approx_{R4}$

Коефицијенти равни дају линеарну једначину а тачка на Римановој сфери лежи на кругу одређеном са равни акко њена репрезентација задовољава линеарну једначину.

```
definition on_sphere_circle_rep where
  "on_sphere_circle_rep α M ⟷
    (let (a, b, c, d) = ⌊α⌋R4; (X, Y, Z) = ⌊M⌋R3
      in a * X + b * Y + c * Z + d = 0)"
lift_definition on_sphere_circle ::
  "plane ⇒ riemann_sphere ⇒ bool" is on_sphere_circle_rep
definition sphere_circle_set :: "riemann_sphere set" where
  "sphere_circle_set α = {A. on_sphere_circle α A}"
```

Приметимо да нисмо морали да уведемо тачке у тродимензионом пројективном простору (и њихове хомогене координате) јер смо ми једино заинтересовани за тачке на Римановој сфери које нису бесконачне.

Следеће, ми уводимо стереографску и инверзну стереографску пројекцију између кругова на Римановој сфери и кругова у проширеној комплексној равни.

```
definition stereographic_circline_rep where
  "stereographic_circline_rep α =
    (let (a,b,c,d) = ⌊α⌋R4; A = cor ((c+d)/2); B = (cor a + i * cor b)/2);
         C = (cor a − i * cor b)/2; D = cor ((d − c)/2))
      in ⌈(A, B, C, D)⌉H"
lift_definition stereographic_circline :: "plane ⇒ circline" is
  stereographic_circline_rep
definition inv_stereographic_circline_rep where
  "inv_stereographic_circline_rep H =
    (let (A,B,C,D) = ⌊H⌋H
      in ⌈(Re(B + C), Re(i * (C − B)), Re(A − D), Re(D + A))⌉R4"
lift_definition inv_stereographic_circline :: "circline ⇒ plane" is
  inv_stereographic_circline_rep
```

Ова два пресликавања су бијективна и међусобно инверзна. Пројекција скупа тачака на круга на Римановој сфери је управо скуп тачака на кругоправи која се добија управо уведеном стереографском пројекцијом круга.

```
lemma "stereographic_circline ∘ inv_stereographic_circline = id"
lemma "inv_stereographic_circline ∘ stereographic_circline = id"
```

```
lemma "bij stereographic_circline" "bij inv_stereographic_circline"
lemma "stereographic ` sphere_circle_set α =
       circline_set (stereographic_circline α)"
```

Тетивне кругоправе. Још једна интересантна чињеница је да су реалне кругоправе ништа друго до скупови тачака које су на једнаком одстојању од неких датих тачака (заправо увек постоје тачно две такве тачке), али посматрајући одстојање у тетивној метрици. На Римановој сфери ове две тачке (звaћемо их тетивни центри) се добијају пресеком сфере и праве која пролази кроз центар круга и нормална је на раван која садржи тај круг.

Тетивна кругоправа са датом тачком a и полупречником r је одређена на следећи начин.

```
definition chordal_circle_rep where "chordal_circle_rep μc rc =
  (let (μ1, μ2) = ⌊μc⌋C2;
       A = 4*|μ2|² - (cor rc)²*(|μ1|² + |μ2|²); B = −4*μ1*cnj μ2;
       C = -4*cnj μ1*μ2; D = 4*|μ1|² - (cor rc)²*(|μ1|² + |μ2|²)
    in mk_circline_rep A B C D)"
lift_definition chordal_circle :: "complexhc ⇒ real ⇒ circline" is
  chordal_circle_rep
lemma "z ∈ circline_set (chordal_circle μc rc) ⟷
       rc ≥ 0 ∧ disthc z μc = rc"
```

За дату кругоправу, њен центар и радијус се могу одредити ослањајући се на следеће леме (у зависности да ли су коефицинети B и C у репрезентативној матрици једнаки нули).

```
lemma
 assumes "is_C2_mat_herm (A, B, C, D)" "Re (A * D) < 0" "B = 0"
 shows
   "mk_circline A B C D =
            chordal_circle ∞hc sqrt(Re ((4 * A)/(A − D)))"
   "mk_circline A B C D =
            chordal_circle 0hc sqrt(Re ((4 * D)/(D − A)))"
lemma
 assumes "Re (mat_det (A, B, C, D)) < 0" "B ≠ 0"
```

"is_C2_mat_herm (A, B, C, D)" "$C * \mu_c^2 + (D - A) * \mu_c - B = 0$"
"r_c = sqrt$((4 + \text{Re}((4 * \mu_c/B) * A))/(1 + \text{Re}(|\mu_c|^2)))$"
shows "mk_circline A B C D = chordal_circle (of_complex μ_c) r_c"

Као и у претходним случајевима, може се увести функција која враћа тетивне параметре (потребно је направити разлику међу случајевима $B = 0$ и $B \neq 0$ и у другом случају је потребно решити квадратну једначину која описује тетивни центар).

Симетрија. Још од античке Грчке, инверзија круга је посматрана као аналогија рефлексији праве. У проширеној комплексној равни не постоји суштинска разлика између кругова и прави, тако да ћемо ми посматрати само једну врсту релације и за две тачке ћемо рећи да су *симетричне у односу на круг* ако се оне сликају једна у другу коришћењем било рефлексије или инверзије у односу на произвољану праву или круг. Када смо тражили алгебраску репрезентацију ове релације изненадили смо се колико је била једноставна и елегантна – тачке су симетричне акко је билинеарна форма њиховог репрезентативног вектора и репрезентативне матрице кругоправе једнака нули.

```
definition circline_symmetric_rep where
  "circline_symmetric_rep z1 z2 H ⟷
              bilinear_form ⌊z1⌋C2 ⌊z2⌋C2 ⌊H⌋H = 0"
lift_definition circline_symmetric :: "complexhc ⇒ complexhc ⇒
  circline ⇒ bool" is circline_symmetric_rep
```

Посматрајући скуп тачака на кругоправи и поредећи наше две дефиниције, постаје јасно да тачке на кругоправи су управо оне које су инваријантне у односу на симетрију у односу на ту кругоправу.

```
lemma "on_circline H z ⟷ circline_symmetric H z z"
```

Дејство Мебијусових трансформација на кругоправе. Већ смо видели како Мебијусове трансформације делују на тачке $\overline{\mathbb{C}}$. Оне такође делују и на кругоправе (и дефиниција је изабрана тако да су два дејства компатибилна). Додатно, дајемо и дефиницију подударности две матрице (која је дефинисана у нашој помоћној теорији линеарне алгебре).

```
definition "congruence M H = mat_adj M *mm H *mm M"
definition mobius_circline_rep ::
  "C2_mat_reg ⇒ C2_mat_herm ⇒ C2_mat_herm" where
  "mobius_circline_rep M H = ⌈congruence (mat_inv ⌊M⌋M) ⌊H⌋H⌉H"
lift_definition mobius_circline :: "mobius ⇒ circline ⇒ circline"
  is mobius_circline_rep
```

Својства која има дејство Мебијусових трансформација на кругоправе је врло слично као и код дејства Мебијусових трансформација на тачке. На пример,

```
lemma "mobius_circline (mobius_comp M1 M2) =
       mobius_circline M1 ∘ mobius_circline M2"
lemma "mobius_circline (mobius_inv M) = inv (mobius_circline M)"
lemma "mobius_circline (mobius_id) = id"
lemma "inj mobius_circline"
```

Централна лема у овом одељку прави везу између дејства Мебијусових трансформација на тачкама и на кругоправама (и што је основно, показује се да Мебијусове трансформације сликају кругоправе на кругоправе).

```
lemma "mobius_pt M ` circline_set H =
       circline_set (mobius_circline M H)"
```

Поред овога чува се и тип кругоправе (што повлачи, на пример, да се реалне кругоправе сликају на реалне кругоправе).

```
lemma "circline_type (mobius_circline M H) = circline_type H"
```

Још једно важно својство (које је нешто општије него претходно наведено) је да симетрија тачака је очувана након дејства Мебијусових трансформација (што се још назива и *ūрицūй симеūрије*).

```
lemma assumes "circline_symmetric z1 z2 H"
      shows "circline_symmetric (mobius_pt M z1) (mobius_pt M z2)
                                (mobius_circline M H)"
```

Последње две леме су веома важни геометријски резултати, и захваљујући веома погодној алгебарској репрезентацији, њих је било прилично лако показати у нашој формализацији. Оба доказа се заснивају на следећој једноставној чињеници из линеарне алгебре.

```
lemma "mat_det M ≠ 0 ⟹ bilinear_form z1 z2 H =
   bilinear_form (M *mv z1) (M *mv z2) (congruence (mat_inv M) H)"
```

Јединственост кругоправе. У Еуклидској геометрији добро је позната чињеница да постоји јединствена права кроз две различите тачке и јединствени круг кроз три различите тачке. Слични резулатати важе и у $\overline{\mathbb{C}}$. Ипак, да би се дошло до закључака потребно је извршити анализу случајева према типу кругоправе. Кругоправе позитивног типа не садрже тачке па код њих не постоји јединственост. Кругоправе нула типа садрже једну тачку и за сваку тачку постоји јединствена кругоправа нула типа која је садржи. Постоји јединствена кругоправа кроз било које три различите тачке (и она мора бити негативног типа).

```
lemma "∃! H. circline_type H = 0 ∧ z ∈ circline_set H"
lemma "⟦z1 ≠ z2; z1 ≠ z3; z2 ≠ z3⟧ ⟹
  ∃! H. z1 ∈ circline_set H ∧ z2 ∈ circline_set H ∧
        z3 ∈ circline_set H"
```

Веома изненађујуће, ми нисмо успели да докажемо ове леме директно. Ипак, након примене „бгно" резоновања и након пресликавања тачака у канонску позицију (0_{hc}, 1_{hc} и ∞_{hc}) добили смо веома кратак и елегантан доказ (јер могуће је показати, коришћењем израчунавања, да је x-оса једина кругоправа кроз ове три канонске тачке). Како су праве карактеризоване као управо оне кругоправе које садрже ∞_{hc}, постаје јасно да постоји јединствена права кроз било које две различите коначне тачке.

Скуп кардиналности кругоправе. Још једна од ствари која се узима „здраво за готово" је кардиналност кругоправи различитог типа. Већ смо рекли да ови докази захтевају „бгно" резоновање, али овог пута користили смо другачију врсту „бгно" резоновања. Испоставља се да је у многим случајевима лакше резоновати о круговима уколико је њихов ценатр у координатном почетку — у том случају, њихова матрица је дијагонална. Ми смо формализовали специјалан случај чувеног резултата из ленеарне алгебре да 2×2 Хермитска матрица је подударна са реалном дијагоналном матрицом (шта више, елементи на дијагонали су реалне сопствене вредности матрице, а подударност је успостављена коришћењем унитарних матрица — подударност се

такође може успоставити коришћењем једноставније матрице (матрице транслације), али онда она не би имала многа лепа својства).

```
lemma assumes "hermitean H"
  shows "∃k1 k2 M. mat_det M ≠ 0 ∧ unitary M ∧
                   congruence M H = (cor k1, 0, 0, cor k2)"
```

Последица је да за сваку кругоправу постоји унитарна Мебијусова трансформација која слика кругоправу тако да је њен центар у координатном почетку (заправо, постоје две такве трансформације ако су сопствене вредности различите). Видећемо да унитарне трансформације одговарају ротацијама Риманове сфере, тако да последња чињеница има једноставно геометријско објашњење. Кругоправе се могу дијагонализовати коришћењем само транслација, али унитарне трансформације често имају лепша својства.

```
lemma "∃ M H'. unitary_mobius M ∧
                mobius_circline M H = H' ∧ circline_diag H'"
lemma assumes "⋀ H'. circline_diag H' ⟹ P H"
              "⋀ M H. P H ⟹ P (mobius_circline M H)"
      shows   "P H"
```

Приметимо да `unitary_mobius` је предикат који подиже `unitary` својство са $\mathbb{C}^2$ матрица на тип `mobius`. Слично, `circline_diag` подиже услов дијагоналне матрице на тип `circline`.

Коришћењем овакве врсте „бгно" резоновања постаје прилично јасно како показати следећу карактеризацију за кардиналност скупа кругоправе.

```
lemma "circline_type H > 0 ⟷ circline_set H = {}"
lemma "circline_type H = 0 ⟷ ∃z. circline_set H = {z}"
lemma "circline_type H < 0 ⟷
   ∃z1 z2 z3. z1 ≠ z2 ∧ z1 ≠ z3 ∧ z2 ≠ z3 ∧ circline_set H ⊇ {z1, z2, z3}"
```

Важна, нетривијална, последица јединствености кругоправе и кардиналности скупа кругоправе је да функција `circline_set` је инјективна, тј. за сваки непразан скуп тачака кругоправе, постоји јединствена класа пропорционалних матрица која их све одређује (`circline_set` је празан за све имагинарне

кругоправе, што значи да ово својство не важи када је скуп тачака кругоправе празан).

lemma "⟦ circline_set H_1 = circline_set H_2; circline_set $H_1 \neq \{\}$ ⟧
$\Longrightarrow$ $H_1 = H_2$"

Оријентисане кругоправе

У овом одељку ми ћемо описати како је могуће увести оријентацију за кругоправе. Многи важни појмови зависе од оријентације. Један од најважнијих појмова је појам *диска* — унуштрањост кругоправе. Слично као што је то био случај код скупа тачака кругоправе, скуп тачака диска се уводи коришћењем квадратне форме у чијем изразу се налази матрица кругоправе — скуп тачка диска кругоправе је скуп тачака за које важи $A*z*$cnj $z+B*$cnj $z+C*z+D < 0$, при чему је $\begin{pmatrix} A & B \\ C & D \end{pmatrix}$ матрица која репрезентује кругоправу. Како скуп тачака диска мора бити инваријантан у односу на избор представника, јасно је да матрице оријентисане кругоправе су еквивалентне само ако су оне пропорционалне у односу на неки реални фактор (подсетимо се да код неоријентисаних кругоправих фактор може бити произвољан реалан ненула број).

definition $\approx_{ocm}$ :: "C2_mat_herm $\Rightarrow$ C2_mat_herm $\Rightarrow$ bool" **where**
"$H_1 \approx_{ocm} H_2 \longleftrightarrow$ ($\exists$ (k::real). $k > 0 \wedge \lfloor H_2 \rfloor_H$ = cor k $*_{sm}$ $\lfloor H_1 \rfloor_H$)"

Лако се показује да је ова дефинисана релација релација еквиваленције, тако да су кругоправе дефинисане преко количничке конструкције као класе еквиваленције.

quotient_type o_circline = C2_mat_herm / $\approx_{ocm}$

Сада можемо користити квадратну форму да дефинишемо унутрашњост, спољашњост и границу оријентисане кругоправе.

definition on_o_circline_rep :: "C2_mat_herm $\Rightarrow$ C2_vec$_{\neq 0}$ $\Rightarrow$ bool"
where "on_o_circline_rep H $z \longleftrightarrow$ quad_form $\lfloor H \rfloor_H$ $\lfloor z \rfloor_{C2}$ = 0"
definition in_o_circline_rep :: "C2_mat_herm $\Rightarrow$ C2_vec$_{\neq 0}$ $\Rightarrow$ bool"
where "in_o_circline_rep H $z \longleftrightarrow$ quad_form $\lfloor H \rfloor_H$ $\lfloor z \rfloor_{C2}$ < 0"
definition out_o_circline_rep :: "C2_mat_herm $\Rightarrow$ C2_vec$_{\neq 0}$ $\Rightarrow$ bool"
where "out_o_circline_rep H $z \longleftrightarrow$ quad_form $\lfloor H \rfloor_H$ $\lfloor z \rfloor_{C2}$ > 0"

Ове дефиниције се подижу на `on_o_circline`, `in_o_circline`, и `out_o_circline` (при томе доказујемо неопходне услове), и, коначно, уводе се следеће три дефиниције.

```
definition o_circline_set :: "complex_hc set" where
  "o_circline_set H = {z. on_o_circline H z}"
definition disc :: "complex_hc set" where
  "disc H = {z. in_o_circline H z}"
definition disc_compl :: "complex_hc set" where
  "disc_compl H = {z. out_o_circline H z}"
```

Ова три скупа су међусобно дисјунктна и заједно испуњавају целу раван.

```
lemma "disc H ∩ disc_compl H = {}"
      "disc H ∩ o_circline_set H = {}"
      "disc_compl H ∩ o_circline_set H = {}"
      "disc H ∪ disc_compl H ∪ o_circline_set H = UNIV"
```

За дату оријентисану кругоправу, може се тривијално одредити њен неоријентисани део, а ове две кругоправе имају исти скуп тачака.

```
lift_definition of_o_circline (_°) :: "o_circline ⇒ circline" is id
lemma "circline_set (H°) = o_circline_set H"
```

У **lift_definition** увели смо краћи запис функције `of_o_circline`, тако да, на пример, H° у леми је скраћеница за `of_o_circline` H.

За сваку кругоправу, постоји тачно једна супротно оријентисана кругоправа.

```
definition "opp_o_circline_rep H = ⌈-1 *sm ⌊H⌋_H⌉^H"
lift_definition opp_o_circline (_↔) :: "o_circline ⇒ o_circline" is
  opp_o_circline_rep
```

Одређивање супротне кругоправе је идемпотентно јер супротне кругоправе имају исти скуп тачака, али размењују диск и његов комплемент.

```
lemma "(H↔)↔ = H"
lemma "o_circline_set (H↔) = o_circline_set H"
      "disc (H↔) = disc_compl H" "disc_compl (H↔) = disc H"
```

Функције _$^\circ$ и o_circline_set су у одређеном смислу инјективне.

```
lemma "H₁° = H₂° ⟹ H₁ = H₂ ∨ H₁ = H₂↔"
lemma
  "⟦o_circline_set H₁ = o_circline_set H₂; o_circline_set H₁ ≠ {}⟧
   ⟹ H₁ = H₂ ∨ H₁ = H₂↔"
```

Дата Хермитска матрица кругоправе представља тачно једну од две могуће оријентисане кругоправе. Избор шта ћемо звати позитивно оријентисана кругоправа је произвољан. Ми смо одлучили да пратимо приступ који је предложио Schwerdtfeger [10], где се користи водећи коефицијент A као први критеријум, који каже да кругоправе са матрицом у којој важи $A > 0$ се зову позитивно оријентисане, а ако у матрици важи $A < 0$ онда се зову негативно оријентисане. Ипак, Schwerdtfeger није дискутовао још један могући случај када је $A = 0$ (у случају прави), тако да смо ми морали да проширимо његову дефиницију да би имали потпуну карактеризацију.

```
definition pos_o_circline_rep where "pos_o_circline_rep H ⟷
  (let (A, B, C, D) = ⌊H⌋_H
    in Re A > 0 ∨
       (Re A = 0 ∧ ((B ≠ 0 ∧ arg B > 0) ∨ (B = 0 ∧ Re D > 0))))"
lift_definition pos_o_circline :: "o_circline ⇒ bool"
  is pos_o_circline_rep
```

Сада, тачно једна од две супротно оријентисане кругоправе је позитивно оријентисана.

```
lemma "pos_o_circline H ∨ pos_o_circline (H↔)"
      "pos_o_circline (H↔) ⟷ ¬ pos_o_circline H"
```

Оријентација кругова је и алгебраски једноставна (посматра се знак коефицијента A) и геометријски природна захваљујући следећој једноставној карактеризацији.

```
lemma "∞ₕ ∉ o_circline_set H ⟹
       pos_o_circline H ⟷ ∞ₕ ∉ disc H"
```

Још једна лепа геометријска карактеризација за позитивну оријентацију је да Еуклидски центар позитивно оријентисаних Еуклидових круговова је садржан у њиховом диску.

```
lemma assumes "is_circle (H∘)" "circline_type (H∘) < 0"
              "(a, r) = euclidean_circle (H∘)"
      shows "pos_oriented H ⟷ of_complex a ∈ disc H"
```

Приметимо да оријентација прави и тачка кругова је вештачки уведена (само да бисмо имали тотално дефинисану позитивну оријентацију), и она нема природну геометријску интерпретацију. Због овога, непрекидност оријентације је прекинута и ми мислимо да није могуће увести оријентацију прави тако да функција оријентације буде свуда непрекидна. Зато, када у неким наредним лемама будемо говорили о оријентацији ми ћемо експлицитно искључити случај прави.

Тотална карактеризација за позитивну оријентацију нам омогућава да створимо пресликавање из неоријентисаних у оријентисану кругоправу (добијамо увек позитивно оријентисану кругоправу).

```
definition of_circline_rep :: "C2_mat_herm ⇒ C2_mat_herm" where
  "of_circline_rep H = (if pos_o_circline_rep H then H
                        else opp_o_circline_rep H)"
lift_definition of_circline (_∘) :: "circline ⇒ o_circline" is
  of_circline_rep
```

Показана су бројна својства функције `of_circline`, а овде ћемо навести само најзначајнија.

```
lemma "o_circline_set (H∘) = circline_set H"
lemma "pos_o_circline (H∘)"
lemma "(H∘)∘ = H" "pos_o_circline H ⟹ (H∘)∘ = H"
lemma "H₁∘ = H₂∘ ⟹ H₁ = H₂"
```

Дејство Мебијусових трансформација на оријентисане кругоправе. На репрезентативном нивоу дејство Мебијусових трансформација на оријентисане кругоправе је исто као и дејство на неоријентисане кругоправе.

```
lift_definition mobius_o_circline ::
  "mobius ⇒ o_circline ⇒ o_circline" is mobius_circline_rep
```

Дејство Мебијуса на (неоријентисане) кругоправе се може дефинисати коришћењем дефиниције за дејство Мебијуса на оријентисане кругоправе, али обрнуто не би могло.

```
lemma "mobius_circline M H = (mobius_o_circline M (H^◯))^◯"
lemma "let H₁ = mobius_o_circline M H;
           H₂ = (mobius_circline M (H^◯))^◯
       in H₁ = H₂ ∨ H₁ = H₂^↔"
```

Дејство Мебијусових трансформација на оријентисане кругоправе има слична својства као и дејство Мебијусових трансформација на неоријентисане кругоправе. На пример, оне се слажу у погледу инверза (`lemma "mobius_o_circline (mobius_inv M) = inv (mobius_o_circline M)"`), композиције, идентитета, обе су инјективне (`inj mobius_circline`), и тако даље. Централне леме у овом одељку повезују дејства Мебијусових трансформација на тачкама, оријентисаним кругоправама и дисковима.

```
lemma "mobius_pt M ` o_circline_set H =
       o_circline_set (mobius_o_circline M H)"
lemma "mobius_pt M ` disc H = disc (mobius_o_circline M H)"
lemma "mobius_pt M ` disc_compl H =
       disc_compl (mobius_o_circline M H)"
```

Све Еуклидске сличности чувају оријентацију кругоправе.

```
lemma assumes "a ≠ 0" "M = similarity a b"
              "∞_hc ∉ o_circline_set H"
  shows
    "pos_o_circline H ⟷ pos_o_circline (mobius_o_circline M H)"
```

Оријентација слике дате оријентисане кругоправе H након дате Мебијусове трансформације M зависи од тога да ли пол M (тачка коју трансформација M слика у ∞_{hc}) лежи на диску или у диску који је комплементаран H (ако је у скупу H, онда се слика у праву, а у том случају не дискутујемо оријентацију).

```
lemma
 "0_hc ∈ disc_compl H ⟹
   pos_o_circline (mobius_o_circline reciprocation H)"
 "0_hc ∈ disc H ⟹
   ¬ pos_o_circline (mobius_o_circline reciprocation H)"
lemma
 assumes "M = mk_mobius a b c d" "c ≠ 0" "a*d - b*c ≠ 0"
 shows "pole M ∈ disc H ⟶
        ¬ pos_o_circline (mobius_o_circline M H)"
       "pole M ∈ disc_compl H ⟶
        pos_o_circline (mobius_o_circline M H)"
```

Приметимо да је ово другачије него што тврди Schwerdtfeger [10]: „Реципроцитет чува оријентацију круга који не садржи 0, али инвертује оријетацију било ког круга који садржи 0 као унутрашњу тачку. Свака Мебијусова трансформација чува оријентацију било ког круга који не садржи свој пол. Ако круг садржи свој пол, онда круг који се слика има супротну оријентацију". Наша формализација показује да оријентација резултујућег круга не зависи од оријентације полазног круга (на пример, у случају реципроцитета, оријентација полазног круга показује релативну позицију круга и тачке бесконачно што је одређено знаком коефицијента A у репрезентативној матрици и то је сасвим независно од релативне позиције круга и нула тачке које су одређене знаком коефицијента D — ова два коефицијента се размењују приликом примене трансформације реципроцитет).

Очување угла. Мебијусове трансформације су конформно пресликавање, што значи да оне чувају оријентисане углове међу оријентисаним кругоправама. Ако се угао дефинише коришћењем чисто алгебарског приступа (пратећи [10]), онда је врло лако показати ово својство. Поред дефиниције угла, навешћемо и дефиницију мешовите детерминанте коју смо дефинисали раније у нашој основној теорији.

```
fun mat_det_mix :: "C2_mat ⇒ C2_mat ⇒ complex" where
 "mat_det_mix (A_1, B_1, C_1, D_1) (A_2, B_2, C_2, D_2) =
    A_1 * D_2 - B_1 * C_2 + A_2 * D_1 - B_2 * C_1"
definition cos_angle_rep where
```

```
 "cos_angle_rep H1 H2 =
        - Re (mat_det_mix ⌊H1⌋H ⌊H2⌋H) /
        2 * (sqrt (Re (mat_det ⌊H1⌋H * mat_det ⌊H2⌋H))))"
lift_definition cos_angle :: "o_circline ⇒ o_circline ⇒ complex"
  is cos_angle_rep
lemma "cos_angle H1 H2 =
  cos_angle (moebius_o_circline M H1) (moebius_o_circline M H_2)"
```

Ипак, ова дефиниција није интуитивна, и из педагошких разлога желели смо да је повежемо са нешто уобичајенијом дефиницијом. Прво, дефинисали смо угао између два комплексна вектора ($\lfloor \_ \rfloor$ означава функцију за нормализацију угла која је описана раније).

```
definition ang_vec ("∡") where "∡ z1 z2 = ⌊arg z2 - arg z1⌋"
```

За дати центар μ обичног Еуклидског круга и тачку z на њему, дефинишемо тангетни вектор у z као радијус вектор $\overrightarrow{\mu z}$, ротиран за $\pi/2$, у смеру казаљке на сату или у супротном смеру у зависности од оријентације.

```
definition tang_vec :: "complex ⇒ complex ⇒ bool ⇒ complex" where
  "tang_vec μ z p = sgn_bool p * i * (z - μ)"
```

У болеан променљивој p енкодира се оријентација круга, а функција `sgn_bool` p враћа 1 када је p тачно, а -1 када је p нетачно. Коначно, угао између два оријентисана круга у њиховој заједничкој тачки z се дефинише као угао између тангентних вектора у z.

```
definition ang_circ where
  "ang_circ z μ1 μ2 p1 p2 = ∡ (tang_vec μ1 z p1) (tang_vec μ2 z p2)"
```

Коначно, веза између алгебарске и геометријске дефиниције косинуса угла дата је следећом лемом.

```
lemma assumes "is_circle (H1∘)" "is_circle (H2∘)"
    "circline_type (H1∘) < 0" "circline_type (H2∘) < 0"
    "(μ1, r1) = euclidean_circle (H1∘)"
    "(μ2, r2) = euclidean_circle (H2∘)"
    "of_complex z ∈ o_circline_set H1 ∩ o_circline_set H2"
  shows "cos_angle H1 H2 =
    cos (ang_circ z μ1 μ2 (pos_o_circline H1) (pos_o_circline H2))"
```

Да би доказали ову лему било је неопходно показати закон косинуса у систему Isabelle/HOL, али се ово показало као веома једноставан задатак.

Неке важне подгрупе Мебијусових трансформација

Већ смо описали параболичку групу (групу Еуклидских сличности), кључну за Еуклидску геометрију равни. Сада ћемо описати карактеристике две веома важне подгрупе Мебијусове групе — групу сферних ротација, важну за елиптичку планарну геометрију, и групу аутоморфизама диска која је важна за хиперболичку планарну геометрију.

Ротације сфере. Генерална унитарна група, коју означавамо са $GU_2(\mathbb{C})$ је група која садржи све Мебијусове трансформације које су репрезентоване уопштеним унитарним матрицама.

```
definition unitary_gen where
 "unitary_gen M ⟷
  (∃ k::complex.  k ≠ 0 ∧ mat_adj M *mm M = k *sm eye)"
```

Иако је у дефиницији дозовољено да k буде комплексан фактор, испоставља се да је једино могуће да k буде реалан. Генерализоване унитарне матрице могу бити растављене на обичне унитарне матрице и јединичне матрице које су помоножене неким позитивним фактором.

```
definition unitary where "unitary M ⟷ mat_adj M *mm M = eye"
lemma "unitary_gen M ⟷
  (∃ k M'.  k > 0 ∧ unitary M' ∧ M = (cor k *sm eye) *mm M')"
```

Група унитарних матрица је веома важна јер описује све ротације Риманове сфере (изоморфна је реалној специјалној ортогоналној групи $SO_3(\mathbb{R})$). Једна од могућих карактеризација $GU_2(\mathbb{C})$ у $\overline{\mathbb{C}}$ је да је то група трансформација таквих да имагинарни јединични круг је фиксан (ово је круг чија матрица репрезентације је јединична и налази се у равни у бесконачности).

```
lemma "mat_det (A, B, C, D) ≠ 0 ⟹ unitary_gen (A, B, C, D) ⟷
  moebius_circline (mk_moebius A B C D) imag_unit_circle =
  imag_unit_circle"
```

Карактеризација генерализованих унитарних матрица у координатама је дата са следећом лемом.

lemma "unitary_gen M $\longleftrightarrow$ ($\exists$ a b k. **let** $M' = (a, b, -\texttt{cnj}\ b, \texttt{cnj}\ a)$ **in**
$k \neq 0 \ \wedge$ mat_det $M' \neq 0 \ \wedge \ M = k *_{sm} M'$)"

Додатно, дефинисали смо специјалну унитарну групу $SU_2(\mathbb{C})$, која садржи генерализоване унитарне матрице са детерминантом једнаком један (оне се препознају по форми $(a, b, -\texttt{cnj}\ b, \texttt{cnj}\ a)$), без множитеља k, и ову специјану групу користимо да би извели координатну форму генерализованих унитарних матрица.

Аутоморфизми диска. Дуална група претходној групи трансформација је група генерализованих унитарних матрица чија сигнатура је $1-1$ ($GU_{1,1}(\mathbb{C})$).

definition unitary11 **where**
"unitary11 $M \longleftrightarrow$ mat_adj $M *_{mm} (1,0,0,-1) *_{mm} M = (1,0,0,-1)$"
definition unitary11_gen **where**
"unitary11_gen $M \longleftrightarrow$ ($\exists$ k::complex. $k \neq 0 \ \wedge$
mat_adj M $*_{mm}(1,0,0,-1)*_{mm}$ M = k $*_{sm}$ $(1,0,0,-1)$)"

Поново, дефиниција дозвољава комплексан фактор k, али се показује да једино реални фактори имају смисла.

Карактеризација $GU_{1,1}(\mathbb{C})$ је да она садржи све Мебијусове трансформације које фиксирају јединични круг.

lemma "mat_det $(A,B,C,D) \neq 0 \implies$ unitary11_gen (A, B, C, D) $\longleftrightarrow$
moebius_circline (mk_moebius A B C D) unit_circle = unit_circle"

Карактеризација генерализоване унитарне 1-1 матрице у координатама је дата са следећим лемама.

lemma "unitary11_gen $M \longleftrightarrow$ ($\exists$ a b k. **let** $M' = (a, b, \texttt{cnj}\ b, \texttt{cnj}\ a)$ **in**
$k \neq 0 \ \wedge$ mat_det $M' \neq 0 \ \wedge$
$(M = k *_{sm} M' \ \vee \ M = k *_{sm} (\texttt{cis}\ pi, 0, 0, 1) *_{sm} M')$"
lemma "unitary11_gen M $\longleftrightarrow$ ($\exists$ a b k. **let** $M' = (a, b, \texttt{cnj}\ b, \texttt{cnj}\ a)$ **in**
$k \neq 0 \ \wedge$ mat_det $M' \neq 0 \ \wedge \ M = k *_{sm} M'$)"

Приметимо да је прва лема садржана у другој леми. Ипак, било је лакше доказати прву лему јер добијамо матрице следећег облика $k*_{sm}(a,\ b,\ -cnj\ b,\ -cnj\ a)$ — геометријски, друга група трансформација комбинује прву групу са додатном централном симетријом.

Још једна важна карактеризација ових трансформација је коришћењем такозваног Блашке фактора. Свака трансформација је композиција Блашке фактора (рефлексије која неку тачку која је на јединичној кружници слика у нула) и ротације.

```
lemma assumes "k ≠ 0" "M' = (a, b, cnj b, cnj a)"
              "M = k *sm M'" "mat_det M' ≠ 0" "a ≠ 0"
  shows "∃ k' ϕ a'. k' ≠ 0 ∧ a' * cnj a' ≠ 1 ∧
        M = k' *sm (cis ϕ, 0, 0, 1) *mm (1, −a', −cnj a', 1)"
```

Изузетак је у случају када је $a = 0$ и онда се уместо Блашке фактора, користи реципроцитет (бесконачно замењује a' у претходној леми).

```
lemma assumes "k ≠ 0" "M' = (0, b, cnj b, 0)" "b ≠ 0" "M = k *sm M'"
      shows "∃ k' ϕ. k' ≠ 0 ∧ M = k' *sm (cis ϕ, 0, 0, 1) *mm (0, 1, 1, 0)"
```

Матрице $GU_{1,1}(\mathbb{C})$ се природно деле у две подгрупе. Све трансформације фиксирају јединични круг, али прва подгрупа се састоји од трансформација које мапирају јединични диск у самог себе (такозвани *аутоморфизми диска*), док се друга подгрупа састоји из трансформација које размењују јединични диск и његов комплемент. За дату матрицу, њена подгрупа се једино може одредити посматрајући знак детерминанте $M' = (a,\ b,$ `cnj` $b,$ `cnj` $a)$. Ако је само $M = (a_1, b_1, c_1, d_1)$ дато, а нису дати M', а ни k, онда је критеријум за утврђивање подгрупе вредност `sgn(Re` $((a_1 * d_1)/(b_1 * c_1)) - 1)$.

Приметимо да су све важне подгрупе овде описане једино у терминима алгебре. Формализовали смо и неке геометријске доказе који дају еквиваленту карактеризацију тврђењима које смо већ описали. Додатно, важи да су сви аналитички аутоморфизми диска једнаки композицији Блашке фактора и ротација (ипак, доказ се заснива на математичкој анализи, принципу максималног модула и Шварцовој леми – техникама које ми нисмо узимали у обзир). Чак и слабије тврђење да су сви Мебијусови аутоморфизми диска ове форме није још формално доказано (кључни корак је показати да ауто-

морфизми диска фиксирају јединични круг, а то је нешто што нисмо могли показати без детаљног испитивања топологије на чему тренутно радимо).

Сличне Мебијусове трансформације и класификација Мебијусових трансформација

Да би могли да класификујемо Мебијусове трансформације прво је било потребно увести пар нових појмова и анализирати њихова својства. Пре свега, анализирали смо фиксне тачке Мебијусових трансформација. Раније смо спомињали да су еуклидске сличности једине Мебијусове трансформације којима је ∞_{hc} фиксна тачка. Ипак, за доказе потребне у овом одељку морали смо да нешто више анализирамо фиксне тачке. Увели смо дефиницију фиксне тачке и дефиницију фиксне тачке која је коначна.

```
definition moebius_fixed_points where
  "moebius_fixed_points M γ ⟷ moebius_pt M γ = γ"
definition moebius_fixed_points_finite_rep where
  "moebius_fixed_points_finite_rep M γ ⟷
   (let (a,b,c,d) = ⌊M⌋_M
     in c * γ * γ - (a - d) * γ - b = 0)"
lift_definition moebius_fixed_points_finite ::
  "moebius ⇒ complex ⇒ bool" is
      moebius_fixed_points_finite_rep
```

За Мебијусову трансформацију могу постојати највише две фиксне тачке које могу бити и једнаке. Оне су обе коначне ако за коефицијент репрезентативне матрице важи $c \neq 0$; једна од њих је коначна, а једна бесконачна ако за коефицијенте важи $c = 0$ и $a \neq d$ и оне су обе једнаке бесконачно ако за коефицијенте важи $c = 0$ и $a = d$. Ово тврђење смо показали у наредним лемама.

```
lemma
  assumes "mat_det (a,b,c,d) ≠ 0" "c ≠ 0"
  shows "∃γ1γ2. moebius_fixed_points (mk_moebius a b c d) γ1 ∧
                moebius_fixed_points (mk_moebius a b c d) γ2 ∧
                γ1 ≠ ∞hc    ∧    γ2 ≠ ∞hc"
lemma
```

```
  assumes "mat_det (a, b, c, d) ≠ 0" "c = 0" "a ≠ d"
  shows "moebius_fixed_points (mk_moebius a b c d) ∞hc"
        "∃γ. moebius_fixed_points (mk_moebius a b c d) γ ∧ γ ≠ ∞hc"
lemma
  assumes "mat_det (a, b, c, d) ≠ 0" "c = 0" "a = d"
  shows "moebius_fixed_points (mk_moebius a b c d) ∞hc"
```

Ова тврђења није било тешко доказати, али су имала бројне кораке и случајеве које је требало размотрити и захтевала су показивање доста ситних алгебарских корака.

Потом дефинишемо како се за две дате Мебијусове трансформације може одредити слична Мебијусова трансформација. Овде уједно дајемо и дефиницију сличних матрица коју смо увели и чија својства смо показали у нашој основној теорији линеарне алгебре.

```
definition similarity_matrices where
  "similarity_matrices I M = I *mm M*mm mat_inv I"
definition moebius_mb_rep where
  "moebius_mb_rep I M = ⌈ similarity_matrices ⌊I⌋M ⌊M⌋M ⌉M"
lift_definition moebius_mb :: "moebius ⇒ moebius ⇒ moebius" is
  moebius_mb_rep
```

Сада је могуће дефинисати релацију сличности између две Мебијусове трансформације. Додатно, показали смо и да је ово и релација еквиваленције, тј. показано је да за релацију важи својство рефлексивности, симетричности и транзитивности и докази су били прилично директни и кратки.

```
definition similar where
  "similar M1 M2 ⟷ (∃I. moebius_mb I M1 = M2)"
lemma "similar M M"
lemma assumes "similar M1 M2"
  shows "similar M2 M1"
lemma assumes "similar M1 M2" "similar M2 M3"
  shows "similar M1 M3"
```

Врло важно тврђење је да је свака Мебијусова трансформација слична некој интегралној трансформацији (Еуклидској сличности). Доказивање овог

тврђења се свело на одређивање параметара Еуклидксе сличности, a и b, за произвољну Мебијусову трансформацију. Да би одредили ове параметре било је потребно одредити фиксне тачке Мебијусове трансформације и користити својства за фиксне тачке које смо нешто раније показали.

```
lemma
  "∃ k t. k ≠ 0 ∧ similar M (similarity a b)"
```

Веома важан параметар за Мебијусове трансформације јесте *инваријанта Мебијусових трансформација*. Она се дефинише коришћењем репрезентативне матрице за дату Мебијусову трансформацију, као однос између трага и детерминанте матрице. Потом, дефиницију са репрезентативног нивоа подижемо на ниво количничког типа.

```
definition similarity_invar_rep where
  "similarity_invar_rep M =
   (let M = ⌊M⌋_M in (mat_trace M)^2 / mat_det M - 4)"
lift_definition similarity_invar :: "moebius ⇒ complex" is
  similarity_invar_rep
```

Важно својство овог параметра је да су Мебијусове трансформације (које нису идентитет) сличне акко имају једнаке инваријанте.

```
lemma assumes "M₁ ≠ id_moebius" "M₂ ≠ id_moebius"
  shows
  "similarity_invar M₁ = similarity_invar M₂ ⟷ similar M₁ M₂"
```

Доказивање у једном смеру („ако су сличне имају једнаке инваријанте") било је једноставно и кратко. Међутим, супротан смер („ако имају једнаке инваријанте, онда су сличне") је представљао изазов, било је потребно раздвојити случајеве када је инваријанта једнака 0 и када је различита од 0, а потом у доказу су коришћене алгебарске трансформације, као и бројна својства релације сличности матрица. Оно што је интресантно је да је доказ у Schwerdtfeger-у значајно краћи (само пар редова), мада се мора рећи да је аутор нотирао све важне тачке доказа, али је у формалном доказу било неопходно ући у дубљу анализу и сваку од ових тачака детаљније испитати.

Коначно, стижемо до класификације Мебијусових трансформација која се управо карактерише коришћењем инваријанте. За Мебијусову трансформацију кажемо да је то пресликавање које је:

параболичко,	`similarity_invar` $= 0$,
	има само једну фиксну тачку
елиптичко,	инваријанта је реална и
	$-4 \leq$ `similarity_invar` < 0
правилно хиперболичко,	инваријанта је реална и
	`similarity_invar` > 0
неправилно хиперболичко,	инваријанта је реална и
	`similarity_invar` ≤ -4
локсодромичко,	инваријанта није реална

Дискусија

Визуелно, геометријски аргументи се често користе у доказима у уџбеницима. Као пример, ми ћемо демонстрирати доказ о очувању својства угла након примене Мебијусових трансформација на који се често може наићи у различитим књигама о овој теми (у овом поглављу ми ћемо пратити приступ Needham [8] који има за циљ да представи област без формалних детаља, па самим тим књига није стриктно формално писана али, ипак, овакав начин резоновања присутан је и код многих других аутора).

Прво важно питање је појам угла. Углови могу бити дефинисани између оријентисаних или неоријентисаних криви, а и сами углови могу бити оријентисани или неорјентисани. Needham дефинише угао између две криве на следећи начин: „Нека су S_1 и S_2 криве које се секу у тачки z. Као што је илустровано, ми можемо повући њихове тангенте T_1 и T_2 у тачки z. Угао између криви S_1 и S_2 у њиховој заједничкој тачки z је оштар угао α од T_1 до T_2. Значи овај угао α има знак који му је додељен: угао између S_2 и S_1 је минус илустровани угао између S_1 и S_2." То значи да је угао дефинисан само између неоријентисаних криви (и то је различито у односу на нашу дефиницију), али сам угао је оријентисан (а то је исто као и у нашој финалној дефиницији). У ранној фази наше формализације ми смо дефинисали и користили неоријентисани конвексан и оштар угао између два вектора.

definition "$\measuredangle_c$" **where** "$\measuredangle_c\ z_1\ z_2 \equiv$ `abs (`$\measuredangle\ z_1\ z_2$`)`"

definition acutize **where** "acutize α = (**if** $\alpha > \frac{\pi}{2}$ **then** π - α **else** α)"
definition "$\measuredangle_a$" **where** "$\measuredangle_a\ z_1\ z_2 \equiv$ acutize ($\measuredangle_c\ z_1\ z_2$)"

Како су наше кругоправе оријентисане од старта, ми смо показали да на оштар угао између два круга не утиче оријентација и да се он може изразити у терминима три тачке (тачке пресека и тачака које представљају центаре кругова).

lemma "$[\![z \neq \mu_1; z \neq \mu_2]\!] \Longrightarrow$
ang_circ_a $z\ \mu_1\ \mu_2\ p_1\ p_2$ = $\measuredangle_a\ (z - \mu_1)\ (z - \mu_2)$"

Функција ang_circ_a је дефинисана као оштар угао између два тангетна вектора (слично функцији ang_circ у нашој коначној формализацији).

Доказ да Мебијусова трансформација чува угао који стоји у уџбенику [8] се ослања на чињеницу да свака Мебијусова трансформација се може раставити на транслацију, ротацију, дилетацију и инверзију. Чињеница да транслације, ротације и дилетације чувају угао је узета као подразумевана и није доказивана (и да будемо искрени формализације ове чињенице није била тешка када смо успели да све појмове формално дефинишемо на одговарајући начин). Централни изазов је показати да инверзија чува углове, тј. доказати тврђење „Инверзија је антикомфорно пресликавање". Доказ се заснива на „чињеници да за било коју дату тачку z која није на кругу инверзије K, постоји тачно један круг који је ортогоналан на K и пролази кроз z у било ком правцу". Даље, доказ се наставља са „Претпоставимо да две криве S_1 и S_2 се секу у z, и да су њихове тангенте T_1 и T_2, а угао између њих је α. Да би сазнали шта се дешава са углом након инверзије у односу на K, заменимо S_1 и S_2 са јединственим круговима R_1 и R_2 ортогоналним на K који пролазе кроз z у истом смеру као што је и смер S_1 и S_2, тј., круговима чије тангенте у z су T_1 и T_2. Како инверзија у односну на K слика сваки од ових кругова на саме себе нови угао у $\tilde{z}$ је $-\alpha$. Крај."

У нашем ранијем покушају ми смо формализовали овај „доказ", али је ово захтевало веома велику количину уложеног труда у поређену са углађеним алгебарским доказом у нашој финалној формализацији. Прво, уџбеник је често врло непрецизан у томе да ли се користи „комплексна инверзија" или „геометријска инверзија" (тј. према нашим терминима које смо раније увели – да ли се користи реципроцитет или инверзија). У доказу из уџбеника

аутор користи инверзију у односу на произвољан круг K, али је довољно посматрати само реципроцитет (који је увек дат у односу на јединични круг). Формализација резоновања које је дато у уџбенику је већ дало прилично велике формуле, и било би још компликованије и монотоније (ако је уопште и могуће) завршити доказ коришћењем инверзије у односу на произвољни круг. На пример, једноставан реципроцитет круга са центром μ и радујусом r даје круг са центром $\tilde{\mu} = \mu/\texttt{cor}\ (|\mu|^2 - r^2)$, и радијусом $\tilde{r} = r/||\mu|^2 - r^2|$, и ова веза би била још комплекснија за произвољну Мебијусову трансформацију, ако би била записана у координатама, без коришћења појма матрица као што смо ми радили у нашој главној формализацији.

Формални запис тврђења о очувању угла је следећи.

```
lemma
  assumes "z ∈ circle μ1 r1" "z ∈ circle μ2 r2"
          "inv ` circle μ1 r1 = circle μ̃1 r̃1"
          "inv ` circle μ2 r2 = circle μ̃2 r̃2"
  shows "ang_circ_a z μ1 μ2 = ang_circ_a z̃ μ̃1 μ̃2"
```

Поред тога што недостаје дискусија за броје специјалне случајеве, у неформалном доказу недостаје и један значајан део. Наиме, лако је показати да $\tilde{z}$ је пресек R_1 и R_2 (то је пресек $\tilde{S}_1$ и $\tilde{S}_2$, које су слике S_1 и S_2 након инверзије), али показати да R_1 и $\tilde{S}_1$ и да R_2 и $\tilde{S}_2$ имају исту тангенту у $\tilde{z}$ је захтевало не тако тривијална израчунавања (тај доказ се заснива на чињеници да су центар μ_i' круга R_i, центар $\tilde{\mu}_i$ круга $\tilde{S}_i$, и $\tilde{z}$ колинеарни).

Једноставан аргумент симетрије који каже да су углови између два круга у њиховим двема различитим тачкама пресека једнаки поново није било једноставно формализовати.

```
lemma assumes "μ1 ≠ μ2" "r1 > 0" "r2 > 0"
              "{z1, z2} ⊆ circle μ1 r1 ∩ circle μ2 r2" "z1 ≠ z2"
  shows "ang_circ_a z1 μ1 μ2 = ang_circ_a z2 μ1 μ2"
```

Ми смо показали ову лему тек након примене „бгно" резоновања и померањем слике тако да центри два круга који се посматрају буду на x-оси.

У доказу смо идентификовали бројне дегенерисане случајеве који су морали да се анализирају одвојено. Прво смо морали да покажемо да кругови који се секу могу имати исти центар (тј. да μ_1=μ_2) само ако су једнаки и

тада је оштар угао између њих једнак 0. Са друге стране, ако су оба центра колинеарна са пресечном тачком z (тј. ако важи `collinear` μ_1 μ_2 z), два круга се додирују (било споља или изнутра), и опет је оштар угао једнак 0.

Постојање круга R_i који је ортогоналан на јединичну кружницу и који има исту тангенту у датој тачки z као и дати круг са центром μ_i је дато следећом лемом (заправо у леми се даје центар μ_i' тог новог круга).

```
lemma
  assumes "⟨μᵢ - z, z⟩ ≠ 0"
          "μᵢ' = z + (1 - z*cnj z) * (μᵢ - z) / (2 * ⟨μᵢ - z, z⟩)"
  shows "collinear z μᵢ μᵢ'" "z ∈ ortho_unit_circ μᵢ'"
```

Аналитички израз је открио још неке дегенерисане случајеве. Бројилац може бити нула једино ако се кругови секу на јединичној кружници (тј. када је $z *$ `cnj` $z = 1$). У том случају, доказ из уџбеника се не може применити јер је $\mu_1' = \mu_2' = z$, и кругови R_1 и R_2 се не могу конструисати (они су празни кругови). Случај када је именилац једнак нули (било за μ_1' или μ_2') је такође дегенерисан. Ово се дешава када су вектори $\mu_i - z$ и z ортогонални. Геометријски, у том случају се круг R_i дегенерише у праву (што и није проблем у проширеној комплексној равни, али јесте проблем у поставци која важи у оригиналном доказу која се налази у обичној комлексној равни). Зато, овај специјалан случај мора да се анализира одвојено. Тако је наша формална анализа брзо показала да једноставно тврђење у Needham да „за дату било коју тачку z која није на кругу инверзије K, постоји тачно један круг који је ортогоналан на K и пролази кроз z у било ком задатом правцу" није тачна у многим случајевима.

Закључци и даљи рад

У овом раду смо показали неке елементе наше формализације геометрије проширене комплексне равни $\overline{\mathbb{C}}$ коришћењем комплексне пројективне равни, али и Риманове сфере. Формализовали смо аритметичке операције у $\overline{\mathbb{C}}$, размеру и дворазмеру, тетивну метрику у $\overline{\mathbb{C}}$, групу Мебијусових трансформација и њихово дејство на $\overline{\mathbb{C}}$, неке њене специјалне подгрупе (Еуклидске сличности, ротације сфере, аутоморфизме диска), кругоправе и њихову везу са круговима и правама, тетивном метриком, Римановом сфером, јединственост кругоправи, дејство Мебијусових трансформација на кругоправе, типове и кардинал-

ност скупа кругоправе, оријентисане кругоправе, однос између Мебијусових трансформација и оријентације, својство очувања угла након дејства Мебијусових трансформација итд. Наша тренутна теорија има око 12,000 линија Isabelle/HOL кода (сви докази су структурни и записани су у језику за доказе Isabelle/Isar и наши ранији покушаји су замењени краћим алгебарским доказима и нису укључени у финалну формализацију), око 125 дефиниција и око 800 лема.

Кључан корак у нашој формализацији је била одлука да се користи алгебарска репрезентација свих важних објеката (вектора хомогених координата, матрица за Мебијусове трансформације, Хермитеове матрице за кругоправе итд.). Иако ово није нов приступ (на пример, Schwerdtfeger's класична књига [10] прати овај приступ прилично конзистентно), он ипак није тако уобичајен у литератури (и у метеријалима курсева који се могу наћи на интернету). Уместо њега преовладао је геометријски приступ. Ми смо покушали да пратимо такву врсту геометријског резоновања у раној фази нашег рада на овој теми, али смо наишли на бројне потешкоће и нисмо имали много успеха. На основу овог искуства, закључујемо да увођење моћне технике ленеарне алгебре омогућава значајно лакши рад на формализацији него што је то случај када се користи геометријско резоновање.

Може се дискутовати да ли у неким случајевима геометријски аргументи дају боље објашњење неких теорема, али када се посматра само доказивање тврђења, алгебраски приступ је јасно супериорнији. Ипак, да би имали везу са стандардним приступом у коме се користи геометријска интуиција увели смо неколико додатних дефиниција (које су више геометријске или више алгебарске) и морали смо показати да су ове дефиниције еквивалентне. На пример, када је дефиниција угла дата само коришћењем алгебарских операција на матрицама и њиховим детерминантама, својство очувања угла је било веома лако показати, али због образовне сврхе ово постаје значајно једино када се та дефиниција споји са стандардном дефиницијом угла између криви (тј. њихових тангетних вектора) — у супротном, формализација постаје игра са симболима који немају никакво значење.

Још један важан закључак до ког смо дошли је да у формалним документима треба што чешће избегавати анализу случајева и екстензије које омогућавају резоновање без анализе случајева треба што чешће користити (нпр. било је много боље користити хомогене координате уместо једне одвојене тач-

ке бесконачно коју би морали засебно да анализирамо у сваком тврђењу или дефиницији; слично, било је много лакше радити са кругоправама него разликовати случај прави и кругова, итд.). Увођење два модела истог концепта (на пример, у нашем случају, хомогених координата и Риманове сфере) такође помаже, јер су неки докази лакши у једном моделу, а неки у другом.

У принципу наши докази нису дугачки (15-20 линија у просеку). Ипак, понекад је било потребно изводити веома досадне закључке, поготову када се пребацивало са реалних на комплексне бројеве и обратно (коришћењем функција за конверзију `Re` и `cor`). Ове конверзије се углавном и не појављују у неформалном тексту и добро би дошла нека аутоматизација оваквог закључивања. Аутоматизација система Isabelle је прилично моћна у резоновању једнакости у којима су обични комплексни бројеви и ту смо често користили метод `(simp add: field_simps)` (са неким мањим изузецима), али када су у питању неједнакости, аутоматизација није била добра и много тога смо морали да показујемо ручно, корак по корак, а оваква тврђења се често сматрају веома тривијалним у неформалном тексту.

У нашем даљем раду планирамо да користимо ове резулатате у формализацији нееуклидских геометрија и њихових модула (посебно, сферични модел елиптичке геометрије, Поинкареов диск модел и модел горње полуравни хиперболичке геометрије).

2.3 Формализација Поинкареовог диск модела

Циљ је показати да Поинкареов диск модел представља модел свих аксиома Тарског са изузетком Еуклидове аксиоме која у овом моделу није тачна и не важи. Потребно је дефинисати основне појмове, тј. релацију између и растојање и показати да дефинисани појмови задовољавају нека својства. Нажалост, због разлога које ћемо касније изложити, нисмо успели да формално покажемо све аксиоме. Ипак, изложићемо нека интересантна својства и закључке до којих смо дошли.

Прво, дефинишемо тип података којим се представљају тачке Поинкареовог диск модела, односно тачке које припадају унутрашњости јединичног диска.

```
typedef unit_disc = "{z::complex_homo.  in_ocircline ounit_circle
z}"
```

Специјална тачка која припада унутрашњости је и 0. Иако већ постоји дефинисана 0_h било је потребно дефинисани и 0_u, односно нулу која припада јединичном диску. Иако тривијано важи да 0_h припада јединичном диску, приликом дефинисања појмова или задавања лема ово није познато и систем може пријављивати грешку јер тип није одговарајући. Управо зато, потребно је дати још једну дефиницију за 0.

```
lift_definition zero_homo_unit :: unit_disc ("0_u") is zero_homo
```

Растојање

Растојање над тачкама јединичног диска се дефинише исто као и растојање над тачкама проширене комплексне равни.

```
lift_definition dist_poincare :: "unit_disc ⇒ unit_disc ⇒ real" is
   dist_homo
```

Релација између

Дефиниција релације између се ослања на већ дефинисани појам `cross_ratio` за који су већ показана бројна својства. Релација између се прво дефинише над проширеном комплексном равни, а потом се подиже на тип `unit_disc`.

```
definition between where
   "between z1 z2 z3 ⟷ ((z1 = z2 ∧ z2 = z3) ∨
       (let CR = to_complex(cross_ratio z1 z2 z3 (inversion_homo z2))
        in
        is_real CR ∧ Re CR ≤ 0))"
lift_definition between_poincare ::
   "unit_disc ⇒ unit_disc ⇒ unit_disc ⇒ bool" is between
```

Као што се може видети у дефиницији разликујемо два случаја. Код Тарског, за тачке које су једнаке такође важи релација између, односно у моделу Тарског је допуштено да тачке буду једнаке. Како `cross_ratio` није дефинисан када су три тачке једнаке, то случај једнаких тачака одвајамо посебно.

Ако све четири тачке припадају једној кругоправи, онда ће двострука размера за те четири тачке бити реална. Неформално, тачке за које важи релација између припадају једној кругоправи и то не било каквој кругоправи, већ оној која је нормална на јединичну кружницу. Кругоправе нормалне на јединичну кружницу могу бити кругови нормални на јединичну кружницу или праве које пролазе кроз координатни почетак. Додатно, инверзија у односу на јединични круг било које од ове три тачке ће такође припадати кругоправи нормалној на јединичну кружницу. Зато, у двоструку размеру уврстимо три тачке и инверзију једне од њих и за ове четири тачке двострука размера мора бити реална.

Додатно, ако је дворазмера негативна онда је друга тачка између прве и треће, а у супротном није. Ако је дворазмера нула онда су две од три тачке једнаке и тада исто важи релација између.

Наравно, да би потврдили да је овако дефинисана релација заиста релација између потребно је доказати аксиоме Тарског за овај модел.

Мебијусове трансформације и релација између

Не посматрају се све Мебијусове трасформције већ само оне које сликају унутрашњост диска у унутрашњост диска. Раније смо видели да $GU_{1,1}(\mathbb{C})$ је група оних Мебијусових трансфорамација које фиксирају јединични круг, али да и ту постоје две групе трансфорамција, тј. оне трансфорамције које сликају унутрашњост круга у унутрашњост (и које су у овом конеткту значајне) и друга група трансформација које размењују унутрашњост и спољашњост диска.

Дефинисићемо својство којим се описују оне Мебијусове трансформације које сликају унутрашњост диска у унутрашњост диска. И ова дефиниција се одвија у два корака, прво се дефинише над матрицама, а потом се подигне на тип `moebius`.

```
definition Unitary11_gen_direct_rep where
   "Unitary11_gen_direct_rep M ⟷
   (let (A, B, C, D) = ⌊M⌋_M
   in unitary11_gen (A, B, C, D) ∧ (B = 0 ∨ Re ((A*D)/(B*C)) > 1))"

lift_definition Unitary11_gen_direct :: "moebius ⇒ bool" is
```

Unitary11_gen_direct_rep

Може се показати следеће тврђење

lemma
"moebius_ocircline M ounit_circle = ounit_circle $\longleftrightarrow$
Unitary11_gen_direct M"

односно, унутрашњост диска је очувана ако и само ако Мебијусова трансформација задовољава својство Unitary11_gen_direct.

Сада се може дефинисати тип, тј. нова група Мебијусових трансформација које чувају унутрашњост диска

typedef moebius_unitary = "{M::moebius. Unitary11_gen_direct M}"

Слично као и раније, Мебијусове трансформације ове групе су дате као дејство над тачкама јединичног диска. Ипак, за ову дефиницију се може искористити дефиниција Мебијусових трансформација над тачкама проширене комплексне равни, тј. потребно је подићи ту дефиницију за тип mobius_unitary и unit_disc.

lift_definition moebius_pt_poincare ::
"moebius_unitary $\Rightarrow$ unit_disc $\Rightarrow$ unit_disc" **is** moebius_pt

Ова дефиниција ствара обавезу да се покаже

$\bigwedge$ M z.
$[\![$ Unitary11_gen_direct M; in_ocircline ounit_circle z $]\!]$
$\Longrightarrow$ in_ocircline ounit_circle (moebius_pt M z)

што се лако показује у неколико корака коришћењем горе дате леме.

Поред ових дефинција интересантно је дефинисати и инверзну трансформацију.

lift_definition moebius_inv_poincare::
"moebius_unitary $\Rightarrow$ moebius_unitary" **is** moebius_inv

И ова дефиниција ствара обавезу да се покаже да је инверзна трансформација такође Unitary11_gen_direct што се показује коришћењем једноставних алгебарских трансформација над матрицама.

Веома важно тврђење које смо показали је да Мебијусове трансформације које чувају унутрашњост диска, такође чувају и релацију између. Ово тврђење се веома лако показује јер смо раније већ показали да Мебијусове трансформације чувају дворазмеру. Ипак, било је потребно показати и да је очувана инверзија у односу на јединични круг. У општем случају инверзија није очувана, али за Мебијусове трансформације које чувају унтрашњост јединичног диска, јесте.

lemma
assumes "Unitary11_gen_direct M"
shows "moebius_pt M (inversion_homo z) =
inversion_homo (moebius_pt M z_2)"

lemma
assumes "z_1' = moebius_pt_poincare M z_1"
"z_2' = moebius_pt_poincare M z_2"
"z_3' = moebius_pt_poincare M z_3"
"between_poincare z_1 z_2 z_3"
shows "between_poincare z_1' z_2' z_3'"

Поред ових показано је још пуно помоћних тврђења, а издвојићемо неколико интересантнијих. Једна од често коришћених чињеница у доказима је да инверзна слика тачке јединичног диска не припада јединичном диску.

lemma
assumes "$x \in$ unit_disc"
shows "inversion_homo $x \notin$ unit_disc"

Такође, тачке које се налазе у јединичном диску су по модулу мање од 1.

lemma
assumes "in_ocircline ounit_circle z"
shows "cmod (to_complex z) < 1"

Важно тврђење је да свака Мебијусова трансформација која је композиција ротације и блашке фактора чији параметар је по модулу мањи од 1 је трансформација која слика унутрашњост диска у унутрашњост диска.

```
lemma
  assumes "cmod a < 1" "a * cnj a ≠ 1" "a ≠ 0"
          "M = rotation_moebius φ + blaschke a"
  shows "Unitary11_gen_direct M"
```

Прво се покаже да се било које две тачке могу сликати у 0_u и у неку тачку на реалној оси, што је тврђење дато у следећој леми.

```
lemma
  "∃ a M. 0u = moebius_pt_poincare M z1 ∧
           is_real (to_complex (Rep_unit_disc a)) ∧
           a = moebius_pt_poincare M z2"
```

Доказ овог тврђења се састоји из два корака. Прво се прва тачка слика у 0_u трансформацијом M' `= blaschke (to_complex` z_1), а потом се врши ротација за угао који одговара тачки која се добила пресликавањем тачке z_2 трансформацијом M'. Како је ротација око координатног почетка, то се 0_u слика у 0_u, а друга тачка се ротацијом слика на реалну осу и тиме управо се и добијају жељене слике тачака. У доказу се користи раније показана чињеница да композиција ротације и блашке фактора чији параметар имао модуо мањи од 1, Мебијусова трансформација која чува унутрашњост диска. Иако је идеја доказа једноставна, постоји неколико случајева које треба размотрити (ако су тачке једнаке или ако је већ нека тачка једнака 0_h), а и у доказу постоји много ситних корака које је требало показати. Зато је доказ готово 300 линија дугачак.

Потом се може показати да ако за три тачке важи релација између, онда се оне могу сликати на реалну осу (а једна од њих у 0). У овом доказу се користи претходно тврђење и чињеница да ако је дворазмера реална, ако су њена три параметра реална, онда и четврти параметар мора бити реалан.

```
lemma
  assumes "between_poincare z1 z2 z3"
  shows "∃ a b M. 0u = moebius_pt_poincare M z1 ∧
        is_real (to_complex (Rep_unit_disc a)) ∧
        a = moebius_pt_poincare M z2 ∧
        is_real (to_complex (Rep_unit_disc b)) ∧
        b = moebius_pt_poincare M z3"
```

Коришћењем свих претходних тврђења може се користити резоновање „без губитка на општости". Наиме, тврђење се може показати на реалној оси на којој је лакше доказати да неко тврђење важи, а онда се може уопштити да важи за било које три тачке за које важи релација између у Поинкареовом диск моделу.

Аксиоме конгруенције

Аксиоме конгруенције се тривијално показују јер су својства растојања већ раније показана и само је потребно позвати се на та својства.

```
lemma ax_1:
   "dist_poincare z_1 z_2 = dist_poincare z_2 z_1"
lemma ax_2:
   assumes "dist_poincare x y = dist_poincare z z"
   shows "x = y"
lemma ax_3:
   assumes "dist_poincare x y = dist_poincare z u"
           "dist_poincare x y = dist_poincare v w"
   shows "dist_poincare z u = dist_poincare v w"
```

Аксиоме релације између

Две аксиоме ове групе се тривијално показују. Аксиома идентитета се показује контрадикцијом. Аксиома горње димензије тврди да постоје три тачке за које не важи релација између. Доказује се тако што се одаберу такве три тачке, на пример, 0_u, $1/2$ и $ii/2$, покаже се да све три тачке заиста припадају Поинкареовом диск моделу, али да дворазмера није реална, па самим тим и релација између не важи.

```
lemma ax_4:
   assumes "between_poincare x y x"
   shows "x = y"
lemma ax_6:
   "∃ a b c. ¬ between_poincare a b c ∧ ¬ between_poincare b c a
   ∧ ¬ between_poincare c a b"
```

Овој групи аксиома припада аксиома континуитета.

```
lemma ax7:
  assumes "∃ a. ∀ x. ∀ y. ϕ x ∧ ψ y ⟶ between_poincare a x y"
  shows "∃ b. ∀ x. ∀ y. ϕ x ∧ ψ y ⟶ between_poincare x b y"
```

Да би доказали ово тврђење било је потребно показати пуно помоћних лема. Доказ се започиње једноставним испитивањем случајева у којима тврђење тривијано важи. Први случај је да не постоје ни x, ни y такви да важи $\phi\ x$ и $\psi\ y$. Следећи случај је да не постоји x такво да важи $\phi\ x$. Трећи случај је да не постоји y такво да важи $\psi\ y$. И последњи тривијалан случај је да постоји b такво да важи $\phi\ b$ и $\psi\ b$.

Доказивање општег случаја се састоји из неколико корака. Прво се све тачке сликају на реалну осу на којој је тврђење лакше показати. Оправданост овог пресликавања смо видели раније. Потом је потребно показати једно тврђење за релацију између које важи на реалној оси. То тврђење тврди да тачке које су у релацији између задовољавају неки поредак.

```
lemma
  assumes "is_real (to_complex (Rep_unit_disc z))"
          "is_real (to_complex (Rep_unit_disc u))"
          "is_real (to_complex (Rep_unit_disc v))"
          "rz = Re (to_complex (Rep_unit_disc z))"
          "ru = Re (to_complex (Rep_unit_disc u))"
          "rv = Re (to_complex (Rep_unit_disc v))"
  shows "between_poincare z u v ⟷
          (rz ≤ ru ∧ ru ≤ rv) ∨
          (rz ≥ ru ∧ ru ≥ rv)"
```

Потом показујемо аксиому континуитета за реалне бројеве:

```
lemma
  assumes "∀ x::real. ∀ y::real. ϕ x ∧ ψ y ⟶ x < y"
          "∃ x. ϕ x" "∃ y. ψ y"
  shows "∃ b. ∀ x. ∀ y. ϕ x ∧ ψ y ⟶ (x ≤ b ∧ b ≤ y)"
```

Ово тврђење се једноставно доказује коришћењем својства супремума. Наиме, посматра се скуп P = "{x::real. ϕ x}". Докаже се да супремум овог скупа управо испуњава тражено тврђење.

Комбинујући последње две леме, показује се и тврђење аксиоме.

Преостале аксиоме Тарског нисмо успели да докажемо. Узмимо Пашову аксиому у разматрање.

lemma ax_5:
  assumes "between_poincare x u z"
    "between_poincare y v z"
  shows "$\exists$ a. between_poincare u a y $\wedge$ between_poincare v a x"

Да би доказали ово тврђење потребно је одредити x које испуњава тражена својства. То значи да треба одредити x као пресек две кругоправе нормалне на јединичну кружницу. Прва кругоправа садржи тачке u и y, а друга кругоправа садржи тачке v и x. То значи да треба одредити пресек два круга. То је кадратна једначина и резултат пресека ће бити корен неког великог израза. Чак и ако би једну кругоправу сликали у праву кроз координатни почетак, то би опет био пресек праве и круга што је опет квадратна једначина и решење је опет комплексан израз. Први изазов је одредити који од два пресека заиста припада диску и јесте тражени пресек. Потом је потребно комплексан израз који садржи квадртни корен уврстити у једначину дворазмере, и проверити да ли је добијени израз реалан и негативан. Ово се показало као веома тежак задатак. Наиме, није могуће лако се ослободити корена, а изрази који се добијају су веома комплексни и тешко је доћи до жељених закључака. Зато, нажалост, овај доказ остаје незавршен.

Исти су проблеми и у другим доказима. Такође је потребно пронаћи пресеке кругоправих, а онда уврстити то у вектор или матрицу и резоновати са тим комплексним изразима.

У многим уџбеницима смо наишли на тврђење да се тривијално показује да је Поинкареов диск модел модел аксиома Тарског изузимајући Еуклидову аксиому. Ипак, ни у једном уџбенику, за сада, нисмо пронашли доказ овог тврђења. Нама није успело да самостално доказ и довршимо, а сматрамо да сам доказ није тријвијалан.

Литература

[1] Clemens Ballarin. Interpretation of locales in isabelle: Theories and proof contexts. In *Mathematical Knowledge Management*, pages 31–43. Springer, 2006.

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

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

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

[5] E Hille. Analytic function theory (chelsea, new york). *Vol. II*, page 375, 1973.

[6] Brian Huffman and Ondřej Kunčar. Lifting and transfer: A modular design for quotients in isabelle/hol. In *Certified Programs and Proofs*, pages 131–146. Springer, 2013.

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

[8] Tristan Needham. *Visual complex analysis*. Oxford University Press, 1998.

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

[10] Hans Schwerdtfeger. *Geometry of complex numbers: circle geometry, Moebius transformation, non-euclidean geometry*. Courier Corporation, 1979.

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, _____

_____