Формализација различитих модела геометрије и примене у верификацији аутоматских доказивача теорема

Данијела Симић
Ментор: др Филип Марић

Математички факултет
Универзитет у Београду

8.08.2017.

Увод

- Различите геометрије:
  - Еуклидска геометрија
  - Хиперболичка геометрија

- Различити приступи изучавања:
  - Синтетички приступ:
    - аксиоматски систем Хилберта
    - аксиоматски систем Тарског
  - Аналитички приступ:
    - у Декартовој координатној равни
    - у комплексној равни

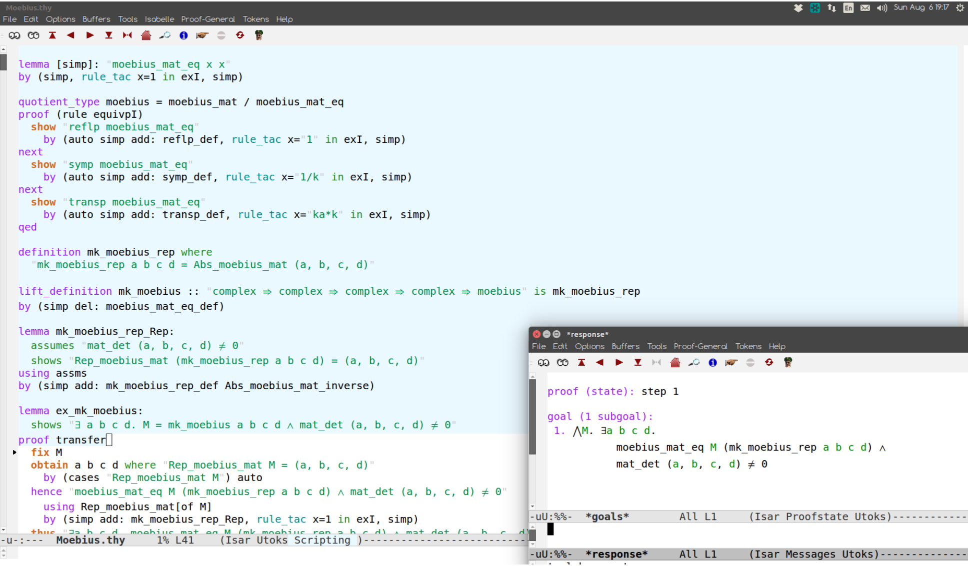
Доказивање у геометрији

- Грешке у математичким доказима.
- Механички провериви докази.
- Интерактивни доказивачи теорема.
- Аутоматски доказивачи теорема.

Интерактивни доказивачи теорема

- Карактеристике интерактивних доказивача теорема.
- Важни резултати:
  - Основна теорема алгебре
  - Геделова теорема непотпуности
  - многе теореме реалне анализе
  - формални доказ теореме о обојивости графа са 4 боје
  - формално верификован компилатор за програмски језик C
  - формално верификован оперативни систем
  - прва група Хилбертових аксиома и последице
  - велики делови књиге Тарског

Isabelle/HOL



Аутоматско доказивање геометријских теорема

- Алгебарски доказивачи – Вуов метод и метод Гребнерових база.
- Синтетички доказивачи.
- Полусинтетички доказивачи – метод површина, метод пуног угла, метод запремине.
- Везе између интерактивних и аутоматских доказивача.

Мотивација и циљеви

- Верификација аутоматских доказивача теорема.

- Формализација мета–теорије потребне да се искаже и докаже коректност алгебарских метода.

- Развој и прилагођавање алгебарских метода.

Циљеви формализације геометрије Декартове равни

- Формализација Декартове координатне равни.
- Различите дефиниције су еквивалентне.
- Стандардна геометрија координатне равни представља модел аксиоматског система Тарског.
- Декартова координатна раван задовољава већину аксиома Хилберта.
- Упоредити ове две формализације.

Основни појмови

- Тачке: **type_synonym** $\texttt{point}^{ag} \;=\;$ "$real \times real$"
- Распоред тачака: $\mathcal{B}(A, B, C)$

Релација *између* у геометрији Тарског

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

- Релација подударно: $AB \cong_t CD$

Релација подударно

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

Права

- $Ax + By + C = 0 \ (kAx + kBy + kC = 0, \ k \neq 0)$
- **typedef** line_coeffs^{ag} $=$
  "$\{((A :: real), (B :: real), (C :: real)). \ A \neq 0 \vee B \neq 0\}$"
- **definition** "$l_1 \approx^{ag} l_2 \longleftrightarrow$
  $(\exists \ A_1 \, B_1 \, C_1 \, A_2 \, B_2 \, C_2.$
  $\lfloor l_1 \rfloor_{R3} = (A_1, B_1, C_1)) \ \wedge \ \lfloor l_2 \rfloor_{R3} = (A_2, B_2, C_2) \ \wedge$
  $(\exists k. \ k \neq 0 \wedge A_2 = k \cdot A_1 \wedge B_2 = k \cdot B_1 \wedge C_2 = k \cdot C_1))$"

Права (тип `line`^{ag}) се дефинише коришћењем `quotient_type` команде као класа еквиваленције над релацијом $\approx^{ag}$.

Инциденција

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

- Да би доказали да је релација заснована на представницима класе добро дефинисана, мора бити доказано да ако се изаберу други представници класе, рецимо A', B', и C' важи $A' \cdot x + B' \cdot y + C = 0$:

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

Права – афина дефиниција

- Вектор: **type_synonym** $\texttt{vec}^{ag} = $ "$real \times real$".
- **typedef** $\texttt{line\_point\_vec}^{ag} =$
  "$\{(p :: \texttt{point}^{ag}, v :: \texttt{vec}^{ag}).\ v \neq (0,0)\}$"
- **definition** "$l_1 \approx^{ag} l_2 \longleftrightarrow (\exists p_1\, v_1\, p_2\, v_2.$
  $\lfloor l_1 \rfloor_{R3} = (p_1, v_1) \wedge \lfloor l_2 \rfloor_{R3} = (p_2, v_2) \wedge$
  $(\exists k m.\ v_1 = k \cdot v_2 \wedge p_2 = p_1 + m \cdot v_1))$"

Изометрије

- Транслација: **definiton** "$\mathtt{transp}^{ag}$ (v_1, v_2) $(x_1, x_2) = (v_1 + x_1, v_2 + x_2)$"
- Ротација: **definition** "$\mathtt{rotp}^{ag}$ α $(x, y) = ((\cos\alpha) \cdot x - (\sin\alpha) \cdot y, (\sin\alpha) \cdot x + (\cos\alpha) \cdot y)$"

Инваријантност

Изометрије чувају основне релације (као што су *између* и *подударно*).

- **lemma** "$\mathcal{B}_T^{ag}$ A B $C \longleftrightarrow \mathcal{B}_T^{ag}$ $(\mathtt{transp}^{ag}$ v $A)$ $(\mathtt{transp}^{ag}$ v $B)$ $(\mathtt{transp}^{ag}$ v $C)$"

Изометрије

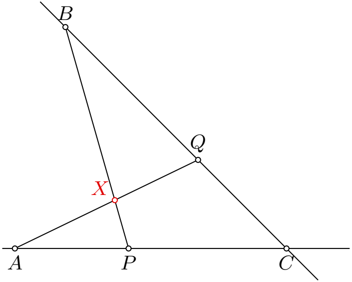
Коришћењем изометријских трансформација значајно се упрошћава формализација.

- Коришћена је техника без губитка на општости:
  definiton "inv $P\ t \longleftrightarrow (\forall\ A\ B\ C.\ P\ A\ B\ C \longleftrightarrow P\ (tA)\ (tB)\ (tC))$"

  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 $(\texttt{transp}^{ag}\ v)$"
  "$\forall \alpha.$ inv P $(\texttt{rotp}^{ag}\ \alpha)$"
  shows "$\forall A\, B\, C.\ \mathcal{B}_T^{ag}\ A\ B\ C \longrightarrow P\ A\ B\ C$"

Пашова аксиома

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



- Алгебраским трансформацијама се одреде координате тачке X и покажу се тражена својства.
- Коришћене су изометријске трансформације.

Пашова аксиома – елементарна својства

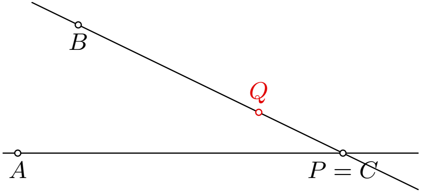
Да би се доказала Пашова аксиома коришћена су елементарна својства:

- Симетрија: **lemma** "$\mathcal{B}_T^{ag}\ A\ B\ C \longrightarrow \mathcal{B}_T^{ag}\ C\ B\ A$"
- Транзитивност:
  lemma "$\mathcal{B}_T^{ag}\ A\ X\ B\ \wedge\ \mathcal{B}_T^{ag}\ A\ B\ Y \longrightarrow \mathcal{B}_T^{ag}\ X\ B\ Y$"

Коришћен је проширен систем аксиома Тарског.

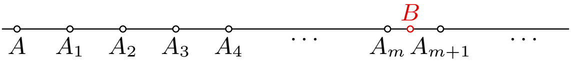
Пашова аксиома – специјални случајеви

- Прва група: једнаке тачке, $P = C$ или $Q = C$



- Друга група: колинеарне тачке, $\mathcal{B}_t(A, B, C)$ или $\mathcal{B}_t(B, A, C)$ или $\mathcal{B}_t(B, C, A)$

Архимедова аксиома



- **definition** "congruentl $l \longrightarrow$ length $l \geq 3 \;\wedge$
  $\forall i.\; 0 \leq i \;\wedge\; i + 2 <$ length $l \longrightarrow$
  $(l \;!\; i)(l \;!\; (i+1)) \cong_h (l \;!\; (i+1))(l \;!\; (i+2)) \;\wedge$
  $\mathcal{B}_h((l \;!\; i), (l \;!\; (i+1)), (l \;!\; (i+2)))$"
- **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: коришћењем Архимедовог правила за реалне бројеве се показује да постоји t: $t \cdot d_{ag}^2 \; A \; A_1 > d_{ag}^2 \; A \; B$
- Користи се индукција за изградњу листе тачака.

Закључци

- Представили смо добро изграђену формализацију Декартове геометрије равни у оквиру система *Isabelle/HOL*.
- Формално је доказано да Декартова координатна раван задовољава све аксиоме Тарског и већину аксиома Хилберта.
- Наше искуство је да доказивање да наш модел задовољава једноставне Хилбертове аксиоме лакше него доказивање да модел задовољава аксиоме Тарског.
- Проблем приликом дефинисања и рада са угловима.
- Најважнија техника коришћена да се упросте докази "без губитка на општости" и коришћење изометријских трансформација.
- Формализација аналитичке геометрије се заснива на аксиомама реалних бројева и у многим доказима су коришћена својства реалних бројева (својство супремума, тактика заснована на Гребнеровим базама).

Циљеви формализације геометрије комплексне равни

- Формализовати теорију проширене комплексне равни, њених објеката и њених трансформација.
- Спојити бројне приступе које можемо срести у препорученој литератури.
- Анализирати и формално доказати све случајеве који често остану недовољно истражени јер их више различитих аутора сматра тривијалним.
- Дискутовати односе између два приступа у формализацији (геометријски и алгебарски) као и њихове предности и мане.
- Анализирати технике које се користе у доказима, као и могућност коришћења аутоматизације.
- Посматрати да ли је доказе лакше извести у моделу Риманове сфере или у моделу хомогених координата.
- Показати да аксиоме Тарског важе у Поенкареовом диск моделу.

- Комплексни бројеви, вектори и матрице у $\mathbb{C}^2$.
- Хермитска матрица: **definition** `hermitean` **where** "`hermitean` H $\longleftrightarrow$ `mat_adj` H = H"
- Унитарна матрица: **definition** `unitary` **where** "`unitary` M $\longleftrightarrow$ `mat_adj` M $*_{mm}$ M = `eye`"
- Проширена комплексна раван, $\overline{\mathbb{C}}$.
- Хомогене координате: $z = \frac{z'}{z''}$

  definition $\approx_{C2}$ :: "$\texttt{C2\_vec}_{\neq 0} \Rightarrow \texttt{C2\_vec}_{\neq 0} \Rightarrow \texttt{bool}$" **where**
  "$z_1 \approx_{C2} z_2 \longleftrightarrow (\exists\ (\texttt{k::complex}).\ \texttt{k} \neq 0 \wedge \lfloor z_2 \rfloor_{C2} = \texttt{k} *_{sv} \lfloor z_1 \rfloor_{C2})$"

  quotient_type $\texttt{complex}_{hc}$ = $\texttt{C2\_vec}_{\neq 0}$ / $\approx_{C2}$

- Бесконачно далека тачка у хомогеним координатама:

  definition `inf_hc_rep` :: "$\texttt{C2\_vec}_{\neq 0}$ **where**
  `inf_hc_rep` = $\lceil (1,0) \rceil^{C2}$"
  lift_definition ∞_{hc} :: "$\texttt{complex}_{hc}$" **is** `inf_hc_rep`

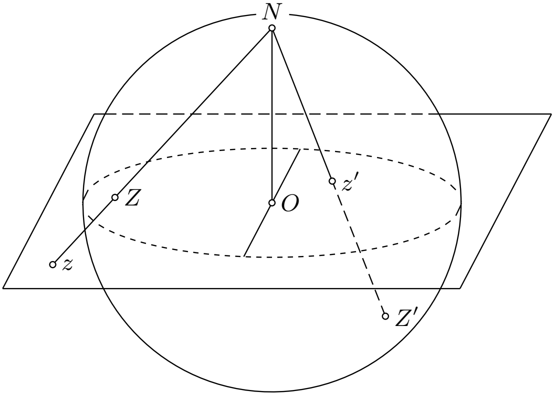
- Аритметичке операције над хомогеним координатама:

  definition plus_hc_rep ::
  "$\texttt{C2\_vec}_{\neq 0} \Rightarrow \texttt{C2\_vec}_{\neq 0} \Rightarrow \texttt{C2\_vec}_{\neq 0}$"
  where "plus_hc_rep z w =
  (**let** $(z_1, z_2) = \lfloor z \rfloor_{C2}$; $(w_1, w_2) = \lfloor w \rfloor_{C2}$
  in $\lceil (z_1 * w_2 + w_1 * z_2, z_2 * w_2) \rceil^{C2}$)"

  lift_definition $+_{hc}$ ::
  "$\texttt{complex}_{hc} \Rightarrow \texttt{complex}_{hc} \Rightarrow \texttt{complex}_{hc}$" **is** plus_hc_rep

- Дворазмера је дефинисана над 4 тачке (z, u, v, w) као $\frac{(z-u)(v-w)}{(z-w)(v-u)}$ – cross_ratio z u v w.

Стереографска пројекција



Стереографска пројекција

- **definition** `stereographic_rep ::`
  `"riemann_sphere` $\Rightarrow$ `C2_vec`$_{\neq 0}$`"` **where**
  `"stereographic_rep` M `=`
  `(`**let** `(`x`,` y`,` z`) =` $\lfloor M \rfloor_{R3}$ **in**
  if `(`x`,` y`,` z`)` $\neq$ `(0, 0, 1)` **then** $\lceil (x + i * y, 1 - z) \rceil^{C2}$
  else $\lceil (1, 0) \rceil^{C2}$`)"`

  lift_definition `stereographic ::`
  `"riemann_sphere` $\Rightarrow$ `complex`$_{hc}$`"` **is** `stereographic_rep`

Стереографска пројекција

- **definition** `inv_stereographic_rep ::` "C2_vec$_{\neq 0}$ $\Rightarrow$ riemann_sphere" **where**
  "inv_stereographic_rep z =
  (**let** (z_1, z_2) = $\lfloor z \rfloor_{C2}$
  in if z_2 = 0 **then** $\lceil (0, 0, 1) \rceil^{R3}$
  else let z = z_1/z_2; XY = (2*z)/cor (1+$|z|^2$);
  Z = ($|z|^2$-1)/(1+$|z|^2$)
  in $\lceil (Re\ XY,\ Im\ XY,\ Z) \rceil^{R3}$)"
  lift_definition `inv_stereographic ::` "complex$_{hc}$ $\Rightarrow$ riemann_sphere" **is**
  inv_stereographic_rep

- **lemma** "stereographic $\circ$ inv_stereographic = id"

Тетивно растојање

- Риманова сфера може бити метрички простор:

```
definition dist_rs ::
   "riemann_sphere ⇒ riemann_sphere ⇒ real" where
   "dist_rs M1 M2 = (let (x1, y1, z1) = ⌊M1⌋R3;
                          (x1, y1, z1) = ⌊M2⌋R3
      in norm (x1 - x2, y1 - y2, z1 - z2))"
```

- Тетивна метрика има своју репрезентацију и у равни.

- Доказано је да су стереографска пројекција и инверзна стереографска пројекција непрекидне.

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

Мебијусове трансформације

- $\mathcal{M}(z) = \frac{a \cdot z + b}{c \cdot z + d} \qquad \lfloor \mathcal{M} \rfloor_M = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$

- **typedef** C2_mat_reg = "{M :: C2_mat. mat_det $M \neq$ 0}"

  definition $\approx_M$ :: "C2_mat_reg $\Rightarrow$ C2_mat_reg $\Rightarrow$ bool"
  where "$M_1 \approx_M M_2 \longleftrightarrow$
  ($\exists$ (k::complex). k $\neq$ 0 $\wedge$ $\lfloor M_2 \rfloor_M$ = k $*_{sm}$ $\lfloor M_1 \rfloor_M$)"

  quotient_type mobius = C2_mat_reg / $\approx_M$

Мебијусова група

Пројективна генерална линеарна група, $PGL(2, \mathbb{C})$

Мебијусови елементи формирају групу над композицијом.

- Композиција Мебијусових елемената се постиже множењем матрица које их репрезентују.
- Инверзна Мебијусова трансформација се добија инверзијом матрице која је представља.
- Мебијусова трансформација која је идентитет је представљена јединичном матрицом.
- Дејство Мебијусове групе: $\mathcal{M}(z) = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} z_1 \\ z_2 \end{bmatrix}$

definition mobius_pt_rep :: "C2_mat_reg $\Rightarrow$ C2_vec$_{\neq 0}$ $\Rightarrow$ C2_vec$_{\neq 0}$"
  where "moebius_pt_rep M z = $\lceil \lfloor M \rfloor_M \ *_{mv} \ \lfloor z \rfloor_{C2} \rceil^{C2}$"
lift_definition mobius_pt :: "mobius $\Rightarrow$ complex$_{hc}$ $\Rightarrow$ complex$_{hc}$" **is**
  mobius_pt_rep

Еуклидске сличности

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

- Формирају параболичку групу.

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

- Свака еуклидска сличност се може добити као композиција транслације, ротације и хомотетије:
  lemma "$a \neq 0 \Longrightarrow$ similarity a b =
  (translation b) + (rotation (arg a)) + (dilatation $|a|$)"

- Реципрочна вредност $(1_{hc} :_{hc} z)$ је такође Мебијусова трансформација.
- Инверзија $(1_{hc} :_{hc} (\mathtt{cnj}\ \ z))$ није Мебијусова трансформација – антихоломорфна функција.

Свака Мебијусова трансформација се може добити композицијом еуклидских сличности и реципрочне функције.

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

- Декомпозиција је веома често коришћена у доказима.

Дворазмера као Мебијусова трансформација

- $\texttt{cross\_ratio}\ z\ z_1\ z_2\ z_3$ је Мебијусова трансформација.
- **lemma** "$[\![\ z_1 \neq z_2;\ z_1 \neq z_3;\ z_2 \neq z_3\ ]\!] \Longrightarrow$
  $(\exists\ M.\ \ \texttt{mobius\_pt}\ M\ z_1\ \texttt{=}\ 0_{hc}\ \wedge$
  $\texttt{mobius\_pt}\ M\ z_2\ \texttt{=}\ 1_{hc}\ \wedge\ \texttt{mobius\_pt}\ M\ z_3\ \texttt{=}\ \infty_{hc})$"

Без губитка на општости

lemma assumes "$P\ 0_{hc}\ 1_{hc}\ \infty_{hc}$" "$z_1 \neq z_2$" "$z_1 \neq z_3$" "$z_2 \neq z_3$"
"$\bigwedge\ M\ u\ v\ w.\ P\ u\ v\ w \Longrightarrow$
$P\ (\texttt{mobius\_pt}\ M\ u)\ (\texttt{mobius\_pt}\ M\ b)\ (\texttt{mobius\_pt}\ M\ c)$"
shows "$P\ z_1\ z_2\ z_3$"

Постоји јединствена Мебијусова трансформација која слика три различите тачке у друге три различите тачке.

Мебијусове трансформације чувају дворазмеру.

Подгрупе Мебијусових трансформација

- Ротације сфере.
- Аутоморфизми диска – трансформација које мапирају јединични диск у самог себе.
- Мебијусове трансформације које фиксирају јединични круг.
- Свака трансформација је композиција Блашке фактора и ротације.

- Сличне Мебијусове трансформације.

Свака Мебијусова трансформација је слична некој еуклидској сличности.

- Инваријанта Мебијусових трансформација.

Мебијусове трансформације (које нису идентитет) сличне акко имају једнаке инваријанте.

параболичко,	$\texttt{similarity\_invar} = 0$, има само једну фиксну тачку
елиптичко,	инваријанта је реална и $-4 \leq \texttt{similarity\_invar} < 0$
правилно хиперболичко,	инваријанта је реална и $\texttt{similarity\_invar} > 0$
неправилно хиперболичко,	инваријанта је реална и $\texttt{similarity\_invar} \leq -4$
локсодромичко,	инваријанта није реална

Кругоправа

- $A * z * \texttt{cnj}\, z + B * \texttt{cnj}\, z + C * z + D = 0$
  Хермитска матрица: $\begin{bmatrix} A & B \\ C & D \end{bmatrix}$; $\quad C = \bar{B}$; $\quad A, D \in \mathbb{R}$
- Скуп тачака на датој кругоправи:
  $$\begin{bmatrix} \bar{z_1} \\ \bar{z_2} \end{bmatrix} \cdot \begin{bmatrix} A & B \\ C & D \end{bmatrix} \cdot \begin{bmatrix} z_1 \\ z_2 \end{bmatrix} = 0$$

definition "quad_form H z = (vec_cnj z) $*_{vm}$ H $*_{vv}$ z"
definition on_circline_rep ::
  "C2_mat_herm ⇒ C2_vec$_{\neq 0}$ ⇒ bool" **where**
  "on_circline_rep H z ⟷ quad_form $\lfloor H \rfloor_H$ $\lfloor z \rfloor_{C2}$ = 0"
lift_definition on_circline :: "circline ⇒ complex$_{hc}$ ⇒ bool" **is**
  on_circline_rep
definition circline_set :: "complex$_{hc}$ set" **where**
  "circline_set H = {z. on_circline H z}"

Повезаност са правама и круговима у обичној еуклидској равни

- Праве су дефинисане као оне кругоправе код којих матрице имају коефицијент $A = 0$, или, еквивалентно као оне кругоправе које садрже тачку ∞_{hc}.
- Сваки еуклидски круг и еуклидска права може бити представљена коришћењем кругоправе.
- Скуп тачака који су одређени кругоправом је увек или еуклидски круг или еуклидска права.

  definition euclidean_circle_rep **where** "euclidean_circle_rep H =
  ($\textbf{let}$ (A, B, C, D) = $\lfloor H \rfloor_H$
  in $(-B/A$, sqrt(Re $((B * C - A * D)/(A * A)))))$"
- Тип кругоправе:
  - имагинарне кругоправе
  - тачка кругоправе
  - реалне кругоправе

Дејство Мебијусових трансформација на кругоправе

Мебијусове трансформације сликају кругоправе на кругоправе.

- Сличност две матрице:

  definition "congruence M H = mat_adj M $*_{mm}$ H $*_{mm}$ M"

- Дефиниција дејства:

  definition mobius_circline_rep ::
  "C2_mat_reg ⇒ C2_mat_herm ⇒ C2_mat_herm" **where**
  "mobius_circline_rep M H = $\lceil$congruence (mat_inv $\lfloor M \rfloor_M$) $\lfloor H \rfloor_H\rceil^H$"
  lift_definition mobius_circline :: "mobius ⇒ circline ⇒ circline"
  is mobius_circline_rep

- **lemma** "mobius_pt M ‘ circline_set H =
  circline_set (mobius_circline M H)"

Дејство Мебијусових трансформација на кругоправе

Мебијусове трансформације чувају и тип кругоправе.

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 произвољну праву или круг:

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

Принцип симетрије

Симетрија тачака је очувана након дејства Мебијусових трансформација.

Оријентисане кругоправе

- Еквивалентне оријентисане кругоправе — пропорционалне у односу на неки позитиван, реални фактор.
- Унутрашњост:

  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"

- $A > 0$ – позитивно оријентисане кругоправе. $A = 0$ (случај правих) – разматрамо коефицијенте B и D.
- Све еуклидске сличности чувају оријентацију кругоправе.
- Оријентација слике дате оријентисане кругоправе H након дате Мебијусове трансформације M зависи од тога да ли пол M лежи на диску или у диску који је комплементаран H.

Оријентација резултујућег круга не зависи од оријентације полазног круга.

Очување угла

- Геометријска дефиниција угла.
- Алгебарска дефиниција угла.

конформно пресликавање

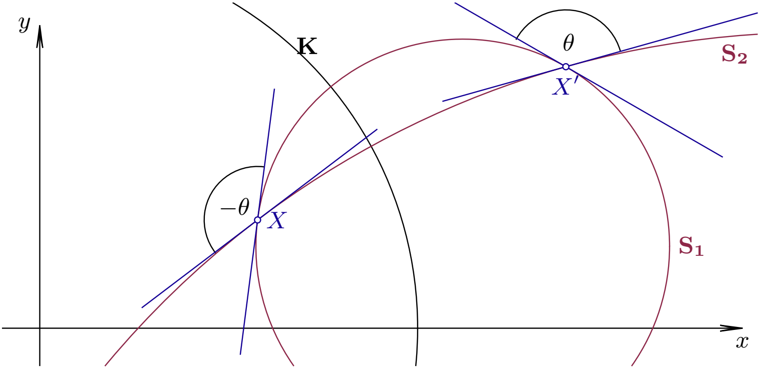
Мебијусове трансформације чувају оријентисане углове међу оријентисаним кругоправама.

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` $H_1\ H_2$ `=`
    `- Re (mat_det_mix` $\lfloor H_1 \rfloor_H\ \lfloor H_2 \rfloor_H$`) /`
    `2 * (sqrt (Re (mat_det` $\lfloor H_1 \rfloor_H$ `* mat_det` $\lfloor H_2 \rfloor_H$`))))"`

Дискусија – очување угла

- Посматрамо Нидамов приступ.
- Доказ се ослања на чињеницу да се свака Мебијусова трансформација може раставити на транслацију, ротацију, хомотетију и инверзију.



Дискусија – очување угла

- Алгебарска дефиниција
  - веома погодна за доказе
  - веома неинтуитивна
- Геометријска дефиниција
  - компликовани докази, много специјалних случајева
  - веома интутивна
- Решење
  - увести алгебарску дефиницију и користити је у доказима
  - показати њену еквивалентност са геометријском дефиницијом

Формализација Поенкареовог диск модела

- Релација *између*

```
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
```

Аутоморфизми диска чувају релацију *између*.

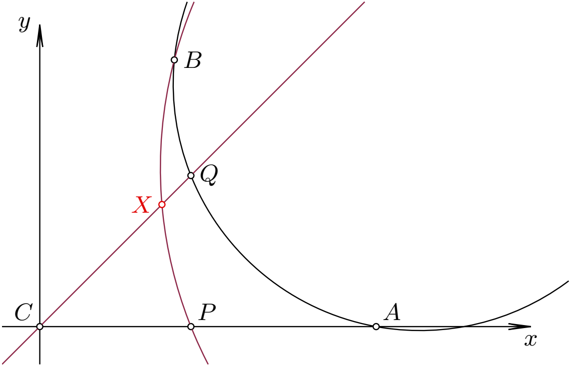
- lemma

```
    assumes "z1' = moebius_pt_poincare M z1"
            "z2' = moebius_pt_poincare M z2"
            "z3' = moebius_pt_poincare M z3"
            "between_poincare z1 z2 z3"
    shows "between_poincare z1' z2' z3'"
```

Ако за три тачке важи релација *између*, онда се оне могу сликати на реалну осу.

Проблем пресека кругоправих

- Одређивање кругоправе: $\overline{u'} \cdot H_1 \cdot u' = 0 \qquad \overline{v'} \cdot H_1 \cdot v' = 0$
- Одређивање пресека: $\overline{x'} \cdot H_1 \cdot x' = 0 \qquad \overline{x'} \cdot H_2 \cdot x' = 0$



Закључци

- Формализовали: 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, кругоправе, дејство Мебијусових трансформација на кругоправе, оријентисане кругоправе, однос између Мебијусових трансформација и оријентације, својство очувања угла итд.
- Кључан корак — коришћење алгебарске репрезентације објеката.
- Што чешће избегавати анализу случајева.
- Увођење више модела истог концепта.
- Око 12,000 линија кода.
- Око 800 лема.
- Око 125 дефиниција.

Закључци

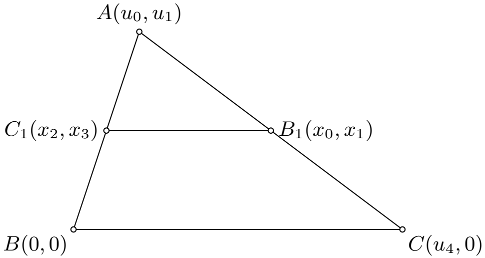
- Дефинисана релација *између* у Поинкареовом диск моделу.
- Показано је да важи 6 аксиома Тарског.
- Показано је да не важи Еуклидова аксиома.
- Одређивање пресека кругоправих представља проблем.

Циљеви формалног изучавања алгебарских метода и њихових проширења

- Формализовати превођење геометријских тврђења у алгебарску форму.
- Веза између синтетичке геометрије и алгебре, категоричност геометрије.
- Дизајнирати систем за запис и трансформацију геометријских тврђења из стереометрије на начин погодан за примену у оквиру алгебарских доказивача.
- Тестирати и упоредити различите приступе алгебризације.

Алгебризација

Средња линија троугла је паралелна насрамној страници.



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

Алгебризација

- Добијају се два скупа полиномијалних једначина.

- let c = Bisector (Point A) (Point B);
  b = Bisector (Point A) (Point C);
  a = Bisector (Point B) (Point C);
  O_1 = Intersect a b;
  O_2 = Intersect a c in
  IsEqualp O_1 O_2

Доказивање исправности

- Алгебарским методама се доказује:
  $\forall v_1, \ldots, v_n \in \mathbb{C} \bigwedge_{i=1}^{k} f_i(v_1, \ldots, v_n) = 0 \Longrightarrow g_i(v_1, \ldots, v_n) = 0$

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

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

Алгебризација геометријских релација у стереометрији

Два приступа:

- Сви објекти су дефинисани коришћењем тачака.
- Сви објекти се представљају коришћењем њихових сопствених координата.

Примери алгебризације:

- `parallel_planes` α β
  1. $\overrightarrow{\beta_A\beta_B} \cdot \overrightarrow{\alpha_A\alpha_C} \times \overrightarrow{\alpha_B\alpha_A} = 0$
     $\overrightarrow{\beta_A\beta_C} \cdot \overrightarrow{\alpha_A\alpha_C} \times \overrightarrow{\alpha_A\alpha_B} = 0$
  2. $\overrightarrow{\alpha_v} \times \overrightarrow{\beta_v} = 0$

Примери алгебризације

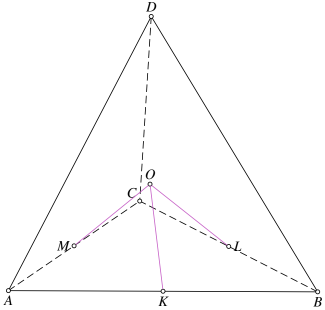
- `equal_angles` $A\ O\ B\ C\ K\ D$
  $\cos^2\angle AOB = \cos^2\angle CKD \qquad \cos^2\angle AOB = \frac{(\overrightarrow{AO}\cdot\overrightarrow{BO})^2}{|AO|^2|BO|^2}$

- `make_tetrahedron` $A\ B\ C\ D$
  $A(0,0,0)$, $B(1,0,0)$, $C(c^x, c^y, 0)$ и $D(c^x, d^y, d^z)$
  Полиноми: $$\begin{aligned} poly_1 &= 2\cdot c^x - 1\\ poly_2 &= 2\cdot {c^y}^2 - 3\\ poly_3 &= 3\cdot d^y - c^y\\ poly_4 &= 3\cdot {d^z}^2 - 2 \end{aligned}$$

- Упрошћавање полинома.

Експерименти

$$\angle MOK = \angle KOL = \angle MOL$$



Експерименти

	број полинома	број полинома доказа	просечан број монома	број проме- нљивих	време
први приступ	24	4	7.2	18	*Меморијски лимит*
други приступ	24	2	3.5	24	$0.835s$

Експерименти

	GeoProver успех	*GeoProver* неуспех	*Гребнерове базе* успех	*Гребнерове базе* неуспех
први приступ	13	16	23	6
други приступ	22	7	29	0

Закључци

- Формализовано је превођење геометријских тврђења у алгебарску форму.
- Извршена је алгебризација геометријских тврђења на два начина.
- Извршено је поређење различитих приступа у алгебризацији.
- Тестирањем се показало да је систем ефикаснији када су полиноми једноставни.

Даљи рад

- Доказ да наша дефиниција Декартове координатне равни задовољава све аксиоме Хилберта.
- Дефинишемо аналитичку геометрију у оквиру аксиоматизације Тарског или Хилберта.
- Доказати категоричност и система аксиома Тарског и система аксиома Хилберта.
- Испитати својства различитих класа Мебијусових трансформација.
- Завршити формализацију Поинкареовог диск модела.
- Испитати примене формализације у другим областима, нпр. физици.
- Услови недегенерисаности у стереометрији.
- Проширити систем тако да обухвати обла тела.
- Повезати направљени доказивач са динамичким геометријским софтвером.