Prijava teze ”Formalizacija različitih modela geometrije i primene u formalizaciji automatskih dokazivača teorema”

Danijela Simić
Mentor: prof. dr. Filip Marić

Zašto koristiti računare za dokazivanje teorema?

- Rigoroznost matematičkih dokaza
- Veliki broj grešaka u istoriji matematike
- Problem nepotpunih definicija
- Problem nekompletnih dokaza, sa namerno ili slučajno izostavljenim delom dokaza
- Problem recezenata

Dokazivači teorema

Sistemi za proveru dokaza:

- Automatski dokazivači
- Poluautomatski dokazavači (asistenti za dokazivanje teorema)

Dokazivači teorema u geometriji:

- Aksiomatski dokazivači
- Algebarski dokazivači

Motivacija

$$
\begin{tikzcd}
\text{Geometrijska teorema} \arrow[rr, "\text{Vu, Dekart}"] \arrow[d, "\text{teško}"] & & \text{Algebarska transformacija} \arrow[d, "\text{Vuov metod, Grebnerove baze}"] \\
\text{Geometrijski dokaz} & & \text{Algebarski dokaz} \arrow[ll, "\text{Hilbert, Tarski, Dekart}"]
\end{tikzcd}
$$

Motivacija

Formalizovati prelazak sa *sintetičke geometrije* na *zapis u polininomima*:

- Formalizovati analitičku geometriju, tj. pokazati da je analitička geometrija model geometrije Tarskog i Hilberta.
- Formalizovati prevodjenje konstrukcija u polinome.

- Postoji mnogo različitih geometrija
- Euklidska (sintetička geometrija): Euklidovi "Elementi", sistemi Tarskog, Hilberta i Avigadov sistem
- Dekartov koordinatni sistem, uspostavlja vezu između sintetičke geometrije i algebre
- Postoji više pokušaja da se formalizuje geometrija
- Korišćenje *dokazivača teorema* povećava se nivo rigoroznosti
- Sistem Isabelle/HOL

Formalizacija analitičke geometrije

- Formalizovana analitička geometrija u okviru dokazivača teorema.
- Različite definicije istih pojmova su pokazane da su međusobno ekvivalentne
- Formalizovano da analitička geometrija predstavlja model geometrije Tarskog i geometrije Hilberta (dokazane aksiome Tarskog i Hilberta u analitičkoj geometriji).
- U dokazima su korišćenje izometrijske transformacije, radi uprošćavanja dokaza
- Naša formalizacija se zasniva na aksiomama realnih brojeva i osobine realnih brojeva su korišćene u dokazima

Formalizacija analitičke geometrije

- *objekti:* tačke (par realnih brojeva $\mathbb{R}^2$), prave

Formalizacija analitičke geometrije

- *objekti:* tačke (par realnih brojeva $\mathbb{R}^2$), prave
- *relacije:* incidencija, između, kongruencija

Formalizacija analitičke geometrije – relacija između

- Relacija *između*: $\mathcal{B}(A, B, C)$
- Aksiomatizacija *Tarskog* dozvoljava jednakost među tačkama:

$$\begin{array}{l}\mathcal{B}_T^{ag}\ \ (xa, ya)\ \ (xb, yb)\ \ (xc, yc) \longleftrightarrow \\ \quad (\exists (k :: real).\ 0 \leq k \ \ \wedge \ \ k \leq 1 \ \wedge \\ \qquad (xb - xa) = k \cdot (xc - xa) \ \ \wedge \ \ (yb - ya) = k \cdot (yc - ya))\end{array}$$

Formalizacija analitičke geometrije – prave

- $A \cdot x + B \cdot y + C = 0$ where $A \neq 0 \vee B \neq 0$
- *ista prava*:
  - $A \cdot x + B \cdot y + C = 0$
  - $k \cdot A \cdot x + k \cdot B \cdot y + k \cdot C = 0$, za realno $k \neq 0$

Prava

`Klasa ekvivalencije nad skupom`

$$\{((A :: real), (B :: real), (C :: real)).\ A \neq 0 \vee B \neq 0\}$$

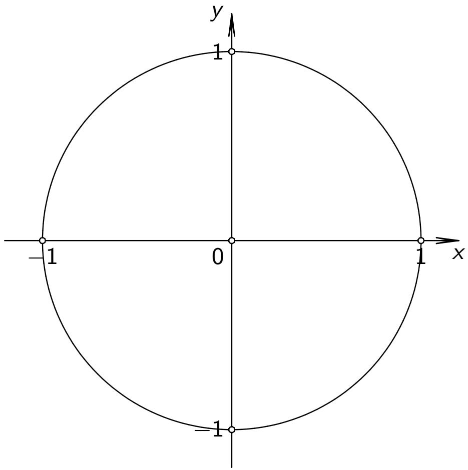
Formalizacija analitičke geometrije – wlog

Bez gubitka na opštosti

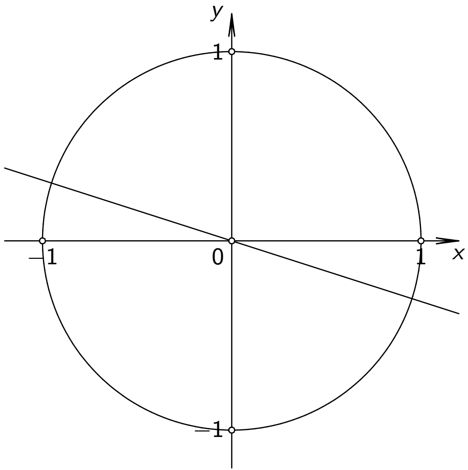
$inv\ \ P\ \ t \longleftrightarrow (\forall\ \ A\ \ B\ \ C.\ \ P\ \ A\ \ B\ \ C \longleftrightarrow P\ \ (tA)\ \ (tB)\ \ (tC))$

- John Harrison, *Without loss of generality*

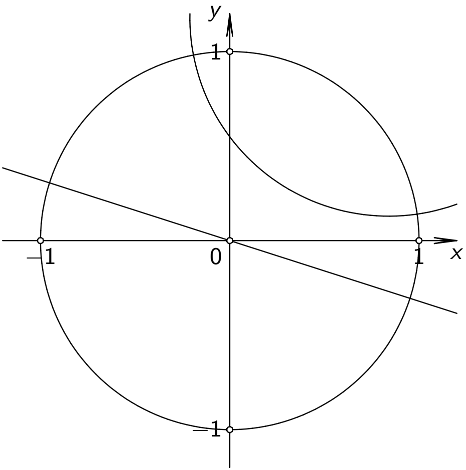
Poinkareov disk model



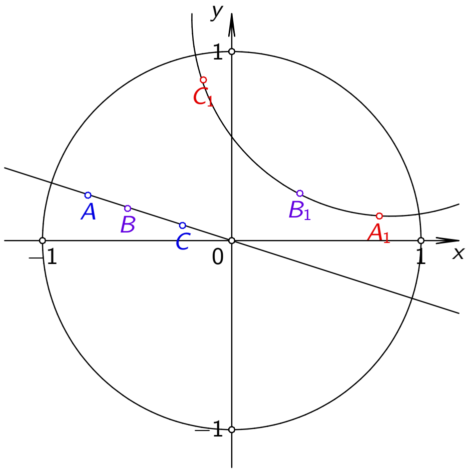
Poinkareov disk model - Prava



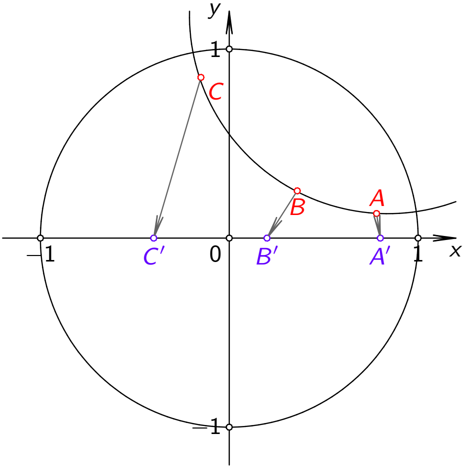
Poinkareov disk model - Prava



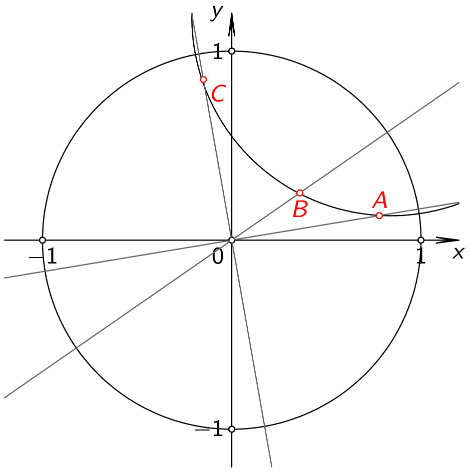
Poinkareov disk model - Između



Poinkareov disk model - Između



Poinkareov disk model - Između



Da li važi: $\sphericalangle AOC = \sphericalangle AOB + \sphericalangle COB$

Kompleksna geometrija

- Zamenom Dekartove ravni sa kompleksnom ravni dobijaju se kompaktnije i manje kompleksne formule.

Kompleksna geometrija

- Zamenom Dekartove ravni sa kompleksnom ravni dobijaju se kompaktnije i manje kompleksne formule.
- Kompleksna ravan ili neki njen deo (jedinični disk ili gornja poluravan) se često uzimaju kao domen u kojima se formalizuju modeli različitih geometrija.

Kompleksna geometrija

- Zamenom Dekartove ravni sa kompleksnom ravni dobijaju se kompaktnije i manje kompleksne formule.
- Kompleksna ravan ili neki njen deo (jedinični disk ili gornja poluravan) se često uzimaju kao domen u kojima se formalizuju modeli različitih geometrija.
- Postoji potreba za formalizacijom

Kompleksna geometrija

- Zamenom Dekartove ravni sa kompleksnom ravni dobijaju se kompaktnije i manje kompleksne formule.
- Kompleksna ravan ili neki njen deo (jedinični disk ili gornja poluravan) se često uzimaju kao domen u kojima se formalizuju modeli različitih geometrija.
- Postoji potreba za formalizacijom
- Postoji više pristupa u izlaganju materije u knjigama

Glavni rezultati u formalizaciji kompleksne geoemtrije

- Proširena kompleksna ravan, dodata je tačka ∞

Glavni rezultati u formalizaciji kompleksne geomtrije

- Proširena kompleksna ravan, dodata je tačka ∞
- Homogene koordinate:

$$z = \frac{z_1}{z_2}$$

pri čemu $z_1, z_2 \neq 0$
Još posmatramo i ovo:

$$z = \frac{k \cdot z_1}{k \cdot z_2}$$

pri čemu $k \neq 0$
Uvodimo relaciju $\approx$: $(z_1, z_2) \approx (k \cdot z_1, k \cdot z_2)$ i posmatramo *klasu ekvivalencije* ove relacije nad skupom ne-nula vektora.

Glavni rezultati u formalizaciji kompleksne geometrije

- $\infty = \frac{1}{0}$ – klasa ekvivalencije elementa (1, 0) nad skupom ne-nula vektora

Glavni rezultati u formalizaciji kompleksne geometrije

- $\infty = \frac{1}{0}$ – klasa ekvivalencije elementa $(1, 0)$ nad skupom ne-nula vektora
- Uvodimo aritmetičke operacije i pokazujemo da su dobro definisane, pokazujemo osnovna svojstva konjugata i inverzije

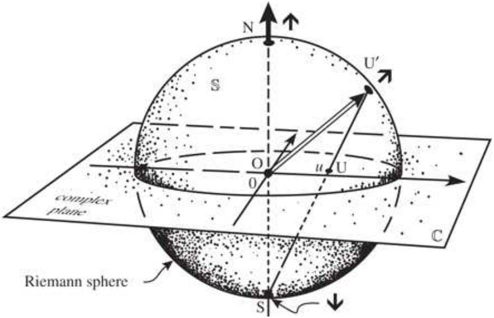
Glavni rezultati u formalizaciji kompleksne geometrije

- $\infty = \frac{1}{0}$ – klasa ekvivalencije elementa $(1, 0)$ nad skupom ne-nula vektora
- Uvodimo aritmetičke operacije i pokazujemo da su dobro definisane, pokazujemo osnovna svojstva konjugata i inverzije
- Definišemo dvorazmeru:

$$(z, u, v, w) = \frac{(z - u)(v - w)}{(z - w)(v - u)}$$

i pokazujemo osnovna svojstva

Rimanova sfera i stereografska projekcija



Mebijusove transformacije

$$M(z) = \frac{a \cdot z + b}{c \cdot z + d}$$

$[M] = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ pri čemu $|[M]| \neq 0$

- Proporcionalne matrice predstavljaju jednu te istu Mebijusovu transformaciju

Mebijusove transformacije

$$M(z) = \frac{a \cdot z + b}{c \cdot z + d}$$

$[M] = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ pri čemu $|[M]| \neq 0$

- Proporcionalne matrice predstavljaju jednu te istu Mebijusovu transformaciju
- *Kompozicija* Mebijusovih transformacija se dobija kao proizvod matrica koje ih predstavljaju

Mebijusove transformacije

$$M(z) = \frac{a \cdot z + b}{c \cdot z + d}$$

$$[M] = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \text{ pri čemu } |[M]| \neq 0$$

- Proporcionalne matrice predstavljaju jednu te istu Mebijusovu transformaciju
- *Kompozicija* Mebijusovih transformacija se dobija kao proizvod matrica koje ih predstavljaju
- *Inverzna* Mebijusova transfomacija se dobija kao inverzna matrica matrice koja predtavlja transformaciju

Mebijusove transformacije

$$M(z) = \frac{a \cdot z + b}{c \cdot z + d}$$

$$[M] = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \text{ pri čemu } |[M]| \neq 0$$

- Proporcionalne matrice predstavljaju jednu te istu Mebijusovu transformaciju
- *Kompozicija* Mebijusovih transformacija se dobija kao proizvod matrica koje ih predstavljaju
- *Inverzna* Mebijusova transfomacija se dobija kao inverzna matrica matrice koja predtavlja transformaciju
- Dejstvo Mebijusa na tačke:

$$M(z) \longleftrightarrow \begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} z_1 \\ z_2 \end{bmatrix}$$

- Pokazujemo da je dvorazmera Mebijusova transformacija i to koristimo da pokažemo da:
- $z_1 \rightarrow$
- $z_2 \rightarrow$
- $z_3 \rightarrow$

- Pokazujemo da je dvorazmera Mebijusova transformacija i to koristimo da pokažemo da:
- $z_1 \to 0$
- $z_2 \to 1$
- $z_3 \to \infty$

- Pokazujemo da je dvorazmera Mebijusova transformacija i to koristimo da pokažemo da:
- $z_1 \to 0$
- $z_2 \to 1$
- $z_3 \to \infty$

Bez gubitka na opštosti

- ako svojstvo P važi za tačke 0, 1 i ∞
- Mebijusova transformacija čuva svojstvo P
- *zaključak:* svojstvo P važi za bilo koje tri različite tačke z_1, z_2 i z_3

Uopšteni krug

Uopšteni krug: može biti prava, ali i krug

$$A \cdot z \cdot \overline{z} + B \cdot \overline{z} + C \cdot z + D = 0$$

$H = \begin{bmatrix} A & B \\ C & D \end{bmatrix}$ pri čemu $B = \overline{C}$ i $A, D \in \mathbb{R}$

$$\begin{bmatrix} z_1 z_2 \end{bmatrix} \begin{bmatrix} A & B \\ C & D \end{bmatrix} \begin{bmatrix} z_1 \\ z_2 \end{bmatrix} = 0$$

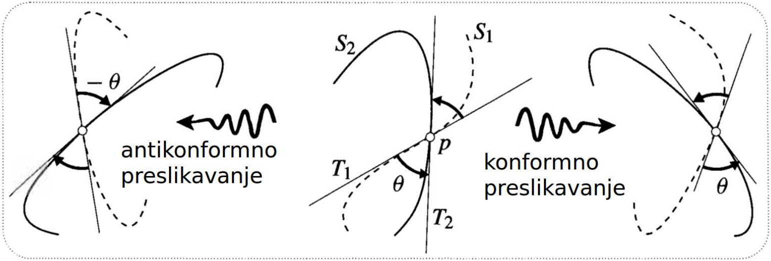
- Svaki uopšteni krug odgovara krugu na Rimanovoj sferi.

Mebijusova transformacija uopštenog kruga

M – Mebijusova transformacija (zadata matricom)
H – Uopšteni krug (zadat Matricom)

$$adj M^{-1} \cdot H \cdot M^{-1}$$

Očuvanje ugla



$$\cos\angle H_1 H_2 = \frac{|H_{1,2}|}{\sqrt{|H_1|}\sqrt{|H_2|}}$$

Statistika formalizacije kompleksne geometrije

- Broj definicija: oko 200
- Broj teorema: oko 800
- Broj linija koda: preko 13000

Poincareov disk model

Primene formalizacije kompleksne geometrije na Poincareov disk model:

- definicija između – korišćenjem dvorazmere
- izometrijske transformacije koje slikaju unutrašnjost diska u unutrašnjost diska
- rastojanje među tačkama

Primena algebarskih metoda u stereometriji

- Predstaviti stereometrijske objekte u vidu algebarskih formula.
- Primeniti na njih Vu-ov metod ili metod Grebnerovih baza

Ostvareni ciljevi:

- Formalizacija analitičke geometrije
- Formalizacija geometrije kompleksne ravni
- Deo formalizacije automatskog dokazivača teorema zasnovanog na Vu-ovoj metodi ili na metodi Grebnerovih baza

Planirani ciljevi:

- Primena algebarskog dokazivača na probleme u stereometriji
- Formalizacija Poinkareovog disk modela