Korišćenje lema u algebarskim dokazivačima geometrijskih teorema

Predrag Janičić
URL: www.matf.bg.ac.rs/~janicic
Matematički fakultet, Univerzitet u Beogradu, Srbija

ARGO seminar
Beograd, 29.04.2009.

Plan izlaganja

- Automatsko dokazivanje geometrijskih teorema
- Algebarske metode za dokazivanje geometrijskih teorema
- Jedan pristup korišćenju lema
- Realizacija u okviru sistema GCLC
- Zaključci

Geometrijske teoreme konstruktivnog tipa

- Tvrdjenja koja odgovaraju svojstvima konstrukcija
- Uglavnom, euklidska ravanska geometrija
- Nedegenerativni uslovi su veoma važni

Metode za dokazivanje geometrijskih teorema

- Sintetičke metode — daju tradicionalne (čitljive) dokaze:
  - Gelertner-ov dokazivač (Gelertner 1950's)
  - Dokazivači zasnovani na koherentnoj logici.
- Polualgebarske metode — koriste izračunavanja, ali ipak daju (više-manje) čitljive dokaze:
  - metod površina (Chou et.al., 1990-ih)
  - metod uglova (Chou et.al., 1990-ih)
- Algebarske metode — ne daju čitljive dokaze, već samo algebarske argumente:
  - metod Gröbner-ovih baza (Buchberger, 1965)
  - Wu-ov metod (Wu, 1977)
- Nijedna implementacija algebarskih i polualgebarskih metoda ne razmatra leme!

Osnovni principi alebarskih metoda

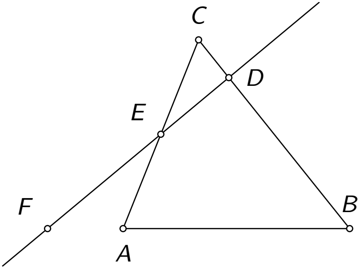
- Geometrijska tvrdjenja imaju formu jednakosti
- Konstrukcijski koraci se transformišu u polinomijalni sistem:

$$\begin{array}{rcl} h_1(u_1, u_2, \ldots, u_d, x_1, \ldots, x_n) & = & 0 \\ h_2(u_1, u_2, \ldots, u_d, x_1, \ldots, x_n) & = & 0 \\ & \ldots & \\ h_t(u_1, u_2, \ldots, u_d, x_1, \ldots, x_n) & = & 0 \end{array}$$

- Cilj je proveriti da li za tvrdjenje važi

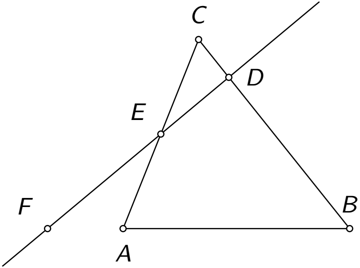
$$g(u_1, u_2, \ldots, u_d, x_1, \ldots, x_n) = 0$$

Primer: Menelajeva teorema



- Tvrdjenje:
$$\frac{\overrightarrow{AF}}{\overrightarrow{FB}} \cdot \frac{\overrightarrow{BD}}{\overrightarrow{DC}} \cdot \frac{\overrightarrow{CE}}{\overrightarrow{EA}} = -1$$

Primer: Menelajeva teorema (2)



- Koordinate pridružene tačkama:
$A(0,0), B(u_1,0), C(u_2,u_3), D(x_1,u_4), E(x_2,u_5), F(x_4,0)$

Primer: Menelajeva teorema (3)

- Uslovi:
  D pripada BC: $p_1 = -u_3x_1 + (u_4u_2 - u_4u_1 + u_3u_1)$
  E pripada AC: $p_2 = -u_3x_2 + u_5u_2$
  F pripada DE: $p_3 = (-u_5 + u_4)x_4 - u_4x_2 + u_5x_1$
- Tvrdjenje:

$$p_4 = (-u_5u_3 + u_4u_3)x_4 + (-u_5u_4u_1 + u_5u_3u_1)$$

Wu-ov metod

- Razvijen od strane Wu-a 1977
- Smatra se najefikasnijim metodom za automatsko dokazivanje teorema (ne samo u geometriji)
- Smatra se jednim od ,,četiri moderna velika kineska izuma"
- Metod sličan Gausovoj proceduri eliminacije

Wu-ov metod primenjen na Menelajevu teoremu

- Triangulacija daje:

$$\begin{aligned} p_1 &= -u_3x_1 + (u_4u_2 - u_4u_1 + u_3u_1) \\ p_2 &= -u_3x_2 + u_5u_2 \\ p_3 &= (-u_5 + u_4)x_4 - u_4x_2 + u_5x_1 \end{aligned}$$

- Wu-ova procedura eliminacije u nekoliko koraka daje $p_4 = 0$, što je i trebalo dokazati

Metod Gröbner-ovih baza

- Razvijen od strane Buchberger-a 1965, široko korišćen CAS (computer-algebra systems) algoritam sa mnogim primenama
- Gröbner-ova baza (GB) je vrsta generativnog podskupa ideala polinomijalnog pristena R
- Buchberger-ov algoritam gradi GB za skup polinoma koji odgovaraju konstrukcijskim koracima i onda proverava tvrdjenje efikasno testirajući da li je njegov ostatak u odnosu na GB jednak 0
- Za svodjenje u odnosu na GB, poredak svodjenja nije bitan

Šta se uopšte dokazuje?

- Svaki uslov (konstrukcijski korak) daje jednu jednakost $c_i = 0$
- Tvrdjenje je tipa $g = 0$
- Potrebno je dokazati:

$$c_1 = 0 \wedge c_2 = 0 \wedge \ldots \wedge c_n = 0 \Rightarrow g = 0$$

- Za mehanizam korišćenja lema nije ni bitno kako se to dokazuje

Podkonstrukcije i leme (1)

- Ukoliko postoji teorema u kojoj je polazna konstrukcija podkonstrukcija zadate konstrukcije, onda uslov te teoreme ($g' = 0$) možemo iskoristiti kao dodatni uslov:

$$c_1 = 0 \wedge c_2 = 0 \wedge \ldots \wedge c_n = 0 \wedge g' = 0 \Rightarrow g = 0$$

- Ovo je saglasno jer važi:

$$c_1 = 0 \wedge c_2 = 0 \wedge \ldots \wedge c_n = 0 \Rightarrow g' = 0$$

- Može se očekivati da je efikasno

Kako detektovati podkonstrukcije?

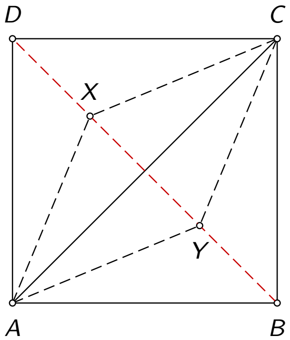
- Tipičan opis konstrukcije:

```
% free points
point A 15 20
point B 80 10
point C 70 90
% side bisectors
med a B C
med b A C
med c B A
% intersections of bisectors
intersection O_1 a b
intersection O_2 a c
...
```

Podkonstrukcije i leme (2)

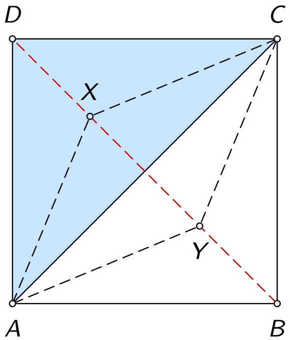
- Preslikati slobodne tačke leme u slobodne tačke glavnog tvrdjenja na sve načine dok se ne pronadje preslikavanje takvo da svi koraci leme imaju pandan u glavnom tvrdjenju

Podkonstrukcije — primer (1)



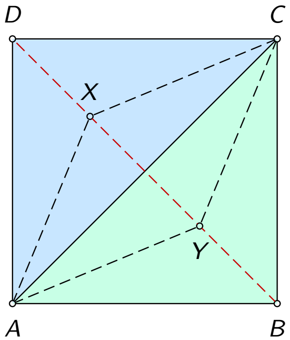
- Tvrdjenje: ako se bisektrise uglova DCA i DAC seku u tački X, a bisektrise uglova BCA i BAC seku u tački Y, onda su tačke D, X, Y, B kolinearne

Podkonstrukcije — primer (2)



- Lema: bisektrise trougla seku se u jednoj tački

Podkonstrukcije — primer (2)



- Lema: bisektrise trougla seku se u jednoj tački

Podkonstrukcije i leme (2)

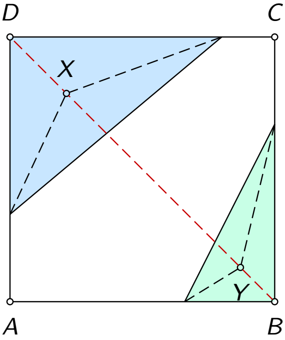
- Za svaku podkonstrukciju tvrdjenja koja odgovara nekoj lemi, dodaje se tvrdjenje te leme kao dodatni uslov:

$$c_1 = 0 \wedge c_2 = 0 \wedge \ldots \wedge c_n = 0 \wedge g_1 = 0 \wedge g_2 = 0 \wedge \ldots \wedge g_m = 0 \Rightarrow g = 0$$

Podkonstrukcije i leme (3)

- Preslikati slobodne tačke leme u slobodne tačke glavnog tvrdjenja na sve načine dok se ne pronadje preslikavanje takvo da svi koraci leme imaju pandan u glavnom tvrdjenju
- Potrebno je i više od toga!
- $\forall A.\forall B.\forall C.\forall O_1.(O_1 = intersection(med(B, C), med(A, C)) \wedge \ldots$
- I konstruisane tačke su univerzalno kvantifikovane, pa i one treba da budu razmatrane za preslikavanja

Podkonstrukcije — primer (4)



Resursi: dokazivači ugradjeni u GCLC

- Postoje dve algebarske metode implementirane u okviru GCLC-a:
  - dokazivač zasnovan na Wu-ovoj metodi
  - dokazivač zasnovan na Buchberger-ovoj methodi
- Raspoloživo je više od 120 teorema u GCLC formatu, dokazanih dokazivačima iz GCLC-a (Goran Predović, Pedro Quaresma, Predrag Janičić)

Koraci

- Napraviti preliminarne eksperimente sa dva postojeća dokazivača i 120 raspoloživih teorema
- Za svaki par tvrdjenja proveriti da li jedno može da posluži kao lema drugom
- Ukoliko se pronadje više takvih parova i ukoliko se dobija značajno ubrzanje, ugraditi generičku podršku u GCLC
- Korisnik bi birao skup teorema koje se mogu koristiti kao leme

Zaključci

- Korišćenje lema u automatskom dokazivanju geometrijskih teorema je izuzetno važno a do sada nije istraživano
- Leme se mogu koristiti relativno jednostavno, na opisani način
- Ukoliko preliminarni rezultati opisanog mehanizma budu dobri, on će biti integrisan u GCLC