

Univerzitet u Beogradu
Matematički fakultet

Goran Predović

Automatsko dokazivanje geometrijskih teorema
primenom Vuove i Buhbergerove metode

- Magistarska teza -

mentor: dr Predrag Janičić

Beograd 2008

Sadržaj

1	Uvod	7
1.1	Kratka istorija automatskog rezonovanja u geometriji	7
1.2	Implementacije algebarskih dokazivača	9
1.3	Motivacija istraživanja geometrijskog zaključivanja	9
2	Osnovni pojmovi i definicije	11
2.1	Osnovne algebarske strukture	11
2.2	Polinomi	12
2.3	Osnovni algebarski algoritmi	14
2.3.1	Algoritam pseudo-deljenja	14
2.3.2	Algoritam sukcesivnog pseudo-deljenja	16
2.3.3	Jednostavan algoritam svođenja na trougaonu formu	17
3	Algebarsko dokazivanje geometrijskih teorema	19
3.1	Propusti u tradicionalnim dokazima	19
3.1.1	Tradicionalni euklidski dokaz	19
3.1.2	Primer algebarskog dokaza	21
3.2	Geometrijska tvrđenja konstruktivnog tipa	21
3.3	Prevođenje geometrijskih konstrukcija u polinome	23
3.4	Pogodan izbor koordinata tačaka	26
3.5	Osnovna ideja algebarskog dokazivanja geometrijskih teorema	27
3.5.1	Apstraktni opis algebarske metode	27
3.5.2	Primeri transformacija sistema polinoma	28
4	Vuova metoda	31
4.1	Opis Vuove metode	31
4.2	Razmatranje uslova nedegenerisanosti	32
4.3	Primene Vuove metode	33
4.3.1	Primer paralelograma	33
4.3.2	Primer Simpsonove teoreme	34
4.3.3	Primer Gausove tačke	37
4.4	Mogući problemi primene Vuove metode	39
4.4.1	Primer ugla nad prečnikom	39
4.4.2	Nekonzistentnost geometrijske konstrukcije	40
4.5	Skica Vuove metode	42
4.6	Čuov dokazivač	43

5	Buhbergerova metoda	45
5.1	Osnovni pojmovi Buhbergerove metode	45
5.2	Buhbergerova metoda	46
5.3	Dokazivanje geometrijskih teorema	49
5.3.1	Primene Buhbergerove metode	50
5.4	Poređenje sa Vuovom metodom	52
6	Implementacija dokazivača geometrijskih teorema	55
6.1	Konstruktivno i opisno zadate teoreme	56
6.2	Dokazivač	57
6.2.1	Biblioteka za rad sa polinomima	57
6.2.2	Algebarski dokazivač	62
6.2.3	Implementacija Vuove metode	63
6.2.4	Implementacija Buhbergerove metode	66
6.3	Integrisanje dokazivača u sistem GCLC	68
6.3.1	Prevođenje konstrukcija u algebarsku formu	69
6.3.2	Dokazivanje tvrđenja	72
6.3.3	Tekstualni izlaz dokazivača	73
7	Zaključci i dalji rad	75
7.1	Zaključci	75
7.1.1	Pregled	75
7.1.2	Rezultati	76
7.1.3	Automatska detekcija nekonzistentne konstrukcije	80
7.2	Pravci daljeg razvoja	82
7.2.1	Unapređivanje metoda	82
7.2.2	Podrška za veći broj geometrijskih teorema	82
7.2.3	Automatsko otkrivanje novih teorema	83
7.2.4	Korišćenje lema pri dokazivanju	85
A	Kolekcija geometrijskih teorema	87
A.1	Uvod	87
A.2	Primer teoreme dokazane u GCLC-u	88
A.3	Teoreme	94

Predgovor

U ovom radu su opisane dve najefikasnije algebarske metode za automatsko dokazivanje geometrijskih teorema — Vuova metoda i Buhbergerova metoda (poznata i kao metoda Grebnerovih baza). Pored kompletnog teorijskog i algoritamskog opisa obe metode, opisana je i implementacija metoda u programskom jeziku C++. Druga celina rada se odnosi na integrisanje implementiranog dokazivača u sistem GCLC — aplikaciju za vizuelizaciju geometrijskih konstrukcija [34]. Geometrijske ilustracije prikazane u ovom radu su urađene korišćenjem upravo ovog programa (verzija za Windows operativni sistem pod nazivom WinGCLC).

Glavni cilj ovog rada je implementacija algebarskih dokazivača geometrijskih tvrđenja. I pored dosta radova koji se mogu pronaći na ovu temu, ukoliko bi neko pokušao da na osnovu teorije izložene u tim radovima implementira dokazivač, to ne bi bio jednostavan posao. Dosta detalja treba interpolisati iz date teorije, a i sama implementacija može sadržati za teoriju neinteresantne detalje koji itekako mogu uticati na performanse (takvi detalji najčešće nisu navedeni u opisima metoda). Dodatni problem je nedostatak izvornog kôda kod postojećih implementacija dokazivača. Ovaj rad trebalo da bude jedan od retkih otvorenih i dostupnih geometrijskih dokazivača algebarskim metodama.

Prva glava rada je uvod u tematiku automatskog dokazivanja geometrijskih teorema (ADGT). Osnovna podela dokazivača je na algebarske metode i metode koje ne zavise od koordinatnog sistema.

Naredna glava uvodi osnovne algebarske pojmove, definicije i algoritme koji se koriste u oblasti kojom se bavi ovaj rad.

Treća glava sadrži uvod u algebarske metode za ADGT. videćemo zbog čega su relativno kasno počele da se koriste iako su najefikasnije, kao i koji problemi su otežavali njihovu efikasnu primenu.

Četvrta glava sadrži opis Vuove¹ metode. Ova metoda je razvijena upravo u svrhu dokazivanja geometrijskih tvrđenja i njena prednost u odnosu na ostale algebarske metode je relativno lako izvođenje dodatnih uslova koji moraju važiti da bi tvrđenje bilo tačno (uslovi nedegenerisanosti). Teorija potrebna za izvođenje Vuove metode je bila poznata još ranije kroz rad Rita (Ritt) na temu karakterističnih skupova.

Peta glava sadrži opis Buhbergerove metode (metode Grebnerovih baza). Ova metoda je univerzalna i ima brojne primene u algebri, pre svega za utvrđivanje pripadnosti polinoma idealu.

Šesta glava sadrži opis implementacije dve algebarske metode (Vuove i Buhbergerove metode) i svih programskih modula koji su urađeni da bi se metode

¹Kineski matematičar Wu-Wen Tsun

mogle implementirati.

GCLC aplikacija je program za vizuelizaciju geometrijskih konstrukcija. Pored osnovne primene, ovo je i pogodan interfejs za postavku geometrijskih tvrđenja konstruktivnog tipa. Šesta glava sadrži i opis integracije algebarskih geometrijskih dokazivača u okruženje GCLC.

Poslednja, sedma glava, daje kratak rezime ovoga rada, sumira postignute rezultate i bavi se mogućim pravcima u kojima se rad može dalje razvijati.

Na kraju je, kao dodatak tekstu, dat spisak teorema dokazanih ovde implementiranim dokazivačima. Kompletno poglavlje je automatski generisano. Ulaz u program je geometrijsko tvrđenje zapisano u GCLC jeziku, a izlaz sadrži ilustraciju teoreme i podatke iz dokaza teoreme, zajedno sa vrednostima koje ukazuju na performanse dokazivača. Teoreme dokazane implementiranim dokazivačima su dodate u web repozitorijum GeoThms [5].

Glava 1

Uvod

U proteklih trideset godina razvijene su veoma uspješne metode za automatsko dokazivanje i otkrivanje geometrijskih tvrđenja. Ova glava sadrži kratak pregled tih metoda i njihovu suštinu (sadržaj ove glave zasnovan je na [3]).

1.1 Kratka istorija automatskog rezonovanja u geometriji

Generalno, postoje dva pristupa mašinskom dokazivanju geometrijskih teorema: pristup zasnovan na veštačkoj inteligenciji (AI) i algebarski pristup. Prvi program na računaru za automatsko dokazivanje geometrijskih teorema (ADGT) je delo Dželerntera (Gelernter) i koautora [7]. Program je simulirao dokaz na način kako bi ga izvodio čovek i smatran je naprednim programom na polju veštačke inteligencije toga vremena. Vos (Wos) i koautori su iskoristili njihov metod rezolucije kao dokazivač opšte namene za eksperimente u dokazivanju geometrijskih teorema preko aksiomatskog sistema Tarskog u elementarnoj geometriji. Jedna metoda dokazivanja teorema u euklidskoj geometriji je opisana u [6]. Uprkos početnim uspesima i unapređivanjima tokom vremena, ove metode nisu prerasle u *moćne* dokazivače geometrijskih teorema.

Na polju algebarskih metoda, najraniji pokušaji dosežu do Hilberta. U svojoj klasičnoj knjizi *Osnovi geometrije* [8], Hilbert je opisao metod odlučivanja u klasi konstruktivnih geometrijskih tvrđenja *afine geometrije*. Kao što je Tarski primetio, Hilbertovi rezultati „su tesno povezani sa metodom odlučivanja u elementarnoj geometriji, ali imaju ograničeni karakter”.

Tarski je 1951. godine objavio metod odlučivanja za teoriju realnih zatvorenih polja čime je pružio i metod odlučivanja u elementarnoj geometriji [9]. Uprkos nekoliko unapređivanja od strane Sajdenberga (Seidenberg) i drugih istraživača, godinama su varijacije metode Tarskog ostale nepraktične za dokazivanje netrivialnih teorema geometrije. Godine 1974., Kolins (Collins) je dao važan doprinos na liniji dokazivača tipa Tarskog [10]. Ovaj metod je implementirao Arnon i nekoliko teških algebarsko-geometrijskih tvrđenja je uspešno dokazano.

Praktično, Dejvis (Davis) je bio prvi koji je istraživao algebarski pristup za ADGT na računarima [11]. Njegov dokaz Paposove teoreme na računaru je u suštini već opisan od strane Hilberta koji međutim nije pružio opšti mehanički algoritam za vođenje dokaza.

Prodor na polju ADGT je napravio kineski matematičar Vu. Ograničavajući se na klasu geometrijskih tvrdjenja koja se mogu izraziti u vidu jednakosti, Vu je 1977. godine predstavio metod koji može efikasno dokazati veoma teške geometrijske teoreme. S obzirom na to da je preko 130 teorema uspešno dokazano ovom metodom [13], Vuov rad je ubrzo postao poznat i izvan Kine. Ko (Ko) i Husein (Hussain), Vang (Wang) i Hu (Hu), Gao (Gao), Kapur (Kapur) i Van (Wan) su uspeali u implementaciji dokazivača zasnovanih na modifikovanim verzijama Vuove metode. Kasnije je utvrđeno da se algebarska teorija potrebna za Vuovu metodu može pronaći i u rezultatima do kojih je došao matematičar Rit mnogo godina ranije [14]. Ova metoda je danas poznata kao Rit-Vu metoda karakterističnih skupova. Do danas je na stotine teorema iz euklidske i ne-euklidskih geometrija dokazano implementacijama Vuove metode.

Uspes Vuove metode je ponovo probudio interesovanje za dokazivanje geometrijskih teorema na računarima. Istraživana je primena metode Grebnerovih baza i Buhbergerovog (Buchberger) algoritma [15] na istu klasu geometrijskih tvrdjenja na koje se odnosi i Vuova metoda. Osamdesetih godina dvadesetog veka tri istraživačke grupe (Ču (Chou) i Šelter (Schelter), Kapur, Kucler (Kutzler) i Stifter) su objavile uspešne rezultate.

Ostale uspešne primene metoda eliminacije na ADGT uključuju metod rezultanti (Jang (Yang), Zang (Zhang), Hu (Hou)) [16], NZD računski pristup (Kalkbrenner), pristup provere numeričkih uzoraka (Hong, Zang, Jang, Deng, Vang), metod Brauer-Sajdenberg-Vang i metod Diksonovih rezultanti.

Vuova metoda i metoda Grebnerovih baza se odnose na geometrijska tvrdjenja zadata u vidu jednakosti. Teorijski, Kolinsova metoda može dokazati (ili opovrgnuti) svaku rečenicu u geometriji Tarskog. Mnogi istraživači su se fokusirali na razvoj efikasnijih algoritama za specijalnu klasu problema koji uključuju nejednakosti. Vu je predložio metod pronalaska minimalne ili maksimalne funkcije nad polinomima pod određenim uslovima korišćenjem metode karakterističnih skupova (eng. Characteristic Sets, CS) i Lagranžovih multiplikatora.

Prethodno nabrojani radovi se odnose na elementarnu geometriju. Kako je metod karakterističnih skupova (CS) takođe primenjiv i na diferencijalne polinome [17], Vu je proširio CS metod i na dokazivanje teorema *diferencijalne geometrije*.

Sve prethodne metode imaju zajedničko da prvo prevode geometrijsku postavku u jednačine na osnovu relativnih koordinata tačaka i zatim barataju tako formiranim jednakostima. Potraga za metodama koji ne barataju koordinatama u ADGT je počela početkom osamdesetih godina prošlog veka jer se verovalo da bi se tako dobili dokazi u čitljivom obliku. Početkom devedesetih predloženo je nekoliko uspešnih nealgebarskih metoda: metoda površina (Ču, Gao, Zang) [18], vektorska metoda za konstruktivna tvrdjenja (Ču, Gao, Zang) [19], metod algebre zagrada (Rikter(Richter)-Gebert) [21] i metoda Klifordove algebre (Li i Čeng (Cheng) [22], Fevre i Vang). Eksperimenti su pokazali da su dokazi dobijeni ovim metodama generalno kraći od dokaza dobijenih algebarskim metodama. Od ovih metoda, metod površina koristi izvorne geometrijske invarijante, kao što su površina, odnos duži, Pitagorina razlika, itd. Glavna prednost ove metode je da svaki korak u dokazu ima jasno geometrijsko značenje. Program zasnovan na metodi površina je uspeo da dokaže preko 500 geometrijskih teorema i pri tom za neke od njih proizvede kraće dokaze od do tada poznatih [18].

U novije vreme, pristup zasnovan na veštačkoj inteligenciji i heuristikama je

napredovao do nivoa da može dokazati na stotine teških geometrijskih problema i proizvede kratke dokaze efikasno [23].

1.2 Implementacije algebarskih dokazivača

Od trenutka objavljivanja Vuove metode do danas, pojavilo se dosta implementacija algebarskih dokazivača. Najviše uspeha su pokazali dokazivači zasnovani upravo na Vuovoj metodi, ali ne zaostaju mnogo ni dokazivači bazirani na Grebnerovim bazama, Kolinsovoj metodi, i ostali.

Postojeće implementacije uglavnom podržavaju više metoda istovremeno. To je i razumljivo s obzirom da je veliki deo implementacije zajednički za sve algebarske metode (svođenje geometrijske teoreme na algebarski problem, algoritmi i operacije nad polinomima, itd.), dok se samo algoritmi specifični za samu metodu razlikuju¹.

Najpoznatija, i verovatno najmoćnija implementacija, je Čuvo dokazivač [4], koji nažalost nije javno dostupan. Ostali popularni dokazivači su GEX — Geometry Expert (autori Ksiao-Šin Gao, Zang i Šang Čing Ču), jGEX - java verzija programa GEX od istih autora (internet adresa: <http://www.cs.wichita.edu/~ye/>), GEOTHER (autor Dongming Vang) i MMP Geometer (autori Ksia-Šin Gao i Čiang Lin). Nažalost, do pomenutih dokazivača se teško dolazi, interfejs samih programa je komplikovan, nedostaju primeri ulaznih teorema i priručnik za korišćenje, te ne postoji širok krug korisnika.

Autoru ovog teksta nije poznata nijedna *potpuno slobodna* implementacija geometrijskih dokazivača korišćenjem algebarskih metoda (sa neke strane to je i razumljivo s obzirom na potencijalne komercijalne primene takvih programa). Zato je jedan od ciljeva ovog rada i da se pruži implementacija dokazivača koja će biti otvorena, javno dostupna, uključujući veliki broj ulaznih teorema i imati širok krug korisnika.

1.3 Motivacija istraživanja geometrijskog zaključivanja

Geometrija je oduvek zahtevala i formalni postupak i matematičku intuiciju pa je potpuno prirodno što se nametnula kao prva oblast matematike koja je počela da se istražuje u okviru veštačke inteligencije. Postoje i drugi razlozi za to, kao što je postojanje odgovarajuće vizuelne ilustracije za geometrijske probleme, što geometrijske dokaze čini pristupačnijim i razumljivijim i ne-stručnjacima iz te oblasti.

Proučavanje geometrijskog zaključivanja je doprinelo razvoju i drugih oblasti. Na primer, rad Dželerntera je doneo nove ideje u oblast automatskog rezonovanja, kao što je korišćenje modela i lema u dokazu. Sa druge strane, Vuov rad je unapređenje metode karakterističnih skupova prethodno razvijenih od strane Rita. Time je ponovo oživljeno interesovanje za rad ovoga matematičara, a primene su pronađene i u drugim oblastima van geometrije.

Na kraju, geometrijski dokazivači imaju i komercijalnu primenu. Različite aplikacije automatskog geometrijskog zaključivanja su našle svoju primenu u

¹Ovaj rad opisuje i sadrži implementacije više od jedne metode

brojnim oblastima, kao što su: učenje podržano računarima, robotika (Huang i Vu [30]), dizajn povezanih lanaca (eng. linkage design) (Gao, Zu i Huang [29]), računarska vizija (mogućnost mašine da razume slike) (Kapur i Mandi [31]), inteligentni računarski dizajn mašina (eng. computer-aided design, CAD) (Gao i Ču [27], [28]), modeliranje integralnih delova objekta (eng. solid modeling) (Vu [32]) i druge.

Glava 2

Osnovni pojmovi i definicije

U prvom delu glave navešćemo osnovne algebarske pojmove i strukture koje se pominju u tekstu (pretpostavlja se prethodno poznavanje osnovnih matematičkih pojmova kao što su skup, relacija i slično). Drugi deo glave sadrži opšte algebarske algoritme koji se koriste u većini algebarskih metoda za dokazivanje geometrijskih teorema.

2.1 Osnovne algebarske strukture

Definicija 1 (Monoid) Monoid $(M, *)$ je uređeni par skupa M i binarne relacije $*$: $M \times M \rightarrow M$ u kojem važe sledeće aksiome:

1. **Zatvorenost:** Za svako a i b iz M , $a * b$ je takođe u M .
2. **Asocijativnost:** Za svaku trojku a, b i c iz M važi:

$$a * (b * c) = (a * b) * c$$

3. **Neutralni element:** Postoji e iz M takvo da za svako a iz M važi:

$$a * e = e * a = a$$

Takvo e zovemo neutralni element monoida.

Definicija 2 (Grupa) Grupa $(G, *)$ je uređeni par skupa G i binarne relacije $*$: $G \times G \rightarrow G$ koji zadovoljava sledeće aksiome:

1. **Zatvorenost:** Za svako a i b iz G , $a * b$ je takođe u G .
2. **Asocijativnost:** Za svaku trojku a, b i c iz G važi:

$$a * (b * c) = (a * b) * c$$

3. **Neutralni element:** Postoji e iz G takvo da za svako a iz G važi:

$$a * e = e * a = a$$

Takvo e zovemo neutralni element grupe.

4. **Inverzni element:** Za svako a iz G , postoji b iz G za koje važi:

$$a * b = e$$

gde je e neutralni element grupe.

Definicija 3 (Komutativna grupa) Grupa $(G, *)$ u kojoj važi komutativnost, odnosno za svako a i b iz G važi:

$$a * b = b * a$$

se naziva komutativna ili Abelova grupa.

Definicija 4 (Prsten) Prsten $(R, +, *, 0, 1)$ je uređena petorka skupa R i dve binarne relacije $+$: $R \times R \rightarrow R$ i $*$: $R \times R \rightarrow R$ u kome važe sledeće aksiome prstena:

1. $(R, +)$ je komutativna grupa sa neutralnim elementom 0
2. $(R, *)$ je monoid sa neutralnim elementom 1
3. Relacija $*$ distribuira nad relacijom $+$, odnosno važe sledeće dve jednakosti:

$$a * (b + c) = a * b + a * c$$

$$(a + b) * c = a * c + b * c$$

gde su a, b i c proizvoljni elementi skupa R .

Definicija 5 (Komutativni prsten) Prsten $(R, +, *, 0, 1)$ je komutativni prsten ako je operacija $*$ komutativna, odnosno ako za svako a i b iz skupa R važi:

$$a * b = b * a$$

Definicija 6 (Polje) Prsten $(R, +, *, 0, 1)$ je polje ako je uređeni par $(R \setminus \{0\}, *)$ grupa sa neutralnim elementom 1 .

2.2 Polinomi

Polinomi su jedna od osnovnih algebarskih struktura i predstavljaju izvesno proširenje prstena. U ovom poglavlju daćemo manje formalnu definiciju polinoma više promenljivih.

Definicija 7 (Polinomsko proširenje prstena) Algebarska struktura $K[x]$, gde je K prsten a x novi objekat ili promenljiva, predstavlja proširenje prstena K i definiše se kao skup svih objekata oblika:

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0$$

za neko $n \geq 0$, gde su koeficijenti a_i iz prstena K ($a_i \in K$). Navedene objekte nazivamo polinomima jedne promenljive nad prstenom K . Indeks n nazivamo stepen polinoma $p(x)$ i pišemo:

$$\deg(p) = n$$

Definicija 8 (Term polinoma) *Faktore oblika $a_i x^i$ iz definicije polinoma nazivamo termima. Broj ne-nula termova (term čiji vodeći koeficijent nije jednak nuli) koje sadrži polinom je broj termova polinoma.*

Primitimo da iz definicije sledi da je $K \subset K[x]$. Ovako definisan skup polinoma $K[x]$ je zatvoren u odnosu na operacije sabiranja i deljenja, pa samim tim važi i naredna teorema:

Teorema 1 (Prsten polinoma) *Polinomi na prstenu K predstavljaju prsten u odnosu na operacije sabiranja i množenja, gde su nula (neutralni element) i jedinica isti kao i u prstenu K . Ukoliko je K komutativni prsten, tada je i $K[x]$ komutativni prsten.*

Kao što smo proširenjem prstena K dobili prsten $K[x]$, na isti način možemo proširiti prsten $K[x]$ novom promenljivom y i dobiti prsten $K[x][y]$. Ovako dobijeno proširenje zapisujemo i u obliku $K[x, y]$. Prsten $K[x, y]$ nazivamo *prsten polinoma dve promenljive nad prstenu K* .

Nastavljajući opisani proces, dolazimo do definicije prstena polinoma više promenljivih nad prstenu K .

Definicija 9 (Polinomi više promenljivih) *Prsten polinoma promenljivih $(x_1, x_2, \dots, x_r) = \mathbf{x}$ nad prstenu K označavamo sa $K[x_1, \dots, x_r]$ (ili $K[\mathbf{x}]$) i definišemo kao skup objekata sledećeg oblika:*

$$p(x_1, x_2, \dots, x_r) = p(\mathbf{x}) = \sum_{i=0}^n a_i x_1^{t_{1,i}} x_2^{t_{2,i}} \dots x_r^{t_{r,i}}$$

gde su koeficijenti a_i iz prstena K .

Definicija 10 (Monomi) *Monični polinomi (monomi) nad prstenu $K[x]$ su svi polinomi oblika:*

$$x^k$$

za neko prirodno k . Nula se ne smatra monomom.

Polinome možemo da definišemo kao funkcije.

Definicija 11 (Funkcija polinoma) *Polinom p iz prstena $K[\mathbf{x}]$ je funkcija koja slika K^r u K . Vrednost u tački $\mathbf{k} = (k_1, \dots, k_r) \in K^r$ se definiše kao:*

$$p(\mathbf{k}) = \sum_{i=0}^n a_i k_1^{t_{1,i}} k_2^{t_{2,i}} \dots k_r^{t_{r,i}}$$

gde je polinom $p(\mathbf{x})$ definisan kao u definiciji 9.

Definicija 12 (Nule polinoma) *Nule polinoma $p(\mathbf{x})$ iz prstena $K[\mathbf{x}]$ su sve tačke $\mathbf{k} = (k_1, \dots, k_r) \in K^r$ za koje važi:*

$$p(\mathbf{k}) = p(k_1, k_2, \dots, k_r) = 0$$

Skup svih nula polinoma $p(\mathbf{x})$ označavamo sa $V(p)$.

Definicija 13 (Sistem polinoma) Skup polinoma (p_1, p_2, \dots, p_n) nad prstenom $K[\mathbf{x}]$ nazivamo sistem polinoma. Zajedničke nule svih polinoma iz sistema označavamo sa:

$$V(p_1, \dots, p_n)$$

Lako je pokazati da važi:

$$V(p_1, \dots, p_n) = V(p_1) \cap V(p_2) \cap \dots \cap V(p_n)$$

Definicija 14 (Ideal) Ideal I prstena K je struktura za koju važi:

- $(I, +)$ je pod-grupa grupe $(K, +)$
- Za svako $a \in I$ i $k \in K$ važi $ka \in I$.

Ovom definicijom je obuhvaćen i ideal nad prstenom polinoma $K[\mathbf{x}]$.

Definicija 15 (Ideal polinoma) Ideal I nad prstenom polinoma $K[\mathbf{x}]$ generisan sistemom polinoma (p_1, p_2, \dots, p_n) je definisan kao:

$$I = \{Q_1 p_1 + \dots + Q_r p_r \mid Q_j \in K[\mathbf{x}]\}$$

Lako je pokazati valjanost prethodne definicije, odnosno da skup iz definicije zadovoljava aksiome ideala.

Teorema 2 (Hilbertova osnovna teorema) Svaki ideal nad prstenom polinoma $K[\mathbf{x}]$ je generisan konačnim sistemom polinoma.

Dakle, za svaki ideal iz prstena polinoma, postoji sistem polinoma (p_1, p_2, \dots, p_n) koji ga generiše.

2.3 Osnovni algebarski algoritmi

U ovom poglavlju razmotrićemo neke algoritme i teoreme opšteg tipa koje se koriste u Vuovoj i ostalim algebarskim metodama.

2.3.1 Algoritam pseudo-deljenja

Jedna od osnovnih operacija u algebarskim metodama je *pseudo-deljenje* polinoma (poznato i kao *ostatak pri deljenju polinoma*).

Definicija 16 (Polu-ostatak pri deljenju polinoma) Neka je A komutativni prsten (na primer, prsten polinoma $Q[y_1, \dots, y_m]$ gde je Q komutativni prsten). Neka su $f = a_n v^n + \dots + a_0$ i $h = b_k v^k + \dots + b_0$ dva polinoma iz $A[v]$ gde je v nova promenljiva. Polu-ostatak pri deljenju polinoma f polinomom h po promenljivoj v definišemo na sledeći način:

$$\text{poluostatak}(f, h) = b_k f - a_n v^{n-k} h$$

Definicija 17 (Pseudo-deljenje polinoma) *Koristeći oznake iz prethodne definicije, razmotrimo sledeći lanac deljenja sa polu-ostatkom polinoma:*

$$\begin{aligned} r_0 &= f \\ r_1 &= \text{poluostatak}(r_0, h) \\ &\dots \\ r_i &= \text{poluostatak}(r_{i-1}, h) \end{aligned}$$

Neka je $m_i = \deg(r_i, v)$ stepen polinoma r_i . Za $m_i \geq k$ važi da je $m_i > m_{i+1}$. Za najmanje t takvo da važi $m_t < k$ (što se mora desiti u konačnom broju koraka) definiše se rezultat pseudo-deljenja na sledeći način:

$$\text{prem}(f, h, v) = r_t$$

Algoritam pseudo-deljenje se može iskoristiti u primeni euklidovog algoritma nad polinomima i tako izračunati najveći zajednički delilac dva ili više polinoma.

Primer 1 (Algoritam pseudo-deljenja) *Neka su data dva polinoma:*

$$\begin{aligned} p(x) &= x^5 + x^4 - x^2 - x + 2 \\ q(x) &= x^5 - 2x^4 + 2x^3 - x^2 + x + 1 \end{aligned}$$

Ponavljaćemo pseudo-deljenje na dva poslednja rezultata sve dok ne dobijemo rezultat nula:

$$\begin{aligned} r(x) &= \text{prem}(p, q) = 3x^4 - 2x^3 + 4x^2 - 2x + 1 \\ s(x) &= \text{prem}(q, r) = -2x^3 + 13x^2 - 2x + 13 \\ t(x) &= \text{prem}(r, s) = x^2 + 1 \\ u(x) &= \text{prem}(s, t) = 0 \end{aligned}$$

Ovim smo dobili da je $NZD(p, q) = t(x) = x^2 + 1$. Pošto smo pronašli zajednički faktor dva polinoma, možemo ih faktorisati i napisati u prostijem obliku:

$$\begin{aligned} p(x) &= (x^2 + 1)(x^3 + x^2 - x + 2) \\ q(x) &= (x^2 + 1)(x^3 - 2x^2 + x + 1) \end{aligned}$$

Teorema 3 (Ostatak pseudo deljenja) *Za ostatak pseudo deljenja u oznakama definicije 16 važi sledeća formula:*

$$b_k^s f = qh + r_t, \text{ gde je } s \leq n - k + 1 \text{ i } \deg(r_0, v) < \deg(h, v) \quad (2.1)$$

Dokaz: Dokazuje se indukcijom po $n = \deg(f, v)$ za fiksno h . Ako je $n < k$, tada je $r_t = r_0 = f$ i $f = 0 \cdot h + r_0$. Pretpostavimo da je $n \geq k$ i da formula 2.1 važi za sve polinome f za koje je $\deg(f, v) < n$. Posle prve iteracije važi $r_1 = b_k f - a_n v^{n-k} h$, gde je a_n vodeći koeficijent of f . Pošto je $\deg(r_1, v) < n$ na osnovu induktivne pretpostavke važi $b_k^l r = q_1 h + r_0$. Zamenom u prethodnoj formuli tvrđenje je dokazano. \square

2.3.2 Algoritam sukcesivnog pseudo-deljenja

U ovom delu će biti izložene definicije trougaone forme sistema polinoma, sukcesivnog pseudo-deljenja i formula ostatka, koje se koriste u Vuovoj metodi.

Definicija 18 (Trougaona forma) *Sistem polinoma (h_1, h_2, \dots, h_n) nad nezavisnim promenljivama (x_1, x_2, \dots, x_n) je trougaoni ako svaki polinom h_i u nizu sadrži najviše jednu novu promenljivu x_j koja nije sadržana ni u jednom prethodnom polinomu (h_1, \dots, h_{i-1}) .*

Definicija 19 (Sukcesivno pseudo deljenje) *Pretpostavimo da je sistem polinoma f_1, f_2, \dots, f_r iz prstena polinoma $K[u_1, \dots, u_d, x_1, \dots, x_r]$ u trougaonoj formi. Bez umanjenja opštosti, možemo preimenovati promenljive tako da se sistem bude u obliku:*

$$\begin{aligned} f_1(u_1, \dots, u_d, x_1) \\ f_2(u_1, \dots, u_d, x_1, x_2) \\ \dots \\ f_r(u_1, \dots, u_d, x_1, x_2, \dots, x_r) \end{aligned} \tag{2.2}$$

Neka je dat polinom $g = g(u_1, \dots, u_d, x_1, \dots, x_r)$ i neka je sukcesivno primenjen algoritam pseudo-deljenja dat definicijom 17:

$$\begin{aligned} R_{r-1} &= \text{prem}(g, f_r, x_r) \\ R_{r-2} &= \text{prem}(R_{r-1}, f_{r-1}, x_{r-1}) \\ &\dots \\ R_0 &= \text{prem}(R_1, f_1, x_1) \end{aligned}$$

R_0 se naziva poslednji ostatak i označava se skraćeno sa $\text{prem}(g, f_r, \dots, f_1)$.

Teorema 4 (Formula ostatka) *Neka su f_1, \dots, f_r i g zadati kao u definiciji 19. Tada postoje nenegativni celi brojevi s_1, \dots, s_r i polinomi Q_1, \dots, Q_r takvi da je:*

- (1) $I_1^{s_1} \cdots I_r^{s_r} g = Q_1 f_1 + \dots + Q_r f_r + R_0$, gde je I_i vodeći koeficijent polinoma f_i .
- (2) $\text{deg}(R_0, x_i) < \text{deg}(f_i, x_i)$, za svako $i = 1, \dots, r$.

Dokaz: Koristimo indukciju po r . Ako je $r = 1$ tada se formula svodi na 2.1. Pretpostavimo da je $r > 1$ i da formula važi za $r - 1$, tj.

$$I_1^{s_1} \cdots I_{r-1}^{s_{r-1}} R_{r-1} = Q_1 f_1 + \dots + Q_{r-1} f_{r-1} + R_0$$

i $\text{deg}(R_0, x_i) < \text{deg}(f_i, x_i)$ za svako $i = 1, \dots, r - 1$. Kombinujući sa $R_{r-1} = I_r^{s_r} g - Q_r f_r$, (takođe posledica teoreme 2.1) dobijamo (1) i (2). \square

2.3.3 Jednostavan algoritam svođenja na trougaonu formu

Postoji puno načina da se sistem polinoma svede na trougaonu formu. Ovde će biti predstavljen jedan od najjednostavnijih algoritama, po svom obliku veoma sličan Gausovoj metodi eliminacije za sistem linearnih jednačina.

Pretpostavimo da je dat sistem polinoma nad prstenom polinoma $K[\mathbf{u}, \mathbf{x}]$:

$$\begin{aligned} h_1(u_1, \dots, u_d, x_1, \dots, x_r) &= 0 \\ h_2(u_1, \dots, u_d, x_1, \dots, x_r) &= 0 \\ &\dots \\ h_r(u_1, \dots, u_d, x_1, \dots, x_r) &= 0 \end{aligned} \tag{2.3}$$

Ovakav sistem polinoma, videćemo kasnije, na algebarski način opisuje geometrijsku konstrukciju. Parametri u_i su nezavisne promenljive i označavaju opšti karakter geometrijske konstrukcije (proizvoljna prava, proizvoljna tačka, itd.). Parametri x_i su zavisne promenljive i označavaju geometrijske uslove (koordinata preseka dveju pravih, normala iz tačke na pravu, itd.). Svaki polinom iz sistema je jedna hipoteza geometrijske konstrukcije. Broj zavisnih promenljivih je jednak broju hipoteza, odnosno svaka hipoteza određuje jednu zavisnu promenljivu. Nakon postupka transformisanja geometrijskog tvrđenja, broj hipoteza i zavisnih promenljivih po pravilu moraju biti jednaki.

Da bi se početni sistem sveo na trougaonu formu, najpre se može eliminisati promenljiva x_r iz $r - 1$ polinoma da bi se dobio sledeći sistem:

$$\begin{aligned} f'_1(u_1, \dots, u_d, x_1, \dots, x_{r-1}) &= 0 \\ &\dots \\ f'_{r-1}(u_1, \dots, u_d, x_1, \dots, x_{r-1}) &= 0 \\ f'_r(u_1, \dots, u_d, x_1, \dots, x_r) &= 0 \end{aligned} \tag{2.4}$$

Zatim se isti postupak primenjuje na prvih $r - 1$ polinoma da bi promenljiva x_{r-1} bila eliminisana iz svih osim jednog polinoma, i tako redom.

Eliminacija promenljive x_r iz $r - 1$ polinoma se izvodi na sledeći način:

Slučaj I Ako se x_r ne pojavljuje ni u jednom polinomu iz skupa od r polinoma, algoritam se prekida i daje se obaveštenje o tome. Radi se o grešci u primeni procedure, tj. pogrešan je izbor parametara tvrđenja.

Slučaj II Ako se promenljiva x_r pojavljuje u samo jednom polinomu f_i , tada se taj polinom postavlja na mesto polinoma f_r . Time je zadovoljena forma 2.4.

Slučaj III Ako jedan polinom f_i ima stepen 1 u odnosu na promenljivu x_r , tj. $\deg(f_i, x_r) = 1$, tada se svi ostali polinomi mogu podeliti tim polinomom i iz njih eliminisati promenljiva x_r . Polinom f_i se postavlja na mesto polinoma f_r i svaki polinom f_j , $j = 1, \dots, r - 1$, zamenjuje se polinomom $f'_j = \text{prem}(f_j, f_i, x_r)$. Time je zadovoljena forma 2.4.

Slučaj IV Postoji više polinoma koji sadrže promenljivu x_r i nijedan od njih nije stepena jedan. Potrebno je izabrati dva polinoma koji imaju minimalni stepen po promenljivoj x_r , neka su to f_r i f_{r-1} (ukoliko se radi o

polinomima sa drugim indeksima, izvršiti odgovarajuću zamenu). Pretstavimo da je $\deg(f_{r-1}, x_r) \leq \deg(f_r, x_r)$. Neka je:

$$r_1 = \text{prem}(f_r, f_{r-1}, x_r)$$

tada je $\deg(r_1, x_r) < \deg(f_{r-1}, x_r)$ (u geometrijskim primerima, često je $\deg(r_1, x_r) = \deg(f_{r-1}, x_r) - 1$). Ako je $\deg(r_1, x_r) > 1$, neka su:

$$r_2 = \text{prem}(f_{r-1}, r_1, x_r)$$

$$r_3 = \text{prem}(r_1, r_2, x_r)$$

i tako dalje, sve dok za neko k nije zadovoljen jedan od sledećih uslova:

1. $\deg(r_k, x_r) = 1$. Uzeti r_k i r_{k-1} za nove vrednosti polinoma f_r i f_{r-1} i vratiti se na **slučaj III**.
2. $r_k = 0$. Zaključujemo da polinomi f_r i f_{r-1} imaju zajednički delilac i da je početni sistem polinoma svodiv. Pošto je ovo jednostavna procedura, ovakvi slučajevi se neće rešavati. Algoritam se zaustavlja uz odgovarajuće obaveštenje (ovakva situacija se retko dešava u geometrijskim problemima).
3. $\deg(r_{k-1}, x_r) > 1$ i $\deg(r_k, x_r) = 0$ (odnosno r_k je slobodan od x_r). Uzeti r_k i r_{k-1} za nove vrednosti polinoma f_r i f_{r-1} i vratiti se na **slučaj II**.

Glava 3

Algebarsko dokazivanje geometrijskih teorema

Algebarska geometrija je oblast matematike koja kombinuje abstraktnu algebru i geometriju. Rene Dekart je prvi uočio jasnu povezanost ove dve oblasti stavivši u istu ravan i geometrijsku sliku i koordinatni sistem. Centralni deo algebarske geometrije je izučavanje sistema polinoma više promenljivih koji se dobija kada se geometrijski objekti i odnosi predstave na analitički način.

Iako je algebarska geometrija primenjiva na sve tipove geometrija, ovaj rad će se baviti isključivo euklidskom geometrijom. Mnogi rezultati prikazani u tekstu su opšteg tipa i važe u svim geometrijama, a na nekim mestima će to biti i naglašeno.

3.1 Propusti u tradicionalnim dokazima

Da bi se mehanički izveli dokazi geometrijskih teorema, moraju se striktno poštovati pravila i aksiome geometrije. Pokazuje se da su naizgled trivijalni dokazi veoma teški ukoliko se traži kompletan i striktan dokaz.

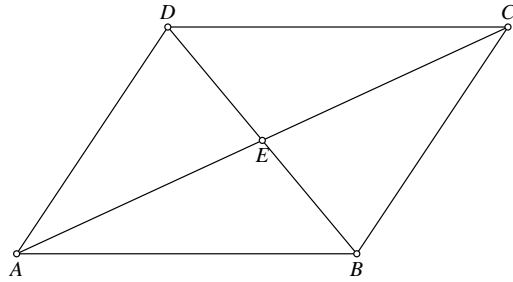
3.1.1 Tradicionalni euklidski dokaz

Jedan od glavnih propusta u tradicionalnim euklidskim dokazima je zanemari-vanje uslova kao što su uslovi vezani za *dve strane jedne prave* i *unutrašnjost ugla*.

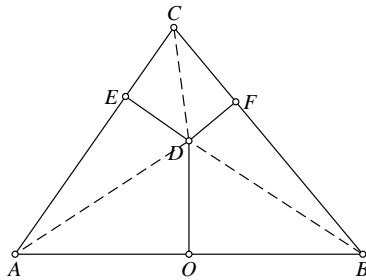
Razmotrimo najpre sledeći primer i tradicionalni analitički dokaz.

Primer 2 *Neka je dat paralelogram $ABCD$ ($AB \parallel CD$, $BC \parallel AD$) i neka je E presek dijagonala AC i BD . Dokazati da je $AE = CE$ (slika 3.1).*

Tradicionalni dokaz ove teoreme počinje time što se pokaže da je $\triangle ACB \cong \triangle CAD$ (iz čega sledi da je $AE \cong CE$). U dokazu podudarnosti ovih trouglova, koristi se činjenica da je $\angle CAB \cong \angle ACD$. Ovo je „očigledno” na osnovu slike imajući u vidu da se radi o alternirajućim uglovima u odnosu na dve paralelne prave AB i CD . Ovde je implicitno pretpostavljena „trivijalna činjenica” da su tačke D i B na suprotnim stranama prave AC . Međutim, ovu „trivijalnu činjenicu” je teže dokazati nego sam problem!



Slika 3.1: Paralelogram



Slika 3.2: Svaki trougao je jednakostraničan

Ovaj jednostavan primer pokazuje teškoće u implementaciji geometrijskih dokazivača polazeći od tradicionalnih dokaza. Najlogičnije rešenje je pored aksioma, dokazivač snabdeti i teoremama koje se mogu koristiti u cilju ubrzanja i proizvođenja kraćih i razumljivijih dokaza. Jedna takva teorema može biti „trivijalna činjenica” navedena u prethodnom primeru, pa bi se ta i ostale teoreme mogle čuvati u bazi podataka gde bi bile dostupne dokazivaču. Međutim, ovakav pristup povlači za sobom niz drugih problema, kao što je, na primer, konzistentnost dokaza što ilustruje naredni primer.

Primer 3 (Svaki trougao je jednakostraničan) *Ako je ABC proizvoljan trougao onda važi da je $CA \cong CB$ (slika 3.2).*

Dokaz: Neka je D presek simetrale duži AB i bisektrise ugla ACB . Neka su DE i DF podnožja normala iz tačke D na prave AC i BC redom. Lako

se pokazuje da je $\triangle CDE \cong \triangle CDF$ i $\triangle ADE \cong \triangle BDF$. Stoga je $CE + EA = CF + FB$, odnosno $CA \cong CB$. \square

Naravno, u pitanju je kontradikcija, ovaj „dokaz“ nikako ne može biti tačan. Ali indikativno je kako korišćenje pomoćnih teorema (ne idući u dokazu do samih aksioma) može dovesti i do ovakvih „dokaza“.

3.1.2 Primer algebarskog dokaza

Analitički dokaz tvrđenja 3 bi izgledao otprilike ovako:

Neka je u ravni dat Dekartov koordinatni sistem i neka u njemu tačke imaju sledeće koordinate: $A = (0, 0)$, $B = (u_1, 0)$, $C = (u_2, u_3)$, $D = (x_2, x_1)$, i $E = (x_4, x_3)$. Tvrđenje zadatka ($AE \cong CE$) je sada ekvivalentno jednakosti $g = 2u_2x_4 + 2u_3x_3 - u_3^2 - u_2^2 = 0$.

Fiksirajmo tačke A , B i C . Na osnovu jednačina za prave AD i CD možemo odrediti koordinate tačke D , a na osnovu jednačina za prave BD i AC možemo odrediti koordinate tačke E . Zatim zamenom dobijenih vrednosti u polinom g možemo utvrditi da li je jednakost tačna.

Dve jednačine za određivanje koordinata tačke D , odnosno za rešavanje nepoznatih x_1 i x_2 su:

$$\begin{aligned} AB \parallel CD: \quad h_1 &= u_1x_1 - u_1u_3 = 0 \\ DA \parallel CB: \quad h_2 &= u_3x_2 - (u_2 - u_1)x_1 = 0 \end{aligned}$$

Slično, dve jednačine za određivanje nepoznatih x_3 i x_4 su:

$$\begin{aligned} E \text{ pripada } BD: \quad h_3 &= x_1x_4 - (x_2 - u_1)x_3 - u_1x_1 = 0 \\ E \text{ pripada } AC: \quad h_4 &= u_3x_4 - u_2x_3 = 0 \end{aligned}$$

Rešavanjem prve dve jednačine dobijamo $x_1 = u_3$ i $x_2 = u_2 - u_1$. Rešavanjem poslednje dve jednačine i korišćenjem dobijenih vrednosti za x_1 i x_2 dobijamo $x_3 = u_3/2$ i $x_4 = u_2/2$. Konačno, zamenom svih vrednosti u g dobijamo da je $g = 0$. Time je dokaz završen.

Navedeni dokaz je sličan dokazu koji je koristio P. J. Dejvis da bi dokazao Paposovu teoremu na računaru [11].

Jedan problem sa ovakvim dokazom je u tome što nisu naglašeni uslovi nedegenerisanosti bez kojih tvrđenje teoreme može biti i netačno. Nije naglašena činjenica da smo dokazali da je geometrijsko tvrđenje tačno samo u „opštem“ slučaju. Na primer, da bismo dobili gornja rešenja za nepoznate x_1, x_2, x_3 i x_4 , moramo pretpostaviti $u_1 \neq 0$ i $u_3 \neq 0$, tj. *uslove nedegenerisanosti* da tačke A , B i C nisu kolinearne.

3.2 Geometrijska tvrđenja konstruktivnog tipa

Uslovi nedegenerisanosti (NDG uslovi) za geometrijsku teoremu se mogu navesti u čitljivoj, geometrijskoj formi (na primer: *nekolinearne tačke, dve prave imaju presek, dva kruga imaju presek* i tako dalje). Međutim, automatsko određivanje NDG uslova i njihovo navođenje u takvoj formi je izuzento težak problem koji do sada nije rešen u opštem slučaju. Problem je delimično rešen za određene

klase geometrijskih teorema, kao, na primer, kod Vuove metode za klasu konstruktivnih geometrijskih teorema. Ova klasa geometrijskih tvrdjenja nije restriktivnog karaktera i, kao što ćemo videti, obuhvata većinu poznatih teorema.

Zbog jednostavnosti, govorimo samo o geometriji ravni, ali su opšti principi proširivi i na prostornu geometriju.

Definicija 20 (Konstrukcija prave) *Neka je Π konačan skup tačaka. Kažemo da je prava l konstruisana direktno iz Π ako:*

- l sadrži dve tačke A i B iz Π
- l sadrži jednu tačku C iz Π i paralelna je sa pravom određenom dvema tačkama A i B iz Π
- l sadrži jednu tačku C iz Π i normalna je na pravu određenu dvema tačkama A i B iz Π
- l je simetrala duži AB , gde su A i B iz Π

Prava l konstruisana direktno iz Π je *dobro definisana* ako su tačke A i B iz definicije 20 različite.

Slično se može definisati *direktna konstrukcija kruga* u Π , odabirom dve različite tačke O i A tako da je O centar kruga i OA poluprečnik kruga.

Definicija 21 (Geometrijske teoreme konstruktivnog tipa) *Geometrijska teorema je konstruktivnog tipa ako tačke, prave i krugovi u tvrdjenju mogu biti konstruisani na konačan način korišćenjem sledećeg skupa konstrukcija, gde je Π skup tačaka prethodno konstruisan:*

- Konstrukcija 1: *Biranje nove, proizvoljne tačke. Za koordinate tačke se uzimaju nove slobodne promenljive (u_i, u_{i+1}) .*
- Konstrukcija 2: *Biranje nove, proizvoljne prave. Svodi se na biranje dve nove tačke.*
- Konstrukcija 3: *Biranje novog, proizvoljnog kruga. Svodi se na biranje dve nove tačke.*
- Konstrukcija 4: *Biranje proizvoljne prave koja sadrži postojeću tačku. Svodi se na biranje nove tačke.*
- Konstrukcija 5: *Biranje proizvoljnog kruga sa poznatim centrom. Svodi se na biranje nove tačke.*
- Konstrukcija 6: *Biranje proizvoljne tačke na postojećoj pravoj. Za koordinate tačke se uzima jedna nova slobodna promenljiva i jedna nova zavisna promenljiva (u_i, x_j) (ili (x_j, u_i)).*
- Konstrukcija 7: *Biranje proizvoljne tačke na krugu. Za koordinate tačke se uzima jedna nova slobodna promenljiva i jedna nova zavisna promenljiva (u_i, x_j) .*
- Konstrukcija 8: *Tačka određena presekom dve postojeće prave. Za koordinate tačke se uzimaju dve nove zavisne promenljive (x_j, x_{j+1}) .*

- Konstrukcija 9: Tačka određena presekom prave i kruga. Za koordinate tačke se uzimaju dve nove zavisne promenljive (x_j, x_{j+1}) .
- Konstrukcija 10: Tačka određena presekom dva kruga. Za koordinate tačke se uzimaju dve nove zavisne promenljive (x_j, x_{j+1}) .
- Konstrukcija 11: Tačka koja je podnožje normale iz postojeće tačke na postojeću pravu. Za koordinate tačke se uzimaju dve nove zavisne promenljive (x_j, x_{j+1}) .
- Konstrukcija 12: Prava koja je bisektrisa ugla koji određuju dve postojeće prave. Svodi se na konstrukciju jedne tačke te prave (druga tačka je teme ugla). Za koordinate tačke se uzimaju dve nove zavisne promenljive (x_j, x_{j+1}) .
- Konstrukcija 13: Tačka koja je simetrala duži određene dvema postojećih tačaka. Za koordinate tačke se uzimaju dve nove zavisne promenljive (x_j, x_{j+1}) .

Definicija 22 (Konstruktivno tvrđenje) Konstruktivno tvrđenje je relacija jednakosti među konstruisanim tačkama.

Treba napomenuti da ovo nije konačan skup konstrukcija. Na sličan način se, na primer, mogu dodati konstrukcije vezane za krive drugog reda i neke druge konstrukcije.

Izbor koordinata se može dodatno pojednostaviti. Prva tačka umesto koordinata (u_1, u_2) može imati koordinate $(0, 0)$, dok druga tačka može imati koordinate $(u_1, 0)$. Ukoliko je neka prava paralelna sa x ili y osom, sve tačke na toj pravoj će imati iste y , odnosno x koordinate.

Neke konstrukcije u pojedinim situacijama mogu biti nekonzistentne sa prethodnim konstrukcijama. Na primer, *konstrukcija 8* ne određuje novu tačku ukoliko su dve prave paralelne. Ovakvi slučajevi se retko dešavaju, zato što se teoreme obično zadaju u ispravnom obliku. Većina metoda za automatsko dokazivanje geometrijskih teorema može automatski otkriti nedoslednost i nekonzistentnost konstrukcija i to prijaviti korisniku.

3.3 Prevođenje geometrijskih konstrukcija u polinome

Jedan od problema kod korišćenja algebarskih metoda jeste rešavanje geometrijskih tvrđenja koja uključuju veličine kao što su mera duži, mera ugla i slične. Mera duži se ne može predstaviti polinomom i da bi se iskazala jednakost koja uključuje ovu meru u obliku polinoma izraz se mora osloboditi operacije korenovanja. Prosto kvadriranje nije dozvoljeno zato što se nakon kvadriranja ne dobija ekvivalentan izraz. Ovaj problem je tesno povezan sa definisanom orijentacijom u geometriji (u euklidskoj geometriji su definisani orijentacija duži, orijentacija površine i orijentacija ugla).

Stoga, većina algebarskih metoda ne može u opštem slučaju rešavati teoreme u kojima se pominje rastojanje između tačaka i druge pomenute mere. Ipak, takve teoreme je u velikom broju slučajeva moguće preformulisati tako da se ovaj problem izbegne (videćemo kako).

Neka su date tačke A, B, C, D, E, F, G i H i neka su koordinate tačke $X = (x_1, x_2)$, gde je X iz skupa prethodno navedenih tačaka.

1. Za tvrđenje " $AB \cong CD$ ", koristićemo kvadrat rastojanja između dve tačke:

$$\overline{AB}^2 - \overline{CD}^2 = (a_1 - b_1)^2 + (a_2 - b_2)^2 - (c_1 - d_1)^2 - (c_2 - d_2)^2 = 0$$

2. "Tačke A, B i C su kolinearne", ili "tačka A pripada pravoj BC ". Ekvivalentna polinomna jednakost je:

$$(a_1 - b_1)(b_2 - c_2) - (a_2 - b_2)(b_1 - c_1) = 0$$

3. " $AB \parallel CD$ ":

$$(a_1 - b_1)(c_2 - d_2) + (a_2 - b_2)(c_1 - d_1) = 0$$

4. " $AB \perp CD$ ":

$$(a_1 - b_1)(c_1 - d_1) + (a_2 - b_2)(c_2 - d_2) = 0$$

5. "Tačka A pripada krugu sa prečnikom BC " je ekvivalentno sa $BA \perp CA$.

6. " B je središte duži AC " je ekvivalentno uslovima da B pripada pravoj AC i dve duži AB i BC su podudarne. Pošto se radi o kolinearnim tačkama, nema razloga da se razmatr sâmo rastojanje, dovoljan je uslov:

$$2b_1 - a_1 - c_1 = 0 \wedge 2b_2 - a_2 - c_2 = 0$$

7. " $AB \cdot CD = EF \cdot GH$ ":

$$\overline{AB}^2 \cdot \overline{CD}^2 - \overline{EF}^2 \cdot \overline{GH}^2 = 0$$

8. " $kAB = lCD$ ":

$$k^2 \overline{AB}^2 - l^2 \overline{CD}^2 = 0$$

9. "Algebarska suma duži AB, CD i EF jednaka je nuli". Ovaj uslov se koristi kada želimo da navedemo da je jedna duž jednaka zbiru druge dve (u opštem slučaju, ove tri duži ne moraju biti paralelne). Zbog ograničenja metode (ne možemo koristiti pravu meru duži pošto ta veličina koristi operaciju korenovanja kada se prevede u algebarski oblik), koristimo ovaj slabiji uslov — da je algebarska suma te tri duži jednaka nuli.

Pošto suma ili razlika dve duži traži orijentaciju (koju pokušavamo da izbegnemo), ovaj uslov se razmatra na sledeći način. Neka je $x^2 = \overline{AB}^2$, $y^2 = \overline{CD}^2$ i $z^2 = \overline{EF}^2$. Traženi uslov je ekvivalentan sa:

$$(x - y - z)(x - y + z)(x + y - z)(x + y + z) = 0$$

Interpretacija je sledeća: poznati su nam kvadrati rastojanja, ali ne i sama rastojanja. Pošto krajnja suma treba biti jednaka nuli, moramo uzeti u obzir sve kombinacije suma po vrednostima x, y i z , zato što neke vrednosti mogu biti i negativne. Takvih kombinacija ima $2^3 = 8$, ali je dovoljno uzeti četiri od njih (preostale četiri su negacije neke od prve četiri).

10. "Krugovi (A, BC) i (D, EF) se dodiruju". Ekvivalentno sa uslovom da je algebarska suma duži AD , BC i EF jednaka nuli. Algebarskom metodom ne mogu se razlikovati slučajevi unutrašnjeg i spoljašnjeg dodirivanja (kao ni unutrašnji i spoljašnji ugao, itd.).

Kao što je pomenuto, kod neuređenih geometrija ne može se raditi "dodavanje" ili "oduzimanje" duži. Ipak, kada je reč o dužima na istoj ili paralelnim pravama, onda se može u potpunosti baratati sa orijentisanim dužima. To je stoga što umesto dužine duži, možemo koristiti udaljenost između x ili y koordinata, a pošto se radi o dužima na paralelnim pravama, svi odnosi će biti jednaki do na konstantni faktor.

11. "Odnos orijentisanih duži $\overline{AB}/\overline{CD}$ gde je $AB \parallel CD$ " je ekvivalentan sa jednim od:

$$(b_1 - a_1)/(d_1 - c_1) \vee (b_2 - a_2)/(d_2 - c_2)$$

Prva vrednost se može koristiti kada prave nisu paralelne y osi, dok se druga vrednost može koristiti kada prave nisu paralelne x osi. Ukoliko je u problemu zadata veličina odnosa dve duži, može se pretpostaviti da je odgovornost onoga koji je postavio teoremu da su duži paralelne ili se to može dokazati od strane dokazivača.

12. "Tačke A, B, C i D su harmonijski spregnute". Tačke A, B, C i D moraju biti kolinearne, i tada se ovaj uslov prevodi u sledeću jednakost:

$$\overline{AC}/\overline{AB} = \overline{DA}/\overline{DB}$$

13. "Unakrsni proizvod tačaka A, B, C i D " se definiše kao:

$$\frac{\overline{CA}}{\overline{CB}} \cdot \frac{\overline{DB}}{\overline{DA}}$$

14. " $\overline{AB} - \overline{CD} - \overline{EF} + \overline{EA} = 0$ " je ekvivalentno sa:

$$(b_1 - a_1) - (d_1 - c_1) - (f_1 - e_1) + (a_1 - e_1) = 0$$

ili

$$(b_2 - a_2) - (d_2 - c_2) - (f_2 - e_2) + (a_2 - e_2) = 0$$

Prva jednakost važi ukoliko prava nije paralelna y osi, dok druga jednakost važi ukoliko prava nije paralelna x osi.

15. Umesto podudarnosti uglova, da bismo zaobišli problem sa orijentacijom, korišćemo slabiji uslov — kongruencija uglova. Dva ugla pripadaju istoj klasi ako i samo ako su podudarni ili se dopunjuju do pravog ugla (tj. tangens uglova je jednak).

Funkcija " $tg(\angle ABC)$ " se definiše na sledeći način: neka su k_1 i k_2 uglovi između pravih BA i BC i x ose (ta vrednost se može definisati kao $(a_1 - b_1)/(a_2 - b_2)$ ili ∞ ukoliko je $a_2 = b_2$). Tangens ugla tada je jednak:

$$\begin{aligned} (k_2 + k_1)/(1 - k_1 k_2) & \text{ ako je } k_1 \neq \infty \wedge k_2 \neq \infty \wedge 1 - k_1 k_2 \neq 0 \\ \infty & \text{ ako je } 1 - k_1 k_2 = 0 \\ -1/k_2 & \text{ ako je } k_1 = \infty \wedge k_2 \neq \infty \\ -1/k_1 & \text{ ako je } k_1 \neq \infty \wedge k_2 = \infty \\ 0 & \text{ ako je } k_1 = k_2 = \infty \end{aligned}$$

16. " $\angle ABC \cong \angle DEF$ " je ekvivalentno sa:

$$\operatorname{tg}(\angle ABC) - \operatorname{tg}(\angle DEF) = 0$$

17. "Tačke A, B, C i D pripadaju istom krugu.":

$$\operatorname{tg}(\angle ACD) - \operatorname{tg}(\angle BCD) = 0$$

18. " $\angle ABC + \angle A_1B_1C_1 + \angle A_2B_2C_2 \cong \angle DEF$ " je ekvivalentno sa:

$$\operatorname{tg}(\angle ABC + \angle A_1B_1C_1 + \angle A_2B_2C_2) - \operatorname{tg}(\angle DEF) = 0$$

Ovim uslovom se može opisati trisetrisa ugla.

19. "Dvostruka orijentisana površina trougla ABC , u oznaci $\nabla(ABC)$ " je jednaka:

$$(a_1 - b_1)(b_2 - c_2) - (a_2 - b_2)(b_1 - c_1)$$

20. "Dvostruka orijentisana površina četvorougla $ABCD$, u oznaci $\diamond(ABCD)$ " je jednaka:

$$\nabla(ABC) + \nabla(CDA)$$

3.4 Pogodan izbor koordinata tačaka

Pri izboru koordinata tačaka u Dekartovom sistemu u primerima iz potpoglavlja 4.3, najčešće je uzimano da prva tačka ima koordinate $(0, 0)$, tj. koordinate koordinatnog početka, a druga tačka pripada osi X i ima koordinate $(u_1, 0)$. Ovakav izbor koordinata smanjuje broj promenljivih za tri i bitno uprošćava dalje računanje i smanjuje vremensku i prostornu složenost izvođenja dokaza (svi termovi u svim polinomima koji bi sadržali neku od te tri promenljive su anulirani).

Ovakav izbor koordinata je postao već standardan i koristi se u svim algebarskim metodama, međutim nigde nije naglašena korektnost i postavljeno pitanje da li se time umanjuje opštost dokaza? Sledeća jednostavna teorema daje odgovor na ovo pitanje.

Teorema 5 *Dat je polinom $h(u_1, \dots, u_d, x_1, \dots, x_r) = 0$ nad skupom promenljivih $(u_1, \dots, u_d, x_1, \dots, x_r)$ koji je dobijen kao jednakost geometrijske konstrukcije. Tada važi:*

$$h(u_1, \dots, u_d, x_1, \dots, x_r) = 0 \Rightarrow h(u'_1, \dots, u'_d, x'_1, \dots, x'_r) = 0$$

gde su koordinate u'_i i x'_i dobijene tako što je na geometrijsku konstrukciju primenjena neka od operacija translacije ili rotacije.

Dokaz: Tvđenje važi s obzirom da se geometrijski odnosi i veličine (dužina segmenata, ugao između pravih, pripadnost tačke pravoj, itd.) čuvaju pri transformacijama translacije i rotacije. \square

Iz navedene teoreme sledi da izbor početnih koordinata ne umanjuje opštost dokaza.

3.5 Osnovna ideja algebarskog dokazivanja geometrijskih teorema

Postoji dosta metoda za algebarsko dokazivanje geometrijskih teorema (u ovoj tezi će biti opisane dve takve metode). Kod svake metode postoje varijacije same metode (u cilju dokazivanja specijalnih slučajeva ili ubrzanja programske implementacije metode). Sada ćemo neformalno iskazati ono što je zajedničko za sve algebarske metode.

3.5.1 Apstraktni opis algebarske metode

Svešćemo problem na geometrijska tvrđenja konstruktivnog tipa u kojima se geometrijsko tvrđenje iskazuje u obliku jednakosti. Dakle, takvo tvrđenje se sastoji od geometrijskih konstrukcija i geometrijskog tvrđenja koje iskazuje jednakost izgrađenu od konstruisanih objekata.

Kod svih metoda se polazna geometrijska konstrukcija prevodi u algebarski oblik, a to je sistem polinoma (p_1, p_2, \dots, p_r) nad prstenom $K[x_1, \dots, x_r]$. Primećimo da broj polinoma u sistemu odgovara broju promenljivih i ova zavisnost odgovara intuitivnoj pretpostavci da je sistem od n jednačina dobro definisan samo ukoliko ima n nezavisnih promenljivih. Način prevođenja u sistem polinoma je izvršen na taj način da je geometrijska konstrukcija tačna (odnosno da se objekti nalaze u položaju opisanom konstrukcijom) u nekoj tački $\mathbf{k} = (k_1, \dots, k_r)$ iz prostora K^r ako i samo ako važi $\mathbf{k} \in V((p_1, p_2, \dots, p_r)$, odnosno \mathbf{k} je zajednička nula polinoma iz sistema.

Na sličan način se i geometrijsko tvrđenje prevodi u polinom g nad istim prstenom polinoma.

Definicija 23 (Algebarska formulacija geometrijske teoreme) *Geometrijsko tvrđenje je dokazano algebarskom metodom ukoliko je dokazana sledeća implikacija:*

$$(\forall \mathbf{k} \in K^r)(\mathbf{k} \in V(p_1, p_2, \dots, p_r) \Rightarrow \mathbf{k} \in V(g))$$

Smisao definicije je sledeći: ukoliko je za neku tačku prostora K^r ostvarena geometrijska konstrukcija, onda u toj tački mora važiti i geometrijsko tvrđenje.

Ovaj početni korak je zajednički većini algebarskih metoda. Nadalje, svaka metoda se sastoji od karakterističnih algoritama za manipulaciju početnog sistema polinoma ne bi li se dokazalo ili opovrglo geometrijsko tvrđenje. U svakom koraku algoritma, trenutni sistem polinoma se uz određene transformacije transformiše u novi sistem polinoma:

$$(p_1^i, p_2^i, \dots, p_{r_i}^i) \rightarrow (p_1^{i+1}, p_2^{i+1}, \dots, p_{r_{i+1}}^{i+1})$$

koji ima isti skup nula kao i prethodni sistem, odnosno:

$$V(p_1^i, p_2^i, \dots, p_{r_i}^i) = V((p_1^{i+1}, p_2^{i+1}, \dots, p_{r_{i+1}}^{i+1}))$$

Ovim je takođe naglašeno i da se broj polinoma u sistemu može menjati između koraka ¹

¹To je, na primer slučaj kod Grebnerove metode, dok kod nekih metoda (na primer kod Vuove metode) broj polinoma u sistemu ostaje uvek isti

Algoritam staje u trenutku kada se sistem polinoma svede na *normalnu formu* za datu metodu (definicija normalne forme sistema zavisi od same metode, na primer kod Vuove metode to je *trougaona forma*, a kod Buhbergerove metode to je *Grebnerova baza*). Kod svake algebarske metode je potrebno dokazati da se svaki sistem polinoma svodi na normalnu formu u konačnom broju koraka. Složenost jednog koraka metode kao i prosečni broj neophodnih koraka da se sistem svede na normalnu formu određuju složenost metode.

Na kraju, algebarska metoda sadrži i algoritam kojim se proverava da li je polinom koji je određen geometrijskim tvrđenjem posledica normalne forme sistema polinoma. Rezultat u ovom slučaju može biti da je tvrđenje tačno ili netačno, ukoliko je algebarska metoda potpun sistem odlučivanja, ili da je tvrđenje tačno ili da se ne zna pouzdano tačnost geometrijskog tvrđenja, ukoliko metoda nije potpun sistem odlučivanja (u ovom drugom slučaju, nepotpunim algebarskim metodama ne možemo dokazati svaku geometrijsku teoreme).

Ovim smo na apstraktan način opisali široku klasu algebarskih metoda za dokazivanje geometrijskih tvrđenja, i na neki način naveli obrazac po kome se mogu konstruisati algebarske metode. Da sumiramo, proces dokazivanja je sledeći:

Korak 1 Geometrijsko tvrđenje se navodi u obliku geometrijske konstrukcije i završnog tvrđenja zadanog kao jednakost nad konstruisanim geometrijskim objektima.

Korak 2 Geometrijska konstrukcija se prevodi u sistem polinoma \mathbf{p}^1 , a geometrijsko tvrđenje se prevodi u polinom g .

Korak 3 U svakom koraku se trenutni sistem polinoma \mathbf{p}^i transformiše u novi sistem polinoma \mathbf{p}^{i+1} sve dok se ne dobije sistem polinoma u normalnoj formi. Metoda garantuje da će se taj proces završiti u konačnom broju koraka.

Korak 4 Metoda sadrži algoritam odlučivanja koja za dati sistem polinoma u normalnoj formi i geometrijsko tvrđenje g daje jedan od sledećih odgovora:

- Tvrđenje je tačno
- Tvrđenje nije tačno
- Tvrđenje nije dokazano niti opovrgnuto

3.5.2 Primeri transformacija sistema polinoma

Invarijanta koja se mora očuvati prilikom transformacije sistema polinoma je skup nula sistema. U okviru algoritama za svodenje sistema polinoma na normalnu formu, može se koristiti svaka transformacija koja ne menja skup nula sistema polinoma.

Razmotrimo primere odgovarajućih transformacija:

Teorema 6 (Osnovne transformacije sistema polinoma) *Sistem polinoma $(\dots, p_i, \dots, p_j, \dots)$ gde su polinomi iz prstena polinoma $K[\mathbf{x}]$ ima isti skup nula kao i sistemi:*

1. $(\dots, p_i, \dots, p_j, \dots, p_i)$

3.5 Osnovna ideja algebarskog dokazivanja geometrijskih teorema 29

2. $(\dots, p_j, \dots, p_i, \dots)$

3. $(\dots, \alpha p_i, \dots, p_j, \dots), \alpha \in K[\mathbf{x}], \alpha \neq 0$

4. $(\dots, \alpha p_i + \beta p_j, \dots, p_j, \dots), \alpha, \beta \in K[\mathbf{x}], \alpha \neq 0, \beta \neq 0$

Teorema 7 *Sistemi polinoma (p_1, p_2, \dots, p_r) i (q_1, q_2, \dots, q_t) imaju isti skup nula ako su ideali koje generišu jednaki.*

Glava 4

Vuova metoda

Pravo iznenađenje u matematičkom svetu je bilo kada je kineski matematičar Vu Ven Cun 1977. godine predstavio algebarsku metodu koja je bila u stanju da dokaže mnoge geometrijske teoreme [12], od kojih su neke iziskivale veome teške tradicionalne dokaze. Malo je oblasti automatskog rezonovanja u kojima se može izdvojiti jedna osoba koja je imala presudan uticaj na tu oblast, kao što je prekretnica koja se dogodila u oblasti automatskog dokazivanja geometrijskih teorema nakon objave Vuovih rezultata.

Kada govorimo o metodi Vua, možemo razlikovati nepotpunu (ili uprošćenu) i potpunu metodu Vua. U ovom radu će biti opisana ova prva, pojednostavljena metoda, a na osnovu pregleda teorema (videti dodatak) koje su dokazive, videćemo da je i uprošćena metoda Vua veoma moćna. S druge strane, implementacija potpune metode Vua je samo nadogradnja implementacije uprošćene metode, te je uprošćena metoda Vua dobar početak koji se iterativno može nadograđivati.

4.1 Opis Vuove metode

Vuova metoda se koristi za dokazivanje tvrdjenja u elementarnoj geometriji¹ za koje, u njihovoj algebarskoj formi, hipoteze i zaključci mogu biti predstavljeni u obliku izraza nad polinomima.

Za takva geometrijska tvrdjenja, posle izbora odgovarajućeg koordinatnog sistema, hipoteze mogu biti predstavljene kao skup jednakosti nad polinomima:

$$\begin{aligned}h_1(u_1, \dots, u_d, x_1, \dots, x_t) &= 0 \\h_2(u_1, \dots, u_d, x_1, \dots, x_t) &= 0 \\&\dots \\h_t(u_1, \dots, u_d, x_1, \dots, x_t) &= 0\end{aligned}$$

dok je zaključak takođe jednakost polinoma:

$$g = g(u_1, \dots, u_d, x_1, \dots, x_t) = 0$$

¹Iako je Vuova metoda lako proširiv na *razne* geometrije, nadalje ćemo razmatrati samo slučaj euklidske geometrije koja je i najbliža najširem krugu čitalaca

gde su h_1, h_2, \dots, h_t, g polinomi iz prstena $K[u_1, \dots, u_d, x_1, \dots, x_t]$, gde je K neko polje. Promenljive u_1, \dots, u_d su parametri ili nezavisne promenljive, a promenljive x_1, \dots, x_t su algebarski zavisne od parametara u_i , gde je zavisnost data gornjim sistemom jednačina². Odabir parametara u_i dolazi od pretpostavke da se objekti u geometrijskom tvrđenju nalaze u opštem položaju, pretpostavka koja se često implicitno uzima kao tačna u postavkama geometrijskih tvrđenja (u primeru 2, implicitna je pretpostavka da su tri tačke A, B i C nekolinearne).

Jednostavna procedura svodenja sistema na trouganu formu 2.3.3 se može iskoristiti da bi se potvrdile geometrijske teoreme (nepotpuna metoda Vua), a u nekim slučajevima (linearni slučajevi) jeste i potpuna procedura odlučivanja. Za kompletnu metodu Vua, potreban je sofisticiraniji algoritam koji bi proveravao svodivost sistema polinoma (što nije pokriveno korakom IV/2 iz 2.3.3).

Da bi se potvrdilo geometrijsko tvrđenje nepotpunom metodom Vua, dovoljno je pokazati sledeće:

1. Finalni ostatak je nula:

$$R_0 = 0$$

2. Zadovoljeni su i sledeći dodatni uslovi:

$$I_i \neq 0$$

$$\text{prem}(I_i, f_1, \dots, f_r) \neq 0$$

Ukoliko je poslednji ostatak jednak nuli, ali dodatni uslovi nisu zadovoljeni, pokazuje se da su polazne hipoteze nekonzistentne. Svako ko želi da implementira dokazivač na osnovu Vuove metode i jednostavnog algoritma svodenje na trougaonu formu, treba da proveri i ovaj poslednji uslov. U knjizi [1] se navodi da na osnovu eksperimentisanja sa stotinama teorema, samo je kod dva ili tri slučaja primećeno da drugi uslov ne važi.

4.2 Razmatranje uslova nedegenerisanosti

Za razliku od drugih algebarskih metoda za ADGT, Vuova metoda može većinu uslova nedegenerisanosti (NDG uslovi) da predstavi u geometrijskoj formi za široku klasu geometrijskih problema.

Kod geometrijskih teorema konstruktivnog tipa 3.2, svodenje sistema polinoma na trougaonu formu 2.3.3 se može efikasno izvesti na način tako da se čuvaju informacije o geometrijskoj interpretaciji dodatnih uslova koji će na kraju biti NDG uslovi Vuove metode. To ilustruje sledeći primer.

Primer 4 (NDG uslovi preseka dvaju pravih) *Konstrukcijom 8 iz definicije 21 određena je nova tačka kao presek dveju pravih. Neka su koordinate nove tačke (x_k, x_{k+1}) . Formule koje određuju pripadnost tačke pravama su:*

$$l_1 = a_1 x_{k+1} + b_1 x_k + c_1 = 0$$

$$l_2 = a_2 x_{k+1} + b_2 x_k + c_2 = 0$$

²Označavanje promenljivih, odnosno konvencija da se nezavisne promenljive označavaju malim slovom u , a zavisne promenljive označavaju malim slovom x , potiče od Hilbertove teoreme za afnu geometriju (*Hilbert mechanization theorem for affine geometry*)

Ovaj mini-sistem se može svesti na trougaoni sa sledeća dva pseudo-deljenja:

$$\text{prem}(l_2, l_1, x_{k+1}) = dx_k - d_k = 0$$

$$\text{prem}(l_1, l_2, x_k) = dx_{k+1} - d_{k+1} = 0$$

gde je $d = a_1b_2 - a_2b_1$, a d_k i d_{k+1} su neki koeficijenti. Ukoliko se konstrukcija 8 pominje u zadatku, mogu se u toku postupka svodenja na trougaoni sistem odabrati ova dva svedena polinoma od kojih jedan uvodi promenljivu x_k , a drugi x_{k+1} , a zatim algoritam biti nastavljen uobičajenim tokom. Time smo dobili jedan dodatni uslov $I_k = I_{k+1} = d$ čije je geometrijsko značenje da dve prave imaju presek (u euklidskoj geometriji ekvivalentno uslovu da dve prave nisu paralelne).

I ostale konstrukcije se mogu tretirati na sličan način. Ukoliko se nove konstrukcije dodaju u dokazivač, za svaku treba odrediti koje uslove nedegenerisanosti može proizvesti i koji je njihov geometrijski smisao.

U poglavlju 4.3.2 je dat primer kako se uslovi nedegenerisanosti mogu pratiti kroz izvođenje dokaza geometrijskog tvrđenja i na kraju prevesti u čitljivu formu.

4.3 Primene Vuove metode

Sledeći primeri ilustruju korišćenje Vuove metode u dokazivanju geometrijskih teorema.

Razmotrimo najpre primer iz prethodnog poglavlja.

4.3.1 Primer paralelograma

Primer 5 (Kao primer 2)

Implicitna pretpostavka da je paralelogram $ABCD$ u opštem položaju ima značenje da su svake tri tačke nekolinearne. Prema tome, promenljive u_1 , u_2 i u_3 se mogu uzeti kao parametri (koristimo istu dodelu koordinata tačaka kao što je korišćeno u prethodnom poglavlju). Dobijamo četiri jednačine $h_1 = 0, \dots, h_4 = 0$ kao hipoteze i jednačinu $g = 0$ kao zaključak.

Neko bi brzopleto mogao da pomisli da je algebarska postavka problema sledeća:

$$(h_1 = 0 \wedge h_2 = 0 \wedge h_3 = 0 \wedge h_4 = 0) \Rightarrow g = 0 \quad (4.1)$$

Međutim, (4.1) tvrđenje je netačno iz razloga što važni uslovi nedegenerisanosti nisu uzeti u obzir. Vuova metoda može automatski generisati neophodne uslove nedegenerisanosti iz postavke problema.

Sledeći korak je svodenje sistema polinoma h_1, h_2, h_3, h_4 na trougaonu formu iz definicije 18 tako da svaki sledeći polinom sadrži najviše jednu novu zavisnu promenljivu x_i u odnosu na prethodne polinome.

Sistem (h_1, h_2, h_3, h_4) nije u trougaonoj formi zato što polinom h_3 uključuje dve nove promenljive x_3 i x_4 koje nisu bile sadržane u polinomima h_1 i h_2 . Korišćenjem jednostavne eliminacione procedure, može se doći do trougaone

forme. Neka je $f_1 = h_1$, $f_2 = h_2$, $f_3 = \text{prem}(h_4, h_3, x_4)^3$, $f_4 = h_4$. Time je dobijena trougaona forma:

$$\begin{aligned} f_1 &= u_1x_1 - u_1u_3 = 0 \\ f_2 &= u_3x_2 - (u_2 - u_1)x_1 = 0 \\ f_3 &= (u_3x_2 - u_2x_1 - u_1u_3)x_3 + u_1u_3x_1 = 0 \\ f_4 &= u_3x_4 - u_2x_3 = 0 \end{aligned}$$

Sukcesivnim pseudo-deljenjem, iz tvrđenja problema se mogu eliminisati nezavisne promenljive:

$$\begin{aligned} R_3 &= \text{prem}(g, f_4, x_4) = (2u_3^2 + 2u_2^2)x_3 - u_3^3 - u_2^2u_3 \\ R_2 &= \text{prem}(R_3, f_3, x_3) = \\ &= (-u_3^4 - u_2^2u_3^2)x_2 + ((u_2 - 2u_1)u_3^3 + (u_2^3 - 2u_1u_2^2)u_3)x_1 + u_1u_3^4 + u_1u_2^2u_3^2 \\ R_1 &= \text{prem}(R_2, f_2, x_2) = (-u_1u_3^4 - u_1u_2^2u_3^2)x_1 + u_1u_3^5 + u_1u_2^2u_3^3 \\ R_0 &= \text{prem}(R_1, f_1, x_1) = 0 \end{aligned}$$

S obzirom na to da je *poslednji ostatak* R_0 jednak nuli, teorema je dokazana uz nekoliko dodatnih uslova. Da bismo videli koji su to dodatni uslovi, podsetimo se formule ostatka (teorema 4) koja važi za sukcesivno deljenje polinoma g u odnosu na trougaonu formu polinoma f_1, \dots, f_r :

$$I_1^{s_1} \cdots I_r^{s_r} g = Q_1 f_1 + \dots + Q_r f_r + R_0 \quad (4.2)$$

gde je I_k vodeći koeficijent polinoma f_k u odnosu na promenljivu x_k .

S obzirom na to da je $R_0 = 0$, tada je i $g = 0$ uz uslov $I_k \neq 0; k = 1, \dots, r$. Dodatni uslovi su dakle $I_k \neq 0$ i to su uslovi nedegenerisanosti. U ovom specifičnom slučaju, jednakost (4.1) je tačna uz dodatne uslove:

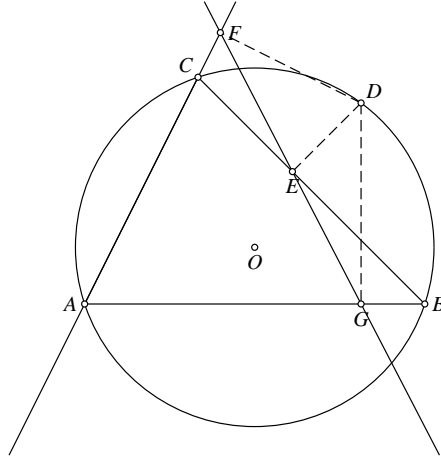
$$\begin{aligned} I_1 &= u_1 \neq 0 \\ I_2 &= u_3 \neq 0 \\ I_3 &= u_3x_2 - u_2x_1 - u_1u_3 \neq 0 \\ I_4 &= u_3 \neq 0 \end{aligned}$$

Uslovi $u_1 \neq 0$ i $u_3 \neq 0$ znače da tačke A , B i C nisu kolinearne. Uslov $u_3x_2 - u_2x_1 - u_1u_3 \neq 0$ znači da prave AC i BD imaju presek.

4.3.2 Primer Simpsonove teoreme

Primer 6 (Simsonova teorema) *Neka je D tačka kruga sa centrom O opisanog oko trougla ABC sa centrom O . Neka su E , F i G podnožja normala iz tačke D na prave BC , AC i AB redom. Dokazati da su tačke E , F i G kolinearne (slika 4.1).*

³ $\text{prem}(h_4, h_3, x_4)$ predstavlja ostatak pseudo-deljenja polinoma h_4 polinomom h_3 po promenljivoj x_4 . U poglavlju 2.3 su detaljno izložene algebarske operacije korišćene u Vuovoj metodi.



Slika 4.1: Simpsonova teorema

Neka je $A = (0, 0)$, $B = (u_1, 0)$, $C = (u_2, u_3)$, $O = (x_1, x_2)$, $D = (x_3, u_4)$, $E = (x_5, x_4)$, $F = (x_7, x_6)$ i $G = (x_3, 0)$. Tada su hipoteze tvrđenja:

$$OA \cong OC: \quad h_1 = 2u_2x_2 + 2u_3x_1 - u_3^2 - u_2^2 = 0$$

$$OA \cong OB: \quad h_2 = 2u_1x_2 - u_1^2 = 0$$

$$OA \cong OD: \quad h_3 = -x_3^2 + 2x_2x_3 + 2u_4x_1 - u_4^2 = 0$$

$$E, B \text{ i } C \text{ su kolinearne: } h_4 = u_3x_5 + (-u_2 + u_1)x_4 - u_1u_3 = 0$$

$$DE \perp BC: \quad h_5 = (u_2 - u_1)x_5 + u_3x_4 - (u_2 - u_1)x_3 - u_3u_4 = 0$$

$$F, A \text{ i } C \text{ su kolinearne: } h_6 = u_3x_7 - u_2x_6 = 0$$

$$DF \perp AC: \quad h_7 = u_2x_7 + u_3x_6 - u_2x_3 - u_3u_4 = 0$$

Zaključak tvrđenja da su tačke E , F i G kolinearne se može predstaviti polinomom:

$$g = x_4x_7 + (-x_5 + x_3)x_6 - x_3x_4 = 0$$

Trougaoni sistem polinoma možemo konstruisati na sledeći način:

$$f_1 = \text{prem}(h_1, h_2, x_2)$$

$$f_2 = h_2$$

$$f_3 = h_3$$

$$f_4 = \text{prem}(h_4, h_5, x_5)$$

$$f_5 = h_4$$

$$f_6 = \text{prem}(h_6, h_7, x_7)$$

$$f_7 = h_7$$

Dobili smo:

$$f_1 = 4u_1u_3x_1 - 2u_1u_3^2 - 2u_1u_2^2 + 2u_1^2u_2 = 0$$

$$f_2 = 2u_1x_2 - u_1^2 = 0$$

$$f_3 = -x_3^2 + 2x_2x_3 + 2u_4x_1 - u_4^2 = 0$$

$$f_4 = (-u_3^2 - u_2^2 + 2u_1u_2 - u_1^2)x_4 + (u_2 - u_1)u_3x_3 + u_3^2u_4 + (-u_1u_2 + u_1^2)u_3 = 0$$

$$\begin{aligned}
f_5 &= u_3x_5 + (-u_2 + u_1)x_4 - u_1u_3 = 0 \\
f_6 &= (-u_3^2 - u_2^2)x_6 + u_2u_3x_3 + u_3^2u_4 = 0 \\
f_7 &= u_2x_7 + u_3x_6 - u_2x_3 - u_3u_4 = 0
\end{aligned}$$

Pošto je $\deg(f_3, x_3) = 2$, pseudo-deljenje će ići brže (stepen polinoma ostataka posle pseudo-deljenja ovim polinomom će biti za dva manji od stepena polinoma delitelja):

$$\begin{aligned}
R_6 &= \text{prem}(g, f_7, x_7) = (-u_2x_5 - u_3x_4 + u_2x_3)x_6 + u_3u_4x_4 \\
R_5 &= \text{prem}(R_6, f_6, x_6) = (u_2^2u_3x_3 + u_2u_3^2u_4)x_5 + (u_2u_3^2x_3 - u_2^2u_3u_4)x_4 - \\
&\quad -u_2^2u_3x_3^2 - u_2u_3^2u_4x_3 \\
R_4 &= \text{prem}(R_5, f_5, x_5) = ((u_2u_3^3 + (u_3^3 - u_1u_2^2)u_3)x_3 - u_1u_2u_3^2u_4)x_4 - \\
&\quad -u_2^2u_3^2x_3^2 + (-u_2u_3^3u_4 + u_1u_2^2u_3^2)x_3 + u_1u_2u_3^3u_4 \\
R_3 &= \text{prem}(R_4, f_4, x_4) = u_1u_2u_3^4x_3^2 - u_1^2u_2u_3^4x_3 + u_1u_2u_3^4u_4^2 + (-u_1u_2u_3^5 + \\
&\quad + (-u_1u_2^3 + u_1^2u_2^2)u_3^3)u_4 \\
R_3 &= \text{prem}(R_3, f_3, x_3) = -2u_1u_2u_3^4x_3x_2 + u_1^2u_2u_3^4x_3 - 2u_1u_2u_3^4u_4x_1 + \\
&\quad + (u_1u_2u_3^5 + (u_1u_2^3 - u_1^2u_2^2)u_3^3)u_4 \\
R_1 &= \text{prem}(R_2, f_2, x_2) = -4u_1^2u_2u_3^4u_4x_1 + (2u_1^2u_2u_3^5 + (2u_1^2u_2^3 - 2u_1^3u_2^2)u_3^3)u_4 \\
R_0 &= \text{prem}(R_1, f_1, x_1) = 0
\end{aligned}$$

Pošto je poslednji ostatak $R_0 = 0$, na osnovu formuli ostatka dokazali smo Simsonovu teoremu pod sledećim dodatnim uslovima:

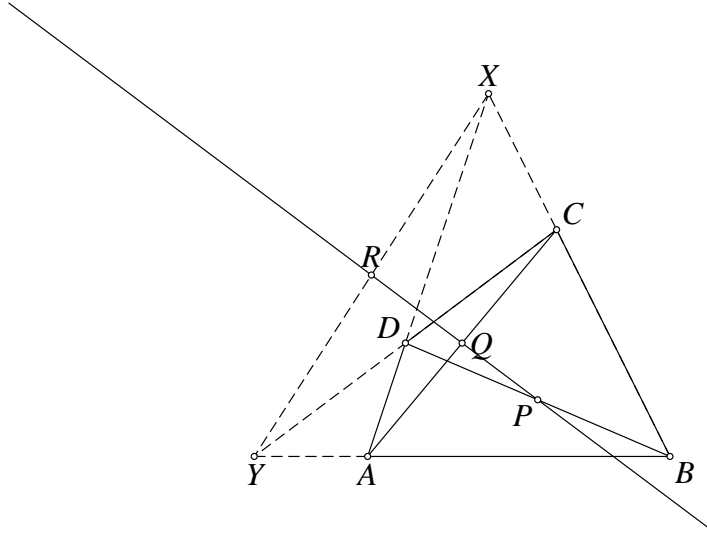
$$\begin{aligned}
I_1 &= 4u_1u_3 \neq 0 \\
I_2 &= 2u_1 \neq 0 \\
I_4 &= -u_3^2 - u_2^2 + 2u_1u_2 - u_1^2 \neq 0 \\
I_5 &= u_3 \neq 0 \\
I_6 &= -u_3^2 - u_2^2 \neq 0 \\
I_7 &= u_2 \neq 0
\end{aligned}$$

Razmatranje dodatnih uslova

Navedeni dodatni uslovi mogu imati i svoju geometrijsku formu. U poglavlju 4.2 su opisani slučajevi u kojima se može pratiti geometrijska forma dodatnih uslova.

Geometrijske konstrukcije ove teoreme koje su transformisane u polinomne jednakosti su:

$$\begin{aligned}
OA &\cong OB \\
OA &\cong OC \\
OD &\cong OA \\
DE &\perp BC \\
B, C &\text{ i } E \text{ su kolinearne} \\
DF &\perp AC \\
A, C &\text{ i } F \text{ su kolinearne} \\
DG &\perp AB
\end{aligned}$$



Slika 4.2: Gausova tačka

A , B i G su kolinearne

Neke dodatne uslove možemo prevesti u jednostavnu geometrijsku formu:

(1) $I_1 \neq 0$ ima značenje da simetrale duži AB i AC imaju jedinstven presek. To je ekvivalentno uslovima $A \neq B$, $A \neq C$ i „prave AB i AC nisu paralelne ni identične” (poslednji uslov je ekvivalentan uslovu da tačke A , B i C nisu kolinearne).

(2) $I_4 \neq 0$ ima značenje da normala iz D na pravu BC ima jedinstven presek sa pravom BC . To je ekvivalentno uslovima da je $B \neq C$ i prava BC nije normalna na samu sebe (uslov $B \neq C$ određuje jedinstvenost normale iz proizvoljne tačke na pravu BC , a uslov da prava BC nije normalna na samu sebe određuje jedinstvenost preseka prave BC i bilo koje prave koja je normalna na nju)⁴. Poslednji uslov je suvišan u euklidskoj geometriji.

(3) Slično, $I_6 \neq 0$ je ekvivalentan uslovu „prava AC nije normalna na samu sebe”, takođe suvišnom u euklidskoj geometriji.

(4) Uslovi $I_2 \neq 0$, $I_5 \neq 0$ i $I_7 \neq 0$ nisu neophodni i pažljivijim postupkom svodenja na trougaoni sistem se mogu izbeći (primer 4).

Dakle, teorema je dokazana uz uslove nedegenerisanosti da tačke A , B i C nisu kolinearne.

Sledeći primer je komplikovaniji od prethodnih. On ilustruje kako Vuova metoda može biti računski zahtevna.

4.3.3 Primer Gausove tačke

Primer 7 (Gausova tačka). Date su četiri nekolinearne tačke A , B , C i D . Neka su tačke X i Y preseki pravih AD i BC , odnosno pravih AB i CD . Neka

⁴Prava normalna na samu sebe se zove izotropna prava, takve prave naravno ne postoje u euklidskoj geometriji. Izotropne prave postoje u nekim modelima metričkih geometrija i u geometriji Minkovskog, pa ukoliko je dokaz namenjen ne-euklidskim geometrijama svi dodatni uslovi moraju biti navedeni.

su tačke P , Q i R središta duži BD , AC i XY redom. Dokazati da su tačke P , Q i R kolinearne (slika 4.2).

Neka su koordinate dodeljene tačkama na sledeći način: $A = (0, 0)$, $B = (u_1, 0)$, $C = (u_3, u_3)$, $D = (u_4, u_5)$, $X = (x_2, x_1)$, $Y = (x_3, 0)$, $P = (x_5, x_4)$, $Q = (x_7, x_6)$ i $R = (x_9, x_8)$. Na osnovu konstrukcija iz problema dobijamo sledeće hipoteze :

$$\begin{aligned}
X \text{ pripada } BC: & \quad h_1 = -u_3x_2 + (u_2 - u_1)x_1 + u_3u_1 \\
X \text{ pripada } AD: & \quad h_2 = -u_5x_2 + u_4x_1 \\
Y \text{ pripada } CD: & \quad h_3 = (-u_5 + u_3)x_3 + (u_5u_2 - u_4u_3) \\
P \text{ pripada } BD: & \quad h_4 = -u_5x_5 + (u_4 - u_1)x_4 + u_5u_1 \\
PB \cong PD: & \quad h_5 = (2u_4 - 2u_1)x_5 + 2u_5x_4 + (-u_5^2 - u_4^2 + u_1^2) \\
Q \text{ pripada } AC: & \quad h_6 = -u_3x_7 + u_2x_6 \\
QA \cong QC: & \quad h_7 = 2u_2x_7 + 2u_3x_6 + (-u_3^2 - u_2^2) \\
R \text{ pripada } XY: & \quad h_8 = x_9x_1 + x_8x_3 - x_8x_2 - x_3x_1 \\
RX \cong RY: & \quad h_9 = 2x_9x_3 - 2x_9x_2 - 2x_8x_1 - x_3^2 + x_2^2 + x_1^2
\end{aligned}$$

Tvrđenje teoreme se može napisati u obliku polinoma:

$$g = -x_9x_6 + x_9x_4 + x_8x_7 - x_8x_5 - x_7x_4 + x_6x_5 = 0$$

Pseudo-deljenja koja mogu biti izvršena su:

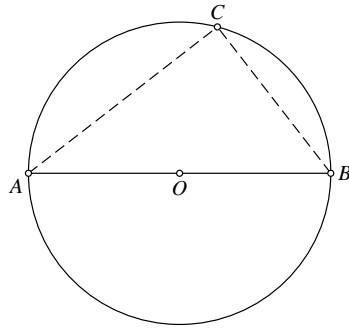
$$\begin{aligned}
f_8 &= \text{prem}(h_8, h_9, x_9) \\
f_6 &= \text{prem}(h_6, h_7, x_7) \\
f_4 &= \text{prem}(h_4, h_5, x_5) \\
f_0 &= \text{prem}(h_0, h_1, x_2) \\
f_i &= h_i, \quad i \in \{1, 2, 3, 5, 7, 9\}
\end{aligned}$$

dajući odgovarajući trougaoni sistem:

$$\begin{aligned}
f_1 &= (-u_5u_2 + u_5u_1 + u_4u_3)x_1 - u_5u_3u_1 \\
f_2 &= -u_5x_2 + u_4x_1 \\
f_3 &= (-u_5 + u_3)x_3 + (u_5u_2 - u_4u_3) \\
f_4 &= (2u_5^2 + 2u_4^2 - 4u_4u_1 + 2u_1^2)x_4 + (-u_5^3 - u_5u_4^2 + 2u_5u_4u_1 - u_5u_1^2) \\
f_5 &= (2u_4 - 2u_1)x_5 + 2u_5x_4 + (-u_5^2 - u_4^2 + u_1^2) \\
f_6 &= (2u_3^2 + 2u_2^2)x_6 + (-u_3^3 - u_3u_2^2) \\
f_7 &= 2u_2x_7 + 2u_3x_6 + (-u_3^2 - u_2^2) \\
f_8 &= 2x_8x_3^2 - 4x_8x_3x_2 + 2x_8x_2^2 + 2x_8x_1^2 - x_3^2x_1 + 2x_3x_2x_1 - x_2^2x_1 - x_1^3 \\
f_9 &= 2x_9x_3 - 2x_9x_2 - 2x_8x_1 - x_3^2 + x_2^2 + x_1^2
\end{aligned}$$

Na ovako dobijenu trougaonu formu, kao i u prethodnim primerima, primenjuje se sukcesivno pseudo-deljenje tvrđenja teoreme, $R_8 = \text{prem}(g, f_9, x_9)$, $R_7 = \text{prem}(R_8, f_8, x_8)$, \dots , $R_0 = \text{prem}(R_1, f_1, x_1)$. Dobija se da je $R_0 = 0$, čime je teorema dokazana uz dodatne uslove:

$$I_1 = -u_5u_2 + u_5u_1 + u_4u_3 \neq 0$$



Slika 4.3: Prav ugao

$$\begin{aligned}
 I_2 &= -u_5 \neq 0 \\
 I_3 &= -u_5 + u_3 \neq 0 \\
 I_4 &= 2u_5^2 + 2u_4^2 - 4u_4u_1 + 2u_1^2 \neq 0 \\
 I_5 &= 2u_4 - 2u_1 \neq 0 \\
 I_6 &= 2u_3^2 + 2u_2^2 \neq 0 \\
 I_7 &= 2u_2 \neq 0 \\
 I_8 &= 2x_3^2 - 4x_3x_2 + 2x_2^2 + 2x_1^2 \neq 0 \\
 I_9 &= 2x_3 - 2x_2 \neq 0
 \end{aligned}$$

koji su povezani sa uslovima nedegenerisanosti, odnosno da su tačke A , B , C i D nalaze u opštem položaju.

Naglasimo da se pri sukcesivnom pseudo-deljenju u ovom primeru dobijaju jako veliki polinomi, na primer, polinom R_2 se sastoji od ukupno 1744 termova. Ovaj primer je praktično nemoguće uraditi ručno na papiru, a i računarska implementacija je bila skoro nemoguća sve do pojave moćnijih računara početkom osamdesetih godina prošlog veka.

4.4 Mogući problemi primene Vuove metode

Ukoliko se ne koristi pravilno, kod primene Vuove metode se mogu pojaviti problemi i nepravilnosti koji u krajnjem slučaju mogu dovesti i do pogrešnih dokaza. Takođe, uprošćena metoda Vua, za razliku od potpune Vuove metode i Buhbergerove metode, nije potpun sistem odlučivanja.

4.4.1 Primer ugla nad prečnikom

Primer 8 (Ugao nad prečnikom) *Dat je krug k sa prečnikom AB i centrom O . Neka je C proizvoljna tačka na krugu k . Dokazati da je ugao $\angle ACB$ prav*

(slika 4.3).

Neka je izbor koordinata sledeći: $A = (0, 0)$, $O = (u_1, 0)$, $B = (x_1, 0)$ i $C = (x_2, u_2)$. Hipoteze tvrđenja u obliku jednakosti nad polinomima su:

$$\begin{aligned} BO \cong AO: \quad h_1 &= x_1^2 - 2u_1x_1 = 0 \\ CO \cong AO: \quad h_2 &= x_2^2 - 2u_1x_2 + u_2^2 = 0 \end{aligned}$$

Tvrđenje problema, da su prave AC i BC normalne, se iskazuje jednakošću:

$$g = x_2^2 - x_2x_1 + u_2^2 = 0$$

Sistem polinoma je trougaoni na samom početku, stoga nikakav dodatni posao u tom koraku ne treba činiti. Eliminacijom zaključnog tvrđenja, dobijamo:

$$\begin{aligned} R_1 &= \text{prem}(g, h_2, x_2) = -x_2x_1 + 2u_1x_2 \\ R_0 &= \text{prem}(R_1, h_1, x_1) = -x_2x_1 + 2u_1x_2 \end{aligned}$$

Pošto finalni ostatak nije jednak nuli, tvrđenje nije dokazano. U čemu je problem, jer je tvrđenje ispravno i čini se trivijalnim?

Ako razmotrimo jednačine koje određuju tačku B , videćemo da tačka B nije jedina tačka u ravni koja ih zadovoljava. Tačka B pripada krugu k i pravoj AO . Postoje dve tačke koje zadovoljavaju iste uslove, to su tačka B i tačka A . U slučaju da je ova potonja tačka izabrana u konstrukciji, tvrđenje ne važi.

Ovo je takozvani slučaj svodivog sistema polinoma. Ako razmotrimo hipotezu h_1 , vidimo da se ona može faktorisati po nepoznatoj x_1 na sledeći način:

$$h_1 = x_1(x_1 - 2u_1) = 0$$

odakle se dobijaju dva rešenja za x_1 . Prvo rešenje je $x_1 = 2u_1$ (tačka B) i drugo rešenje je $x_1 = 0$ (tačka A).

Ukoliko umesto h_1 izaberemo polinom $h'_1 = x_1 - 2u_1$, koji određuje onu tačku na koju se i mislilo u zadatku, tada je:

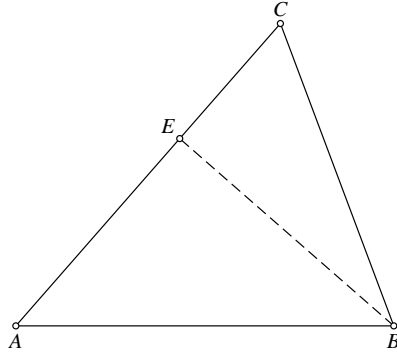
$$\begin{aligned} R'_1 &= \text{prem}(g, h_2, x_2) = -x_2x_1 + 2u_1x_2 \\ R'_0 &= \text{prem}(R'_1, h'_1, x_1) = 0 \end{aligned}$$

Tvrđenje je dokazano bez dodatnih uslova.

Videli smo da ovaj jednostavan primer nije dokaziv uprošćenom metodom Vua, zbog problema u jednoznačnosti konstrukcije tačke B . Nemogućnost obrade ovakvih slučajeva je i glavni nedostatak uprošćene metode, ali kako se ovakvi slučajevi ne pojavljuju često u praksi, najveći broj geometrijskih teorema je dokaziv ovom metodom. Primer je dokazan tek kada je jedna od hipoteza faktorisana — to je upravo način kako bi se problem rešio kompletnom Vuovom metodom.

4.4.2 Nekonzistentnost geometrijske konstrukcije

Razmotrimo sledeći primer i dva „dokaza”, od kojih će jedan namerno biti pogrešan.



Slika 4.4: Nekonkistentnost geometrijskih konstrukcija

Primer 9 *Dat je trougao ABC . Neka je E podnožje normale iz B na pravu AC . Dokazati da je $AB \cong CB$ (slika 4.4).*

Navedimo ispravan dokaz:

Dokaz: Neka su tačke A , B i C proizvoljne. Neka E pripada pravoj AC i neka pripada pravoj koja sadrži B i normalna je na AC .

Na osnovu konstrukcije, koordinate tačaka će biti dodeljene na sledeći način: $A = (0, 0)$, $B = (u_1, 0)$, $C = (u_2, u_3)$ i $E = (x_1, x_2)$. Time dobijamo hipoteze i zaključak tvrđenja:

$$\begin{aligned} EB \perp AC: & \quad h_1 = u_3x_2 + u_2x_1 - u_1u_2 = 0 \\ E \text{ pripada } AC: & \quad h_2 = u_2x_2 - u_3x_1 = 0 \\ AC \cong BC: & \quad g = u_3^2 + u_2^2 - 2u_1u_2 = 0 \end{aligned}$$

Posle svođenja na trougaoni sistem dobijamo:

$$\begin{aligned} f_1 &= (u_3^2 + u_2^2)x_1 - u_1u_2^2 = 0 \\ f_2 &= u_2x_2 - u_3x_1 = 0 \end{aligned}$$

Međutim $\text{prem}(g, f_1, f_2) \neq 0$. Pošto se radi o linearnom slučaju ($\text{deg}(f_1, x_1) = \text{deg}(f_2, x_2) = 1$), možemo zaključiti da je tvrđenje netačno.

□

Ukoliko se konstrukcija izvodi na nepravilan način, moguće je dobiti i „pogrešan dokaz“:

Dokaz: Neka su tačke A , B i E proizvoljne. Neka C pripada pravoj AE i pravoj koja sadrži A i normalna je na BE .

Na osnovu konstrukcije, koordinate tačaka će biti dodeljene na sledeći način: $A = (0, 0)$, $B = (u_1, 0)$, $E = (u_2, u_3)$ i $C = (x_1, x_2)$. Time dobijamo hipoteze i zaključak tvrđenja:

$$\begin{aligned} EB \perp AC: & \quad h_1 = u_3x_2 + (u_2 - u_1)x_1 = 0 \\ E \text{ pripada } AC: & \quad h_2 = u_2x_2 - u_3x_1 = 0 \\ AC \cong BC: & \quad g = x_3^2 + x_1^2 - 2u_1x_1 = 0 \end{aligned}$$

Posle svođenja na trougaoni sistem dobijamo:

$$\begin{aligned} f_1 &= (u_3^2 + u_2^2 - u_1u_2)x_1 = 0 \\ f_2 &= u_2x_2 - u_3x_1 = 0 \end{aligned}$$

Sada je $\text{prem}(g, f_1, f_2) = 0$, prema tome tvrđenje je dokazano uz dodatne uslove $u_3^2 + u_2^2 - u_1u_2 \neq 0$ i $u_2 \neq 0$!

□

Greška je u opisu konstrukcije tačke C . Ako je $AE \perp BE$, onda C može biti proizvoljna tačka na pravoj AE , međutim tačke A , B i E su date u opštem položaju i u dokazu se ne može pretpostaviti da je ugao $\angle AEB$ prav. Jedina tačka koja u opštem slučaju zadovoljava navedene uslove za tačku C je tačka A , i u tom slučaju zaista važi $AB \cong CB$. Prema tome, dokazivač je zaista dokazao postavljeno tvrđenje opisanom konstrukcijom, ali opisana konstrukcija nije korektna za zadati problem.

Ovakve greške su mašinskom dokazivaču teške za otkrivanje. Neke neispravne konstrukcije mogu biti sprečene ugradnjom heuristike u dokazivač, ali generalno odgovornost je na korisniku da dokazivaču prosledi validne geometrijske konstrukcije.

4.5 Skica Vuove metode

Iz prethodnih primera i objašnjenja koja su išla uz njih, videli smo da se Vuova metoda sastoji iz sledećih koraka:

Korak 1 Konverzija geometrijskog tvrđenja u odgovarajući sistem polinomnih jednakosti.

Korak 2 Svođenje sistema polinoma na trougaonu formu korišćenjem algoritma pseudo-deljenja. U kompletnom metodu Vuova, dekompozicija i provera svodivosti je neophodna (pogledati poslednji primer iz poglavlja 1.2).

Korak 3 Primena sukcesivnog pseudo-deljenja da bi se dobio finalni ostatak R_0 . Ako je poslednji ostatak jednak nuli, onda je teorema dokazana uz dodatne uslove koji su iskazani kao nejednakosti među polinoma (dodatni uslovi se čitaju iz trougaonog sistema polinoma, kao vodeći koeficijenti svakog polinoma). Ako poslednji ostatak nije jednak nuli, teorema nije dokazana, ali nije ni opovrgnuta pošto uprošćena metoda Vua nije kompletna metoda odlučivanja.

U slučaju linearnog sistema polinoma (kada je $\deg(f_i, x_i) = 1$), i uprošćena Vuova metoda je potpuna procedura odlučivanja u euklidskoj geometriji. Drugim rečima, za ovakve slučajeve finalni ostatak će potvrditi da je tvrđenje tačno (uz dodatne uslove) ili da je tvrđenje netačno (i da ga nikakvi dodatni uslovi ne mogu pretvoriti u tačno)⁵.

Korak 4 Analiza uslova nedegenerisanosti: $I_1 \neq 0, \dots, I_r \neq 0$. Neki od uslova se mogu automatski prevesti u geometrijsku formu kao uslovi koji isključuju degenerativne slučajeve konstrukcije. To nije uvek moguće uraditi automatski. Za neke od uslova može se pokazati da čak nisu ni neophodni (o tome će biti više reči kasnije, ukratko neki uslovi nedegenerisanosti nisu potrebni u geometrijama gde takav degeneritet ni ne postoji, kao na primer uslov da prava nije izotropna u euklidskoj geometriji).

Nekoliko pitanja se odmah nameće:

1. Posle sukcesivnog pseudo-deljenja, ako poslednji ostatak nije jednak nuli, šta možemo zaključiti iz toga?
2. Za koju teoriju ova metoda može dokazivati teoreme?
3. Algoritam se završava dodavanjem dodatnih uslova teoremi. Da li je teorema oslabljena ovim dodatnim uslovima? Da li hipoteze ostaju konzistentne uz dodatne uslove?
4. Da li su svi dodatni uslovi neophodni? Ukoliko neke od dodatnih uslova određuje nedegenerativne slučajeve teoreme, da li taj uslov može iskazati u geometrijskoj formi umesto kao nejednakost polinoma?

Odgovore na većinu pitanja nudi kompletna metoda Vua [12]. Nepotpuna metoda Vua nam pruža mogućnost dokazivanja nekih geometrijskih teorema i ostavlja otvoreno pitanje kod ostalih geometrijskih teorema. Što se tiče prevođenja dodatnih uslova u geometrijsku formu, ne postoji opšti način da se to uradi. Ipak, za veliku klasu geometrijskih konstrukcija, postoji algoritam mašinskog prevođenja dodatnih uslova u odgovarajuću geometrijsku formu, kao što smo videli u prethodnim primerima.

4.6 Čuov dokazivač

Najpoznatija implementacija Vuove metode je dokazivač čiji je autor kineski matematičar Ču ([1]). Do danas ne postoji implementacija potpune Vuove metode, a Čuova implementacija je njena najpotpunija aproksimacija. Sadrži veliki

⁵Prema podacima iz knjige [1], od 366 teorema sa kojima je eksperimentisano, 219 je linearnog oblika, uključujući i veliki broj netrivialnih problema

broj poboljšanja u odnosu na Vuov rad i potpuna je u slučajevima kada su ulazni polinomi najviše kvadratni.

I pored svojih ograničenja, Čuov dokazivač važi za *najmoćniji geometrijski dokazivač* uopšte, a Vuova metoda za *najmoćniju metodu* za dokazivanje geometrijskih teorema.

Svoj rad u oblasti ADGT, Vu je započeo na univerzitetu u Kini 1976. godine. Velike zasluge za upoznavanje svetske javnosti sa rezultatima Vuovog rada ima upravo Ču, koji je 1986. godine na univerzitetu u Teksasu predstavio Vuovu metodu i implementirao svoj dokazivač koji je uspešno dokazao na stotine netrivialnih teorema.

Vuova metoda je takođe poznata i kao Rit-Vu metoda, a pomenuti dokazivač kao Rit-Vu-Ču dokazivač, a takođe i kao *kineski dokazivač*.

Glava 5

Buhbergerova metoda

Metodu Grebnerovih baza¹ [15] predstavio je Buhberger 1965. godine. Radi se o moćnom algoritmu koji se može koristiti za rešavanje brojnih problema i u teoriji ideala polinoma. Uspeh Vuove metode je nagnao istraživače da na istu klasu geometrijskih teorema na koje se odnosi i ta metoda primene metodu Grebnerovih baza. Jedan od uspešnijih radova na tu temu je i [24]. Korišćenjem metode opisane u tom radu uspešno je dokazano 358 od ukupno 366 teoreme iz kolekcije teorema [25].

U ovoj glavi biće predstavljena metoda iz rada [24] i biće data uporedna analiza dve metode u kontekstu dokazivanja geometrijskih teorema.

5.1 Osnovni pojmovi Buhbergerove metode

Neka je K polje i neka je $A = K[y_1, \dots, y_n]$ prsten polinoma nad poljem K .

Definicija 24 (Kompatibilno uređenje) *Totalno uređenje $<$ u skupu M svih monoma u prstenu polinoma $K[y]$ nazivamo kompatibilno uređenje (sa množenjem), ako važi:*

1. $1 < m$, za svako $m \neq 1$;
2. $m_1 < m_2 \Rightarrow sm_1 < sm_2$, za svako $s, m_1, m_2 \in M$.

Primer 10 (Leksičko i uređenje po stepenu) *Sledeća dva uređenja zadovoljavaju definiciju kompatibilnog uređenja i najčešće se koriste u Buhbergerovoj metodi Grebnerovih baza:*

1. **Leksičko uređenje** $y_1^{s_1} \dots y_n^{s_n} < y_1^{t_1} \dots y_n^{t_n}$ ako postoji $k \leq n$ takvo da je $s_i = t_i$ za $i < k$ i $s_k < t_k$.
2. **Uređenje po stepenu** $y_1^{s_1} \dots y_n^{s_n} < y_1^{t_1} \dots y_n^{t_n}$ ako je $s = s_1 + \dots + s_n < t = t_1 + \dots + t_n$ ili je $s = t$ i prvi monom je leksički manji od drugog monoma.

¹U literaturi se kao ime metode najčešće koristi ime metoda Grebnerovih baza, ime koje je metodi dao autor, Bruno Buhberger, u čast svom profesoru Volkangu Grebneru (Wolfgang Gröebner).

Teorema 8 (Kompatibilno uređenje) *Svako kompatibilno uređenje je dobro definisano* ².

Dokaz: Pretpostavimo suprotno, tj. pretpostavimo da postoji beskonačni opadajući niz monoma $m_1 > m_2 > \dots > m_k > \dots$. Tvđenje se može jednostavno dokazati indukcijom po n , broju promenljivih prstena polinoma $K[y_1, \dots, y_n]$. Ovde ćemo navesti drugi, indirektan dokaz koristeći osnovnu Hilbertovu teoremu (teorema 2).

Neka je $J_k = (m_1, \dots, m_k)$ ideal polinoma u prstenu $K[y_1, \dots, y_n]$. Tada je $J_1 \subset J_2 \subset \dots$ rastući niz ideala. Prema osnovnoj Hilbertovoj teoremi, postoji ceo broj t takvo da je $J_t = J_{t+k}$ za svako $k > 0$. Prema tome, $m_{t+1} = p_1 m_1 + \dots + p_t m_t$. Ovo je moguće jedino ako su svi monomi m_i za $i \leq t$ delitelji monoma m_{t+1} , odnosno $m_{t+1} = s_i m_i$. Na osnovu definicije kompatibilnog uređenja:

$$1 < s_i \Rightarrow m_i < m_i s_i \Rightarrow m_i < m_{t+1}$$

što je kontradikcija. □

Izbor totalnog uređenja $<$ je predmet implementacije — za izvođenje Buhbergerove metode se može iskoristiti svako uređenje koje zadovoljava definiciju 24. Najčešće se koristi uređenje po stepenu.

5.2 Buhbergerova metoda

Razmatramo dalje prsten polinoma $A = K[y_1, \dots, y_n]$ nad poljem K .

Za dato kompatibilno uređenje $<$ među monomima polinoma, svaki ne-nula polinom p iz A se može jednoznačno napisati u obliku:

$$p = c_1 m_1 + \dots + c_k m_k$$

gde su $c_i \neq 0$ i monomi m_i su poređani u opadajućem poretku, odnosno $m_1 > m_2 > \dots > m_k$. Pri ovoj reprezentaciji, uvodimo nove pojmove:

Definicija 25 (Vodeći monom i vodeći term polinoma) *Monom m_1 se naziva vodeći monom polinoma p , a polinom $c_1 m_1$ se naziva vodeći term polinoma p . Takođe kažemo da su m_1, m_2, \dots, m_k monomi polinoma p . Za skraćeni zapis uvodimo i sledeće dve oznake koje se redom odnose na vodeći monom i vodeći term polinoma p , to su $lm(p)$ i $lt(p)$.*

Neka je S skup polinoma iz A i neka je g proizvoljan polinom.

Definicija 26 (B-svođenje) *Polinom g je b-svodiv po modulu S ako postoji polinom $f \in S$ takav da je vodeći monom $m_1 = lm(f)$ faktor nekog monoma m iz polinoma g . U tom slučaju se može izvršiti b-svođenje na sledeći način:*

1. f se može napisati u obliku $f = c_1 m_1 + f_1$ gde je $c_1 f_1 = lt(f)$

²Relacija totalnog uređenja je dobro definisana ukoliko svaki neprazni skup S ima najmanji element, ili ekvivalentno ukoliko ne postoji beskonačni opadajući niz $m_1 > m_2 > \dots$

2. $m = sm_1$, zato što je m_1 faktor od m
3. g se može napisati u obliku $g = cm + g'$
4. zamenom dobijamo novi polinom $g_1 = csm_1 + g'$

B-svođenjem smo od polinoma g dobili polinom g_1 tako što smo u njemu monom m zamenili termom c_1m_1 .

Izvođenjem b-svođenja kažemo da je polinom g sveden na polinom g_1 po modulu S u jednom koraku. Prateći pravila zamene, lako se pokazuje da važi:

$$g - g_1 \in \text{Ideal}(S)$$

Ako je dalje g_1 b-svodiv po modulu S , on se istim postupkom može svesti na polinom g_2 , i ovaj proces se može dalje nastaviti na isti način. Primenom teoreme 8 se može lako dokazati da svođenje ne može da se nastavi u beskonačnost — za neko k polinom g_k neće biti b-svodiv po modulu S .

Definicija 27 (Normalna forma) Polinom g_k koji je poslednji u nizu svođenja polinoma g po modulu S se naziva normalna forma polinoma g po modulu S .

Na osnovu definicije b-svođenja koja dozvoljava izbor proizvoljnog polinoma skupa S da se izvrši jedno b-svođenje, proces svođenja nad istim polinomom se može obaviti na više različitih načina, pa prema tome i normalna forma možda neće biti jednoznačno određena. Međutim, pokazaće se da za neke skupove S , redosled svođenja nije bitan i da svako svođenje vodi ka istoj normalnoj formi.

Definicija 28 (Grebnerova baza) Baza G ideala $I \subset K[y]$ se naziva Grebnerova baza od ideala I ako svako svođenje polinoma $g \in K[y]$ po modulu G kao rezultat ima istu normalnu formu.

Teorema 9 (Pripadnost polinoma idealu) Ako je G Grebnerova baza ideala I , tada $g \in I$ ako i samo ako je normalna forma polinoma g po modulu G jednaka nuli.

Prvi smer navedene teoreme se trivijalno dokazuje, za dokaz drugog smera pogledati [26].

Značaj teoreme je u tome što kada se jednom odredi Grebnerova baza ideala I , tada se pripadnost proizvoljnog polinoma idealu može utvrditi jednostavno. Sada ćemo opisati Buhbergerov algoritam konstrukcije konačne Grebnerove baze ideala I .

Definicija 29 (S-polinom) Neka su $p_1 = c_1m_1 + f_1$ i $p_2 = c_2m_2 + f_2$ dva polinoma različita od konstante sa vodećim termovima c_1m_1 i c_2m_2 . Neka je monom m najmanji zajednički sadržalac monoma m_1 i m_2 i neka su s_1 i s_2 dva monoma takvi da je $m = s_1m_1 = s_2m_2$.

Tada polinom:

$$p = s_1f_1 - \frac{c_1}{c_2}s_2f_2$$

nazivamo S-polinomom³ polinoma p_1 i p_2 .

³S iz naziva S-polinom nije povezano sa skupom S koji je prethodno pominjan.

Algoritam 1 (Buhbergerov algoritam konstrukcije Grebnerove baze) Neka je dat konačan skup S koji generiše ideal I . Grebnerove baza ideala I može se konstruisati na sledeći način:

Formirati S -polinome svih parova polinoma iz skupa $S_0 = S$. Svesti svaki od ovih polinoma na njihovu normalnu formu po modulu S_0 i ukoliko je taj rezultat različit od nule, dodati normalnu formu polinoma u skup S_1 za koji inicijalno važi $S_1 = S_0$. Ponaviti proces sa skupom S_1 da bi se dobio novi skup polinoma S_2 , i tako dalje formirati skupove S_3, S_4, \dots sve dok za neko k ne važi:

$$S_k = S_{k+1}$$

Teorema 10 (Buhbergerova teorema) Algoritam 1 se zaustavlja u konačnom broju koraka i poslednji skup u nizu S_k je Grebnerova baza ideala I .

Na sličan način kao u dokazu teoreme 8 može se pokazati da se Buhbergerov algoritam zaustavlja u konačnom broju koraka. Za drugi deo tvrdjenja, da je S_k Grebnerova baza, pogledati rad [26].

U Buhbergerovom algoritmu izvođenja Grebnerove baze osnovna operacija je izračunavanje S -polinoma dva polinoma i dodavanje rezultata u trenutni skup polinoma ukoliko je rezultat različit od nule. Sledeći primer pokazuje da se u određenim slučajevima i bez računanja može utvrditi da će rezultat biti upravo nula.

Primer 11 (S-polinom kod uzajamno prostih vodećih monoma) Neka su m_1 i m_2 vodeći monomi polinoma p_1 i p_2 i neka je najveći zajednički delilac monoma m_1 i m_2 jednak 1 (pišemo $NZD(m_1, m_2) = 1$). Tada se S -polinom p polinoma p_1 i p_2 može svesti na nulu po modulu skupa $\{p_1, p_2\}$.

Dokaz: Pošto je $NZD(m_1, m_2) = 1$, tada je $NZS(m_1, m_2) = m_1 m_2$ (najveći zajednički sadržalac). Prema tome, $s_1 = m_2$ i $s_2 = m_1$ pa je S -polinom jednak:

$$p = m_2 f_1 - \frac{c_1}{c_2} m_1 f_2$$

Vodeći monom polinoma p_1 je delilac drugog monoma polinoma p , pa možemo po njemu izvesti b-svođenje. Monom m_1 se zamenjuje polinomom $-f_1/c_1$ i dobija se polinom p' :

$$p' = m_2 f_1 + \frac{f_1 f_2}{c_2}$$

Sledeće b-svođenje se može izvršiti vodećim monomom polinoma p_2 . Vršimo zamenu monoma m_2 polinomom $-f_2/c_2$ i dobijamo:

$$p'' = -\frac{f_1 f_2}{c_2} + \frac{f_1 f_2}{c_2} = 0$$

□

Ovo jednostavno svojstvo ima značajnu primenu kod implementacije Buhbergerovog algoritma time što omogućava da se veliki broj operacija S -polinoma izbegne.

5.3 Dokazivanje geometrijskih teorema

Buhbergerova metoda se može koristiti za dokazivanje iste klase geometrijskih teorema za koje se primenjuje i Vuova metoda. Geometrijska teorema je zadata geometrijskom konstrukcijom i tvrđenjem koje je relacija između uvedenih objekata i koja se može svesti na jednakost (to su, na primer, relacije da su tačke kolinearne, da je zbir dva ugla jednak trećem, ali ne i da je zbir dve duži veći od treće duži). Odabirom koordinata tačaka iz konstrukcije i izborom slobodnih i zavisnih promenljivih, geometrijsko tvrđenje se može algebarski iskazati kao sistem polinoma (h_1, h_2, \dots, h_n) , koje nazivamo *hipoteze*:

$$\begin{aligned} h_1(u_1, \dots, u_d, x_1, \dots, x_t) &= 0 \\ h_2(u_1, \dots, u_d, x_1, \dots, x_t) &= 0 \\ &\dots \\ h_t(u_1, \dots, u_d, x_1, \dots, x_t) &= 0 \end{aligned}$$

i polinomom g koji predstavlja tvrđenje:

$$g = g(u_1, \dots, u_d, x_1, \dots, x_t) = 0$$

Za primenu metode Grebnerovih baza, korišćićemo proizvoljno kompatibilno uređenje među promenljivama za koje važi:

$$u_1 < u_2 < \dots < u_d < x_1 < \dots < x_t$$

Navedeni polinomi pripadaju prstenu polinoma $K[u_1, \dots, x_t]$, gde je K neko polje⁴. Polinomi se takođe mogu razmatrati i kao polinomi prstena $K(u_1, \dots, u_d)[x_1, \dots, x_t]$, i na taj način su slobodne promenljive izdvojene od zavisnih promenljivih. Razlika je samo u tome šta se smatra za koeficijente polinoma: u prvom slučaju to su elementi skupa K , dok su u drugom slučaju to elementi skupa $K(\mathbf{u})$.

U zavisnosti kom prstenu polinomi pripadaju, zavisi i rezultat funkcija vodeći monom i vodeći term polinoma. Razmotrimo sledeći primer.

Primer 12 (Dva različita pogleda na isti polinom) *Neka je dat polinom p :*

$$p = u_2 u_1 x_2 + u_1 x_2 + u_2^2 x_1$$

Ukoliko se radi o polinomu prstena $K[u_1, u_2, x_1, x_2]$, tada su vodeći monom i vodeći term polinoma:

$$\begin{aligned} lm(p) &= x_2 \\ lt(p) &= u_2 u_1 x_2 \end{aligned}$$

Međutim, ukoliko se radi o polinomu prstena $K(u_1, u_2)[x_1, x_2]$, onda su vodeći monom i vodeći term polinoma:

$$\begin{aligned} lm(p) &= x_2 \\ lt(p) &= (u_2 u_1 + u_1) x_2 \end{aligned}$$

⁴U praksi se koriste polja \mathbb{Q} i \mathbb{R}

Sada ćemo predstaviti algoritam Buhbergerove metode za dokazivanje geometrijskih teorema.

Algoritam 2 *Neka je J ideal koji generisan sistemom polinoma (h_1, \dots, h_n) .*

Korak 1 *Odrediti Grebnerovu bazu sistema polinoma (h_1, \dots, h_n) u prstenu polinoma $K(\mathbf{u})[\mathbf{x}]$ (primena algoritma 1). Svođenjem polinoma g na tako dobijenu bazu proveriti da li $g \in J$. Ukoliko g pripada idealu, tada je tvrdjenje tačno uz dodatne uslove nedegenerisanosti. U suprotnom, preći na sledeći korak.*

Korak 2 *Odrediti Grebnerovu bazu GB sistema polinoma $(h_1, \dots, h_n, zg - 1)$ u prstenu polinoma $K(\mathbf{u})[\mathbf{x}]$ (primena algoritma 1). Ukoliko je baza jedinična, odnosno ako je $GB = \{1\}$, tada je tvrdjenje tačno uz dodatne uslove nedegenerisanosti. U suprotnom, tvrdjenje nije tačno.*

Uslovi nedegenerisanosti se dobijaju prilikom izvođenja Grebnerove baze. To su svi delioci koji su uklonjeni u tom procesu (videti naredne primere). Uslovi nedegenerisanosti se navode kao nejednakosti polinoma (u obliku $q \neq 0$) i ne postoji opšta procedura prevođenja u geometrijsku formu (kao što postoji kod Vuove metode).

Za dokaz korektnosti algoritma pogledati rad [1]. Prvi korak algoritma je računski znatno manje zahtevan od drugog koraka. Iako je drugi korak kompletniji, u implementaciji Buhbergerove metode korišćen je samo prvi korak koji se pokazuje sasvim dovoljan za najveći broj geometrijskih teorema obrađenih u ovom radu.

Kod dokazivanja teorema euklidske geometrije, bazno polje polinoma je polje realnih brojeva \mathbb{R} .

5.3.1 Primene Buhbergerove metode

Primer 13 (Teorema o paralelogramu) *Isti kao i primer 2.*

U prstenu polinoma $R(u_1, u_2, u_3)[x_1, x_2, x_3, x_4]$ Buhbergerovim algoritmom određujemo Grebnerovu bazu sistema polinoma (h_1, h_2, h_3, h_4) :

$$\begin{aligned} GB(h_1, h_2, h_3, h_4) = & \\ & u_1x_1 - u_3u_1 \\ & u_3x_2 - u_3(u_2 - u_1) \\ & 2u_1x_3 - u_3u_1 \\ & -2u_3x_4 - u_3^2 \end{aligned}$$

Uslovi nedegenerisanosti su koeficijenti vodećih termova polinoma Grebnerove baze, u ovom slučaju to su: $u_3 \neq 0$ i $u_1 \neq 0$. Nakon deljenja sa uslovima nedegenerisanosti, Grebnerova baza se može zapisati u sledećem, standardnom, obliku:

$$\begin{aligned} GB(h_1, h_2, h_3, h_4) = & \\ & x_1 - u_3 \end{aligned}$$

$$\begin{aligned}x_2 &= (u_2 - u_1) \\x_3 &= \frac{u_3}{2} \\x_4 &= \frac{u_3}{2}\end{aligned}$$

Svođenje tvrđenja g u odnosu na bazu GB kao rezultat ima nula polinom, pa je tvrđenje dokazano uz NDG uslove: $u_3 \neq 0$ i $u_1 \neq 0$. Ovi uslovi imaju isto geometrijsko značenje kao i u primeru urađenom Vuovom metodom.

Primer 14 (Simsonova teorema) *Isti kao i primer 6*

Grebnerova baza sistema polinoma geometrijske konstrukcije je:

$$\begin{aligned}GB(h_1, \dots, h_7) = \\x_1 &= (u_3^2 + u_2^2 - u_1 u_2)/2u_3 \\x_2 &= u_1/2 \\x_3^2 &= (u_1 u_3 x_3 - u_3 u_4^2 + (u_3^2 + u_2^2 - u_1 u_2)u_4)/u_3 \\x_4 &= ((u_2 - u_1)u_3 x_3 + u_3^2 u_4 + (-u_1 u_2 + u_1^2)u_3)/(u_3^2 + u_2^2 - 2u_1 u_2 + u_1^2) \\x_5 &= ((u_2^2 - 2u_1 u_2 + u_1^2)x_3 + (u_2 - u_1)u_3 u_4 + u_1 u_3^2)/(u_3^2 + u_2^2 - 2u_1 u_2 + u_1^2) \\x_6 &= (u_2 u_3 x_3 + u_3^2 u_4)/(u_3^2 + u_2^2) \\x_7 &= (u_2^2 x_3 + u_2 u_3 u_4)/(u_3^2 + u_2^2)\end{aligned}$$

Grebnerova baza svodi geometrijsko tvrđenje g na nula polinom, čime je Simsonova teorema dokazana. Uslovi nedegenerisanosti su: $u_2 \neq 0$, $u_1 \neq 0$, $u_3 \neq 0$, $u_3^2 + u_2^2 - 2u_1 u_2 + u_1^2 \neq 0$, $u_3^2 + u_2^2 \neq 0$.

Sledeći primer je teorema koja ne može biti dokazana osnovnom metodom Vua.

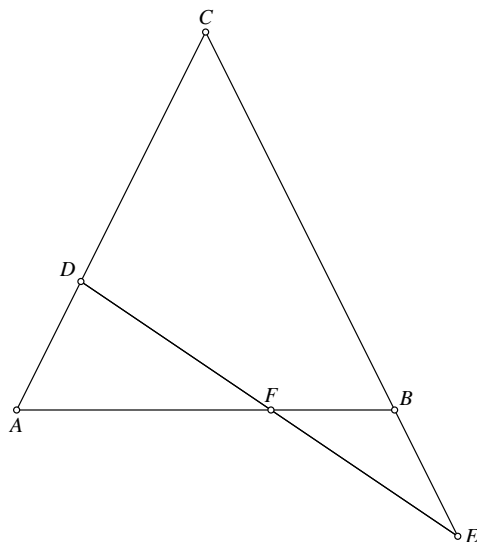
Primer 15 (Jednakokraki trougao) *Dat je jednakokraki trougao ABC gde je $AC \cong BC$. Tačke D i E se nalaze na pravama AC i BC i važi $AD \cong BE$. Neka je F presek pravih DE i AB . Dokazati da je $DF \cong EF$ (slika 5.1).*

Koristimo koordinatni sistem u kome će tačke konstrukcije imati sledeće koordinate: $A = (0, 0)$, $B = (u_1, 0)$, $C = (x_1, x_2)$, $D = (u_3, u_2)$, $E = (x_3, x_4)$ i $F = (x_5, 0)$. Tada su konstrukcija i tvrđenje opisani sledećim jednakostima:

$$\begin{aligned}AC \cong BC: & h_1 = 2u_1 x_1 - u_1^2 = 0 \\D \text{ pripada } AC: & h_2 = -x_1 x_2 + u_2 u_3 = 0 \\AD \cong BE: & h_3 = x_4^2 + x_3^2 - 2u_1 x_3 - x_2^2 - u_3^2 + u_1^2 = 0 \\E \text{ pripada } BC: & h_4 = (-x_1 + u_1)x_4 + u_2 x_3 - u_1 u_2 = 0 \\F \text{ pripada } ED: & h_5 = (-x_4 + x_2)x_5 + u_3 x_4 - x_2 x_3 = 0 \\tvrđenje } DF \cong EF: & g = (2x_3 - 2u_3)x_5 - x_4^2 - x_3^2 + x_2^2 + u_3^2 = 0\end{aligned}$$

Grebnerova baza sistema polinoma je:

$$\begin{aligned}GB(h_1, \dots, h_5) = \\x_5 &= (2u_3 + u_1)/2 \\x_4 &= 2u_2 u_3 / u_1 \\x_3 &= (u_3 + u_1) \\x_2 &= 2u_2 u_3 / u_1 \\x_1 &= u_1 / 2\end{aligned}$$



Slika 5.1: Jednakokraki trougao

Navedena baza svodi tvrđenje g na nula polinom, čime je teorema dokazana. Uslovi nedegenerisanosti su: $u_3 \neq 0$, $2u_3 - u_1 \neq 0$, $u_2 \neq 0$, $4u_2^2 + u_1^2 \neq 0$.

5.4 Poređenje sa Vuovom metodom

Vuova metoda i metoda Grebnerovih baza imaju isti domen, tj. obe se koriste za dokazivanje geometrijskih teorema zadatih u obliku sistema polinomnih jednačina i sa zaključkom zadatim takođe kao polinomna jednakost. Obe metode koriste uslove nedegenerisanosti da bi tvrđenje dokazali kao tačno u opštem slučaju.

Vuova metoda je orijentisana ka dokazivanju geometrijskih teorema, dok je metoda Grebnerovih baza opštija i ima mnogo šire primene. Vuova metoda u nekim slučajevima (geometrijske teoreme konstruktivnog tipa) može da dodatne uslove prevede u čitljivu formu. Takođe, Vuova metoda može biti uspešno primenjena i na neke slučajeve svodivih problema (Morlijeva teorema o trisekciji), dok to nije slučaj sa osnovnim oblikom metode Grebnerovih baza. Sa druge strane, metoda Grebnerovih baza može potvrditi neke teoreme koje nisu dokazive sa osnovnim oblikom Vuove metode (primer 8 iz prethodne glave).

Obe metode su potpune procedure odlučivanja, ali za Vuovu metodu još uvek ne postoji potpuna implementacija⁵. Sa druge strane, i takve nepotpune implementacije Vuove metode obično pokazuju bolje rezultate od potpunih implementacija Buhbergerove metode.

Do sada ne postoji temeljna uporedna teorijska studija o efikasnosti dve metode. Empirijski je utvrđeno da je Vuova metoda u proseku efikasnija, a osnovni razlog za ovo je brže vreme izvođenja karakterističnog skupa (korišćenog

⁵Čuov dokazivač je potpun samo za kvadratne slučajeve.

u Vuovoj metodi od izvođenja Grebnerove baze). Slični rezultati su potvrđeni i u ovom radu. U dodatku je navedeno 100 geometrijskih teorema od kojih su sve dokazane Vuovim metodom, dok neke nisu dokazane Buhbergerovom metodom zbog velike računске složenosti izvođenja Grebnerove baze. Obe metode su predmet interesovanja istraživača i do sada su pronađene brojne optimizacije implementacija osnovnih algoritama, pa se konačni zaključak o efikasnosti obe metode još uvek ne može doneti.

Glava 6

Implementacija dokazivača geometrijskih teorema

U ovoj glavi će biti opisana implementacija algebarskih dokazivača geometrijskih teorema na osnovu Vuove i Buhbergerove metode. Veliki deo implementacije je zajednički za većinu algebarskih metoda, pa se ova implementacija može iskoristiti ne samo za unapređivanje postojećih metoda, već i za razvoj novih algebarskih metoda.

Iz postavke problema (pogledati glavu 3.2), zaključujemo da je jedna od osnovnih struktura podataka koja će se koristiti pri dokazivanju geometrijskih teorema algebarskim metodama polinom nad prstenom:

$$\mathbb{R}(u_1, \dots, u_d)[x_1, \dots, x_t]$$

Prvi i bazni deo implementacije je biblioteka za rad sa polinomima ovoga tipa koja će podržavati osnovne operacije koje se koriste u algoritmima metoda (aritmetičke operacije, pseudo-deljenje, b-svođenje).

Drugi deo implementacije se odnosi na same metode dokazivanja. Svaku metodu karakterišu karakteristični algoritmi, a najveća kompleksnost metoda je u operacijama koje se vrše nad polinomima i koje su deo biblioteke za rad sa polinomima.

Ovako implementiran dokazivač je dovoljno opšt da se može koristiti u raznih kontekstima. Može biti integrisan u proizvoljnu klijent aplikaciju koja bi podatke o teoremi prenosila dokazivaču. U ovom radu će biti opisano jedno takvo integrisanje.

GCLC je aplikacija za vizuelizaciju geometrijskih konstrukcija koja podržava i komande za navođenje geometrijskih tvrđenja u obliku izraza nad geometrijskim objektima. Aplikacija je već sadržala jedan geometrijski dokazivač, zasnovan na metodi površina (koja je ne-algebarska metoda). U GCLC okruženje su sada implementirana i oba dokazivača opisana u ovom radu.

Integrisani sistem se sastoji iz dva dela. Prvi deo je zajednički deo za svaku algebarsku metodu i sastoji se od obrade zadatih konstrukcija i geometrijskog tvrđenja i njihovog prevođenja u algebarsku formu. Posebna pažnja je posvećena optimalnom izboru koordinata tačkaka.

Drugi deo integrisanog sistema se odnosi na pozivanje odgovarajuće algebarske metode za dokazivanje date teoreme i kreiranje odgovarajućeg tekstu-

alnog izlaza. Podržana su dva popularna i široko portabilna formata — L^AT_EX format i XML format.

Ceo projekat sadrži još mnogo tehničkih detalja koji su zanimljivi sa strane dizajna softvera, ali su manje zanimljivi u kontekstu dokazivanja geometrijskih teorema pa stoga neće biti opisani u ovom radu. Neki od ovih detalja su opcija prekidanja procesa dokazivanja kada se probije data vremenska granica, efikasna memorijska alokacija polinoma sa stotinama hiljada termova, kreiranje tekstualnog izlaza u više nivoa i u više datoteka, automatsko generisanje dodatka ove teze polazeći od geometrijskih konstrukcija sačuvanih u GCLC datotekama i drugi.

Dokazivač je implementiran u programskom jeziku C++. Izvorni kôd programa je slobodan i dostupan za korišćenje u nekomercijalne svrhe.

6.1 Konstruktivno i opisno zadate teoreme

U ovom poglavlju razmatraćemo na koji način se geometrijski problem može postaviti tako da je „razumljiv“ mašinskom programu. U tu svrhu, razlikovaćemo dva osnovna modela, to su konstruktivno zadate teoreme i opisno zadate teoreme.

Konstruktivno zadate teoreme odgovaraju intuitivnom načinu na koji se postavlja geometrijski problem i koji je široko prihvaćen u nastavi geometrije. Geometrijska konstrukcija je opisana nizom koraka, a geometrijsko tvrđenje je relacija između konstruisanih objekata. S druge strane, opisno zadate teoreme polaze od objekata koji čine geometrijsku konfiguraciju, opisuju međusobne odnose između njih, i na kraju (na isti način kao i kod konstruktivnih postavki) izražavaju geometrijsko tvrđenje kao relaciju između geometrijskih objekata sadržanih u konfiguraciji.

Ukoliko želimo da opišemo poznatu teoremu da svaki trougao ima ortocentar (visine trougla seku se u jednoj tački), odgovarajuća konstruktivna i opisna teorema bi mogle da izgledaju ovako:

Primer 16 (Ortocentar trougla — konstruktivna teorema) *U trouglu ABC , A_1 je podnožje visine iz temena A na stranicu BC , B_1 je podnožje visine iz temena B na stranicu AC i C_1 je podnožje visine iz temena C na stranicu AB . Prave AA_1 i BB_1 se seku u tački H . Dokazati da su tačke C , C_1 i H kolinearne.*

Primer 17 (Ortocentar trougla — opisna teorema) *Date su tačke A , B , C , A_1 , B_1 i C_1 . Tačke A , B i C su izabrane proizvoljno, važi da tačka A_1 pripada pravoj BC i $AA_1 \perp BC$, tačka B_1 pripada pravoj AC i $BB_1 \perp AC$, tačka C_1 pripada pravoj AB i $CC_1 \perp AB$, tačka H pripada pravoj AA_1 i pripada pravoj BB_1 . Dokazati da su tačke C , C_1 i H kolinearne.*

Zadati teoremu na konstruktivan način je često jednostavnije. Opisno postavljene teoreme su „pogodnije“ za algebarsko dokazivanje. Opis svake relacije među geometrijskim objektima se, kod algebarskih dokazivača, prevodi u jednu hipotezu izraženu polinomnom jednakošću. U prethodnom primeru, hipoteze tvrđenja su:

- A_1 se nalazi na pravoj BC

- $AA_1 \perp BC$
- B_1 se nalazi na pravoj AC
- $BB_1 \perp AC$
- C_1 se nalazi na pravoj AB
- $CC_1 \perp AB$
- H se nalazi na pravoj AA_1
- H se nalazi na pravoj BB_1

Iste hipoteze bi algebarski dokazivač postavio i u slučaju kada je teorema zadata na konstruktivan način, ali bi u tom slučaju bilo više posla zato što hipoteze nisu eksplicitno zadate kao u slučaju opisnih teorema. Kod konstruktivno zadatih teorema, hipoteze se generišu od konstrukcija gde svakoj konstrukciji može odgovarati nula, jedan, dva ili više polinoma hipoteza.

Dokazivač opisan u ovom radu dokazuje tvrđenja konstruktivnog tipa. U posebnoj poglavlju je opisana integracija dokazivača i aplikacije GCLC koja pruža interfejs za opisivanje geometrijskih konstrukcija. Verovatno najuspešniji dokazivač geometrijskih teorema, Čuov dokazivač [1], spada u grupu dokazivača kod kojih se teoreme navode u opisnom obliku. Mogućnost unošenja teorema u konstruktivnom obliku pruža veći komfor u radu korisnika, dok zadavanje teorema u opisnom obliku eliminiše moguće konflikte, ali i zahteva napredno poznavanje sistema od strane korisnika zato što analizu toga šta su hipoteze kod geometrijskog tvrđenja izvodi on sam, a ne program.

Na kraju, treba dodati da konstruktivni pristup ima ograničenja koja nisu prisutna kod opisnog pristupa. Da bi se, na primer, zadala Morlijeva teorema koja uključuje trisekciju ugla, kod dokazivača koji prihvata teoreme konstruktivno opisane potrebno je imati komandu koja će izvoditi konstrukciju trisekcije ugla (zato što se takva konstrukcija ne može izvesti od *elementarnih* konstrukcija). Ukoliko se koriste samo konstrukcije zasnovane na lenjiru i šestaru, onda se konstruktivnim pristupom može opisati strogo manji skup tvrđenja nego opisnim pristupom.

6.2 Dokazivač

Dokazivač se sastoji od tri celine — biblioteke za rad sa polinomima, implementacije Vuove metode i implementacije Buhbergerove metode. Dokazivač rešava problem dokazivanja teorema u strogo algebarskoj formi, pa su za njega geometrijski pojmovi nepoznati. Pretpostavka je da se obrada geometrijskih konstrukcija dešava u klijent aplikaciji i da se dokazivaču prosleđuje samo algebarski oblik teoreme.

6.2.1 Biblioteka za rad sa polinomima

Imajući u vidu problem koji se rešava, pre samog dizajniranja biblioteke polinoma postavljamo sledeće opšte uslove koje biblioteka treba da ispuni:

1. Polinomi pripadaju prstenu polinoma $\mathbb{R}(\mathbf{u})[\mathbf{x}]$;

2. Aritmetičke operacije nad polinomima su efikasne;
3. Operacije pseudo-deljenja i b-svođenja su efikasne;
4. Definisano je uređenje promenljivih $u_1 < u_2 < \dots < x_1 < \dots$.

Prvi uslov obezbeđuje mogućnost biblioteke da se koristi u implementaciji proizvoljne algebarske metode. Drugi uslov će garantovati efikasnost same biblioteke. Treći uslov se odnosi na dve osnovne operacije koje se koriste u Vuovoj i Buhbergerovoj metodi. Poslednji uslov je karakterističan za Buhbergerovu metodu, ali takođe obezbeđuje konzistentan zapis polinoma.

Zapis polinoma

Za dato uređenje promenljivih $u_1 < u_2 < \dots < x_1 < \dots$, zapis polinoma iz prstena polinoma $\mathbb{R}(\mathbf{u})[\mathbf{x}]$ je jednoznačno određen. Na primer, polinom koji sadrži termine $u_1x_2^4x_1$, $2u_2u_1x_2^2x_1$, $u_3x_2^2x_1$, $u_2^2u_1x_1$ i $u_3u_2x_1$ se zapisuje na sledeći način:

$$u_1x_2^4x_1 + u_3x_2^2x_1 + 2u_2u_1x_2^2x_1 + u_3u_2x_1 + u_2^2u_1x_1$$

Takođe se koristi i kompaktan zapis polinoma u kome se grupišu termini čiji su podskupovi koji se sastoje samo od promenljivih x_i jednaki. Kompaktan zapis je takođe jednoznačan, i za gornji polinom on izgleda:

$$u_1x_2^4x_1 + (u_3 + 2u_2u_1)x_2^2x_1 + (u_3u_2 + u_2^2u_1)x_1$$

Množenje polinoma

Razmotrimo operaciju množenja dva polinoma. Efikasno izvođenje ove operacije je veoma kompleksan problem i optimizacija ove operacije bitno utiče na strukturu podataka koja će se koristiti u implementaciji.

Pretpostavimo da su data dva polinoma od kojih svaki ima nekoliko stotina termova (polinom razmatramo kao skup termova). Rezultat množenja dva polinoma je suma proizvoda svakog terma iz prvog polinoma sa svakim termom iz drugog polinoma, a u ovom slučaju to je nekoliko stotina hiljada množenja termova. Međutim to nije sve — kada se dva terma pomnože i rezultat doda u skup termova, on može imati isti monom kao neki term koji je već sadržan u skupu. U tom slučaju, ta dva terma treba sabrati (sabiranje se izvodi tako što zajednički monom ostaje isti, a koeficijenti se sabiraju). Dakle, pri svakom od par stotina hiljada množenja, treba izvršiti pretragu u trenutnom skupu termova (koji predstavlja međurezultat množenja) i proveriti da li postoji term sa istim monomom — sve zajedno ovo je veoma skupa operacija. Razmotrimo sledeći primer:

Primer 18 (Množenje polinoma) Pomnožiti polinome $p = u_1x_2^2x_1 + (u_2u_1 + u_3)x_1$ i $q = x_2^2 + u_2$.

Množenje se izvodi tako što se svaki član skupa $\{u_1x_2^2x_1, (u_2u_1 + u_3)x_1\}$ množi sa svakim članom skupa $\{x_2^2, u_2\}$ i proizvod doda u krajnji rezultat. Dobijamo:

$$u_1x_2^2x_1x_2^2 + u_1x_2^2x_1u_2 + (u_2u_1 + u_3)x_1x_2^2 + (u_2u_1 + u_3)x_1u_2$$

Posle sređivanja (sortiranja po uređenju) dobijamo:

$$u_1x_2^4x_1 + u_2u_1x_2^2x_1 + (u_3 + u_2u_1)x_2^2x_1 + (u_3u_2 + u_2^2u_1)x_1$$

Drugi i treći sabirak imaju isti faktor, pa se mogu sabrati. Pri sabiranju, opet se dobija slučaj jednakih monoma, ovoga puta to je monom u_2u_1 . Krajnji rezultat je:

$$u_1x_2^4x_1 + (2u_2u_1 + u_3)x_2^2x_1 + (u_2^2u_1 + u_3u_2)x_1 \quad \blacksquare$$

Ukoliko je broj termova u prvom polinomu m , a u drugom polinomu n , množenje polinoma opisano na gornji način bi imalo složenost $O(m^2n^2) \cdot C$ gde je C složenost operacije poređenja monoma. Ova složenost dolazi odatle što imamo mn množenja termova, posle svakog množenja term se dodaje u skup koji ima $O(mn)$ termova. Za svaki član skupa se proverava da li ima zajednički monom sa dodatim termom.

Da bi se množenje polinoma ubrzalo, najpre treba odabrati pogodnu strukturu podataka koja će predstavljati skup termova. Ukoliko koristimo sortirani niz (vektor), tada se operacija pretrage (u cilju pronalaska člana skupa koji ima zajednički monom sa novim termom koji se dodaje skupu) može izvršiti u $O(\log(mn))$ vremenu binarnom pretragom. Ali operacija dodavanja novog člana u skup će zahtevati vreme proporcionalno sa $O(mn)$ (srednje vreme dodavanja novog člana u sortirani niz), tako da, iako je izvršavanje ubrzano, složenost je ostala ista.

Sledeći kandidat za strukturu podataka skupa termova jeste balansirano binarno stablo. Ova struktura podataka garantuje logaritamsko vreme izvršavanja tri osnovne operacije: pretraga, dodavanje i brisanje člana skupa. Pri dodavanju novog terma u skup termova koji je implementiran balansiranim stablom, koriste se sve tri navedene operacije. Prvo je potrebno proveriti da li u skupu postoji term koji ima zajednički monom sa termom koji se dodaje (operacija pretrage); ukoliko postoji, stari term se sabira sa novim termom, ukoliko je rezultat jednak nuli, stari term se izbacuje iz skupa (operacija brisanja); ukoliko term sa istim monomom ne postoji, novi term se dodaje u skup (operacija dodavanja). Korišćenjem balansiranog binarnog stabla, skup termova će se čuvati u sortiranom obliku i složenost operacije množenja će biti $O(mn \cdot \log(mn) \cdot C)$, što je verovatno i optimalno vreme izvršavanja tog problema.

Sada kada su tehnički problemi delimično objašnjeni, može se preći na dizajn klasa i struktura podataka. Polinomi su dizajnirani tehnikom od dna do vrha (eng. bottom-up approach), polazeći od prostijih objekata i redom gradeći složenije objekte.

Promenljive

Pošto se radi o polinomu iz prstena $\mathbb{R}(\mathbf{u})[\mathbf{x}]$, razlikujemo dva tipa promenljivih. Prvi tip su promenljive klase u_i , a drugi tip su promenljive klase x_i . I nadalje će neki od objekata biti duplirani (imaćemo u -objekte i x -objekte) kao posledica dva osnovna tipa promenljivih. I za prvi i za drugi tip promenljivih dovoljno je znati kojoj klasi promenljiva pripada i koji joj je indeks (na primer, u_3 promenljiva pripada u klasi sa indeksom 3). Objekat tipa **Promenljiva** nije definisan, umesto njega direktno je definisan objekat tipa **Monom**. Tip promenljive je definisan enumeracijom.

Stepeni

Stepeni su monomi jedne promenljive. Primeri stepena su: u_1^2 , u_3 , x_4^5 , itd. Objekat klase `Stepen` je određen svojom promenljivom (koja je određena tipom i indeksom promenljive) i celobrojnim stepenom. Klasa `Stepen` je definisana na sledeći način:

```
enum TIP_PROMENLJIVE
{
    TIP_PROMENLJIVE_U = 1,
    TIP_PROMENLJIVE_X = 2
};

class UStepen
{
    int indeks;
    int stepen;
};

class XStepen
{
    int indeks;
    int stepen;
};
```

Monomi

Monom je proizvod svojih termova, gde je jedan term monoma stepen promenljive. Primeri monoma su: u_1 , $u_2^2 u_1$, $x_2 x_1^3$, itd. Monom se predstavlja strukturom podataka skupa stepena.

Pošto implementacija skupa stepena ne utiče bitno na performanse biblioteke polinoma, skup koji je tipa vektora je sasvim zadovoljavajući:

```
vector<Stepen*> vecStepeni;
```

Termovi

Term polinoma je uređeni par koji čine koeficijent i monom polinoma. Prvi skup termova se odnosi na polinome prstena $\mathbb{R}[\mathbf{u}]$, a drugi skup termova se odnosi na polinome prstena $\mathbb{R}(\mathbf{u})[\mathbf{x}]$. Kod prvih (koje ćemo zvati u -termovi), koeficijenti su elementi skupa \mathbb{R} , a kod drugih (koje ćemo zvati x -termovi), koeficijenti su polinomi prstena $\mathbb{R}[\mathbf{u}]$.

Primeri u -termova su:

$$2u_1, 0.5u_3^2u_2, \frac{1}{3}u_4^2u_2^3u_1$$

Primeri x -termova su:

$$x^4, 2u_1x_1^3, (u_3^2u_2 + \frac{1}{3}u_2)x_2^2x_1^2$$

Termovi su definisani na sledeći način (x -termovi sadrže u -polinome koji su kasnije definisani):

```

class Term
{
    vector<Stepen*> vecStepeni;    // Monom terma
};

class UTerm : public Term
{
    double koeficijent;
};

class XTerm: public Term
{
    UPolinom* upKoficijent;
};

```

Polinomi

Polinom je zbir svojih termova i može se predstaviti strukturom podataka skupa termova. u -polinom je skup u -termova, dok je x -polinom skup x -termova. Kao što je rečeno u uvodnom delu, implementacija skupa termova bitno utiče na performanse biblioteke polinoma. Prvo ćemo navesti apstraktnu definiciju klase skupa termova, a zatim i samih polinoma.

```

class SkupTermova
{
    // dodaj term u skup
    void Dodaj(Term* term);

    // velicina skupa
    int Velicina();

    // vrati clan skupa za dati indeks
    Term* Clan(int indeks);

    // da li postoji term sa istim monomom kao zadati term
    bool Postoji(Term* term);
};

```

Apstraktna definicija klase `SkupTermova` se sastoji samo od javnog interfejsa. Interfejs je isti bez obzira kojom strukturom podataka je implementiran `SkupTermova` (bilo da je u pitanju neuređeni niz, sortirani vektor, balansirano stablo, itd.).

Optimalna struktura podataka za implementaciju klase `SkupTermova` je balansirano stablo. U ovom radu je korišćena posebna vrsta balansiranih stabla — AVL stabla [33].

Skup termova je implementiran kao balansirano binarno stablo, koje garantuje logaritamsko vreme operacija dodavanja, brisanja i traženja objekta iz skupa. Operacija dodavanja terma u skup koristi sve tri osnovne operacije (dodavanje, brisanje i traženje objekta u skupu). Prvo, treba proveriti da li u

skupu postoji term sa istim monomom kao i term koji se dodaje. Ako takav term postoji, onda taj term treba zameniti zbirom tog terma i terma koji se dodaje. Može se desiti da rezultat sabiranja bude nula i u tom slučaju term treba izbaciti iz skupa.

Klasa polinom ima sledeći minimalni interfejs:

```
class Polinom
{
    // termovi polinoma
    // x-polinom sadrzi x-termove, u-polinom sadrzi u-termove
    SkupTermova* skupTermova;

    // aritmetičke operacije
    Polinom* Pomnozi(Polinom* polinom);
    Polinom* Saberi(Polinom* polinom);
    void      Negacija();

    // operacije koje koristi Vuova metoda
    // pseudo deljenje
    Polinom* prem(Polinom* polinom);

    // operacije koje koristi Buhbergerova metoda
    // b-svodjenje
    Polinom* sPolinom(Polinom* polinom);
};
```

Klasa polinom je dovoljno apstraktna da može predstavljati i u -polinome i x -polinome istovremeno — prva klasa polinoma bi sadržala samo u -termove dok bi druga klasa polinoma sadržala samo x -termove.

Ovim su nabrojani osnovni objekti biblioteke polinoma i metode nad njima.

6.2.2 Algebarski dokazivač

Algebarskim dokazivačem geometrijskih teorema nazivamo dokazivač koji za ulazne vrednosti ima hipoteze geometrijske teoreme i tvrđenje teoreme u obliku polinoma iz prstena polinoma $\mathbb{R}(\mathbf{u})[\mathbf{x}]$, a kao izlaz, pored statusa dokaza koji može biti da je teorema dokazana, opovrgnuta ili nedokazana, daje i skup dodatnih uslova nedegenerisanosti koji moraju važiti da bi teorema bila tačna.

Algebarski dokazivač je implementiran sledećom apstraktnom klasom:

```
class AlgDokazivac
{
public:
    // funkcija vraća enumeraciju TvrđenjeStatus:
    virtual TvrđenjeStatus
    Prove(
        // ulazni parametar, sistem hipoteza
        Vector<Polinom> vecPolHipoteze,
        // ulazni parametar, tvrđenje teoreme
        Polinom* polTvrđenje,
```

```

        // ulazni parametar, vreme u milisekundama nakon
        // koga prekinuti se dokaz prekida
        double vremeGranica,
        // izlazni parametar, skup uslova nedegenerisanosti
        Vector<Polinom> vecPolNDGUslovi
    ) = 0;
};

// definicija enumeratora statusa dokaza
enum TvrdjenjeStatus
{
    TVRDJENJE_DOKAZANO,
    TVRDJENJE_OPOVRGNUTO,
    NEPOZNATO,
    PREKID_VREME,
    PREKID_SLOZENOST,
    PREKID_OSTALO
};

```

Pošto je kompleksnost algoritama algebarskih dokazivača eksponencijalna (bez obzira o kojoj se metodi radilo, svi algoritmi otkriveni do sada imaju eksponencijalnu složenost u opštem slučaju), u apstraktnu klasu algebarskih dokazivača je dodata i opcija da se rad prekine ukoliko je vreme potrošeno na dokaz probilo zadatu vremensku granicu.

6.2.3 Implementacija Vuove metode

Tri osnovne operacije Vuove metode su pseudo deljenje polinoma, svodenje sistema polinoma na trougaonu formu i računanje finalnog ostatka. Sve tri operacije su detaljno opisane u glavi 4 (glava o Vuovoj metodi). Ovde će biti prikazane konkretne implementacije u pseudo kôdu i programskom jeziku C++.

Vuova metoda, na način na koji je implementirana u ovom radu (nepotpun oblik Vuove metode), kao rezultat može potvrditi da je tvrđenje tačno, može za linearni sistem hipoteza potvrditi da tvrđenje nije tačno, i u svim ostalim slučajevima vratiti rezultat *nepoznato* što znači da tvrđenje nije ni potvrđeno, ali ni opovrgnuto.

Algoritam 3 (Vuova metoda) *Dokazivanje tvrđenja korišćenjem Vuove metode.*

Ulaz:

```

// sistem polinoma - hipoteze geometrijskih konstrukcija
Vector<Polinom> vecSistemPolinoma,
// tvrdjenje
Polinom polTvrdjenje

```

Izlaz: iz skupa {Tacno, Netacno, Nepoznato}

Procedura VuovaMetoda(vecSistemPolinoma, polTvrdjenje)

begin

```

// svesti ulazni sistem na trougaoni sistem
SvediNaTrougaoni(vecSistemPolinoma);

```

```

// finalni ostatak tvrdjenja po modulu trougaonog sistema
polOstatak = FinalniOstatak(vecSistemPolinoma, polTvrđenje);

if polOstatak == NulaPolinom
    return Tacno

// ako je ulazni sistem linearni, tada je Vuova metoda potpuna
if LinearniSistem(vecSistemPolinoma):
    return Netacno

// ulazni sistem nije linearni, Vuova metoda nije potpuna
return Nepoznato
end

```

Algoritam 4 (Pseudo ostatak deljenja polinoma)

Pseudo deljenje sa ostatkom dva polinoma više promenljivih je slično algoritmu deljenja polinoma jedne promenljive. Pseudo deljenje se uvek vrši po zadatoj promenljivoj i polinomi se razmatraju kao polinomi nad jednom promenljivom (po kojoj se vrši deljenje) dok se ostale promenljive razmatraju kao konstante.

Ulaz:

```

// polinom delilac
Polinom polDelilac,
// polinom delitelj
Polinom polDelitelj,
// indeks promenljive po kojoj se vrsi pseudo deljenje
int indeks

```

Izlaz:

```

// ostatak pseudo deljenja
Polinom polOstatak

```

Procedura PseudoOstatak(polDelilac, polDelitelj, indeks)

begin

```

// na pocetku ostatak je jednak deliocu
polOstatak = polDelilac

// dok je najveći stepen promenljive po kojoj se deli veći
// u polinomu ostatka nego u polinomu delitelja
while Stepen(polOstatak, indeks) >=
    Stepen(polDelitelj, indeks)
    //
    // polinome treba predstaviti kao polinome
    // promenljive po kojoj se deli
    // polOstatak = p = p1 * x^v + p2
    // polDelitelj = q = q1 * x^w + q2
    // ovde su (p1 * x^v) i (q1 * x^w) vodeći monomi
    // u odnosu na promenljivu x
    //

```



```

// operacija koju treba izvršiti je:
//  $p * q_1 - q * p_1 * x^{(v - w)}$ 

// vodeći monomi i stepeni promenljive po kojoj se deli
v = Stepen(polOstatak, indeks)
p1 = VodeciMonom(polOstatak, indeks) / Stepenuj(indeks, v)

w = Stepen(polDelitelj, indeks)
q1 = VodeciMonom(polDelitelj, indeks) / Stepenuj(indeks, w)

polOstatak = polOstatak * q1 -
             polDelitelj * p1 * Stepenuj(indeks, v - w)
end

return polOstatak
end

```

Algoritam 5 (Svođenje sistema polinoma na trougaonu formu)

Ovaj algoritam je opisan u poglavlju 2.3.3. U osnovi to je jednostavan algoritam gde se najveći deo izvođenja svodi na pravilan izbor sledeće promenljive u trougaonom sistemu.

Algoritam 6 (Finalni ostatak)

Finalni ostatak deljenja polinoma po sistemu polinoma se dobija sukcesivnim pseudo deljenjem svim polinomima iz sistema redosledom od poslednjeg do prvog polinoma iz skupa.

Ulaz:

```

// sistem polinoma - hipoteze geometrijskih konstrukcija
// u trougaonoj formi
Vector<Polinom> vecSistemPolinoma,
// polinom koji predstavlja tvrdjenje teoreme
Polinom polTvrđenje

```

Izlaz:

```

// polinom finalni ostatak sukcesivnog pseudo deljenja
Polinom polFinalniOstatak

```

Procedura FinalniOstatak(vecSistemPolinoma, polTvrđenje)

begin

```

    polFinalniOstatak = polTvrđenje

```

```

    // poslednji indeks
    indeks = vecSistemPolinoma.size()

```

```

    // pseudo deljenje od poslednjeg do prvog polinoma

```

```

    while indeks > 0:

```

```

        polFinalniOstatak = PseudoOstatak(
            vecSistemPolinoma[indeks - 1],

```

```

                                polFinalniOstatak,
                                indeks)
    end

    return polFinalniOstatak
end

```

6.2.4 Implementacija Buhbergerove metode

U glavi 5 su opisani algoritmi b-svođenja, konstrukcije Grebnerove baze i provera pripadnosti polinoma idealu. Sada će biti izloženi odgovarajući algoritmi u pseudo kôdu.

Algoritam 7 (Grebnerova baza) *Određivanje Grebnerove baze skupa polinoma $\mathbf{h} = (h_1, \dots, h_n)$*

Ulaz: Vector<Polinom> h = (h1, h2, ..., hn)

Izlaz: Grebnerova baza ulaznog skupa polinoma,
GB = (g1, g2, ..., gk)

Procedura GrebnerovaBaza(h1, ..., hn)

```

//
// 1) Pocetni skup S(0) je skup ulaznih polinoma
// 2) Skup S(1) se na pocetku postavlja na S(0).
//    Za svaki par polinoma (pi, pj) iz S(0) se
//    formira S-polinom q. q se svodi na normalnu
//    formu po modulu skupa S(0).
//    Ukoliko je rezultat ne-nula polinom, rezultat
//    se dodaje u skup S(1).
// 3) Na isti nacin se formira skup S(2) od skupa S(1)
// 4) Proces se zaustavlja kada vazi S(i+1) = S(i).
//

// pomocni vektor za formirane s-polinome parove polinoma
Vector<Polinom> vIzvedeniPolinomi

// u prvom koraku skup S0 je skup hipoteza h

ponavljaj
    vIzvedeniPolinomi.clear()

    // formiraj S-polinome svih parova
    za svaki par (pi, pj) iz h:
        q = Spolinom(pi, pj)
        r = NormalnaForma(q, h)

        if r != 0:
            vIzvedeniPolinomi.push_back(r)

```

```

// dodaj ne-nula S-polinome u trenutni skup Si
// da bi se formirao skup Si+1
za svaki p iz vIzvedeniPolinomi
    h.push_back(p)

// ako je skup vIzvedeniPolinomi prazan,
// znaci da je Si = Si+1
dok vIzvedeniPolinomi.size() > 0

return GB
end

```

Pomoćne procedure korišćene u glavnoj metodi za određivanje Grebnerove baze.

Algoritam 8 (S-polinom dva polinoma) *Algoritam formiranja S-polinoma dva data polinoma.*

```

Ulaz: Polinom p = c1m1 + f1,
      Polinom q = c2m2 + f2,

Izlaz: Polinom r = S-polinom(p, q)

BOOL Spolinom(p, q)
    s = NZD(m1, m2)
    s1 = s / m1
    s2 = s / m2
    r = c2 * s1 * f1 - c1 * s2 * f2

    return r
end

```

Algoritam 9 (b-svođenje polinoma g sa polinomom f)

B-svođenju polinoma g polinomom f . Proverava se da li je moguće izvršiti b-svođenje po nekom monomu polinoma g , i ukoliko je moguće vrši se svođenje. B-svođenje se uvek vrši najvećim mogućim monomom polinoma g ¹.

```

Ulaz: Polinom g = c1m1 + c2m2 + ...,
      Polinom f = cm + f1,
      indeks i

Izlaz: TRUE ukoliko je g svodiv po nekom monomu mi vrši
       se svodjenje
       FALSE ukoliko g je nesvodiv po svakom monomu mi,
       polinom g ostaje nepromenjen

```

BOOL B-svodjenje(g, f)

¹B-svođenje se može izvršiti po proizvoljnom monomu polinoma, izbor implementacije da to uvek bude najveći mogući monom je postavljen zbog determinisanosti dokazivača.

```

i = 1
while i < g.BrojTermova()
  if m.DeljivoSa(mi)
    g = g - ci * mi - c(mi / m)f1
    return TRUE
  i = i + 1

// ni sa jednim monomom polinoma g svodjenje nije moguće
return FALSE
end

```

Algoritam 10 (Određivanje normalne forme polinoma g)

Svođenje polinoma g na normalnu formu po modulu skupa polinoma $f = (f_1, f_2, \dots, f_n)$.

Ulaz: Polinom g ,
 Vector<Polinom> $f = \{f_1, f_2, \dots, f_n\}$

Izlaz: polinom g je sveden na normalnu formu po modulu skupa f

Procedura NormalnaForma(g, f)

```

j = 1
while j <= f.size()
  // svodjenje i-tog monoma sa j-tim
  // polinomom dokle god je moguće
  if B-svodjenje(g, f[j]) == FALSE
    // prelazak na sledeci polinom
    j = j + 1
end

```

Predstavljeni algoritmi su centralni deo implementiranog dokazivača korišćenjem Buhbergerove metode..

6.3 Integrisanje dokazivača u sistem GCLC

GCLC je aplikacija za vizuelizaciju geometrijskih konstrukcija ([34]). Geometrijska konstrukcija se zadaje komandama GCLC jezika gde svaka bazična konstrukcija (izbor tačke, presek dve prave, konstruisanje paralelne ili normalne prave iz jedne tačke u odnosu na drugu pravu, presek prave i kruga, presek dva kruga, itd) ima posebnu komandu. Na kraju, moguće je zadati tvrđenje geometrijske teoreme u obliku izraza nad konstruisanim geometrijskim objektima.

Integracija dokazivača u sistem GCLC se sastoji od analize geometrijske konstrukcije i njenog prevođenja u sistem polinoma koji predstavljaju hipoteze, zatim prevođenja izraza tvrđenja u polinom za koji treba dokazati da je posledica hipoteza i dodatnih uslova nedegenerisanosti² i na kraju pozivanje dokazivača

²Uslove nedegenerisanosti određuje sâm dokazivač

sa datim parametrima i vraćanja rezultata dokazivanja aplikaciji GCLC koja će ga prikazati korisniku.

Najteži deo integracije je upravo analiza geometrijskih konstrukcija i njihovo prevođenje u hipoteze teoreme.

6.3.1 Prevođenje konstrukcija u algebarsku formu

Prevođenje geometrijskog problema u algebarsku formu je operacija koja se vrši u svakoj algebarskoj metodi za dokazivanje geometrijskih teorema. Sa stanovišta implementacije algebarskih dokazivača, sloj programa koji stoji između geometrije i algebre je jedinstven i njega koriste svi implementirani algebarski dokazivači.

Uobičajeni tok dokazivanja jedne teoreme je sledeći:

1. Opisuje se geometrijska konstrukcija, na primer kroz interfejs aplikacije WinGCLC;
2. Postavlja se tvrđenje vezano za konstrukciju, na primer dve tačke su identične, tri prave su kolinearne, dve duži su jednake, dva vektora su jednaka, itd.;
3. Geometrijski problem se prevodi u algebarsku formu;
4. Algebarski formulisan problem se prosleđuje algebarskom dokazivaču;
5. Dokazivač dokazuje teoremu i vraća status dokaza. Status je iz skupa vrednosti: tvrđenje je dokazano, tvrđenje je opovrgnuto, tvrđenje nije ni dokazano niti opovrgnuto, dokazivanje je prekinuto;
6. U slučaju da je tvrđenje dokazano, dokazivač može vratiti i listu dodatnih uslova koji moraju važiti da bi tvrđenje bilo tačno, takozvane uslove nedegenerisanosti.

Broj konstrukcija koji je podržan od strane dokazivača, odnosno od strane sloja programa koji prevodi geometrijski problem u algebarski, je konačan. Za svaku konstrukciju postoje posebna pravila prevođenja konstrukcije u odgovarajuće polinome. Podržane geometrijske konstrukcije su opisane u poglavlju 3.2.

Prvi korak u prevođenju geometrijske konstrukcije u algebarsku formu je uvođenje koordinatnog sistema u ravni (razmatranje se odnosi na planarnu geometriju, s tim da većina iznetog važi i u slučaju višedimenzionone geometrije). Time su svakoj tački konstrukcije dodeljene koordinate (a, b) . Kao što je opisano u poglavlju 3.2, koordinata tačke može biti 0 (što znači da je tačka na x ili y osi), promenljiva u_i (nezavisna promenljiva, označava slobodan izbor tačke) ili promenljiva x_i (zavisna promenljiva, označava zavisnost tačke od drugih tačaka i objekata).

Svaka konstrukcija može generisati nula, jedan ili dva polinoma. Izbor proizvoljne tačke, recimo, ne generiše polinom. Presek dve prave će obično generisati dva polinoma; prvi polinom je uslov da tačka preseka pripada prvoj pravoj i drugi polinom je uslov da tačka preseka pripada i drugoj pravoj. Konstrukcija prave koja sadrži jednu tačku i paralelna je jednoj pravoj obično generiše jedan polinom, to je uslov da su dve prave paralelne. Međutim, za istu

konstrukciju moguće je i da nijedan polinom ne bude generisan — u slučaju da se konstruiše paralela iz tačke kojoj ta tačka pripada.

Postoji nekoliko detalja implementacije koji omogućavaju uspešno izvršavanje prevođenja u algebarsku formu. Poteškoće nastaju onda kada tekuća konstrukcija ne generiše automatski nijedan polinom. Ukoliko su, na primer, date dve tačke A i B , može se konstruisati prava m koja je simetrala duži AB . Međutim, to se još uvek ne može iskazati nijednim uslovom u obliku polinoma. Tek kasnije, ukoliko se naknadnim konstrukcijama dogodi, na primer, da pravoj m pripada neka tačka M , generisaće se polinom koji opisuje uslov da su duži MA i MB jednake. Ovakvi problemi se rešavaju obilaskom konstrukcija u više prolaza. U prvom prolazu se nabroje osnovni objekti — to su tačke, prave i krugovi, i lokalizuju se relacije pripadnosti među njima. Posle prvog koraka je poznato za svaku pravu koje tačke sadrži i za svaki krug koje tačke sadrži. U sledećem prolazu se konstrukcije prevode u polinome. Kada bi se sada obrađivala konstrukcija simetrale duži, automatski bi se za svaku tačku koja pripada simetrali generisao po jedan polinom koji opisuje uslov da je tačka jednako udaljena od krajeva duži. Treba napomenuti da se u ovom koraku, prevođenja geometrijske konstrukcije u sistem polinoma, ne uvodi nijedan novi objekat u konstrukciju — nijedna nova tačka, prava ili krug.

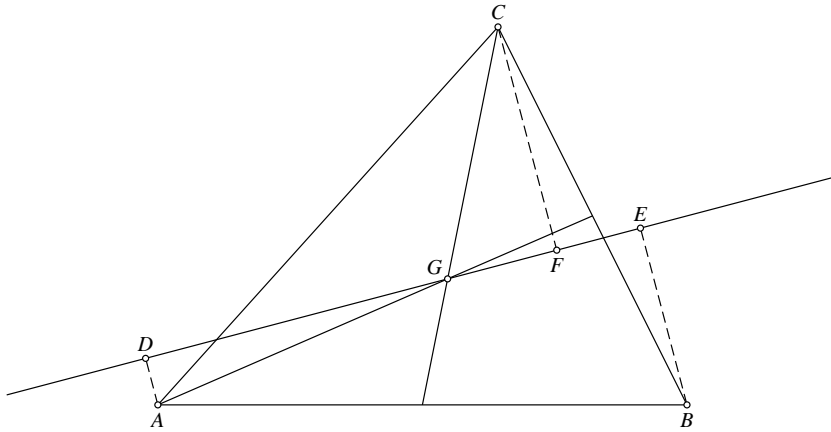
Tokom generisanja sistema polinoma od geometrijskih konstrukcija (generisanje sistema hipoteza), izvodi se i važna optimizacija pred sâmo dokazivanje teoreme — to je minimizacija broja promenljivih. Izbor proizvoljne tačke ravni u aplikaciji GCLC se zadaje komandom *point*, na primer:

```
point A 20.0 25.0
```

gde je A naziv tačke, a sledeće dve vrednosti su koordinate tačke u Dekartovoj ravni za ilustraciju koju proizvodi GCLC. Svaka ovako zadata tačka se smatra slobodnom tačkom konstrukcije, tj. tačkom koja zauzima opšti položaj. Dokazivač će prvoj slobodnoj tački konstrukcije dodeliti koordinate $(0, 0)$ (koordinatni početak). Druga slobodna tačka konstrukcije će dobiti koordinate $(u_1, 0)$, treća slobodna tačka će dobiti koordinate (u_2, u_3) , itd.

Sistem dalje čuva uglove koje prave grade u odnosu na x osu. Ukoliko se prve dve navedene tačke nalaze na x osi, prava koja ih sadrži gradi ugao od 0° sa x osom (paralelna je x osi). Slicno, ukoliko su prve dve tačke date na y osi, prava koja ih sadrži gradi ugao od 90° sa x osom. Ugao se ne može odrediti za svaku pravu, pošto se geometrijska konstrukcija navodi u opštem slučaju najveći broj pravih će graditi proizvoljan ugao sa x osom. Međutim, kao što smo videli za pravu koja sadrži prve dve tačke konstrukcije, za neke prave se ovaj ugao može pouzdano odrediti. Ukoliko je za pravu p ugao pouzdano određen, onda je ugao pouzdano određen i za sve prave paralelne sa tom pravom ili normalne na nju, ili koje grade fiksni ugao sa tom pravom. Tako se mogu lokalizovati sve prave sa određenim uglom u odnosu na x osu, jednim prolazom kroz sve konstrukcije geometrijske konfiguracije.

Za dokazivač je bitno da su određene sve prave konstrukcije za koje se pouzdano zna da su paralelne x osi ili da su normalne na x osu. Prvo, takve prave se koriste u minimizaciji broja promenljivih, zato što će sve tačke na jednoj takvoj pravoj imati istu promenljivu za x (odnosno y) koordinatu. Drugo, takve prave su bitne i kod generisanja polinoma nekih tvrđenja. Takvo je recimo tvrđenje da su dva vektora jednaka. Pošto su vektori paralelni, ovo tvrđenje je ekvivalentno



Slika 6.1: Neoptimizovana konfiguracija

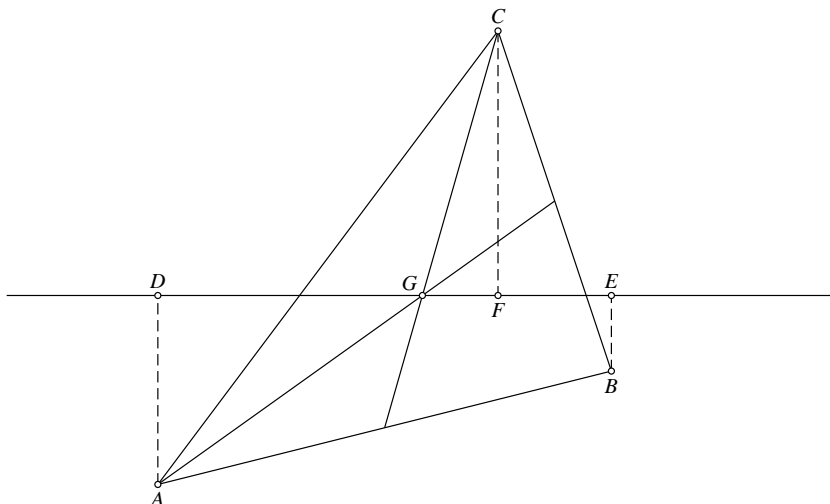
da su x projekcije vektora jednake – ako vektor nije paralelan y osi ili tvrđenju da su y projekcije vektora jednake — ako vektor nije paralelan x osi. Da bi se znalo koje ekvivalentno tvrđenje od dva navedena treba iskoristiti za generisanje polinoma, mora se znati da li prava ima specijalan položaj paralelnosti sa x ili y osom.

Izborom da prve dve slobodne tačke konstrukcije određuju koordinatni početak i jednu tačku x ose postavljenog Dekartovog koordinatnog sistema se i korisniku koji zadaje tvrđenje ostavlja mogućnost dodatne optimizacije. Sve tačke konstrukcije koje su detektovane da se uvek nalaze na x osi će imati y koordinatu jednaku nuli, čime je za svaku takvu tačku broj promenljivih smanjen za jedan. U zavisnosti kojim redom se navode slobodne tačke konstrukcije, broj tačaka čije je koordinate moguće optimizovati može biti veći ili manji.

Razmotrimo dve geometrijske konfiguracije ilustrovane slikama 6.1 i 6.1 — neoptimizovanu konfiguraciju i optimizovanu konfiguraciju.

Kod prve konfiguracije konstrukcija je započeta tačkama A i B , dok je kod druge konfiguracije konstrukcija započeta tačkama D i G . Ove dve konfiguracije su ekvivalentne i za obe važe ista tvrđenja, ali druga konfiguracija ima dve tačke više na x osi (prva konfiguracija ima dve, a druga četiri tačke na x osi). Time je broj promenljivih u drugom slučaju manji za dva što kao posledicu ima brže izvođenje dokaza.

U dodatku A.2 je kroz primer Paposove teoreme prikazano kako se geometrijski problem zadaje u programu GCLC i, kao početni deo dokaza, kako se problem prevodi u algebarsku formu korak po korak. Na ovom primeru se mogu videti na delu sve opisane optimizacije, mogu se videti koje prave su prepoznate da grade fiksni ugao u odnosu na x osu i kako su tačkama na tim pravama



Slika 6.2: Optimizovana konfiguracija

dodeljene posebne (optimizovane) koordinate.

6.3.2 Dokazivanje tvrđenja

Algebarski dokazivači, u osnovnoj implementaciji, nemaju nikakvih dodirnih tačaka sa geometrijom. Oni kao ulaz imaju algebarsku formulaciju problema, a kao izlaz daju status dokaza i, ukoliko je tvrđenje dokazano, listu dodatnih uslova koja moraju važiti da bi tvrđenje bilo tačno (uslovi nedegenerisanosti). Dodatni uslovi su takođe u algebarskoj formi, dati kao nejednakosti nad polinomima (npr. $u_1 \neq u_2$). Uslovi se dalje mogu analizirati i neki od njih prevesti u geometrijsku formu.

Algebarski dokazivači imaju zajednički interfejs. Minimalni ulazni podaci za algebarski dokazivač su sistem polinoma (hipoteze teoreme) i polinom tvrđenja teoreme. Ostali ulazni podaci mogu biti opcije za prekidanje dokaza u slučaju da je kompleksnost problema prevelika za dokazivač.

Vreme izvršavanja algebarskih dokazivača geometrijskih teorema je eksponencijalno za sve postojeće metode. U praksi, to znači da realno vreme rada programa može dosta da varira u zavisnosti od zadatog problema. Dokaz za većinu teorema (preko 90 teorema) dokazanih ovde implementiranim dokazivačem traje manje od po 100 milisekundi na trenutno prosečnoj računarskoj konfiguraciji. Međutim, zbog eksponencijalne složenosti metode, vreme izvršavanja raste veoma brzo kako se dokazivaču postavljaju kompleksnija tvrđenja. Za očekivati je da dokazi nekih problema traju nekoliko minuta, nekoliko sati, pa i nekoliko dana.

Dva su osnovna načina da se kontroliše vreme izvršavanja. Prva opcija je da se programu zada maksimalno vreme izvršavanja i ukoliko dokaz nije završen u tom vremenu, prekida se dalje izvršavanje i daje signal o prekidu rada. Druga opcija je da se izvršavanje prekine ukoliko broj termova u nekom polinomu koji je

dobijen tokom izvršavanja dokaza premaši unapred zadatu granicu. Ova opcija, naravno, ne garantuje donju granicu trajanja dokazivanja. Njen smisao je da sve dok su veličine polinoma u okviru neke granice, dokaz se odvija u okviru prihvatljive kompleksnosti.

Ovim smo opisali i dve mere kompleksnosti dokaza. Prva mera je vreme trajanja dokaza, a druga mera je maksimalni broj termova u nekom polinomu koji je dobijen tokom izvršavanja dokaza. Obe vrednosti se prikazuju u odgovarajućem izveštaju (pogledati primer iz dodatka A.2).

Izlaz dokazivača su status dokaza i eventualno uslovi nedegenerisanosti. Status dokaza je jedan od sledećih:

Dokazano — tvrđenje je dokazano

Opvrgnuto — tvrđenje je opovrgnuto

Nepoznato — tvrđenje nije ni dokazano ni opovrgnuto

Vreme — dokazivanje je prekinuto zato što je premašena postavljena vremenska granica

Kompleksnost — dokazivanje je prekinuto zato što je premašena zadata kompleksnost (iskazana kao maksimalan broj termova kod među-polinoma kreiranog tokom dokaza)

Lista mogućih statusa dokaza je proširiva dodavanjem novih opcija dokazivaču (opcije koje trenutno nisu podržane). Korisna opcija bi bila prekidanje dokaza u proizvoljnom trenutku, u tom slučaju bi se definisao novi status sa imenom **Prekid**. Treba predvideti i nepredvidljive greške tokom dokazivanja (eng. exceptions), takvom slučaju bi odgovarao status **Ostalo**.

6.3.3 Tekstualni izlaz dokazivača

Algebarski dokazivači, skoro bez izuzetka, proizvode dokaze koji se ne mogu geometrijski rekonstruisati. Za takve dokaze kažemo da su *geometrijski nečitljivi*. Ovakav opis, iako široko prihvaćen, nije najtačniji. Algebarski dokaz je itekako čitljiv i nudi obilje informacija. Posebna pažnja u razvoju dokazivača je posvećena kreiranju potpunog i kvalitetnog tekstualnog izlaza. Upoređujući sa tekstualnim izlazima koje proizvode drugi postojeći dokazivači (javno dostupni dokazivači su nabrojani u poglavlju 1.2), tekstualni izlaz je podignut na viši nivo, otkrivajući potpun tok dokaza i sve korake koji su izvedeni.

Implementirani algebarski dokazivači, kroz integraciju u sistem GCLC, proizvode tekstualni izlaz dokaza u dva tekstualna formata — \LaTeX i XML. Uz podršku GCLC za XML, prisutna je i skripta XSLT transformacija koja od XML izlaza kreira HTML verziju dokaza koja u najvećoj meri liči na \LaTeX izlaz.

Podrškom dva popularna formata — \LaTeX i XML, dokazi dobijeni od algebarskih dokazivača kroz sistem GCLC se mogu koristiti na svim operativnim sistemima i na internetu.

Glava 7

Zaključci i dalji rad

U ovoj glavi su prikazani osnovni rezultati rada na implementaciji programa algebarskih dokazivača. Pored kratkog pregleda šta je sve urađeno i sa kolikom uspešnošću, ukratko su opisani i dalji mogući pravci razvoja rada.

7.1 Zaključci

7.1.1 Pregled

Rad prezentovan u ovom tekstu je implementiran u vidu programskih biblioteka i integracije u druge geometrijske aplikacije. Sledeća lista daje pregled programskih modula koji su napisani:

- Biblioteka za rad sa polinomima više promenljivih. Biblioteka podržava osnovne aritmetičke operacije nad polinomima, algoritme koji se koriste u algebarskim metodama (psedo deljenje polinoma, b-svođenje polinoma), ispis polinoma u \LaTeX i XML formatima. Biblioteka je optimizovana za efikasan rad sa polinomima koji imaju i nekoliko stotina hiljada termova.
- Implementacije Vuove i Buhbergerove metode. Obe metode su implementirane nad apstraktnom algebarskom metodom koja se može iskoristiti kao polazna osnova za dodavanje novih metoda. Apstraktna metoda pruža podršku za ograničavanje kompleksnosti dokazu u vidu prekidanja dokaza nakon zadate vremenske granice, kao i zajednički programski interfejs algebarskih metoda.
- Integracija algebarskih dokazivača u sistem GCLC. GCLC aplikacija ([34]) je softverski proizvod za vizuelizaciju i učenje geometrije čija je prva verzija izašla još 1996. godine. Detalji o integrisanju su opisani u glavi 6, a ovde će biti naglašeno da je sama integracija u popularan softver sa tradicijom od preko 10 godina, kakav je GCLC, dokaz kvaliteta i stabilnosti kôda.
- Bogat tekstualni izlaz koji proizvode dokazivači u \LaTeX i XML formatima. Podrška popularnih formata je jedan od doprinosa otvorenosti rada.
- Javna dostupnost kôda u izvornom obliku. Studentima i istraživačima koje zanima ova oblast je na taj način pružen kompletni uvod u algebarske dokazivače: tekst koji opisuje teorijsku osnovu, GCLC aplikacija sa

jednostavnim interfejsom za zadavanje geometrijskih tvrdjenja, korpus od preko 100 geometrijskih teorema koje su dokazive izloženim dokazivačima i, na kraju, izvorni kôd programa koji može poslužiti kao polazna tačka za nove radove i nove algebarske dokazivače.

7.1.2 Rezultati

Pored navedenih rezultata u programskom delu rada, izdvaja se i:

- Više od 100 teorema dokazano Vuovom metodom
- Više od 70 teorema dokazano Buhbergerovom metodom
- Preko polovine teorema dokazano je u vremenu manjem od 30 milisekundi

Sledeća tabela prikazuje poređenje tri metode implementirane u sistemu GCLC na korpusu geometrijskih navedenih u dodatku.

Teorema	Vuova metoda	Buhbergerova metoda	Metoda površina
Talesova teorema (primer 21)	0.002s	0.002s	0.003s
Altitude Center Exists Theorem (primer 28)	0.005s	0.048s	0.006s
Altitude Center Exists Theorem (primer 28)	0.005s	0.048s	0.006s
Dualna teorema visinama trougla (primer 29)	0.011s	0.03s	0.01s
Upisani krug trougla (primer 30)	0.011s	0.043s	nepoznata greška
Središnja duž trougla (primer 31)	0.004s	0.004s	0.001s
Paralelogram teorema (primer 32)	0.002s	0.002s	0.0s
Paralelogram teorema 2 (primer 33)	0.005s	0.004s	0.075s
Opisani krug trougla (primer 34)	0.003s	0.003s	0.071s
Paposova teorema (primer 35)	0.012s	vreme > 21s	0.186s
Paposova teorema (druga verzija) (primer 36)	0.03s	1.325s	0.079s
Dualna Paposova teorema (primer 37)	0.026s	vreme > 21s	—
Paposov heksagon (primer 38)	0.028s	1.41s	0.074s
Površina trougla (primer 27)	0.001s	0.001s	0.001s
Tri kvadrata (primer 39)	0.022s	0.132s	—

Teorema	Vuova metoda	Buhbergerova metoda	Metoda površina
Gergonova tačka (primer 40)	0.076s	vreme > 21s	nepoznata greška
Adamsov krug (primer 41)	22.162s	vreme > 21s	—
Teorema 3 iz [1] (primer 42)	1.565s	vreme > 21s	1.713s
Harmonične tačke 2 (primer 22)	0.01s	vreme > 21s	0.004s
Teorema 25 iz [1] (primer 43)	3.411s	vreme > 21s	vreme > 21s
Teorema 28 iz [1] (primer 44)	0.046s	vreme > 21s	0.016s
Teorema 29 iz [1] (primer 45)	0.144s	0.015s	—
Teorema 30 iz [1] (primer 46)	0.008s	0.012s	—
Teorema 31 iz [1] (primer 47)	0.005s	0.01s	—
Teorema 35 iz [1] (primer 48)	0.067s	vreme > 21s	nepoznata greška
Teorema 37 iz [1] (primer 49)	0.004s	0.003s	nepoznata greška
Teorema 42 iz [1] (primer 50)	0.034s	0.062s	0.008s
Teorema 46 iz [1] (primer 51)	0.127s	vreme > 21s	vreme > 21s
Teorema 49 iz [1] (primer 52)	0.006s	0.328s	0.007s
Dezargova teorema (primer 23)	0.234s	0.494s	0.534s
Teorema 55 iz [1] (primer 53)	0.006s	0.005s	3.059s
Teorema 56 iz [1] (primer 54)	0.005s	0.006s	0.132s
Teorema 58 iz [1] (primer 56)	0.081s	0.631s	—
Teorema 59 iz [1] (primer 57)	0.047s	vreme > 21s	—
Teorema 69 iz [1] (primer 58)	0.028s	0.087s	0.045s
Teorema 75 iz [1] (primer 59)	0.031s	vreme > 21s	nepoznata greška
Teorema 77 iz [1] (primer 60)	0.033s	—	nepoznata greška
Teorema 82 iz [1] (primer 61)	0.059s	vreme > 21s	vreme > 21s

Teorema	Vuova metoda	Buhbergerova metoda	Metoda površina
Teorema 84 iz [1] (primer 62)	0.021s	0.388s	vreme > 21s
Menelajeva teorema (primer 24)	0.003s	0.003s	0.038s
Teorema 85 iz [1] (primer 63)	0.038s	0.032s	vreme > 21s
Teorema 86 iz [1] (primer 64)	0.017s	0.082s	—
Teorema 88 iz [1] (primer 65)	0.275s	0.104s	—
Teorema 91 iz [1] (primer 66)	0.006s	0.02s	—
Teorema 92 iz [1] (primer 67)	0.104s	vreme > 21s	—
Teorema 94 iz [1] (primer 68)	2.515s	vreme > 21s	nepoznata greška
Teorema 95 iz [1] (primer 69)	0.005s	0.014s	—
Teorema 97 iz [1] (primer 70)	0.022s	vreme > 21s	nepoznata greška
Teorema 5.1 iz [1] (primer 71)	0.01s	0.04s	—
Teorema 101 iz [1] (primer 72)	0.156s	vreme > 21s	—
Teorema 104 iz [1] (primer 75)	0.044s	0.09s	—
Konstrukcija pravog ugla (primer 26)	0.001s	0.002s	nepoznata greška
Teorema 102 iz [1] (primer 73)	0.059s	1.527s	—
Čevina teorema (primer 20)	0.007s	0.018s	0.001s
Teorema 103 iz [1] (primer 74)	0.003s	0.003s	0.489s
Teorema 108 iz [1] (primer 76)	0.014s	0.181s	—
Teorema 110 iz [1] (primer 77)	0.142s	0.146s	—
Teorema 114 iz [1] (primer 78)	0.029s	0.039s	—
Teorema 117 iz [1] (primer 79)	4.037s	vreme > 21s	—
Teorema 119 iz [1] (primer 80)	0.025s	0.04s	—
Teorema 120 iz [1] (primer 81)	0.005s	0.004s	0.073s

Teorema	Vuova metoda	Buhbergerova metoda	Metoda površina
Teorema 121 iz [1] (primer 82)	0.004s	0.003s	—
Teorema 123 iz [1] (primer 84)	0.7s	vreme > 21s	nepoznata greška
Teorema 126 iz [1] (primer 85)	0.053s	1.649s	—
Teorema 127 iz [1] (primer 86)	0.051s	vreme > 21s	nepoznata greška
Teorema 132 iz [1] (primer 87)	0.071s	vreme > 21s	nepoznata greška
Teorema 133 iz [1] (primer 88)	0.005s	0.006s	—
Teorema 136 iz [1] (primer 89)	0.049s	vreme > 21s	—
Teorema 137 iz [1] (primer 90)	0.007s	0.019s	nepoznata greška
Teorema 138 iz [1] (primer 91)	0.006s	0.008s	nepoznata greška
Teorema 140 iz [1] (primer 92)	0.005s	0.008s	—
Teorema 141 iz [1] (primer 93)	0.005s	0.008s	nepoznata greška
Teorema 145 iz [1] (primer 94)	0.231s	0.134s	—
Teorema 150 iz [1] (primer 95)	0.095s	0.106s	—
Teorema 155 iz [1] (primer 97)	0.027s	vreme > 21s	—
Teorema 172 iz [1] (primer 98)	0.101s	vreme > 21s	nepoznata greška
Teorema 219 iz [1] (primer 100)	0.014s	1.145s	—
Sinusna teorema (primer 101)	0.004s	0.004s	—
Kosinusna teorema (primer 102)	0.001s	0.001s	—
Ojlerova formula (primer 103)	0.125s	4.101s	nepoznata greška
Brahmaguptina teorema (primer 104)	0.006s	vreme > 21s	nepoznata greška
Vivianijeva teorema (primer 105)	4.358s	—	—
Krug šest tačkica. (primer 106)	0.381s	vreme > 21s	—
Harmonijska spregnutost (primer 107)	0.048s	0.068s	1.111s

Teorema	Vuova metoda	Buhbergerova metoda	Metoda površina
Leptir teorema (primer 108)	7.627s	vreme > 21s	nepoznata greška
Krug osam tačaka (primer 109)	1.632s	vreme > 21s	nepoznata greška
Uopštena Menelajeva teorema (primer 25)	0.012s	0.04s	0.043s
Ojlerova prava (primer 110)	0.038s	0.38s	vreme > 21s
Gausova prava (primer 111)	2.591s	vreme > 21s	0.036s
Uglovi nad istom tetivom (primer 112)	0.004s	0.004s	nepoznata greška
Teorema 20 iz [5] (primer 113)	1.205s	6.062s	0.061s
Teorema 22 iz [5] (primer 114)	0.012s	0.06s	vreme > 21s
Problem u jednakstraničnom pravouglom trouglu (primer 115)	0.005s	0.02s	vreme > 21s
Konstrukcija jednakostraničnog trougla (primer 116)	0.002s	0.002s	nepoznata greška
Leon-An teorema (primer 117)	0.079s	vreme > 21s	—
Krug devet tačaka (primer 118)	6.855s	vreme > 21s	nepoznata greška
Nobsova teorema (primer 119)	0.081s	vreme > 21s	nepoznata greška
Paskalova teorema (primer 120)	0.298s	vreme > 21s	nepoznata greška
Ptolomejeva teorema (primer 121)	0.107s	0.046s	—
Simsonova teorema (primer 122)	0.097s	vreme > 21s	nepoznata greška
Vorinjonova teorema (primer 123)	5.584s	10.382s	0.01s

7.1.3 Automatska detekcija nekonzistentne konstrukcije

U sistemu za vizuelizaciju geometrijskih konstrukcija, kakav je aplikacija GCLC, geometrijska konstrukcija se zadaje kao niz elementarnih konstrukcija¹ od kojih svakoj odgovara po jedna komanda koja se prosleđuje aplikaciji. Nije svaka

¹Geometrijska konstrukcija, možemo još reći i geometrijska konfiguracija, je skup geometrijskih objekata i relacija koje važe između njih. Jedna elementarna konstrukcija je jedan korak u opisivanju geometrijske konstrukcije. Elementarna konstrukcija može biti konstrukcija preseka dve prave, konstrukcija prave koja prolazi kroz dve date tačke, konstrukcija podnožja iz date tačke na datu pravu, itd.

komanda validna geometrijska konstrukcija. Recimo, prava određena tačkama A i B nije pravilno definisana ukoliko jedna od tačaka nije prethodno uvedena. Prava određena tačkama A i A je takođe nepravilno definisana. Ova dva slučaja su primeri *sintakasnih* grešaka, a to su tipovi grešaka koji se lako detektuju od strane aplikacije za vizuelizaciju geometrijske konstrukcije.

Ukoliko su sve komande koje čine geometrijsku konstrukciju sintaksno ispravne, to i dalje ne znači da one čine validnu geometrijsku konstrukciju. Prava određena tačkama A i B nije ispravno definisana ukoliko su tačke A i B identične u opštem slučaju. Presek dve prave nije moguć ukoliko su te dve prave paralelne u opštem slučaju. Ovo su primeri *deduktivnih* grešaka. Ovaj tip grešaka se ne može jednostavno detektovati od strane aplikacije. Identitet dve tačke u opštem slučaju ili paralelnost dve prave u opštem slučaju je poseban odnos između objekata koji su uvedeni komandama konstrukcije i predstavlja geometrijsko tvrđenje koje treba dokazati.

Ono što aplikacija može lako da detektuje, to su *semantičke* greške — nekonzistentost niza elementarnih konstrukcija u konkretnom slučaju (za razliku od opšteg). Aplikacija za vizuelizaciju geometrijskih konstrukcija svakoj tački konstrukcije dodeljuje realne dekartovske koordinate i nadalje je svaki objekat (prava, krug, kriva drugog reda, itd.) određen jednačinom sa konkretnim vrednostima. U opštem slučaju, koordinate tačaka bi bile promenljive, a ne realne vrednosti i parametri geometrijskih objekata bi bili u funkciji ovih promenljivih. Realne vrednosti koje su dodeljene objektima umesto promenljivih opisuju jedan konkretan primer geometrijske konstrukcije. U ovom konkretnom primeru aplikacija može detektovati poseban odnos između datih objekata — da li su dve tačke identične, da li su dve prave paralelne, da li su dve prave normalne, itd. Time se može detektovati nekonzistentnost niza geometrijskih konstrukcija u konkretnom slučaju. Ali identitet dve tačke u jednom, posebnom slučaju ne znači da su te dve tačke identične u svakom, odnosno opštem slučaju (dok obratno uvek važi). Prema tome, aplikacija za vizuelizaciju konstrukcija može u najboljem slučaju detektovati samo *moгуćnost* da je niz konstrukcija nekonzistentan, ali tako nešto ne može i potvrditi bez pomoći dokazivača. Dokazivač je neophodan zato što su iskazi poput onoga da su dve tačke identične ili da su dve prave paralelne upravo geometrijska tvrđenja pri zadatoj konstrukciji.

Prethodno razmatranje se može pretočiti u efikasan algoritam korišćenja geometrijskog dokazivača u cilju otkrivanja nekonzistente geometrijske konstrukcije:

1. Geometrijska konstrukcija se zadaje aplikaciji kao niz komandi od kojih svaka opisuje jednu elementarnu konstrukciju.
2. Aplikacija obrađuje jednu po jednu komandu, kreira geometrijske objekte i njihovim parametrima dodeljuje realne vrednosti.
3. Ukoliko nije moguće izračunati vrednosti parametra nekog objekta (ne može sa odrediti presek dve prave, ne može se konstruisati prava kroz dve zadate tačke, itd), aplikacija detektuje mogućnost nekonzistentnosti konstrukcije. Relacija između objekata koja sprečava da se pravilno obradi tekuća komanda se prosleđuje dokazivaču kao tvrđenje koje sledi iz prethodno zadatih komandi.
4. Ukoliko dokazivač potvrdi tvrđenje, korisnik se obaveštava o nevalidnosti konstrukcija u opštem slučaju. Ukoliko tvrđenje nije tačno, korisnik se

obaveštava da se konstrukcija može izvesti, ali ne sa trenutno zadatim vrednostima, odnosno konstrukcija nije validna u zadatom, posebnom slučaju (obično je dovoljno da se promene koordinate nekih od početnih tačaka). Ukoliko dokazivač ne uspe ni da dokaže niti da opovrgne tvrđenje, korisnik se obaveštava da konstrukcija nije validna u zadatom položaju i da možda nije validna u opštem slučaju.

GCLC ima ugrađenu podršku za automatsku verifikaciju regularnosti geometrijske konstrukcije ([35]) sa mogućnošću korišćenja proizvoljnog geometrijskog dokazivača. Sada ta podrška ima na raspolaganju tri različita geometrijska dokazivača koja su implementirana u sistemu GCLC.

7.2 Pravci daljeg razvoja

Tema obrađena u ovom radu nije zatvorenog tipa. Naprotiv, osim teorijskih i praktičnih primena koje pruža, automatsko dokazivanje geometrijskih teorema (algebarskim putem) se može dalje razvijati kako kao samostalan projekat, tako i kao deo drugih projekata.

7.2.1 Unapređivanje metoda

Samo iz nabrojanog iz čega se sastoji programski deo projekta, može se naslutiti kompleksnost teme automatskog dokazivanja geometrijskih teorema. Program koji je napisan se može dalje unapređivati poboljšanjem opcija koje trenutno podržava, kao i dodavanjem novih. Lista je dugačka, i na samom početku se nalaze sledeća unapređivanja:

- Poboljšanje Buhbergerove metode. Ova metoda trenutno postiže slabije rezultate od Vuove metode i to iznad očekivanja navedenih u drugim radovima koji su se bavili poređenjem dve metode. Jasno je da na ovom polju ima dosta prostora za napredak.
- Poboljšanje performansi dokazivača. Trenutne performanse su zadovoljavajuće, ali se mogu unaprediti na nekoliko načina, kao što su paralelizacija i optimizacija rada sa memorijom.
- Podrška svodivih sistema polinoma do kvadratnih stepena. Sa tom podrškom, dokazivač bi bio u stanju da dokaže najveći broj teorema planarne geometrije i bio bi u rangu sa najboljim postojećim dokazivačem (Čuov dokazivač).
- Prevođenje uslova nedegenerisanosti u geometrijsku formu.

7.2.2 Podrška za veći broj geometrijskih teorema

Dokazivanje geometrijske teoreme algebarskim metodama se sastoji od tri osnovna koraka:

1. Zadavanje teoreme;
2. Prevođenje teoreme u algebarsku formu;

3. Dokazivanje algebarske forme teoreme.

Osigurati podršku za veći broj geometrijskih teorema znači obezbediti takvu podršku u sva tri koraka. Trenutno nepodržane teoreme su, između ostalih, one koje uključuju krive drugog reda ili trisektrise ugla.

U ovom radu se, kada se govori o interfejsu za postavku geometrijskih teorema, uglavnom misli na sistem GCLC. U toj aplikaciji moguće je konstruisati proizvoljne krive drugog reda, ali one nisu podržane u smislu dokazivanja geometrijskih teorema zato što nedostaje podrška u drugom koraku — njihovom prevođenju u algebarsku formu. S druge strane, GCLC ne sadrži komande za izvođenje konstrukcije trisekcije ugla tako da podrška teorema koje traže takvu konstrukciju (npr. Morlijeva teorema) nije obezbeđena već u prvom koraku.

Rad na obezbeđivanju podrške za dokazivanje šireg opsega geometrijskih teorema se zato proteže na nekoliko nivoa, od kojih su neki (prvi korak) i izvan dokazivača.

7.2.3 Automatsko otkrivanje novih teorema

Dokazivači geometrijskih teorema se u najvećem broju slučajeva koriste da dokažu postojeće i do sada poznate teoreme. Sa istraživačke strane dobit je u tome što je dobijen još jedan dokaz date teoreme, produbljuje se razumevanje same teoreme i, naravno, razvija se oblast automatskog dokazivanja čiju važnost ne treba naglašavati.

Otkrivanje novih geometrijskih teorema je, s druge strane, zadatak koji jasno doprinosi samoj geometriji. Od nastanka geometrije, istraživači se bave otkrivanjem novih teorema i njihovim dokazivanjem. Pojava računara i programa za automatsko dokazivanje geometrijskih teorema pruža potrebne alate da se automatizuje i otkrivanje novih teorema.

Procedura kojom bi moglo da se automatski traga za novim teoremama bi u nagrubljem obliku izgledala ovako:

1. Traganje za novim teoremama počinje od zadate geometrijske konstrukcije. Konstrukcija se može zadati na više načina:
 - Konstrukcija se bira slučajno — polazi se od prazne konstrukcije na koju se dodaju nasumično izabrane elementarne konstrukcije;
 - Konstrukcija se ručno zadaje;
 - Konstrukcija se preuzima iz poznate teoreme;
 - ...
2. Početna konstrukcija se proširuje novim elementarnim konstrukcijama na način koji podseća na poznati algoritam teorije grafova *pretrage u širinu*. Trenutna konstrukcija se proširuje novom elementarnom konstrukcijom na sve moguće načine. Svaka nova dobijena konstrukcija se zatim na isti način obrađuje dodavanjem nove elementarne konstrukcije na sve moguće načine i tako dalje. Svaka konstrukcija dobijena na ovaj način se obrađuje narednim korakom.
3. Trenutna konstrukcija se oslobađa parametara — svakoj tački će biti dodeljene konkretne realne koordinate, svaka prava će imati izračunate parametre koji je određuju, itd. U ovu svrhu se koristi aplikacija za vizuelizaciju geometrijskih konstrukcija, na primer GCLC.

4. Za zadati posebni slučaj geometrijske konstrukcije (oslobađanjem od parametara je pređeno sa opšteg na posebni slučaj), proverava se da li postoji *posebna relacija* između dva ili više objekata, a koja nije posledica zadate konstrukcije. Neke od posebnih relacija su:
- Dve tačke su identične;
 - Dve prave su paralelne, normalne ili grade ugao od 30, 45, 60, 75 stepeni;
 - Četiri ili više tačaka pripadaju istom krugu;
 - Četiri tačke su harmonijski spregnute;
 - Tačka je središte duži ili odnos dve duži je ceo broj;
 - ...
5. Ukoliko je posebni slučaj detektovan, on se prosleđuje dokazivaču kao tvrđenje koje je posledica konstrukcije. Teorema je otkrivena ukoliko je ovakvo tvrđenje dokazano.

Od ove ideje do realizacije je dug put. Automatsko otkrivanje novih geometrijskih teorema metodom koja je opisana deluje efikasno i izvodljivo. Prva dva koraka, generisanje geometrijske konstrukcije, se računski mogu veoma brzo izvesti. Pretpostavka je da se na hiljade probnih konstrukcija može generisati u jednoj sekundi. U rezultatima implementiranih dokazivača je napisano da je prosečno vreme dokazivanja teoreme manje od 100 milisekundi. Kombinacijom ova dva vremena dolazi se do zaključka o efikasnosti metode otkrivanja novih teorema.

Poteškoće koje se očekuju tokom realizacije su brojne, pa se ne može sa sigurnošću predvideti uspešnost metode — jedini pokazatelj uspešnosti u ovom slučaju bi bio broj novo-otkrivenih interesantnih teorema primenom metode. Neki od problema koji se unapred mogu predvideti su:

- Optimalan način za generisanje početne konstrukcije. Optimalnost se meri *udaljenošću* početne konstrukcije od konstrukcija koje sadrže nove teoreme;
- Prepoznavanje posebnih odnosa između geometrijskih objekata uvedenih konstrukcijom koji su posledica same konstrukcije i ne predstavljaju novo geometrijsko tvrđenje;
- Iako je srednje vreme dokazivača na najvećem broju teorema veoma efikasno, na pojedinim slučajevima dokazivač može raditi veoma dugo, što je posledica eksponencijalne složenosti algebarskih metoda;
- Otkrivene teoreme je potrebno klasifikovati. Pretpostavka je da bi se u najvećem broju slučajeva radilo o trivijalnim tvrđenjima, poznatim tvrđenjima ili na neki drugi način neinteresantnim teoremama. Poseban problem je opisivanje interesantnih teorema.

Automatsko otkrivanje geometrijskih teorema je izazovan zadatak u svakom smislu — istraživačkom, programerskom i naučnom. Pored svega toga, sama oblast je atraktivna i zbog činjenice što bi uspešni rezultati imali veliku vrednost — svaka nova otkrivena teorema, do sada nepoznata i nigde klasifikovana, bi obogatila geometriju, a to je nagrada koju svaki geometričar priželjkuje.

7.2.4 Korišćenje lema pri dokazivanju

Jedan od rezultata ovoga rada je i prikupljanje korpusa geometrijskih teorema. Više od 100 teorema je sakupljeno (tekstovi i ilustracije teorema su navedeni u dodatku) i sve su dodate u repozitorijum GeoThms [5] koji je javno dostupan.

Baza geometrijskih teorema je vredna sama po sebi; može se koristiti u cilju učenja geometrije, klasifikacije i sistematizacije geometrijskih znanja, a u projektima razvoja novih sistema automatskih dokazivača i kao materijal za testiranje i upoređivanje programa. Još jedna od atraktivnih primena baze geometrijskih teorema na polju automatizacije geometrije je korišćenje lema pri izvođenju novih dokaza.

Geometrijsko tvrđenje se sastoji od geometrijske konstrukcije i tvrđenja koje se postavlja u odnosu na nju. Tvrđenje je dokazano ukoliko se pokaže da je posledica konstrukcije (koju u ovom slučaju zovemo hipoteza) i dodatnih uslova nedegenerisanosti koji određuju opšti položaj konstrukcije. Dodatni uslovi nedegenerisanosti se odnose samo na konstrukciju i ni na koji način ne zavise od samog tvrđenja. Posledica tvrđenja u odnosu na hipoteze konstrukcija i dodatne uslove nedegenerisanosti se može zapisati na sledeći način:

$$(h_1 \wedge h_2 \wedge \dots \wedge h_n \wedge ndg_1 \wedge \dots \wedge ndg_k) \Rightarrow g \quad (7.1)$$

gde su h_i pojedinačne elementarne konstrukcije, ndg_j uslovi nedegenerisanosti i g tvrđenje.

Dokazane teoreme koje se čuvaju u bazi teorema se mogu koristiti kao leme pri dokazivanju novih tvrđenja. Recimo da je u bazi teorema pronađena teorema čija konstrukcija je podskup konstrukcije novog tvrđenja (i da je novo tvrđenje iskazano formulom 7.1). Ova teorema bi tada imala oblik:

$$(h_{p_1} \wedge h_{p_2} \wedge \dots \wedge h_{p_m} \wedge ndg_1^{(1)} \wedge \dots \wedge ndg_r^{(1)}) \Rightarrow g_1$$

gde su h_{p_i} iz skupa $\{h_1, h_2, \dots, h_n\}$. Ono što je važno primetiti, a posledica je toga da uslovi nedegenerisanosti zavise samo od geometrijske konstrukcije, je da su uslovi nedegenerisanosti $ndg_j^{(1)}$ takođe iz skupa $\{ndg_1, ndg_2, \dots, ndg_k\}$. To je stoga što ako jedan uslov nedegenerisanosti važi za jednu geometrijsku konstrukciju, onda taj uslov mora važiti i za svaku nad-konstrukciju date konstrukcije.

Iz svega razmatranog, lako se pokazuje da ukoliko je sledeća implikacija tačna:

$$(h_1 \wedge h_2 \wedge \dots \wedge h_n \wedge ndg_1 \wedge \dots \wedge ndg_k \wedge g_1) \Rightarrow g$$

onda je tačna i implikacija 7.1. Odnosno, ukoliko je pokazano da je tvrđenje g posledica hipoteza konstrukcije, dodatnih uslova nedegenerisanosti i dodatne leme (koja je tačna za pod-konstrukciju date konstrukcije), onda je tvrđenje g takođe posledica osnovnih hipoteza konstrukcije i dodatnih uslova nedegenerisanosti. Time je pokazana korektnost korišćenja lema pri dokazivanju geometrijskih tvrđenja, sa akcentom na algebarski pristup dokazivanju geometrijskih tvrđenja.

Postoji nekoliko ideja na koji način bi se leme mogle iskoristiti u cilju ubrzanja izvođenja dokaza, ali nijedna od tih ideja nije još proverena u praksi:

- Iskoristiti lemu da se uproste hipoteze (tj. da se smanji stepen polinoma koji predstavlja hipotezu ukoliko je to moguće). Kod Vuove metode, uprošćavanje se pokušava pseudo deljenjem, kod Buhbergerove metode, uprošćavanje se pokušava B-svođenjem.
- Iskoristiti lemu da se uprosti tvrđenje.
- Dodati lemu u skup hipoteza.
- Zameniti jednu ili više hipoteza lemom (na način koji ne ugrožava korektnost dokaza).

Da bi se ideja o korišćenju lema mogla realizovati, potrebno je rešiti još jedan kompleksan problem — efikasno pronalaženje teoreme u bazi teorema čija konstrukcija je podskup konstrukcije zadatog tvrđenja. Otežavajući faktor je mogućnost postavke ekvivalentne geometrijske konstrukcije na više različitih načina. Da bi se dve konstrukcije uporedile, potrebno ih je nekako svesti na *kanonsku formu*, a idealno bi bilo definisati kanonsku formu koja bi imala svojstvo da je za svaku konstrukciju u kanonskoj formi, svaki njen podskup takođe u kanonskoj formi. Time bi se omogućila laka pretraga kroz bazu teorema.

Dodatak A

Kolekcija geometrijskih teorema

Svrha geometrijskog dokazivača je dokazivanje geometrijskih teorema, a moć geometrijskog dokazivača opisuje opseg i kompleksnost teorema koje može dokazati. U ovom dodatku je kroz veliki broj primera (preko 100 geometrijskih teorema) prikazana praktična vrednost implementiranih dokazivača.

A.1 Uvod

Teoreme navedene u ovom dodatku su izabrane iz opsega teorema koje može dokazati implementirani dokazivač. Taj opseg čine teoreme konstruktivnog tipa geometrije euklidske ravni koje se mogu iskazati jednakostima (najveći broj teorema pripada upravo toj klasi) i kod kojih dobijeni sistem polinoma koji čine hipoteze tvrđenja nije *svodiv*, ili je svodiv ali je tvrđenje tačno za svaku nesvodivu komponentu sistema. Da bismo izbegli formalnu definiciju pojmova svodivosti i nesvodivosti sistema polinoma, navedimo nekoliko primera koji ilustruju kada dolazi do svodivosti sistema.

Svodivost je posledica nejednoznačnosti geometrijske konstrukcije, na primer presek prave i kruga. U opštem slučaju, tim presekom su određene dve tačke, recimo tačka A sa koordinatama (x_1, x_2) i tačka B sa koordinatama (x_3, x_4) . Neka se dalje rešavanjem sistema polinomnih jednakosti dobijaju sledeća rešenja: $A = (p, q)$ i $B = (r, s)$. Međutim, zbog simetrije postoji još rešenja koja zadovoljavaju uslove preseka prave i kruga, ta rešenja su:

$$A = (p, q), B = (p, q)$$

$$A = (r, s), B = (p, q)$$

$$A = (r, s), B = (r, s)$$

Ukupno, postoji četiri rešenja po nepoznatama x_1, x_2, x_3 i x_4 za problem konstrukcije preseka prave i kruga. Svako od ovih četiri rešenja gradi jednu komponentu polaznog sistema polinoma koji je svodiv. Ukoliko tvrđenje nije tačno bar u jednoj od ovih komponenti, onda takvo tvrđenje nije dokazivo ovde implementiranim dokazivačem.


```

cmark_b A
cmark_b B
cmark_b C

point A_1 55 50
point A_2 45 43
line A_1A_2 A_1 A_2

line A_1B A_1 B
parallel AB_1 A A_1B
intersec B_1 A_1A_2 AB_1

line CB_1 C B_1
parallel BC_1 B CB_1
intersec C_1 A_1A_2 BC_1

cmark_lt A_1
cmark_lt B_1
cmark_lt C_1

drawline A C
drawline A_1 C_1

drawsegment A B_1
drawsegment B A_1
drawsegment B C_1
drawsegment C B_1

drawsegment A C_1
drawsegment C A_1

prove { parallel A_1 C A C_1 }

```

Tvrđenje teoreme ($A_1C \parallel AC_1$) je iskazano komandom *prove*.

GCLC aplikacija sadrži tri dokazivača geometrijskih teorema. Ukoliko bismo ovu teoremu dokazali dokazivačem koji je baziran na Vuovoj metodi, GCLC aplikacija bi proizvela sledeći izveštaj:

GCLC Prover Output for conjecture „Paposova teorema”

Construction and prover internal state

Construction commands:

```

POINT: A
POINT: B
ONLINE: C A B
POINT: A_1
POINT: A_2
LINE: A_1A_2 A_1 A_2

```

LINE: A_1B $A_1 B$
 PARALLEL: AB_1 $A A_1B$
 INTERSECTION OF LINES: $B_1 A_1A_2 AB_1$
 LINE: CB_1 $C B_1$
 PARALLEL: BC_1 $B CB_1$
 INTERSECTION OF LINES: $C_1 A_1A_2 BC_1$

Coordinates assigned to points:

$A = (0, 0)$
 $B = (u_1, 0)$
 $C = (u_7, 0)$
 $A_1 = (u_3, u_4)$
 $A_2 = (u_5, u_6)$
 $B_1 = (x_3, x_2)$
 $C_1 = (x_5, x_4)$

Conjecture(s):

1.
 - **GCLC code:**
 $\{ \textit{parallel } A_1 C A C_1 \}$
 - **Expression:**
 $A_1C \parallel AC_1$

Resolving constructed lines

$AB = (A, B)$, (line is horizontal), (generated by the prover)
 $A_1A_2 = (A_1, A_2)$
 $A_1B = (A_1, B)$
 $AB_1 = (A, B_1)$
 $CB_1 = (C, B_1)$
 $BC_1 = (B, C_1)$

Creating polynomials from hypotheses

- POINT: A
no condition
- POINT: B
no condition
- ONLINE: C A B
 - point C is on the line (A, B)
true by the construction
no condition
- POINT: A_1
no condition

- POINT: A_2
no condition
- LINE: $A_1A_2 A_1 A_2$
 - point A_1 is on the line (A_1, A_2)
no condition
 - point A_2 is on the line (A_1, A_2)
no condition
- LINE: $A_1B A_1 B$
 - point A_1 is on the line (A_1, B)
no condition
 - point B is on the line (A_1, B)
no condition
- PARALLEL: $AB_1 A A_1B$
 - line (A, B_1) parallel with line (A_1, B)

$$p_1 = -u_4x_3 + (u_3 - u_1)x_2$$

- INTERSECTION OF LINES: $B_1 A_1A_2 AB_1$
 - point B_1 is on the line (A_1, A_2)

$$p_2 = (-u_6 + u_4)x_3 + (u_5 - u_3)x_2 + (u_6u_3 - u_5u_4)$$

- point B_1 is on the line (A, B_1)
no condition
- LINE: $CB_1 C B_1$
 - point C is on the line (C, B_1)
no condition
 - point B_1 is on the line (C, B_1)
no condition

- PARALLEL: $BC_1 B CB_1$
 - line (B, C_1) parallel with line (C, B_1)

$$p_3 = x_5x_2 - x_4x_3 + u_7x_4 - u_1x_2$$

- INTERSECTION OF LINES: $C_1 A_1A_2 BC_1$
 - point C_1 is on the line (A_1, A_2)

$$p_4 = (-u_6 + u_4)x_5 + (u_5 - u_3)x_4 + (u_6u_3 - u_5u_4)$$

- point C_1 is on the line (B, C_1)
no condition

Creating polynomial from the conjecture

line (A_1, C) parallel with line (A, C_1)

$$p_5 = u_4x_5 + (u_7 - u_3)x_4$$

Conjecture 1 :

$$p_6 = u_4x_5 + (u_7 - u_3)x_4$$

Invoking the theorem prover

The used proving method is Wu's method.

The input system is:

$$\begin{aligned} p_0 &= -u_4x_3 + (u_3 - u_1)x_2 \\ p_1 &= (-u_6 + u_4)x_3 + (u_5 - u_3)x_2 + (u_6u_3 - u_5u_4) \\ p_2 &= x_5x_2 - x_4x_3 + u_7x_4 - u_1x_2 \\ p_3 &= (-u_6 + u_4)x_5 + (u_5 - u_3)x_4 + (u_6u_3 - u_5u_4) \end{aligned}$$

Triangulation, step 1

Choosing variable: Trying the variable with index 5.

Variable x_5 selected: The number of polynomials with this variable is 2.

Minimal degrees: 3 polynomials with degree 1 and 2 polynomials with degree 1.

Polynomial with linear degree: Removing variable x_5 from all other polynomials by reducing them with polynomial p_3 .

Finished a triangulation step, the current system is:

$$\begin{aligned} p_0 &= -u_4x_3 + (u_3 - u_1)x_2 \\ p_1 &= (-u_6 + u_4)x_3 + (u_5 - u_3)x_2 + (u_6u_3 - u_5u_4) \\ p_2 &= (u_6 - u_4)x_4x_3 + (-u_5 + u_3)x_4x_2 + (-u_7u_6 + u_7u_4)x_4 + \\ &\quad (-u_6u_3 + u_6u_1 + u_5u_4 - u_4u_1)x_2 \\ p_3 &= (-u_6 + u_4)x_5 + (u_5 - u_3)x_4 + (u_6u_3 - u_5u_4) \end{aligned}$$

Triangulation, step 2

Choosing variable: Trying the variable with index 4.

Variable x_4 selected: The number of polynomials with this variable is 1.

Single polynomial with chosen variable: No reduction needed.

The triangular system has not been changed.

Triangulation, step 3

Choosing variable: Trying the variable with index 3.

Variable x_3 selected: The number of polynomials with this variable is 2.

Minimal degrees: 1 polynomials with degree 1 and 0 polynomials with degree 1.

Polynomial with linear degree: Removing variable x_3 from all other polynomials by reducing them with polynomial p_1 .

Finished a triangulation step, the current system is:

$$\begin{aligned}
 p_0 &= (-u_6u_3 + u_6u_1 + u_5u_4 - u_4u_1)x_2 + (u_6u_4u_3 - u_5u_4^2) \\
 p_1 &= (-u_6 + u_4)x_3 + (u_5 - u_3)x_2 + (u_6u_3 - u_5u_4) \\
 p_2 &= (u_6 - u_4)x_4x_3 + (-u_5 + u_3)x_4x_2 + (-u_7u_6 + u_7u_4)x_4 + \\
 &\quad (-u_6u_3 + u_6u_1 + u_5u_4 - u_4u_1)x_2 \\
 p_3 &= (-u_6 + u_4)x_5 + (u_5 - u_3)x_4 + (u_6u_3 - u_5u_4)
 \end{aligned}$$

Triangulation, step 4

Choosing variable: Trying the variable with index 2.

Variable x_2 selected: The number of polynomials with this variable is 1.

Single polynomial with chosen variable: No reduction needed.

The triangular system has not been changed.

The triangular system is:

$$\begin{aligned}
 p_0 &= (-u_6u_3 + u_6u_1 + u_5u_4 - u_4u_1)x_2 + (u_6u_4u_3 - u_5u_4^2) \\
 p_1 &= (-u_6 + u_4)x_3 + (u_5 - u_3)x_2 + (u_6u_3 - u_5u_4) \\
 p_2 &= (u_6 - u_4)x_4x_3 + (-u_5 + u_3)x_4x_2 + (-u_7u_6 + u_7u_4)x_4 + \\
 &\quad (-u_6u_3 + u_6u_1 + u_5u_4 - u_4u_1)x_2 \\
 p_3 &= (-u_6 + u_4)x_5 + (u_5 - u_3)x_4 + (u_6u_3 - u_5u_4)
 \end{aligned}$$

Final remainder

Calculating final remainder of the conclusion:

$$g = u_4x_5 + (u_7 - u_3)x_4$$

with respect to the triangular system.

1. Pseudo remainder with p_3 over variable x_5 :

$$g = (-u_7u_6 + u_7u_4 + u_6u_3 - u_5u_4)x_4 + (-u_6u_4u_3 + u_5u_4^2)$$

2. Pseudo remainder with p_2 over variable x_4 :

$$g = (-u_6^2 u_4 u_3 + u_6 u_5 u_4^2 + u_6 u_4^2 u_3 - u_5 u_4^3) x_3 + \\ (-u_7 u_6^2 u_3 + u_7 u_6^2 u_1 + u_7 u_6 u_5 u_4 + u_7 u_6 u_4 u_3 - 2u_7 u_6 u_4 u_1 - \\ u_7 u_5 u_4^2 + u_7 u_4^2 u_1 + u_6^2 u_3^2 - u_6^2 u_3 u_1 - u_6 u_5 u_4 u_3 + u_6 u_5 u_4 u_1 - \\ u_6 u_4 u_3^2 + u_6 u_4 u_3 u_1 + u_5 u_4^2 u_3 - u_5 u_4^2 u_1) x_2 + \\ (u_7 u_6^2 u_4 u_3 - u_7 u_6 u_5 u_4^2 - u_7 u_6 u_4^2 u_3 + u_7 u_5 u_4^3)$$

3. Pseudo remainder with p_1 over variable x_3 :

$$g = (u_7 u_6^3 u_3 - u_7 u_6^3 u_1 - u_7 u_6^2 u_5 u_4 - 2u_7 u_6^2 u_4 u_3 + 3u_7 u_6^2 u_4 u_1 + \\ 2u_7 u_6 u_5 u_4^2 + u_7 u_6 u_4^2 u_3 - 3u_7 u_6 u_4^2 u_1 - u_7 u_5 u_4^3 + u_7 u_4^3 u_1 - \\ u_6^3 u_3^2 + u_6^3 u_3 u_1 + 2u_6^2 u_5 u_4 u_3 - u_6^2 u_5 u_4 u_1 + u_6^2 u_4 u_3^2 - \\ 2u_6^2 u_4 u_3 u_1 - u_6 u_5^2 u_4^2 - 2u_6 u_5 u_4^2 u_3 + 2u_6 u_5 u_4^2 u_1 + \\ u_6 u_4^2 u_3 u_1 + u_5^2 u_4^3 - u_5 u_4^3 u_1) x_2 + \\ (-u_7 u_6^3 u_4 u_3 + u_7 u_6^2 u_5 u_4^2 + 2u_7 u_6^2 u_4^2 u_3 - 2u_7 u_6 u_5 u_4^3 - \\ u_7 u_6 u_4^3 u_3 + u_7 u_5 u_4^4 + u_6^3 u_4 u_3^2 - 2u_6^2 u_5 u_4^2 u_3 - \\ u_6^2 u_4^2 u_3^2 + u_6 u_5^2 u_4^3 + 2u_6 u_5 u_4^3 u_3 - u_5^2 u_4^4)$$

4. Pseudo remainder with p_0 over variable x_2 :

$$g = 0$$

Prover report

Status: The conjecture has been proved.

There are no ndg conditions.

Space Complexity: The biggest polynomial obtained during proof process contained 34 terms.

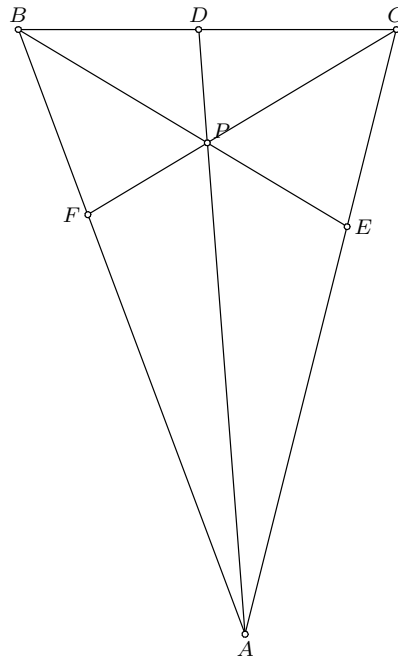
Time Complexity: Time spent by the prover is 0.006 seconds.

A.3 Teoreme

Ovo poglavlje je potpuno automatski generisano polazeći od direktorijuma sa kolekcijom GCLC datoteka u kojima su teoreme navedene. Sve teoreme su zadate svojim tekstom, ilustracijom, napomenom ukoliko postoji i kratkim izveštajem o dokazu teoreme.

Izveštaj se sastoji od koordinata koje su dodeljene tačkama iz konstrukcije od strane dokazivača i statusa dokaza za oba dokazivača (dokazivač Vuovom metodom i dokazivač Buhbergerovom metodom).

Status može biti da je teorema dokazana i u tom slučaju je navedeno vreme izvršavanja i kompleksnost dokaza (kompleksnost je određena maksimalnim brojem termova nekog polinoma dobijenog tokom dokaza). Ukoliko teorema nije



Slika A.2: Čevina teorema

dokazana, navodi se razlog zbog koga dokazivanje nije uspelo (razlog može biti da metoda nije u stanju da dokaže tvrđenje ili da je dokazivanje probilo vremenski limit).

Sve teoreme su dokazane Vuvom metodom, dok je Buhbergerovom metodom dokazano više od polovine teorema iz kolekcije. Najveći broj teorema je preuzet iz knjige [1]. Navedena vremena izvršavanja su dobijena na računaru sledeće konfiguracije: procesor AMD Sempron 2500+ 1.81GH, 1GB RAM memorije, 32-bitni operativni sistem Microsoft Windows Vista.

Primer 20 Čevina teorema (slika A.2). Dat je trougao ABC i tačka P unutar njega. Neka su D , E i F redom preseči pravih PA , PB i PC sa stranicama trougla BC , CA i AB . Dokazati da je $\frac{AF}{FB} \cdot \frac{BD}{DC} \cdot \frac{CE}{EA} = 1$.

$A = (0, 0)$, $B = (u_1, 0)$, $C = (u_2, u_3)$, $P = (u_4, u_5)$, $D = (x_2, x_1)$, $E = (x_4, x_3)$, $F = (x_6, 0)$.

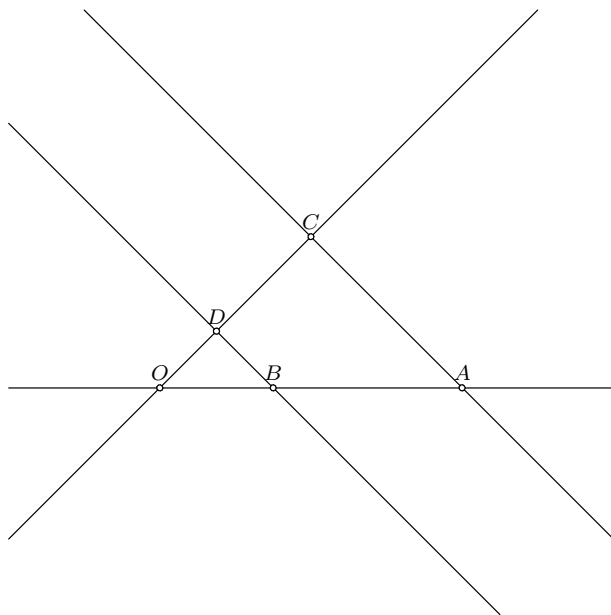
Teorema je dokazana metodom Wu-a.

Kompleksnost: 0.007s, 13 terma.

Teorema je dokazana metodom Groebner-a.

Kompleksnost: 0.014s, 45 terma.

Primer 21 Talesova teorema (slika A.3). Na pravoj p date su tri tačke O , A i B . Neka je C tačka van prave p i neka je D presečna tačka prave OC i prave koja sadrži D a paralelna je sa AC . Dokazati da je odnos duži OA i OB jednak odnosu duži OC i OD , odnosno da je $\frac{OA}{OB} = \frac{OC}{OD}$



Slika A.3: Talesova teorema

$O = (0, 0)$, $A = (u_1, 0)$, $C = (u_2, u_3)$, $B = (u_5, 0)$, $D = (x_3, x_2)$.

Teorema je dokazana metodom Wu-a.

Kompleksnost: 0.002s, 4 terma.

Teorema je dokazana metodom Groebner-a.

Kompleksnost: 0.002s, 4 terma.

Primer 22 *Harmonične tačke 2 (slika A.4). Dat je četvorougao ABCD. Neka je K presek pravih AD i BC, L presek pravih AB i CD, F presek pravih KL i FD i G presek pravih KL i AC. Dokazati da je četvorka LFKG harmonijski spregnuta, odnosno da je $\frac{LK}{KF} = \frac{GL}{GF}$.*

Isti primer je ponovljen sa drugačijom konfiguracijom. Obratiti pažnju na sliku, odabir koordinata i kompleksnost dokaza.

$A = (0, 0)$, $B = (u_1, 0)$, $C = (u_2, u_3)$, $D = (u_4, u_5)$, $L = (x_2, 0)$, $K = (x_4, x_3)$, $F = (x_6, x_5)$, $G = (x_8, x_7)$.

Teorema je dokazana metodom Wu-a.

Kompleksnost: 0.008s, 7 terma.

Teorema nije dokazana metodom Groebner-a.

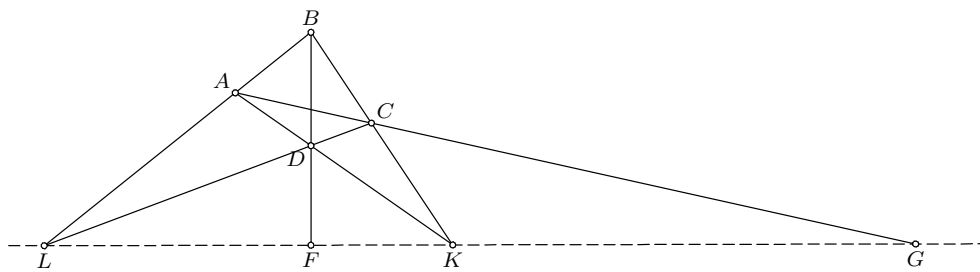
Izvršavanje prekinuto posle 21.612s.

Primer 23 *Dezargova teorema (slika A.5). Ako se prave A_1B_1 , A_2B_2 i A_3B_3 seku u jednoj tački, tada su preseki pravih $A_1A_2 \cap B_1B_2$, $A_1A_3 \cap B_1B_3$ i $A_2A_3 \cap B_2B_3$ tri kolinearne tačke.*

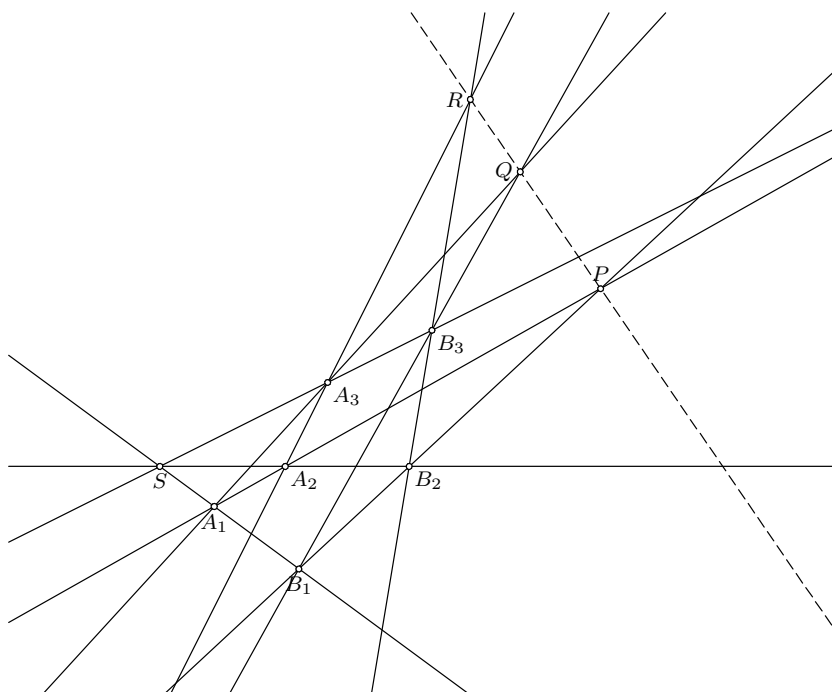
$S = (0, 0)$, $A_2 = (u_1, 0)$, $B_2 = (u_9, 0)$, $A_1 = (u_3, u_4)$, $B_1 = (x_2, u_5)$, $A_3 = (u_6, u_7)$, $B_3 = (x_3, u_8)$, $P = (x_5, x_4)$, $Q = (x_7, x_6)$, $R = (x_9, x_8)$.

Teorema je dokazana metodom Wu-a.

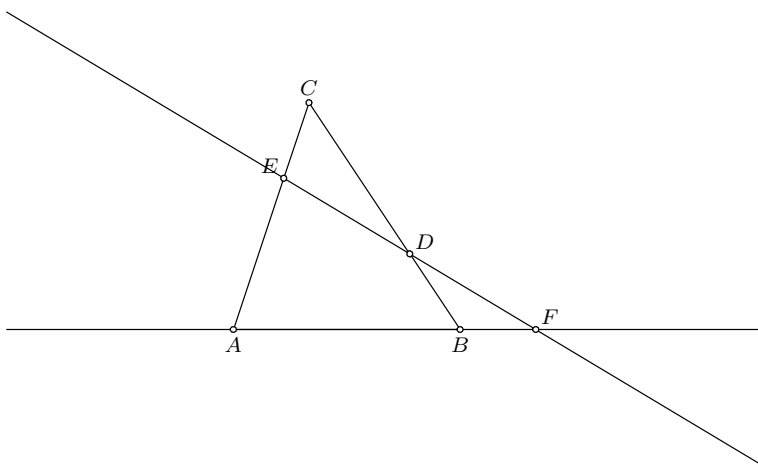
Kompleksnost: 0.184s, 402 terma.



Slika A.4: Harmonične tačke 2



Slika A.5: Desargova teorema



Slika A.6: Menelajeva teorema

Teorema je dokazana metodom Groebner-a.

Kompleksnost: 0.293s, 544 terma.

Primer 24 Menelajeva teorema (slika A.6). Dat je trougao ABC . Neka su D i E proizvoljne tačke na pravama BC i AC redom. Neka je F presek prave DE sa pravom AB . Dokazati da je $\frac{AF}{FB} \cdot \frac{BD}{DC} \cdot \frac{CE}{EA} = -1$. $\frac{AF}{FB} \cdot \frac{BD}{DC} \cdot \frac{CE}{EA} = -1$.

$A = (0, 0)$, $B = (u_1, 0)$, $C = (u_2, u_3)$, $D = (x_1, u_4)$, $E = (x_2, u_5)$, $F = (x_4, 0)$.

Teorema je dokazana metodom Wu-a.

Kompleksnost: 0.003s, 8 terma.

Teorema je dokazana metodom Groebner-a.

Kompleksnost: 0.003s, 8 terma.

Primer 25 Uopštena Menelajeva teorema (slika A.7). Dati su četvorougao $ABCD$, tačka A_1 na pravoj AB i tačka B_1 na pravoj BC . Neka su C_1 i D_1 preseki prave A_1B_1 sa pravama CD i AD redom. Dokazati da je $\frac{AA_1}{A_1B} \cdot \frac{BB_1}{B_1C} \cdot \frac{CC_1}{C_1D} \cdot \frac{DD_1}{D_1A} = 1$

$A = (0, 0)$, $B = (u_1, 0)$, $C = (u_2, u_3)$, $D = (u_4, u_5)$, $A_1 = (u_8, 0)$, $B_1 = (x_2, u_7)$, $C_1 = (x_4, x_3)$, $D_1 = (x_6, x_5)$.

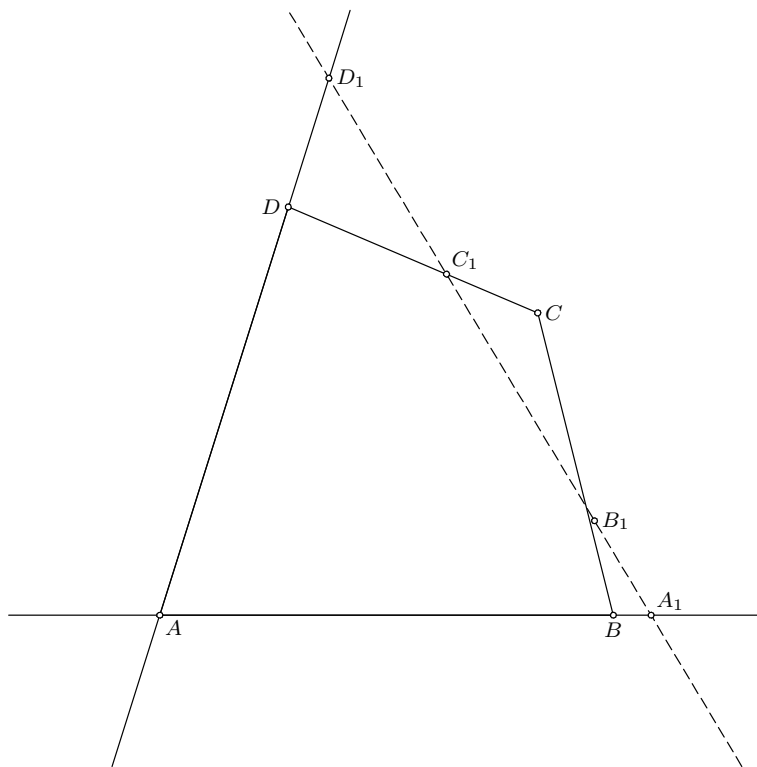
Teorema je dokazana metodom Wu-a.

Kompleksnost: 0.011s, 30 terma.

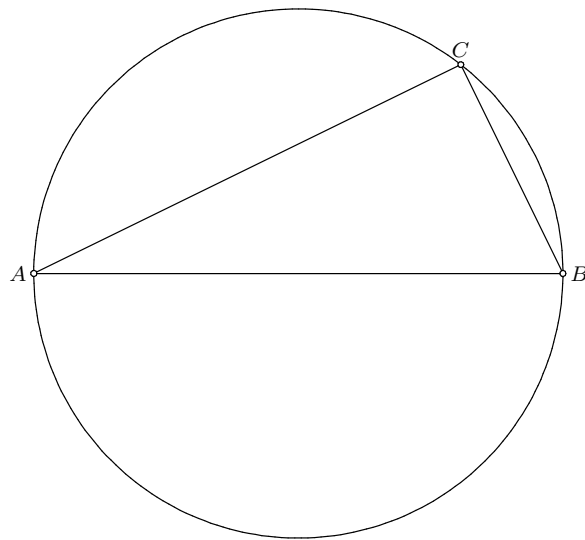
Teorema je dokazana metodom Groebner-a.

Kompleksnost: 0.027s, 48 terma.

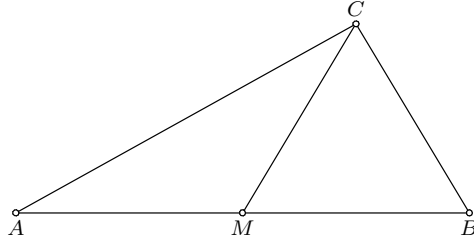
Primer 26 Konstrukcija pravog ugla (slika A.8). Dokazati da je ugao nad prečnikom prav



Slika A.7: Uopštena Menelajeva teorema



Slika A.8: Konstrukcija pravog ugla



Slika A.9: Površina trougla

$$A = (0, 0), B = (u_1, 0), O = (x_2, 0), C = (x_3, u_2).$$

Teorema je dokazana metodom Wu-a.

Kompleksnost: 0.002s, 3 terma.

Teorema je dokazana metodom Groebner-a.

Kompleksnost: 0.001s, 3 terma.

Primer 27 *Površina trougla (slika A.9). Dat je trougao ABC. Neka je M središte stranice AB. Dokazati da trouglovi AMC i MBC imaju jednaku površinu.*

$$A = (0, 0), B = (u_1, 0), C = (u_2, u_3), M = (x_2, 0).$$

Teorema je dokazana metodom Wu-a.

Kompleksnost: 0.001s, 2 terma.

Teorema je dokazana metodom Groebner-a.

Kompleksnost: 0.001s, 2 terma.

Primer 28 *Visine trougla (slika A.10). Dokazati da se visine trougla seku u jednoj tački.*

$$A = (0, 0), B = (u_1, 0), C = (u_2, u_3), A_1 = (x_2, x_1), B_1 = (x_4, x_3), C_1 = (u_2, 0), H = (x_8, x_7).$$

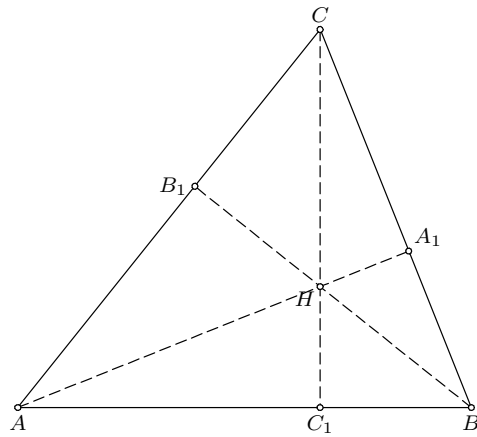
Teorema je dokazana metodom Wu-a.

Kompleksnost: 0.004s, 6 terma.

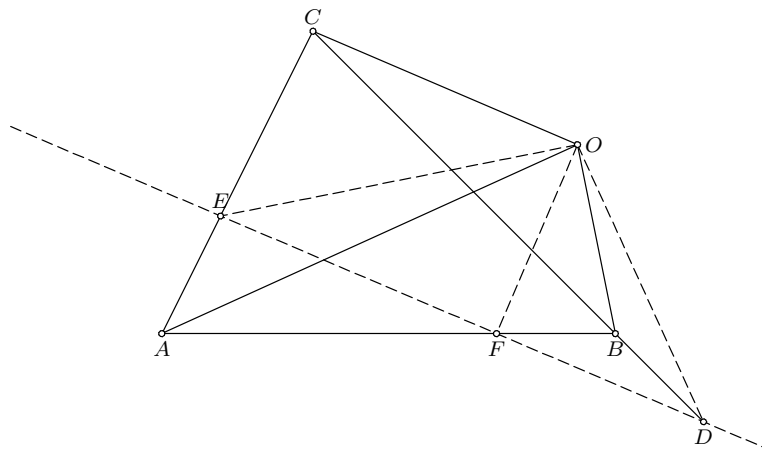
Teorema je dokazana metodom Groebner-a.

Kompleksnost: 0.036s, 30 terma.

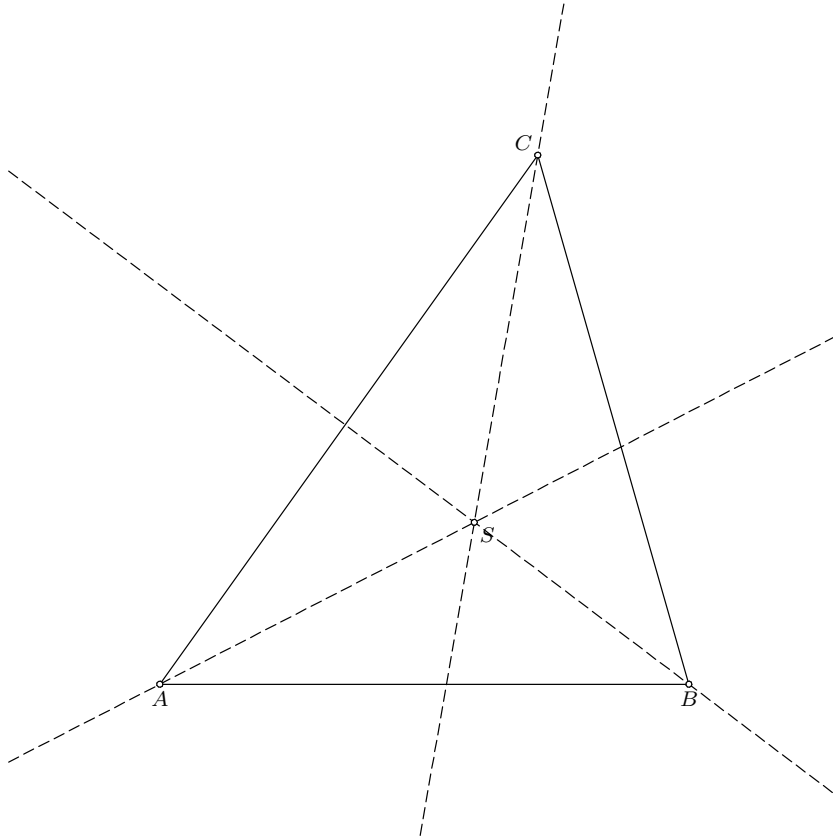
Primer 29 *Dualna teorema visinama trougla (slika A.11). Dat je trougao ABC i tačka O u istoj ravni. Neka su p, q i r prave koje prolaze kroz O i normalne su sa pravama OA, OB i OC redom. Neka su D, E i F presečne tačke pravih p, q i r sa pravama BC, AC i BC redom. Dokazati da su D, E i F kolinearne.*



Slika A.10: Visine trougla



Slika A.11: Dualna teorema visinama trougla



Slika A.12: Upisani krug trougla

$A = (0, 0)$, $B = (u_1, 0)$, $C = (u_2, u_3)$, $O = (u_4, u_5)$, $D = (x_2, x_1)$, $E = (x_4, x_3)$, $F = (x_6, 0)$.

Teorema je dokazana metodom Wu-a.

Kompleksnost: 0.009s, 27 terma.

Teorema je dokazana metodom Groebner-a.

Kompleksnost: 0.021s, 86 terma.

Primer 30 *Upisani krug trougla (slika A.12). U svaki trougao se može upisati krug.*

$A = (0, 0)$, $B = (u_1, 0)$, $C = (u_2, u_3)$, $S = (x_2, x_1)$.

Teorema je dokazana metodom Wu-a.

Kompleksnost: 0.009s, 23 terma.

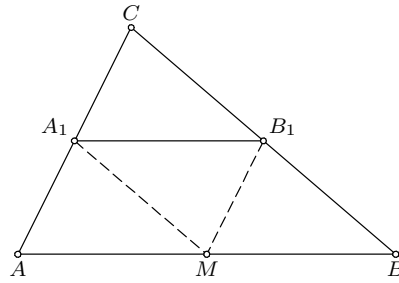
Teorema je dokazana metodom Groebner-a.

Kompleksnost: 0.035s, 31 terma.

Primer 31 *Središnja duž trougla (slika A.13). Dokazati da je središnja duž trougla paralelna odgovarajućoj stranici.*

$A = (0, 0)$, $B = (u_1, 0)$, $C = (u_2, u_3)$, $B_1 = (x_2, x_1)$, $A_1 = (x_4, x_3)$.

Teorema je dokazana metodom Wu-a.



Slika A.13: Središnja duž trougla

Kompleksnost: 0.004s, 8 terma.

Teorema je dokazana metodom Groebner-a.

Kompleksnost: 0.004s, 8 terma.

Primer 32 Paralelogram teorema (slika A.14). U ravni je dat trougao ABC . Neka je prava p paralela na BC iz tačke A i neka je prava q paralela na AB iz tačke C . Neka je D presek pravih p i q . Dokazati da je $\overline{AB} = \overline{DC}$.

$A = (0, 0)$, $B = (u_1, 0)$, $C = (u_2, u_3)$, $D = (x_2, x_1)$.

Teorema je dokazana metodom Wu-a.

Kompleksnost: 0.002s, 4 terma.

Teorema je dokazana metodom Groebner-a.

Kompleksnost: 0.002s, 4 terma.

Primer 33 Paralelogram teorema 2 (slika A.15). U ravni je dat trougao ABC . Neka je prava p paralela na BC iz tačke A i neka je prava q paralela na AVB iz tačke C . Neka je D presek pravih p i q i neka je E presek pravih AC i BCD . Dokazati da je $\overline{AE} = \overline{EC}$.

$A = (0, 0)$, $B = (u_1, 0)$, $C = (u_2, u_3)$, $D = (x_2, u_3)$, $E = (x_4, x_3)$.

Teorema je dokazana metodom Wu-a.

Kompleksnost: 0.004s, 6 terma.

Teorema je dokazana metodom Groebner-a.

Kompleksnost: 0.005s, 6 terma.

Primer 34 Opisani krug trougla (slika A.16). Dokazati da se simetrale stranica trougla seku u jednoj tački.

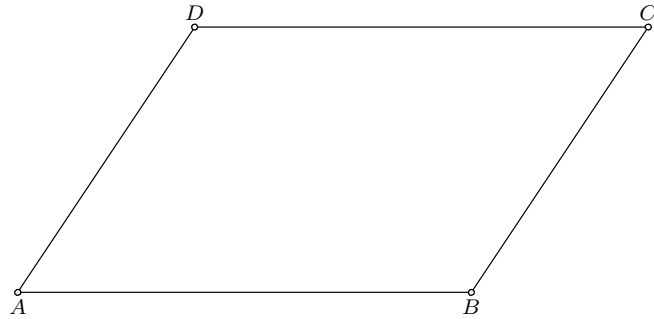
$A = (0, 0)$, $B = (u_1, 0)$, $C = (u_2, u_3)$, $O = (x_2, x_1)$, $M = (x_4, 0)$.

Teorema je dokazana metodom Wu-a.

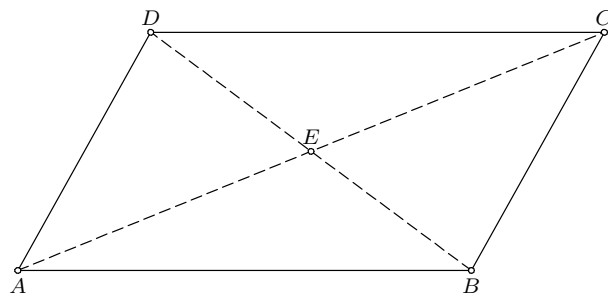
Kompleksnost: 0.003s, 6 terma.

Teorema je dokazana metodom Groebner-a.

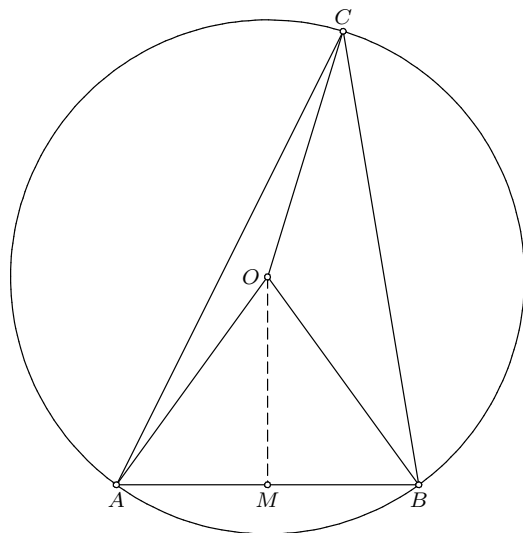
Kompleksnost: 0.003s, 6 terma.



Slika A.14: Paralelogram teorema



Slika A.15: Paralelogram teorema 2



Slika A.16: Opisani krug trougla

Primer 35 Paposova teorema (slika A.17). Data je prava p sa tačkama A , B i C , i tačke A_1 i A_2 van prave p . Neka je B_1 presek prave A_1A_2 sa pravom koja sadrži A i paralelna je sa A_1B . Neka je C_1 presek prave A_1A_2 sa pravom koja sadrži B i paralelna je sa CB_1 . Dokazati da je AC_1 paralelna sa CA_1 .

$$A = (0, 0), B = (u_1, 0), C = (u_7, 0), A_1 = (u_3, u_4), A_2 = (u_5, u_6), B_1 = (x_3, x_2), C_1 = (x_5, x_4).$$

Teorema je dokazana metodom Wu-a.

Kompleksnost: 0.010s, 34 terma.

Teorema je dokazana metodom Groebner-a.

Kompleksnost: 12.526s, 4172 terma.

Primer 36 Paposova teorema (druga verzija) (slika A.18). Neka su ABC i $A_1B_1C_1$ dve prave i neka je $P = AB_1 \cap A_1B$, $Q = AC_1 \cap A_1C$ i $S = BC_1 \cap B_1C$. Dokazati da su P , Q i S kolinearne.

$$A = (0, 0), B = (u_1, 0), C = (u_8, 0), A_1 = (u_3, u_4), B_1 = (u_5, u_6), C_1 = (x_2, u_7), P = (x_4, x_3), Q = (x_6, x_5), S = (x_8, x_7).$$

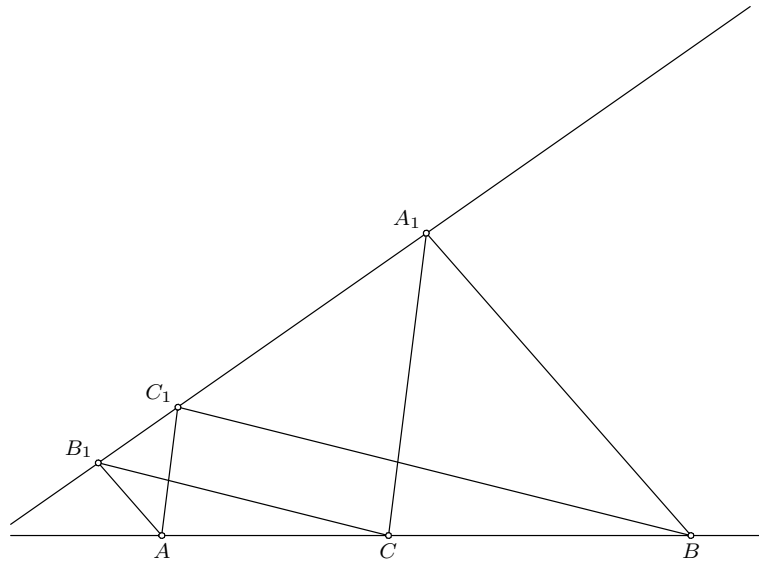
Teorema je dokazana metodom Wu-a.

Kompleksnost: 0.018s, 28 terma.

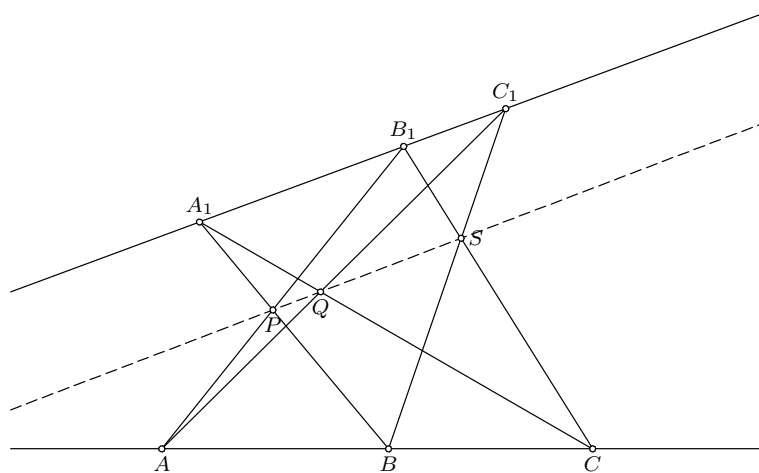
Teorema je dokazana metodom Groebner-a.

Kompleksnost: 0.774s, 899 terma.

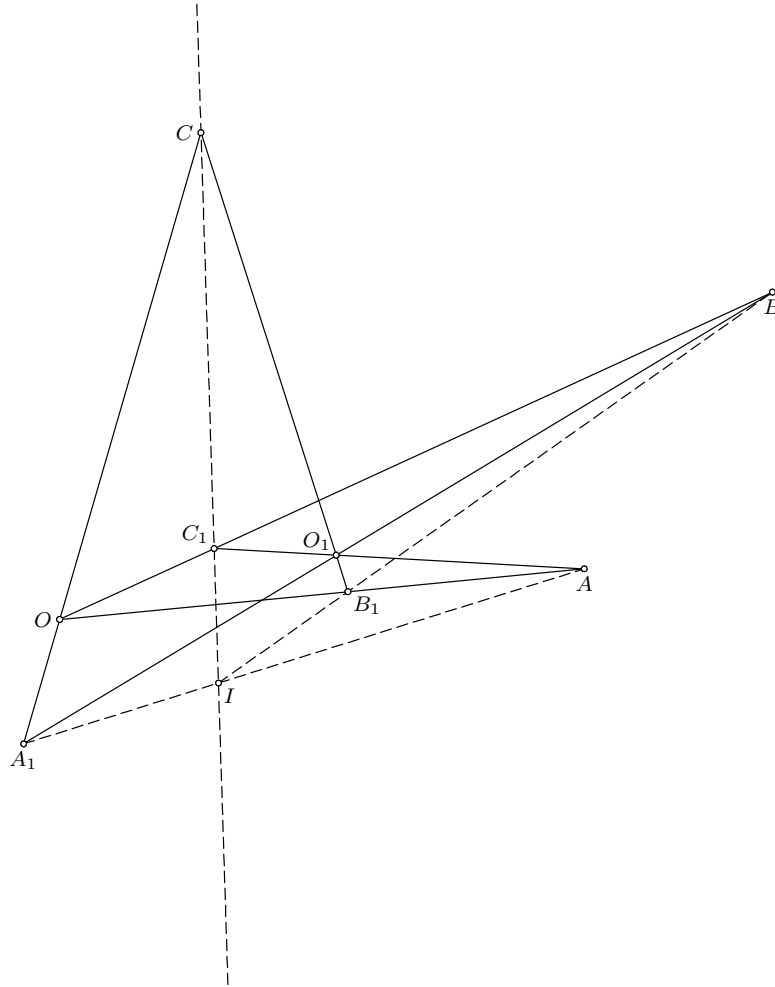
Primer 37 Dualna Paposova teorema (slika A.19). U ravni su date tačke O , A , B , C i O_1 . Tačke A_1 , B_1 , C_1 i I su konstruisane kao preseoci parova pravih:



Slika A.17: Paposova teorema



Slika A.18: Paposova teorema (druga verzija)



Slika A.19: Dualna Paposova teorema

O_1B i OC , OA i O_1C , OB i O_1A , BB_1 i AA_1 . Dokazati da su tačke C , C_1 i I kolinearne.

$O = (0, 0)$, $A = (u_1, 0)$, $B = (u_2, u_3)$, $C = (u_4, u_5)$, $O_1 = (u_6, u_7)$, $A_1 = (x_2, x_1)$, $B_1 = (x_4, 0)$, $C_1 = (x_6, x_5)$, $I = (x_8, x_7)$.

Teorema je dokazana metodom Wu-a.

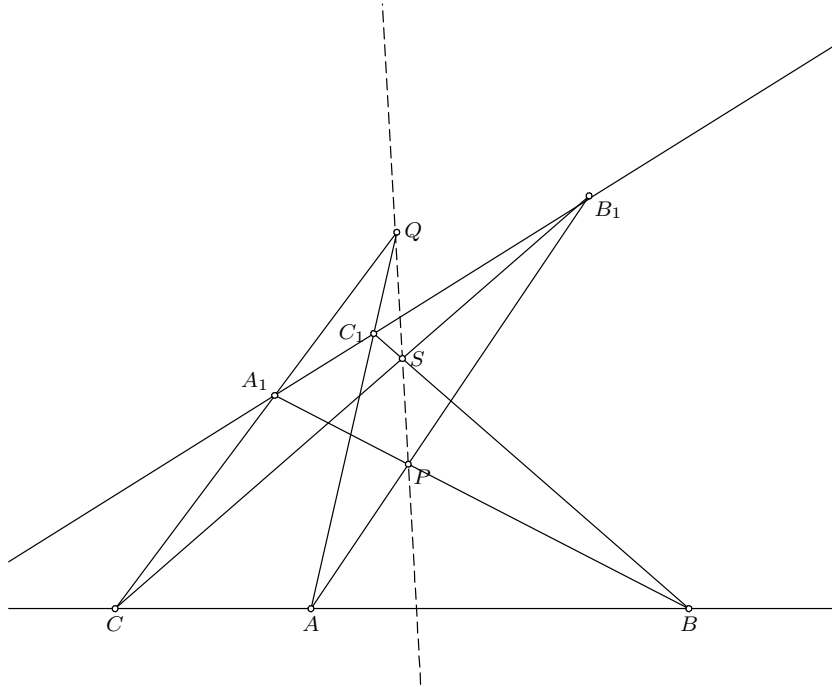
Kompleksnost: 0.020s, 36 terma.

Teorema nije dokazana metodom Groebner-a.

Izvršavanje prekinuto posle 23.097s.

Primer 38 Paposov heksagon (slika A.20). Na pravoj p su date tačke A , B i C , dok su na pravoj q date tačke A_1 , B_1 i C_1 . Neka je $P = AB_1 \cap A_1B$, $Q = AC_1 \cap A_1C$ i $R = BC_1 \cap B_1C$. Dokazati da su tačke P , Q i R kolinearne.

Ova teorema je posledica Paskalove teoreme za krive drugog reda. Dve prave su specijalan slučaj krive drugog reda.



Slika A.20: Paposov heksagon

$A = (0, 0)$, $B = (u_1, 0)$, $C = (u_8, 0)$, $A_1 = (u_3, u_4)$, $B_1 = (u_5, u_6)$, $C_1 = (x_2, u_7)$, $P = (x_4, x_3)$, $Q = (x_6, x_5)$, $S = (x_8, x_7)$.

Teorema je dokazana metodom Wu-a.

Kompleksnost: 0.018s, 28 terma.

Teorema je dokazana metodom Groebner-a.

Kompleksnost: 0.822s, 899 terma.

Primer 39 *Tri kvadrata (slika A.21). Data su tri kvadrata: ABB_1A_1 , BCC_1B_1 i CDD_1C_1 . Dokazati da je $\angle D_1AD + \angle D_1BD = \angle D_1CD$.*

$A = (0, 0)$, $B = (u_1, 0)$, $C = (x_2, 0)$, $D = (x_4, 0)$, $A_1 = (0, x_5)$, $A_2 = (0, x_7)$, $D_1 = (x_4, x_5)$.

Teorema je dokazana metodom Wu-a.

Kompleksnost: 0.016s, 40 terma.

Teorema je dokazana metodom Groebner-a.

Kompleksnost: 0.036s, 40 terma.

Primer 40 *Gergonova tačka (slika A.22). Upisani krug trougla ABC dodiruje stranice trougla BC , CA i AB redom u tačkama D , E i F . Dokazati da su prave AD , BE i CF konkurentne.*

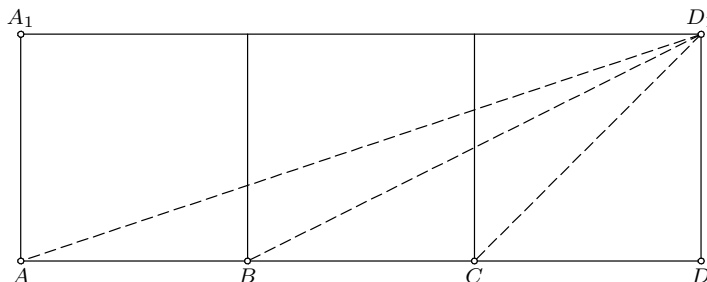
$A = (0, 0)$, $B = (u_1, 0)$, $C = (u_2, u_3)$, $I = (x_2, x_1)$, $D = (x_4, x_3)$, $E = (x_6, x_5)$, $F = (x_2, 0)$, $G = (x_{10}, x_9)$.

Teorema je dokazana metodom Wu-a.

Kompleksnost: 0.053s, 97 terma.

Teorema nije dokazana metodom Groebner-a.

Izvršavanje prekinuto posle 21.056s.



Slika A.21: Tri kvadrata

Primer 41 Adamsov krug (slika A.23). Upisani krug trougla ABC , sa centrom I , dodiruje stranice trougla BC , CA i AB redom u tačkama D , E i F . Prave AD , BE i CF konkurentne i seku se u Gergonovoj tački. Iz Gergonove tačke su povučene paralele sa stranicama trougla DEF koje seku stranice trougla ABC u tačkama P , Q , R , S , T i U . Dokazati da se ovih šest tačaka nalazi na krugu sa centrom I .

Zbog simetrije problema, dovoljno je pokazati za tačke S , T i Q da se nalaze na krugu sa centrom I .

$A = (0, 0)$, $B = (u_1, 0)$, $C = (u_2, u_3)$, $I = (x_2, x_1)$, $D = (x_4, x_3)$, $E = (x_6, x_5)$, $F = (x_2, 0)$, $G = (x_{10}, x_9)$, $Q = (x_{12}, x_{11})$, $S = (x_{14}, 0)$, $T = (x_{16}, 0)$.

Teorema je dokazana metodom Wu-a.

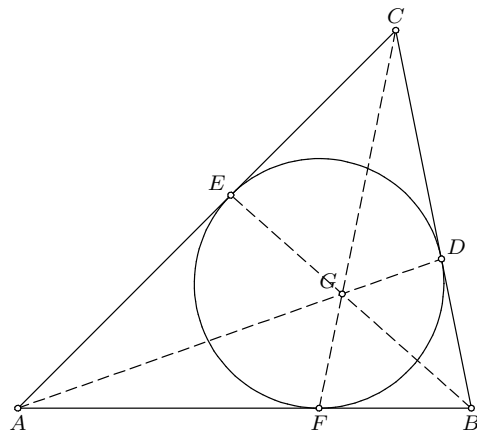
Kompleksnost: 12.877s, 8738 terma.

Teorema nije dokazana metodom Groebner-a.

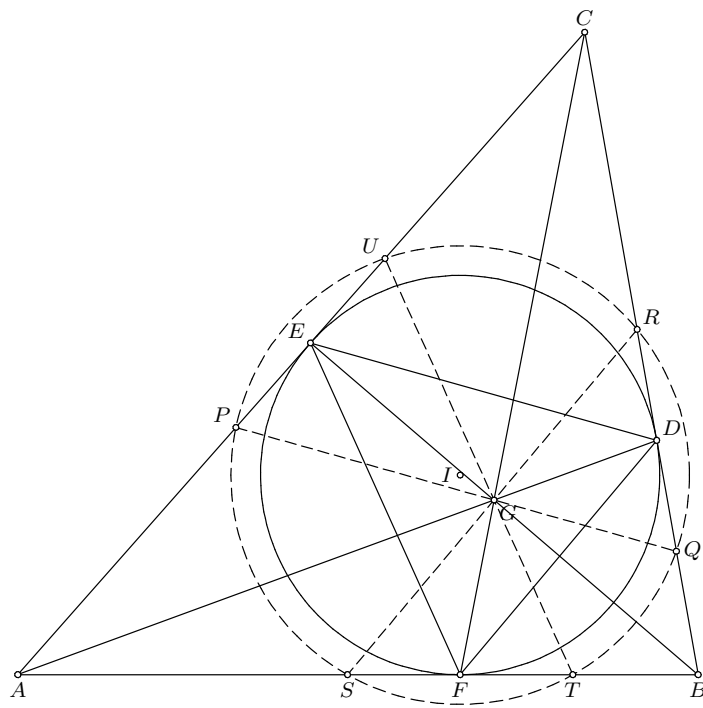
Izvršavanje prekinuto posle 21.437s.

Primer 42 Primer 3 iz [1] (slika A.24). Date su tri kolinearne tačke A , B i C i tačke D i E van prave AB . Tačke J , G , K , I , L , H i F su konstruisane kao redom preseči parova pravih: AE i CD , AD i BE , BD i EC , AE i BD , CD i BE , EC i AD i na kraju DE i AB . Neka je dalje O presek pravih JH i IG . Dokazati da su tačke O , E i D kolinearne, kao i da su tačke O , L i K takođe kolinearne.

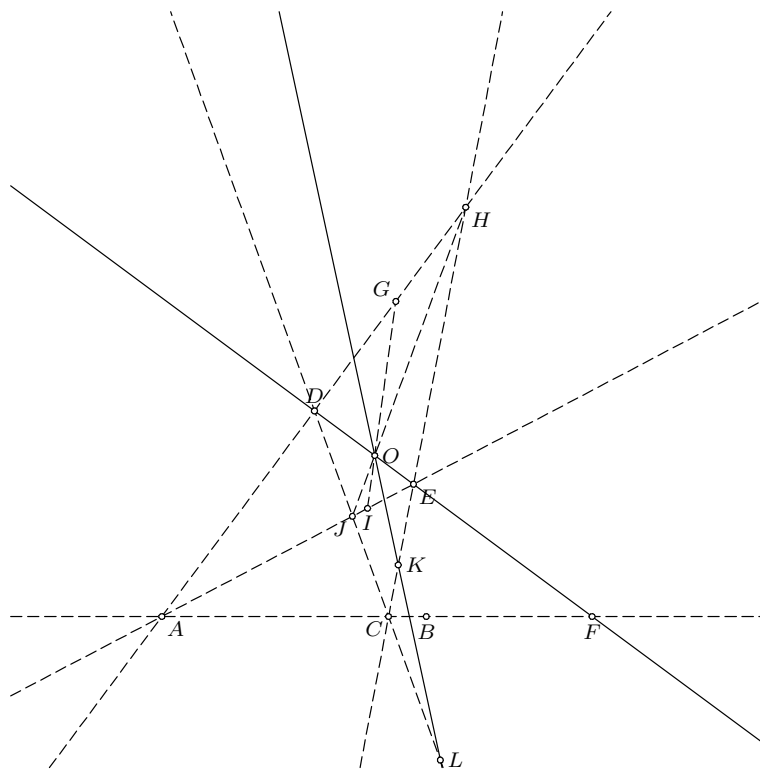
$A = (0, 0)$, $B = (u_1, 0)$, $C = (u_7, 0)$, $D = (u_3, u_4)$, $E = (u_5, u_6)$, $J = (x_3, x_2)$, $G = (x_5, x_4)$, $K = (x_7, x_6)$, $I = (x_9, x_8)$, $L = (x_{11}, x_{10})$, $H =$



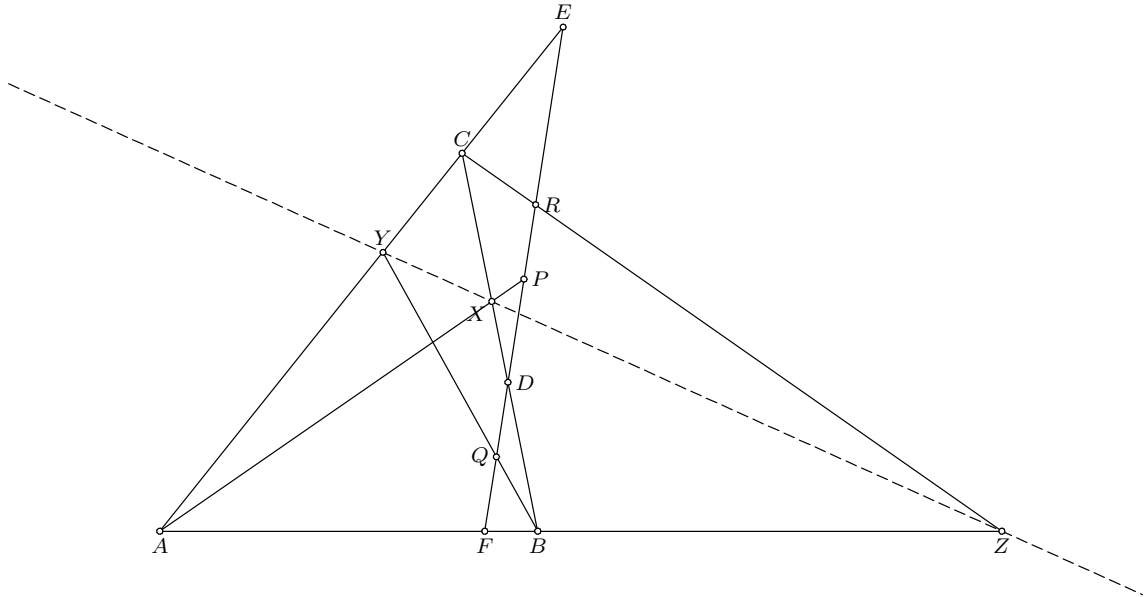
Slika A.22: Gergonova tačka



Slika A.23: Adamsov krug



Slika A.24: Primer 3 iz [1]



Slika A.25: Primer 25 iz [1]

$(x_{13}, x_{12}), F = (x_{15}, 0), O = (x_{17}, x_{16}).$

Teorema je dokazana metodom Wu-a.

Kompleksnost: 1.037s, 1022 terma.

Teorema nije dokazana metodom Groebner-a.

Izvršavanje prekinuto posle 21.328s.

Primer 43 *Primer 25 iz [1] (slika A.25). Proizvoljna prava seče stranice trougla ABC u tačkama D, E i F. Neka su P, Q i R središta duži EF, FD i DE. Dalje, neka prave AP, BQ i CR seku prave BC, CA i AB u tačkama X, Y i Z. Dokazati da su X, Y i Z kolinearne.*

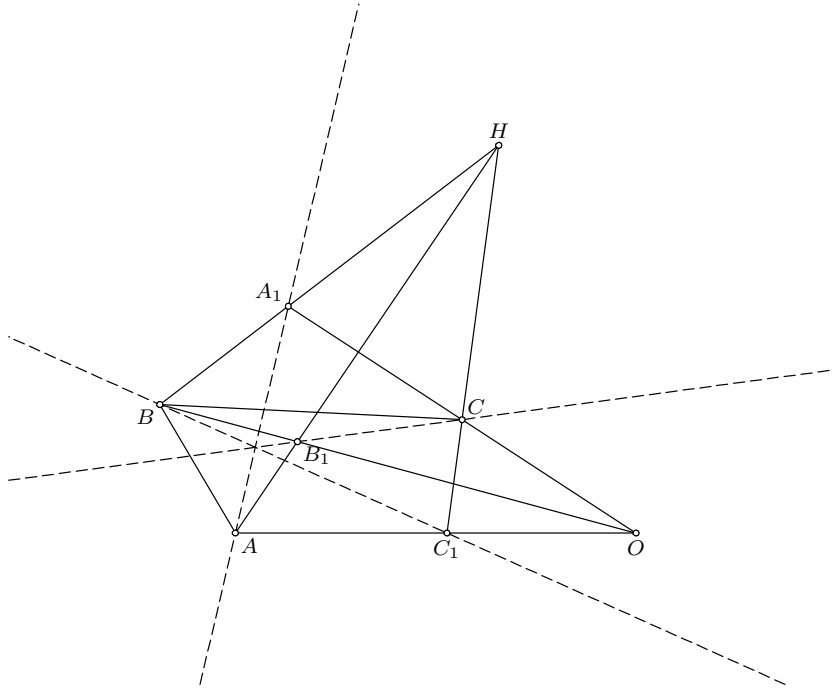
$A = (0, 0), B = (u_1, 0), C = (u_2, u_3), F = (u_6, 0), D = (x_2, u_5), E = (x_4, x_3), P = (x_6, x_5), Q = (x_8, x_7), R = (x_{10}, x_9), X = (x_{12}, x_{11}), Y = (x_{14}, x_{13}), Z = (x_{16}, 0).$

Teorema je dokazana metodom Wu-a.

Kompleksnost: 2.569s, 2302 terma.

Teorema nije dokazana metodom Groebner-a.

Izvršavanje prekinuto posle 21.046s.



Slika A.26: Primer 28 iz [1]

Primer 44 *Primer 28 iz [1] (slika A.26). Kod šestougla $AC_1BA_1CB_1$ trojka pravih BB_1 , C_1A i A_1C je konkurentna, kao i trojka pravih CC_1 , A_1B i B_1A . Dokazati da je i trojka pravih AA_1 , B_1C i C_1B takođe konkurentna.*

Pošto dokazujemo teoreme konstruktivnog tipa, a ne opisnog, ova opisna teorema mora biti iskazana u konstruktivnom tipu. Prvo će biti konstruisan šestougao koji zadovoljava svojstva iz zadatka, i potom će na njemu biti dokazana teorema.

$A = (0, 0)$, $C_1 = (u_1, 0)$, $B = (u_2, u_3)$, $A_1 = (u_4, u_5)$, $C = (u_6, u_7)$, $O = (x_2, 0)$, $H = (x_4, x_3)$, $B_1 = (x_6, x_5)$, $I = (x_8, x_7)$.

Teorema je dokazana metodom Wu-a.

Kompleksnost: 0.036s, 90 terma.

Teorema nije dokazana metodom Groebner-a.

Izvršavanje prekinuto posle 21.084s.

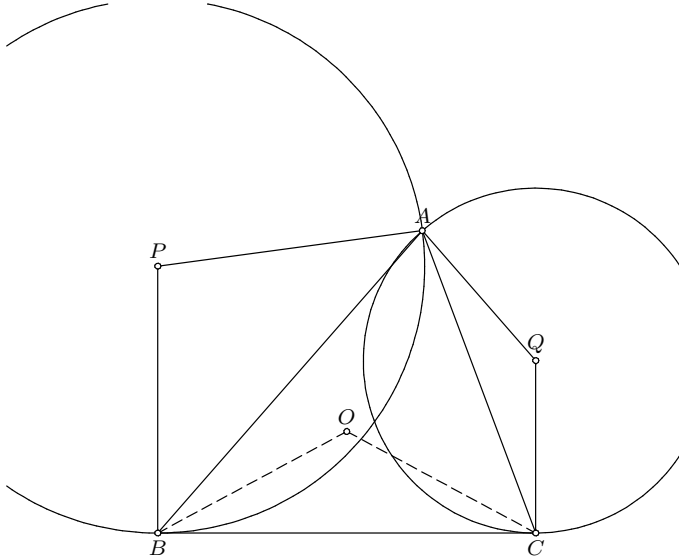
Primer 45 *Primer 29 iz [1] (slika A.27). U ravni je dat trougao ABC . Krugovi k_1 i k_2 sadrže teme A i dodiruju pravu BC u temenima B i C redom. Ako su p i q poluprečnici krugova k_1 i k_2 , dokazati da je $pq = R^2$, gde je R poluprečnik opisanog kruga trougla ABC .*

Prvo su konstruisani krugovi k_1 i k_2 sa centrima P i Q .

$B = (0, 0)$, $C = (u_1, 0)$, $A = (u_2, u_3)$, $O = (x_2, x_1)$, $P = (0, x_3)$, $Q = (u_1, x_5)$.

Teorema je dokazana metodom Wu-a.

Kompleksnost: 0.016s, 73 terma.



Slika A.27: Primer 29 iz [1]

Teorema je dokazana metodom Groebner-a.

Kompleksnost: 0.015s, 73 terma.

Primer 46 Primer 30 iz [1] (slika A.28). Neka su H i O ortocentar i centar opisanog kruga trougla ABC . Dokazati da je $\angle HAO = |\angle B - \angle C|$.

$C = (0, 0)$, $B = (u_1, 0)$, $A = (u_2, u_3)$, $D = (u_2, 0)$, $O = (x_4, x_3)$.

Teorema je dokazana metodom Wu-a.

Kompleksnost: 0.009s, 25 terma.

Teorema je dokazana metodom Groebner-a.

Kompleksnost: 0.011s, 36 terma.

Primer 47 Primer 31 iz [1] (slika A.29). Dokazati da u proizvoljnom trouglu važi jednakost: $OH^2 = 9R^2 - a^2 - b^2 - c^2$.

$A = (0, 0)$, $B = (u_1, 0)$, $C = (u_2, u_3)$, $O = (x_2, x_1)$, $H = (u_2, x_3)$.

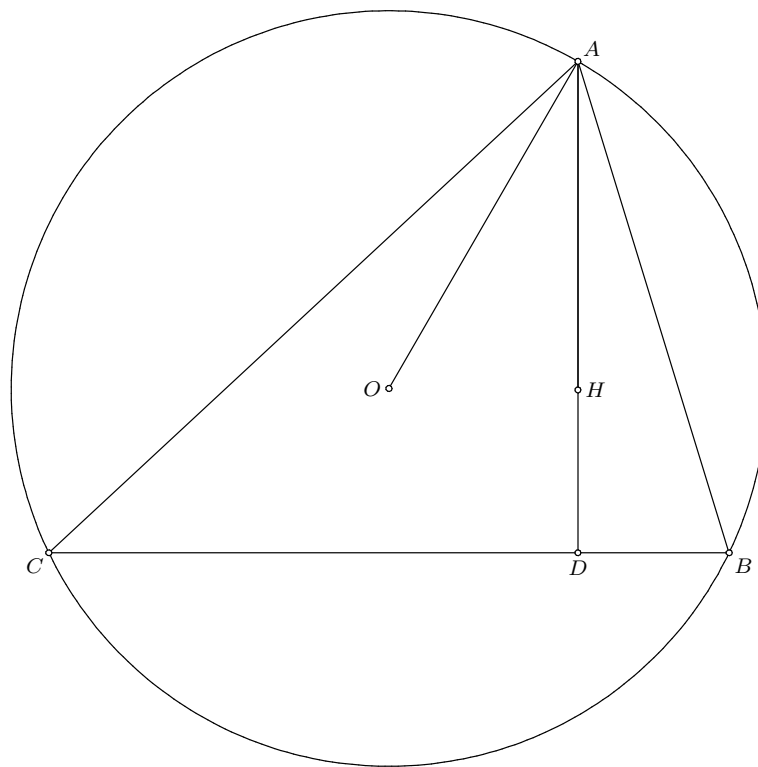
Teorema je dokazana metodom Wu-a.

Kompleksnost: 0.006s, 12 terma.

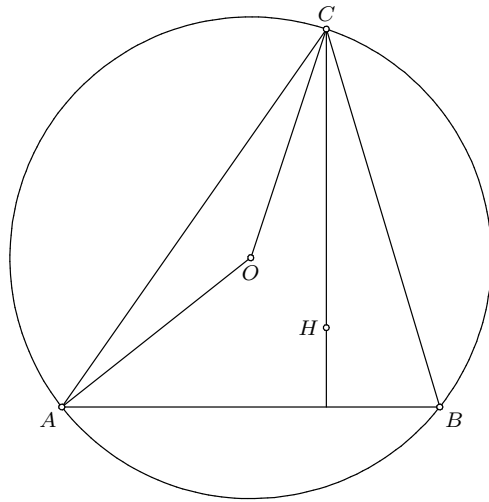
Teorema je dokazana metodom Groebner-a.

Kompleksnost: 0.008s, 32 terma.

Primer 48 Primer 35 iz [1] (slika A.30). Neka je ABC jednakokranični trougao upisan u krug sa centrom O , i neka je P proizvoljna tačka na krugu. Dokazati da Simsonova linija iz tačke P polovi poluprečnik PO .



Slika A.28: Primer 30 iz [1]



Slika A.29: Primer 31 iz [1]

$A = (0, 0)$, $B = (u_1, 0)$, $C = (x_2, x_1)$, $C1 = (x_2, x_3)$, $O = (x_2, x_5)$, $P = (x_7, u_2)$, $D = (x_9, x_8)$, $E = (x_{11}, x_{10})$, $I = (x_{13}, x_{12})$.

Teorema je dokazana metodom Wu-a.

Kompleksnost: 0.050s, 64 terma.

Teorema nije dokazana metodom Groebner-a.

Izvršavanje prekinuto posle 21.003s.

Primer 49 *Primer 37 iz [1] (slika A.31). Iz tačke P su povučene tangente PT i PB na krug k sa centrom O . Neka je BA prečnik kruga k i neka je H normala spuštена iz T na prečnik AB . Dokazati da prava AP polovi duž TH .*

Konstrukcija u dokazu je izvedena na drugačini način, polazeći od prečnika AB i odabirom proizvoljne tačke T na krugu (pogledati koordinate tačaka u konstrukciji).

$A = (0, 0)$, $B = (u_1, 0)$, $O = (x_2, 0)$, $T = (x_3, u_2)$, $P = (u_1, x_4)$, $H = (x_3, 0)$, $I = (x_9, x_8)$.

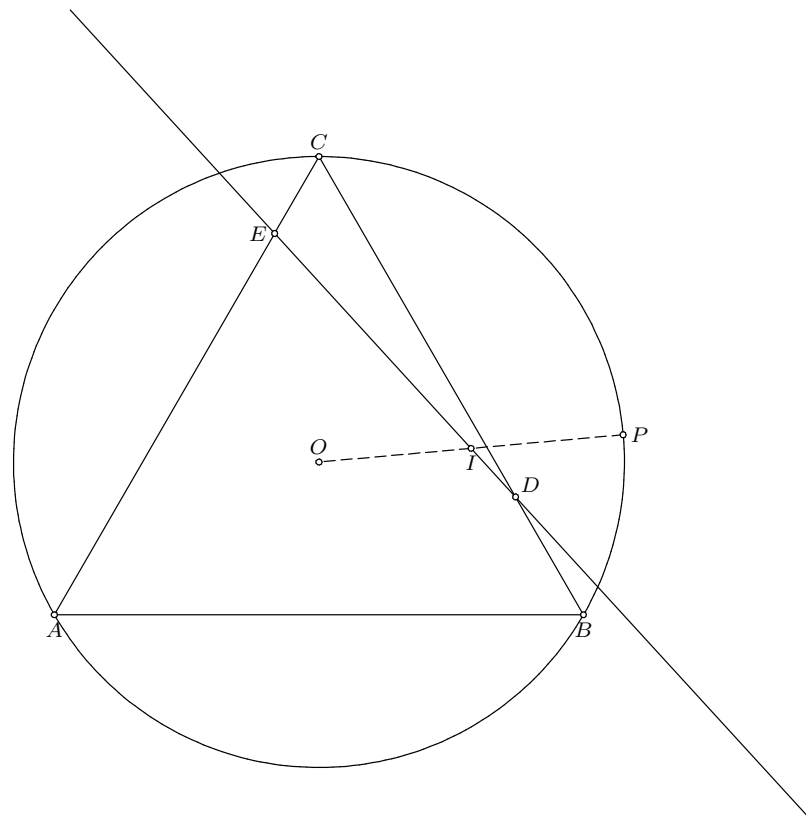
Teorema je dokazana metodom Wu-a.

Kompleksnost: 0.003s, 6 terma.

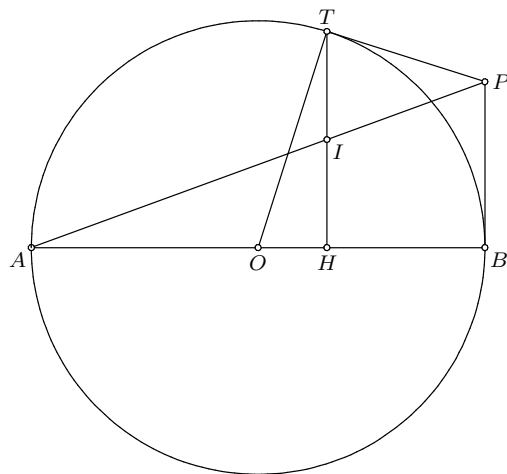
Teorema je dokazana metodom Groebner-a.

Kompleksnost: 0.003s, 6 terma.

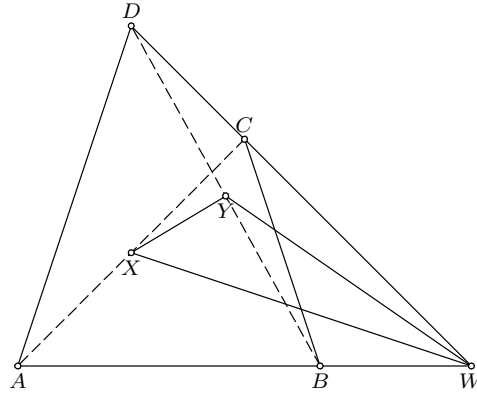
Primer 50 *Primer 42 iz [1] (slika A.32). Dat je četvorougao $ABCD$. Neka se prave AB i CD seku u tački W i neka su X i Y središta dijagonala AC i BD . Dokazati da je površina trougla XYW četiri puta manja od površine četvorougla $ABCD$.*



Slika A.30: Primer 35 iz [1]



Slika A.31: Primer 37 iz [1]



Slika A.32: Primer 42 iz [1]

Teorema se dokazuje za orijentisane površine. Posmatraju se orijentisani trougao XWY i orijentisani četvorougao $ABCD$.

$A = (0, 0)$, $B = (u_1, 0)$, $C = (u_2, u_3)$, $D = (u_4, u_5)$, $W = (x_2, 0)$, $X = (x_4, x_3)$, $Y = (x_6, x_5)$.

Teorema je dokazana metodom Wu-a.

Kompleksnost: 0.016s, 48 terma.

Teorema je dokazana metodom Groebner-a.

Kompleksnost: 0.024s, 96 terma.

Primer 51 Primer 46 iz [1] (slika A.33). Dat je paralelogram $ABEFD$. Na dvema paralelnim stranicama AE i BD date su tačke C i F . Neka je M presek pravih CD i AF i neka je N presek pravih BC i EF . Neka su dalje P i Q preseči prave MN sa stranicama paralelograma AD i BE . Dokazati da su duži AP i BQ jednake.

Dovoljno je dokazati da su duži AP i BQ paralelne i istog odnosa.

$A = (0, 0)$, $E = (u_1, 0)$, $B = (u_2, u_3)$, $C = (u_6, 0)$, $D = (x_3, u_3)$, $F = (u_7, u_3)$, $M = (x_6, x_5)$, $N = (x_8, x_7)$, $P = (x_{10}, x_9)$, $Q = (x_{12}, x_{11})$.

Teorema je dokazana metodom Wu-a.

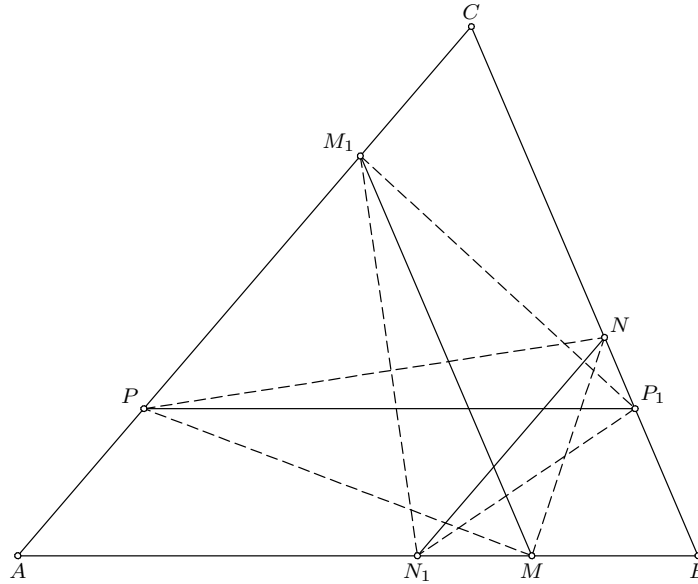
Kompleksnost: 0.104s, 114 terma.

Teorema nije dokazana metodom Groebner-a.

Izvršavanje prekinuto posle 21.019s.

Primer 52 Primer 49 iz [1] (slika A.34). Dat je trapez $ABCD$ gde su AB i CD paralelne. Dokazati da prava koja sadrži presek dijagonala trapeza i presek suprotnih stranica trapeza polovi bazu AB trapeza.

Slika A.34: Primer 49 iz [1]



Slika A.35: Primer 55 iz [1]

Dovoljno je dokazati jednak odnos duži pošto se nalaze na istoj pravoj.
 $A = (0, 0)$, $B = (u_1, 0)$, $C = (u_2, u_3)$, $D = (u_5, u_3)$, $F = (x_3, x_2)$, $E = (x_5, x_4)$, $G = (x_7, 0)$.

Teorema je dokazana metodom Wu-a.

Kompleksnost: 0.007s, 5 terma.

Teorema je dokazana metodom Groebner-a.

Kompleksnost: 0.043s, 114 terma.

Primer 53 Primer 55 iz [1] (slika A.35). Dat je trougao ABC i tačke M , N i P na stranicama AB , BC i CA redom. Neka su M_1 , N_1 i P_1 tačke na pravama CA , AB i BC takve da je $MM_1 \parallel BC$, $NN_1 \parallel AC$ i $PP_1 \parallel AB$. Dokazati da su površine trouglova MNP i $M_1N_1P_1$ jednake.

$A = (0, 0)$, $B = (u_1, 0)$, $C = (u_2, u_3)$, $M = (u_7, 0)$, $N = (x_2, u_5)$, $P = (x_3, u_6)$, $P_1 = (x_5, u_6)$, $M_1 = (x_7, x_6)$, $N_1 = (x_9, 0)$.

Teorema je dokazana metodom Wu-a.

Kompleksnost: 0.008s, 8 terma.

Slika A.36: Primer 56 iz [1]

Teorema je dokazana metodom Groebner-a.
Kompleksnost: 0.005s, 9 terma.

Primer 54 *Primer 56 iz [1] (slika A.36). Dat je paralelogram $MNPQ$. Prava koja prolazi kroz M seče prave PQ , NP i NQ u tačkama S , R i T . Dokazati da je $\frac{1}{MR} + \frac{1}{MS} = \frac{1}{MT}$.*

Pošto se tačke M , R , S i T nalaze na istoj pravoj, dovoljno je dokazati da je $\frac{MT}{MR} + \frac{MT}{MS} = 1$.

$M = (0, 0)$, $N = (u_1, 0)$, $P = (u_2, u_3)$, $Q = (x_2, u_3)$, $S = (u_5, u_3)$, $T = (x_5, x_4)$, $R = (x_7, x_6)$.

Teorema je dokazana metodom Wu-a.
Kompleksnost: 0.005s, 4 terma.
Teorema je dokazana metodom Groebner-a.
Kompleksnost: 0.005s, 9 terma.

Primer 55 *Primer 57 iz [1] (slika A.37). Dat je paralelogram $ABCD$. Neka je C_1 tačka na stranici AB koja deli tu stranicu u odnosu 1 : 2. Na sličan način konstruisane su i tačke D_1 , A_1 i B_1 na stranicama BC , CD i DA . Neka su dalje $A_2 = AA_1 \cap DD_1$, $B_2 = BB_1 \cap CC_1$, $C_2 = CC_1 \cap DD_1$ i $D_2 = DD_1 \cap AA_1$. Dokazati da je površina četvorougla $ABCD$ trinaest puta veća od površine četvorougla $A_2B_2C_2D_2$.*

$A = (0, 0)$, $B = (u_1, 0)$, $C = (u_2, u_3)$, $D = (x_2, u_3)$, $C_1 = (x_4, 0)$, $D_1 = (x_6, x_5)$, $A_1 = (x_8, u_3)$, $B_1 = (x_{10}, x_9)$, $A_2 = (x_{12}, x_{11})$, $B_2 = (x_{14}, x_{13})$, $C_2 = (x_{16}, x_{15})$, $D_2 = (x_{18}, x_{17})$.

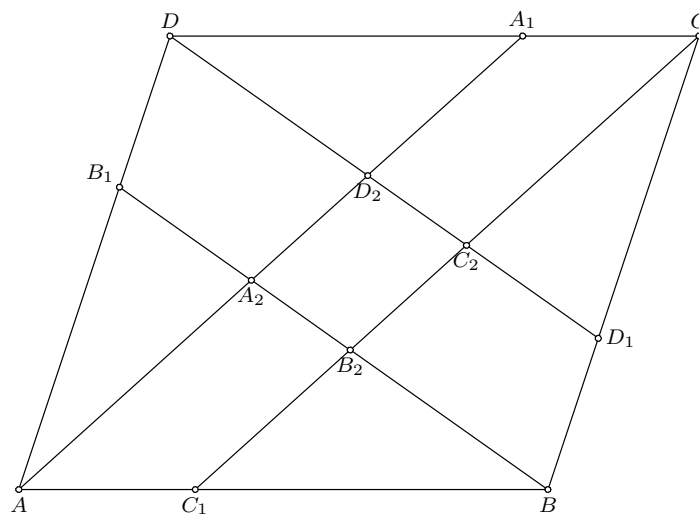
Teorema je dokazana metodom Wu-a.
Kompleksnost: 1.015s, 987 terma.
Teorema je dokazana metodom Groebner-a.
Kompleksnost: 2.967s, 987 terma.

Primer 56 *Primer 58 iz [1] (slika A.38). Dat je trougao ABC . Neka je C_1 tačka na stranici AB koja deli tu stranicu u odnosu 1 : 2. Na sličan način konstruisane su i tačke A_1 i B_1 na stranicama BC i CA . Neka su dalje $A_2 = BB_1 \cap CC_1$, $B_2 = AA_1 \cap CC_1$ i $C_2 = AA_1 \cap BB_1$. Dokazati da je površina trougla ABC sedam puta veća od površine trougla $A_2B_2C_2$.*

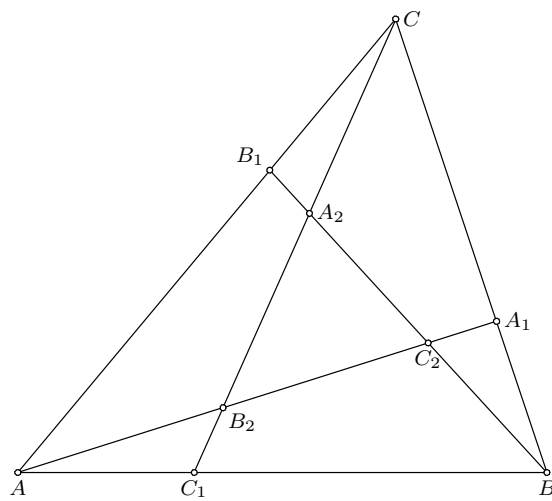
$A = (0, 0)$, $B = (u_1, 0)$, $C_1 = (x_2, 0)$, $C = (u_2, u_3)$, $A_1 = (x_4, x_3)$, $B_1 = (x_6, x_5)$, $A_2 = (x_8, x_7)$, $B_2 = (x_{10}, x_9)$, $C_2 = (x_{12}, x_{11})$.

Teorema je dokazana metodom Wu-a.
Kompleksnost: 0.036s, 36 terma.
Teorema je dokazana metodom Groebner-a.
Kompleksnost: 1.022s, 67 terma.

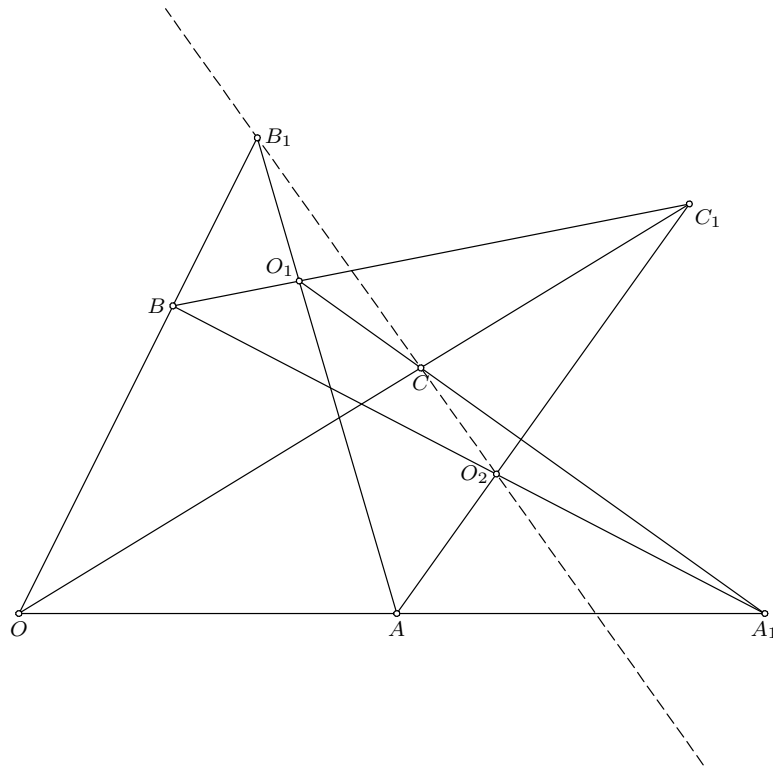
Primer 57 *Primer 59 iz [1] (slika A.39). Dva duplo perspektivna trougla su istovremeno i troustruko perspektivna.*



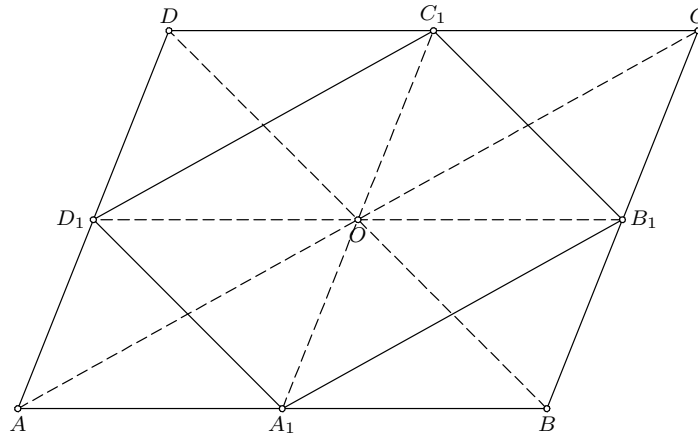
Slika A.37: Primer 57 iz [1]



Slika A.38: Primer 58 iz [1]



Slika A.39: Primer 59 iz [1]



Slika A.40: Primer 69 iz [1]

Dva trougla ABC i $A_1B_1C_1$ su perspektivna ukoliko su prave AA_1 , BB_1 i CC_1 kolinearne. Konstrukcija duplo perspektivnog je polazna u dokazu teoreme (iskusniji čitalac može na osnovu izbora koordinata tačaka rekonstruisati korake konstrukcije).

$O = (0, 0)$, $A = (u_1, 0)$, $B = (u_2, u_3)$, $C = (u_4, u_5)$, $O_1 = (u_6, u_7)$, $A_1 = (x_2, 0)$, $B_1 = (x_4, x_3)$, $C_1 = (x_6, x_5)$, $O_2 = (x_8, x_7)$.

Teorema je dokazana metodom Wu-a.

Kompleksnost: 0.035s, 68 terma.

Teorema nije dokazana metodom Groebner-a.

Izvršavanje prekinuto posle 24.049s.

Primer 58 Primer 69 iz [1] (slika A.40). Dijagonale paralelograma i upisanog paralelograma su konkurentne.

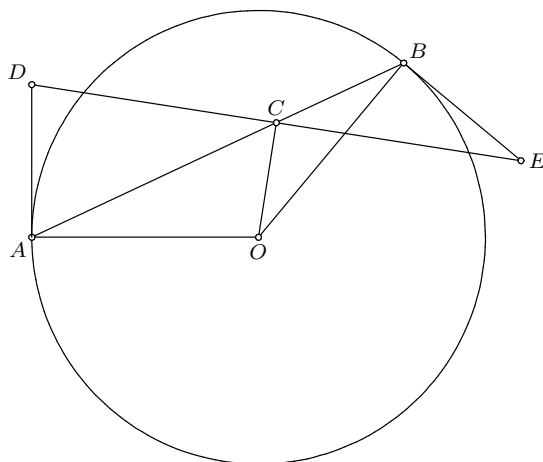
$A = (0, 0)$, $B = (u_1, 0)$, $C = (u_2, u_3)$, $D = (x_2, u_3)$, $A_1 = (x_4, 0)$, $B_1 = (x_6, x_5)$, $C_1 = (x_8, u_3)$, $D_1 = (x_{10}, x_9)$, $O = (x_{12}, x_{11})$.

Teorema je dokazana metodom Wu-a.

Kompleksnost: 0.023s, 39 terma.

Teorema je dokazana metodom Groebner-a.

Kompleksnost: 0.065s, 39 terma.



Slika A.41: Primer 75 iz [1]

Primer 59 *Primer 75 iz [1] (slika A.41). Na tetivi AB kruga k sa centrom O , izabrana je tačka C . Neka su D i E preseči normale iz tačke C na pravu OC sa tangentama kruga k iz tačkaka A i B . Dokazati da je C središte duži DE .*

Dovoljno je pokazati da su projekcije duži CD i CE na x osu jednake.

$A = (0, 0)$, $O = (u_1, 0)$, $B = (x_1, u_2)$, $C = (x_2, u_3)$, $E = (x_4, x_3)$, $D = (0, x_5)$.

Teorema je dokazana metodom Wu-a.

Kompleksnost: 0.023s, 69 terma.

Teorema nije dokazana metodom Groebner-a.

Izvršavanje prekinuto posle 21.013s.

Primer 60 *Primer 77 iz [1] (slika A.42). Harmonijska spregnutost četiri tačke na krugu je jednaka u odnosu na svaku tačku kruga.*

$A = (0, 0)$, $B = (u_1, 0)$, $C = (u_2, u_3)$, $O = (x_2, x_1)$, $D = (x_3, u_4)$, $P = (x_4, u_5)$, $Q = (x_5, u_6)$, $F = (x_7, 0)$, $G = (x_9, 0)$, $F_1 = (x_{11}, 0)$, $G_1 = (x_{13}, 0)$.

Teorema je dokazana metodom Wu-a.

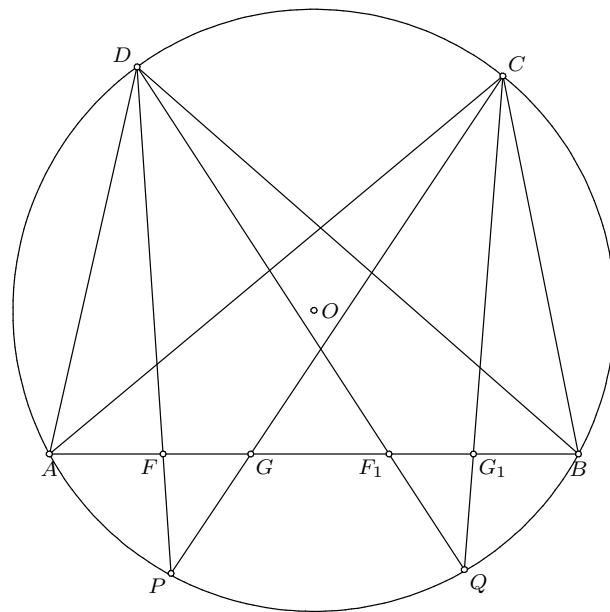
Kompleksnost: 0.028s, 64 terma.

Teorema nije dokazana metodom Groebner-a.

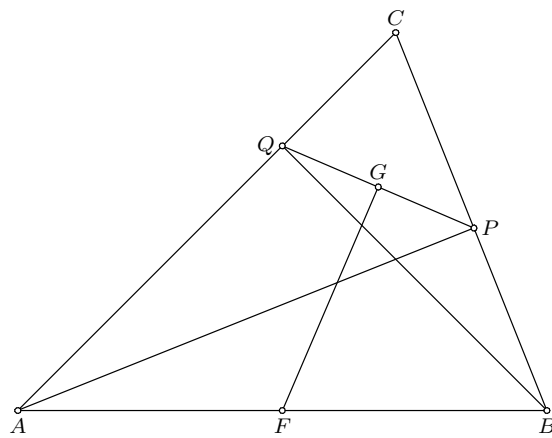
Krajnje svodenje nije rezultiralo nula polinomom!

Primer 61 *Primer 82 iz [1] (slika A.43). U ravni je dat trougao ABC . Neka je F središte stranice AB i neka su P i Q podnožja visina spuštenih iz temena A i B . Neka je G podnožje normale iz F na pravu PQ . Dokazati da je G središte duži PQ .*

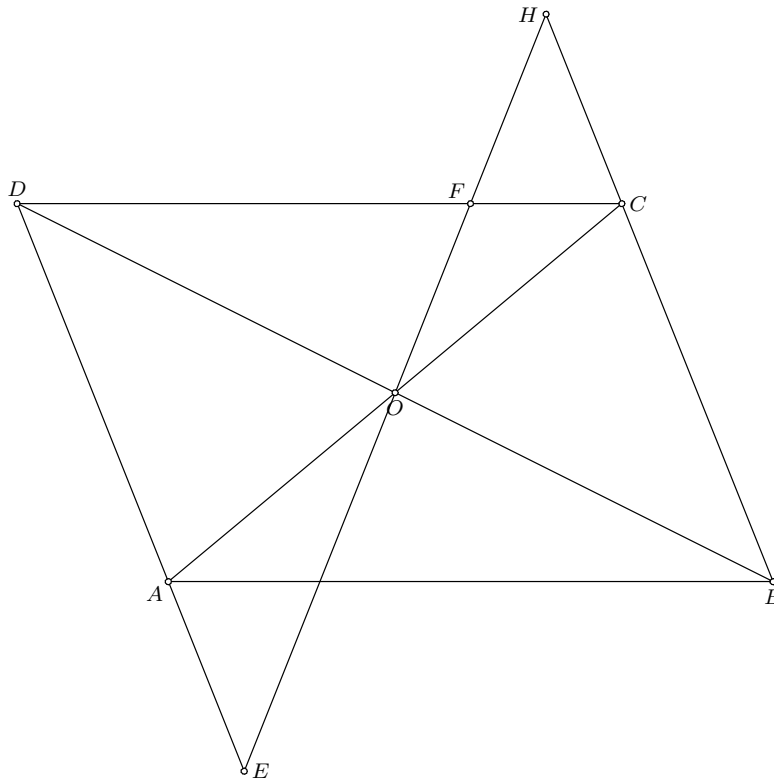
$A = (0, 0)$, $B = (u_1, 0)$, $C = (u_2, u_3)$, $F = (x_2, 0)$, $P = (x_4, x_3)$, $Q = (x_6, x_5)$, $G = (x_8, x_7)$.



Slika A.42: Primer 77 iz [1]



Slika A.43: Primer 82 iz [1]



Slika A.44: Primer 84 iz [1]

Teorema je dokazana metodom Wu-a.

Kompleksnost: 0.034s, 114 terma.

Teorema nije dokazana metodom Groebner-a.

Izvršavanje prekinuto posle 21.157s.

Primer 62 *Primer 84 iz [1] (slika A.44). Prava koja prolazi kroz presek dijagonala paralelograma ABCD seče prave određene stranicama paralelograma u tačkama E, F, G i H. Dokazati da je $EF \cong GH$.*

$A = (0, 0)$, $B = (u_1, 0)$, $C = (u_2, u_3)$, $D = (x_2, u_3)$, $H = (x_3, u_4)$, $O = (x_5, x_4)$, $F = (x_7, u_3)$, $G = (x_9, 0)$, $E = (x_{11}, x_{10})$.

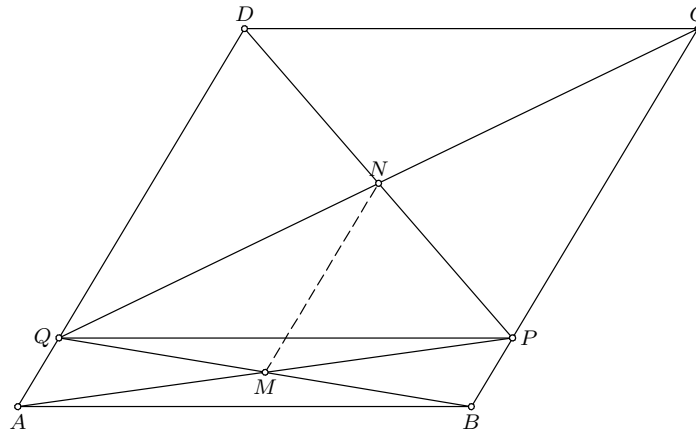
Teorema je dokazana metodom Wu-a.

Kompleksnost: 0.007s, 14 terma.

Teorema je dokazana metodom Groebner-a.

Kompleksnost: 0.240s, 69 terma.

Primer 63 *Primer 85 iz [1] (slika A.45). Dat je paralelogram ABCD. Neka su P i Q tačke na stranicama BC i AD takve da je $PQ \parallel AB$. Neka su dalje $M = BQ \cap AP$ i $N = CQ \cap PD$. Dokazati da je MN paralelna sa AD i jednaka polovini te stranice.*



Slika A.45: Primer 85 iz [1]

Kada se dokaže paralelnost, druga pretpostavka se dokazuje kroz odnos duži.

$A = (0, 0)$, $B = (u_1, 0)$, $C = (u_2, u_3)$, $D = (x_2, u_3)$, $P = (x_3, u_4)$, $Q = (x_5, u_4)$, $N = (x_7, x_6)$, $M = (x_9, x_8)$.

Teorema je dokazana metodom Wu-a.

Kompleksnost: 0.028s, 39 terma.

Teorema je dokazana metodom Groebner-a.

Kompleksnost: 0.017s, 39 terma.

Primer 64 Primer 86 iz [1] (slika A.46). Neka je ABC trougao takav da je ugao kod temena B dva puta veći od ugla u temenu C . Neka je D podnožje normale iz tačke A i neka je M središte stranice BC . Dokazati da je $AB = 2DM$.

Slika je konstruisana tako što je prvo konstruisan jednakokraki trougao CFB , a zatim tačka A određena kao presek simetrane ugla $\angle C$ i stranice BF .

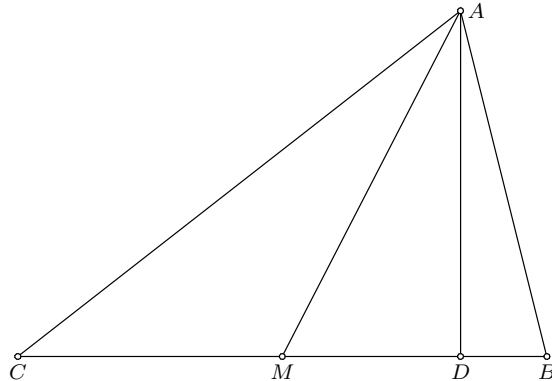
$C = (0, 0)$, $B = (u_1, 0)$, $A_1 = (u_2, u_3)$, $F = (x_2, x_1)$, $A = (x_4, x_3)$, $M = (x_2, 0)$, $D = (x_4, 0)$.

Teorema je dokazana metodom Wu-a.

Kompleksnost: 0.122s, 37 terma.

Teorema je dokazana metodom Groebner-a.

Kompleksnost: 0.068s, 65 terma.



Slika A.46: Primer 86 iz [1]

Primer 65 *Primer 88 iz [1] (slika A.47). Data je tačka D na osnovi AC jednakostraničnog trougla ABC . Neka su E i F podnožja normala iz tačke D na stranice AB i BC i neka je H podnožje visine trougla ABC iz temena C . Dokazati da je zbir duži DE i DF jednak visini CH .*

Dovoljno je dokazati da je algebarska suma duži DE , DF i CH jednaka nuli.

$A = (0, 0)$, $B = (u_1, 0)$, $C = (x_1, u_2)$, $D = (x_2, u_3)$, $E = (x_2, 0)$, $F = (x_6, x_5)$, $H = (x_1, 0)$.

Teorema je dokazana metodom Wu-a.

Kompleksnost: 0.191s, 426 terma.

Teorema je dokazana metodom Groebner-a.

Kompleksnost: 0.076s, 426 terma.

Primer 66 *Primer 91 iz [1] (slika A.48). Neka je D tačka na stranici BC pravouglog trougla ABC takva da krug sa centrom O i prečnikom CD dotiče hipotenuzu AB u tački E . Neka je $F = AC \cap DE$. Dokazati da je $AF \cong AE$.*

Konstrukcija je izvedena tako što su tačke C i D izabrane proizvoljno, tačka E je izabrana proizvoljno na krugu sa prečnikom CD , a ostale tačke tako da zadovoljavaju uslove konstrukcije.

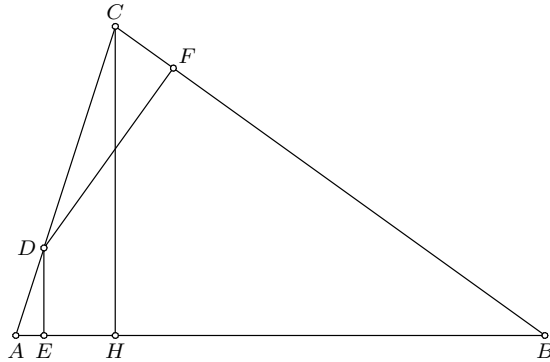
$C = (0, 0)$, $D = (u_1, 0)$, $O = (x_2, 0)$, $E = (x_3, u_2)$, $A = (0, x_4)$, $B = (x_7, 0)$, $F = (0, x_8)$.

Teorema je dokazana metodom Wu-a.

Kompleksnost: 0.004s, 9 terma.

Teorema je dokazana metodom Groebner-a.

Kompleksnost: 0.017s, 11 terma.



Slika A.47: Primer 88 iz [1]

Primer 67 *Primer 92 iz [1] (slika A.49). Sa prečnika CD kruga sa centrom O , spuštene su normale CE i DF na tetivu AB . Dokazati da je $OE \cong OF$.*

Konstrukcija je izvedena tako što su izabrane proizvoljne tačke A, B, X, Y i Z . Centar kruga je određen kao presek prave XY i simetrane duži AB . Prečnik CD je određen kao presek prave OZ i kruga.

$A = (0, 0)$, $B = (u_1, 0)$, $X = (u_2, u_3)$, $Y = (u_4, u_5)$, $O = (x_2, x_1)$, $Z = (u_6, u_7)$, $D = (x_4, x_3)$, $C = (x_6, x_5)$, $E = (x_6, 0)$, $F = (x_4, 0)$.

Teorema je dokazana metodom Wu-a.

Kompleksnost: 0.048s, 78 terma.

Teorema nije dokazana metodom Groebner-a.

Izvršavanje prekinuto posle 102.404s.

Primer 68 *Primer 94 iz [1] (slika A.50). Oko trougla ABE opisan je krug k sa centrom O . Neka je PE proizvoljna tangenta na krug k . Simetrana ugla $\angle APE$ seče duži EA i BE u tačkama C i D . Dokazati da je $EC \cong ED$.*

$E = (0, 0)$, $O = (u_1, 0)$, $A = (x_1, u_2)$, $B = (x_2, u_3)$, $P = (0, x_3)$, $C = (x_6, x_5)$, $D = (x_8, x_7)$.

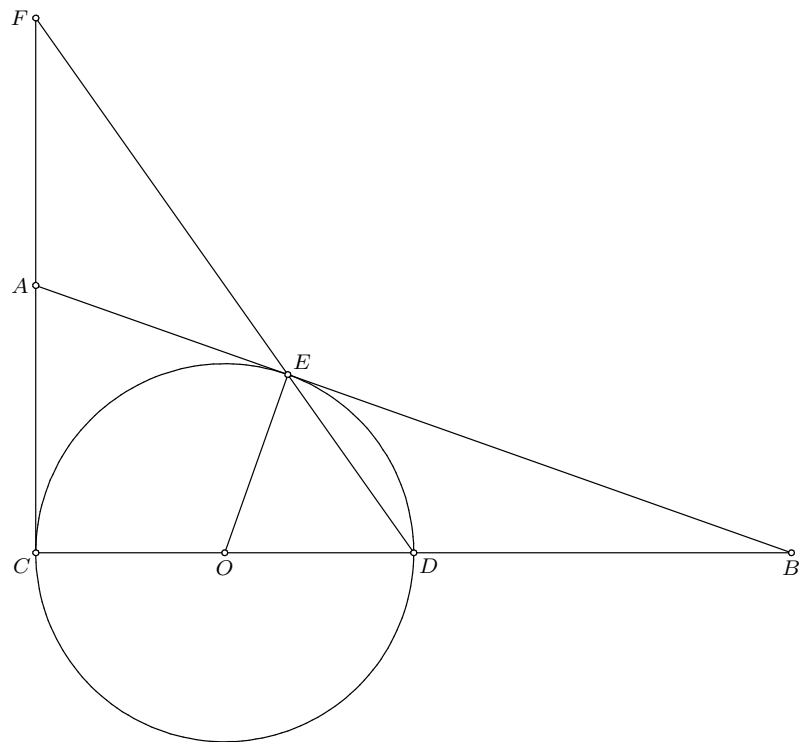
Teorema je dokazana metodom Wu-a.

Kompleksnost: 1.746s, 1833 terma.

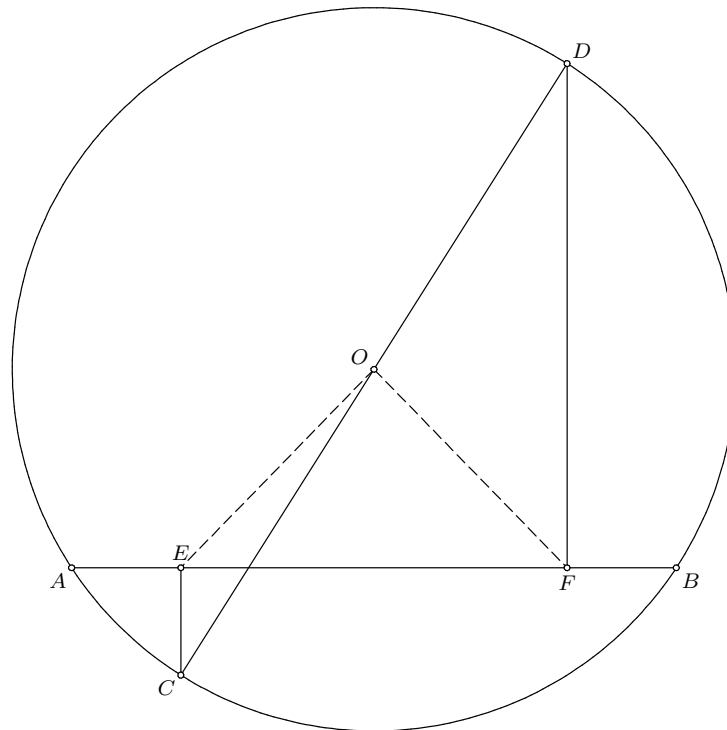
Teorema nije dokazana metodom Groebner-a.

Izvršavanje prekinuto posle 21.009s.

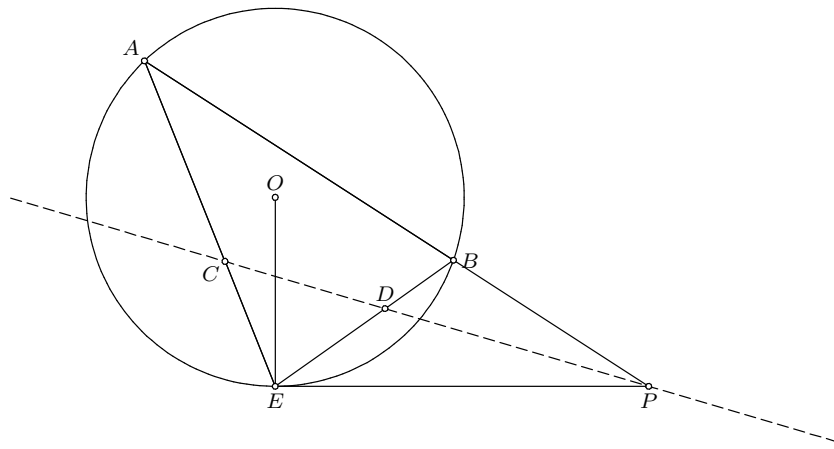
Primer 69 *Primer 95 iz [1] (slika A.51). Na krugu k sa centrom O data je tetiva AB . Neka je D središte tetive AB i neka je M sredina luka AB kruga k . Neka je E podnožje normale spuštene iz M na pravu koja prolazi kroz A i normalna je na poluprečnik AO . Dokazati da je $ME \cong MD$.*



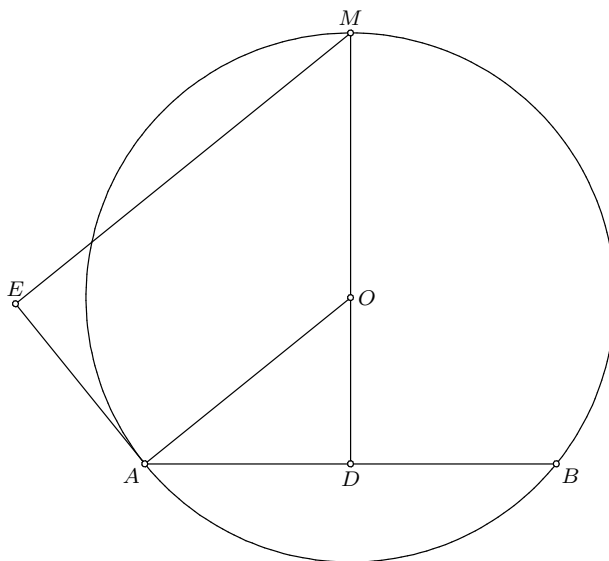
Slika A.48: Primer 91 iz [1]



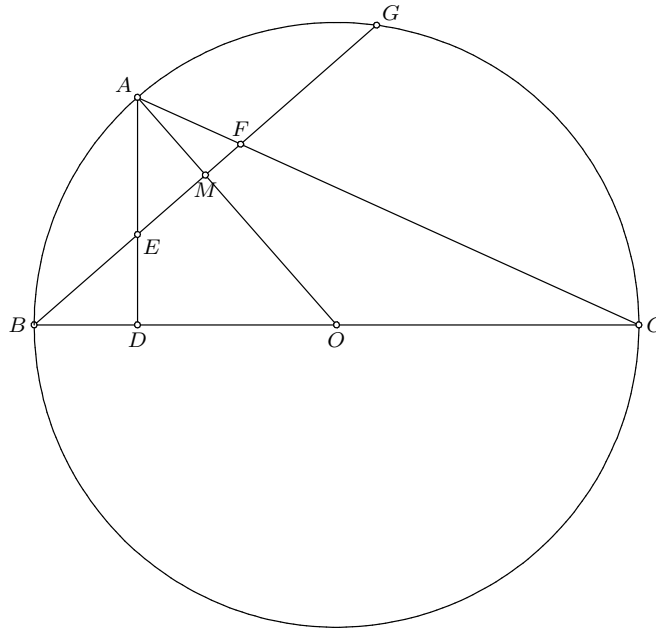
Slika A.49: Primer 92 iz [1]



Slika A.50: Primer 94 iz [1]



Slika A.51: Primer 95 iz [1]



Slika A.52: Primer 97 iz [1]

$D = (0, 0)$, $O = (u_1, 0)$, $M = (u_3, 0)$, $B = (0, x_2)$, $A = (0, x_4)$, $E = (x_7, x_6)$.

Teorema je dokazana metodom Wu-a.

Kompleksnost: 0.004s, 6 terma.

Teorema je dokazana metodom Groebner-a.

Kompleksnost: 0.008s, 15 terma.

Primer 70 *Primer 97 iz [1] (slika A.52). Neka je G tačka na krugu k sa centrom O i prečnikom BC i neka je A sredina luka BG istoga kruga. Tačka D je podnožje normale spuštene iz A na prečnik BC . Neka su dalje $E = AD \cap BG$ i $F = AC \cap BG$. Dokazati da je $AE \cong BE \cong EF$.*

$B = (0, 0)$, $C = (u_1, 0)$, $O = (x_2, 0)$, $G = (x_3, u_2)$, $A = (x_5, x_4)$, $A_1 = (x_7, x_6)$, $E = (x_5, x_8)$, $D = (x_5, 0)$, $F = (x_{13}, x_{12})$.

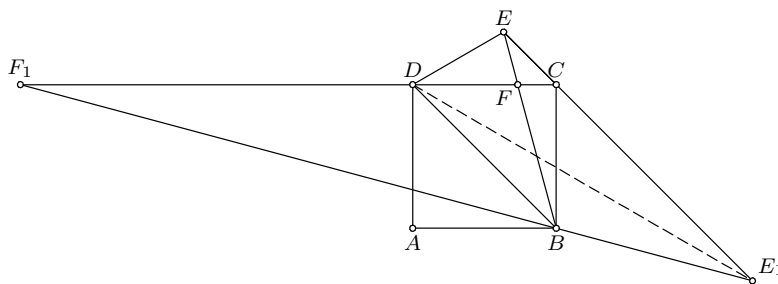
Teorema je dokazana metodom Wu-a.

Kompleksnost: 0.017s, 16 terma.

Teorema nije dokazana metodom Groebner-a.

Izvršavanje prekinuto posle 21.000s.

Primer 71 *Primer 5.1 iz [1] (slika A.53). Dat je kvadrat $ABCD$. Na pravoj koja prolazi kroz teme C i paralelna je dijagonali kvadrata BD izabrana je tačka E takva da je $BD \cong BE$. Neka je F presek prave BE i prave CD . Dokazati da je $DE \cong DF$.*



Slika A.53: Primer 5.1 iz [1]

Slika A.54: Primer 101 iz [1]

Ova teorema ima dve različite slike (pogledati tačke E_1 i F_1). Algebarski dokaz za obe konfiguracije je isti, dok se elementarni dokaz razlikuje u zavisnosti od izabrane slike.

$A = (0, 0)$, $B = (u_1, 0)$, $D = (0, x_1)$, $D_1 = (0, x_3)$, $C = (u_1, x_1)$, $E = (x_8, x_7)$, $E_1 = (x_{10}, x_9)$, $F = (x_{12}, x_{11})$.

Teorema je dokazana metodom Wu-a.

Kompleksnost: 0.008s, 10 terma.

Teorema je dokazana metodom Groebner-a.

Kompleksnost: 0.058s, 10 terma.

Primer 72 Primer 101 iz [1] (slika A.54). Nad hipotenuzom AB pravouglog trougla ABC izdignut je kvadrat $ABFE$ sa centrom P . Dokazati da je $\angle ACP = \angle PCB$.

Problem ima dve konfiguracije, kao što je prikazano na slici. Teorema je tačna za obe konfiguracije.

$C = (0, 0)$, $B = (u_1, 0)$, $A = (0, u_2)$, $E = (x_3, x_2)$, $E_1 = (x_5, x_4)$, $F = (x_7, x_6)$, $P = (x_9, x_8)$.

Teorema je dokazana metodom Wu-a.

Kompleksnost: 0.067s, 92 terma.

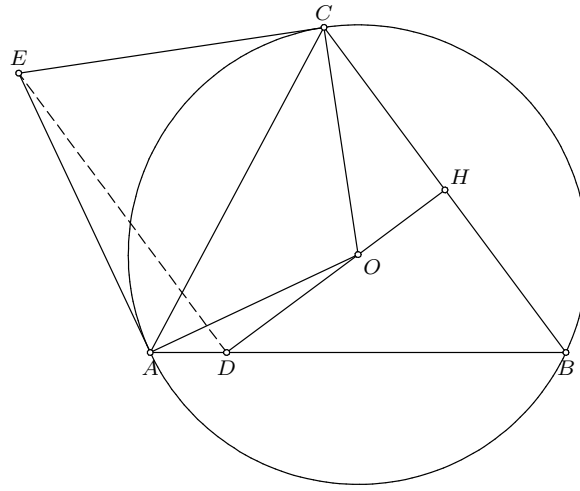
Teorema nije dokazana metodom Groebner-a.

Izvršavanje prekinuto posle 21.000s.

Primer 73 Primer 102 iz [1] (slika A.55). Dve tangente povučene iz A i C na opisan kruga trougla ABC seku se u tački E . Neka je D presek simetrale duži BC i prave AB . Dokazati da je $DE \parallel BC$.

$A = (0, 0)$, $B = (u_1, 0)$, $C = (u_2, u_3)$, $O = (x_2, x_1)$, $H = (x_4, x_3)$, $D = (x_6, 0)$, $E = (x_8, x_7)$.

Teorema je dokazana metodom Wu-a.



Slika A.55: Primer 102 iz [1]

Slika A.56: Primer 103 iz [1]

Kompleksnost: 0.025s, 91 terma.
 Teorema je dokazana metodom Groebner-a.
 Kompleksnost: 0.969s, 345 terma.

Primer 74 *Primer 103 iz [1] (slika A.56). Prava paralelna sa bazom trapeza ABCD seče stranice i dijagonale trapeza u tačkama H, G, F i E. Dokazati da je: $EF \cong GH$.*

$A = (0, 0)$, $B = (u_1, 0)$, $D = (u_2, u_3)$, $C = (u_6, u_3)$, $H = (x_2, u_5)$, $E = (x_4, u_5)$, $G = (x_6, u_5)$, $F = (x_8, u_5)$.

Teorema je dokazana metodom Wu-a.

Kompleksnost: 0.003s, 6 terma.

Teorema je dokazana metodom Groebner-a.

Kompleksnost: 0.004s, 6 terma.

Primer 75 *Primer 104 iz [1] (slika A.57). Neka je E tačka na krugu opisanom oko jednakostraničnog trougla ABC. Ako je D presek pravih BC i AE, dokazati da je $BE \cdot CE = ED \cdot EA$.*

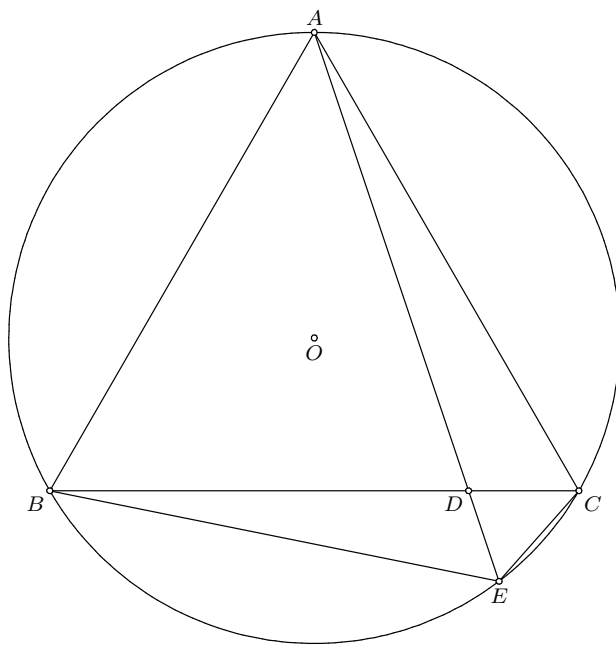
$B = (0, 0)$, $C = (u_1, 0)$, $A = (x_2, x_1)$, $A1 = (x_2, x_3)$, $O = (x_2, x_5)$, $E = (x_7, u_2)$, $D = (x_9, 0)$.

Teorema je dokazana metodom Wu-a.

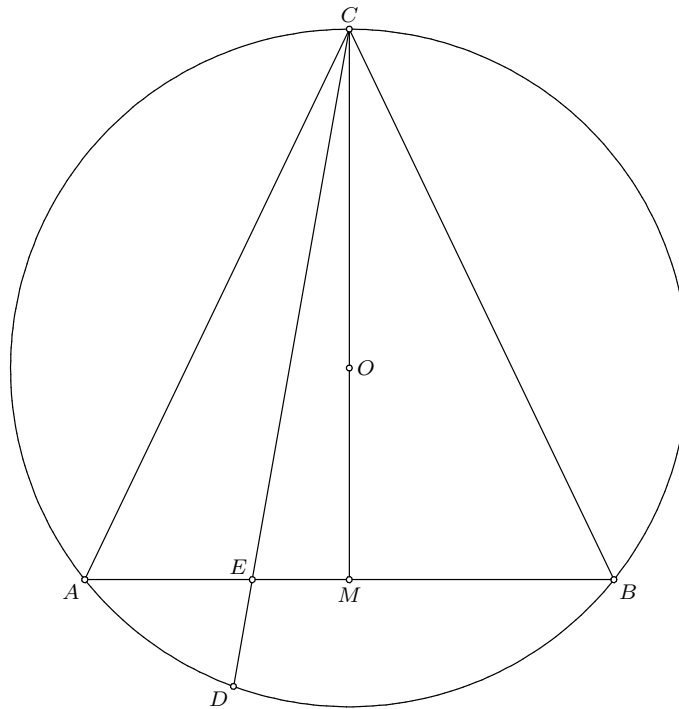
Kompleksnost: 0.025s, 45 terma.

Teorema je dokazana metodom Groebner-a.

Kompleksnost: 0.043s, 49 terma.



Slika A.57: Primer 104 iz [1]



Slika A.58: Primer 108 iz [1]

Primer 76 *Primer 108 iz [1] (slika A.58). Oko jednakokrakog trougla ABC ($AC \cong BC$) je opisan krug sa centrom O . Neka je D tačka na krugu i neka je $E = AB \cap CD$. Dokazati da je: $CA^2 = CE \cdot CD$.*

$A = (0, 0)$, $B = (u_1, 0)$, $X = (u_2, u_3)$, $O = (x_2, x_1)$, $M = (x_2, 0)$, $C = (x_2, x_5)$, $C1 = (x_2, x_7)$, $D = (x_9, u_4)$, $E = (x_{11}, 0)$.

Teorema je dokazana metodom Wu-a.

Kompleksnost: 0.011s, 28 terma.

Teorema je dokazana metodom Groebner-a.

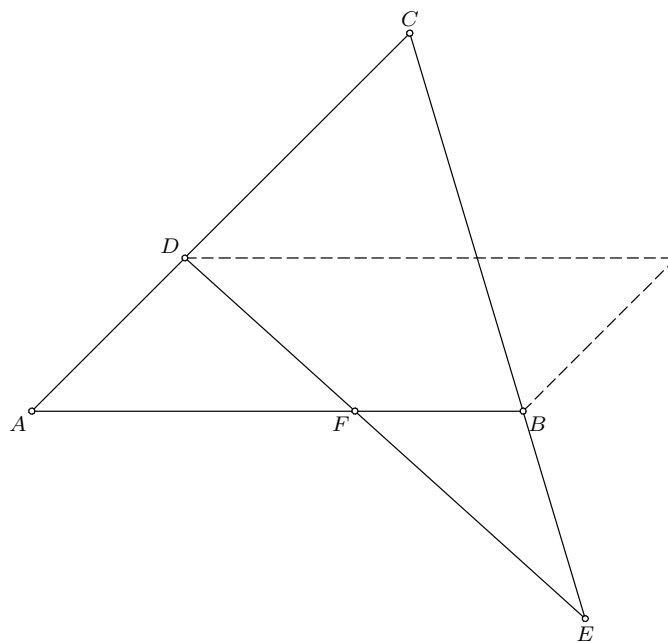
Kompleksnost: 0.138s, 206 terma.

Primer 77 *Primer 110 iz [1] (slika A.59). Na pravama AC i BD trougla ABC date su D i E takve da je $AD \cong BE$. Neka je $F = DE \cap AB$. Dokazati da je: $FD \cdot AC = EF \cdot BC$.*

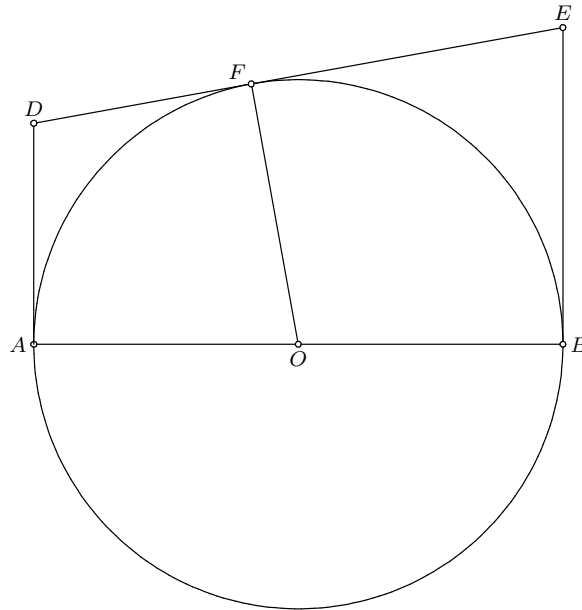
Konstrukcija je izvedena tako što su tačke A , B , C izabrane proizvoljno, D izabrana proizvoljno na pravoj AC . Zatim je konstruisan paralelogram ADD_1B i tačka E je određena kao presek kruga sa poluprečnikom BD_1 prave BC .

$A = (0, 0)$, $B = (u_1, 0)$, $C = (u_2, u_3)$, $D = (x_1, u_4)$, $D1 = (x_3, u_4)$, $E1 = (x_5, x_4)$, $E = (x_7, x_6)$, $F = (x_9, 0)$.

Teorema je dokazana metodom Wu-a.



Slika A.59: Primer 110 iz [1]



Slika A.60: Primer 114 iz [1]

Kompleksnost: 0.095s, 514 terma.

Teorema je dokazana metodom Groebner-a.

Kompleksnost: 0.100s, 514 terma.

Primer 78 *Primer 114 iz [1] (slika A.60). Na krugu sa prečnikom AB data je tačka F. Tangenta iz tačke F seče normale na pravu AB povučene iz tačaka A i B u tačkama D i E. Dokazati da je: $OA^2 = DF \cdot EF$.*

$A = (0, 0)$, $B = (u_1, 0)$, $O = (x_2, 0)$, $F = (x_3, u_2)$, $D = (0, x_4)$, $E = (u_1, x_6)$.

Teorema je dokazana metodom Wu-a.

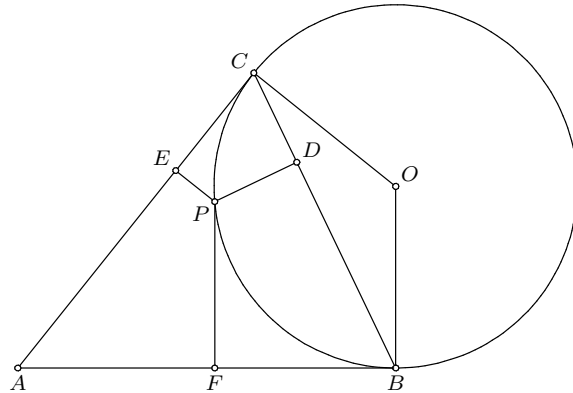
Kompleksnost: 0.019s, 37 terma.

Teorema je dokazana metodom Groebner-a.

Kompleksnost: 0.028s, 37 terma.

Primer 79 *Primer 117 iz [1] (slika A.61). Iz tačke A dve tangente su povučene na krug sa centrom O, dotičući krug u tačkama B i C. Iz proizvoljne tačke P na krugu, spuštene su normale PE, PF i PD na prave AC, AB i BC redom. Dokazati da je: $PD^2 = PE \cdot PF$.*

Konstrukcija je izvedena na sledeći način: izabrane su proizvoljne nekolinearne tačke A, B i X. Tačka O je određena kao presek normale iz B na AB



Slika A.61: Primer 117 iz [1]

i simetrale ugla BAX. Tačka C je podnožje normale iz O na AX. Tačka P je izabrana proizvoljno na krugu sa poluprečnikom OB, i E, F, D su podnožja normale iz P na AC, AB i BC.

$A = (0, 0)$, $B = (u_1, 0)$, $X = (u_2, u_3)$, $O = (u_1, x_1)$, $C = (x_4, x_3)$, $P = (x_5, u_4)$, $F = (x_5, 0)$, $E = (x_9, x_8)$, $D = (x_{11}, x_{10})$.

Teorema je dokazana metodom Wu-a.

Kompleksnost: 2.719s, 1921 terma.

Teorema nije dokazana metodom Groebner-a.

Izvršavanje prekinuto posle 21.022s.

Primer 80 *Primer 119 iz [1] (slika A.62). Neka je P tačka na krugu opisanom oko jednakostraničnog trougla ABC. Dokazati da među tri duži PA, PB i PC, jedna je jednaka sumi druge dve.*

Dovoljno je pokazati da je algebarska suma duži PA, PB i PC jednaka nuli.

$A = (0, 0)$, $B = (u_1, 0)$, $C = (x_2, x_1)$, $C1 = (x_2, x_3)$, $O = (x_2, x_5)$, $P = (x_7, u_2)$.

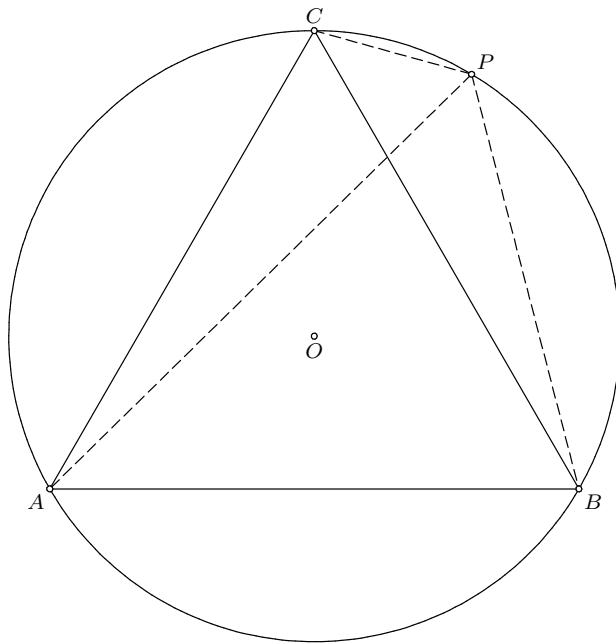
Teorema je dokazana metodom Wu-a.

Kompleksnost: 0.016s, 35 terma.

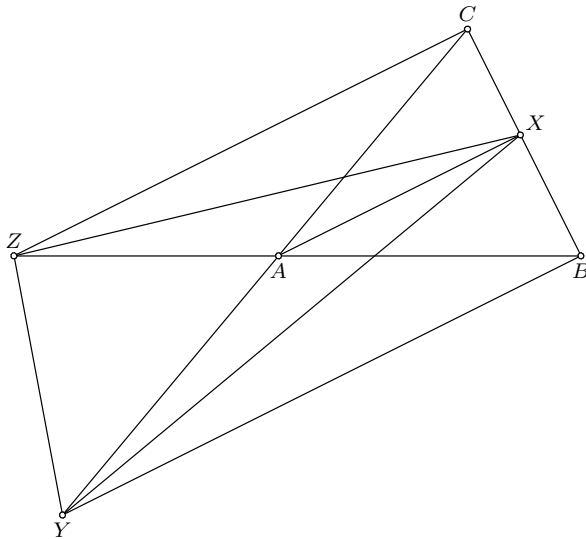
Teorema je dokazana metodom Groebner-a.

Kompleksnost: 0.030s, 35 terma.

Primer 81 *Primer 120 iz [1] (slika A.63). U ravni je dat trougao ABC. Iz tri temena trougla povučene su paralelne prave koje seku prave određene naspranim stranicama u tačkama X, Y, i Z. Dokazati da je površina trouglov XYZ dva puta veća od površine trougla ABC.*



Slika A.62: Primer 119 iz [1]



Slika A.63: Primer 120 iz [1]

Dovoljno je pokazati da je odnos orijentisanih površina trouglova ABC i XZY jednak $1 : 2$. Obratiti pažnju da tražimo orijentisanu površinu trougla XZY , a ne trougla XYZ . Ove dve veličine su suprotnog znaka. Sa slike se vidi da je orijentacija tačaka kod trouglova ABC i XZY ista, u oba slučaja tačke su raspoređene u smeru suprotnom od smera kretanja kazaljke na satu.

$A = (0, 0)$, $B = (u_1, 0)$, $C = (u_2, u_3)$, $X = (x_1, u_4)$, $Y = (x_3, x_2)$, $Z = (x_5, 0)$.

Teorema je dokazana metodom Wu-a.

Kompleksnost: 0.005s, 7 terma.

Teorema je dokazana metodom Groebner-a.

Kompleksnost: 0.004s, 7 terma.

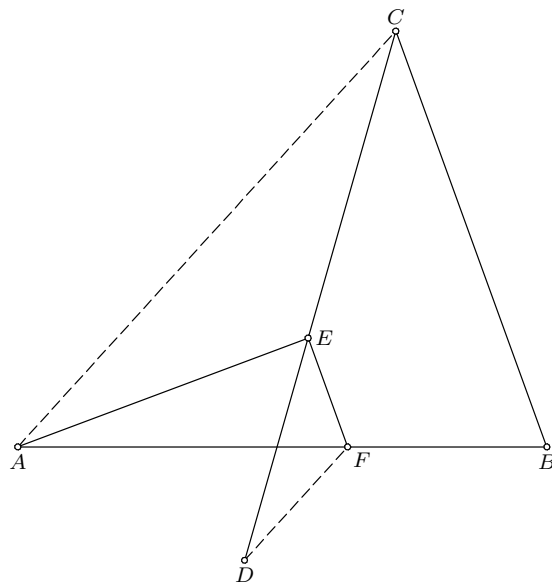
Primer 82 *Primer 121 iz [1] (slika A.64).* Date su četiri nekolinearne tačke A, B, C i D . Prava koja prolazi kroz tačku A i paralelna je sa pravom BD seče pravu AD u tački E . Prava koja prolazi kroz tačku E i paralelna je sa pravom BC seče pravu AB u tački F . Dokazati da je prava AC paralelna sa pravom DF .

$A = (0, 0)$, $B = (u_1, 0)$, $C = (u_2, u_3)$, $D = (u_4, u_5)$, $E = (x_2, x_1)$, $F = (x_4, 0)$.

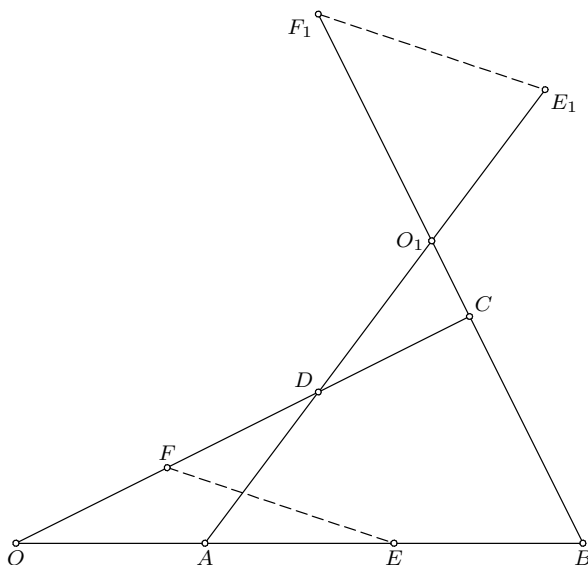
Teorema je dokazana metodom Wu-a.

Kompleksnost: 0.003s, 6 terma.

Teorema je dokazana metodom Groebner-a.



Slika A.64: Primer 121 iz [1]



Slika A.65: Primer 122 iz [1]

Kompleksnost: 0.005s, 6 terma.

Primer 83 *Primer 122 iz [1] (slika A.65). Stranice BC i CD četvorougla ABCD seku se u tački O, dok se stranice AD i BC seku u tački O₁. Na pravama OA, OC, O₁A, O₁C su redom konstruisane tačke E, F, E₁ i F₁ takve da je $\overline{OE} \cong \overline{AB}$, $\overline{OF} \cong \overline{DC}$, $\overline{O_1E_1} \cong \overline{AD}$, $\overline{O_1F_1} \cong \overline{BC}$. Dokazati da su prave EF i E₁F₁ paralelne.*

$A = (0, 0)$, $B = (u_1, 0)$, $C = (u_2, u_3)$, $D = (u_4, u_5)$, $O = (x_2, 0)$, $O_1 = (x_4, x_3)$, $E = (x_6, x_5)$, $F = (x_8, x_7)$, $E_1 = (x_{10}, x_9)$, $F_1 = (x_{12}, x_{11})$.

Teorema je dokazana metodom Wu-a.

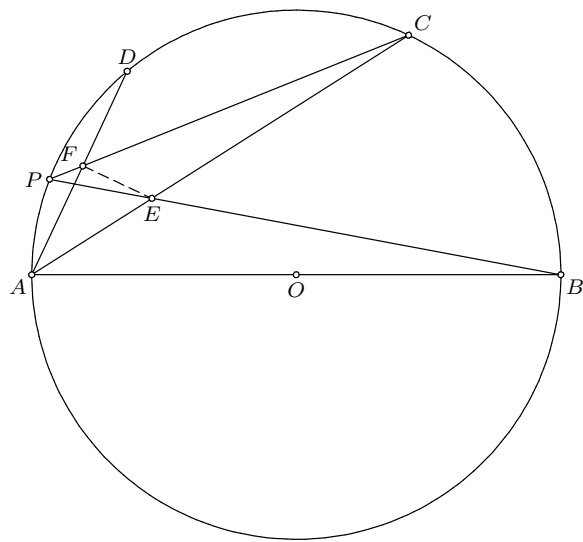
Kompleksnost: 0.013s, 32 terma.

Teorema je dokazana metodom Groebner-a.

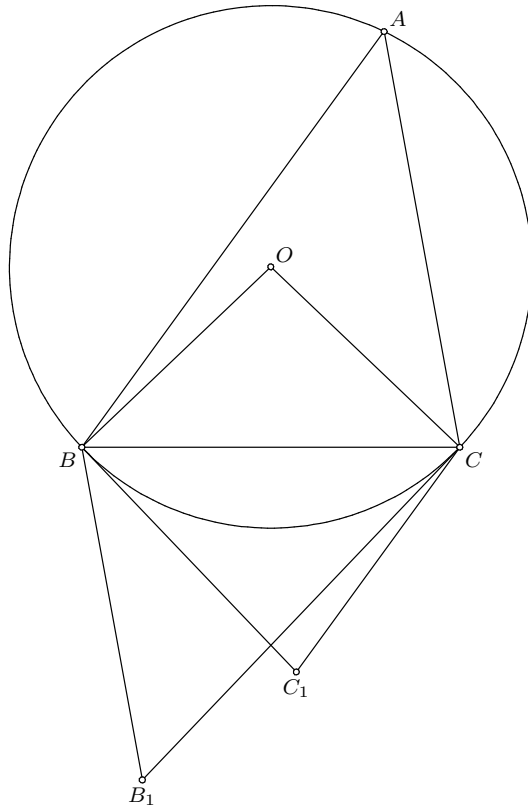
Kompleksnost: 0.072s, 165 terma.

Primer 84 *Primer 123 iz [1] (slika A.66). Neka je P proizvoljna tačka na polukrugu sa prečnikom AB. Ako su C i D tačke na polukrugu takve da su lukovi BC i CD jednaki, i ako su E i F presečne tačke pravih AC i PB, odnosno pravih AD i PC, dokazati da se prave EF i AD seku pod pravim uglom.*

$A = (0, 0)$, $B = (u_1, 0)$, $O = (x_2, 0)$, $D = (x_3, u_2)$, $C = (x_5, x_4)$, $C_1 = (x_7, x_6)$, $P = (x_8, u_3)$, $E = (x_{10}, x_9)$, $F = (x_{12}, x_{11})$.



Slika A.66: Primer 123 iz [1]



Slika A.67: Primer 126 iz [1]

Teorema je dokazana metodom Wu-a.

Kompleksnost: 0.364s, 830 terma.

Teorema nije dokazana metodom Groebner-a.

Izvršavanje prekinuto posle 21.002s.

Primer 85 *Primer 126 iz [1] (slika A.67).*

$B = (0, 0)$, $C = (u_1, 0)$, $A = (u_2, u_3)$, $O = (x_2, x_1)$, $B_1 = (x_4, x_3)$, $C_1 = (x_6, x_5)$.

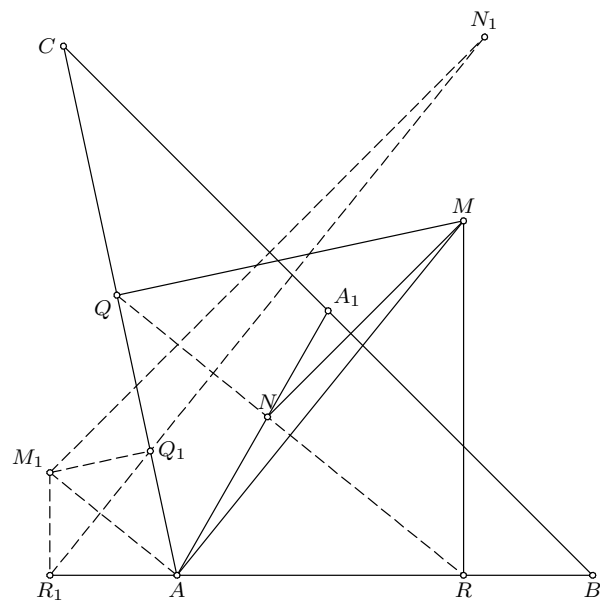
Teorema je dokazana metodom Wu-a.

Kompleksnost: 0.032s, 57 terma.

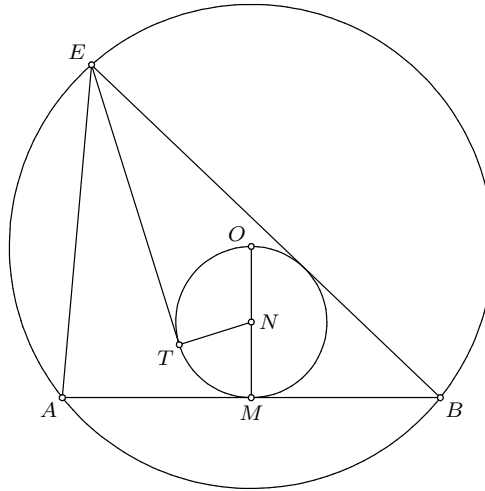
Teorema je dokazana metodom Groebner-a.

Kompleksnost: 1.156s, 140 terma.

Primer 86 *Primer 127 iz [1] (slika A.68).* *Dat je trougao ABC i tačka M na simetrali ugla BAC. Iz M su spuštene normale MQ i MR na prave AC i AB. Neka je N presek prave QR i prave AA₁, gde je A₁ središte stranice BC. Dokazati da je prava MN normalna na pravu BC.*



Slika A.68: Primer 127 iz [1]



Slika A.69: Primer 132 iz [1]

Teorema važi za unutrašnji ugao temena A , kao i za spoljašnji ugao (pogledati alternativnu sliku).

$A = (0, 0)$, $B = (u_1, 0)$, $C = (u_2, u_3)$, $X = (x_2, x_1)$, $M = (x_3, u_4)$, $Q = (x_5, x_4)$, $R = (x_3, 0)$, $A_1 = (x_9, x_8)$, $N = (x_{11}, x_{10})$.

Teorema je dokazana metodom Wu-a.

Kompleksnost: 0.034s, 78 terma.

Teorema nije dokazana metodom Groebner-a.

Izvršavanje prekinuto posle 21.071s.

Primer 87 Primer 132 iz [1] (slika A.69). Neka je M središte tetive AB kruga sa centrom O . Nad OM kao prečnikom nacrtan je novi krug sa centrom N . Neka je T proizvoljna tačka na novom krugu i neka tangenta iz T drugog kruga seče prvi krug u tački E . Dokazati da je: $AE^2 + BE^2 = 4ET^2$.

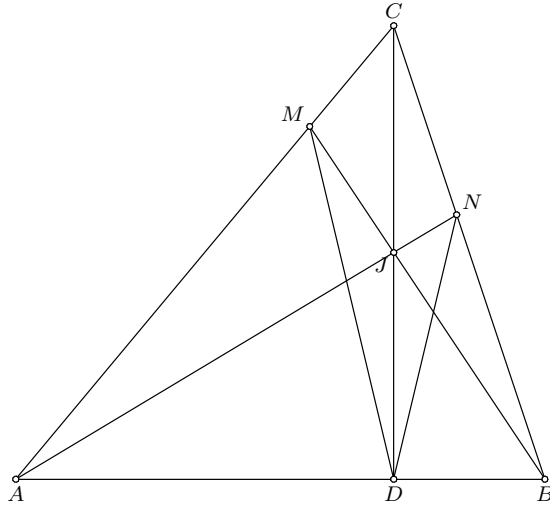
$A = (0, 0)$, $B = (u_1, 0)$, $X = (u_2, u_3)$, $O = (x_2, x_1)$, $M = (x_2, 0)$, $N = (x_2, x_5)$, $T = (x_7, u_4)$, $E = (x_9, x_8)$, $E1 = (x_{11}, x_{10})$.

Teorema je dokazana metodom Wu-a.

Kompleksnost: 0.047s, 118 terma.

Teorema nije dokazana metodom Groebner-a.

Izvršavanje prekinuto posle 21.015s.



Slika A.70: Primer 133 iz [1]

Primer 88 *Primer 133 iz [1] (slika A.70). Na stranicama AC i BC trougla ABC date su tačke M i N. Ako se prave BM i AN seku na visini AD trougla, dokazati da je CD simetrala ugla $\angle MDN$.*

Konstrukcija je izvedena tako što je izabrana proizvoljna tačka J na visini CD. Posledica ove teoreme ja da ako su H_a , H_b i H_c podnožja visina trougla ABC, tada je ortocentar H centar upisanog kruga trougla $H_aH_bH_c$.

$A = (0, 0)$, $B = (u_1, 0)$, $C = (u_2, u_3)$, $D = (u_2, 0)$, $J = (u_2, u_4)$, $M = (x_5, x_4)$, $N = (x_7, x_6)$.

Teorema je dokazana metodom Wu-a.

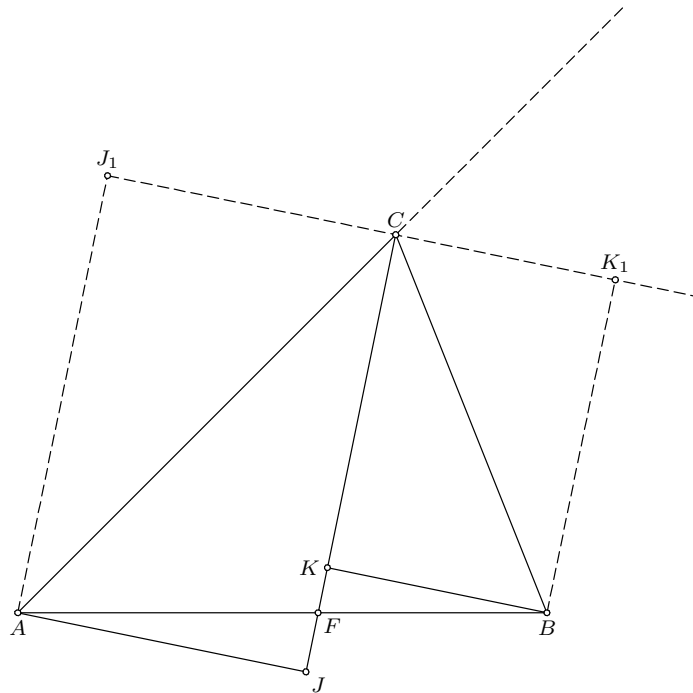
Kompleksnost: 0.005s, 6 terma.

Teorema je dokazana metodom Groebner-a.

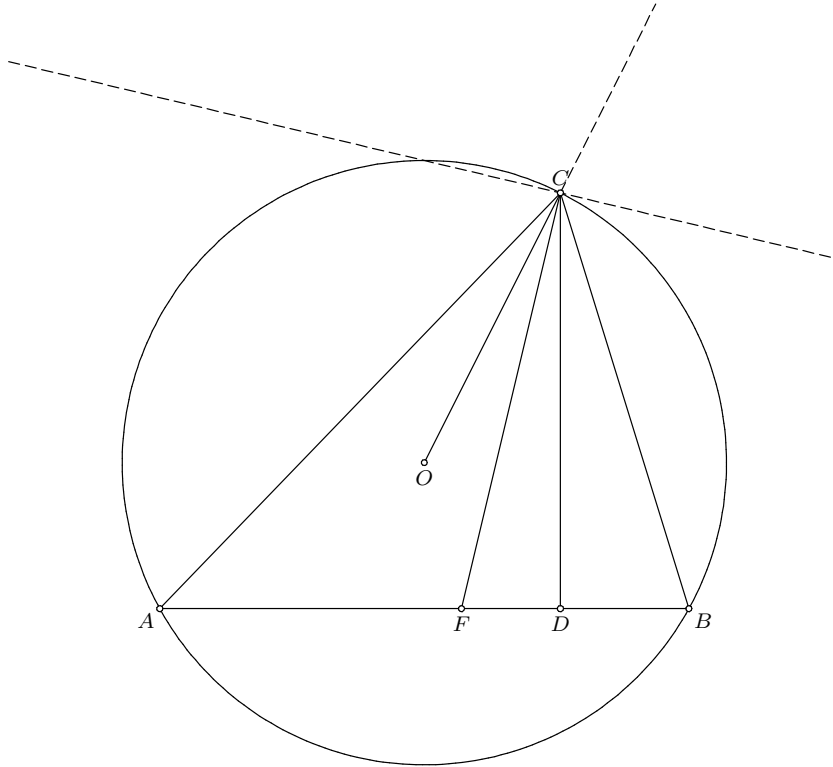
Kompleksnost: 0.007s, 10 terma.

Primer 89 *Primer 136 iz [1] (slika A.71). Dat je trougao ABC i neka je CF simetrala ugla $\angle ACB$ gde je F tačka na pravoj AB. Ako su K i J podnožja normala iz temena B i A na simetralu CF, pokazati da su tačke C, F, J i K harmonijski spregnute.*

Teorema važi i za unutrašnju simetralu ugla $\angle C$, kao i za spoljašnju simetralu. Pogledati alternativnu sliku.



Slika A.71: Primer 136 iz [1]



Slika A.72: Primer 137 iz [1]

$A = (0, 0)$, $B = (u_1, 0)$, $C = (u_2, u_3)$, $K = (x_2, x_1)$, $J = (x_4, x_3)$, $F = (x_6, 0)$.

Teorema je dokazana metodom Wu-a.

Kompleksnost: 0.034s, 85 terma.

Teorema nije dokazana metodom Groebner-a.

Izvršavanje prekinuto posle 21.018s.

Primer 90 *Primer 137 iz [1] (slika A.72). Simetrala ugla kod temena C, trougla ABC, je takođe simetrala ugla $\angle OCD$ gde je O centar opisanog kruga trougla ABC, a CD je visina istog trougla.*

Teorema važi i za simetralu unutrašnjeg ugla, kao i za simetralu spoljašnjeg ugla.

$A = (0, 0)$, $B = (u_1, 0)$, $C = (u_2, u_3)$, $O = (x_2, x_1)$, $F = (x_4, 0)$, $D = (u_2, 0)$.

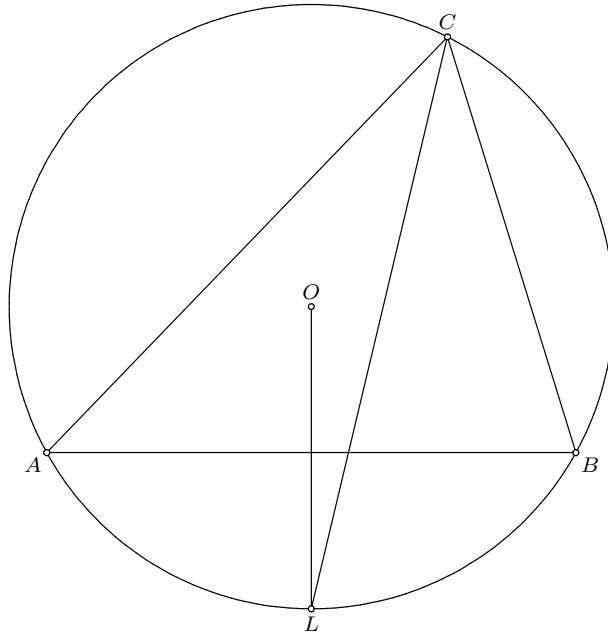
Teorema je dokazana metodom Wu-a.

Kompleksnost: 0.006s, 18 terma.

Teorema je dokazana metodom Groebner-a.

Kompleksnost: 0.012s, 55 terma.

Primer 91 *Primer 138 iz [1] (slika A.73). Simetrala ugla $\angle C$ trougla ABC polovi luk AB opisanog kruga trougla ABC.*



Slika A.73: Primer 138 iz [1]

Dokazano je ekvivalentno tvrdnje: ako je L središte luka AB , onda je CL simetrala ugla $\angle ACB$. Na taj način je izbegnut svodiv slučaj preseka simetrale ugla $\angle C$ i kruga opisanog oko trougla.

$A = (0, 0)$, $B = (u_1, 0)$, $C = (u_2, u_3)$, $O = (x_2, x_1)$, $L_1 = (x_2, x_3)$, $L = (x_2, x_5)$.

Teorema je dokazana metodom Wu-a.

Kompleksnost: 0.006s, 15 terma.

Teorema je dokazana metodom Groebner-a.

Kompleksnost: 0.011s, 20 terma.

Primer 92 *Primer 140 iz [1] (slika A.74). Proizvod dve stranice trougla je jednak proizvodu visine povučene iz trećeg temena i prečnika opisanog kruga.*

$A = (0, 0)$, $B = (u_1, 0)$, $C = (u_2, u_3)$, $O = (x_2, x_1)$, $F = (u_2, 0)$.

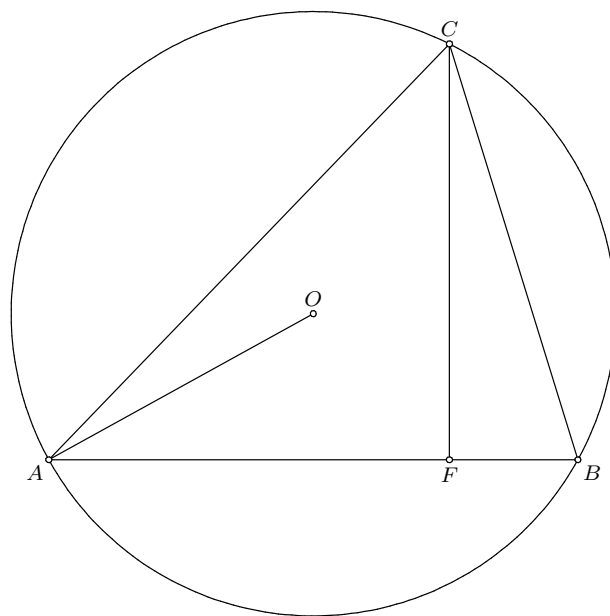
Teorema je dokazana metodom Wu-a.

Kompleksnost: 0.004s, 12 terma.

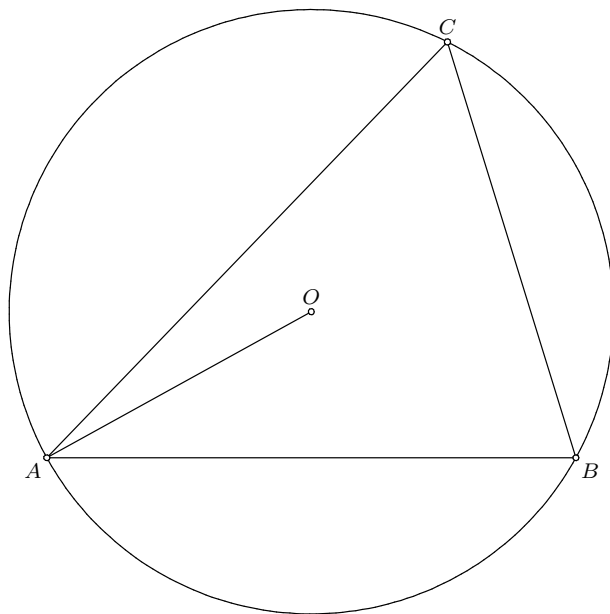
Teorema je dokazana metodom Groebner-a.

Kompleksnost: 0.007s, 29 terma.

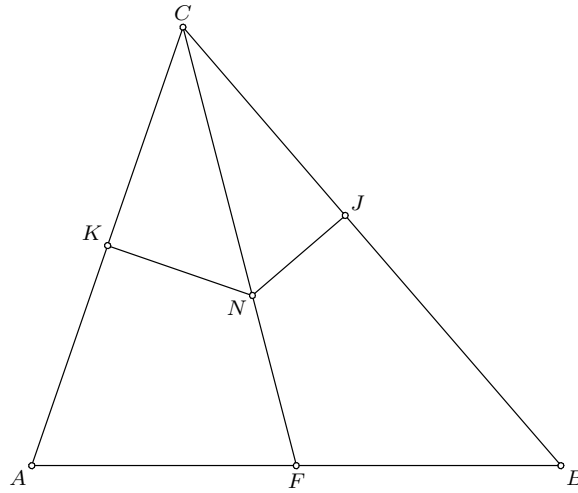
Primer 93 *Primer 141 iz [1] (slika A.75). Površina trougla je jednaka količniku proizvoda tri stranice i dvostrukog prečnika opisanog kruga, tj. $P_{\triangle ABC} = \frac{abc}{2R}$*



Slika A.74: Primer 140 iz [1]



Slika A.75: Primer 141 iz [1]



Slika A.76: Primer 145 iz [1]

$$A = (0, 0), B = (u_1, 0), C = (u_2, u_3), O = (x_2, x_1).$$

Teorema je dokazana metodom Wu-a.

Kompleksnost: 0.004s, 12 terma.

Teorema je dokazana metodom Groebner-a.

Kompleksnost: 0.007s, 29 terma.

Primer 94 *Primer 145 iz [1] (slika A.76). Dokazati da su rastojanja tačke na težišnoj liniji trougla od stranica trougla inverzno proporcionalna dvema stranicama trougla, odnosno: $NK : NJ = BC : AC$.*

$$A = (0, 0), B = (u_1, 0), C = (u_2, u_3), F = (x_2, 0), N = (x_3, u_4), K = (x_5, x_4), J = (x_7, x_6).$$

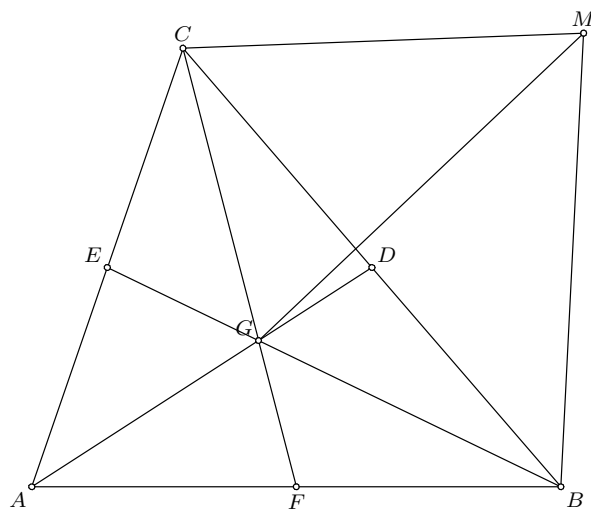
Teorema je dokazana metodom Wu-a.

Kompleksnost: 0.075s, 222 terma.

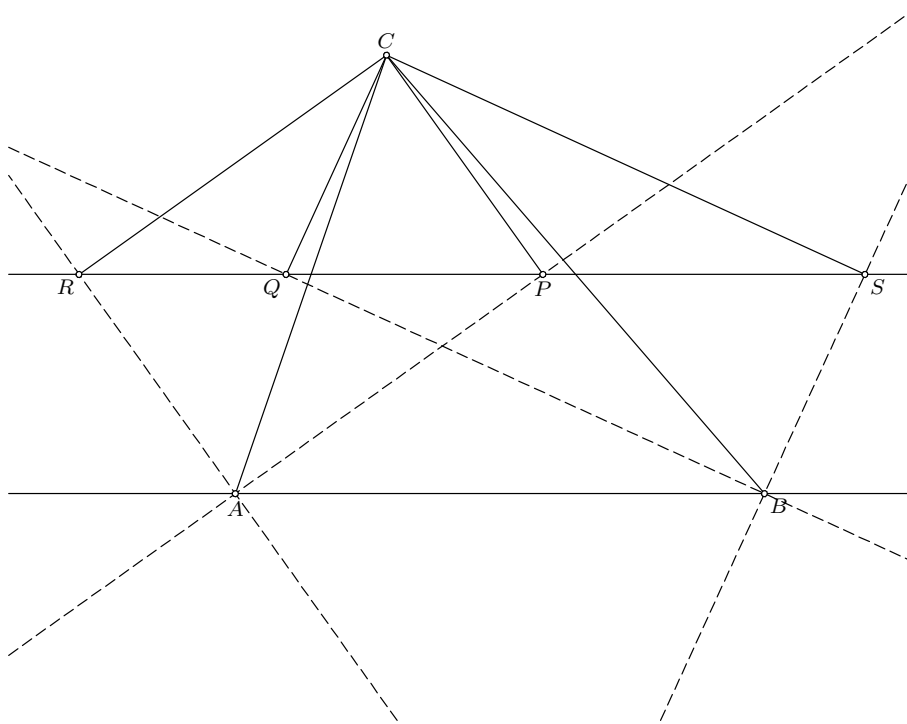
Teorema je dokazana metodom Groebner-a.

Kompleksnost: 0.082s, 222 terma.

Primer 95 *Primer 150 iz [1] (slika A.77). Neka je G težište trougla ABC i neka je M proizvoljna tačka u ravni. Dokazati da je: $3 \cdot MG^2 + AG^2 + BG^2 + CG^2 = AM^2 + BM^2 + CM^2$.*



Slika A.77: Primer 150 iz [1]



Slika A.78: Primer 152 iz [1]

$A = (0, 0)$, $B = (u_1, 0)$, $C = (u_2, u_3)$, $M = (u_4, u_5)$, $F = (x_2, 0)$, $E = (x_4, x_3)$, $D = (x_6, x_5)$, $G = (x_8, x_7)$.

Teorema je dokazana metodom Wu-a.

Kompleksnost: 0.063s, 197 terma.

Teorema je dokazana metodom Groebner-a.

Kompleksnost: 0.072s, 197 terma.

Primer 96 *Primer 152 iz [1] (slika A.78). Četiri podnožja normala spuštenih iz jednog temena trougla na četiri simetrale ugla preostala dva temena (dva unutrašnja i dva spoljašnja ugla) su kolinearna.*

Takođe, prava PQRS je paralelna sa pravom AB.

$A = (0, 0)$, $B = (u_1, 0)$, $C = (u_2, u_3)$, $P = (x_2, x_1)$, $Q = (x_4, x_3)$.

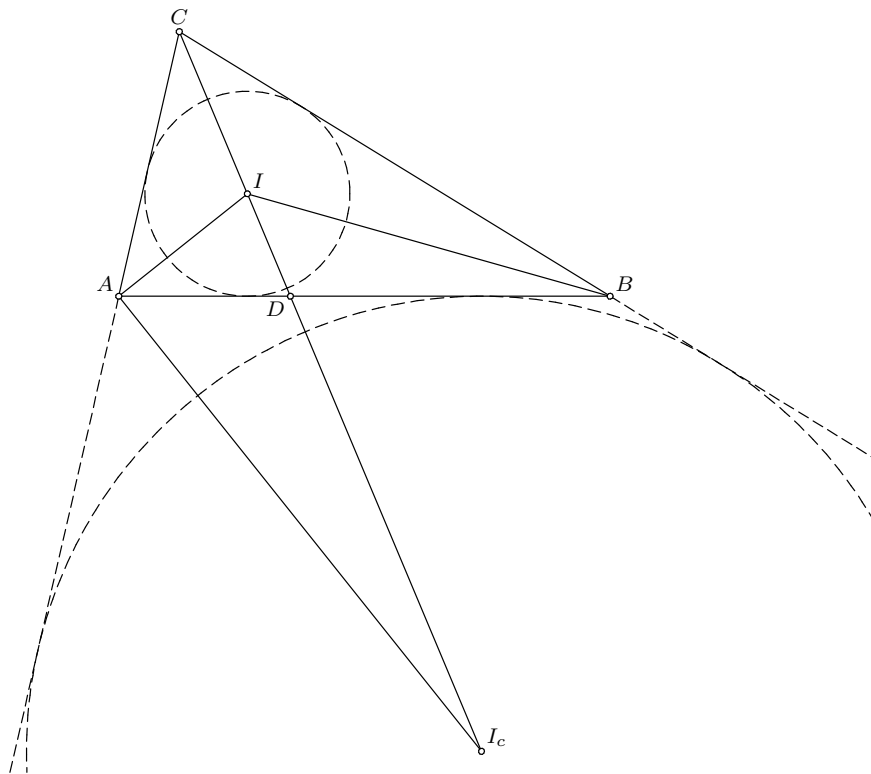
Teorema nije dokazana metodom Wu-a.

Krajnje svođenje nije rezultiralo nula polinomom!

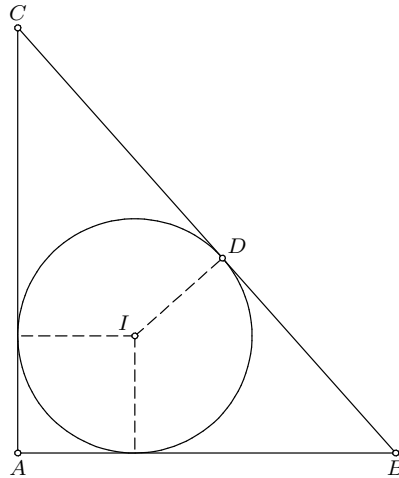
Teorema nije dokazana metodom Groebner-a.

Krajnje svođenje nije rezultiralo nula polinomom!

Primer 97 *Primer 155 iz [1] (slika A.79). Centar upisanog i centar ekterno upisanog kruga dele simetralu ugla na kojoj se nalaze u harmoničnom odnosu. Odnosno, tačke C, D, I i I_c su harmonijski spregnute.*



Slika A.79: Primer 155 iz [1]



Slika A.80: Primer 172 iz [1]

$A = (0, 0)$, $B = (u_1, 0)$, $C = (u_2, u_3)$, $I = (x_2, x_1)$, $I_c = (x_4, x_3)$, $D = (x_6, 0)$.

Teorema je dokazana metodom Wu-a.

Kompleksnost: 0.051s, 42 terma.

Teorema nije dokazana metodom Groebner-a.

Izvršavanje prekinuto posle 21.009s.

Primer 98 *Primer 172 iz [1] (slika A.80). Dokazati da je površina pravouglog trougla jednaka proizvodu dva segmenta na koje je podeljena hipotenuza tačkom dodira sa upisanim krugom.*

$A = (0, 0)$, $B = (u_1, 0)$, $X = (u_2, u_3)$, $C = (0, x_1)$, $I = (x_4, x_3)$, $D = (x_6, x_5)$.

Teorema je dokazana metodom Wu-a.

Kompleksnost: 0.065s, 106 terma.

Teorema nije dokazana metodom Groebner-a.

Izvršavanje prekinuto posle 21.034s.

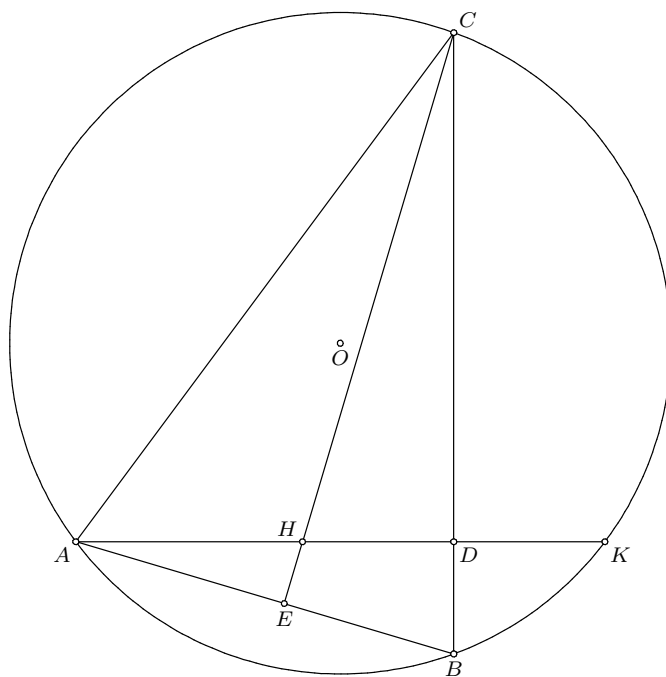
Primer 99 *Primer 174 iz [1] (slika A.81). Visina AD trougla ABC je produžena i seče opisani krug trougla u tački K. Ako je H ortocentar trougla ABC, dokazati da tačka D polovi duž HK.*

$A = (0, 0)$, $K = (u_1, 0)$, $D = (u_5, 0)$, $X = (u_3, u_4)$, $O = (x_3, x_2)$, $C = (u_5, x_4)$, $B = (u_5, x_6)$, $E = (x_9, x_8)$, $H = (x_{11}, 0)$.

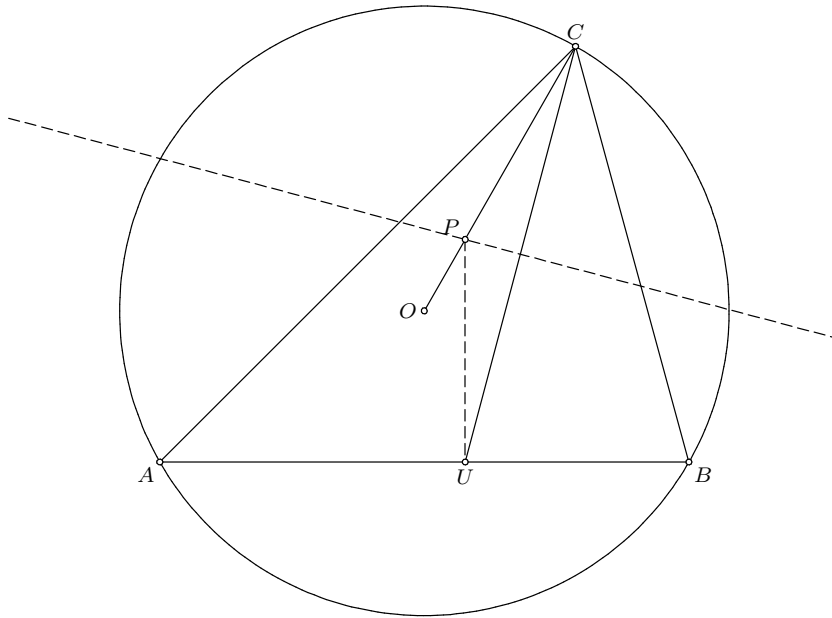
Teorema je dokazana metodom Wu-a.

Kompleksnost: 0.007s, 6 terma.

Teorema nije dokazana metodom Groebner-a.



Slika A.81: Primer 174 iz [1]



Slika A.82: Primer 219 iz [1]

Krajnje svođenje nije rezultiralo nula polinomom!

Primer 100 *Primer 219 iz [1] (slika A.82). U trouglu ABC, O je centar opisanog kruga, a U je presek simetrane ugla $\angle ACB$ i prave AB. Dokazati da su prave CO, simetrana duži CU i normala iz U na pravu AB konkurentne.*

Ekvivalentno tvrđenje je da ako je P presek prave AO i simetrane duži CU, onda je prava PU normalna sa pravom AB.

$A = (0, 0)$, $B = (u_1, 0)$, $C = (u_2, u_3)$, $O = (x_2, x_1)$, $U = (x_4, 0)$, $P = (x_6, x_5)$.

Teorema je dokazana metodom Wu-a.

Kompleksnost: 0.066s, 32 terma.

Teorema je dokazana metodom Groebner-a.

Kompleksnost: 0.669s, 671 terma.

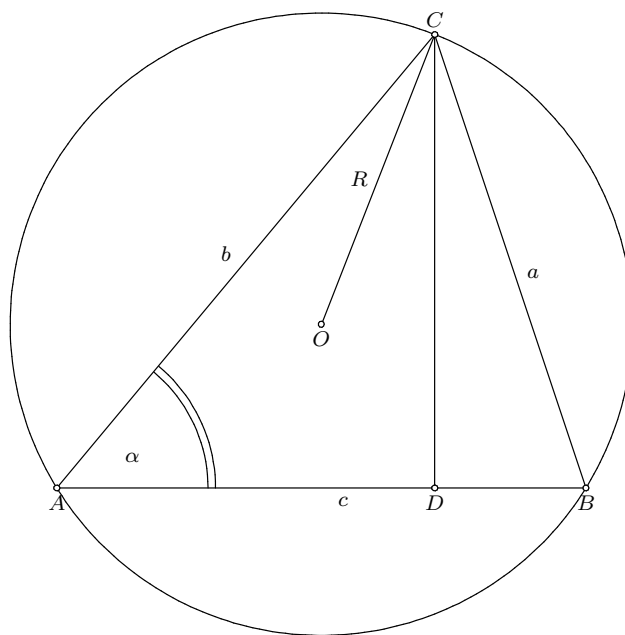
Primer 101 *Sinusna teorema (slika A.83). Dokazati da je u proizvoljnom trouglu odnos stranice i prečnika opisanog kruga jednak sinusnu naspramnog ugla, odnosno: $\frac{a}{2R} = \sin \alpha$*

$$\sin \alpha = \frac{AD}{AC}$$

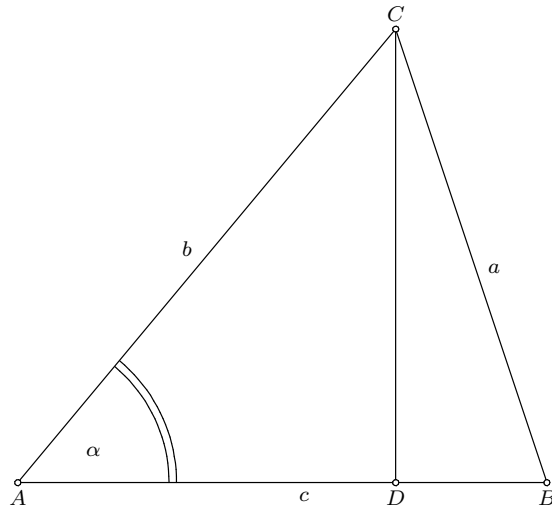
$A = (0, 0)$, $B = (u_1, 0)$, $C = (u_2, u_3)$, $O = (x_2, x_1)$, $D = (u_2, 0)$.

Teorema je dokazana metodom Wu-a.

Kompleksnost: 0.003s, 11 terma.



Slika A.83: Sinusna teorema



Slika A.84: Kosinusna teorema

Teorema je dokazana metodom Groebner-a.
Kompleksnost: 0.003s, 11 terma.

Primer 102 Kosinusna teorema (slika A.84). $c^2 + b^2 - 2bc \cos \alpha = a^2$

$$\cos \alpha = \frac{CD}{AC}$$

$$A = (0, 0), B = (u_1, 0), C = (u_2, u_3), D = (u_2, 0).$$

Teorema je dokazana metodom Wu-a.

Kompleksnost: 0.002s, 0 terma.

Teorema je dokazana metodom Groebner-a.

Kompleksnost: 0.002s, 0 terma.

Primer 103 Ojlerova formula (slika A.85). Dokazati da je $d^2 = R(R - 2r)$ gde su R i r poluprečnici opisanog i upisanog kruga trougla, a d rastojanje između njih.

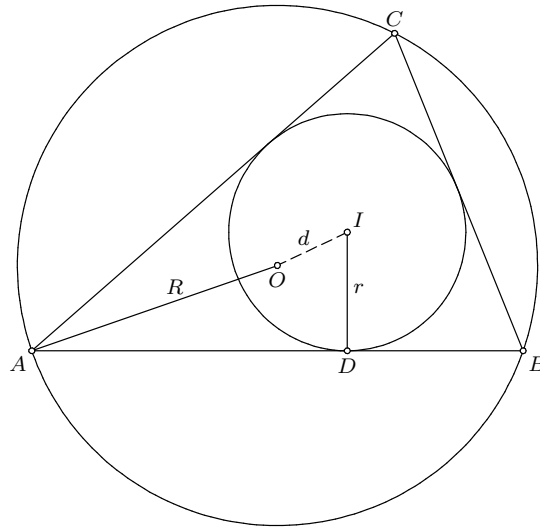
$$A = (0, 0), B = (u_1, 0), C = (u_2, u_3), I = (x_2, x_1), O = (x_4, x_3), D = (x_2, 0).$$

Teorema je dokazana metodom Wu-a.

Kompleksnost: 0.170s, 194 terma.

Teorema je dokazana metodom Groebner-a.

Kompleksnost: 2.459s, 815 terma.



Slika A.85: Ojlerova formula

Primer 104 Brahmaguptina teorema (slika A.86). Četvorougao $ABCD$ čije dijagonale grade prav ugao je upisan u krug. Dokazati da prava koja prolazi kroz presek dijagonala i normalna je na jednu stranicu četvorougla, polovi suprotnu stranicu.

Da bi se izbegao slučaj svodivosti u koji bi dokazivač upao ukoliko bi pokušao da odredi presečne tačke prave i kruga (do svodivosti dolazi zato što presek nije jednoznačan), polazeći od tačaka B , T i O , ostala temena četvorougla su konstruisana malo dužim, ali jednoznačnim putem.

$B = (0, 0)$, $T = (u_1, 0)$, $O = (u_2, u_3)$, $X = (u_2, 0)$, $D = (x_4, 0)$, $A = (u_1, x_5)$, $C1 = (u_1, x_7)$, $Y = (u_1, u_3)$, $C = (u_1, x_{11})$, $P = (x_{14}, x_{13})$, $Q = (x_{16}, x_{15})$.

Teorema je dokazana metodom Wu-a.

Kompleksnost: 0.006s, 5 terma.

Teorema nije dokazana metodom Groebner-a.

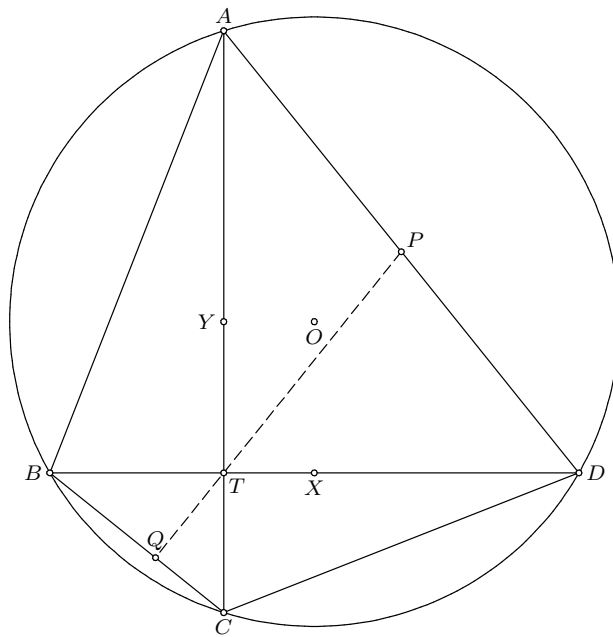
Izvršavanje prekinuto posle 21.016s.

Primer 105 Vivianijeva teorema (slika A.87). Iz tačke P unutar trougla jednakostraničnog ABC spuštene su normale na stranice trougla. Dokazati da je suma ove tri normale jednaka visini trougla ABC .

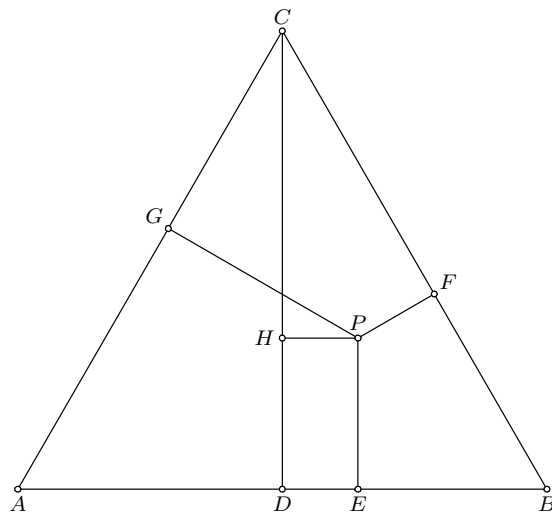
Dovoljno je dokazati da je algebarska suma duži CH , PF i PG jednaka nuli. Pogledati sliku.

$A = (0, 0)$, $B = (u_1, 0)$, $P = (u_2, u_3)$, $C = (x_2, x_1)$, $C1 = (x_2, x_3)$, $D = (x_2, 0)$, $G = (x_8, x_7)$, $F = (x_{10}, x_9)$, $E = (u_2, 0)$, $H = (x_2, u_3)$.

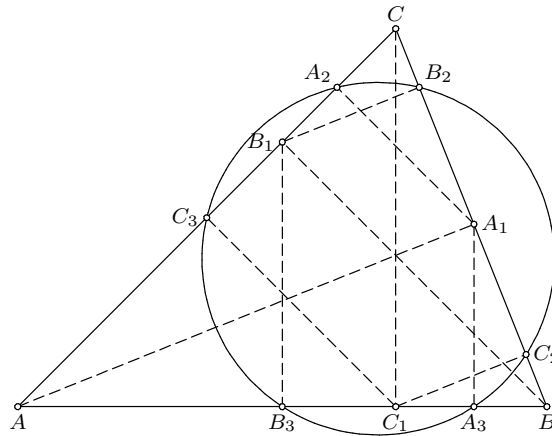
Teorema je dokazana metodom Wu-a.



Slika A.86: Brahmaguptina teorema



Slika A.87: Vivianijeva teorema



Slika A.88: Krug šest tačkaka.

Kompleksnost: 2.616s, 2000 terma.

Teorema nije dokazana metodom Groebner-a.

Krajnje svođenje nije rezultiralo nula polinomom!

Primer 106 *Krug šest tačkaka.* (slika A.88). U ravni je dat trougao ABC . Neka su A_1 , B_1 i C_1 podnožja visina trougla povučene iz temena A , B i C redom. Neka su dalje A_2 i A_3 podnožja normala spuštenih iz tačke A_1 na prave AC i AB . Na sličan način su konstruisane i tačke B_2 , B_3 , C_2 i C_3 . Dokazati da se šest tačkaka A_2 , A_3 , B_2 , B_3 , C_2 i C_3 nalaze na istom krugu.

$A = (0, 0)$, $B = (u_1, 0)$, $C = (u_2, u_3)$, $A_1 = (x_2, x_1)$, $B_1 = (x_4, x_3)$, $C_1 = (u_2, 0)$, $C_2 = (x_8, x_7)$, $C_3 = (x_{10}, x_9)$, $A_2 = (x_{12}, x_{11})$, $A_3 = (x_2, 0)$, $B_2 = (x_{16}, x_{15})$, $B_3 = (x_4, 0)$, $O = (x_{20}, x_{19})$.

Teorema je dokazana metodom Wu-a.

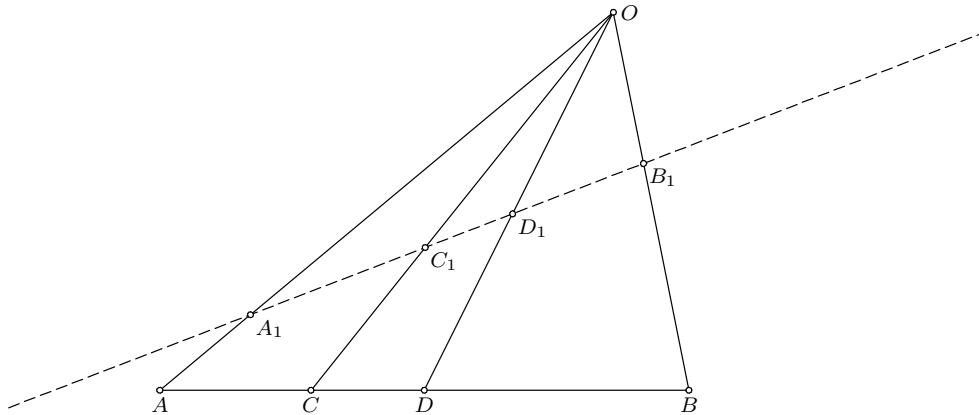
Kompleksnost: 0.258s, 355 terma.

Teorema nije dokazana metodom Groebner-a.

Izvršavanje prekinuto posle 21.011s.

Primer 107 *Harmonijska spregnutost* (slika A.89). Harmonijska spregnutost tačkaka ostaje ista nakon projekcije.

$A = (0, 0)$, $C = (u_1, 0)$, $D = (u_8, 0)$, $B = (u_9, 0)$, $O = (u_4, u_5)$, $A_1 = (x_3, u_6)$, $B_1 = (x_4, u_7)$, $C_1 = (x_6, x_5)$, $D_1 = (x_8, x_7)$.



Slika A.89: Harmonijska spregnutost

Teorema je dokazana metodom Wu-a.

Kompleksnost: 0.031s, 100 terma.

Teorema je dokazana metodom Groebner-a.

Kompleksnost: 0.025s, 100 terma.

Primer 108 *Leptir teorema (slika A.90). Date su četiri tačke na krugu k sa centrom O , to su P_1, P_2, P_3 i P_4 . Neka je M presek pravih P_1P_3 i P_2P_4 . Neka je prava l normala iz tačke M na pravu OM i neka su X i Y preseoci prave l sa pravama P_2P_3 i P_1P_4 redom. Dokazati da je M središte duži XY .*

Pošto su X, Y i M na istoj pravoj, dovoljno je dokazati da je odnos paralelnih duži \overline{XM} i \overline{MY} jednak 1.

$P_1 = (0, 0), O = (u_1, 0), P_2 = (x_1, u_2), P_3 = (x_2, u_3), P_4 = (x_3, u_4), M = (x_5, x_4), X = (x_7, x_6), Y = (x_9, x_8)$.

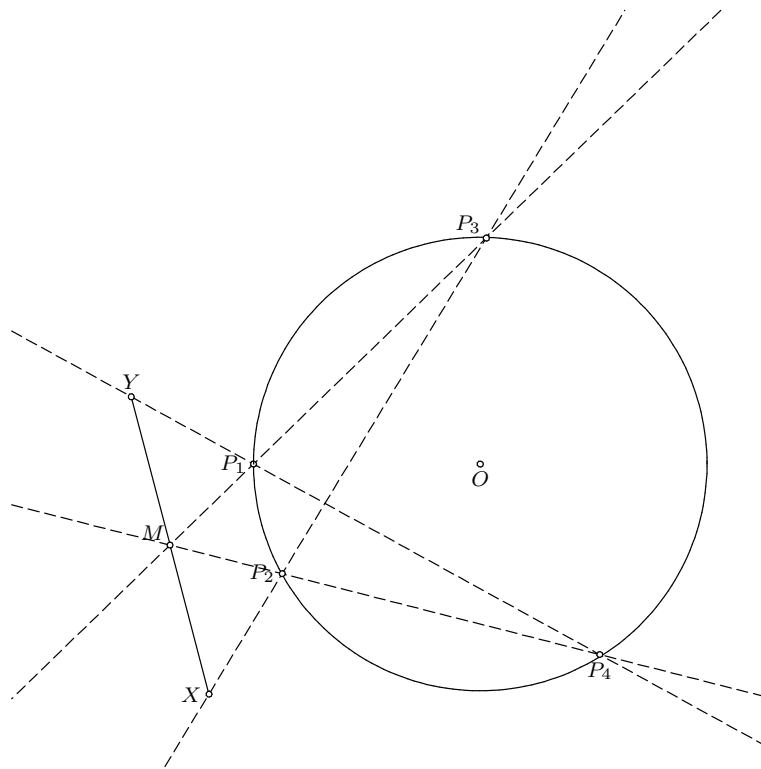
Teorema je dokazana metodom Wu-a.

Kompleksnost: 3.895s, 4561 terma.

Teorema nije dokazana metodom Groebner-a.

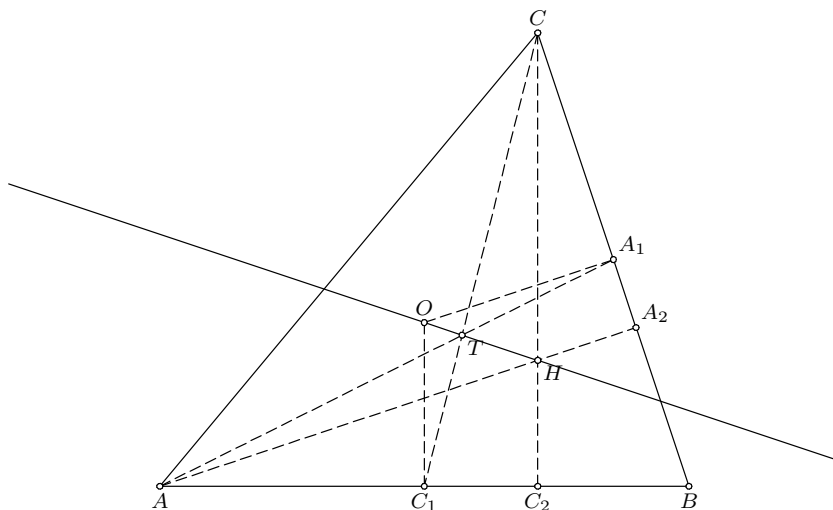
Izvršavanje prekinuto posle 21.065s.

Primer 109 *Krug osam tačaka (slika A.91). U ravni je dat četvorougao $ABCD$ gde su dijagonale AD i BC pod pravim uglom. Neka su A_1, B_1, C_1 i D_1 središta stranica AB, BC, CD i DA redom. Neka su dalje A_2, B_2, C_2 i D_2 normale spuštene iz A_1, B_1, C_1 i D_1 na naspramne stranice CD, DA, AB i BC redom. Dokazati da su osam tačaka $A_1, B_1, C_1, D_1, A_2, B_2, C_2$ i D_2 sve nalaze na istom krugu.*



Slika A.90: Leptir teorema

Slika A.91: Krug osam tačaka



Slika A.92: Ojlerova prava

Neka je krug k sa prečnikom A_1C_1 . Dovoljno je dokazati da tačke B_1 , D_1 i A_2 pripadaju krugu k .

$A = (0, 0)$, $C = (u_1, 0)$, $B = (u_2, u_3)$, $D = (u_2, u_4)$, $A_1 = (x_3, x_2)$, $B_1 = (x_5, x_4)$, $C_1 = (x_7, x_6)$, $D_1 = (x_9, x_8)$, $A_2 = (x_{11}, x_{10})$, $B_2 = (x_{13}, x_{12})$, $C_2 = (x_{15}, x_{14})$, $D_2 = (x_{17}, x_{16})$, $O = (x_{19}, x_{18})$.

Teorema je dokazana metodom Wu-a.

Kompleksnost: 0.102s, 168 terma.

Teorema nije dokazana metodom Groebner-a.

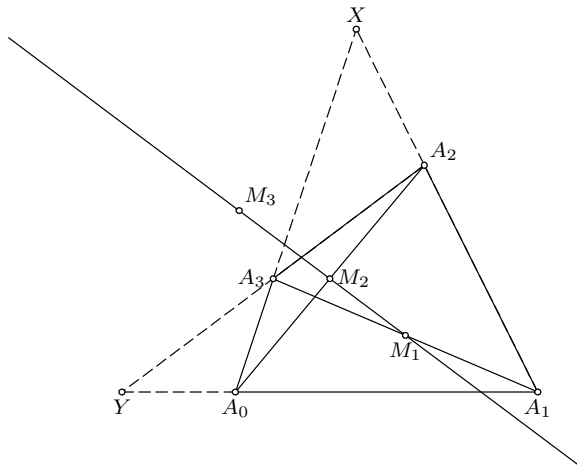
Izvršavanje prekinuto posle 21.187s.

Primer 110 Ojlerova prava (slika A.92). Dokazati da se ortocentar, težište i centar opisanog kruga trougla nalaze na istoj pravoj.

Biće dokazano opštije tvrđenje. Tačke se nalaze na istoj pravoj, težište je između ortocentra i centra opisanog kruga i deli tu duž u odnosu 2 : 1.

$A = (0, 0)$, $B = (u_1, 0)$, $C = (u_2, u_3)$, $C_1 = (x_2, 0)$, $A_1 = (x_4, x_3)$, $T = (x_6, x_5)$, $O = (x_8, x_7)$, $C_2 = (u_2, 0)$, $A_2 = (x_{12}, x_{11})$, $H = (x_{14}, x_{13})$.

Teorema je dokazana metodom Wu-a.



Slika A.93: Gaussova prava

Kompleksnost: 0.028s, 40 terma.

Teorema je dokazana metodom Groebner-a.

Kompleksnost: 0.274s, 157 terma.

Primer 111 *Gaussova prava (slika A.93).* Dat je četvorougao $A_0A_1A_2A_3$. Neka je X presek pravih A_0A_3 i A_1A_2 i neka je Y presek pravih A_0A_1 i A_2A_3 . Neka su M_1 , M_2 i M_3 središta duži A_1A_3 , A_0A_2 i XY redom. Dokazati da su tačke M_1 , M_2 i M_3 kolinearne.

$A_0 = (0, 0)$, $A_1 = (u_1, 0)$, $A_2 = (u_2, u_3)$, $A_3 = (u_4, u_5)$, $X = (x_2, x_1)$, $Y = (x_4, 0)$, $M_1 = (x_6, x_5)$, $M_2 = (x_8, x_7)$, $M_3 = (x_{10}, x_9)$.

Teorema je dokazana metodom Wu-a.

Kompleksnost: 1.324s, 1744 terma.

Teorema nije dokazana metodom Groebner-a.

Izvršavanje prekinuto posle 22.252s.

Primer 112 *Uglovi nad istom tetivom (slika A.94).* Dokazati da su svi uglovi nad istom tetivom jednaki ili se dopunjuju do opruženog ugla.

$A = (0, 0)$, $B = (u_1, 0)$, $X = (u_2, u_3)$, $O = (x_2, x_1)$, $C = (x_3, u_4)$, $D = (x_4, u_5)$.

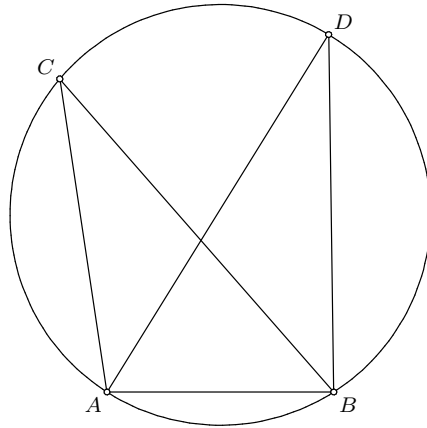
Teorema je dokazana metodom Wu-a.

Kompleksnost: 0.004s, 6 terma.

Teorema je dokazana metodom Groebner-a.

Kompleksnost: 0.004s, 6 terma.

Primer 113 *Primer 20 iz [5] (slika A.95).* U ravni je dat trougao ABC sa težištem T . Kroz proizvoljnu tačku X povučena je prava TX . Dokazati da je zbir rastojanja dva temena od prave TX jednak rastojanju trćeg temena.



Slika A.94: Uglovi nad istom tetivom

Obratiti pažnju na sliku koja je izabrana tako da se maksimalno pojednostavi proces dokazivanja. Slika je konstruisana na način da najveći broj tačaka leži na pravoj koja je paralelna koordinatnoj osi. Pažljivom analizom redosleda konstrukcija tačaka, iskusniji čitalac može rekonstruisati korake konstrukcije.

$A = (0, 0)$, $C = (u_1, 0)$, $T = (u_2, u_3)$, $A_1 = (x_2, x_1)$, $C_1 = (x_4, x_3)$, $B = (x_6, x_5)$, $X = (u_4, u_5)$, $D = (x_8, x_7)$, $E = (x_{10}, x_9)$, $F = (x_{12}, x_{11})$.

Teorema je dokazana metodom Wu-a.

Kompleksnost: 0.757s, 1211 terma.

Teorema nije dokazana metodom Groebner-a.

Krajnje svodenje nije rezultiralo nula polinomom!

Primer 114 Primer 22 iz [5] (slika A.96). Dat je paralelogram $ABCD$. Tačka N je konstruisana kao presek prave povučene iz C paralelne sa dijagonalom BD i prave povučene iz A normalne na dijagonalu BD . Prave AN i BN seku pravu CD u tačkama P i Q . Dokazati da je Q središte duži CP .

$A = (0, 0)$, $B = (u_1, 0)$, $C = (u_2, u_3)$, $D = (x_2, u_3)$, $N = (x_4, x_3)$, $P = (x_6, u_3)$, $Q = (x_8, u_3)$.

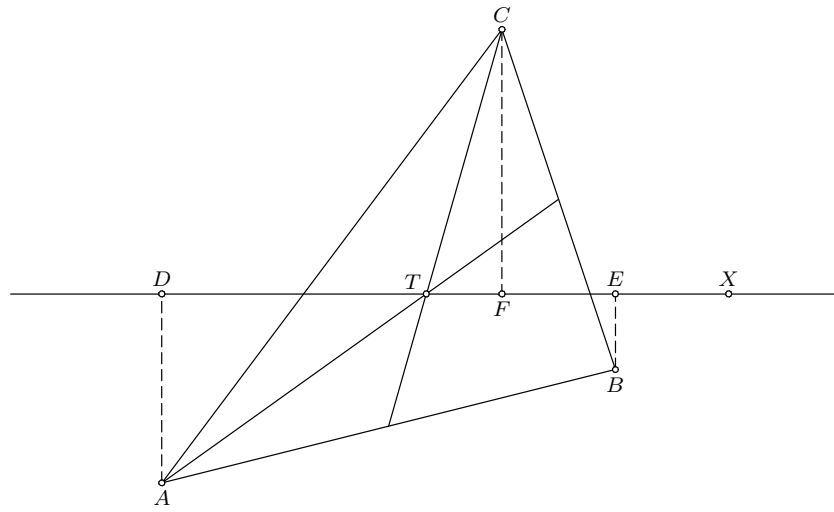
Teorema je dokazana metodom Wu-a.

Kompleksnost: 0.010s, 24 terma.

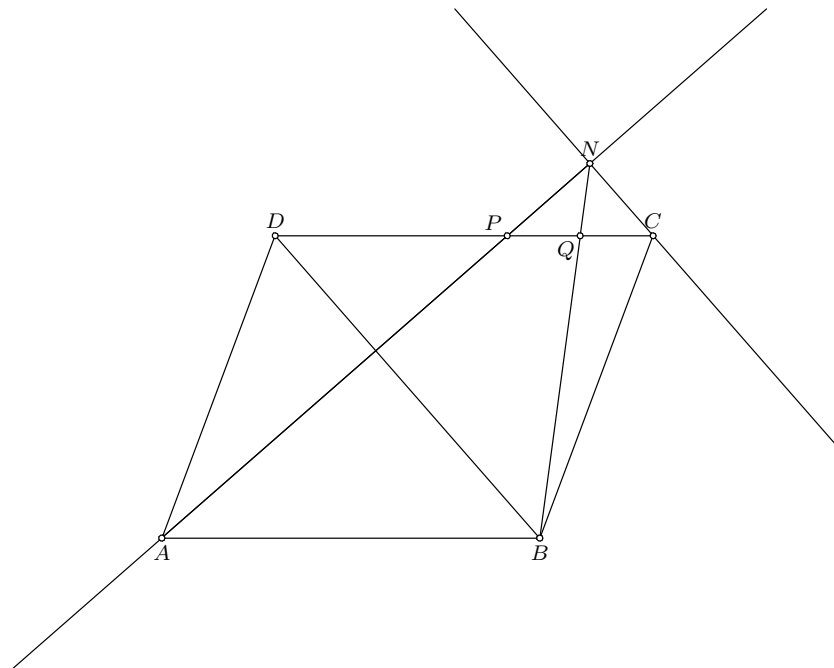
Teorema je dokazana metodom Groebner-a.

Kompleksnost: 0.043s, 28 terma.

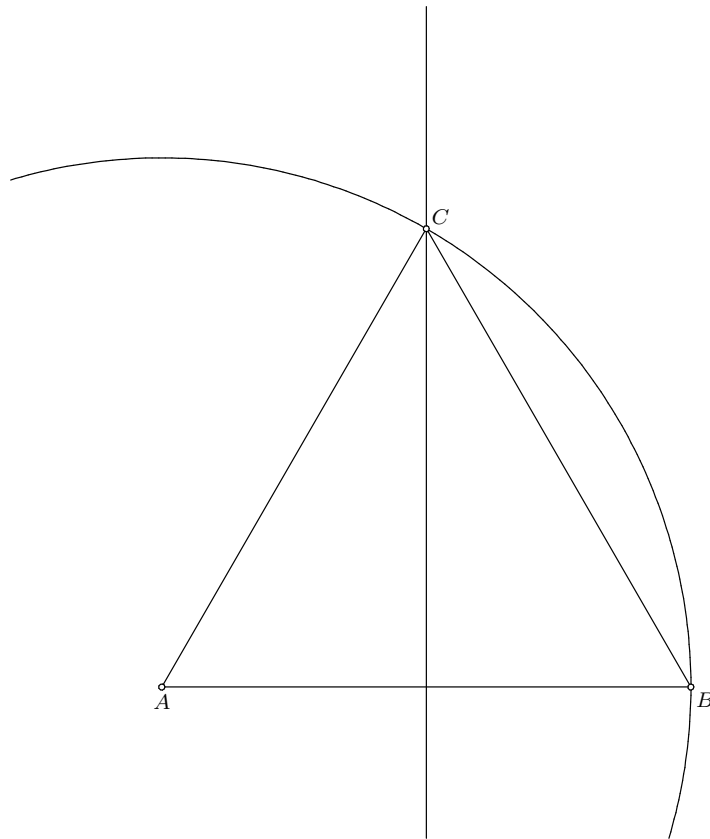
Primer 115 Problem u jednakokraničnom pravouglom trouglu (slika A.97). Dat je jednakokranični pravougli trougao ABC sa pravim uglom kod temena



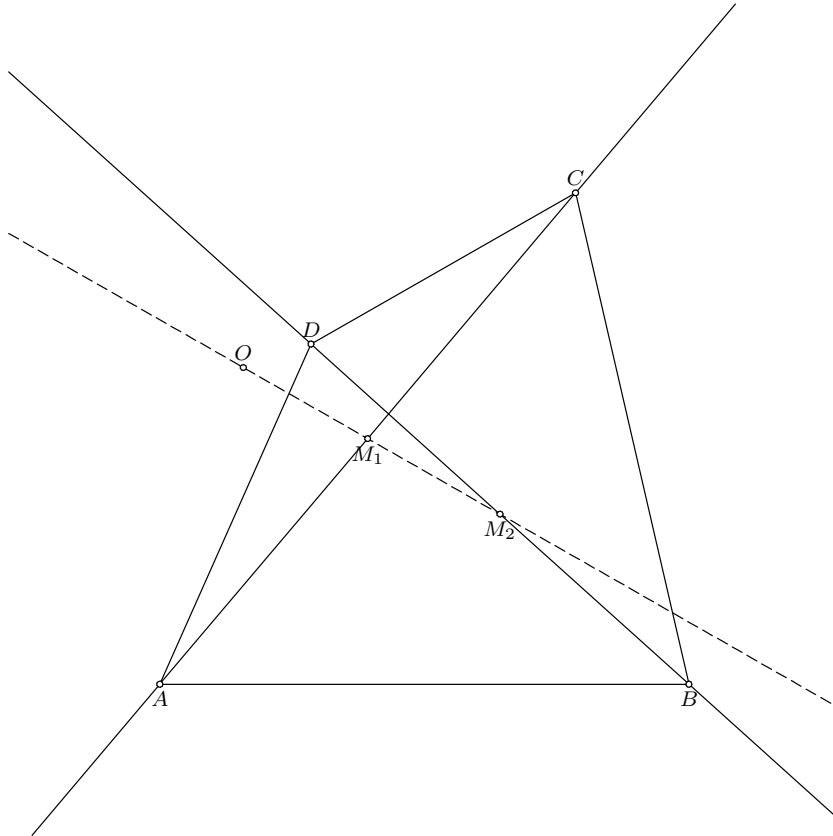
Slika A.95: Primer 20 iz [5]



Slika A.96: Primer 22 iz [5]



Slika A.98: Konstrukcija jednakostraničnog trougla



Slika A.99: Leon-An teorema

Kompleksnost: 0.002s, 3 terma.

Primer 117 Leon-An teorema (slika A.99). U ravni je dat četvorougla $ABCD$. Neka su M_1 i M_2 središta dijagonala AC i BD i neka je O proizvoljna tačka na pravoj M_1M_2 . Dokazati da je zbir površina trouglova ABO i CDO jednak polovini površine četvorougla $ABCD$.

$A = (0, 0)$, $B = (u_1, 0)$, $C = (u_2, u_3)$, $D = (u_4, u_5)$, $M_1 = (x_2, x_1)$, $M_2 = (x_4, x_3)$, $O = (x_5, u_6)$.

Teorema je dokazana metodom Wu-a.

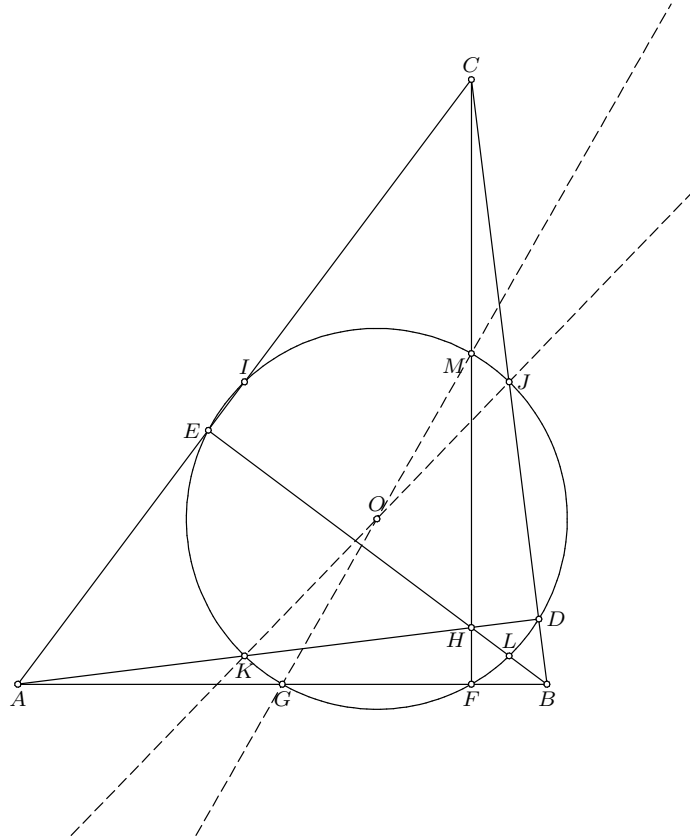
Kompleksnost: 0.026s, 96 terma.

Teorema je dokazana metodom Groebner-a.

Kompleksnost: 12.481s, 6640 terma.

Primer 118 Krug devet tačaka (slika A.100). Dokazati da se podnožja visina trougla, središta stranica i središta duži koje povezuju temena sa ortocentrom, nalaze na istom krugu.

Slika nam daje ideju gde se centar kruga nalazi. Iskoristićemo to i dokazati da su tri para tačaka istovremeno i prečnici kruga devet tačaka (odnosno biće dokazano i više nego što se traži u zadatku, ali će to učiniti dokaz ne težim, već



Slika A.100: Krug devet tačkaka

Slika A.101: Nobsova teorema

lakšim!). Krug devet tačkaka je takođe poznat pod mnogim imenima: Fojerbahov krug, Ojlerov krug, Terkvemov krug, krug šest tačkaka, itd.

$A = (0, 0)$, $B = (u_1, 0)$, $C = (u_2, u_3)$, $D = (x_2, x_1)$, $E = (x_4, x_3)$, $F = (u_2, 0)$, $G = (x_8, 0)$, $J = (x_{10}, x_9)$, $I = (x_{12}, x_{11})$, $H = (x_{14}, x_{13})$, $K = (x_{16}, x_{15})$, $L = (x_{18}, x_{17})$, $M = (x_{20}, x_{19})$, $O = (x_{22}, x_{21})$.

Teorema je dokazana metodom Wu-a.

Kompleksnost: 0.334s, 642 terma.

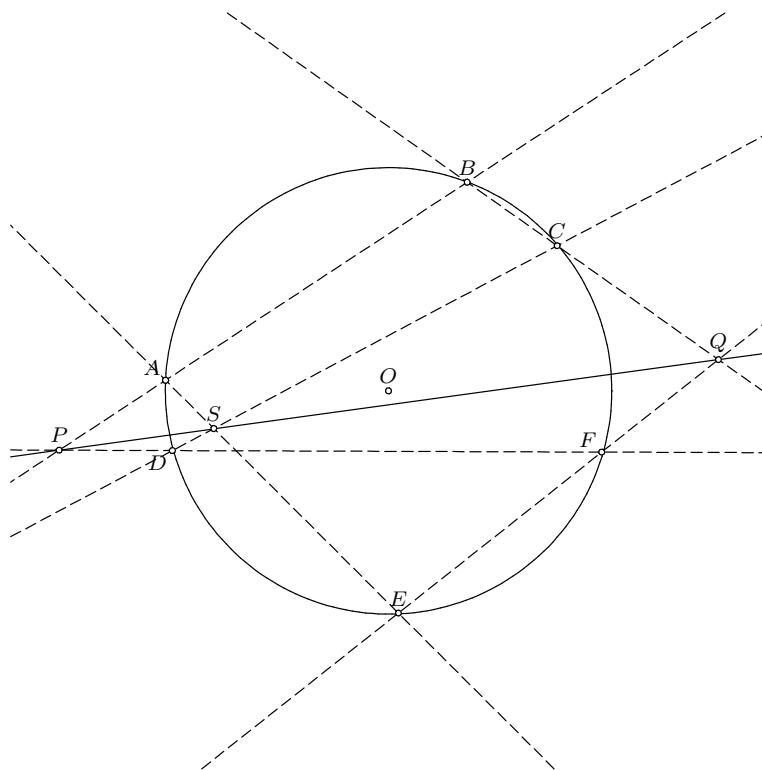
Teorema nije dokazana metodom Groebner-a.

Izvršavanje prekinuto posle 21.162s.

Primer 119 Nobsova teorema (slika A.101). U trougao ABC je upisan krug k koji dodiruje stranice trougla u tačkama S_1 , S_2 i S_3 . Neka su $P = BC \cap S_1S_3$, $Q = AC \cap S_2S_3$ i $R = AB \cap S_1S_2$. Dokazati da su tačke P , Q i R kolinearne.

$X = (0, 0)$, $Y = (u_1, 0)$, $S_3 = (u_6, 0)$, $O = (u_6, u_3)$, $S_1 = (x_3, u_4)$, $S_2 = (x_4, u_5)$, $A = (x_6, 0)$, $B = (x_8, 0)$, $C = (x_{10}, x_9)$, $P = (x_{12}, x_{11})$, $Q = (x_{14}, x_{13})$, $R = (x_{16}, 0)$.

Teorema je dokazana metodom Wu-a.



Slika A.102: Paskalova teorema

Kompleksnost: 0.037s, 96 terma.

Teorema nije dokazana metodom Groebner-a.

Izvršavanje prekinuto posle 21.363s.

Primer 120 Paskalova teorema (slika A.102). Na krugu k sa centrom O date su tačke $A, B, C, D, E,$ i F . Neka su P, Q i S preseki parova pravih AB i FD, BC i EF, AE i CD redom. Dokazati da su tačke P, Q i S kolinearne.

Paskalova teorema važi i ako se umesto na krugu tačke nalaze na proizvoljnoj krivoj drugog reda. To je posledica osobina projektivne geometrije — svaki krug se može projektivnim transformacijama koje čuvaju incidentnost pravih i tačaka preslikati u proizvoljnu krivu drugog reda.

$A = (0, 0), O = (u_1, 0), B = (x_1, u_2), C = (x_2, u_3), D = (x_3, u_4), E = (x_4, u_5), F = (x_5, u_6), P = (x_7, x_6), Q = (x_9, x_8), S = (x_{11}, x_{10})$.

Teorema je dokazana metodom Wu-a.

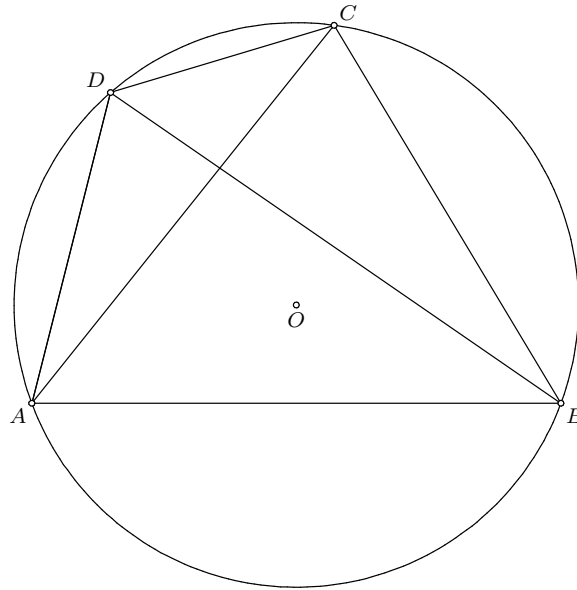
Kompleksnost: 0.174s, 496 terma.

Teorema nije dokazana metodom Groebner-a.

Izvršavanje prekinuto posle 21.062s.

Primer 121 Ptolomejeva teorema (slika A.103). Proizvod dijagonala četvorougla upisanog u krug jednak je zbiru proizvoda naspramnih stranica.

Dokazaćemo slabije tvrđenje, da je algebarska suma tri proizvoda iz zadatka jednaka nuli (odnosno da je jedan od njih jednak zbiru druga dva).



Slika A.103: Ptolomejeva teorema

$A = (0, 0)$, $B = (u_1, 0)$, $C = (u_2, u_3)$, $O = (x_2, x_1)$, $D = (x_3, u_4)$.

Teorema je dokazana metodom Wu-a.

Kompleksnost: 0.021s, 49 terma.

Teorema je dokazana metodom Groebner-a.

Kompleksnost: 0.033s, 83 terma.

Primer 122 *Simsonova teorema (slika A.104).* U ravni je dat trougao ABC oko koga je opisan krug k sa centrom O . Neka je D proizvoljna tačka na krugu k i neka su E , F i G podnožja normala iz tačke D na prave AB , AC i BC redom. Dokazati da su tačke E , F i G kolinearne.

$A = (0, 0)$, $O = (u_1, 0)$, $B = (x_1, u_2)$, $C = (x_2, u_3)$, $D = (x_3, u_4)$, $E = (x_5, x_4)$, $F = (x_7, x_6)$, $G = (x_9, x_8)$.

Teorema je dokazana metodom Wu-a.

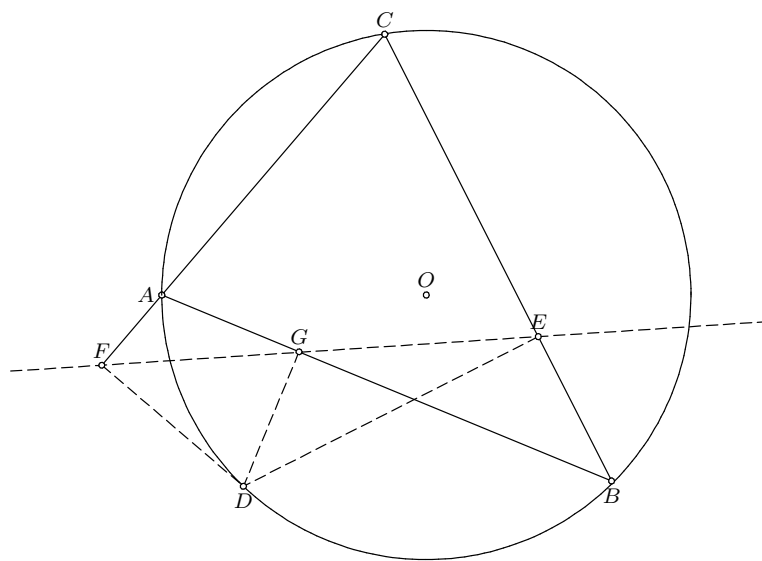
Kompleksnost: 0.044s, 81 terma.

Teorema nije dokazana metodom Groebner-a.

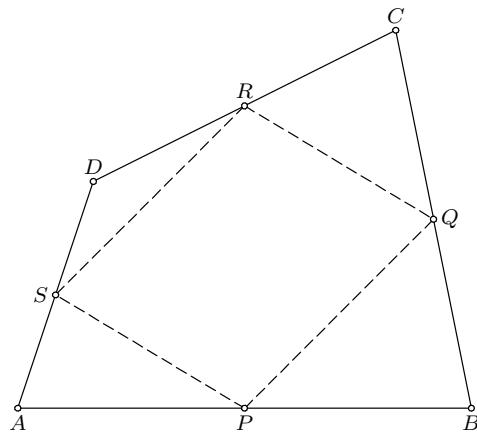
Izvršavanje prekinuto posle 21.440s.

Primer 123 *Vorinjonova teorema (slika A.105).* Dat je četvorougao $ABCD$. Neka su P , Q , R i S središta stranica AB , BC , CD i DA redom. Dokazati da je četvorougao $PQRS$ paralelogram.

$A = (0, 0)$, $B = (u_1, 0)$, $C = (u_2, u_3)$, $D = (u_4, u_5)$, $P = (x_2, 0)$, $Q = (x_4, x_3)$, $R = (x_6, x_5)$, $S = (x_8, x_7)$.



Slika A.104: Simsonova teorema



Slika A.105: Vorinjonova teorema

Teorema je dokazana metodom Wu-a.

Kompleksnost: 2.422s, 3170 terma.

Teorema je dokazana metodom Groebner-a.

Kompleksnost: 5.400s, 3170 terma.

Literatura

- [1] Shang-Ching Chou, *Mechanical Geometry Theorem Proving*, (D.Reidel Publishing Company, Dordrecht, 1988).
- [2] Dongming Wang, *On Wu's Method for Proving Constructive Geometric Theorems*, (Proceedings of the 11th International Joint Conference on Artificial Intelligence (IJCAI-89) (Detroit, USA, August 20-25, 1989), pp. 419-424).
- [3] Shang-Ching Chou, Xiao-Shan Gao *Automated Reasoning in Geometry*.
- [4] Shang-Ching Chou, *Proving and Discovering Theorems in Elementary Geometries Using Wu's Method*, (PhD Thesis, Department of Mathematics, University of Texas, Austin 1985).
- [5] Predrag Janičić and Pedro Quaresma *System Description: GCLCprover + GeoThms*. (In Ulrich Furbach and Natarajan Shankar, editors, Automated Reasoning, volume 4130 of Lecture Notes in Artificial Intelligence, pages 145-150. Springer, 2006.).
- [6] Predrag Janičić Stevan Kordić *EUCLID - the Geometry Theorem Prover*, (FILOMAT, Niš 9:3 (1995), 723-732).
- [7] Gelertner H. *Realization of a Geometry Theorem Machine*, in 'Proc. Int. Conf. in Info. Process', (Paris, pp. 273-282).
- [8] Hilbert D. *Foundation of Geometry*, Open Court Publishing Company, La Salla, Illinois
- [9] Tarski A. *A decision method for elementary algebra and geometry*, Technical Report, Report R-109, The Rand Corporation, Santa Monica. second revised ed.
- [10] Collins G. *Quantifier elimination for real closed fields by cylindrical algebraic decomposition*, in 'LNCS 33', Springer-Verlag, Berlin, pp. 134-183
- [11] Davis P. and Cerruti E. *Formac meets Pappus*, The American Mathematical Monthly 76, 895-905
- [12] Wu W. *On the decision problem and the mechanization of theorem proving in elementary geometry*, J. Sys. Sci. and Math. Scis. 21, 157-179
- [13] Chou S. *Proving elementary geometry theorems using Wu's algorithm*, in W. Bledsoe and D. Loveland, eds. 'Automated Theorem Proving: After 25 years', AMS Contemporary Mathematics Series, pp. 243-286
- [14] Ritt J. *Differential Algebra*, AMS Colloquium Publications, New York
- [15] Buchberger B. *Grobner bases: An algorithmic method in polynomial ideal theory*, in N. Bose, ed., 'Multidimensional Systems Theory', D. Reidel Publ., pp. 184-232

- [16] Yang L., Zhang J. and Hou X. *A criterion of dependancy between algebraic equations and its applications*, in 'Proc. IWMM'92', Inter. Academic Publishers, Beijing, pp. 110-134.
- [17] Ritt J. *Differential Equations from Algebraic Standpoint*, Vol. 14, AMS Colloquium Publications, New York
- [18] Chou S., Gao X. and Zhang J. *Automated production of traditional proofs for constructive geometry theorems*, in 'Proc. of Eight IEEE Symposium on Logic in Computer Science', IEEE Computer Society Press, pp. 48-56
- [19] Chou S., Gao X. and Zhang J. *Mechanical geometry theorem proving by vector calculation*, in 'Proc. of ISSAC'93(Kiev)', ACM Press, New York, pp. 284-291
- [20] Stifter S. *Geometry theorem proving in vector spaces by means of Grobner bases*, in 'Proc. of ISSAC'92, (Kiev)', ACM Press, New York, pp. 301-310
- [21] Richter-Gebert J. *Mechanical theorem proving in projective geometry*, Ann. of Math. and AI 13, 139-172
- [22] Li H. and Cheng M. *Proving geometric theorems with Clifford algebraic method*, Technical Report MM Preprints, NO. 14, MMRC, Academia Sinica
- [23] Chou S., Gao X. and Zhang J. *Automated generation of readable proofs with geometryc invariants part i: Multiple and shortest proof generation*, J. of Automates Reasoning 17, 325-347
- [24] S. C. Chou, W. Schelter and G. J. Yang *Proving Geometry Theorems with Rewrite Rules*, Journal of Automated Reasoning, 2(4) (1986), 253-273
- [25] S. C. Chou *Proving Geometry Theorems Using Wu's Method: A Collection of Geometry Theorems Proved Mechanically*, Technical Report 50, Insitute for Computing Science, University of Texas at Austin, July 1986
- [26] L. Bachmair and B. Buchberger *A Simplified Proof of the Characterization Theorem for Grobner Bases*, ACM SIGSAM Bull 14(4) (1980), 29-34
- [27] Gao X. and Chou S. *Solving geometric constraint systems, i. a global propagation approach*, Computer Aided Design 30(1), 47-54
- [28] Gao X. and Chou S. *Solving geometric constraint systems, ii. a symbolic computation approach*, Computer Aided Design 30(2), 115-122
- [29] Gao X., Zhu C. C. and Huang Y. *Building dynamic mathematical models with geometry expert, ii. linkages*, Z. Li, ed., 'Proc. of ASCM'98', LanZhou Univ. Press, LanZhou, pp. 15-22
- [30] Huang Y. Z. and Wu W. D. *Kinematic solution of a Stewart platform*, 'Proc. IWMM'92', Inter. Academic Publishers, Beijing, pp. 181-188
- [31] Kapur M. and Mundy J. *Wu's method and its application to perspective viewing*, Artificial Intelligence 37, 15-36
- [32] Wu W. *On surface-fitting problem in CAGD*, Technical Report MM Research Preprints No. 10, MMRC, Academia Sinica
- [33] Brad Appleton *AVL Trees: Tutorial and C++ Implementation*, <http://www.cmcrossroads.com/bradapp/ftp/src/libs/C++/AvlTrees.html>

- [34] Predrag Janicic *GCLC – A Tool for Constructive Euclidean Geometry and More than That*, Springer-Verlag, 2006.
- [35] Predrag Janicic, Pedro Quaresma *Automated Verification of Regular Constructions, Automated Deduction in Geometry*, Lecture Notes in Artificial Intelligence, volume 4869, Springer-Verlag, 2007.