Grebnerove baze

Vesna Marinković

Sadržaj

1 Uvod **5**
1.1 Modelovanje problema 6
1.2 Specijalni slučajevi Grebnerovih baza 9

2 Uvodni pojmovi **15**
2.1 Poredak monoma 17
2.2 Deljenje polinoma u prstenu više promenljivih 24

3 Grebnerova baza **31**

4 Primene Grebnerovih baza **41**
4.1 Rešavanje sistema polinomijalnih jednačina 41
4.2 Rešavanje sistema nepolinomijalnih jednačina 45
4.3 Rešavanje problema celobrojnog linearnog programiranja 48
4.4 Računanje hromatskog broja grafa 54
4.5 Sudoku 57

5 Radikali i dokazivanje teorema u geometriji **61**
5.1 Radikali ideala 61
5.2 Osnovni postupak dokazivanja 65
5.3 Algebrizacija osnovnih geometrijskih tvrđenja 78
5.4 Identifikovanje uslova nedegenerisanosti 81
5.5 Dokazivanje ispravnosti rešenja konstruktivnih problema u geometriji . . . 84
5.5.1 GCLC 84
5.5.2 Konstruktivni problemi u geometriji 86
5.5.3 Automatsko rešavanje konstruktivnih problema 88

Glava 1

Uvod

Grebnerova baza predstavlja skup polinoma nad više promenljivih koji imaju određena pogodna svojstva. Grenbnerove baze omogućavaju jednostavna algoritamska rešenja za mnoge fundamentalne probleme u matematici i prirodnim i tehničkim naukama. Često se kaže da Grebnerove baze predstavljaju važan gradivni blok moderne algebre i posebno algebarske geometrije. Teoriju Grebnerovih baza razvio je Bruno Buhberger u svom doktoratu 1965. godine i dao im ime po svom mentoru Volfgangu Grebneru. Međutim, kao što je to često slučaj sa važnim otkrićima u to doba, smatra se da je do istog koncepta nezavisno došlo još nekoliko matematičara, i to Nikolaj Ginter još davne 1913. godine i Heisuke Hironaka 1964. godine, koji ih je nazvao standardnim bazama (ovaj termin se i danas može sresti u literaturi kao sinonim za Grebnerovu bazu).

Koncept Grebnerovih baza bi se ukratko mogao opisati na sledeći način: razmatramo skup $F = \{f_1, f_2, \ldots, f_m\}$ polinoma nad većim brojem promenljivih i odgovarajući skup polinomijalnih jednačina $f_1 = 0, f_2 = 0, \ldots, f_m = 0$. Skup polinoma F transformišemo u drugi skup polinoma G koji predstavlja Grebnerovu bazu skupa F, tako da skupovi polinoma F i G imaju isti skup rešenja ali da, dodatno, skup G ima i neka lepa svojstva koja skup F ne poseduje. Teorija Grebnerovih baza nam govori da je probleme koje je teško rešiti u terminima skupa polinoma F jednostavno rešiti u terminima skupa polinoma Grebnerove baze G i da, dodatno, postoji algoritam za transformisanje proizvoljnog skupa F u njemu ekvivalentan skup G: jedan takav algoritam je Buhbergerov algoritam.

Dva glavna pitanja koja se javljaju pri radu sa polinomima i idealima generisanim ovim polinomima su:

- Da li za proizvoljni polinom f nad promenljivim $x_1, x_2, \ldots, x_n$ možemo utvrditi da li pripada idealu $I = \langle f_1, f_2, \ldots, f_m \rangle$? Ovo odgovara tome da ako važe neki uslovi koji se mogu zapisati kao $f_1 = 0, f_2 = 0, \ldots, f_m = 0$ za neke polinome $f_1, f_2, \ldots, f_m$, onda važi i zaključak koji se iskazuje u vidu $f = 0$ za neki polinom f.
- Da li je moguće pronaći rešenja sistema polinomijalnih jednačina

  $$f_1(x_1, x_2, \ldots, x_n) = 0, \ldots, f_m(x_1, x_2, \ldots, x_n) = 0?$$

  Nekada je pak situacija takva da je veći broj nepoznatih nego jednačina, pa ne možemo eksplicitno rešiti neki sistem, ali možemo da zaključimo da važi neki odnos među nepoznatima.

Grebnerove baze omogućavaju uniformni pristup rešavanju problema koji se mogu izraziti u terminima sistema polinomijalnih jednačina nad većim brojem promenljivih. One imaju veliki broj različitih primena, kao što su rešavanje sistema nelinearnih jednačina, rešavanje problema celobrojnog linearnog programiranja, rešavanje trigonometrijskih jednačina, analiza i konstrukcija nelinearnih kriptosistema. Interesantno, i problemi koji koji na prvi pogled nemaju dodirnih tačaka sa algebrom, kao što su automatsko dokazivanje i otkrivanje teorema u geometriji, rešavanje nekih grafovskih problema poput bojenja grafa i rešavanje igara poput sudokua, mogu se svesti na izračunavanje Grebnerove baze.

1.1 Modelovanje problema

U nastavku ćemo videti nekoliko problema koje je moguće rešiti tehnikom Grebnerovih baza.

Primer 1. *Ana, Bojan i Ceca zajedno imaju 14 jabuka. Ako Bojan ima 4 jabuke više od Ane i Cece zajedno, proveriti da li onda Ana i Ceca imaju zajedno 5 jabuka.*

Ako broj jabuka koje ima Ana označimo sa A, broj jabuka koje ima Bojan sa B, a broj jabuka koje ima Ceca sa C, onda ovaj problem možemo opisati sistemom jednačina:

$$\begin{aligned} A + B + C &= 14 \\ B &= A + C + 4 \end{aligned}$$

Prethodni sistem možemo nešto drugačije zapisati, tako što ćemo vrednosti odgovarajućih polinoma izjednačiti sa nulom:

$$\begin{aligned} f(A, B, C) &= A + B + C - 14 = 0 \\ g(A, B, C) &= A - B + C + 4 = 0 \end{aligned}$$

U ovom sistemu figuriše veći broj nepoznatih nego što imamo jednačina, te ovaj sistem ne možemo da rešimo. Ipak, možemo da zaključimo nešto o nepoznatima. Nas konkretno interesuje da li iz ove dve jednačine sledi uslov $A + C = 5$, odnosno uslov:

$$h(A, B, C) = A + C - 5 = 0$$

Može se pokazati da se polinom h može predstaviti kao linearna kombinacija polinoma f i g:

$$h = \frac{1}{2}f + \frac{1}{2}g$$

te kada važi $f(A, B, C) = 0$ i $g(A, B, C) = 0$ važiće i $h(A, B, C) = 0$. Ovo odgovara tome da polinom h pripada idealu definisanom polinomima f i g, te se zaključak h može izvesti na osnovu pretpostavki f i g.

Primer 2. *Jedan od važnih problema u kriptografiji jeste kako osmisliti shemu prenosa informacija kroz komunikacione kanale tako da je moguće detektovati ako tokom prenosa dođe do greške i, dodatno, omogućiti da primalac te greške ispravi.*

Standardni način kodiranja se sastoji u tome da se umesto direktnog slanja podataka $a_0, a_1, \ldots, a_n$ *izračuna vrednost polinoma*

$$p(x) = a_0 + a_1 x + \ldots + a_n x^n$$

i šalju, na primer, vrednosti $p(0), p(1), p(2), \ldots, p(n), p(n+1), \ldots, p(n+5)$. *Primetimo da namerno šaljemo veći broj vrednosti polinoma nego što je minimalno potrebno da se rekonstruišu koeficijenti polinoma* p. *Ako je prenos bio uspešan, tada je na osnovu vrednosti* $p(k),\ 1 \leq k \leq n+5$ *moguće izračunati koeficijente polinoma* p *procesom interpolacije. Ukoliko to nije slučaj, odnosno ako su neke od vrednosti* $p(k)$ *pogrešno prenesene, tada najčešće neće biti moguće izračunati koeficijente polinoma* p *stepena* n *koji zadovoljava sve date uslove.*

Grebnerove baze predstavljaju jedan od mehanizama za utvrđivanje mogućih kandidata za ispravan vektor podataka na osnovu vektora primljenih podataka koji sadrži greške. Pretpostavimo da je primalac primio vrednosti $p_0, p_1, \ldots, p_{n+5}$. *Cilj je konstruisati polinom* $p(x) = a_0 + a_1 x + \ldots + a_n x^n$ *stepena najviše* n *tako da važi* $p(k) = p_k$ *za veliki broj tačaka* k. *U ovim tačkama važiće uslov:*

$$a_0 + a_1 k + a_2 k^2 + \ldots + a_n k^n = p_k$$

U tačkama u kojima se prilikom prenosa dogodila greška, ova jednačina neće važiti. Međutim, kada bismo znali da se greška dogodila na pet pozicija $e_1, e_2, \ldots, e_5$, *tada bi jednačina:*

$$(k - e_1)(k - e_2)(k - e_3)(k - e_4)(k - e_5)(a_0 + a_1 k + a_2 k^2 + \ldots + a_n k^n - p_k) = 0$$

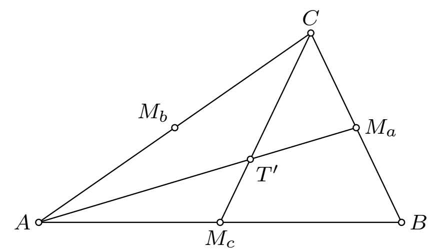
bila tačna za svako $k = 0, 1, \ldots, n+5$.

Ako vrednosti $e_1, e_2, \ldots, e_5$ *i* $a_0, a_1, \ldots, a_n$ *razmotrimo kao nepoznate, dobijamo sistem algebarskih jednačina*

$$\begin{array}{rcl}
e_1 \cdot e_2 \cdot e_3 \cdot e_4 \cdot e_5 \cdot (a_0 - p_0) & = & 0 \\
(1 - e_1)(1 - e_2)(1 - e_3)(1 - e_4)(1 - e_5)(a_0 + a_1 + \ldots + a_n - p_1) & = & 0, \\
(2 - e_1)(2 - e_2)(2 - e_3)(2 - e_4)(2 - e_5)(a_0 + a_1 \cdot 2 + \ldots + a_n \cdot 2^n - p_2) & = & 0 \\
 & \ldots &
\end{array}$$

sa $n+6$ *promenljivih i* $n+6$ *jednačina, koji se može rešiti korišćenjem Grebnerovih baza. Primetimo da je neophodno poslati barem* $n+1$ *podataka da bi problem mogao da se reši.*

Primer 3. *Poznato geometrijsko tvrđenje glasi da se težišne duži trougla seku u jednoj tački. Ta tačka naziva se težištem trougla i označava sa* T. *Pokažimo na koji način bismo*



Slika 1.1: Težišne duži trougla ABC seku se u jednoj tački.

mogli da dokažemo ovo tvrđenje.

Razmotrimo primer trougla ABC u ravni. Najpre je potrebno svim značajnim tačkama koje se javljaju u zadatku dodeliti koordinate. Bez narušavanja opštosti, temenima trougla mogu se dodeliti koordinate $A(0,0)$, $B(b_x,0)$ i $C(c_x,c_y)$. Tačka M_c kao središte duži AB imaće koordinate $M_c(b_x/2,0)$, tačka M_a kao središte duži BC koordinate $M_a((b_x+c_x)/2,c_y/2)$, a tačka M_b kao središte duži AC koordinate $M_b(c_x/2,c_y/2)$. Označimo presek težišne duži iz temena A i težišne duži iz temena C sa $T'(t_x,t_y)$. Dokažimo da tačka T' pripada i težišnoj duži iz temena B (slika 5.1).

U opštem slučaju uslov da su tačke $P(p_1,p_2)$, $Q(q_1,q_2)$ i $R(r_1,r_2)$ kolinearne možemo zadati izjednačavanjem koeficijenata pravaca pravih PR i QR:

$$\begin{aligned} \frac{r_2-p_2}{r_1-p_1} &= \frac{r_2-q_2}{r_1-q_1} \\ h &= (r_2-p_2)(r_1-q_1)-(r_2-q_2)(r_1-p_1)=0 \end{aligned}$$

Prema pretpostavci zadatka tačka $T'(t_x,t_y)$ kolinearna je sa tačkama $A(0,0)$ i $M_a((b_x+c_x)/2,c_y/2)$, što odgovara uslovu:

$$f = c_y/2\cdot((b_x+c_x)/2-t_x)-(c_y/2-t_y)(b_x+c_x)/2=0$$

a u isto vreme tačka T' je kolinearna sa tačkama $C(c_x,c_y)$ i $M_c(b_x/2,0)$ što odgovara uslovu:

$$g=(-c_y)(b_x/2-t_x)-(-t_y)(b_x/2-c_x)=0$$

Zaključak koji treba izvesti može se opisati uslovom da su tačke $B(b_x,b_y)$, $T'(t_x,t_y)$ i $M_b(c_x/2,c_y/2)$ kolinearne:

$$h=c_y/2\cdot(c_x/2-t_x)-(c_y/2-t_y)(c_x/2-b_x)=0$$

Može se pokazati da polinom h pripada idealu generisanom polinomima f i g, odnosno da iz $f=0$ i $g=0$ sledi $h=0$ te polazno tvrđenje važi.

Primer 4. *Razmotrimo površi zadate jednačinama:*

$$\begin{aligned} x^2+y^2+z^2-1 &= 0 \\ x^2+y^2+z^2-2x &= 0 \\ x-y+2z &= 0 \end{aligned}$$

Tačke preseka ovih površi možemo naći tako što odredimo Grebnerovu bazu ideala generisanog polinomima $\langle x^2+y^2+z^2-1, x^2+y^2+z^2-2x, x-y+2z\rangle$. *Kao Grebnerovu bazu dobijamo skup polinoma* $\{-1+4z+10z^2, -1+2y-4z, -1+2x\}$ *koji se može jednostavno rešiti. Naime, prvo bismo rešili prvu jednačinu i našli dve moguće vrednosti za* z, *iz druge jednačine bismo onda našli vrednost za* y, *a iz treće izračunali vrednost promenljive* x.

1.2 Specijalni slučajevi Grebnerovih baza

Većini studenata, iako ne pod ovim nazivom, već je poznat koncept Grebnerovih baza u dva specijalna slučaja, a to su:

- *Gausova metoda eliminacije* u slučaju sistema polinoma koji su linearni po promenljivim $x_1, x_2, \ldots, x_n$ i
- *Euklidov algoritam* u slučaju sistema polinoma jedne promenljive.

Ako su svi polinomi u sistemu jednačina linearni po promenljivim, onda je Grebnerova baza ideala generisanog ovih polinomima u stvari novi sistem polinoma dobijen Gausovom metodom eliminacije. Novi sistem ima isti skup rešenja kao i polazni, ali se jednostavnije rešava. Takođe, iz novog sistema jednačina možemo odmah zaključiti da li ovaj sistem ima nula, jedno ili beskonačno mnogo rešenja. Proces transformisanja matrice sistema jednačina u oblik gornje trougaone matrice prati ideje Buhbergerovog algoritma za konstrukciju Grebnerove baze koji ćemo naknadno videti.

Primer 5. *Cena goriva se promenila u toku dana. Jutarnja cena iznosila je 160 dinara po litru, a popodnevna 200. Ako znamo da je prodato ukupno 1200 litara goriva i da ukupna zarada u tom danu iznosi 200000 dinara, koliko je goriva prodato po kojoj ceni?*

Ako količinu goriva prodatu po jutarnjoj ceni označimo sa k_j, *a količinu goriva prodatu po popodnevnoj ceni sa* k_p *dobijamo naredni sistem linearnih jednačina:*

$$\begin{aligned} f_1(k_j,k_p) = k_j + k_p &= 1200 \\ f_2(k_j,k_p) = 160k_j + 200k_p &= 200000 \end{aligned}$$

koji lako rešavamo Gausovom metodom eliminacije:

$$\begin{aligned} f_1(k_j,k_p) = k_j + k_p &= 1200 \\ f_3(k_j,k_p) = 40k_p &= 40000 \end{aligned}$$

pri čemu važi $f_3 = f_2 - 160 f_1$. *Ovaj proces možemo razumeti kao redukciju polinoma* f_2 *u odnosu na polinom* f_1, *a polinom* f_3 *kao ostatak pri deljenju polinoma* f_2 *polinomom* f_1. *Novi sistem jednačina možemo jednostavno rešiti i njegovo rešenje je* $k_p = 200$ *i* $k_j = 1000$.

Primer 6. *Razmotrimo polinome* f *i* g *nad promenljivim* x, y *i* z:

$$\begin{aligned} f(x,y,z) &= 3x+7y-5z-2 \\ g(x,y,z) &= 2x+3y-8z-6 \end{aligned} \tag{1.1}$$

Razmotrimo na koji način pojednostaviti ovaj sistem linearnih jednačina. Najmanji zajednički sadržalac koeficijenata uz x *jednak je 6 pa možemo pomnožiti prvu jednačinu sa* $6/3$ *i od nje oduzeti drugu pomnoženu sa* $6/2$ *i na taj način iz druge jednačine eliminisati član uz* x:

$$S_{f,g} = \frac{6}{3}(3x+7y-5z-2) - \frac{6}{2}(2x+3y-8z-6) = 5y+14z+14$$

Dakle, sistem polinoma (1.1) možemo zameniti njemu ekvivalentnim sistemom polinoma koji je jednostavniji (jer druga jednačina ne sadrži član po x*):*

$$\begin{aligned} f &= 3x+7y-5z-2 \\ S_{f,g} &= 5y+14z+14 \end{aligned} \tag{1.2}$$

Primer 7. *Razmotrimo malo složeniji sistem linearnih jednačina po promenljivim* x, y *i* z:

$$\begin{aligned} 2x+3y-z &= 0 \quad (J1) \\ x+y-1 &= 0 \quad (J2) \\ x+z-3 &= 0 \quad (J3) \end{aligned}$$

Krećemo od matrice sistema dopunjene vektorom slobodnih članova, a zatim Gausovom metodom eliminacije svodimo matricu sistema jednačina na gornje trougaonu.

$$\left[\begin{array}{ccc|c} 2 & 3 & -1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 3 \end{array}\right] \longrightarrow_{J_1=J_3,\ J_2=J_1-2J_2,\ J_3=J_1-2J_3}$$

$$\left[\begin{array}{ccc|c} 1 & 0 & 1 & 3 \\ 0 & 1 & -1 & -2 \\ 0 & 3 & -3 & -6 \end{array}\right] \longrightarrow_{J_3=J_3-3J_2}$$

$$\left[\begin{array}{ccc|c} 1 & 0 & 1 & 3 \\ 0 & 1 & -1 & -2 \\ 0 & 0 & 0 & 0 \end{array}\right]$$

Forma ove matrice nam govori da je promenljiva z slobodna i postavljanjem da je $z = t$ dobijamo skup rešenja ovog sistema jednačina:

$$\begin{aligned} x &= -t + 3 \\ y &= t - 2 \\ z &= t \end{aligned}$$

Drugi dobro poznat primer je slučaj sistema polinoma jedne promenljive. Najveći zajednički delilac polinoma $f_1, f_2, \ldots, f_m$ je polinom h koji deli sve f_i i, dodatno, važi da ako je p neki drugi polinom koji deli polinome $f_1, f_2, \ldots, f_m$ onda p deli i polinom h. Dakle, najveći zajednički delilac skupa polinoma datog sistema jednačina je polinom čije su nule sva zajednička rešenja polinoma polaznog sistema. Pokazuje se da on predstavlja Grebnerovu bazu ideala generisanog polaznim sistemom polinoma. Pritom, i Euklidov algoritam za izračunavanje najvećeg zajedničkog delioca skupa polinoma prati ideje Buhbergerovog algoritma za izračunavanje Grebnerove baze.

Primer 8. *Neka je dat sistem jednačina:*

$$\begin{aligned} x^2 + 7x + 6 &= 0 \\ x^2 - 5x - 6 &= 0 \end{aligned}$$

Rešenje ovog sistema jednačina predstavlja polinom koji je najveći zajednički delilac polinoma $f(x) = x^2 + 7x + 6$ i $g(x) = x^2 - 5x - 6$ i koga je moguće izračunati Euklidovim algoritmom. Euklidov algoritam izračunava niz ostataka r_i, počev od $r_0 = f = x^2 + 7x + 6$ i $r_1 = g = x^2 - 5x - 6$ sukcesivnim deljenjem susednih elemenata u nizu ostataka sve dok ne dobije ostatak nula:

$$\begin{aligned} r_0 &= q_1 r_1 + r_2 \\ r_1 &= q_2 r_2 + r_3 \\ &\ldots \\ r_{n-1} &= q_n r_n + 0 \end{aligned}$$

Poslednji nenula ostatak r_n biće jednak najvećem zajedničkom deliocu polinoma f i g.

$$\begin{aligned} x^2 + 7x + 6 &= 1 \cdot (x^2 - 5x - 6) + (12x + 12) \quad \Rightarrow \quad r_2 = 12x + 12 \\ x^2 - 5x - 6 &= (12x + 12) \cdot (1/12x - 1/2) + 0 \quad \Rightarrow \quad r_3 = 0 \end{aligned}$$

Poslednji nenula ostatak je $r_2 = 12x + 12$ i on predstavlja najveći zajednički delilac ovih polinoma. Uobičajeno se vodeći koeficijent polinoma postavlja na jedinicu, te polinom $r_2/12 = x + 1$ proglašavamo najvećim zajedničkim deliocem ovih polinoma.

Praktična vežba 1. Singular *je računarski sistem za algebarska izračunavanja otvorenog koda, sa značajnom primenom na polinomijalna izračunavanja*[1]*. Alat Singular ima sintasku veoma blisku programskom jeziku C: na primer naredbe kontrole toka* `if` *i* `for` *se analogno definišu. Svaka naredba se u alatu Singular završava sa* `;`*.*

U Singularu je moguće vršiti različita izračunavanja, deklarisati promenljive i koristiti ih u narednim naredbama.

```
> 1 + 1;
2
> int a = 9;
> a;
9
> a div 2;
4
> a mod 2;
1
> string s = "Zdravo";
> s;
Zdravo
```

Niz celih brojeva deklariše se ključnom rečju `intvec`*. Indeksiranje elemenata u nizu kreće od 1.*

```
> intvec v = a,3,1;
> v;
9,3,1
v[2];
3
```

Komentari počinju od znaka `//` *i važe do kraja reda. Naredba* `help` *startuje u veb pregledaču onlajn manual.*

Pored velikog broja već podržanih funkcija raspoloživih kroz različite biblioteke, moguće je pisati i svoje funkcije i definisati svoje biblioteke. Mi ćemo se ovde zadržati na korišćenju već definisanih funkcija za rad sa polinomima, idealima i Grebnerovim bazama.

Prvi korak u radu sa polinomima u programu Singular je definisanje prstena nad kojim će biti definisani polinomi i to se postiže naredbom:

```
ring <ime> = <koeficijenti>, <imena promenljivih>, <oznaka_poretka>
```

Dakle, potrebno je zadati kom skupu pripadaju koeficijenti polinoma, skup promenljivih nad kojim su polinomi formulisani i željeni poredak monoma (kojim ćemo se kasnije detaljnije baviti). Ako su koeficijenti polinoma iz skupa $\mathbb{Q}$ racionalnih brojeva navodimo vrednost 0, ako želimo da zadamo skup $\mathbb{Z}$ celih brojeva navodimo `integer`*, ako želimo da radimo sa skupom $\mathbb{C}$ kompleksnih brojeva navodimo* `complex`*, a ako pak želimo da radimo sa polinomima čiji su koeficijenti iz skupa $\mathbb{R}$ realnih brojeva izraženi na 5 decimala navodimo* `(real,5)`*. Skup promenljivih nad kojim su polinomi definisani navodimo* *u malim zagradama međusobno razdvojene zapetom i to u opadajućem poretku značaja promenljivih.*

Funkcija `gcd` *računa najveći zajednički delilac dva broja ili dva polinoma.*

Izračunajmo najveći zajednički delilac polinoma iz primera 8. Najpre je potrebno definisati okruženje u kome radimo: kom polju pripadaju koeficijenti polinoma, nad kojim promenljivim su polinomi definisani i koju vrstu poretka monoma koristimo (o ovome poslednjem će biti više reči u narednom poglavlju).

```
> ring r = 0, (x,y,z), lp;
> poly f = x2 + 7x + 6;
> poly g = x2 - 5x - 6;
> gcd(f,g);
x+1
```

Kao što smo mogli da vidimo, umesto `x^2` *možemo skraćeno pisati* `x2`*, a umesto* `7*x` *skraćeno* `7x`.

Stoga se izračunavanje Grebnerove baze može videti s jedne strane kao uopštenje Gausovog metoda eliminacije na nelinearne sisteme jednačina, a s druge strane i kao uopštenje Euklidovog algoritma za izračunavanje najvećeg zajedničkog delioca polinoma na polinome više promenljivih.

[1] Alat Singular je dostupan na adresi `https://www.singular.uni-kl.de/`, a tutorijal programa Singular na adresi `https://www.singular.uni-kl.de/DEMOS/SummerSchool-Trieste-09/Singular_Tutorial.pdf`.

Glava 2

Uvodni pojmovi

Da bismo mogli da precizno definišemo pojam Grebnerovih baza, potrebno je da uvedemo neke algebarske koncepte.

Razmatraćemo polinome po promenljivim $x_1, x_2, \ldots, x_n$ čiji su koeficijenti iz polja K, gde je K najčešće polje racionalnih brojeva $\mathbb{Q}$, polje realnih brojeva $\mathbb{R}$ ili polje kompleksnih brojeva $\mathbb{C}$. Skup svih polinoma nad promenljivim $x_1, x_2, \ldots, x_n$ sa koeficijentima u K označavaćemo sa $K[x_1, x_2, \ldots, x_n]$. Definisanjem operacija sabiranja i množenja polinoma na uobičajen način dobijamo da je $K[x_1, x_2, \ldots, x_n]$ komutativni prsten polinoma. Primetimo da $K[x_1, x_2, \ldots, x_n]$ nije polje jer za proizvoljni polinom iz $K[x_1, x_2, \ldots, x_n]$ ne postoji uvek multiplikativni inverz. Na primer, ne postoji inverz polinoma $f = x + y$ jer $\frac{1}{x+y} \notin \mathbb{R}[x, y]$ nije polinom.

Definicija 1 (Ideal)**.** *Neka je $(K, +, \cdot)$ komutativni prsten i I neprazan podskup od K. Tada je I* ideal *ako:*

1. *za sve $x, y \in I$ važi $x + y \in I$,*
2. *za sve $a \in K$ i $x \in I$ važi $a \cdot x \in I$.*

Primer 9. *Skup parnih brojeva $2\mathbb{Z}$ predstavlja ideal prstena $\mathbb{Z}$, dok skup neparnih brojeva nije ideal. U opštem slučaju, skup $k\mathbb{Z}$ celih brojeva deljivih sa k je jedan ideal.*

Primer 10. *Skup polinoma iz $\mathbb{Z}[x]$ čiji su svi koeficijenti parni čini jedan ideal.*

Teorema 1. *Neka su $f_1, f_2, \ldots, f_m$ polinomi iz prstena polinoma $K[x_1, x_2, \ldots, x_n]$. Tada*

$$\langle f_1, f_2, \ldots, f_m \rangle = \{h_1 f_1 + h_2 f_2 + \ldots + h_m f_m \mid h_i \in K[x_1, x_2, \ldots, x_n]\}$$

predstavlja jedan ideal. Za ovaj ideal ćemo reći da je generisan polinomima *$f_1, f_2, \ldots, f_m$.*

Naime, ideal u prstenu polinoma je podskup prstena koji je zatvoren u odnosu na sabiranje i množenje svim polinomima iz tog prstena. Ovaj ideal je generisan datim skupom polinoma. Grebnerova baza predstavlja bolji skup generatora (bolju bazu) ovog ideala.

Primer 11. *Razmotrimo prsten polinoma nad dve promenljive, na primer $K[x, y]$. Onda je ideal generisan polinomima $x^2 - 1$ i $yx + y$ jednak:*

$$\langle x^2 - 1, yx + y\rangle = \{h_1 \cdot (x^2 - 1) + h_2 \cdot (yx + y) \mid h_1, h_2 \in K[x, y]\}.$$

Elementi ovog ideala su svi polinomi koji se mogu napisati u obliku $h_1 \cdot (x^2 - 1) + h_2 \cdot (yx + y)$, pri čemu su h_1 i h_2 proizvoljni polinomi iz prstena $K[x, y]$. Na primer, ako uzmemo $h_1 = 1$ i $h_2 = 0$ dobijamo da ovom idealu pripada polinom $x^2 - 1$, a, slično, ako odaberemo $h_1 = -y$ i $h_2 = x$ dobijamo da ovom idealu pripada i polinom $yx + y$.

Primer za vežbu 1. *Odrediti barem četiri različita polinoma koji pripadaju idealu $I = \langle 2x + y^2 - 1, 3x^2y - xy + 2\rangle$.*

Primer 12. *Razmotrimo ideal $I = \langle f_1, f_2\rangle = \langle 1 + x, 1 + y\rangle \subset \mathbb{Q}[x, y]$. Polinomi $0, x - y, x + xy$ su elementi ideala I, dok polinomi $1, xy$ i $1 + x^2$ nisu.*

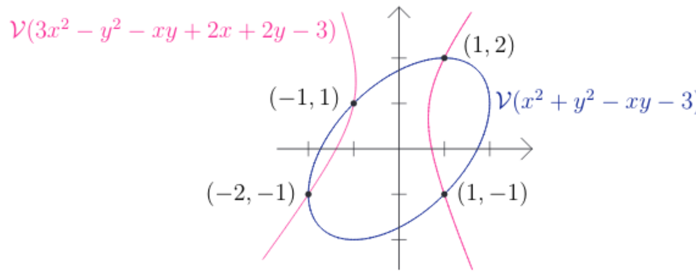
Definicija 2 (Afini varijetet)**.** Afini varijetet $V(f_1, f_2, \ldots, f_m)$ *skupa polinoma* $\{f_1, f_2, \ldots, f_m\}$ *nad n promenljivih je podskup skupa K^n koji sadrži sve zajedničke nule polinoma $f_1, f_2, \ldots, f_m \in K[x_1, x_2 \ldots, x_n]$, odnosno:*

$$V(f_1, f_2, \ldots, f_m) = \{(a_1, a_2, \ldots, a_n) \in K^n \mid f_i(a_1, a_2, \ldots, a_n) = 0 \text{ za sve } 1 \leq i \leq m\}$$

Afini varijetet predstavlja rešenje sistema polinomijalnih jednačina.

Primer 13. *Skup od četiri tačke $(-2, -1), (-1, 1), (1, -1), (1, 2)$ u $\mathbb{R}^2$ je afini varijetet polinoma $f_1(x, y) = x^2 + y^2 - xy - 3$ i polinoma $f_2(x, y) = 3x^2 - y^2 - xy + 2x + 2y - 3$. Naime, on predstavlja presek elipse zadate jednačinom $x^2 + y^2 - xy - 3 = 0$ i hiperbole koja je data jednačinom $3x^2 - y^2 - xy + 2x + 2y - 3 = 0$ (slika 2.1).*

Primer za vežbu 2. *Izračunati afini varijetet $V(2x + y - 1, 3x - y + 2)$.*



Slika 2.1: Presek elipse (plavo) i hiperbole (crveno). Sve tačke sa elipse su afini varijeteti polinoma f_1, a sa hiperbole polinoma f_2. Presek elipse i hiperbole kao presek dva afina varijeteta je ponovo afini varijetet (preuzeto sa `https://www.math.tamu.edu/~sottile/teaching/15.1/Chapters/Ch1.pdf`).

2.1 Poredak monoma

Da bismo mogli da definišemo operaciju deljenja u prstenu više promenljivih, potrebno je da definišemo uređenje na skupu monoma. Naime, ako razmotrimo algoritam deljenja u prstenu jedne promenljive $K[x]$, možemo uočiti da poredak termova u polinomima predstavlja važan faktor (iako se često eksplicitno ne ističe). Na primer, pri deljenju polinoma $f(x) = x^5 - 3x^2 + 1$ polinomom $g(x) = x^2 - 4x + 7$ na standardni način, mi bismo:

1. zapisali termove u oba polinoma u opadajućem redosledu stepena po x,

2. vodeći term (term sa najvećim stepenom po x) u polinomu f je

$$x^5 = x^3 \cdot x^2 = x^3 \cdot \text{vodeci term u } g.$$

   Zatim bismo od polinoma $f(x)$ oduzeli izraz $x^3 \cdot g(x)$ da bi se poništio vodeći term i ostali bismo sa polinomom:

$$f_1(x) = f(x) - x^3 \cdot g(x) = x^5 - 3x^2 + 1 - x^3(x^2 - 4x + 7) = 4x^4 - 7x^3 - 3x^2 + 1,$$

3. ponovili bismo isti postupak sa polinomima $f_1(x)$, $f_2(x)$, itd. sve dok ne dobijemo polinom čiji je stepen manji od 2, odnosno u opštem slučaju manji od stepena polinoma g kojim vršimo deljenje.

Pošto polinom predstavlja sumu monoma, potrebno je da na jednoznačan način uredimo termove unutar polinoma u opadajućem (ili rastućem) poretku. Iz tog razloga potrebno je da budemo u mogućnosti da međusobno uporedimo svaki par monoma da bismo utvrdili njihov relativni poredak.

Ako bismo razmatrali polinome nad samo jednom promenljivom x, definisanje poretka monoma bi odgovaralo definisanju poretka nad stepenima promenljive x i zadaje se kao:

$$1 < x < x^2 < \ldots < x^{k-1} < x^k < x^{k+1} < \ldots \tag{2.1}$$

U slučaju monoma nad većim brojem promenljivih, postoji veći broj poredaka koje možemo razmatrati.

Ako bismo pak razmatrali sistem linearnih jednačina nad promenljivim $x_1, x_2, \ldots, x_n$, poredak monoma bi se sveo na uređenje promenljivih:

$$x_1 > x_2 > \ldots > x_n.$$

Napomenimo i to da kada u praksi radimo sa polinomima nad dve ili tri promenljive, promenljive uobičajeno nazivamo x, y, z umesto x_1, x_2, x_3. Ukoliko ne bude drugačije eksplicitno rečeno podrazumevaćemo uređenje promenljivih $x > y > z$.

Kad priču uopštimo na sistem nelinearnih polinoma nad većim brojem promenljivih, možemo definisati različita uređenja monoma: na primer u odnosu na neki poredak može da važi $xy^2 < y^4$ ili pak da važi $xy^2 > y^4$.

Razmotrimo skup monoma nad n promenljivih $x_1, x_2, \ldots, x_n$ za koje važi $x_1 > x_2 > \ldots > x_n$: definisanje uređenja u skupu monoma $x_1^{\alpha_1} \cdot \ldots \cdot x_n^{\alpha_n}$ odgovara definisanju uređenja nad n-torkama vrednosti $(\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{Z}^n_{\geq 0}$ njegovih ekponenata.

Definicija 3 (Poredak monoma)**.** Poredak monoma *na* $K[x_1, x_2, \ldots, x_n]$ *je proizvoljna relacija* $>$ *na skupu njegovih eksponenata* $\mathbb{Z}^n_{\geq 0} = \{(\alpha_1, \alpha_2, \ldots, \alpha_n) \mid \alpha_i \in \mathbb{Z}_{\geq 0}\}$ *koja zadovoljava:*

1. $>$ *je totalni poredak na* $\mathbb{Z}^n_{\geq 0}$ *(za svako* $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$ *važi* $\alpha > \beta$, $\alpha = \beta$ *ili* $\alpha < \beta$*),*

2. *ako je* $\alpha > \beta$ *i* $\gamma \in \mathbb{Z}^n_{\geq 0}$ *onda važi* $\alpha + \gamma > \beta + \gamma$*,*

3. $>$ *je dobro uređenje na* $\mathbb{Z}^n_{\geq 0}$ *(svaki neprazan podskup od* $\mathbb{Z}^n_{\geq 0}$ *ima najmanji element, tj. ako je* A *neprazan skup, onda postoji* $\alpha \in A$ *tako da je* $\beta > \alpha$ *za svako* $\beta \neq \alpha$ *u* A*).*

Da bi postupak deljenja polinoma bio jednostavniji, zahtevaćemo da se množenjem polinoma monomom ne menja vodeći term originalnog polinoma. Naime, ako je $x^\alpha > x^\beta$ onda zahtevamo da važi i $x^\alpha x^\gamma > x^\beta x^\gamma$. U terminima vektora eksponenata, ovo znači da ako je $\alpha > \beta$, onda za svako $\gamma \in \mathbb{Z}^n_{\geq 0}$ važi $\alpha + \gamma > \beta + \gamma$. Zato nam je potrebno drugo svojstvo poretka monoma.

Važi da je relacija poretka na $\mathbb{Z}^n_{\geq 0}$ dobro uređena ako i samo ako se svaki strogo opadajući niz elemenata u $\mathbb{Z}^n_{\geq 0}$ zaustavlja. Zahtev da je poredak monoma dobro uređen skup je potreban jer on garantuje da će se procedura deljenja polinoma više promenljivih i, analogno, Buhbergerov algoritam zaustaviti.

Postoji veći broj interesantnih poredaka monoma, a mi ćemo u nastavku razmotriti nekoliko najčešće korišćenih.

Definicija 4 (Leksikografski poredak (lex))**.** *Neka su* $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$*. Kažemo da je* $\alpha >_{lex} \beta$ *ako je u vektoru* $\alpha - \beta \in \mathbb{Z}^n$ *najlevija nenula vrednost pozitivna.*

Napomenimo da postoji veći broj leksikografskih poredaka monoma, u zavisnosti od toga kako su promenljive $x_1, x_2, \ldots, x_n$ uređene. Naime, mi smo do sada razmatrali poredak $x_1 > x_2 > \ldots > x_n$, međutim, drugačiji poredak promenljivih $x_1, x_2, \ldots, x_n$ bi dao drugačiji leksikografski poredak. Tačnije, u slučaju polinoma nad n promenljivih postoji tačno $n!$ različitih leksikografskih poredaka.

Primer 14. *Za $x > y > z$ važi:*

- $x^5y^2z^3 >_{lex(x>y>z)} x^2y^3z^4$ *jer je* $(5,2,3) - (2,3,4) = (3,-1,-1)$ *a najleviji nenula element u trojci* $(3,-1,-1)$ *je pozitivan,*
- $x^3y^5z^7 >_{lex(x>y>z)} x^3y^2z^9$ *jer je* $(3,5,7) - (3,2,9) = (0,3,-2)$ *a najleviji nenula element u trojci* $(0,3,-2)$ *je pozitivan,*
- $x >_{lex(x>y>z)} y^{200}z^{500}$ *jer je* $(1,0,0) - (0,200,500) = (1,-200,-500)$*, a najleviji nenula element u trojci* $(1,-200,-500)$ *je pozitivan.*

Primetimo da u leksikografskom poretku monoma ukupan stepen monoma nije ni od kakvog značaja. Leksikografski poredak monoma se koristi kada je potrebno transformisati sistem jednačina u gornje trougaonu formu, kako bi se on jednostavnije rešio. Međutim, pokazuje se da je za računanje Grebnerove baze korišćenje leksikografskog poretka monoma dosta skuplje, te se često izbegava, osim za vrlo jednostavna izračunavanja.

Definicija 5 (Graduirani leksikografski poredak (grlex))**.** *Neka su* $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$. *Kažemo da je* $\alpha >_{grlex} \beta$ *ako je:*

- $|\alpha| = \sum_{i=1}^n \alpha_i > |\beta| = \sum_{i=1}^n \beta_i$ *ili*
- $|\alpha| = |\beta|$ *i* $\alpha >_{lex} \beta$.

Primer 15. *Za $x > y > z$ važi:*

- $x <_{grlex(x>y>z)} y^{200}z^{500}$ *jer je* $|(1,0,0)| = 1,$ *a* $|(0,200,500)| = 700,$
- $x^3y^4z^5 >_{grlex(x>y>z)} x^4y^3z^4$ *jer je* $|(3,4,5)| = 12 > |(4,3,4)| = 11,$
- $x^5y^4z^2 >_{grlex(x>y>z)} x^3y^4z^4$ *jer je* $|(5,4,2)| = |(3,4,4)|$ *i* $(5,4,2) - (3,4,4) = (2,0,-2)$*, a krajnji levi nenula element u trojci* $(2,0,-2)$ *je pozitivan.*

Graduirani poredak monoma je pogodno koristiti kada nije cilj iz nekog polinoma eliminisati neku konkretnu promenljivu, već pre svega smanjiti stepen polinoma $p - q$ u polinomijalnoj jednačini $p = q$. Dakle, cilj ovog poretka je smanjiti ukupni stepen izraza.

Definicija 6 (Obrnuti graduirani leksikografski poredak (grevlex))**.** *Neka su* $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$. *Kažemo da je* $\alpha >_{grevlex} \beta$ *ako je*

- $|\alpha| > |\beta|$ *ili*
- $|\alpha| = |\beta|$ *i u vektoru* $\alpha - \beta \in \mathbb{Z}^n$ *najdesnija nenula vrednost je negativna.*

Primer 16. *Za $x > y > z$ važi:*

- $x^4y^2z^5 >_{grevlex(x>y>z)} x^4y^3z^2$ *jer je* $|(4,2,5)| = 11 > |(4,3,2)| = 9$,
- $xy^4z^2 >_{grevlex(x>y>z)} x^2yz^4$ *jer je* $|(1,4,2)| = |(2,1,4)|$ *i važi* $(1,4,2) - (2,1,4) = (-1,3,-2)$ *a krajnji desni nenula element je negativan. Primetimo da bi za ova dva monoma važilo* $xy^4z^2 <_{grlex(x>y>z)} x^2yz^4$.

Kao i u slučaju leksikografskog poretka, u zavisnosti od toga kako su promenljive uređene postoji $n!$ različitih graduiranih i obrnuto graduiranih leksikografskih poredaka monoma.

Primetimo da za utvrđivanje leksikografskog poretka ukupni stepen monoma nije od važnosti. U slučaju graduiranog leksikografskog poretka i obrnutog graduiranog leksikografskog poretka, ukupni stepen monoma igra veći značaj nego niz eksponenata tog monoma.

Pokazuje se da je računanje Grebnerove baze najjednostavnije u slučaju kada se koristi graduirani leksikografski poredak monoma, pa se iz tog razloga često koristi.

Definicija 7 (Težinski poredak monoma)**.** *Neka je $c \in \mathbb{R}[x_1, x_2, \ldots, x_n]$ proizvoljni vektor. Njime je definisan težinski poredak monoma $>_c$ na sledeći način: $\alpha >_c \beta$ ako je:*

- $c \cdot \alpha > c \cdot \beta$ *ili je*
- $c \cdot \alpha = c \cdot \beta$ *i* $\alpha >_{lex} \beta$,

gde je sa $c \cdot \alpha$ označen skalarni proizvod vektora c i α.

Primer 17. *Za $x > y > z$ i $c = (1,5,10)$ važi:*

- $xz^3 >_c x^5yz^2$ *jer je* $(1,5,10) \cdot (1,0,3) = 31$ *i* $(1,5,10) \cdot (5,1,2) = 30$ *i* $31 > 30$.

Definisanje poretka nad monomima nam omogućava da unutar polinoma uredimo monome na jedinstven način.

Primer 18. *Razmotrimo primer polinoma*

$$f = 4xy^2z + 4z^2 - 5x^3 + 7x^2z^2 \in K[x,y,z]$$

i poretka promenljivih $x > y > z$. Ako preuredimo termove polinoma u opadajućem redosledu u odnosu na leksikografski poredak monoma dobijamo naredni zapis polinoma f:

$$f = -5x^3 + 7x^2z^2 + 4xy^2z + 4z^2$$

Ako bismo umesto toga razmatrali graduirani leksikografski poredak monoma, dobili bismo:

$$f = 7x^2z^2 + 4xy^2z - 5x^3 + 4z^2$$

dok bismo u odnosu na obrnuti graduirani leksikografski poredak monoma dobili:

$$f = 4xy^2z + 7x^2z^2 - 5x^3 + 4z^2$$

Primer za vežbu 3. *Urediti monome polinoma* $f(x, y, z) = 3yz^3 - x^2y^2 + x^3 + y^2z^3$ *u odnosu na (a) leksikografski poredak termova (b) graduirani leksikografski poredak termova ako važi* $x > y > z$.

Primer za vežbu 4. *Urediti monome polinoma* $f(x, y, z) = x^6 + y^5 - 2x^5z^3 + 4x^4y^3z^4 + 3x^3y^4z^4 - 6z^4 + xyz - 4y^3$ *korišćenjem leksikografskog, graduiranog leksikografskog i obrnutog graduiranog leksikografskog poretka monoma ako važi* $x > y > z$.

Praktična vežba 2. *Pri radu sa polinomima u alatu Singular neophodno je zadati željeni poredak monoma. Oznaka poretka monoma završava se karakterom* `p`*, čime se referiše na prsten polinoma, i može biti:*

- `lp` *za leksikografski poredak monoma,*
- `Dp` *za graduirani leksikografski poredak monoma,*
- `dp` *za obrnuti leksikografski poredak monoma.*

Monomi unutar polinoma se ispisuju uređeno u opadajućem poretku u odnosu na izabrani poredak monoma, od najvećeg ka najmanjem.

Na primer, možemo izlistati monome polinoma $4xy^2z + 4z^2 - 5x^3 + 7x^2z^2$ *definisanog nad promenljivim* x*,* y *i* z *u leksikografskom poretku za koji važi* $x > y > z$ *na sledeći način:*

```
> ring A1 = 0, (x,y,z), lp;
> poly f = 4xy2z + 4z2 - 5x3 + 7x2z2;
> f;
-5x3+7x2z2+4xy2z+4z2
```

Ako bismo želeli da članove polinoma izlistamo u graduiranom leksikografskom poretku monoma, umesto parametra `lp` *naveli bismo* `Dp`*:*

```
> ring A2 = 0, (x,y,z), Dp;
> poly g = 4xy2z + 4z2 - 5x3 + 7x2z2;
> g;
7x2z2+4xy2z-5x3+4z2
```

Primetimo da je dobijeni poredak monoma u polinomu sad drugačiji. Ako bismo želeli da članove polinoma uredimo u obrnutom graduiranom leksikografskom poretku monoma, kao oznaku poretka naveli bismo `dp`*:*

```
> ring A3 = 0, (x,y,z), dp;
> poly h = 4xy2z + 4z2 - 5x3 + 7x2z2;
> h;
4xy2z+7x2z2-5x3+4z2
```

Ako bismo pak hteli da koristimo težinski poredak monoma sa težinskom koeficijentima $(1, 5, 2)$ *trebalo bi kao oznaku poretka navesti* `Wp` *za kojim slede koordinate težinskog vektora. Dužina težinskog vektora odgovara broju promenljivih nad kojim je polinom definisan.*

```
> ring A4 = 0, (x,y,z), Wp(1,5,2);
> poly u = 4xy2z + 4z2 - 5x3 + 7x2z2;
> u;
4xy2z+7x2z2+4z2-5x3
```

Primer za vežbu 5. *Dokazati da je* $(0, 0, \dots, 0)$ *najmanji element u* $\mathbb{Z}^n_{\geq 0}$ *u odnosu na razmatrane poretke monoma.*

Definicija 8 (Multistepen, vodeći koeficijent, vodeći monom, vodeći term)**.** *Neka je* $x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ *i neka je* $f = \sum_\alpha a_\alpha x^\alpha$ *nenula polinom iz* $K[x_1, x_2, \dots, x_n]$*, gde je* $\alpha \in \mathbb{Z}^n_{\geq 0}$ *i* $a_\alpha \in K$*.* Multistepen *polinoma* f *je*

$$md(f) = \max\{\alpha \in \mathbb{Z}^n_{\geq 0} \mid a_\alpha \neq 0\}$$

pri čemu se maksimum gleda u odnosu na odabrani poredak monoma. Vodeći koeficijent *polinoma* f *je* $LC(f) = a_{md(f)} \in K$*,* vodeći monom *polinoma* f *je* $LM(f) = x^{md(f)}$*, a* vodeći term *polinoma* f *je* $LT(f) = LC(f) \cdot LM(f) = a_{md(f)} \cdot x^{md(f)}$*.*

Dakle, multistepen polinoma je najveća n-torka eksponenata u odnosu na izabrani poredak monoma, dok je vodeći koeficijent polinoma koeficijent uz član polinoma sa najvećim eksponentom.

Primer 19. *Neka je* $f(x, y, z) = 2x^4 - 4x^2y^3 + 5x^2y^2z - 3z^4$ *i neka važi* $x > y > z$*. Ako je* $>$ *graduirani leksikografski poredak monoma tada važi* $md(f) = (2, 3, 0)$*,* $LC(f) = -4$*,* $LM(f) = x^2y^3$*, a* $LT(f) = -4x^2y^3$*.*

Praktična vežba 3. *Proverimo prethodni primer u alatu Singular. U alatu Singular multistepen polinoma možemo dobiti pozivom funkcije* `leadexp` *(skraćeno od vodeći eksponent), vodeći koeficijent polinoma pozivom funkcije* `leadcoef`*, vodeći monom funkcijom* `leadmonom`*, a vodeći term funkcijom* `lead`*.*

```
> ring A = 0, (x,y,z), Dp;
> poly f = 2x4 - 4x2y3 + 5x2y2z - 4z4;
> leadexp(f);
2,3,0
> leadcoef(f);
-4
> leadmonom(f);
x2y3
> lead(f);
-4x2y3
```

Primer za vežbu 6. *Neka je* $f(x,y,z) = 2x^4 - 4x^2y^3 + 5x^2y^2z - 4z^4$ *i neka važi* $z > y > x$*. Izračunati multistepen, vodeći koeficijent, vodeći monom i vodeći term u odnosu na leksikografski poredak monoma.*

Primer za vežbu 7. *Neka je* $f(x,y,z) = 2x^2y^8 - 3x^5yz^4 + xyz^3 - xy^4$ *i neka važi* $x > y > z$*. Izračunati multistepen, vodeći koeficijent, vodeći monom i vodeći term u odnosu na graduirani leksikografski i u odnosu na obrnuti graduirani leksikografski poredak monoma.*

Praktična vežba 4. *Alat Singular omogućava izvršavanje komandi koje se nalaze u nekoj datoteci. Na primer, neka se datoteka* `ulaz.txt` *nalazi u tekućem direktorijumu i neka ima naredni sadržaj:*

```
int a = 5;
int b = 10;
a+b;
```

Pozivom naredbe `Singular -q < ulaz.txt` *dobijamo naredni sadržaj na izlazu:*

```
15
```

Opciju `-q` *navodimo da se ne bi ispisivala pozdravna i odjavna poruka, već samo rezultat izračunavanja. Moguće je rezultat izračunavanja zapamtiti u datoteci* `izlaz.txt` *narednom naredbom* `Singular -q < ulaz.txt > izlaz.txt`

2.2 Deljenje polinoma u prstenu više promenljivih

Sada kada smo definisali poredak monoma, možemo definisati deljenje polinoma skupom polinoma u prstenu više promenljivih. Zadatak je za proizvoljni polinom f i skup polinoma $(f_1, f_2, \ldots, f_m)$ izračunati količnike $q_1, q_2, \ldots, q_m$ i ostatak r tako da važi $f = q_1 f_1 + q_2 f_2 + \ldots + q_m f_m + r$. Osnovna ideja algoritma deljenja polinoma f skupom polinoma $(f_1, f_2, \ldots, f_m)$ ista je kao i u slučaju polinoma definisanih nad jednom promenljivom: želimo da poništimo vodeći term polinoma f množenjem nekog od polinoma f_i odgovarajućim monomom i oduzimanjem tog proizvoda od polinoma f. Onda ovaj monom postaje term u odgovarajućem količniku q_i.

Primer 20. *Podelimo polinom $f(x, y) = xy^2 + 1$ polinomima $f_1(x, y) = xy + 1$ i $f_2(x, y) = y + 1$, korišćenjem leksikografskog poretka za koji važi $x > y$. I vodeći term polinoma f_1 koji je jednak $LT(f_1) = xy$ i vodeći term polinoma f_2 koji je jednak $LT(f_2) = y$ dele vodeći term polinoma f: $LT(f) = xy^2$, te imamo mogućnost izbora kojim od polinoma f_1 i f_2 ćemo najpre vršiti deljenje. Izaberimo da najpre vršimo deljenje polinomom f_1. Pošto važi $LT(f) = y \cdot LT(f_1)$, kao količnik dobijamo y, a potom oduzimanjem izraza $y \cdot f_1$ od f dobijamo novi polinom*

$$f' = f - y \cdot f_1 = -y + 1.$$

Nastavljamo isti postupak sa polinomom f'. Ovoga puta moramo da koristimo polinom f_2 jer $LT(f_1) = xy$ ne deli $LT(f') = -y$. Kao ostatak pri deljenju polinoma f' polinomom $y + 1$ dobijamo vrednost 2. Pošto ni $LT(f_1)$ ni $LT(f_2)$ ne dele 2, ostatak pri deljenju polinoma f polinomima f_1 i f_2 je $r = 2$. Dakle, došli smo do narednog izraza:

$$xy^2 + 1 = y \cdot (xy + 1) + (-1) \cdot (y + 1) + 2$$

odnosno

$$f = y \cdot f_1 - f_2 + 2.$$

Primer 21. *Ilustrujmo još jedan scenario koji se može dogoditi kada vršimo deljenje polinoma u prstenu više promenljivih.*

Razmotrimo deljenje polinoma $f = x^2y + xy^2 + y^2$ polinomima $f_1 = xy - 1$ i $f_2 = y^2 - 1$. Kao i u prethodnom primeru kao poredak monoma razmatraćemo leksikografski poredak za koji važi $x > y$. Vodeći term polinoma f_1 deli vodeći term polinoma f i važi $LT(f) = x \cdot LT(f_1)$ pa vršimo deljenje polinoma f polinomom f_1 i ostajemo sa polinomom:

$$f' = f - xf_1 = (x^2y + xy^2 + y^2) - x(xy - 1) = xy^2 + x + y^2$$

Pošto vodeći term polinoma f_1 deli vodeći term polinoma f' vršimo deljenje polinoma f' polinomom f_1 i dobijamo:

$$f'' = f' - yf_1 = (xy^2 + x + y^2) - y(xy - 1) = x + y^2 + y,$$

odnosno dobijamo

$$f = (x + y) \cdot f_1 + (x + y^2 + y).$$

Primetimo da u ovom trenutku niti $LT(f_1) = xy$ niti $LT(f_2) = y^2$ dele $LT(x+y^2+y) = x$. Ipak, $x+y^2+y$ ne može biti ostatak pri deljenju polinoma f polinomima f_1 i f_2 jer $LT(f_2)$ deli y^2. Stoga izraz $x + y^2 + y$ nazivamo međuostatkom, član x međuostatka prebacujemo u ostatak, a nakon toga razmatramo da li možemo nastaviti sa deljenjem[2]. Ako je vodeći term međuostatka deljiv sa $LT(f_1)$ ili sa $LT(f_2)$, nastavljamo na uobičajen način, a ako ga nijedan od vodećih termova polinoma f_1 i f_2 ne deli, prebacujemo vodeći term međuostatka u kolonu ostatka. U ovom primeru se, dakle, kao konačna vrednost ostatka dobija $x + y + 1$ i važi:

$$x^2y + xy^2 + y^2 = (x + y) \cdot f_1 + 1 \cdot f_2 + x + y + 1.$$

Izvodimo naredni zaključak: ostatak pri deljenju polinoma f polinomima f_1 i f_2 je suma monoma, pri čemu nijedan od njih nije deljiv niti vodećim termom polinoma f_1 niti vodećim termom polinoma f_2.

Prethodni primer u potpunosti ilustruje algoritam deljenja polinoma u prstenu većeg broja promenljivih. On nam, takođe, pokazuje koja svojstva želimo da poseduje ostatak: nijedan od njegovih termova ne sme biti deljiv vodećim termom nijednog od polinoma kojima vršimo deljenje. Sada možemo i formalno formulisati algoritam deljenja u prstenu više promenljivih.

Teorema 2 (Algoritam deljenja u prstenu više promenljivih)**.** *Neka je fiksiran poredak monoma $>$ na $\mathbb{Z}^n_{\geq 0}$ i neka je $F = (f_1, f_2, \dots, f_m)$ uređena m-torka polinoma. Tada se svako $f \in K[x_1, x_2, \dots, x_n]$ može zapisati kao:*

$$f = q_1f_1 + q_2f_2 + \ldots + q_mf_m + r$$

gde su $q_i, r \in K[x_1, x_2, \dots, x_n]$ i pritom važi $r = 0$ ili je r linearna kombinacija monoma sa koeficijentima u K, tako da nijedan od njih nije deljiv niti sa jednim od termova $LT(f_1), LT(f_2), \dots, LT(f_m)$. Vrednost r zovemo ostatkom *pri deljenju polinoma f skupom polinoma F. Dodatno, ako je $q_if_i \neq 0$ tada je $md(f) \geq md(q_if_i)$.*

Algoritam *Deljenje polinoma f skupom polinoma F*
Ulaz: polinom f, skup polinoma $F = (f_1, f_2, \dots, f_m)$
Izlaz: količnici $q_1, q_2, \dots, q_m$ i ostatak r

$q_1 \leftarrow 0, \dots, q_m \leftarrow 0$
$r \leftarrow 0$
$h \leftarrow f$ {međuostatak pri deljenju}
while $h \neq 0$
  if postoji j tako da $LT(f_j)$ deli $LT(h)$
    za najmanje j tako da $LT(f_j)$ deli $LT(h)$ {vršimo deljenje}
    $q_j \leftarrow q_j + \frac{LT(h)}{LT(f_j)}$
    $h \leftarrow h - \frac{LT(h)}{LT(f_j)} f_j$
  else {dodajemo $LT(h)$ ostatku }

[2] Primetimo da se ovakva situacija nikada ne javlja u slučaju polinoma jedne promenljive.

10. $\quad r \leftarrow r + LT(h)$
11. $\quad h \leftarrow h - LT(h)$
12. **return** $q_1, q_2, \ldots, q_m, r$

Primer 22. *U prstenu $\mathbb{Q}[x,y]$ u kom razmatramo leksikografski poredak monoma za koji važi $x > y$, podelimo polinom $f = x^2y + xy^3 + xy^2$ polinomima $f_1 = xy + 1$ i $f_2 = y^2 + 1$, pri čemu najpre vršimo deljenje polinomom f_1 pa polinomom f_2.*

Inicijalna vrednost polinoma h jednaka je f. Primetimo da $LT(f_1)|LT(h)$ te je:

$$\begin{aligned} q_1 &= 0 + \frac{x^2y}{xy} = x \\ h &= (x^2y + xy^3 + xy^2) - x(xy+1) = xy^3 + xy^2 - x. \end{aligned}$$

U narednoj iteraciji vidimo da i dalje $LT(f_1)|LT(h)$ te je:

$$\begin{aligned} q_1 &= x + \frac{xy^3}{xy} = x + y^2 \\ h &= (xy^3 + xy^2 - x) - y^2(xy+1) = xy^2 - x - y^2. \end{aligned}$$

I u narednoj iteraciji važi $LT(f_1)|LT(h)$ te je:

$$\begin{aligned} q_1 &= x + y^2 + \frac{xy^2}{xy} = x + y^2 + y \\ h &= (xy^2 - x - y^2) - y(xy+1) = -x - y^2 - y. \end{aligned}$$

Primetimo da sad važi $LT(f_1) \not| LT(h)$ i istovremeno važi $LT(f_2) \not| LT(h)$, te u vrednost ostatka prebacujemo vodeći term međuostatka h:

$$\begin{aligned} r &= 0 + (-x) = -x \\ h &= -x - y^2 - y - (-x) = -y^2 - y. \end{aligned}$$

U narednoj iteraciji važi da $LT(f_1) \not| LT(h)$, ali zato važi $LT(f_2)|LT(h)$, te je:

$$\begin{aligned} q_2 &= 0 + \frac{-y^2}{y^2} = -1 \\ h &= (-y^2 - y) - (-1) \cdot (y^2 + 1) = -y + 1. \end{aligned}$$

U narednom prolazu $LT(f_1) \not| LT(h)$ i istovremeno $LT(f_2) \not| LT(h)$ te ažuriramo vrednost ostatka:

$$\begin{aligned} r &= -x + (-y) = -x - y \\ h &= (-y + 1) - (-y) = 1. \end{aligned}$$

U narednoj iteraciji takođe važi $LT(f_1) \not| LT(h)$ i $LT(f_2) \not| LT(h)$ te dobijamo:

$$\begin{aligned} r &= -x - y + 1 \\ h &= 1 - 1 = 0. \end{aligned}$$

Konačno, dobijamo:

$$\begin{aligned} q_1 &= x + y^2 + y \\ q_2 &= -1 \\ r &= -x - y + 1 \end{aligned}$$

odnosno važi:

$$x^2y + xy^3 + xy^2 = (x + y^2 + y) \cdot (xy + 1) - 1 \cdot (y^2 + 1) + (-x - y + 1)$$

Primer 23. *Razmotrimo primer polinoma $f = x^2+xy+2x^3$ i skupa polinoma $F = (f_1, f_2)$ gde je $f_1 = xy-x^3$, $f_2 = x+y^2$ i neka je izabran leksikografski poredak monoma za koji važi $x > y$. Ukoliko najpre vršimo deljenje polinomom f_1, a zatim polinomom f_2, dobijamo:*

$$f = -2f_1 + (x - y^2 + 3y)f_2 + (y^4 - 3y^3)$$

Ukoliko promenimo značaj polinoma f_1 i f_2 dobijamo:

$$f = (2x^2 + 2xy^4 - 2xy^2 + x - y^2 + y)f_2 + 0 \cdot f_1 + (-2y^6 + y^4 - y^3)$$

Primetimo da je ovako definisana procedura deljenja osetljiva na redosled polinoma f_1 i f_2 u F: izmenom redosleda polinoma menjaju se količnici q_1 i q_2 i ostatak r. Takođe, ako bismo zadržali poredak polinoma u F, ali izmenili poredak monoma i umesto poretka promenljivih $x < y$ razmatrali poredak za koji važi $y < x$ dobile bi se drugačije vrednosti količnika q_1 i q_2 i ostatka r. Ovaj problem se, međutim, neće javljati kada budemo vršili deljenje polinomima Grebnerove baze.

Primer za vežbu 8. *Podeliti polinom $f(x, y) = x^2y - y$ skupom polinoma $F = (f_1, f_2)$ pri čemu je $f_1 = xy + x$ i $f_2 = x^2 - 1$ pod pretpostavkom leksikografskog poretka za koji važi $x > y$. Šta se dešava ukoliko se promeni poredak polinoma f_1 i f_2?*

Praktična vežba 5. *Ideal nad datim skupom polinoma se u programu Singular definiše naredbom* `ideal` *za kojom slede polinomi nad kojim je definisan razdvojeni zapetama. Funkcijom* `reduce` *se vrši svođenje polinoma u odnosu na datu bazu ideala, odnosno računa ostatak pri deljenju polinoma f skupom polinoma $(f_1, f_2, \ldots, f_m)$. Izračunajmo ostatak pri deljenju polinoma iz primera 23.*

```
> ring r = 0, (x,y), lp;
```

```
> poly f1 = xy - x3;
> poly f2 = x + y2;
> ideal I = f1, f2;
> poly f = x2 + xy + 2x3;
> reduce(f,I);
// ** I is no standard basis
-2y6+y4-y3
```

Poruka koju dobijamo jeste da `I` *nije Grebnerova baza datog ideala, te da vrednost ostatka nije relevantna za donošenje zaključaka o pripadnosti polinoma idealu.*

Primetimo da ako bismo zamenili poredak polinoma u definiciji ideala dobili bismo istu vrednost ostatka. Naime u programu Singular ne možemo zadati prioritet polinomima f_i*. Međutim, ako bi se promenio poredak promenljivih i razmatrao leksikografski poredak za koji važi* $y > x$*, dobila bi se drugačija vrednost ostatka:*

```
> ring r = 0, (y,x), lp;
> poly f1 = xy - x3;
> poly f2 = x + y2;
> ideal I = f1, f2;
> poly f = x2 + xy + 2x3;
> reduce(f,I);
// ** I is no standard basis
3x3+x2
```

Sada kada smo definisali algoritam deljenja u prstenu polinoma više promenljivih, možemo se zapitati da li se odgovor na pitanje da li dati polinom $f \in K[x_1, x_2, \ldots, x_n]$ pripada idealu $I = \langle f_1, f_2, \ldots, f_m \rangle$ može dobiti primenom algoritma deljenja polinoma f skupom polinoma $F = (f_1, f_2, \ldots, f_m)$. Pokazuje se sledeće: ako je ostatak pri deljenju polinoma f skupom polinoma $f_1, f_2, \ldots, f_m$ jednak nuli onda je jasno da polinom f pripada idealu I. Međutim, ako je dobijeni ostatak različit od nule, to nužno ne znači da polinom f ne pripada idealu I. Naime, možda postoji neki drugi način da ga podelimo (na primer promenimo značaj polinoma f_i u F), tako da se dobije ostatak 0, kao što ćemo videti u narednom primeru.

Primer 24. *Razmotrimo primer polinoma* $f_1 = x^2 - 1$ *i* $f_2 = xy + 2$ *i polinoma* $f = x^2y + xy + 2x + 2$ *u odnosu na leksikografski poredak monoma za koji važi* $x > y$*. Deljenjem polinoma* f *polinomima* f_1 *i* f_2 *dobijamo:*

$$f = yf_1 + f_2 + (2x + y)$$

Dobijeni ostatak $r = 2x + y$ *je različit od nule i stoga bismo mogli zaključiti da polinom* f *ne pripada idealu* $\langle f_1, f_2 \rangle$*, ali ako bismo promenili poredak delilaca u* f_2, f_1 *dobili bismo:*

$$f = 0f_1 + (x + 1)f_2 + 0$$

odnosno zaključili bismo da polinom f *pripada idealu* $\langle f_1, f_2 \rangle$*.*

Primer 25. *Neka su dati polinomi* $f_1 = x + y$ *i* $f_2 = x - y$ *i polinom* $f = 2y$ *u prstenu polinoma* $\mathbb{R}[x, y]$ *i neka je fiksiran leksikografski poredak monoma za koji važi* $x > y$. *Očigledno važi* $f = f_1 - f_2 \in \langle f_1, f_2 \rangle$, *ali s obzirom na to da je* $LT(x+y) = LT(x-y) = x$ *i da važi* $x > y$, *razmatrani algoritam deljenja vraća kao ostatak* $r = 2y$.

Slično bi se desilo i u slučaju leksikografskog poretka za koji važi $y > x$.

Ipak, postoje baze ideala I za koje je ostatak pri deljenju polinoma f datom bazom jedinstven i koje omogućavaju da se dâ nedvosmislen odgovor na pitanje pripada li polinom f idealu I ili ne. Takve baze zovu se *Grebnerove baze*. Pored metode Grebnerovih baza postoje i drugi algoritmi za proveru pripadnosti polinoma idealu kao što je Vuov metod.

Glava 3

Grebnerova baza

Grebnerova baza je specijalni generatorski skup (tj. baza) ideala $\langle f_1, f_2, \ldots, f_m \rangle$ za koji algoritam deljenja proizvoljnog polinoma f tim skupom generatora vraća ostatak 0 ako i samo ako $f \in \langle f_1, f_2, \ldots, f_m \rangle$.

Primetimo da važi naredna teorema.

Teorema 3 (Hilbertova osnovna teorema)**.** *Svaki ideal $I \subset K[x_1, x_2, \ldots, x_n]$ je konačno generisan.*

Naime, u prstenu polinoma nad konačno mnogo promenljivih, svaki ideal je generisan konačnim brojem elemenata, odnosno ima konačnu bazu.

Neka je I proizvoljni ideal $I \subset K[x_1, x_2, \ldots, x_n]$. Označimo sa $LT(I)$ skup vodećih termova nenula polinoma ideala I:

$$LT(I) = \{cx^\alpha \mid \text{postoji } f \in I \text{ tako da je } LT(f) = cx^\alpha\}$$

a sa $\langle LT(I) \rangle$ ideal generisan elementima iz $LT(I)$, odnosno važi:

$$\langle LT(I) \rangle = \langle LT(f) \mid f \in I \rangle.$$

Drugim rečima, ovo je ideal generisan vodećim termovima polinoma ideala I.

Već smo videli da vodeći termovi polinoma igraju važnu ulogu u algoritmu deljenja polinoma. Za dati konačno generisani ideal $I = \langle f_1, f_2, \ldots, f_m \rangle$ primamljivo je poverovati da je ideal generisan vodećim termovima polinoma f_i jednak baš $\langle LT(I) \rangle$. Međutim, ovo ne važi uvek: naime, ideali $\langle LT(f_1), \ldots, LT(f_m) \rangle$ i $\langle LT(I) \rangle$ se mogu razlikovati.

Primer 26. *Razmotrimo ideal $I = \langle x + y, x \rangle \subset K[x, y]$. Korišćenjem leksikografskog poretka monoma za koji važi $x > y$ dobijamo $LT(x + y) = LT(x) = x$, te je $\langle LT(x + y), LT(x) \rangle = \langle x \rangle$. Međutim, $y = (x + y) - x \in I$ i važi $LT(y) = y \in LT(I)$, a istovremeno važi $y \notin \langle x \rangle$. Stoga je $\langle LT(I) \rangle \neq \langle LT(x + y), LT(x) \rangle$.*

Primer 27. *Neka je* $I = \langle x^2+1, xy\rangle$ *i razmotrimo leksikografski poredak monoma za koji važi* $x > y$. *Važi* $LT(x^2+1) = x^2$ *i* $LT(xy) = xy$, *pa je* $\langle LT(x^2+1), LT(xy)\rangle = \langle x^2, xy\rangle$. *S obzirom na to da važi* $y(x^2+1) - x(xy) = y$ *znamo da* $y \in I$ *i stoga* $LT(y) \in \langle LT(I)\rangle$. *Međutim,* $LT(y) = y \notin \langle x^2, xy\rangle$. *Stoga,* $\langle LT(I)\rangle \neq \langle LT(x^2+1), LT(xy)\rangle$.

Primer za vežbu 9. *Neka je* $I = \langle g_1, g_2, g_3\rangle \subset \mathbb{R}[x, y, z]$ *gde je* $g_1 = xy^2 - xz + y, g_2 = xy - z^2$ *i* $g_3 = x - zy^4$. *Korišćenjem leksikografskog poretka monoma dati primer polinoma* $g \in I$ *tako da važi* $LT(g) \notin \langle LT(g_1), LT(g_2), LT(g_3)\rangle$.

Ipak, iako za proizvoljne polinome $f_1, f_2, \ldots, f_m$ i ideal $I = \langle f_1, f_2, \ldots, f_m\rangle$ nužno ne važi da je $\langle LT(I)\rangle = \langle LT(f_1), \ldots, LT(f_m)\rangle$, postoje polinomi za koje će ovo tvrđenje važiti.

Definicija 9. Grebnerova baza *ideala* $I \subset K[x_1, x_2, \ldots, x_n]$ *(u odnosu na dati poredak monoma) je konačni podskup* $G = \{g_1, g_2, \ldots, g_t\}$ *ideala* I *tako da važi:*

$$\langle LT(I)\rangle = \langle LT(g_1), LT(g_2), \ldots, LT(g_t)\rangle$$

Dakle, konačni podskup ideala I je Grebnerova baza ako su vodeći termovi elemenata iz G dovoljni da se generiše čitav ideal $\langle LT(I)\rangle$. Alternativno, Grebnerova baza se može okarakterisati i na sledeći način: vodeći term svakog polinoma ideala I je umnožak vodećeg terma nekog polinoma baze.

Naredna važna tvrđenja navodimo bez dokaza.

Teorema 4. *Grebnerova baza ideala* I *jeste baza ideala* I.

Teorema 5. *Svaki nenula ideal* $I \subset K[x_1, x_2, \ldots, x_n]$ *ima Grebnerovu bazu.*

Teorema 6. *Ako je* $G = \{g_1, g_2, \ldots, g_t\}$ *Grebnerova baza ideala* I, *ostatak pri deljenju polinoma* f *polinomima Grebnerove baze za proizvoljno* $f \in I$ *ne zavisi od poretka polinoma* g_i *u* G.

Ispitivanje da li polinom $f \in K[x_1, x_2, \ldots, x_n]$ pripada idealu $I = \langle f_1, f_2, \ldots, f_m\rangle$ može se svesti na izračunavanje Grebnerove baze G ideala I i traženje ostatka pri deljenju polinoma f polinomima baze G.

Ostaje još pitanje kako za dati ideal I konstruisati Grebnerovu bazu. Postoji veći broj različitih algoritama za izračunavanje Grebnerove baze. Najpoznatiji je Buhbergerov algoritam koji koristi koncept S-polinoma koji predstavlja uopštenje S-polinoma pomenutog u primeru 6.

Definicija 10 (S-polinom)**.** *Neka su* $f, g \in K[x_1, x_2, \ldots, x_n]$ *dva nenula polinoma i neka je sa* z *označen najmanji zajednički sadržalac njihovih vodećih monoma:*

$$z = NZS(LM(f), LM(g)).$$

Tada je S-polinom *polinoma f i g jednak:*

$$S(f,g) = \frac{z}{LT(f)} \cdot f - \frac{z}{LT(g)} \cdot g$$

Primer 28. *Neka je dat prsten polinoma $\mathbb{R}[x,y]$ i dva polinoma iz ovog prstena: $f = x^3y^2 - x^2y^3$ i $g = 3x^4y + y^2$. Ako razmatramo graduirani leksikografski poredak monoma za koji važi $x > y$ onda je $LM(f) = x^3y^2$, $LM(g) = x^4y$, a najmanji zajednički sadržalac njihovih vodećih monoma jednak je x^4y^2 i važi:*

$$S(f,g) = \frac{x^4y^2}{x^3y^2} \cdot f - \frac{x^4y^2}{3x^4y} \cdot g = x \cdot f - \frac{1}{3} \cdot y \cdot g = -x^3y^3 - \frac{1}{3}y^3$$

Praktična vežba 6. *U programu Singular postoji funkcija* `spoly` *u biblioteci* `"teachstd.lib"` *koja računa S-polinom dva data polinoma. Za učitavanje biblioteke u sesiju, u Singularu se koristi naredba* `LIB`*:*

```
> LIB "teachstd.lib";
> poly f = x3y2 - x2y3;
> poly g = 3x4y + y2;
> spoly(f,g)
-x3y3-1/3y3
```

Primetimo da S-polinomi omogućavaju poništavanje vodećih termova polinoma f i g. Na osnovu ovog opažanja, Buhberger je definisao naredni kriterijum.

Primer za vežbu 10. *Izračunati S-polinom polinoma $f = xy^3z + y^4 + y^2z^2$ i $g = x^2y + xz^4 + y^2z^2$ iz prstena $\mathbb{R}[x,y,z]$ u odnosu na leksikografski poredak monoma za koji važi $x > y > z$.*

Teorema 7 (Buhbergerova teorema)**.** *Neka je I ideal. Tada je baza $G = \{g_1, g_2, \ldots, g_t\}$ ideala I Grebnerova baza ideala I ako i samo ako je za svako $i \neq j$ ostatak pri deljenju S-polinoma $S(g_i, g_j)$ polinomima baze G jednak nula.*

Buhbergerova teorema nam daje kriterijum po kome možemo da utvrdimo da li je neka baza Grebnerova ili ne. Ostaje pitanje, ako baza nije Grebnerova, da li je možemo nekako “popraviti” tako da ona to bude?

Primer 29. *Razmotrimo prsten* $\mathbb{Q}[x, y]$ *sa graduiranim leksikografskim poretkom monoma za koji važi* $x > y$ *i neka je* $I = \langle f_1, f_2 \rangle = \langle x^3 - 2xy, x^2y - 2y^2 + x \rangle$*. Skup* (f_1, f_2) *nije Grebnerova baza ideala* I *jer je* $S(f_1, f_2) = -x^2$*, pa važi:*

$$LT(S(f_1, f_2)) = -x^2 \notin \langle LT(f_1), LT(f_2) \rangle = \langle x^3, x^2y \rangle.$$

Da bismo dobili Grebnerovu bazu, prirodna ideja je nekako proširiti polazni skup baznih elemenata. Koje nove elemente treba dodati? S obzirom na to da je ostatak pri deljenju S-polinoma $S(f_1, f_2) = -x^2 \in I$ *sa* $F = (f_1, f_2)$ *jednak* $-x^2$*, deluje intuitivno dodati taj ostatak kao novi element baze:* $f_3 = -x^2$*.*

Razmotrimo sada skup polinoma $\{f_1, f_2, f_3\}$*. Primetimo ponovo da je* $S(f_1, f_3) = (x^3 - 2xy) - (-x)(-x^2) = -2xy$ *i da je ostatak pri deljenju ovog S-polinoma sa* $F = (f_1, f_2, f_3)$ *jednak* $-2xy$ *i različit je od 0. Stoga i ovaj ostatak dodajemo kao novi element baze:* $f_4 = -2xy$*. Ako sada razmotrimo novu bazu* $F = (f_1, f_2, f_3, f_4)$ *možemo uočiti da je ostatak pri deljenju S-polinoma* $S(f_2, f_3) = (x^2y - 2y^2 + x) - (-y)(-x^2) = -2y^2 + x$ *sa* F *različit od nule i ovaj ostatak dodajemo kao novi element u skup baznih elemenata* $f_5 = -2y^2 + x$*. Sada možemo proveriti da je ostatak pri deljenju proizvoljnog S-polinoma* $S(f_i, f_j)$ *sa* F *jednak* 0 *za svako* $1 \leq i < j \leq 5$*. Konačno, skup* $F = (f_1, f_2, f_3, f_4, f_5)$ *predstavlja jednu Grebnerovu bazu ideala* I*.*

Primer 30. *Baza* $B = \{f, g\}$ *gde je* $f = xy + 2x - z$ *i* $g = x^2 + 2y - z$ *nije Grebnerova baza ideala* $\langle f, g \rangle$ *u odnosu na leksikografski poredak jer je ostatak pri deljenju S-polinoma:*

$$S(f, g) = x(xy + 2x - z) - y(x^2 + 2y - z) = 2x^2 - 2y^2 - xz + yz$$

sa polinomima baze B *jednak* $-xz - 2y^2 + yz - 4y + 2z$*, odnosno različit je od nule.*

Primer za vežbu 11. *Ako razmatramo graduirani leksikografski poredak monoma za koji važi* $x > y > z$ *da li je* $\{x^4y^2 - z^5, x^3y^3 - 1, x^2y^4 - 2z\}$ *Grebnerova baza ideala generisanog ovim polinomima?*

Primer za vežbu 12. *Pokazati da je baza* $\{x + z, y - z\}$ *Grebnerova baza.*

Dakle, za bazu važi da je Grebnerova baza ako i samo ako za S-polinom proizvoljna dva bazna elementa važi da je ostatak pri deljenju sa polinomima baze jednak 0. Ovaj kriterijum čini osnovu *Buhbergerovog algoritma* za izračunavanje Grebnerove baze.

Algoritam *Buhbergerov algoritam*

Ulaz: Skup polinoma $\{f_1, f_2, \ldots, f_m\}$
Izlaz: Grebnerova baza ideala $\langle f_1, f_2, \ldots, f_m\rangle$

$G \leftarrow (f_1, f_2, \ldots, f_m)$
repeat
    $G' \leftarrow G$ {pamtimo prethodno G}
    for svaki par $g_i, g_j \in G, i \neq j$
        izračunaj $S(g_i, g_j)$ i ostatak r_{ij} pri deljenju $S(g_i, g_j)$ sa G
        if $r_{ij} \neq 0$
            then $G \leftarrow G \cup \{r_{ij}\}$
until $G = G'$

Na osnovu činjenice da vodeći term polinoma r_{ij} koji se dodaje u skup ne može biti umnožak vodećih termova polinoma iz skupa G i da na osnovu Diksonove leme (koju u ovom materijalu nećemo razmatrati) važi da ne može postojati beskonačni niz termova u kome nijedan nije umnožak terma koji se ranije javlja u nizu sledi zaustavljanje Buhbergerovog algoritma. Primetimo da izlaz G algoritma može biti znatno veći od broja polinoma na ulazu. Naime, ako je broj promenljivih jednak n, i ako ukupni stepen svakog od polinoma f_i ne prelazi d, tada je ukupni stepen svakog od polinoma redukovane Grebnerove baze G ograničen sa $2(\frac{1}{2}d^2 + d)^{2^{n-1}}$, što je dvostruko eksponencijalna funkcija po n, ali polinomijalna po d. Ovim je opisana složenost problema, a ne konkretnog algoritma za njegovo rešavanje. Uprkos lošim performansama u najgorem slučaju, pokazuje se da se u mnogim slučajevima koji su od praktičnog značaja Grebnerova baza konstruiše u razumnom vremenu.

Primer 31. *Izračunati Grebnerovu bazu ideala* $\langle f_1, f_2\rangle = \langle x^2 - y, x^3 - z\rangle$ *u odnosu na leksikografski poredak za koji važi* $x > y > z$. *Rešenje:* $\{x^2 - y, x^3 - z, xy - z, xz - y^2, y^3 - z^2\}$.

Primer 32. *Izračunati Grebnerovu bazu ideala* $\langle f_1, f_2\rangle = \langle x^3 - 2xy, x^2y - 2y^2 + x\rangle \subset K[x, y]$ *u odnosu na graduirani leksikografski poredak za koji važi* $x > y$. *Rešenje:* $\{x^3 - 2xy, x^2y - 2y^2 + x, -x^2, -2xy, -2y^2 + x\}$.

Većina računarskih sistema kojima se vrše algebarska izračunavanja (eng. computer algebra system) poput Singulara, Mejpla, Volfram Matematike sadrži procedure za izračunavanje Grebnerove baze datog ideala. S obzirom na to da je Buhbergerov algoritam zasnovan na algoritmu deljenja polinoma u prstenu više promenljivih, koji opet zavisi od poretka monoma, računanje Grebnerove baze zavisiće od izabranog poretka monoma.

Pomenimo i to da je Grebnerova baza izračunata pomoću Buhbergerovog algoritma obično veoma velika i sadrži dosta veći broj baznih elemenata nego što je to neophodno. Dakle, baza dobijena Buhbergerovim algoritmom ne mora biti optimalna i moguće je eliminisati neke nepotrebne bazne elemente korišćenjem narednog tvrđenja.

Teorema 8. *Neka je G Grebnerova baza ideala $I \subset K[x_1, x_2, \ldots, x_n]$. Neka je $p \in G$ polinom za koji važi $LT(p) \in \langle LT(G \setminus \{p\})\rangle$. Tada je $G \setminus \{p\}$ takođe Grebnerova baza ideala I.*

Eliminacijom iz skupa G svih polinoma p za koje važi $LT(p) \in \langle LT(G \setminus \{p\})\rangle$ i postavljanjem da su svi vodeći koeficijenti polinoma Grebnerove baze G jednaki 1 dobijamo tzv. *minimalnu Grebnerovu bazu.*

Primer 33. *Da bismo ilustrovali proceduru smanjenja Grebnerove baze, vratimo se idealu I koji smo razmatrali u primeru 29. Korišćenjem graduiranog leksikografskog poretka monoma, odredili smo Grebnerovu bazu ovog ideala:*

$$\begin{aligned} f_1 &= x^3 - 2xy \\ f_2 &= x^2y - 2y^2 + x \\ f_3 &= -x^2 \\ f_4 &= -2xy \\ f_5 &= -2y^2 + x \end{aligned}$$

Primetimo da je $LT(f_1) = x^3 = -x \cdot LT(f_3)$. Prema teoremi 8 možemo izostaviti polinom f_1 u minimalnoj Grebnerovoj bazi. Slično, s obzirom da važi $LT(f_2) = x^2y = -(1/2)x \cdot LT(f_4)$, iz Grebnerove baze možemo ukloniti polinom f_2. Ne postoje dalji slučajevi u kojima vodeći term nekog elementa Grebnerove baze deli vodeći term nekog drugog elementa baze. Dodatno, s obzirom na to da su neki od vodećih koeficijenata polinoma baze različiti od 1, pomnožićemo elemente pojednostavljene baze pogodnim konstantama da bi vodeći koeficijenti baznih elemenata postali jednaki 1. Stoga polinomi:

$$\begin{aligned} f_3' &= x^2 \\ f_4' &= xy \\ f_5' &= y^2 - (1/2)x \end{aligned}$$

čine minimalnu Grebnerovu bazu ideala I.

Primetimo da ideal I može imati veći broj minimalnih Greberovih baza. Na primer, ako umesto polinoma f_3' u bazu uvrstimo polinom $x^2 + axy$ za $a \in \mathbb{Q}$ dobićemo, takođe, minimalnu Greberovu bazu istog ideala.

Praktična vežba 7. *Proverimo prethodni primer u alatu Singular:*

```
> ring r = 0, (x,y), Dp;
> poly f1 = x3 - 2xy;
> poly f2 = x2y - 2y2 + x;
> poly f3 = -x2;
> poly f4 = -2xy;
> poly f5 = -2y2 + x;
```

```
> ideal i1 = lead(f2), lead(f3), lead(f4), lead(f5);
> reduce(lead(f1),i1);
// ** i is no standard basis
0
> ideal i2 = lead(f3), lead(f4), lead(f5);
> reduce(lead(f2),i2);
// ** i is no standard basis
0
> ideal i3 = lead(f4), lead(f5);
> reduce(lead(f3),i3);
// ** i is no standard basis
-x2
```

Primer za vežbu 13. *Koji od navedenih skupova predstavljaju minimalne Grebnerove baze ideala* $I = \langle y^2 + yx + x^2, y + x, y\rangle$*? (a)* $G_1 = \{y, x\}$ *(b)* $G_2 = \{y, x^2\}$*, (c)* $G_3 = \{y + x, x\}$*, (d)* $G_4 = \{y + x, y\}$

Ovako definisan koncept Grebnerovih baza ima jedan nedostatak. Pretpostavimo da su data dva strukturalno različita sistema polinoma F i F' i da želimo da saznamo da li su ova dva sistema ekvivalentna. Možemo izračunati minimalnu Grebnerovu bazu G sistema polinoma F i minimalnu Grebnerovu bazu G' sistema polinoma F'. Prema trenutnoj definiciji Grebnerovih baza ne možemo ništa zaključiti o sistemima F i F' na osnovu baza G i G'. Međutim, teorija Grebnerovih baza nam govori da kada izračunamo tzv. redukovanu Grebnerovu bazu ova dva sistema polinoma, onda je sistem polinoma F ekvivalentan sistemu polinoma F' ako su redukovane Grebnerove baze ova dva sistema jednake, odnosno ako važi $G = G'$. Uvedimo stoga koncept redukovane Grebnerove baze.

Definicija 11 (Redukovana Grebnerova baza)**.** Redukovana Grebnerova baza *ideala* I *je Grebnerova baza* G *za koju dodatno važi:*

- $\forall g_i \in G$ *nijedan monom polinoma* g_i *nije deljiv sa* $LT(g_j)$ *gde je* $i \neq j$*,*
- $\forall g_i \in G : \quad LC(g_i) = 1.$

Primetimo da je redukovana Grebnerova baza automatski i minimalna. Međutim, kod redukovane Grebnerove baze važi da ne samo da vodeći term nijednog polinoma baze g_i nije deljiv vodećim termom nekog drugog polinoma baze g_j, već to treba da važi za svaki term polinoma g_i.

Ako razmotrimo primer 33, jedino Grebnerova baza za koju važi $a = 0$ jeste redukovana (jer bi inače term axy bio deljiv vodećim termom polinoma f_4'). Štaviše, redukovana Grebnerova baza je uvek jedinstvena.

Do redukovane Grebnerove baze može se doći na osnovu proizvoljne Grebnerove baze G na sledeći način: svako $g_i \in G$ menjamo njegovim ostatkom pri deljenju sa polinomima iz skupa $G \setminus \{g_i\}$. Konačno, postavljamo da vodeći koeficijent svakog polinoma g_i bude 1.

Procedure za računanje Grebnerove baze u računarskim algebarskim sistemima uglavnom vraćaju redukovanu Grebnerovu bazu.

Praktična vežba 8. *Funkcija* `groebner` *u sistemu Singular ne vraća nužno redukovanu Grebnerovu bazu: da bismo dobili redukovanu Grebnerovu bazu potrebno je uključiti ovu opciju:*

```
> option(redSB);
> ideal G = groebner(I);
```

Primer 34. *Izračunati redukovanu Grebnerovu bazu za bazu iz primera 32 u odnosu na graduirani leksikografski poredak. Rešenje:* $\{x^2, xy, y^2 - x/2\}$.

Praktična vežba 9. *Izračunajmo u sistemu Singular redukovanu Grebnerovu bazu skupa polinoma* $\{-x^3 + y, x^2y - y^2\}$ *kada se koristi leksikografski poredak termova za koju važi* $x > y$*:*

```
> ring r1 = 0, (x,y), lp;
> poly f1 = -x3 + y;
> poly f2 = x2y - y2;
> ideal I1 = f1, f2;
> ideal G1 = groebner(I1);
> G1;
G1[1]=y3-y2
G1[2]=xy2-y2
G1[3]=x2y-y2
G1[4]=x3-y
```

Dobijena je naredna Grebnerova baza: $g_1 = y^3 - y^2, g_2 = xy^2 - y^2, g_3 = x^2y - y^2, g_4 = x^3 - y$. *Primetimo da dobijeni rezultat nije isti kao kada bi se koristio leksikografski poredak monoma za koji važi* $y > x$.

```
> ring r2 = 0, (y,x), lp;
> poly f1 = -x3 + y;
> poly f2 = x2y - y2;
> ideal I2 = f1, f2;
> ideal G2 = groebner(I2);
> G2;
G2[1]=x6-x5
G2[2]=y-x3
```

Možemo izračunati i Grebnerovu bazu istog skupa polinoma u odnosu na težinski vektor $(1, 3)$.

```
> ring r3 = 0, (x,y), Wp(1,3);
> poly f1 = -x3 + y;
> poly f2 = x2y - y2;
> ideal I3 = f1, f2;
> ideal G3 = groebner(I3);
> G3;
G3[1]=x3-y
G3[2]=y2-x2y
```

Primer za vežbu 14. *Proveriti ispravnost tvrđenja iz primera 3 u programu Singular.*

Glava 4

Primene Grebnerovih baza

Matematička teorija se može smatrati utoliko vrednijom ukoliko se ona može primeniti u širem polju različitih oblasti. Da bismo stekli uvid u moć Grebnerovih baza razmotrićemo samo neke od njihovih primena.

4.1 Rešavanje sistema polinomijalnih jednačina

Praktična vežba 10. *Proverimo primer 1 u sistemu Singular. Potrebno je utvrditi da li iz $f(A, B, C) = 0$ i $g(A, B, C) = 0$ sledi $h(A, B, C) = 0$. Ovo odgovara ispitivanju da li polinom h pripada idealu I generisanom nad polinomima f i g. Za ideal I možemo odrediti Grebnerovu bazu, a zatim izračunati ostatak pri deljenju polinoma h polinomima Grebnerove baze.*

U Singularu se funkcijom `groebner` *izračunava standardna (Grebnerova) baza ideala. Napomenimo da je implementacija Buhbergerovog algoritma za izračunavanje Grebnerove baze u alatu Singular jedna od najefikasnijih implementacija ovog algoritma.*

```
> ring r = 0, (A,B,C), lp;
> poly f = A + B + C - 14;
> poly g = A - B + C + 4;
> ideal I = f, g;
> ideal G = groebner(I);
> G;
G[1]=B-9
G[2]=A-B+C+4
> poly h = A + C - 5;
> reduce(h,G);
0
> reduce(h,I);
// ** I is no standard basis
B-9
```

Primetimo da su u ovom primeru svi polinomi sa kojima radimo linearni po promenljivim A, B i C. Takođe, ako vršimo deljenje skupom polinomima koji ne predstavljaju Grebnerovu bazu kao ostatak dobijamo vrednost različitu od 0.

Grebnerove baze se mogu koristiti za rešavanje sistema linearnih jednačina, ali i opštije, za rešavanje proizvoljnog sistema polinomijalnih jednačina.

Primer 35. *Ana želi da napravi pravougaonu tortu za rođendan. Zapremina torte iznosi $351cm^3$. Dužina torte je za 4cm veća od širine, a visina torte iznosi 1/3 širine. Koje dimenzije treba da bude pleh za tortu?*

Znamo da je zapremina kvadra jednaka proizvodu njegove dužine, širine i visine. Ako sa d označimo njegovu dužinu, sa s širinu, a sa v visinu torte, rešavanje ovog problema svodi se na rešavanje narednog sistema polinomijalnih jednačina nad promenljivim d, s i v:

$$\begin{aligned} d \cdot s \cdot v &= 351 \\ d &= s + 4 \\ v &= \frac{1}{3}s \end{aligned}$$

odnosno:

$$\begin{aligned} p_1(d,s,v) &= d \cdot s \cdot v - 351 = 0 \\ p_2(d,s,v) &= d - s - 4 = 0 \\ p_3(d,s,v) &= 3v - s = 0 \end{aligned}$$

Ako izračunamo Grebnerovu bazu ideala generisanog polinomima p_1, p_2 i p_3 u odnosu na leksikografski poredak za koji važi $d > s > v$ dobijamo sistem polinoma:

$$\begin{aligned} g_1 &= 3v^3 + 4v^2 - 117 \\ g_2 &= s - 3v \\ g_3 &= d - 3v - 4 \end{aligned}$$

koji je jednostavno rešiti.

Praktična vežba 11. *Izračunajmo Grebnerovu bazu ideala nad polinomima p_1, p_2 i p_3 u sistemu Singular.*

```
> ring r = 0, (d,s,v), lp;
> poly p1 = dsv - 351;
> poly p2 = d - s - 4;
```

```
> poly p3 = 3v - s;
> ideal I = p1, p2, p3;
> ideal G = groebner(I);
> G;
G[1]=3v3+4v2-117
G[2]=s-3v
G[3]=d-3v-4
```

Dobijeni sistem možemo rešiti tako što odredimo sva rešenja po v prve jednačine, a onda ih zamenimo u ostale dve jednačine.

```
LIB "solve.lib";
laguerre_solve(G[1]);
```

Izračunavanje redukovane Grebnerove baze za ideal generisan polinomima p_1, p_2 i p_3 može znatno pojednostaviti formu jednačina. Poredak koji se koristi mora biti neki eliminacioni poredak termova; jedan takav je leksikografski poredak termova. Naime, korišćenjem leksikografskog poretka monoma, eliminišemo vodeće termove u leksikografskom poretku te se dobija sistem jednačina u kojem se promenljive sukcesivno eliminišu. Primetimo, takođe, da poredak eliminisanja promenljivih odgovara poretku promenljivih, odnosno u prvom polinomu Grebnerove baze figuriše samo najmanja promenljiva u razmatranom poretku, drugi polinom Grebnerove baze sadrži samo najmanju i drugu najmanju promenljivu itd. Polinomi Grebnerove baze mogu biti višeg stepena nego polazni polinomi, međutim, ovakav sistem jednačina je jednostavno rešiti: naime, možemo rešiti prvu jednačinu, njena rešenja uvrstiti u preostale i rešiti preostali sistem na isti način po ostalim promenljivim.

U opštem slučaju moguće je da sistem polinomijalnih jednačina nema rešenja. Postavlja se pitanje kako to zaključiti na osnovu Grebnerove baze ideala generisanog polinomima iz ovog sistema? Pokazuje se da će u tom slučaju redukovana Grebnerova baza ideala biti jednaka $G = \{1\}$. Jasno je da jednačina $g_1 = 0$ u ovom slučaju nema rešenja.

S druge strane, sistem polinomijalnih jednačina ima konačno mnogo rešenja ako i samo ako za redukovanu Grebnerovu bazu $G = \{g_1, g_2, \ldots, g_t\}$ za svako $i = 1, 2, \ldots, n$ postoji $j \in \{1, 2, \ldots, t\}$ tako da je $LM(g_j) = x_i^\alpha$. Dakle, za svaku promenljivu iz sistema postoji neki polinom Grebnerove baze čiji je vodeći monom jednak nekom stepenu te promenljive. Primetimo da u primeru 35 važi $LM(g_1) = v^3$, $LM(g_2) = s$ i $LM(g_3) = d$, te važi prethodno tvrđenje i sistem ima konačno mnogo rešenja.

Primer 36. *Razmotrimo sistem jednačina:*

$$\begin{aligned} x^2 + y^2 + z^2 &= 1 \\ x^2 + z^2 &= y \\ x &= z \end{aligned}$$

u $\mathbb{C}^3$. *Polinomi koji odgovaraju ovim jednačinama zadaju ideal:*

$$I = \langle x^2 + y^2 + z^2 - 1, x^2 + z^2 - y, x - z \rangle \subset \mathbb{C}[x, y, z]$$

Podsetimo se da je rešenje sistema $f_1 = 0, f_2 = 0, \ldots, f_m = 0$ *jedan afini varijetet* $V(I)$ *definisan idealom* $I = \langle f_1, f_2, \ldots, f_m \rangle$. *Dakle, rešavanje sistema polinoma svodi se na računanje svih tačaka u* $V(I)$. *Redukovana Grebnerova baza ideala* I *u odnosu na leksikografski poredak monoma za poredak promenljivih* $x > y > z$ *jednaka je:*

$$\begin{aligned} g_1 &= x - z \\ g_2 &= y - 2z^2 \\ g_3 &= z^4 + (1/2)z^2 - 1/4 \end{aligned}$$

Primetimo da polinom g_3 *zavisi samo od promenljive* z *i da se jednačina* $g_3 = 0$ *može jednostavno rešiti po* z^2. *Četiri vrednosti za* z *su:*

$$z = \pm\frac{1}{2}\sqrt{\pm\sqrt{5} - 1}$$

Zamenom ovih vrednosti redom u jednačine $g_1 = 0$ *i* $g_2 = 0$ *dobijamo i vrednosti promenljivih* x *i* y. *Ukupno nalazimo 4 rešenja polaznog sistema jednačina: dva realna i dva kompleksna. Primetimo da je* $LM(g_1) = x$, $LM(g_2) = y$ *i* $LM(g_3) = z^4$, *te sistem ima konačno mnogo rešenja.*

Primer za vežbu 15. *Proveriti prethodni primer u alatu Singular.*

Primer 37. *Razmotrimo sistem jednačina:*

$$\begin{aligned} x + y &= 0 \\ y^2 - 1 &= 0 \\ x^2 - 2y &= 0 \end{aligned}$$

Polinomi koji odgovaraju ovim jednačinama zadaju ideal:

$$I = \langle x + y, y^2 - 1, x^2 - 2y \rangle$$

S obzirom na to da je redukovana Grebnerova baza ovog ideala jednaka $\{1\}$, *ovaj sistem jednačina nema rešenja.*

Praktična vežba 12. *Proverimo ovaj primer u alatu Singular.*

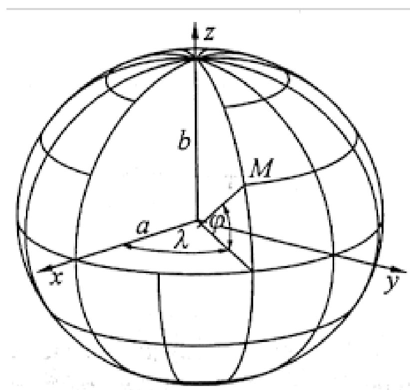
```
> ring r = 0, (x,y), lp;
> poly p1 = x + y;
> poly p2 = y2 - 1;
> poly p3 = x2 - 2y;
> ideal I = p1, p2, p3;
> ideal G = groebner(I);
> G;
G[1]=1
```

Primer za vežbu 16. *Izračunati tačke koje pripadaju afinom varijetetu*

$$V(x^2 + y^2 + z^2 - 1, x^2 + y^2 + z^2 - 2x, 2x - 3y - z).$$

4.2 Rešavanje sistema nepolinomijalnih jednačina

Razmotrimo problem rešavanja sistema jednačina u kojima mogu da figurišu trigonometrijske funkcije.



Slika 4.1: Geodetski koordinatni sistem (preuzeto sa `https://www.geoskola.hr/~gsurina/Geodetske%20mre%C5%BEe%20i%20koord.%20sustavi.pdf`).

Primer 38. *Razmotrimo jedan primer koji potiče iz oblasti računarske geodezije. Odnos između geocentričnih dekartovskih koordinata x, y i z tačke M na površini ili blizu površine* *zemlje i geodetskih koordinata h (visina – udaljenost tačke od tangentne ravni elipsoida u odgovarajućoj tački), λ (geografska dužina – ugao između ravni nultog meridijana i meridijana u datoj tački) i φ (geografska širina – ugao između ravni ekvatora i normale na elipsoid u datoj tački) njene projekcije na geocentričnom elipsoidu može se opisati narednim sistemom jednačina:*

$$\begin{aligned} x &= (N+h)\cos\varphi\cos\lambda \\ y &= (N+h)\cos\varphi\sin\lambda \\ z &= (N(1-e^2)+h)\sin\varphi \end{aligned} \tag{4.1}$$

gde je sa N označen vertikalni poluprečnik zakrivljenosti, a sa e ekscentricitet elipsoida, koji su definisani sa:

$$\begin{aligned} N &= \frac{a}{\sqrt{1-e^2\sin\varphi^2}} \\ e &= \sqrt{\frac{a^2-b^2}{a^2}} \end{aligned}$$

gde su a i b velika i mala poluosa elipsoida (slika 4.1).

Na osnovu jednačina (4.1), mogu se za date geodetske koordinate h, λ i φ tačke sa elipsoida direktno izračunati odgovarajuće dekartovske koordinate x, y i z. Računanje koordinata h, λ i φ na osnovu koordinata x, y i z je znatno teže: potrebno je rešiti nelinearni sistem jednačina u funkciji nepoznatih h, λ i φ, ako su poznate vrednosti x, y i z. Primetimo da u ovom sistemu figurišu i trigonometrijske funkcije i funkcija za računanje kvadratnog korena.

Datom sistemu jednačina pridružićemo sistem polinomijalnih jednačina tako što ćemo za svaki trigonometrijski entitet uvesti po jednu promenljivu (npr. za $\sin\varphi$ promenljivu sf, a za $\cos\varphi$ promenljivu sf). Ovako uvedene promenljive nisu međusobno nezavisne, tako da sistemu jednačina dodajemo nove polinomijalne jednačine koje odgovaraju dobro poznatim trigonometrijskim identitetima (npr. da je $sf^2+cf^2=1$). U ovom problemu uvodimo sledeće nove promenljive:

$$\begin{aligned} cf &= \cos\varphi \\ sf &= \sin\varphi \\ cl &= \cos\lambda \\ sl &= \sin\lambda \end{aligned}$$

Dodatno, uvešćemo promenljivu S da označimo vrednost izraza:

$$S = \sqrt{1-e^2\cdot sf^2}$$

koji se javlja u definiciji vrednosti N. Na ovaj način dolazimo do sistema od sedam poli-

nomijalnih jednačina:

$$
\begin{aligned}
p_1 &= x-(N+h)\cdot cf\cdot cl=0\ \{\textit{definicija koordinate } x\}\\
p_2 &= y-(N+h)\cdot cf\cdot sl=0\ \{\textit{definicija koordinate } y\}\\
p_3 &= z-(N(1-e^2)+h)\cdot sf=0\ \{\textit{definicija koordinate } z\}\\
p_4 &= cf^2+sf^2-1=0\ \{\textit{osnovni trigonometrijski identitet}\}\\
p_5 &= cl^2+sl^2-1=0\ \{\textit{osnovni trigonometrijski identitet}\}\\
p_6 &= N\cdot S-a=0\ \{\textit{veza promenljive } S \textit{ i } N\}\\
p_7 &= S^2+e^2\cdot sf^2-1=0\ \{\textit{definicija promenljive } S\}
\end{aligned}
$$

Računamo Grebnerovu bazu ideala $\langle p_1, p_2 \ldots, p_7\rangle$ *u odnosu na leksikografski poredak monoma za koji važi:*

$$N > S > h > cl > sl > cf > sf.$$

Kao jedan od polinoma Grebnerove baze dobija se polinom jedne promenljive po promenljivoj sf *koji je osmog stepena i koji se može analitički rešiti. Nakon toga moguće je izračunati vrednost jedne po jedne promenljive, a nakon toga, kada recimo dobijemo vrednosti promenljivih* cf *i* sf *možemo doći i do vrednosti ugla* φ*.*

Praktična vežba 13. *Proverimo ovaj primer u alatu Singular. Dekartovske koordinate* x*,* y *i* z*, kao i veliku poluosu elipsoida* a *i ekscentricitet elipsoida* e *možemo videti kao parametre po kojima treba rešiti ovaj sistem jednačina. U Singularu to zadajemo tako što prilikom definisanja prstena polinoma nad kojim radimo skup koeficijenata obogaćujemo skupom parametra.*

```
> ring r = (0,x,y,z,e,a), (N,S,h,cl,sl,cf,sf), lp;
> poly p = x-(N+h)*cf*cl;
> poly q = y-(N+h)*cf*sl;
> poly s = z-(N*(1-e2)+h)*sf;
> poly t = cf^2+sf^2-1;
> poly u = cl^2+sl^2-1;
> poly v = NS-a;
> poly w = S2+e2*sf^2-1;
> ideal I = p,q,s,t,u,v,w;
> ideal G = groebner(I);
```

Rešavanje sistema polinoma koji u sebi uključuju pozive trigonometrijskih funkcija ima primenu i u robotici, na primer za izračunavanje na koji način zglobovi robota treba da se okrenu da bi on došao u određeni položaj. Ovaj problem može se rešiti korišćenjem Grebnerovih baza.

Primer za vežbu 17. *Izrazi sistem jednačina kao sistem polinomijalnih jednačina:*

$$\begin{aligned} x &= (2+\cos t)\cos u \\ y &= (2+\cos t)\sin u \\ z &= \sin t \end{aligned}$$

4.3 Rešavanje problema celobrojnog linearnog programiranja

Razmotrimo najpre jedan poznat algoritamski problem, u kome je zadatak isplatiti dati iznos korišćenjem minimalnog broja novčića.

Primer 39. *Pronaći minimalan broj novčića od* $1, 2, 5$ *i* 10 *dinara koji je potreban da bi se platio iznos od* 48 *dinara.*

Ovaj problem se može rešiti metodom Grebnerovih baza. Ključna ideja jeste da se broj novčića izrazi kao stepen odgovarajuće promenljive. Označimo sa A *novčić od 1 dinara, sa* B *novčić od* 2 *dinara, sa* C *novčić od* 5 *dinara, a sa* D *novčić od* 10 *dinara: monomom* $A^3B^2C^7D$ *predstavili bismo iznos formiran od tri novčića od 1 dinara, dva novčića od 2 dinara, 7 novčića od 5 dinara i 1 novčić od 10 dinara. Ukupan broj novčića onda je jednak ukupnom stepenu ovog monoma i iznosi* $3 + 2 + 7 + 1 = 13$.

Najpre je potrebno formulisati vezu između novčića različitih vrednosti: dva novčića od dinar vrede ko jedan od dva dinara, pet novčića od dinar kao jedan od pet dinara, a deset novčića od dinar kao jedan novčić od deset dinara. Ove veze možemo formulisati u vidu narednih jednačina:

$$\begin{aligned} A^2 &= B \\ A^5 &= C \\ A^{10} &= D \end{aligned}$$

Ovi polinomi formiraju ideal $I = \langle A^2 - B, A^5 - C, A^{10} - D\rangle$. *Pošto mi težimo dobijanju monoma sa minimalnim ukupnim stepenom, u daljem razmatranju koristićemo neki graduirani poredak. Računamo Grebnerovu bazu ideala* I *u odnosu na graduirani leksikografski poredak za koji važi* $A > B > C > D$. *Ona je jednaka:*

$$G = \{C^2 - D, A^2 - B, B^3 - AC, AB^2 - C\}.$$

Primetimo da dobijene veze daju veoma korisna pravila zamene: na primer zameniti 2 novčića od 5 dinara jednim novčićem od 10, zameniti dva novčića od 1 dinar jednim novčićem od 2, zameniti tri novčića od 2 dinara jednim novčićem od 1 i jednim novčićem od 5 dinara, kao i zameniti jedan novčić od 1 i dva novčića od 2 dinara jednim od 5 dinara. Naime, uvek ćemo favorizovati način kojim se isti iznos postiže sa manjim brojem novčića, tj. monom čiji je ukupni stepen manji.

Zbog izabranog poretka monoma, redukcija polinoma u odnosu na Grebnerovu bazu G daje polinom čiji je ukupni stepen minimalan u odnosu na sve polinome koji su ekvivalentni polaznom. Stoga je optimalan način da platimo iznos od 48 dinara jednak normalnoj formi proizvoljnog načina da platimo ovaj iznos: na primer sa 3 novčića od 10 dinara, dva novčića od 5 dinara, tri novčića od 2 dinara i dva novčića od 1 dinara. Odgovarajuću normalnu formu računamo kao ostatak pri deljenju polinoma $A^2B^3C^2D^3$ polinomima Grebnerove baze G. On je jednak $ABCD^4$ te je minimalan broj novčića jednak $1+1+1+4=7$ i odgovara kombinaciji od po jednog novčića od 1, 2 i 5 dinara i četiri novčića od 10 dinara.

Prethodni problem pripada problemu celobrojnog linearnog programiranja koji se u opštem slučaju može opisati na sledeći način. Neka važi $a_{i,j} \in \mathbb{Z}$, $b_i \in \mathbb{Z}$ i $c_j \in \mathbb{R}$ za $i = 1, 2, \ldots, m$ i $j = 1, 2, \ldots, n$. Potrebno je odrediti rešenje $\overrightarrow{x} = (x_1, x_2, \ldots, x_n) \in \mathbb{N}^n$ sistema jednačina:

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n &= b_1 \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n &= b_2 \\ &\cdots \\ a_{m1}x_1 + a_{m2}x_2 + \ldots + a_{mn}x_n &= b_m \end{aligned} \tag{4.2}$$

kojim se minimizuje vrednost funkcije cene:

$$c(x_1, x_2, \ldots, x_n) = \sum_{j=1}^{n} c_j x_j.$$

Pritom su sve vrednosti a_{ij} i b_i celobrojne, a sva ograničenja nad promenljivim x_i i funkcija cene su linearni po x_i.

U primeru 39 funkcija cene bila bi jednaka zbiru broja novčića od 1, 2, 5 i 10 dinara. Naime, ako sa a označimo broj novčića od 1 dinara, sa b broj novčića od 2 dinara, sa c broj novčića od 5 dinara, a sa 10 broj novčića od 10 dinara, funkcija cene jednaka je

$$c(a, b, c, d) = a + b + c + d,$$

a sistem jednačina se svodi na narednu jednačinu:

$$1 \cdot a + 2 \cdot b + 5 \cdot c + 10 \cdot d = 48$$

Razmotrimo na koji način se Grebnerove baze mogu iskoristiti za rešavanje problema celobrojnog linearnog programiranja. Sistem jednačina (4.2) se sastoji od m jednačina i svakoj jednačini pridružujemo novu promenljivu: k-toj jednačini sistema, $k = 1, 2, \ldots, m$ pridružujemo promenljivu X_k na sledeći način:

$$\begin{aligned} X_1^{a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n} &= X_1^{b_1} \\ X_2^{a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n} &= X_2^{b_2} \\ &\cdots \\ X_m^{a_{m1}x_1 + a_{m2}x_2 + \ldots + a_{mn}x_n} &= X_m^{b_m} \end{aligned}$$

Naime, postavljanjem da je i-ta jednačina sistema (4.2) eksponent promenljive X_i dobijamo sistem jednačina nad monomima. Množenjem levih i desnih strana jednakosti dobijamo jedinstvenu jednačinu nad monomima koja predstavlja celokupni polazni sistem. Dakle, sistem (4.2) možemo kompaktnije zapisati kao:

$$X_1^{a_{11}x_1+a_{12}x_2+\ldots+a_{1n}x_n} \cdot \ldots \cdot X_m^{a_{m1}x_1+a_{m2}x_2+\ldots+a_{mn}x_n} = X_1^{b_1} \cdot \ldots \cdot X_m^{b_m}$$

Grupisanjem činilaca s leve strane znaka jednakosti čiji su eksponenti redom jednaki x_i dobijamo:

$$(X_1^{a_{11}} \cdot \ldots \cdot X_m^{a_{m1}})^{x_1} \cdot \ldots \cdot (X_1^{a_{1n}} \cdot \ldots \cdot X_m^{a_{mn}})^{x_n} = X_1^{b_1} \cdot \ldots \cdot X_m^{b_m}$$

Svakom od izraza u zagradi u prethodnoj jednačini pridružujemo novu promenljivu Y_k za $k = 1, 2, \ldots, n$ tako da važi:

$$Y_k = X_1^{a_{1k}} \ldots X_m^{a_{mk}}$$

odnosno, polinom p_k:

$$p_k = Y_k - X_1^{a_{1k}} \ldots X_m^{a_{mk}} = 0$$

Na ovaj način dobijamo sistem jednačina $p_1 = 0, p_2 = 0, \ldots, p_n = 0$ nad promenljivim $X_1, \ldots, X_m, Y_1, \ldots, Y_n$. Na osnovu nekoliko teorema koje ovde nećemo navoditi važi da rešenja polaznog sistema jednačina (4.2) možemo naći narednim postupkom:

1. izračunamo redukovanu Grebnerovu bazu G ideala

$$I = \langle p_1, p_2, \ldots, p_n \rangle = \langle Y_k - X_1^{a_{1k}} X_2^{a_{2k}} \cdots X_m^{a_{mk}} | 1 \leq k \leq n \rangle$$

   u prstenu polinoma $K[X_1, X_2, \ldots, X_m, Y_1, Y_2, \ldots, Y_n]$ u odnosu na težinski poredak monoma u kome je težinski vektor izabran tako da koeficijenti uz Y_k odgovaraju koeficijentima c_k (što je veći značaj promenljive u ciljnoj funkciji, to joj je veći značaj i ovde), i pritom promenljive X_i imaju veći težinski koeficijent nego promenljive Y_k,

2. izračunamo ostatak r pri deljenju monoma $X_1^{b_1} X_2^{b_2} \cdots X_m^{b_m}$ polinomima baze G,

3. ako $r \notin K[Y_1, Y_2, \ldots, Y_n]$ onda polazni sistem nema celobrojna rešenja; ako je $r = Y_1^{\alpha_1} \cdot Y_2^{\alpha_2} \cdot \ldots \cdot Y_n^{\alpha_n}$ onda je $(\alpha_1, \alpha_2, \ldots, \alpha_n)$ optimalno rešenje polaznog sistema.

Napomenimo da ovo važi u slučaju kada su svi koeficijenti u jednačinama pozitivni. U situaciji kada je neka vrednost a_{ij} ili b_k negativna, potrebno je uvesti novu promenljivu i malo izmeniti polinome kojima se generiše ideal. U ovom materijalu nećemo razmatrati taj slučaj.

Primer 40. *Razmotrimo sistem jednačina:*

$$\begin{aligned} 2x_1 + x_2 &= 3 \\ x_1 + x_2 + 3x_3 &= 5 \end{aligned} \tag{4.3}$$

Potrebno je pronaći rešenje ovog sistema kojim se minimizuje vrednost funkcije cene

$$c(x_1, x_2, x_3) = x_1 + 2x_2 + 3x_3.$$

Pridružimo prvoj jednačini promenljivu X_1, a drugoj promenljivu X_2. Na taj način dobijamo:

$$X_1^{2x_1+x_2} = X_1^3$$
$$X_2^{x_1+x_2+3x_3} = X_2^5$$

Množenjem ove dve jednačine dobijamo:

$$X_1^{2x_1+x_2} \cdot X_2^{x_1+x_2+3x_3} = X_1^3 X_2^5$$

Grupisanjem članova uz isti eksponent dobijamo:

$$(X_1^2 X_2)^{x_1} \cdot (X_1 X_2)^{x_2} \cdot (X_2^3)^{x_3} = X_1^3 X_2^5$$

Svakoj od zagrada pridružujemo promenljivu Y_i i odgovarajući polinom:

$$\begin{aligned} p_1 &= Y_1 - X_1^2 X_2 \\ p_2 &= Y_2 - X_1 X_2 \\ p_3 &= Y_3 - X_2^3 \end{aligned}$$

Razmatramo ideal:

$$I = \langle Y_1 - X_1^2 X_2, Y_2 - X_1 X_2, Y_3 - X_2^3 \rangle.$$

Potrebno je odrediti Grebnerovu bazu ideala I u odnosu na težinski poredak monoma za $X_1 > X_2 > Y_1 > Y_2 > Y_3$ sa težinskim vektorom $(10, 5, 1, 2, 3)$. Ona je jednaka:

$$\begin{aligned} G = \{&X_2Y_1 - Y_2^2, Y_2^6 - Y_1Y_3, X_2^2Y_2 - X_1Y_3, X_1Y_2 - Y_1, X_2Y_2^4 - Y_1^2Y_3, \\ &X_1Y_1Y_3 - X_2Y_2^3, X_2^3 - Y_3, X_1X_2 - Y_2, X_1^2Y_3 - X_2Y_2^2\} \end{aligned}$$

Deljenjem polinoma $g = X_1^3 X_2^5$ polinomima Grebnerove baze G u odnosu na dati težinski poredak monoma dobijamo ostatak $r = Y_1Y_2Y_3$. Pošto u dobijenom monomu figurišu samo promenljive Y_i i pošto je uz sve tri promenljive Y_i eksponent jednak 1, zaključujemo da je optimalno rešenje polaznog sistema:

$$x_1 = 1, x_2 = 1, x_3 = 1.$$

Praktična vežba 14. *Proverimo prethodni primer u alatu Singular. Promenljivim X_1, X_2, Y_1, Y_2, Y_3 pridružujemo promenljive x, y, z, u, v i zapisujemo odgovarajuće polinome. Izračunavamo ideal nad ovim polinomima i njegovu Grebnerovu bazu u odnosu na težinski poredak monoma, a zatim i ostatak pri deljenju polinoma g polinomima Grebnerove baze.*

```
> ring r = 0, (x,y,z,u,v), Wp(10,5,1,2,3);
> poly h1 = z - x2y;
> poly h2 = u - xy;
```

```
> poly h3 = v - y3;
> ideal I = h1, h2, h3;
> ideal G = groebner(I);
> G;
G[1]=yz-u2
G[2]=u6-z3v
G[3]=y2u-xv
G[4]=xu-z
G[5]=yu4-z2v
G[6]=xzv-yu3
G[7]=y3-v
G[8]=xy-u
G[9]=x2v-yu2
> poly g = x3y5;
> reduce(g,G);
zuv
```

Primer za vežbu 18. *Opisanu opštu proceduru za rešavanje problema linearnog celobrojnog programiranja možemo sprovesti i na primeru problema vraćanja kusura (primer 39). U ovom problemu sistem jednačina se svodi na samo jednu jednačinu:*

$$x_1 + 2x_2 + 5x_3 + 10x_4 \quad = \quad 48$$

i potrebno je naći rešenje kojim se minimizuje vrednost funkcije cene:

$$c(x_1, x_2, x_3, x_4) = x_1 + x_2 + x_3 + x_4.$$

Pridruživanjem promenljive X_1 jedinoj jednačini sistema dobijamo:

$$X_1^{x_1+2x_2+5x_3+10x_4} = X_1^{48}$$

Grupisanjem članova uz isti eksponent sa leve strane znaka jednakosti dobijamo:

$$(X_1)^{x_1} \cdot (X_1^2)^{x_2} \cdot (X_1^5)^{x_3} \cdot (X_1^{10})^{x_4} = X_1^{48}$$

Svakoj od zagrada pridružujemo promenljivu $Y_i, 1 \leq i \leq 4$ i odgovarajući polinom:

$$\begin{aligned} p_1 &= Y_1 - X_1 \\ p_2 &= Y_2 - X_1^2 \\ p_3 &= Y_3 - X_1^5 \\ p_4 &= Y_4 - X_1^{10} \end{aligned}$$

Generišemo ideal I nad ovim polinomima i konstruišemo Grebnerovu bazu ovog ideala u odnosu na težinski poredak monoma za $X_1 > Y_1 > Y_2 > Y_3 > Y_4$ sa težinskim vektorom

$(2,1,1,1,1)$. *Deljenjem polinoma* $g = X_1^{48}$ *polinomima Grebnerove baze* G *u odnosu na dati težinski poredak monoma dobijamo ostatak* $r = Y_1Y_2Y_3Y_4^4$. *Pošto u dobijenom ostatku figurišu samo promenljive* Y_i, *zaključujemo da je optimalno rešenje polaznog sistema:*

$$x_1 = 1, x_2 = 1, x_3 = 1, x_4 = 10.$$

Praktična vežba 15. *Proverimo prethodni primer u alatu Singular. Promenljivim* X_1, Y_1, Y_2, Y_3, Y_4 *pridružujemo promenljive* x, y, z, u, v *i zapisujemo odgovarajuće polinome. Izračunavamo ideal generisan nad ovim polinomima i njegovu Grebnerovu bazu u odnosu na dati težinski poredak monoma, a zatim računamo ostatak pri deljenju polinoma* g *polinomima Grebnerove baze.*

```
> ring r = 0, (x,y,z,u,v), Wp(2,1,1,1,1);
> poly p1 = y - x;
> poly p2 = z - x2;
> poly p3 = u - x5;
> poly p4 = v - x^10;
> ideal I = p1, p2, p3, p4;
> ideal G = groebner(I);
> G;
G[1]=u2-v
G[2]=y2-z
G[3]=x-y
G[4]=z3-yu
G[5]=yz2-u
> poly g = x^48;
> reduce(g,G);
yzuv4
```

Primer za vežbu 19. *Odrediti rešenje sistema jednačina:*

$$\begin{aligned} 3x_1 + 2x_2 + x_3 + x_4 &= 1 \\ 4x_1 + x_2 + x_3 &= 5 \end{aligned}$$

kojim se minimizuje vrednost funkcije cene $c(x_1, x_2, x_3, x_4) = 1000x_1 + x_2 + x_3 + 100x_4$.

4.4 Računanje hromatskog broja grafa

Primer 41. *Na fakultetu je potrebno napraviti raspored ispita. Dat je spisak kurseva i studenata koji pohađaju svaki od kurseva. Mnogi kursevi imaju zajedničke studente. Potrebno je napraviti raspored ispita tako da ispiti iz nikoja dva kursa koja pohađa isti student ne budu u isto vreme. Koliki je minimalan broj termina potreban za izvođenje svih ispita?*

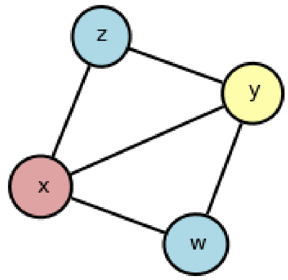
Problem pravljenja rasporeda ispita može se predstaviti kao grafovski problem tako što se svakom kursu dodeli jedan čvor u grafu, dok grana između dva čvora postoji ako postoji bar jedan student koji pohađa oba odgovarajuća kursa. Dakle, problem pravljenja rasporeda se može svesti na problem bojenja čvorova u grafu tako da nikoja dva susedna čvora ne budu obojena istom bojom, gde minimalan broj termina odgovara minimalnom broju boja potrebnih da se graf oboji.

Primer 42. *U optimizaciji kompajlera, alokacija registara je proces dodeljivanja potencijalno velikog broja programskih promenljivih ograničenom broju registara procesora. Naime, računar može brzo da piše u i čita iz registara procesora, te se program brže izvršava ako je veći broj promenljivih smešten u registrima. Naravno, ne koriste se sve promenljive u svakom trenutku, te tokom rada programa jedan isti registar može da sadrži vrednost različitih promenljivih, s tim da dve promenljive koje se koriste u isto vreme ne mogu biti dodeljene jednom istom registru. Na koji način se može izvršiti odgovarajuća dodela?*

I problem dodeljivanja promenljivih registrima se može razmatrati kao problem bojenja grafova, gde je svakoj promenljivoj dodeljen jedan čvor u grafu, grana postoji ako se dve promenljive koriste u isto vreme, a maksimalan dozvoljen broj boja ograničen je brojem raspoloživih registara.

Graf $G = (V, E)$ je *k-obojiv* ako je čvorove grafa moguće obojiti nekom od k raspoloživih boja tako da nikoja dva susedna čvora nemaju istu boju. Graf od n čvorova sigurno se može obojiti sa n boja. *Hromatski broj grafa* $\chi(G)$ je najmanji broj boja potreban da se oboji graf $G = (V, E)$ tako da nikoja dva susedna čvora ne budu obojena istom bojom. Hromatski broj grafa je izučavan i određen za različite familije grafova, pa je recimo u cikličkom grafu koji sadrži paran broj čvorova hromatski broj jednak 2, dok je u cikličkom grafu sa neparnim brojem čvorova on jednak 3. Hromatski broj grafa sa slike 4.2 iznosi 3. Postoji veliki broj otvorenih problema i hipoteza koje se odnose na hromatski broj grafa.

Pokazaćemo na koji način se problem odlučivosti k-obojivosti grafa može svesti na problem pripadnosti idealu. Radićemo u prstenu $\mathbb{C}[V]$, u kome je svakom čvoru grafa pridružena jedna promenljiva. Svakoj od k različitih boja pridružujemo po jednu različitu vrednost, npr. jedan od k različitih k-tih korena iz jedinice u polju $\mathbb{C}$. Svakom od čvorova grafa G pridružujemo jednu promenljivu v_i i uslov da je čvor obojen nekom od k boja možemo kodirati polinomom $v_i^k = 1$.



Slika 4.2: Bojenje grafa.

Polinom f_G *grafa* G pridružen grafu $G = (V, E)$ jednak je:

$$f_G = \prod_{(u,v)\in E} (u - v)$$

Teorema 9. *Neka je k pozitivan ceo broj. Neka je I ideal generisan polinomima $v^k - 1$ za $v \in V$. Graf G je k-obojiv ako i samo ako $f_G \notin I$.*

Ovaj kriterijum daje algoritam kojim se može utvrditi da li je dati graf k-obojiv: izračunamo Grebnerovu bazu ideala I i izvršimo deljenje polinoma f_G polinomima Grebnerove baze ovog ideala. Ukoliko se kao ostatak pri deljenju dobije vrednost 0 onda graf G nije obojiv sa k boja, a ako se dobije nenula ostatak onda jeste.

Intuicija iza ovog tvrđenja je sledeća: svaka od k različitih boja predstavlja jedan različiti k-ti koren iz jedinice u polju $\mathbb{C}$. Dakle, polinomi nad kojima je ideal I generisan odgovaraju dodeli vrednosti nekog k-tog korena iz jedinice promenljivim, odnosno odgovara dodeli jedne od k raspoloživih boja svakom čvoru grafa. Ako polinom f_G pripada idealu I, to znači da će bez obzira na to kojom bojom je obojen koji čvor grafa njegova vrednost biti 0, što dalje implicira da se nužno nekim susednim čvorovima grafa mora dodeliti ista boja. Stoga, graf G nije k-obojiv.

Traženje hromatskog broja datog grafa sa $n = |V|$ čvorova može se sprovesti narednim algoritmom:

Algoritam *Hromatski broj grafa*
Ulaz: Graf $G = (V, E)$ sa n čvorova zadat matricom susedstva M
Izlaz: Hromatski broj grafa $\chi(G)$

$k \leftarrow 1$
repeat
    $I \leftarrow \cup_{v=1}^{n} \{x[v]^k - 1\}$
    izračunaj Grebnerovu bazu B ideala I
    na osnovu matrice susedstva M grafa G izračunaj polinom f_G
    if $f_G \in I$ {ostatak pri deljenju f_G polinomima baze B jednak je 0 }
      then $k \leftarrow k + 1$
until $f_G \notin I$
return k

Međutim, s obzirom na to da se zna gornja granica za k i da za obojivost grafa sa k boja važi svojstvo monotonosti, moguće je ovaj problem rešiti i efikasnije, binarnom pretragom po rešenju.

Praktična vežba 16. *Odredimo hromatski broj grafa G sa slike 4.2. Proverimo da li se G može obojiti sa 3 boje. Razmotrimo prsten $\mathbb{C}[x, y, z, w]$ i ideal $I = \langle x^3 - 1, y^3 - 1, z^3 - 1, w^3 - 1\rangle$. Pokazuje se da je ovo takođe i Grebnerova baza ideala I. Polinom f_G grafa G jednak je $f_G = (x - y) \cdot (y - z) \cdot (z - x) \cdot (x - w) \cdot (y - w)$. Ostatak pri deljenju polinoma f_G polinomima Grebnerove baze ideala I različit je od nula, te je graf G 3-obojiv.*

```
> ring A = complex, (x,y,z,w), lp;
> poly f1 = x3 - 1;
> poly f2 = y3 - 1;
> poly f3 = z3 - 1;
> poly f4 = w3 - 1;
> ideal I = f1, f2, f3, f4;
> ideal G = groebner(I);
> poly f = (x-y)*(y-z)*(z-x)*(x-w)*(y-w);
> reduce(f,G);
-x2yz2-x2yzw-x2yw2+x2z2w+x2zw2+x2+xy2z2+xy2zw+xy2w2
-xz2w2-xz-xw-y2z2w-y2zw2-y2+yz2w2+yz+yw
```

Međutim, dati graf nije 2-obojiv jer polinom f_G pripada idealu $I_1 = \langle x^2 - 1, y^2 - 1, z^2 - 1, w^2 - 1\rangle$

```
> ring A = complex, (x,y,z,w), lp;
> poly g1 = x2 - 1;
> poly g2 = y2 - 1;
> poly g3 = z2 - 1;
> poly g4 = w2 - 1;
> ideal I1 = g1, g2, g3, g4;
> ideal G1 = groebner(I1);
> poly h = (x-y)*(y-z)*(z-x)*(x-w)*(y-w);
> reduce(h,G1);
0
```

Zaključujemo da je hromatski broj grafa G jednak 3.

Moguće je i odrediti sva k-bojenja datog grafa G. Naime, i dalje svaku od k različitih boja označavamo različitim k-tim korenom iz jedinice, a uslov da je čvor grafa v obojen nekom od k boja polinomom:

$$v^k - 1 = 0. \tag{4.4}$$

Razmotrimo proizvoljnu granu (u, w) grafa G: oba čvora su obojena nekom od raspoloživih boja te važi:

$$(u^k - 1) - (w^k - 1) = u^k - w^k = 0,$$

a pošto čvorovi u i w moraju biti obojeni različitim bojama istovremeno važi $u - w \neq 0$. Iz jednakosti:

$$\frac{u^k - w^k}{u - w} = u^{k-1} + u^{k-2}w + \ldots + uw^{k-2} + w^{k-1},$$

sledi da uslov da su čvorovi u i w obojeni različitim bojama možemo kodirati polinomom:

$$u^{k-1} + u^{k-2}w + \ldots + uw^{k-2} + w^{k-1} = 0. \tag{4.5}$$

Praktična vežba 17. *Odredimo sva moguća 3-bojenja grafa G sa slike 4.2. Problem se svodi na rešavanje sistema jednačina u prstenu $\mathbb{C}[x, y, z, w]$ koji za svaki čvor grafa sadži po jedan polinom oblika (4.4) kojim se kodira da je čvor obojen jednom od k raspoloživih boja i za svaku granu grafa sadrži po jedan polinom oblika (4.5). Ako je redukovana Grebnerova baza ovog ideala jednaka $\{1\}$ onda bojenje ne postoji, u suprotnom rešenja sistema kodiraju ispravna 3-bojenja grafa.*

```
> ring A = complex, (x,y,z,w), lp;
> poly f1 = x3 - 1;
> poly f2 = y3 - 1;
> poly f3 = z3 - 1;
> poly f4 = w3 - 1;
> poly f5 = x2+xy+y2;
> poly f6 = x2+xz+z2;
> poly f7 = x2+xw+w2;
> poly f8 = y2+yz+z2;
> poly f9 = y2+yw+w2;
> ideal I = f1,f2,f3,f4,f5,f6,f7,f8,f9;
> ideal G = groebner(I);
> G;
G[1]=w3-1
G[2]=z-w4
G[3]=y2+yw+w2
G[4]=x+0.333333*y2w2+1.33333*yw3+1.33333*w4
```

Jedno od rešenja ovog sistema jednačina je $w = \omega, z = \omega, x = \omega^2, y = 1$, gde je $\omega = e^{2\pi i/3}$ primitivni treći koren iz jedinice. Dakle, čvorove w i z možemo obojiti istom bojom, a čvorove x i y drugim dvema raspoloživim bojama.

4.5 Sudoku

Sudoku je problem popunjavanja tabele dimenzije 9×9 brojevima od 1 do 9 tako da se u svakom vrsti, svakoj koloni i svakom podkvadratu dimenzija 3×3 nalaze svi brojevi od 1 do 9 (slika 4.3).

Da bismo ilustrovali mogućnost rešavanja problema sudoku tehnikom Grebnerovih baza, radićemo sa jednostavnijom varijantom problema koji se zove šidoku. Šidoku tabla je dimenzije 4×4 kod koje svaka vrsta, svaka kolona i svaki 2×2 podkvadrat sadrži brojeve od 1 do 4 tačno jednom (slika 4.4). Postoji veći broj načina na koje je moguće predstaviti uslove šidoku problema u vidu polinoma.

Jedan način da se to uradi jeste da se svakom od 16 polja table dodeli po jedna promenljiva v_i koja može imati vrednost $1, 2, 3$ ili 4. Za svaku od promenljivih $v_i, 1 \leq i \leq$

7				1				5
		5				6	8	
	1	2					9	
					4			
1				7				3
			5					
	3					4	1	
	9	7				5		
6				3				2

7	6	9	8	1	3	2	4	5
3	4	5	2	9	7	6	8	1
8	1	2	6	4	5	3	9	7
5	7	6	3	8	4	1	2	9
1	2	4	9	7	6	8	5	3
9	8	3	5	2	1	7	6	4
2	3	8	7	5	9	4	1	6
4	9	7	1	6	2	5	3	8
6	5	1	4	3	8	9	7	2

Slika 4.3: Sudoku problem i jedno njegovo rešenje.

			4
4		2	
	3		1
1			

3	2	1	4
4	1	2	3
2	3	4	1
1	4	3	2

Slika 4.4: Šidoku problem i jedno njegovo rešenje.

16 ovu činjenicu možemo kodirati narednim polinomom:

$$(v_i - 1)(v_i - 2)(v_i - 3)(v_i - 4) = 0. \tag{4.6}$$

Ovakvih jednačina ima ukupno 16.

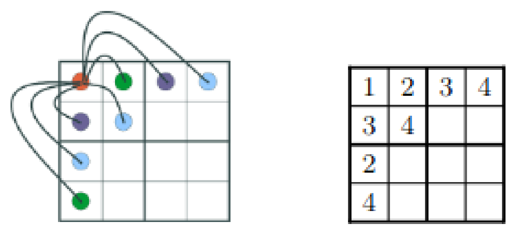
Ukoliko promenljive v_i, v_j, v_k i v_l odgovaraju poljima iste vrste (iste kolone ili istog 2×2 podkvadrata), njima je potrebno dodeliti različite vrednosti. Pokazuje se da je jedini način da se izaberu četiri broja iz skupa $\{1, 2, 3, 4\}$ čiji je zbir 10 a proizvod 24 da se izabere svaki od brojeva po jednom. To znači da se uslov na svakoj vrsti, koloni i podkvadratu dimenzije 2×2 može opisati parom polinomijalnih jednačina oblika:

$$\begin{aligned} v_i + v_j + v_k + v_l - 10 &= 0 \\ v_i v_j v_k v_l - 24 &= 0 \end{aligned} \tag{4.7}$$

Šidoku tabla ima 4 vrste, 4 kolone i 4 kvadrata dimenzije 2×2, pa je ove uslove potrebno zadati na 12 kombinacija od po 4 promenljive. Na ovaj način dobija se $2 \cdot 12 = 24$ nove jednačine. Zajedno sa prethodnih 16, dobijamo sistem od ukupno 40 polinomijalnih jednačina kojim se opisuju pravila popunjavanja šidoku table.

Dodatno, da bismo predstavili konkretan šidoku problem kod koga su neke vrednosti u tabeli već fiksirane potrebno je da dodamo jednačine kojima se zadaju konkretne vrednosti za promenljive koje odgovaraju tim poljima, npr. $v_4 = 4, v_5 = 4, v_7 = 2, v_{10} = 3, v_{12} = 1, v_{13} = 1$ za problem sa slike 4.4.

Interesantno je da ovaj problem možemo rešiti i drugačijim kodiranjem. Naime, umesto da istovremeno posmatramo sva polja tabele koja pripadaju istoj koloni, vrsti ili 2×2 kvadratu, možemo posmatrati parove polja koji moraju imati različite vrednosti. Ovo je u tesnoj vezi sa problemom bojenja grafa: sva polja tabele odgovaraju čvorovima grafa, dok je svako od polja granom povezano sa svim poljima iz iste vrste, iste kolone i odgovarajućeg 2×2 regiona (slika 4.5). Pitanje koje se onda postavlja jeste da li je dati graf 4-obojiv: ako jeste, onda svakoj od boja možemo pridružiti jednu od vrednosti $1, 2, 3$ i 4 i uslovi problema biće zadovoljeni.



Slika 4.5: Deo grafa koji odgovara šidoku problemu.

Ovo možemo uraditi na sledeći način: četiri boje odgovaraće četvrtim korenovima iz jedinice: $1, -1, i, -i$. Uslov da je svako polje tabele obojeno nekom bojom kodiramo uslovom:

$$v_i^4 - 1 = 0,$$

a za svaka dva polja v_i i v_j iz iste vrste, kolone ili 2×2 kvadrata potrebno je da važi da su im pridružene različite vrednosti, što možemo kodirati činjenicom da je:

$$\frac{v_i^4 - v_j^4}{v_i - v_j} = (v_i + v_j)(v_i^2 + v_j^2) = 0.$$

Na ovaj način dobijamo po 6 uslova za svaku kolonu, po 6 uslova za svaku vrstu i po 2 nova uslova za svaki 2×2 kvadrat, odnosno ukupno 56 polinomijalnih jednačina, koji zajedno sa prethodnih 16 jedanačina čine sistem od 72 polinomijalne jednačine.

Glava 5

Radikali i dokazivanje teorema u geometriji

Teoreme elementarne geometrije su oduvek smatrane dobrim test skupom u oblasti metoda za automatsko dokazivanje teorema. Najveći uspeh u automatskom dokazivanju teorema u geometriji imaju algebarske metode. Osnovna ideja algebarskih metoda je u tome da se pretpostavke geometrijskih tvrđenja transformišu u jednakosti nad koordinatama odgovarajućih tačaka i da se zatim nizom algebarskih transformacija pokaže da važi i zaključak odgovarajućeg tvrđenja. Algebarske metode su efikasne, međutim dokazi koji se pomoću njih dobijaju ne oslikavaju geometrijsku prirodu problema koji se rešava, nisu čitljivi niti nalik tradicionalnim geometrijskim dokazima, te nisu pogodni za obrazovne primene. Pored metode Grebnerovih baza, druga veoma uspešna algebarska metoda za dokazivanje teorema u geometriji je Vuova metoda, o kojoj ovde neće biti reči. Pomenimo i to da se metodom Grebnerovih baza mogu dokazati neka tvrđenja, međutim da postoje tvrđenja koja na ovaj način nije moguće dokazati.

5.1 Radikali ideala

Da bismo mogli da dokazujemo geometrijska tvrđenja neophodno je da uvedemo još neke algebarske pojmove.

Definicija 12 (Radikal). *Ideal I je* radikal *ako iz toga da važi $f^m \in I$ za neki ceo broj $m \geq 1$ sledi da i $f \in I$.*

Primer 43. *Razmotrimo najjednostavniji scenario, kada je ideal generisan samo jednim polinomom nad samo jednom promenljivom. Neka je ideal $I = \langle x^2 - 2x + 1 \rangle$ i polinom $f = x - 1$. Primetimo da polinom $f^2 = (x-1)^2 = x^2 - 2x + 1$ trivijalno pripada idealu I, kao element skupa generatora ideala. Međutim, polinom $f = x - 1$ ne pripada idealu I, jer je proizvoljni element ideala I oblika $h(x) \cdot (x^2 - 2x + 1) = h(x) \cdot (x-1)^2$, odnosno deljiv je sa $(x-1)^2$, a f nije deljivo sa $(x-1)^2$. Stoga ideal I nije radikal.*

Primer 44. *U prstenu polinoma nad jednom promenljivom, radikali su ideali generisani polinomima bez ponovljenih nula. Na primer, ideali* $I_1 = \langle x^2 + 1 \rangle$ *i* $I_2 = \langle x^2 - 1 \rangle$ *jesu radikali. S druge strane, ideal* $I_3 = \langle (x+1)^2 \cdot (x-1) \rangle$ *nije radikal jer za* $f = (x+1)(x-1)$ *važi* $f^2 \in I_3$*, ali* $f \notin I_3$*.*

Primer 45. *Razmotrimo nešto složeniji ideal* $I = \langle x^2 - y^2, x \rangle$ *iz prstena polinoma nad dve promenljive* x *i* y*. Označimo polinome nad kojima je ideal generisan sa* $p(x) = x^2 - y^2$ *i* $q(x) = x$*. Važi* $x \cdot q(x) - p(x) = x^2 - (x^2 - y^2) = y^2$ *te* $f^2 = y^2 \in I$*. Međutim, polinom* $f = y \notin I$ *jer za sve termove polinoma iz ideala* I *u kojima se javlja promenljiva* y *važi da su barem drugog stepena po* y*.*

Navedeni primeri govore da neki ideali jesu radikali, a neki nisu.

Definicija 13 (Radikal ideala)**.** *Neka je* $I \subset K[x_1, x_2, \ldots, x_n]$ *ideal.* Radikal ideala I *(u oznaci* $\sqrt{I}$*) je skup* $\{f \mid f^m \in I$ *za neki ceo broj* $m \geq 1\}$*.*

Važi da je radikal nekog ideala i sam jedan ideal. Primetimo i to da je neki ideal radikal ako je jednak svom radikalu.

Primer 46. *Za ideal* $I = \langle x^2 - 2x + 1 \rangle$ *i polinom* $f = x - 1$ *iz primera 43 možemo zaključiti da pošto* f^2 *pripada idealu* I*, onda trivijalno i polinom* f^2 *pripada radikalu* $\sqrt{I}$*, ali takođe i polinom* f *pripada radikalu* $\sqrt{I}$ *ideala* I*. Šta više, radikal ideala* I *biće ideal sam po sebi i biće generisan polinomom* $x - 1$*, tj.* $\sqrt{I} = \langle x - 1 \rangle$*.*

Praktična vežba 18. *Funkcija* `radical` *iz biblioteke* `primdec.lib` *za dati ideal* I *izračunava njegov radikal. Izračunajmo radikal ideala iz primera 46.*

```
> LIB "primdec.lib";
> ring r = 0, (x), lp;
> poly  p = x2 - 2x + 1;
> ideal I = p;
> ideal R = radical(I);
> R;
R[1]=x-1
```

Zaključujemo da je radikal ideala $I = \langle x^2 - 2x + 1 \rangle$ *generisan polinomom* $x - 1$*.*

Praktična vežba 19. *Izvršimo proveru da li je ideal* $I_1 = \langle x^2 - 1 \rangle$ *iz primera 44 radikal.*

```
> poly q = x2 - 1;
> ideal I = q;
> ideal R = radical(I);
> R;
R[1]=x2-1
```

Pošto je radikal ideala I *generisan polinomom* $x^2 - 1$*, zaključujemo da je ideal* I *radikal.*

Praktična vežba 20. *Funkcija* `radicalMemberShip` *iz biblioteke* `tropical.lib` *proverava da li polinom* f *pripada radikalu ideala* I *i vraća 1 ako* $f \in \sqrt{I}$*, a 0 inače. Izvršimo proveru pripadnosti polinoma* $x - 1$ *i polinoma* $x + 1$ *radikalu ideala* $I = \langle x^2 - 2x + 1 \rangle$ *iz primera 46.*

```
> LIB "tropical.lib";
> ring r = 0, (x), lp;
> poly p = x2 - 2x + 1;
> ideal I = p;
> poly q = x - 1;
> radicalMemberShip(q,I);
1
> poly s = x + 1;
> radicalMemberShip(s,I);
0
```

Primer 47. *Radikal ideala* $I = \langle x^2 - y^2, x \rangle$ *iz primera 45 je* $\sqrt{I} = \langle x, y \rangle$*. Naime, trivijalno važi* $x \in \sqrt{I}$*, a pošto* $y^2 \in I$*, onda i* $y \in \sqrt{I}$*, a pošto* x *i* y *pripadaju radikalu ideala* I*, onda je on njima i generisan.*

Praktična vežba 21. *Proverimo prethodni primer u Singularu.*

```
> LIB "primdec.lib";
> ring r = 0, (x,y), lp;
> poly p = x2 - y2;
> poly q = x;
> ideal I = p, q;
> ideal R = radical(I);
```

```
> R;
R[1]=y
R[2]=x
```

Primer 48. *Radikal ideala* $I = \langle x^4 \rangle$ *jednak je* $\sqrt{I} = \langle x \rangle$.

Praktična vežba 22. *Proverimo prethodni primer u alatu Singular.*

```
> LIB "primdec.lib";
> ring r = 0, (x), lp;
> poly p = x4;
> ideal I = p;
> ideal R = radical(I);
> R;
R[1]=x
```

Teorema 10. *Pretpostavimo da* $f_1, f_2, \ldots, f_m, f \in K[x_1, x_2, \ldots, x_n]$. *Ako je* $I = \langle f_1, f_2, \ldots, f_m \rangle$ *i* $f \in \sqrt{I}$, *onda* $f \in V(I)$, *tj. iz uslova da važi*

$$f_1(a_1, a_2, \ldots, a_n) = 0, f_2(a_1, a_2, \ldots, a_n) = 0, \ldots, f_m(a_1, a_2, \ldots, a_n) = 0$$

sledi

$$f(a_1, a_2, \ldots, a_n) = 0.$$

Tvrđenje Teoreme 10 možemo iskoristiti za dokazivanje da iz nekog skupa tvrđenja $f_i = 0$, $1 \leq i \leq m$ sledi tvrđenje $f = 0$. Međutim, potrebno je imati neki jednostavan test kojim bi se moglo proveriti da li neki polinom f pripada radikalu ideala I. Bilo bi jako neefikasno za svako $m > 0$ proveravati da li $f^m \in I$ i stati kada pronađemo takvo m. S druge strane, može se desiti da $f \notin \sqrt{I}$ što na ovaj način ne bismo mogli da utvrdimo. Dakle, potrebno je pronaći neki efektivni test za ispitivanje pripadnosti polinoma radikalu. Naredna teorema nam daje takav test.

Teorema 11 (Pripadnost radikalu)**.** *Neka je* K *proizvoljno polje i neka je* $I = \langle f_1, f_2, \ldots, f_m \rangle \subset K[x_1, x_2, \ldots, x_n]$ *ideal. Tada* $f \in \sqrt{I}$ *ako i samo ako konstantni polinom* 1 *pripada idealu* $I' = \langle f_1, f_2, \ldots, f_m, 1 - yf \rangle \subset K[x_1, x_2, \ldots, x_n, y]$, *gde je* y *nova promenljiva.*

Tvrđenje da za svako $x_1, \ldots, x_n$ iz skupa jednakosti $f_1(x_1, \ldots, x_n) = 0, \ldots, f_m(x_1, \ldots, x_n) = 0$ sledi jednakost $f(x_1, \ldots, x_n) = 0$ ekvivalentno je tvrđenju da ne postoje $x_1, x_2, \ldots, x_n$ tako da istovremeno važi $f_1(x_1, \ldots, x_n) = 0, \ldots, f_m(x_1, \ldots, x_n) = 0$ i $f(x_1, \ldots, x_n) \neq 0$. Ako je $f(x_1, \ldots, x_n) \neq 0$ onda $f(x_1, \ldots, x_n)$ ima inverz u odnosu na množenje, tj. postoji neko y tako da je $y \cdot f(x_1, \ldots, x_n) = 1$, odnosno $1 - y \cdot f(x_1, \ldots, x_n) = 0$. Ovo pak odgovara tome da ne postoje $x_1, x_2, \ldots, x_n$ i y tako da istovremeno važi $f_1(x_1, \ldots, x_n) =$

$0, \ldots, f_m(x_1, \ldots, x_n) = 0$ i $1 - y \cdot f(x_1, \ldots, x_n) = 0$. Ovim smo problem sveli na rešavanje ovog sistema polinomijalnih jednačina, odnosno na ispitivanje postojanja zajedničkih nula polinoma što je moguće utvrditi metodom Grebnerovih baza: naime, kao što je već navedeno u poglavlju 4.1 skup polinoma nema zajedničkih nula ako i samo ako je njegova redukovana Grebnerova baza jednaka $\{1\}$.

Pokazuje se, međutim, da u mnogim situacijama odgovarajući sistem jednačina ima zajedničke nule, odnosno odgovarajuća Grebnerova baza daje moguća rešenja koja se mogu razmatrati kao degenerisani slučajevi. U tim slučajevima se ne može garantovati da iz tvrđenja $f_1, f_2, \ldots, f_m$ sledi tvrđenje f, dok u ostalim slučajevima tvrđenje može biti tačno.

Uvođenje novih promenljivih (kao u prethodnoj teoremi) se pokazuje kao korisna tehnika za rešavanje problema pripadnosti radikalu. Napomenimo i to da ako ideal sadrži vrednost 1, onda je redukovana Grebnerova baza tog ideala jednaka $\{1\}$.

Na osnovu Teoreme 10 i Teoreme 11 sledi naredna teorema.

Teorema 12. *Neka su $h_1, h_2, \ldots, h_m$ hipoteze, a g zaključak tvrđenja koje treba dokazati. Zaključak g sledi iz hipoteza $h_1, h_2, \ldots, h_m$ ako i samo ako je $\{1\}$ redukovana Grebnerova baza ideala $\langle h_1, h_2, \ldots, h_m, 1 - yg\rangle$, gde je y nova promenljiva.*

Ova teorema biće korišćena za dokazivanje geometrijskih tvrđenja.

5.2 Osnovni postupak dokazivanja

Razmatraćemo geometriju kao teoriju prvog reda i njenu interpretaciju u domenu koji čini brojevni sistem koji je algebarsko zatvorenje[1] $\overline{K}$ polja K, odnosno geometrijski objekti leže u $\overline{K}^n$ za neko $n \in \mathbb{N}$. Razlog zbog koga je neophodno da polje bude algebarski zatvoreno ćemo navesti na kraju ovog poglavlja. Tvrđenja koja je moguće dokazivati se sastoje od određenog broja hipoteza i jednog ili većeg broja zaključaka, gde se na hipoteze i zaključke može gledati kao na neku konfiguraciju geometrijskih objekata poput tačaka, pravih i krugova. Uvođenjem Dekartovih koordinata u Euklidsku ravan, moguće je definisati odgovarajući skup polinoma $h_1, h_2, \ldots, h_m$ u terminima koordinata tačaka $x_1, x_2, \ldots, x_n$ tako da je $h_1(x_1, x_2, \ldots, x_n) = \ldots = h_m(x_1, x_2, \ldots, x_n) = 0$ tačno kada su uslovi tvrđenja zadovoljeni. Tvrđenja koja ćemo dokazivati su oblika:

$$(\forall x \in \overline{K}^n)(h_1(x) = \ldots = h_m(x) = 0 \Rightarrow g(x) = 0)$$

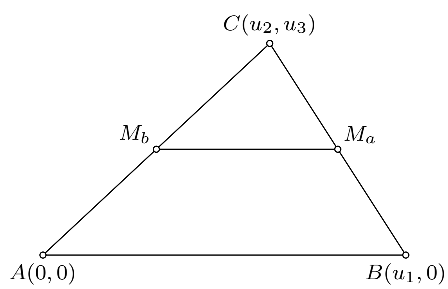
gde su $h_1, h_2, \ldots, h_m, f$ polinomi u $K[x_1, x_2, \ldots, x_n]$. Polinome $h_1, h_2, \ldots, h_m$ zvaćemo *hipotezama* ili *premisama*, a polinom f *zaključkom* tvrđenja koje dokazujemo. Na ovaj način možemo da rezonujemo o raznim geometrijskim tvrđenjima kao što su incidencija tačaka, paralelnost i upravnost pravih, pripadnost tačaka krugu i dr.

Najpre je potrebno smestiti osnovne objekte u koordinatnu ravan, pridruživanjem koordinata svim značajnim tačkama i to tako da tačke čiji je položaj nezavisan od pozicija ostalih tačaka sa slike imaju koordinate u_i, a tačke čiji položaj zavisi od položaja ostalih

[1] Algebarsko zatvorenje polja K je njegovo raširenje koje je algebarski zatvoreno, odnosno za koje važi da svaki nekonstantan polinom sa koeficijentima iz K ima koren u K. Polje realnih brojeva $\mathbb{R}$ nije algebarski zatvoreno, jer na primer jednačina $x^2 + 1 = 0$ čiji su koeficijenti iz skupa $\mathbb{R}$ nema rešenja u polju realnih brojeva. Slično, ni polje racionalnih brojeva $\mathbb{Q}$ nije algebarski zatvoreno. Međutim, polje kompleksnih brojeva $\mathbb{C}$ jeste algebarski zatvoreno.

tačaka na slici sa x_i. Dodeljivanje koordinata tačkama omogućava prevođenje hipoteza i zaključka (ili zaključaka) teoreme iz jezika geometrije u polinomijalne jednakosti u odnosu na pogodno odabran koordinatni sistem. Da bi teorema važila potrebno je da polinomi koji predstavljaju zaključak teoreme pripadaju idealu koji je generisan polinomima koji predstavljaju hipoteze. To se može proveriti na sledeći način: za ideal generisan hipotezama tvrđenja koje se dokazuje računa se njegova Grebnerova baza, a zatim se polinom koji predstavlja zaključak deli skupom polinoma Grebnerove baze: ako se pritom dobije ostatak 0, tada se zaključak može zapisati kao linearna kombinacija polinoma Grebnerove baze što znači da je on element ideala generisanog hipotezama tvrđenja koje dokazujemo. Napomenimo da je postupak ispitivanja da li neki polinom pripada datom idealu primenom algoritma deljenja u prstenu više promenljivih vremenski zahtevan i da se zbog toga često koristi metod koji proverava pripadnost radikalu, a koji se svodi na računanje redukovane Grebnerove baze malo izmenjenog ideala.

U kom smislu zaključak g tvrđenja treba da sledi iz hipoteza $h_1, h_2, \ldots, h_m$? Potrebno je da se tvrđenje g anulira u svakoj od tačaka u kojoj se anuliraju hipoteze $h_1, h_2, \ldots, h_m$. Drugim rečima, potrebno je da svaka tačka afinog varijeteta definisanog hipotezama $h_1, h_2, \ldots, h_m$ zadovoljava i zaključak g.



Slika 5.1: Srednja linija trougla paralelna je naspramnoj stranici trougla.

Primer 49. *Neka je ABC trougao i neka je M_b središte stranice AC, a M_a središte stranice BC. Dokazati da je srednja linija M_bM_a trougla ABC paralelna stranici AB.*

Potrebno je najpre smestiti osnovne objekte u koordinatnu ravan i nakon toga interpretirati hipoteze i zaključak teoreme kao tvrđenja u terminima koordinata. Pritom, želimo da napravimo razliku između koordinata nezavisnih i zavisnih tačaka; naime, vrednostima u_i obeležavamo koordinate nezavisnih tačaka, a vrednostima x_i koordinate tačaka čija pozicija zavisi od drugih tačaka na slici. Naravno, da bi dokaz bio korektan u opštem slučaju, koordinate tačaka ne smeju biti direktno zadate; ipak, možemo zadati koordinate kojima se ne narušava opštost, a sa kojima se lakše računa. Naime, svojstva geometrijskih figura kao što su prave, uglovi, poligoni i krugovi se ne menjaju pod dejstvom translacije i rotacije u euklidskoj ravni, te prilikom uvodjenja Dekartovih koordinata možemo objekat smestiti na neku pogodnu lokaciju. Na primer, teme A možemo smestiti u koordinatni početak, tj.

možemo mu pridružiti koordinate $A(0,0)$, a stranicu AB postaviti tako da bude paralelna x osi, tj. temenu B možemo pridružiti koordinate $B(u_1,0)$. Na koordinate temena C ne smemo postaviti nikakva ograničenja da bismo razmatrali proizvoljan trougao. Dakle, temenu C pridružujemo koordinate $C(u_2,u_3)$ (slika 5.1).

Pozicije tačaka M_b i M_a zavise od pozicija temena trougla ABC te ćemo njima pridružiti koordinate $M_b(x_1,y_1)$ i $M_a(x_2,y_2)$. Tačka M_b je središte duži AC te za x koordinatu tačke M_b važi uslov:

$$\begin{aligned} 2x_1 &= u_2 \\ h_1 &= 2x_1 - u_2 = 0 \end{aligned}$$

Slično, za y koordinatu tačke M_b važi:

$$\begin{aligned} 2y_1 &= u_3 \\ h_2 &= 2y_1 - u_3 = 0 \end{aligned}$$

Pošto je tačka M_a središte duži BC za njenu x koordinatu važi uslov:

$$\begin{aligned} 2x_2 &= u_1 + u_2 \\ h_3 &= 2x_2 - u_1 - u_2 = 0 \end{aligned}$$

i slično važi:

$$\begin{aligned} 2y_2 &= u_3 \\ h_4 &= 2y_2 - u_3 = 0 \end{aligned}$$

Jednakosti $h_1 = 0, h_2 = 0, h_3 = 0$ i $h_4 = 0$ predstavljaju hipoteze tvrđenja koje treba dokazati. Zaključak tvrđenja, da su duži M_bM_a i AB paralelne, s obzirom na to da je duž AB paralelna x osi može se zapisati u vidu uslova da su y koordinate tačaka M_b i M_a jednake, odnosno da važi:

$$\begin{aligned} y_1 &= y_2 \\ g &= y_2 - y_1 = 0 \end{aligned}$$

Dakle, treba pokazati da svaka n-torka vrednosti koja zadovoljava jednačine $h_1 = 0, h_2 = 0, h_3 = 0, h_4 = 0$ takođe zadovoljava i jednačinu $g = 0$, odnosno da važi:

$$\begin{aligned} &\forall u_1\ u_2\ u_3\ x_1\ y_1\ x_2\ y_2 \in \mathbb{R} \\ 2x_1 - u_2 = 0 \ \wedge\ 2y_1 - u_3 = 0 \ \wedge\ &2x_2 - u_1 - u_2 = 0 \ \wedge 2y_2 - u_3 = 0 \\ &\Rightarrow y_2 - y_1 = 0 \end{aligned}$$

Primetimo da je

$$g = y_2 - y_1 = \frac{1}{2}h_4 - \frac{1}{2}h_2$$

te pripada idealu $I = \langle h_1, h_2, h_3, h_4 \rangle$ odakle sledi tačnost polaznog tvrđenja.

Praktična vežba 23. *Proverimo ovaj primer u alatu Singular. Promenljive* u_1, u_2 *i* u_3 *preimenovaćemo u* a, b *i* c, *redom, dok ćemo promenljive* x_1, x_2, y_1 *i* y_2 *preimenovati u* x, y, z *i* w *(želimo da napravimo razliku između koordinata polaznih, nezavisnih tačaka i koordinata tačaka čije vrednosti zavise od pozicije polaznih tačaka). Definišemo polinome* h_1, h_2, h_3 *i* h_4 *koji predstavljaju hipoteze i polinom* g *koji predstavlja zaključak tvrđenja koje se dokazuje. Proverimo da li polinom* g *pripada idealu* I *koji je generisan polinomima hipoteza tvrđenja.*

```
> ring r = 0, (a,b,c,x,y,z,w), lp;
> poly h1 = 2x - b;
> poly h2 = 2y - c;
> poly h3 = 2z - a - b;
> poly h4 = 2w - c;
> poly g = w - y;
> ideal I = h1, h2, h3, h4;
> ideal G = groebner(I);
> reduce(g,G);
0
```

Kao ostatak pri deljenju polinoma g *polinomima Grebnerove baze ideala* I *dobijamo 0, te zaključujemo da polinom* g *pripada idealu* I *i da će njegova vrednost biti jednaka* 0 *uvek kada polinomi hipoteza* h_i *imaju vrednost 0.*

Do istog zaključka možemo doći i na drugačiji način, na osnovu Teoreme 12: izračunavamo redukovanu Grebnerovu bazu ideala I *definisanog nad skupom hipoteza* h_1, h_2, h_3 *i* h_4 *i nad polinomom* $1 - v \cdot g$, *gde je* v *nova promenljiva i proveravamo da li je ona jednaka* $\{1\}$. *U ovom slučaju prilikom definisanja prstena polinoma, potrebno je navesti i dodatnu promenljivu* v.

```
> ring r = 0, (a,b,c,x,y,z,w,v), lp;
> poly h1 = 2x - b;
> poly h2 = 2y - c;
> poly h3 = 2z - a - b;
> poly h4 = 2w - c;
> poly g = w - y;
> ideal I = h1, h2, h3, h4, 1 - v * g;
> ideal G = groebner(I);
> G;
G[1]=1
```

Pošto je Grebnerova baza ovog ideala jednaka $\{1\}$ *zaključujemo da zaključak tvrđenja opisan polinomom* g *sledi iz premisa tvrđenja opisanih polinomima* h_1, h_2, h_3 *i* h_4.

Kazaćemo da zaključak g *sledi striktno* (eng. follows strictly) iz hipoteza $h_1, h_2, \ldots, h_m$ ako $g \in I(V) \subset K[u_1, u_2, \ldots, u_l, x_1, x_2, \ldots, x_j]$ gde je $V = V(h_1, h_2, \ldots, h_m)$. U nekim slučajevima geometrijsko tvrđenje je tačno, ali zaključak ne sledi striktno iz skupa hipoteza. Kada zaključak ne sledi striktno iz skupa hipoteza, potencijalno zbog degenerisanih slučajeva, želeli bismo da analiziramo tačnost tvrđenja izuzimajući degenerisane slučajeve. U tom slučaju ispitivaćemo da li zaključak *sledi uopšteno* (eng. follows generically) iz skupa hipoteza.

Važe naredna dva tvrđenja:

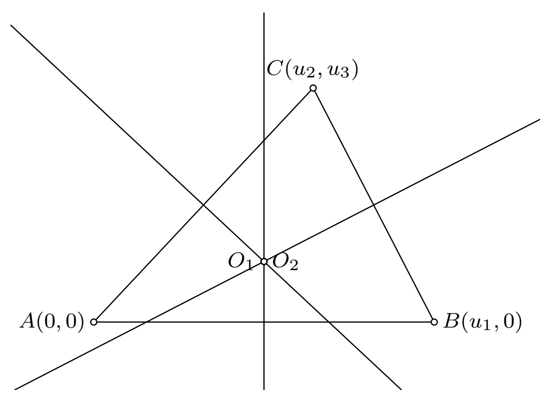
Teorema 13. *Ako* $g \in \sqrt{\langle h_1, h_2, \ldots, h_m \rangle}$ *gde su* $h_1, h_2, \ldots, h_m \in \mathbb{R}[u_1, u_2, \ldots, u_m, x_1, x_2, \ldots, x_n]$ *onda* g *sledi striktno iz* $h_1, h_2, \ldots, h_m$.

Teorema 14. *Ako* $g \in \sqrt{\langle h_1, h_2, \ldots, h_m \rangle}$ *gde su* $h_1, h_2, \ldots, h_m \in \mathbb{R}(u_1, u_2, \ldots, u_m)[x_1, x_2, \ldots, x_n]$ *onda* g *sledi uopšteno iz* $h_1, h_2, \ldots, h_m$.

Na osnovu Teoreme 12 slede naredna dva tvrđenja koja ćemo koristiti za dokazivanje da neki zaključak sledi striktno, odnosno uopšteno iz nekog skupa hipoteza.

Teorema 15. *Neka su* $h_1, h_2, \ldots, h_m$ *hipoteze, a* g *zaključak tvrđenja. Zaključak* g *sledi striktno iz hipoteza* $h_1, h_2, \ldots, h_m$ *ako i samo ako je* $\{1\}$ *redukovana Grebnerova baza ideala* $\langle h_1, h_2, \ldots, h_m, 1-yg \rangle \subset \mathbb{R}[u_1, u_2, \ldots, u_m, x_1, x_2, \ldots, x_n, y]$*, gde je* y *nova promenljiva.*

Teorema 16. *Neka su* $h_1, h_2, \ldots, h_m$ *hipoteze, a* g *zaključak tvrđenja. Zaključak* g *sledi uopšteno iz hipoteza* $h_1, h_2, \ldots, h_m$ *ako i samo ako je* $\{1\}$ *redukovana Grebnerova baza ideala* $\langle h_1, h_2, \ldots, h_m, 1 - yg \rangle \subset \mathbb{R}(u_1, u_2, \ldots, u_m)[x_1, x_2, \ldots, x_n, y]$*, gde je* y *nova promenljiva.*



Slika 5.2: Medijatrise stranica trougla seku se u jednoj tački.

Primer 50. *Dokazati da se medijatrise (simetrale) stranica trougla* ABC *seku u jednoj tački.*

Teme A *smeštamo u koordinatni početak, tj. pridružujemo mu koordinate* $A(0,0)$*, a stranicu* AB *postavljamo tako da bude paralelna* x *osi, tj. temenu* B *možemo pridružiti koordinate* $B(u_1, 0)$*. Na koordinate temena* C *ne postavljamo nikakva ograničenja i pridružujemo mu koordinate* $C(u_2, u_3)$ *(slika 5.2).*

Razmotrimo na koji način možemo doći do jednačine medijatrise duži PQ čije krajnje tačke imaju koordinate $P(p_1, p_2)$ i $Q(q_1, q_2)$. Medijatrisu duži PQ možemo okarakterisati kao pravu koja prolazi kroz središte duži PQ i koja je upravna na duž PQ. Označimo središte duži PQ sa M – ono ima koordinate $M(\frac{p_1+q_1}{2}, \frac{p_2+q_2}{2})$. Za koeficijente pravaca međusobno upravnih pravih (osim kada je jedna od njih horizontalna) važi da im je proizvod jednak -1. Duž PQ ima koeficijent pravca $k_1 = \frac{q_2-p_2}{q_1-p_1}$, te medijatrisa duži PQ kao njoj upravna prava ima koeficijent pravca $k_2 = -\frac{1}{k_1} = -\frac{q_1-p_1}{q_2-p_2}$. Dakle, medijatrisa duži PQ ima jednačinu:

$$y - y_M = k_2(x - x_M).$$

Zamenom vrednosti x i y koordinata tačke M i vrednosti koeficijenta pravca medijatrise duži PQ dobijamo jednačinu medijatrise duži PQ:

$$y - \frac{p_2+q_2}{2} = -\frac{q_1-p_1}{q_2-p_2}\Big(x - \frac{p_1+q_1}{2}\Big).$$

Grupisanjem članova uz x i y dobijamo:

$$\frac{q_1-p_1}{q_2-p_2}x + y - \frac{q_2^2 - p_2^2 + q_1^2 - p_1^2}{2(q_2-p_2)} = 0.$$

odnosno:

$$2(q_1-p_1)x + 2(q_2-p_2)y - q_2^2 + p_2^2 - q_1^2 + p_1^2 = 0.$$

Specijalno, kada razmatramo trougao ABC, medijatrise njihovih stranica imaju naredne jednačine: medijatrisa m_c stranice AB zadata je jednačinom:

$$\begin{aligned} x - \frac{u_1}{2} &= 0 \\ m_c:\ 2x - u_1 &= 0 \end{aligned}$$

medijatrisa m_a stranice BC jednačinom:

$$\begin{aligned} \frac{u_2-u_1}{u_3}x + y - \frac{u_3^2+u_2^2-u_1^2}{2u_3} &= 0 \\ m_a:\ 2(u_2-u_1)x + 2u_3y - u_3^2 - u_2^2 + u_1^2 &= 0 \end{aligned}$$

a medijatrisa m_b stranice AC jednačinom:

$$\begin{aligned} \frac{u_2}{u_3}x + y - \frac{u_3^2+u_2^2}{2u_3} &= 0 \\ m_b:\ 2u_2x + 2u_3y - u_3^2 - u_2^2 &= 0 \end{aligned}$$

Postavlja se pitanje kako formulisati tvrđenje ove teoreme. Pretpostavimo da se medijatrise stranica AB i BC seku u tački $O_1(x_1, y_1)$, a medijatrise stranica AB i AC u tački $O_2(x_2, y_2)$. Dobijamo naredni sistem jednačina:

$$\begin{aligned} h_1 &= 2x_1 - u_1 = 0 \ \ (O_1 \in m_c) \\ h_2 &= 2(u_2-u_1)x_1 + 2u_3y_1 - u_3^2 + u_1^2 - u_2^2 = 0 \ \ (O_1 \in m_a) \\ h_3 &= 2x_2 - u_1 = 0 \ \ (O_2 \in m_c) \\ h_4 &= 2u_2x_2 + 2u_3y_2 - u_3^2 - u_2^2 = 0 \ \ (O_2 \in m_b) \end{aligned}$$

kojim je zadata konstrukcija tačaka O_1 *i* O_2. *Tvrđenje koje treba pokazati jeste da za ovako konstruisane tačke* O_1 *i* O_2 *važi* $O_1 = O_2$, *odnosno da važi* $x_1 = x_2$ *i istovremeno važi* $y_1 = y_2$, *odnosno da li važe uslovi:*

$$\begin{aligned} g_1 &= x_1 - x_2 = 0 \\ g_2 &= y_1 - y_2 = 0 \end{aligned}$$

Dato tvrđenje je moguće pokazati na nekoliko načina. Prvi način se zasniva na proveri da li polinomi g_1 *i* g_2 *pripadaju idealu* $I = \langle h_1, h_2, h_3, h_4 \rangle$. *Da bismo to utvrdili izračunaćemo Grebnerovu bazu* B *ideala generisanog skupom polinoma* $S = \{h_1, h_2, h_3, h_4\}$ *u prstenu* $K[u_1, u_2, u_3, x_1, x_2, y_1, y_2]$ *i pokazati da je ostatak pri deljenju polinoma* $g_1 = x_1 - x_2$ *polinomima baze* B *jednak* 0 *i, analogno, da je ostatak pri deljenju polinoma* $g_2 = y_1 - y_2$ *polinomima baze* B *jednak* 0. *Kao redukovanu Grebnerovu bazu datog ideala dobijamo* $B = \{b_1, b_2, b_3, b_4\}$, *pri čemu važi:*

$$\begin{aligned} b_1 &= x_1 - x_2 = 0 \\ b_2 &= u_3 y_1 - u_3 y_2 = 0 \\ b_3 &= u_2^2 - 2u_2 x_1 + u_3^2 - 2u_3 y_2 = 0 \\ b_4 &= u_1 - 2x_2 = 0 \end{aligned}$$

Lako se pokazuje da je ostatak pri deljenju polinoma $g_1 = x_1 - x_2$ *polinomima Grebnerove baze* B *jednak 0, međutim to ne važi za polinom* g_2. *Dakle, tvrđenje teoreme ne sledi striktno. Proverimo da li sledi uopšteno. Naime, ako* u_3 *ne posmatramo kao promenljivu nad kojom su definisani polinomi, već kao vrednost parametra iz skupa racionalnih brojeva, vidimo da važi:*

$$y_1 - y_2 = \frac{1}{u_3} b_2$$

te polinom g_2 *trivijalno pripada idealu* $\mathbb{R}(u_1, u_2, u_3)[x_1, x_2, y_1, y_2]$.

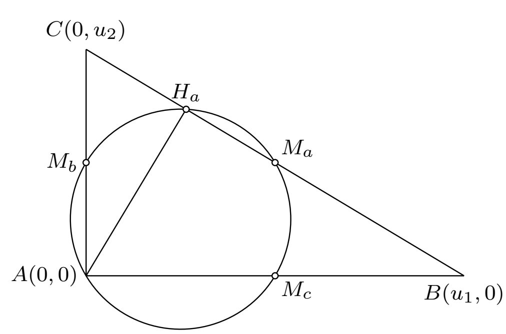
Praktična vežba 24. *Proverimo prethodni primer u alatu Singular. Najpre je potrebno zadati da su koeficijenti polinoma koje razmatramo racionalni brojevi, da su polinomi iz hipoteza i zaključaka formulisani u terminima promenljivih* u_1, u_2 *i* u_3 *(koje odgovaraju koordinatama tačaka koje su inicijalno date) i promenljivih* x_1, x_2, y_1 *i* y_2 *koje odgovaraju koordinatama zavisnih tačaka. Redom ćemo ih preimenovati u* a, b *i* c, *odnosno* x, y, z *i* w. *Definišemo polinome* h_1, h_2, h_3 *i* h_4 *koji predstavljaju hipoteze tvrđenja koje se dokazuje i polinome* g_1 *i* g_2 *koji predstavljaju zaključke. Proverimo da li polinomi* g_1 *i* g_2 *pripadaju idealu* $I = \langle h_1, h_2, h_3, h_4 \rangle$.

```
> ring r = 0, (a,b,c,x,y,z,w), lp;
> poly h1 = 2x - a;
> poly h2 = 2*(b-a)*x + 2cz - c2 + a2 - b2;
> poly h3 = 2y - a;
> poly h4 = 2*b*y + 2cw - c2 - b2;
```

```
> ideal I = h1, h2, h3, h4;
> ideal G = groebner(I);
> poly g1 = x - y;
> reduce(g1,G);
0
> poly g2 = z-w;
> reduce(g2,G);
z-w
```

Pošto ostatak pri deljenju polinoma g_2 polinoma Grebnerove baze nije jednak 0, zaključujemo da dato tvrđenje nije uvek tačno, tj. da možda postoje neki dodatni uslovi nedegenerisanosti koje treba uključiti. Probajmo da dokažemo tvrđenje do na uslove nedegenerisanosti. Jedino što menjamo jeste definicija prstena – sada na koordinate nezavisnih tačaka gledamo kao na parametre, a ne kao na promenljive u polinomu:

```
> ring r = (0,a,b,c), (x,y,z,w), lp;
> poly h1 = 2x - a;
> poly h2 = 2*(b-a)*x + 2cz - c2 + a2 - b2;
> poly h3 = 2y-a;
> poly h4 = 2*b*y + 2cw - c2 - b2;
> ideal I = h1, h2, h3, h4;
> ideal G = groebner(I);
> poly g1 = x - y;
> reduce(g1,G);
0
> poly g2 = z - w;
> reduce(g2,G);
0
```



Slika 5.3: Ilustracija Apolonijeve teoreme.

Primer 51. *Neka je ABC pravougli trougao sa pravim uglom kod temena A. Središta tri stranice trougla i podnožje visine iz temena A pripadaju jednom krugu (slika 5.3). Ovo tvrđenje poznato je pod nazivom* Apolonijeva teorema *i odnosi se na krug koji je poznat kao* Ojlerov krug, *odnosno* krug devet tačaka.

Smestimo teme A u koordinatni početak, a teme B u tačku sa koordinatama $B(u_1, 0)$. Pošto je trougao pravougli, x koordinata tačke C je 0, dok y koordinata ima proizvoljnu vrednost, te temenu C pridružujemo koordinate $C(0, u_2)$. Označimo središta stranica AB, AC i BC redom sa M_c, M_b i M_a i neka ona imaju koordinate $M_c(x_1, 0)$, $M_b(0, x_2)$ i $M_a(x_3, x_4)$. Tvrđenje da je tačka M_c središte duži može se zapisati kao $x_1 = \frac{u_1}{2}$. Dakle prva hipoteza tvrđenja koje dokazujemo glasi:

$$h_1 = 2x_1 - u_1 = 0.$$

Slično, tvrđenju da je tačka M_b središte duži AC odgovara hipoteza:

$$h_2 = 2x_2 - u_2 = 0.$$

Tvrđenju da je tačka M_a središte duži BC odgovaraju uslovi da je $x_3 = \frac{u_1}{2}$ i $x_4 = \frac{u_2}{2}$, odnosno naredne dve hipoteze:

$$h_3 = 2x_3 - u_1 = 0$$

$$h_4 = 2x_4 - u_2 = 0$$

Dodelimo podnožju visine iz temena A koordinate $H_a(x_5, x_6)$. Duž AH_a je upravna na stranicu BC ako je skalarni proizvod vektora $AH_a(x_5, x_6)$ i vektora $BC(-u_1, u_2)$ jednak 0, te iz ovog uslova dobijamo narednu hipotezu:

$$h_5 = (x_5, x_6) \cdot (-u_1, u_2) = -u_1x_5 + u_2x_6 = 0$$

Dodatno, važi da su tačke B, H_a i C kolinearne, te za koeficijente pravaca duži BC i BH_a važi $k_{BC} = k_{BH_a}$, odnosno $\frac{u_2}{-u_1} = \frac{x_6}{x_5 - u_1}$, odakle dobijamo novu hipotezu:

$$h_6 = x_5u_2 - u_1u_2 + x_6u_1 = 0$$

Razmotrimo tvrđenje da tačke M_a, M_b, M_c i H_a pripadaju krugu. Možemo ga pogodnije formulisati na sledeći način: ako konstruišemo krug kroz tačke M_a, M_b i M_c, onda tačka H_a takođe pripada ovom krugu. Da bismo konstruisali krug kroz tačke M_a, M_b i M_c potrebno je da razmotrimo njegovo središte O i pridružimo mu koordinate $O(x_7, x_8)$: tačke M_a, M_b i M_c su na krugu sa središtem O ako važi da je $|M_aO| = |M_cO|$ i $|M_bO| = |M_cO|$. Odavde dobijamo

$$(x_7 - x_3)^2 + (x_8 - x_4)^2 = (x_7 - x_1)^2 + x_8^2$$

i

$$x_7^2 + (x_8 - x_2)^2 = (x_7 - x_1)^2 + x_8^2,$$

odnosno dobijamo dve nove hipoteze tvrđenja koje treba pokazati:

$$h_7 = (x_7 - x_1)^2 + x_8^2 - (x_7 - x_3)^2 - (x_8 - x_4)^2 = 0$$

$$h_8 = (x_7 - x_1)^2 + x_8^2 - x_7^2 - (x_8 - x_2)^2 = 0$$

Zaključak, da tačka H_a pripada krugu kroz tačke M_a, M_b i M_c, odnosno da važi $|H_aO| = |M_cO|$, može se formulisati u vidu uslova:

$$g = (x_7 - x_5)^2 + (x_8 - x_6)^2 - (x_7 - x_1)^2 - x_8^2 = 0$$

Ukoliko radimo u prstenu polinoma $K[u_1, u_2, x_1, \ldots, x_8]$ pri deljenju polinoma g polinomima Grebnerove baze dobijamo vrednost različitu od 0, te zaključak g ne sledi striktno iz skupa hipoteza $h_1, h_2, \ldots, h_m$.

Podsetimo se da su sa u_i označene vrednosti koje su proizvoljno izabrane i čija vrednost treba da bude različita od nule ako hoćemo da izbegnemo degenerisane slučajeve. Stoga, možemo ispitati da li zaključak tvrđenja sledi uopšteno (do na degenerisane slučajeve) iz hipoteza tvrđenja i izračunavanja izvršavati u prstenu $\mathbb{R}(u_1, u_2)[x_1, x_2, \ldots, x_8]$. Naime, ako vrednosti u_1 i u_2 posmatramo kao parametre iz polja K onda se može pokazati da polinom g pripada idealu nad polinomima $h_1, h_2, \ldots, h_8$ u prstenu polinoma $K(u_1, u_2)[x_1, x_2, \ldots, x_8]$. U ovom slučaju je ostatak pri deljenju polinoma g polinomima Grebnerove baze $G = \{g_1, g_2, \ldots, g_8\}$ ovog ideala jednak 0, odnosno da polinom g pripada idealu definisanim hipotezama $h_1, h_2, \ldots, h_8$:

$$\begin{aligned} g &= (-x_1 + 2x_7 - \frac{u_1}{2}) \cdot g_1 + (x_5 - 2x_7 + \frac{u_1 u_2^2}{u_1^2 + u_2^2}) \cdot g_5 \\ &+ (x_6 - 2x_8 + \frac{u_1^2 u_2}{u_1^2 + u_2^2}) \cdot g_6 + \frac{u_1^3 - u_1 u_2^2}{u_1^2 + u_2^2} \cdot g_7 + \frac{-2u_1^2 u_2}{u_1^2 + u_2^2} \cdot g_8 \end{aligned}$$

Obratimo pažnju da kada bismo radili u prstenu polinoma $K[u_1, u_2, x_1, \ldots, x_8]$ prethodna veza ne bi označavala pripadnost idealu, jer recimo izraz $\frac{u_1 u_2^2}{u_1^2 + u_2^2}$ ne predstavlja polinom nad promenljivim u_1 i u_2. S druge strane, kada radimo u prstenu polinoma $K(u_1, u_2)[x_1, \ldots, x_8]$, izrazi po promenljivim u_i su parametrizovani koeficijenti u polju K, i prethodna veza označava pripadnost datom idealu. Primetimo da bi je zbog vrednosti u imeniocu razlomka neophodno da važi $u_1^2 + u_2^2 \neq 0$, odnosno ne smeju istovremeno vrednosti u_1 i u_2 biti jednake 0. Ovo odgovara situaciji kada se sva tri temena trougla ABC poklapaju, što svakako treba isključiti pošto je polazna pretpostavka da radimo sa pravouglim trouglom ABC.

Praktična vežba 25. *Proverimo prethodni primer u alatu Singular. Pokažimo najpre da ako i vrednosti promenljivih u_1 i u_2 razmatramo na isti način kao i promenljive x_i, ispitivanje pripadnosti polinoma g idealu $I = \langle h_1, h_2, \ldots, h_8 \rangle$ u prstenu polinoma $K[u_1, u_2, x_1, x_2, \ldots, x_8]$ neće uspeti.*

U Singularu ćemo promenljive u_1 i u_2 preimenovati u a i b, redom, dok ćemo promenljive $x_1, x_2, \ldots, x_8$ nazvati redom x, y, z, u, v, w, s i t.

```
> ring r = 0, (a,b,x,y,z,u,v,w,s,t), lp;
> poly h1 = 2x - a;
> poly h2 = 2y - b;
```

```
> poly h3 = 2z - a;
> poly h4 = 2u - b;
> poly h5 = -av + bw;
> poly h6 = bv - ab + aw;
> poly h7 = (s-x)^2 + t2 - (s-z)^2 - (t-u)^2;
> poly h8 = (s-x)^2 + t2 - s2 - (t-y)^2;
> ideal I = h1, h2, h3, h4, h5, h6, h7, h8;
> ideal G = groebner(I);
G;
G[1]=uw2s2+uw2t2-4uws2t
G[2]=uvs-uwt
G[3]=uvwt+uw2s-4uwst
G[4]=uv2+uw2-4uwt
G[5]=u2-2ut
G[6]=zwt-u2v+2uvt-uws
G[7]=zw2-2u2v+uvw+4uvt-4uws
G[8]=zv-uw
G[9]=2zu-zw-uv
G[10]=z2-2zs-u2+2ut
G[11]=y-u
G[12]=x-z
G[13]=b-2u
G[14]=a-2z
> poly g = (s-v)^2 + (t-w)^2 - (s-x)^2 - t2;
> reduce(g,G);
v2-2vs+w2-2wt
```

Slično, ispitivanje pripadnosti polinoma g radikalu ideala nad polinomima $h_1, h_2, \ldots, h_8$ u prstenu polinoma $K[u_1, u_2, x_1, x_2, \ldots, x_8, y]$ neće uspeti. Na osnovu Teoreme 10 i Teoreme 11 važi $g \in \sqrt{\langle h_1, h_2, \ldots, h_8\rangle}$ ako i samo ako $1 \in \langle h_1, h_2, \ldots, h_8, 1-yg\rangle$ u prstenu polinoma $\mathbb{R}[u_1, u_2, x_1, \ldots, x_8]$. Međutim, kada izračunamo redukovanu bazu ovog ideala, možemo zaključiti da nismo dobili $\{1\}$ i test pripadnosti radikalu ne uspeva. Novu promenljivu y preimenovaćemo u n.

```
> ring r = 0, (a,b,x,y,z,u,v,w,s,t,n), lp;
> poly h1 = 2x - a;
> poly h2 = 2y - b;
> poly h3 = 2z - a;
> poly h4 = 2u - b;
> poly h5 = -av + bw;
> poly h6 = bv - ab + aw;
> poly h7 = (s-x)^2 + t2 - (s-z)^2 - (t-u)^2;
> poly h8 = (s-x)^2 + t2 - s2 - (t-y)^2;
> poly g = (s-v)^2 + (t-w)^2 - (s-x)^2 - t2;
> ideal I1 = h1, h2, h3, h4, h5, h6, h7, h8, 1 - n*g;
> ideal G1 = groebner(I1);
```

```
> G1;
G1[1]=v2n-2vsn+w2n-2wtn-1
G1[2]=u
G1[3]=z
G1[4]=y-u
G1[5]=x-z
G1[6]=b-2u
G1[7]=a-2z
```

Primetimo da kao redukovanu bazu ideala nismo dobili $\{1\}$.

Probajmo sada da isključimo razmatranje degenerisanih slučajeva i da koeficijente polinoma koje razmatramo vidimo kao racionalne izraze u terminima promenljivih u_1 *i* u_2. *Podsetimo se da vrednosti* u_i *predstavljaju vrednosti koje su nezavisne od ostalih i one treba da budu različite od nula ako želimo da isključimo degenerisane slučajeve. Stoga izračunavanja možemo da vršimo u prstenu polinoma* $\mathbb{R}(u_1, u_2)[x_1, x_2, \ldots, x_8]$. *Proverimo najpre da li polinom* g *pripada idealu* $\langle h_1, h_2, \ldots, h_8\rangle$ *u prstenu polinoma* $K(u_1, u_2)[x_1, \ldots, x_8]$. *Ovo možemo proveriti računanjem ostatka pri deljenju polinoma* g *polinomima Greberove baze ideala* $\langle h_1, h_2, \ldots, h_8\rangle$.

```
> ring r = (0,a,b), (x,y,z,u,v,w,s,t), lp;
> poly h1 = 2x - a;
> poly h2 = 2y - b;
> poly h3 = 2z - a;
> poly h4 = 2u - b;
> poly h5 = -av + bw;
> poly h6 = bv - ab + aw;
> poly h7 = (s-x)^2 + t2 - (s-z)^2 - (t-u)^2
> poly h8 = (s-x)^2 + t2 - s2 - (t-y)^2;
> ideal I = h1, h2, h3, h4, h5, h6, h7, h8;
> ideal G = groebner(I);
G;
G[1]=(4b)*t+(-b2)
G[2]=(4a)*s+(-4b)*t+(-a2+b2)
G[3]=(a2+b2)*w+(-a2b)
G[4]=(b)*v+(a)*w+(-ab)
G[5]=2*u+(-b)
G[6]=2*z+(-a)
G[7]=2*y+(-b)
G[8]=2*x+(-a)
> poly g = (s-v)^2 + (t-w)^2 - (s-x)^2 - t2;
> reduce(g,G);
0
```

Primetimo da je prvi polinom Grebnerove baze samo po promenljivim t, *drugi polinom je po promenljivim* t *i* s, *i slično.*

Isto tvrđenje možemo proveriti i na drugi način. Generisaćemo ideal nad skupom *polinoma $h_1, h_2, \ldots, h_8, 1 - gy$ u prstenu polinoma $K(u_1, u_2)[x_1, \ldots, x_8, y]$ i proveriti da li je njegova redukovana Grebnerova baza jednaka $\{1\}$.*

```
> ring r = (0,a,b), (x,y,z,u,v,w,s,t,n), lp;
> poly h1 = 2x - a;
> poly h2 = 2y - b;
> poly h3 = 2z - a;
> poly h4 = 2u - b;
> poly h5 = -av + bw;
> poly h6 = bv - ab + aw;
> poly h7 = (s-x)^2 + t2 - (s-z)^2 - (t-u)^2;
> poly h8 = (s-x)^2 + t2 - s2 - (t-y)^2;
> poly g = (s-v)^2 + (t-w)^2 - (s-x)^2 - t2;
> ideal I = h1, h2, h3, h4, h5, h6, h7, h8, 1 - n*g;
> option(redSB);
> ideal G = groebner(I);
> G;
G[1]=1
```

S obzirom na to da kao redukovanu Grebnerovu bazu dobijamo $\{1\}$ zaključujemo da tvrđenje važi ako isključimo degenerisane slučajeve.

Procedura dokazivanja geometrijskih tvrđenja korišćenjem metode Grebnerovih baza se sastoji iz narednih koraka:

1. skicirati geometrijske objekte na koje se referiše u teoremi i detektovati sve relevantne tačke koje se javljaju u geometrijskom problemu koji rešavamo;
2. značajnim tačkama dodeliti koordinate tako da:
   - vrednosti u_i predstavljaju koordinate tačaka koje su nezavisne od pozicija ostalih tačaka na slici,
   - vrednosti x_i predstavljaju koordinate tačaka koje zavise od pozicija ostalih tačaka na slici;
3. zapisati hipoteze $h_1, h_2, \ldots, h_m$ i zaključak (zaključke) g tvrđenja u vidu polinoma nad promenljivim u_i i x_i;
4. proveriti da li polinom g pripada radikalu ideala $\langle h_1, h_2, \ldots, h_m \rangle$ testiranjem da li je konstanta $\{1\}$ redukovana Grebnerova baza ideala $\langle h_1, h_2, \ldots, h_m, 1 - yg \rangle$ u prstenu polinoma $K[u_1, \ldots, u_l, x_1, \ldots, x_n, y]$, gde je sa y označena nova promenljiva:
   (a) ako ovo važi, onda na osnovu Teoreme sledi da zaključak g sledi striktno iz hipoteza $h_1, h_2, \ldots, h_m$;
   (b) ako ne važi, onda nezavisne promenljive u_i pridružujemo polju koeficijenata i testiramo da li je redukovana Grebnerova baza ideala $\langle h_1, h_2, \ldots, h_m, 1 - yg \rangle$ u prstenu polinoma $K(u_1, u_2, \ldots, u_l)[x_1, x_2, \ldots, x_n]$ jednaka $\{1\}$. Ako ovo važi onda na osnovu Teoreme zaključak g sledi uopšteno iz hipoteza $h_1, h_2, \ldots, h_m$.

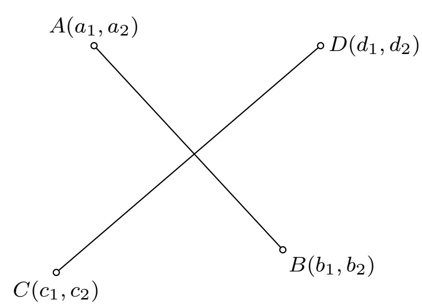
Važan korak prilikom dokazivanja teorema na ovaj način čini prelaz sa pitanja da li se polinom g poništava na afinom varijetetu ideala I generisanog polinomima $h_1, h_2, \ldots, h_m$ na pitanje da li polinom g pripada radikalu ideala I. Ovo je moguće samo u afinim varijetetima koji su definisani na algebarski zatvorenim poljima. Stoga, na primer, nije moguće testirati odlučivost geometrijskog tvrđenja u polju realnih brojeva, već samo u polju kompleksnih brojeva. Međutim, s obzirom na to da je tvrđenje koje razmatramo univerzalno kvantifikovano, tačnost tvrđenja u odnosu na kompleksne brojeve povlači i tačnost tvrđenja u odnosu na realne brojeve. Ako bi se, u suprotnom, pokazalo da tvrđenje nije tačno u polju kompleksnih brojeva, nikakva odluka o tačnosti tvrđenja u polju realnih brojeva se ne bi mogla doneti. Dakle, teoreme u polju realnih brojeva se na ovaj način mogu samo dokazati, ali se ne mogu opovrgnuti.

5.3 Algebrizacija osnovnih geometrijskih tvrđenja

Pri radu sa geometrijskim teoremama neki od osnovnih predikata sa kojim manipulišemo su paralelnost pravih, upravnost pravih, kolinearnost tačaka i dr. Razmotrimo na koji način je moguće u vidu jednog ili većeg broja polinoma formulisati osnovna geometrijska tvrđenja.

Upravnost duži Neka su koordinate tačaka A, B, C i D redom jednake $A(a_1, a_2)$, $B(b_1, b_2)$, $C(c_1, c_2)$ i $D(d_1, d_2)$. Uslov da je duž AB upravna na duž CD (slika 5.4) može se zapisati u vidu uslova da je skalarni proizvod vektora $\overrightarrow{AB}(b_1 - a_1, b_2 - a_2)$ i $\overrightarrow{CD}(d_1 - c_1, d_2 - c_2)$ jednak 0.

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



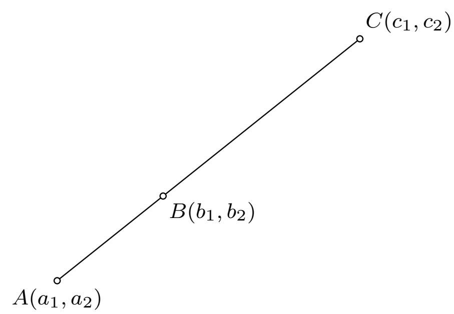
Slika 5.4: Ilustracija kada su duži AB i CD međusobno upravne.

Do istog uslova smo mogli doći i na osnovu toga da za koeficijente pravaca k_1 i k_2 pravih AB i CD važi: $k_1 \cdot k_2 = -1$:

$$\begin{aligned} \frac{b_2 - a_2}{b_1 - a_1} \cdot \frac{d_2 - c_2}{d_1 - c_1} &= -1 \\ (b_1 - a_1)(d_1 - c_1) + (b_2 - a_2)(d_2 - c_2) &= 0 \end{aligned}$$

Kolinearnost tačaka Uslov da su tačke $A(a_1, a_2)$, $B(b_1, b_2)$ i $C(c_1, c_2)$ kolinearne (slika 5.5) možemo zadati izjednačavanjem koeficijenata pravaca pravih AC i BC:

$$\begin{aligned} \frac{c_2 - a_2}{c_1 - a_1} &= \frac{c_2 - b_2}{c_1 - b_1} \\ h &= (c_2 - a_2)(c_1 - b_1) - (c_2 - b_2)(c_1 - a_1) = 0 \end{aligned}$$



Slika 5.5: Slučaj kada su tačke A, B i C kolinearne.

Ovo odgovara interpretaciji da je površina trougla ABC jednaka 0.

Pripadnost krugu Uslov da tačka $B(b_1, b_2)$ pripada krugu sa središtem $O(o_1, o_2)$ koji prolazi kroz tačku $A(a_1, a_2)$ (slika 5.6) može se zadati izjednačavanjem rastojanja tačaka A i B od središta kruga O.

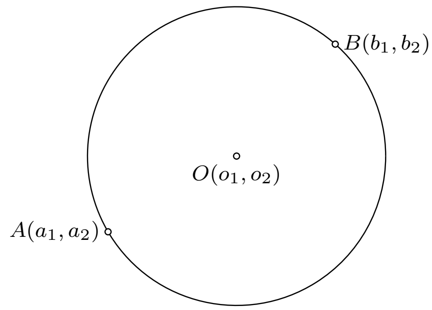
$$\begin{aligned} |OB|^2 &= |OA|^2 \\ (b_2 - o_2)^2 + (b_1 - o_1)^2 &= (a_2 - o_2)^2 + (a_1 - o_1)^2 \\ h &= (b_2 - o_2)^2 + (b_1 - o_1)^2 - (a_2 - o_2)^2 - (a_1 - o_1)^2 = 0 \end{aligned}$$

Središte duži Neka je tačka $M(m_1, m_2)$ središte duži AB, pri čemu važi $A(a_1, a_2)$ i $B(b_1, b_2)$ (slika 5.7). Odatle sledi da je x koordinata tačke M jednaka aritmetičkoj sredini x koordinata tačaka A i B.

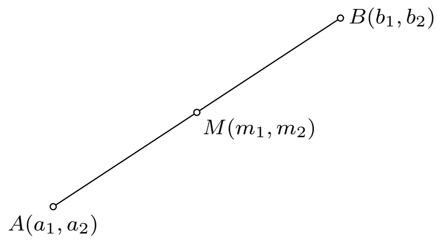
$$\begin{aligned} m_1 &= \frac{a_1 + b_1}{2} \\ 2m_1 &= a_1 + b_1 \\ h_1 &= 2m_1 - a_1 - b_1 = 0 \end{aligned}$$

Analogno važi i za y koordinatu tačke M:

$$\begin{aligned} m_2 &= \frac{a_2 + b_2}{2} \\ 2m_2 &= a_2 + b_2 \\ h_2 &= 2m_2 - a_2 - b_2 = 0 \end{aligned}$$



Slika 5.6: Slučaj kada tačka B pripada krugu $c(O, A)$ sa središtem O koji sadrži tačku A.



Slika 5.7: Tačka M je središte duži AB.

Primer za vežbu 20. *Formulisati u vidu polinoma uslov:*

- *paralelnosti duži AB i CD,*
- *da tačka X pripada duži AB i deli duž AB u odnosu $2 : 1$,*
- *da je duž AB tangentna na krug $c(O, C)$ sa središtem O koji prolazi kroz tačku C,*
- *da su krugovi $c(O_1, A)$ i $c(O_2, B)$ tangentni.*

Primer za vežbu 21. *Dokazati da se dijagonale paralelograma seku u tački koja polovi obe dijagonale.*

Primer za vežbu 22. *Dokazati da se težišne linije trougla seku u jednoj tački.*

Primer za vežbu 23. *Dokazati da se visine trougla seku u jednoj tački.*

Primer za vežbu 24. *Dokazati da su centar opisanog kruga, težište i ortocentar trougla kolinearne tačke.*

5.4 Identifikovanje uslova nedegenerisanosti

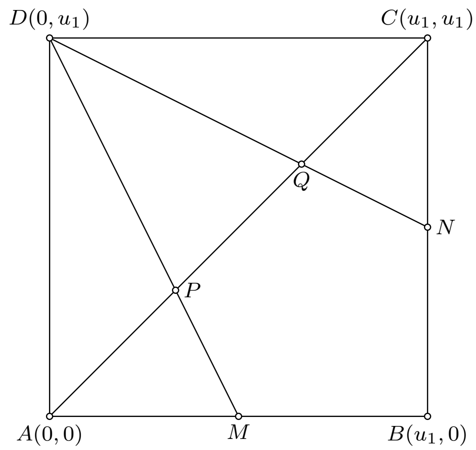
Geometrijska tvrđenja često nisu sasvim precizna, već prave neke implicitne pretpostavke o geometrijskim figurama čija se svojstva dokazuju. Dešava se da je geometrijska teorema tačna samo ako važe neki dodatni uslovi (uslovi nedegenerisanosti). U ovom slučaju kažemo da zaključak tvrđenja koje dokazujemo sledi uopšteno iz skupa hipoteza (eng. generically true). Degenerisani slučajevi najčešće odgovaraju situaciji kada su neke dve polazne tačke identične ili kada su neke tri polazne tačke kolinearne. Automatske procedure za dokazivanje geometrijskih tvrđenja moraju da budu u stanju da se izbore sa ovom vrstom problema, odnosno da automatski nađu odgovarajuće uslove nedegenerisanosti (i to što jednostavnije moguće) koji čine tvrđenje tačnim, ako oni uopšte postoje. Kao i za hipotezu i zaključak tvrđenja koje dokazujemo, da bismo mogli da odredimo te dodatne uslove neophodno je da se taj dodatni uslov može izraziti u terminima polinoma i to u vidu (jedne ili više) nejednakosti oblika $s(x_1, x_2, \ldots, x_n) \neq 0$. Dakle, potrebno je ispitati tačnost tvrđenja:

$$(\forall x \in \overline{K}^n)(h_1(x) = \ldots = h_m(x) = 0 \wedge s(x) \neq 0 \Rightarrow g(x) = 0)$$

Često kada se javi degenerisanost, to je zato što jednačina koja je zavisna samo od jednog u_i važi na afinom varijetetu, što je problematično jer su vrednosti u_i nezavisne promenljive. Pokazuje se da kada kao jedan od polinoma redukovane Grebnerove baze dobijemo polinom g koji se može formulisati u vidu proizvoda polinoma p i q pri čemu je polinom p formulisan samo u terminima nezavisnih promenljivih u_i, onda nam situacije kada je vrednost polinoma p jednaka 0 daju potencijalne degenerisane slučajeve.

Primer 52. *Dokazati da dve prave koje prolaze kroz isto teme kvadrata i središta suprotnih strana seku naspramnu dijagonalu kvadrata na tri jednaka dela (slika 5.8).*

Označimo temena kvadrata redom sa A, B, C i D i bez narušavanja opštosti dodelimo im koordinate $A(0,0)$, $B(u_1, 0)$, $D(0, u_1)$, $C(u_1, u_1)$. Središte stranice AB označimo sa M, središte stranice BC sa N, a preseke dijagonale AC sa dužima DM i DN redom sa



Slika 5.8: Ilustracija tvrđenja o podeli dijagonale kvadrata na tri jednaka dela.

P i Q. Dodelimo koordinate ovim tačkama uzimajući u obzir da tačke sa dijagonale AC imaju istu x i y koordinatu: $M(u_1/2, 0)$, $N(u_1, u_1/2)$, $P(x_1, x_1)$, $Q(x_2, x_2)$.

Tačke D, P i M su kolinearne, odakle sledi prva hipoteza:

$$\begin{aligned} k_{DP} &= k_{MP} \\ \frac{x_1 - u_1}{x_1} &= \frac{x_1}{x_1 - u_1/2} \\ x_1^2 &= (x_1 - u_1)(x_1 - u_1/2) \\ h_1 &= u_1^2 - 3u_1x_1 = 0 \end{aligned}$$

Tačke D, Q i N su kolinearne, odakle sledi druga hipoteza:

$$\begin{aligned} k_{DQ} &= k_{NQ} \\ \frac{x_2 - u_1}{x_2} &= \frac{x_2 - u_1/2}{x_2 - u_1} \\ (x_2 - u_1)^2 &= x_2(x_2 - u_1/2) \\ h_2 &= 2u_1^2 - 3u_1x_2 = 0 \end{aligned}$$

Potrebno je dokazati da važi $|AP| = |PQ|$ i $|PQ| = |QC|$. Dakle, treba pokazati tačnost tvrđenja:

$$\begin{aligned} 2x_1^2 &= 2(x_2 - x_1)^2 \\ g_1 &= x_1^2 - (x_2 - x_1)^2 = 0 \end{aligned}$$

i, slično, tvrđenja:

$$\begin{aligned} 2(x_2 - x_1)^2 &= 2(x_2 - u_1)^2 \\ g_2 &= (x_2 - x_1)^2 - (x_2 - u_1)^2 = 0 \end{aligned}$$

Praktična vežba 26. *Razmotrimo prsten polinoma $\mathbb{R}[u_1, x_1, x_2]$, pri čemu ćemo promenljivoj u_1 pridružiti oznaku u, a promenljivim x_1 i x_2 oznake x i y. Dodatnu promenljivu, potrebnu za ispitivanje pripadnosti radikalu, nazvaćemo z.*

```
> ring r = 0, (u,x,y,z), lp;
> poly h1 = u2 - 3ux;
> poly h2 = 2u2 - 3uy;
> poly g1 = x2 - (y-x)*(y-x);
> ideal I1 = h1, h2, 1 - z*g1;
> ideal G1 = groebner(I1);
> G1;
G1[1]=2xyz-y2z-1
G1[2]=u
> poly g2 = (y-x)^2 - (y-u)^2;
> ideal I2 = h1, h2, 1 - z*g2;
> ideal G2 = groebner(I2);
> G2;
G2[1]=x2z-2xyz+1
G2[2]=u
```

Primetimo da kao redukovanu Grebnerovu bazu ideala ne dobijamo $\{1\}$, te tvrđenje ne sledi striktno. Šta više, iz redukovane Grebnerove baze možemo zaključiti da se degenerisani slučaj dešava kada je $u_1 = 0$ i tada se sva temena polaznog kvadrata poklapaju.

Pokušajmo da tvrđenje dokažemo isključujući degenerisane slučajeve. Stoga ćemo izračunavanja izvršavati u prstenu polinoma $\mathbb{R}(u_1)[x_1, x_2]$. Najpre računamo Grebnerovu bazu $B = \{b_1, b_2\}$ ideala $\langle h_1, h_2\rangle$, a zatim računamo Grebnerovu bazu ideala $\langle b_1, b_2, 1-yg_1\rangle$ i, analogno, Grebnerovu bazu ideala $\langle b_1, b_2, 1 - yg_2\rangle$.

Primetimo da je u Singularu potrebno u situaciji kada je u oznaka parametra iz $\mathbb{R}$, a ne promenljiva, a x promenljiva, term polinoma nužno zadati kao ux, a ne kao xu.

```
> ring r = (0,u), (x,y,z), lp;
> poly h1 = u2 - 3ux;
> poly h2 = 2u2 - 3uy;
> poly g1 = x2 - (y-x)*(y-x);
> poly g2 = (y-x)^2 - (y-u)^2;
> ideal I = h1, h2;
> ideal B = groebner(I);
> B;
```

```
B[1]=3*y+(-2u)
B[2]=3*x+(-u)
> ideal I1 = B[1], B[2], 1 - z*g1;
> ideal G1 = groebner(I1);
> G1;
G1[1]=1
> ideal I2 = B[1], B[2], 1 - z*g2;
> ideal G2 = groebner(I2);
> G2;
G2[1]=1
```

Kao redukovanu Grebnerovu bazu oba ideala I_1 i I_2 dobijamo $\{1\}$ te dato tvrđenje važi do na uslove degenerisanosti.

Uslovi nedegenerisanosti generisani algebarskim metodama su dati u algebarskim terminima. U kontekstu dokazivanja teorema u geometriji, važan i ne tako lako problem jeste formulisanje njihovih interpretacija sa jasnim geometrijskim značenjem. Kada se uslovi nedegenerisanosti formulišu u formi geometrijskih pretpostavki (što često nije nimalo lako), dobija se konačni oblik geometrijske teoreme, koji isključuje neke degenerisane slučajeve za koje polazno tvrđenje nije tačno. Primetimo da je nekada moguće da je tvrđenje tačno i pod nekim slabijim dodatnim pretpostavkama. Dodatno, tvrđenje nekada može biti tačno i kada uslovi nedegenerisanosti nisu zadovoljeni.

5.5 Dokazivanje ispravnosti rešenja konstruktivnih problema u geometriji

U ovom poglavlju razmotrićemo primenu Grebnerovih baza na dokazivanje ispravnosti rešenja konstruktivnih problema u geometriji. Za formalno zadavanje konstrukcija, njihovu vizuelizaciju i dokazivanje metodom Grebnerovih baza koristićemo alat GCLC.

5.5.1 GCLC

GCLC je alat za vizuelizaciju geometrije koji omogućava generisanje digitalnih matematičkih ilustracija visokog kvaliteta i može biti od pomoći prilikom učenja geometrije[2]. Naime, pored vizuelizacije geometrijskih figura, on raspolaže i automatskim dokazivačima teorema i to:

- dokazivačem teorema zasnovanim na metodi površina (eng. area method),
- dokazivačem teorema zasnovanim na Vuovoj metodi i
- dokazivačem teorema zasnovanim na metodi Grebnerovih baza

[2] Alat GCLC dostupan je sa adrese `http://poincare.matf.bg.ac.rs/~janicic/gclc/`.

U alatu GCLC se matematičke figure zadaju korišćenjem jezika GCLC, bliskog LaTeX formatu. Razmotrimo neke osnovne primitivne konstrukcije i neke osnovne naredbe u alatu GCLC. Trougao ABC čije su koordinate $A(15, 10)$, $B(50, 10)$ i $C(40, 35)$ možemo zadati i iscrtati na sledeći način.

```
point A 15 10
point B 50 10
point C 40 35
cmark_lb A
cmark_rb B
cmark_rb C
drawsegment A B
drawsegment B C
drawsegment C A
```

Naime, naredbom `point P x y` zadaje se tačka P sa koordinatama x i y, dok se naredbama `cmark_lb` i `cmark_rb` odgovarajuća tačka označava svojim imenom i to kad je sufiks naredbe `lb` levo-dole (eng. left-bottom), a kad je sufiks `rb` desno-dole (eng. right-bottom) u odnosu na poziciju tačke. Naredbom `drawsegment P Q` duž PQ se iscrtava.
Pravu a kroz tačke B i C možemo konstruisati i iscrtati narednim kodom:

```
line a B C
drawline a
```

Tačku M_a kao središte duži BC možemo konstruisati i označiti na sledeći način:

```
midpoint M_a B C
cmark_b M_a
```

Pravu m_a kroz tačku M_a upravnu na pravu a (drugim rečima medijatrisu duži BC) možemo konstruisati i iscrtati narednim kodom:

```
perp m_a M_a a
drawline m_a
```

Presečnu tačku M'_a pravih a i m_a možemo konstruisati i označiti narednim kodom:

```
intersec M_a' a m_a
cmark_b M_a'
```

Tačku M_b za koju važi $\overrightarrow{AM_b} = 0.5 \cdot \overrightarrow{AC}$ možemo konstruisati i označiti sledećim kodom:

```
towards M_b A C 0.5
cmark_b M_b
```

Geometrijsko tvrđenje možemo probati da dokažemo nekim od raspoloživih dokazivača teorema korišćenjem naredbe `prove {tvrdjenje}`. Na primer, tvrđenje da se prethodno definisane tačke M_a i M_a' poklapaju možemo formulisati na sledeći način:

```
prove { identical M_a M_a' }
```

Pritom je naravno potrebno izabrati metodu dokazivanja koju želimo da koristimo. Ako izaberemo metodu Grebnerovih baza, ovo tvrđenje se uspešno dokazuje.

Neki od predikata koji se mogu naći unutar naredbe `prove` su `identical`, `midpoint`, `collinear`, `perpendicular`, `collinear`[3].

5.5.2 Konstruktivni problemi u geometriji

Problemi konstrukcije trougla su problemi u kojima je potrebno uz pomoć lenjira i šestara konstruisati trougao koji zadovoljava dati skup ograničenja (najčešće tri). Naime, zadatak konstruktivnih problema je da se za datu deklarativnu specifikaciju geometrijske figure odredi odgovarajuća, po mogućstvu ekvivalentna, proceduralna specifikacija zasnovana na raspoloživim konstruktivnim koracima. Dakle, konstrukcija nije slika, već procedura kojom se na osnovu zadatih primitivnih konstrukcija daje uputstvo kako konstruisati traženi objekat.

Formalno, pod konstrukcijom pomoću lenjira i šestara se podrazumeva niz elementarnih konstruktivnih koraka, tako da je svaki od njih iz narednog skupa koraka:

- konstrukcija proizvoljne tačke,
- konstrukcija prave (pomoću lenjira) kroz dve date tačke,
- konstrukcija kruga (pomoću šestara) sa središtem u nekoj zadatoj tački kroz neku drugu zadatu tačku,

[3] Kompletno upustvo za korišćenje alata GCLC dostupno je na adresi `http://poincare.matf.bg.ac.rs/~janicic/gclc/gclc_man.pdf`

- konstrukcija preseka (ukoliko postoji) dve prave, dva kruga ili prave i kruga.

Ipak, tradicionalno se prilikom opisivanja geometrijskih konstrukcija kao primitivni koraci razmatraju i tzv. složeni konstruktivni koraci koji se sastoje iz više elementarnih koraka, kao što su konstrukcija središta duži, normale na datu pravu kroz datu tačku, prave paralelne sa datom pravom kroz datu tačku i sl.

Glavnu poteškoću prilikom rešavanja konstruktivnih problema, i za čoveka i za računar, predstavlja kombinatorna eksplozija uslovljena ogromnim prostorom pretrage: naime, postoji veliki broj primitivnih koraka i svaki od njih se može primeniti na veliki broj načina, i broj načina na koji se mogu primeniti raste kako konstrukcija napreduje.

Tradicionalno, rešenje konstruktivnog problema se sastoji od četiri faze:

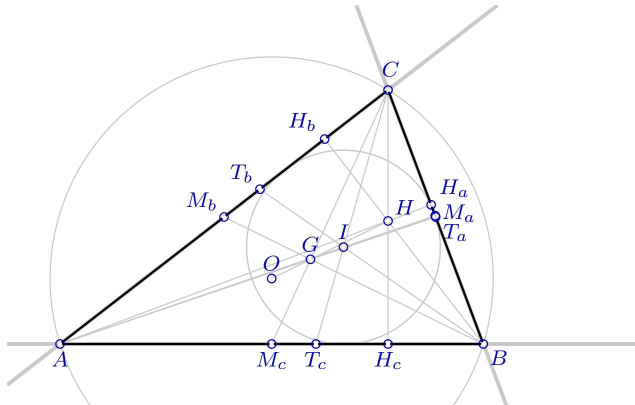
- analize – u kojoj se kreće od pretpostavke da geometrijski objekti zadovoljavaju specifikaciju problema, a onda se dokazuje da važe neka svojstva koja omogućavaju konstrukciju,
- konstrukcije – u kojoj se na osnovu analize formuliše konstrukcija pomoću lenjira i šestara,
- dokaza – u ovoj fazi se dokazuje da generisana konstrukcija (pomoću lenjira i šestara) zadovoljava specifikaciju problema,
- diskusije – u kojoj se razmatra koliko problem ima rešenja i pod kojim uslovima ona postoje.

Vernikov korpus predstavlja jedan od značajnih korpusa konstruktivnih problema. On sadrži spisak lokacijskih problema konstrukcije trougla kod kojih je zadatak konstruisati trougao ABC ako su poznate lokacije neke tri značajne tačke trougla od narednih 16 (slika 5.9):

- temena trougla A, B i C, središte opisanog kruga O,
- središta stranica trougla M_a, M_b i M_c, težište T,
- podnožja visina H_a, H_b i H_c, ortocentar H,
- preseci bisektrisa unutrašnjih uglova sa naspramnim stranicama trougla T_a, T_b i T_c i središte upisanog kruga I.

Vernikov korpus sadrži ukupno $\binom{16}{3} = 560$ instanci problema; za neke probleme je dokazano da su rešivi, za neke da su redundantni (da je na osnovu neke dve date tačke moguće konstruisati treću), za neke da su zavisni od položaja (da je lokacija jedne od zadatih tačaka uslovljena položajem druge dve tačke), a za neke da se ne mogu rešiti uz pomoć lenjira i šestara[4].

[4]Status svih problema iz Vernikovog korpusa dat je na adresi `http://hydra.nat.uni-magdeburg.de/wernick/`.



Slika 5.9: Značajne tačke Vernikovog korpusa.

5.5.3 Automatsko rešavanje konstruktivnih problema

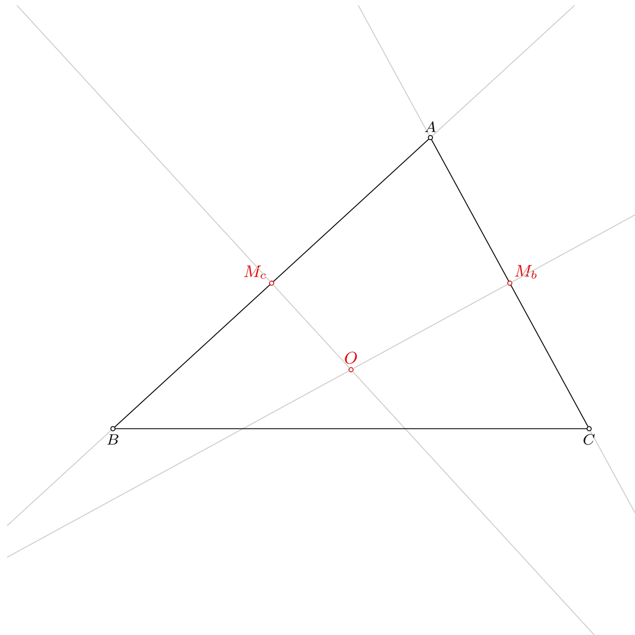
Uprkos dugoj tradiciji rešavanja konstruktivnih zadataka uz pomoć lenjira i šestara, njihovo automatsko rešavanje se malo pominje u literaturi i postoji tek nekoliko alata za njihovo rešavanje. Jedan od takvih sistema je i ArgoTriCS koji predstavlja alat za automatsko rešavanje konstruktivnih problema u geometriji, koji je u stanju da reši veliki broj problema iz Vernikovog korpusa[5]. On se zasniva na geometrijskom znanju identifikovanom kao potrebno za rešavanje ovih problema, a koje je razvrstano na skup definicija, skup lema i skup primitivnih konstrukcija. Neke od raspoloživih primitivnih konstrukcija su:

- konstrukcija prave kroz dve tačke,
- konstrukcija kruga sa središtem u jednoj tački kroz drugu tačku,
- konstrukcija presečnih tačaka dve prave, prave i kruga, i dva kruga,
- konstrukcija prave kroz datu tačku upravne na drugu datu pravu,
- konstrukcija prave kroz datu tačku paralelne sa drugom datom pravom,
- konstrukcija tačke Y za koju važi $\overrightarrow{XY}/\overrightarrow{XZ} = k$, gde su tačke X i Z date, a k je neki racionalni broj.

ArgoTriCS kao izlaz automatski generiše neformalni opis konstrukcije na prirodnom jeziku (poput onih u udžbenicima), formalni opis konstrukcije u jeziku GCLC uz generisanje odgovarajuće ilustracije, dokaz ispravnosti konstrukcije i uslove kada rešenje postoji.

Dokazivanje ispravnosti konstrukcije se svodi na dokazivanje da ako se objekti konstruišu na dati način, onda oni zadovoljavaju specifikaciju problema. ArgoTriCS za dokazivanje ispravnosti generisanih konstrukcija koristi dokazivač OpenGeoProver i dokazivače implementirane u okviru alata GCLC. Tvrđenje koje se dokazuje jeste da su tačke koje

[5] Zbirka rešenih problema iz Vernikove liste dostupna je na adresi `http://poincare.matf.bg.ac.rs/~vesnap/animations/compendium_wernick.html`.



Slika 5.10: Ilustracija konstrukcije trougla ABC ako su data središta dve stranice M_b i M_c i središte opisanog kruga O.

su zadate postavkom problema zaista odgovarajuće tačke konstruisanog trougla ABC. Na primer, ako je cilj konstruisati trougao ABC ako su zadati središte M_b stranice AC, središte M_c stranice AB i središte opisanog kruga O, onda je cilj pokazati da su tačke M_b, M_c i O zaista odgovarajuće značajne tačke konstruisanog trougla ABC. Da bismo to pokazali koristimo definicije značajnih tačaka trougla.

Primer 53. *Razmotrimo problem konstrukcije trougla ABC ako su dati središte opisanog kruga O, tačka M_b koja predstavlja središte stranice AC i tačka M_c koja predstavlja središte stranice AB.*

Konstrukcija na prirodnom jeziku automatski generisana korišćenjem alata ArgoTriCS glasi[6]*:*

1. *Konstruisati pravu m_b kroz tačke O i M_b;*
2. *Konstruisati pravu m_c kroz tačke O i M_c;*
3. *Konstruisati pravu b kao pravu koja prolazi kroz tačku M_b i upravna je na pravu m_b;*
4. *Konstruisati pravu c kao pravu koja prolazi kroz tačku M_c i upravna je na pravu m_c;*
5. *Konstruisati presečnu tačku A pravih b i c;*

6. *Konstruisati tačku* C *za koju važi* $\overrightarrow{AC}/\overrightarrow{AM_b} = 2$;

7. *Konstruisati tačku* B *za koju važi* $\overrightarrow{M_cB}/\overrightarrow{M_cA} = -1$.

Ilustracija odgovarajuće konstrukcije prikazana je na slici 5.10.

Odgovarajući automatski generisani formalni opis konstrukcije u jeziku GCLC glasi:

```
point O 65 51.14
point M_{b} 95 67.5
point M_{c} 50 67.5

cmark_t O
cmark_rt M_{b}
cmark_lt M_{c}

% Constructing a line m_{b} passing through point O and point M_{b}
line m_{b} O M_{b}
drawline m_{b}

% Constructing a line m_{c} passing through point O and point M_{c}
line m_{c} O M_{c}
drawline m_{c}

% Constructing a line b which is perpendicular to line m_{b}
% and which passes through point M_{b}
perp b M_{b} m_{b}
drawline b

% Constructing a line c which is perpendicular to line m_{c}
% and which passes through point M_{c}
perp c M_{c} m_{c}
drawline c

% Constructing a point A which belongs to line c and line b
intersec A c b
cmark_t A

% Constructing a point C such that AC/AM_{b}=2
towards C A M_{b} 2
cmark_b C

% Constructing a point B such that M_{c}B/M_{c}A=-1
towards B M_{c} A -1
cmark_b B

drawsegment A B
```

```
drawsegment A C
drawsegment B C

% Proving constuctions correct

% Defining significant points of constructed triangle ABC
line c' A B
line b' A C
midpoint M_{b}' A C
midpoint M_{c}' A B
perp m_{c}' M_{c}' c
perp m_{b}' M_{b}' b
intersec O' m_{b}' m_{c}'

% prove {identical M_{b} M_{b}'}
prove {identical M_{c} M_{c}'}
% prove {identical O O'}
```

Sva tri tvrđenja moguće je dokazati korišćenjem dokazivača zasnovanog na metodi Grebnerovih baza implementiranih u okviru alata GCLC. Generisani dokazi dostupni su na adresama:

- `https://github.com/milanbankovic/symbolic_computing/blob/main/Grebnerove_baze/konstrukcija_trougla_proof1.pdf`,
- `https://github.com/milanbankovic/symbolic_computing/blob/main/Grebnerove_baze/konstrukcija_trougla_proof2.pdf` *i*
- `https://github.com/milanbankovic/symbolic_computing/blob/main/Grebnerove_baze/konstrukcija_trougla_proof3.pdf`.

U generisanim dokazima možemo uvideti na koji način su tačkama pridružene koordinate, kako su prevedena neka geometrijska tvrđenja, kao i korak po korak izvršavanje Buhbergerovog algoritma za konstrukciju Grebnerove baze.

Bibliografija

[1] F. Winkler, Groebner basis in geometry theorem proving and simplest degeneracy conditions, Mathematica Pannonica, pp. 15-32, 1990.

[2] I. Eser, Automated geometry theorem proving, Master Thesis, 2011.

[3] K. Rivas, Geometric theorem proving using the Groebner basis algorithm, Theses Digitization Project, 3531, 2009.

[4] M. Mencinger, On Groebner Bases and Their Use in Solving Some Practical Problems, Universal Journal of Computational Mathematics 1(1): 5-14, 2013.

[5] D. A. Cox et al, Ideals, Varieties, and Algorithms, Undergraduate Texts in Mathematics, Springer International Publishing Switzerland, 2015.

[6] R. Ablamowitz, Some applications of Groebner bases in robotics and engineering, Tennesse Technological University, 2008.

[7] M. Steglehner, Flexible solutions of polynomial systems and their applications in robotics, Master thesis, JKU Linz, 2014.

[8] B. Buchberger, M. Kauers, Scholarpedia, 5(10):7763, 2010, `http://www.scholarpedia.org/article/Groebner_basis`

[9] B. Buchberger, Groebner Bases and Applications, Cambridge University Press, 1998.

[10] K.O.Geddes, S.R.Czapor, G.Labahn, Algorithms for Computer Algebra, Kluwer Academic Publishers, 1992.

[11] L.Redman, Algebraic Methods for Proving Geometric Theorems, Electronic Theses, Projects, and Dissertations, 2019.

[12] K. Madlener, Automatic Geometric Theorem Proving using Groebner Bases, Bachelor's Thesis, 2008.