GRÖBNERJEVE BAZE IN REŠEVANJE SISTEMOV NELINEARNIH POLINOMSKIH ENAČB

BRIGITA FERČEC[1,2], MATEJ MENCINGER[3,4]

[1]Center za uporabno matematiko in teoretično fiziko, Univerza v Mariboru
[2]Fakulteta za energetiko, Univerza v Mariboru
[3]Fakulteta za gradbeništvo, prometno inženirstvo in arhitekturo
Univerza v Mariboru
[4]Inštitut za matematiko, fiziko in mehaniko, Ljubljana

Math. Subj. Class. (2010): 13A15, 13B25, 68N30

Obravnavamo Gröbnerjeve baze, ki so pomemben teoretični gradnik moderne teorije polinomskih kolobarjev. Razložimo pomen multideljenja, S-polinoma in Buchbergerjevega algoritma. Opišemo reševanje nekaterih problemov, ki se nanašajo na ideale v polinomskih kolobarjih in se osredotočimo na uporabo pri reševanju sistemov polinomskih enačb ter problemu implicitizacije.

GRÖBNER BASES AND SOLVING NONLINAR POLYNOMIAL SYSTEMS

Gröbner bases, which are an important building block of modern theory of polynomial ring theory, are considered. The meaning of the multidivision, S-polynomial and Buchberger's algorithm is explained. The use of Gröbner bases in some theoretical aspects concerning the ideals in polynomial rings is considered. We are interested in the use of solving polynomial systems and implicitization problem.

Uvod

V grobem lahko rečemo, da uporabo Gröbnerjevih baz najdemo povsod, kjer nastopijo polinomski ideali oz. polinomske enačbe. Torej ne le v matematiki, temveč tudi v številnih drugih vedah – nekaterih inženirskih problemih, kot je na primer robotika [3, pogl. 6]. V matematiki Gröbnerjeve baze nastopijo pri odgovoru na vprašanje, ali je neki polinom element danega ideala, pri problemu enakosti idealov, izračunu preseka dveh ali več idealov in podobno (glej npr. [3, 9]). Teorijo Gröbnerjevih baz je leta 1965 vpeljal Bruno Buchberger [2]. Na teorijo lahko gledamo s stališča posplošitve Evklidovega algoritma, pa tudi kot na posplošitev Gaussove eliminacije linearnega sistema, katere rezultat je (zgornje-) trikotna oblika linearnega sistema. Teorija Gröbnerjevih baz omogoča računanje (deljenje) v kolobarju polinomov več spremenljivk, ki je analogno računanju (deljenju) v polinomskih kolobarjih ene spremenljivke.

Pogosto moramo v praksi rešiti sistem polinomskih enačb (več spremenljivk)

$$f_1(x,y,z) = 0,\ f_2(x,y,z) = 0,\ f_3(x,y,z) = 0 \tag{1}$$

ali pa imamo podano ploskev ali krivuljo v parametrični obliki

$$x = f_1(u,v),\ y = f_2(u,v),\ z = f_3(u,v);\ u,v \in \mathbb{R} \tag{2}$$

ali

$$x = f_1(t),\ y = f_2(t),\ z = f_3(t);\ t \in \mathbb{R} \tag{3}$$

ali

$$x = f_1(t),\ y = f_2(t);\ t \in \mathbb{R} \tag{4}$$

in želimo zapisati pripadajočo enačbo (enačbi) v implicitni obliki. Poglejmo si dva konkretna motivacijska primera:

Primer 1. a) $x = t^5,\ y = t^2+1,\ z = t^3-1.$

b) $x = \frac{u+v}{u-v},\ y = 2\frac{v^2+u^2}{(u-v)^2},\ z = 2v\frac{v^2+3u^2}{(u-v)^3}.$

c) $x = u+v,\ y = 2uv+v^2,\ z = 3uv^2+v^3.$

Začnimo s primerom c). Če želimo iz enačb eliminirati parametra u in v, hitro opazimo, da zaradi nelinearnosti naloga ni tako preprosta, kot npr. pri linearnem primeru

$$x = 1+2u-v,\ y = u+v,\ z = 2-u+3v.$$

Čeprav lahko poskusimo s podobno »strategijo« in iz prvih dveh enačb nekako izrazimo parametra u in v (z x in y) in rezultata vstavimo v tretjo enačbo ter jo preoblikujemo tako, da le-ta ne vsebuje več nobenih korenov – nam po dolgem računanju celo uspe dobiti implicitno enačbo ploskve c):

$$4x^3z + 4y^3 - 3x^2y^2 - 6xyz + z^2 = 0.$$

V nadaljevanju tega članka želimo ugotoviti, ali lahko zgornjo enačbo dobimo z metodo, podobno Gaussovi eliminaciji, oz. z neke vrste metodo nasprotnih koeficientov.

Nadaljujmo s krivuljo a), kjer nastopajo t^5, t^2 in t^3. Spodnja računa ne potrebujeta dodatnih pojasnil, saj sta precej očitna: $t^{5\cdot 2} = x^2$ in $t^{2\cdot 5} = (y-1)^5$, zato je $(y-1)^5 - x^2 = 0$ in $t^{5\cdot 3} = x^3$, $(z+1)^5 = t^{3\cdot 5}$, zato je $(z+1)^5 - x^3 = 0$. Tako dobljeni enačbi zagotovo pomenita implicitno enačbo krivulje a), ki pa verjetno ni »najboljša možna« v smislu največje potence spremenljivk, ki v implicitnih enačbah nastopajo. Hitro lahko preverimo, da je ena od možnosti tudi $y^3 - 3y^2 + 3y - z^2 - 2z - 2 = 0$ in $yz + y - z - x - 1 = 0$ (z najvišjo potenco 3).

Nazadnje poglejmo še točko b):

$$x = \frac{u+v}{u-v},\ y = 2\frac{v^2+u^2}{(u-v)^2},\ z = 2v\frac{v^2+3u^2}{(u-v)^3}.$$

Hitro lahko preverimo, da z uvedbo nove spremenljivke $t = \frac{u+v}{u-v}$ enačbe b) postanejo »enoparametrične«: $x = t$, $y = t^2 + 1$, $z = t^3 - 1$, kar pomeni, da imamo za neskončno različnih vrednosti u in v isto vrednost t; torej se pri implicitizaciji lahko pojavi »problem inverza«, ki algebrsko pomeni problem neodvisnosti parametrov u in v (podrobnosti najdete v [6]).

Zgoraj naštete probleme uspešno reši teorija Gröbnerjevih baz, ki npr. polinomom $x - t^5, y - t^2 - 1, z - t^3 + 1$ priredi polinome $-2 + 3y - 3y^2 + y^3 - 2z - z^2, 1 + x - y + z - yz, -1 + t + 2y - y^2 + tz, -1 - t + ty - z, 1 + t^2 - y$, ki predstavljajo njihovo Gröbnerjevo bazo. Če bi bili eliminacijski problemi iz primera 1 linearni, bi bil rang razširjene matrike pripadajočega sistema manjši od števila neznank v sistemu. Če za linearni sistem velja, da sta ranga (pripadajoče) matrike sistema in razširjene matrike sistema enaka številu neznank, je rešitev enolična.

V nadaljevanju bomo videli, da je edina ustrezna posplošitev Gaussove eliminacije za nelinearne polinomske sisteme iskanje Gröbnerjeve baze sistemu pripadajočega ideala (polinomov sistema). Iz »novega« eliminacijskega postopka mora biti na koncu tudi razvidno, ali je rešitev v obliki izoliranih točk, ali pa so rešitve krivulje, ploskve (tj. kakšna raznoterost pripada sistemu enačb). Osnovna ideja pri reševanju sistema (1) temelji na tako imenovanih S-polinomih in spominja na (srednješolsko) metodo nasprotnih koeficientov, zato ni presenetljivo, da pri tej teoriji postane pomembno tako imenovano »multideljenje« (posplošitev deljenja polinomov ene spremenljivke), kjer želimo polinom $f(x_1, \ldots, x_n)$ deliti z več polinomi $p_1(x_1, \ldots, x_n), \ldots, p_k(x_1, \ldots, x_n)$. Kot bomo videli, dobimo pri takem deljenju ustrezne koeficiente $q_1(x_1, \ldots, x_n), \ldots, q_k(x_1, \ldots, x_n)$ ter (enoličen) ostanek $r(x_1, \ldots, x_n)$

$$f = q_1 p_1 + \cdots + q_k p_k + r,$$

kar bo podrobneje opisano v naslednjem poglavju.

Primer 2. Motivacijo končajmo z dvema sistemoma oblike (1):

(A) $f_1 = -xy^3 - y^2 z + yz^2 + \mathbf{2}xz^3$, $f_2 = z^2 + xy + z$, $f_3 = y^2 + xz + y$;

(B) $g_1 = -xy^3 - y^2 z + yz^2 + \mathbf{1}xz^3$, $f_2 = z^2 + xy + z$, $f_3 = y^2 + xz + y$.

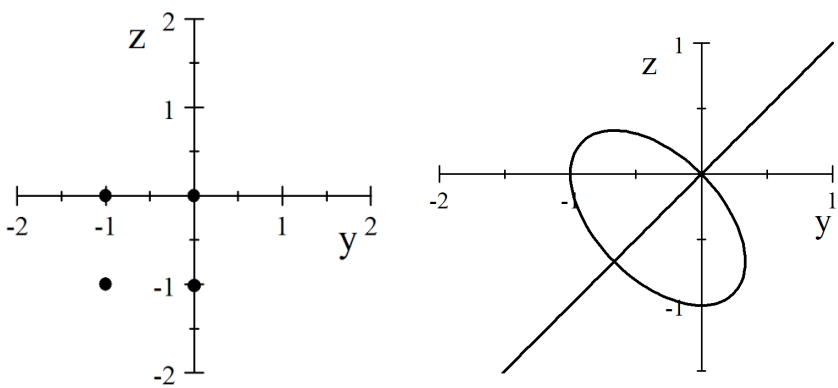
Po eni strani (npr. po videzu) sta si sistema (A) in (B) zelo podobna, saj se razlikujeta le v enem koeficientu (prikazan z debelejšo pisavo). Po drugi strani pa sta sistema (A) in (B) bistveno različna, saj ima sistem (A) končno mnogo rešitev (rešitve so izolirane) za z, medtem ko ima sistem (B) za z neizolirane rešitve (jih je neskončno mnogo). Za zdaj povejmo, da razlog za to tiči v tem, da je $g_1 = -y^2 f_2 + z^2 f_3$, čemur v nadaljevanju pravimo, da

je g_1 v idealu, ki ga tvorita f_2 in f_3, oziroma da se deljenje polinoma g_1 z množico $\{f_2, f_3\}$ »izide«, medtem ko za f_1 velja

$$f_1 = -y^2 f_2 + z^2 f_3 + xz^3,$$

čemur v nadaljevanju pravimo, da f_1 ni element ideala, ki ga tvorita f_2 in f_3, oziroma da se deljenje polinoma f_1 z množico $\{f_2, f_3\}$ »ne izide« (ostanek $r = xz^3$ je neničeln). Oboje lahko enostavno preverimo. Na koncu »izdajmo«, da je Gröbnerjeva baza množice polinomov $\{f_1, f_2, f_3\}$ (kar bomo definirali kasneje), če damo spremenljivki x »večji pomen« kot spremenljivki y in obema »večji pomen« kot spremenljivki z, enaka $G_A = \{z^4 + z^5, z^3 + yz^3 + z^4 + yz^4, yz^2 + y^2z^2, y^2 + y^3 - z^2 - z^3, y + y^2 + xz, xy + z + z^2\}$, medtem ko je Gröebnerjeva baza množice polinomov $\{g_1, f_2, f_3\}$ enaka $G_B = \{y^2 + y^3 - z^2 - z^3, y + y^2 + xz, xy + z + z^2\}$. Če za zdaj na Gröbnerjevo bazo pogledamo kot na preoblikovanje sistema $f_1 = 0, f_2 = 0, f_3 = 0$ tako, da vedno ohranimo množico rešitev sistema, je očitno, da ima sistem (A) glede na neznanko z izolirane (realne) rešitve $z_{1,2,3,4} = 0$ in $z_5 = -1$ (kot sledi iz prve enačbe $z^4 + z^5 = 0$), medtem ko ima sistem (B) rešitve na krivulji $\widetilde{y}^2 + \widetilde{y}^3 - \widetilde{z}^2 - \widetilde{z}^3 = 0$ (glej sliko 1b), torej so rešitve oblike $\left(-\frac{\widetilde{y}+\widetilde{y}^2}{\widetilde{z}}, \widetilde{y}, \widetilde{z}\right)$, če je $\widetilde{z} \neq 0$, ter $(\widetilde{x}, 0, 0)$ oziroma $(0, -1, 0)$ sicer. Na sliki 1a so v (y, z)-ravnini prikazane rešitve sistema (A); hitro lahko preverimo, da rešitev sestavljajo izolirane točke $(0, -1, 0)$, $(0, -1, -1)$, $(0, 0, -1)$ ter premica $(x, 0, 0)$.

Osnovna ideja Gröbnerjevih baz je posplošiti korak v klasičnem algoritmu Gaussove eliminacije, kjer npr. par polinomov $f = 5x + 2y - z - 1$ in $g = 3x + 4y - 2z - 2$ zamenjamo z ekvivalentnim parom polinomov $f = 5x + 2y - z - 1$ in $S_{f,g} = 7z - 14y + 7$. Če koeficiente monomov



(a) Rešitev sistema (A). **(b)** Rešitev sistema (B).

Slika 1. Primer 2: rešitve projicirane na ravnino $x = 0$.

polinomov f in g zapišemo v prvo vrstico matrike, dobimo matriko

$$\begin{pmatrix} 5 & 2 & -1 & -1 \\ 3 & 4 & -2 & -2 \end{pmatrix},$$

kjer sta v prvem stolpcu matrike koeficienta pred spremenljivko x, v drugem stolpcu sta koeficienta pred spremenljivko y, v tretjem stolpcu sta koeficienta pred spremenljivko z, v četrtem stolpcu pa stojita prosta člena obeh polinomov. Sedaj s pomočjo Gaussove metode (nasprotni koeficienti) eliminiramo spremenljivko x v drugem polinomu, in sicer pomnožimo prvo vrstico matrike s 3 in drugo z -5 ter obe vrstici seštejemo, da dobimo

$$\begin{pmatrix} 5 & 2 & -1 & -1 \\ 0 & -14 & 7 & 7 \end{pmatrix}.$$

Poudarimo, da smo zadnjo vrstico dobili z metodo nasprotnih koeficientov:

$$S_{f,g} = \frac{15}{5}(5x + 2y - z - 1) - \frac{15}{3}(3x + 4y - 2z - 2) = -14y + 7y + 7.$$

V nadaljevanju tega poglavja bomo podali nekaj definicij, ki pomagajo razumeti pomen Gröbnerjevih baz. Več podrobnosti in splošnejši pristop najdete na primer v [3, 9]. Obravnavajmo polinome f spremenljivk $x_1, \ldots, x_n$ s koeficienti iz polja k:

$$f = \sum_{\alpha \in S} a_\alpha x_1^{\alpha_1} \cdots x_n^{\alpha_n},$$

kjer je S končna podmnožica množice $\mathbb{N}_0^n$ in $\alpha = (\alpha_1, \ldots, \alpha_n)$. Pravimo, da je $x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ *monom*, $a_\alpha \in k \setminus \{0\}$ *koeficient* in $a_\alpha x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ *člen* polinoma. Množico vseh polinomov spremenljivk $x_1, \ldots, x_n$ s koeficienti iz k označimo s $k[x_1, \ldots, x_n]$. Z operacijama seštevanje in množenje polinomov je $k[x_1, \ldots, x_n]$ komutativen kolobar. Nadalje rečemo, da je $|\alpha| = \alpha_1 + \cdots + \alpha_n$ *stopnja monoma* ter $\mathrm{st}(f) = \max\{|\alpha| : \alpha \in S\}$ stopnja polinoma. Za vsako naravno število n je $k^n = \{(a_1, \ldots, a_n) : a_1, \ldots, a_n \in k\}$ *afin prostor* dimenzije n. Množica polinomov $f_1, \ldots, f_s$ je naravno povezana s sistemom enačb $f_1(x_1, \ldots, x_n) = 0, f_2(x_1, \ldots, x_n) = 0, \ldots, f_s(x_1, \ldots, x_n) = 0$, kar zapišemo krajše:

$$\vec{f}(\vec{x}) = \vec{0}. \tag{5}$$

Množica vseh rešitev sistema (5) je definirana kot *afina raznoterost*, določena s polinomi $f_1, \ldots, f_s$:

$$\mathbf{V}(f_1, \ldots, f_s) = \{(a_1, \ldots, a_n) \in k^n : f_j(a_1, \ldots, a_n) = 0 \text{ za } 1 \le j \le s\}.$$

Ideal v $k[x_1, \ldots, x_n]$ je podmnožica I kolobarja $k[x_1, \ldots, x_n]$, ki zadošča naslednjima pogojema:

(i) če sta $f, g \in I$, potem je $f + g \in I$ in

(ii) če je $f \in I$ in $h \in k[x_1, \ldots, x_n]$, je $hf \in I$.

Kot najpreprostejši primer ideala v $k[x_1, \ldots, x_n]$ vzemimo množico vseh možnih linearnih kombinacij, ki lahko nastanejo iz polinomov $f_1, \ldots, f_s$:

$$\langle f_1, \ldots, f_s \rangle = \left\{ \sum_{j=1}^{s} h_j f_j : h_1, \ldots, h_s \in k[x_1, \ldots, x_n] \right\}.$$

Ta množica je ideal, ki mu pravimo *ideal, generiran s polinomi* $f_1, \ldots, f_s$. Če je ideal $I \subset k[x_1, \ldots, x_n]$ generiran s končno mnogo elementi $f_1, \ldots, f_s$, pravimo, da je I *končno generiran ideal.* Potem je $I = \langle f_1, \ldots, f_s \rangle$ in množica $\{f_1, \ldots, f_s\}$ se imenuje *baza* ideala I. Na primer, baza ideala $\langle f_1, f_2, f_3 \rangle$ iz primera 2 (A) je $\{f_2, f_3\}$, baza ideala $\langle g_1, f_2, f_3 \rangle$ iz primera 2 (B) pa je $\{g_1, f_2, f_3\}$. Po izreku o Hilbertovi bazi (glej npr. [3, str. 74: Theorem 4]) je vsak polinomski ideal v kolobarju $k[x_1, \ldots, x_n]$ končno generiran. Ekvivalentno, vsaka naraščajoča veriga idealov $I_1 \subset I_2 \subset I_3 \subset \cdots$ v $k[x_1, \ldots, x_n]$ se ustali [9, str. 4: Corollary 1.1.7], kar pomeni, da obstaja takšen $m \geq 1$, da je $I_j = I_m$ za vsak $j > m$.

Algebraična geometrija, ki obravnava zveze med algebro (ideali) in geometrijo (afine raznoterosti), je zelo obširna (glej npr. [3, 9]). Glavno vlogo pri tem imata »naravni« preslikavi, $\mathbf{V}$ ($\mathbf{I}$), med množicama vseh afinih raznoterosti $\mathbb{V}$ in vseh idealov $\mathbb{I}$ ter radikal ideala.

Preslikava $\mathbf{I} : \mathbb{V} \to \mathbb{I}$ je definirana z

$$\mathbf{I}(V) = \{f \in k[x_1, \ldots, x_n] : f(a_1, \ldots, a_n) = 0 \text{ za vse } (a_1, \ldots, a_n) \in V\}. \tag{6}$$

Preslikava $\mathbf{V} : \mathbb{I} \to \mathbb{V}$ je definirana z

$$\langle f_1, \ldots, f_k \rangle \longmapsto \mathbf{V}(f_1, \ldots, f_k), \tag{7}$$

kjer je $\mathbf{V}(f_1, \ldots, f_k)$ tako imenovana ničelna množica polinomov $f_1, \ldots, f_k$ (torej rešitev sistema $f_1 = 0, \ldots, f_k = 0$).

Radikal ideala I, ki ga označimo s $\sqrt{I}$, je definiran takole:

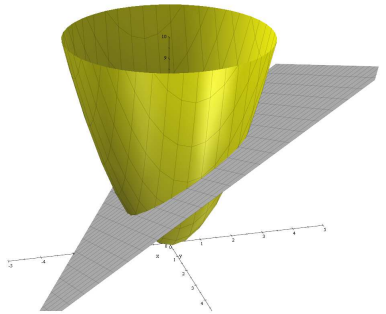
$$\sqrt{I} = \{f \in k[x_1, \ldots, x_n] : \text{obstaja tak } p \in \mathbb{N}, \text{ da je } f^p \in I\}.$$

Ideal $I \subset k[x_1, \ldots, x_n]$ je *radikalni ideal*, če je enak svojemu radikalu:

$$I = \sqrt{I}.$$

Zvezo med algebro in geometrijo si bomo ogledali na primeru vsote in produkta idealov, ki imata tu zanimivo in pomembno vlogo, ki sledi iz formul za raznoterost vsote in produkta idealov:

$$\mathbf{V}(I + J) = \mathbf{V}(I) \cap \mathbf{V}(J), \tag{8}$$



Slika 2. Ploskvi $\mathbf{V}(I)$ in $\mathbf{V}(J)$ iz primera 3.

$$\mathbf{V}(I \cdot J) = \mathbf{V}(I) \cup \mathbf{V}(J). \tag{9}$$

Vsota, $I + J$, idealov I in J je ideal, definiran z vsemi možnimi vsotami elementov iz obeh idealov:

$$I + J := \{f + g : f \in I, g \in J\},$$

produkt, $I \cdot J$, idealov I in J je ideal, definiran z (vsemi) vsotami produktov, kjer nastopajo faktorji iz obeh idealov:

$$I \cdot J := \{f_1 g_1 + \cdots + f_r g_r : f_1, \ldots, f_r \in I, g_1, \ldots, g_r \in J, r \in \mathbb{N}\}.$$

Če sta $I = \langle f_1, \ldots, f_k \rangle$ in $J = \langle g_1, \ldots, g_s \rangle$, sta vsota $I + J$ in produkt $I \cdot J$ generirana tako (glej npr. [3, str. 181–183])

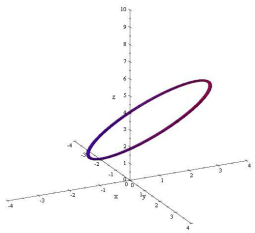
$$\begin{aligned} I + J &= \langle f_1, \ldots, f_k, g_1, \ldots, g_s \rangle \text{ in} \\ I \cdot J &= \langle f_i g_j : 1 \le i \le k, 1 \le j \le s \rangle, \end{aligned}$$

torej je $\langle f_1 \rangle + \cdots + \langle f_k \rangle = \langle f_1, \ldots, f_k \rangle$. Geometrijska pomena enačb (8) in (9) si oglejmo na enostavnih primerih.

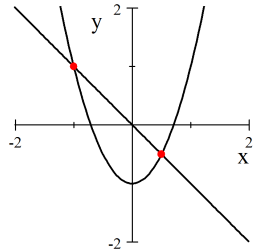
Primer 3. Naj bosta $I = \langle x + 2y + 6 - 2z \rangle$ in $J = \langle x^2 + y^2 - z \rangle$ ideala v $\mathbb{R}[x, y, z]$. Tedaj je $I + J = \langle x + 2y + 6 - 2z, x^2 + y^2 - z \rangle$ in $\mathbf{V}(I + J) = \mathbf{V}(I) \cap \mathbf{V}(J)$, kot je prikazano na slikah 2 in 3.

Primer 4. Naj bosta $I = \left\langle (x + y)^2, 2x^2 - y - 1 \right\rangle$ in $J = \langle x + y, x^3 + 2y \rangle$ ideala v $\mathbb{R}[x, y]$. Tedaj je

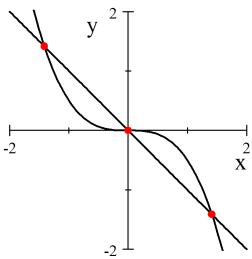
$$I \cdot J = \left\langle (x+y)^3, (x+y)^2\Big(x^3 + 2y\Big), \Big(2x^2 - y - 1\Big)(x+y), \Big(2x^2 - y - 1\Big)\Big(x^3 + 2y\Big) \right\rangle$$



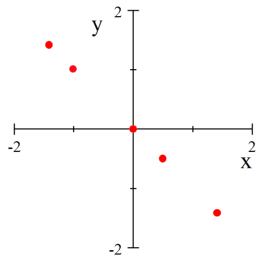
Slika 3. Presek ploskev $\mathbf{V}(I)$ in $\mathbf{V}(J)$ iz primera 3.



Slika 4. Raznoterost $\mathbf{V}(I)$ iz primera 4 (dve točki).



Slika 5. Raznoterost $\mathbf{V}(J)$ iz primera 4 (tri točke).



Slika 6. Raznoterost $\mathbf{V}(I \cdot J)$ iz primera 4 (pet točk).

in

$$\mathbf{V}\left(I \cdot J\right) = \mathbf{V}\left(I\right) \cup \mathbf{V}\left(J\right),$$

kar je prikazano na slikah 4, 5 in 6. **Opomba:** Raznoterost $\mathbf{V}\left(I \cdot J\right)$ je določena z $x + y = 0$ in $\left(2x^2 - y - 1\right)\left(x^3 + 2y\right) = 0$, kar nam da pet točk na sliki 6.

V nadaljevanju opozorimo na pomen preslikav (6) in (7). Vemo, da vsaka raznoterost V določa neki ideal $\mathbf{I}(V)$ in vsak ideal I določa neko raznoterost $\mathbf{V}\left(I\right)$. Če velja $\mathbf{I}\left(V_1\right) = \mathbf{I}\left(V_2\right)$, je nujno $V_1 = V_2$, toda če je $\mathbf{V}\left(I_1\right) = \mathbf{V}\left(I_2\right)$, ni nujno, da je $I_1 = I_2$. Najpreprostejši tak par je $I_1 = \langle x \rangle$ in $I_2 = \langle x^2 \rangle$. Tudi za $f_1 = x^2 - y^2$ in $f_2 = (x-y)^2(x+y)$ velja $I_1 = \langle f_1 \rangle$, $I_2 = \langle f_2 \rangle$ in $I_1 \neq I_2$, toda $\mathbf{V}\left(I_1\right) = \mathbf{V}\left(I_2\right)$. Iz enakosti raznoterosti pa sledi, da sta pripadajoča radikala enaka, $\sqrt{I_1} = \sqrt{I_2}$. O tem govori tako imenovani Hilbertov Nullstellensatz [3, str. 170–171].

Izrek 1 (Krepki Hilbertov Nullstellensatz). *Naj bo $\mathbb{A}^n$ afin prostor nad algebraično zaprtim poljem k in naj bo I ideal v $k\left[x_1, \ldots, x_n\right]$. Tedaj za vsak ideal $I \in k\left[x_1, \ldots, x_n\right]$ velja*

$$\mathbf{I}\left(\mathbf{V}\left(I\right)\right) = \sqrt{I}.$$

V nadaljevanju želimo natančno definirati Gröbnerjevo bazo in s tem povezano (že omenjeno) »multideljenje«. Zato najprej definirajmo *monomsko ureditev*, $<$, v $k[x_1, \ldots, x_n]$ kot relacijo dobre ureditve $<$ v množici $\mathbb{N}_0^n$ z naslednjima dvema lastnostma:

(i) vsaka neprazna podmnožica monomov ima najmanjši element in

(ii) če velja $x^\alpha < x^\beta$, potem velja $x^\alpha x^\gamma < x^\beta x^\gamma$ za vsak monom x^γ.

Najbolj običajna in splošno znana monomska ureditev je *leksikografska ureditev*: obravnavajmo monome $x_1^2x_2^8x_3^{50}$, $x_1^3x_2^2x_3^5$, $x_1^2x_2^9x_3^4 \in \mathbb{R}[x_1, x_2, x_3]$ in recimo, da je x_1 »pomembnejši« od x_2 (in x_3) in da je x_2 »pomembnejši« kot x_3. Potem je

$$x_1^3x_2^2x_3^5 > x_1^2x_2^9x_3^4 > x_1^2x_2^8x_3^{50}.$$

Splošno je $x^\alpha < x^\beta$ natanko tedaj, ko prvi koordinati α_i in β_i od leve proti desni v α in β, ki sta različni, zadoščata $\alpha_i < \beta_i$. Obstaja še veliko drugih monomskih ureditev: inverzna leksikografska, stopenjsko inverzna leksikografska itd. (glej npr. [3, 9]). Če imamo opravka z več različnimi ureditvami, lahko poudarimo ime monomske ureditve. Na primer, leksikografsko ureditev označimo z $<_{lex}$.

Ko je monomska ureditev izbrana, lahko govorimo o *vodilnem monomu* (LM), *vodilnem členu* (LT) in *vodilnem koeficientu* (LC) polinoma. Vodilni člen je definiran kot največji monom (glede na izbrano ureditev). Na primer, če je $f = -x_1^2x_2^8x_3^{50} + 2x_1^3x_2^2x_3^5 + 3x_1^2x_2^9x_3^4$ in je ureditev leksikografska, je vodilni člen polinoma f enak $LT(f) = 2x_1^3x_2^2x_3^5$, medtem ko je njegov vodilni koeficient enak $LC(f) = 2$, vodilni monom pa je $LM(f) = x_1^3x_2^2x_3^5$.

Omenimo tudi, da poljuben vektor $\vec{c} \in \mathbb{R}^n$ določa monomsko ureditev $<_{\vec{c}}$ v $\mathbb{R}[x_1, x_2, \ldots, x_n]$ na naslednji način:

$$x^\alpha < x^\beta \Leftrightarrow \begin{cases} \vec{c}\alpha < \vec{c}\beta & \text{ali} \\ \vec{c}\alpha = \vec{c}\beta & \text{in} \quad \alpha <_{lex} \beta, \end{cases}$$

kjer $\vec{c}\alpha$ označuje standardni skalarni produkt vektorjev, $\vec{c}\alpha = \sum_i c_i\alpha_i$. Monomsko ureditev $<_{\vec{c}}$, definirano z vektorjem $\vec{c}$, imenujemo *utežena monomska ureditev*. Na primer, če je $\vec{c} = (2, 3, 20)$, je $x_1^8x_2^1x_3^2 <_{\vec{c}} x_1^1x_2^1x_3^3$, saj je $\vec{c}\alpha = (2, 3, 20) \cdot (8, 1, 2) = 59$ in $\vec{c}\beta = (2, 3, 20) \cdot (1, 1, 3) = 65$. Opazimo, da je glede na ureditev $<_{\vec{c}}$ vodilni člen polinoma $g = 7x_1^8x_2^1x_3^2 - 8x_1^1x_2^1x_3^3$ enak $LT(g) = -8x_1^1x_2^1x_3^3$, medtem ko je vodilni člen $LT(g)$ glede na $<_{lex}$ enak $7x_1^8x_2^1x_3^2$.

Ko sta kolobar in monomska ureditev izbrana, lahko delimo polinom s polinomom ali celo z (urejeno) množico polinomov, kar lahko imenujemo tudi »multideljenje«. Posplošitev procesa Gaussove eliminacije za reševanje sistema (5) namreč zahteva deljenje polinoma z množico polinomov. Dobro poznane elementarne vrstične operacije Gaussove eliminacije temeljijo na

dejstvu, da na vsakem koraku, j, Gaussove eliminacije za $\vec{f}(\vec{x}) = \vec{0}$ množica rešitev spremenjenega sistema ostane enaka množici rešitev začetnega sistema. Spomnimo se primera: v smislu oznake $\vec{f_j}(\vec{x}) = \vec{0}$ je bil začetni sistem

$$f_0 = 5x + 2y - z - 1,$$
$$g_0 = 3x + 4y - 2z - 2.$$

Nadomestili smo ga s $f_1 = f_0$ in $g_1 = S_{f,g} = 7z - 14y + 7$. Opazimo, da je $g_1 = 3f_0 - 5g_0$, kar pomeni, da iz $f_0(\widetilde{x}, \widetilde{y}) = 0$ in $g_0(\widetilde{x}, \widetilde{y}) = 0$ (za neki par $(\widetilde{x}, \widetilde{y})$), sledi enakost $g_1(\widetilde{x}, \widetilde{y}) = 0$ (za isti par $(\widetilde{x}, \widetilde{y})$). Osnovna ideja je, da lahko zamenjamo začetni par f_0, g_0 s f_1, g_1 in sta oba polinoma f_1 in g_1 »deljiva« z množico začetnih polinomov f_0, g_0:

$$f_1 = 1f_0 + 0g_0 \quad \text{in} \quad g_1 = 3f_0 - 5g_0.$$

Kot bomo videli v naslednjem poglavju (glej tudi [3]), deljenje polinomov z množico polinomov (v smislu zgornjih enakosti) vodi k definiciji Gröbnerjevih baz.

Deljenje polinomov z množico polinomov

Polinom $f \in k[x_1, \ldots, x_n]$ želimo deliti z množico polinomov $f_1, \ldots, f_n \in k[x_1, \ldots, x_n]$, pri čemer želimo proces in sam smisel deljenja »ohraniti« čim bolj podoben tistemu pri deljenju polinomov ene spremenljivke. Začnimo s primerom:

Primer 5. Naj bo $f_1 = XY + Y$, $f_2 = X^2 + Y$ in $f = X^2Y + XY^2$ in izberimo leksikografsko ureditev $X > Y$. Če f delimo z urejeno množico (f_1, f_2), pričakujemo rezultat oblike $f = q_1f_1 + q_2f_2 + r$.

Zapis sheme multideljenja je skladen s shemo multideljenja v [9, str. 14]. Oznaka $\sqrt{f}$ pomeni, da je f polinom, ki ga delimo z množico polinomov (f_1 in f_2).

Oba vodilna člena $LT(f_1) = XY$ in $LT(f_2) = X^2$ delita vodilni člen $LT(f) = X^2Y$. Toda ker je v urejeni množici (f_1, f_2), s katero delimo, najprej naveden f_1, delimo X^2Y z XY in dobimo X, ki ga zapišemo h kvocientu q_1. Nato pomnožimo X s f_1 in rezultat podpišemo pod polinom f, od katerega slednjega tudi odštejemo. Dobimo polinom $XY^2 - XY$, katerega vodilni člen delimo z $LT(f_1)$ in dobimo Y, ki ga pripišemo h q_1. Postopek ponovimo in nov polinom, ki ga delimo z $LT(f_1)$ ali $LT(f_2)$, je $-XY - Y^2$. Njegov vodilni člen je prav tako deljiv z $LT(f_1)$: faktor -1 pripišemo h q_1. Na koncu dobimo polinom $-Y^2 + Y$, katerega vodilni člen ni več deljiv niti z $LT(f_1)$ niti z $LT(f_2)$, zato vodilni člen $-Y^2$ pripišemo v

desni stolpec kot ostanek in ostane polinom Y, ki ga pa prav tako pripišemo k ostanku. Nazadnje h q_2 pripišemo 0 in polinom $-Y^2+Y$ je (končni) ostanek, r, pri tem multideljenju. Celotna shema multideljenja je taka:

$$\begin{array}{rl}
q_1: & X+Y-1 \\
q_2: & 0 \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \underline{r\quad} \\
f_1: XY+Y & \sqrt{X^2Y+XY^2} \\
f_2: X^2+Y & \underline{X^2Y+XY} \\
 & \quad \underline{XY^2-XY} \\
 & \qquad XY^2-XY \\
 & \qquad \underline{XY^2+Y^2} \\
 & \qquad\quad -XY-Y^2 \\
 & \qquad\quad \underline{-XY-Y} \\
 & \qquad\qquad -Y^2+Y \\
 & \qquad\qquad \underline{Y} \quad \to \quad -Y^2 \\
 & \qquad\qquad 0 \quad \to \quad -Y^2+Y,
\end{array}$$

kar pomeni

$$f=(X+Y-1)f_1+0f_2-Y^2+Y.$$

Po drugi strani, če zamenjamo »vrstni red« polinomov f_1 in f_2, torej če delimo z urejeno množico (f_2,f_1), s podobnim izračunom kot zgoraj dobimo

$$f=Yf_1+Yf_2-2Y^2.$$

Očitno je rezultat tovrstnega deljenja zelo odvisen od vrstnega reda polinomov, s katerimi delimo, saj lahko sprememba vrstnega reda spremeni tako vrednosti kvocientov q_1,q_2 kot tudi vrednost ostanka r. Ko delimo polinom f z množico polinomov $F=(f_1,f_2)$, lahko pišemo $f=\{\{q_1,q_2\},r\}$ namesto $f=q_1f_1+q_2f_2+r$. Z uporabo teh simbolov lahko prvi primer zapišemo kot $f=\{\{X+Y-1,0\},-Y^2+Y\}$, drugi primer pa pomeni $f=\{\{Y,Y\},-2Y^2\}$. Omenimo še, da je rezultat v osnovi odvisen tudi od izbire ureditve monomov. Če izberemo leksikografsko ureditev $Y>X$, je rezultat deljenja spet drugačen, kar je razvidno iz naslednjega primera, ki ga izvedemo s pomočjo sistema računske algebre `Mathematica`. V programu Mathematica se procedura deljenja polinoma $f(x_1,\ldots,x_k)$ z množico polinomov $\{f_1,\ldots,f_n\}$ (upoštevajoč ureditev $x_1>\ldots>x_k$) izvede z ukazom `PolynomialReduce`$[f,\{f_1,\ldots,f_n\},\{x_1,\ldots,x_k\}]$. Rezultat je oblike $\{\{q_1,\ldots,q_n\},r\}$ in pomeni $f=q_1f_1+q_2f_2+\cdots+q_sf_s+r$. Na primer: `PolynomialReduce`$[X^2Y+XY^2,\{XY+Y,X^2+Y\},\{Y,X\}]$ nam vrne $\{\{-2+2X+Y,2-Y\},-2X^2\}$, kar pomeni $X^2Y+XY^2=(2X+Y-2)\cdot(XY+Y)+(-Y+2)\cdot(X^2+Y)-2X^2$.

Iz primera 5 je razvidno, da lahko smiseln rezultat v zvezi z deljenjem polinoma z množico polinomov podamo samo pri vnaprej izbrani ureditvi in

pri vnaprej izbranem vrstnem redu polinomov v množici, s katero delimo. Multideljenje je smiselno definirati, kot kaže spodnji algoritem, ki je povzet po [9, str. 12].

Preden zapišemo algoritem, zapišimo definicijo reduciranosti ostanka r pri deljenju polinoma z množico polinomov.

Definicija 1. Naj bodo $f, f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$, $f_j \neq 0$ (za $1 \leq j \leq s$) in naj bo $F = \{f_1, \ldots, f_s\}$. Ostanek $r \in k[x_1, \ldots, x_n]$ je reduciran glede na F, če je bodisi $r = 0$ bodisi noben monom, ki nastopi v polinomu r, ni deljiv z nobenim elementom množice $\{LM(f_1), \ldots, LM(f_s)\}$, tj. r ima manjšo stopnjo kot katerikoli polinom $f_1, \ldots, f_s$.

Sedaj si poglejmo algoritem multideljenja. V algoritem vstavimo $f \in k[x_1, \ldots, x_n]$ in urejeno množico $F = (f_1, \ldots, f_s) \in k[x_1, \ldots, x_n] \setminus \{0\}$. Rezultat algoritma so takšni polinomi $q_1, \ldots, q_s, r \in k[x_1, \ldots, x_n]$, da velja:

(i) $f = q_1 f_1 + \cdots + q_s f_s + r$,

(ii) r je reduciran glede na $(f_1, \ldots, f_s)$,

(iii) $\max(LM(q_1) LM(f_1), \ldots, LM(q_s) LM(f_s)) = LM(f)$.

*Algoritem 1 (**Multideljenje**).* Koraki algoritma v psevdokodu:

POSTAVI
$q_1 := 0, \ldots, q_s := 0, h := f$
DOKLER $h \neq 0$ **DELAJ:**
  ČE
  obstaja j tak, da $LM(f_j)$ deli $LM(h)$
  POTEM
  Za najmanjši j, za katerega $LM(f_j)$ deli $LM(h)$:
  $q_j := q_j + \frac{LT(h)}{LT(f_j)}$, $h := h - \frac{LT(h)}{LT(f_j)} f_j$
  SICER
  $r := r + LT(h)$, $h := h - LT(h)$.

Zgornji algoritem je osnova za naslednji izrek, ki je povezan z deljenjem polinoma z množico polinomov.

Izrek 2. *Naj bo podana (urejena) množica polinomov $F = (f_1, \ldots, f_s)$. Naj bo v kolobarju $k[x_1, \ldots, x_n]$ izbrana monomska ureditev $<$. Tedaj lahko vsak polinom $f \in k[x_1, \ldots, x_n]$ zapišemo v obliki*

$$f = q_1 f_1 + \cdots + q_s f_s + r,$$

kjer je r reduciran glede na $F = \{f_1, \ldots, f_s\}$.

Dokaz lahko najdete na primer v [3, str. 62–63]. Če dobimo pri deljenju polinoma f z urejeno množico polinomov F ostanek r, to običajno krajše zapišemo takole:

$$f \xrightarrow{F} r.$$

V nadaljevanju želimo uporabiti algoritem multideljenja za rešitev nekaterih (dobro znanih) teoretičnih problemov teorije polinomskih kolobarjev (kot je na primer problem članstva v idealu in njegovem radikalu). Vemo, da ničeln ostanek pri deljenju polinoma f s polinomi $f_1, \ldots, f_s$ pomeni $f \in I$. Obrat tedaj ne velja (vedno). Četudi ima f pri deljenju s $f_1, \ldots, f_s$ neničeln ostanek, lahko obstaja deljenje polinoma f s polinomi $f_1, \ldots, f_s$ (v drugem vrstnem redu), ki da ostanek 0, saj smo videli, da ostanki (dokler ni izbrana monomska ureditev) niso enolično določeni. Poglejmo primer:

Primer 6. Naj bo $f = x^2y + xy + 2x + 2$, $f_1 = x^2 - 1$ in $f_2 = xy + 2$. Izberimo leksikografsko ureditev $x > y$. Potem z algoritmom multideljenja dobimo

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

Ostanek $r = 2x+y$ je neničeln in tako bi lahko zaključili, da $f \notin \langle f_1, f_2 \rangle$. Če pa spremenimo vrstni red deliteljev f_1 in f_2, imamo $f \xrightarrow{F} 0$ za $F = (f_2, f_1)$, saj je

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

kar pomeni $f \in \langle f_1, f_2 \rangle$.

Kot bomo videli kasneje, lahko težave, ki so nakazane v primeru 6, odpravimo z definicijo Gröbnerjevih baz.

Gröbnerjeve baze in njihova uporaba

Gröbnerjeva baza ideala $\langle f_1, \ldots, f_s \rangle$ je posebna množica $\{g_1, \ldots, g_t\}$, za katero algoritem 1 (multideljenje) iz prejšnjega poglavja za poljuben polinom f vrne ostanek $r = 0$ natanko tedaj, ko je $f \in \langle f_1, \ldots, f_s \rangle$. Natančneje: Gröbnerjeva baza ideala $I \subset k[x_1, \ldots, x_n]$ je končna podmnožica $G = \{g_1, \ldots, g_t\}$ ideala I z lastnostjo

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

Spodnji izrek je splošno znan (glej npr. [3, str. 75]). Poudarimo, da je funkcija LT (in LM) smiselna samo pri izbrani (znani) monomski ureditvi $<$.

Izrek 3. *Vsak neničelni ideal $I \subset k[x_1, \ldots, x_n]$ ima Gröbnerjevo bazo.*

Če je $G = \{g_1, \ldots, g_t\}$ Gröbnerjeva baza ideala I, je očitno ostanek vsakega polinoma $f \in I$ pri multideljenju enoličen. Če je $f = q_1 g_1 + \cdots + q_t g_t + r$ in $f = q_1' g_1 + \cdots + q_t' g_t + r'$, potem je $r - r' = (q_1 - q_1')g_1 + \cdots + (g_t - q_t')g_t \in I$. Če je $r - r' \neq 0$, je $LT(r - r') \in \langle LT(I) \rangle$, kar pomeni, da $LT(g_i)$ deli $LT(r - r')$ za neki i. To je protislovje, saj noben člen ostankov r in r' ni deljiv z $LT(g_i)$ za noben $i = 1, \ldots, t$. Zato je $r = r'$ in $q_i = q_i'$ za vsak $i = 1, \ldots, t$.

Gröbnerjeva baza je tesno povezana s tako imenovanim *S-polinomom* za dan par polinomov $f, g \in k[x_1, \ldots, x_n]$; gre za posplošitev S-polinoma, definiranega v uvodu. Naj bosta $f, g \in k[x_1, \ldots, x_n]$ neničelna polinoma. Najmanjši skupni večkratnik njunih vodilnih monomov naj bo $LCM(LM(f), LM(g)) = x^\gamma$. Potem je S-polinom polinomov f in g definiran kot

$$S_{f,g} = \frac{x^\gamma}{LT(f)} \cdot f - \frac{x^\gamma}{LT(g)} \cdot g.$$

Opazimo, da S-polinomi poskrbijo za eliminacijo vodilnih členov in so v bistvu edini način, da se ta eliminacija zgodi med seštevanjem členov iste stopnje.

Buchbergerjeva osnovna ideja pri definiciji Gröbnerjevih baz je bil naslednji kriterij. Naj bo I ideal. Potem je $G = \{g_1, \ldots, g_t\}$ Gröbnerjeva baza ideala I natanko tedaj, ko je za vsak $i \neq j$ ostanek deljenja polinoma S_{g_i,g_j} z G enak nič:

$$S_{g_i,g_j} \xrightarrow{G} 0.$$

Buchbergerjev algoritem, ki je prikazan v nadaljevanju, je povzet po [9]; prvič je bil opisan v Buchbergerjevi doktorski disertaciji [3]. Algoritem zahteva vnos množice polinomov $\{f_1, \ldots, f_s\} \in k[x_1, \ldots, x_n] \setminus \{0\}$ in vrne Gröbnerjevo bazo G ideala $\langle f_1, \ldots, f_s \rangle$.

*Algoritem 2 (**Buchberger**).* Procedura v psevdokodu je:

POSTAVI
$G := \{f_1, \ldots, f_s\}$.
Korak 1. Za vsak par $g_i, g_j \in G,\ i \neq j$, izračunaj S_{g_i,g_j}
S pomočjo algoritma za multideljenje izračunaj $r_{i,j}$:

$$S_{g_i,g_j} \xrightarrow{G} r_{i,j}$$

ČE
Vsi $r_{i,j} = 0$, izpiši G
SICER
K množici G dodaj vse neničelne $r_{i,j}$ in se **vrni** na Korak 1.

Opomnimo, da imajo vsi najučinkovitejši sistemi računske algebre ukaze (»rutine«) za izračun Gröbnerjevih baz. V sistemu `Mathematica` je ukaz

`GroebnerBasis`. Ker Buchbergerjev algoritem temelji na algoritmu 1, ta pa temelji na monomski ureditvi členov, je izračun Gröbnerjeve baze odvisen od monomske ureditve. (Toda pri izbrani monomski ureditvi je Gröbnerjeva baza enolična.) Poleg `Mathematice` imajo takšne rutine med drugimi še `Singular` in `Maculay2`.

Opazimo, da lahko Buchbergerjev algoritem proizvede več baznih elementov, kot je potrebno, in s tega stališča ni optimalen. To pa lahko izboljšamo, če zahtevamo dodatni pogoj, da noben člen polinoma g_i ni deljiv z $LT(g_j)$ za $j \neq i$. Enoličnost množice G končno zagotovimo, če zahtevamo še, da je vsak g_i *moničen* (tj. $LC(g_i) = 1$ za vsak i). Tako dobimo t. i. *reducirano* Gröbnerjevo bazo. Reducirana Gröbnerjeva baza vedno obstaja in je enolična (glej npr. [9, Theorem 1.2.24]). Preprost algoritem, ki proizvede reducirano Gröbnerjevo bazo in se začne s katerokoli Gröbnerjevo bazo, je naslednji: začnemo z G in naredimo vsak polinom $g_i \in G$ moničen, nato vsak $g \in G$ zamenjamo z njegovim ostankom pri deljenju g z elementi $G \backslash \{g\}$ (pri fiksni monomski ureditvi). Seveda ukazi v vseh sistemih računske algebre izračunajo Gröbnerjevo bazo, ki je že reducirana. Na primer: Gröbnerjeva baza ideala $I = \langle -x^3 + y, x^2y - y^2 \rangle$ glede na leksikografsko ureditev $x > y$ je $G = \{-y^2 + y^3, -y^2 + xy^2, x^2y - y^2, x^3 - y\}$.

V nadaljevanju bomo obravnavali problem iskanja Gröbnerjeve baze v zvezi z nelinearnimi sistemi enačb. Med številnimi uporabami Gröbnerjevih baz bomo na koncu omenili tudi uporabo pri celoštevilskem programiranju, kjer uporabimo Gröbnerjevo bazo z uteženo ureditvijo (glej [5]).

Recimo, da iščemo rešitev $(a_1, \ldots, a_n) \in \overline{k}^n$ (nelinearnega) polinomskega sistema (5), kjer je $\overline{k}$ algebraično zaprtje polja k. Naslednji izrek (glej [3, str. 170]) poda kriterij za obstoj rešitve sistema (5).

Izrek 4. *Naj bo* $G = \{g_1, \ldots, g_t\}$ *reducirana Gröbnerjeva baza ideala* $\langle f_1, \ldots, f_s \rangle$. *Sistem nima rešitve natanko tedaj, ko je* $G = \{1\}$.

Med glavnimi problemi v teoriji polinomskih kolobarjev je problem, ali je neki polinom f v danem idealu $I = \langle f_1, \ldots, f_n \rangle$, in problem, ali je neki polinom v radikalu $\sqrt{I}$ [9, str. 30]. S tem problemom je povezanih več sorodnih problemov; od relacije (v smislu podmnožice) med dvema idealoma do enakosti idealov in preseka idealov [9, str. 36–37], ter nenazadnje problem tako imenovane primarne dekompozicije ideala [9, str. 40–42].

Če sistem (5) nima končno mnogo rešitev, je za njegovo razrešitev treba izračunati primarno dekompozicijo ideala I, kar je znatno zahtevnejše kot račun v spodnjem primeru (podrobnosti glej v [9, poglavje 1.4]), kjer je prikazan tudi postopek uporabe Buchbergerjevega algoritma.

Primer 7. Poiščimo rešitev sistema:

$$\begin{aligned} f_1 &= x^2 + y = 0, \\ f_2 &= 2x^2y + x^4 = 0, \\ f_3 &= xz + x^4 + xy + x^2y^2 = 0. \end{aligned}$$

Izračunajmo Gröbnerjevo bazo z uporabo Buchbergerjevega algoritma. Fiksiramo leksikografsko ureditev $z > y > x$ in uredimo zapis polinomov f_1, f_2, f_3 glede na to ureditev:

$$\begin{aligned} f_1 &= y + x^2, \\ f_2 &= 2yx^2 + x^4, \\ f_3 &= zx + y^2x^2 + yx + x^4. \end{aligned}$$

Sedaj izračunamo posamezne S-polinome, ki so

$$\begin{aligned} S_{f_1,f_2} &= \tfrac{yx^2}{y}(y + x^2) - \tfrac{yx^2}{2yx^2}(2yx^2 + x^4) = \tfrac{x^4}{2}, \\ S_{f_1,f_3} &= \tfrac{zyx}{y}(y + x^2) - \tfrac{zyx}{zx}(zx + y^2x^2 + yx + x^4) = zx^3 - y^3x^2 - y^2x - yx^4, \\ S_{f_2,f_3} &= \tfrac{zyx^2}{2yx^2}(2yx^2 + x^4) - \tfrac{zyx^2}{zx}(zx + y^2x^2 + yx + x^4) = \tfrac{zx^4}{2} - y^3x^3 - y^2x^2 - yx^5. \end{aligned}$$

Sedaj $S_{f_1,f_2} = \frac{1}{2}x^4$ delimo z urejeno množico polinomov (f_1, f_2, f_3) in dobimo ostanek $\frac{1}{2}x^4$. Ker je le-ta neničeln, ga pripišemo k začetni množici polinomov in dobimo urejeno množico $G = (f_1, f_2, f_3, f_4)$, kjer je $f_4 = \frac{1}{2}x^4$. Če delimo polinoma S_{f_1,f_3} in S_{f_2,f_3} z množico polinomov G, obakrat dobimo ostanek 0. Tako je Gröbnerjeva baza ideala $\langle f_1, f_2, f_3\rangle$ enaka $G_B = \{f_1, f_2, f_3, f_4\}$. Bazo reduciramo tako, da vse vodilne koeficiente polinomov f_1, f_2, f_3 in f_4 postavimo na 1. Opazimo tudi, da če polinom f_2 delimo z množico (f_1, f_4), dobimo ostanek 0. Zato lahko f_2 odstranimo iz Gröbnerjeve baze. Če pa polinom f_3 delimo z množico (f_1, f_4), dobimo ostanek $zx - x^3$, ki ga v Gröbnerjevi bazi zapišemo namesto f_3. Tako je reducirana Gröbnerjeva baza ideala $\langle f_1, f_2, f_3\rangle$ enaka

$$G_R = \{y + x^2, x^4, zx - x^3\}.$$

Sedaj lahko sistem $f_1 = f_2 = f_3 = 0$ rešimo zelo preprosto. Ker je drugi polinom v G_R odvisen samo od spremenljivke x, je očitno $x = 0$. Prvi polinom v Gröbnerjevi bazi vsebuje samo x in y, od koder sledi $y = 0$. Zadnji polinom vsebuje spremenljivki x in z, $x = 0$ pa očitno reši enačbo $zx - x^3 = 0$ za vsak z, torej je z poljuben in sistem ima neskončno rešitev, ki jih zapišemo kot

$$\{(0, 0, z) : z \in \mathbb{R}\}.$$

Nazadnje omenimo, da lahko s pomočjo Gröbnerjevih baz rešujemo splošni problem celoštevilskega programiranja (IP) (glej [5]), ki se glasi takole:

$$\text{minimiziraj} \quad \vec{c} \cdot \vec{x} \quad \text{pri pogoju} \quad A\vec{x} = \vec{b}, \tag{10}$$

kjer je $A \in \mathbb{Z}^{m \times n}$ in $\vec{b} = (b_1, \ldots, b_m)^T \in \mathbb{Z}^m$, in da je zelo obsežna tudi uporaba Gröbnerjevih baz pri kvalitativni obravnavi sistemov navadnih diferencialnih enačb (glej npr. [4, 8, 9]).

LITERATURA

[1] M. Beaudin, G. Picard in G. Savard, *Polynomial Systems Solving with Nspire CAS*, V: Galán García, José Luis (ur.). ACA 2013, Málaga, July 2nd–6th, 2013, Hotel Málaga Palacio, Málaga, Spain. Proceedings of Applications of Computer Algebra, 2013, str. 41.

[2] B. Buchberger, *Ein Algorithmus zum Auffinden der Basiselemente des Restlassenringes nach einem nulldimensionalen Polynomideal,* PhD Thesis, Mathematical Institute, University of Innsbruck, Austria, 1965; *An Algorithm for finding the basis elements of the residue class ring of a zero dimensional polynomial ideal*, *J. Symbolic Comput.* **41** (2006), 475–511.

[3] D. Cox, J. Little in D. O'Shea, *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*, 3rd edition, Springer, New York, 2007.

[4] V. F. Edneral, A. Mahdi, V. G. Romanovski in D. S. Shafer, *The center problem on a center manifold in* $\mathbb{R}^3$, Nonlinear Anal. **75** (2012), 2614–2622.

[5] S. Flory in E. Michel, *Integer Programming with Gröbner basis*, `http://www.iwr.uni-heidelberg.de/groups/amj/People/Eberhard.Michel/Documents/Else/DiscreteOptimization.pdf`, ogled 29. 9. 2015.

[6] X. S. Gao in S. Chou, *Implicitization of rational parametric equations*, J. Symbolic Comput. **14** (1992), 459–470.

[7] G.-M. Greuel, G. Pfister in H. A. Schönemann, `SINGULAR 3.0` *A Computer Algebra System for Polynomial Computations*, Centre for Computer Algebra, University of Kaiserlautern (2005), `http://www.singular.uni-kl.de`, ogled 29. 9. 2015.

[8] V. Romanovski, M. Mencinger in B. Ferčec, *Investigation of center manifolds of three-dimensional systems using computer algebra*, Program. comput. softw. **39** (2013), 67–73.

[9] V. G. Romanovski in D. S. Shafer, *The Center and cyclicity Problems: A computational Algebra Approach*, Birkhäuser, Boston, 2009.