Analogoni Gröbnerovih baza na lokalnim prstenima

Manuela Muzika Dizdarević

Matematički institut

Beograd, 2011.

Gröbnerove baze u prstenima polinoma

Standardne baze

Primjeri

Uređenja u skupu monoma

Definicija

Monomijalno uređenje u skupu monoma $x^\alpha \in k[x_1, \ldots, x_n]$ je relacija $>$ za koju vrijedi:

a) $>$ *je totalno uređenje*

b) *kompatibilno je sa množenjem u* $k[x_1, \ldots, x_n]$

c) $>$ *je dobro uređenje*

Primjer (Leksikografski poredak)

Za monome $x^\alpha,\ x^\beta \in k[x_1, \ldots, x_n]$ vrijedi $x^\alpha >_{lex} x^\beta$ ako je u razlici $\alpha - \beta \in \mathbb{Z}^n$ krajnji lijevi element različit od nule pozitivan.

Primjer (Graduirani leksikografski poredak)

Za monome $x^\alpha,\ x^\beta \in k[x_1, \ldots, x_n]$ vrijedi $x^\alpha >_{grlex} x^\beta$ ako je $\sum_{i=1}^n \alpha_i > \sum_{i=1}^n \beta_i$ ili ako je $\sum_{i=1}^n \alpha_i = \sum_{i=1}^n \beta_i$ i $x^\alpha >_{lex} x^\beta$

Algoritam za dijeljenje polinoma

S obzirom na izabrano uređenje u skupu monoma prstena $k[x_1, \ldots, x_n]$, za polinom $f = \sum_\alpha c_\alpha x^\alpha \in k[x_1, \ldots, x_n]$ definišemo vodeći član, vodeći koeficijent i vodeći monom na slijedeći način:

$$LT_>(f) = c_\alpha x^\alpha$$

gdje je x^α najveći monom u odnosu na datu relaciju uređenja, i u tom je slučaju:

$$LC_>(f) = c_\alpha$$
$$LM_>(f) = x^\alpha$$

Algoritam za dijeljenje polinoma: Izaberimo uređenje $>$ u skupu monoma prstena $k[x_1, \ldots, x_n]$.
Ako je $F = (f_1, \ldots, f_s)$ uređena $s-$torka polinoma prstena $k[x_1, \ldots, x_n]$ onda za svako $f \in k[x_1, \ldots, x_n]$ postoje polinomi $r, a_i \in k[x_1, \ldots, x_n]$ takvi da vrijedi

$$f = a_1 f_1 + \cdots + a_s f_s + r$$

pri čemu je $a_i f_i = 0$ ili je $LT_>(f) \geq LT_>(a_i f_i)$ i $r = 0$ ili je r linearna kombinacija monoma od kojih ni jedan nije djeljiv ni jednim od $LT_>(f_1), \ldots, LT_>(f_s)$.

Gröbnerova baza

Definicija (Gröbnerova baza)

Neka je I ideal prstena $k[x_1, \dots, x_n]$. Gröbnerova baza ideala I s obzirom na dato monomijalno uređenje je konačna familija polinoma $G = \{g_1, \dots, g_t\} \subset I$ takva da je za svaki polinom $f \in I$, $f \neq 0$, $LT(f)$ djeljiv sa $LT(g_i)$ za neko i.

Ako izaberemo uređenje $>$ u skupu monoma prstena $k[x_1, \dots, x_n]$ i ako je $G = \{g_1, \dots, g_s\}$ Gröbnerova baza s obzirom na dato uređenje onda je ostatak dijeljenja bilo kojeg polinoma $f \in k[x_1, \dots, x_n]$ polinomima skupa G jednoznačno određen i zovemo ga NORMALNA FORMA polinoma f u odnosu na $G = \{g_1, \dots, g_s\}$.

S-polinom

Primjer

Neka je ideal $I \in k[x,y,z]$ generisan sa $I = \langle x^2+2y^2-y-2z, x^2-8y^2+10z-1, x^2-7yz \rangle$. Gröbnerova baza ovog ideala računata s obzirom na leksikografski poredak u skupu monoma prstena $k[x,y,z]$ je

$$
\begin{aligned}
G &= \{-2+37z-313z^2+980z^3, \\
&\quad -13+201z-980z^2+18y, -7+84z-392z^2+9x^2\}
\end{aligned}
$$

Definicija (S-polinom)

Neka je u skupu monoma prstena $k[x_1,\ldots,x_n]$ fiksirano uređenje i neka su $f,g \in k[x_1,\ldots x_n]$ nenulti polinomi. Za

$$LT(f) = cx^\alpha \text{ i } LT(g) = dx^\beta$$

sa x^γ označimo najmanji zajednički sadržalac monoma x^α i x^β. Tada je S-polinom ponoma f i g dat sa

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

Buchbergerov algoritam

Buchbergerov kriterij:

Konačan skup $G = \{g_1, \ldots, g_t\}$ je Gröbnerova baza ideala $I = \langle g_1, \ldots, g_t \rangle$ ako i samo ako je ostatak dijeljenja polinoma $S(g_i, g_j)$ familijom G jednak nuli za sve parove $i \neq j$.

Buchbergerov algoritam:

Input: $F = (f_1, \ldots, f_s)$

Output: Gröbnerova baza $G = \{g_1, \ldots, g_t\}$ ideala $I = \langle F \rangle$

$G := F$

REPEAT

  $G' = G$
  FOR svaki par $p \neq q$ iz G' DO
    S :=ostatak dijeljenja $S(p, q)$ sa G'
    IF $S \neq 0$ THEN $G := G \cup \{S\}$

UNTIL $G = G'$

Višestrukost tačke varijeteta

Definicija

Neka je I $0-$dimenzionalni ideal prstena $k[x_1, \ldots, x_n]$ i neka je $p_i = (a_1, \ldots, a_n)$ jedna od tačaka varijeteta $V(I)$.Sa $\mathcal{O}_i$ označimo prsten racionalnih funkcija definisanih u tački p_i. Višestrukost tačke p_i označavamo sa $m(p_i)$ i definišemo na slijedeći način:

$$m(p_i) = dim\, \mathcal{O}_i / I\mathcal{O}_i$$

Teorema

Neka je k algebarski zatvoreno polje i neka je I $0-$dimenzionalni ideal u $k[x_1, \ldots, x_n]$. Broj tačaka varijeteta $V(I)$ računat zajedno sa njihovim višestrukostima jednak je $dim\, k[x_1, \ldots, x_n]/I$ Naime, ako su $p_1, \ldots, p_m$ različite tačke varijeteta $V(I)$, a za svako i sa $\mathcal{O}_i$ označimo prsten racionalnih funkcija definisanih u tački p_i onda je

$$dim\, k[x_1, \ldots, x_n]/I = \sum_{i=1}^{m} dim \mathcal{O}_i / I\mathcal{O}_i = \sum_{i=1}^{m} m(p_i)$$

Primjer

Posmatrajmo sistem jednačina:

$$x^2 + x^3 = y^2 = 0$$

Rješenja ovog sistema su tačke $(0,0)$ i $(-1,0)$.
U odnosu na leksikografski poredak polinomi $x^3 + x^2$ i y^2 predstavljaju Gröbnerovu bazu ideala I što znači da je

$$dim\, k[x,y]/I = dim\, k[x,y]/\langle LT(I)\rangle = dim\, k[x,y]/\langle x^3, y^2\rangle = 6$$

Odredimo višestrukost svake od ovih tačaka i provjerimo tačnost prethodne teoreme. Posmatrjamo najprije tačku $(0,0)$.
Neka je $R = k[x,y]_{\langle x,y\rangle}$
$\frac{1}{x+1} \in R$ što znači da je $(x+1)$ jedinica prstena R. Kako je, dalje

$$x^2 = x^2(x+1)\cdot\frac{1}{x+1} \in \langle x^2+x^3, y^2\rangle R$$

i

$$x^2 + x^3 = x^2(x+1) \in \langle x^2, y^2\rangle R$$

zaključujemo da je $\langle x^2, y^2\rangle R = \langle x^2 + x^3, y^2\rangle R$.

Primjer

Proizvoljno $f \in R$ se može napisati u obliku $f = \frac{g}{1+h}$, gdje je $g \in k[x,y]$ i $h \in \langle x, y \rangle$. Osim toga

$$\frac{g}{1+h} - g \cdot (1 - h + h^2) = \frac{g - g(1-h+h^2)(1+h)}{1+h} = \frac{-gh^3}{h+1}$$

Zbog toga što je $h \in \langle x, y \rangle$, $h^3 \in \langle x^2, y^2 \rangle$, pa je

$$f - g \cdot (1 - h + h^2) \in \langle x^2, y^2 \rangle R$$

odakle slijedi da je $[f] = [g \cdot (1 - h + h^2)] \in R / \langle x^2, y^2 \rangle R$.
$h \in \langle x, y \rangle$, pa postoje $a, b, c, d \in k$ za svko $f \in$ tako da je

$$[f] = [g \cdot (1 - h + h^2)] = [a + bx + cy + dxy]$$

Iz svega rečenog zaključujemo da je

$$dim\, R / \langle x^2, y^2 \rangle R = 4$$

Primjer

Da bi odredili višestrukost tačke $(-1, 0)$ najprije translirajmo koordinatni sistem u tačku $(-1, 0)$. Naš sistem sada postaje

$$(x-1)^2 + (x-1)^2 = x^3 - 2 \cdot x^2 + x = y^2 = 0$$

Odredimo $dim\, R/\langle x^3 - 2x^2 + x, y^2 \rangle R$.
$x^3 - 2x^2 + x = x(x-1)^2$, a kako je $(x-1)$ jedinica prstena R, na isti način kao ranije zaključujemo da je $\langle x^3 - 2x^2 + x, y^2 \rangle R = \langle x, y^2 \rangle R$. Svako $f \in R$ može se napisati kao $\frac{g}{1+h}$ za $h \in \langle x, y \rangle$, pa je $[f] = [g \cdot (1 - h + h^2)]$, a svaka takva kalsa jednaka je klasi $[a + by]$ za neke $a, b \in k$. Zbog toga zaljučujemo da je

$$dim\, R/\langle x^3 - 2x^2 + x, y^2 \rangle R = 2$$

Dakle, višestrukost tačke $(-1, 0)$ jednaka je 2. Vidimo da posmatrani sistem ima dvije nule $(0, 0)$ višestrukosti 4 i $(-1, 0)$ višestrukosti 2, što znači da je broj nula zajedno sa višestrukostima jednak 6, a to je upravo

$$dim\, k[x, y]/\langle x^3 + x^2, y^2 \rangle$$

Lokalna uređenja

Definicija (Lokalno uređenje)

Lokalno uređenje u skupu monoma $x^\alpha \in k[x_1, \dots, x_n]$ *je relacija* $>$ *za koju vrijedi:*

a) $>$ *je totalno uređenje*

b) *kompatibilno je sa množenjem u* $k[x_1, \dots, x_n]$

c) *za svako* $1 \leq i \leq n$ *vrijedi* $1 > x_i$

Primjer (Antigraduirani leksikografski poredak)

Za monome $x^\alpha,\ x^\beta \in k[x_1, \dots, x_n]$ *vrijedi* $x^\alpha >_{alex} x^\beta$ *ako je*

$$|\alpha| = \sum_{i=1}^{n} \alpha_i < \sum_{i=1}^{n} \beta_i = |\beta|$$

ili je $|\alpha| = |\beta|$ *i* $x^\alpha >_{lex} x^\beta$

Polugrupna uređenja

Definicija (Polugrupno uređenje)

Polugrupno uređenje u skupu monoma $x^\alpha \in k[x_1, \ldots, x_n]$ *ili* $x^\alpha \in k[x_1, \ldots, x_n]_{\langle x_1, \ldots, x_n \rangle}$ *je relacija* $>$ *za koju vrijedi:*

a) $>$ *je totalno uređenje*

b) *kompatibilno je sa množenjem u* $k[x_1, \ldots, x_n]$

Definicija

Neka je $>$ *polugrupno uređenje u skupu monoma prstena* $k[x_1, \ldots, x_n]$ *i neka je*

$$S = \{1 + g \in k[x_1, \ldots, x_n] \mid g = 0 \ \vee \ LT_>(g) < 1\}$$

Lokalizacija prstena $k[x_1, \ldots, x_n]$ *s obzirom na uređenje* $>$ *je prsten*

$$Loc_>(k[x_1, \ldots, x_n]) = S^{-1}k[x_1, \ldots, x_n] = \{\frac{f}{1+g} \mid 1 + g \in S\}$$

Mora algoritam za dijeljenje

Neka su $f, g \in k[x_1, \ldots, x_n]$ i neka je $m = cx^\alpha$ tako da vrijedi $LT(f) = m \cdot LT(g)$. Kažemo da smo polinom f reducirali polinomom g ako smo odredili razliku oblika:

$$Red(f, g) = f - mg$$

U slučaju lokalnog uređenja uobičajeni proces dijeljenja zahtijeva beskonačno mnogo redukcija.

Primjer:
Podijelimo polinom $f = x$ polinomom $g = 1 - x$ u prstenu $k[x]$ s obzirom na lokalno uređenje $(1 > x > x^2 > \ldots)$
$f_1 = Red(f, g) = x - x(1 - x) = x^2$
$f_2 = Red(f_1, g) = x^2 - x^2(1 - x) = x^3$
$\vdots$

Mora algoritam za dijeljenje

Mora algoritam za dijeljenje polinoma: Izaberimo polugrupno uređenje $>$ u skupu monoma prstena $k[x_1, \dots, x_n]$. Ako je $F = (f_1, \dots, f_s)$ uređena $s-$torka polinoma prstena $k[x_1, \dots, x_n]$ onda za svako $f \in k[x_1, \dots, x_n]$ postoje polinomi $u, h, a_i \in k[x_1, \dots, x_n]$ takvi da vrijedi

$$u \cdot f = a_1 \cdot f_1 + \cdots + a_s \cdot f_s + h$$

pri čemu je $LT(u) = 1$, $LT(a_i)LT(f_i) \leq LT(f)$ za sve i za koje je $a_i \neq 0$, a $h = 0$ ili $LT(h)$ nije djeljiv sa $LT(f_i)$ ni za jedno i.

Ako Mora algoritam za dijeljenje primjenimo u prethodnom primjeru imaćemo:
$u = (1 - x)$, $a_1 = x$ i $r = 0$ tj.
$(1 - x) \cdot x = x \cdot (1 - x) + 0$

Standardna baza

Definicija (Standardna baza)

Neka je $>$ polugrupno uređenje na skupu monoma prstena $k[x_1, \ldots, x_n]$ i neka je $R = Loc_>(k[x_1, \ldots, x_n])$. Standardna baza ideala $I \subset R$ je skup $\{g_1, \ldots, g_t\} \subset I$ za koje vrijedi $\langle LT(I) \rangle = \langle LT(g_1), \ldots, LT(g_t) \rangle$.

Ako izaberemo polugrupno uređenje $>$ u skupu monoma prstena $k[x_1, \ldots, x_n]$ i ako je $G = \{g_1, \ldots, g_s\}$ standardna baza s obzirom na dato uređenje onda je $LM_>(r)$ ostatka dijeljenja polinoma $f \in k[x_1, \ldots, x_n]$ polinomima skupa G jednoznačno određen pa r zovemo SLABA NORMALNA FORMA polinoma f u odnosu na $G = \{g_1, \ldots, g_s\}$.

Standardna baza

Analogon Bucbergerovog kriterija:

Neka je u prstenu $k[x_1, \ldots, x_n]$ dato polugrupno uređenje $>$, neka je S njegov konačan podskup i neka je I ideal prstena $R = Loc_>(k[x_1, \ldots, x_n])$ generisan skupom S.
$S = \{g_1, \ldots, g_t\}$ je standardna baza ideala I ako i samo ako je ostatak dijeljenja Mora algoritmom za dijeljenje svih S polinoma skupa G, polinomima skupa G jednak nuli.

Analogon Buchbergerovog algoritma:

Primjena Buchbergerovog algoritma s tom razlikom da se umjesto uobičajenog dalgoritma za dijeljenje polinoma koristi Mora algoritam, nakon konačno mnogo koraka dovodi do standardne baze ideala $I \subset R$ koji je generisan skupom S.

Milnorov broj

Definicija (Milnorov broj)

Neka je $p = (0, \ldots, 0) \in \mathbb{C}^n$ *izolovana singularna tačka funkcije* $f \in \mathbb{C}\{x_1, \ldots, x_n\}$. *Milnorov broj singularne tačke* p *koji označavamo sa* $\mu(p)$ *definiše se sa*

$$\mu(p) = dim\, \mathbb{C}\{x_1, \ldots, x_n\}/\langle \frac{\partial f}{\partial x_1}, \ldots, \frac{\partial f}{\partial x_n} \rangle$$

Primjer

Za svaku od slijedećih funkcija $f(x, y) \in \mathbb{C}[x, y]$ *odrediti Milnorov broj izolovane singularne tačke* $(0, 0)$

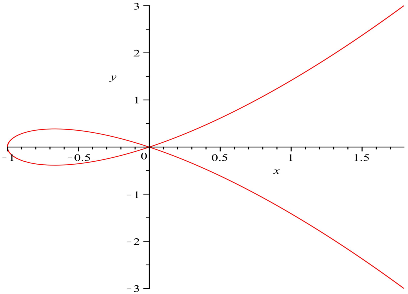
a) $f(x, y) = y^2 - x^2 - x^3$
b) $f(x, y) = y^2 - x^3$
c) $f(x, y) = y^2 - x^5$

Milnorov broj

a) Za $f(x,y) = y^2 - x^2 - x^3$ imamo da je $\frac{\partial f}{\partial x} = -2x - 3x^3$ i $\frac{\partial f}{\partial y} = 2y$, pa je po definiciji Milnorovog broja

$$\mu = dim\mathbb{C}[x,y]_{\langle x,y\rangle} / \langle -2x - 3x^2, 2y\rangle \mathbb{C}[x,y]_{\langle x,y\rangle}$$

Standardna baza ideala $I = \langle -2x - 3x^2, 2y\rangle$ u loklanom prstenu $\mathbb{C}[x,y]_{\langle x,y\rangle}$ jednaka je $std(I) = \{x, y\}$, što znači da je $\mu = 1$.

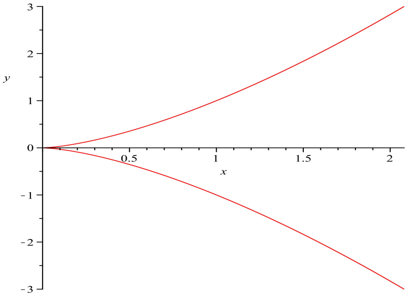


Milnorov broj

b) Za $f(x,y) = y^2 - x^3$ imamo da je $\frac{\partial f}{\partial x} = -3x^2$ i $\frac{\partial f}{\partial y} = 2y$, pa je po definiciji Milnorovog broja

$$\mu = dim\mathbb{C}[x,y]_{\langle x,y\rangle}/\langle -3x^2, 2y\rangle\mathbb{C}[x,y]_{\langle x,y\rangle}$$

Standardna baza ideala $I = \langle -3x^2, 2y\rangle$ u loklanom prstenu $\mathbb{C}[x,y]_{\langle x,y\rangle}$ jednaka je $std(I) = \{x^2, y\}$, što znači da je $\mu = 2$.

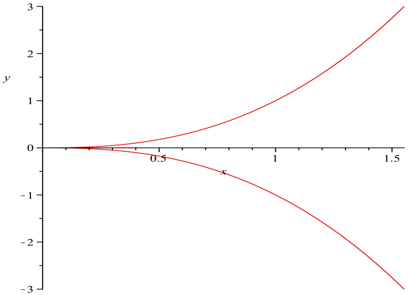


Milnorov broj

c) Za $f(x,y) = y^2 - x^5$ imamo da je $\frac{\partial f}{\partial x} = -5x^4$ i $\frac{\partial f}{\partial y} = 2y$, pa je po definiciji Milnorovog broja

$$\mu = dim \mathbb{C}[x,y]_{\langle x,y \rangle} / \langle -5x^4, 2y \rangle \mathbb{C}[x,y]_{\langle x,y \rangle}$$

Standardna baza ideala $I = \langle -5x^4, 2y \rangle$ u loklanom prstenu $\mathbb{C}[x,y]_{\langle x,y \rangle}$ jednaka je $std(I) = \{x^4, y\}$, što znači da je $\mu = 4$.



Primjer

Odredimo višestrukost rješenja u nuli slijedećeg sistema jednačina

$$\begin{aligned} x^3 - 3xy^7 + z^6 &= 0 \\ 5xy^2 + y^3 + z^4 &= 0 \\ x^2 + 2y^2 - 4z^2 &= 0 \end{aligned}$$

Vidjeli smo da je ta višestrukost jednaka

$$m = dim k[x,y,z]_{\langle x,y,z\rangle} / I\, k[x,y,z]_{\langle x,y,z\rangle}$$

gdje je $I = \langle x^3 - 3xy^7 + z^6, 5xy^2 + y^3 + z^4, x^2 + 2y^2 - 4z^2\rangle$.
Odredimo li standardnu bazu ideala I imat ćemo:

$$\begin{aligned} std(I) \;=\; & \{x^2 + 2y^2 - 4z^2,\ xy^2 - 12801y^3 - 12801z^4, \\ & xz^2 + 9601y^3 + 9601z^4,\ y^4 - 2512y^2z^2 + 6275xz^4 - 1255yz^4, \\ & y^2z^2 + 11076z^4 - 13232yz^4,\ yz^4, z^6\} \end{aligned}$$

Primjer

Kako je

$$dim k[x,y,z]_{\langle x,y,z\rangle}/I\ k[x,y,z]_{\langle x,y,z\rangle} = \text{broj standardnih monoma}$$

a standardni monomi su u ovom slučaju

$$1, x, xy, xz, xyz, xyz^2, y, y^2, y^3, yz, y^2z, yz^2, yz^3, z, z^2, z^3, z^4, z^5$$

zaključujemo da je tražena višestrukost $m = 18$

KRAJ

HVALA NA PAŽNJI!