Gröbnerove baze i politopi

Manuela Muzika Dizdarević

CGTA seminar

Beograd, 2011.

Univerzalna Gröbnerova baza

State politop

Torusni varijeteti i univerzalna Gröbnerova baza

Uređenja u skupu monoma

Definicija

Globalno 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 (Leksikografsko uredjenje)

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 (Graduirano leksikografsko uredjenje)

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 $x^\alpha >_{lex} x^\beta$

Definicija Gröbenrove baze

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

$$in_>(f) = x^\alpha$$

gdje je x^α najveći monom u odnosu na datu relaciju uređenja.
Za svaki ideal $I \in k[x_1, \dots, x_n]$ s obzirom na izabrano urđenje definišemo inicijalni ideal $in_>(I)$ sa:

$$in_>(I) = \langle in_>(f) \ : \ f \in I \rangle$$

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 $in_>(I)$ generisan skupom $\{in_>(g) \ : \ g \in G\}$.

Ako, osim toga, za svaka dva elementa $g, g' \in G$ nijedan član od g' nije djeljiv sa $in_>(g)$ kažemo da je Gröbnerova baza reducirana.

Prirodno je zapitati se slijedeće:

- Koliko različitih reduciranih Gröbnerovih baza može imati jedan ideal?
- Da li je moguće naći bazu za svaki ideal koja je njegova Gröbnerova baza u odnosu na sva moguća uređenja?
- Ako takva baza postoji da li postoji efektivan algoritam za njeno određivanje?
- Da li takva baza određuje neki geometrijski objekat koji pridružujemo idealu?

Univerzalna Gröbnerova baza

Svaki ideal $I \in k[x_1, \ldots, x_n]$ je konačno generisan.

Za svaki ideal $I \in k[x_1, \ldots, x_n]$ postoji samo konačno mnogo različitih inicijalnih ideala.

Definicija (Univerzalna Gröbnerova baza)

Neka je I ideal prstena $k[x_1, \ldots, x_n]$. Konačan podskup $U \in I$ zovemo univerzalna Gröbnerova baza ideala I ako je U Gröbnerova baza ideala I s obzirom na sva moguća globalana uređenja.

Svaki ideal $I \in k[x_1, \ldots, x_n]$ posjeduje univerzalnu Gröbnerovu bazu.

UGB ideala generisanog linearnim formama

Primjer

Neka je $I \in \mathbb{C}[x_1, \ldots, x_6]$ *ideal generisan slijedećim linearnim formama:*

$$2x_1 + x_2 + x_3$$
$$x_2 + 2x_4 + x_5$$
$$x_3 + x_5 + 2x_6$$

Univerzalna Gröbnerova baza ovog ideala sastoji se od slijedećih 9 *polinoma:*

$$\begin{array}{rcc} x_3 + x_5 + 2x_6 & x_2 + 2x_4 + x_5 & 2x_1 + x_2 + x_3 \\ x_2 - x_3 + 2x_4 - 2x_6 & x_1 - 2x_4 - x_5 - x_6 & x_1 + x_3 - x_4 + x_6 \\ 2x_1 + x_3 - 2x_4 - x_5 & 2x_1 + x_2 - x_5 - 2x_6 & x_1 - x_2 + x_4 + x_6 \end{array}$$

Poliedralni konus i konveksni politop

Definicija

Skup P oblika
$P = cone(S) = \{\sum_{u \in S} \lambda_u u \ : \ \lambda_u \geq 0\}$
pri čemu je S konačan podskup od $\mathbb{R}^n$ zovemo konveksan poliedralni konus generisan skupom S.

Definicija

Skup $Q \in \mathbb{R}^n$ oblika
$Q = conv(S) = \{\sum_{u \in S} \lambda_u u \ : \ \lambda_u \geq 0, \ \sum_{u \in S} \lambda_u = 1\}$
pri čemu je S konačan podskup od $\mathbb{R}^n$ zovemo konveksni politop.

Stranicom poliedralnog konusa $P \in \mathbb{R}^n$ zovemo svaki podskup oblika
$face_\omega(P) := \{u \in P : \omega \cdot u \geq \omega \cdot v \ \forall v \in P\}$
gdje je ω vektor iz $\mathbb{R}^n$.

Normalna lepeza

Definicija

Konačnu familiju Δ poliedralnih konusa u $\mathbb{R}^n$ za koje vrijedi:

- *Ako je $P \in \Delta$ i F je stranica od P onda je $F \in \Delta$*
- *Ako su P_1 i P_2 poliedralni konusi familije Δ, onda je $P_1 \cap P_2$ stranica svakog od njih*

zovemo lepeza.

Neka je P poliedralni konus i neka je F njegova stranica. Normalni konus $\mathcal{N}_p(F)$ od F u P definišemo sa:

$$\mathcal{N}_P(F) = \{\omega \in \mathbb{R}^n \ : \ face_\omega(P) = F\}$$

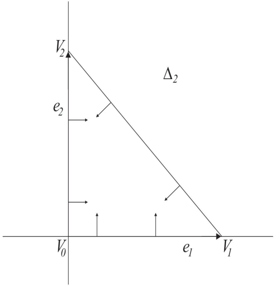
Familija svih normalnih konusa $\mathcal{N}_P(F)$ gdje F prolazi svim stranicama poliedralnog konusa P je lepeza.

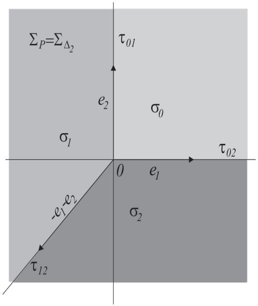
Primjer normalne lepeze

Posmatrajmo $2-$simpleks $\Delta_2 \subseteq \mathbb{R}^2$ sa vrhovima $0, e_1$ i e_2. Lepeza Σ_{Δ_2} sastoji se od tri dvodimenzionalna konusa

$$\sigma_0 = Cone(e_1, e_2),\ \sigma_1 = Cone(-e_1 - e_2, e_2) \text{ i } \sigma_2 = Cone(e_1, -e_1 - e_2),$$

tri jednodimenzionalna konusa (zrake) $\tau_{ij} = \sigma_i \cap \sigma_j$, $i \neq j$ i koordinatnog početka.





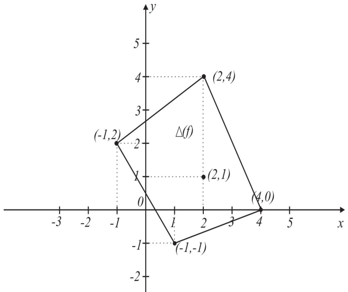
Newtonov politop

Svakom polinomu $f := \sum_{i=1}^{m} c_i \cdot x^{a_i} \in k[x_1^{\pm 1}, \ldots, x_n^{\pm 1}]$ možemo pridružiti Newtonov politop sa

$$New(f) = conv\{a_i \ : \ i = 1, \ldots, n\}$$

Primjer

Newtonov poligon polinoma
$f(x,y) = a_1 xy^{-1} + a_2 x^4 + a_3 x^2 y^4 + a_4 x^2 y + a_5 x^{-1} y^2$
je konveksno zatvorenje skupa $A = \{(1,-1), (4,0), (2,4), (-1,2), (2,1)\}$



Karakterizacija uređenja

Odaberimo vektor $\omega = (\omega_1, \dots, \omega_n) \in \mathbb{R}^n$. Za svaki polinom $f = \sum c_i x^{a_i}$ definišemo inicijalnu formu $in_\omega(f)$ kao sumu svih članova $c_i x^{a_i}$ za koje je proizvod $\omega \cdot a_i$ maksimalan.
Za svaki ideal I možemo definisati njegov inicijalni ideal $in_\omega(I)$ s obzirom na ω kao ideal generisan inicijalnim linearnim formama, tj

$$in_\omega(I) := \langle in_\omega(f) \ : \ f \in I \rangle$$

Za svaki ideal $I \in k[x_1, \dots, x_n]$ i svako uređenje $>$ postoji nenegativan vektor $\omega \in \mathbb{N}^n$ takav da je

$$in_>(I) = in_\omega(I)$$

U tom slučaju kažemo da je ω predstavnik uređenja $>$ na idealu I.

Uređenja i konusi

Za dva vektora ω i ω' iz $\mathbb{R}^n$ kažemo da su ekvivalentni s obzirom na ideal I ako i samo ako je

$$in_\omega(I) = in_{\omega'}(I)$$

Skup svih klasa ekvivalencije vektora ω koji predstavljaju isto uređenje na idealu I je otvoreni poliedralni konus koji označavamo sa $C[\omega]$.
Ako je G Gröbnerova baza ideala I s obzirom na uređenje $>_\omega$, onda je

$$C[\omega] = \{\omega' \in \mathbb{R}^n \ : \ in_{\omega'}(g) = in_\omega(g) \ \forall g \in G\}$$

Geometrijska reformulacija ove formule u terminima normalnih konusa Newtonovih politopa je

$$C[\omega] = \mathcal{N}_Q(face_\omega(Q))$$

gdje je $Q = New(\prod_{g \in G} g) = \sum_{g \in G} New(g)$.

Definicija politopa stanja (state politopa)

Familija svih zatvorenih konusa $\overline{C[\omega]}$ ideala I za $\omega \in \mathbb{R}^n$ je lepeza u smislu gornje definicije koju zovemo Gröebnerova lepeza ideala I i označavamo sa $GF(I)$. Ukoliko je ideal I homogen njegova Gröebnerova lepeza je kompletna sto znaci da je $|GF(I)| = \cup_{\omega\in\mathbb{R}}\overline{C[\omega]} = \mathbb{R}^n$.

Definicija (State politop)

Neka je $I \in k[x_1, \ldots, x_n]$ homogen ideal. Kažemo da je politop P state politop ideala I ako je njegova normalna lepeza $\mathcal{N}(Q)$ izomorfna sa Gröbnerovom lepezom ideala I tj sa $GF(I)$.

Primjer

Odrediti state politop ideala I generisanog homogenim polinomom

a) $f = x^2 + xy + y^2 \in \mathbb{R}[x, y]$

b) $f = x + y + z \in \mathbb{R}[x, y, z]$

Politop stanja za neke specijalne ideale

Propozicija

Neka je f homogen polinom i $I = \langle f \rangle$ glavni ideal generisan polinomom f, tada je Newtonov politop polinoma f politop stanja ideala I

Ako je G univerzalna Gröbnerova baza ideala I i ako je G reducirana Gröebnerova baza s obzirom na bilo koje uređenje na idealu I onda je $\sum_{g \in G} New(g)$ politop stanja ideala I.

Propozicija

Ako je ideal I generisan linearnim formama onda je njegov matroid politop

$$Mat(I) = conv\{e_{i_1} + \cdots + e_{i_d} \ : \ \{i_1, \ldots, i_d\} baza\}$$

politop stanja ideala I.

Algoritmi za određivanje politopa stanja i univerzalne Gröebnerove baze

Postoje:

- Algoritam za određivanje politopa stanja proizvoljnog homogenog ideala *I*
- Algoritam za izračunavanje univerzalne Gröbnerove baze iz poznatog politopa stanja homogenog ideala *I*
- Algoritam za određivanje politopa stanja iz poznate univerzalne Gröebnerove baze homogenog ideala *I*
- Algoritam za određivanje najpogodnijeg uređenja za najefikasnije izračunavanje Gröebnerove baze datog ideala

Definicija torusnog varijeteta

Neka nam je dat skup vektora $\mathcal{A} = \{a_1, \ldots, a_n\} \subset \mathbb{Z}^d$. Definišimo preslikavanje $\Phi_{\mathcal{A}} : T \to k^d$ sa

$$\Phi_{\mathcal{A}}(t) = (t^{a_1}, \ldots, t^{a_n})$$

Definicija

Zariski zatvorenje slike preslikavanja $\Phi_{\mathcal{A}}$ je afin torusni varijetet $V(I_{\mathcal{A}})$

Definišimo preslikavanje $\pi : \mathbb{Z}^n \to \mathbb{Z}^d$ sa

$$\pi(u_1 \ldots, u_n) = u_1 \cdot a_1 + \cdots + u_n \cdot a_n$$

Za vektor $u = (u_1 \ldots, u_n) \in \ker(\pi)$ stavimo da je $u^+ = \sum_{u_i > 0} u_i e_i$ i $u^- = \sum_{u_i < 0} u_i e_i$. Jasno je da je $u = u^+ - u^-$.

Definicija

Ideal oblika $I_{\mathcal{A}} = \langle x^{u^+} - x^{u^-} \ : \ u \in ker(\pi) \rangle$ zovemo torusni ideal, a varijetet oblika $V(I_{\mathcal{A}})$ je torusni varijetet.

Gröbnerova i Graverova baza ideala $I_{\mathcal{A}}$

Za svako uređenje $>$ na skupu monoma postoji konačan skup vektora $\mathcal{G}_> \subset \ker(\pi)$ za koji je reducirana Gröbnerova baza ideala $I_{\mathcal{A}}$ s obzirom na dato uređenje jednaka

$$\{x^{u^+} - x^{u^-} \;:\; u \in \mathcal{G}_>\}$$

Skup vektora $\mathcal{G}_>$ zovemo reducirana Gröbnerova baza skupa $\mathcal{A}$ s obzirom na uređenje $>$. Unija reduciranih Gröbnerovih baza $\mathcal{G}_{\mathcal{A}}$ torusnog ideala $I_{\mathcal{A}}$ gdje $>$ prolazi svim uređenjima je univerzalna Gröbnerova baza torusnog ideala $I_{\mathcal{A}}$ koju označavamo sa $\mathcal{U}_{\mathcal{A}}$.

Za binom $x^{u^+} - x^{u^-} \in I_{\mathcal{A}}$ kažemo da je primitivan ako ne postoji binom $x^{v^+} - x^{v^-} \in I_{\mathcal{A}}$ takav da x^{v^+} dijeli x^{u^+} i x^{v^-} dijeli x^{u^-}

Definicija

Skup svih primitivnih polinoma ideala $I_{\mathcal{A}}$ zovemo Graverova baza ideala $I_{\mathcal{A}}$ i označavamo sa $Gr_{\mathcal{A}}$

Graverova baza i ciklovi

- Za nenulti vektor $u \in \ker(\pi)$ kažemo da je cikl ako je $supp(u)$ minimalan s obzirom na inkluziju, a koordinate su relativno proste
- Svaki cikl je primitivan vektor
- Ako je cikl $u \in \ker(\pi)$ onda $supp(u)$ ima najviše $d+1$ element
- Skup svih ciklova ideala $I_{\mathcal{A}}$ označavamo sa $C_{\mathcal{A}}$

Teorema

Za svaki konačan skup $\mathcal{A} \subset \mathbb{Z}^d$ vrijedi

$$C_{\mathcal{A}} \subseteq U_{\mathcal{A}} \subseteq Gr_{\mathcal{A}}$$

Određivanje Graverove baze torusnog ideala

Definicija

Neka nam je data matrica $\mathcal{A} \in \mathbb{Z}^{d \times n}$. Matricu $\Lambda(\mathcal{A})$ formata $(d+n) \times 2n$ i oblika

$$\Lambda(\mathcal{A}) = \begin{bmatrix} \mathcal{A} & 0 \\ E & E \end{bmatrix}$$

zovemo Lawrenceova matrica matrice $\mathcal{A}$

Teorema

Ako je $\Lambda(\mathcal{A})$ matrica Lawrenceovog tipa onda su slijedeći skupovi binoma jednaki:

- *Graverova baza od $\Lambda(\mathcal{A})$*
- *Univerzalna Gröbnerova baza od $\Lambda(\mathcal{A})$*
- *Bilo koja reducirana Gröbnerova baza ideala $I_{\Lambda(\mathcal{A})}$*

Određivanje univerzalne Gröbnerove baze torusnog ideala

Za vektor $u \in \mathbb{Z}^n$ kažemo da je relativno prost ako su njegove koordinate relativno proste.

Teorema

Relativno prost vektor $u \in \ker(\pi)$ leži u univerzalnoj Gröbnerovoj bazi $U_{\mathcal{A}}$ ako i samo ako je linijski segment $[u^+, u^-]$ ivica politopa $conv(\pi^{-1}(\pi(u^+)))$

Neka je $\mathcal{A} \in \mathbb{N}^d$. Vektor $b \in \mathbb{N}\mathcal{A}$ zovemo Gröbnerov stepen ako postoji binom $x^{u^+} - x^{u^-} \in U_{\mathcal{A}}$ takav da je $\pi(u^+) = \pi(u^-) = b$.
Ako je b Gröbnerov stepen, onda se politop $conv(\pi^{-1}(b))$ zove Gröbnerov fiber.

Teorema

Minkowski suma svih Gröbnerovih fiber-i je politop stanja ideala $I_{\mathcal{A}}$

KRAJ

HVALA NA PAŽNJI!