Linearna algebra nad polkolobarji

Jimmy Zakeršnik

mentor: prof. dr. Tomaž Košir

20. maj 2022

Napovednik:

Napovednik:

Motivacija:

Polkolobarjev je veliko - pojavljajo se v skoraj vsakem področju matematike. Nekateri primeri so:

- $\mathbb{N}_0$ oz. $\mathbb{Z}^+$, $\mathbb{Q}^+$, $\mathbb{R}^+$ za standardne operacije $+$ in $*$
- *max-plus algebra* $(\mathbb{R} \cup \{-\infty\}, max, +)$ in *min-plus algebra* $(\mathbb{R} \cup \{\infty\}, min, +)$
- Boolove algebre
- Polkolobarji (pod)množic za $\cup$ in $\cap$

Kanonično urejeni monoidi in grupe:

Definicija

Za komutativen monoid $(M, *)$ pravimo, da je kanonično urejen, če je operacija $*$ usklajena s kanonično delno urejenostjo $\leq$ na M. To pomeni:

$$a \leq \acute{a} \Rightarrow a * \hat{a} \leq \acute{a} * \hat{a} \text{ za vse } a, \acute{a}, \hat{a} \in M.$$

Izrek

Komutativen monoid M ne more hkrati biti kanonično urejen in grupa.

Razred monoidov torej lahko razdelimo na razred grup, razred kanonično urejenih monoidov in na razred ostalih.

Polkolobarji:

Definicija

Za neprazno množico R, ki je opremljena z operacijama $\oplus$ in $\otimes$ pravimo, da je *polkolobar*, če zanjo velja naslednje:

1. $(R, \oplus)$ je komutativen monoid z nevtralnim elementom 0,
2. $(R, \otimes)$ je monoid z enoto 1,
3. $a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$ in $(b \oplus c) \otimes a = (b \otimes a) \oplus (c \otimes a); \; \forall a, b, c \in R$,
4. $0 \otimes a = 0 = a \otimes 0; \forall a \in R$ - 0 izniči operacijo $\otimes$.

Oznaka: $(R, \oplus, \otimes)$.

Dioidi:

Klasifikacija monoidov $\Rightarrow$ klasifikacija polkolobarjev: kolobarji, dioidi in ostali.

Definicija

Polkolobarju $(R, \oplus, \otimes)$, na katerem je kanonična relacija šibke urejenosti $\leq$, definirana preko $\oplus$, delna urejenost, pravimo dioid.

Trditev

Kanonična delna urejenost je v dioidu usklajena z obema operacijama.

Če je $(R, +)$ kanonično urejen komutativen monoid in $H = \{\varphi \ : R \to R \mid \varphi \text{ endomorfizem}\}$, je $(H, +, \circ)$ dioid.

Polmoduli

Definicija

Naj bo R polkolobar. *Levi R-polmodul* je komutativen monoid $(M, +)$ z aditivno identiteto θ, na katerem imamo definirano množenje s skalarjem $\cdot \ : R \times M \to M$, ki zadošča naslednjim pogojem za vsaka $\lambda, \mu \in R$ in vsaka $a, b \in M$:

1. $(\lambda\mu) \cdot a = \lambda \cdot (\mu \cdot a)$,
2. $\lambda \cdot (a + b) = \lambda \cdot a + \lambda \cdot b$ in $(\lambda + \mu) \cdot a = \lambda \cdot a + \mu \cdot a$,
3. $1 \cdot a = a$ in $\lambda \cdot \theta = \theta = 0 \cdot a$

Če je $\otimes$ na R komutativna, koncepta levega in desnega R-polmodula sovpadata.
Če je R dioid in $(M, +)$ kanonično urejen, pravimo, da je M (levi) moduloid.

Linearne preslikave in matrike nad polkolobarji

Tudi na polmodulih lahko definiramo linearne preslikave: Zahtevamo aditivnost in homogenost.
Nad polkolobarjem $(R, +, \cdot)$ lahko definiramo mxn matrike, za poljubna $m, n \in \mathbb{N}$. Pri tem seštevanje definiramo enako kot za matrike nad obsegi (po komponentah), množenje pa na sledeč način za $A \in M_{m\times n}(R), B \in M_{n\times l}(R)$:

$$A \times B = C \in M_{m\times l}(R);\ c_{ij} = \sum_{k=1}^{n}(a_{ik}b_{kj})\forall i \in \underline{m}\ \&\ \forall j \in \underline{l}$$

Baze Polmodulov

Definicija

Družina $X = (x_i)_{i \in I}$ elementov levega R-polmodula M je linearno neodvisna natanko tedaj, ko:

$$\forall I_1, I_2 \subset I; I_1 \cap I_2 = \emptyset : \langle X_{I_1} \rangle \cap \langle X_{I_2} \rangle = \{\theta\}$$

Če X ni linearno neodvisna, pravimo, da je linearno odvisna.

Definicija

Pravimo, da je X baza levega R-polmodula M, če je linearno neodvisna in generira M. Baza X za M je prosta, če lahko vsak element iz M enolično zapišemo kot linearno kombinacijo elementov iz X.

Kardinalnost Baz

Izrek

Če levi R-polmodul premore kako neskončno bazo, so vse njegove baze neskončne.

Definicija

Naj bo $(M, +, \cdot)$ levi polmodul nad polkolobarjem $(R, \oplus, \otimes)$ in denimo, da imamo dano neko množico vektorjev $V = (V_k)_{k \in K} \subset M$. Vektor x je *razcepen* nad $\langle V \rangle$ natanko tedaj, ko obstajata taka vektorja $y, z \in \langle V \rangle$, ki sta oba različna od x, da velja $x = y + z$. V primeru ko x ni razcepen, pravimo da je *nerazcepen*.

Trditev 1

Trditev

Naj no $(R, \oplus, \otimes)$ dioid in označimo z 0 nevtralni element za $\oplus$ ter z 1 nevtralni element za $\otimes$. Denimo dodatno, da velja: $r \oplus p = 1 \Rightarrow r = 1$ ali $p = 1$. Naj bo $(M, +, \cdot)$ R-moduloid, ki je kanonično urejen glede na $+$. Z $\propto$ označimo kanonično delno urejenost na M. Dodatno predpostavimo, da za $x, y \in M$, ki zadoščata pogojem $x \neq y \;\&\; y \neq \theta$ in $\lambda \in R$ velja:

$$y = \lambda \cdot y + x \Rightarrow \lambda = 1$$

Trdimo, da če veljajo omenjene predpostavke, za linearno neodvisno družino
$X = (x_i)_{i \in I}$ elementov iz M (kjer velja $x_i \neq \theta \forall i \in I$) velja, da je za vsak indeks $j \in I$ element x_j nerazcepen nad $\langle X \rangle$.

Trditev 2

Trditev

Denimo, da veljajo vse predpostavke trditve 1 in naj poleg tega velja še $r, p \in R : r \otimes p = 1 \Rightarrow r = 1$ in $p = 1$. Potem, če ima $(M, +, \otimes)$ bazo, je enolično določena.

Dokaz Trditve 2

- Denimo, da imamo dve bazi $X = (x_i)_{i\in I}$ in $Y = (y_j)_{j\in J}$.
- Ker sta X in Y linearno neodvisni, so po trditvi 1 vsi x_i in vsi y_j nerazcepni nad $\langle X\rangle = M = \langle Y\rangle$
- Izberemo poljuben $x_i \in X$ in zapišemo $x_i = \sum_{j\in J} \mu_j^i \cdot y_j$.
- $\exists j \in J : x_i = \mu_j^i \cdot y_j$ za nek $\mu_j^i \in R$ in $y_j \in Y$.
- Enako $\exists k \in I : y_j = \nu_k^j \cdot x_k$ za nek $\nu_k^j \in R$ in $x_k \in X$.
- sledi $x_i = (\mu_j^i \otimes \nu_k^j) \cdot x_k \Rightarrow k = i$
- Sledi $(\mu_j^i \otimes \nu_k^j) = 1$
- Sledi $\mu_j^i = 1$ in $\nu_k^j = 1$, posledično $x_i = y_j$
- Za vsak $x_i \in X$ smo našli $y_j \in Y$, da je $x_i = y_j$

Končne baze:

Med dvema končnima bazama lahko definiramo prehodno matriko.

Trditev

Naj ima levi R-polmodul M prosto bazo in naj bo $r(M) = r$ kardinalnost najmanjše množice, ki generira M. Naj bo T prosta baza za M. Potem so za bazo S za M naslednje trditve ekvivalentne:

1. S je prosta baza za M
2. $|S| = r$
3. Prehodna matrika med bazama T in S je enolično določena in obrnljiva.

Končne baze:

Posledica

V končno generiranem R-polmodulu M sta naslednji trditvi ekvivalentni:

1. Vse baze za M imajo enako kardinalnost
2. Vse baze za M so proste baze.

Trditev

Za vsak komutativen polkolobar R je kardinalnost vsake baze R^n enaka n natanko tedaj, ko je
$\max\{t \in \mathbb{N} \mid R\text{-polmodul } R \text{ ima bazo s } t \text{ elementi}\} = 1$

Bideterminanta kvadratne matrike

Definicija

Naj bo $\sigma \in S_n$ permutacija. Količino $w(\sigma) = \prod_{i=1}^{n} a_{i,\sigma(i)}$ imenujemo utež permutacije σ.

Definicija:

Naj bo A neka $n \times n$ matrika nad komutativnim polkolobarjem R. *Bideterminanta matrike* A je urejeni par $\Delta(A) = (det^+(A), det^-(A))$, kjer sta vrednosti $det^+(A)$ in $det^-(A)$ definirani na naslednji način:

$$det^+(A) = \sum_{\sigma \in Per^+(n)} w(\sigma)$$

$$det^-(A) = \sum_{\sigma \in Per^-(n)} w(\sigma)$$

Velja: $\Delta(A) = \Delta(A^\top)$.

Nekatere lastnosti bideterminante

- Če kak stolpec/vrstica v A vsebuje samo aditivno enoto 0, je $\det^+(A) = \det^-(A) = 0$
- Če ima matrika A dva identična stolpca oz. vrstici, je $\det^+(A) = \det^-(A)$
- Naj v polkolobarju $(R, \oplus, \otimes)$ velja, da so vsi elementi R okrajšljivi glede na $\oplus$ in vsi elementi $R \setminus \{0\}$ okrajšljivi za $\otimes$. Če so stolpci v $A \in M_n(R)$ linearno odvisni, velja $\det^+(A) = \det^-(A)$.
- Še več zanimivih latnosti na določenih tipih dioidov.

Bideterminanta produkta matrik

Izrek

Naj bosta A in B $n \times n$ kvadratni matriki nad komutativnim polkolobarjem $(R, \oplus, \otimes)$. Potem velja:

$$det^+(A \times B) = det^+(A) \otimes det^+(B) \oplus det^-(A) \otimes det^-(B) \oplus \gamma$$
$$det^-(A \times B) = det^+(A) \otimes det^-(B) \oplus det^-(A) \otimes det^+(B) \oplus \gamma$$

kjer je

$$\gamma = \sum_{f \in \acute{F}(n)} \sum_{\sigma \in Per^+(n)} \left(\prod_{i=1}^{n} a_{i,f(i)} \otimes b_{f(i),\sigma(i)} \right)$$

in $\acute{F}$ množica preslikav $f \ : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$, ki niso permutacije.

Permanenta kvadratne matrike

Definicija

Naj bo $\Delta(A)$ bideterminanta matrike $A \in M_n(R)$ nad polkolobarjem R. Permanenta matrike A je definirana kot:

$$\text{Perm}(A) = det^+(A) \oplus det^-(A) = \sum_{\sigma \in Per(n)}^{\oplus} w(\sigma)$$

Opazimo, da če v matriki A pomnožimo kak stolpec ali vrstico z neničelnim skalarjem λ_i, se potem tudi permanenta pomnoži z λ_i.

ε-determinanta kvadratne matrike

Poleg bideterminante lahko kvadratni matriki priredimo še t. i. ε-determinanto, ki nam tudi zna povedati kar veliko o dani matriki.

Definicija

Naj bo R polkolobar. Bijekcija ε na R se imenuje ε-*funkcija*, če velja:

- ε je idempotentna,
- ε je aditivna,
- $\varepsilon(a \otimes b) = a \otimes \varepsilon(b) = \varepsilon(a) \otimes b$ za vse $a, b \in R$
- $\varepsilon(a) = -a$ za aditivno obrnljive $a \in R$.

ε-determinanta kvadratne matrike

Defincija

Naj bo R komutativen polkolobar z ε funkcijo in $A \in M_n(R)$ ε-determinanto matrike A, označimo z $\det_\varepsilon(A)$ in definiramo s predpisom:

$$\det_\varepsilon(A) = \sum_{\sigma \in S_n}^{\oplus} \varepsilon^{t(\sigma)} \otimes (a_{1\sigma(1)} \otimes a_{2\sigma(2)} \otimes \ldots \otimes a_{n\sigma(n)})$$

Kjer je $t(\sigma)$ enako številu transpozicij permutacije σ in $\varepsilon^{(k)}(a) = \varepsilon^{(k-1)}(\varepsilon(a)); \varepsilon^{(0)}(a) = a$.

Več o tem v nalogi.

Karakteristični bipolinom

Definicija:

Naj bo A neka $n \times n$ matrika nad komutativnim polkolobarjem R. *Karakteristični bipolinom matrike* A je dvojica $(P_A^+(\lambda), P_A^-(\lambda))$, kjer sta $P_A^+(\lambda)$ in $P_A^-(\lambda)$ polinoma stopnje n v spremenljivki λ, definirana na naslednji način:

$$P_A^+(\lambda) = \sum_{q=1}^{n} \left(\left(\sum_{\substack{\sigma \in Part^+(n) \\ |dom(\sigma)|=q}} \left(\prod_{i \in dom(\sigma)} (a_{i,\sigma(i)}) \right) \right) \otimes \lambda^{n-q} \right) \oplus \lambda^n$$

$$P_A^-(\lambda) = \sum_{q=1}^{n} \left(\left(\sum_{\substack{\sigma \in Part^-(n) \\ |dom(\sigma)|=q}} \left(\prod_{i \in dom(\sigma)}^{n} (a_{i,\sigma(i)}) \right) \right) \otimes \lambda^{n-q} \right)$$

Karakteristični bipolinom

V posebnem primeru, ko v bipolinom vstavimo aditivno enoto 0, dobimo naslednje:

- $P_A^+(0) = \sum_{\substack{\sigma \in Part^+(n) \\ |dom(\sigma)|=n}} \left(\prod_{i=1}^n a_{i,\sigma(i)} \right)$
- $P_A^-(0) = \sum_{\substack{\sigma \in Part^-(n) \\ |dom(\sigma)|=n}} \left(\prod_{i=1}^n a_{i,\sigma(i)} \right)$

Ker je za $|dom(\sigma)| = n$ karakteristika $char(\sigma) = (-1)^n \otimes sign(\sigma)$, je za sode n $Part^+(n) = Per^+(n)$, za lihe n je pa $Part^+(n) = Per^-(n)$. V prvem primeru je torej $P_A^+(0) = \det^+(A)$ in $P_A^-(0) = \det^-(A)$, v drugem pa $P_A^+(0) = \det^-(A)$ in $P_A^-(0) = \det^+(A)$.

Cayley-Hamiltonov izrek nad polkolobarji

Izrek:

Naj bo A neka $n \times n$ matrika nad komutativnim polkolobarjem z nevtralnim elementom 0 in enoto 1 in naj bo $(P_A^+(\lambda), P_A^-(\lambda))$ bipolinom, ki pripada matriki A. Tedaj velja:

$$P_A^+(A) = P_A^-(A) \tag{1}$$

kjer sta $P_A^+(A)$ in $P_A^-(A)$ matriki, ki ju dobimo, če v $P_A^+(\lambda)$ in $P_A^-(\lambda)$ λ^{n-q} zamenjamo z A^{n-q}. Pri tem razumemo A^0 kot multiplikativno identiteto v polkolobarju $M_n(R)$.

Literatura:

- Yi-Jia Tan *Invertible matrices over semirings*, https://www.tandfonline.com/doi/abs/10.1080/03081087.2012.703191
- Yi-Jia Tan *Bases in semimodules over commutative semirings,*, https://www.sciencedirect.com/science/article/pii/S0024379513007234
- Yi-Jia Tan *Determinants of matrices over semirings*, https://www.tandfonline.com/doi/abs/10.1080/03081087.2013.784285
- Michel Gondran, Michel Minoux *Combinatorial Properties of (Pre)-Semirings*, https://www.researchgate.net/publication/319772435_Combinatorial_Properties_of_Pre-Semirings

Litaratura:

- Jonathan S. Golan *Semirings and their applications*,
- *Semiring*, `https://en.wikipedia.org/wiki/Semiring`