DAUGAVPILS UNIVERSITĀTE
Dabaszinātņu un matemātikas fakultāte
Matemātikas katedra
Bakalaura studiju programma "Matemātika"

Studiju kurss

Polinomu algebra

7.lekcija

Docētājs: Dr. P. Daugulis

2012./2013.studiju gads

Saturs

Lekcijas mērķis:

- vispārināt VAPG gadījumā dalīšanu ar atlikumu ar vienu vai vairākiem polinomiem,
- apgūt polinomiālu vienādojumu sistēmu risināšanas pamatfaktus.

Lekcijas kopsavilkums:

- VAPG var definēt polinomu dalīšanu ar atlikumu izmantojot termu un polinomu leksikogrāfisko sakārtojumu,
- PVS var mēģināt risināt izmantojot dalīšanu ar atlikumu un citas operācijas.

Svarīgākie jēdzieni: VAP redukcija, VAP dalīšana ar vienu un vairākiem dalītājiem, polinomiāla vienādojumu sistēma, S-polinoms.

Svarīgākie fakti un metodes: redukcijas īpašības, VAP dalījuma un atlikuma eksistence, PVS pētīšanas metode.

1. Vairāku argumentu polinomu dalīšana ar atlikumu

Sākot no šīs sadaļas $R = k$ ir lauks.

1.1. Redukcija

$f, g \in k[X_1, ..., X_n]$. Ja kāds f terms aX^μ dalās ar $\mathcal{H}(g)$, tad pārveidojumu

$$f \longrightarrow \underbrace{f - \frac{aX^\mu}{\mathcal{H}(g)} g}_{=\tilde{f}}$$

sauc par *redukcijas soli* un apzīmē ar

$$f \xrightarrow{g} \tilde{f}.$$

1.1. piemērs. $f = X_1^2 X_2 + X_2^2$, $g = X_1 X_2 - 1$.
$\tilde{f} = f - X_1 g = X_1 + X_2^2$.

1.1. teorēma.

1. Redukcijas solis

$$f \longrightarrow f - \frac{aX^{\mu}}{\mathcal{H}(g)} g = \tilde{f}$$

samazina polinomu leksikogrāfiskajā sakārtojumā:

$$f \succ \tilde{f}.$$

2. Ja $\mathcal{H}(g) \Big| \mathcal{H}(f)$, tad redukcijas solis

$$f \longrightarrow f - \frac{\mathcal{H}(f)}{\mathcal{H}(g)} g = \tilde{f}$$

samazina polinoma vecāko termu:

$$\mathcal{H}(f) \succ \mathcal{H}(\tilde{f}).$$

PIERĀDĪJUMS

1. Redzam, ka $\mathcal{H}(f - \tilde{f}) \prec aX^{\mu}$, jo aX^{μ} saīsinās.

2. Seko no 1. ■

$f \in k[X_1, ..., X_n]$, $G = \{g_1, ..., g_m\} \subseteq k[X_1, ..., X]$.

Teiksim, ka f *reducējas uz* $\widehat{f}$ mod G (apzīmē ar $f \xrightarrow{G} \widehat{f}$), ja $\exists$ redukcijas soļu virkne

$$f \xrightarrow{g_{i_1}} f_1 \xrightarrow{g_{i_2}} f_2 ... \xrightarrow{g_{i_l}} f_l = \widehat{f}.$$

Jebkuru (pabeigtu) redukcijas rezultātu apzīmēsim ar $\overline{f}^G$.

1.2. piemērs. $f = X_1^2 X_2 + X_2^2$, $g_1 = X_1 X_2 - 1$, $g_2 = X_2 + 1$.
$f \xrightarrow{g_1} X_1 + X_2^2 \xrightarrow{g_2} X_1 - X_2 \xrightarrow{g_2} X_1 + 1 = \overline{f}^{\{g_1, g_2\}}$.

1.2. Viens dalītājs

Ja ir doti divi VAP f un g, tad var vispārināt viena argumenta polinomu dalīšanas procedūru, ko var pamatot divos veidos:

- var atņemt no dalāmā f dalītāja g daudzkārtņus tā, lai atlikums būtu pēc iespējas mazāks leksikogrāfiskajā sakārtojumā;
- var veikt maksimāli garu f redukcijas soļu virkni ar g.

Dabiski ir izvēlēties šādu algoritmu: katrā solī reducēt lielāko f termu, kas dalās ar $\mathcal{H}(g)$.

1.3. piemērs. Izdalīsim $X_1^3X_2 + X_1^2 + X_1X_2$ ar $X_1X_2 + X_2^2$ virs $\mathbb{Q}$ vai $\mathbb{R}$. Iegūsim, ka

$$d = X_1^2 - X_1X_2 + X_2^2 + 1,$$
$$r = X_1^2 - X_2^4 - X_2^2.$$

1.2. teorēma. $f, g \in k[X_1, ..., X_n]$, $f \neq 0, g \neq 0$. Tad $\exists$ tieši viens polinomu pāris (d, r), kuram izpildās nosacījumi

1. $f = dg + r$;
2. $r = 0$ vai neviens r terms nedalās ar $\mathcal{H}(g)$.

PIERĀDĪJUMS
Eksistence
Algoritms.

Doti $f, g \in k[X_1, ..., X_n]$. Sākot ar f veiksim redukcijas izmantojot g tik ilgi, kamēr redukcijas ir iespējamas - kamēr kārtējās redukcijas rezultāts satur monomus, kas dalās ar $\mathcal{H}(g)$:

$$f \dashrightarrow \underbrace{f - d_1 g}_{r_1} \dashrightarrow \underbrace{(f - d_1 g) - d_2 g}_{r_2} \dashrightarrow ...$$

Algoritms apstāsies pēc galīga skaita soļu izpildes, jo pēc katras redukcijas izpildes atlikums samazinās leksikogrāfiskajā sakārtojumā.

Savelkot līdzīgos locekļus, iegūsim, ka

$$f - \Big(\sum_{i=1}^{m} d_i\Big) g = r \iff f = dg + r$$

kur $r = 0$ vai neviens r monoms nedalās ar $\mathcal{H}(g)$. ■

Vienīgums Pieņemsim, ka

$$f = dg + r = \tilde{d}g + \tilde{r},$$

kur r un $\tilde{r}$ apmierina teorēmas nosacījumu.

$\Longrightarrow\ r-\tilde{r}=g(\tilde{d}-d)\ \Longrightarrow\ \mathcal{H}(g)\Big|\mathcal{H}(r-\tilde{r})\vee\ g=0.$

$g=0\ \Longrightarrow\ r=\tilde{r}.$

$\mathcal{H}(g)\Big|\mathcal{H}(r-\tilde{r})\ \Longrightarrow$ vismaz viens no r vai $\tilde{r}$ termiem dalās ar $\mathcal{H}(g)$

$\Longrightarrow$ redukciju var turpināt attiecībā uz r vai $\tilde{r}$ - pretruna. ■

1.3. Vairāki dalītāji

Dots viens dalāmais f un vairāki dalītāji $g_1,...,g_m$.

Var veikt vairākus redukcijas soļus, iespējams, ar dažādiem dalītājiem, katrs redukcijas solis samazina atlikumu leksikogrāfiskajā sakārtojumā $\Longrightarrow$ redukcijas process apstāsies pēc galīga soļu skaita.

1.3. teorēma. $\{f,g_1,g_2,...,g_m\}\subseteq k[X_1,...,X_n]$, $f\neq 0$, $g_i\neq 0$.
Tad $\exists$ polinomu virkne $(d_1,d_2,...,d_m,r)$:

1. $f = d_1 g_1 + d_2 g_2 + ... + d_m g_m + r$;
2. $r = 0$ vai neviens r terms nedalās ar $\mathcal{H}(g_i)\ \forall\ i$.

PIERĀDĪJUMS Sākot ar f veiksim redukcijas izmantojot $g_1, .., g_m$ tik ilgi, kamēr redukcijas ir iespējamas - kamēr kārtējās redukcijas rezultāts satur monomus, kas dalās ar kādu $\mathcal{H}(g_i)$:

$$f \dashrightarrow \underbrace{f - d_1 g_{i_1}}_{r_1} \dashrightarrow \underbrace{(f - d_1 g_{i_1}) - d_2 g_{i_2}}_{r_2} \dashrightarrow ...$$

Algoritms apstāsies pēc galīga skaita soļu izpildes, jo pēc katras redukcijas izpildes atlikums samazinās leksikogrāfiskajā sakārtojumā.

Savelkot līdzīgos locekļus, iegūsim, ka

$$f - \sum_{i=1}^{m} d_i g_i = r \iff f = \sum_{i} d_i g_i + r,$$

kur $r = 0$ vai neviens r monoms nedalās ne ar kādu $\mathcal{H}(g_i)$. ■

r sauc par f *atlikumu* vai *redukciju* mod $(g_1, ..., g_m)$.

1.1. piezīme. Reducijas algoritmu var standartizēt vairākos veidos. Piemēram, katrā redukcijas solī izvēlamies leksikogrāfiski lielāko reducējamo monomu un mazāko reducējošo polinomu g_i.

1.4. piemērs. Atradīsim $X^4 + Y^4$ redukciju mod $(XY + 1, X^2 + Y)$ virs $\mathbb{Q}$ vai $\mathbb{R}$ (definējot $X \succ Y$).

1. Reducējam ar g_2: $r_1 := f - X^2 g_2 = -X^2 Y + Y^4$.
2. Reducējam ar g_1: $r_2 := r_1 - (-X)g_1 = X + Y^4$
3. Jāapstājas, jo X un Y^4 nedalās ne ar XY, ne ar X^2.

Tādējādi

$$r = X + Y^4 = f - X^2 g_2 - (-X)g_1$$

vai

$$\underbrace{X^4 + Y^4}_{f} = \underbrace{(-X)}_{d_1}\underbrace{(XY + 1)}_{g_1} + \underbrace{X^2}_{d_2}\underbrace{(X^2 + Y)}_{g_2} + \underbrace{(X + Y^4)}_{r}.$$

Mainot dalītāju kārtību, mainīsies rezultāts:

$$X^4 + Y^4 = (X^2 - Y)(X^2 + Y) + 0 \cdot (XY + 1) + \underbrace{(Y^4 + Y^2)}_{=r}.$$

1.2. piezīme. Dalīšanas rezultāts (atlikums) ir atkarīgs no dalītāju kārtības.

2. Polinomiālas vienādojumu sistēmas

2.1. Definīcija

Vienādojumu sistēmu

$$\begin{cases} f_1(X_1, ..., X_n) = 0, \\ ..., \\ f_m(X_1, ..., X_n) = 0, \end{cases} \quad \text{kur } f_i \in k[X_1, ..., X_n],$$

sauc par *polinomiālu vienādojumu sistēmu (PVS).*

Atrisināt PVS - atrast visus atrisinājumus $(a_1, ..., a_n)$.

Divas PVS $\mathcal{P}$ un $\mathcal{P}'$ sauc par ekvivalentām, ja tām ir vienādas atrisinājumu kopas.

2.1. piezīme. Kursa sākumā tika apskatītas PVS ar vienu nezināmo.

2.2. PVS seku vienādojumi

R - gredzens. Dota PVS P

$$\begin{cases} f_1(X_1, ..., X_n) = 0 \\ ... \\ f_n(X_1, ..., X_n) = 0 \end{cases}, f_i \in R[X_1, ..., X_n].$$

Vienādojumu $g(X_1, ..., X_n) = 0$ sauc par P *seku vienādojumu*, ja $\forall$ P atrisinājums $(t_1, ..., t_n)$ apmierina vienādojumu $g(t_1, ..., t_n) = 0$:

$$\begin{cases} f_1(X_1, ..., X_n) = 0 \\ ... \\ f_n(X_1, ..., X_n) = 0 \end{cases} \Longrightarrow g(X_1, ..., X_n) = 0.$$

2.1. piemērs. Vienkārša seku vienādojumu konstrukcija - kāpināšana naturālā pakāpē: $f(X_1, ..., X_n) = 0 \Longrightarrow f^n(X_1, ..., X_n) = 0$.

2.1. teorēma. Ir dota PVS P un tās seku vienādojums $g(X_1, ..., X_n) = 0$.

Tad $\left\{ \text{ P } \iff \begin{cases} \text{P} \\ g(X_1, ..., X_n) = 0 \end{cases} \right.$

PIERĀDĪJUMS Ja $(t_1, ..., t_n)$ apmierina PVS P, tad t apmierina arī papildināto PVS $\begin{cases} \text{P} \\ g(X_1, ..., X_n) = 0 \end{cases}$, pēc seku vienādojuma definīcijas.

Ja t apmierina papildināto PVS $\begin{cases} \text{P} \\ g(X_1, ..., X_n) = 0 \end{cases}$, tad $(t_1, ..., t_n)$ apmierina arī PVS P, kas satur mazāk vienādojumu. ■

2.3. PVS seku vienādojumu iegūšanas metodes

2.3.1. Dalīšana ar atlikumu

2.2. teorēma. R - gredzens. Ja ir dota PVS

$$\begin{cases} f_1(X_1, ..., X_n) = 0 \\ ... \\ f_n(X_1, ..., X_n) = 0 \end{cases}, f_i \in R[X_1, ..., X_n],$$

tad jebkuru divu polinomu f_i, f_j dalīšanas atlikums definē seku vienādojumu.

PIERĀDĪJUMS Pieņemsim, ka

$$f_i = d \cdot f_j + r.$$

Pieņemsim, ka $(t_1, ..., t_n)$ ir PVS atrisinājums.

Tad $\begin{cases} f_i(t_1, ..., t_n) = 0 \\ f_j(t_1, ..., t_n) = 0 \end{cases} \Longrightarrow$

$f_i(t_1, ..., t_n) = d(t_1, ..., t_n) f_j(t_1, ..., t_n) + r(t_1, ..., t_n)$

$\Longrightarrow \quad r(t_1, ..., t_n) = 0.$ ■

2.3.2. S-polinomi

Ja $f, g \in k[X_1, ..., X_n]$, tad pieņemsim, ka

$$\mathcal{H}(f) = aX^{\alpha},$$
$$\mathcal{H}(g) = bX^{\beta}.$$

Definēsim $X^\gamma = MKD(X^\alpha, X^\beta)$ un

$$S(f,g) = \left(\frac{X^\gamma}{\mathcal{H}(f)}\right) \cdot f - \left(\frac{X^\gamma}{\mathcal{H}(g)}\right) \cdot g.$$

Citiem vārdiem sakot, reizinām f un g ar tādiem termiem, lai vecākie locekļi būtu vienādi un pēc iespējas mazāki - vienādi ar f un g vecāko locekļu MKD, un saīsinātos.

$S(f,g)$ sauksim par f un g S-polinomu.

2.2. piemērs. Ja $f = XY + 1$ un $g = Y^2 - 1$, tad

$$S(f,g) = \frac{XY^2}{XY}(XY+1) - \frac{XY^2}{Y^2}(Y^2-1) = X + Y.$$

2.3. teorēma. R - gredzens. Ja ir dota PVS

$$\begin{cases} f_1(X_1, ..., X_n) = 0 \\ ... \\ f_n(X_1, ..., X_n) = 0 \end{cases}, f_i \in R[X_1, ..., X_n],$$

tad jebkuru divu polinomu f_i, f_j S-polinoms definē seku vienādojumu.

PIERĀDĪJUMS ■

2.4. PVS risināšanas metode

2.5. Vispārīgi apsvērumi

Risinot PVS ar vairākiem nezināmajiem var vadīties pēc šādiem apsvērumiem:

- vēlams noteikt *elementāros pārveidojumus*, kas maina, vienkāršo vienādojumus, nemainot atrisinājumu kopas,
- vēlams veikt elementāros pārveidojumus tā, lai
  - izslēgtu pēc iespējas vairāk nezināmos,
  - samazinātu vienādojumu pakāpes vai lielumu leksikogrāfiskajā sakārtojumā (multipakāpi).

1960.gados tika izstrādāta teorija, kas atrisināja šādas problēmas konstruktīvā veidā - Grobnera bāzu teorija (1965.g, B.Buhbergers).

2.5.1. Algoritms

1. Veikt dalīšanas ar atlikumu, lai iegūtu polinomus, kas ir pēc iespējas mazāki leksikogrāfiskajā sakārtojumā.
2. Atrast mazāko polinomu S-polinomus, atgriezties uz soli 1), ja nepieciešams.
3. Ja nav iespējams iegūt mazākus polinomus veicot dalīšanas un S-operācijas, tad apskatīt PVS, ko veido mazākie polinomi, mēģināt atrisināt šo sistēmu.

3. 7.mājasdarbs

3.1. Obligātie uzdevumi

7.1 Atrast f redukciju mod g, ja

(a) $f = X^3 + XY^2 + Y^3$, $g = X - Y$, virs $\mathbb{Q}$, $X \succ Y$,

(b) $f = X^6 + X^2Y^2Z^2 + Y^4Z^2$, $g = XYZ + 1$, virs $\mathbb{F}_2$, $X \succ Y \succ Z$.

7.2 Atrast vismaz vienu f redukciju mod (g_1, g_2), ja

(a) $f = X^3 + XY^2 + Y^3$, $g_1 = X + Y$, $g_2 = Y + 1$, virs $\mathbb{Q}$, $X \succ Y$,

(b) $f = X^3 + Y^3 + Z^3$, $g_1 = X + Y + Z$, $g_2 = Y + Z$, virs $\mathbb{F}_2$, $X \succ Y \succ Z$.

7.3 Mēģināt atrisināt dotās PVS.

(a) $\begin{cases} X^2 + Y^2 + Z^2 = 0 \\ X - Y + Z = 0 \\ X + Y^2 = 0 \end{cases}$, virs $\mathbb{R}$.

(b) $\begin{cases} XZ - 2Y + 1 = 0 \\ XYZ + YZ + Z = 0 \end{cases}$, virs $\mathbb{R}$.

(c) $\begin{cases} X^2 - 2Y + 1 = 0 \\ XY + Z - 1 = 0 X - Y - Z^2 = 0 \end{cases}$, virs $\mathbb{R}$.

3.2. Paaugstinātas grūtības un pētnieciska rakstura uzdevumi

7.4