Počítačová algebra

Alexandr Kazda

Univerzita Karlova

24. dubna 2020

Opakování: NSD polynomů v $\mathbb{Z}[x]$, $\mathbb{Q}[x, y]$ atd.

- Gaussovo lemma – souvislost NSD v $R[x]$ a $Q[x]$
- Euklidův algoritmus $\Rightarrow$ nárůst koeficientů
- Oprava z minule: Euklid nad $\mathbb{Q}[x]$ nevede k exponenciálnímu růstu, jenom asi kvadratickému
- Pseudodělení bez krácení ale dá exponenciální nárůst (základ asi $1 + \sqrt{2}$)
- Dělení mezivýsledků pomocí α_i udrží velikost koeficientů na uzdě
- $\text{res}(f, g) = \det(M(f, g))$

Rezultant

$$
\operatorname{res}(f,g) = \det \begin{pmatrix}
f_n & 0 & 0 & \dots & g_m & 0 & 0 & \dots & 0 \\
f_{n-1} & f_n & 0 & \dots & g_{m-1} & g_m & 0 & \dots & 0 \\
f_{n-2} & f_{n-1} & f_n & \dots & g_{m-2} & g_{m-1} & g_m & \dots & 0 \\
\vdots & & & \ddots & & & & & \\
f_0 & f_1 & f_2 & \ddots & \ddots & & & & \vdots \\
0 & f_0 & f_1 & \ddots & & \ddots & & & \\
0 & 0 & f_0 & \ddots & g_0 & g_1 & g_2 & \dots & g_{n-1} \\
0 & 0 & & \ddots & 0 & g_0 & g_1 & \dots & g_{n-2} \\
 & & \ddots & & & \ddots & & & \\
0 & 0 & 0 & f_0 & 0 & 0 & 0 & \dots & g_0
\end{pmatrix}
$$

- Determinant má smysl i nad obecným oborem integrity!
- Netriviální příklad: $\mathbb{Q}[y][x]$; prvky matice jsou polynomy v y

Rezultant

Theorem (Sylvesterovo kritérium)

Buď R gaussovský, Q jeho podílové těleso, f, g stupně > 1 nad R. PNTJE

1. *f, g jsou soudělné v $Q[x]$*
2. $\operatorname{res}(f, g) = 0$

- Důkaz $\Downarrow$: Z minule víme, že existují netriviální řešení rovnice $uf + vg = 0$
- To je homogenní lineární soustava daná maticí $M(f, g)^T$, tedy $\operatorname{res}(f, g) = \det(M(f, g)) = 0$
- $\Uparrow$ Pokud je determinant nula, existují netriviální u, v (malého stupně), že $uf + vg = 0$
- Minule jsme si ukázali, že to jde jen pro f, g soudělné v $Q[x]$

Více o rezultantu a Sylvesterově matici

Theorem

Buď R obor integrity, $f, g \in R[x]$ nekonstantní. Pak $\exists u, v \in R[x] \setminus \{0\}$, že $\deg u < \deg g$, $\deg v < \deg f$ a

$$\operatorname{res}(f, g) = uf + vg$$

- Jemnější výsledek než Sylvesterovo kritérium
- Důkaz: Vzpomeňte si v lineární algebře na adjungovanou matici
- Prvky $\operatorname{adj}(A)$ jsou determinanty podmatic A
- $A \operatorname{adj}(A) = \det(A)E$
- Toto lze dokázat bez dělení – tedy platí to ve všech okruzích

$\mathrm{res}(f, g) = uf + vg$

- Volme $A = M(f, g)^T$. Máme

$$M(f,g)^T \operatorname{adj}(M(f,g)^T) \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix} = \det(M(f,g)) \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ \det(M(f,g)) \end{pmatrix}$$

- Značme

$$\operatorname{adj}(M(f,g)^T) \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} u_{m-1} \\ \vdots \\ u_0 \\ v_{n-1} \\ \vdots \\ v_0 \end{pmatrix}$$

$\operatorname{res}(f,g) = uf + vg$

- Z rovností z předchozího slajdu máme:

$$M(f,g)^T \begin{pmatrix} u_{m-1} \\ \vdots \\ u_0 \\ v_{n-1} \\ \vdots \\ v_0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ \det(M(f,g)) \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ \operatorname{res}(f,g) \end{pmatrix}$$

- Přepneme z vektorů na polynomy
- Levá strana je $uf + vg$, pravá strana je konstantní polynom $\operatorname{res}(f,g)$

Souvislost rezultantu s kořeny polynomů

- Minule: f, g soudělné v $Q[x]$ právě když f, g mají společný kořen v $\overline{Q}$
- Rezultant je určený kořeny a vedoucími koeficienty!

Theorem (bez důkazu)

Buď R obor integrity, Q jeho podílové těleso, f, g polynomy stupňů $n, m \geq 1$ z $R[x]$. Nechť $\alpha_1, \ldots, \alpha_n$ jsou kořeny f, $\beta_1, \ldots, \beta_m$ kořeny g (násobné kořeny vyjmenujeme víckrát; kdyby kořeny chyběly, tak Q rozšíříme). Potom

$$\operatorname{res}(f, g) = \operatorname{lc}(f)^m \operatorname{lc}(g)^n \prod_{\substack{i=1,\ldots n \\ j=1,\ldots,m}} (\alpha_i - \beta_j)$$

- Důsledek: Rezultant je 0 $\Leftrightarrow$ f, g sdílí kořen

Příklad rezultantu přes kořeny polynomů

- Minule $\operatorname{res}(x^2 - 5x + 6, x - 6) = 12$ z definice
- $x^2 - 5x + 6$ má kořeny $2, 3$; vedoucí koeficient 1
- $x - 6$ má kořen 6; vedoucí koeficient 1
- $\operatorname{res}(x^2 - 5x + 6, x - 6) = (2 - 6)(3 - 6) = 4 \cdot 3 = 12$

Subrezultanty [podle Joachim von zur Gathen: Modern Computer Algebra]

- Z $M(f, g)$ lze vykoukat hodně věcí o Euklidově algoritmu pro f, g (klidně s pseudodělením)
- Stupně f, g buďte $n \geq m \geq 1$
- Značme (a_i, u_i, v_i) mezivýsledky v E. algoritmu
- Vstupy jsou $(a_0, u_0, v_0) = (f, 1, 0)$, $(a_1, u_1, v_1) = (g, 0, 1)$
- Značme $n_i = \deg a_i$; nechť $a_\ell \neq 0$, $a_{\ell+1} = 0$ (tj. a_ℓ je NSD)
- Normálně je $n_{i+1} = n_i - 1$; ale ne vždy...
- Kdy se číslo k vyskytne v posloupnosti $n_0 \geq n_1 > n_2 > n_3 > \cdots > n_\ell$?

Souvislost stupňů a_i, u_i, v_i

- Značme $n_i = \deg a_i$
- Vstupy jsou $(a_0, u_0, v_0) = (f, 1, 0)$, $(a_1, u_1, v_1) = (g, 0, 1)$

Theorem

Pro každé $i = 2, \ldots, \ell$ platí $\deg u_i = m - n_{i-1}$ *a* $\deg v_i = n - n_{i-1}$

- Důkaz indukcí dle i
- Pozorování: $n_{i-1} > n_i$ pro $i \geq 2$. Tedy pokud tvrzení platí, tak stupně u_i, v_i rostou počínaje $i = 1$
- $i = 2$; značme $q_1 = f \operatorname{div} g$; platí $\deg q_1 = n - m$
- $u_2 = 1$ má stupeň $0 = m - m = m - n_1$
- $v_2 = -q_1$ má stupeň $\deg q_1 = n - m = n - n_1$

$\deg u_i = m - n_{i-1}$ a $\deg v_i = n - n_{i-1}$

- Nechť tvrzení platí pro indexy $\leq i$
- Tedy $\deg u_{i-1} < \deg u_i$, $\deg v_{i-1} < \deg v_i$
- Značme $q_i = a_{i-1} \operatorname{div} a_i$; stupeň $n_{i-1} - n_i$
- Pak $u_{i+1} = u_{i-1} - q_i u_i$
- Víme $\deg u_{i-1} < \deg u_i$
- Tedy $\deg u_{i+1} = \deg(q_i u_i) = n_{i-1} - n_i + m - n_{i-1} = m - n_i$
- Podobně pro v_{i+1}

Příklad

- Volme $f = x^3 + 3x + 1$, $g = x^2 + 3$
- Běh Euklida (normální dělení)

$$\begin{aligned}(a_0, u_0, v_0) &= (x^3 + 3x + 1, 1, 0), n_0 = 3\\ (a_1, u_1, v_1) &= (x^2 + 3, 0, 1), n_1 = 2\\ (a_2, u_2, v_2) &= (1, 1, -x), n_2 = 0\end{aligned}$$

- Přeskočili jsme stupeň 1

Které stupně se objeví v Euklidovi?

Theorem

Bud Q těleso, $f, g \in Q[x]$ nekonstantní. Buďte $0 \leq k \leq m \leq n$, kde $\deg f = n$, $\deg g = m$. Pak se k neobjeví v posloupnosti stupňů Euklidova algoritmu pro f, g, právě když existují nenulové polynomy u, v, že

$$\begin{aligned} \deg u &< m - k \\ \deg v &< n - k \\ \deg(uf + vg) &< k \end{aligned}$$

- Pokud stupeň nulového polynomu bereme jako -1, tak pro $k = 0$ to je věta, kterou jsme začali sekci 13.
- Ukážeme si jenom $\Rightarrow$

Nechť k se neobjeví v Euklidovi

- Nejprve speciální případ $n_\ell > k$. Pak volme jako minule $u = g/a_\ell$, $v = -f/a_\ell$
- Bude $\deg u = m - n_\ell < m - k$, $\deg v = n - n_\ell < n - k$
- Zjevně $fu + gv = fg/a_\ell - fg/a_\ell = 0$
- Jinak existuje $i \geq 2$, že $n_i < k < n_{i-1}$
- Tvrdíme, že pak $u = u_i$, $v = v_i$ fungují
- Stupně: $\deg u_i = m - n_{i-1} < m - k$; $\deg v_i = n - n_{i-1} < n - k$
- Máme $fu_i + gv_i = a_i$; to má stupeň $n_i < k$

Příklad

- Pro $f = x^3 + 3x + 1$, $g = x^2 + 3$ chceme vyloučit jedničku
- Volme $u = 1$, $v = -x$; je $n = 3, m = 2$
- $\deg u < 2 - 1$, $\deg v < 3 - 1$
- Přitom $fu + gv = 1$ má stupeň $0 < 1$

Kde je rezultant?

- Podmínka

$$
\begin{aligned}
\deg u &\leq m-k-1 \\
\deg v &\leq n-k-1 \\
\deg uf+vg &\leq k-1
\end{aligned}
$$

  se dá zformulovat jako soustava lineárních rovnic pro $u_{m-k-1},\dots,u_0,v_{n-k-1},\dots,v_0$
- Poslední nerovnost napíšeme jako $n+m-k$ rovností pro nulové koeficienty
- Matice soustavy je podmatice $M(f,g)^T$