Počítačová algebra

Alexandr Kazda

Univerzita Karlova

15. května 2020

Opakování: Které stupně se objeví v Euklidovi?

Theorem

Bud Q těleso, $f, g \in Q[x]$ nekonstantní. Buďte $0 \leq k \leq n \leq m$, 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

$$\deg u < m - k$$
$$\deg v < n - k$$
$$\deg(uf + vg) < k$$

- Například pro $f = x^3 + 3x + 1$, $g = x^2 + 3$ umíme 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 $m + n - 2k$ proměnných $u_{m-k-1}, \ldots, u_0, v_{n-k-1}, \ldots, v_0$
- Poslední nerovnost napíšeme jako $m + n - 2k$ rovností pro nulové koeficienty
- Matice soustavy je podmatice $M(f, g)^T$

Sylveterova matice

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

Zahodíme: prvních a posledních k řádků a sloupce číslo 1 až k a $m+1$ až $m+k$

Matice pro rozhodování $k \in \{n_1, n_2, \ldots, n_\ell\}$

$$M_k(f,g)^T = \begin{pmatrix} f_n & 0 & \ldots & 0 & g_m & 0 & \ldots & 0 \\ f_{n-1} & f_n & \ldots & 0 & g_{m-1} & g_m & \ldots & 0 \\ f_{n-2} & f_{n-1} & \ldots & 0 & g_{m-2} & g_{m-1} & \ldots & 0 \\ \vdots & & \ddots & & & & \ddots & \\ \vdots & & & f_n & & & & g_m \\ \vdots & & \ddots & & & \ddots & & \\ f_{2k-m+1} & f_{2k-m} & \ldots & f_k & g_{2k-n+1} & g_{2k-n} & & g_k \end{pmatrix}$$

- Je to $(m+n-2k) \times (m+n-2k)$ čtvercová matice
- Řešení soustavy jsou právě $u_{m-k-1}, \ldots, u_0, v_{n-k-1}, \ldots, v_0$, že $uf + vg$ nemá členy stupně $\geq k$
- Netriviální řešení $\Leftrightarrow \det M_k(f,g) = 0$

Příklad

- Pro $f = x^3 + 3x + 1$, $g = x^2 + 3$

$$M_0(f,g)^T = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 3 & 0 & 3 & 0 & 1 \\ 1 & 3 & 0 & 3 & 0 \\ 0 & 1 & 9 & 0 & 3 \end{pmatrix}$$

- Determinant 5 $\Rightarrow$ polynom stupně 0 je NSD
- Teď zahoďme první a poslední řádek a sloupce 1 a 3...

Příklad

- Pro $f = x^3 + 3x + 1$, $g = x^2 + 3$ hledáme konstantní u, lineární v, že $uf + vg$ je konstantní

$$M_1(f,g)^T = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 3 & 3 & 0 \end{pmatrix}$$

- Determinant 0, tedy lineární polynom se neobjeví v E. algoritmu
- Vraťme se k M_0^T a zahoďme první a poslední dva řádky řádek a sloupce 1,2, 3,4...

Příklad

- Pro $f = x^3 + 3x + 1$, $g = x^2 + 3$ hledáme konstantní v, že $0f + vg$ je stupně ≤ 1

$$M_2(f, g)^T = (1)$$

- Determinant nenulový $\Rightarrow$ kvadratický polynom se objeví v E. algoritmu

Subrezultanty

- Buďte f, g polynomy stupňů $n \geq m$
- Čísla $\sigma_i = \det M_i(f, g)$ jsou subrezultanty polynomů f, g
- Pozor, v učebnici jsou subrezultanty nějaké polynomy (viz dále)
- $\sigma_0(f, g) = \mathrm{res}(f, g)$
- i jde od 0 do $\min(m, n)$
- Víme: $\sigma_i(f, g) \neq 0$ právě když se v E. algoritmu objeví polynom stupně i
- Pozorování: Polynomy v PRS jsou určené jednoznacně až na podobnost (násobení konstantou)
- Otázka: Lze polynomy z PRS nějak dostat z matic $M_i(f, g)$?

Fundamentální věta o PRS

- Nechť $\sigma_k(f,g) \neq 0$. Nechť $(p_{m-k-1}, \ldots, p_0, q_{n-k-1}, \ldots, q_0)$ je (jednoznačné) řešení rovnice

$$M_k(f,g)^T \begin{pmatrix} p_{m-k-1} \\ \vdots \\ p_0 \\ q_{n-k-1} \\ \vdots \\ q_0 \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ \sigma_k(f,g) \end{pmatrix}$$

- To je totéž jako požadovat, aby $fp + gq$ byl polynom stupně k s vedoucím koeficientem σ_k
- Značme (pro částečnou kompatibilitu s učebnicí) $S_k(f,g) = fp + gq$
- Nechť $f_1, f_2, \ldots$ je PRS; $\deg f_i = k$
- Pak f_i je stupně k a je tvaru $fu_i + gv_i$ pro $\deg u_i \leq m - (k+1)$, $\deg v_i \leq n - (k+1)$ (viz 24. dubna, slajd 11)

Fundamentální věta o PRS

- Víme: f_i je stupně k a je tvaru $fu_i + gv_i$ pro $\deg u_i \leq m - (k+1)$, $\deg v_i \leq n - (k+1)$ (viz 24. dubna, slajd 11)
- Tedy u_i, v_i jsou polynomy stupňů nejvýš $m - k - 1$ resp. $n - k - 1$, že $fu_i + gv_i$ má stupeň k
- Tedy

$$M_k(f,g)^T \begin{pmatrix} (u_i)_{m-k-1} \\ \vdots \\ (u_i)_0 \\ (v_i)_{n-k-1} \\ \vdots \\ (v_i)_0 \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ (f_i)_k \end{pmatrix}$$

- Matice $M_k(f,g)^T$ je regulární, tedy $fu_i + gv_i$ je násobek $S_k(f,g)$

Fundamentální věta o PRS

Věta (Fundamentální o PRS, zjednodušeno oproti učebnici)

Buď R gaussovský obor $f_1, \ldots, f_k$ PRS v $R[x]$. Značme $n_i = \deg f_i$. Potom pro $i = 3, \ldots, k-1$ platí $\sigma_{n_i}(f_1, f_2) \neq 0$ a $f_i \sim S_{n_i}(f_1, f_2)$.

- Například pro $f_1 = x^3 + 3x + 1$, $f_2 = x^2 + 3$ máme $f_3 = 1$, $n_3 = 0$ a dopočteme $S_0(f_1, f_2) = \sigma_0(f_1, f_2) = 5 \sim f_3$

Více o subrezulatntech

- Souvislosti s algebraickou geometrií (průsečíky křivek)
- V učebnici se říká subrezulatanty polynomům $S_k(f, g)$
- Polynomy $S_k(f, g)$ jsou tam definovány pomocí determinantů složitých podmatic; to je jenom Cramerov pravidlo pro soustavu $\deg(fp + gq) = k$
- Ze vzorečku pro $S_k(f, g)$ lze vydobýt rekuretní formuli pro subrezultantovou PRS
- Podobné úvahy pak vedou i na odhad růstu koeficientů pro výpočet NSD v $\mathbb{Q}$

14. Modulární algoritmus na výpočet NSD

- Jiná (a v praxi rychlejší) metoda
- Idea: Místo počítání v $\mathbb{Z}[x]$ a růstu koeficientů spočteme NSD v $\mathbb{Z}_p[x]$ a pak přejdeme zpátky do $\mathbb{Z}[x]$
- Budu psát $\%p$ pro „modulo p“; $f\%p$ zmodulí všechny koeficienty
- Tedy $f\%p \in \mathbb{Z}_p[x]$
- Reprezentace pro přechod zpátky

$$\mathbb{Z}_p = \{-\lfloor p/2 \rfloor, \ldots, 0, \ldots, \lfloor p/2 \rfloor\}$$

- Evidentně potřebujeme p dost velké, aby nám koefeicienty NSD „nepřetekly“
- Ale má to i další obtíže (smolná prvočísla)
- Pokročilejší verze (a dú): Počítáme modulo více malých prvočísel

Příklad

- Volme $f = x^3 - x^2 + x - 1 = (x^2 + 1)(x - 1)$,
  $g = x^3 + 2x^2 - x - 2 = (x - 1)(x + 1)(x + 2)$
- NSD je $x - 1$
- NSD v $\mathbb{Z}_2[x]$ je $(x + 1)^2$
- NSD v $\mathbb{Z}_3[x]$ je $x - 1$
- NSD v $\mathbb{Z}_5[x]$ je $(x - 1)(x + 2)$
- NSD v $\mathbb{Z}_7[x]$ je $x - 1$
- Co se stalo pro 2, 5?!

Vztah NSD v $\mathbb{Z}[x]$ a $\mathbb{Z}_p[x]$

Pozorování

Buďte $f, g \in \mathbb{Z}[x]$, p prvočíslo. Pak v tělese $\mathbb{Z}_p[x]$ platí

$$\mathrm{NSD}_{\mathbb{Z}[x]}(f,g)\%p \mid \mathrm{NSD}_{\mathbb{Z}_p[x]}(f\%p, g\%p)$$

- Buď $h = \mathrm{NSD}_{\mathbb{Z}[x]}(f,g)$. Pak $f = hr, g = hs$ v $\mathbb{Z}[x]$.
- Modulo p je homomorfismus, tedy

$$f\%p = (h\%p)(r\%p)$$
$$g\%p = (h\%p)(s\%p)$$

- Tedy $h \mod p$ dělí $f\%p$, $g\%p$
- Ale opačně to platit nemusí (viz $p = 5$ na předchozím slajdu)
- Pokud $\deg NSD_{\mathbb{Z}[x]}(f,g) = \deg NSD_{\mathbb{Z}_p[x]}(f,g)$, tak se od sebe oba NSD liší jenom násobením konstantou v $\mathbb{Z}_p[x]$

Šťastná to prvočísla

- Prvočíslo p je použitelné pro $f, g \in \mathbb{Z}[x]$, pokud $p \not| \mathrm{NSD}_{\mathbb{Z}}(\mathrm{lc}(f), \mathrm{lc}(g))$
- Použitelné prvočíslo je šťastné, pokud

$$\deg NSD_{\mathbb{Z}[x]}(f, g) = \deg NSD_{\mathbb{Z}_p[x]}(f, g)$$

- Použitelné prvočíslo je smolné, pokud

$$\deg NSD_{\mathbb{Z}[x]}(f, g) < \deg NSD_{\mathbb{Z}_p[x]}(f, g)$$

- V našem příkladě, byla všechna prvočísla použitelná, 2, 5 smolná a 3,7 šťastná
- Potíž: Jak poznat, že je p šťastné, když neznáme $\mathrm{NSD}_{\mathbb{Z}[x]}$?

Smolných prvočísel je konečně mnoho

Lemma

Buď p smolné pro f, g. Značme $h = \mathrm{NSD}_{\mathbb{Z}[x]}(f, g)$. Pak

$$p | \operatorname{res}\left(\frac{f}{h}, \frac{g}{h}\right).$$

- Důkaz: Ať p je smolné
- Modulo p máme pro vhodné r, s, t, kde $\deg r \geq 1$

$$\frac{f\%p}{h\%p} = rs \quad \frac{g\%p}{h\%p} = rt$$

- Přitom h dělí f, g v $\mathbb{Z}[x]$, takže můžeme psát

$$\frac{f}{h}\%p = rs \quad \frac{g}{h}\%p = rt$$

Smolná prvočísla dělí rezultant

Lemma

Buď p smolné pro f, g. Značme $h = \mathrm{NSD}_{\mathbb{Z}[x]}(f, g)$. Pak

$$p \mid \mathrm{res}\left(\frac{f}{h}, \frac{g}{h}\right).$$

- Dostáváme $r = \mathrm{NSD}_{\mathbb{Z}_p[x]}\left(\frac{f}{h}\%p, \frac{g}{h}\%p\right)$ stupně ≥ 1
- Proto $\mathrm{res}(\frac{f}{h}\%p, \frac{g}{h}\%p) = 0$
- Přitom rezulant je determinant, tedy rezultant v $\mathbb{Z}_p$ je rezultant v $\mathbb{Z}$ modulo p:

$$\mathrm{res}(\frac{f}{h}\%p, \frac{g}{h}\%p) = \mathrm{res}(f/h, g/h)\%p$$

- Tedy $p \mid \mathrm{res}(\frac{f}{h}, \frac{g}{h})$

Jak volit prvočíslo

- Pro dané f, g musí smolná prvočísla dělit nějaké konkrétní číslo, tedy smolných prvočísel je jenom konečně
- Není z toho tedy moc jasné, kolik vlastně těch smolných prvočísel je...
- Dobrá zpráva: Pro smolná prvočísla vypočtený NSD nebude dělit v $\mathbb{Z}$ jak f, tak g
- Můžeme tedy spočíst kandidáta na NSD a testovat, jestli jsme měli smůlu
- Další problém: Jak volit p, aby abs. hodnoty koeficientů $\mathrm{NSD}_{\mathbb{Z}[x]}(f, g)$ nebyly větší než $p/2$?
- Potřebujeme odhad na koeficienty $\mathrm{NSD}_{\mathbb{Z}[x]}(f, g)$

Landau-Mignottova mez

Věta (Landau-Mignottova mez)

Buďte $f, h \in \mathbb{Z}[x]$ takové, že $h|f$. Pak

$$\sum_{i=0}^{k} |h_i| \leq 2^k \left|\frac{h_k}{f_n}\right| \sqrt{\sum_{i=0}^{n} f_i^2},$$

kde k je stupeň h a n stupeň f.

- Důkaz dělat nebudeme, ale ukážeme si, jak nám to dá odhad na velikosti koeficientů NSD

Odhad mc(NSD(f, g))

- Uvažme $f, g, h \in \mathbb{Z}[x]$ stupňů n, m, k, že $h = \mathrm{NSD}_{\mathbb{Z}[x]}(f, g)$

Pozorování

Platí $h_k | f_n, g_m$, *tedy* $|h_k| \leq |\mathrm{NSD}_{\mathbb{Z}}(f_n, g_m)|$

- To plyne algoritmu pro dělení a toho, že $h | f, g$
- Také jistě $k \leq \min(m, n)$
- Potom máme z L-M meze pro f, h

$$\mathrm{mc}(h) \leq \sum_{i=0}^{k} |h_i| \leq 2^k \left|\frac{h_k}{f_n}\right| \sqrt{\sum_{i=0}^{n} f_i^2}$$

$$\leq 2^{\min(m,n)} |\mathrm{NSD}_{\mathbb{Z}}(f_n, g_m)| \frac{1}{|f_n|} \sqrt{\sum_{i=0}^{n} f_i^2}$$

- Podobně máme i odhad pro g, h

Odhad na mc(NSD(f, g))

- Spojením obou odhadů z L-M meze dostaneme

$$\mathrm{mc}(h) \leq 2^{\min(m,n)} \, |\mathrm{NSD}_{\mathbb{Z}}(f_n, g_m)| \, \min\left(\frac{1}{|f_n|} \sqrt{\sum_{i=0}^{n} f_i^2}, \frac{1}{|g_m|} \sqrt{\sum_{i=0}^{m} g_i^2} \right)$$

- Značme obludu na pravé straně jako $LM(f, g)$.
- Potřebujeme $p > 2LM(f, g)$, aby bylo jasné, jak přejít z $\mathbb{Z}_p[x]$ zpět do $\mathbb{Z}[x]$ i pro záporné koeficienty
- S takto velkým p nám stačí vždy brát reprezentatnty z $\{-\lfloor p/2 \rfloor, \ldots, 0, \ldots, \lfloor p/2 \rfloor\}$
- Vyhráli jsme? Ještě ne!

Problém vedoucího koeficientu

- Poslední potíž: $\mathbb{Z}_p$ je těleso, tedy máme celkem $p-1$ možných $\mathrm{NSD}_{\mathbb{Z}_p[x]}(f\%p, g\%p)$
- Různé volby NSD nám dají výrazně jiné polynomy v $\mathbb{Z}[x]$
- Problém vedoucího koeficientu: Jak určit $\mathrm{lc}(\mathrm{NSD}_{\mathbb{Z}[x]}(f,g))$?
- Pokud bychom vedoucí koeficient znali, volíme NSD v $\mathbb{Z}_p$, který má tento vedoucí koeficient modulo p (pro použitelné prvočíslo p)
- Značme $d = \mathrm{NSD}_{\mathbb{Z}}(\mathrm{lc}(f), \mathrm{lc}(g))$

Pozorování

Buďte $f, g \in \mathbb{Z}[x]$. *Pak* $\mathrm{lc}(\mathrm{NSD}_{\mathbb{Z}[x]}(f,g)) | d$.

- Mohli bychom zkoušet všechny dělitele d, ale komu by se chtělo faktorizovat d...

Návrat primitivních polynomů

- Předpokládejme, že $f, g \in \mathbb{Z}[x]$ jsou primitivní
- Pak $\mathrm{NSD}_{\mathbb{Z}[x]}(f, g)$ je také primitivní a jeho vedoucí koeficient dělí d
- Tedy vhodný násobek $\mathrm{NSD}_{\mathbb{Z}[x]}(f, g)$ má vedoucí koeficient d
- Bavíme se o nejvýše d-násobku $\mathrm{NSD}_{\mathbb{Z}[x]}(f, g)$
- Spočteme tedy $\mathrm{NSD}_{\mathbb{Z}_p[x]}(f \% p, g \% p)$ s vedoucím koeficientem d a vrátíme se do $\mathbb{Z}[x]$
- Značme výsledný polynom $h \in \mathbb{Z}[x]$
- Víme, že $h = c\,\mathrm{NSD}_{\mathbb{Z}[x]}(f, g)$ pro $|c| \leq d$; berme $\mathrm{pp}(h) = \mathrm{NSD}_{\mathbb{Z}[x]}(f, g)$
- Odhad na velikost p kvůli koeficientům h musíme kvůli d zvednout na $p > 2d \cdot LM(f, g)$

Konečně dokončení

- Spočetli jsme $h = c\,\mathrm{NSD}_{\mathbb{Z}[x]}(f, g)$
- Teď nám stačí spočíst primitivní část h
- Tím se vyloučí c, protože víme, že $\mathrm{NSD}_{\mathbb{Z}[x]}(f, g)$ musí být primitivní
- Pak otestujeme, zda výsledek dělí f i g
- Pokud ano, vyhráváme
- Pokud ne, bylo p smolné a musíme zvětšit p a restartovat

Modulární násobení nešikovně – algoritmus 21

Data: $f, g \in \mathbb{Z}[x]$ primitivní polynomy
Result: $\mathrm{NSD}_{\mathbb{Z}[x]}(f, g)$

1 $d := \mathrm{NSD}_{\mathbb{Z}}(\mathrm{lc}(f), \mathrm{lc}(g))$;
2 $p :=$ nejmenší prvočíslo $> 2d \cdot LM(f, g)$;
3 $h := \mathrm{NSD}_{\mathbb{Z}_p[x]}(f\%p, g\%p)$, aby $\mathrm{lc}(h) = d\%p$;
4 $h := \mathrm{pp}(h)$;
5 **if** $h | f, g$ **then**
6 | **return** h;
7 **else**
8 | zvol větší prvočíslo p, jdi na 3;
9 **end**

Správnost algoritmu 21

- Vzhledem k velikost $2d \cdot LM(f,g)$ bude $p > d$ vždy použitelné
- Pokud je p šťastné, tak $h = c\,\mathrm{NSD}(f,g)$ a $\mathrm{pp}(h) = \mathrm{NSD}(f,g)$
- Pokud je p smolné, tak h má větší stupeň než $\mathrm{NSD}(f,g)$, takže to zjistíme a restartujeme
- Protože smolných prvočísel je konečně mnoho, nakonec najdeme nějaké šťastné
- Je to nepraktické, protože naše prvočíslo bude hodně velké
- Příště si ukážeme, jak to dělat ještě lépe

Příklad

- $f = x^3 - x^2 + x - 1$, $g = x^3 + 2x^2 - x - 2$
- $d = 1$
- $LM(f, g) = 16$ (v učebnici jim vyšlo asi 25)
- $p > 2 \cdot 16 = 32$, tedy $p := 37$
- $h = x - 1$
- $h | f, g$, tedy vrátíme h