Algoritmy na mřížích

Faktorizace celočíselných polynomů s využitím LLL

8. 12. 2020

Berlekampův-Henselův algoritmus, předhled

1. Na vstupu je primitivní polynom $f \in \mathbb{Z}[x], \deg f \geq 1$
2. Budeme předpokládat, že f je bezčtvercový.
3. Najdeme prvočíslo p tak, aby $\mathrm{lc}(f)$ nebylo dělitelné p a $f \bmod p \in \mathbb{Z}_p[x]$ byl bezčtvercový.
4. Spočteme ireducibilní rozklad $f \bmod p$ v $\mathbb{Z}_p[x]$, $f \bmod p = u_1 u_2 \cdots u_r$, kde $u_1, \ldots, u_r \in \mathbb{Z}_p[x]$ ireducibilní po dvou neasociované a $u_2, \ldots, u_r$ monické.
5. Pro dostatečně vysoké k určíme rozklad $f \bmod p^k$ v okruhu $\mathbb{Z}_{p^k}[x]$: $f \bmod p^k = v_1 v_2 \cdots v_r$, kde $v_2, \ldots, v_r$ jsou monické, a $u_i = v_i \bmod p$ pro každé $i = 1, \ldots, r$.
6. Kombinací polynomů $v_1, \ldots, v_r$ se snažíme najít ireducibilní faktory f.

Kombinační fáze trochu podrobněji

1. $C := \{2, \ldots, r\}$, $t := 0$, $s := 0$
2. **while** $|C| > t$ **do:**
   - 2.1 $t := t + 1$
   - 2.2 pro t-prvkovou podmnožinu $I := \{i_1, \ldots, i_t\} \subseteq C$ **do**:
     - 2.2.1 $h := \mathrm{lc}(f) v_{i_1} \cdots v_{i_t} \mod p^k$
     - 2.2.2 $h := pp(h)$
     - 2.2.3 **if** $h \mid f$ **then** $s := s + 1$, $g_s := h$, $f := f/h$, $C := C \setminus I$
3. **return** $g_1, \ldots, g_s, f$

Náročnost kombinační fáze se odvíjí of čísla r. Pokud f je ireducibilní, je potřeba vyzkoušet $2^{r-1} - 1$ podmnožin C. V extrémním případě bude f ireducibilní a $r = \deg f$.

Norma polynomu (připomenutí)

Je-li $g \in \mathbb{Z}[x]$ polynom stupně $\leq d$, $g = \sum_{i=0}^{d} g_i x^i$ pak normou polynomu g rozumíme číslo $||g|| = \sqrt{\sum_{i=0}^{d} g_i^2}$. Definice nezávisí na volbě d, tedy máme normu zavedenou pro všechny prvky $\mathbb{Z}[x]$. Všimněme, si že $||g|| \leq \sum_{i=0}^{d} |g_i|$.

Tvrzení 14.6 (Landau-Mignottova mez)

Tvrzení

Máme celočíslené polynomy $f = \sum_{i=0}^{n} a_i x^i$, $h = \sum_{j=0}^{k} b_j x^j$, $b_k, a_n \neq 0$. *Pokud* $h \mid f$, *pak*

$$\sum_{j=0}^{k} |b_j| \leq 2^k \frac{|c_k|}{|a_n|} \sqrt{\sum_{i=0}^{n} a_i^2}$$

Důsledek

Necht' $h, f \in \mathbb{Z}[x]$ *jsou nenulové. Pokud* $h \mid f$, *je*

$$||h|| \leq 2^{\deg(h)} \frac{|\mathrm{lc}(h)|}{|\mathrm{lc}(f)|} ||f|| \leq 2^{\deg(f)} ||f|| \,.$$

Tvrzení 26.2

Tvrzení

Máme nekonstatní polynomy $f, g \in \mathbb{Z}[x]$, $\deg f = n$, $\deg g = k$ *a* $m \in \mathbb{N}$. *Předpokládejme, že existuje monický polynom* $u \in \mathbb{Z}_m[x]$ *stupně alespoň* 1 *takový, že v okruhu* $\mathbb{Z}_m[x]$ *je* $u \mid (f \bmod m)$ *a* $u \mid (g \bmod m)$. *Pokud* $||f||^k ||g||^n < m$, *pak je* $\mathrm{NSD}(f, g)$ *nekonstantní.*

Důkaz: Podle Sylvesterova kriteria (Věta 13.2) potřebujeme dokázat, že $\mathrm{res}(f, g) = 0$.
Podle Tvrzení 13.3 existují polynomy $r, s \in \mathbb{Z}[x]$ tak, že

$$\mathrm{res}(f, g) = rf + sg\,.$$

Polynom $\mathrm{res}(f, g) \bmod m \in \mathbb{Z}_m[x]$ je proto dělitelný (v okruhu $\mathbb{Z}_m[x]$) polynomem u. Naproti tomu $\mathrm{res}(f, g) \in \mathbb{Z}$, tedy $\mathrm{res}(f, g) \bmod m$ je konstatní polynom. Proto musí být

$$m \mid \mathrm{res}(f, g)\,.$$

Tvrzení 26.2, dokončení důkazu

Dále $\mathrm{res}(f,g)$ je determinant Sylvesterovy matice polynomů f a g. Řádky této matice tvoří vektory koeficientů vektorů polynomů

$$x^{k-1}f, x^{k-2}f, \ldots, xf, f, x^{n-1}g, x^{n-2}g, \ldots, xg, g$$

Tedy prvních k řádků matice má normu $||f||$ a zbylých n řádků matice má normu $||g||$. Podle Hadamardovy nerovnosti je

$$|\mathrm{res}(f,g)| \leq ||f||^k ||g||^n$$

Dle předpokladu tvrzení je $||f||^k ||g||^n < m$, musí proto být $\mathrm{res}(f,g) = 0$.

Aplikace pro faktorizaci polynomů, idea

Předpokládejme, že pro $m \in \mathbb{N}$ známe polynomy $v_1, v_2, \ldots, v_r \in \mathbb{Z}_m[x]$, $v_2, \ldots, v_r$ monické takové, že v $\mathbb{Z}_m[x]$ platí

$$f \bmod m = v_1 v_2 \ldots v_r .$$

V kontextu Berlekampova-Henselova algoritmu je pro $r = 1$ je f ireducibilní, předpokládejme proto $r > 1$.
Pokud f není ireducibilní, pro $i = 2, \ldots, r$ obsahuje množina

$$L_i := \{h \in \mathbb{Z}[x] \mid \deg(h) < \deg(f), v_i \mid (h \bmod m) \text{ v } \mathbb{Z}_m[x]\}$$

nenulový polynom normy nejvýše $2^{n-1}||f||$ (Tvrzení 14.6 resp. jeho důsledek aplikujeme pro vlastní faktor f dělitelný v $\mathbb{Z}_m[x]$ polynomem u_i).
L_i lze přirozeně chápat jako úplnou celočíselnou mříž v $\mathbb{R}^n$, kde $n = \deg(f)$. Označme $b_1, \ldots, b_n$ nějakou *LLL*-redukovanou bázi L_i. Pak $||b_1|| \leq 2^{(n-1)/2} 2^{n-1}||f|| = 2^{\frac{3(n-1)}{2}}||f||$ (podle Tvrzení 25.3 je $||b_1|| \leq 2^{(n-1)/2}||v||$ pro každý nenulový vektor $v \in L_i$).

Vektor b_1 odpovídá nenulovému polynomu $h \in L_i$ stupně nejvýše $n-1$, pro který platí

$$||h|| = ||b_1|| \leq 2^{\frac{3(n-1)}{2}} ||f|| \,.$$

Pokud bude navíc platit

$$||f||^{n-1} ||h||^n < m \,.$$

lze tento polynom h použít pro získání netriviálního dělitele f. Podle Tvrzení 26.2 je totiž $\mathrm{NSD}(f, h)$ nekonstantní polynom. Levou stranu nerovnosti $||f||^{n-1} ||h||^n < m$ lze odhadnout nezávisle na m:

$$||f||^{n-1} ||b_1||^n \leq ||f||^{n-1} \cdot 2^{\frac{3(n-1)n}{2}} ||f||^n = 2^{\frac{3(n-1)n}{2}} ||f||^{2n-1} \,.$$

Tvrzení 26.3

Tvrzení

Mějme $m, j \in \mathbb{N}$, $u \in \mathbb{Z}_m[x]$ monický polynom stupně $d \leq j$. Označme

$$L_{j,u} := \{h \in \mathbb{Z}[x] \mid \deg(h) < j, u \mid (g \bmod m) \text{ v } \mathbb{Z}_m[x]\}$$

Pak $L_{j,u}$ ve volná komutativní grupa s volnou bází

$$B_{j,u} := \{m, mx, mx^2, \ldots, mx^{d-1}, u, ux, \ldots, ux^{j-d-1}\}.$$

Vektory koeficientů polynomů $L_{j,u}$ tvoří mříž v $\mathbb{R}^j$, bázi této mříže tvoří vektory koeficientů polynomů z $B_{j,u}$.

Cvičení

Spočtěte determinant mříže $L_{j,u}$.

Tvrzení 26.3, důkaz

Máme dokázat, že každý prvek $L_{j,u}$ lze jednoznačně vyjádřit jako celočíselnou lineární kombinaci polynomů z $B_{j,u}$.
Polynomy $m, mx, mx^2, \ldots, mx^{d-1}, u, ux, \ldots, ux^{j-d-1}$ mají stupně $0, 1, 2, \ldots, d-1, d, d+1, \ldots, j-1$. Pouze triviální lineární kombinace těchto polynomů může být nulová.
Vezměme nyní $g \in L_{j,u}$. Tedy $g \in \mathbb{Z}[x]$ splňuje $\deg(g) < j$ a $u \mid (g \bmod m)$ v $\mathbb{Z}_m[x]$.
Tuto podmínku lze přepsat tak, že existují polynomy $r, s \in \mathbb{Z}[x]$ takové, že

$$g = ru + ms\,.$$

Tuto rovnost uvažujeme v okruhu $\mathbb{Z}[x]$. Polynom s můžeme vydělit se zbytkem (monickým) polynomem u:

$$s = qu + u_1\,,$$

kde $q, u_1 \in \mathbb{Z}[x]$ a přitom $\deg(u_1) < \deg(u)$. Dostaneme $g = (r + mq)u + mu_1$.

Tvrzení 26.3, dokončení důkazu

Označme $r_1 = r + mq \in \mathbb{Z}[x]$. Protože $r_1 u = g - mu_1$ je polynom stupně $< j$, musí být

$$\deg(r_1) < j - \deg(u) = j - d\,.$$

Napišme $r_1 = \sum_{i=0}^{j-d-1} z_i x^i$, $u_1 = \sum_{i=0}^{d-1} \check{z}_i x^i$, kde $z_i, \check{z}_i \in \mathbb{Z}$.
Pak $g = r_1 u + mu_1 = \sum_{i=0}^{j-d-1} z_i x^i u + \sum_{i=0}^{d-1} \check{z}_i m x^i$ ukazuje, že g je celočíselnou lineární kombinací prvků $B_{j,u}$.

Nalezení ireducibilního faktoru pomocí LLL

1. Postup je stejný jako v Berlekampově-Henselově algoritmu, pouze Henselův zdvih provedeme tolikrát, aby platilo $p^k = m > 2^{\frac{3(n-1)n}{2}} ||f||^{2n-1}$, kde $n = \deg(f)$.
2. Získáme tak $f \mod m = v_1 v_2 \dots v_r$
3. **for** $j = 2, 3, \dots, \deg(f)$ **do:**
   for $i = 2, \dots, r$
   spočti LLL-redukovanou bázi L_{j,v_i}
   $h :=$ polynom daný prvním vektorem nalezené báze
   $g := \mathrm{NSD}(h, f)$
   if $\deg(g) > 0$ **then GOTO** 5.
4. **return** 'f ireducibilní'
5. **return** g

Volba m zaručuje, že pokud f není ireducibilní, bude nalezen netriviální dělitel f.

Postup výpočtu zaručí, že jako první bude odhalen netriviální dělitel f nejmenšího možného stupně.

Pokud bychom chtěli získat ireducibilní faktorizaci f, můžeme celý postup zopakovat znovu s polynomem f/g.

Pár slov ke složitosti

Počet volaných LLL redukcí je nejvýše $(r-1)(n-1)$. Mříž L_{j,v_i} má dimenzi j a normy vektorů B_{j,v_i} odhadneme jm. Pokud LLL běží v čase $\mathcal{O}(j^6 \log(jm)^3)$, dostaneme pro $m \leq p.2^{\frac{3(n-1)n}{2}} ||f||^{2n-1}$ složitost $\mathcal{O}(j^6(\log(p) + \frac{3(n-1)n}{2}\log(2) + (2n-1)\log(||f||))^3)$.
I když dostaneme polynomiální algoritmus, pro praktické účely není příliš vhodný. Henselův zdvih zpravidla musíme provést na mnohem vyšší mocninu p.
Praktický algoritmus pro faktorizaci polynomů založený na LLL redukci publikoval až Mark van Hoeij v roce 2002.

Konec

D. Stanovský, L. Barto: *Počítačová algebra*, str. 176-178.
Doporučuji prostudovat příklad pro polynom $x^3 - 1$.