Algoritmy na polynomech — Cvičení 5

ondrej.jezil@email.cz

November 2023

1 Teoretická část

Gröbnerovy báze

1. Ukažte, že problém určit zda polynom $p(\overline{x})$ náleží danému ideálu $I \leq \mathbb{Q}[\overline{x}]$ je **coNP**-těžký?

   Převedeme úlohu určení, zda je výroková formule tautologie na úlohu určení, zda-li polynom náleží nějakému ideálu. Začněme s výrokovou formulí φ, její negaci lze obecně přepsat na ekvisplnitelnou 3-CNF, $\tilde{\varphi}$, tedy konjuknci disjunkcí nejvýše tří literálů. Za každou disjunkci literálů C z $\tilde{\varphi}$ zapíšu jako polynom p_C a do množiny I přidám polynom $p_C - 1$, nakonec do množiny I pridám polynomy $z^2 - z$, za každou proměnnou z. Podle Hilbertovy věty o nulách, tak $V(I) = \varnothing$ právě tehdy když $1 \in \langle I \rangle$. Lze nahlédnout, že $V(I) = \varnothing$ právě tehdy, když φ není tautologie.

Bezčtvercová faktorizace polynomů

2. Spočtěte bezčtvercovou faktorizaci polynomu $x^5 + 2x^4 - 2x^3 - 4x^2 + x + 2$ nad $\mathbb{Z}[x]$. $(x+2)(x^2-1)^2$

3. Spočtěte bezčtvercovou faktorizaci polynomu $x^7 + x^6 - x^5 - x^4 - x^3 - x^2 + x + 1$ nad $\mathbb{Z}[x]$. $(x^2+1)(x-1)^2(x+1)^3$

4. Spočtěte bezčtvercovou faktorizaci polynomu $x^6 + x^4 + x^2 + 1$ nad $\mathbb{Z}_2[x]$. $(x+1)^6$

5. Spočtěte bezčtvercovou faktorizaci polynomu $x^7 + x^6 + x^4 + x^3 + x + 1$ nad $\mathbb{Z}_3[x]$. $(x+1)(x+2)^6$

6. Nechť $\mathbf{R}$ je gaussovský obor charakteristiky 0 a nechť f je primitivní polynom z $\mathbf{R}[x_1, ..., x_m]$. Dokažte:

   - f je bezčtvercový $\iff \gcd(f, \frac{\partial f}{\partial x_1}, ..., \frac{\partial f}{\partial x_m}) = 1$;
   - Pokud $f = \prod_{i=1}^{k} h_i^i$ je bezčtvercový rozklad, potom

   $$\gcd(f, \frac{\partial f}{\partial x_1}, ..., \frac{\partial f}{\partial x_m}) = \prod_{i=1}^{k} h_i^{i-1}.$$

Postupujte podle tvrzení o polynomech jedné proměnné, zamyslete se, proč je potřeba největší společný dělitel s derivacemi podle všech proměnných, například u polynomu: x^2y

Aplikujte toto tvrzení na návrh algoritmu pro bezčtvercovou faktorizaci polynomů více proměnných nad gausovskými obory charakteristiky 0.

7. Formulujte a dokažte analogické tvrzení jako v minulé úloze, ale pro kladnou charakteristiku.