

Algoritmy na polynomech, cvičení 5

borysek@karlin.mff.cuni.cz

<https://karlin.mff.cuni.cz/~borysek/>

28. listopadu 2024

Gröbnerovy báze

1. Ukažte, že problém určit zda polynom $p(\bar{x})$ náleží danému ideálu $I \leq \mathbb{Q}[\bar{x}]$ je NP-těžký, pomocí redukce SATu na tento problém. Náповěda: Nejprve si to rozmyslete pro situaci v $\mathbb{C}[\bar{x}]$. Může se hodit Důsledek 22.3 ze skript.

Bezčtvercová faktorizace polynomů

2. Spočtete bezčtvercovou faktorizaci polynomu

- $x^5 + 2x^4 - 2x^3 - 4x^2 + x + 2$ nad $\mathbb{Z}[x]$.
- $x^7 + x^6 - x^5 - x^4 - x^3 - x^2 + x + 1$ nad $\mathbb{Z}[x]$.
- $x^6 + x^4 + x^2 + 1$ nad $\mathbb{Z}_2[x]$.
- $x^7 + x^6 + x^4 + x^3 + x + 1$ nad $\mathbb{Z}_3[x]$.

Na dělení polynomů a počítání NSD můžete využít **Sagemath**.

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

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

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

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

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