Algoritmy na polynomech — Domácí úkol 2

ondrej.jezil@email.cz

Prosinec 2023

1 Teoretická část

1.1 Redundance bezčtvercovosti

1. Ukažte, že pro monický polynom $f \in \mathbb{F}_q[x]$, a libovolný polynom $h \in \mathbb{F}_q[x]$ takový, že
$$h^q \equiv h \mod f,$$
platí
$$f = \prod_{a \in \mathbb{F}_q} \gcd(f, h - a),$$
i bez předpokladu, že f je bezčtvercový.

2. * Co bude výstupem Berlekampova algoritmu, pokud dostane na vstupu monický polynom $f \in \mathbb{F}_q[x]$, který není nutně bezčtvercový?

1.2 Faktorizace polynomů více proměnných

1. Nechť je $\mathbf{R}$ Gaussovský obor a nechť ϕ_d je zobrazení z $\mathbf{R}[x_1, \ldots, x_k]$ do $\mathbf{R}[y]$ definované následovně:
$$\phi_d(f) = f(y, y^d, y^{d^2}, \ldots, y^{d^{k-1}}).$$
Ukažte, že ϕ_d je okruhový homomorfismus a že restrikce ϕ_d na množinu
$$\{f \in \mathbf{R}[x_1, \ldots, x_k]; \deg_{x_i} f < d \text{ pro každé } i\}$$
je bijekce.
Uvažte $f = x_1^2 x_2 + x_1 x_2^2 + x_1 + x_2 \in \mathbb{Z}[x_1, x_2]$ a ϕ_3 podle definice výše. Ukažte, jak lze f zrekonstruovat z $\phi_3(f)$.

2. * Předchozí pozorování je základem Kroneckerova algoritmu. Hlavní myšlenka je místo přímého faktorizování polynomu f faktorizovat $\phi_d(f)$ pomocí Berlekampova-Henselova algoritmu a potom z této faktorizace zrekonstruovat faktorizaci f. Zkuste napsat pseudokód tohoto algoritmu a spočítat jeho časovou složitost.

3. Použijte algoritmus z předchozího cvičení na naleztení ireducibilního rozkladu $f = x^2y^2 + xy^2 - x^2y + y - x - 1 \in \mathbb{Z}[x, y]$.

2 Výpočetní část

1. Implementujte Berlekampův algoritmus pro $\mathbb{Z}_2[x]$.
2. * Implementujte Berlekampův-Henselův algoritmus (zde můžete použít Berlekampův algoritmus zabudovaný v sage, Henselovo zdvihání ale implementujte sami).