Algebraic Algorithms

mykyta.narusevych@matfyz.cuni.cz

December 2022

1 Theoretical part

1.1 Redundancy of square-free factorization

1. Show that for a monic polynomial $f \in \mathbb{F}_q[x]$ and an arbitrary $h \in \mathbb{F}_q[x]$ such that

$$h^q \equiv h \mod f$$

it holds that

$$f = \prod_{a \in \mathbb{F}_q} \gcd(f, h - a)$$

even without the assumption that f is necessarily square-free.

2. * What will be the result of applying Berlekamp's algorithm on a monic polynomial $f \in \mathbb{F}_q[x]$ which is not necessarily square-free?

1.2 Towards factorization of multivariate polynomials

1. Let $\mathbf{R}$ be a gaussian domain and let ϕ_d be a mapping from $\mathbf{R}[x_1, ..., x_k]$ to $\mathbf{R}[y]$ defined as

$$\phi_d(f) = f(y, y^d, y^{d^2}, ..., y^{d^{k-1}}).$$

Show that ϕ_d is a ring homomorphism and the restriction of ϕ_d onto the set

$$\{f \in \mathbf{R}[x_1, ..., x_k] \mid \deg_{x_i} f < d \text{ for all } i\}$$

is a bijection.

Consider $f = x_1^2 x_2 + x_1 x_2^2 + x_1 + x_2 \in \mathbb{Z}[x_1, x_2]$ and ϕ_3 defined as above. Show how can one reconstruct f from $\phi_3(f)$.

2. * The above observation is the foundation of the Kronecker's algorithm. The main idea is that instead of trying to decompose a polynomial f directly inside $\mathbf{R}[x_1, ..., x_k]$ one instead decomposes an univariate polynomial $\phi_d(f)$ using Berlekamp - Hensel's method and then combines factors to reconstruct f's decomposition inside $\mathbf{R}[x_1, ..., x_k]$. Try to write a pseudocode of this algorithm and compute its time complexity.

3. Apply the above algorithm (or any other its specification) to find irreducible decomposition of $f = x^2y^2 + xy^2 - x^2y + y - x - 1 \in \mathbb{Z}[x, y]$.

2 Computational part

1. Implement Berlekamp's algorithm for $\mathbb{Z}_2[x]$.

2. * Implement Berlekamp - Hensel's algorithm (you can use sage's in-built functions to directly use Berlekamp's algorithm, although Hensel's lifting must be implemented from scratch).