Algebraic Algorithms

mykyta.narusevych@matfyz.cuni.cz

December 2022

1 Theoretical part

1. Let f be from $\mathbb{F}_q[x]$ and let

$$W = \{h \in \mathbb{F}_q[x] : \deg h < \deg f,\ h^q \equiv h \bmod f\}.$$

   Prove that W is a linear space over $\mathbb{F}_q$ directly without applying lemmas from the lecture.

2. Compute decomposition of $f = x^4+1 \in \mathbb{Z}_3[x]$ using Berlekamp's algorithm (do not forget to check whether f is square-free).

3. Using Berlekamp's method design an algorithm to test irreducibility of members of $\mathbb{F}_q[x]$. Compute its (time) complexity.

4. * Using (randomized) algorithms to find irreducible decompositions of polynomials it is possible to design efficient algorithms which find roots of the given polynomials. Why is it not a good idea to derive such an algorithm just using the deterministic version of the Berlekamp's method?

5. Apply Berlekamp's algorithm on $f = x^7 + 2x^5 + 2x^4 + x^3 + 2x + 2 \in \mathbb{Z}_5[x]$ (do not forget to check whether f is square-free).

6. * Where is the assumption that f is square-free used in the Berlekmap's factorization method? Is this assumption really necessary?

7. * Compute upper bounds on the probability that a randomly generated polynomial h of degree smaller than $\deg f$ has non-trivial common divisor with f (assume f is square-free and is a product of m different irreducible polynomials g_i of degree d over $\mathbb{F}_q[x]$).

2 Computational part

1. Verify 2 using sage.

2. Verify 5 using sage.