

Math 288X: Algorithms in Algebra and Number Theory

Fall 2021

Problem set #4

Let $\mu(n) = n \log n \log \log n$.

Problem 1 (Computing resultants). a) Let $f, g \in K[X]$ be polynomials with $f \neq 0$. Show that

$$\text{Res}(f, g) = \text{lc}(f)^{\deg(g) - \deg(g \bmod f)} \cdot \text{Res}(f, g \bmod f),$$

where $\text{lc}(f)$ is the leading coefficient of f .

b) Assuming that arithmetic in K can be done in $\mathcal{O}(1)$, show that you can compute the resultant of polynomials $f, g \in K[X]$ of degree at most n in time $\mathcal{O}(\mu(n) \log n)$ on an $\mathcal{O}(\log n)$ -bit RAM (for large n).

Problem 2 (Subresultants). a) Show that for nonzero polynomials $f, g \in K[X]$ of degrees n, m , the degree of $\gcd(f, g)$ is the smallest integer $0 \leq d \leq \min(n, m)$ such that the linear map

$$\varphi_d : K[X]_{< m-d} \times K[X]_{< n-d} \rightarrow K[X]_{n+m-2d}$$

sending (a, b) to $[(fa + gb)/X^d]$ is an isomorphism.

b) Denote the determinant of φ_d (with respect to the standard bases $(1, \dots, X^{e-1})$ of $K[X]_{< e}$) by $s_d(f, g)$. Assuming

$$f(X) = \prod_{i=1}^n (X - \alpha_i) \quad \text{and} \quad g(X) = \prod_{i=1}^m (X - \beta_i),$$

show that $s_d(f, g)$ is a homogeneous polynomial in $\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_m$ of degree $(n-d)(m-d)$.

Problem 3 (Primes in $\mathbb{F}_q[X]$). Let \mathbb{F}_q be a finite field and assume that we can perform arithmetic in \mathbb{F}_q in time $\mathcal{O}(1)$, and that the RAM is given a list of the elements of \mathbb{F}_q . Let $\tilde{\mu}$ be the Möbius function.

- a) Show that the number of elements of \mathbb{F}_q that are not contained in a proper subfield is $\sum_{d|n} \tilde{\mu}\left(\frac{n}{d}\right) q^d$.
- b) Show that the number of irreducible monic polynomials $f \in \mathbb{F}_q[X]$ of degree n is $\frac{1}{n} \sum_{d|n} \tilde{\mu}\left(\frac{n}{d}\right) q^d \asymp q^n/n$.
- c) Show that you can find all irreducible monic polynomials $f \in \mathbb{F}_q[X]$ of degree at most n in time $\mathcal{O}(q^n n)$ (for large n) on an $\mathcal{O}(n \log q)$ -bit RAM.
- d) Show that you can compute the determinant of an $n \times n$ -matrix whose coefficients are polynomials in $\mathbb{F}_q[X]$ of degree at most d in time $\mathcal{O}_q(n^{\omega+1} d \mu(\log(nd)))$ on an $\mathcal{O}_q(\log(nd))$ -bit RAM (for large n, d).