max planck institut informatik

SAARLAND UNIVERSITY
COMPUTER SCIENCE

Michael Sagraloff **Winter term 2014/15**

Computer Algebra

https://resources.mpi-inf.mpg.de/departments/d1/teaching/ws14/ComputerAlgebra

Assignment sheet 7 due: Wednesday, December 17

Exercise 1: Representation of subresultants as determinants (3 points)

Prove Lemma II.3.11.

Exercise 2: Applications of subresultants (6 points)

(a) Let

$$f = x^3 + 4x^2 - 2ax - a^2 \quad \text{and}$$
$$g = x^2 - 2a^2.$$

Choose a such that $\deg \gcd(f, g) = 1$.

(b) Determine the gcd of

$$f = x^2 + \Big(\frac{1}{10}\sqrt{5} - \frac{3}{10}\Big)x + \Big(\frac{3}{50}\sqrt{5} - \frac{7}{50}\Big) \quad \text{and}$$
$$g = 4x^2 + \Big(-\frac{1}{10}\sqrt{5} + \frac{3}{10}\Big)x + \Big(\frac{1}{25}\sqrt{5} - \frac{4}{25}\Big).$$

(c) Does there exist a value for a such that

$$\gcd(x^3 + ax - a^2 + 1,\ 4x^3 - ax + a^2 - a)$$

has degree larger than 1?

Exercise 3: The size of divisors of multivariate polynomials (4 points)

Let $f \in \mathbb{Z}[x_1, \ldots, x_k]$ be a multivariate integer polynomial for some fixed number k of variables. Denote its total degree by $n := \deg f$, and let τ be the maximum bitsize of its coefficients; that is,

$$f = \sum_{\substack{\alpha=(\alpha_1,\ldots,\alpha_k)\in(\mathbb{Z}_{\geq 0})^k,\\ \alpha_1+\cdots+\alpha_k\leq n}} a_\alpha \cdot x_1^{\alpha_1} \cdots x_k^{\alpha_k} \quad \text{with } a_\alpha \in \mathbb{Z} \text{ and } |a_\alpha| < 2^\tau.$$

Show that any divisor $g \in \mathbb{Z}[x_1, \ldots, x_k]$ of f has coefficients of bitsize $\tilde{O}(n + \tau)$.

Hints:

1. *Use that, for any fixed value $x_k = \lambda \in \mathbb{Z}$, we have that $g(x_1, \ldots, x_{k-1}, \lambda) \mid f(x_1, \ldots, x_{k-1}, \lambda)$, and use induction over k to bound the bitsize of $g(x_1, \ldots, x_{k-1}, \lambda)$.*
2. *Use Lagrange interpolation to recover $g(x_1, \ldots, x_{k-1}, x_k)$ from $g(x_1, \ldots, x_{k-1}, \lambda_j)$ for suitably chosen values λ_j.*

Exercise 4: Bivariate gcds (3 points + 3 bonus points)

(a) Let

$$f = y^m + a_{m-1}(x) \cdot y^{m-1} + \cdots + a_0(x) \quad \text{and}$$
$$g = y^n + b_{n-1}(x) \cdot y^{n-1} + \cdots + b_0(x)$$

be bivariate integer polynomials with coefficients $a_i, b_i \in \mathbb{Z}[x]$.

Show how to compute $\gcd(f, g) \in \mathbb{Z}[x, y]$ using subresultants!

(Hint: Consider f and g as polynomials in $F[y]$, where F is the field of fractions of $\mathbb{Z}[x]$, and use Theorem II.3.15.)

(b) **(Bonus)** Can you generalize this approach to arbitrary (i.e., not necessarily monic) polynomials $f, g \in \mathbb{Z}[x][y]$?