max planck institut informatik

SAARLAND UNIVERSITY
COMPUTER SCIENCE

Michael Sagraloff **Winter term 2017/18**

Computer Algebra

https://www.mpi-inf.mpg.de/departments/algorithms-complexity/teaching/winter17/comp-alg/

Assignment sheet 11 due: Monday, January 22

Exercise 1: Descartes' Rule of Signs (4 points)

Descarte's Rule of Signs states that, for a polynomial $f = a_0 + \cdots + a_n \cdot x^n \in \mathbb{R}[x]$, the number m of positive real roots of f (counted with multiplicities) is upper bounded by $v = \mathrm{var}(f)$ and that $m = v \mod 2$, where we define

$$\mathrm{var}(f) := \#\{(i,k) \in \{0,\ldots,n\}^2 : i < k,\ a_i a_k < 0,\ \text{and } a_j = 0 \text{ for all } j \text{ with } i < j < k\}$$

as the number of sign variations in the coefficient sequence of f.

(a) Show that, for an interval $I = (a, b)$, the mapping

$$\Phi : \mathbb{R} \mapsto \mathbb{R} : x \mapsto \frac{ax + b}{x + 1}$$

maps the positive real axis $\mathbb{R}^+$ one-to-one onto the interval I.

(b) Conclude from (a) and Descarte's Rule of Signs that

$$v_I := \mathrm{var}(f, I) := \mathrm{var}\left((x+1)^n \cdot f\left(\frac{ax+b}{x+1}\right)\right)$$

is an upper bound on the number m_I of real roots of f in I, and that $m_I = v_I \mod 2$. In particular, show that $v_I \leq 1$ implies that $m_I = v_I$.

Exercise 2: The Descartes method (4 points + 4 bonus points)

(a) Use the results from the first exercise to derive a subdivision algorithm to isolate all real roots of a square-free polynomial $f \in \mathbb{Z}[x]$. For this, consider recursive bisection as for the complex solver and use $\mathrm{var}(f, I)$ as an exclusion and inclusion test.

Hint: You may assume that, for small enough intervals I, it holds that $v_I \leq 1$. Notice that this is not true for polynomials with multiple real roots as each interval I containing such a root yields $\mathrm{var}(f, I) > 1$.

(b) Implement your algorithm (e.g. in Maple or Sage) and run your implementation on

- dense polynomials (i.e. most of the coefficients are non-zero) with randomly generated integer coefficients
- sparse polynomials (i.e. most of the coefficients are zero) with randomly generated integer coefficients
- polynomials of the form $x^n - (a \cdot x - 1)^2$, with varying degree n and a positive integer a of varying bit size.

What do you observe?

Exercise 3: Newton-Rhapson Iteration (4 points + 4 bonus points)

Let α be a simple real root of a polynomial $f \in \mathbb{R}[x]$.

(a) Provide a bound $\epsilon_0 > 0$ in terms of the degree n of f and the separation $\mathrm{sep}(\alpha, f)$ of α (i.e. the minimal distance between α and any other (also complex) root of f) such that, for an arbitrary x_0 with $|x_0 - \alpha| < \epsilon_0$, the sequence

$$x_k := x_{k-1} - \frac{f(x_{k-1})}{f'(x_{k-1})} \quad \text{for } k \in \mathbb{N}_{>0}$$

converges against α under guarantee.

Hint: Use that $\frac{f'(x)}{f(x)} = \sum_{i=1}^{n} \frac{1}{x - z_i}$ *for all* x *with* $f(x) \neq 0$*, where* z_1 *to* z_n *denote the complex roots of* f*.*

(b) Can you even prove quadratic convergence? For this, you have to prove that there exists some constant C such that $|x_k - \alpha| < C \cdot |x_{k-1} - \alpha|^2$ for all k.

Exercise 4: Complexity of the $T_\star$-Test

Estimate the complexity of the $T_\star(\Delta, 1, f)$-Test for a polynomial $f \in \mathbb{Z}[x]$ of degree n and with coefficients of length L, and $\Delta = \Delta(m, r)$ a disk with dyadic center and radius of bitsize ℓ.