



Michael Sagraloff

Winter term 2014/15

## Computer Algebra

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

Assignment sheet 11

due: Wednesday, January 28

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

- (a) Finalize the proof of Theorem IV.1.2., that is, show that if all roots of a polynomial  $f(x) = \sum_{i=0}^n a_i x^i \in \mathbb{R}[x]$  are real, then  $\text{var}(a_0, \dots, a_n)$  equals the number of positive real roots of  $f$ .
- (b) Prove the one-circle theorem, that is, show that  $\text{var}(f, I) = 0$  if the one-circle region  $A_0 \subset I$  of  $I$  (as defined in Theorem IV.1.4) contains no root of  $f$ .

*Hint: You should first prove that  $\text{var}(a_0, \dots, a_n) = 0$  if each root of  $f$  has a real part that is smaller than or equal to 0. Then, consider the image of the half plane  $H := \{x + i \cdot y \in \mathbb{C} : x \leq 0\}$  under the Möbius transformation  $\Phi_I$ .*

### Exercise 2: Implementation of the Descartes method (4 points)

Implement the Descartes method 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: Analysis of the Descartes method (4 points + 4 bonus points for (c))

- (a) Derive a bound (of polynomial size in  $n$  and  $\tau$ ) on the number of iterations that is needed by the Descartes method to isolate the real roots of a polynomial  $f \in \mathbb{Z}[x]$  of degree  $n$  with coefficients of bit size  $\tau$ .
- (b) Derive a bound on the number of bit operations that is needed in each iteration and provide a bit complexity bound for the overall algorithm that is polynomial in  $n$  and  $\tau$ .
- (c) Can you even give a bound of size  $\tilde{O}(n\tau)$  in (a)? How does this affect the bit complexity of the Descartes method.

- *Hint: Consider the subdivision tree  $\mathcal{T}$  induced by the Descartes method, where the nodes of  $\mathcal{T}$  are the intervals produced by the algorithm. Notice that, for each non-terminal node  $I$  (i.e.  $\text{var}(f, I) \neq 0$ ), the one-circle region  $A_0$  of  $I$  contains at least one root. Now, consider a mapping  $\varphi$  from the set of non-terminal nodes to the roots of  $f$  such that each root  $z$  of  $f$  has at most  $O(\tau + \log \text{sep}(z, f))$  pre-images. Finally, use Theorem II.3.7.*

**Exercise 4: Newton-Rhapson Iteration (4 points)**

Let  $\alpha$  be a root of a polynomial  $f \in \mathbb{R}[x]$ . Provide a bound  $\epsilon_0 > 0$  in terms of the degree  $n$  of  $f$  and the separation  $\text{sep}(\alpha, f)$  of  $\alpha$  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  $\alpha$  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 roots of  $f$ .*