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 8 due: Monday, December 18

Exercise 1: Mignotte Polynomials (4 points)

For polynomials $f, g \in \mathbb{C}[x]$ and a disk Δ in complex space, Rouché's Theorem states that if

$$|f(z)| > |f(z) - g(z)| \text{ for all } z \in \partial\Delta,$$

with $\partial\Delta$ the boundary of Δ, then f and g have the same number of roots in Δ. Use Rouché's Theorem to show that, for $n \geq 8$, the so-called *Mignotte polynomial*

$$f(x) = x^n - (2^L \cdot x - 1)^2$$

has two distinct real roots x_1 and x_2 with $|x_1 - x_2| < 2^{-\frac{nL}{2}+1}$.

Hint: Use the fact that $g := -(2^L \cdot x - 1)^2$ has a root of multiplicity 2 at $m = 2^{-L}$. Then, consider a disc Δ centered at m and of suitable radius, and compare the values of $|f|$ and $|f - g|$ at the boundary of Δ.

Exercise 2: Specialization property of resultants (4 points)

(a) Let $\varphi : R \to R'$ be a ring homomorphism. Consider the canonical extension of φ to a ring homomorphism between the polynomial rings $R[x]$ and $R'[x]$ given by

$$\bar{\varphi} : R[x] \to R'[x], \quad a_n x^n + \cdots + a_1 x + a_0 \mapsto \varphi(a_n)\, x^n + \cdots + \varphi(a_1)\, x + \varphi(a_0).$$

Let f and g be polynomials in $R[x]$. Prove the following *specialization theorem for resultants:* If $\bar{\varphi}$ preserves the degrees of f and g (i.e., $\deg \bar{\varphi}(f) = \deg f$ and $\deg \bar{\varphi}(g) = \deg g$), then

$$\operatorname{Res}(\bar{\varphi}(f), \bar{\varphi}(g)) = \varphi(\operatorname{Res}(f, g)).$$

(b) Let $f := y^2 + 2 \cdot x^2 + x \cdot y - 4 \cdot x - 2 \cdot y + 2$ and $g := 3 \cdot x^2 + y^2 - 4 \cdot x$ be two polynomials in $\mathbb{Z}[x]$. Show that $f = g = 0$ has exactly one real solution and determine this solution.

Hint: Consider f and g as polynomials in $R[y]$, with $R = \mathbb{Z}[x]$. Then, use Part (a) with the ring homomorphism $\varphi : \mathbb{R} \mapsto \mathbb{R}$ that maps an $h \in \mathbb{Z}[x]$ to its value $h(x_0)$ at some fixed point $x_0 \in \mathbb{R}$. You should also use the fact that $f(x_0, y)$ and $g(x_0, y)$ have a common (complex) root if and only if their greatest common divisor is non-trivial.

Exercise 3: Conditions for multiple roots of polynomials (4 points)

- Show that $f = a_2x^2 + a_1x + a_0 \in \mathbb{C}[x]$ has a multiple root if and only if $a_1^2 - 4a_0a_2 = 0$.
- Give a corresponding formula for $f = a_3x^3 + a_2x^2 + a_1x + a_0 \in \mathbb{C}[x]$.

Exercise 4: The set of algebraic numbers is a field (6 points + 2 bonus points)

In this exercise, you will show that the set of algebraic numbers

$$\bar{\mathbb{Q}} \coloneqq \{\alpha \in \mathbb{C} : \text{there exists an } f \in \mathbb{Z}[x] \text{ such that } f(\alpha) = 0\} \subset \mathbb{C}$$

is a field.

(a) Let $\alpha, \beta \in \mathbb{C}$ and f and g be polynomials in $\mathbb{Z}[x]$ such that $f(\alpha) = 0$ and $g(\beta) = 0$. Show how to construct polynomials $h \in \mathbb{Z}[x]$ that satisfy

- $h(\alpha + \beta) = 0$ or $h(\alpha - \beta) = 0$, or
- $h(\alpha \cdot \beta) = 0$, or
- $h(1/\alpha) = 0$, or
- $h(\sqrt[k]{\alpha}) = 0$ for some $k \in \mathbb{N}_{\geq 2}$,

respectively.

Hint: Use resultants to show that the coordinates of any solution of a bivariate system $F(x, y) = G(x, y) = 0$, with $F, G \in \mathbb{Z}[x, y]$, is a root of a polynomial with integer coefficients. Then, derive a corresponding bivariate system in α and γ, where $\gamma = \alpha + \beta, \alpha \cdot \beta, 1/\alpha$, etc.

(b) Determine a polynomial $f \in \mathbb{Z}[x]$ with $f(\sqrt{3} - \sqrt[3]{3} + 1) = 0$.