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 6 due: Wednesday, December 10

Exercise 1: 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

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

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. Conclude that $\bar{\mathbb{Q}}$ is a field extension of $\mathbb{Q}$ that is closed under (rational) root extraction.

Bonus: What can you say about the size of $\bar{\mathbb{Q}}$?

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

Exercise 2: Yun's algorithm (4 points)

Prove that Yun's algorithm as presented in the lecture computes a square-free decomposition. Proceed as follows:

1. Let $h_1, \ldots, h_m \in F[x]$ be monic, square-free and pairwise coprime polynomials over a field F, and denote

$$h = h_1\, h_2 \cdots h_m \qquad \text{and} \qquad p = \sum_{i=1}^{m} \frac{c_i\, h_i' \cdot h}{h_i}$$

for some $c_i \in F$. Show that, in this situation,

$$\gcd(h, p - c\, h') = \prod_{c_j = c} h_j$$

for arbitrary $c \in F$.

2. Let $f \in F[x]$ be a polynomial. Prove by induction (simultaneously for both claims) that

(a) the polynomials g_i as computed in Yun's algorithm equal f_i, where $f = \prod f_j^j$ is the square-free decomposition of f, and

(b) $v_{i+1} = \prod_{i=1}^{m} f_i$ and $w_{i+1} = \sum_{j=1}^{m} \frac{(j-i)\, g_j' \cdot v_{i+1}}{g_j}$.

Exercise 3: Specialization property of resultants (4 points)

1. Let $\varphi : R \to R'$ be a ring homomorphism. There is a 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

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

2. A planar algebraic curve $\mathcal{C}_f$ (over the reals) is defined as the vanishing locus of a bivariate polynomial $f \in \mathbb{R}[x, y]$:

$$\mathcal{C}_f = \mathcal{V}_{\mathbb{R}}(f) = \{(x, y) \in \mathbb{R} \times \mathbb{R} : f(x, y) = 0\}, \quad \text{where} \quad f = \sum_{0 \le i+j \le n} a_{i,j} x^i y^j \in \mathbb{R}[x, y].$$

   Determine the intersection $\mathcal{C}_f \cap \mathcal{C}_g = \{(x, y) \in \mathbb{R} \times \mathbb{R} : f(x, y) = g(x, y) = 0\}$ of the curves $\mathcal{C}_f$ and $\mathcal{C}_g$ defined by

$$f(x, y) = 4y^2 + 8y + x^2 - 4x - 1 \qquad \text{and}$$
$$g(x, y) = y^2 + 2y + 4x^2 - 24x + 21.$$

   In other words, find the common solutions of the bivariate polynomial equation system $f(x, y) = g(x, y) = 0$.

   Hint: You may consider f and g as polynomials in $\mathbb{C}[x][y]$ and use the fact that the evaluation homomorphism

$$\varphi_a : \mathbb{C}[x] \to \mathbb{C}, \quad p \mapsto p(a)$$

   at any $a \in \mathbb{C}$ is a ring homomorphism between $\mathbb{C}[x]$ and $\mathbb{C}$.

Exercise 4: Conditions for multiple roots of polynomials (2 points)

- Show that $f = a_2 x^2 + a_1 x + a_0 \in \mathbb{C}[x]$ has a multiple root if and only if $a_1^2 - 4a_0 a_2 = 0$.
- Give a corresponding formula for $f = a_3 x^3 + a_2 x^2 + a_1 x + a_0 \in \mathbb{C}[x]$.