max planck institut informatik

Computer Algebra
Michael Sagraloff

Summer 2011
To be handed in on June, 7th.
Discussion on June, 8th.

Exercise 8

8.1 Horner's rule

Let R be a ring (commutative, with 1) and $u \in R$. Prove that Horner's rule not only computes the remainder $f(u)$ of a polynomial $f \in R[x]$ on division by $x-u$, but also the coefficients of the quotient $(f - f(u))/(x-u)$.

8.2 Homogeneous bivariate polynomials

We call a bivariate polynomial $f(x, y)$ *homogeneous* if the degree of all terms in f is the same. So $x^2 - y^2 - xy$ and $xy^3 - x^2y^2 + y^4$ are homogeneous, but $x^2 + y$ is not.

- Use `http://exacus.mpi-inf.mpg.de/cgi-bin/xalci.cgi` to plot the curves $x^2 - y^2 - xy = 0$, and $xy^3 - x^2y^2 + y^4 = 0$, and $x^2 - y^2 = 0$. Formulate a conjecture about the shape of vanishing sets of homogeneous polynomials.
- Show that any homogeneous polynomial factors into linear factors of the form $ax + by$ with $a, b \in \mathbb{C}$.

8.3 The shape of a curve near the origin

Let f be a bivariate polynomial, and let f^* be the homogeneous polynomial formed by the lowest order terms of f. For $f(x, y) = y^3 + x^2 - y^2 + 2xy$, f^* consists of all terms of degree 2, that is, $f^* = x^2 - y^2 + 2xy$.

- Experiment with different f's. Use `http://exacus.mpi-inf.mpg.de/cgi-bin/xalci.cgi` to plot the curves $f(x, y) = 0$ and $f^*(x, y) = 0$ near the origin. Formulate a conjecture.
- Prove the conjecture.

8.4 Chinese remaindering

Let $a_1, \ldots, a_r \in \mathbb{R}$ be pairwise distinct interpolation points with corresponding multiplicities $m_1, \ldots, m_r \in \mathbb{N}$ such that $\sum_{i=1}^{r} m_i = n + 1$.
Use the Chinese Remainder Theorem to show that, for each combination

$$b_{1,0}, \ldots, b_{1,m_1-1}, \ldots, b_{r,0}, \ldots, b_{r,m_r-1} \in \mathbb{R},$$

there is a unique polynomial $f \in \mathbb{R}[x]$ of degree n such that

$$f^{(j)}(a_i) = b_{i,j}$$

for all $i = 1, \ldots, r$ and $j = 0, \ldots, m_i - 1$.

8.5 Bounds on polynomial coefficients and root separation

(Bonus) Let $f = \sum_{i=0}^{n} a_i x^i = a_n \prod_{j=1}^{n}(x - \zeta_j) \in \mathbb{Z}[x]$ be square-free, with (complex) roots $\zeta_1, \ldots, \zeta_n$. We denote by $\operatorname{sep}(f) := \min\{|\zeta_i - \zeta_j| : i \neq j\}$ the *minimum root separation* of f, that is the minimal distance between distinct complex roots.
Now assume that the bitlengths of the coefficients of f are bounded by $\tau \in \mathbb{N}$, that is $|a_i| \leq 2^\tau$ for all i, j. Show that $\operatorname{sep}(f)$ is bounded from below by $2^{-\mathcal{O}(n(\tau + \log n))}$, that is there exists a $c \in \mathbb{R}_{>0}$ such that $\operatorname{sep}(f) \geq 2^{-cn(\tau + \log n)}$.

Hint 1: Recall exercise 4.3 and, in particular, the idea of the proof of part (iii).

Hint 2: Use the fact that the *Mahler measure* $\operatorname{Mea}(g) := |b_n| \cdot \prod_{i=1}^{n} \max\{1, |\xi_i|\}$ of a polynomial $g \in \mathbb{Z}[x]$ of degree n is bounded by $\|g\| = \sqrt{b_0^2 + b_1^2 + \cdots + b_n^2}$ from above, where the ξ_i's are the complex roots of g and the b_i's its coefficients.

Have fun with the solution!