max planck institut informatik

Computer Algebra
Michael Sagraloff

Summer 2011
To be handed in on May, 31th.
Discussion on June, 1st.

Exercise 7

7.1 Complex bitstream solver

In the lecture, we used a root solver for univariate polynomials with arbitrary algebraic coefficients for the lifting over critical fibers. In this exercise, we aim to show that there are algorithms better suited for the root isolation of those polynomials. In particular, they do not require the costly symbolic operations involved in the exact handling of non-rational coefficients.
In the following considerations, let $f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{R}[x]$, $a_n \neq 0$, be a univariate polynomial with real coefficients.

1. Show that

$$M := 1 + \max_{0 \leq i < n} \left\{ \frac{|a_i|}{|a_n|} \right\}$$

   is a *root bound* for f, that is, for each root α of f, it holds that $|\alpha| < M$.

   In particular, $g(x) := f(\lceil M \rceil x)$ has all its roots in the complex unit disc $\Delta_1(0)$.

2. Let $f \in \mathbb{R}[x]$ be a square-free polynomial. Assume that each coefficient a of f can be approximated arbitrarily well with dyadic numbers, that is, we can get values $\tilde{a} \in \mathbb{Z}[\frac{1}{2}]$ satisfying $|\tilde{a} - a| \leq \mu$ for arbitrary $\mu \in \mathbb{R}_{>0}$.

   In addition, you have the following theorem, which describes the quantitative relation between the roots of a polynomial $F = \sum_{i=0}^{n} F_i x^i$ and a μ-*approximation* $\tilde{F} = \sum_{i=0}^{n} \tilde{F}_i x^i$ of F:

   Theorem (Schönhage)**.** *Let F be a polynomial of degree n with roots $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ such that $|\alpha_i| < 1$. Let $\mu < 2^{-7n}$ and $\tilde{F}$ be a polynomial of degree n with complex roots $\tilde{\alpha}_1, \ldots, \tilde{\alpha}_n$ such that*

$$||F - \tilde{F}||_1 < \mu ||F||_1,$$

   where $||F||_1 = \sum_{i=0}^{n} |F_i|$. Then, up to a permutation of the $\tilde{\alpha}_i$'s, it holds that

$$|\alpha_i - \tilde{\alpha}_i| < 9 \sqrt[n]{\mu}.$$

   In particular, all roots of $\tilde{F}$ are in the complex unit circle $\Delta_1(0)$.

   Combine this information with the preceding parts to devise a root isolator for all complex roots of a polynomial $f \in \mathbb{R}[x]$ with real-valued coefficients.

Hints:

(a) Use CEVAL (your root solver from exercise 5.2) to find solutions of $\tilde{g} = 0$, where g is defined as in the first part of this exercise.

(b) Derive isolating regions for the roots of g from those of $\tilde{g}$.

(c) Consider a reasonable threshold for the minimal size of the boxes in the subdivision process.

3. **(Bonus)** How can you isolate the roots of an $f \in \mathbb{R}[x]$ if f is *not* square-free, but you know the degree $\deg \gcd(f, f')$ in advance?

7.2 Topological analysis of algebraic curves

1. Use the *implicit function theorem* and the result from exercise 7.1, part 1, to prove thefollowing theorem:

   Theorem (Delineability of algebraic curves)**.** *Let $f \in \mathbb{Z}[x, y]$ be square-free and $I \subset \mathbb{R}$ be an open interval not containing an x-critical coordinate of f. Then, f is* delineable *over I, which means that there exist $m \in \mathbb{N}$ and C^∞ functions $g_1, \ldots, g_m : I \to \mathbb{R}$ such that:*

   - $g_1(x_0) < g_2(x_0) < \cdots < g_m(x_0)$ *for all* $x_0 \in I$, *and*
   - $\mathcal{V}_\mathbb{R}(f) \cap (I \times \mathbb{R}) = \bigcup_{i=1}^{m} \{(x, g_i(x)) : x \in I\}$.

   In other words, f decomposes over I into m distinct function graphs.

2. Give the isotopy between the curve $\mathcal{C} = \mathcal{V}_\mathbb{R}(f)$ and its topology graph as determined in the lecture.

   Hint: First devise the isotopic transformation along a single fiber, then generalize to the complete graph.

7.3 Topology of a planar curve

Determine the topology of the planar curve $\mathcal{C} := \mathcal{V}_\mathbb{R}(x^3 - 2xy + 2y^2 + x^2)$, that is, compute an isocomplex (topology graph) for $\mathcal{C}$.

Have fun with the solution!