



A Descartes Algorithm for Polynomials with Approximate Coefficients

Kurt Mehlhorn

joint work with Arno Eigenwillig, Lutz Kettner, Werner Krandick,
Susanne Schmitt, and Nicola Wolpert

MPI für Informatik

Saarbrücken

Germany

Root Isolation



MAX-PLANCK-GESELLSCHAFT

- given a square-free polynomial $p(x) = \sum_{0 \leq i \leq n} p_i x^i$ with real coefficients
- compute isolating intervals for its real roots
- square-free = no double roots
- an interval $[a, b]$ is *isolating* if it contains exactly one root of p .
- **Theorem:** Isolating intervals can be computed in time polynomial in n and $\log \text{sep}(p)$.
- $\text{sep}(p) = \min \{ |x - y| ; x \neq y \text{ and } p(x) = p(y) = 0 \}$,
the *root separation of p*
- use σ to denote $2^{-\lfloor \log \text{sep}(p) \rfloor}$
- assumption: can approximate coefficients to any precision
- previously: coefficients are integers
- for integer coefficients, our algorithm has the same time bound as previous algs

On the Use of Isolating Intervals



MAX-PLANCK-GESELLSCHAFT

- can be refined: let $[a, b]$ be an isolating interval for a root of p
 - if $p(a) = 0$ or $p(b) = 0$ can shrink to a point
 - ow., let $m = (a + b)/2$. If $p(m) = 0$ shrink to a point, otherwise shrink to $[a, m]$ if $p(a)$ and $p(m)$ have opposite signs and to $[m, b]$ ow
- comparison of algebraic numbers: let $p(\alpha) = 0$ with isolating interval $[a, b]$ and $q(\beta) = 0$ with isolating interval $[c, d]$ compare α and β
 - if $[a, b]$ and $[c, d]$ are disjoint, answer is obvious.
 - otherwise, split $[a, b] \cup [c, d]$ into three intervals, and find the intervals containing α and β . if disjoint, answer is obvious
 - otherwise, we have the same isolating interval $[e, f]$ for both roots
 - let $h = \gcd(f, g)$ and $f_1 = f/h$ and $g_1 = g/h$.
 - either h has a root in $[e, f]$ and then $\alpha = \beta$
 - or (exclusively) f_1 and g_1 have roots in $[e, f]$ and then $\alpha \neq \beta$.
 - in the latter case refine intervals until they are distinct
- gcd-computations require exact coefficients; *I do not know how to do*

Descartes Rule of Signs



- $a = (a_0, \dots, a_n)$, sequence of real numbers
- *number of sign variations* $\text{var}(a)$, is the number of pairs (i, j) of integers with $0 \leq i < j \leq n$ and $a_i a_j < 0$ and $a_{i+1} = \dots = a_{j-1} = 0$
- $\text{var}(-3, 0, -2, 2, -1) = 3$.
- **Descartes' Rule of Signs:** $q(x) = \sum_{i=0}^n a_i x^i$, non-zero polynomial. Then $\text{var}(a)$ exceeds the number of positive real roots—counting multiplicities—by a non-negative, even integer.
- $\text{var}(a) = 0$, q has no positive real root
- $\text{var}(a) = 1$, q has exactly one positive real root
- $\text{var}(a) \geq 2$, ???, can we use bisection?
- yes, but it easier to apply bisection to $(0, 1)$ than to $(0, \infty)$
- $x \mapsto \frac{1}{1+x}$ maps $(0, \infty)$ to $(0, 1)$
- the zeroes of $q(x)$ in $(0, 1)$ correspond to the zeroes of $(1+x)^n q(\frac{1}{1+x})$ in $(0, \infty)$, i.e., can also estimate # of roots in $(0, 1)$.

The Bernstein Basis



- interval $[c, d]$, integer n
- for $0 \leq i \leq n$

$$B_i^n(x) = B_i^n[c, d](x) = \binom{n}{i} \frac{(x-c)^i (d-x)^{n-i}}{(d-c)^n}$$

i -th Bernstein polynomial of degree n with respect to interval $[c, d]$

- mostly, I will use $[c, d] = [0, 1]$
- Bernstein polynomials have many nice properties, e.g.,
 - $\sum_{0 \leq i \leq n} B_i(x) = \frac{1}{(d-c)^n} \sum_{0 \leq i \leq n} \binom{n}{i} (x-c)^i (d-x)^{n-i} = \frac{(d-c)^n}{(d-c)^n} = 1$
 - $B_i(x) \geq 0$ for $x \in [c, d]$
 - If $p(x) = \sum_{i=0}^n b_i B_i^n(x)$ and $\tilde{p}(x) = \sum_{i=0}^n \tilde{b}_i B_i^n(x)$ and $|\tilde{b}_i - b_i| \leq \varepsilon$ for all i , then for all $x \in [c, d]$

$$\left| \sum_i \tilde{b}_i B_i^n(x) - \sum_i b_i B_i^n(x) \right| \leq \varepsilon \sum_i |B_i^n(x)| = \varepsilon \sum_i B_i^n(x) = \varepsilon$$

The Bernstein Basis II



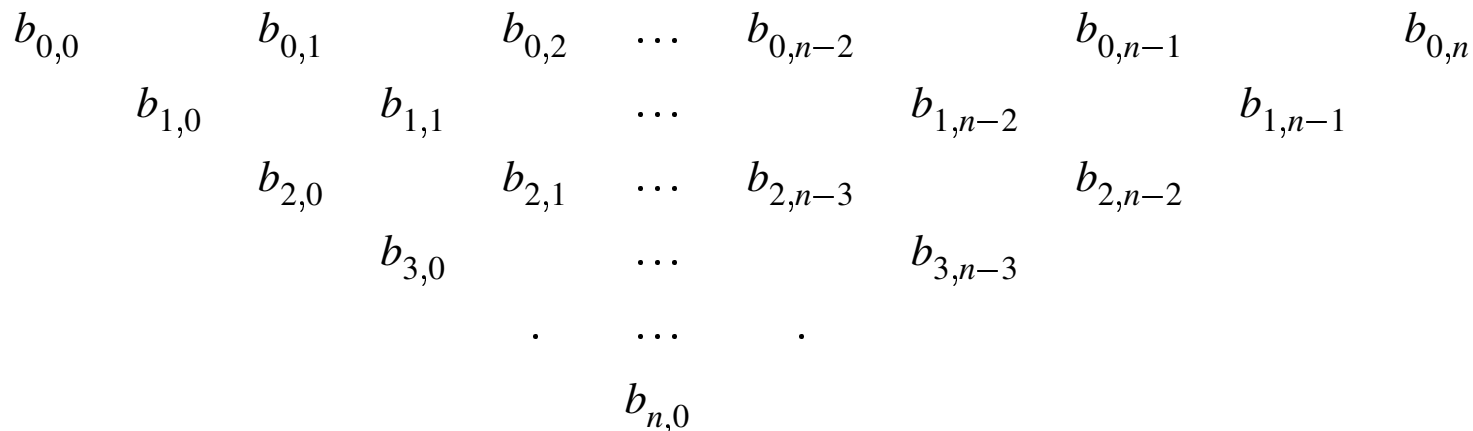
MAX-PLANCK-GESELLSCHAFT

- Any polynomial p of degree at most n can be written as $p(x) = \sum_{i=0}^n b_i B_i^n(x)$.
- Bernstein coefficients b_i depend on $[c, d]$.
- $p(c) = b_0$ and $p(d) = b_n$.
- $\text{var}(b)$ gives us information about number of zeroes of p in $(0, 1)$.
 - exceeds by an even non-negative integer
 - $\text{var}(b) = 0$, no root
 - $\text{var}(b) = 1$, exactly one root
 - if the disc centered at $1/2$ and passing through the origin contains no zero of p (real or complex), $\text{var}(b) = 0$.
 - if the union of the discs centered at $1/2 \pm i\sqrt{3}/6$ and passing through the origin contains exactly one root of p (this root is then guaranteed to be a real root) then $\text{var}(b) = 1$.

The Recursion



- $p(x) = \sum_i b_i B_i[c, d](x)$
- if $\text{var}(b) = 0$ return;
- if $\text{var}(b) = 1$, return $[c, d]$ as an isolating interval
- compute representations of $p(x)$ with respect to $[c, m]$ and $[m, d]$ where $m = (c + d)/2$ by means of de Casteljau triangle. Each $b_{j,i}$ is the average $(b_{j-1,i} + b_{j-1,i+1})/2$ of the two elements above it.



- if $p(m) = 0$ report $[m, m]$ as an isolating interval
- recurse on both sub-intervals.

A First Analysis



- recursion depth is approximately $\log \sigma$
- stopping criteria apply at intervals of length approximately $1/\sigma$.
- numbers grow by n bits in every node of the recursion tree (because of the averaging)
- so numbers grow to $L + n \log \sigma$ bits were L is the initial length
- need to be able to add coefficients and to determine their sign
- this is difficult to do for coefficients like π , $\ln 2$, $\sin(\pi/19)$.
- idea: compute with approximate coefficients: instead of b_i use $[b_i - \varepsilon, b_i + \varepsilon]$.
- our polynomials become interval polynomials
- $[a, b] + [c, d] = [a + c, b + d]$
- here $([a - \varepsilon, a + \varepsilon] + [b - \varepsilon, b + \varepsilon])/2 = [(a + b)/2 - \varepsilon, (a + b)/2 + \varepsilon]$, so we only need to compute with midpoints and simply interpret the numbers as intervals

Some Observations



- For a sequence of intervals $\mathbf{a} = (\mathbf{a}_0, \dots, \mathbf{a}_n)$, define its *set of potential sign variations*: $\text{var}(\mathbf{a}) = \{ \text{var}((a_0, \dots, a_n)) \mid a_i \in \mathbf{a}_i \text{ for } 0 \leq i \leq n \}$



$$\text{var}(([2, 3], [-1, 1])) = \{0, 1\},$$

$$\text{var}(([2, 3], [-1, 1], [2, 3])) = \{0, 2\},$$

$$\text{var}(([2, 3], [-1, 1], [-2, -1])) = \{1\}.$$

- The Descartes method hinges crucially on the ability to make the following decisions:
 - For all nodes in the recursion tree: Does the Descartes test yield 0, 1, or at least 2 sign variations?
 - For internal nodes of the recursion tree: Does the polynomial vanish at the interval midpoint? (This amounts to testing a certain coefficient for zero, see above.)

With an interval polynomial, making either decision may be impossible and hence the approach is doomed.

BUT, THERE IS HOPE



- Let $p_0(x)$ be a polynomial having all its roots in $(1/4, 3/4)$.
- $\alpha \in [-1/4, +1/4]$ uniformly at random.
- The polynomial $p_\alpha(x) = p_0(x + \alpha)$ has all its roots in $(0, 1)$.
- Apply the Descartes method to $p = p_\alpha$.
- *The probability that the Descartes method will inspect the sign of a vanishing coefficient is zero.*
- this holds because the coefficients of all intermediate polynomials can be viewed as polynomials in α .
- so the idea might work for p_α : if we approximate the coefficients by sufficiently small intervals, we should never encounter an interval whose sign cannot be determined
- what is sufficiently small? can we detect whether we are using small enough intervals?

The Key Observations



- \tilde{b} a vector of intervals of width ε each represented by its mid-point.
- \tilde{b}_i is determinate if $|\tilde{b}_i| > \varepsilon$
- \tilde{b}_i is *large* if $|\tilde{b}_i| > C\varepsilon$ and *small* otherwise. C some constant.
- \tilde{b}' and \tilde{b}'' are the sequences computed from \tilde{b} by de Casteljaou
- Let $C \geq 2^{n+1}$. If \tilde{b}_0 and \tilde{b}_n are large and positive, and if there is no negative determinate element in \tilde{b} , then all elements of \tilde{b}' and \tilde{b}'' are determinate and positive.

Proof: All entries $\tilde{b}_{j,i}$ in the de Casteljaou triangle are convex combinations of the inputs \tilde{b}_j and thus at least $-\varepsilon$. Furthermore, \tilde{b}_0 and \tilde{b}_n contribute one 2^j -th of their value to $\tilde{b}_{j,0}$ and $\tilde{b}_{j,n-j}$, respectively. Hence any element in \tilde{b}' and \tilde{b}'' is larger than $2^{-n}C\varepsilon + (1 - 2^{-n})(-\varepsilon) > \varepsilon$.

The Key Observations



- \tilde{b} a vector of intervals of width ε each represented by its mid-point.
- \tilde{b}_i is determinate if $|\tilde{b}_i| > \varepsilon$
- \tilde{b}_i is *large* if $|\tilde{b}_i| > C\varepsilon$ and *small* otherwise. C some constant.
- \tilde{b}' and \tilde{b}'' are the sequences computed from \tilde{b} by de Casteljau
- Let $C \geq 2^{n+1}$. If \tilde{b}_0 and \tilde{b}_n are large and positive, and if there is no negative determinate element in \tilde{b} , then all elements of \tilde{b}' and \tilde{b}'' are determinate and positive.
- Let $C \geq 8^n$. Suppose that \tilde{b}_0 is large and positive, \tilde{b}_n is large and negative, that $\tilde{b}'_n = \tilde{b}''_0$ at the tip of the de Casteljau triangle is large and negative, and that $1 \in \text{var}_\varepsilon(\tilde{b})$. Then $\text{var}_\varepsilon(\tilde{b}') = \{1\}$ and $\text{var}_\varepsilon(\tilde{b}'') = \{0\}$.

An Incomplete Algorithm with a Guarantee



MAX-PLANCK-GESELLSCHAFT

- given $\mathbf{p}(x) = \sum_{i=0}^n \mathbf{b}_i B_i^n(x)$ with $\mathbf{b}_i = [\tilde{b}_i - \varepsilon, \tilde{b}_i + \varepsilon]$.
- Procedure $Descartes_{\text{approx}}(\tilde{p} = \sum_{i=0}^n \tilde{b}_i B_i^n(x), \varepsilon)$:
 1. If \tilde{b}_0 or \tilde{b}_n is small, abort and signal failure.
Otherwise compute $V = \text{var}_{\varepsilon}(\tilde{b})$, the set of potential sign variations
 2. If $V = \{0\}$, return.
 3. If $V = \{1\}$, report an isolating interval and return.
 4. Invoke de Casteljaou's algorithm on \tilde{b} and recurse.
- Observe that $Descartes_{\text{approx}}$ recurses whenever V contains a value larger than 1.
- if alg does not fail, it terminates at most one level below the exact algorithm and returns isolating intervals
- if the alg fails, then $p(x)$ is small at one of the bisection points
so, this is what the randomization has to avoid

More on the Randomization



MAX-PLANCK-GESELLSCHAFT

- we need that our shifted polynomial has value at least $8^n \varepsilon$ at all bisection points (= interval endpoints)
- wishful thinking: make sure that the random shift keeps roots at a reasonable distance from the endpoints of isolating intervals.
- we have up to n roots and isolating intervals of length $1/\sigma$. So we cannot do better than $1/(n\sigma)$
- a random shift achieves distance $1/(4n\sigma)$ for all roots with probability at least $1/2$
- now we are done since a polynomial can be small only close to one of its roots

The Smith Bound



Let f be a square-free polynomial of degree n with complex roots ξ_1 to ξ_n and $\sigma \leq \text{sep}(f)$.

Let $\tilde{f}(x) = f(x) + e(x)$ be an approximation of f with error term $e(x) = \sum_{i=0}^n \varepsilon_i B_i^n[c, d](x)$ where $|\varepsilon_i| \leq \varepsilon$ for all i and some fixed $\varepsilon \geq 0$.

Let $\gamma \geq 0$ and $z \in [c, d]$.

If $|\tilde{f}(z)| \leq \gamma$, then $|f(z)| \leq \gamma + \varepsilon$, and there is a root ξ_i of f such that

$$|z - \xi_i| \leq \frac{n(\gamma + \varepsilon)}{\text{lcf}(f) \cdot \prod_{j \neq i} |\xi_j - \xi_i|} \leq \frac{n(\gamma + \varepsilon)}{\text{lcf}(f) \sigma^{n-1}} .$$

$\text{lcf}(f)$ is the lead coefficient of f (= the coefficient of x^n)

And ...



a few pages of tedious calculations finish the proof

Summary:

- can isolate the real roots of arbitrary real polynomials
- even if we cannot really compute with the coefficients
- only need to be able to approximate them
- running time is polynomial in the degree and the logarithm of the root separation of the input polynomial
- and this is also the approximation quality needed for the coefficients of the input polynomial