Root Isolation for one-variable polynomials

Yves Bertot
Joint work with
Assia Mahboubi and Frédérique Guilhot

July 2010

Introduction

- Solving systems of inequations and geometrical problems
- Does there exist (x, y) so that the following comparisons hold?

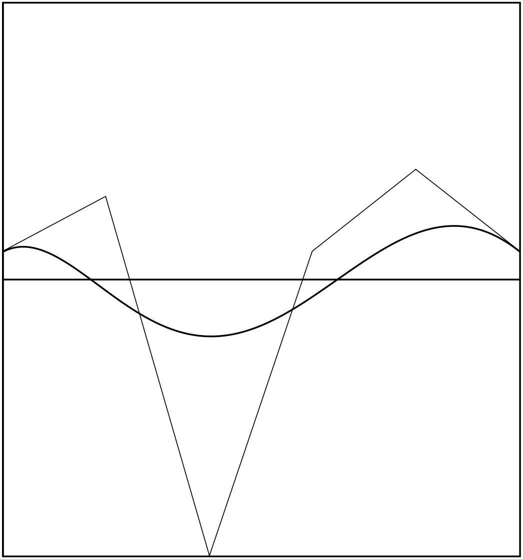
$$\begin{aligned} x^2 &\leq y \\ y &\leq 18 - 3x + 9x^2 \\ x &< 1 \end{aligned}$$

- Here find whether the roots of $18 - 3x + 10x^2$ are in some interval.
- More general applications in quantifier elimination and cylindrical decomposition
- Can be used to define algebraic numbers

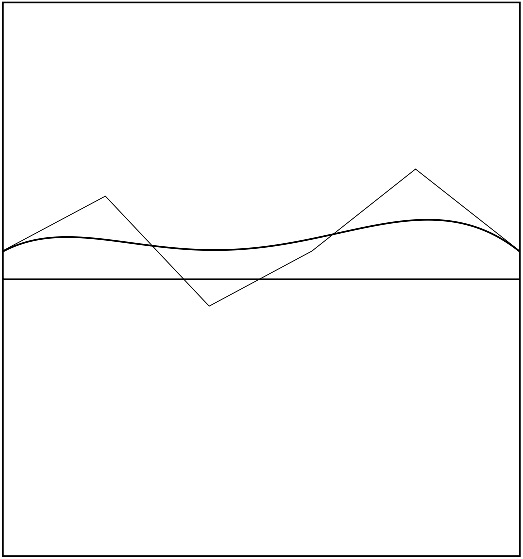
Method

- Bernstein coefficient approximate a polynomial's curve
- Discrete approximation
  - Associated to bounded intervals
- Exactly one sign change implies exactly one root in the interval
- No sign change implies no root in the interval
  - More than one sign change: no conclusion
- Refinement: cut the interval in halves and start again
  - Use a simple combinatorial algorithm

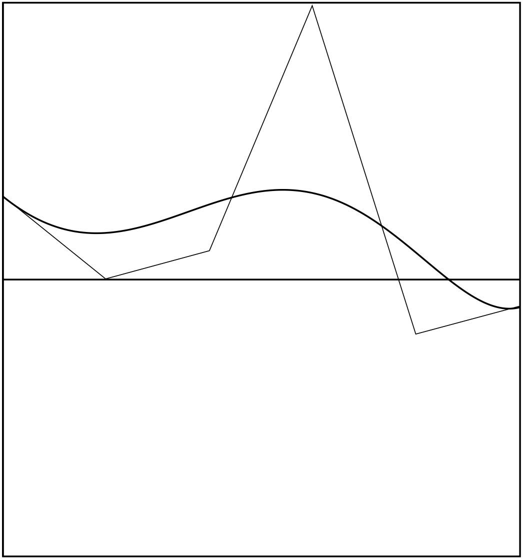
Geometric intuition: Bernstein



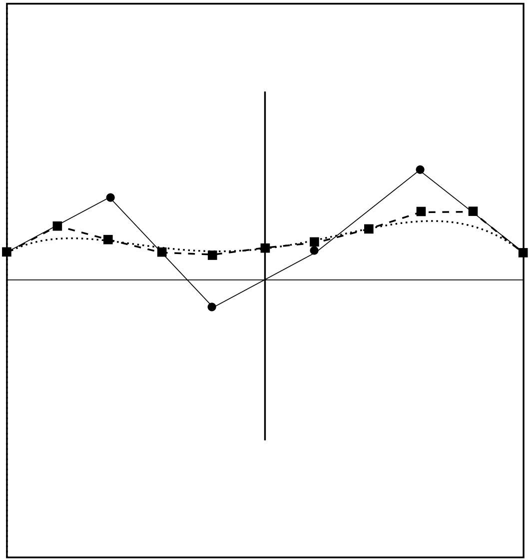
Geometric intution: False alert



Geometric intution: Exactly one root



Geometric intuition: interval splitting



Computing Bernstein coefficients

- Polynomial $a_0 + a_1 X + \cdots + a_n X^n$
- Bernstein coefficients for interval (l, r)

$$b_i = \sum_{j=0}^{n} \left(\begin{array}{c} j \\ n \end{array} \right) a_i \frac{r^j l^{n-j}}{r - l}$$

- Easy computation of Bernstein coefficients for the half intervals
  - de Casteljau's algorithm

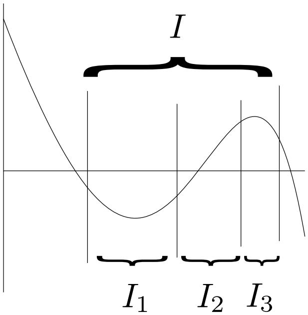
Correctness proof

- Relate Bernstein coefficients with plain coefficients of another polynomial
  - Using an automorphism
- Prove Descartes' law of signs (on a simple case)
- Establish correspondances between the roots of both polynomials
- Make the combinatorial proof for interval splitting

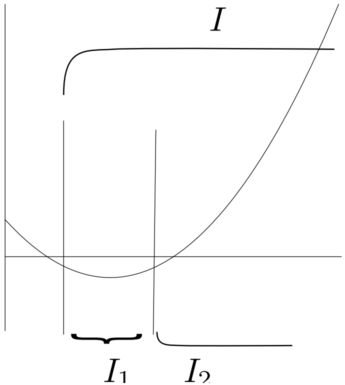
Constructive proof

- Use rational numbers
- New meaning of “having a root”
- Decompose interval into several parts
  - parts where the absence of root is guaranteed
  - parts where the polynomial changes sign, with monotonicity
- Replacement for the intermediate value theorem
  - Express that one can find a value that is arbitrary close to 0.
  - Upper bound on slopes for polynomials and bounded intervals
  - Deduce uniform continuity
  - take regularly spaced points and work in a discrete setting

Sufficient conditions for one root only



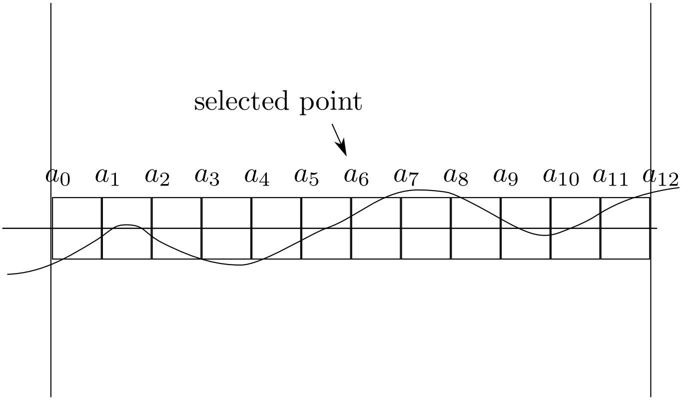
Sufficient conditions for one root only



Intermediate value theorem replacement

- The intermediate value theorem is used to produce a root
- Here, we only want to use to produce a two values x' and y'
  - The polynomial in these two values is close enough to 0
  - The polynomial is negative in x' and positive in y'
- Proof using an upper bound on slopes

Intermediate value theorem replacement



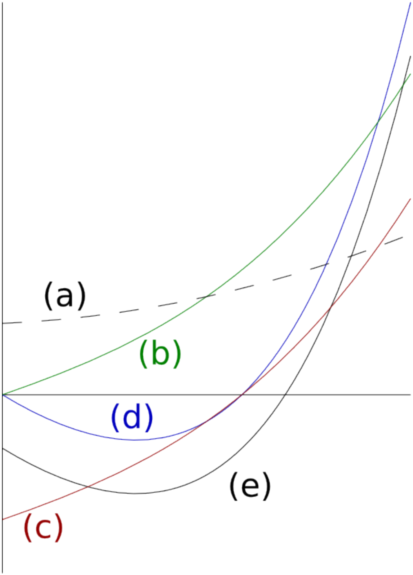
Descartes' law of signs

- A relation between sign changes and the number of positive roots
- The number of changes is larger than the number of roots
  - More precisely, the difference is a multiple of 2
  - Counting multiplicity of roots
- $(x-1)*(x^2+2) = x^3+x^2-2:$ 1 sign change
- $(x-1)^2 = x^2-2x+1:$ 2 sign changes
- $(x-1)(x-2) = x^2-3x+2:$ 2 sign changes
- If there is exactly one sign change, there is exactly one root
  - A specific proof for this corollary

Proving Descartes' corollary

- A finite state approach
- five kinds of polynomial curves,
- move from one kind to the other by apply Horner's scheme
- move depends on the sign of the added constant.

Geometric intuition for Descartes' corollary



More on Descartes

- Use interval decompositions,
- Assume P has a slope larger than $k > 0$ above a bound y
- When multiplying by X, new slope is $kx + P(x)$
- Use intermediate value replacement to make $P(x)$ negligible
- in a closed field we would simply use the existing root
- When adding a negative constant a, take a value so that $0 \leq P(x) < P(a)$

From Bernstein to Descartes

- Reversing the list of coefficients: nice trick!
- $P = rev(R) \Leftrightarrow P(x) = 1/x^n R(1/x)$
- Root of P in $(0, 1)$ correspond to roots of R in $(1, +\infty)$
- $R'(x) = R(1 + x)$ and use Descartes' corollary for R'
- For an arbitrary interval (l, r), use change of variable $y = rx + (1 - x)l$

Difficulties in formalization

- relate the slopes of P $P(1/x)$ and R
- Also use upper bounds of slopes

Interval splitting

- Remember Bernstein coefficients are obtained after translating, flipping, and affine variable change
- All linear invertible operations
- Call v the vector of Bernstein coefficients
- Call ϕ the function so that $\phi(p) = v$
- ϕ can also be seen as function mapping polynomials to polynomials
- consider $P_b'(n, l, r, k)$ the inverse image of X^k
- $phi(p) = \sum_{k=0}^{n} v_i X^k \Leftrightarrow p = \sum_i v_i(P_b'(n, l, r, k))$
- Bernstein coefficients are coefficients in a precise basis
- $P_b(n, l, r, k) = \left(\begin{array}{c} k \\ n \end{array} \right) x^{n-k}(1-x)^k$

Combinatorial computation

```
Variables l r : Qcb.

Fixpoint dc (b : nat -> Qcb) (n : nat) :=
  if n is i.+1 then
     fun j => l * dc b i j + r * dc b i j.+1
   else b.

Definition dicho' b i := de_casteljau b i 0.
Definition dicho p b i := de_casteljau b (p - i) i.
```

On Casteljau's algorithm

- Algorithm due to P. de Casteljau (work on CAD)
- Same scheme as for binomial coefficients
- Combinatorial proof, relying on the Bernstein basis

Conclusion

- Basic blocs for a decision procedure
- Start with an large bounded interval
- Apply dichotomy until 0 or 1 alternation in Bernstein coefficients
- Termination not proved yet (one known proof, using complex numbers)
- First proofs done with real numbers (not maintained)
- More recent proofs redone with `ssreflect`