Bernstein basis and real root isolation

ref: B Mourrain, M. Vrahatis, J.C. Yakoubsohn

Algorithms in real algebraic geometry
Basu Pollack Roy chapter 10

Budan-Fourier Theorem and Descartes's Law of Signs

Number of sign changes, $V(a)$, $a = a_0, \cdots, a_p$, in $\mathbb{R} \setminus \{0\}$:

$$V(a_0) = 0$$

$$V(a) = \begin{cases} V(a_1, \cdots, a_p) + 1 & \text{if } a_0 a_1 < 0 \\ \\ V(a_1, \cdots, a_p) & \text{if } a_0 a_1 > 0 \end{cases}$$

Extends to any finite sequence a of elements in $\mathbb{R}$ by dropping the zeros in a.

$\mathcal{P} = P_0, P_1, \ldots, P_d$ a sequence of polynomials in $\mathbb{R}[X]$, a be an element of $\mathbb{R} \cup \{-\infty, +\infty\}$.

Number of sign changes of $\mathcal{P}$ at a,

$$V(\mathcal{P}; a) = V(P_0(a), \ldots, P_d(a)).$$

a and b in $\mathbb{R} \cup \{-\infty, +\infty\}$,

$$V(\mathcal{P}; a, b) = V(\mathcal{P}; a) - V(\mathcal{P}; b).$$

$$\mathrm{Der}(P) = P, P', \ldots, P^{(p)},$$

~~$\mathrm{Der}(P)_\mu = P, P', \ldots, P^{(\mu)}$~~.

$n(P; (a, b])$ number of roots of P in $(a, b]$ counted with multiplicities.

Theorem 1 (Budan-Fourier theorem) *Let P be a univariate polynomial of degree p in $\mathbb{R}[X]$. Given a and b in $\mathbb{R} \cup \{-\infty, +\infty\}$*

$$n(P; (a, b]) \leq \mathrm{V}(\mathrm{Der}(P); a, b),$$

$\mathrm{V}(\mathrm{Der}(P); a, b) - n(P; (a, b])$ *is even.*

$$P = a_p X^p + \ldots + a_0$$

$V(P) = V(a_0, \ldots, a_p)$

$\mathrm{pos}(P)$ number of positive real roots of P, counted with multiplicity.

Theorem 2 (Descartes' law of signs)

$\mathrm{pos}(P) \leq V(P)$,

$V(P) - \mathrm{pos}(P)$ *is even.*

Descartes's particular case of Budan-Fourier since

$$V(P) = V(\mathrm{Der}(P); 0, +\infty).$$

Isolating Real Roots

P a polynomial of degree $\leq p$ in $\mathbb{R}[X]$. Characterization of the roots of P in $\mathbb{R}$ will be performed by finding intervals with rational end points. Based on Descartes's law of signs and Bernstein basis.

Bernstein polynomials of degree p for c, d

$$B_{p,i}(c,d) = \binom{p}{i} \frac{(X-c)^{p-i}(d-X)^i}{(d-c)^p},$$

for $i = 0, \ldots, p$.

$V(b)$ number of sign changes in the list b of coefficients of P in the Bernstein basis of c, d, $n(P;(c,d))$ number of roots of P in (c,d) counted with multiplicities.

Proposition 5

$$V(b) \geq n(P;(c,d)),$$

$$V(b) - n(P;(c,d)) \text{ is even.}$$

Proof: Follows from Descartes's law of signs.

The image of (c,d) under the translation by $-c$ followed by the contraction of ratio $d-c$ is $(0,1)$. The image of $(0,1)$ under the inversion followed by the translation by -1 is $(0,+\infty)$.

By the same transformation

$$\binom{p}{i} \frac{(X-c)^{p-i}(d-X)^i}{(d-c)^p}$$

becomes into $\binom{p}{i} X^i$. □

$$b = b_0, \ldots, b_p$$

related to the shape of the polynomial P on the interval c, d.

Control line of P on $[c, d]$: union of the segments $[M_i, M_{i+1}]$ for $i = 0, \ldots, p-1$, with

$$M_i = \left(\frac{ic + (p-i)d}{p}, b_i \right).$$

The graph of P goes through M_0 and M_p and the line M_0, M_1 (resp M_{p-1}, M_p) is tangent to the graph of P at M_0 (resp. M_p).

Control polygon of P on $[c, d]$:

convex hull of the points M_i for $i = 1, \ldots, p$.

Proposition 6 *The graph of P on $[c, d]$ is contained in the control polygon of P on $[c, d]$.*

Proof: Any line L defined by $Y = aX + b$, above all the points in the control polygon of P on $[c, d]$ is above the graph of P on $[c, d]$.

Express the polynomial $aX+b$ in the Bernstein basis, use

$$1 = \left(\frac{X - c}{d - c} + \frac{d - X}{d - c}\right)^p,$$

using

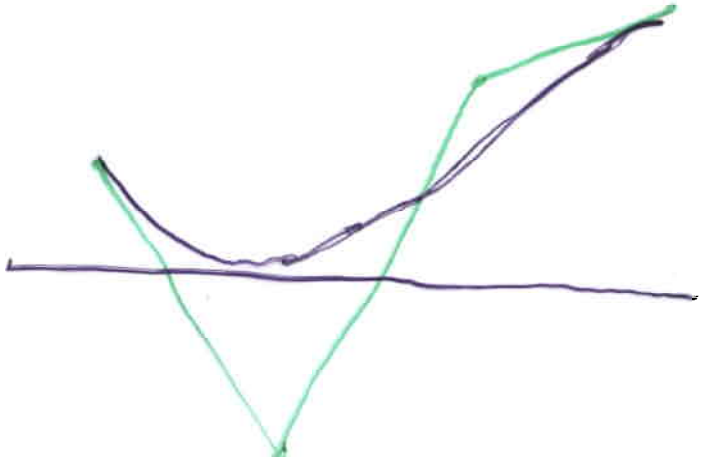
$$X = \left(d\left(\frac{X - c}{d - c}\right) + c\left(\frac{d - X}{d - c}\right)\right).$$

□

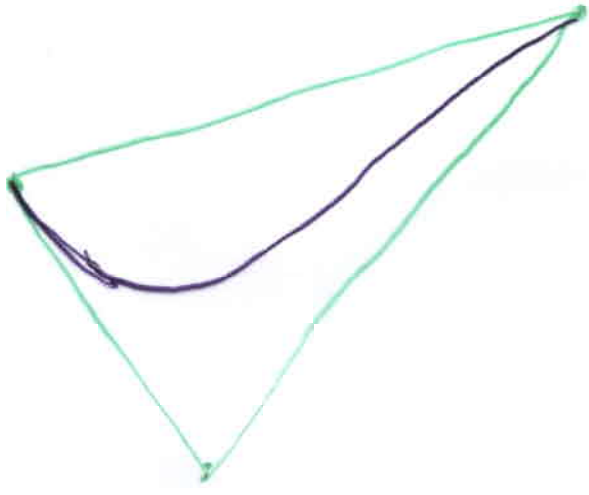
$p = 3$

$(1-x)^3 \quad 3(1-x)^2 x \quad , 3(1-x)x^2 , x^3$

$b = (4, -6, 7, 10)$



graph and control line



graph and control polygon

De Casteljau's Algorithm

Input: $b = b_0, \ldots, b_0$, coefficients of P in the Berstein basis of c, d, and $e \in \mathbb{R}$.

Output: $b' = b'_0, \ldots, b'_p$ coefficients of P in the Berstein basis of c, e.

Procedure: $\alpha = \dfrac{d-e}{d-c}, \beta = \dfrac{e-c}{d-c}$,

$b_j^{(0)} := b_j,\ j = 0, \ldots, p.$

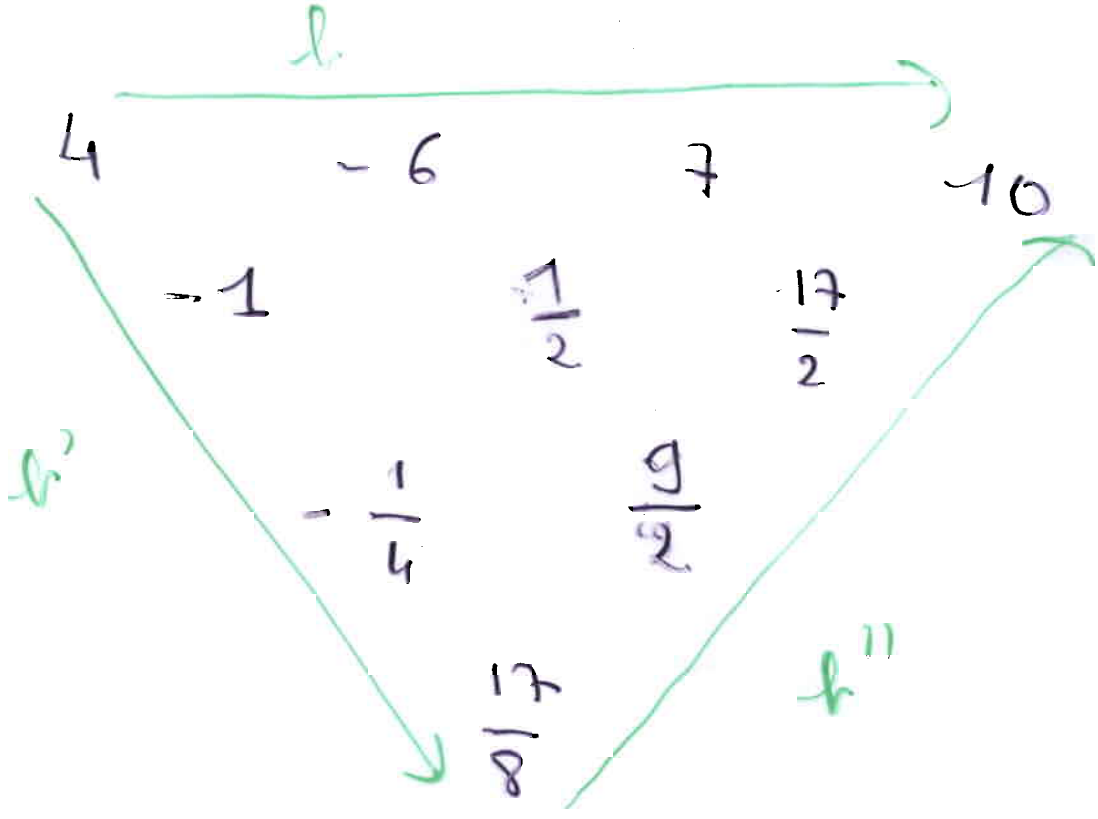
For $i = 1, \ldots, p$, for $j = 0, \ldots, p-i$, compute

$$b_j^{(i)} := \alpha b_j^{(i-1)} + \beta b_{j+1}^{(i-1)}$$

Output

$$b' = b_0^{(0)}, \ldots, b_0^{(j)}, \ldots, b_0^{(p)}$$

example $\alpha = \beta = \frac{1}{2}$



f on $[0, 1]$

f' on $[0, \frac{1}{2}]$

f'' on $[\frac{1}{2}, 1]$

Proposition 7 *Let b, b' and b'' be the lists of coefficients of P in the Bernstein basis of c, d; c, e; and e, d. If $c < e < d$, then*

$$\mathrm{V}(b') + \mathrm{V}(b'') \leq \mathrm{V}(b).$$

Moreover $\mathrm{V}(b) - \mathrm{V}(b') - \mathrm{V}(b'')$ is even.

Proof: The proof of the proposition is based on the following easy observations:

Inserting in a list $a = a_0, \ldots, a_n$ a value x in $[a_i, a_{i+1}]$ if $a_{i+1} \geq a_i$ (resp. in $[a_{i+1}, a_i]$ if $a_{i+1} < a_i$) between a_i and a_{i+1} does not modify the number of sign variations.

Removing from a list $a = a_0, \ldots, a_n$ with first non-zero $a_k, k \geq 0$, and last non-zero $a_\ell, k \leq \ell \leq n$, an element a_i, $i \neq k, i \neq \ell$ decreases the number of sign variation by an even (possibly zero) natural number.

□

P squarefree

Let $d > c$, $\mathcal{C}((c,d))_0$ be the closed disk with center $(c,0)$ and radius $d-c$, and $\mathcal{C}((c,d))_1$ closed disk with center $(d,0)$ and radius $d-c$.

Theorem 8 (Theorem of 2 circles) *If P has either no root or exactly one simple root in (c,d) and P has no complex root in $\mathcal{C}((c,d))_0 \cup \mathcal{C}((c,d))_1$, then*

P has one root in (c,d) if and only if

$$V(b) = 1,$$

P has no root in (c,d) if and only if

$$V(b) = 0.$$

$P \in \mathbb{R}[X]$ is a polynomial of degree p with all its real zeroes in $(-2^\ell, 2^\ell)$, squarefree. Consider natural numbers k and c such that $0 \leq c \leq 2^k$ and define

$$I_{c,k} = (\frac{-2^{\ell+k} + c2^{\ell+1}}{2^k}, \frac{-2^{\ell+k} + (c+1)2^{\ell+1}}{2^k}).$$

It is clear that, for k big enough, the polynomial P has at most one root in $I_{c,k}$ and has no other complex root in $\mathcal{C}(I_{c,k})_0 \cup \mathcal{C}(I_{c,k})_1$. $b(P, c, k)$ coefficients of P on the Bernstein basis of $I_{c,k}$.

Using the Theorem of two circles, it is possible to decide, for k big enough, whether P has exactly one root in $I_{c,k}$ or has no root on $I_{c,k}$ by testing whether $\mathrm{V}(b(P, c, k))$ is zero or one.

P square free, no root $\frac{c}{2^k}$

$I(P,0,0)$ $(-2^l, 2^l)$ contains the roots

Algorithm 9 (Real Root Isolation)

Input: $b(P,0,0)$.

Output: *a list* $L(P)$ *isolating the zeroes of* P.

Procedure:

Initialization: $Pos := \{(b(P,0,0)\}$ *and* $L(P)$ *is the empty list.*

While Pos *is non-empty,*

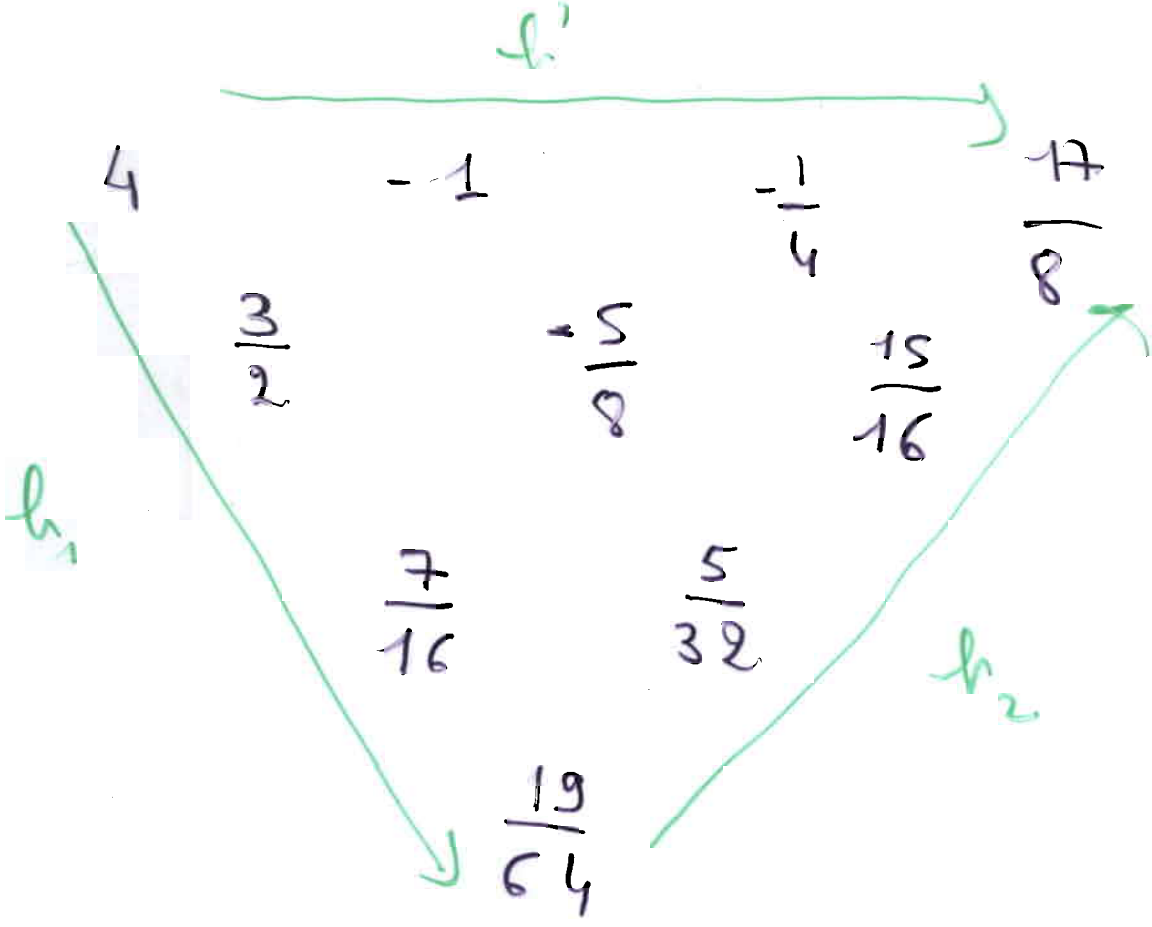
Remove $b(P,c,k)$ *from* Pos.

If $\mathrm{V}(b(P,c,k)) = 1$ *add* $I_{c,k}$, *to* $L(P)$.

If $\mathrm{V}(b(P,c,k)) = 0$ *do nothing.*

If $\mathrm{V}(b(P,c,k)) > 1$, *compute* $b(P,2c,k+1)$ *and* $b(P,2c+1,k+1)$ *using De Casteljau's Algorithm and add them to* Pos.

Multivariate generalization



f' $\quad [0, \frac{1}{2}] \quad v(f') = 2$

f_1 $\quad [0, \frac{1}{4}] \quad v(f_1) = 0$

f_2 $\quad [\frac{1}{4}, \frac{1}{2}] \quad v(f_2) = 0$

$p \in \mathbb{Z}[x]$ τ bound on

bit size

$$\text{sep} \leq p^{-(p+2)/2} \, (p+1)^{(1-p)/2} \, 2^{\tau(1-p)}$$

$$\ell \leq \tau + \log_2 (p+1)$$

compute square free parts

$$\vdots$$

$$O\left(p^6 (\tau + \log_2 (p))^2 \right).$$

better in practice Hom Sturm seq

$p = 4000$

$\tau = 1000$

constant space modification

complexity analysis

p, l, sep minimal distance between roots in C

k bounded

$$-\log_2(sep) + l + 2$$

(Two circles)

number of intervals in Pos: at most p

total number of intervals

$$(-\log_2(sep) + l + 2)\, p$$

each triangle $O(p^2)$ additions

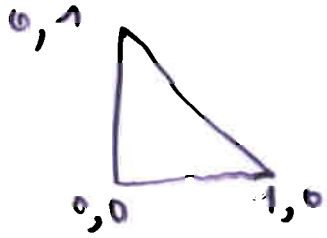
$$O((-\log_2(sep) + l + 2)\, p^3)$$

Multivariate generalizations

(open)

$n = 2$

curve. $P(X, Y) = 0$

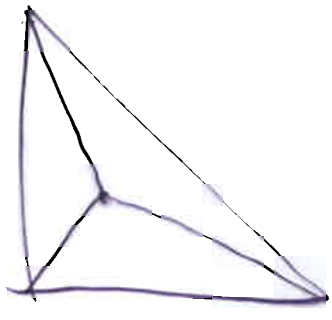


✓ Bernstein basis

$$\left[X + Y + (1 - X - Y) \right]^P$$

✓ Casteljau's algorithm

tetrahedron

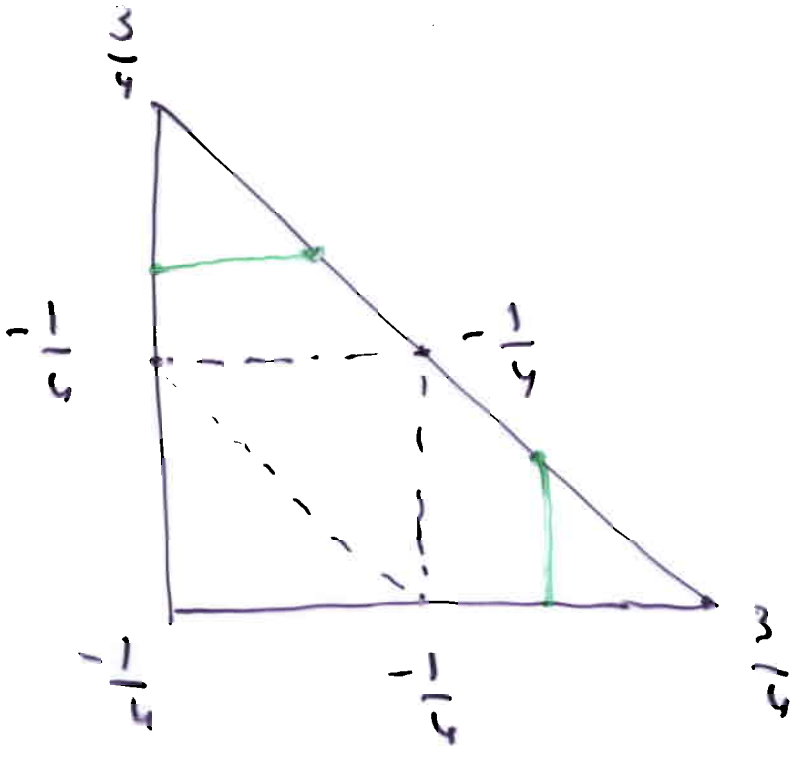


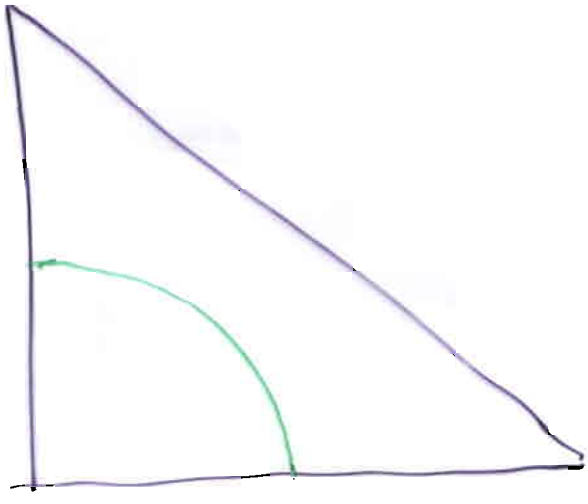
✓ $v(t)$ discrete curve

separating + from −

$$x^2 + y^2 - \frac{1}{4}$$

$$1 = x^2 + y^2 + 2xy + 2x(1-x-y)$$
$$+2y(1-x-y) + (1-x-y)^2$$





refine !

? $v(t)$ - n even

? $n(t) \geq v(t') + v(t'')$

difference even

? after refinement
"same thing"

? complexity

? two circles