Tutorial on real root isolation of polynomial systems

Marc Moreno Maza

Univ. of Western Ontario, Canada

May 21, 2013

An overview of this tutorial

• **Main objective:** an introduction for non-experts.

• **Prerequisites:** some familiarity with univariate polynomials (division, Euclidean Algorithm, roots of a polynomial), polynomial rings (partial degree, ideal).

• **Outline:**

- Basic results
- Root estimation
- Sturm's Rule
- Theorem of Budan - Fourier
- Descartes's rule
- Vincent's Theorem

Ordered Fields

DEFINITION. A field $\mathbb{K}$ is **ordered** if it is endowed with an order relation $>$ satisfying: $x \leq y \Rightarrow x + z \leq y + z$ and $(x \geq 0 \text{ and } y \geq 0) \Rightarrow xy \geq 0$, for all $x, y, z \in \mathbb{K}$. A field $\mathbb{K}$ is **real** if it can be ordered. A real field $\mathbb{K}$ is **real closed** if it has no non-trivial real algebraic extension. An ordered field $\mathbb{L}$ is a **real closure** of an ordered field $\mathbb{K}$ if the following hold:

1. $\mathbb{L}$ is real closed,
2. $\mathbb{L}$ is an algebraic extension of $\mathbb{K}$,
3. the total order of $\mathbb{L}$ extends that of $\mathbb{K}$.

PROPOSITION. The field $\mathbb{L}$ can be ordered if and only if -1 cannot be expressed as a sum of squares of elements of $\mathbb{L}$.

PROPOSITION. Every ordered field has characteristic zero.

PROPOSITION. Let $\mathbb{K}$ be a real closed field. Then $\mathbb{L} = \mathbb{K}[x]/\langle x^2 + 1\rangle$ is algebraically closed.

Some notations before we start the theory (I)

NOTATION. Throughout the talk, we consider a **real closed field** $\mathbb{K}$. and $X = x_1 < \cdots < x_n$ n variables. Typically $\mathbb{K}$ will be

- the field $\mathbb{R}$ of real numbers,
- the real closure of $\mathbb{Q}$.

We will denote by $\overline{\mathbb{K}}$ the **algebraic closure** of $\mathbb{K}$.

- In particular, $\overline{\mathbb{K}}$ is a field containing $\mathbb{K}$ over which any non-constant polynomial factorizes into factors of degree 1,
- For $\mathbb{K} = \mathbb{R}$, we have $\overline{\mathbb{K}} = \mathbb{C}$, the field of *complex numbers*.

Basic results (I)

PROPOSITION. The only irreducible polynomials $f \in \mathbb{K}[x]$ are those of degree 1 and those of degree 2 with (strictly) negative discriminant.

PROOF $\triangleright$ Let $f \in \mathbb{K}[x]$ be monic, irreducible, and thus non-constant. If f admits a root $\alpha \in \mathbb{K}$, then $x - \alpha$ divides f and thus $f = x - \alpha$ holds.

If f does not admit any roots in $\mathbb{K}$, then let α be a complex root of f. Since f has coefficients in $\mathbb{K}$, the conjugate $\overline{\alpha}$ of α is also a root of f in $\overline{K}$; then $(x - \alpha)(x - \overline{\alpha})$ divides f and thus equals f. $\triangleleft$

REMARK. If $f \in \mathbb{K}[x]$ is irreducible and has degree 2 then the sign of f is constant over $\mathbb{K}$.

Basic results (II)

NOTATION. Let $f \in \mathbb{K}[x]$ be non-constant. Let $a, b \in \mathbb{K}$ such that $a < b$. Then $Z_{\mathbb{K}}(f; a, b)$ denotes the multi-set of the roots of f in the closed interval $[a, b]$, each root being repeated a number of times equal to its multiplicity.

PROPOSITION. Let $f \in \mathbb{K}[x]$ be non-constant. Let $a, b \in \mathbb{K}$ such that $a < b$ and $f(a)f(b) \neq 0$. Then, the cardinality of $Z_{\mathbb{K}}(f; a, b)$ is even if and only $f(a)f(b) > 0$. In particular, if $f(a)f(b) < 0$ holds, then $Z_{\mathbb{K}}(f; a, b)$ is not empty.

PROOF $\triangleright$ Consider a factorization of f into irreducible factors of $\mathbb{K}[x]$:

$$f(x) = c\prod\nolimits_i (x - \alpha_i)\prod\nolimits_j (x^2 + \beta_j x + \gamma_j).$$

Then write down the quotient $\frac{f(a)}{f(b)}$. Observe that its sign depends only on the number of roots (counted with multiplicities) of f in $[a, b]$. $\triangleleft$

Basic results (III)

PROPOSITION.[Rolle] Let $f \in \mathbb{K}[x]$ be non-constant. Let $a, b \in \mathbb{K}$ be two successive roots of f. Then, the number of roots of the derivative f' in the open interval $]a, b[$ is odd.

PROOF $\triangleright$ Let m be the multiplicity of a, hence we can write

$$f(x) = (x-a)^m g(x) \text{ with } g(a) \neq 0.$$

Thus we have

$$f'(x) = m(x-a)^{m-1} g(x) + (x-a)^m g'(x).$$

Hence, for h small $f(a+h)/f'(a+h)$ is equivalent to h/m. Thus, for $x - a > 0$ and $x - a$ small we have $f(x)f'(x) > 0$. Similarly, for $x - b < 0$ and $x - b$ small we have $f(x)f'(x) < 0$. Since f does not vanish on $]a, b[$, for h small enough we have $f'(a+h)f'(b-h) < 0$. We conclude with the previous proposition. $\triangleleft$

Basic results (IV)

COROLLARY. Let $f \in \mathbb{K}[x]$ with exactly m roots in $\mathbb{K}$, counted with multiplicities. Then f' has at least $m-1$ roots in $\mathbb{K}$, counted with multiplicities.

PROOF $\triangleright$ Consider the m real roots $\alpha_1 \leq \cdots \leq \alpha_m$. Apply the last proposition on each interval $[\alpha_i, \alpha_{i+1}]$ where $\alpha_i \neq \alpha_{i+1}$. Conclude by observing that every multiple root of f with multiplicity $\mu > 1$ is a root of f' with multiplicity $\mu - 1$. $\triangleleft$

COROLLARY. Let $f \in \mathbb{K}[x]$ Let $a, b \in \mathbb{K}$ such that $a < b$. Then there exists c in the open interval $]a, b[$ such that we have $f(b) - f(a) = (b-a)f'(c)$.

PROOF $\triangleright$ Apply the last proposition to

$$u(x) = (b-a)(f(x) - f(a)) - (x-a)(f(b) - f(a)).$$

$\triangleleft$

Basic results (V)

COROLLARY. Let $f \in \mathbb{K}[x]$ Let $a, b \in \mathbb{K}$ such that $a < b$. Assume f' is strictly positive (resp. negative) on the open interval $]a, b[$. Then f is strictly increasing (resp. decreasing) on the open interval $]a, b[$.

PROOF $\triangleright$ Let $x, y \in \mathbb{K}$ such that $a \leq x < y \leq b$. We prove that $f(x) < f(y)$ holds. From the previous corollary, there exists $c \in]x, y[$ such that we have $f(y) - f(x) = (y - x)f'(c)$. Since $f'(c) > 0$ holds, we deduce $f(x) < f(y)$. $\triangleleft$

Basic results (VI)

PROPOSITION.[Taylor's Formula for polynomials] Let $f \in \mathbb{K}[x]$ be of degree $d \geq 0$. Then, for all $c, x \in \mathbb{K}$ we have:

$$f(x) = f(c) + f'(c)(x-c) + \frac{f''(c)}{2}(x-c)^2 + \cdots + \frac{f^{(d)}(c)}{d!}(x-c)^d.$$

PROOF $\triangleright$ The claim is clear for $d = 0$; so we proceed by induction and assume $d \geq 1$. Denoting by $q(x)$ the quotient in the Euclidean of $f(x)$ by $x - c$, we have:

$$f(x) = f(c) + (x-c)q(x).$$

The induction hypothesis implies:

$$q(x) = q(c) + q'(c)(x-c) + \frac{q''(c)}{2}(x-c)^2 + \cdots + \frac{q^{(d-1)}(c)}{(d-1)!}(x-d)^{d-1}.$$

Observe $f'(x) = q(x) + (x-c)q'(x)$ and thus $f'(c) = q(c)$. More generally, for $1 \leq k \leq d$, we have $f^{(k)}(x) = kq^{(k-1)}(x) + (x-c)q^{(k)}(x)$ and thus $f^{(k)}(c) = kq^{(k-1)}(c)$ holds. The conclusion follows. $\triangleleft$

Root estimation (I)

PROPOSITION.[Newton] Let $f \in \mathbb{K}[x]$ be of degree $d > 0$. Assume that there exists $c \in \mathbb{K}$ such that $f(c), f'(c), \ldots, f^{(d)}(c)$ are all positive or null. Then, for all root $\alpha \in \mathbb{K}$ of f we have $\alpha \leq c$.

PROOF $\triangleright$ The hypothesis $d > 0$ and Taylor's Formula imply that $f'(c), \ldots, f^{(d)}(c)$ cannot be all null. Thus, with Taylor's Formula again, we deduce $f(x) > f(c)$ for all $x > c$. Since $f(c) \geq 0$, the conclusion follows. $\triangleleft$

PROPOSITION.[Lagrange and Mac Laurin] Let $f \in \mathbb{K}[x]$ be of degree $d > 0$

$$f = x^d + a_1 x^{d-1} + \cdots + a_m x^{d-m} + a_{m+1} x^{d-m-1} + \cdots + a_d$$

such that $a_1, \ldots, a_m$ are positive or null and $a_{m+1}, \ldots, a_d$ are negative or null. Define $A = \max\{-a_{m+1}, \ldots, -a_d, 0\}$. Then, for root $\alpha \in \mathbb{K}$ of f we have

$$\alpha < 1 + A^{1/m}.$$

PROOF $\triangleright$ We have: $f(x) \geq x^d - A(1 + x + \cdots + x^{d-m-1}) = x^d - A\frac{x^{d-m}-1}{x-1}$ which implies $f(x) \geq x^d(1 - A/x^m) > 0$ for $x \geq 1 + A^{1/m}$. $\triangleleft$

Root estimation (II)

PROPOSITION.[Descartes] Let $f \in \mathbb{K}[x]$ be of degree $d > 0$ writing

$$f = x^d + a_1 x^{d-1} + \cdots + a_m x^{d-m} + \cdots + a_d$$

such that $a_1, \ldots, a_d$ are positive or null. Let $c \in \mathbb{K}$ with $f(c) \geq 0$ and $c \geq 0$. Then, for all $x > c$ we have $f(x) > 0$, thus, every root $\alpha \in \mathbb{K}$ of f satisfies $\alpha \leq c$.

HINT $\triangleright$ Observe that $f(c), f'(c), \ldots, f^{(d)}(c)$ are all positive or null. $\triangleleft$

PROPOSITION.[Cauchy] Let $f \in \mathbb{K}[x]$ be of degree $d > 0$ writing

$$f = x^d + a_1 x^{d-1} + \cdots + a_m x^{d-m} + \cdots + a_d.$$

Let $a_{i_1}, \ldots, a_{i_k}$ be all the coefficients of f that are strictly negative. Define

$$M = \max\{(|k a_{i_j}|)^{1/i_j} \mid 1 \leq j \leq k\}.$$

Then, for all root $\alpha \in \mathbb{K}$ of f we have $\alpha \leq M$.

HINT $\triangleright$ We have: $f(x) \geq x^d - a_{i_1} x^{d-i_1} - \cdots - a_{i_k} x^{d-i_k}$ which implies $f(x) > 0$ for $x > M$. $\triangleleft$

Root counting (I)

DEFINITION. Let $f \in \mathbb{K}[x]$ and let $a, b \in \mathbb{K}$ such that $a < b$. A sequence $f_0 = f, f_1, \ldots, f_s$ of non-zero polynomials in $\mathbb{K}[x]$ is a **Sturm sequence** for f on (the closed interval) $[a, b]$ if the following conditions hold:

(i) $f(a)f(b) \neq 0$,

(ii) f_s does not vanish on $[a, b]$,

(iii) if there exists $c \in \mathbb{K}$ and an index $0 < j < s$ such that $a < c < b$ and $f_j(c) = 0$ hold then we have $f_{j-1}(c)f_{j+1}(c) < 0$.

(iv) if there exists $c \in \mathbb{K}$ such that $a < c < b$ and $f(c) = 0$ hold, then the polynomial $f(x)f_1(x)$ has the sign of $x - c$ for x in a neighborhood of c.

Let $f_0 = f, f_1, \ldots, f_s$ be a Sturm sequence for f on $[a, b]$ and let $x \in [a, b]$. The **sign variation** denoted by $V(f_0, \ldots, f_s; x)$, or simply by $V(x)$, is defined by

$$V(x) = \#\{(i, j) \mid 0 \leq i \leq j \leq s \text{ and } f_i(x)f_j(x) < 0 \text{ and } (\forall i < k < j)\ f_k(x) = 0\}.$$

Root counting (II)

THEOREM.[Sturm] Let $f \in \mathbb{K}[x]$ and let $a, b \in \mathbb{K}$ such that $a < b$. Let $f_0 = f, f_1, \ldots, f_s$ be a Sturm sequence for f on $[a, b]$. Then, the number of distinct roots of f in $[a, b]$ is given by $V(a) - V(b)$.

PROOF $\triangleright$ Define $I := [a, b]$. Observe that $x \longmapsto V(x)$ is constant on every interval $J \subseteq I$ where none of the polynomials $f, f_1, \ldots, f_s$ possesses a root. Since the f_i's have in total finitely many roots in $\mathbb{K}$, proving the theorem reduces to prove the following statements

(1) $V(x)$ decreases by 1 when x traverses a root c of f in I from left to right,

(2) $V(x)$ is unchanged when x traverses a root c of one of the $f_1, \ldots, f_s$ which is not a root of f.

Let c be a root of f. From (iii) we have $f_1(c) \neq 0$. From (iv) the sign of $f(c+h)f_1(c+h)$ is that of h for h small enough. We deduce (1). Consider now c a root of one of the f_i for some $1 \leq i \leq s$ which is not a root of f. From (ii) we have $i < s$. From (iii), there is no sign variation for the f_j for $i - 1 \leq j \leq j + 1$ when traversing c. We deduce (2). $\triangleleft$

Root counting (III)

PROPOSITION.[Sturm] Let $f \in \mathbb{K}[x]$ and let $a, b \in \mathbb{K}$ such that $a < b$ and $f(a)f(b) \neq 0$ hold. Let $f_0 = f$ and $f_1 = f'$. Then, define $f_{i+2} = -f_i \text{ rem } f_{i+1}$ for $i \geq 0$ until $f_{i+2} = 0$; let f_{s+1} be this null remainder. Define, for $0 \leq i \leq s$

$$g_i = f_i / f_s.$$

Then, the sequence $g_0, g_1, \ldots, g_s$ is a Sturm sequence of g_0 on $[a, b]$.

PROOF $\triangleright$ First, observe that f_s is GCD of f and f'. Next, observe that (i) and (ii) are trivially satisfied. Indeed $g_s = 1$. We prove (iii). For $0 < j < s$ we have $g_{j-1}(x) = q_j(x)g_j(x) - g_{j+1}(x)$. If for some $a < c < b$ and for some $0 < j < s$ we have $g_j(c) = 0$ we deduce $g_{j-1}(c)g_{j+1}(c) < 0$. (Observe that $g_{j-1}(c) = 0$ or $g_{j+1}(c) = 0$ would lead to $g_s(c) = 0$.) This proves (iii). Let us prove (iv). Let c be a root of g_0. Observe that $g_1(c) = 0$ would imply that $(x - c)f_s$ divides f and f', which is impossible. Therefore, we have $g_1(x) \neq 0$ for x in a neighborhood of c. If there was no sign change for $g_0(x)$ when x traverses c then $g_1'(c) = 0$ would hold. Since $g_1'(x) = \frac{f'(x)f_s(x) - f(x)f_s'(x)}{f_s^2(x)} = g_1(x) - g_0(x)\frac{f_s'(x)}{f_s(x)}$ this would imply $g_1(c) = 0$. A contradiction. $\triangleleft$

Budan - Fourier Theorem (I)

THEOREM.[Budan - Fourier] Let $a, b \in \mathbb{K} \cup \{-\infty, +\infty\}$ with $a < b$. Let $f \in \mathbb{K}[x]$ be of degree $d > 0$.

Let $v(x)$ be the number of sign changes in the sequence $f(x), f'(x), \ldots, f^{(d)}(x)$ (skipping over zeros). Then, we have

(1) $\#Z(f,]a, b]) \equiv v(a) - v(b) \mod 2$,

(2) $\#Z(f,]a, b]) \leq v(a) - v(b)$.

where $Z(f, I)$ is the multiset of the roots of f (counted with multiplicity) lying in the interval I, for any interval $I \subseteq \mathbb{K}$ (open, closed or semi-open).

REMARK. With the notations of the above theorem, observe that

1. $v(a) - v(b) = 0$ implies $\#Z(f; a, b) = 0$,
2. $v(a) - v(b) = 1$ implies $\#Z(f; a, b) = 1$.

Budan - Fourier Theorem (II)

PROOF ▷ Let $c_1 < \cdots < c_r$ be all roots of $f(x), f'(x), \ldots, f^{(d-1)}(x)$ in the open interval $]a, b[$. Define $c_0 := a$ and $c_{r+1} = b$.

For each $0 \leq i \leq r$, let $e_i \in]c_i, c_{i+1}[$ such that we have:

$$a = c_0 < c_1 < e_1 < c_2 < \cdots < c_r < e_r < c_{r+1} = b.$$

Therefore, we have:

$$v(a) - v(b) = \Sigma_{i=0}^{i=r}(v(c_i) - v(e_i) + v(e_i) - v(c_{i+1})). \tag{1}$$

Now observe that for every $c \in]a, b[$ the following relation clearly hold:

$$\#Z(f,]a, b]) = \#Z(f,]a, c]]) + \#Z(f,]c, b]]).$$

Therefore, we also have:

$$\#Z(f,]a, b]) = \Sigma_{i=0}^{i=r}(\#Z(f,]c_i, e_i]) + \#Z(f,]e_i, c_{i+1})) \tag{2}$$

We conclude by applying the following lemma to (1) and (2). ◁

Budan - Fourier Theorem (III)

LEMMA. Let $f \in \mathbb{K}[x]$ be of degree $d > 0$. Let $c \in \mathbb{K}$ be a root of f of multiplicity $\mu \geq 0$. (Note that $\mu = 0$ simply means $f(c) \neq 0$.) Let $e, e' \in \mathbb{K}$ with $e < c < e'$ such that none of the polynomials $f(x), f'(x), \ldots, f^{(d-1)}(x)$ vanishes on $[e, c[\cup]c, e']$. Then the following two properties hold:

(i) $v(e) - v(c) \equiv \mu \mod 2$ and $v(e) - v(c) \geq \mu$,

(ii) $v(c) - v(e') = 0$.

PROOF $\triangleright$ The proof is by induction on d. For convenience, we denote by $v'(x)$ the number of sign changes in the sequence $f'(x), \ldots, f^{(d)}(x)$ (skipping over zeros). Consider $d = 1$. If $f(c) \neq 0$ then $v(e) - v(c) = 0 = \mu$ and $v(c) - v(e') = 0$. If $f(c) = 0$ then $v(e) - v(c) = 1 = \mu$ and $v(c) - v(e') = 0$. Suppose now $d > 1$ and $f(c) = 0$, thus $\mu \geq 1$. By induction hypothesis, we have:

(1) $v'(e) - v'(c) \equiv \mu - 1 \mod 2$ and $v'(e) - v'(c) \geq \mu$,

(2) $v'(c) - v'(e') = 0$.

(to be continued) $\triangleleft$

Budan - Fourier Theorem (IV)

PROOF $\triangleright$ From the third corollary of Rolle's Theorem, we observe that

- $f(x)f'(x) < 0$ for all $x \in]e, c[$,
- $f(x)f'(x) > 0$ for all $x \in]c, e'[$.

Therefore we have:

$$v(e) = v'(e) + 1, \;\; v(c) = v'(c) \;\text{ and }\; v(e') = v'(e').$$

This proves the claim in the case $d > 1$ and $\mu \geq 1$.

Suppose now $d > 1$ and $f(c) \neq 0$, thus $\mu = 0$. Let ν be the multiplicity of c as a root of f'. By induction hypothesis, we have:

(1) $v'(e) - v'(c) \equiv \nu \mod 2$ and $v'(e) - v'(c) \geq \nu$,

(2) $v'(c) - v'(e') = 0$.

(to be continued) $\triangleleft$

Budan - Fourier Theorem (V)

PROOF ▷ There are four cases to consider. Here are the first two:

(a) If $\nu \equiv 1 \mod 2$ and $f^{(\nu+1)}(c)f(c) > 0$ then:

$$v(e) = v'(e) + 1, \;\; v(c) = v'(c) \;\text{ and }\; v(e') = v'(e').$$

Therefore, we have:

$$v(e) - v(c) \equiv v'(e) + 1 - v'(c) \equiv \nu + 1 \equiv 0 \mod 2 \; \textit{and} \; v(e) - v(c) \geq \mu = 0.$$

(b) If $\nu \equiv 1 \mod 2$ and $f^{(\nu+1)}(c)f(c) < 0$ then:

$$v(e) = v'(e), \;\; v(c) = v'(c) + 1 \;\text{ and }\; v(e') = v'(e') + 1.$$

Therefore, we have:

$$v(e) - v(c) \equiv \nu - 1 \equiv 0 \mod 2 \; \textit{and} \; v(e) - v(c) \geq \mu = 0.$$

(to be continued) ◁

Budan - Fourier Theorem (VI)

PROOF ▷ Remain two cases:

(c) If $\nu \equiv 0 \mod 2$ and $f^{(\nu+1)}(c)f(c) > 0$ then:

$$v(e) = v'(e), \;\; v(c) = v'(c) \;\text{ and }\; v(e') = v'(e').$$

Therefore, we have:

$$v(e) - v(c) \equiv \nu \equiv 0 \mod 2 \;\; and \;\; v(e) - v(c) \geq \mu = 0.$$

(d) If $\nu \equiv 0 \mod 2$ and $f^{(\nu+1)}(c)f(c) < 0$ then:

$$v(e) = v'(e) + 1, \;\; v(c) = v'(c) + 1 \;\text{ and }\; v(e') = v'(e') + 1.$$

Therefore, we have:

$$v(e) - v(c) \equiv \nu \equiv 0 \mod 2 \;\; and \;\; v(e) - v(c) \geq \mu = 0.$$

Finally, the claim is true in each of these four cases. This completes the proof. ◁

Descartes's rule (I)

THEOREM.[Descartes] Let $f = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ with $a_n a_0 \neq 0$. Let v be the number of sign changes in the sequence $a_n, a_{n-1}, \ldots, a_0$ and let r be the number of positive roots of f. Then, there exits a non-negative integer m such that we have

$$r = v - 2m.$$

In particular, when $v = 0$ or $v = 1$ holds, we have $r = v$.

PROOF $\triangleright$ Let M be an upper bound for the positive roots of f and let $L \geq M$. Observe that for all $0 \leq i \leq n$

- $f^{(i)}(0)$ has the sign of a_i,
- $f^{(i)}(L)$ has the sign of a_n.

The conclusion follows from the Theorem of Budan - Fourier applied to the interval $[0, L]$. $\triangleleft$

EXAMPLE. Consider $\mathbb{K} = \mathbb{Q}$ and $f = x^6 - x^4 + 2x^2 - 3x - 1$. We have $v = 3$. Hence, we deduce $r = 1$ or $r = 3$.

Descartes's Rule (II)

COROLLARY. Let $f = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$ with $a_n a_0 \neq 0$. Let v be the number of sign changes in the sequence of the coefficients of $f(x)$ and v' be the number of sign changes in the sequence of the coefficients of $f(-x)$. Let r (resp. r') be the number of positive (resp. negative) roots of f. Then, we have

$$r \leq v \ \text{ and } \ r' \leq v'.$$

Moreover, if all roots of f are in $\mathbb{K}$, then we have

$$r = v \ \text{ and } \ r' = v'.$$

PROOF $\triangleright$ First observe that $f(0) \neq 0$. The first claim follows from the fact that the negative roots of f are the positive roots of $x \longmapsto f(-x)$. The second claim results from the hypothesis $n = r + r'$ and the following lemma. $\triangleleft$

LEMMA. Let f, v, v' be as above. If all roots of f are in $\mathbb{K}$ then $v + v' \leq n$ holds.
HINT $\triangleright$ By induction on the number of zero coefficients among $a_n, \ldots, a_0$. $\triangleleft$

Vincent's Theorem (I)

THEOREM. Let $f \in \mathbb{K}[x]$ be square-free of degree d. Let $a_0, a_1, \ldots, a_n, \ldots$ be an arbitrary sequence of positive integers. Define

$$x_0 = x \ \text{ and } \ x_i = a_i + \frac{1}{x_{i+1}} \ \text{ for } \ i \geq 0.$$

Then define

$$f_{i+1}(x_{i+1}) = {x_{i+1}}^d f_i(a_i + \frac{1}{x_{i+1}}) \ \text{ for } \ i \geq 0.$$

There exists $n \geq 0$ such that the coefficient list of f_n has at most one sign change.

REMARK. Observe that

$$\begin{aligned} x_{i+1} \geq 0 \quad &\Longleftrightarrow \quad a_i < x_i \quad \Longleftrightarrow \quad a_{i-1} < x_{i-1} < a_{i-1} + \tfrac{1}{a_i} \\ &\Longleftrightarrow \quad a_{i-2} + \frac{1}{a_{i-1} + \frac{1}{a_i}} < x_{i-2} < a_{i-2} + \frac{1}{a_{i-1}} \end{aligned}$$

Therefore, with n as in the above theorem, from $a_0, a_1, \ldots, a_n$, we obtain an isolation interval for a root of f. (remark to be continued)

Vincent's Theorem (II)

REMARK. With the notations of the theorem, let $M > 0$ be such that all roots of f are in the interval $[-M, M]$. Let us **isolate** the **positive** roots of f, that is, let us compute pairwise disjoint intervals such that

- each of them contains exactly one positive root of f,
- their union contains all positive roots of f.

Isolating the negative roots can be done similarly by replacing $f(x)$ with $f(-x)$.

(1) Let $0 < a < b < M$. If $f(a) = 0$ then output $[a, a]$; if $f(b) = 0$ output $[b, b]$.

(2) Assume $f(a)f(b) \neq 0$. Recall that for f to have a root in $]a, b[$ we must have $v(a) > v(b)$. If $v(a) = v(b) + 1$ then output $[a, b]$.

(3) Assume $f(a)f(b) \neq 0$ and $v(a) > v(b) + 1$. Let $f_i = f$. Then define $x_i = a + \frac{b}{x_{i+1}}$ and $f_{i+1}(x_{i+1}) = {x_{i+1}}^d f_i(a + \frac{b}{x_{i+1}})$. Observe that the roots of f_i in $[a, b]$ correspond to those of f_{i+1} in $[1, \infty[$ for which we return to (1), after partitioning $[1, \infty[$ and rescaling (so as to apply Descartes's rule).

(4) This **informal** algorithm stops thanks to Vincent's Theorem.

Vincent-Collins-Akritas Algorithm (I)

Input: $p \in \mathbb{Q}[x]$ squarefree and $a < b$ rational.

Output: an interval decomposition of $V(p) \cap]a, b[$.

1: $nsv \leftarrow \mathsf{RootNumberBound}(p,]a, b[)$
2: **if** $nsv = 0$ **then return** $\emptyset$
3: **else if** $nsv = 1$ **then return** $]a, b[$
4: **else**
5: $\quad m \leftarrow (a + b)/2 \quad res \leftarrow \emptyset$
6: $\quad$ **if** $p(m) = 0$ **then** $res \leftarrow \{\{m\}\}$
7: $\quad \{$Next line ensures the roots are sorted increasingly$\}$
8: $\quad$ **return** $\mathsf{VCA}(p,]a, m[) \cup res \cup \mathsf{VCA}(p,]m, b[)$

Vincent-Collins-Akritas Algorithm (II)

Input: $p \in \mathbb{Q}[x]$ and $a < b$ rational

Output: a bound on the number of roots of p in the interval $]a, b[$

1: $\bar{p} \leftarrow (x+1)^d \, p\left(\frac{a\,x+b}{x+1}\right)$ where d is the degree of p, and denote $\bar{p} = \sum_{i=0}^{d} a_i x^i$

2: $a'_e, \ldots, a'_0 \leftarrow$ the sequence obtained from $a_d, \ldots, a_0$ by removing zero coefficients

3: **return** the number of sign variations in the sequence $a'_e, \ldots, a'_0$