History of algorithms in real algebraic geometry

BY MARIE-FRANCOISE ROY

IRMAR (Université de Rennes 1/CNRS)

MAP School Genova
28 august 2 september 2006

1 Introduction

Thanks to the project "Sources in real algebraic geometry/Aux sources de la géométrie algébrique réelle" (sources = before 1970).

- scientific committee: Hourya Benis Sinaceur, Michel Coste, Catherine Godstein, Alain Herreman, M-F R.
- so far 25 participants
  list of participants

  Francesca Acquistapace
  Liliane Alfonsi
  Saugata Basu
  Hourya Benis Sinaceur
  Fabrizio Broglia
  Jean-Luc Chabert
  Solen Corvez
  Michel Coste
  Martin Davis
  Charles Delzell
  Max Dichmann
  Eric Féron
  Danielle Gondard
  Catherine Goldstein
  Alain Herreman
  Johan Huisman
  Alain Lascoux
  Henri Lombardi
  Hervé Perdry
  Daniel Perrucci
  Richard Pollack
  Alex Prestel
  Marie-Françoise Roy
  Norbert Schappacher
  Niels Schwartz
- read sources, combining mathematicians and historians of mathematics
- make a website of bibliographical references on real algebraic geometry
  http://thamous.univ-rennes1.fr/sites/gar/
- including on line versions and comments for a list of identified "sources texts"
- publish a source-book as a subset
- various activities
  - activities
    - working group in Rennes since 2004
      http://www.math.univ-rennes1.fr/geomreel/gtsources.html
    - Belle Ile workshop 2005
    - special day in Paris: séminaire d'histoire des mathématiques, trimester on real geometry at Centre Emile Borel, IHP
    - Cortona workshop 2006
    - CIRM workshop 2007
- support: IRMAR, Centre Emile Borel, Institut Henri Poincaré (trimester on real geometry), Real Algebraic and Analytic Geometry network
- not limited to algorithmic aspects of real algebraic geometry but including them

- should be linked to interactive book [1].

These two lectures: a first try to communicate information about this activity without reading together.

2 Answers and remarks

- Why real algebra ? In complex algebra, a univariate polynomial has always roots. The only problem is the question of singularities: are the roots multiple ? This is done through gcd computations, or elimination (resultants, discriminants). In the real case there might be no roots. The miracle in the real case is that the same computations (carefully done: take care of signs) provides also the information on the number of real roots. Sturm is gcd computation + right signs. Hermite (see today's lecture) is computing the signature of the matrix whose determinant is the discriminant .... So more information, but not much mopre computations. In several cases, algebraic computation followed by sign conditions.
- Why algorithms in real algebraic geometry ? There is not one generic case, there are many, and we want to know what is what !
- Resolution of algebraic equations: splitting of one problem into many
  - Laplace Gauss: add the root of an equation of big odd degree, and then extraction of square roots
  - Abel and Galois: no general resolution of algebraic equations by radicals, group theoretic conditions. Solvable groups, effective Galois theory
  - deciding the existence of real roots: exact methods
  - isolating real roots exactly
  - numerical methods
- Sturm and Newton: Sturm does quote Newton method once he approached the root by decimalchotomy (cut into 10 rather than in 2).

3 Real root counting

3.1 Descartes, Budan-Fourier

- Descartes : number of roots by sign of coefficients
  - Gallica BNF [4] page 57

    Descartes takes one example

    $$x^4 - 4x^3 - 19x^2 + 106x - 120 = 0$$

    3 sign changes: 3 positive roots ("true")

    changing x in $-x$:

    $$x^4 + 4x^3 - 19x^2 - 106x - 120 = 0$$

    1 sign change: 1 negative root ("false")
  - Compute

```
Maxima 5.9.3 http://maxima.sourceforge.net
Using Lisp CLISP 2.34 (2005-07-20)
Distributed under the GNU Public License. See the file COPYING.
Dedicated to the memory of William Schelter.

(%i1) factor(x^4-4*x^3-19*x^2+106*x-120);
```

(%o3) $(x-4)\,(x-3)\,(x-2)\,(x+5)$

in the section where he proves that a polynomial of degree d has at most d roots

- Budan [2], Fourier [6]: number of roots in an interval by signs of the derivatives
- modern statement [1]
  - Budan-Fourier in modern terms

Notation 1. [Sign variations] The **number of sign variations**, $\mathrm{Var}(a)$, in a sequence, $a = a_0, \cdots, a_p$, of elements in $\mathrm{R}\setminus\{0\}$ is defined by induction on p by:

$$\begin{aligned}\mathrm{Var}(a_0) &= 0\\ \mathrm{Var}(a_0,\cdots,a_p) &= \begin{cases}\mathrm{Var}(a_1,\cdots,a_p)+1 & \text{if } a_0a_1<0\\ \mathrm{Var}(a_1,\cdots,a_p) & \text{if } a_0a_1>0\end{cases}\end{aligned}$$

This definition extends to any finite sequence a of elements in R by considering the finite sequence b obtained by dropping the zeros in a and defining

$$\mathrm{Var}(a)=\mathrm{Var}(b),\ \mathrm{Var}(\emptyset)=0.$$

For example $\mathrm{Var}(1,-1,2,0,0,3,4,-5,-2,0,3)=4$. □

Notation 2. [Sign variations in a sequence of polynomials at a] Let $\mathcal{P}=P_0, P_1, \ldots, P_d$ be a sequence of polynomials and let a be an element of $\mathrm{R}\cup\{-\infty,+\infty\}$. The **number of sign variations** of $\mathcal{P}$ at a, denoted by $\mathrm{Var}(\mathcal{P};a)$, is $\mathrm{Var}(P_0(a),\ldots,P_d(a))$ (at $-\infty$ and $+\infty$ the signs to consider are the signs of the leading monomials).

Given a and b in $\mathrm{R}\cup\{-\infty,+\infty\}$, we denote

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

□

We denote by $\mathrm{num}(P;(a,b])$ the number of roots of P in $(a,b]$ counted with multiplicities.

Theorem 3. [Budan-Fourier theorem] *Let P be a univariate polynomial of degree p in $\mathrm{R}[X]$. Given a and b in $\mathrm{R}\cup\{-\infty,+\infty\}$*

- $\mathrm{Var}(\mathrm{Der}(P);a,b)\geq\mathrm{num}(P;(a,b])$,
- $\mathrm{Var}(\mathrm{Der}(P);a,b)-\mathrm{num}(P;(a,b])$ *is even.*

- recent research [5] [1]
  - Virtual roots

    A natural question when looking at Budan-Fourier's Theorem, is to interpret the even difference $\mathrm{Var}(\mathrm{Der}(P);\,a,\,b)-\mathrm{num}(P;\,(a,\,b])$. This can be done through the notion of virtual roots.

    The virtual roots of P will enjoy the following properties:

    a) the number of virtual roots of P counted with virtual multiplicities is equal to the degree p of P,

    b) on an open interval defined by its virtual roots, the sign of P is fixed,

    c) virtual roots of P and virtual roots of P' are interlaced: if $x_1\leq\ldots\leq x_p$ are the virtual roots of P and $y_1\leq\ldots\leq y_{p-1}$ are the virtual roots of P, then

    $$x_1\leq y_1\leq\ldots\leq x_{p-1}\leq y_{p-1}\leq x_p.$$

    Given these properties, in the particular case where P is a polynomial of degree p with all its roots real and simple, virtual roots and real roots clearly coincide.

Definition 4. [Virtual roots] The definition of **virtual roots** proceeds by induction on $p = \deg(P)$. We prove simultaneously that properties a), b), c) hold.

If $p=0$, P has no virtual root and properties a), b), c) hold.

Suppose that properties a), b), c) hold for the virtual roots of P'.

By induction hypothesis the virtual roots of P' are $y_1 \leq ... \leq y_{p-1}$. Let

$$I_1 = (-\infty, y_1], ..., I_i = [y_{i-1}, y_i], ..., I_p = [y_{p-1}, +\infty).$$

By induction hypothesis, the sign of P' is fixed on the interior of each I_i. Let x_i be unique value in I_i such that the absolute value of P on I_i reaches its minimum. The virtual roots of P are $x_1 \leq ... \leq x_p$.

According to this inductive definition, properties a), b) and c) are clear for virtual roots of P. Note that the virtual roots of P are always roots of a derivative of P.

The **virtual multiplicity** of x with respect to P, denoted $v(P, x)$ is the number of times x is repeated in the list $x_1 \leq ..., \leq x_p$ of virtual roots of P. In particular, if x is not a virtual root of P, its virtual multiplicity is equal to 0. Note that if x is a virtual root of P' with virtual multiplicity ν with respect to P, the virtual multiplicity of x with respect to P' can only be ν, $\nu+1$ or $\nu-1$. Moreover, if x is a root of P', the virtual multiplicity of x with respect to P' is necessarily $\nu+1$. □

Example 5. The virtual roots of a polynomial P of degree 2 are

- the two roots of P with virtual multiplicity 1 if P has two distinct real roots,
- the root of P' with virtual multiplicity 2 if P does not have two distinct real roots. □

Given a and b, we denote by $v(P; (a, b])$ the number of virtual roots of P in $(a, b]$ counted with virtual multiplicities.

Theorem 6.

$$v(P; (a, b]) = \mathrm{Var}(\mathrm{Der}(P); a, b).$$

Lemma 7. *All the roots of P are virtual roots of P. The virtual multiplicity is at least equal to the multiplicity and the difference is even.*

- issues in constructive mathematics: virtual roots can be followed continuously while real roots cannot, might be useful in real algebraic geometry with real numbers (where the sign cannot be decided).

• 3.2 Laplace Gauss

- Laplace gave an algebraic proof of the fundamental theorem of algebra : every even degree real polynomial factors in products of quadratic factors. [10]
- Reduces the existence of a complex root for a real polynomial P of degree $2^i s$ to the existence of a complex root for real polynomials Q_m , $m \in \mathbb{Z}$ of degree $2^{i-1} s(2^i s - 1) = 2^{i-1} s'$ with s' odd, whose roots are

$$a + b + m\, a\, b,$$

for a and b roots of P. Use pidgeon hole principle (since $\mathbb{Z}$ is infinite) as well as resolution of equation of degree 2. Finally, get a polynomial of odd degree $O(d^d)$. Polynomial of odd degrees have real roots.

- Discussion by Gauss [7]: assume the existence of roots is not correct (section 1). Beautiful work on elementary symmetric functions: talk about the roots without assuming having the existence of the roots. Same mechanism as Laplace (who is not quoted) (section 19).

- modern statement [1]
  - Laplace-Gauss in modern terms

    A **real closed field** R is an ordered field whose positive cone is the set of squares $R^{(2)}$ and such that every polynomial in $R[X]$ of odd degree has a root in R.

    Theorem 8. *If* R *is a real closed field then* $R[i] = R[T]/(T^2+1)$ *is an algebraically closed field.*

- issues in constructive mathematics: the discussion Laplace versus Gauss plays a role on on going research on effective positivstellensatz (Lombardi/R.): Gaus gives smaller degree estimates than Laplace.

• 3.3 Sturm

- Sturm: number of roots by euclidean division
  - Gallica BNF [14]
    - quotes Lagrange (exhaustion of intervals knowing the minimal distance between the roots), but too many computations, Fourier (not Budan) but sometime there are no roots
    - statement section 2
    - rigourous proof starting from section 3
    - examples of degree 3, including a symbolic one section 17
    - numerical methods in the case of very close roots, using decimal notation
- modern statement [1]
  - Sturm in modern terms

    Definition 9. [Signed remainder sequence] Given $P, Q \in K[X]$, not both 0, we define the **signed remainder sequence of P and Q**,

$$\begin{aligned}
\mathrm{SRemS}_0(P,Q) &= P,\\
\mathrm{SRemS}_1(P,Q) &= Q,\\
\mathrm{SRemS}_2(P,Q) &= -\mathrm{Rem}(\mathrm{SRemS}_0(P,Q),\mathrm{SRemS}_1(P,Q)),\\
&\vdots\\
\mathrm{SRemS}_k(P,Q) &= -\mathrm{Rem}(\mathrm{SRemS}_{k-2}(P,Q),\mathrm{SRemS}_{k-1}(P,Q)) \neq 0,\\
\mathrm{SRemS}_{k+1}(P,Q) &= -\mathrm{Rem}(\mathrm{SRemS}_{k-1}(P,Q),\mathrm{SRemS}_k(P,Q)) = 0.
\end{aligned}$$

    Note the signs. □

    Theorem 10. [Sturm's theorem] *Given a and b in* $R \cup \{-\infty, +\infty\}$,

$$\mathrm{Var}(\mathrm{SRemS}(P,P');a,b)$$

    is the number of roots of P in the interval (a,b).

  - Compute

```
Maxima 5.9.3 http://maxima.sourceforge.net
Using Lisp CLISP 2.34 (2005-07-20)
Distributed under the GNU Public License. See the file COPYING.
Dedicated to the memory of William Schelter.
```

```
(%i6) load("./sarag/loadSARAG.mc");
(%o2) ./sarag/loadSARAG.mc
(%i3) V0:x^3-2*x+5;
```

```
(%o7)  x^3 - 2 x + 5
(%i8)  V1:diff(V0,x);
(%o8)  3 x^2 - 2
(%i9)  V2:-remainder(V0,V1,x);
(%o9)  (4 x - 15)/3
(%i10) V3:-remainder(V1,V2,x);
(%o10) -643/16
(%i11) signChanges([1,3,4,-643]);
(%o11) 1
(%i12)
```

– more generally: Cauchy index, already in Sturm (section 20)
  • Cauchy index

Definition 11. [Cauchy index]
Cauchy index of Q/P on $(a,\ b)$, $\mathrm{Ind}(Q/P;\ a,\ b)$, to be the number of jumps of the function Q/P from $-\infty$ to $+\infty$ minus the number of jumps of the function Q/P from $+\infty$ to $-\infty$ on the open interval (a, b). □

Theorem 12. *Let P, $P \neq 0$, and Q be two polynomials with coefficients in a real closed field* R, *and let a and b (with $a < b$) be elements of* $\mathrm{R} \cup \{-\infty, +\infty\}$ *that are not roots of P. Then,*

$$\mathrm{Var}(\mathrm{SRemS}(P, Q); a, b) = \mathrm{Ind}(Q/P; a, b).$$

– method of proof: from left to right through real roots.

– issues in constructive mathematics: computation made in the field generated by the coefficients (typically $\mathbb{Q}$); needs the field to be discrete (the sign of an element can be decided); complexity $O(d^2)$ where d is the degree, growth of size of coefficients

• 3.4 Hermite

– Hermite number of roots given by the signature of a quadratic form
  • references [9]

$$P \ = \ X^p + a_{p-1}X^{p-1} + \cdots + a_1 X + a_0$$

Hermite quadratic form $\mathrm{Her}(P)$ depending of the p variables $f_1, ..., f_p$:

$$\mathrm{Her}(P)(f_1, ..., f_p) = \sum_{x \in \mathrm{Zer}(P, \mathrm{C})} \mu(x)(f_1 + f_2\, x + \cdots + f_p\, x^{p-1})^2,$$

where $\mu(x)$ is the multiplicity of x. Note that

$$\begin{aligned} \mathrm{Her}(P) \ &= \ \sum_{k=1}^{p} \sum_{j=1}^{p} \sum_{x \in \mathrm{Zer}(P, \mathrm{C})} \mu(x)\, x^{k+j-2} f_k\, f_j \\ &= \ \sum_{k=1}^{p} \sum_{j=1}^{p} N_{k+j-2} f_k\, f_j \end{aligned}$$

where N_n is the n-th Newton sum of P

$$N_i = \sum_{x \in \mathrm{Zer}(P, \mathrm{C})} \mu(x)\, x^i.$$

Matrix of Newton sums associated to Hermite's quadratic form

$$\mathrm{Newt}(P)=\begin{bmatrix} N_0 & N_1 & \iddots & & \iddots & N_{p-1} \\ N_1 & \iddots & & \iddots & N_{p-1} & N_p \\ \iddots & & \iddots & N_{p-1} & N_p & \iddots \\ & \iddots & N_{p-1} & N_p & \iddots & \\ \iddots & N_{p-1} & N_p & \iddots & & \iddots \\ N_{p-1} & N_p & \iddots & & \iddots & N_{2p-2} \end{bmatrix}$$

with entries the Newton sums of the monic polynomial P of degree p.

Hermite Sylvester formulae [15]

$$\begin{aligned} \mathrm{Disc}(P)=\det(\mathrm{Newt}(P)) &= \prod_{p\geq i>j\geq 1}(x_i-x_j)^2 \\ \mathrm{sDiscP}_{p-k}(P)=\det(....) &= \sum_{\substack{I\subset\{1,\dots,p\}\\ \#(I)=k}}\prod_{\substack{(j,\ell)\in I\\ \ell>j}}(x_j-x_\ell)^2\prod_{n\notin I}(X-x_n) \end{aligned}$$

algebraic identities expressing naturally the gcd of P and P'

Theorem 13. [Hermite] *The rank of* $\mathrm{Her}(P)$ *is equal to the number of roots of* P *in* C. *The signature of* $\mathrm{Her}(P)$ *is equal to the number of roots of* P *in* R.

– modern statement [1]

- Hermite in modern terms

$\mathrm{Her}(P)$ expressed in terms of the trace map. Tr the usual **trace** of a linear map from a finite dimensional vector space A to A.

Notation 14. [Multiplication map] For $f\in \mathrm{A}=\mathrm{K}[X]/(P)$, denote by L_f: $\mathrm{A}\to\mathrm{A}$ the linear map of multiplication by f, sending any $g\in\mathrm{A}$ to the remainder of fg in the euclidean division by P. □

Proposition 15. *The quadratic form* $\mathrm{Her}(P)$ *is the quadratic form associating to*

$$f=f_1+f_2X\cdots+f_pX^{p-1}\in A=\mathrm{K}[X]/(P)$$

the expression $\mathrm{Tr}(L_{f^2})$.

– generalization (not known in 19 th century)

- Generalized Hermite

$$\begin{aligned} P &= X^p+a_{p-1}X^{p-1}+\cdots+a_1X+a_0 \\ Q &= b_qX^q+b_{q-1}X^{q-1}+\cdots+b_1X+b_0. \end{aligned}$$

Hermite quadratic form $\mathrm{Her}(P,Q)$ depending of the p variables $f_1,\dots,f_p$

$$\mathrm{Her}(P,Q)(f_1,\dots,f_p)=\sum_{x\in\mathrm{Zer}(P,\mathrm{C})}\mu(x)Q(x)(f_1+f_2x+\cdots+f_px^{p-1})^2,$$

where $\mu(x)$ is the multiplicity of x. Note that

$$\mathrm{Her}(P,Q)=\sum_{k=1}^{p}\sum_{j=1}^{p}\sum_{x\in\mathrm{Zer}(P,\mathrm{C})}\mu(x)\,Q(x)\,x^{k+j-2}\,f_k\,f_j.$$

When $Q=1$, we get $\mathrm{Her}(P)$.

Notation 16. [Tarski-query] **Tarski-query** of Q for P

$$\mathrm{TaQ}(Q,P) = \sum_{x\in\mathbb{R},P(x)=0}\mathrm{sign}(Q(x)).$$

Note that $\mathrm{TaQ}(Q,P)$ is equal to

$$\#(\{x\in\mathbb{R}\mid P(x)=0\wedge Q(x)>0\})-\#(\{x\in\mathbb{R}\mid P(x)=0\wedge Q(x)<0\}) \qquad \square$$

Theorem 17. [Hermite]

$$\begin{aligned}\mathrm{Rank}(\mathrm{Her}(P,Q)) &= \#\{x\in\mathrm{C}\mid P(x)=0\wedge Q(x)\neq 0\},\\ \mathrm{Sign}(\mathrm{Her}(P,Q)) &= \mathrm{TaQ}(Q,P).\end{aligned}$$

Tarski queries are related to Cauchy index and can be computed also through Sturm sequences since it is clear that

$$\mathrm{TaQ}(Q,P) = \mathrm{Ind}(P'Q/P).$$

– recent research [11] [12] [1]
  - Multivariate Hermite

    Zero dimensional polynomial system $\mathcal{P}$, i.e. with a finite number of complex solutions and $\mathrm{A}=\mathrm{K}[X_1,\ldots,X_k]/(\mathcal{P})$ finite dimensional vector space [1]. Tarski-query of Q for $\mathcal{P}$ as

$$\mathrm{TaQ}(Q,\mathcal{P})=\sum_{x\in\mathrm{Zer}(\mathcal{P},\mathrm{R}^k)}\mathrm{sign}(Q(x))$$

Hermite's quadratic form,

$$\begin{array}{rccc}\mathrm{Her}(\mathcal{P},Q): & \mathrm{A} & \longrightarrow & K\\ & f & \longmapsto & \mathrm{Tr}(L_{f^2Q})\end{array}.$$

Theorem 18. [Multivariate Hermite]

$$\begin{aligned}\mathrm{Rank}(\mathrm{Her}(\mathcal{P},Q)) &= \#\{x\in\mathrm{Zer}(\mathcal{P},\mathrm{C}^k)\mid Q(x)\neq 0\},\\ \mathrm{Sign}(\mathrm{Her}(\mathcal{P},Q)) &= \mathrm{TaQ}(Q,\mathcal{P}).\end{aligned}$$

– method of proof: conjugate complex roots dont contribute

– issues in constructive mathematics: in the univariate case, complexity also $O(d^2)$ because Hankel matrix; in the multivariate case, needed to know a basis of the quotient: Groebner bases. Wanted: algebraic identities expressing the signature without looking at the roots.

• 3.5 Habicht

– Habicht: compute "Sturm sequence without denominators"
  - reference [8]
  - Habicht (simple case: no drop of degree in the euclidean sequence)

Definition 19. [Subresultant sequence]

$$\begin{aligned}\mathrm{sResP}_d(P,Q) &= P,\\ \mathrm{sResP}_{d-1}(P,Q) &= Q,\\ \mathrm{sResP}_{d-2}(P,Q) &= -\mathrm{Rem}(s_{d-1}^2\,\mathrm{sResP}_d(P,Q),\mathrm{sResP}_{d-1}(P,Q)),\\ &\vdots\\ \mathrm{sresP}_{k-1}(P,Q) &= -\mathrm{Rem}(s_k^2\,\mathrm{SRemS}_{k+1}(P,Q),\mathrm{SRemS}_k(P,Q))/s_{k+1}^2,\\ &\vdots\\ \text{with } s_k &= \mathrm{lcoff}(\mathrm{sResP}_k(P,Q)\end{aligned}$$

$\square$

Slight modificatin of the signed remainder sequence

No denominators: $\mathrm{sResP}_i(P,\ Q)\in\mathrm{D}[X]$: coefficients are determinants extracted from the Sylvester matrix of P and Q.

Theorem 20.

$$\mathrm{Var}(\mathrm{sResP}(P,P'))$$

is the number of roots of P.

- Sylvester formulae

$$\begin{aligned}\mathrm{sResP}_0(P,P')=\mathrm{Disc}(P) &= \prod_{p\geq i>j\geq 1}(x_i-x_j)^2\\ \mathrm{sResP}_{p-k}(P,P')=\mathrm{sDiscP}_{p-k}(P) &= \sum_{\substack{I\subset\{1,\ldots,p\}\\ \#(I)=k}}\prod_{\substack{(j,\ell)\in I\\ \ell>j}}(x_j-x_\ell)^2\prod_{n\notin I}(X-x_n)\end{aligned}$$

– very active topic of research

– issues in constructive mathematics: complexity ($O(d\ \log^2 d)$ rather than $O(d^2)$). What is going on in the non generic case in terms of expression of the roots ?

• 4 Quantifier elimination

• 4.1 Tarski

– Tarski

- my webpage [16]

  Tarski proves the decidability of the theory of the reals, through quantifier elimination. Any first order formula in the language of ordered fields is equivalent to a formula without quantifiers in the theory of real closed fields.

– modern statement [1]

- Tarski in modern terms

  logical statement: the theory of real closed fields admits quantifier elimination in the language of ordered fields (needs symbol $>$)

  geometric statement: semi-algebraic sets are stable under projection

– language is important (by Skoleim always possible to eliminate quantifiers when you can add a lot of functions); without $y>0$ you cannot eliminate quantifiers, even though

$$y>0 \text{ can be replaced by } \exists x\, x^2=y$$

– method of proof: based on Tarski-query (hence the terminology), induction on the number of variables, signed remainder sequence with discussions when coefficients vanish

– start with equalities, get inequalities

– example of polynomial of degree 4

- example

  General polynomial of degree 4 $P=X^4+a\,X^2+b\,X+c$.

  Signed remainder sequence of P and P'

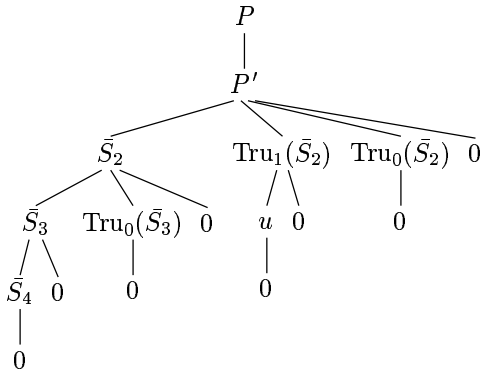
$$\begin{aligned}P &= X^4+a\,X^2+b\,X+c\\ P' &= 4\,X^3+2\,a\,X+b\\ S_2 &= -\mathrm{Rem}(P,P')\\ &= -\frac{1}{2}a\,X^2-\frac{3}{4}b\,X-c\\ S_3 &= -\mathrm{Rem}(P',S_2)\\ &= \frac{\left(8\,a\,c-9\,b^2-2\,a^3\right)X}{a^2}-\frac{b\left(12\,c+a^2\right)}{a^2}\\ S_4 &= -\mathrm{Rem}(S_2,S_3)\\ &= \frac{1}{4}\frac{a^2\left(256\,c^3-128\,a^2\,c^2+144\,a\,c\,b^2-16\,a^4\,c-27\,b^4-4\,b^2\,a^3\right)}{\left(8\,a\,c-9\,b^2-2\,a^3\right)^2}\end{aligned}$$

Note that when (a, b, c) are specialized to values in $\mathbb{C}^3$ for which $a = 0$ or $8\,a\,c - 9\,b^2 - 2\,a^3 = 0$, the signed remainder sequence of P and P' for these special values is not obtained by specializing a, b, c in the signed remainder sequence in $\mathbb{Q}(a, b, c)[X]$.

Denoting

$$\begin{aligned}
\overline{S_2} &= -8\,a\,X^2 - 12\,b\,X - 16\,c,\\
\overline{S_3} &= (8\,a\,c - 9\,b^2 - 2\,a^3)X - b\,(12\,c + a^2),\\
\overline{S_4} &= a^2\left(256\,c^3 - 128\,a^2\,c^2 + 144\,a\,b^2\,c + 16\,a^4\,c - 27\,b^4 - 4\,a^3\,b^2\right),\\
u &= b\left(-27\,b^4 + 72\,a\,c\,b^2 + 256\,c^3\right)\text{(remainder when } a = 0)
\end{aligned}$$

the tree of possible remainders of P, P' TRems(P, P') is the following. Tru stands for truncation.



Define

$$\begin{aligned}
s &= 8\,a\,c - 9\,b^2 - 2\,a^3,\\
t &= -b\,(12\,c + a^2)\\
\delta &= 256\,c^3 - 128\,a^2\,c^2 + 144\,a\,b^2\,c + 16\,a^4\,c - 27\,b^4 - 4\,a^3\,b^2.
\end{aligned}$$

The leftmost path in the tree going from the root to a leaf, namely the path $P, P', S_2, S_3, S_4, 0$ can be understood as follows: if $(a, b, c) \in \mathrm{C}^3$ are such that the degree of the polynomials in the remainder sequence of P and P' are $4, 3, 2, 1, 0$, i.e. when $a \neq 0$, $s \neq 0$, $\delta \neq 0$ (getting rid of obviously irrelevant factors), then the signed remainder sequence of $P = X^4 + a\,X^2 + b\,X + c$ and P' is proportional (up to non-zero squares of elements in C) to $P, P', \overline{S_2}, \overline{S_3}, \overline{S_4}$.

e describe the projection of the algebraic set

$$\{(a, b, c, X) \in \mathrm{R}^4 \mid X^4 + a\,X^2 + b\,X + c = 0\}$$

to R^3, i.e. the set

$$\{(a; b; c) \in \mathrm{R}^3 \mid \exists X \in \mathrm{R} \quad X^4 + a\,X^2 + b\,X + c = 0\},$$

as a semi-algebraic set.

We look at all leaves of TRems(P, P') and at all possible signs for leading coefficients of all possible signed pseudo-remainders (using Example $-$). We denote by n the difference between the number of sign variations at $-\infty$ and $+\infty$ in the Sturm sequence of $P = X^4 + a\,X^2 + b\,X + c$ for each case.

$$(a \neq 0 \wedge s \neq 0 \wedge \delta \neq 0, (4, 3, 2, 1, 0))$$

a	$-$	$-$	$-$	$-$	$+$	$+$	$+$	$+$
s	$+$	$+$	$-$	$-$	$+$	$+$	$-$	$-$
δ	$+$	$-$	$+$	$-$	$+$	$-$	$+$	$-$
n	4	2	0	2	0	-2	0	2

The first column can be read as follows: for every polynomial

$$P = X^4 + a\,X^2 + b\,X + c$$

satisfying $a < 0, s > 0, \delta > 0$, the number of real roots is 4. Indeed the degrees of the polynomials in the signed pseudo-remainder sequence of P and P' are $4, 3, 2, 1, 0$, the signs of the signed pseudo-remainder sequence of P and P' at $-\infty$ are $+-+-+$ and at $+\infty$ are $+++++$.

Similarly, for the other leaves of $\mathrm{TRems}(P, P')$

$$(a \neq 0 \wedge s \neq 0 \wedge \delta = 0, (4, 3, 2, 1))$$

a	$-$	$-$	$+$	$+$
s	$+$	$-$	$+$	$-$
n	3	1	-1	1

$$(a \neq 0 \wedge s = 0 \wedge t \neq 0, (4, 3, 2, 0))$$

a	$-$	$-$	$+$	$+$
t	$+$	$-$	$+$	$-$
n	2	2	0	0

$$(a \neq 0 \wedge s = t = 0, (4, 3, 2))$$

a	$-$	$+$
n	2	0

$$(a = 0 \wedge b \neq 0 \wedge u \neq 0, (4, 3, 1, 0))$$

b	$+$	$+$	$-$	$-$
u	$+$	$-$	$+$	$-$
n	2	0	0	2

$$(a = 0 \wedge b \neq 0 \wedge u = 0, (4, 3, 1))$$

b	$+$	$-$
n	1	1

$$(a = b = 0 \wedge c \neq 0, (4, 3, 0))$$

c	$+$	$-$
n	0	2

$$(a = b = c = 0, (4, 3))$$

$$n \;=\; 1$$

Finally, the formula $\exists\, X \quad X^4 + a\,X^2 + b\,X + c = 0$ is R-equivalent to the quantifier-free formula $\Phi(a, b, c)$:

$$\begin{array}{c}
(a < 0 \wedge s > 0) \\
\vee\ (a < 0 \wedge s < 0 \wedge \delta < 0) \\
\vee\ (a > 0 \wedge s < 0 \wedge \delta < 0) \\
\vee\ (a < 0 \wedge s \neq 0 \wedge \delta = 0) \\
\vee\ (a > 0 \wedge s < 0 \wedge \delta = 0) \\
\vee\ (a < 0 \wedge s = 0 \wedge t \neq 0) \\
\vee\ (a < 0 \wedge s = 0 \wedge t = 0) \\
\vee\ (a = 0 \wedge b < 0 \wedge u < 0) \\
\vee\ (a = 0 \wedge b > 0 \wedge u > 0) \\
\vee\ (a = 0 \wedge b \neq 0 \wedge u = 0) \\
\vee\ (a = 0 \wedge b = 0 \wedge c < 0) \\
\vee\ (a = 0 \wedge b = 0 \wedge c = 0),
\end{array}$$

by collecting all the sign conditions with $n \geq 1$. Thus, we have proven that the projection of the algebraic set

$$\{(x, a, b, c) \in \mathrm{R}^4 \mid x^4 + a\,x^2 + b\,x + c\}$$

into R^3 is the semi-algebraic subset defined by Φ.

– issues in constructive mathematics: clearly an algorithm, complexity issues: not elementary recursive, needs a discrete field where the sign of an element is well defined.

• 4.2 Seidenberg

– Seidenberg: use distance to a fixed point, more geometrical

• [13]

Seidenberg has many contributions to constructive commutative algebra: see his paper Constructions in algebra. Particularly: impossibility to factorize in a general field.

• 4.3 Collins

– Collins: use subresultants rather than signed remainder sequence, simplifies complexity of Tarski

• [3] , see [1]

doubly exponential complexity in terms of the number of variables

example

• polynomial of degree 4

Consider again $P = X^4 + a\,X^2 + b\,X + c$,

$$\begin{aligned}
\mathrm{sDisc}_3(P) &= 4,\\
\mathrm{sDisc}_2(P) &= -8\,a,\\
\mathrm{sDisc}_1(P) &= 4\,(8\,a\,c - 9\,b^2 - 2\,a^3)\\
\mathrm{sDisc}_0(P) &= 256\,c^3 - 128\,a^2\,c^2 + 144\,a\,b^2\,c + 16\,a^4\,c - 27\,b^4 - 4\,a^3\,b^2.
\end{aligned}$$

Let

$$\begin{aligned}
s &= 8\,a\,c - 9\,b^2 - 2\,a^3,\\
\delta &= 256\,c^3 - 128\,a^2\,c^2 + 144\,a\,b^2\,c + 16\,a^4\,c - 27\,b^4 - 4\,a^3\,b^2.
\end{aligned}$$

We indicate in the following tables the number of real roots of P in the various cases corresponding to all the possible signs for a, s, δ:

1	+	+	+	+	+	+	+	+	+
4	+	+	+	+	+	+	+	+	+
$-a$	+	+	+	+	+	+	+	+	+
s	+	+	+	−	−	−	0	0	0
δ	+	−	0	+	−	0	+	−	0
n	4	2	3	0	2	1	2	2	2

1	+	+	+	+	+	+	+	+	+
4	+	+	+	+	+	+	+	+	+
$-a$	−	−	−	−	−	−	−	−	−
s	+	+	+	−	−	−	0	0	0
δ	+	−	0	+	−	0	+	−	0
n	0	−2	−1	0	2	1	0	0	0

1	$+$	$+$	$+$	$+$	$+$	$+$	$+$	$+$	$+$
4	$+$	$+$	$+$	$+$	$+$	$+$	$+$	$+$	$+$
$-a$	0	0	0	0	0	0	0	0	0
s	$+$	$+$	$+$	$-$	$-$	$-$	0	0	0
δ	$+$	$-$	0	$+$	$-$	0	$+$	$-$	0
n	2	0	1	0	2	1	0	2	1

We represent in Figure 1 the set of polynomials of degree 4 in the plane $a = -1$ and the zero sets of s, δ.

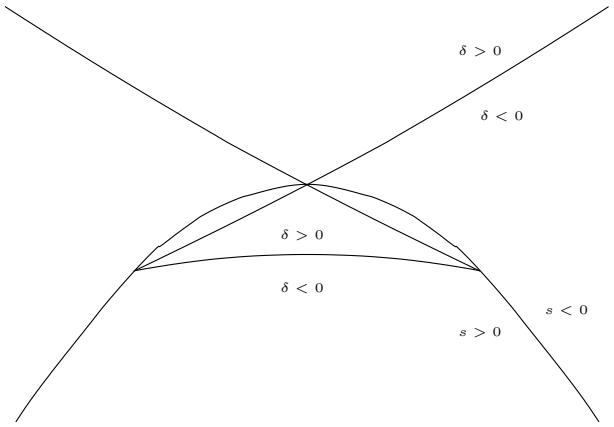


Figure 1. $a = -1, s = \delta = 0$

Finally, in Figure 2 we represent the set of polynomials of degree 4 in a, b, c space and the zero sets of s, δ.

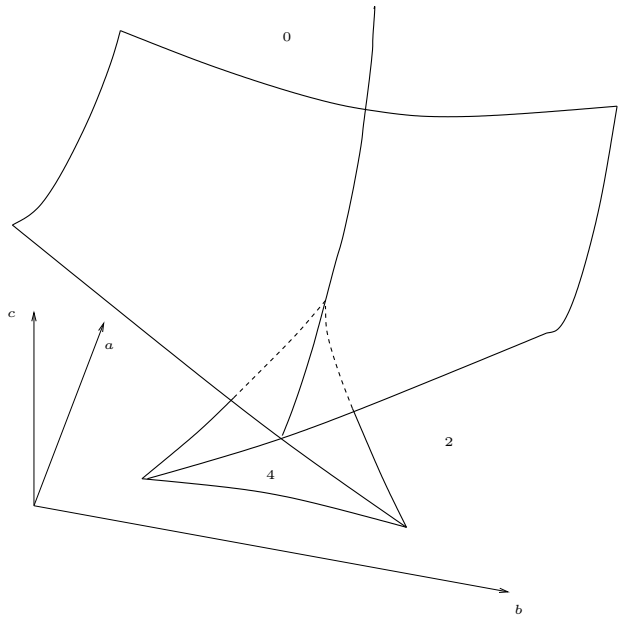


Figure 2. The set defined by $\delta = 0$ and the different regions labelled by the number of real roots

– issues in constructive mathematics: double exponential complexity.

Bibliography

1. S. BASU, R. POLLACK, M.-F. ROY, *Algorithms in real algebraic geometry*, Springer-Verlag, second edition (2006). Interactive version.
2. F. BUDAN DE BOISLAURENT, *Nouvelle méthode pour la résolution des équations numériques d'un degré quelconque*, (1807), 2nd edition, Paris (1822).
3. G. COLLINS, *Quantifier elimination for real closed fields by cylindric algebraic decomposition*, In Second GI Conference on Automata Theory and Formal Languages. Lecture Notes in Computer Science, vol. 33, 134–183, Springer- Verlag, Berlin (1975).
4. R. DESCARTES, *Géométrie* (1636). A source book in Mathematics, 90–31. Harvard University press (1969).
5. M. COSTE, T. LAJOUS-LOEZA, H. LOMBARDI, M.-F. ROY, *Generalized Budan-Fourier theorem and virtual roots*, Journal of Complexity, 21, 478–486, (2005).
6. J. FOURIER, *Analyse des équations déterminées*, F. Didot, Paris (1831).
7. C. F. GAUSS, *Demonstratio Nova Altera Theorematis Omnem Funct. Alg.*, Commentationes societatis regieae scientiarum Gottingensis recentiores, 3, 107–134 (1816). Werke III 31-56 (1876).
8. W. HABICHT, *Eine Verallgemeinerung des Sturmschen Wurzelzählverfahrens,* Comm. Math. Helvetici 21, 99–116 (1948).
9. C. HERMITE, *Remarques sur le théorème de Sturm*, C. R. Acad. Sci. Paris 36, 52–54 (1853).
10. S. LAPLACE, *Sur la résolution des équations. Théorème sur la forme de leurs racines imaginaires. Cinquième leçon*. Leçons Math. Ecole Normale (1795).
11. P. PEDERSEN, *Counting real zeroes of polynomials*, PhD Thesis, Courant Institute, New York University (1991).
12. P. PEDERSEN, M.-F. ROY, A. SZPIRGLAS, *Counting real zeroes in the multivariate case*, Computational algebraic geometry, Eyssette et Galligo ed. Progress in Mathematics 109, 203–224, Birkhauser (1993).
13. A. SEIDENBERG, *A new decision method for elementary algebra*, Annals of Mathematics, 60:365–374, (1954).
14. C. STURM, *Mémoire sur la résolution des équations numériques.* Inst. France Sc.Math. Phys.6 (1835).
15. J. J. SYLVESTER, *On a theory of syzygetic relations of two rational integral functions, comprising an application to the theory of Sturm's function.* Trans. Roy. Soc. London (1853).
16. A. TARSKI, *A Decision method for elementary algebra and geometry*, University of California Press (1951).