To be Announced

by Fabrice Rouillier

INRIA Paris

OURAGAN TEAM
IMJ-PRG - Sorbonne Université - Paris Université

General Framework : certified algorithms for studying the real roots of systems of polynomial {equations, inequations, inequalities}

- Certified algorithms
  - Always end
  - Never provide wrong results
  - Never based on uncheckable assumptions
- Real roots of systems of polynomial {equations, inequations, inequalities}
  - univariate polynomials
  - zero-dimensional systems
  - parametric generically zero-dimensional systems
  - general positive dimensional systems
- Focus on systems of two equations in two variables with rational coefficients.

Zero-dimensional systems

$I \subset \mathbb{Q}[X_1, ..., X_n]$

$t = X_1 + u_2 X_2 + \cdots + u_n X_n$, $f_t = \prod_{\alpha \in V(I)} (T - t(\alpha))^{\mu(\alpha)}$,

$v \in \{1, X_1, ..., X_n\}$, $f_{v,t} = \sum_{\alpha \in V(I)} \mu(\alpha) v(\alpha) \big(\prod_{\beta \in V(I), \beta \neq \alpha} (T - t(\beta)) \big)$

Then $f_t \in \mathbb{Q}[T]$, $f_{t,v} \in \mathbb{Q}[T]$ and, if t separates $V(I)$,

$$\begin{array}{lcl} V(\langle f, g \rangle) & \approx & V(f_t) \\ \alpha = (\alpha_1, ..., \alpha_n) & \to & t(\alpha) \\ (\frac{f_{t,X_1}(\beta)}{f_{t,1}(\beta)}, ..., \frac{f_{t,X_n}(\beta)}{f_{t,1}(\beta)}) & \leftarrow & \beta \end{array}$$

and the multiplicities of the zeroes are preserved.

$\bar{f}_t(T) = H_d = \sum_{i=0}^{d} a_i T^{d-i} = \prod_{\alpha \in V_{\mathbb{C}}(I)} (T - t(\alpha))$

$g_{t,v}(T) = \sum_{i=0}^{d-1} \mathrm{Trace}(M_{vt^i}) H_{d-i-1}(T)$ with $H_j(T) = \sum_{i=0}^{j} a_i T^{j-i}$

$P = \sum_{i=0}^{d} a_i X^i \in \mathbb{Z}[X]$ with $a_d = 1$ and $a_0 \neq 0$ without multiple factors.

- $P(\alpha) = 0 \Rightarrow |\alpha| < 1 + \max_{i=0}^{d}(|a_i|)$
- $\mathrm{Sep}(P) = \min_{\alpha \neq \beta, \alpha, \beta \in V(P)} |\alpha - \beta| \geq \sqrt{\frac{3}{d^d + 2}} \cdot \frac{1}{||P||_2^{d-1}}$ where $||P||_2 = \sqrt{\sum_{i=0}^{d} a_i^2}$

We can thus assume that we look for roots in $I_{0,0} =]0, 1[$

Algorithm Bissection($I_{k,c}$,p,V)

Input : $I_{k,c} =]\frac{c}{2^k}, \frac{c+1}{2^k}[$, $p \in \mathbb{Q}[X]$ square-free, $V(p, I)$ counts the number of root of p in an open interval I

Output : $\{I_{k',c'} \subseteq I_{k,c}, V(p, I_{k',c'}) = 1\}$

/* the enpoints $\frac{c+1}{2^k}$ are considered separately : suppose $P(\frac{c+1}{2^k}) \neq 0$ */

If $V(p, I_{k,c}) = 1$ **then** RETURN($\{I_{k,c}\}$);

If $V(p, I_{k,c}) > 1$ **then** RETURN(Bissection($I_{k+1,2c}$,p)$\cup$Bissection($I_{k+1,2c+1}$, p))

RETURN($\{\}$)

Univariate polynomials

1970's replace the count by a bound (Descartes' rule of signs) : Collin's / Akritas

1990's speed up with trys using interval arithmetic (Krandick)

2000's Multiprecision interval arithmetic (Zimmermann and R.)

2016 Quasi-optimal algorithm $\tilde{O}(d\,t + d^2)$ bit operations (Köbel, Sagraloff, R.)

$$\mathcal{E} = \{p_1, ..., p_r\}, \mathcal{F} = \{f_1, ..., f_l\}, \text{ with } p_i, f_i \in \mathbb{Q}[U, X]$$

$$U = U_1, ..., U_d \Rightarrow \textbf{parameters}$$

$$X = X_{d+1}, ..., X_n \Rightarrow \textbf{ indeterminates}$$

$$\mathcal{C} = \{x \in \mathbb{C}^n, p_1 = 0, ..., p_r = 0, f_1 \neq 0, ..., f_s \neq 0\}$$

$$\mathcal{S} = \{x \in \mathbb{R}^n, p_1 = 0, ..., p_r = 0, f_1 > 0, ..., f_s > 0\}$$

- $\Pi_U : \mathbb{C}^n \longrightarrow \mathbb{C}^d$ the canonical proj. on the parameters' space.
- $\phi_u : U \mapsto u$ (specialization map)

We suppose that $\overline{\Pi_U(V(\mathcal{C}))} = \mathbb{C}^d$.

If one wants (at least) to discuss the number of roots, one needs to characterize parameter's subsets $\mathcal{U} \subset \Pi_U(\mathcal{C})$ such that $\#(\Pi_U^{-1}(u) \cap \mathcal{C})$ is constant over $\mathcal{U}$.

$O_\infty = \alpha \in \mathbb{C}^k$ such that $\Pi_U^{-1}(\mathcal{U}) \cap \mathcal{S}$ is not compact for any compact neighborhood $\mathcal{U}$ of α in $\mathbb{C}^k$

$O_c =$ projection on the parameter space of the singular points of $\mathcal{S}$ and critical values of the projection onto the parameter space. In other words $O_c = \Pi_U(\mathcal{E} \cap \{X \in \mathbb{C}^n, \mathrm{Jac}(\mathcal{E}, X) = 0\})$ onto the parameter space.

O_{sd} the projection by Π_U of components of $\mathcal{C}$ of dimension$<\dim(\mathcal{C})$ (empty under our conditions)

When having inequalities/inequations : $O_{\mathcal{F}} = \left\{ u \in \overline{\Pi_U(\mathcal{C})}, \Pi_U^{-1}(u) \cap \bar{\mathcal{C}} \cap V(\Pi_{f \in \mathcal{F}}) \neq \emptyset \right\}$, then necessarilly $\mathcal{U} \cap O_{\mathcal{F}} = \emptyset$.

Discriminant Variety (2007) $\mathcal{D} = O_\infty \cup O_c \cup O_{\mathrm{sd}} \cup O_{\mathcal{F}}$ is an algebraic variety, and is the smallest algebraic variety such that $\forall \mathcal{U} \in \Pi_U(\mathcal{C})$, $\mathcal{U} \cap \mathcal{D} = \emptyset$, $(\Pi_U^{-1}(\mathcal{U}) \cap \mathcal{C}, \Pi_U)$ is an analytic cover of $\mathcal{U}$.

Computation (2007) : $O_\infty = \overline{O_\infty}$ can be "read" on a Gröbner basis, $\overline{O_c} = V(\langle \mathcal{E}, \mathrm{Jac}(\mathcal{E}, X) \rangle \cap \mathbb{Q}[U])$, $\overline{O_{\mathcal{F}}}$ $V(\langle \mathcal{E}, \prod_{f \in \mathcal{F}} f \rangle \cap \mathbb{Q}[U])$ in favorable situations (in fact one must saturate before by $\prod_{f \in \mathcal{F}} f$)

$\mathcal{S} = \{p_1, ..., p_r\} \subset \mathbb{Q}[X_1, ..., X_n]$ with $\dim(V(\mathcal{S})) = d$.

- $V = V(\mathcal{S}) \subset \mathbb{C}^n$

The principle : $A \in \mathbb{Q}^n$, the set of extrema of $d(A, V(\mathcal{S}) \cap \mathbb{R}^n)$ intersects each connected component of $V(\mathcal{S}) \cap \mathbb{R}^n$.

In practice :

$V(\mathcal{C}(A)) = \{M \in V(\mathcal{S}), \mathrm{rank}(\mathrm{grad}_M(p_1), ...\mathrm{grad}_M(p_r), \overrightarrow{\mathrm{AM}})\} \leq n - d$;

$V(\mathcal{J}) = \{M \in V(\mathcal{S}), \mathrm{rank}(\mathrm{grad}_M(p_1), ..., \mathrm{grad}_M(p_r))\} < n - d$.

Result (Aubry, R., Safey El Din, 2002):

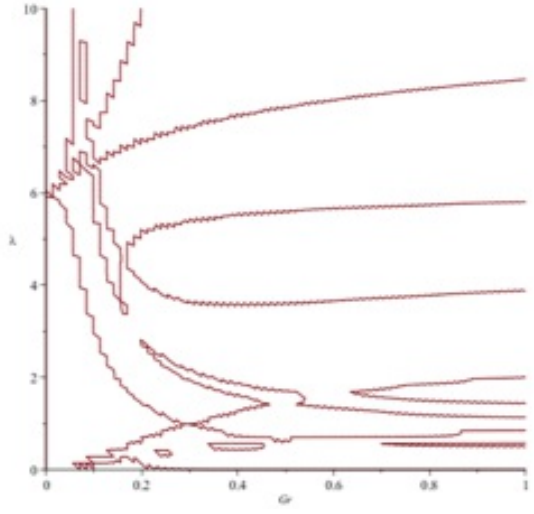
If $\langle p_1, ..., p_r \rangle$ is equi-dimensionnal and radical, then $\exists D \in \mathbb{N}^\star$ and $A \in \{1, ..., D\}^n$:

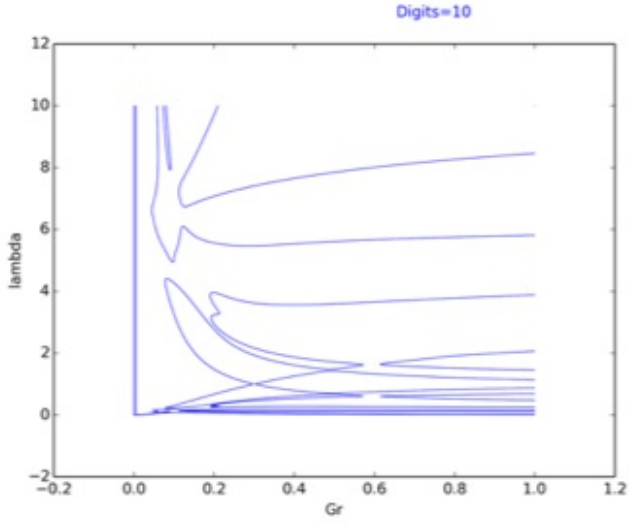
- $V(\mathcal{C}(A))$ intersects each semi-algebric connectec component of $V \cap \mathbb{R}^n$;
- $V(\mathcal{C}(A)) = V(\mathcal{J}) \cup V_{0,A}$ with $\#V_{0,A} < \infty$;
- $\dim(V(\mathcal{J})) < \dim(V)$;

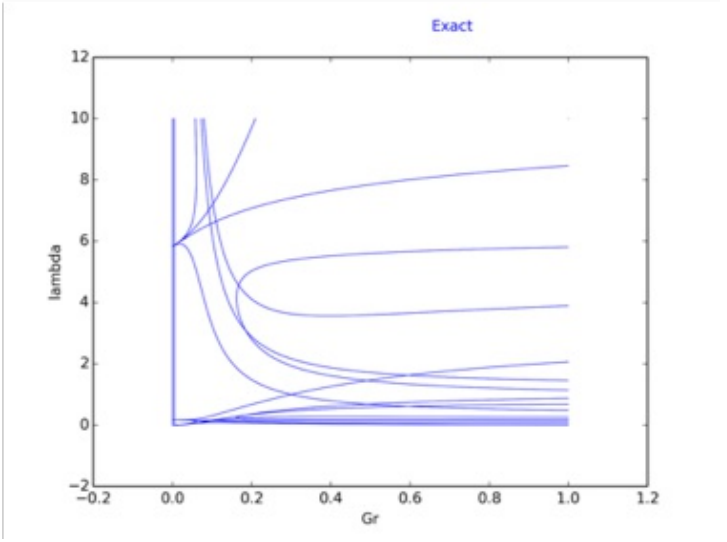
$$\mathcal{C} = \{(x, y) \in \mathbb{R}^2, P(x, y) = 0, P \in \mathbb{Q}[X, Y]\}$$

- **Step 1. Computing a finite set of study points.**
  - Projection of singular points of $\mathcal{C}$:
$$\mathcal{S}_c = \left\{x \in \mathbb{R}, (x, y) \in \mathcal{C}, \frac{\partial P}{\partial X}(x, y) = 0, \frac{\partial P}{\partial Y}(x, y) = 0\right\}$$
  - Critical values of the projection wrt some direction :
$$\mathcal{S}_Y = \left\{x \in \mathbb{R}^2, (x, y) \in \mathcal{C}, \frac{\partial P}{\partial Y}(x, y) = 0\right\}$$
  - Projection of "points at infinity" of $\mathcal{C}$: $\mathcal{S}_\infty = \{x \in \mathbb{R}, \mathrm{Lc}_Y(P) = 0\}$
- **Step 2. Computing the (local) topology arround the characteristic points.**
  - At least the number of half branches crossing a small box containing a study point ("approximate topology")
- ***Step 3. Connecting the local descriptions*** *of $\mathcal{C}$ around the points of $\mathcal{S}$ to get an isotopic description of $\mathcal{C}$ by means of a graph.*

Systems in 2 variables : motivations






Exact
lambda
Gr
12
10
8
6
4
2
0
−2
−0.2
0.0
0.2
0.4
0.6
0.8
1.0
1.2

$f, g \in \mathbb{D}[Y] \quad \Rightarrow \quad (s_i f + t_i g = r_i)_{i=1\ldots l}$ avec $s_i, t_i, r_i \in \mathbb{F}[Y]$

$\rho_0 = \mathrm{lc}(f), \rho_1 = \mathrm{lc}(g), r_0 = \frac{f}{\rho_0}, r_1 = \frac{g}{\rho_1}, s_0 = \frac{1}{\rho_0}, s_1 = 0, t_0 = 0, t_1 = \frac{1}{\rho_1}, i = 1$

While $(r_i \neq 0)$ do

- $q_i, r_{i+1} = \mathrm{Division}(r_{i-1}, r_i)$
- $\rho_{i+1} = \mathrm{lc}(r_{i+1})$, $r_{i+1} = \frac{r_{i+1}}{\rho_{i+1}}$, $s_{i+1} = \frac{s_{i-1} - q_i s_i}{\rho_{i+1}}$, $t_{i+1} = \frac{t_{i-1} - q_i t_i}{\rho_{i+1}}$
- i:=i+1

l=i-1

RETURN$(l, (\rho_i, s_i, t_i, r_i)_{i=0\ldots l+1}, (q_i)_{i=1\ldots l})$

EEA vs Normalized EEA

$\underbrace{q_i, r_i, t_i, s_i}_{\text{Normalized}} \quad \underbrace{q_i^\star, r_i^\star, t_i^\star, s_i^\star}_{\text{Classical}} \quad \alpha_i = \left\{ \begin{array}{l} \rho_i \rho_{i-2} \cdots \rho_2 \rho_0 \ \text{ if } i \text{ is odd} \\ \rho_i \rho_{i-2} \cdots \rho_3 \rho_1 \ \text{ if } i \text{ is even} \end{array} \right\}$

then $q_i^\star = \frac{\alpha_{i-1}}{\alpha_i} q_i$, $r_i^\star = \alpha_i r_i$, $s_i^\star = \alpha_i s_i$ and $t_i^\star = \alpha_i t_i$

$$\begin{array}{rccc} \Phi_k : & P_{m-k} \times P_{n-k} & \to & P_{n+m-2k} \\ & (s,t) & & (s\,f + t\,g) \operatorname{quo} Y^k \end{array}$$

Convention : if $l<0, u_l=0$ and P_l= polynomials of degree $<l$

$$S_k = \left(\underbrace{\begin{array}{cccc} f_n & 0 & \cdots & 0 \\ f_{n-1} & f_n & \ddots & \vdots \\ \vdots & & \ddots & 0 \\ f_{n-m+k+1} & \cdots & \cdots & f_n \\ \vdots & & & \vdots \\ f_{k+1} & \cdots & \cdots & f_m \\ \vdots & & & \vdots \\ \vdots & & & \vdots \\ f_{2k-m+1} & \cdots & \cdots & f_k \end{array}}_{m-k} \underbrace{\begin{array}{ccccc} g_m & 0 & \cdots & \cdots & 0 \\ g_{m-1} & g_m & \ddots & & \vdots \\ \vdots & & \ddots & \ddots & \vdots \\ g_{k+1} & \cdots & \cdots & g_m & \vdots \\ \vdots & & & & 0 \\ g_{m-n+k+1} & \cdots & \cdots & \cdots & g_m \\ \vdots & & & & \vdots \\ \vdots & & & & \vdots \\ g_{2k-n+1} & \cdots & \cdots & \cdots & g_k \end{array}}_{n-k} \right)$$

If $s = \sum_{i=0}^{m-k-1} y_i\,X^i$, $t = \sum_{i=0}^{n-k-1} y_i\,X^i$ and $s\,f + t\,g = \sum_{i=0}^{n+m-k-1} u_i\,X^i$, then

$S_k\,[y_{m-k-1}, \ldots, y_0, z_{n-k-1}, \ldots z_0]^T = [u_{n+m-k-1}, \ldots, 0, u_k]^T$

Basic tools

Let (r_i, s_i, t_i) be the sequence that appears in the normalized EEA : $r_i = s_i\, f + t_i\, g$

Set $n_i = \deg(r_i)$ and $\sigma_{n_i} = \det(S_{n_i})$

- if $f, g \in \mathbb{D}[X]$, then
  - $r_i, s_i, t_i \in \mathbb{F}[X]$ where $\mathbb{F}$ is the fraction field of $\mathbb{D}$
  - $\underbrace{\sigma_{n_i} r_i}_{\in \mathbb{D}} = \underbrace{\sigma_{n_i} s_i}_{\in \mathbb{D}} f + \underbrace{\sigma_{n_i} t_i}_{\in \mathbb{D}} g$
- $k \in \{n_0, ..., n_l\} \iff \sigma_k \neq 0$ (Φ_k is an isomorphism)
- In fact, if $k = n_i < n$ and if $(y_0, ..., y_{m-k-1}, z_{n-k-1}, ...z_0)$ is the unique solution of $S_k\, [y_{m-k-1}, ..., y_0, z_{n-k-1}, ...z_0]^T = [0, ..., 0, 1]^T$, then

$$s_i = \sum_{0 \leqslant j < m-k} y_j X^j \quad \text{and} \quad t_i = \sum_{0 \leqslant j < n-k} z_j X^j$$

Basic tools

$$\sigma_k = \begin{cases} (-1)^{\tau_i} \rho_0^{m-n_i} \prod_{1 \leqslant j \leqslant i} \rho_j^{n_{j-1}-n_j} \text{ with } \tau_i = \sum_{1 \leqslant j \leqslant i} (n_{j-1}-n_i)(n_j-n_i) & \text{if } k = n_i \\ 0 & \text{otherwise} \end{cases}$$

Input : A and B in $\mathbb{D}$[X] with deg(B) < deg(A)

Output : the last non nul subresultant of A and B

- f=g=s=1.
- while deg(B)>0
  - d=deg(A)−deg(B)
  - R=pseudoRemainder(A,B)
  - if deg(A) and deg(B) are odd set $s := -s$
  - $A := B$ and B:=$\frac{R}{f\, g^d}$ and f:=Lc(A) and $g := \frac{f^d}{g^{d-1}}$
- d:=deg(A)
- B:=$\frac{s\, B^d}{g^{d-1}}$

All the divisions performed are EXACT

Let define

- σ_{n_i}=$\mathrm{sres}_{n_i}(f,g) = n_i$-th (principal) subresultant coefficient
- $\sigma_{n_i} r_i = \mathrm{Sres}_{n_i}(f,g)$= n_i-th subresultant polynomial

A fundamental result is the following :

Let $\phi : \mathbb{D} \to \mathbb{D}'$ be a ring morphism such that $\phi(\mathrm{Lc}(f)\,\mathrm{Lc}(g)) \neq 0$, then ,

$$\phi(\mathrm{Sres}_k(f,g)) = \mathrm{Sres}_k(\phi(f),\phi(g))$$

Definition : the subresultant $\mathrm{Sres}_0(f,g)$ of degree 0 is the resultant of the two polynomials.

Property : $f, g \in \mathbb{D}[X]$ have a commun factor in $\mathbb{D}[X]$ if and only if their resultant is null

A direct consequence is the following :

If $f, g \in \mathbb{Q}[X][Y]$, then the (complex) roots of $\mathrm{Sres}_0(f,g)$ are the values that either cancel $\mathrm{Lc}_Y(f)$ and $\mathrm{Lc}_Y(g)$ or the X-coordinate of roots of $f = 0, g = 0$.

Basic tools

Note : $\mathrm{sres}_k(f,g)=0 \Rightarrow \mathrm{Sres}_k(f,g)\equiv 0$

$\boldsymbol{R=\mathbf{Sres_0}(f,g)}$ is the resultant of (f,g)

$f,g\in\mathbb{Z}[Y]$, $R\in\mathbb{Z}\quad R=0\Longleftrightarrow \deg(\gcd(f,g))>0$

Moreover, if $l=\inf\{k,\mathrm{sres}_k(f,g)\neq 0\}$ then $\mathrm{Sres}_l(f,g)\sim\gcd(f,g)$

$f,g\in\mathbb{Z}[X,Y], R\in\mathbb{Z}[X]$ then $R(a)=0$ for some $a\in\mathbb{C}$ if and only of

either $\mathrm{lc}_Y(f)(a)=0$ or $\mathrm{lc}_Y(g)(a)=0$

or $\exists l_a=\inf\{k,\mathrm{sres}_k(f,g)(a)\neq 0\}$ and $\mathrm{Sres}_{l_a}(f,g)(a,Y)\sim\gcd(f(a,Y),g(a,Y))$

In particular if $R\equiv 0$, then f,g have a commun factor.

One can then decompose the system $\{f=0, g=0\}$ into a finite union of triangular systems $\cup_{i=1}^{m-1}\{\mathrm{Sres}_i(f,g), R_i(f,g)\}$ where $\mathrm{Sres}_0(f,g) = R_0 \prod_{i=1}^{m} R_i$ where the $R_i \in \mathbb{Q}[X]$ are coprime.

$G_0 = \mathrm{squareFreePart}(\mathrm{Sres}_0(f,g))$

for $i = 1 \ldots m-1$

- $G_i = \gcd\left(\mathrm{sres}_i(f,g), G_{i-1}\right)$
- $R_i = \frac{G_{i-1}}{G_i}$

$R_0 = G_{m-1}$

Remark : There is a unique solution to $\{f(\alpha, Y) = 0, g(\alpha, Y) = 0\}$ or, equivalently to $\{R_i(\alpha) = 0, \mathrm{Sres}_i(\alpha, Y) = 0\}$,

iff $\mathrm{Sres}_i(\alpha, Y) = \mathrm{sres}_i(\alpha)\,(Y - b(\alpha))^i$

iff $\overline{\mathrm{Sres}_i}(\alpha, Y) = \mathrm{sres}_i(\alpha)\,(Y - b(\alpha))^i$ where $\overline{\mathrm{Sres}_i}(X, Y) = \mathrm{sres}_i(X)(Y - b(X))^i \bmod R_i(X)$

In such case, the (unique) solution above α is : $\left(\alpha, -\frac{\mathrm{sres}_{i,i-1}(\alpha)}{i\,\mathrm{sres}_{i,i}(\alpha)}\right)$

Remark : the identification $\mathrm{Sres}_i(X, Y) = \mathrm{sres}_{i,i}(X)(Y - b(X))^i$ can provide an algorithm to decompose reach $\{R_i(X), \mathrm{Sres}_i(X, Y)\}$ into two disjoint components $\{\mathrm{Ru}_i(X), \mathrm{Sres}_i(X, Y)\}$ and $\{\mathrm{Rm}_i(X), \mathrm{Sres}_i(X, Y)\}$ such that

- $\{\mathrm{Ru}_i(X), \mathrm{Sres}_i(X, Y)\}$: over each root of Ru_i, $\mathrm{Sres}_i(X, Y)$, has a unique root
- $\{\mathrm{Rm}_i(X), \mathrm{Sres}_i(X, Y)\}$: over each root of Rm_i, $\mathrm{Sres}_i(X, Y)$, has a least 2 roots

We thus get and algorithm that computes $\cup_{i=1}^{d_g}\left\{R_i(X) = 0, Y = -\frac{\mathrm{sres}_{i,i-1}(X)}{i\,\mathrm{sres}_{i,i}(X)}\right\} \cup \{R_0(X)\}$

Finding $a \in \mathbb{Z}$ such that $\forall \alpha, \beta \in V(\langle f, g \rangle)$, $\alpha \neq \beta \Rightarrow t(\alpha) \neq t(\beta)$ with $t = X + a\,Y$.

If T separates the roots then we get $\cup_{i=1}^{d_g} \left\{ R_i(T) = 0, Y = -\frac{\mathrm{sres}_{i,i-1}(T)}{i\,\mathrm{sres}_{i,i}(T)}, X = T - a\,Y \right\}$

Naive algorithm :

Lemma : $\{X + a\,Y, a = 0 \ldots d^2\}$ contains at least a separating form.

The separating forms are those that maximize the degree of the squarefree part of $\mathrm{Resultant}(f(T - a\,Y, Y), g(T - a\,Y, Y), Y)$

Cost of the decomposition ?

Cost of finding a separating element ?

Expected vs worst case computation times

Example : $f, g \in \mathbb{Z}[X]$, with degree $\leqslant d$ and bitsize t.

$\gcd(f, g)$ has bitsize $O(t+d)$ and degree $\leqslant d$.

For almost all primes, $\gcd(f \bmod p, g \bmod p) = \gcd(f, g) \bmod p$

If lucky enough, one can expect computing the $\gcd$ in $\tilde{O}(d\,(t+d))$ bit operations. $\Rightarrow$ **Monte − Carlo algorithm**.

Unlucky primes are those dividing $\mathrm{Resultant}(f, g)$ which has bitsize $O(d\,t)$ and thus the **worst case algorithm** is in $\tilde{O}(d\,d\,t)$

If choosing primes that do not divide the leading coefficients, bad primes induces modular gcd of too high degree and the final result can be checked by a simple division.

$\Rightarrow$ **Las-Vegas algorithm.** Expected time (few bad primes in practice) $\tilde{O}(d(t+d))$

Computing subresultants

Fast computation of subresultants :

- Hadamard's bound for the coefficients sizes : degree $O(d^2)$, bitsize $O(d\,t)$
- Specialization property of subresultants $\Rightarrow$ can avoid easily bad primes and at least 1 luky prime per index in a set of $\tilde{O}(d\,t)$ primes.

Half-GCD like : 1 subresultant polynomial or all the principal subresultant coefficients can be computed in $\tilde{O}(d^4\tau)$ bit operations - « optimal »

Classical remainder sequence : the full subresultant sequence can be computed in $\tilde{O}(d^5\tau)$ bit operations.

Naive estimate : $O(d)$ gcds of polynomials of degrees $O(d^2)$ with bitsizes $O(d\,t+d^2)$ ..... too much ?.

Thm (2015) : $(R_i)_{i=0\dots d_f}$ can be computed in $\tilde{O}(d^5t+d^6)$ bit operations in the worst case and $\tilde{O}(d^4t+d^5)$ expected bit operations.

Main arguments : if $\deg(G_i)=d_i$ and t_i is the bitsize of G_i then each $G_i=\gcd\left(\mathrm{sres}_{i,i},G_{i-1}\right)$ is computed in $\tilde{O}(d^2\left(t_id^2+d_idt\right))$ bit operations in the worst case or $\tilde{O}(d\left(t_id^2+d_idt\right))$ expected bit operations.

Remark that $\mathrm{resultant}(f,g)=\prod R_i^{\mu_i}$ with $\mu_i\geqslant i$ so that $\prod R_i^i$ divides resultant(f,g) and so that each G_i^{i+1} divides $\mathrm{resultant}(f,g)$.

Then $d_i\leqslant\frac{d^2}{i+1}$ and $\sum d_i\leqslant d^2$.

Mahler measure for f of degree d and coefficients of bitsize t :

$M(f)=\mathrm{Lc}(f)\prod_{\alpha\in V(f)}\max\left(1,|\alpha|\right)$

$t\leqslant 1+d+\log(M(f))$ and $\log(M(f))=O(t+\log(d))$

G_i^{i+1} divides $R\ \Rightarrow\ M(G_i^{i+1})\leqslant M(R)\ \Rightarrow\ \log(M(G_i))\leqslant\frac{\log(M(R))}{i+1}$ and thus $t_i\leqslant 1+\frac{d^2}{i+1}+\frac{\log(M(R))}{i+1}$ so that $t_i=O\left(\frac{dt+d^2}{i+1}\right)$ and $\sum t_i=\tilde{O}(dt+d^2)$.

Def : the degree of the decomposition is $\mathrm{TriDeg}(f,g) = \sum_{i=1}^{d_f-1} i\,\mathrm{degree}(R_i)$

Corollary (2015) : One can compute $\mathrm{TriDeg}(f,g)$ in $\tilde{O}(d^5t + d^6)$ bit operations in the worst case and in $\tilde{O}(d^4t + d^5)$ expected bit operations.

Warning : it still claims $\tilde{O}(d^5t + d^6)$ to compute the full sequence of « usefull » subresultant polynomials.

Notation : if $(R_i,(X),\mathrm{Sres}_i(X,Y))_{i=0\ldots d_g-1}$ is a triangular decomposition of (f,g) such that $\mathrm{Sres}_i(\alpha,Y)\approx\gcd(f(\alpha,Y),g(\alpha,Y))$, $\forall\alpha, R_i(\alpha)=0$ and R_i squarefree, then $\mathrm{TriDeg}(f,g,Y):=\sum i\,\mathrm{degree}(R_i)$

If f and g squarefree, coprime and monic in Y the solutions of $\{f=0,g=0\}$ are contained in the finite set of critical points of the projection onto X of the curve $fg=h=0$: $\left\{h=0,\frac{\partial h}{\partial Y}=0\right\}$. $\left(\frac{\partial fg}{\partial y}=f\frac{\partial g}{\partial y}+g\frac{\partial f}{\partial y}=0\right)$.

The key point : let $(\alpha,\beta)\in V(h)$. The multiplicity of β as a zero of $\gcd\left(h(\alpha,Y),\left(\frac{\partial h}{\partial Y}\right)^2(\alpha,Y)\right)$ is greater by one than the multiplicity of β as a zero of $\gcd\left(h(\alpha,Y),\frac{\partial h}{\partial Y}(\alpha,Y)\right)$.

Taking the sum over the zeroes of $\langle h,\frac{\partial h}{\partial Y}\rangle$:

TriDeg($\langle h,\left(\frac{\partial h}{\partial Y}\right)^2\rangle$)-TriDeg($\langle h,\frac{\partial h}{\partial Y}\rangle$)=$\sharp$V($\langle h,\frac{\partial h}{\partial Y}\rangle$)

In particular, one can compute $\sharp$V($\langle h,\frac{\partial h}{\partial Y}\rangle$) in $\tilde{O}(d^5t+d^6)$ bit operations and in $\tilde{O}(d^4t+d^5)$ expected bit operations.

$\Rightarrow$ We know how to check if a linear form is separating V$\left(\langle h,\frac{\partial h}{\partial Y}\rangle\right)$ and thus $V(\langle f,g\rangle)$ or not

For computing a separating linear form, the game consists in

- looking for linear forms that separate $V\Big(\langle f\,g, \frac{\partial f\,g}{\partial Y}\rangle\Big)$
- finding a « good » prime number p such that if $X + a\,Y$ separates $V(\langle f \bmod p, g \bmod p\rangle)$ then it also separates $V(\langle f\,, g\rangle)$
- make several guess/check ($O(d^4)$) modulo p

A prime that is lucky for the specialization of the subresultants and lucky for the several univariate gcds in the decomposition preserves the degree of de decomposition ($\sum i\,\mathrm{degree}(R_i)$) and $\sharp V(\langle f \bmod p, g \bmod p\rangle) = \sharp V(\langle f\,, g\rangle)$.

The main unlucky primes for the additional gcd's computations in the decomposition :

- $G_0 = \gcd\left(\mathrm{Sres}_0, \mathrm{Sres}_0'\right)$
- $G_i = \gcd\left(G_{i-1}, \mathrm{sres}_{i,i}\right)$

These are primes that do not divide some subresultant coefficients.

The product of all these integers (certificate) has bitsize $\tilde{O}(d^3t + d^4)$ and can be computed in $\tilde{O}(d^5t + d^6)$ bit operations in the worst case using the same amortizing arguments as for the decomposition.

A deterministic search consists in (mainly) :

- Set $h = f\,g$ and compute $\sharp V\left(\langle h, \frac{\partial h}{\partial Y}\rangle\right)$
- Choose a prime p that do not divide the certificate for the decomposition of $\langle h, \frac{\partial h}{\partial Y}\rangle$
- Compute the resultant $R(s,T)$ of $f(T - SY, Y)$ and $g(T - SY, Y)$ modulo p
- Compute $R(a,T)$ mod p for $a = 1 \ldots 2\,d^4$ using multipoint evaluation.
- for $a = 1 \ldots 2\,d^4$ compute the squarefree part of $R(a,T)$ until its degree equals $\sharp V\left(\langle h, \frac{\partial h}{\partial Y}\rangle\right)$

Complexity in $\tilde{O}(d^5 t + d^6)$ in the worst case.

For the Las-Vegas variant, less room for doing computations over the integers.

The key ideas are

- Set $h = f\,g$ and compute $\sharp V\Big(\langle h, \frac{\partial h}{\partial Y}\rangle\Big)$
- choose « randomly » $a \leqslant 2\,d^4$ and a prime p
- compute the squarefree part of $\mathrm{resultant}\Big(h(T - a\,Y, Y), \frac{\partial h}{\partial Y}(T - a\,Y, Y)\Big)$ mod p

  and check if its degree equals $\sharp V\Big(\langle h, \frac{\partial h}{\partial Y}\rangle\Big)$

Note : in practice, choosing the prime (with a probability greater than 1/2 to be lucky) in the present case is a problem since one might compute an explicit bound for the number of primes to be used.

$t = X + aY$, $f_t = \prod_{\alpha \in V(\langle f,g \rangle)} (T - t(\alpha))^{\mu(\alpha)}$,

$v \in \{X, Y, 1\}$, $f_{v,t} = \sum_{\alpha \in V(\langle f,g \rangle)} \mu(\alpha) v(\alpha) \left(\prod_{\beta \in V(\langle f,g \rangle), \beta \neq \alpha} (T - t(\beta)) \right)$

Then $f_t \in \mathbb{Q}[T]$, $f_{t,v} \in \mathbb{Q}[T]$ and, if t separates $V(\langle f, g \rangle)$,

$$\begin{array}{lcl} V(\langle f, g \rangle) & \approx & V(f_t) \\ \alpha = (\alpha_1, ..., \alpha_n) & \rightarrow & t(\alpha) \\ (\frac{f_{t,x_1}(\beta)}{f_{t,1}(\beta)}, ..., \frac{f_{t,x_n}(\beta)}{f_{t,1}(\beta)}) & \leftarrow & \beta \end{array}$$

and the multiplicities of the zeroes are preserved.

In the bivariate case, all these polynomials can be viewed as specializations factors of polynomials in two variables with the same magnitude than some resultant.

$f_S(T, Y) = f(T - SY, Y), g_S(T, Y) = g(T - SY, Y)$

$R_S(S, T) = \text{Resultant}(f_S, g_S, Y)$

$f_t(T)$ divides $R(a, T)$, $f_{t,1}(T) = \overline{f'_t}(T)$, $f_{t,Y}(T)$ divides $\left(\frac{\partial R}{\partial S} - R \frac{\partial \text{Lc}(R)}{\partial S} \right)_{S=a}$

For $a \in \mathbb{Z}$ of bitsize $O(\log(d))$ such that $X + aY$ separates $V(\langle f, g \rangle)$, a RUR of the system has degree $\leqslant d^2$ and coefficients of bitsize in $\tilde{O}(d\,t + d^2)$.

From a triangular set : $\langle R_i(X), \mathrm{Sres}_{i,i}(X,Y)\rangle$

By construction, we know that $\mathrm{Sres}_i(X,Y) = \mathrm{sres}_{i,i}(X)\,Y^i + \ldots.$ and that $\mathrm{sres}_{i,i}(X)$ is invertible modulo R_i so that $\langle R_i(X), (\mathrm{sres}_{i,i}^{-1}(X) \bmod R_i)\mathrm{Sres}_{i,i}(X,Y)\rangle$ is a lexicographic Gröbner basis.

One thus might use the general existing algorithm but the complexity will be quite large over the rationals.

From a triangular set after a shear by a separating linear form

We know that the system is equivalent to $\cup_{i=1}^{d_g}\left\{R_i(X)=0, Y = -\frac{\mathrm{sres}_{i,i-1}(X)}{i\,\mathrm{sres}_{i,i}(X)}\right\}$

and we want to change the rational functions to get $\cup_{i=1}^{d_g}\left\{R_i(X)=0, Y = \frac{f_{i,t,Y}(X)}{R_i'(X)}\right\}$

Well known : One can compute $(\mathrm{sres}_{i,i})_{i=0\ldots d_g-1}$ or $\mathrm{Sres}_i(X,Y)$ for a fixed i in $\tilde{O}(d^4t)$ bit operations in the worst case.

Thm (2015) : one can compute $(\mathrm{sres}_{i,i}, \mathrm{sres}_{i,i-1})_{i=0\ldots d_g-1}$ in $\tilde{O}(d^4t)$ bit operations in the worst case (same base as the Half GCD)

It then « suffice » to compute $f_{i,t,Y}(X) = (i\,\mathrm{sres}_{i,i}(X))^{-1}\,\mathrm{sres}_{i,i-1}(X)\,R_i'(X) \bmod R_i$

We again use a multi-modular method.

- Choosing the primes using the « certificate » lead to a complexity $\tilde{O}(d^5t + d^6)$ bit operations for the worst case
- Chosing the primes randomly in some set give again $\tilde{O}(d^4t + d^5)$ expected bit operations.

Summary

For the time being we get the following for computing a parameterizations of the solutions:

- Worst case in $\tilde{O}(d^5\tau + d^6)$
- Las -Vegas in $\tilde{O}(d^4\tau + d^5)$
- Monte-Carlo algorithm in $d^{2+\epsilon}\tilde{O}(d^2 + \mathrm{dt} + d\mathcal{P} + \mathcal{P}^2)$, correct result with probability $1 - \frac{1}{2^{\mathcal{P}}}$ by Merhabi/Schost (2015)

Using the rational parameterization for isolating the roots of the system claims anyways $\tilde{O}(d^5 t + d^6)$ bit operations.

2016 : solving a bivariate system has the same cost as just solving the resultant of two polynomials

2019 : computing the topology of a curve has the same cost as solvin its discriminant.