Symbolic deformation techniques for polynomial system solving

Lecture 3

by Grégoire Lecerf

Université de Versailles & CNRS
France
http://www.math.uvsq.fr/~lecerf

Complexity of Numerical Computation, 2009

The Kronecker solver

$\mathbb{K}$: any field of characteristic 0.
$f_1, \ldots, f_n, g$: polynomials in $\mathbb{K}[x_1, \ldots, x_n]$.

$$f_1(x_1, \ldots, x_n) = \cdots = f_n(x_1, \ldots, x_n) = 0, \qquad g(x_1, \ldots, x_n) \neq 0$$

$\mathcal{I}_i = (f_1, \ldots, f_i) : g^\infty$, $\mathcal{J}_i = \mathcal{I}_i + (x_1, \ldots, x_{n-i})$, $\mathcal{K}_i = \mathcal{I}_i + (x_1, \ldots, x_{n-i-1})$

We assume that the system is regular and reduced:

- f_{i+1} is a nonzero divisor modulo $\mathcal{I}_i$,
- $\mathcal{I}_i$ is radical.

With generic coordinates:

- $\mathcal{V}(\mathcal{J}_i)$ is a finite set of regular points, called the ith lifting fiber,
- $\mathcal{V}(\mathcal{K}_i)$ is a curve, called the ith lifting curve.

Algorithm overview

1. Perform a random affine change of the variables.
2. Initialize the process with the solution set of $\mathcal{J}_0 = (x_1, \ldots, x_n)$.

   From the solution set of $\mathcal{J}_i$ compute the one of $\mathcal{J}_{i+1}$ as follows:

   a) Lifting step: compute a representation of the lifting curve $\mathcal{K}_i$.

   b) Intersection step: compute $\mathcal{V}(\mathcal{K}_i) \cap \mathcal{V}(f_{i+1})$.

   c) Cleaning step: deduce $\mathcal{V}(\mathcal{J}_{i+1}) = (\mathcal{V}(\mathcal{K}_i) \cap \mathcal{V}(f_{i+1})) \setminus \mathcal{V}(g)$.
3. Rewrite the solutions if $\mathcal{J}_n$ in terms of the orginal variables.

Contents

- Univariate representations of zero and one dimensional varieties
- Algorithmic details of each step with cost analysis
- Overview of the extensions and generalizations

Univariate representations

$\mathcal{I}$ of dimension $r \geq 0$ in general Noether position:

$$\mathbb{A} := \mathbb{K}[x_1, \ldots, x_r] \hookrightarrow \mathbb{K}[x_1, \ldots, x_n] / \mathcal{I} =: \mathbb{B}$$

is an integral ring extension s.t.:

$$\forall i \geq r+1, \exists q \in \mathbb{A}[T], q(x_i) \in \mathcal{I} \text{ and } \deg_{x_1, \ldots, x_r, T} q = \deg_T q.$$

Let $\mathbb{A}' = \mathbb{K}(x_1, \ldots, x_r)$, $\mathbb{B}' = \mathbb{A}'[x_{r+1}, \ldots, x_n] / \mathcal{I}'$.

$\mathbb{B}'$ is a finite $\mathbb{A}'$ algebra of dimension $\delta := \deg \mathcal{I} = \dim_{\mathbb{A}'} \mathbb{B}'$.

Let $u = \lambda_{r+1} x_{r+1} + \cdots + \lambda_n x_n$ be a $\mathbb{K}$-linear form.

Proposition 1. *Assume that $\mathcal{I}$ is radical. Then the following assertions are equivalent:*

a) *The powers of u generate $\mathbb{B}'$.*

b) *The degree of the minimal polynomial of u in $\mathbb{B}'$ equals δ.*

c) *There exist unique polynomials $q, v_{r+1}, \ldots, v_n$ in $\mathbb{A}'[T]$ such that*

$$\mathcal{I}' = (q(u), x_{r+1} - v_{r+1}(u), \ldots, x_n - v_n(u)),$$

q monic, and $\deg v_j \leq \deg q - 1$ for all j.

d) *There exist unique polynomials $q, w_{r+1}, \ldots, w_n$ in $\mathbb{A}'[T]$ such that*

$$\mathcal{I}' = (q(u), q'(u)x_{r+1} - w_{r+1}(u), \ldots, q'(u)x_n - w_n(u)),$$

q monic, and $\deg w_j \leq \deg q - 1$ for all j.

Definition 2. *u satisfying the assertions above is a primitive element for $\mathcal{I}$.*
$q, v_{r+1}, \ldots, v_n$ is called a univariate representation of $\mathcal{I}$.
$q, w_{r+1}, \ldots, w_n$ is called a Kronecker representation of $\mathcal{I}$.

Such a representation encodes the birational morphism between $\mathcal{V}(\mathcal{I})$ and $\mathcal{V}(q)$.

$\mathcal{V}(\mathcal{I})$ is the Zariski closure of

$$\{(\alpha_1, \ldots, \alpha_r, v_{r+1}(\alpha_1, \ldots, \alpha_r, \beta), \ldots, v_n(\alpha_1, \ldots, \alpha_r, \beta)) \mid \\ q(\alpha_1, \ldots, \alpha_r, \beta) = 0, v_j(\alpha_1, \ldots, \alpha_r, \beta) \text{ well defined for all } j\}$$

Example 3. If $\mathcal{V}(\mathcal{I})$ is a finite set of points $p_1, \ldots, p_\delta$, the minimal polynomial of u is

$$q = \prod_{\alpha \in \{u(p_1), \ldots, u(p_\delta)\}} (T - \alpha).$$

u is primitive iff it takes different values at the p_i.

Kronecker's trick (1882)

"The birational map is a first order deformation of the eliminant polynomial."

$u_\Lambda = \Lambda_{r+1}x_{r+1} + \cdots + \Lambda_n x_n$, with symbolic coefficients.
q_Λ: minimal polynomial of u_Λ in $\mathbb{B}'$.
$w_{\Lambda,j} = -\frac{\partial q_\Lambda}{\partial \Lambda_j}$, for all $j \in \{r+1, \ldots, n\}$.

Proposition 4. *If $\mathcal{I}$ is unmixed of degree δ, and in general Noether position then:*

a) *$\mathcal{I}$ is radical iff q_Λ is squarefree.*

b) *If $\mathcal{I}$ is radical then u_Λ is primitive, $q_\Lambda \in \mathbb{A}[T]$, $q_\Lambda(u_\Lambda) \in \mathcal{I}$.*

c) *$\deg_{x_1, \ldots, x_r, T} q_\Lambda = \delta$.*

Proof. By differentiating $q_\Lambda(u_\Lambda) \in \mathcal{I}$ wrt Λ_j:

$$q'_\Lambda(u_\Lambda)x_j - w_{\Lambda,j}(u_\Lambda) \in \mathcal{I}. \tag{1}$$

$\mathcal{I}$ radical $\Rightarrow \mathcal{I}_\Lambda$ radical $\Rightarrow q_\Lambda$ is squarefree.
Conversely, if q_Λ is squarefree then $q'_\Lambda(u_\Lambda)$ is invertible in $\mathbb{B}'$, hence $\mathcal{I}'$ is radical.
The unmixedness hypothesis implies the radicality of $\mathcal{I}$. $\square$

$u = \lambda_{r+1} x_{r+1} + \cdots + \lambda_n x_n$

$q_\lambda, w_{\lambda,r+1}, \ldots, w_{\lambda,n}$:
specializations of $q_\Lambda, w_{\Lambda,r+1}, \ldots, w_{\Lambda,n}$ at $\Lambda_{r+1} = \lambda_{r+1}, \ldots, \Lambda_n = \lambda_n$.

Corollary 5. *Assume that $\mathcal{I}$ is radical, unmixed, and in general Noether position.*

a) u is primitive for $\mathcal{I}$ iff q_λ is squarefree.

b) If u is primitive for $\mathcal{I}$ then

- *$q_\lambda, w_{\lambda,r+1}, \ldots, w_{\lambda,n}$ is a Kronecker representation of $\mathcal{I}$,*
- *$q_\lambda(u)$, $q_\lambda'(u) x_{r+1} - w_{\lambda,r+1}(u), \ldots, q_\lambda'(u) x_n - w_{\lambda,n}(u)$ belong to $\mathcal{I}$,*
- *$\deg_{x_1,\ldots,x_r,T} q_\lambda = \delta$, $\deg_{x_1,\ldots,x_r,T} w_{\lambda,j} \leq \delta$.*

Example 6. $f_1 = (x_2 - 2x_3)^2 + x_1^2 + x_3^2 - 2$, $f_2 = (x_2 - 2x_3)^2 + x_1^2 - 1$.

The ideal $\mathcal{I} = (f_1, f_2)$ admits the following Kronecker representation with $u = x_2$:

$$u^4 + \left(2x_1^2 - 10\right) u^2 + x_1^4 + 6x_1^2 + 9 = 0, \quad \begin{array}{rcl} x_2 & = & \frac{(-4x_1^2 + 20)u^2 - 4x_1^4 - 24x_1^2 - 36}{4u^3 + (4x_1^2 - 20)u}, \\ x_3 & = & \frac{8u^2 - 8x_1^2 - 24}{4u^3 + (4x_1^2 - 20)u}. \end{array}$$

Remark 7. The denominator in a univariate representation is the discriminant of q, which has degree $\delta(\delta - 1)$ in general. Therefore the size of a Kronecker representation is in general smaller than a univariate one.

Remark 8. These goods properties in terms of degrees also hold for the size of the integer coefficients. This is used in the RUR algorithm (Rational Univariate Representation) by Rouillier and Roy (1996).

Specialization of the independent variables

"Kronecker representations can actually represent **all** points of $\mathcal{V}(\mathcal{I})$."

Let $q, w_{r+1}, \ldots, w_n$ be a Kronecker representation of $\mathcal{I}$ with primitive element u.
Let $\mathcal{J} = \mathcal{I} + (x_1, \ldots, x_r)$.
Let $Q, W_{r+1}, \ldots, W_n$ be the specializations of $q, w_{r+1}, \ldots, w_n$ at $x_1 = \cdots = x_r = 0$.

Assume that:

- $\mathcal{I}$ is radical, unmixed, and in Noether position,
- u is primitive for $\sqrt{\mathcal{J}}$ – otherwise change u.

Proposition 9. *Let $M = \gcd(Q, Q')$, $\tilde{q} = Q/M$ (squarefree part of Q). Then M divides all the W_j, so that we can compute $\tilde{w}_j = \tilde{q}'(W_j/M)/(Q'/M) \bmod \tilde{q}$.*
$\tilde{q}, \tilde{w}_{r+1}, \ldots, \tilde{w}_n$ is a Kronecker representation of $\sqrt{\mathcal{J}}$.

Computational model and cost analysis

- We focus on the dense representation for polynomials.

Example: the size of a bivariate polynomial of bi-degree (n,m) is

$$(n+1)(m+1).$$

- When over an effective field $\mathbb{K}$, each binary arithmetic operation $(\times, +, -, /, =)$ costs $\mathcal{O}(1)$.
- "Soft big Oh" notation: $f(d) \in \tilde{\mathcal{O}}(g(d))$ means $f(d) \in g(d)(\log g(d))^{\mathcal{O}(1)}$.
- "Softly linear in d"= $\tilde{\mathcal{O}}(d)$,
  "Softly quadratic in d"= $\tilde{\mathcal{O}}(d^2)$,...
- The product, division, (sub)resultant, and extended gcd of two univariate polynomials of degree d over a field take softly linear time.

Example 10.

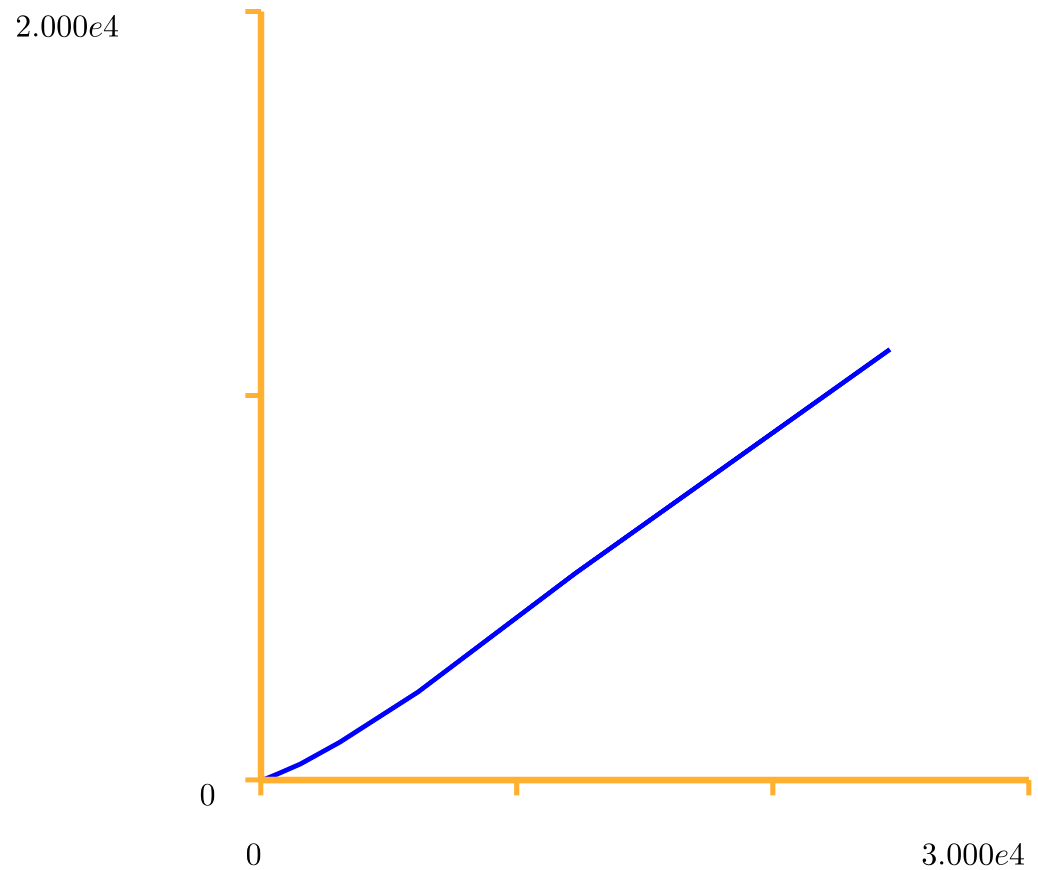
```
Mmx] use "algebramix"; p == modulus probable_next_prime 2^30
```

1073741827

```
Mmx] gcd_time_sample (d: Int): Floating == {
       F == polynomial (i mod p| i in 0..d);
       G == polynomial (random () mod p | i in 0..d);
       b == time(); gcd (F, G); as_floating (time() - b) };
Mmx] v == [ [3*2^i, gcd_time_sample (3*2^i)] | i in 4..14]
```

$[[48, 13.00], [96, 15.00], [192, 35.00], [384, 83.00], [768, 192.0], [1536, 417.0], [3072, 978.0], [6144, 2.291e3], [12288, 5.387e3], [24576, 1.120e4]]$

```
Mmx] include "graphix/diagram.mmx"
Mmx] $draw_diagram v
```



Mmx]

Back to the Kronecker solver

$\mathbb{K}$: any field with characteristic 0 or sufficiently high.

$f_1, \ldots, f_n, g$: polynomials in $\mathbb{K}[x_1, \ldots, x_n]$.

$$f_1(x_1, \ldots, x_n) = \cdots = f_n(x_1, \ldots, x_n) = 0, \qquad g(x_1, \ldots, x_n) \neq 0$$

$\mathcal{I}_i = (f_1, \ldots, f_i) \colon g^\infty$, $\mathcal{J}_i = \mathcal{I}_i + (x_1, \ldots, x_{n-i})$, $\mathcal{K}_i = \mathcal{I}_i + (x_1, \ldots, x_{n-i-1})$

Assumptions:

- f_{i+1} is a nonzero divisor modulo $\mathcal{I}_i$,
- $\mathcal{I}_i$ is radical.

Proposition 11. *For all $i \in \{0, \ldots, n-1\}$, the ideals $\sqrt{\mathcal{I}_i + (f_{i+1})}$ and $\mathcal{I}_{i+1}$ are unmixed of dimension $n-i-1$.*

After a random affine change of the variables we can assume that the following properties hold with a high probability:

- $\mathcal{I}_i$ is in general Noether position for all i.
- $\mathcal{I}_i + (f_{i+1})$ is in general Noether position.
- $\mathcal{J}_i$ is radical.
- $\mathcal{J}_{i+1} = \sqrt{\mathcal{K}_i + (f_{i+1})} \colon g^\infty$.
- x_{n-i} is primitive for $\mathcal{I}_i + (f_{i+1})$.

Lifting step

Let $r = n - i$.

Input: $Q, W_{r+1}, \ldots, W_n$, a Kronecker representation of $\mathcal{J}_i$.

Ouput: $\tilde{Q}, \tilde{W}_{r+1}, \ldots, \tilde{W}_n$, a Kronecker representation of $\mathcal{K}_i$.

Assumptions: $\mathcal{I}_i + (x_1, \ldots, x_r)$ is radical with primitive element x_{r+1}.

$\hat{\mathbb{A}} = \mathbb{K}[[x_1, \ldots, x_r]]$, $\hat{\mathbb{B}} = \hat{\mathbb{A}}[x_{r+1}, \ldots, x_n]/\hat{\mathcal{I}}$, where $\hat{\mathcal{I}}$ is the extension of $\mathcal{I}$.

Let $q, w_{r+1}, \ldots, w_n$ (resp. $v_{r+1}, \ldots, v_n$) be the Kronecker (resp. univariate) representation of $\mathcal{I}$.

We already know:

- $Q, W_{r+1}, \ldots, W_n$ are the specializations of $q, w_{r+1}, \ldots, w_n$ at

$$x_1 = \cdots = x_r = 0.$$

- $\tilde{Q}, \tilde{W}_{r+1}, \ldots, \tilde{W}_n$ are the specializations of $q, w_{r+1}, \ldots, w_n$ at
$$x_1 = \cdots = x_{r-1} = 0.$$
- q' is invertible in $\hat{\mathbb{A}}[T]/q$.

Strategy: approximate in $\hat{\mathbb{A}}$ with a variant of the Newton operator.

Successive approximations: $\mathfrak{o}_0$, $\mathfrak{o}_1$, $\mathfrak{o}_2, \ldots$ with $\mathfrak{o}_k = (x_1, \ldots, x_{r-1}, x_r^{2^k})$.

Proposition 12. *(half of the Jacobian Criterion)*

- $\hat{\mathcal{I}} = (q(x_{r+1}), x_{r+1} - v_{r+1}(x_{r+1}), \ldots, x_n - v_n(x_{r+1}))$.
- *The Jacobian matrix J of $f_1, \ldots, f_i$ w.r.t. $x_{r+1}, \ldots, x_n$ is invertible in $\hat{\mathbb{B}}$.*

Let $q^{[k]}, v_{r+1}^{[k]}, \ldots, v_n^{[k]}$ be the approximations of $q, v_{r+1}, \ldots, v_n$ to precision $\mathfrak{o}_k$.

Algorithm 13. *Lifting step*

1. *Initialize with $q^{[0]} = Q$, $v_j^{[0]} = W_j / Q' \bmod Q$, for all j.*
2. *Do the following steps while precision 2^k is less than $\delta = \deg Q + 1$:*
   a. *Apply the following Newton iteration modulo $q^{[k]}$ and $\mathfrak{o}_{k+1}$:*
   $$\begin{pmatrix} \tilde{v}_{r+1}^{[k+1]} \\ \vdots \\ \tilde{v}_n^{[k+1]} \end{pmatrix} = \begin{pmatrix} v_{r+1}^{[k]} \\ \vdots \\ v_n^{[k]} \end{pmatrix} - J^{-1} \begin{pmatrix} f_1 \\ \vdots \\ f_i \end{pmatrix} \left(x_1, \ldots, x_r, v_{r+1}^{[k]}, \ldots, v_n^{[k]} \right)$$
   b. *$\Delta = \tilde{v}_{r+1}^{[k+1]} - v_{r+1}^{[k]} = \tilde{v}_{r+1}^{[k+1]} - T$, belongs to $\mathfrak{o}_k[T]$.*
   c. *$q^{[k+1]} = q^{[k]} - (\Delta\, q^{[k]\prime} \bmod q^{[k]})$ to precision $\mathfrak{o}_{k+1}$.*
   d. *$v_j^{[k+1]} = \tilde{v}_j^{[k+1]} - (\Delta\, \tilde{v}_j^{[k+1]\prime} \bmod q^{[k]})$ to precision $\mathfrak{o}_{k+1}$.*
3. *$\tilde{Q}$ is the truncation of $q^{[k+1]}$ to precision $\delta + 1$.*
4. *$\widetilde{W}_j$ is the truncation of $q^{[k]\prime} v_{r+1}^{[k]} \bmod q^{[k]}$ to precision $\delta + 1$.*

Example 14.

```
Mmx] include "gregorix/kronecker_naive.mmx";
Mmx] f1 == x2^2 + 5*x3^2 - 4*x2*x3 - 2
```

$$x2^2 - 4\, x2\, x3 + 5\, x3^2 - 2$$

```
Mmx] d == 2; q == polynomial (-2/5,0,1)
```

$$x^2 - \frac{2}{5}$$

```
Mmx] v3 == polynomial (rational 0, 1)
```

$$x$$

```
Mmx] evaluate (f1, [x2, x3],
                    [polynomial rational 0, v3],
                     e :-> polynomial e) mod q
```

$$0$$

```
Mmx] Q == polynomial (series q[i] | i in 0..d+1)
```

$$(1 + O(z^{10}))\, x^2 + O(z^{10})\, x - \frac{2}{5} + O(z^{10})$$

```
Mmx] V3 == modular (polynomial (series v3[i] | i in 0..d), Q);
     z == modular (polynomial series (rational 0, rational 1),Q);
     V3
```

$$(1+O(z^{10}))\,a+O(z^{10})$$

```
Mmx] op == newton_operator ([f1], [x3])
```

$$\left[\frac{x2^2-4\,x2\,x3+5\,x3^2-2}{4\left(x2-\frac{5\,x3}{2}\right)}+x3\right]$$

```
Mmx] series_precision := 2;
     Vt == evaluate (op, [x2, x3], [z, V3],
                     e :-> modular (polynomial series e, Q))
```

$$\left[(1+O(z^2))\,a+\frac{2}{5}\,z+O(z^2)\right]$$

```
Mmx] Delta == preimage Vt[0] - preimage V3
```

$$O(z^2)\,x+\frac{2}{5}\,z+O(z^2)$$

```
Mmx] Q - (Delta * derive Q mod Q)
```

$$(1+O(z^2))\,x^2+\left(\frac{-4}{5}\,z+O(z^2)\right)x-\frac{2}{5}+O(z^2)$$

```
Mmx] f1 / 5
```

$$\frac{x2^2}{5}-\frac{4\,x2\,x3}{5}-\frac{2}{5}+x3^2$$

```
Mmx]
```

Cost analysis

Since the precision is doubled at each step it suffices to examine the cost of the last step only, where the precision is $\delta+1$.

1. Cost of operations in $\mathbb{K}[[x_r]][T]/(q)$: $\tilde{\mathcal{O}}(\delta^2)$.
2. Evaluation of $f_1,\ldots,f_i$: L operations in $\mathbb{K}[[x_r]][T]/(q)$.
3. Evaluation of J: $n\,L$ operations in $\mathbb{K}[[x_r]][T]/(q)$.
4. Inverse of the value of J via a specific application of Newton's method: $\mathcal{O}(n^4)$ operations in $\mathbb{K}[[x_r]][T]/(q)$.

Total: $(n\,L+n^4)\tilde{\mathcal{O}}(\delta^2)$ operations in $\mathbb{K}$.

Intersection step

Input: Kronecker representation of the curve $\mathcal{K}_i$:

$$\tilde{Q}(x_r,T)=0,\quad x_1=\cdots=x_{r-1}=0,$$

$$x_{r+1}=T,\quad \tilde{Q}'(x_r,T)x_j=\tilde{W}_j(x_r,T),\quad \text{for } j\geq r+2.$$

Output: univariate representation of $\mathcal{K}_i+(f_{i+1})$:

$$\hat{Q}(T)=0,\quad x_1=\cdots=x_{r-1}=0,$$

$$x_r=T,\quad x_j=\hat{V}_j(T), \text{for } j\geq r+1.$$

Proposition 15. *The caracteristic polynomial of x_r modulo $\mathcal{K}_i + (f_{i+1})$ is*

$$\hat{Q}(x_r) = \text{Resultant}_T(f(x_r, \tilde{V}_{r+1}(T), \ldots, \tilde{V}_n(T)), \tilde{Q}(T)),$$

where $\tilde{V}_j = \tilde{W}_j / \tilde{Q}' \bmod \tilde{Q}$.

Proof. The coordinates being sufficiently generic, the constant coefficient χ_0 of the characteristic polynomial of f_{i+1} modulo $\mathcal{K}_i$ is the characteristic polynomial of x_r modulo $\mathcal{K}_i + (f_{i+1})$. □

Let $S_1 = \text{SubResultant}_{1,T}(f(x_r, \tilde{V}_{r+1}(T), \ldots, \tilde{V}_n(T)), \tilde{Q}(T)) = D(x_r)T - N(x_r)$.

$S_1 \in \mathbb{K}(x_r)[T]$.

Proposition 16. *With sufficiently generic coordinates:*

- $D(x_r)$ *is invertible modulo* $\hat{Q}(x_r)$,
- $x_{r+1} = N(x_r)/D(x_r)$ *modulo* $\mathcal{K}_i + (f_{i+1})$.
- $S_1(x_r) \bmod \hat{Q}(x_r)$ *can be computed directly in* $\mathbb{K}[x_r]/(\hat{Q}(x_r))[T]$.

Algorithm 17. $\delta = \deg \mathcal{K} = \deg \tilde{Q}$, $d = \deg f_{i+1}$.

1. *Compute* $\hat{Q}(x_r)$ *by interpolation at* $d\,\delta + 1$ *points.*
2. *Compute* $S_1(x_r) \bmod \hat{Q}(x_r)$. *Let* $\hat{V}_{r+1}(x_r) = N(x_r)/D(x_r) \bmod \hat{Q}(x_r)$.
3. *For* $j \geq r+2$, *compute* $\hat{V}_j(x_r) = \tilde{V}(x_r, \hat{V}_{r+1}(x_r)) \bmod \hat{Q}(x_r)$.

Proof. $\deg \hat{Q} \leq d\,\delta$ (Bézout theorem). □

Cost

1. With fast multipoint evaluation the parametrization of the curve can be specialized at all the points with $\tilde{\mathcal{O}}(n\,d\,\delta^2)$ operations in $\mathbb{K}$. Then each value of $\hat{Q}$ takes $L\,\tilde{\mathcal{O}}(\delta)$. The interpolation costs $\tilde{\mathcal{O}}(d\,\delta)$.
2. $S_1(x_r)$ mod $\hat{Q}(x_r)$ takes $L\ \tilde{\mathcal{O}}(d\ \delta^2)$ for the evaluation of f_{i+1} and then $\tilde{\mathcal{O}}(d\ \delta^2)$ more operations for the subresultant.
3. The substitution takes $\tilde{\mathcal{O}}(n\,d\,\delta^2)$ by naive evaluation.

Total cost: $(L+n)\,\tilde{\mathcal{O}}(d\,\delta^2)$.

Example 18.

```
Mmx] include "gregorix/kronecker_naive.mmx"; type_mode?:= true;
Mmx] f_org: Vector Symbolic == [ x1^2 + x2^2 + x3^2 - 2,
                                 x1^2 + x2^2 - 1,
                                 x1 - x2 + 3 * x3 ];
     x: Vector Symbolic == [x1, x2, x3];
     y: Vector Symbolic == [x1, x2 - 2 * x3, x3];
     f: Vector Symbolic == replace (f_org, x, y)
```

$\left[(x2 - 2\,x3)^2 + x1^2 + x3^2 - 2, (x2 - 2\,x3)^2 + x1^2 - 1, x1 - x2 + 5\,x3\right]$: `Vector (Symbolic)`

```
Mmx] t == polynomial quotient polynomial (rational 0, 1);
     V3 == polynomial (quotient polynomial rational 0,
                       quotient polynomial rational 1);
     q == monic_part evaluate (replace (f[0],x1,0), x[1,3],
            [t, V3], e :-> polynomial quotient polynomial e)
```

$y^2-\frac{4}{5}x\,y+\frac{1}{5}x^2-\frac{2}{5}$: `Polynomial (Quotient (Polynomial (Rational)))`

```
Mmx] val == evaluate (replace (f[1],x1,0), x[1,3], [t,V3],
              e :-> polynomial quotient polynomial e) mod q
```

$\frac{-4}{5}x\,y+\frac{1}{5}x^2+\frac{3}{5}$: `Polynomial (Quotient (Polynomial (Rational)))`

```
Mmx] q == monic_part numerator resultant (val, q)
```

$x^4-10\,x^2+9$: `Polynomial (Rational)`

```
Mmx] v2 == polynomial (rational 0, 1);
     aux == - val[0] / val[1];
     v3 == preimage (modular (numerator aux, q)
                     / modular (denominator aux, q))
```

$\frac{-1}{12}x^3+\frac{13}{12}x$: `Polynomial (Rational)`

```
Mmx] vals ==evaluate (replace (f[0,2],[x1],[0:>Symbolic]),
                      x[1,3], [v2,v3], e :-> polynomial e)
```

$\left[\frac{5}{144}x^6-\frac{41}{72}x^4+\frac{365}{144}x^2-2, \frac{1}{36}x^6-\frac{7}{18}x^4+\frac{49}{36}x^2-1\right]$: `Vector (Generic)`

```
Mmx] [ e mod q | e in vals ]
```

$[0,0]$: `Vector (Generic)`

Cost summary

At step i with degree $\delta_i=\deg \mathcal{I}_i$ and $d=\max_i \deg f_i$.

- lifting: $(n\,L+n^4)\tilde{\mathcal{O}}(\delta_i^2)$
- intersection: $(L+n)\,\tilde{\mathcal{O}}(d\,\delta_i^2)$
- cleaning: $(L+n)\,\tilde{\mathcal{O}}(\delta_i)$

Total cost: $(n\,L+n^4)\tilde{\mathcal{O}}(d\delta^2)$, with $\delta=\max_{i=1\ldots n-1}\delta_i$.

Equidimensional decomposition

For any $\mathcal{I}=(f_1,\ldots,f_s)$, and any polynomial g compute the equidimensional decomposition of

$$\mathcal{V}(\mathcal{I}:g^\infty)=\mathcal{V}_0\cup\cdots\cup\mathcal{V}_n,$$

where $\mathcal{V}_i$ is the equidimensional component of dimension i.

Algorithm 19. *(overview)*
Let $\mathcal{V}_0^i\cup\cdots\cup\mathcal{V}_n^i$ be the equidimensional decomposition of $\mathcal{V}((f_1,\ldots,f_i):g^\infty)$.

For i from 0 to $s-1$ do:

1. *For j from 0 to n compute $\overline{(\mathcal{V}_j^i \cap \mathcal{V}(f_{i+1})) \setminus \mathcal{V}(g)}$: that produces components of dimensions i or $i-1$:*
$$\begin{aligned} \mathcal{V}_n^i \cap \mathcal{V}(f_{i+1}) &= \mathcal{W}_n \cup \mathcal{W}'_{n-1}, \\ \mathcal{V}_{n-1}^i \cap \mathcal{V}(f_{i+1}) &= \mathcal{W}_{n-1} \cup \mathcal{W}'_{n-2}, \\ &\dots \\ \mathcal{V}_1^i \cap \mathcal{V}(f_{i+1}) &= \mathcal{W}_1 \cup \mathcal{W}'_0, \\ \mathcal{V}_0^i \cap \mathcal{V}(f_{i+1}) &= \mathcal{W}_0. \end{aligned}$$
2. *Deduce the decomposition $\mathcal{V}((f_1, \dots, f_{i+1}) \colon g^\infty)$ from the $\mathcal{W}_j$ and $\mathcal{W}'_j$.*

Theorem 20. (Lecerf, 2001, 2003) *The equidimensional decomposition can be computed with*
$$s\, n^4\, (n\, L + n^4) \tilde{\mathcal{O}}((d\, \delta_a)^3),$$
operations in $\mathbb{K}$, with a probabilistic algorithm, where
$$\delta_a = \max_{i=0,\dots,s} \sum_{\mathcal{Q} \in \text{Isolated primaries}(\mathcal{I})} \deg(\mathcal{Q}).$$
Each component is represented by a set of lifting fibers.

Remark 21.

- Step 2 requires the following subroutine: $(\mathcal{V}, \mathcal{W}) \mapsto \overline{\mathcal{V} \setminus \mathcal{W}}$.
  This is responsible of the cubic exponent in δ_a.
- Lifting a curve for a multiple component needs a generalization of Newton's operator.
- Irreducible decomposition reduces to polynomial factorization.

Example 22. $f_1 = (x_1 + x_2 - 1)^2\, x_2,\ f_2 = x_1\, x_2$.

- $\mathcal{V}(f_1) = \mathcal{V}(x_2) \cup \mathcal{V}(x_1 + x_2 - 1)$: irreducible components of dimension 1 and degree 1 and resp. multiplicities 1 et 2.
- $\mathcal{V}(x_2) \cap \mathcal{V}(f_2) = \mathcal{V}(x_2)$,
  $\mathcal{V}(x_1 + x_2 - 1) \cap \mathcal{V}(f_2) = \mathcal{V}(x_1, x_2 - 1) \cup \mathcal{V}(x_2, x_1 - 1)$.
- $\mathcal{V}(f_1) \cap \mathcal{V}(f_2) = \mathcal{V}(x_2) \cup \mathcal{V}(x_1, x_2 - 1)$.

Example 23. Generalization of Newton's methods in singular cases:

- $\{(0,1)\}$ is a lifting fiber for $\mathcal{V}(x_1 + x_2 - 1)$ with multiplicity 2 in (f_1).
- But $\{(0,1)\}$ is a lifting fiber for $\mathcal{V}(x_1 + x_2 - 1)$ with mult. 1 in $(\partial f_1 / \partial x_2)$.

This technique is known as deflation – it extends to the multivariate case with good complexity [Lecerf, 2002].

Other references. Alternative strategy, by replacing the original system by random linear combinations of the equations – thanks to Bertini's theorem:

$$f_1 = x_1^2,\ f_2 = x_2^2,\ f_3 = x_3^2 \rightsquigarrow f_1 = x_1^2 + x_2^2 + x_3^2,\ f_2 = x_1^2 + 2\, x_2^2 + 3\, x_3^2,\ f_3 = 3\, x_1^2 + x_2^2 + 5\, x_3^2$$

- Krick and Pardo, 1996: idea of using Bertini's theorem for polynomial system solving.

- Lecerf, 2000.
- Jeronimo, Puddu, Sabia, 2000, 2001, 2002.
- Jeronimo, Krick, Sabia, Sombra, 2004.

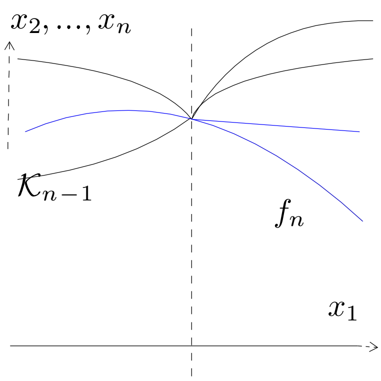
Primary decomposition

Open problems

- What is a good representation for primary ideals with a functional representation?
- Is there a best representation for the embedded components?

First partial results for the zero-dimensional isolated primary components [Durvye, 2005, 2008]

1. Replace the system by generic linear combinations of the equations.
2. Apply the Kronecker solver to compute the isolated solutions only.
3. At each solution, compute the module defined by the germ of the last lifting curve.
4. Compute the coimage of the multiplication by the last equation in this module.



⇝ The overhead only concerns the multiple roots and is polynomial in the multiplicities.

More references

Specific types of systems

- Heintz, Krick, Puddu, Sabia, Waissbein (2000): extended deformation techniques.
- Pardo, San Martín (2004): Pham systems.
- Jeronimo, Matera, Solerno, Waissbein (2008): sparse systems.

Numerical framework

- Castro, Pardo, Hägele, Morais (2001): comparison between numeric and symbolic solving.
- Sommese, Verschelde, and Wampler (2005): purely numerical versions of the incremental equidimensional and primes decompositions.

Real algebraic geometry

- Bank, Giusti, Heintz, and Mbakop (1997, 2001).
- Bank, Giusti, Heintz, and Pardo (2004, 2005, 2009).
- Safey el Din, and Schost (2004, 2005).