Symbolic deformation techniques for polynomial system solving

Lecture 2

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 $\mathbb{K}[x_1, \ldots, x_n]$.

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

$\mathcal{I}_i = (f_1, \ldots, f_i) : g^\infty = \{f \mid \exists n, g^n f \in (f_1, \ldots, f_i)\}$

$\mathcal{J}_i = \mathcal{I}_i + (x_1, \ldots, x_{n-i}), \;\; \mathcal{K}_i = \mathcal{I}_i + (x_1, \ldots, x_{n-i-1})$

For simplicity we assume that the system is regular and reduced:

- f_{i+1} is a nonzero divisor modulo $\mathcal{I}_i$: $f_{i+1} h \in \mathcal{I}_i \Rightarrow h \in \mathcal{I}_i$,
- $\mathcal{I}_i$ is radical: $\mathcal{I}_i = \sqrt{\mathcal{I}_i} = \{f \mid \exists n, f^n \in \mathcal{I}_i\}$.

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

Proof of the correctness of the Kronecker solver from scratch:

- **Prerequisite:** primary decomposition and integral ring extensions.
- **Computational dimension theory:** prove the dimension of the intermediate solution sets.
- **Incremental solving and degree theory:** describe the intersection step, and bound the degrees of the polynomials in the lifting fibers and curves.

References

- Durvye and Lecerf, A concise proof of the Kronecker polynomial system solver from scratch, *Expositiones Mathematicae*, 2007.
- Durvye's Ph.D thesis, `http://www.math.uvsq.fr/~durvye`, 2008.

Motivations

- Elementary and concise proof of the solver.
- Extend the solver to compute the primary decomposition.

Prerequisite

$\mathbb{K}$: any field, with algebraic closure $\bar{\mathbb{K}}$.

Primary decomposition

Definition 1. *An ideal $\mathcal{Q}$ is primary if $f\,g \in \mathcal{Q} \Rightarrow f \in \mathcal{Q}$ or $\exists m, g^m \in \mathcal{Q}$.*

The radical of $\mathcal{Q}$ is prime, it is called the prime belonging to $\mathcal{Q}$.

Example 2. $\mathcal{Q} = (x_1^2, x_1\,x_2, x_2^2)$ is primary with radical (x_1, x_2).

Example 3. $\mathcal{I} = (x_2^2, x_1\,x_2)$ is not primary: take $f = x_2$ and $g = x_1$.
But $\sqrt{\mathcal{I}} = (x_2)$ is prime.

Theorem 4. *Any ideal $\mathcal{I}$ admits a primary decomposition that is: $\mathcal{I} = \cap_{l=1}^{s} \mathcal{Q}_l$, with $\mathcal{Q}_l$ primary, and none of the $\mathcal{Q}_l$ can be discarded.*

Proof. Decompose $\mathcal{I}$ as much as possible. By Noetherianity this leads to a finite intersection. Then show that an irreducible ideal is primary. □

Example 5. $(x_2^2, x_1\,x_2) = (x_2) \cap (x_1^2, x_1\,x_2, x_2^2) = (x_2) \cap (x_1, x_2^2)$ – no uniqueness!

Definition 6.

- $\sqrt{\mathcal{Q}_1}, \ldots, \sqrt{\mathcal{Q}_s}$ *are called the primes associated to $\mathcal{I}$.*
- *An associated prime is isolated if it does not contain an other one, otherwise it is said embedded.*

Example 7. $(x_2^2, x_1\,x_2) = (x_2) \cap (x_1^2, x_1\,x_2, x_2^2) = (x_2) \cap (x_1, x_2^2)$.
(x_2) is isolated, while (x_1, x_2) is embedded.

Integral dependencies

$\mathbb{A}$: a subring of $\mathbb{K}[x_1, \ldots, x_n]$ containing $1 \in \mathbb{K}$ – *e.g.* $\mathbb{A} = \mathbb{K}[x_1, \ldots, x_r]$.

Definition 8. *$e_1, \ldots, e_s$ in $\mathbb{K}[x_1, \ldots, x_n]$ are algebraically dependent modulo $\mathcal{I}$ if $\exists E \in \mathbb{K}[z_1, \ldots, z_s]$ non-zero s.t. $E(e_1, \ldots, e_s) \in \mathcal{I}$.
Otherwise they are algebraically independent, or free, modulo $\mathcal{I}$.*

Example 9. x_1, x_2 are algebraically independent modulo $(x_1^2 + x_2^2 + x_3^2 - 1)$.

Definition 10. *e in $\mathbb{K}[x_1, \ldots, x_n]$ is algebraic over $\mathbb{A}$ modulo $\mathcal{I}$ if $\exists q \in \mathbb{A}[T]$ non-zero s.t. $q(e) \in \mathcal{I}$.*

Example 11. x_3 is algebraic over $\mathbb{K}[x_1, x_2]$ modulo $(x_1^2\,x_3^4 + x_2^2 + x_1^2 - 1)$.

Definition 12. *e in $\mathbb{K}[x_1, \ldots, x_n]$ is integral over $\mathbb{A}$ modulo $\mathcal{I}$ if $\exists q \in \mathbb{A}[T]$ non-zero and monic s.t. $q(e) \in \mathcal{I}$.*

Example 13. x_2 is not integral over $\mathbb{K}[x_1]$ modulo $(x_1 x_2 - 1)$.
After replacing x_2 by $x_1 + x_2$ the equation becomes $x_2^2 + x_1 x_2 - 1$, and x_2 becomes integral.

Proposition 14. *Integral elements over $\mathbb{A}$ modulo $\mathcal{I}$ form a subring of* $\mathbb{K}[x_1, \ldots, x_n]$.

Proof. $q_1(e_1) = 0$, $q_2(e_2) = 0$. Consider:

$$\mathrm{Resultant}_{T_2}(\mathrm{Resultant}_{T_1}(T - (T_1 + T_2), q_1(T_1)), q_2(T_2)). \qquad \square$$

Definition 15. *e in generally integral over $\mathbb{A}$ modulo $\mathcal{I}$ if $\exists q \in \mathbb{A}[T]$ non-zero and monic s.t. $q(e) \in \mathcal{I}$ and* $\deg q(x_1, \ldots, x_n, T^{\deg e}) = \deg_T q(x_1, \ldots, x_n, T^{\deg e})$.

Example 16. x_2 is integral but not generally integral over $\mathbb{K}[x_1]$ modulo $(x_2 - x_1^2)$.

Example 17. x_2 is generally integral over $\mathbb{K}[x_1]$ modulo $(x_2^2 - x_1^2)$.

Dimension

Definition 18. *Transcendence degree of $\mathbb{F}$ over $\mathbb{K}$: cardinality of a maximal subset of $\mathbb{F}$ whose elements are algebraically independent over $\mathbb{K}$.*

Theorem 19. *If Γ is a set of generators of $\mathbb{F}$ over $\mathbb{K}$, then any subset of algebraically independent elements of Γ can be completed into a transcendence basis with elements of Γ.*

Example 20. $\mathrm{trdeg}_{\mathbb{K}} \mathbb{K}(x_1, \ldots, x_n) = n$.

Definition 21. *If $\mathcal{I}$ is a **prime** ideal then the dimension* $\dim \mathcal{I}$ *of $\mathcal{I}$ is the transcendence degree of $\mathbb{K}[x_1, \ldots, x_n]/\mathcal{I}$ over $\mathbb{K}$.*
By convention $\dim(1) = -1$. *In general* $\dim \mathcal{I} = \max_{\mathcal{P} \in \mathrm{Ass}(\mathcal{I})} \dim \mathcal{P}$, *where* $\mathrm{Ass}(\mathcal{I})$ *is the set of associated primes of $\mathcal{I}$.*

Example 22. $\dim(x_1, \ldots, x_i) = n - i$, $\dim(f) = n - 1$ if $f \notin \mathbb{K}$.

Definition 23. *$\mathcal{I}$ is unmixed if the dimensions of its associated primes are all equal.*

Noether position

Definition 24. *$\mathcal{I}$ is in Noether position if there exists $r \in \{0, \ldots, n\}$ s.t.:*

- *$x_1, \ldots, x_r$ are algebraically independent modulo $\mathcal{I}$,*
- *$x_{r+1}, \ldots, x_n$ are integral over $\mathbb{K}[x_1, \ldots, x_r]$ modulo $\mathcal{I}$.*

Example 25. $(x_2 - x_1^2)$ is in Noether position with $r = 1$.

Example 26. $(x_3^2 - x_1, x_2^2 - x_1)$ is in Noether position with $r = 1$.

Theorem 27. *Assume $\mathcal{I} \neq (1)$.*

a) If $x_{r+1}, \ldots, x_n$ are integral over $\mathbb{K}[x_1, \ldots, x_r]$ modulo $\mathcal{I}$ then $\dim \mathcal{I} \leq r$. *Equality holds iff $x_1, \ldots, x_r$ are in addition algebraically independent modulo $\mathcal{I}$.*

b) If $x_1, \ldots, x_r$ are algebraically independent modulo $\mathcal{I}$ then $\dim \mathcal{I} \geq r$. *If equality holds then $x_{r+1}, \ldots, x_n$ are algebraic over $\mathbb{K}[x_1, \ldots, x_r]$ modulo $\mathcal{I}$ – converse holds if $\mathcal{I}$ is unmixed.*

Example 28. $n=3$, $\mathcal{I}=(x_1 x_2-1, x_3)\cap(x_1)$, $\dim\mathcal{I}=2$.
x_1 is algebraically independent modulo $\mathcal{I}$.
x_2 and x_3 are algebraic over $\mathbb{K}[x_1]$ modulo $\mathcal{I}$.

Part (a) does not hold with "algebraic" instead of "integral".

Definition 29. *$\mathcal{I}$ is in general Noether position if there exists $r\in\{0,\ldots,n\}$ s.t.:*

- *$x_1,\ldots,x_r$ are algebraically independent modulo $\mathcal{I}$,*
- *$x_{r+1},\ldots,x_n$ are generally integral over $\mathbb{K}[x_1,\ldots,x_r]$ modulo $\mathcal{I}$.*

Example 30. $(x_2-x_1^2)$ is not in general Noether position.

Example 31. $(x_3^2-x_1, x_2^2-x_1^2)$ is in general Noether position with $r=1$.

Algorithm

Following [Giusti and Heintz, 1993].

Algorithm 32. ***Computation of a general Noether position***
Input: ideal $\mathcal{I}$.
Ouput: the dimension r of $\mathcal{I}$, and a matrix M such that $\mathcal{I}\circ M$ is in general Noether position, where $\mathcal{I}\circ M=\{f\circ M(x_1,\ldots,x_n)^t \mid f\in\mathcal{I}\}$.

1. Initialize i with n and M with the identity matrix.
2. While $(\mathcal{I}\circ M)\cap\mathbb{K}[x_1,\ldots,x_i]\neq(0)$ do
   a) take $a\in\mathcal{I}\cap\mathbb{K}[x_1,\ldots,x_i]$ non-zero,
   b) let h be the homogeneous component of highest degree of a,
   c) take $(\alpha_1^{(i)},\ldots,\alpha_{i-1}^{(i)},1)\in\mathbb{K}^i$ s.t. $h(\alpha_1^{(i)},\ldots,\alpha_{i-1}^{(i)},1)\neq 0$
   – at random whenever $\mathbb{K}$ has sufficiently many elements,
   d) for k from 1 to $i-1$ replace $M_{i,k}$ with $\alpha_k^{(i)}$,
   e) decrease i by 1.
3. Return $r=i$ and M.

Proof.

By induction we show that x_{i+1}, ..., x_n are generally integral over $\mathbb{K}[x_1, \ldots, x_i]$ when entering step i.

Therefore $\dim\mathcal{I}\leq i$ with equality iff $\mathcal{I}\circ M\cap\mathbb{K}[x_1,\ldots,x_i]=(0)$.

Effect of the local change of variables:

$$h(x_1+\alpha_1^{(i)}x_i,\ldots,x_{i-1}+\alpha_{i-1}^{(i)}x_i,x_i)=h(\alpha_1^{(i)},\ldots,\alpha_{i-1}^{(i)},1)x_i^{\deg a}+\cdots.$$

It follows that x_i becomes generally integral over $\mathbb{K}[x_1,\ldots,x_{i-1}]$. □

Example 33. $\mathcal{I} = (f_1, f_2)$

$$f_1 = x_2\,x_3 - x_1, \quad f_2 = x_1\,x_2 - x_3$$

- $a = f_1$, replace x_2 by $x_2 + x_3$. The equations become:

$$f_1 = x_3^2 + x_2\,x_3 - x_1, \quad f_2 = x_1\,x_2 + x_1\,x_3 - x_3.$$

- $a = \mathrm{Res}_{x_3}(f_1, f_2) = x_1\,x_2^2 - (x_1 - 1)^2$, replace x_1 by $x_1 + x_2$, so that

$$a = x_2^3 + (x_1 - 1)\,x_2^2 - 2\,(x_1 - 1)\,x_2 - (x_1 - 1)^2.$$

Theorem 34. *There exists a Zariski dense subset of upper triangular $n \times n$ matrices M with 1 on their diagonal such that $\mathcal{I} \circ M$ is in general Noether position.*

Unmixedness and torsion

Proposition 35. *Assume that $\mathcal{I}$ is in Noether position. Then $\mathbb{B} = \mathbb{K}[x_1, \ldots, x_n]/\mathcal{I}$ is a torsion-free $\mathbb{A}$-module iff $\mathcal{I}$ is unmixed. – Recall that $\mathbb{A} = \mathbb{K}[x_1, \ldots, x_r]$.*

Proof. Consider the primary decomposition of $\mathcal{I} = \mathcal{Q}_1 \cap \cdots \cap \mathcal{Q}_s$, with associated primes $\mathcal{P}_1, \ldots, \mathcal{P}_s$. $\mathcal{I}$ is unmixed iff $\mathbb{A} \cap \mathcal{P}_l = (0)$ for all l.

If $\mathbb{B}$ has torsion then $\exists a \in \mathbb{A} \setminus \{0\}$ and $b \notin \mathcal{I}$ s.t. $a\,b \in \mathcal{I}$. There exists l s.t. $b \notin \mathcal{Q}_l$, whence $a \in \mathcal{P}_l$.

Conversely, if $\mathcal{I}$ is not unmixed, $\exists a \in \mathbb{A} \cap \mathcal{P}_l \setminus \{0\}$ for some l, and thus $\exists n, a^n \in \mathcal{Q}_l$. Let $b \in \cap_{i \neq l} \mathcal{Q}_i \setminus \mathcal{Q}_l$, we have $a^n\,b \in \mathcal{I}$. Therefore a^n is a torsion element for $\mathbb{B}$. $\square$

Example 36. $(x_2^2, x_1\,x_2) = (x_2) \cap (x_1, x_2^2)$, x_1 is a torsion element.

Example 37. $(x_1\,x_2)$ is unmixed of dimension 1, but $\mathbb{B}$ has torsion. The Noether position is thus necessary.

Characteristic and Minimal Polynomials

$\mathcal{I} \neq (1)$, $r = \dim \mathcal{I}$,
$\mathbb{A} = \mathbb{K}[x_1, \ldots, x_r]$, $\mathbb{A}' = \mathbb{K}(x_1, \ldots, x_r)$, $\mathbb{B} = \mathbb{K}[x_1, \ldots, x_n]/\mathcal{I}$, $\mathbb{B}' = \mathbb{A}'[x_{r+1}, \ldots, x_n]/\mathcal{I}'$,
where $\mathcal{I}'$ is the extension of $\mathcal{I}$ to $\mathbb{A}'[x_{r+1}, \ldots, x_n]/\mathcal{I}'$.
Let $f \in \mathbb{K}[x_1, \ldots, x_n]$.

If $\mathcal{I}'$ is in Noether position then $\mathbb{B}'$ is a finite dimensional $\mathbb{A}'$-vector space.
$\chi(T) \in \mathbb{A}'[T]$: characteristic polynomial of the multiplication by f in $\mathbb{B}'$.
$\mu(T) \in \mathbb{A}'[T]$: minimal polynomial of the multiplication by f in $\mathbb{B}'$.

Theorem 38. *Assume that $\mathcal{I}$ is in Noether position, and let $d = \deg f$.*

a) *χ and μ belong to $\mathbb{A}[T]$. If $\mathcal{I}$ an f are homogeneous then $\chi(T^d)$ and $\mu(T^d)$ are homogeneous when seen in $\mathbb{K}[x_1, \ldots, x_r, T]$.*

b) *If the Noether position is general then*

$$\deg \chi(x_1, \ldots, x_r, T^d) = \deg_T \chi(x_1, \ldots, x_r, T^d).$$

Idem for μ.

c) *If $\mathcal{I}$ is unmixed then $\chi(f)$ and $\mu(f)$ belong to $\mathcal{I}$.*

Proof. (a) f integral over $\mathbb{A}$ $\Rightarrow \exists q \in \mathbb{A}[T]$ monic s.t. $q(f) \in \mathcal{I}$.

Since μ divides q in $\mathbb{A}'[T]$, we deduce that $\mu \in \mathbb{A}[T]$, by the classical Gauss lemma.
If $\mathcal{I}$ and f are homogeneous we can take q such that $q(T^d)$ is homogeneous.

(b) We can take q such that

$$\deg q(x_1, \ldots, x_r, T^d) = \deg_T q(x_1, \ldots, x_r, T^d).$$

The same property holds for the irreducible factors of q, hence for χ and μ.

(c) $\mu(f) \in \mathcal{I}' \Rightarrow \exists a \in \mathbb{A} \setminus \{0\}$ and $b \in \mathcal{I}$, $\mu(f) = b/a$. It follows that $a\,\mu(f) = 0$ holds in $\mathbb{B}$.
Since $\mathbb{B}$ is torsion-free we have $\mu(f) = 0$ in $\mathbb{B}$. □

Example 39. $\mathcal{I} = (x_1^2, x_1\, x_2)$ and $f = x_2 + 1$. We have $\mathcal{I}' = (x_2)$ and $\mu = T - 1$. But $\mu(f) = x_2 \notin \mathcal{I}$. Unmixedness is necessary in (c).

Example 40. $\mathcal{I} = (x_2 - x_1^2)$, $f = x_2$, $\mu = T - x_1^2$ shows that the general Noether position is necessary in (b).

Incremental solving

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

$\chi(T) \in \mathbb{A}'[T]$: characteristic polynomial of the multiplication by f in $\mathbb{B}'$.
$\mu(T) \in \mathbb{A}'[T]$: minimal polynomial of the multiplication by f in $\mathbb{B}'$.

χ_0 and μ_0: constant coefficients of χ and μ.

Lemma 41. *Assume that $\mathcal{I}$ is unmixed of dimension r, and in general Noether position.*

a) *μ_0 and χ_0 belong to $\mathcal{I} + (f)$, $(\mathcal{I} + (f)) \cap \mathbb{A} \subseteq \sqrt{(\mu_0)} = \sqrt{(\chi_0)}$.*

b) *f is a zerodivisor in $\mathbb{B}$ $\Leftrightarrow$ $\chi_0 = 0$ $\Leftrightarrow$ $\mu_0 = 0$ $\Leftrightarrow$ $x_1, \ldots, x_r$ are algebraically independent modulo $\mathcal{I} + (f)$.*

c) *$\mathcal{I} + (f) = (1)$ $\Leftrightarrow$ $\chi_0 \in \mathbb{K} \setminus \{0\}$ $\Leftrightarrow$ $\mu_0 \in \mathbb{K} \setminus \{0\}$.*

Proof. (a) We know that $\mu(f) \in \mathcal{I}$. It follows that $\mu_0 \in \mathcal{I} + (f)$. Idem for χ_0.
Let $a \in (\mathcal{I} + (f)) \cap \mathbb{A}$. Let $g \in \mathbb{K}[x_1, \ldots, x_n]$ such that $a - g\, f \in \mathcal{I}$.

g integral $\Rightarrow \exists g^\alpha + \nu_{\alpha-1}\, g^{\alpha-1} + \cdots + \nu_0 \in \mathcal{I}$.

Multiplying by f^α: $a^\alpha + \nu_{\alpha-1}\, a^{\alpha-1} f + \cdots + \nu_0\, f^\alpha \in \mathcal{I}$.

Therefore $\mu(T)$ divides $a^\alpha + \nu_{\alpha-1}\, a^{\alpha-1} T + \cdots + \nu_0\, T^\alpha$, whence $a^\alpha \in (\mu_0)$.

(b) If $\mu_0 = 0$ then $f\,\nu(f) \in \mathcal{I}$, with $\nu(T) = \mu(T)/T$ and $\nu(f) \notin \mathcal{I}$.

Conversely, if f is a zerodivisor, let $g \notin \mathcal{I}$ s.t. $f g \in \mathcal{I}$.

There exists a primary component $\mathcal{Q}$ of $\mathcal{I}$ such that $g \notin \mathcal{Q}$ and $f g \in \mathcal{Q}$.

It follows that $f \in \sqrt{\mathcal{Q}}$, and that $\mu_0 \in \sqrt{\mathcal{Q}}$. Since $\mathcal{I}$ is unmixed, $\sqrt{\mathcal{Q}}$ has dimension r, hence $\mu_0 = 0$.

(c) follows directly from (a). $\square$

Incremental unmixedness of the radical

Theorem 42. *(Principal ideal theorem) Assume that $\mathcal{I}$ is unmixed, and let $f \in \mathbb{K}[x_1, \ldots, x_n]$ be a nonzerodivisor in $\mathbb{B}$. If $\mathcal{I} + (f) \neq (1)$ then $\sqrt{\mathcal{I} + (f)}$ is unmixed of dimension $r - 1$.*

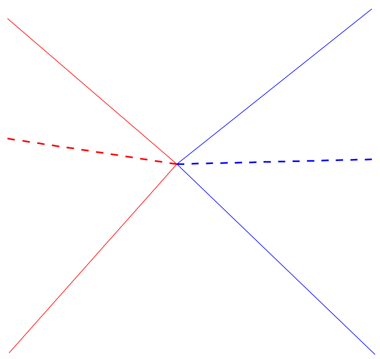
Proof. *(sketch, following* Shafarevich*)*
We assume: $r \geq 1$, $\mathcal{I} + (f) \neq (1)$, $\mathcal{I}$ and $\mathcal{I} + (f)$ are in general Noether position, $\deg_{x_r} \mu_0 = \deg \mu_0 \geq 1$, *and that $\mathcal{I}$ and (f) are homogeneous.*

- $\mathbb{B} = \mathbb{K}[x_1, \ldots, x_n]$ *is an integral ring extension of* $\mathbb{K}[x_1, \ldots, x_{r-1}, f]$*:*
  - $E(x_1, \ldots, x_{r-1}, f) \in \mathcal{I} \Rightarrow \mu_0$ divides $E(x_1, \ldots, x_{r-1}, 0) \Rightarrow f = 0$,
  - $\deg_{x_r} \mu_0 = \deg \mu_0 \Rightarrow x_r$ *is integral over* $\mathbb{K}[x_1, \ldots, x_{r-1}, f]$ *mod* $\mathcal{I}$.
- *It suffices to prove that* $\mathbb{K}[x_1, \ldots, x_n] / \sqrt{\mathcal{I} + (f)}$ *is* $\mathbb{K}[x_1, \ldots, x_{r-1}]$ *torsion-free.*
- *Let* $b \in \mathbb{K}[x_1, \ldots, x_n]$ *and* $a \in \mathbb{K}[x_1, \ldots, x_{r-1}] \setminus \{0\}$ *s.t.* $a\, b \in \sqrt{\mathcal{I} + (f)}$.
- *Let m and g s.t.* $a^m b^m - f g \in \mathcal{I}$.
- *Let $\mathbb{B}_f$ be $\mathbb{B}$ viewed as a* $\mathbb{K}[x_1, \ldots, x_{r-1}, f]$*-module, and $\mathbb{B}'_f$ be the corresponding vector space.*
- Let $\rho(T) = T^\alpha + \rho_{\alpha-1} T^{\alpha-1} + \cdots + \rho_0$, be the minimal polynomial of g in $\mathbb{B}'_f$. We have that $\rho \in \mathbb{K}[x_1, \ldots, x_{r-1}, f][T]$.
- The minimal polynomial of b^m in $\mathbb{B}'_f$ is

$$f^\alpha \rho(a^m T / f) / a^{m\alpha} = T^\alpha + \rho_{\alpha-1} \frac{f}{a^m} T^{\alpha-1} + \cdots + \frac{f^j}{a^{mj}} \rho_0.$$

- a^{mj} divides $f^j \rho_{\alpha-j}$ in $\mathbb{K}[x_1, \ldots, x_{r-1}, f]$ for all j, whence $(b^m)^\alpha \in \mathcal{I} + (f)$. $\square$

Example 43. $\mathcal{I} = (x_1, x_2) \cap (x_3, x_4)$ is unmixed. With the nonzerodivisor $f = x_2 - x_3$ we have $\sqrt{\mathcal{I} + (f)} = (x_1, x_2, x_3) \cap (x_2, x_3, x_4)$ is unmixed, while $\mathcal{I} + (f) = (x_1, x_2, x_3) \cap (x_2, x_3, x_4) \cap (x_1, x_2 - x_3, x_3^2, x_4)$ is not.



Incremental computation of the characteristic polynomial

Proposition 44. *Assume that $\mathcal{I}$ has dimension $r \geq 1$, is unmixed, and is in Noether position. Let f be a nonzerodivisor in $\mathbb{B}$. Then $\chi_0(x_1, \ldots, x_{r-1}, T)$ is proportional over $\mathbb{K}(x_1, \ldots, x_{r-1})$ to the characteristic polynomial of x_r modulo the extension $\mathcal{J}'$ of $\mathcal{J} = \mathcal{I} + (f)$ to $\mathbb{K}(x_1, \ldots, x_{r-1})[x_r, \ldots, x_n]$.*
The proportionality over $\mathbb{K}$ holds iff $\mathcal{J}$ is in Noether position.

Proof.

- Let $\tilde{\mathcal{I}}$ be the extension of $\mathcal{I}$ to $\mathbb{K}(x_1, \ldots, x_{r-1})[x_r, x_{r+1}, \ldots, x_n]$, and let $\tilde{\mathbb{B}} = \mathbb{K}(x_1, \ldots, x_{r-1})[x_r, x_{r+1}, \ldots, x_n]/\tilde{\mathcal{I}}$.
- Since $\mathbb{B}$ is a torsion-free $\mathbb{A}$-module, so is $\tilde{\mathbb{B}}$ seen as a $\mathbb{K}(x_1, \ldots, x_{r-1})[x_r]$-module. Therefore $\tilde{\mathbb{B}}$ is free of finite rank thanks to Noether position.
- Smith form of the multiplication by f: there exists two bases $e_1, \ldots, e_\delta$ and $e'_1, \ldots, e'_\delta$ of $\tilde{\mathbb{B}}$, and monic polynomials $h_1, \ldots, h_\delta$ such that h_l divides h_{l+1} and that $f e_l = h_l e'_l$ in $\tilde{\mathbb{B}}$ for all l: $\tilde{\mathbb{B}}/(f) \simeq \oplus_{l=1}^{\delta} \mathbb{K}(x_1, \ldots, x_{r-1})[x_r]/(h_l)$.
- Since a basis of $\tilde{\mathbb{B}}$ induces a basis of $\mathbb{B}'$ we have that $\chi_0 = a\, h_1 \cdots h_\delta$ for some $a \in \mathbb{K}(x_1, \ldots, x_{r-1})$.
- $B = \{x_r^{\alpha_l} e'_l \,|\, 1 \leq l \leq \delta,\ 0 \leq \alpha_l \leq \deg h_l - 1\}$ is a basis of $\tilde{\mathbb{B}}/(f)$ seen as a $\mathbb{K}(x_1, \ldots, x_{r-1})$-algebra:
  - In $\tilde{\mathbb{B}}$, $(f) = (h_1 e'_1, \ldots, h_\delta e'_\delta)$.
  - Any $g = \sum_{l=1}^{\delta} g_l e'_l \in \tilde{\mathbb{B}}$ can be reduced mod (f) so that $\deg g_l < \deg h_l$.
  - Let $\sum_{l=1}^{\delta} r_l e'_l = 0$ in $\tilde{\mathbb{B}}/(f)$ with $\deg r_l < \deg h_l$. There exist q_l such that $\sum_{l=1}^{\delta} (r_l + q_l h_l) e'_l = 0$ holds in $\tilde{\mathbb{B}}$. It follows that $r_l + q_l h_l = 0$, and that $r_l = 0$.
- In the basis B the multiplication matrix of x_r in $\tilde{\mathbb{B}}/(f)$ is block diagonal formed by the companion matrices of the h_l. It follows that that the characteristic polynomial q of x_r in $\tilde{\mathbb{B}}/(f)$ equals $h_1, \ldots, h_\delta$, hence is proportional to q.

We leave out the last assertion. □

Example 45. $n = 2$, $\mathcal{I} = (x_2^2 + x_1 x_2)$, $r = 1$, and $f = x_1^2$.
$\{1, x_2\}$ form a basis of the $\mathbb{K}[x_1]$-module $\tilde{\mathbb{B}} = \mathbb{K}[x_1, x_2]/\tilde{\mathcal{I}}$, $h_1 = h_2 = x_1^2$.
The matrix of multiplication by f is $\begin{pmatrix} x_1^2 & 0 \\ 0 & x_1^2 \end{pmatrix}$.

$$\tilde{\mathbb{B}}/(f) = \mathbb{K}[x_1]/(h_1) \oplus \mathbb{K}[x_1]/(h_1) x_2$$

These two submodules are stable by multiplication by x_1 but $\mathbb{K}[x_1]/(h_1)$ is not stable by multiplication by x_2. The above direct sum can not be seen as a decomposition of $\tilde{\mathbb{B}}/(f)$ into stable $\mathbb{K}(x_1, \ldots, x_{r-1})$-algebras.

Degree and Bézout theorem

M: invertible $n \times n$ matrix over $\mathbb{K}$.
$\mathcal{I}_M = \mathcal{I} \circ M$, $\mathbb{B}_M = \mathbb{K}[x_1, \ldots, x_n]/\mathcal{I}_M$, $\mathbb{B}'_M = \mathbb{A}'[x_{r+1}, \ldots, x_n]/\mathcal{I}'_M$.
δ: dimension of $\mathbb{B}'$.
δ_M: dimension of $\mathbb{B}'_M$.

Theorem 46. *Assume that $\mathcal{I}$ is unmixed and in general Noether position.*

a) $\delta_M \leq \delta$.

b) $\delta_M = \delta$ *iff* $\mathcal{I}_M$ *is in general Noether position.*

Proof. The longest and most technical proof... but it can be done using the same induction as in the Kronecker solver. □

Remark 47. This theorem is not necessary to the cost analysis of the solver.

Definition 48. *The degree of an unmixed ideal $\mathcal{I}$, written* $\deg \mathcal{I}$*, is δ_M for any matrix M such that $\mathcal{I}_M$ is in general Noether position.*

Proposition 49. *Assume that $\mathcal{I}$ is unmixed.*

a) $\deg \sqrt{\mathcal{I}} \leq \deg \mathcal{I}$, *with equality iff $\mathcal{I}$ is radical.*

b) $\deg \mathcal{I}\colon g^\infty \leq \deg \mathcal{I}$, *with equality iff g is a nonzerodivisor in $\mathbb{B}$.*

Theorem 50. *(Bézout theorem) Assume that $\mathcal{I}$ is unmixed. Let f be a nonzerodivisor in $\mathbb{B}$, and let $\tilde{\mathcal{J}}$ denote the intersection of the isolated primary components of $\mathcal{J} = \mathcal{I} + (f)$. Then we have* $\deg \tilde{\mathcal{J}} \leq \deg \mathcal{I} \deg f$.
If $\mathcal{I}$ and f are homogeneous, this is an equality.

Proof. We can assume that $\mathcal{I}$ and $\mathcal{J}$ are in general Noether position. We know that $\tilde{\mathcal{J}}$ is unmixed of dimension -1 or $r-1$.
The extensions of $\tilde{\mathcal{J}}$ and $\mathcal{J}$ coincide in $\mathbb{K}(x_1, \ldots, x_{r-1})[x_r, \ldots, x_n]$.
Thefore $\deg \tilde{\mathcal{J}} = \deg \chi_0 \leq \deg \mathcal{I} \deg f$, with equality in the homogenous case. □