The computation of the radical of an ideal

Santiago Laplagne
Universidad de Buenos Aires

Linz, Febraury 2006

Summary

1. Basics
2. Zero dimensional ideals (Seidenberg, Kemper)
3. Positive characteristic (Matsumoto)
4. General case

Basics

- $k[\boldsymbol{x}] = k[x_1, \ldots, x_n]$, k a field
- I ideal in $k[\boldsymbol{x}]$

The radical of an ideal

$$\sqrt{I} = \{f \in k[\boldsymbol{x}] \ / \ f^m \in I \text{ for some } m \in \mathbb{N}\}$$

- I is radical if $I = \sqrt{I}$.
- $\mathbf{V}(I) = \mathbf{V}(\sqrt{I})$.
- $\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$.

Radical membership

$$f \in \sqrt{I} \iff 1 \in \langle I, tf - 1\rangle k[\boldsymbol{x}, t]$$

with t a new variable.

Applications - The Shape Lemma

(Rouillier's talk)

$I \subset k[\boldsymbol{x}]$ a zero-dimensional ideal (k perfect).

G a reduced Gröbner basis of $\sqrt{I}$ w.r.t. a lexicographical order $\boldsymbol{x} \setminus x_n >> x_n$. If x_n separate the points of $\mathbf{V}_{\bar{k}}(I)$,

then G has the following form:

$$\begin{aligned} G = \{ & g_n(x_n); \\ & x_{n-1} - g_{n-1}(x_n); \\ & \dots \\ & x_1 - g_1(x_n)\} \end{aligned}$$

and g_n has no multiple roots in $\overline{k}$.

Primary decomposition

Every ideal $I \subset k[\boldsymbol{x}]$ can be decomposed as an intersection

$$I = Q_1 \cap \cdots \cap Q_t$$

of primary ideals, with $\sqrt{Q_i} = P_i$ prime.

Primary ideals are a generalization of powers of prime ideals.

$$\sqrt{I} = \sqrt{Q_1} \cap \cdots \cap \sqrt{Q_t} = P_1 \cap \cdots \cap P_t.$$

is the *prime decomposition* of $\sqrt{I}$ (some of the primes may be redundant).

The following algorithms don't work!

- To check if I is radical: Check if $f \in \sqrt{I}$ for all generators of I, using radical membership.

  This only says that $I \subset \sqrt{I}$.

- To compute $\sqrt{I}$: compute a Gröbner basis G of I and take $\sqrt{g}$ for each $g \in G$ (the usual "Gröbner magic").

  $\sqrt{f}$ = squarefree part of f ($= \frac{f}{\gcd(f,f')}$ in characteristic 0)

Perfect and separable

- A polynomial $f \in k[x]$ is *separable* if it has only simple roots in $\bar{k}[x]$.
- k is *perfect* if every irreducible polynomial $f \in k[x]$ is separable.
- If k is perfect of characteristic $p > 0$, $\sqrt[p]{a} \in k$ for all $a \in k$.

Examples

$f = x^2 - 2 \in \mathbb{Q}[x]$ separable

$g = x^3 - t \in \mathbb{Q}(t)[x]$ separable.
$g = (x - \sqrt[3]{t})(x - \eta\sqrt[3]{t})(x - \eta^2\sqrt[3]{t})$

$h = x^3 - t \in \mathbb{Z}_3(t)[x]$ not separable. $h = (x - \sqrt[3]{t})^3$.

Finite fields, algebraically closed fields and fields of characteristic 0 are perfect.

The 0-dimensional case

Seidenberg algorithm

$I \subset k[\boldsymbol{x}]$ a 0-dimensional ideal, k a perfect field.

$f_i \in I \cap k[x_i]$, for $i = 1, \ldots, n$.

$g_i = \sqrt{f_i}$, the squarefree part.

Then,

$$\sqrt{I} = \langle I, g_1, \ldots, g_n \rangle.$$

Example

$I = \langle y + z, z^2 \rangle \subset \mathbb{Q}[y, z]$.

- $z^2 \in I$
- $y^2 = (y - z)(y + z) + z^2 \in I$.

Then,

$$\sqrt{I} = \langle y + z, z^2, y, z \rangle = \langle y, z \rangle.$$

The 0-dimensional case

If the field is not perfect, Seidenberg algorithm might fail.

Example

$I = \langle x^p - t, y^p - t \rangle \subset \mathbb{Z}_p(t)[x, y]$.

Both polynomials are squarefree, but $x^p - y^p \in I$ and therefore $x - y \in \sqrt{I} \setminus I$.

The separable part

$$f = c\prod(x-\alpha_i)^{d_i}\prod(x-\beta_i)^{pe_i}$$

Computation of $\prod(x-\beta_i)^{e_i}$

$$f' = \sum d_i \frac{f}{x-\alpha_i}$$

$$h := \gcd(f, f')$$

$$= \prod(x-\alpha_i)^{d_i-1}\prod(x-\beta_i)^{pe_i}$$

Iterating,

$$\tilde{h} = \prod(x-\beta_i)^{pe_i} = u(x^p)$$

$$v := \sqrt[p]{\tilde{h}} = \prod(x-\beta_i)^{e_i}$$

$$\in K(\sqrt[p]{t_1}, \ldots, \sqrt[p]{t_m})[x]$$

Computation of $\prod(x-\alpha_i)$

$$g_1 = \frac{f}{\gcd(f,f')} = c\prod(x-\alpha_i)$$

Example

Computation of $\prod(x-\beta_i)^{e_i}$

$$f = (x-1)^2(x^p-t)$$

$$= (x-1)^2(x-\sqrt[p]{t})^p$$

$$f' = 2(x-1)(x-\sqrt[p]{t})^p = 2\frac{f}{x-1}$$

$$h = (x-1)(x-\sqrt[p]{t})^p$$

$$\tilde{h} = (x-\sqrt[p]{t})^p = x^p - t$$

$$v = x - \sqrt[p]{t}$$

Computation of $\prod(x-\alpha_i)^{d_i}$

$$g_1 = \frac{(x-1)^2(x^p-t)}{(x-1)(x^p-t)} = x-1$$

$$\mathrm{sep}(f) = (x-1)(x-\sqrt[p]{t})$$

The 0-dimensional case over non-perfect fields

Kemper algorithm (2002)

$I \subset k[\boldsymbol{x}]$ 0-dim ideal, $k = K(t_1, \ldots, t_m)$, K perfect of characteristic $p > 0$.

$f_i \in I \cap k[x_i]$, for $i = 1, \ldots, n$. $\text{sep}(f_i) \in K(\sqrt[p^{r_i}]{t_1} \ldots \sqrt[p^{r_i}]{t_m})[x_i]$

Take $g_i \in k[y_1, \ldots, y_m, x_i]$ s.t. $\text{sep}(f_i) = g_i(\sqrt[q]{t_1}, \ldots, \sqrt[q]{t_m}, x_i)$, $q = p^r$, $r = \max\{r_1, \ldots, r_n\}$,

$$J = Ik[x_1, \ldots, x_n, y_1, \ldots, y_m] +$$
$$+ \langle g_1, \ldots, g_n \rangle +$$
$$+ \langle y_1^q - t_1, \ldots, y_m^q - t_m \rangle$$

$\sqrt{I} = J \cap k[x_1, \ldots, x_n]$

Example

$$I = \langle x_1^p - t, x_2^p - t \rangle$$
$$\subset \mathbb{Z}_p(t)[x_1, x_2]$$

$\text{sep}(x_i^p - t) = x_i - \sqrt[p]{t}$

$$g_i = x_i - y$$
$$J = \langle x_1^p - t, x_2^p - t \rangle +$$
$$+ \langle x_1 - y, x_2 - y \rangle +$$
$$+ \langle y^p - t \rangle \subset k[x_1, x_2, y]$$
$$G = \{y - x_2, x_1 - x_2, x_2^p - t\}$$
$$\sqrt{I} = \langle x_1 - x_2, x_2^p - t \rangle$$

The general case over finite fields

Matsumoto algorithm (2001)

$I \subset k[\boldsymbol{x}]$ an ideal, with k a finite field of p^r elements

$\phi : f \mapsto f^p$, $f \in k[\boldsymbol{x}]$, morphism

$I \subset \phi^{-1}(I) \subset \sqrt{I}$ and $I = \sqrt{I} \iff I = \phi^{-1}(I)$.

$\phi_c(\sum a_{m_1,\ldots,m_n} x_1^{m_1} \ldots x_n^{m_n}) := \sum a^p_{m_1,\ldots,m_n} x_1^{m_1} \ldots x_n^{m_n}$

$\phi_v(f(x_1, \ldots, x_n)) := f(x_1^p, \ldots, x_n^p)$

$\phi = \phi_v \circ \phi_c$

Matsumoto algorithm

Let $I = \langle f_1, \ldots, f_s \rangle$.

Computation of $\phi_c^{-1}(I)$
$\phi_c^{-1}(I) = \langle \phi_c^{-1}(f_1), \ldots, \phi_c^{-1}(f_s) \rangle$

Computation of $\phi_v^{-1}(I)$
$J = I + \langle y_1 - x_1^p, \ldots, y_n - x_n^p \rangle$
$\phi_v^{-1}(I) = J \cap k[y_1, \ldots, y_n]$, with y_i replaced by x_i.

We have

$$\phi^{-1}(I) = \phi_v^{-1}(\phi_c^{-1}(I)).$$

If $I = \phi^{-1}(I)$, then $\sqrt{I} = I$. Else, replace I by $\phi^{-1}(I)$ and iterate.

Example in $\mathbb{Z}_2[x, y, z, w]$.

- $I = \langle y + z, xz^2w, x^2z^2 \rangle$
- $\phi_c^{-1}(I) = I$
- $J = I + \langle X - x^2, Y - y^2, Z - z^2, W - w^2 \rangle$
- $G = \{Y + Z, XZ, w^2 + W, z^2 + Z, y + z, xZW, xwZ, x^2 + X\}$, Gröbner base of J for lexicographical order.
- $\phi^{-1}(I) = \langle y + z, xz \rangle$

If we iterate, we obtain the same ideal. Therefore,

$$\sqrt{I} = \langle y + z, xz \rangle$$

General case - Reduction to the 0-dimensional case

Maximal independent set

$\boldsymbol{u} \subset \boldsymbol{x}$ is *independent* if

$$I \cap k[\boldsymbol{u}] = \langle 0 \rangle.$$

$\boldsymbol{u}$ is a *maximal independent set* if it is not properly included in any other independent set.

Reduction. If $\boldsymbol{u}$ is a maximal independent set,

$$Ik(\boldsymbol{u})[\boldsymbol{x} \setminus \boldsymbol{u}]$$

is 0-dimensional in $k(\boldsymbol{u})[\boldsymbol{x} \setminus \boldsymbol{u}]$. $\sqrt{Ik(\boldsymbol{u})[\boldsymbol{x} \setminus \boldsymbol{u}]}$ can be computed by the 0-dimensional case.

Example Let

$$I = \langle y+z, xz^2w, x^2z^2 \rangle \subset \mathbb{Q}[x,y,z,w].$$

$\boldsymbol{u} = \{x, w\}$ is a maximal independent set.

$$I\ \mathbb{Q}(x,w)[y,z] = \langle y+z, z^2 \rangle$$

is 0-dimensional in $\mathbb{Q}(x,w)[y,z]$.

$$\sqrt{I\ \mathbb{Q}(x,w)[y,z]} = \langle y, z \rangle$$

How to use the 0-dimensional case?

$I = Q_1 \cap \cdots \cap Q_t$ (unknown) s.t.

$Q_i \cap k[\boldsymbol{u}] = \{0\}$ for $1 \leq i \leq s$ and

$Q_i \cap k[\boldsymbol{u}] \neq \{0\}$ for $s+1 \leq i \leq t$

Then:

- $Ik(\boldsymbol{u})[\boldsymbol{x} \setminus \boldsymbol{u}] \cap k[\boldsymbol{x}] = Q_1 \cap \cdots \cap Q_s$
- $\sqrt{I} = \sqrt{Q_1 \cap \cdots \cap Q_s} \cap \sqrt{Q_{s+1}} \cap \cdots \cap \sqrt{Q_t}$
  $= \sqrt{Ik(\boldsymbol{u})[\boldsymbol{x} \setminus \boldsymbol{u}] \cap k[\boldsymbol{x}]} \cap \sqrt{Q_{s+1}} \cap \cdots \cap \sqrt{Q_t}$
  $= (\sqrt{Ik(\boldsymbol{u})[\boldsymbol{x} \setminus \boldsymbol{u}]} \cap k[\boldsymbol{x}]) \cap \sqrt{Q_{s+1}} \cap \cdots \cap \sqrt{Q_t}.$
- $J := \sqrt{Ik(\boldsymbol{u})[\boldsymbol{x} \setminus \boldsymbol{u}]} \cap k[\boldsymbol{x}]$ can be computed (by saturation).
- It remains to consider $\sqrt{Q_{s+1}} \cap \cdots \cap \sqrt{Q_t}$.

Krick-Logar algorithm (1991)

$J := \sqrt{Ik(\boldsymbol{u})[\boldsymbol{x} \setminus \boldsymbol{u}]} \cap k[\boldsymbol{x}]$

$\exists h \in k[\boldsymbol{u}]$ such that

$$\sqrt{I} = J \cap \sqrt{(I, h)}.$$

Now $\boldsymbol{u}$ is not independent with respect to $\langle I, h \rangle$.
We can compute $\sqrt{\langle I, h \rangle}$ by induction on the number of independent sets.

Example We have

- $I = \langle y + z, xz^2w, x^2z^2 \rangle$.
- $\sqrt{I \; \mathbb{Q}(x, w)[y, z]} \cap \mathbb{Q}[\boldsymbol{x}] = \langle y, z \rangle$.
- We can take $h := xw$.
- $\sqrt{I} = \langle y, z \rangle \cap \sqrt{\langle I, xw \rangle}$.
- Carrying on the algorithm, we get $\sqrt{\langle I, xw \rangle} = \sqrt{\langle y + z, x \rangle} \cap \sqrt{\langle w, y + z, z^2 \rangle}$.

The last component is redundant.

$$\sqrt{I} = \langle y, z \rangle \cap \sqrt{\langle y + z, x \rangle} = \langle y + z, xz \rangle.$$

A different algorithm

$J := \sqrt{Ik(\boldsymbol{u})[\boldsymbol{x} \setminus \boldsymbol{u}]} \cap k[\boldsymbol{x}]$
$\sqrt{I} = J \cap \sqrt{Q_{s+1} \cap \cdots \cap Q_t}$
If $\sqrt{I} \neq J$, $\exists g$ in any set of generators of J such that $g \notin \sqrt{I}$.
Then $\exists P$ minimal prime s.t. $g \notin P$ and

$$(I : g^\infty) = \bigcap_{g \notin P_i} Q_i$$

is the intersection of some componets among $Q_{s+1}, \ldots, Q_t$.
Iterating with $(I : g^\infty)$, we get new components of I.

Example

- We look for $g \in \langle y, z \rangle$ such that $g \notin \sqrt{I}$ (using Radical Membership).
  We take $g := z \notin \sqrt{I}$.
- $(I : z^\infty) = \langle y + z, xw, x^2 \rangle$ intersection of new primary components of I.

Let's finish the example

- $I = \langle y + z, xz^2w, x^2z^2 \rangle$.
- $\sqrt{I\ \mathbb{Q}(x,w)[y,z] \cap \mathbb{Q}[\boldsymbol{x}]} = \langle y, z \rangle$.
- $z \notin \sqrt{I}$ and $I_2 := (I : z^\infty) = \langle y + z, xw, x^2 \rangle$ contains only new primary components of I.
- $\boldsymbol{u} := \{z, w\}$ is a maximal independent set w.r.t. I_2.
- $\sqrt{I_2\ \mathbb{Q}(z,w)[x,y]} \cap \mathbb{Q}[\boldsymbol{x}] = \langle y + z, x \rangle$.
- We intersect the two ideals found.

$$\tilde{P} = \langle y, z \rangle \cap \langle y + z, x \rangle = \langle y + z, xz \rangle.$$

- All the generators of $\tilde{P}$ are in $\sqrt{I}$. Then, $\sqrt{I} \subset \tilde{P} \subset \sqrt{I}$.
- $\sqrt{I} = \langle y + z, xz \rangle$.

There is a kind of situation that occurs quite frequently when Grobner basis computations are involved:

Even the most sophisticated complexity theory is -at least at present- not strong enough to allow a clear decision between two possible versions of an algorithm. One has therefore to rely on practical experience, and it is not impossible for different people to arrive at different conclusions.

Thomas Becker, Volher Weispfenning. Gröbner Bases.
Springer-Verlag, 1993

References

[1] W. Decker, G. Gruel, G. Pfister. Primary Decomposition: Algorithms and Comparisons. *Algorithmic algebra and number theory*, 187-220, 1999.

[2] P. Gianni, B. Trager, and G. Zacharias. Bases and primary decomposition of ideals. *J. Symbolic Computation*, (6):149–167, 1988.

[3] G. Kemper. The calculation of radical ideals in positive characteristic. *J. Symbolic Computation*, (34):229–238, 2002.

[4] T. Krick and A. Logar. An algorithm for the computation of the radical of an ideal in the ring of polynomials. *AAECC9, Springer LNCS*, (539):195–205, 1991.

[5] M. Kreuzer and L. Robbiano. Computational Commutative Algebra 1. *Springer-Verlag*, 2000.

[6] R. Matsumoto. Computing the radical of an ideal in positive characteristic. *J. Symbolic Computation*, (32):263–271, 2001.

[7] A. Seidenberg. Constructions in algebra. *Trans. Amer. Math. Soc.*, (197):273–313, 1974.

Other algorithms

M. Caboara, P. Conti, and C. Traverso. Yet another algorithm for ideal decomposition. *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, (12):39–54, 1997.

D. Eisenbud, C. Huneke, and W. Vasconcelos. Direct methods for primary decomposition. *Invent. Math.*, (110):207–235, 1992.

E. Fortuna, P. M. Gianni, B. M. Trager. Derivations and Radicals of Polynomial Ideals over Fields of Arbitrary Characteristic. *J. Symb. Comput.*, (33):609–625, 2002.