An algorithm for the computation of the radical of an ideal

Santiago Laplagne
Universidad de Buenos Aires

Colonia, Agosto 2005

Basics

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

The radical of an ideal

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

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

Radical membership

$$f \in \sqrt{I} \iff 1 \in \langle I, tf - 1 \rangle_{k[x_1, \ldots, x_n, t]}$$

with t a new variable.

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.

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

(some of the primes may be redundant).

The 0-dimensional case

Seidenberg's algorithm

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

$f_i \in I \cap k[x_i]$, 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,

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

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,

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

is 0-dimensional in $k(\boldsymbol{u})[\boldsymbol{x} \setminus \boldsymbol{u}]$. $\sqrt{I k(\boldsymbol{u})[\boldsymbol{x} \setminus \boldsymbol{u}]}$ 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 $\boldsymbol{u}$ in 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, $\sqrt{I} \subset \tilde{P} \subset \sqrt{I}$.
- $\sqrt{I} = \langle y+z, xz\rangle$.