An Introduction to CAS SINGULAR. Part II Solving

Viktor Levandovskyy, RWTH Aachen, Germany

4th SCIence Training School in Symbolic Computation

10.07.2009, RISC, Hagenberg

Useful links

You can find test files I present for SINGULAR at

```
http://www.math.rwth-aachen.de/~Viktor.Levandovskyy/filez/risc/
```

Singular Online Manual: keep it open

```
http://www.singular.uni-kl.de/Manual/latest/index.htm
```

Nice Surfaces online and SURFER

```
http://www.imaginary2008.de/?lang=en
```

Symbolic-Numerical Solving

A system of equations S over the field $\mathbb{K}$ corresponds to the ideal $I = I(S)$. There is a finite number of solutions over $\bar{\mathbb{K}}$ if and only if the *dimension* (Krull dimension) of I is 0.

What does solving mean?

There might be different wishes, like

- compute one, some or all the roots with or without multiplicities numerically with a given precision
- compute a field extension $\mathbb{K} \subseteq L$, such that there are exact symbolic expressions for the roots of S in L

SINGULAR has procedures for both ways of solving. The second way can be done, using the primary decomposition.

Symbolic-Numerical Solving. Numerical Fashion.

Recipe for the numerical solving:

1. Check that a given system is consistent (i.e. it has solutions). Compute a Gröbner basis G of the given ideal $I \subset R := \mathbb{K}[x_1, \ldots, x_n]$ with respect to a fast ordering like `dp`. A system has solutions if and only if G does not contain a constant.
2. A consistent system has finitely many solutions over $\mathbb{K}$ if and only if $\dim R/I = \dim R/\langle G \rangle = 0$. Compute $\dim R/\langle G \rangle$.
3. If $\dim R/\langle G \rangle = 0$, compute another Gröbner basis T of I with respect to lexicographical ordering (not easy!)
4. Apply your favourite numerical solver to T. In SINGULAR, many different solvers are implemented.

Gröbner basics

The most important and fundamental applications of GB

- Ideal (resp. module) membership problem: `NF, reduce`
- Elimination of variables: `eliminate`
- Intersection of ideals (resp. submodules): `intersect`
- Quotient and saturation of ideals: `quot`
- Kernel of a module homomorphism: `modulo`
- Kernel of a ring homomorphism: `preimage`
- Algebraic relations between polynomials: ALGEBRA.LIB
- Hilbert polynomial of graded ideals and modules: `hilb`

Various Features

Visualization Tools

- LATEX.LIB converts SINGULAR output of different types to LaTeX
- SURF, SURFER provide HQ plotting of curves and surfaces

Third-party Functionality

- nearly 100 libraries distributed with SINGULAR
- dynamical modules mechanism is available
- namespaces (type `package`)
- `libSingular` is possible to use with your C code!

Selected Strong Points

- PRIMDEC.LIB, MPRIMDEC.LIB

  primary decomposition (including the absolute one!)

  radical, minimal associated primes
- SOLVE.LIB, PRESOLVE.LIB, TRIANG.LIB etc.

  various methods for numerical solving 0-dimensional systems of polynomial equations
- RESOLVE.LIB, RESZETA.LIB

  resolution of singularities and its applications
- INTPROG.LIB, TORIC.LIB

  integer programming, toric ideals and Gröbner bases
- CONTROL.LIB

  algebraic analysis tools for System and Control Theory

Characterizations of Gröbner Bases

Definition

Let S be any subset of R.

- We define a **monoideal of leading exponents** $\mathcal{L}(S) \subseteq \mathbb{N}^n$ to be a $\mathbb{N}^n$–monoideal $\mathcal{L}(S) = {}_{\mathbb{N}^n}\langle \alpha \mid \exists s \in S,\ \mathrm{lex}(s) = \alpha \rangle$, generated by the leading exponents of elements of S.
- $L(S)$, the **span of leading monomials of** S, is defined to be the $\mathbb{K}$–vector space, spanned by the set $\{x^\alpha \mid \alpha \in \mathcal{L}(S)\} \subseteq R$.

Equivalences

- G is a Gröbner basis of $I \Leftrightarrow \forall\, f \in I \setminus \{0\}$ there exists a $g \in G$ satisfying $\mathrm{lm}(g) \mid \mathrm{lm}(f)$,
- G is a Gröbner basis of $I \Leftrightarrow L(G) = L(I)$ as $\mathbb{K}$–vector spaces,
- G is a Gröbner basis of $I \Leftrightarrow \mathcal{L}(G) = \mathcal{L}(I)$ as $\mathbb{N}^n$–monoideals.

Criteria for detecting useless critical pairs

Product Criterion

Let $f, g \in \mathbb{K}[\mathbf{x}] \setminus \{0\}$. Suppose that $\mathrm{lm}(f)$ and $\mathrm{lm}(g)$ have no common factors, then $\mathrm{spoly}(f, g) \to_{\{f,g\}} 0$.

The following criterion is more involved but more powerful

Chain Criterion

If (f_i, f_j), (f_i, f_k) and (f_j, f_k) are in the set of pairs P, denote $\mathrm{lm}(f_\nu) = x^{\alpha_\nu}$. If $x^{\alpha_j} \mid \mathrm{lcm}(x^{\alpha_i}, x^{\alpha_k})$ holds, then we can delete (f_i, f_k) from P.

Characterization of zero-dimensional ideals

Let $\mathbb{K}[\mathbf{x}] := \mathbb{K}[x_1, \ldots, x_n]$.

Theorem

The following conditions are equivalent:

1. $I \subset \mathbb{K}[\mathbf{x}]$ *is zero-dimensional, that is* $\dim_{\mathbb{K}} \mathbb{K}[\mathbf{x}]/I$ *is finite*
2. $\forall 1 \leq i \leq n,\ \exists\, f \in I$ *and* $d_i \in \mathbb{N}$, *such that* $\mathrm{lm}(f) = x_i^{d_i}$
3. $\forall 1 \leq i \leq n,\ \exists\, f \in I$ *such that* $f \in \mathbb{K}[x_i]$

In particular, if G is a Gröbner basis of I, then $\forall 1 \leq i \leq n,\ \exists\, g \in G$, such that $\mathrm{lm}(g) = x_i^{d_i}$.

Characterization of zero-dimensional ideals

Let $\mathbb{K}[\mathbf{x}] := \mathbb{K}[x_1, \ldots, x_n]$.

Theorem

The following conditions are equivalent:

1. $I \subset \mathbb{K}[\mathbf{x}]$ *is zero-dimensional, that is* $\dim_{\mathbb{K}} \mathbb{K}[\mathbf{x}]/I$ *is finite*
2. $\forall 1 \leq i \leq n,\ \exists\, f \in I$ *and* $d_i \in \mathbb{N}$, *such that* $\mathrm{lm}(f) = x_i^{d_i}$
3. $\forall 1 \leq i \leq n,\ \exists\, f \in I$ *such that* $f \in \mathbb{K}[x_i]$

In particular, if G is a Gröbner basis of I, then $\forall 1 \leq i \leq n,\ \exists\, g \in G$, such that $\mathrm{lm}(g) = x_i^{d_i}$.

Characterization of zero-dimensional ideals II

The last characterization says that $\forall 1 \leq i \leq n,\ I \cap \mathbb{K}[x_i] \neq 0$. Since $\mathbb{K}[x_i]$ is a principal ideal domain, $I \cap \mathbb{K}[x_i] = \langle g(x_i) \rangle$.

$L(I) = \{\mathrm{lm}(f) \mid f \in I\}$ is a monomial ideal, called the leading ideal of I. The Gröbner approach leads to the following isomorphism of $\mathbb{K}$-vector spaces:

$$\mathbb{K}[x_1, \ldots, x_n] \ \cong\ \mathbb{K}[x_1, \ldots, x_n]/I \oplus L(I) \quad f \mapsto r\ +\ \sum a_i f_i$$

Since $\dim_{\mathbb{K}} \mathbb{K}[x_1, \ldots, x_n]/I < \infty$, let $V := \mathbb{K}[x_1, \ldots, x_n]/I$ be fin. dim. $\mathbb{K}$-vector space. Hence $\phi : V \to V,\ v \mapsto vx_i$ is an endomorphism and thus ϕ has a well-defined minimal polynomial!

Principal Intersection

Require: $s \in R, J \subset R$ an ideal such that $Kr.dim\ R/J = 0$.
Ensure: $b \in \mathbb{K}[s]$ monic such that $J \cap \mathbb{K}[s] = \langle b \rangle$

$G :=$ a Gröbner basis of J
$i := 1$
loop
  if there exist $a_0, \ldots, a_{i-1} \in \mathbb{K}$ such that

$$\mathrm{NF}(s^i, G) + \sum_{j=0}^{i-1} a_j \mathrm{NF}(s^j, G) = 0 \textbf{ then}$$

    return $b := s^i + \sum_{j=0}^{i-1} a_j s^j$
  else
    $i := i + 1$
  end if
end loop

Primary Decomposition: The Beginning

Definition

Let A be a Noetherian ring, and let $I \subset A$ be an ideal.

1. The set of *associated primes* of I, denoted by $\mathrm{Ass}(I)$, is defined as

$$\mathrm{Ass}(I) = \left\{ P \subset A \,\middle|\, P \text{ prime}, P = I : \langle b \rangle \text{ for some } b \in A \right\}.$$

   Elements of $\mathrm{Ass}(\langle 0 \rangle)$ are also called *associated primes* of A.
2. Let $P, Q \in \mathrm{Ass}(I)$ and $Q \subsetneq P$, then P is called an *embedded prime ideal* of I. We define $\mathrm{Ass}(I, P) := \{Q \mid Q \in \mathrm{Ass}(I), Q \subset P\}$.
3. I is a *primary ideal* if, for any $a, b \in A$, $ab \in I$ and $a \notin I$ imply $b \in \sqrt{I}$. Let P be a prime ideal, then a primary ideal I is called *P–primary* if $P = \sqrt{I}$.
4. A *primary decomposition* $I = Q_1 \cap \cdots \cap Q_s$ with Q_i primary ideals, is called *irredundant* if no Q_i can be omitted in the decomposition and if $\sqrt{Q_i} \neq \sqrt{Q_j}$ for all $i \neq j$.

Primary Decomposition: Main Theorems

Theorem

Let A be a Noetherian ring and $I \subset A$ be an ideal, then there exists an irredundant decomposition $I = Q_1 \cap \cdots \cap Q_r$ of I as intersection of primary ideals $Q_1, \ldots, Q_r$.

Theorem

Let A be a ring and $I \subset A$ be an ideal with irredundant primary decomposition $I = Q_1 \cap \cdots \cap Q_r$. Then $r = \#\,\mathrm{Ass}(I)$,

$$\mathrm{Ass}(I) = \{\sqrt{Q_1}, \ldots, \sqrt{Q_r}\},$$

and if $\{\sqrt{Q_{i_1}}, \ldots, \sqrt{Q_{i_s}}\} = \mathrm{Ass}(I, P)$ for $P \in \mathrm{Ass}(I)$ then $Q_{i_1} \cap \cdots \cap Q_{i_s}$ is independent of the decomposition.

Primary Decomposition: Detailed Example

Example (Cyclic 4–th)

The system is given by the following equations:

$$\begin{aligned} &x + y + z + t, \\ &xy + yz + xt + zt, \\ &xyz + xyt + xzt + yzt, \\ &xyzt - 1 \end{aligned}$$

Unlike `cyclic(3)` or `cyclic(5)`, the system is not 0–dimensional. In $\mathbb{Q}(t)[x, y, z]$ we have however for the ideal I of the system

$$\sqrt{I} = \langle x - \frac{1}{t}, y + t, z + \frac{1}{t} \rangle \cap \langle x + \frac{1}{t}, y + t, z - \frac{1}{t} \rangle$$

Primary Decomposition: a Recipe

1. Compute the Gröbner basis G of I (fast ordering)
2. Compute the radical R of G with e.g. `radical`
3. Compute the minimal associated primes with e.g. `minAssGTZ` or `minAssChar`
4. Analyze each component separately, eventually passing to an extension field

Alternatively, obtain numerical solutions for 0–dimensional components with e.g. `solve`.
If one wish to compute the multiplicities of solutions, one needs the primary decomposition (`primdecGTZ, primdecSY` etc.) and, in particular, the information on primary (and not only prime) components.
The procedures for the primary decomposition are gathered in the `primdec.lib`.