Algorithms in Singular

Hans Schönenmann

October 14, 1996

Abstract

Some algorithms for singularity theory and algebraic geometry

The use of Gröbner basis computations for treating systems of polynomial equations
has become an important tool in many areas. This paper introduces of the concept of
standard bases (a generalization of Gröbner bases) and the application to some problems
from algebraic geometry. The examples are presented as SINGULAR commands. A general
introduction to Gröbner bases can be found in the textbook [CLO], an introduction to
syzygies in [E] and [St1].

SINGULAR is a computer algebra system for computing information about singularities,
for use in algebraic geometry. The basic algorithm in SINGULAR is a general standard basis
algorithm for general monomial orderings (see [GG]). This includes wellorderings (Buch-
berger algorithm ([B1],[B2]) and tangent cone orderings (Mora algorithm ([M1],[MPT]))
as special cases: It is able to work with non-homogeneous and homogeneous input and
also to compute in the localization of the polynomial ring in 0. For a complete description
of SINGULAR see [Si].
1 Basic definitions

1.1 Monomial orderings

The basis ingredient for all standard basis algorithms is the ordering of the monomials (and the concept of the leading term: the term with the highest monomial).

A monomial ordering (term ordering) on \( K[x_1, \ldots, x_n] \) is a total ordering \(<\) on the set of monomials (power products) \( \{x^\alpha | \alpha \in \mathbb{N}^n \} \) which is compatible with the natural semigroup structure, i.e. \( x^\alpha < x^\beta \) implies \( x^\gamma x^\alpha < x^\gamma x^\beta \) for any \( \gamma \in \mathbb{N}^n \).

The ordering \(<\) is called a wellordering iff 1 is the smallest monomial. Most of the algorithms work for general orderings.

Robbiano (cf. [R]) proved that any semigroup ordering can be defined by a matrix \( A \in GL(n, \mathbb{R}) \) as follows (matrix ordering):

Let \( a_1, \ldots, a_k \) be the rows of \( A \), then \( x^\alpha < x^\beta \) if and only if there is an \( i \) with \( a_j \alpha = a_j \beta \) for \( j < i \) and \( a_i \alpha < a_i \beta \). Thus, \( x^\alpha < x^\beta \) if and only if \( A \alpha \) is smaller than \( A \beta \) with respect to the lexicographical ordering of vectors in \( \mathbb{R}^n \).

We call an ordering a degree ordering if it is given by a matrix with coefficients of the first row either all positive or all negative.

Let \( K \) be a field; for \( g \in K[x] \), \( g \neq 0 \), let \( L(g) \) be the leading monomial with respect to the ordering \( <^{-1} \) and \( c(g) \) the coefficient of \( L(g) \) in \( g \), that is \( g = c(g)L(g) + \) smaller terms with respect to \(<\).

\(<\) is an elimination ordering for \( x_{r+1}, \ldots, x_n \) iff \( L(g) \in K[x_1, \ldots, x_r] \) implies \( g \in K[x_1, \ldots, x_r] \).

1.2 Examples for monomial orderings

Important orderings for applications are:

- The lexicographical ordering \( lp \), given by the matrix:

\[
\begin{pmatrix}
1 & 0 \\
1 & 0 \\
\vdots & \ddots & \ddots & \ddots \\
0 & \cdots & 1 \\
\end{pmatrix}
\]

resp. is:

\[
\begin{pmatrix}
-1 & 0 \\
-1 & 0 \\
\vdots & \ddots & \ddots & \ddots \\
0 & \cdots & 1 \\
\end{pmatrix}
\]

\textbf{Remark 1.1} The positive lexicographic ordering \( lp \) on \( K[x_1, \ldots, x_n] \) is an elimination ordering for \( x_1, \ldots, x_i \forall 1 \leq i \leq n \)

The definition of rings with these orderings in SINGULAR:

(Each definition starting with \(/\) is a comment in SINGULAR.)

\footnote{We write the terms of a polynomial in decreasing order}
ring R1=0,(x(1..5)),lp;
ring R2=0,(x(1..5)),ls;

- The **weighted degree reverse lexicographical ordering**, given by the matrix

\[
wp : \begin{pmatrix}
  w_1 & w_2 & \ldots & w_n \\
  -1 & & & \\
  0 & -1 & & \\
\end{pmatrix}
\]

\(w_i > 0\forall i\) (resp. \(ws : w_1 \neq 0, w_i \in \mathbb{Z} \forall i\)).

If \(w_i = 1\) (respectively \(w_i = -1\)) for all \(i\) we obtain the **degree reverse lexicographical ordering**, \(dp\) (respectively \(ds\)).

The definition of rings with these orderings in **SINGULAR**:

ring R3=0,(x(1..5)),wp(2,3,4,5,6);
// correspond to \(w_i:2,3,4,5,6\)
ring R4=0,(x(1..5)),ws(2,3,4,5,6);
// correspond to \(w_i:-2,-3,-4,-5,-6\)
ring R5=0,(x(1..4)),dp;
ring R6=0,(x(1..4)),ds;

- An example for an **elimination ordering** for \(x_{r+1}, \ldots, x_n\) in \(K[x] = \text{Loc}_< K[x]\) is given by the matrix

\[
\begin{pmatrix}
  0 & 0 & \ldots & 0 & w_{r+1} & w_{r+2} & \ldots & w_n \\
  w_1 & w_2 & \ldots & w_r & 0 & 0 & \ldots & 0 \\
  & & & & & 0 & 0 & \ldots & 0 \\
  & & & & & & -1 & & \\
\end{pmatrix}
\]

with \(w_1 > 0, \ldots, w_n > 0\). In \(K[x_1, \ldots, x_r][x_{r+1}, \ldots, x_n] = \text{Loc}_< K[x]\) it is given by the same matrix with \(w_1 < 0, \ldots, w_r < 0\) and \(w_{r+1} > 0, \ldots, w_n > 0\).

The definition of a polynomial ring with an elimination ordering for \(x_3\) and \(x_4\) in **SINGULAR**:

ring E=0,(x(1..4)),(a(0,0,1,1),a(1,1,1),dp);
// correspond to \(w_i=1\) for all \(i, r=2\)
// or simpler:
ring EE=0,(x(1..4)),(a(0,0,1,1),dp);

- The **product ordering**, given by the matrix

\[
\begin{pmatrix}
  A_1 \\
  A_2 \\
  \vdots \\
  0 \\
  A_k
\end{pmatrix}
\]
if the $A_i$ define orderings on monomials given by the corresponding subsets of $\{x_1, \ldots, x_n\}$. Such an ordering can be used to compute in

\begin{align*}
- K(\overline{y|x}) \ (A_1 : \text{dp on } x, \ A_2 : \text{dp on } y) \\
- (K[y|x]) \ (A_1 : \text{dp on } x, \ A_2 : \text{ds on } y) \\
- (K[y]|x) \ (A_1 : \text{ds on } x, \ A_2 : \text{dp on } y)
\end{align*}

(See [GTZ], [GG], definition 2.1).

The definition of a ring with this ordering in SINGULAR:

```
ring P=0,(x(1..6)),(dp(4),ds(2));
// correspond to
// a first block of 4 variables with ordering dp
// and a second block of 2 variables with ordering ds
```
2 Standard bases

**Definition 2.1** We define \( \text{Loc}_< K[x] := S_0^{-1} K[x] \) to be the localization of \( K[x] \) with respect to the multiplicative closed set \( S_0 = \{1 + g \mid g = 0 \text{ or } g \in K[x] \setminus \{0\} \text{ and } 1 > L(g)\} \).

**Remark 2.2**

1) \( K[x] \subseteq \text{Loc}_< K[x] \subseteq K[x(x)] \), where \( K[x(x)] \) denotes the localization of \( K[x] \) with respect to the maximal ideal \( (x_1, \ldots, x_n) \). In particular, \( \text{Loc}_< K[x] \) is noetherian, \( \text{Loc}_< K[x] \) is \( K[x] \)-flat and \( K[x(x)] \) is \( \text{Loc}_< K[x] \)-flat.

2) If \( \triangle < \triangle \) is a wellordering then \( x^0 = 1 \) is the smallest monomial and \( \text{Loc}_< K[x] = K[x] \). If \( 1 > x_i \) for all \( i \), then \( \text{Loc}_< K[x] = K[x(x)] \).

3) If, in general, \( x_1, \ldots, x_r < 1 \) and \( x_{r+1}, \ldots, x_n > 1 \) then

\[
1 + (x_1, \ldots, x_r) K[x_1, \ldots, x_r] \subseteq S_0 \subseteq 1 + (x_1, \ldots, x_r) K[x] =: S,
\]

hence

\[
K[x_1, \ldots, x_r][x_{r+1}, \ldots, x_n] \subseteq \text{Loc}_< K[x] \subseteq S^{-1} K[x].
\]

2.1 Definition

**Definition 2.3**

1) \( L(I) \) denotes the ideal of \( K[x] \) generated by \( \{L(f) \mid f \in I\} \).

2) \( f_1, \ldots, f_s \in I \) is called a standard basis of \( I \) if \( \{L(f_1), \ldots, L(f_s)\} \) generates the ideal \( L(I) \subset K[x] \).

**Singular example** A standard basis computation:

```plaintext
// define a ring R= (Z/32003)[x,y,z]
ring R = 32003, (x,y,z), dp ;
// define 3 polynomials
poly s1 = x^3*y^2 + 151*x^5*y + 169*x^2*y^4
       + 151*x^2*y*z^3 + 186*x*y^6 + 169*y^9;
poly s2 = x^2*y^2*z^2 + 3*z^8;
poly s3 = 5*x^4*y^2 + 4*x*y^5 + 2*x^2*y^2*z^3 + y^7 + 11*x^10;
// define the ideal i generated by s1, s2, s3
ideal i = s1, s2, s3;
// compute standard basis j of i
ideal j = std(i);
// display j;
j;
```

2.2 Standard bases for submodules of free modules

We consider also **module orderings** \( <_m \) on the set of "monomials" \( \{x^a e_i\} \) of \( K[x]^r = \sum_{i=1,\ldots,r} K[x] e_i \) which are compatible with the ordering \( < \) on \( K[x] \). That is for all monomials \( f, f' \in K[x]^r \) and \( p, q \in K[x] \) we have: \( f <_m f' \) implies \( pf <_m pf' \) and \( p < q \) implies \( pf <_m qf \).
We now fix an ordering $<_m$ on $K[x]^r$ compatible with $<$ and denote it also with $<$. Again we have the notion of coefficient $c(f)$ and leading monomial $L(f)$. $<$ has the important property:

$$L(qf) = L(q)L(f) \quad \text{for } q \in K[x] \text{ and } f \in K[x]^r,$$

$$L(f + g) \leq \max(L(f), L(g)) \quad \text{for } f, g \in K[x]^r.$$

**Definition 2.4**

1) $L(I)$ denotes the submodule of $K[x]^r$ generated by $\{L(f) | f \in I\}$.

2) $f_1, \ldots, f_s \in I$ is called a standard basis of $I$ if $\{L(f_1), \ldots, L(f_s)\}$ generates the submodule $L(I) \subset K[x]^r$.

In SINGULAR submodules of free modules are defined by a set of generators. These sets are of type module.

**SINGULAR example (see [PS]):**

```plaintext
// ===============Poincare complex ===============
// counterexample to a possible generalization of a theorem of Kyoji
// Saito. A complete intersection with exact Poincare complex at 0
// but which is in no coordinate system weighted homogeneous
// see [PS] for an exact description.
//
// define (Z/32003)[[x,y,z]]
ring Rp=32003,(x,y,z),(c,ds);
// load additional procedures (milnor, tjurina)
LIB "sing.lib";
// select an example, parametrized by n and m
int n=883; int m=937;
poly f1=xy+z^(n-1);
poly f2=xz+y^(m-1)+yz2;
ideal f=f1,f2;
// define the basering as Rp/f and fetch the data
qring R=std(f);
ideal f=fetch(Rp,f);
poly f1,f2=fetch(Rp,f1),fetch(Rp,f2);
// the module Omega2:
module omega2=
[diff(f1,y),diff(f1,z),0],
[diff(f1,x),0,-diff(f1,z)],
[0,diff(f1,x),diff(f1,y)],
[diff(f2,y),diff(f2,z),0],
[diff(f2,x),0,-diff(f2,z)],
[0,diff(f2,x),diff(f2,y)];
// it can be shown, that the Poincare complex is exact, if (in this case)
//Milnor number f)+1 = multiplicity(omega2)
omega2=std(omega2);
multiplicity(omega2);
// The Milnor number of the complete intersection f";
milnor(f);
```

6
// The Tjurina number of the complete intersection f
tjurina(f);
// since the Milnor number and the Tjurina number do not coincide,
// the singularity is not weighted homogeneous

2.3 Basic properties
2.3.1 Ideal membership

**Definition 2.5** A function $NF : K[x]^r \times \{G|G \text{ standard basis}\} \to K[x]^r, (p, G) \mapsto NF(p|G)$, is called a **normal form** if for any $p \in K[x]^r$ and any $G$ the following holds: if $NF(p|G) \neq 0$ then $L(g) / L(NF(p|G))$ for all $g \in G$. $NF(g|G)$ is called the **normal form of** $p$ with respect to $G$.

**Lemma 2.6** $f \in I$ iff $NF(f, std(I)) = 0$.

SINGULAR example:

```
// f defines a trimodal singularity for generic moduli
ring R = 0,(x,y),ds;
int a1,a2,a3=random(1,100),random(-100,1),random(1,100);
poly f = (x^2-y^3)*(y+a1*x)*(y+a2*x)*(y+a3*x);
ideal J = jacob(f);
ideal I = f;
// J: I, ideal of the closure of V(J) \ V(I)
ideal Q = quotient(J,I);
// the Hessian of f
poly Hess = det(jacob(jacob(f)));
// Hess is contained in Q iff NF is 0
reduce(Hess, std(Q));
```

2.3.2 Elimination

**Lemma 2.7** Let $< \text{ be an elimination order for } y_1, \ldots, y_n, R = K[x_1, \ldots, x_r, y_1, \ldots, y_n]$. Then $std(I) \cap K[x_1, \ldots, x_r] = std(I \cap K[x_1, \ldots, x_r])$.

SINGULAR example:

```
// find the equations from a parametrization t->(t^3,t^4,t^5)
ring R=0,(x,y,z,t),dp;
ideal i=x-t^3,
    y-t^4,
    z-t^5;
ideal j=eliminate(i,t);
j;
```
2.3.3 Hilbert series

**Definition 2.8** Let $M$ be a graded module over $K[x]$. The **Hilbert series** of $M$ is the power series

$$H(M)(t) = \sum_{i=-\infty}^{\infty} \dim_K M_i t^i$$

**Lemma 2.9** Let $<$ be a (positive or negative) degree ordering and $H(M)$ the Hilbert function of (the homogenization of) $I$. Then $H(M) = H(L(M))$.

**Remark 2.10** It turns out that $H(M)(t)$ can be written in two useful ways:

1. $H(M)(t) = Q(t)/(1 - t)^n$, where $Q(t)$ is a polynomial in $t$ and $n$ is the number of variables in $K[x]$.
2. $H(M)(t) = P(t)/(1 - t)^{\dim M}$ where $P(t)$ is a polynomial and $\deg M = P(1)$.
3. vector space dimension $\dim_K(M) = \dim_K(L(M))$.

**Remark 2.11** Let $<$ be a degree ordering.

- Krull dimension: $\dim(M) = \dim(L(M))$.
- degree (for a positive degree ordering) resp. multiplicity (for a negative degree ordering) is equal for $M$ and $L(M)$.

**SINGULAR example:**

```plaintext
// the rational quartic curve J in P^3:
ring R=0,(a,b,c,d),dp;
ideal J=c3-bd2,bc-ad,b3-a2c,ac2-b2d;
// the output of hilb is Q, then P:
hilb(J);
```

2.4 Applications

2.4.1 Submodule

**Lemma 2.12** $(F) \subseteq (G)$ iff $NF(F, std(G)) = 0$.

**SINGULAR example:**

```plaintext
ring r=...;
module F=...;
module G=...;
reduce(F, std(G));
```
2.4.2 Euclidian algorithm

Lemma 2.13 If \( < \) is a wellordering and \( I = \{f,g\} \subseteq K[x] \) then the computation of the standard basis of \( I \) yields the greatest common divisor of \( f \) and \( g \).

SINGULAR example:

```plaintext
ring R=32003,x,dp;
poly f=(x^3+5)^2*(x-2)*(x^2+2)^4;
poly g=(x^3+5)*(x^2-3)*(x^2+2);
ideal I=f,g;
std(I);
// and the expected result:
(x^3+5)*(x^2+2);
```

2.4.3 Gaussian algorithm

Lemma 2.14 If \( < \) is a wellordering and the generators of \( I \) are linear then the computation of the standard basis of \( I \) is a Gaussian algorithm with the columns of \( \text{matrix}(I) \).

SINGULAR example:

```plaintext
ring R=32003,(x,y,z),dp;
ideal I=22*x+77*y+z-3,
    0*x+ 1*y+z-77,
    1*x+ 0*y+z+11;
std(I);
```

2.4.4 Kernel of a ring homomorphism

Lemma 2.15 Let \( \Phi \) be an affine ring homomorphism

\[
\Phi : R = K[x_1, \ldots, x_m]/I \rightarrow K[y_1, \ldots, y_n]/(g_1, \ldots, g_s)
\]

given by \( f_i = \Phi(x_i) \in K[y_1, \ldots, y_n]/(g_1, \ldots, g_s) \), \( i = 1, \ldots, m \).

Then \( \text{Ker}(\Phi) \) is generated by

\[
(g_1(y), \ldots, g_s(y), (x_1 - f_1(y)), \ldots, (x_m - f_m(y))) \cap K[x_1, \ldots, x_m]
\]
in \( K[x_1, \ldots, x_m]/I \).

Remark 2.16 For \( \text{std}(H) \cap R \) use lemma 2.7.

SINGULAR example:

```plaintext
ring r=...;
ideal null;
ideal F=...;
preimage(r,F,null);
```
2.4.5 Radical membership

Lemma 2.17 Let \( I \subseteq R = \operatorname{LcK}[x_1, \ldots, x_n] \), \( I \) generated by \( F \). \( f \in \sqrt{I} \)
iff \( 1 \in \text{std}(F + (yf - 1)) \subseteq R[y] \).

2.4.6 Principal ideal

Lemma 2.18 \( I = (F) \) is principal (i.e. has a one-element ideal basis) iff \( \text{std}(F) \) has exactly one element.

2.4.7 Trivial ideal

Lemma 2.19 \( (F) \) is the whole ring \( R \) iff \( \text{std}(F) = \{1\} \).

2.4.8 Module intersection 1

Lemma 2.20 Let \( (F) \subseteq R \) and \( (G) \subseteq R \).
Then \( \text{std}((F) \cap (G)) = \text{std}(y(F) + (1 - y)(G)) \cap R \) in \( R[y] \).

Remark 2.21 For \( \text{std}(H) \cap R \) use lemma 2.7.

SINGULAR example:

```sage
ing ring r1 = 32003,(x,y,z),(c,ds);
poly s1=x2y3+45x6y3+68x4z5+80y6x8;
poly s2=6x5+3y6+8z6;
poly s3=12xyz3+2y3z6;
ideal i1=s1,s2,s3;
ideal i2=s1+s2,s2,s1;
intersect(i1,i2);
```
3 Solving equations

The simplest way to "solve" systems of polynomial equations via standard basis computation is the computation of a lexicographical standard basis.

Other Possibilities include the command \texttt{eliminate} or preprocessing etc.

\texttt{SINGULAR} example:

\begin{verbatim}
// consider a line and a plane:
ring R=0,(x,y,z),lp;
number a,b,c,d,e=0,1,1,1,1;
ideal L=a*x+b*y,z;
poly P=c*x+d*y+e*z;
ideal I=L,P;
// force the complete reduction of the standard basis:
option(redSB);
std(I);
eliminate(I,x);
\end{verbatim}

3.1 Simplification

\texttt{SINGULAR} example:

\begin{verbatim}
ring R=...;
ideal I=.....;
interred(I);
\end{verbatim}

3.2 Solvability

\textbf{Lemma 3.1} The set of polynomials $F$ is solvable iff \{1\} $\neq \text{std}(F)$. (See lemma 2.19.)

\texttt{SINGULAR} example:

\begin{verbatim}
// consider two parallel lines:
ring R=0,(x,y),dp;
poly l1=x+y-3;
poly l2=x+y-600;
ideal F=l1,l2;
std(F);
// consider a circle and a line
poly c=x^2+y^2-4;
F=c,l1;
std(F);
F=c,l2;
std(F);
// solvable means: solvable in the algebraic closure !
\end{verbatim}
3.3 Finite solvability

**Lemma 3.2** The set of polynomials $F \subseteq K[x_1, ..., x_n]$ has only finitely many solutions iff 
$\forall 1 \leq i \leq n : \exists f \in \text{std}(F) : L(f) \text{ is a power of } x_i$. (See remark 2.11.)

SINGULAR example:

```plaintext
// consider a line and a plane:
ring R=0,(x,y,z),dp;
number a,b,c,d,e=1,1,1,1,1;
ideal L=a*x+b*y,z;
poly P=c*x+d*y+e*z;
ideal I=L,P;
std(I); // the zero set is a line
a=0;
L=a*x+b*y,z;
I=L,P;
std(I); // the zero set is finite (a point)
```
4 Syzygies

4.1 Definition

Definition 4.1 Let $I = \{g_1, \ldots, g_q\} \subseteq K[x]^r$.

The module of syzygies $\text{syz}(I)$ is $\ker (K[x]^q \rightarrow K[x]^r, \sum w_i e_i \mapsto \sum w_i g_i)$.

Lemma 4.2 The module of syzygies of $I$ is

$$(g_1(x) - e_{r+1}, \ldots, g_q(y) - e_{r+q}) \cap \{0\}^r \times K[x]^q$$

in $(K[x_1, \ldots, x_m]/J)^q$.

Remark 4.3 Use a module ordering with $e_i > e_j \forall i \leq r < j$ and the elimination property of lemma 2.7.

SINGULAR example:

```sage
ring R=0,(x,y,z),(c,dp);
ideal I=maxideal(1);
// the syzygies of the (x,y,z)
syz(I);
// syz yields a generating set for the module of syzygies
// but may not be a standard basis!
```

4.2 Resolutions

Iterating the syz command yields a free resolution of a module or ideal. SINGULAR does this if the res or mres command is used.

Another algorithm due to Schreyer is presented in [S]. It will be used by the sres command.

For a comparison of these algorithms see [GG].

SINGULAR example:

```sage
ring r=0,(x,y,z),dp;
ideal I=x,y,z;
list Ir=res(I,0);
// print the results:
Ir;
list Im=mres(I,0);
// print the results:
Im;
list Is=sres(std(I),0);
// print the results:
Is;
```
4.3 Kernel of a module homomorphism

**Definition 4.4** Let \( R = K[x_1, \ldots, x_n]/(h_1, \ldots, h_p) \), \( A \in \text{Mat}(m \times r, R) \) and \( B \in \text{Mat}(m \times s, R) \) then define

\[
\text{modulo}(A, B) := \ker(R^r \xrightarrow{A} R^m / \text{Im}(B))
\]

(modulo\((A, B)\) is the preimage of \( B \) under the homomorphism given by \( A \).)

**Lemma 4.5** Let \( \{(\alpha_i, \beta_i, \gamma_i) \mid i = 1, \ldots, k\} \subset R^{r+s+p} =: R^N \) be a generating set of syz\((D)\) where

\[
C = \begin{pmatrix}
    h_1 & \cdots & h_p & 0 & \cdots & \cdots & \cdots \\
    0 & \cdots & 0 & h_1 & \cdots & h_p & 0 & \cdots \\
    \vdots & & \vdots & \vdots & & \vdots & \vdots & \\
    0 & \cdots & \cdots & \cdots & \cdots & h_1 & h_p
\end{pmatrix} \in \text{Mat}(m \times pm, R)
\]

and

\[
D = \begin{pmatrix}
    a_{11} & \cdots & a_{1r} & b_{11} & \cdots & b_{1s} & c_{11} & \cdots & c_{1,pm} \\
    \vdots & & \vdots & \vdots & & \vdots & \vdots & & \vdots \\
    a_{m1} & \cdots & a_{mr} & b_{m1} & \cdots & b_{ms} & c_{m1} & \cdots & c_{m,pm}
\end{pmatrix} \in \text{Mat}(m \times r + s + pm, R)
\]

Then

\[
\text{modulo} \ (A, B) := (\alpha_1 \cdots \alpha_k) \in \text{Mat}(r \times k, R)
\]

(see lemma 4.2.)

**Remark 4.6** In practice, one need not compute the entire syzygy module of \( D \): it is better to find modulo\((A, B)\) as:

\[
\begin{pmatrix}
    a_{11} & \cdots & a_{1r} & b_{11} & \cdots & b_{1s} & c_{11} & \cdots & c_{1,pm} \\
    \vdots & & \vdots & \vdots & & \vdots & \vdots & & \vdots \\
    a_{m1} & \cdots & a_{mr} & b_{m1} & \cdots & b_{ms} & c_{m1} & \cdots & c_{m,pm}
\end{pmatrix} \cap \begin{pmatrix}
    0 \\
    \vdots \\
    0
\end{pmatrix}
\]

(see sections 4.2, 2.7.)

4.4 Module intersection 2

Let \( R \) be an affine ring, and let \( I, J, K \subseteq R \) be ideals. One can compute generators for the intersection \( L = I \cap J \cap K \) in the following way: \( L \) is the kernel of the \( R \)-module homomorphism \( \phi : R \to R/I \oplus R/J \oplus R/K \) which sends \( 1 \) to \((1,1,1)\).

**Lemma 4.7**

\[
I \cap J \cap K = \text{modulo} \left( \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} I & 0 & 0 \\ 0 & J & 0 \\ 0 & 0 & K \end{pmatrix} \right).
\]

14
4.5 Ideal quotient

**Lemma 4.8** The quotient \( (I : J) \) of two ideals \( I = (a_1, \ldots, a_r) \) and \( J = (b_1, \ldots, b_s) \) in \( R \) is the kernel of the map

\[
R \rightarrow R/I \oplus \cdots \oplus R/I \\
1 \mapsto (b_1, \ldots, b_s)
\]

It can be computed as

\[
(I : J) = \text{modulo } ((b_1|\ldots|b_s)^T, (a_1|\ldots|a_r) \oplus \cdots \oplus (a_1|\ldots|a_r))
\]

**SINGULAR example** (see example in section 2.3.1):

```plaintext
ring R=...;
ideal I=...;
ideal J=...;
quotient(I,J)
```

4.6 Saturation

The saturation \( (I : J)\infty \) of \( I \) with respect \( J \) can be computed by computing \( (I : J), ((I : J) : J), \ldots \) until it stabilizes.

**SINGULAR example**:

```plaintext
ring R=...;
ideal I=...;
ideal J=...;
int ii;
I = std(I);
while ( ii<=size(II) )
{
    II=quotient(I,J);
    for ( ii=1; ii<=size(II); ii=ii++)
    {
        if (reduce(II[ii],I)!=0) break;
    }
    I=std(II);
}
// II is now (I:J)\infty.
```

4.7 Annihilator of a module

**Lemma 4.9** Let \( R = \text{Loc}_< K[x_1, \ldots, x_n]/(h_1, \ldots, h_p) \), \( M \subseteq R^n \).

\( \text{Ann}_R(R^n/M) := \{ g \in R | gR^n \subseteq M \} \) is generated by first entries of syzygies of the module

\[
\begin{pmatrix}
e_1 & M & 0 & \cdots & 0 \\
e_2 & 0 & M & \ddots & \vdots \\
\vdots & \vdots & \ddots & \ddots & \vdots \\
e_n & 0 & \cdots & 0 & M
\end{pmatrix}
\]
where \( e_i \) is the \( i \)-th unit vector in \( \mathbb{R}^m \).
(We identify a matrix with the module generated by it columns.)
5 Examples

5.1 Ext modules Ext(M,R)

Let $M$ be given as $R^n/Im(A_0)$, where $R = K[x_1,\ldots,x_n]/(h_1,\ldots,h_p)$. For each free resolution

$$0 \longrightarrow F_k \overset{A_{k-1}}\longrightarrow F_{k-1} \longrightarrow \cdots \longrightarrow F_1 \overset{A_0}{\longrightarrow} F_0 = R^n \longrightarrow M \longrightarrow 0$$

is $Ext^j_R(M,R) = H^j(Hom(F_{\bullet},R))$.

**Algorithm 5.1** $Ext^j_R(M,R)$:

- compute a free resolution of $M$ by $A_k = \text{syz}(A_{k-1})$ for $k = 1,\ldots,j$ (or use $\text{mres}$, see section 4.2).
- $Ext^j_R(M,R) = \text{Im}(\text{syz}(A^T_j))/\text{Im}(A^T_{j-1})$ is a free module modulo the image of the matrix $\text{mod}(\text{syz}(A^T_j), A^T_{j-1})$

**SINGULAR example:** a complete version can be found in the **SINGULAR** library **homog.lib**.

```
proc qmod (module M, module N)
  //USAGE:  qmod(<module_M>,<module_N>);
  // N a submodule of M, a submodule of a free one
  //COMPUTE: presentation S of M/N, i.e. M/N<<-F<<-[S],
  // F free of rank = size(M),
  //RETURNS: module(S)
  {
    return(lift(M,N)+syz(M));
  }

proc ext (int n, ideal i)
  // USAGE:  Ext^n(R/i,R);  i ideal in the basering R
  // SHOWS:  degree of Ext^n
  // RETURN:  Ext as quotient of a free module
  {
    //---------------- compute resolution of R/i ----------------
    // 0<<-R/i<<-L(0)<<-[i]--L(1)<<-[RE[2]]--- ...
    list RE=mres(i,n+1);
    //---------------- apply Hom(_,R) at n-th place ------
    module g = module(transpose(matrix(RE[n+1])));
    module f = module(transpose(matrix(RE[n])));
    //---------------- ker(g)/im(f) ----------------
    module ext = qmod(syz(g),f);
```

17
//---- return Ext as quotient of a free module (std) ----
  return(std(ext));
}
5.2 \( \text{Hom}_R(M, N) \)

Let \( M \) be given as \( R^n/\text{Im}(A_0) \), \( N \) as \( R^p/\text{Im}(B_0) \), where \( R = K[x_1, \ldots, x_n]/(h_1, \ldots, h_p) \) together with free resolutions

\[
\cdots \rightarrow F_k \xrightarrow{A_{k-1}} F_{k-1} \rightarrow \cdots F_1 \xrightarrow{A_0} F_0 = R^n \rightarrow M \rightarrow 0
\]

and

\[
\cdots \rightarrow G_k \xrightarrow{B_{k-1}} G_{k-1} \rightarrow \cdots G_1 \xrightarrow{B_0} G_0 = R^p \rightarrow N \rightarrow 0.
\]

We get the following commutative diagram with exact columns and rows:

\[
\begin{array}{cccc}
0 & & \downarrow & \\
& \downarrow & & \\
\text{Hom}_R(M, N) & & \downarrow & \\
& \downarrow & & \\
0 & \leftarrow F^*_0 \otimes N & \leftarrow F^*_0 \otimes G_0 & \leftarrow F^*_0 \otimes G_1 & \downarrow & \\
& \downarrow & & \\
0 & \leftarrow F^*_1 \otimes N & \leftarrow F^*_1 \otimes G_0 & \leftarrow F^*_1 \otimes G_1
\end{array}
\]

Algorithm 5.2

\( \text{Hom}_R(M, N) = \text{Im}(\text{modulo } (A^T_0 \otimes \text{id}_{G_0}, \text{id}_{F^*_1} \otimes B_0)) / \text{Im}(\text{id}_{F^*_0} \otimes B_0) \)

is a free module modulo the image of the matrix

\( \text{modulo}(\text{modulo } (A^T_0 \otimes \text{id}_{G_0}, \text{id}_{F^*_1} \otimes B_0), \text{id}_{F^*_0} \otimes B_0) \)
5.3 $T^1_X$ and $T^1_X(M)$

This section and the corresponding SINGULAR procedure is a joint work of G.M. Greuel and B.Martin.

Let $X \in K^n$ be given by the ideal $I = (f_1, \ldots, f_k) \subseteq P = K[x_1, \ldots, x_n]$ and $R = P/I$.

Consider the canonical exact sequence

$$I/I^2 \xrightarrow{d} \Omega^1_P \otimes_P R \longrightarrow \Omega^1_R \longrightarrow 0$$

(1)

where $\Omega^1_P$ denotes the module of Kähler differentials and $d$ is induced by the exterior derivation. ([d] → [df]).

$\Omega^1_P$ is free with generators $dx_1, \ldots, dx_n$ (isomorphic to $P^n$) and $\Omega^1_R$ (isomorphic to $R^n$) is by definition the cokernel of the map

$$d : [f_i] \mapsto [df_i] = \left[ \sum_j (df_i/\partial x_j) \right]$$

Let $M$ be any finitely generated $R$-module. The $M$-dual of (1) is

$$0 \rightarrow \Theta_X(M) \rightarrow \text{Hom}_R(\Omega^1_P \otimes_R M) \xrightarrow{d^*} \text{Hom}_R(I/I^2, M) \rightarrow T^1_X(M) \rightarrow 0$$

where $\Theta_X(M) = \text{Hom}_R(\Omega^1_R, M)$ is the module of the $M$-valued $R$-derivations and $T^1_X(M)$ is by definition the cokernel of $d^*$ (the dual of $d$) and is called the module of first order infinitesimal deformations of $X$ (resp. $R$) with values in $M$.

The module $T^1_{X/K^n}(M) := \text{Hom}_R(I/I^2, M)$ is called the module of first order embedded deformations of $R$ with values in $M$. If $M$ is omitted, we define $T^1_X := T^1_X(R)$ as the module of first order deformations of $X$.

Remark: $\text{Hom}_R(\Omega^1_R, R) \cong \text{Hom}_P(R^n, R) \cong R^n$.

**Algorithm 5.3** Consider a presentation of $I$ as a $P$-module:

$$0 \leftarrow I \leftarrow P^k \leftarrow P^n$$

(2)

We note that for any $R$-module $M$

$$\text{Hom}_P(I/I^2, M) = \text{Hom}_R(I, M)$$

(3)

Hence, choosing $dx_1, \ldots, dx_n$ as a basis of $\Omega^1_P$ and the canonical basis of $P^k$, the right part of (3) is identified with the exact sequence

$$\text{Hom}_P(P^n, R) \xrightarrow{\text{jac}} \text{Hom}_P(I, M) \rightarrow T^1_X(M) \rightarrow 0$$

(4)

where $\text{jac} : \text{Hom}_P(P^n, M) \rightarrow \text{Hom}_P(I, M) \subseteq \text{Hom}_P(P^k, M) = M^k$ is given by the Jacobian matrix $(df_i/\partial x_j)_{i,j}$ of $I$. In particular, for $M = R$, we get

$$\text{Hom}_P(P^n, R) \xrightarrow{\text{jac}} \text{Hom}_P(I, R) \rightarrow T^1_X(M) \rightarrow 0$$

(5)
as defining sequence of $T_X^1$.

Applying $\text{Hom}_P(-, R)$ to (2), we get

$$0 \rightarrow \text{Hom}_P(I, R) = \text{ker}(A^t) \rightarrow \text{Hom}_P(P_k, R) \xrightarrow{A^t} \text{Hom}_P(P^p, R)$$  \hspace{1cm} (6)

where $A^t$ is the transposed matrix of $A$. Consider a 3-term partial resolution of $\text{im}(A^t)$:

$$R^l \xrightarrow{B_3} R^r \xrightarrow{B_2} \text{Hom}_P(P_k, R) \xrightarrow{B_1} \text{Hom}_P(P^p, R)$$  \hspace{1cm} (7)

together with the $J : \text{Hom}_P(P^p, R) \rightarrow \text{Hom}_P(P^p, R)$ (induced by the Jacobian $\text{jac}$) and a lifting of $J$ to a map $L : \text{Hom}(P^n, R) \rightarrow R^r$. This lifting exists since $\text{im}(\text{jac})$ is contained in the normal bundle of $I$:

$$\text{im}(J) \subseteq \text{Hom}_R(I/I^2, R) = \text{ker}(B_1) = \text{im}(B_2)$$  \hspace{1cm} (8)

Finally we get (keeping notations for $B_3$ and $L$ when lifted to $P$)

$$T_X^1 = \text{im}(B_2)/\text{im}(J) = R^r/\text{im}(L) + \text{im}(B_3) = P^p/\text{im}(L) + \text{im}(B_3) + l*P^r$$  \hspace{1cm} (9)

**SINGULAR** example: a complete version can be found in the **SINGULAR** library **sing.lib**.

ideal I=f1,...,fk;
list A=res(I,2);  //compute the presentation (4) of I
module A'=transpose(A[2]);  //A'=transposed 1st syzygy module of I
module jac=jacob(I);  //jacobian matrix of I (as module)

// So far we are in the polynomial ring P, now we pass to the ring R=P/I:

qring R=std(I);  //defines the quotient ring R=P/I
module A'=fetch(P,A');  //map A' to R
module J=fetch(P,jac);  //map jac to R
list B=res(A',3);  //compute the exact sequence (7)
module t1=lift(B[2],jac)+B[3];  //im(L)+im(B3)
int r=rank(t1);  //compute the rank r
// Hence T1_X = R^r/t1 as R-module. (see (9))

// Now we pass back to the original basering P:
setting P;  //makes P the basering
module t1 = fetch(R,t1)+J*freemodule(r);  //im(L)+im(B3)+J*P^r:=T1
fetch(R,B(2));  // (generators of) normal bundle
fetch(R,B(3));  // presentation of normal bundle
References


Contents

1 Basic definitions .................................................. 2
  1.1 Monomial orderings ........................................... 2
  1.2 Examples for monomial orderings ........................... 2

2 Standard bases .................................................. 5
  2.1 Definition .................................................... 5
  2.2 Standard bases for submodules of free modules ......... 5
  2.3 Basic properties .............................................. 7
    2.3.1 Ideal membership ....................................... 7
    2.3.2 Elimination ............................................. 7
    2.3.3 Hilbert series ........................................... 8
  2.4 Applications ................................................ 8
    2.4.1 Submodule ............................................... 8
    2.4.2 Euclidian algorithm .................................... 9
    2.4.3 Gaussian algorithm .................................... 9
    2.4.4 Kernel of a ring homomorphism ....................... 9
    2.4.5 Radical membership ................................... 10
    2.4.6 Principal ideal ......................................... 10
    2.4.7 Trivial ideal ............................................ 10
    2.4.8 Module intersection 1 .................................. 10

3 Solving equations .............................................. 11
  3.1 Simplification ............................................... 11
  3.2 Solvability .................................................. 11
  3.3 Finite solvability .......................................... 12

4 Syzygies .......................................................... 13
  4.1 Definition .................................................... 13
  4.2 Resolutions .................................................. 13
  4.3 Kernel of a module homomorphism ......................... 14
  4.4 Module intersection 2 ....................................... 14
  4.5 Ideal quotient ............................................... 15
  4.6 Saturation ................................................... 15
  4.7 Annihilator of a module ..................................... 15

5 Examples ....................................................... 17
  5.1 Ext modules $\text{Ext}(M, R)$ ................................. 17
  5.2 $\text{Hom}_R(M, N)$ .......................................... 19
  5.3 $T^1_X$ and $T^1_X(M)$ ...................................... 20

References .................................................................. 22