UNIVERSITÄT KAISERSLAUTERN

GRÖBNER BASES IN ALGEBRAS WITH ZERODIVISORS

Thomas Nüßler and Hans Schönemann

Preprint Nr. 244

ISSN 0943–8874

FACHBEREICH MATHEMATIK

GRÖBNER BASES IN ALGEBRAS WITH ZERODIVORS

Thomas Nüßler and Hans Schönemann

Preprint Nr. 244

ISSN 0943–8874

UNIVERSITÄT KAISERSLAUTERN
Fachbereich Mathematik
Erwin–Schrödinger–Straße
6750 Kaiserslautern

Gröbner Bases in Algebras with Zerodivisors

Thomas Nüßler * Hans Schönemann *

June 1993

Contents

*Partially supported by the 'Deutsche Forschungsgemeinschaft' (DFG) and the European Community (Esprit BRA 6846, POSSO)

1 Preface

In 1965 Bruno Buchberger presented his Gröbner basis algorithm for polynomial algebras. Later several people, as for instance Mora ([M85]), Weispfenning ([K-W90], [W92]) have extended this algorithm to other structures. In this paper, we will contribute to the case when the monoid algebra or only the monoid action on the algebra or module itself has zerodivisors. Via the map from a suitable polynomial algebra $k[x_1, .., x_n]$ which maps the x_i to the generators of the monoid and 1 to it's neutral element we have the notion of monomials, polynomials and degree in our monoid algebra $\mathcal{R}$. Given an ordering on the monoid we can define the leading monomial $lm(t)$ for any $t \in \mathcal{R}$. But because of the zerodivisors in $\mathcal{R}$ the equation :

$$lm(m \circ t) = m \circ lm(t)$$

is no longer valid for some monomial $m \in \mathcal{R}$. Thus there cannot exist an admissible (that is compatible with the monoid structure) wellordering on M. An admissible order is in the zerodivisor free case used to describe reducibility ($f \xrightarrow{t} r \iff f = g \circ t + r, lm(f) > lm(r)$) by the order on leading terms. This paper deals with a refined description of reducibility to tackle with this problem in the zerodivisor case.

In chapter 2 we shall delineate the general notation and an introduction to the problem of constructing a complete basis for a normalform problem.

Chapter 3 is devoted to the orderings on monoids and algebras and modules with an monoid action. Here we shall see that orderings are generally no longer admissible to a monoid action.

In chapter 4 we shall define the above announced refinement and are dealing with the zerodivisor case from there on. It is no longer possible to describe reducibility of one object with another only in terms of leading monomials. From there on it is necessary to study the rest of the object. This will be done by 'augmentation' introduced in chapter 3. The augmentation more or less enlarges a generating set by the leading terms hidden in the tail of the polynomials. In this chapter we will introduce the pertinent definition and prove that it is a generalization of Groebnerbasis which is by definition a complete system of reduction rules. A special case of this where the augmentation is defined directly by multiplication of the monoid will be treated in chapter 5.

Chapter 6 is devoted to the description of the augementation algorithm. It involves the augmentation $Aug(T)$ constructed to each generating set T and the proof of the termination in the case of finitely generated annihilator ideals and the finite generating set of the ideal. Certainly the algorithm terminates in noetherian algebras. This is a condition usually fulfilled in algebraic geometry.

Syzygies have important applications in algebraic geometry. In chapter 7 we will introduce an algorithm to compute Gröbner bases of modules over such k-algebras and apply it to compute syzygies.

apply it to compute syzygies.

A first implementation of this algorithm was made in the winter of 1991/92. It was used for calculations in the exterior algebra and the tensor product of an exterior and a polynomial algebra. This task came from algebraic geometry to compute monads of vectorbundles and their deformations.

This is to a certain extent a generalization of Gröbner bases in algebras of solvable type (i.e. for generators x, y the commutator is given by the rule: $yx = cxy+$ terms of lower degree, with c an element in the field k and the product of any two monomials cannot be zero), which was studied by Kredel ([K]). In the case of the exterior algebra Kredel defines the "saturated left reduction" which is equivalent to our reduction with the augmented polynomial set. (He gives a different algorithm for the "saturated set of polynomials" but it leads in this case to the same set Aug(F)).

Analogous results to ours were obtained by Madlener and Reinert in a more general setting not using a grading on the algebra ([MR93]). They reduce an element in one reduction step to its normal form and define the "saturating set" to be any set having the property that each element of the algebra can be reduced by this set in one step to its normal form. The construction of the saturated set leads to large sets which diminesh later. Their algorithm , though more general, seams however to be too complex, at least for the applications to be explained in chapter 8. Even our algorithm which takes only necessary elements into the reducing set has to handle about 30000 polynomials in order to get the desired answer for realistic applications.

Exploiting the fact, that exterior algebras are finite dimensional vector spaces, Stokes also ([S]) developed Gröbner bases for this class of algebras.

2 Noetherian Reduction Structures

For convenience let us recall the general settings of reduction structure in which the case of Gröbneri bases of algebras are included. Let us first recall the notion of wellordering and quasiordering.

Definition 2.1 (ordering and quasiordering) *1. A quasiordering is an irreflexive and transitive binary relation.*

2. If a quasiordering compares any two elements we call it an ordering.

General notation:

- Let $(R, <)$ be a quasiordered set. Later this will be our algebra or module with the quasiordering induced by the ordering on the monoid of generators in degree 1.
- Let $(M, \circ, id)$ be a monoid with distinct neutral element.

Definition 2.2 (Monoid action) *We call a map*

$$\begin{aligned} \phi: \quad & M \times R \to R \\ & (\alpha, u) \mapsto \alpha(u) \end{aligned}$$

a monoid action if it respects the following conditions
1.) $\alpha(\beta(u)) = \alpha \circ \beta(u) \quad \forall \alpha, \beta \in M \text{ and } u \in R$
2.) $id(u) = u \qquad\qquad \forall\, u \in R$
In sequel this action will be simply denoted by $\circ$.

Definition 2.3 *An ordering $>_m$ on a monoid M is called an admissible ordering with respect to M, if and only if it is compatible with the monoid action:*

$$m_1 <_m m_2 \implies m \circ m_1 <_m m \circ m_2 \text{ for all } m, m_1, m_2 \in (M, \circ, <_m)$$

A quasiordering on R is called admissible with respect to M, if and only if it is compatible with the monoid action:

$$r_1 < r_2 \implies m \circ r_1 < m \circ r_2 \quad \text{for all } m \in (M, \circ, <_m) \text{ and } r_1, r_2 \in (R, <)$$

An ordering is called a wellordering if there is a minimal element in M with respect to $<_m$.

Remark 2.4 There are admissible wellorderings in the case of zerodivisor free monoids and rings (e.g. ring of polynomials). But in this paper we want to treat the case of algebras which contain zero divisors. Therefore these conditions will be violated in general, as for instance in the case of the exterior algebra $\bigwedge^\bullet V$ on a vector space V. Nevertheless it is useful to describe the reduction rules in the sequel, and we have to take into account that the ordering is not longer admissible.

Let us now define a reduction structure for sets with a monoid structure and a distinguished element 0 (the neutral element for the addition) in $(R, <, 0)$. We need two preparatory definitions first. Let therefore $\mathcal{K}$ denote a set of congruence relations in $R \times R$, containing the trivial congruences $R \times R$ and the diagonal.

Definition 2.5 (Normal form property) *1. A quasiordered set $(R, <)$ has the normal form property relative to a congruence relation $\sim \in \mathcal{K}$ if and only if there exists a unique minimal element in each congruence class. We call such an element in the congruence class of $u \in R$ $NF(u, \mathcal{K})$ or $NF(u)$ if $\mathcal{K}$ is fixed.*

2. A triple $(R, <, \mathcal{K})$ has the normal form property if and only if $(R, <)$ has the normal form property relative to each congruence in $\mathcal{K}$.

Notation 2.6 1. $S := \{u \in R | u > 0\}$

2. $I(\sim) := \{u \in R |\ u > 0 \text{ and } u \sim 0\}$, denote the ideal representing $\sim$

Remark: Obviously for rings the congruences are in bijectivity to the ideals (as defined above). These ideals become ideals in the sense of rings if further assumptions are satisfied.

Definition 2.7 (Rewriting rule) *A rewriting rule is a coordination of a relation $\xrightarrow{t} \subset R \times R$ for every $t \in S$ according to the subsequent rules.*

$\mathcal{F}1$ $u \xrightarrow{t} v \Longrightarrow u > v$

$\mathcal{F}2$ $(t, 0) \in \xrightarrow{t}$ *and* $\xrightarrow{t} \subset \tilde{t}$
with $\tilde{t}$ the smallest relation containing t

$\mathcal{F}3$ *Let $T \subset S$. We define $u \xrightarrow{T} v$ if and only if there exists a $t \in T$ with $u \xrightarrow{t} v$*

Definition 2.8 $\mathcal{F}$ describes the set of all rewriting rules

$$\mathcal{F} := \{\xrightarrow{T} | T \subset S\}.$$

In our situation we define the rewriting rule as follows:

Definition 2.9 *Let $(R, <, 0)$ be a quasiordered set with a neutral element 0 and $(M, <_m)$ a monoid acting on $(R, <, 0)$. We define now a rewriting rule with respect to the monoid action by:*

$$u \xrightarrow{t} v \iff \exists\, \alpha \in (M, <_m) \text{ with } u = \alpha(t), v = \alpha(0), \text{ for } u > v \text{ and } t \in S$$

We see the advantage of the monoid action generating all the reduction rules from a smaller set of 'generators'. Thus we keep this action even if it has the drawback that it does not allow an admissible wellordering.

Remark 2.10 Obviously a reduction rule $u \xrightarrow{t} v$ defined in this way satisfies $\mathcal{F}_1 \cdots \mathcal{F}_2$

Let's define now the notation of a reduction system.

Definition 2.11 (Reduction System) *We call a quadruple $(R, <, \mathcal{F}, \mathcal{K})$ according to the rules below a reduction system:*

- $\mathcal{Q}_1$ *$(R, >)$ is a quasiordered set*
- $\mathcal{K}1$ *$\mathcal{K}$ is a set of equivalence relations on R containing $R \times R$ and the diagonal $D := \{(u, v) \in R \times R | u = v\}$ and $\mathcal{K}$ is closed by taking intersections.*
- $\mathcal{K}2$ *$(R, >, \mathcal{K})$ respects the normal form property*
- $\mathcal{K}3$ *$\sim = \tilde{u}$ for $I(u) = I(\sim)$ (alway fulfilled for ideals)*
- $\mathcal{F}$ *$\mathcal{F}$ is the set of all rewriting rules*
  In addition $\mathcal{F}$ suffices:
- $\mathcal{F}4$ *Let $T \subset S$. Then it exists for every $u \in R$ a T-irreducible element v such that $u \sim v$ and one of the two relations $u > v$ or $u = v$ are true.*

A reduction system is called noetherian , if and only if each congruence $\sim \in \mathcal{F}$ has a finite basis.

A very important question concerning a reduction system is : Can it reduce every element $u \in (R, <)$ to its normal form NF(u)?
This leads to the notion of completeness and hence the definition of a Gröbner basis.

Notation 2.12 *We denote by $Irred(T)$ all elements in $(R, <)$ irreducible by a set $T \subset S$ and $NF(T)$ all normalforms in $(R, <)i$ with respect to T.*

Definition 2.13 *A reduction system $(R, <, \mathcal{F}, \mathcal{K})$ is complete if and only if it satisfies the two equivalent conditions below for every subset $T \subset S$.*

1. $NF(T) = Irred(T)$
2. $u \xrightarrow{T} NF(u, T)$

We call a complete reduction system a Gröbner basis.

The purpose of the rest of this paper is to develop criteria for the existence of a complete reduction system (Gröbnerbasis) and an algorithm for the completion of a basis, where R is a noetherian algebra or a module over it and the ordering is no longer a admissible ordering.

3 Quasi-ordering in a Noetherian Ring

For the rest of this paper R will be a module over a noetherian algebra with a 1_R-element and a monoid action on R. In the case of the polynomial algebra the grading is given by the ideal of the zeropoint. Hence the monoid is generated as a monoid by the degree-1-part of this grading.
Certainly $(R, <)$ must accord to the descending chain condition. This means that each chain $r_1 > r_2 > \ldots$ becomes stationary. Such an ordering is called a noetherian ordering.

Let now $(M, <_m)$ be a monoid given with an ordering $<_m$. This order is generaly no longer an admissible ordering compatible with the monoid structure, because the monoid can contain zerodivisors,
e.g.: Let $R = \wedge^\bullet V$ and M be the monoid multiplicatively generated by the k-vectorspace $V := \langle x_1, ..., x_n \rangle_k$. Choose an ordering $x_1 <_m ... <_m x_n$ and let $<$ be any lexicographical extension of $<_m$. Then $x_1 < x_2$ but $0 = x_1x_1 < x_1x_2 < x_2x_2 = 0 \Longrightarrow 0 < 0$. This example alludes the fact below.
In the sequel we will describe an element $m \in M$ via the generators $m_1 \ldots m_n$ of M :

$$m^v := m_1^{v_1} \ldots m_n^{v_n} \text{ where } v \in N^n$$

Thus an element of R is of the form $\sum_i c_i m^{v_i}$, for $v_i \in N^u$.

Proposition 3.1 *If a monoid ring (algebra) contains zerodivisors, then there cannot exist a M admissible wellordering.*

But still we can extend an ordering to a quasiordering in R;

Definition 3.2 ((lm)) *Let $v \in S$ be with a monoid structure $(M, <_m)$ then we will denote by $lm(v)$ the highest monomial in v with respect to the ordering $<_m$ and refer to it as a leading monomial.*

After this preparation we are now ready to define with the help of $<_m$ the quasiorder $<$ on R.

Definition 3.3 ((Quasiorder)) *Let R and $(M, <_m)$ be as above and take two elements $u, v \in R$. We define now $<$ recursively by*

$$u > v \iff lm(u) > lm(v)$$
$$u \simeq v \iff lm(u) = lm(v)$$

$$u > 0 \; \forall \; u \in R \backslash \{0\}$$

Remark: We have $u > 0 \; \forall \; u \in R \backslash \{0\}$ if $0 \in M$.

4 The Augmentation of a Generating Set of an Ideal

In the description of reducibility for (alternating) forms we have encountered an example where it is no longer sufficient to describe reduction rules by the "divisibility" of leading terms of one element , because the fundamental equation

$$lm(m \circ t) = m \circ lm(t) \; \forall \; m, t \in (R, >) \quad (**)$$

is violated. Thus "new" leading terms in $m \circ t$ are possible, which are not multiples of $lm(t)$.
This fact justifies the definition of the augmentation of a generating set.

Definition 4.1 (red(t)) *$u \in R$ is reducible by t: $u \in red(t) \Longrightarrow \exists v, m$ with $u = m \circ t + v$ and $u > v$*

Definition 4.2 ((Aug(T))) *Let $(R, <)$ be a ordered ring which possibly contains zero divisors. T is a generating set of an ideal I.*
An augmentation $Aug(T)$ of T is defined to be minimal among the sets S containing T satifying:

$$\forall \; t \in T, \; u \in red(t) \quad \exists t' \in S \text{ with } lm(t') | lm(u) \qquad (1)$$

Remark 4.3 1. In the case where the generating set consists of one element ($T = \{t\}$), T is obviously a Gröbner basis if the equation (**) is satisfied. If (**) is violated, this is no longer true, but still we have that $Aug(T) = Aug\{t\}$ is a Gröbner basis, as we will see from the next theorem.

2. $Aug(T)$ is the union of all $Aug(t)$ $\forall t \in T$:

$$Aug(T) = \bigcup_{t \in T} Aug(t)$$

3. The general inclusion sequence looks like:

$$T \subset Aug(T) \subset GB(I) \subset I \text{ if } I \text{ is generated by } T. \qquad (2)$$

with GB(I) being a Gröbner base of I.

With the concept of augmentation the description of reducibility simplifies to

Proposition 4.4 *For all $u \in (R, <)$ and for all $t \in T$ is equivalent:*

1. $u \in red(T)$

2. *It exists a* $t' \in Aug(T)$ *with* $lm(t')|lm(u)$

Proof:
$1 \Longrightarrow 2)$
$u \in red(t) \Longrightarrow \exists v$ with $u = m \circ t + v$ and $u > v \Longrightarrow lm(v) = lm(m \circ t)$
$2 \Longrightarrow 1)$
$>$ is an ordering. Each polynomial has only one leading monomial. Thus

$$u > v - lm(u) = u - m \circ lm(t') > v - m \circ t' = v \; e.g. \; u \xrightarrow{T} v$$

#

Remark 4.5 In practice, this concept reduces a more elaborate reduction mechanism to a simpler one, but with an enlarged set of rules, the set $Aug(T)$.

Analogously to the description of reducibility the construction of S-polynomials changes.

Definition 4.6 (S-polynomial) *Let* S *be the map below*

$$\begin{array}{rccc} S & : & (R,<) & \rightarrow & \mathcal{P}(R,<) \\ & & (f,g) & \mapsto & S(f,y) \end{array}$$

defined as follows:
For all $t \in Aug(f), t' \in Aug(g)$ *choose the minimal* $m_{(t,t')}, m'_{(t,t')} \in M$ *such that* $lm(m_{(t,t')}t) = lm(m'_{(t,t')}t')$. *Now we can define* S *by*

$$S(f,g)' = \{m_{(t,t')}t - m'_{(t,t')}t'\}_{t \in Aug(f), t' \in Aug(g)}$$

Now we can describe the Gröbner base of an ideal in terms of the augmented generating set.

Theorem 4.7 *Let* $(R,<)$ *be a noetherian ring with a quasiordering* $<$ *fulfilling the descending chain condition,* I *an ideal in* $(R,<)$, T *a generating set of* I *and* $Aug(T)$ *its augmentation. Then the three statements below are equivalent.*

1. T *is a complete system of reduction rules.* $(NF(u,T) = 0 \; \forall u \in I)$

2. $NF(S(t_i,t_j),T) = \{0\}$ *for all* $t_i, t_j \in Aug(T)$

3. *The ideal* $\{lm(f)|\forall f \in I\}$ *is generated by* $\{lm(f)|\forall f \in Aug(t)\}$

Proof:

$1 \Longrightarrow 2$ This is obvious by definition, because $S(t_i, t_j) \subseteq I$.

$1 \Longrightarrow 3$ This is clear from the description of reducibility 4.4

$3 \Longrightarrow 1$ This is clear from the description of reducibility 4.4

$2 \Longrightarrow 1$ Only this step needs some consideration. We can show that this condition 2) is sufficient for reducing an $u \in I$ to zero. Let $\{f_i\} = T$ the generating set of I, therefore $u = \sum_{f_i \in T} r_i f_i$ with appropriate $r_i \in (R, <)$. Remember the monoid structure $(M, <_m)$ is given by a set of generators of $(R, <)$ in degree 1 with an ordering which induces a quasiordering $<$ on R. Thus we can compare highest monomials. Let $Max := \{i | lm(r_i f_i)$ be maximal with respect to $<\}$
We must distinguish two cases:

1. $\#\{Max\} = 1$
   We have only one maximal monomial $r_i f_i$. Thus

   $$u - r_i f_i < u \quad r_i f_i \in I$$

   e.g. $u \in red(T)$. Now apply this again.
2. $\#\{Max\} > 1$
   This gives a decomposition of u as :

   $$u = \sum_{i \in Max} r_i f_i + \tilde{u} \text{ with } lm(\tilde{u}) < lm(u) \tag{3}$$

   $$u = \sum_{i \in Max} r_i f_i + r_2 f_2 - r_1 f_1 + r_3 f_3 - r_1 f_1 + \ldots + \tilde{u} \tag{4}$$

   $$= (\#Max) lm(r_1 f_1) + s_2 + s_3 + \ldots + \tilde{u} \tag{5}$$

Thus every s_i is in a S-polynomial (or a multiple of an element in a S-polynomial) and therefore reduces to zero, so only $lm(r_i f_i)$ is left. But this case in solved in 1). Hence we are done.

#

Remark 4.8 We do not benefit from the fact that we inspect in characterization 2) only elements from T and not from $Aug(T)$, because for a Gröbner basis T the equation

$$T = Aug(T)$$

is valid.

Remark 4.9 Now we have all tools to use a sligthly modified Buchberger algorithm to compute a Gröbner base.

For practical reasons we will use the commutative S-polynomial s(f,g) and do the augmentation with Aug(T). Let F be a set of polynomials, the algorithm to compute a Gröbner base S of F is as follows:

```
S:=Aug(F);
B:={{f,g}|f,g ∈ S, f ≠ g};
WHILE B≠ ∅ DO
      CHOOSE {f,g} ∈B, {f,g} "optimal";
      B:=B\{f,g};
      h := s(f,g);
      h :=NF(h,S);
      IF h ≠ 0 THEN
          B:=B∪{{f,g},f ∈S,g ∈Aug(h)}∪{{f,g},f,g ∈Aug(h)};
          S:= Aug(h)∪S
      END
END
```

5 Description of Reducibility in Terms of "Exponents"

We have implemented the augmentation in the special case where the ideal of zero divisors is generated by monomials. The augmentation in this case can be described by multiplying leading terms with monomials which kill them. Now we will describe this situation in this chapter explicitly. In the wellknown polynomial case the equation

$$lm(m \circ v) \;=\; m \circ lm(v) \quad \forall\, m, v \in K[X]$$

is valid, and no terms can vanish by multiplications. But in our case leading terms can vanish by monomial multiplications. (Monoid action). Thus a refined description of reducibility is necessary.

Proposition 5.1 *$\forall u \in (R,<)$ and $\forall\, t \in I$ is equivalent:*

$$i)\;\; u \in red(t) \tag{6}$$
$$ii)\;\; \exists\, m \in M \quad with\ lm(u) = lm(m \circ t) \tag{7}$$

Proof: This is a special case of proposition 3.2.
$i \Longrightarrow ii)$
$u \in red(t) \Longrightarrow \exists v$ with $u = m \circ t + v$ and $u > v \Longrightarrow lm(v) = lm(m \circ t)$
$ii \Longrightarrow i)$
$>$ is an ordering. Therefore only one leading monomial exists. Thus

$$u > v - lm(u) = u - lm(m \circ t) > v - mt = v$$

#

Remark: In the nice polynomial case the second condition is equivalent to

$$ii')\ lm(t) | lm(u)$$

because of the equality $lm(m \circ t) = m \circ lm(t)\ \forall\ m \in (M,<), t \in (R,<)$. This makes computations considerably easier because reducibility is defined by the leading monomials of t. There is no need to inspect the whole polynomial t.

Generalizing the notation of an S-polynomial from the zerodivisorfree case we receive:

Definition 5.2 (S-polynomial) *Let S be the map below*

$$\begin{array}{rccc} S & : & (R,<) \times (R,<) & \to & \mathcal{P}(R,<) \\ & & (f,g) & \mapsto & S(f,g) \end{array}$$

defined as follows:
For all $t \in Aug(f), t' \in Aug(g)$ *choose the minimal* $m_{(t,t')}, m'_{(t,t')} \in M$ *such that* $lm(m_{(t,t')}t) = lm(m'_{(t,t')}t')$. *Now we can define* S *by*

$$S(f,g)' = \{m_{(t,t')}t - m'_{(t,t')}t'\}_{t \in Aug(f), t' \in Aug(g)}$$

Hence $lm(S(f,g)) < lm(mf) = lm(m'g)$
For example in the case of polynomials a special case of this "algorithm" is used.
Let $f = lc(f)x^{\mu'} + ...$ and $g = lc(g)x^{\mu''} + ...$
$\nu = max(\mu', \mu''), \nu' = \nu - \mu', \nu'' = \nu - \mu''$
In this situation $S(f,y)$ can be defined by :

$$S(f,y) = lc(f)x^{\nu'}g - lc(g)x^{\nu''}f$$

Here the leading term is denoted by lc. Now we can generalize the wellknown characterization of Groebner bases by leading terms.

Theorem 5.3 *Let* I *be an ideal of* $(R, <)$, T *a generating set of* I, *then all three conditions below are equivalent.*

1. T *is a Gröbner basis. (A complete system of reduction rules)*
2. $NF(S(t_i, t_j), T) = \{0\}\ \forall\ t_i, t_j \in T$.
3. *The Ideal* $\{lm(I)\}$ *is generated by* $\{lm(m \circ t_i) | \forall\ t_i \in T$ *and* $m \in M\}$

6 The Augmentation-Algorithm

In this chapter we will propose an algorithm computing the augmentation in the case where R is a module over a noetherian algebra with a 1_R-element and a monoid action on it. To describe the algorithm properly we must describe what causes the defect. Those elements of $(M, <_m)$ do not act freely on $(R, <)$. This will be our definition of $Ann(t)$.

Definition 6.1 *Let $t \in (R, <)$ then we will define $Ann(t)$ by:*

$$Ann(t) := \{m \in (M, <_m) | lm(m \circ t) < m \circ lm(t)\}$$

$$Ann(T) := \{m \in (M, <_m) | \exists t \in T \text{ with } lm(m \circ t) < m \circ lm(t)\}$$

Remark 6.2 1. $Ann(T)$ and $Ann(t)$ are ideals.

2. $Ann(T) = \bigcup_{t \in T} Ann(t)$

With this prepration we can now define the algorithm, which reflects:

$$Aug(T) := \bigcup_{t \in T} Aug(\{t\}) \tag{8}$$

$$Aug(\{t\}) := \{t\} \cup \bigcup_{a \in A} Aug(\{a \circ t\}) \setminus \{0\} \tag{9}$$

A is a generating set of $Ann(\{t\})$ which is finite because $Ann(\{t\})$ is a ideal in an noetherian algebra.

Definition 6.3 (length) *Let $u \in (R, <)$. By $length(u)$ we denote the number of generators (summands) of $u = \sum_{i=1}^{length(u)} r_i f_i$*

Definition 6.4 (trivial multiple) *Let $f, g \in (R, <)$ with $length(f) = length(g) = k$ and $f = \sum_{i=1}^{k} b_i f_i$, $g = \sum_{i=1}^{k} c_i g_i$, $f_i \in M, g_i \in M, b_i \in K, c_i \in K$. We call f a trivial multiple of g iff there exists $m \in M$ and $k \in K$ with $b_i = k c_i$ and $f_i = m \circ g_i$ for all i.*

Now we present an algorithm which computes the augmentation $Aug(T)$

$Aug(T) := \emptyset$;
WHILE $T \neq \emptyset$
    $A := Ann(T)$;
    take $t \in T$;
    $Aug(T) := Aug(T) \cup \{t\}$;
    $T := T \setminus \{t\}$;
    WHILE $A \neq \emptyset$
        choose $a \in A$;
        $A := A \setminus a$;
        IF $lm(a \circ t) \neq a \circ lm(t)$ THEN
            IF $\forall f \in Aug(T) : a \circ t$ is not a trivial multiple of f THEN
                $Aug(T) := Aug(T) \cup \{a \circ t\}$
            END
        END
    END
END

Proposition 6.5 *This algorithm is terminating and calculating an augmentation in the case of noetherian orderings which include*

1. *graded orderings*
2. *lexicographical orderings*
3. *any orderings for finite algebras (e.g. the exterior algebra)*

Proof: T is finite because we are working in and over a noetherian algebra.
By definition of $Ann(\{t\})$ it is true that $lm(m \circ t) < m \circ lm(t)$ for all $m \in (M, <_m)$.
Thus it is sufficient to proof that

$$\#\{m \in (M, <_m) | 1 < m < m' \; \forall \; m' \in (M, <_m)\} < \infty$$

1. This is clearly fulfilled for graded orderings.
2. For lexicographical orderings this is also true, if we allow only elements of finite length.
3. Obviously only a finite number of monomials can exist.

#

The case $\bigwedge^\bullet V$, where $V := \langle v_1 \cdots v_n \rangle$ is a n-dimensional vectorspace is very easy because we have only the simple relation $x^2 = 0$ in the monoid. Now let us describe now $Ann(t)$ in this case.

Lemma 6.6 *Let I be a multiindex in N^n with $lm(t) = v^I$.*
Then $Ann(t) = \{v_i, i \in I\}$.

7 Modules and Syzygies

An ordering $(M, <_m)$ or a quasi-ordering $(R, <)$ can be generalized to a quasi-ordering $(R^s, <)$ in the following way:
Let $e_1, ..e_s$ be the generators of R^s, then we define an extension of $(M, <_m)$ to $(M^s, <_m)$

Definition 7.1 (Extension of an ordering to a module)
$(M^s, <_m)$ is an extension of an ordering $(M, <_m)$ iff

- $m_1 e_i <_m m_2 e_i \Leftrightarrow m_1 <_m m_2$ *for all* $i \in 1..s$
- *all elements of the form me_i $(m \in M)$ can be compared using $(M^s, <_m)$*

Remark: There are many ways of extending a given ordering $(M, <_m)$ to an ordering $(M^s, <_m)$, but we use the ordering:

$$m_1 e_i <_m m_2 e_j \Leftrightarrow (i < j \text{ or } (i = j \text{ and } m_1 <_m m_2))$$

We have generalized an ordering $(M, <_m)$ to a quasi-ordering $(R, <)$ and we can do the same with $(M^s, <_m)$ to get a quasi-ordering $(R^s, <)$. Now we can define leading terms, modules of leading terms of a submodule of R^s and Gröbner bases. Also the algorithms to compute Gröbner bases are the same (remember that $m_1 e_j | m_2 e_j$ iff $m_1 | m_2$ and $i = j$).

Definition 7.2 (syzygy) *Let $F = \{f_1, .., f_l\} \subset R^s$.*
A syzygy of F is an element $h = h_1 e_1 + ... + h_l e_l \in R^l$ which maps to $0 \in R^s$ under the map $e_i \in R^l \mapsto f_i \in R^s$.

Proposition 7.3 *Consider the module N generated by $\{f_i - e_i, i = 1..l\} \in R^{s+l}$ then $N \cap \{0\} \times R^l$ is the module of syzygies of a given $F = \{f_1, .., f_l\} \subset R^s$.*

To compute a Gröbner base of this module of syzygies of F we use the elimination property of Gröbner bases with respect to a partial lexicographic ordering: (see [B87])

Proposition 7.4 (Elimination property of Gröbner bases)
If $(R^{s+l}, <)$ is a quasi-ordering with $m_1 < m_2$ for all $m_1 \in R^s \times \{0\}$ and all $m_2 \in \{0\} \times R^l$, then $GB(N \cap (\{0\} \times R^l)) = GB(N) \cap (\{0\} \times R^l)$.

Our quasi-ordering $(R^{s+l}, <)$ has this property. So we can compute syzygies of $F = \{f_1, .. f_l\} \subset R^s$ by computing a Gröbner base G of $\{f_1 - e_{s+1}, ... f_l - e_{s+l}\}$. The elements of G which have no monomials of the form me_i with $i \leq s$ form a Gröbner base of the module of syzygies of F (remember a Gröbner basis is a generating set).

8 Applications

Our implementation works in the tensor product of a symmetric and an exterior algebra $S^\bullet \otimes \wedge^\bullet$. Thus we can calculate deformation of matrices whose entries are in the exterior algebra. In the sequel we will present some examples of applications where the implementation was used. In the theory of vector bundles those matrices occur in short sequences (monads). The chapter below will present a short introduction to these problems.

The Smoothness of the moduli space of instantons on P_3

A mathematical instanton bundle on P_3 is a stable rank 2 vector bundle $\mathcal{E}$ with first Chern class $c_1\mathcal{E} = 0$ and vanishing condition $h^1\mathcal{E}(-2) = 0$, see [B-H]. The stability condition implies $n = c_2\mathcal{E} > 0$. It is well–known that $\mathcal{E}$ is the cohomology of a Beilinson complex

$$0 \to n\Omega^3(3) \xrightarrow{M} n\Omega^1(1) \xrightarrow{B} (2n-2)\mathcal{O} \to 0 \tag{10}$$

in which M and B are induced by linear maps

$$k^n \xrightarrow{M} k^n \otimes \wedge^2 V, \qquad k^n \xrightarrow{B} k^{2n-2} \otimes V.$$

The conditions for M, B to define an instanton bundle are:

(i) M is symmetric

(ii) the induced sequence

$$k^n \otimes V \xrightarrow{\wedge M} k^n \otimes \wedge^3 V \xrightarrow{\wedge B} k^{2n-2} \otimes \wedge^4 V \to 0$$

is exact

(iii) $k^{2n-2} \xrightarrow{B^t} k^n \otimes V$ satisfies $Im(B^t) \cap (k^n \otimes v) = 0$ for any nonzero $v \in V$

see [B-T], section 1. We let $MI(n)$ denote the open subscheme of the Maruyama scheme $M(2;0,n,0)$ of all semi–stable coherent sheaves on P_3 of rank 2 and Chern classes $(c_1,c_2,c_3) = (0,n,0)$ whose closed points are the isomorphism classes of mathematical instanton bundles. Up to now it is not known whether $MI(n)$ is smooth and irreducible for all n. $MI(n)$ is smooth at $\mathcal{E}$ if $Ext^2(\mathcal{E},\mathcal{E}) = 0$. There are reasons to believe that

the stronger condition $Ext^2(\mathcal{E}, \mathcal{E}(-1)) = 0$ holds for any $\mathcal{E} \in MI(n)$. Indeed this is true for the so-called special *'t Hooft* instanton bundles characterized by $h^0\mathcal{E}(1) = 2$, see [B-T]. This was shown in [H-N], or can easily be derived from the normal form of B in [B-T]. In [N-T] the same result is prooven for the more general case for any $\mathcal{E} \in MI(n)$ satisfying $h^0\mathcal{E}(1) = 1$. Note that by [B-T] $h^0\mathcal{E}(1) \leq 2$ for any $\mathcal{E} \in MI(n)$. We assume $n \geq 3$, since for $n = 2$ always $h^0\mathcal{E}(1) = 2$.

If one follows the proof of lemma 4.1.7 in [OSS] for $Ext^2(\mathcal{E}, \mathcal{E}) \simeq H^2(\mathcal{E}nd(\mathcal{E}))$ one sees how to compute this group as the cokernel of the operator

$$H^0(2n\Omega^3(3) \otimes 2(2n-2)\mathcal{O})\tilde{B} := (Id \otimes B | B \otimes Id)H^0((2n-2)^2/calO)$$

where B is the "right monad" arrow, a matrix with entries in $\wedge^\bullet V$ and | indicates the concatination of matrices. Thus the question is to compute the linear syzyies of the transpose of $\tilde{B}$. This is a nice job for our program.

Deformations of Monads

Another problem is finding deformations of a given family of vector bundles, constructed by deformations of Monads where the correspondence between vector bundles and monads is the same as in the previous section. So we are starting with vector bundles given by the monads. One can take for example the instanton bundle given by the monad below:

$$0 \to n\Omega^3(3) \xrightarrow{M} n\Omega^1(1) \xrightarrow{B} (2n-2)\mathcal{O} \to 0$$

The task is to find matrices M_1 and B_1 solving for the given matrices M and B the monad equation

$$(M + tM_1) \wedge (B + tB_1) = 0$$

which comes for the exactness of the sequence ii) in the previous section in order to receive a first order deformation of the monad :

$$0 \to n\Omega^3(3) \overset{M+tM_1}{\to} n\Omega^1(1) \overset{B+tB_1}{\to} (2n-2)\mathcal{O} \to 0$$

This equation divides up into a 'linear' and 'quadratic' part which can be solved separately :

$$\begin{aligned} M \wedge tB_1 + tM_1 \wedge B &= 0 \text{ and} \\ tM_1 \wedge tB_1 &= 0 \end{aligned}$$

The second equation is only relevant for higher order deformation. As before this can also be done by the program.

Obviously there are many more concrete calculations waiting for this program.

References

[B-H] W. Barth, K.Hulek *Monads and Moduli of Vector Bundles* manuscripta mathh. 25, 323-347, 1977

[B-T] W. Böhmer, G. Trautmann *Special instanton bundles and Ponceletcurves* Sigularities,Representaions of Algebras and Vector Bundles, Proceedings Lambrecht 1985

[B65] B. Buchberger *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal.* Dissertation Univ. Innsbruck 1965

[B87] B. Buchberger *Applications of Gröbner bases in non-linear computational geometry* Proc. Int. Symp. Trends in Computer Algebra, Bad Neuenahr, 19.-21. Mai 1987, e. R.Janßen, LNCS

[H-N] A. Hirschowitz, M.S. Narasimhan *Fibrés de t'Hooft speciaux et applications* Proc.Nice Conf. 1981, Birkhäuser

[K] H. Kredel *Solvable Polynomial Rings* Dissertation Univ. Passau 1992

[K-W90] A. Kandri-Rody, V. Weispfenning. *Non-Commutative Gröbner Bases in Algebras of Solvable Type* Journal of Symbolic Computation 9(1990), 1-26

[KR85] H. Kredel *On a generalization of the Gauss' algorithm to modules over polynomial rings* Manuscript 1985

[LeChe] Philippe Le Chenandec *Canonical Forms in Finitely Presented Algebras* Research Notes in Theoretical Computer Science Wiley & Sons (1986)

[MR93] K. Madlener, B. Reinert *Computing Gröbner Bases in Monoid and Group Rings* Proc. ISSAC 93, to appear

[M85] F. Mora *Gröbner Bases for Non-Commutative Polynomial Rings* Proc. AAECC-3(1985). Springer LNCS 229, 353-362

[NO89] P. Narendran, C.Ó'Dúnlaing *Cancellativity in Finitely Presented Semigroups* Journal of Symbolic Computation 7 1989, 457-472

[N-T] T. Nüßler, G. Trautmann *Multiple Koszul Structures on Lines and Instanton Bundles* DFG-Forschungsschwerpunkt Komplexe Mannigfaltigkeiten Preprint Nr.172, to appear in ...

[OSS] Ch. Okonek, M. Schneider, H. Spindler *Vector Bundles on Complex Projective Spaces* Birkhäuser 1980

[P-S] G. Pfister, H. Schönemann *Singularities with exact Poincaré complex but not quasihomogeneous* Revista Matematica Univ. Complutense de Madrid, Vol. 2, n.2y3 1989

[R] L. Robbiano *Term orderings on the polynomial ring* Proc. EUROCAL 85, LNCS 204 (1985), 513-517

[S] T. Stokes *Gröbner bases in exterior algebra* Preprint Universtiy of Tasmania, 1989

[W92] V. Weispfenning *Finite Gröbner Bases in Non-Noetherian Skew Polynomial Rings* Proc. ISSAC 92, 329-334

[ZIMNO] M. Zimnol *Beispiele Algebraischer Reduktionsstrukturen* Preprint No.124 Kaiserlautern 1987

Fachbereich Mathematik
Universität Kaiserslautern
D- 67663 Kaiserslautern
email: thomas@mathematik.uni-kl.de
email: hannes@mathematik.uni-kl.de