Algorithms in Local Algebra*

Hans-Gert Gräbe
Institut für Informatik, Universität Leipzig
Leipzig, Germany

May 30, 1994; Revised August 1, 1995

Abstract

Let k be a field, $S = k[x_v : v \in V]$ be the polynomial ring over the finite set of variables $(x_v : v \in V)$, and $m = (x_v : v \in V)$ the ideal defining the origin of *Spec S*.

It is theoretically known (see e.g. Alonso *et al.* 1991) that the algorithmic ideas for the computation of ideal (and module) intersections, quotients, deciding radical membership etc. in S may be adopted not only for computations in the local ring S_m but also for term orders of mixed type with standard bases replacing Gröbner bases. Using the generalization of Mora's tangent cone algorithm to arbitrary term orders we give a detailed description of the necessary modifications and restrictions.

In a second part we discuss a generalization of the deformation argument for standard bases and independent sets to term orders of mixed type. For local term orders these questions were investigated in (Gräbe 1991).

The main algorithmic ideas described are implemented in the author's REDUCE package CALI (Gräbe 1993a).

1 Introduction

Let $S := k[x_v : v \in V]$ be a (finitely generated) polynomial ring over the field k and $m := (x_v, v \in V)$ the defining ideal of the origin in *Spec S*.

Gröbner basis techniques proved to be useful for the solution of a wide range of algorithmic problems concerning ideals and modules over the polynomial ring S as e.g.

- the ideal membership problem,
- the radical membership problem,
- the computation of dimension and degree of a (projective) variety,
- the computation of Hilbert series,
- the computation of elimination ideals,
- the computation of ideal intersections,
- the computation of quotients and stable quotients,
- primality testing,
- the computation of primary decompositions,

*Appeared in *J. Symb. Comp.* **19** (1995), 545 - 557.

cf. e.g. (Becker *et al.* 1993), (Buchberger 1988) or (Gianni *et al.* 1988) for a survey.

If we are interested in local properties of an ideal $I \subset S$ (or module) at m, the origin of *Spec* S, one should prefer direct computations over the localization S_m of S at m, since an intermediate application of Gröbner basis techniques in S followed by localization at m may produce many unnecessary components not passing through the origin. Moreover, the intermediate ideal of leading terms of I, containing terms of *highest* degree, will reflect the global behaviour of I rather than the local one.

For local computations in S_m one has to equip S with a non-noetherian term order and to use standard sets instead of Gröbner bases. In general, standard sets in S are standard bases in $Loc(S)$, a certain localization of the polynomial ring, depending on the special kind of the underlying term order (cf. Mora 1988). For *local term orders*, e.g. supported by negative weights, we have $Loc(S) = S_m$.

There are two approaches to standard sets, Lazard's approach, using homogenization techniques (cf. Lazard 1983) and Mora's tangent cone algorithm (cf. Mora 1982). Both produce (polynomial) standard bases in $Loc(S)$, such that the ideal of leading terms of I, in this case containing terms of *lowest* degree, will reflect the local behaviour of I at the origin.

More advanced computations in families of singularities need even more complicated term orders, where some of the parameters occur as global variables whereas other as local ones. Such term orders are called *of mixed type*.

Lazard's approach may be applied to arbitrary term orders, but adding a new variable may (and often will) increase the computational amount. Moreover homogenized standard bases produced this way usually contain many more elements than a minimal standard basis does.

For Mora's tangent cone algorithm several improvements were suggested, see (Mora *et al.* 1992) for a summary, so that the experts commonly prefer the latter. In the same paper the authors also give a generalization of the tangent cone algorithm that applies to certain term orders of mixed type. Such a generalization makes available algorithmic approaches using elimination techniques that are essential for good algorithms to compute quotients and intersections. A first short description of a generalization of the basic algorithms described e.g. in (Gianni *et al.* 1988) for Gröbner bases to $Loc(S)$ appeared in (Alonso *et al.* 1991).

In (Gräbe 1994) we introduced another version of the tangent cone algorithm (with encoupled ecart vector), that applies to arbitrary term orders and seems to be a more practical generalization than the one given in (Mora *et al.* 1992).[1] Based on this version and its implementation in CALI we consider constructive approaches to the following problems in $Loc(S)$ in more detail :

- computation of ideal intersections,
- computation of the quotient of an ideal by a polynomial,
- computation of the stable quotient of an ideal by a polynomial, and
- deciding radical membership.

We discuss both the homogenization and the tangent cone approaches. The former one leads to direct Gröbner basis computations and one has only to give a correct interpretation of the dehomogenized results. For the latter one we describe in more detail how to modify the algorithms, mainly based on elimination techniques, themselves.

[1] This generalization was independently found by the SINGULAR group, see (Grassmann *et al.* 1994)

In (Alonso *et al.* 1989 and 1993) the authors discussed a computational approach to algebraic power series rings $R \subset k[[x_v : v \in V]]_{alg}$ that are finitely generated extensions of S_m. Their ideas can be embedded into the concept of computations in factor rings of local rings (a facility available, e.g., in the computer algebra system MACAULAY for Gröbner bases over polynomial rings) and hence used for a constructive solution over R of the problems formulated above. This concept, already developed in (Alonso *et al.* 1991), thus becomes a practical computational tool and will be available in a forthcoming version of CALI.

(Bayer 1982) introduced a flat deformation argument for Gröbner bases, that proved to be useful many times. It can be exploited in two different manners, namely as a flat deformation itself and through a homogenization argument, see e.g. (Gräbe 1993b) for the latter. In the last part of the paper we discuss, how these arguments may be generalized to arbitrary term orders. This was discussed so far mainly for local term orders, where $Loc(S)$ admits a completion, see e.g. (Gräbe 1991) for a spectral sequence argument. (Grassmann *et al.* 1994, prop. 5.3.) generalized the deformation argument to arbitrary term orders and drew some conclusions about the dimension and, for zero dimensional ideals and modules, the multiplicity.

Here we generalize the second approach, homogeneous local rings, to term orders of mixed type. Using *homogeneous* instead of ordinary localization this leads to a different deformation and allows to derive bounds for Betti numbers, depth and CM-type of $Loc(S)/I$ in terms of the initial ideal.

Further we show that the concept of independent sets, see (Kredel, Weispfenning 1988) transfers to $Loc(S)$ as well. This implies the validity of the unmixedness results in (Gräbe 1993b) also in the general case.

As usual most of the algorithms presented below have an easy extension to finitely generated modules over the rings considered so far (and are implemented in CALI in this generality). For simplicity we restrict ourselves to the case of polynomial ideals.

2 Preliminaries

Let S, as before, be a polynomial ring in finitely many indeterminates over a field k. In the following we assume the monoid of terms of S to be equipped with a linear semigroup order, *term order* for short, that will be denoted $TO(S)$.

Usually term orders are defined as refinements of linear quasiorders, i.e. linear, reflexive, transitive, and monotone relations, to true orders. With such a quasiorder $\leq$ we associate in a natural way two other relations, the equivalence relation $a \equiv b$ iff $a \leq b$ and $b \leq a$ and the partial (true) irreflexive order $a < b$ iff $a \leq b$ and $a \not\equiv b$. On the other hand, given $\equiv$ and $<$ with obvious compatibility conditions, one can recover the quasiorder $\leq$ as $a \leq b$ iff $b \not< a$. We will freely use both notations. For such a linear quasiorder $\leq$ and each pair of terms one of the following alternatives holds : $x^a < x^b$ or $x^b < x^a$ or $x^a \equiv x^b$.

Given two (quasi)orders TO_1 and TO_2 on S, $TO_1 \mid TO_2$ denotes their *lexicographical product*, i.e.

$$x^a \leq x^b \quad :\Leftrightarrow \quad (x^a <_1 x^b) \text{ or } (x^a \equiv_1 x^b \text{ and } x^a \leq_2 x^b)$$

Let $LEX(x_1, \ldots, x_k)$ resp. $REVLEX(x_1, \ldots, x_k)$ denote the *lexicographic* resp. *reverse lex.* (quasi)orders with respect to the (ordered) variable set $\{x_1, \ldots, x_k\}$, i.e.

$$x^a < x^b \quad :\Leftrightarrow \quad \exists j : \forall (i < j)\ a_i = b_i \text{ and } a_j < b_j \text{ (lex.) or } a_j > b_j \text{ (revlex.)}$$

$$x^a \equiv x^b \quad :\Leftrightarrow \quad \forall i \; a_i = b_i$$

For a given term order and a nonzero polynomial $f = \sum c_\alpha x^\alpha \in S$ we define as in (Gräbe 1994)

$$in(f) := c_{\alpha_0} x^{\alpha_0} \text{ with } \alpha_0 = max\{\alpha : c_\alpha \neq 0\},$$
$$deg\; f := \alpha_0,$$
$$red(f) := f - in(f) \text{ and}$$
$$in(B) := \{in(f) : f \in B\} \text{ for any set } B \subset S.$$

$TO(S)$ is called *noetherian* iff it is well-founded or, equivalently, $1 < x^a$ for all nontrivial terms in S. For non-noetherian term orders the set

$$U = U(S) := \{1 + f \in S \; : \; in(f) < 1 \text{ or } f = 0\}$$

plays an important role, as explained e.g in (Robbiano 1986) or (Mora 1988). If $1 > x^a$ for all nontrivial terms in S we refer to $TO(S)$ as a *local order*. In this case $U^{-1}S = S_m$. Term orders that are neither noetherian nor local are called *of mixed type*.

Let $I \subset S$ be an ideal and $B \subset I$ a finite set. B is a *standard set* of I iff $in(B)$ generates the ideal $in(I)$. Although not unique for a fixed term order we will denote such a standard set by some abuse of notation $STB(I)$.

In contrast to noetherian term orders, where standard sets automatically generate I, see (Becker *et al.*, prop 5.38.), the same does not hold for arbitrary term orders. But it turns out, that standard sets always generate the extension of I to $Loc(S) := U^{-1}S$. Moreover standard sets are standard bases in $Loc(S)$ in the sense of (Mora 1988). Here $B = \{b_\alpha\}$ is a *standard basis* of I in $Loc(S)$ iff

$$\forall f \in I \cdot Loc(S) \, \exists g_\alpha \in Loc(S) \; : \; f = \sum b_\alpha g_\alpha \text{ and } in(f) \geq max\{in(b_\alpha g_\alpha)\}.$$

Clearing denominators, each ideal $I \subset Loc(S)$ has a "denominator-free" basis $B(I) \subset S$. We will assume this henceforth without further mention. Note that $B(I)$ must not generate $I \cap S$.

Let $w \in (\mathbf{R}^V)^*$ be a linear functional on $\mathbf{R}^V$. Such w is called a *weight vector* and induces a grading on $\mathbf{N}^V$. Denote by $DO(w)$ the quasiorder pre-image on $\mathbf{N}^V$ of the natural order $\leq$ on $\mathbf{R}$ under w. We refer to this quasiorder as the *degree order* associated with w. By (Robbiano 1986) we know that every monotone linear order is a refinement of such a degree order. If $<$ is a refinement of $DO(w)$ we say that $<$ is *supported* by the weight vector w.

If w has only positive weights, every refinement of $DO(w)$ is noetherian. If w has only negative weights, every refinement of $DO(w)$ is a local order. We call term orders, supported by $(-1, \ldots, -1)$, *tangent cone term orders* (since in this case the lowest degree parts of all $f \in STB(I)$ generate the tangent cone of I at the origin).

3 Lazard's approach

3.1 Homogenization

Let S be as above and t be another variable. Given $w \in (\mathbf{Z}^V)^*$, an *ecart vector*, we define for $f = \sum c_a \cdot x^a \in S$ with $d = max\{w(a) : c_a \neq 0\}$, $F(t) \in S[t]$, and $B = \{f_1, \ldots, f_r\}$

the homogenization ${}^h f := \sum c_a \cdot t^{d-w(a)} \cdot x^a$,
the (w-)ecart $e_w(f) := d - w(deg(f))$,
the homogenization ${}^h B := \{ {}^h f_1, \ldots, {}^h f_r\}$,
the dehomogenization ${}^a F := F(1)$.

This yields applications ${}^h : S \longrightarrow S[t]$ and ${}^a : S[t] \longrightarrow S$ as in (Mora, Robbiano 1988).

Extending the definition of w by $w(t) = 1$ we equip $S[t]$ with the term order $TO_w := DO(w) \mid TO(S)$, i.e.

$$t^a \cdot x^\alpha <' t^b \cdot x^\beta :\Leftrightarrow \quad \begin{array}{c} a + w(\alpha) < b + w(\beta) \text{ or} \\ a + w(\alpha) = b + w(\beta) \text{ and } x^\alpha < x^\beta \end{array}$$

If w has only positive weights this term order is noetherian.

3.2 A "classical" solution for local problems

For an ideal $I \subset R$ in a ring R and $f \in R$ set

$$I : f^\infty := \{g \in R \mid \exists\, n \ : \ f^n g \in I\},$$

the stable quotient of I with respect to f.

The following proposition describes, how one can solve local problems through homogenization (with respect to a positive ecart vector), Gröbner basis computations, and dehomogenization.

Proposition 1 *Let S be a polynomial ring equipped with an arbitrary term order $TO(S)$, ^{h} and ^{a} as in the preceding paragraph homogenization and dehomogenization with respect to a positive ecart vector and the homogenizing variable t, $I, J \subset Loc(S)$ ideals, given by denominator-free polynomial bases $B(I), B(J) \subset S$ and $f \in S$ another polynomial. Then in $Loc(S)$ we have*

1. $I \bigcap J = {}^a(\langle {}^h B(I)\rangle \bigcap \langle {}^h B(J)\rangle)$,
2. $I : f = {}^a(\langle {}^h B(I)\rangle : {}^h f)$,
3. $I : f^\infty = {}^a(\langle {}^h B(I)\rangle : {}^h f^\infty)$,
4. $f \in Rad(I \cdot Loc(S))$ *iff* $1 \in {}^a(\langle {}^h B(I)\rangle : {}^h f^\infty)$,
   i.e. an arbitrary standard basis of $\langle {}^h B(I)\rangle : {}^h f^\infty$ contains an element with a pure t-power as leading term.

PROOF: Let's prove e.g. 1) :
Assume $B(I) = \{i_a\}, B(J) = \{j_a\}$. We have $f \in I \bigcap J$ in $Loc(S)$ iff there exists a unit $e \in U$ such that $e \cdot f = \sum r_a i_a = \sum s_a j_a$ with certain $r_a, s_a \in S$. Homogenizing this relation we get for appropriate powers of t

$$t^n\, {}^h e \cdot {}^h f = \sum t^{m_a}\, {}^h r_a\, {}^h i_a = \sum t^{n_a}\, {}^h s_a\, {}^h j_a.$$

Dehomogenizing yields $e \cdot f \in {}^a(\langle {}^h B(I)\rangle \bigcap \langle {}^h B(J)\rangle)$.

The other assertions are proved in a similar way. $\square$

Note that all these problems have well-known solutions for the noetherian term order TO_w that may be invoked with the homogenized basis ${}^h B(I)$.

4 Direct methods

4.1 Reduction with bounded ecart

Recall (a slight modification of) the algorithm RME in (Gräbe 1994, thm. 1).

Let $w \in (\mathbf{N}_+^V)^*$ be a positive ecart vector. Then for arbitrary term orders $TO(S)$ the following normal form algorithm terminates after a finite number of steps:

RBE(f,B) – Reduction with bounded w-ecart

INPUT: A polynomial $f \in S$, a finite set $B \subset S$.
OUTPUT: A polynomial $h \in S$ and a unit $u \in U$ with $h \equiv u \cdot f \ (mod\ (B))$ and either $h = 0$ or $in(h)$ not divisible by any $in(g),\ g \in B$.
LOCAL: A list L of simplifier-unit/zero pairs, updated during the algorithm.

– $L := \{(g, u_g := 0)\ :\ g \in B\},\ (h, u_h) := (f, 1)$.
– While $h \neq 0$ and $M := \{(g, u_g) \in L : in(g)|in(h)\} \neq \emptyset$ do
  (1) $M_1 := \{(g, u_g) \in M : e_w(g) \leq e_w(h)\}$
  (2) If $M_1 \neq \emptyset$ then choose $(g, u_g) \in M_1$ else
    (a) Choose $(g, u_g) \in M$.
    (b) $L := L \bigcup \{(h, u_h)\}$.
  (3) $h' := h - m \cdot g$ with $m := \frac{in(h)}{in(g)}$.
  (4) Set $h := h',\ u_h := u_h - m \cdot u_g$.
– Return (h, u_h).

This normal form algorithm yields a finite standard set algorithm for arbitrary term orders $TO(S)$ in the usual way. See (Gräbe 1994) for a discussion of this subject and also for some improvements. It gives also an immediate algorithm to solve the ideal membership problem in $Loc(S)$, given a standard set B for the ideal I.

4.2 Supporting weights

Above we introduced the notion of the weight vector supporting a term order $<$. For Gröbner bases Bayer observed in (Bayer 1982) that for a given ideal $I \subset S$ the term order $<$ may be changed in such a way to $<'$, that a (totally interreduced) Gröbner basis of I with respect to $<$ remains a (totally interreduced) Gröbner basis also with respect to $<'$, but $<'$ is supported by a positive integer weight vector. For arbitrary term orders a similar result can be proved[2] :

Lemma 1 *Given an ideal $I \subset S$ with a fixed (finite) standard set $STB(I)$ there is even an integer weight vector $w \in (\mathbf{Z}^V)^*$ such that $in(I) = in_{<'}(I)$ with respect to every refinement $<'$ of $DO(w)$ to a term order and $w(deg\ f) > w(deg\ red\ f)$ for $f \in STB(I)$ (with nonzero reductum). If $<$ is a local order, w can be chosen to have only negative weights.*

PROOF: One cannot deduce this result as for the noetherian case, since in general we have neither uniquely defined (finite polynomial reduced) standard bases nor finite *total* normal forms with respect to $B = STB(I)$. But since there is a finite algorithm to verify the standard set property, involving only a finite number of (finite) polynomials, we get a finite number

[2] As pointed out to us by the referee, the corresponding fact for standard bases in power series rings was established already in (Becker 1990) in the same way.

of open conditions on w to guarantee that B is a standard set also with respect to $<'$ and $w(deg\ f) > w(deg\ red\ f)$ for $f \in B$. $\Box$

We say, that under these conditions $(I, <)$ is *strongly supported* by w (with respect to $STB(I)$).

4.3 The elimination method

Let S be as above and t be another variable. Consider the following problem :

Given a finite ideal basis of $I \subset Loc(S)[t]$

find a finite ideal basis of $I_0 = I \bigcap Loc(S)$.

Based on RBE it may be solved for arbitrary term orders $TO(S)$.

Lemma 2 *(cf. Alonso* et al. *1991) Let $TO(S)$ be an arbitrary term order on S and I be an ideal in $Loc(S)$. Equipping $S[t]$ with the term order $LEX(t) \mid TO(S)$ we get $Loc(S)[t] = Loc(S[t])$ and*

$$STB(I_0) = \{f \in STB(I)\ :\ in(f) \text{ is free of } t\}.$$

REMARK: $TO(S[t])$ is not inflimited if $TO(S)$ is not noetherian and different from TO_w introduced in the preceding section.

PROOF: By the choice of the term order $in(f)$ being free of t implies f being free of t. $\Box$

The elimination lemma allows to compute intersections and quotients (cf. Alonso *et al.* 1991) :

Proposition 2 *With S and $S[t]$ as in the lemma we get for ideals $I, J \subset Loc(S)$ and $f \in S$*

1. $I \bigcap J = (t \cdot I + (1-t) \cdot J) \bigcap Loc(S)$,
2. $I : (f) = (I \bigcap \langle f \rangle) \cdot \frac{1}{f}$,
3. $I : f^\infty = (I + \langle 1 - f \cdot t \rangle) \bigcap Loc(S)$
   and especially
4. $f \in Rad(I)$ *iff* $1 \in (I + \langle 1 - f \cdot t \rangle)$.

The proof is the same as in the noetherian case, given in (Gianni *et al.* 1988) or (Becker *et al.* 1993). Note that the first assertion can be generalized as in (Becker *et al.* 1993, prop. 6.19).

In 2) one has to divide out the common factor f from all generators $g \in I \bigcap \langle f \rangle$ in $Loc(S)$. For this purpose the usual division-remainder algorithm must be modified in a similar way as RBE modifies the usual normal form algorithm :

divmod(f,g) - (Local) division with remainder

INPUT: Polynomials $f, g \in S$.
OUTPUT: Polynomials $h, q \in S$ and a unit $u \in U$ with $u \cdot f = q \cdot g + h$ and either $h = 0$ or $in(h)$ not divisible by $in(g)$.
LOCAL: A list L of triples (k, q_k, u_k), updated during the algorithm, such that $k = u_k f - q_k g$.

– $L := \{(g, q_g := -1, u_g := 0)\},\ (h, q_h, u_h) := (f, 0, 1)$.
– While $h \neq 0$ and $M := \{(k, q_k, u_k) \in L : in(k)|in(h)\} \neq \emptyset$ do
  (1) $M_1 := \{(k, q_k, u_k) \in M : e_w(k) \leq e_w(h)\}$
  (2) If $M_1 \neq \emptyset$ then choose $(k, q_k, u_k) \in M_1$ else
    (a) Choose $(k, q_k, u_k) \in M$.
    (b) $L := L \bigcup \{(h, q_h, u_h)\}$.
  (3) $h' := h - m \cdot k$ with $m := \frac{in(h)}{in(k)}$.
  (4) Set $h := h',\ u_h := u_h - m \cdot u_k,\ q_h := q_h - m \cdot q_k$.
– Return (h, q_h, u_h).

Correctness and termination (provided w has positive weights) follow immediately as for RBE.

4.4 An alternative quotient algorithm

D. Bayer gave in (Bayer 1982) an alternative algorithm to compute the quotient of an homogeneous ideal by a homogeneous polynomial. In (Alonso *et al.* 1991) the authors sketched its generalization to not necessarily homogeneous input with respect to a local term order on S. Below we discuss this approach in more detail and show by means of examples its natural restrictions.

So let's assume that $TO(S)$ is a local term order. Let t be another variable. Equip $S[t]$ with the term order $REVLEX(t) \mid TO(S)$.

Proposition 3 *For a local term order on S let $I \subset Loc(S)$ be an ideal and $f \in S$ a polynomial, such that $in(f) < 1$. Under these assumptions we have*

1. $I : f = (I + \langle f - t \rangle) : t|_{t=f}$ *and*

2. $I : f^\infty = (I + \langle f - t \rangle) : t^\infty|_{t=f}$,

where the ideal quotients are computed in Loc(S) and Loc(S[t]) respectively and $|_{t=f}$ denotes the map induced by the substitution $t \mapsto f$.

PROOF: Let's prove the first assertion since the second one follows immediately from the first one. Since

$$U := U(S) \subset U_t := U(S[t]) = \{e + t \cdot s(t) : e \in U, s(t) \in S[t]\}$$

we have $I : f \subset (I + \langle f - t \rangle) : t|_{t=f}$. For the other direction assume $g(t) \in (I + \langle t - f \rangle) : t \bigcap S[t]$, i.e. $(e + t \cdot s(t)) \cdot t \cdot g(t) \in I + \langle t - f \rangle$ for some unit $e + t \cdot s(t) \in U_t$. By our assumption $e + f \cdot s(f) \in U$ and hence $g(f) \in I : f$. $\square$

REMARK: For $f \in U$ the assertion is false, since in this case $I : f = I$ whereas $f - t \in U_t$ and hence $I + \langle f - t \rangle = \langle 1 \rangle$. In general it does not hold as well for term orders $TO(S)$ that aren't local. Indeed, e.g. for $S = k[x]$ with $TO(S) = LEX(x)$ we get $\langle x-1\rangle : x = \langle x-1\rangle$, but $\langle x-1, x-t\rangle = \langle 1\rangle$ in $Loc(S[t])$ (with $TO(S[t]) = REVLEX(t) \mid TO(S)$). In general we have

$$I : f = (I + \langle f - t\rangle) : t \bigcap Loc(S)$$

only for $TO(S[t]) = LEX(t) \mid TO(S)$. But for this term order the second step of Bayer's approach doesn't apply.

In the following $TO(S)$ may be arbitrary. Let $S[t]$ be as above equipped with $TO(S[t]) = REVLEX(t) \mid TO(S)$. By the definition of this term order for any $f \in S[t]$ the t-power of $in(f)$ divides f. Thus we may define $f : t$ as $\frac{1}{t} f$ if t divides $in(f)$ and f otherwise and $f : t^\infty$ as $\frac{1}{t^m} f$, where t^m is the greatest t-power dividing $in(f)$.

Proposition 4 *Under these assumptions we get for an ideal $I \subset Loc(S[t])$*

1. $\{f : t \mid f \in STB(I)\}$ *is a standard basis of $I : t$ in $Loc(S[t])$.*
2. $\{f : t^\infty \mid f \in STB(I)\}$ *is a standard basis of $I : t^\infty$ in $Loc(S[t])$.*

Proof: For the first assertion assume $g \in I : t$. Hence there is $e \in U_t$ and a standard representation $egt = \sum_{f \in STB(I)} r_f f$. Since t divides $in(egt) \geq in(r_f f)$, t divides $in(r_f)$ or $in(f)$. Hence eg has a standard representation

$$eg = \sum{}^{(1)} (r_f : t) f + \sum{}^{(2)} r_f (f : t),$$

where the first sum ranges over all $f \in STB(I)$ such that t doesn't divide $in(f)$ and the second sum ranges over the remaining $f \in STB(I)$.

The second assertion follows similarly. $\square$

Remark: After the substitution $t = f$ in the assertion of the proposition the basis obtained need not to be a standard set with respect to $TO(S)$ any more.

5 Locally smooth systems

Let $J \subset Loc(S)$ be an ideal and $R := Loc(S)/J$. It is possible to do algebraic computations also over R due to the following elementary observation :

Let $\bar{I}_1, \bar{I}_2 \subset R$ be ideals, $\bar{f} \in R$ and I_1, I_2, f their pre-images in $Loc(S)$. Then

$$\begin{aligned}
&\bar{I}_1 \bigcap \bar{I}_2 = (I_1 + J) \bigcap (I_2 + J)/J,\\
&\bar{I}_1 : \bar{f} = (I_1 + J) : f/J \text{ and}\\
&\bar{I}_1 : \bar{f}^\infty = (I_1 + J) : f^\infty/J.
\end{aligned}$$

Hence the algebraic questions considered above may be solved constructively also over R. Using a standard basis of J one can moreover solve the zero decision problem (and hence the equality problem) over R. It is also possible to compute Hilbert series and syzygies over R.

This technique can be applied to computational problems concerning algebraic power series in $k[[x_v : v \in V]]_{alg}$. In the remaining part of this paragraph we assume $TO(S)$ to be a local term order.

In (Alonso *et al.* 1989 and 1992) the authors introduced a concept that allows a constructive handling of systems of algebraic power series as elements of a finite extension $Loc(S) \subset R \subset k[[x_v : v \in V]]_{alg}$. For this purpose they consider polynomials $F_1, F_2, \ldots, F_r \in$

$S' := S[Y_1, \dots Y_r]$, such that their Jacobian $\|\frac{\partial F_i}{\partial Y_j}\|$ is a nonsingular (w.l.o.g.) lower triangular matrix at the origin $x_v = Y_i = 0$ ($v \in V, i = 1, \dots r$). By the Implicit Function Theorem the system of equations $F_1 = \dots = F_r = 0$ has a unique solution $f_1, \dots, f_r \in k[[x_v : v \in V]]_{alg}$ in algebraic power series vanishing at the origin. Such a system they call a *locally smooth system* (LSS).

The map $\sigma : Loc(S') \longrightarrow k[[x_v : v \in V]]_{alg}$ via $Y_i \mapsto f_i$ with kernel $J := ker\ \sigma = (F_1, \dots, F_r) \cdot Loc(S')$ defines a surjection on $R = im\ \sigma$, the extension of $Loc(S)$ by $f_1, \dots, f_r$. The authors give conditions on the term order $TO(S')$ to be satisfied to reformulate and solve problems in R as problems in $Loc(S')/J$. Such term orders they call *uniform term-orderings*. See also (Mora *et al.* 1992) for a short explanation. As a natural uniform term-ordering may serve $TO(S) \mid TO_Y$, where TO_Y is the tangent cone order

$$DO(-1, \dots, -1) \mid REVLEX(Y_1, \dots, Y_r)$$

on $Y_1, \dots, Y_r$. If the algebraic power series $f_1, \dots, f_r$ are defined recursively, i.e. F_i is free of $Y_j, j > i$, even $TO(S) \mid REVLEX(Y_1, \dots, Y_r)$ may be used.

Proposition 5 *(cf. Alonso* et al. *1991) Let R be a finite algebraic extension of $Loc(S)$ in $k[[x_v : v \in V]]_{alg}$ defined by a LSS. Then one can*

1. *compute ideal intersections,*
2. *compute ideal quotients,*
3. *compute stable quotients,*
4. *decide radical membership problems.*

constructively in R.

6 The deformation argument for term orders of mixed type

For Gröbner bases there exists a deformation over $\mathbf{A}^1$ connecting S/I as the general fiber with $S/in(I)$ as the special fiber, see (Bayer 1982). It proved to be useful many times.

There is a natural extension of this result, previously investigated mainly for local term orders, see e.g. (Gräbe 1991). (Grassmann *et al.* 1994, prop 5.3.) generalize the flatness argument to arbitrary term orders using a straightforward generalization of the original ideas and draw some conclusions about the dimension and, for zero dimensional ideals and modules, the multiplicity of $Loc(S)/I$ in terms of $Loc(S)/in(I)$.

Below we discuss the deformation argument from another point of view, using its connection to homogenizations of (local) rings. This approach also applies to arbitrary term orders of mixed type. Different to (Grassmann *et al.* 1994) it uses *homogeneous* localization and connects $Loc(S)/I$ with $S/in(I)$.

6.1 The deformation

Given $I \subset S$ assume that $(I, <)$ has a standard set $B = STB(I)$, that is strongly supported by w. Consider the homogenization ${}^h : S \longrightarrow S[t]$ with respect to w, i.e. $TO(S[t]) = TO_w$. By definition we get $in(I) \cdot S[t] = in({}^hI) = \langle in(B) \rangle \cdot S[t]$.

In the spirit of (Goto,Watanabe 1978) one can develop a theory of homogeneous localizations over $S[t]$ (wrt. w). More precisely, if U is the set of units $U(S)$ for S then let $U(t) := \{{}^h u \ : \ u \in U\}$ be the set of ($w-$)homogeneous units for $S[t]$. Define $S(t) = H\text{-}Loc(S[t]) := U(t)^{-1} S[t]$. This localization is w-homogeneous, too, assuming $w(t) = 1$. Set $I(t) := {}^h I$ and $R(t) := S(t)/I(t)$.

Proposition 6 *Under these assumptions for $B := STB(I)$ the set ${}^h B$ is a standard basis of ${}^h I$ in H-Loc($S[t]$), t and $t-1$ (and more generally $t-c$ for $c \in k$) are nonzero divisors on $R(t)$, and*

$$R(c) := R(t)/(t-c) \quad \cong \quad \begin{cases} Loc(S)/I & \text{for } c \neq 0 \\ S/in(I) & \text{for } c = 0. \end{cases}$$

Proof: By the special choice of w we get for $f = \sum c_a x^a \in I$ that $max\{w(a) : c_a \neq 0\} = w(deg\ f)$ and hence

$${}^h f = \sum c_a x^a \cdot t^{w(deg\ f) - w(a)}.$$

If $ef = \sum r_k f_k$ ($e \in U, r_k \in S, f_k \in B$) is a standard representation of f in $Loc(S)$ this implies immediately that

$${}^h e \ {}^h f = \sum {}^h r_k \ {}^h f_k \, t^{w(deg\ f) - w(deg\ r_k f_k)}$$

is a standard representation of ${}^h f$ in H-Loc($S[t]$).

The other assertions are obvious. $\square$

As in (Grassmann *et al.* 1994) this generalizes immediately the following well known fact to arbitrary term orders of possibly mixed type :

Proposition 7 *R(0) and R(1) have equal dimension, and, in the case of tangent cone orderings, their Hilbert series also coincide.*

For local term orders $R(1)$ is a local ring and w can be chosen to have only negative weights. In (Gräbe 1991) we exploited a spectral sequence argument over the completion of $R(1)$ to prove even stronger results :

Proposition 8 *For a local term order we conclude*

1. *The Betti numbers of $R(1)$ are bounded above by the Betti numbers of $R(0)$.*
2. *depth $R(1) \geq$ depth $R(0)$,*
3. *If $R(0)$ is Cohen-Macaulay, then $R(1)$ is Cohen-Macaulay, and type $R(1) \leq$ type $R(0)$.*
4. *If $R(0)$ is Gorenstein, then $R(1)$ is Gorenstein.*
5. *If $R(0)$ is a generalized Cohen-Macaulay ring, then $R(1)$ is also.*
6. *grade $I \cdot Loc(S) \geq$ grade $in(I)$.*

In particular this holds for ideals in $k[[x]]_{alg}$ given by a LSS.

For term orders of mixed type there is no obvious completion of $R(1)$ with good properties and $R(1)$ is no more a local ring. As usual, in this situation we can ask for Betti numbers, depth etc. for localizations of $R(1)$ at maximal ideals instead.

Proposition 9 *Let $<$ be an arbitrary term order and R a localization of R(1) at some k-rational point. Then*

1. *The Betti numbers of R are bounded above by the Betti numbers of $R(0)$.*
2. *depth $R \geq$ depth $R(0)$,*
3. *If $R(0)$ is Cohen-Macaulay, then R is Cohen-Macaulay, and type $R \leq$ type $R(0)$.*
4. *If $R(0)$ is Gorenstein, then R is Gorenstein.*

PROOF: $S(t)$ and $R(t)$ are H-local rings since $(t, x_v : v \in V)$ is their unique maximal homogeneous ideal.

Take a minimal homogeneous resolution $F_*(t)$ of $R(t)$ over $S(t)$. Factoring out a nonzero divisor $(t-c)$, $c \in k$, we obtain a free resolution $F_*(c)$ of $R(c)$ over $S(c)$. Moreover, factoring out the homogeneous element t the resolution remains a minimal H-local resolution. Hence $R(t)$ and $R(0)$ have equal Betti numbers. Localizing $F_*(1)$ at a k-rational point we obtain a (not necessarily minimal) free resolution of R over the localization of $S(1)$. Since the residue field is k this proves 1).

2) - 4) are then easy consequences. □

6.2 Independent sets

Let I be an ideal in S. $\sigma \subset V$ is an *(locally) independent set mod I* iff $\{x_v : v \in \sigma\}$ is an algebraically independent set in $R = Loc(S)/I$, i.e.

$$I \cdot Loc(S) \bigcap k[x_v : v \in \sigma] = \emptyset.$$

If $I \subset Loc(S)$ is prime the collection of all independent sets form a matroid and all maximal independent sets are of equal size *dim R*.

In general, it is difficult to find all independent sets. (Kredel,Weispfenning 1988) therefore introduced the notion of strongly independent sets. The following, as given in (Gräbe 1993b) may serve as a general definition: $\sigma \subset V$ is a *strongly independent set mod I* iff it is an independent set *mod in*(I).

Strongly independent sets are independent sets also in our more general setting : If $f \in I \cdot Loc(S) \bigcap k[x_v : v \in \sigma]$ is a nonzero polynomial then $in(f) \in in(I) \bigcap k[x_v : v \in \sigma]$ would be a nonzero term. Since R and $S/in(I)$ have equal dimension we obtain as in the noetherian case:

Proposition 10 *dim $Loc(S)/I$ is the maximal possible size of a strongly independent set mod I.*

See (Gräbe 1993b) for a discussion of algorithms to find all maximal strongly independent sets.

The deformation argument extended in the preceding section to our more general setting is the main tool for proving connections between I and $in(I)$ in (Gräbe 1993b). Hence these results transfer to arbitrary term orders :

Proposition 11 *If $I \cdot Loc(S)$ is (radically) unmixed (e.g. Cohen-Macaulay) then $in(I)$ is radically unmixed and every maximal (with respect to inclusion) strongly independent set has equal size.*

In particular, under this assumption dim $Loc(S)/I$ can be determined from $in(I)$ in linear time (w.r.t the embedding dimension).

The proof is the same as (Gräbe 1993b, thm.1).

Acknowledgment: The author thanks the anonymous referee for pointing out to him a misunderstanding of the deformation argument in the final version of (Grassmann *et al.* 1994).

References

[1] Alonso M., Mora T., Raimondo M. (1989). Computing with algebraic series. In *Proc. ISSAC'89*. ACM Press, 101–111.

[2] Alonso M., Mora T., Raimondo M. (1991). Local decomposition algorithms. In *Proc. AAECC Tokyo 1990, L.N.C.S.* **508**, 208–221.

[3] Alonso M., Mora T., Raimondo M. (1992). A computational model for algebraic power series. *J. Pure Applied Alg.* **77**, 1–38.

[4] Bayer D.A. (1982). *The division algorithm and the Hilbert scheme.* Thesis, Harvard Univ.

[5] Becker T. (1990). Stability and Buchberger criterion for standard bases in power series rings. *J. Pure Appl. Alg.* **66**, 219–227.

[6] Becker T., Weispfenning V., Kredel H. (1993). *Gröbner bases. A computational approach to commutative algebra.* New York: Springer.

[7] Buchberger B. (1988). Applications of Gröbner bases in non-linear computational geometry. In *Trends in computer algebra (Bad Neuenahr), L.N.C.S.* **296**, 52–80.

[8] Gianni P., Trager B., Zacharias G. (1988). Gröbner bases and primary decomposition of polynomial ideals. *J. Symb. Comp.* **6**, 149–167.

[9] Goto S., Watanabe K. (1978). On graded rings, I. *J. Math. Soc. Japan* **30**, 179–213.

[10] Gräbe H.-G. (1991). Homology modules and standard bases. *Beitr. Alg. Geom.* **32**, 11–20.

[11] Gräbe H.-G. (1993a). CALI—A REDUCE package for commutative algebra, version 2.2. Available through the REDUCE library `redlib@rand.org`.

[12] Gräbe H.-G. (1993b). Two remarks on independent set. *J. Alg. Comb.* **2**, 137–145.

[13] Gräbe H.-G. (1994). The tangent cone algorithm and homogenization. *J. Pure Appl. Alg.* **97**, 303–312.

[14] Grassmann H., Greuel, G.-M., Martin, B., Neumann, W., Pfister, G., Pohl, W., Schönemann, H., Siebert, T. (1994). Standard bases, syzygies, and their implementation in SINGULAR. In *Beiträge zur angewandten Analysis und Informatik*, Shaker, Aachen, 69–96.

[15] Kredel H., Weispfenning V. (1988). Computing dimension and independent sets for polynomial ideals. *J. Symb. Comp.* **6**, 231–247.

[16] Lazard D. (1983). Gröbner bases, Gaussian elimination, and resolution of systems of algebraic equations. In *Proc. EUROCAL'83, L.N.C.S.* **162**, 146–156.

[17] Mora T. (1982). An algorithm to compute the equations of tangent cones. In *Proc. EUROSAM-82, L.N.C.S.* **144**, 24–31.

[18] Mora T. (1988). Seven variations on standard bases. Unpublished preprint, Univ. Genova.

[19] Mora T., Robbiano L. (1988). The Gröbner fan of an ideal. *J. Symb. Comp.* **6**, 183–208.

[20] Mora T., Pfister G., Traverso C. (1992). An introduction to the tangent cone algorithm. In *Issues in non-linear geometry and robotics, C.M. Hoffmann ed.*. JAI Press.

[21] Robbiano L. (1986). On the theory of graded structures. *J. Symb. Comp.* **2**, 139–170.