An Algorithm for Constructing Detaching Bases in the Ring of Polynomials over a Field

Franz Winkler
Institut für Mathematik
Arbeitsgruppe CAMP
Johannes Kepler Universität
A-4040 Linz, Austria

Abstract

Most ideal theoretic problems in a polynomial ring are extremely hard to solve, if the ideal is given by an arbitrary basis. B. Buchberger, 1965, was the first to show that for polynomials over a field it is possible to construct a "detaching" basis from a given arbitrary one, such that the problems mentioned above become easily soluble. Other authors (e.g. M. Lauer, 1976, and S.C. Schaller, 1979) have considered different coefficient domains. In this paper we investigate a method, developed by C.Sims and C.Ayoub, for constructing "detaching" bases in the ring of polynomials over $\mathbb{Z}$, where the power products are ordered lexicographically. We show that the method also works for polynomials over a field, with only weak conditions on the ordering of the power products. New proofs of correctness and termination are presented. Furthermore we are able to improve the complexity behaviour of Ayoub's algorithm for the case of polynomials over a field.

1. Introduction and problem specification

Let K be a field. Then $K[x_1,\dots,x_n]$, the ring of polynomials over K in n indeterminates, is a Noetherian ring [vdW70]. This means that every ideal I in $K[x_1,\dots,x_n]$ is generated by a finite basis F (I=ideal(F)). If we are given a finite basis F for an ideal I in $K[x_1,\dots,x_n]$, a great number of problems still remain extremely difficult to solve. Among these problems are the problem of deciding whether a given polynomial belongs to I, the problem of deciding whether the polynomial ideal has dimension zero, the reduction of polynomials to canonical forms with respect to the ideal I and many more (compare [Wi78]). Therefore it is essential to compute from the basis F a "detaching" basis G, such that G generates the same ideal as F, but G makes the solutions of these problems easy.

In the following we assume that we have a total linear ordering $<_t$ on pp_n, the set of power products of the indeterminates $x_1,\dots,x_n$, which satisfies the two conditions

(T1) $1=x_1^0 \dots x_n^0 <_t p$ for all $p \in pp_n$ and

(T2) $p \cdot q_1 <_t p \cdot q_2$ for all $p, q_1, q_2 \in pp_n$ such that $q_1 <_t q_2$.

These two conditions imply that $<_t$ is a Noetherian relation on pp_n.

Throughout this paper we use the following notations. If p is the power product $x_1^{e_1} \dots x_n^{e_n}$ in pp_n and $i \in \mathbb{N}$ then by $\mathrm{rear}_i(p)$ we denote the power product $x_i^{e_i} \dots x_n^{e_n}$ (if $i>n$ then $\mathrm{rear}_i(p)=1$), and by $\deg_i(p)$ we denote e_i, the degree of p in x_i.

If f is a nonzero polynomial in $K[x_1,\dots,x_n]$, then ldpp(f) is the greatest power product in pp_n which has a nonzero coefficient in f. ldc(f) is the coefficient of ldpp(f). ldt(f)=ldc(f)ldpp(f). red(f)=f-ldt(f).

Following Buchberger's notation, for an arbitrary subset F of $K[x_1,\dots,x_n]$ we define a <u>reduction relation</u> $\xrightarrow[1,F]{}$ on $K[x_1,\dots,x_n]$:

$f \xrightarrow[1,F]{} g$ iff there is a power product p, which occurs with coefficient $a \neq 0$ in f, and a nonzero polynomial h in F such that p is a multiple of ldpp(h) and

$$g = f - \frac{a}{\mathrm{ldc}(h)} \cdot \frac{p}{\mathrm{ldpp}(h)} \cdot h.$$

By $\xrightarrow[F]{}$ we denote the reflexive transitive closure of $\xrightarrow[1,F]{}$.

$\xrightarrow[1,F]{}$ is a Noetherian relation, so a chain of reductions starting with a polynomial f terminates with some g such that g cannot be reduced further. In this case we say that g is a <u>simplified version</u> of f with respect to F. Clearly $g \equiv f$ modulo the ideal generated by F.

We say that $f \in K[x_1,\dots,x_n]$ is <u>reduction unique</u> with respect to F if there is a unique simplified version of f w.r.t. F.

If every $f \in K[x_1,\dots,x_n]$ is reduction unique w.r.t. F
then we call F a <u>detaching basis</u> (Gröbner-basis or complete basis)
for ideal(F).

<u>Lemma 1.1</u>: Let F be a finite subset of $K[x_1,\dots,x_n]$. If for every polynomial f in ideal(F) $f \xrightarrow[F]{} 0$ then F is a detaching basis for ideal(F).

In [Bu65], [Bu70], and [Bu76] B.Buchberger presented an algorithm for constructing a detaching basis G for an ideal I in $K[x_1,\dots,x_n]$, for which some basis F is given. The main step in this algorithm is to take two polynomials f and g in the basis, compute the least common multiple p of ldpp(f) and ldpp(g), reduce p to some h_1 using f and to some h_2 using g and compute simplified versions h_1' and h_2' of h_1 and h_2. If $h_1' \neq h_2'$ the new polynomial $h_1'-h_2'$ is added to the basis.

Other authors ([La76a], [La76b], [Sc79]) have considered different coefficient domains. In [Si78] C.Sims presented an algorithm for constructing a basis for an ideal in $\mathbb{Z}[x]$, which allows to decide whether a given polynomial is contained in the ideal.

His work was extended to multivariate polynomials over $\mathbb{Z}$ by C.Ayoub in [Ay80]. Ayoub proves her result only for the case where $<_t$ is the lexicographic ordering on the power products. This ordering is sufficient for deciding whether a given polynomial is contained in an ideal I. But when detaching bases should be used for simplifying polynomials with respect to polynomial side relations, it is desirable to have a wider range of possible definitions of the notion of "simpler" to choose from.

We present an algorithm for computing detaching bases for polynomial ideals in $K[x_1,\ldots,x_n]$, where the underlying ordering $<_t$ on the power products has to satisfy only the two conditions (T1) and (T2). Detailed proofs of the various lemmata can be found in [Wi82].

We hope that this paper helps to understand the relations between Buchberger's and Ayoub's algorithms for completing bases for polynomial ideals.

2. A first algorithm for constructing detaching bases

A finite set F of polynomials in $K[x_1,\ldots,x_n]$ is called *staggered*, if $0 \notin F$ and for $f,g \in F$, $f \neq g$, we have $\mathrm{ldpp}(f) \neq \mathrm{ldpp}(g)$.

Lemma 2.1: For every finite set of polynomials F in $K[x_1,\ldots,x_n]$, a finite set of polynomials G can be constructed, such that ideal(F)=ideal(G) and G is staggered.

Proof: Let F' be F-{0}. As long as there are two different polynomials f,g in F' with $\mathrm{ldpp}(f)=\mathrm{ldpp}(g)$, we carry out the following process:
compute $h=f-(\mathrm{ldc}(f)/\mathrm{ldc}(g)).g$. If h=0 then delete f from F'. Otherwise replace f by h in F'.
Obviously the ideal generated by F' remains unchanged during this process.
The process terminates after a finite number of steps, since the leading power products of the polynomials in F' decrease with respect to the Noetherian ordering $<_t$.
Finally we get a set of polynomials F' which generates the same ideal as F and is staggered. So we let G=F'. ●

For a finite,staggered set F in $K[x_1,\ldots,x_n]$ we define the following *tower of admissible pairs* in $pp_n \times K[x_1,\ldots,x_n]$:

$F^{[0]} := \{(1,f) \mid f \in F\}$ and for $1<i<n$

$F^{[i]} := F^{[i-1]} \cup \{(p.x_i{}^s,f) \mid (p,f) \in F^{[i-1]},\ \max(f,F,i),\ s \in \mathbb{N}\}$,

where $\max(f,F,i)$ iff $(\forall g \in F)(\mathrm{rear}_{i+1}(\mathrm{ldpp}(g))=\mathrm{rear}_{i+1}(\mathrm{ldpp}(f)) \Longrightarrow$
$\mathrm{deg}_i(\mathrm{ldpp}(g)) < \mathrm{deg}_i(\mathrm{ldpp}(f))$).

For the proof of the main theorem we will need the following lemmata.

Lemma 2.2: Let F be a finite, staggered subset of $K[x_1,\dots,x_n]$. $p,q \in pp_n$, $f \in F$. If $(p,f),(q,f) \in F^{[n]}$ then $(p.q,f) \in F^{[n]}$.

Lemma 2.3: Let F be a finite, staggered subset of $K[x_1,\dots,x_n]$, $f \in F$, $1<m<n$, $(q,g) \in F^{[n]}$, $f \neq g$ and $ldpp(x_m.f)=ldpp(q.g)$. Then the exponents of $x_m,\dots,x_n$ in q are 0.

Based on $F^{[n]}$ we define the set of reductors $F^{(n)}$ by $F^{(n)}=\{p.f \mid (p,f) \in F^{[n]}\}$.

Lemma 2.4: Let F be a finite, staggered subset of $K[x_1,\dots,x_n]$. Then $F^{(n)}$ is also staggered.

By $mod_K(F)$ let us denote the K-module generated by F for any $F \subseteq K[x_1,\dots,x_n]$, i.e. $mod_K(F) = \{ a_1f_1+\dots+a_mf_m \mid \text{for } m \in \mathbb{N}_0,\ a_1,\dots,a_m \in K,\ f_1,\dots,f_m \in F \}$. Now we are ready to state the fundamental theorem for the construction of detaching bases.

Theorem 2.1: Let F be a finite, staggered subset of $K[x_1,\dots,x_n]$.
Then the following two assertions are equivalent:
(i) $x_i.f \in mod_K(F^{(n)})$ for all $f \in F$, $1<i<n$,
(ii) $p.f \in mod_K(F^{(n)})$ for all $f \in F$, $p \in pp_n$.

Proof: Obviously (ii) implies (i), since (i) is a special case of (ii).
It remains to show that (i) implies (ii). This we prove by induction on $ldpp(p.f)$ with respect to the Noetherian relation $<_t$.
Suppose that for some $p^* \in pp_n$ we know that
(IH1) if $ldpp(p.f) <_t p^*$ then $p.f \in mod_K(F^{(n)})$ for all $f \in F$, $p \in pp_n$.
From the induction hypothesis (IH1) we have to show
(1) if $ldpp(p.f)=p^*$ then $p.f \in mod_K(F^{(n)})$ for all $f \in F$, $p \in pp_n$.
We prove (1) by induction on p with respect to the lexicographic ordering $<_l$ on pp_n (which is a Noetherian relation).
Suppose that for some $\underline{p} \in pp_n$ we know that
(IH2) if $p <_l \underline{p}$ and $ldpp(p.f) = p^*$ then $p.f \in mod_K(F^{(n)})$
for all $f \in F$, $p \in pp_n$.
From the induction hypothesis (IH2) we have to show
(2) if $ldpp(\underline{p}.f) = p^*$ then $\underline{p}.f \in mod_K(F^{(n)})$ for all $f \in F$.
If for all indices m, $1<m<n$, such that $deg_m(\underline{p}) \neq 0$ we have $(x_m,f) \in F^{[n]}$, then by lemma 2.2 $(\underline{p},f) \in F^{[n]}$ and hence $\underline{p}.f \in F^{(n)} \subseteq mod_K(F^{(n)})$.
Otherwise there is an index m, $1<m<n$, such that $deg_m(\underline{p}) \neq 0$ and $(x_m,f) \notin F^{[n]}$.
Because of (i) we have $x_m.f \in mod_K(F^{(n)})$, i.e. there are $l \in \mathbb{N}$, $a_1,\dots,a_l \in K-\{0\}$. $g_1,\dots,g_l \in F^{(n)}$ such that

$$x_m.f = \textstyle\sum_{j=1}^{l} a_j.g_j \quad \text{and } g_i \neq g_k \text{ for } i \neq k.$$

Because of lemma 2.4 $ldpp(g_i) \neq ldpp(g_k)$ for $i \neq k$. W.l.o.g. we assume $ldpp(g_j) <_t ldpp(g_1)$ for $1<j<l$.

$$\underline{p}\cdot f = (\underline{p}/x_m)\cdot x_m\cdot f = a_1\cdot(\underline{p}/x_m)\cdot g_1 + \textstyle\sum_{j=2}^{l} a_j\cdot(\underline{p}/x_m)\cdot g_j.$$

All the power products occurring in $\sum_{j=2}^{l} a_j\cdot(\underline{p}/x_m)\cdot g_j$ are less than p^* (here we need the property (T2) of $<_t$), so by the induction hypothesis (IH1)

$$\textstyle\sum_{j=2}^{l} a_j\cdot(\underline{p}/x_m)\cdot g_j \;\varepsilon\; \mathrm{mod}_K(F^{(n)}).$$

So it remains to show that $(\underline{p}/x_m)\cdot g_1 \;\varepsilon\; \mathrm{mod}_K(F^{(n)})$.
$g_1=q\cdot g$ for some $(q,g) \;\varepsilon\; F^{[n]}$, where by lemma 2.3 $\deg_r(q)=0$ for $m<r<n$.
Now we set $q'=(\underline{p}/x_m)\cdot q$ and get $(\underline{p}/x_m)\cdot g_1 = q'\cdot g$.
But $q' <_1 \underline{p}$, so by the induction hypothesis (IH2)

$$(\underline{p}/x_m)\cdot g_1 = q'\cdot g \;\varepsilon\; \mathrm{mod}_K(F^{(n)}).$$

This completes the proof of (2),(1) and (i) ==> (ii). •

Now it is easy to show that condition (i) in theorem 2.1 is equivalent to $\mathrm{mod}_K(F^{(n)})=\mathrm{ideal}(F)$. Using this equivalence together with lemma 1.1 one can prove that (i) is a sufficient condition for F being a detaching basis.

• <u>Theorem 2.2</u>: Let F be a finite, staggered subset of $K[x_1,\dots,x_n]$.
• If $x_i\cdot f \;\varepsilon\; \mathrm{mod}_K(F^{(n)})$ for all $1<i<n$, $f \;\varepsilon\; F$, then F is a detaching basis
• for ideal(F).

For a set of polynomials F in $K[x_1,\dots,x_n]$ we introduce the notion of <u>restricted reducibility</u> modulo F: $f \xrightarrow[1,r,F]{} g$ iff there is a power product p, which occurs with coefficient $a\neq 0$ in f, and a polynomial $h \;\varepsilon\; F$ such that $p=\mathrm{ldpp}(h)$ and

$$g = f - \frac{a}{\mathrm{ldc}(h)}\cdot h.$$

By $\xrightarrow[r,F]{}$ we denote the reflexive transitive closure of $\xrightarrow[1,r,F]{}$.
$\xrightarrow[1,r,F]{}$ is a Noetherian relation, so a chain of reductions of a polynomial f has to terminate with some g, such that g cannot be reduced further. In this case we say that g is a <u>restricted simplified version</u> of f modulo F. Clearly $g \equiv f$ modulo the ideal generated by F.

<u>Lemma 2.5</u>: Let F be a finite, staggered subset of $K[x_1,\dots,x_n]$, $f\varepsilon K[x_1,\dots,x_n]$.
Then $f \;\varepsilon\; \mathrm{mod}_K(F^{(n)})$ if and only if $f \xrightarrow[r,F^{(n)}]{} 0$.

In order to be able to prove the termination of our algorithm, we need to introduce the notion of triangularity: a staggered subset F of $K[x_1,\dots,x_n]$ is called <u>triangular</u> iff for all $f \;\varepsilon\; F$, $1<i<n$ there exists a polynomial g in $F^{(n)}$ such that $\mathrm{ldpp}(g)=\mathrm{ldpp}(x_i\cdot f)$.

<u>Lemma 2.6</u>: If F is a finite, staggered subset of $K[x_1,\dots,x_n]$, then in finitely many steps a finite, triangular subset G of $K[x_1,\dots,x_n]$ can be constructed such that ideal(F)=ideal(G).

Proof: Initially we let G be F. As long as there are $f \in G$, $1<i<n$ such that there is no $g \in G^{(n)}$ with $\mathrm{ldpp}(g)=\mathrm{ldpp}(x_i.f)$, we add $x_i.f$ to G.
The process terminates, since for every k, $1<k<n$, no polynomial h is added such that $\deg_k(\mathrm{ldpp}(h)) > \max\{\deg_k(\mathrm{ldpp}(g)) \mid g \in F\}$. ●

<u>Lemma 2.7</u>: If F is triangular, then for every $p \in pp_n$, $f \in F$, there is a $g \in F^{(n)}$ such that $p.\mathrm{ldpp}(f)=\mathrm{ldpp}(g)$.

<u>Lemma 2.8</u>: If F is a finite, triangular subset of $K[x_1,\ldots,x_n]$ and the nonzero polynomial h is irreducible modulo ${}_{1,r,F^{(n)}}$, then there is no $f \in F$ such that ldpp(h) is a multiple of ldpp(f).

Now we can state a first version of the algorithm for constructing a detaching basis G for ideal(F):

```
G ← detbl(F)
[Algorithm for constructing a detaching basis, 1.version. F is a finite subset
of $K[x_1,\ldots,x_n]$. G is a finite detaching basis for ideal(F)]
(1) Let G be a finite, triangular basis for ideal(F);
    [an algorithm for constructing such a basis can be extracted from the
    proofs of lemma 2.1 and lemma 2.6]
(2) Set $C \leftarrow \{(i,f) \mid 1<i<n,\ f\in G,\ (x_i,f)\notin G^{[n]}$ and $x_i.f \notin G\}$;
(3) while  $C \neq \emptyset$  do
        {Choose (i,f) ε C;
         Let h be a restricted simplified version of $x_i.f$ modulo $G^{(n)}$;
         [an algorithm is given in [Ay80]]
         if  $h \neq 0$  then  {Set $G' \leftarrow G \cup \{h\}$;
                                Let G be a finite, triangular basis for ideal(G');
                                Set $C \leftarrow \{(i,f) \mid 1<i<n,\ f\in G,\ (x_i,f)\notin G^{[n]}$ and $x_i.f \notin G\}$;
                     else  Delete (i,f) from C };
    return  ●
```

The correctness of the algorithm follows from theorem 2.2 and lemma 2.5. Now let us consider the problem of termination. If detbl would not terminate, this would mean that it continuously adds polynomials $h_1,h_2,\ldots$ to the basis, where by lemma 2.8 no h_i is a multiple of some $h_1,\ldots,h_{i-1}$. Such a sequence of polynomials, however, cannot exist [Bu70]. So detbl has to terminate.

A rather annoying property of detbl is that whenever a new polynomial is added to the basis G in (3), then all the reductions of pairs (i,f) done so far are rendered useless and $x_i.f$ has to be reduced anew. This is because adding a new polynomial to the basis may totally destroy the structure of $G^{(n)}$. So it would be desirable to modify the basic concept in such a way that each pair (i,f) must be considered only once.

3. Improvement of the algorithm

The cost for improving detbl has to be paid in notational complexity. There are two major changes in notation. Firstly we consider sequences of polynomials rather than sets of polynomials, i.e. we consider "ordered" bases. Secondly the set of reductors $F^{(n)}$ for a basis F is defined somewhat differently, so that adding new polynomials to F does not destroy the structure of $F^{(n)}$ but merely add new reductors.

We define staggeredness for sequences of polynomials as in chapter 2 - a sequence of polynomials in $K[x_1,\dots,x_n]$ is called staggered if every element of F occurs only once in F and the set of elements in F is staggered - and again we can prove that for every finite sequence F of polynomials in $K[x_1,\dots,x_n]$ in finitely many steps a finite staggered sequence G can be constructed such that F and G generate the same ideal.

A *substitution* σ is a mapping from $\{0,x_1,\dots,x_n\}$ into $\mathbb{N}_0$ such that $\sigma(0)=0$.

Let $(a,f),(b,g)$ be pairs in $X_n \times K[x_1,\dots,x_n]-\{0\}$, where X_n is the set $\{(a_1,\dots,a_n) \mid a_i=0 \text{ or } a_i=x_i \text{ for } 1<i<n\}$. We say that (a,f) and (b,g) are *unifiable*, if there are substitutions σ_f and σ_g such that
$x_1^{\sigma_f(a_1)}\dots x_n^{\sigma_f(a_n)}.\mathrm{ldpp}(f) = x_1^{\sigma_g(b_1)}\dots x_n^{\sigma_g(b_n)}.\mathrm{ldpp}(g)$.

For a finite, staggered sequence of polynomials F in $K[x_1,\dots,x_n]$ we define the *sequence of multipliers* $F^{\sim}$ as follows:
if $\mathrm{length}(F)=0$ then $F^{\sim}=()$. If $F=G\circ h$ then $F^{\sim}=G^{\sim}\circ(a_1,\dots,a_n)$, where for $1<k<n$ $a_k=x_k$ if $\max(h,F,k)$ and $(G^{\sim}{}_j,G_j)$ and $((a_1,\dots,a_{k-1},x_k,0,\dots,0),h)$ are not unifiable for $1<j<\mathrm{length}(G)$, and $a_k=0$ otherwise. ($\circ$ denotes the operation of adding a last element to a sequence.)

The *set of reductors* F^* for a finite, staggered sequence of polynomials F is defined as $F^*=\{p.F_j \mid (p,j) \in F^{\approx}\}$, where
$F^{\approx}=\{(x_1^{\sigma(a_1)}\dots x_n^{\sigma(a_n)},j) \mid (a_1,\dots,a_n)=F^{\sim}{}_j,\ \sigma \text{ a substitution},\ 1<j<\mathrm{length}(F)\}$.

Lemma 3.1: Let F be a finite, staggered sequence in $K[x_1,\dots,x_n]$, $p,q \in pp_n$, $1<j<\mathrm{length}(F)$.
If $(p,j),(q,j) \in F^{\approx}$ then $(p.q,j) \in F^{\approx}$.

A staggered sequence F in $K[x_1,\dots,x_n]$ is called *unambiguous* if
$(\forall (p,j),(q,k) \in F^{\approx})\ ((p,j)\neq(q,k) \Longrightarrow p.\mathrm{ldpp}(F_j)\neq q.\mathrm{ldpp}(F_k))$.

Lemma 3.2: Let F be a finite, unambiguous sequence in $K[x_1,\dots,x_n]$, h a nonzero polynomial in $K[x_1,\dots,x_n]$ such that there is no $g \in F^*$ with $\mathrm{ldpp}(h)=\mathrm{ldpp}(g)$.
Then $F\circ h$ is unambiguous.

Lemma 3.3: Let F be a finite staggered sequence of polynomials in $K[x_1,\dots,x_n]$.
Then there is a permutation π such that $(F_{\pi(1)},\dots,F_{\pi(\mathrm{length}(F))})$ is unambiguous.

Proof: We induct on l=length(F). For $l=0$ F is already unambiguous.
Now let $l>1$. We choose $j \in \{1,\dots,l\}$ such that ldpp(F_j) is not a multiple of any ldpp(F_i) for $1<i<l$, $i \neq j$. Let $F'=(F_1,\dots,F_{j-1},F_{j+1},\dots,F_l)$. By the induction hypothesis there is a reordering G' of F' such that G' is unambiguous.
So $G=G' \circ F_j$ is a reordering of F and by lemma 3.2 G is unambiguous. •

Lemma 3.4: Let F be a finite, unambiguous sequence of polynomials in $K[x_1,\dots,x_n]$.
Then F^* is a staggered set of polynomials.

Again we define the notion of triangularity: an unambiguous sequence F is called triangular if for all i,j, $1<i<n$, $1<j<$length(F), there exists a pair $(q,k) \in F^{=}$, $k<j$, such that ldpp($x_i \cdot F_j$)=ldpp($q \cdot F_k$).

Lemma 3.5: Let F be a finite, triangular sequence in $K[x_1,\dots,x_n]$, h a nonzero polynomial in $K[x_1,\dots,x_n]$ such that there is no $g \in F^*$ with ldpp(h)=ldpp(g), and m such that $\deg_m$(ldpp(h)) > max$\{\deg_m$(ldpp(F_i)) $\mid 1<i<$length(F)$\}$.
Then (x_m,length(F)+1) $\in (F \circ h)^{=}$ and $F \circ h$ is unambiguous.

Lemma 3.6: Let F be a finite triangular sequence in $K[x_1,\dots,x_n]$, h a nonzero polynomial in $K[x_1,\dots,x_n]$ such that there is no $g \in F^*$ with ldpp(h)=ldpp(g).
Then there are polynomials $h_1,\dots,h_m \in K[x_1,\dots,x_n]$, $h_m=h$, such that $G=F \circ h_1 \circ \dots \circ h_m$ is triangular and ideal($F \circ h$)=ideal(G).

Proof: Let $g=h$. As long as there is an index m such that there is no $f \in (F \circ g)^*$ with ldpp($x_m \cdot g$)=ldpp(f), set $g=x_m \cdot g$. The process terminates, since by lemma 3.5 $\deg_m$(ldpp(g)) cannot surpass max$\{\deg_m$(ldpp(h)),max$\{\deg_m(F_i) \mid 1<i<$length(F)$\}\}$.
By lemma 3.2 $F \circ g$ is unambiguous. F is triangular and for every i, $1<i<n$, there is a $(p,j) \in (F \circ g)^{=}$ with ldpp($x_i \cdot g$)=ldpp($p \cdot (F \circ g)_j$), so $F \circ g$ is triangular. So we let $h_1=g$.
Iterating this process we get the desired $h_2,\dots,h_m$.
Clearly ideal($F \circ h$)=ideal(G). •

Lemma 3.7: Let F be a finite, unambiguous sequence in $K[x_1,\dots,x_n]$.
Then there is a finite, triangular sequence G such that every polynomial in G is a multiple of some polynomial in F and ideal(G)=ideal(F).

Proof: Because of the proof of lemma 3.3 we may assume that ldpp(F_j) is not a multiple of ldpp(F_i) for $1<i<j<$length(F).
We induct on l=length(F). If $l=0$ then obviously F is triangular.
So let $l>1$. For $F'=(F_1,\dots,F_{l-1})$ by the induction hypothesis there is a finite, triangular sequence G' such that every polynomial in G' is a multiple of some polynomial in F' and ideal(G')=ideal(F'). By lemma 3.6 there are multiples $h_1,\dots,h_m$ of F_l such that $G=G' \circ h_1 \circ \dots \circ h_m$ is triangular and ideal(G)=ideal(F). •

Lemma 3.8: Let F be a finite, triangular sequence in $K[x_1,\dots,x_n]$.
Then for every $p \in pp_n$, $1<j<\text{length}(F)$ there is a pair $(q,F_k) \in F^{\approx}$, $k<j$, such that $\text{ldpp}(p.F_j)=\text{ldpp}(q.F_k)$.

Lemma 3.9: Let F be a finite, triangular sequence in $K[x_1,\dots,x_n]$ and h a nonzero polynomial in $K[x_1,\dots,x_n]$ such that there is no $g \in F^*$ with $\text{ldpp}(h)=\text{ldpp}(g)$.
Then there is no j, $1<j<\text{length}(F)$, such that $\text{ldpp}(h)$ is a multiple of $\text{ldpp}(F_j)$.

With these new notations, a theorem analogous to theorem 2.1 holds.

Theorem 3.1: Let F be a finite, triangular sequence in $K[x_1,\dots,x_n]$.
Then the following two assertions are equivalent:
(i) $x_i.F_j \in \text{mod}_K(F^*)$ for all $1<j<\text{length}(F)$, $1<i<n$,
(ii) $p.F_j \in \text{mod}_K(F^*)$ for all $1<j<\text{length}(F)$, $p \in pp_n$.

Proof: Obviously (ii) implies (i), since (i) is a special case of (ii).
It remains to show that (i) implies (ii). This we prove by induction on $\text{ldpp}(p.F_j)$ with respect to the Noetherian relation $<_t$.
Suppose that for some $p^* \in pp_n$ we know that
(IH1) if $\text{ldpp}(p.F_j) <_t p^*$ then $p.F_j \in \text{mod}_K(F^*)$ for all $p \in pp_n$, $1<j<\text{length}(F)$.
From the induction hypothesis (IH1) we have to show
(1) if $\text{ldpp}(p.F_j)=p^*$ then $p.F_j \in \text{mod}_K(F^*)$ for all $p \in pp_n$, $1<j<\text{length}(F)$.
We prove (1) by induction on j.
If j=1 then $(p,1) \in F^{\approx}$ and therefore $p.F_1 \in F^* \subseteq \text{mod}_K(F^*)$.
Now suppose that for some j^*, $2<j^*<\text{length}(F)$ we know that
(IH2) if $\text{ldpp}(p.F_j)=p^*$ and $j<j^*$ then $p.F_j \in \text{mod}_K(F^*)$
for all $p \in pp_n$, $1<j<\text{length}(F)$.
From the induction hypothesis (IH2) we have to show
(2) if $\text{ldpp}(p.F_{j^*})=p^*$ then $p.F_{j^*} \in \text{mod}_K(F^*)$ for all $p \in pp_n$.
If for all indices m, $1<m<n$, such that $\deg_m(p)\neq 0$ we have $(x_m,j^*) \in F^{\approx}$, then by lemma 3.1 $(p,j^*) \in F^{\approx}$ and hence $p.F_{j^*} \in F^* \subseteq \text{mod}_K(F^*)$.
Otherwise there is an index m, $1<m<n$, such that $\deg_m(p)\neq 0$ and $(x_m,j^*) \notin F^{\approx}$.
Because of (i) we have $x_m.F_{j^*} \in \text{mod}_K(F^*)$, i.e. there are $l \in \mathbb{N}$, $a_1,\dots,a_l \in K-\{0\}$, $g_1,\dots,g_l \in F^*$ such that

$$x_m.F_{j^*} = \textstyle\sum_{j=1}^{l} a_j.g_j \quad \text{and } g_i \neq g_k \text{ for } i\neq k.$$

Because of lemma 3.4 $\text{ldpp}(g_i)\neq\text{ldpp}(g_k)$ for $i\neq k$. W.l.o.g. we assume $\text{ldpp}(g_j) <_t \text{ldpp}(g_1)$ for all $2<j<l$.

$$p.F_{j^*} = (p/x_m).x_m.F_{j^*} = a_1.(p/x_m).g_1 + \textstyle\sum_{j=2}^{l} a_j.(p/x_m).g_j.$$

All the power products occurring in $\sum_{j=2}^{l} a_j.(p/x_m).g_j$ are less than p^*, so by the induction hypothesis (IH1)

$$\textstyle\sum_{j=2}^{l} a_j.(p/x_m).g_j \in \text{mod}_K(F^*).$$

It remains to show that $(p/x_m).g_1 \in \mathrm{mod}_K(F^*)$.
$g_1=q.F_k$ for some $(q,k) \in F^{\approx}$. Since $\mathrm{ldpp}(x_m.F_{j^*})=\mathrm{ldpp}(q.F_k)$ and F is triangular, k must be less or equal to j^*. But $j^*=k$ is impossible, because $(x_m,j^*) \notin F^{\approx}$. So $k<j^*-1$.
Therefore $(p/x_m).g_1 = (p/x_m).q.F_k \in \mathrm{mod}_K(F^*)$ by the induction hypothesis (IH2).
This completes the proof of (2),(1) and (i) ==> (ii). ●

In analogy to chapter 2 it turns out that (i) in theorem 3.1 is equivalent to $\mathrm{mod}_K(F^*)=\mathrm{ideal}(F)$. Using this equivalence together with lemma 1.1 one can prove that (i) is a sufficient condition for F being a detaching basis.

● Theorem 3.2: Let F be a finite, triangular sequence in $K[x_1,\dots,x_n]$.
● If $x_i.F_j \in \mathrm{mod}_K(F^*)$ for all $1<j<\mathrm{length}(F)$, $1<i<n$, then F is a detaching
● basis for ideal(F).

As in chapter 2 we need a method for deciding whether $f \in \mathrm{mod}_K(F^*)$ for a polynomial f in $K[x_1,\dots,x_n]$ and a finite, triangular sequence F.

Lemma 3.10: Let F be a finite, unambiguous sequence in $K[x_1,\dots,x_n]$ and f a polynomial in $K[x_1,\dots,x_n]$.
Then $f \in \mathrm{mod}_K(F^*)$ if and only if $f \xrightarrow[r,F^*]{} 0$.

Lemma 3.11: Let F be a finite, unambiguous sequence in $K[x_1,\dots x_n]$, h a polynomial in $K[x_1,\dots,x_n]$ such that $\mathrm{ldpp}(h)\neq\mathrm{ldpp}(g)$ for all $g \in F^*$.
If $f_1 \xrightarrow[r,F^*]{} f_2$ then $f_1 \xrightarrow[r,(F\circ h)^*]{} f_2$, for any $f_1,f_2 \in K[x_1,\dots,x_n]$.

Lemma 3.11 is the key observation for reducing every polynomial $x_i.G_j$ only once in the subsequent algorithm for constructing detaching bases.

Now we are ready to state the improved version of the algorithm:

```
G ← detb2(F)
[Algorithm for constructing a detaching basis, 2.version. F is a finite sequence
in $K[x_1,\dots,x_n]$. G is a finite detaching basis for ideal(F)]
(1) Let G be a finite, triangular basis for ideal(F);
    [an algorithm for constructing such a basis can be extracted from the
    proofs of lemma 3.3 and lemma 3.7]
(2) Set $C \leftarrow \{(i,j) \mid 1<i<n,\ 1<j<\mathrm{length}(G),\ (x_i,j)\notin G^{\approx}$ and $x_i.G_j \notin G\}$;
(3) while  $C \neq 0$  do
        {Choose $(i,j) \in C$;
        Let h be a restricted simplified version of $x_i.G_j$ modulo $G^*$;
        if  $h \neq 0$  then  {Construct $h_1,\dots,h_{m-1}$ such that $G'=G\circ h_1\circ\dots\circ h_{m-1}\circ h$ is
                                  a triangular basis for ideal$(G\circ h)$;
                               [use the method described in the proof of lemma 3.6]
```

```
                    Set $C \leftarrow C \cup \{(i,j) \mid 1<i<n,\ length(G)+1<j<length(G)+m,$
                                $(x_i,j) \notin G'^{\approx}$ and $x_i.G'_j \notin G'\}$;
                    Set $G \leftarrow G'\}$;
        Delete $(\underline{i},\underline{j})$ from $C\}$;
    return   ●
```

The correctness of the algorithm follows from theorem 3.2 and lemma 3.10. The proof of termination of detb2 is analogous to the one for detbl. One merely has to use lemma 3.9 instead of lemma 2.8.

Example:

We consider the ideal in $\mathbb{Z}_5[x,y,z]$ which is generated by the set of polynomials

$F = \{ xy^2z + 3x^2z,\ xy^3 + xz + 2y,\ xyz + 2y^2 \}$.

As the linear ordering $<_t$ on the set of power products we choose the graduated lexicographic ordering ([Bu79]).

A detaching basis for ideal(F) is computed first by Buchberger's algorithm GB with criterion 3 (compare [Bu79]) and then by the algorithm detb2.

GB generates the sequence of polynomials (G1)-(G13)

(G1) $xy^2z + 3x^2z$
(G2) $xy^3 + xz + 2y$
(G3) $xyz + 2y^2$
(G4) $y^3 + x^2z$
(G5) $x^3z + 4xz + 3y$
(G6) x^2y^2
(G7) $x^2z + 2xy$
(G8) $x^2y + 3xz + y$
(G9) $xz^2 + xy^2 + 2yz$
(G10) $xz + 2y$
(G11) xy^2
(G12) xy
(G13) y^2.

13.12/2 = 78 S-polynomials have to be considered for reduction, but only 21 reductions have to be carried out according to criterion 3.

The algorithm detb2 generates the sequence of polynomials (G'1)-(G'16)

(G'1) $xy^2z + 3x^2z$
(G'2) $xy^3 + xz + 2y$
(G'3) $xyz + 2y^2$
(G'4) $y^3z + x^2z^2$
(G'5) $y^3 + x^2z$
(G'6) $x^3z + 4xz + 3y$
(G'7) x^2y^2
(G'8) $x^2z + 2xy$
(G'9) $x^2y + 3xz + y$
(G'10) $xz^2 + xy^2 + 2yz$
(G'11) $xz + 2y$
(G'12) xy^2
(G'13) xy
(G'14) y^2z^2
(G'15) y^2z
(G'16) y^2.

23 of the 48 polynomials v.f, $v \in \{x,y,z\}$, $f \in G'$, have to be reduced to normal form during the execution of detb2.

Since the reductions are the most time consuming steps in either GB and detb2, the efficiency of the two algorithms for this example is fairly the same (the two extra reductions in detb2 are counterbalanced by the number of tests for criterion 3 in GB).

Unfortunately, up to now it has not been possible to derive upper bounds on the computing time of detb2. The same is true for Buchberger's algorithm for constructing detaching bases (except for n=2, see [Bu79],[BW79]). One has to wait for an implementation of detb2 in order to be able to compare the run time efficiencies of the two algorithms.

References

[Ay80] C.Ayoub: On Constructing Bases for Ideals in Polynomial Rings over the Integers, Research Report, Dept.Math., Pennsylvania State Univ., 1980

[Bu65] B.Buchberger: Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal, Ph.D. Dissertation, Univ. Innsbruck, 1965

[Bu70] B.Buchberger: Ein algorithmisches Kriterium für die Lösbarkeit eines algebraischen Gleichungssystems, Aequ.math., vol.4/3, pp.374-383, 1970

[Bu76] B.Buchberger: A Theoretical Basis for the Reduction of Polynomials to Canonical Forms, ACM SIGSAM Bull. 39, pp.19-29, Aug.1976

[Bu79] B.Buchberger: A Criterion for Detecting Unnecessary Reductions in the Construction of Gröbner-Bases, Proc. EUROSAM'79, pp.3-21, June 1979

[BW79] B.Buchberger, F.Winkler: Miscellaneous Results on the Construction of Gröbner-Bases for Polynomial Ideals, Techn.Rep. Nr. 137, Inst. f. Math., Univ. Linz, June 1979

[La76a] M.Lauer: Canonical Representatives for Residue Classes of a Polynomial Ideal, Proc. 1976 ACM Symp. on Symbolic and Algebraic Computation, pp.339-345, Aug.1976

[La76b] M.Lauer: Kanonische Repräsentanten für die Restklassen nach einem Polynomideal, Diplomarbeit, Univ. Kaiserslautern, 1976

[Sc79] S.C.Schaller: Algorithmic Aspects of Polynomial Residue Class Rings, Ph.D. Dissertation, Univ. Wisconsin-Madison, 1979

[Si78] C.Sims: The Role of Algorithms in the Teaching of Algebra, in: M.F.Newman (ed.): Topics in Algebra, Springer Lecture Notes in Math., Nr.697, pp.95-107, 1978

[vdW70] B.L.van der Waerden: Modern Algebra, vol.2, New York, Ungar, 1970

[Wi78] F.Winkler: Implementierung eines Algorithmus zur Konstruktion von Gröbner-Basen, Diplomarbeit, Univ. Linz, 1978

[Wi82] F.Winkler: An Algorithm for Constructing Detaching Bases in the Ring of Polynomials over a Field, Techn.Rep. Nr. CAMP 82-20.0, Inst. f. Math., Univ. Linz, December 1982