J. Symbolic Computation (1988) **6**, 275–286

On an Installation of Buchberger's Algorithm

RÜDIGER GEBAUER AND H. MICHAEL MÖLLER†

Springer-Verlag, New York, 175 Fifth Avenue, New York, NY 10010, USA

†FB Mathematic und Informatik, Fernuniversität, D-5800 Hagen 1, FRG

(*Received* 26 *January* 1987, *and in revised form* 23 *October* 1987)

Buchberger's algorithm calculates Groebner bases of polynomial ideals. Its efficiency depends strongly on practical criteria for detecting superfluous reductions. Buchberger recommends two criteria. The more important one is interpreted in this paper as a criterion for detecting redundant elements in a basis of a module of syzygies. We present a method for obtaining a reduced, nearly minimal basis of that module. The simple procedure for detecting (redundant syzygies and) superfluous reductions is incorporated now in our installation of Buchberger's algorithm in SCRATCHPAD II and REDUCE 3.3. The paper concludes with statistics stressing the good computational properties of these installations.

1. Introduction

The concept of Groebner bases for polynomial ideals, introduced first for performing algorithmic computations in residue classes of polynomial rings by Buchberger (1965), now permits the algorithmic solution of a series of problems in polynomial rings and modules and especially the problem of finding all solutions of systems of algebraic equations; for a survey see Buchberger (1985). Buchberger's algorithm for computing Groebner bases is fitted for automatic computation and is installed in nearly all Computer Algebra Systems.

This algorithm is roughly described as follows. Given a finite set F of polynomials, calculate for each pair of polynomials in F a so called S-polynomial and reduce it relatively to F to a polynomial. If this reduced polynomial is not 0, insert it into F. At termination of the algorithm all S-polynomials reduce to 0 and F is a Groebner basis.

The reduction of the S-polynomials is the most time consuming part of the algorithm. Therefore Buchberger developed criteria for predicting reductions to 0, i.e. criteria for avoiding superfluous reductions. There are two types of criteria. The second one depends only on the two polynomials in question (their head terms have to be without common divisors). However, when we apply the first criterion, only very few instances remain, where the second criterion can be used successfully. The first type depends on the pairs considered before. This type is studied in detail by Buchberger (1979); and the most effective criterion of this type together with the second one (and a strategy, which cancels superfluous elements in F) is presented in Buchberger (1985).

The starting point for this paper was the observation, that Groebner bases can be characterized using a basis of its module of syzygies, as already remarked by some authors, for example Bayer (1982), and that reduction strategies to obtain reduced bases from a special basis, the so called Taylor basis, give simpler Groebner basis tests, as

This work was supported by IBM Germany.

0747–7171/88/020275 + 12 $03.00/0

already stated by Möller (1985). In this paper, we present a reduction strategy, which constructs a reduced basis of the module of syzygies (Proposition 3.5). Bayer (1986) assumed that this reduced basis is already irreducible, but this is not true as example 3.6 shows. However our experiences, and the discussion in 3.8, indicate that in only a few instances are all redundant syzygies not detected.

Using the one-to-one correspondence of Taylor basis elements and the pairs for the S-polynomial computation, redundant Taylor basis elements correspond to pairs satisfying a criterion of the first type. This is used to develop a variant of Buchberger's algorithm based on our reduction strategy. The detecting of redundant elements, i.e. the detecting of superfluous reductions, requires only the comparison of exponent vectors of some power products and is for technical reasons splitted into three criteria. These three criteria are very similar to criterion 1 of Buchberger (1985). But they are, in contrast to Buchberger's, independent of the succession of pairs considered before, and each pair detected once as superfluous or already used as a pair for the S-polynomial computation and reduction is no longer needed for subsequent tests of a criterion. This allows more flexibility and leads to a speeding up of the tests of the criteria. The flexibility is also used to implement Buchberger's criterion 2 in an optimal way. Also very important for a fast variant of Buchberger's algorithm is to keep the set F of polynomials as small as possible. Therefore, as in Buchberger's algorithm (1985), whenever a new element is inserted into F, redundant elements of F are cancelled. This is taken into account by a slight modification of the criteria.

The resulting algorithm is already installed in the Computer Algebra Systems SCRATCHPAD II (see Gebauer & Möller, 1987), and REDUCE (release 3.3), (see Hearn, 1987). We illustrate it in detail by an example and compare its complexity in 14 examples with an existing installation of Buchberger's algorithm.

2. Groebner Bases

2.1. Let K be a field and $P = K[x_1, \ldots, x_n]$ the ring of polynomials in $x_1, \ldots, x_n$ over K. T denotes the set of terms (power products) $x_1^{i_1} \ldots x_n^{i_n}$, $i_1, \ldots, i_n$ nonnegative integers. We assume T to be totally ordered by $<_T$, such that

$$(1 :=) x_1^0 \ldots x_n^0 <_T \varphi \quad \text{for all} \quad \varphi \in T \backslash \{1\}$$

$$\varphi_i <_T \varphi_j \Rightarrow \varphi\varphi_i <_T \varphi\varphi_j \quad \text{for all} \quad \varphi, \varphi_i, \varphi_j \in T.$$

For $f = \sum_{i=1}^{m} c(f, \varphi_i)\varphi_i$ with $\varphi_1 <_T \varphi_2 <_T \cdots <_T \varphi_m$ and $c(f, \varphi_i) \in K \backslash \{0\}$, we define as in Möller & Mora (1986)

$$Hcoeff(f) := c(f, \varphi_m), \qquad Hterm(f) := \varphi_m$$

$$M_T(f) := c(f, \varphi_m)\varphi_m.$$

2.2. In the following, F will always be a finite set of polynomials, $F = \{f_1, \ldots, f_r\}$, $0 \notin F$, and *w.l.o.g.* $Hcoeff(f_i) = 1$, $i = 1, \ldots, r$. Mainly for avoiding tedious notations, we define

$$T(i) := Hterm(f_i),$$

$$T(i, j) := lcm\{T(i), T(j)\},$$

$$T(i, j, k) := lcm\{T(i), T(j), T(k)\}.$$

2.3. For polynomials $f \in P\backslash\{0\}$ being represented as in 2.1 Buchberger (1965) introduced the reduction

$$f \xrightarrow[F]{} g \quad (f \text{ reduces to } g \text{ modulo } F)$$

which means

$$g = f - c(f, \varphi_k)\frac{\varphi_k}{T(i)} f_i$$

for appropriate $f_i \in F$ and $k \in \{1, \ldots, m\}$, such that $T(i)$ divides φ_k.

f is called irreducible modulo F, if $f = 0$ or if $f \xrightarrow[F]{} g$ holds for no $g \in P$. Denoting by $\xrightarrow[F]{}^+$ the transitive reflexive closure of $\xrightarrow[F]{}$, Buchberger showed, that $\xrightarrow[F]{}^+$ is Noetherian, i.e. any reduction

$$f \xrightarrow[F]{} g_1 \xrightarrow[F]{} g_2 \xrightarrow[F]{} \cdots$$

is finite: $f \xrightarrow[F]{} g_1 \xrightarrow[F]{} \cdots \xrightarrow[F]{} g_s$, g_s irreducible modulo F.

2.4. DEFINITION. $F = \{f_1, \ldots, f_r\} \subset P\backslash\{0\}$ is called a Groebner basis of $\text{Ideal}(F) := \{\sum_{i=1}^r g_i f_i \mid g_i \in P\}$, if the so called S-polynomials

$$S(f_i, f_j) := \frac{T(i,j)}{T(i)} f_i - \frac{T(i,j)}{T(j)} f_j$$

satisfy $S(f_i, f_j) \xrightarrow[F]{}^+ 0$, $1 \leqslant i < j \leqslant r$.

(Buchberger gives in his publications a different definition for Groebner bases, but he showed already in his thesis (Buchberger, 1965), that the definition given here is equivalent to his one.) There are many equivalent definitions for Groebner bases of ideals (and even for submodules). For instance eleven definitions for ideals and submodules are given in Möller & Mora (1986). In the following, we need only three equivalent characterizations:

2.5. THEOREM. *Let $F = \{f_1, \ldots, f_r\} \subset P\backslash\{0\}$ and $I = \text{Ideal}(F)$. Then the following conditions are equivalent.*

(*C*1) *F is a Groebner basis of I.*

(*C*2) *$M_T(F) = \{T(1), \ldots, T(r)\}$ generates $M_T(I)$, the least ideal containing $M_T(f)$ for all $0 \neq f \in I$.*

(*C*3) *Let L be a basis of the module of syzygies*

$$S^{(1)} := \left\{(h_1, \ldots, h_r) \in P^r \;\middle|\; \sum_{i=1}^r h_i T(i) = 0\right\}.$$

Then for each $(g_1, \ldots, g_r) \in L$

$$\sum_{i=1}^r g_i f_i \xrightarrow[F]{}^+ 0.$$

The proof of $C1 \Leftrightarrow C2$ can be found in Möller & Mora (1986). $C1 \Leftrightarrow C3$ is shown for instance by Möller (1985).

2.6. An element f_i of a Groebner basis F is called redundant, if $F' := F\backslash\{f_i\}$ is also a Groebner basis, and if $\text{Ideal}(F) = \text{Ideal}(F')$. If $\text{Ideal}(F) = \text{Ideal}(F')$ and F is a Groebner

basis, then by $C2$, F' is a Groebner basis too, if and only if a $j \neq i$ exists, such that $T(j)$ divides $T(i)$, i.e. $T(i,j) = T(i)$.

For testing $\text{Ideal}(F) = \text{Ideal}(F')$ in the case $T(i,j) = T(i)$ for a $j \neq i$, it is sufficient to test

$$(S(f_i,f_j) =)f_i - \frac{T(i,j)}{T(j)} f_j \in \text{Ideal}(F').$$

Using the reduction procedure, this holds in the case

$$S(f_i,f_j) \xrightarrow[F]{}{}^{+} 0,$$

or equivalently, since here $Hterm(S(f_i,f_j)) <_T Hterm(f_i)$,

$$S(f_i,f_j) \xrightarrow[F]{}{}^{+} 0.$$

Therefore, if F is a Groebner basis and $T(i,j) = T(i)$ holds for a $j \neq i$, then by the definition of Groebner bases $F' = F \setminus \{f_i\}$ is a Groebner basis of the same ideal. This explains why in Groebner bases redundant elements are cancelled without additional modifications as for instance in Buchberger (1985).

3. A Reduced Basis for the Module Syzygies

3.1. The main tools in this section are the resolution of Taylor (1966) and methods for reducing the bases contained in this resolution. In Möller & Mora (1986), the Taylor resolution and reduction strategies are presented. Since we are dealing here only with the first modules of this resolution, we will not explain the complete technical details and refer the interested reader to the mentioned paper.

3.2. Given terms $T(1), \ldots, T(r)$, we call $(g_1, \ldots, g_r) \in P^r$ homogeneous of degree $\varphi \in T$, if for every $i \in \{1, \ldots, r\}$ a $c_i \in K$ exists, such that $g_i T(i) = c_i \varphi$. Then

$$S^{(1)} := \left\{ (g_1, \ldots, g_r) \in P^r \;\middle|\; \sum_{i=1}^{r} g_i T(i) = 0 \right\}$$

has the Taylor basis $L^{(1)} := \{S_{ij} \mid 1 \leqslant i < j \leqslant r\}$ with

$$S_{ij} := \frac{T(i,j)}{T(i)} e_i - \frac{T(i,j)}{T(j)} e_j$$

homogeneous of degree $T(i,j)$, where e_k is the kth canonical unit vector of P^r. Using this specific basis, $C3 \Rightarrow C1$ of theorem 2.5 is obvious.

3.3. For finding a reduced basis of $S^{(1)}$, we introduce the module of syzygies for $L^{(1)}$. We order the $r(r-1)/2$ syzygies S_{ij} by $<_1$,

$$S_{ij} <_1 S_{kl} :\Leftrightarrow T(i,j) <_T T(k,l) \quad \text{or} \quad (T(i,j) = T(k,l), j \leqslant l, j = l \Rightarrow i < k).$$

Using this order, we denote the canonical kth unit vector in $P^{r(r-1)/2}$ no longer by e_k but by e_{ij}, if S_{ij} is the kth syzygy in this order. For instance let $S_{12} <_1 S_{35} <_1 S_{23}$ be the three first of the S_{ij}, then $e_{12} = (1, 0, \ldots, 0)$, $e_{35} = (0, 1, 0, \ldots, 0)$, $e_{23} = (0, 0, 1, 0, \ldots, 0)$.

The module of syzygies

$$S^{(2)} = \left\{ \sum_{\substack{i,j=1 \\ i<j}}^{r} g_{ij} e_{ij} \in P^{r(r-1)/2} \;\middle|\; \sum_{\substack{i,j=1 \\ i<j}}^{r} g_{ij} S_{ij} = 0 \right\}$$

has the Taylor basis $L^{(2)} := \{S_{ijk} \mid 1 \leqslant i < j < k \leqslant r\}$ with

$$S_{ijk} = \frac{T(i,j,k)}{T(i,j)} e_{ij} - \frac{T(i,j,k)}{T(i,k)} e_{ik} + \frac{T(i,j,k)}{T(j,k)} e_{jk}.$$

S_{ijk} is homogeneous of degree $T(i,j,k)$ if we call now $\Sigma\, g_{ij}e_{ij}$ homogeneous of degree $\varphi \in T$, if for all $1 \leqslant i < j \leqslant r$ a $c_{ij} \in K$ exists, such that $g_{ij}T(i,j) = c_{ij}\varphi$.

Let us denote the maximal syzygy being involved in S_{ijk} by $MS(i,j,k)$, i.e.

$$MS(i,j,k) := \max_{<_1}\{S_{ij}, S_{ik}, S_{jk}\}.$$

If and only if $MS(i,j,k)$ and S_{ijk} are homogeneous of the same degree, i.e. $T(i,j,k) = \max\{T(i,j), T(i,k), T(j,k)\}$, then one of the three nonvanishing components of S_{ijk} is a constant. In that case, $MS(i,j,k)$ can be expressed in terms of lesser syzygies *w.r.t.* $<_1$. For instance let $MS(i,j,k) = S_{ik}$ and $T(i,j,k) = T(i,k)$. Then using $S_{ijk} \in S^{(2)}$

$$(*) \quad S_{ik} = \frac{T(i,j,k)}{T(i,j)} S_{ij} + \frac{T(i,j,k)}{T(j,k)} S_{jk}.$$

This allows to remove S_{ik} from $L^{(1)}$. The set $L^{(1)} \setminus \{S_{ik}\}$ still generates $S^{(1)}$, because in every basis representation of an $S \in S^{(1)}$, S_{ik} can be replaced by the lesser syzygies S_{ij} and S_{jk} using $(*)$.

3.4. The procedure for removing elements from $L^{(1)}$ can be applied iteratively. Whenever an S_{ijk} and its corresponding $MS(i,j,k)$ have the same degree, then $MS(i,j,k)$ can be expressed by lesser syzygies and hence it can be removed from the (eventually already reduced) generating set for $S^{(1)}$, as an elementary inductive argument shows.

The tests for detecting reducible elements of $L^{(1)}$ can be done by inspecting the elements of $L^{(2)}$. These tests do not require the explicit representations of the elements of $L^{(2)}$ but only divisibility tests of terms.

We say criterion M holds for (i,k) briefly $M(i,k)$, if a $j < k$ exists, such that $T(j,k)$ divides properly $T(i,k)$. (M stands for Multiple.)

We say criterion F holds for (i,k) briefly $F(i,k)$, if a $j < i$ exists, such that $T(j,k) = T(i,k)$. (F stands for the fact that in the set $\{S_{lk} \mid \text{degree } S_{lk},\ 1 \leqslant l < k\}$ the First w.r.t. $<_1$ is different from S_{lk}.)

We say criterion B_k holds for (i,j), briefly $B_k(i,j)$, if $j < k$ and $T(k)$ divides $T(i,j)$ and $T(i,k) \neq T(i,j) \neq T(j,k)$. ($B$ stands for the fact that when we are considering already elements of type S_{ik} for reduction, we have to go Backwards w.r.t. $<_1$ for reducing S_{ij}.)

3.5. PROPOSITION. *The module of syzygies $S^{(1)}$ us generated by*

$$L^* := \{S_{ij} \mid 1 \leqslant i < j \leqslant r,\ \neg M(i,j), \neg F(i,j), \neg B_k(i,j) \text{ for all } k > j\}.$$

PROOF. If $M(i,k)$ holds true, then a $j < k$ exists, such that $T(j,k)$ divides properly $T(i,k)$, especially $T(i,k) = T(i,j,k)$ and $j \neq i$. This means, a syzygy S_{ijk} (in case $i < j$) or S_{jik} (in case $j < i$) exists which is homogeneous of degree $T(i,k)$ and has S_{ik} for its maximal syzygy:

$$S_{jk} <_1 S_{ik} \quad \text{because} \quad T(j,k) <_T T(i,k)$$

$$S_{ij} \quad \text{or} \quad S_{ji} <_1 S_{ik} \quad \text{because} \quad j < k,\ i < k \quad \text{and} \quad T(i,j) \leqslant_T T(i,k).$$

If $F(j,k)$ holds, then $T(j,k) = T(i,k)$ for a $j < i$. This means that S_{jik} is homogeneous of

degree $T(j, i, k) = T(i, k)$ and by similar arguments as before $MS(j, i, k) = S_{ik}$.

If $B_k(i, j)$ holds, then analogously $MS(i, j, k) = S_{ij}$.

The arguments in 3.4 give the assertion.

3.6. The reduced basis L^* is not always a completely reduced basis as the following example shows.

EXAMPLE. Let $r = 4$ and $T(1) = x^2y^2$, $T(2) = y^2z$, $T(3) = x^2z$, $T(4) = xyz$. Then

$$T(1, 2) = T(1, 3) = T(2, 3) = T(1, 4) = x^2y^2z,$$

$$T(2, 4) = xy^2z, \qquad T(3, 4) = x^2yz.$$

$M(1, 4)$, $F(2, 3)$, and $B_4(2, 3)$ hold but no other criterion of 3.5. Therefore the reduced basis by 3.5 is

$$L^* = \{S_{12}, S_{13}, S_{24}, S_{34}\}.$$

But

$$S_{13} = S_{14} - yS_{34} \quad \text{by} \quad S_{134} \in S^{(2)},$$

$$S_{14} = S_{12} + xS_{24} \quad \text{by} \quad S_{124} \in S^{(2)}.$$

This implies

$$S_{13} = S_{12} + xS_{24} - yS_{34}.$$

Hence S_{13} is redundant in L^* and

$$\{S_{12}, S_{24}, S_{34}\}$$

also generates $S^{(1)}$.

3.7. A modification of criterion F would have given the minimal basis in the example. Criterion $F(2, 3)$ was based on the syzygy S_{123} yielding

$$0 = S_{12} - S_{13} + S_{23}$$

and used to cancel S_{23} because S_{12} and S_{13} are kept in L^*. But S_{13} is redundant, if L^* contains S_{12} and S_{23}. Hence $\{S_{12}, S_{23}, S_{14}, S_{24}, S_{34}\}$ is a basis of $S^{(1)}$, too. By $M(1, 4)$ and $B_4(2, 3)$ as before, S_{23} and S_{14} may be omitted. This gives the irreducible basis $\{S_{12}, S_{24}, S_{34}\}$.

A consequent application of this data is, when already redundant syzygies of degree $<_T \tau$ and syzygies S_{ij} of degree τ with $j < k$ are cancelled by the criteria, then to delay the decision, what element S_{ik} of the set

$$S_{\tau,k} = \{S_{jk} \mid 1 \leqslant j < k,\ T(j, k) = \tau\}$$

not to cancel. We may take an arbitrary $S_{ik} \in S_{\tau,k}$, because $i \neq j$, $S_{jk} \in S_{\tau,k}$ we have (*w.l.o.g.* $i < j$)

$$0 = \frac{\tau}{T(i, j)} S_{ij} - S_{ik} + S_{jk},$$

and S_{ij} can be expressed by lower order syzygies of the basis.

3.8. Condition $C3$ of theorem 2.5 allows an easier Groebner basis test, when the basis of $S^{(1)}$ is a minimal basis. Since $S^{(1)}$ is homogeneous, it is reasonable to restrict the considerations to homogeneous bases, such that the notions minimality and irreducibility coincide. A (homogeneous) basis L of $S^{(1)}$ is irreducible if and only if no syzygy for L exists, which has a $c \in K\backslash\{0\} =: K^x$ for a component (allowing the cancellation of an additional element of L). If L is constructed by a successive cancellation of reducible elements from $L^{(1)}$, then each syzygy for L with a component $c \in K^x$ originates from an S_{ijk}, which also has a component from K^x, allowing the cancellation of the same element, cf. Möller & Mora (1986).

The strategy for finding the reduced basis L^* works in a similar way. We take each S_{ijk}, which has a component from K^x, but we always decide to take $MS(i, j, k)$ for redundant. If S_{ijk} has more than one component from K^x, then our choice of the redundant element may cause that we cancel the "wrong" basis element as seen in 3.7.

Only when many S_{ijk} exist, such that at least two of the three non-zero components are constants, and when we often select the "wrong" basis element for cancellation in such situation, then we have still many reducible elements in L^*. Fortunately, we found only more or less artificial examples like 3.6, where this occurs.

4. Buchberger's Algorithm

4.1. Buchberger's algorithm deals with the problem of finding a Groebner basis of a polynomial ideal, when a finite basis of the ideal is given. This algorithm was originally introduced by Buchberger (1965) and refined in subsequent papers. For a survey see Buchberger (1985).

4.2. We will present briefly a version of the algorithm recommended by Buchberger (1985). In order to avoid the technical details for reducing Groebner bases, we concentrate on the construction without reduction.

INPUT: $\{f_1, \ldots, f_r\} \subset P\backslash\{0\}$.

INITIALIZATION: $B := \{\{i, j\}/1 \leqslant i < j \leqslant r\}$;
$G := \{f_1, \ldots, f_r\}$; $R := r$.

ITERATION: *while* there exists $\{I, J\} \in B$ *repeat*
if $\neg$ criterion 1 *and* $T(I)T(J) \neq T(I, J)$ *then*
$h := S(f_I, f_J)$;
$h := NF(h, G)$;
if $h \neq 0$ *then*
$f_{R+1} := h$; $G := G \cup \{f_{R+1}\}$;
$B := B \cup \{\{i, R+1\}/1 \leqslant i \leqslant R\}$;
$R := R + 1$;
$B := B\backslash\{\{I, J\}\}$.

OUTPUT: G, a Groebner basis of $(f_1, \ldots, f_r)$.

Here, $NF(h, G)$ means a polynomial irreducible modulo G, such that $h \xrightarrow[G]{}{}^{+} NF(h, G)$. Criterion 1 applied to $\{I, J\}$ means that there is a $K \in \{1, \ldots, R\}\backslash\{I, J\}$ with $T(I, J) = T(I, J, K)$ and $\{I, K\} \notin B$, $\{J, K\} \notin B$. The criterion $T(I)T(J) = T(I, J)$ is criterion 2 of Buchberger (1985).

4.3. The correctness of algorithm 4.2 is shown by Buchberger (1979). Let us prove it by means of $C3$ of theorem 2.5. The syzygies S_{ij} correspond bijectively to all $\{i,j\}$ which are assigned once in the algorithm to B and removed later from B. We order the S_{ij} by $<_B$, such that $S_{ij} <_B S_{kl}$, if $\{i,j\}$ is removed from B earlier than $\{k,l\}$. If criterion 1 holds for $\{I,J\} \in B$, i.e. $\{I,K\} \notin B$, $\{J,K\} \notin B$, $T(I,J,K)$, then let for simplicity of notation $I < J < K$. The syzygy S_{IJK} shows

$$0 = S_{IJ} - \frac{T(I,J,K)}{T(I,K)} S_{IK} + \frac{T(I,J,K)}{T(J,K)} S_{JK}.$$

By the ordering $<_B$, $S_{IK} <_B S_{IJ}$ and $S_{JK} <_B S_{IJ}$. Hence S_{IJ} is expressible in terms of lower order syzygies. Thus, if criterion 1 holds for $\{I,J\}$, then S_{IJ} is redundant. For the remaining syzygies S_{IJ} we have in case $T(I)T(J) = T(I,J)$

$$S(f_I, f_J) \xrightarrow[\{f_I,f_J\}]{}{}^{+} 0, \qquad \text{i.e. } S(f_I,f_J) \xrightarrow[G]{}{}^{+} 0,$$

as already shown in Buchberger (1965), and otherwise

$$S(f_I,f_J) \xrightarrow[G]{}{}^{+} NF(S(f_I,f_J), G) = f_{R+1} \xrightarrow[f_{R+1}]{} 0.$$

Therefore at termination $B = \emptyset$, we have

$$\frac{T(I,J)}{T(I)} f_I - \frac{T(I,J}{T(J)} f_J \xrightarrow[G]{}{}^{+} 0 \quad \text{for all} \quad S_{IJ},$$

which are not redundant, and hence G is a Groebner basis by $C3$ of theorem 2.5.

4.4. A consequent use of the reduction strategy in 3.5 gives the following modifications of Buchberger's algorithm.

INPUT: $\{f_1, \ldots, f_r\} \subset P \backslash \{0\}$.

INITIALIZATION:
$G := \{f_1\}$; $D := \emptyset$;
for $t := 2$ *to* r
  $D :=$ updatePairs (D, t);
  $G := G \cup \{f_t\}$;
$R := r$.

ITERATION:
while there exists $(I,J) \in D$ *repeat*
  $h := S(f_I, f_J)$;
  $h := NF(h, G)$;
  if $h \neq 0$ *then*
    $f_{R+1} := h$;
    $D :=$ updatePairs $(D, R+1)$;
    $G := G \cup \{f_{R+1}\}$; $R := R+1$;
  $D := D \backslash \{(I,J)\}$.

OUTPUT: G, a Groebner basis of $\{f_1, \ldots, f_r\}$.

Here the subalgorithm updatePairs works in the following way, when applied to a set of pairs D and a positive integer t. Cancel in D all pairs (i,j), which satisfy $T(i,j) = T(i,j,t)$, $T(i,t) \neq T(i,j) \neq T(j,t)$, i.e. all pairs (i,j) with $B_t(i,j)$. Denote the set of remaining pairs by D'. Let $D1 := \{(i,t) \mid 1 \leqslant i < t\}$. Cancel in $D1$ each (i,t) for which a $(j,t) \in D1$ exists, s.t. $T(i,t)$ is a proper multiple of $T(j,t)$, i.e. each (i,t) with $M(i,t)$. The subset of $D1$ containing the remaining pairs (i,t) is denoted by $D1'$. In each nonvoid

subset $\{(j, t) \mid T(j, t) = \tau\}$ of $D1'$ with $\tau \in T$ fix an element (i, t) satisfying $T(i)T(t) = T(i, t)$ or if no such (i, t) exists, fix an arbitrary (i, t). Cancel the other elements of $\{(j, t) \mid T(j, t) = \tau\}$ in $D1'$. Finally delete in $D1'$ all (i, t) with $T(i)T(t) = T(i, t)$ and denote again by $D1'$ this finally obtained subset of $D1'$. The set $D1' \cup D'$ is returned by the subalgorithm.

By construction of the subalgorithm, we have after the call of $D :=$ updatePairs (D, t), that $\{S_{ij} \mid (i, j) \in D\}$ together with some S_{ij} with $1 \leqslant i < j \leqslant t$, $T(i)T(j) = T(i, j)$, constitute a basis of the module of syzygies

$$\left\{(g_1, \ldots, g_t) \in P^t \;\middle|\; \sum_{i=1}^{t} g_i T(i) = 0\right\}.$$

This follows from proposition 3.5 and the modification in 3.7.

4.5. The correctness of algorithm 4.4 is shown in analogy to 4.3. Its termination results from the same arguments as the termination of algorithm 4.2. By construction, each new f_{R+1} is irreducible with respect to $f_1, \ldots, f_R$. Therefore especially

$$(T(1), \ldots, T(R)) \subset (T(1), \ldots, T(R+1)).$$

This gives for (strictly) increasing R a strictly increasing chain of ideals. By Noetherianity, this chain is finite. Thus the iteration is repeated only a finite number of times.

4.6. Buchberger (1985) presented algorithm 4.2 in a version, which already cancels redundant basis elements in G. In a similar way, algorithm 4.4 can be modified. This modification for reducing redundant basis elements is already installed by the authors in SCRATCHPAD II and with minor changements also in REDUCE 3.3. The modification of algorithm 4.4 is based on the following idea.

If the input elements $f_1, \ldots, f_r$ are ordered, such that $T(1) \geqslant_T \cdots \geqslant_T T(r)$, then an f_i is redundant in the final Groebner basis, if and only if for a $j > i$ $T(i, j) = T(i)$ holds, see 2.6. ($j < i$ is excluded by the order of the input elements for $i \leqslant r$ and for $i > r$ it is impossible because then f_i is a f_{R+1} and $T(R+1)$ has no divisor $T(j), j < R+1$.) Then $T(j, t)$ divides $T(i, t)$ for all $t > j$. Hence $M(i, t)$ holds or $T(i, t) = T(j, t)$. Therefore S_{it} is redundant or equivalent to S_{jt} by 3.7.

Thus, when $T(i, j) = T(i)$, then f_i is removed from the actual G and in the subsequent calls of updatePairs (D, t), $t > j$, the pair (i, t) is ignored.

4.7. The cancelling of redundant basis elements in the actual set G leads in both algorithms to space savings and to faster tests of criterion 1 in algorithm 4.2 or faster applications of updatePairs in algorithm 4.4 respectively. However, for several reasons it is to be expected that algorithm 4.4 is faster than algorithm 4.2, as the statistics in section 5 will confirm,

(1) B contains usually more elements than D, because pairs $\{I, J\}$ are assigned to B before being tested by criterion 1 or criterion 2, whereas in updatePairs all possible tests are already done, before pairs (i, j) are assigned to D.

(2) If in the iteration of algorithm 4.2 the pair $\{I, J\}$ is in one loop $\{I, J_1\}$ and in a later loop $\{I, J_2\}$ with the same I, then the test of criterion 1 includes in both cases the testing of the same $\{I, K\}$ for some K. Such surplus tests do not occur in updatePairs.

(3) Following a recommendation of Buchberger, in algorithm 4.2 the pairs $\{I, J\} \in B$ is always selected, such that

$$T(I, J) = \min\{T(K, L)/\{K, L\} \in B\},$$

but it is left to chance, what pair $\{I, J\} \in B$ with minimal $T(I, J)$ is selected. updatePairs selects among all (i, t) with $1 \leqslant i < t$ and same $T(i, t)$ one element which satisfies criterion 2 and omits the other (i, t). This chance of omitting some pairs if one satisfies criterion 2 is sometimes lost in algorithm 4.2 as the careful analysis of some involved examples showed and it causes, that in some examples more reductions $S(f_I, f_J) \xrightarrow{G}{}^{+} 0$ are detected by the criteria in algorithm 4.4 than in algorithm 4.2.

5. Examples

5.1. In 4.6 we described how algorithm 4.4 has to be modified in order to obtain a Groebner basis without redundant elements. The following example illustrates this version of algorithm 4.4.

Let $P := Q[x, y, z]$, Q the field of rationals, and $<_T$ be the lexicographical term ordering with $x <_T y <_T z$. We want to calculate a Groebner basis of (f_1, f_2, f_3) with

$$f_1 := zy^2 + 2x + \frac{1}{2},$$

$$f_2 := zx^2 - y^2 - \frac{1}{2}x,$$

$$f_3 := -z + y^2x + 4x^2 + \frac{1}{4},$$

see example 6.15 of Buchberger (1985). In the iteration of the algorithm, we always select $(I, J) \in D$, such that

$$T(I, J) = \min\{T(K, L) \mid (K, L) \in D\}.$$

f_1 and f_2 are redundant because of $T(1, 3) = T(1)$ and $T(2, 3) = T(2)$. Therefore the initialization gives first $(t = 2) G = \{f_1, f_2\}$ and $D = \{(1, 2)\}$ and then $(t = 3)$

$$G = \{f_3\}, D = \{(1, 3), (2, 3)\}.$$

Because of $B_3(1, 2)$ the pair $(1, 2)$ was removed from D.

The first pair (I, J) is $(2, 3)$. Then

$$f_4 := NF(S(f_2, f_3), G) = -y^2x^3 + y^2 - 4x^4 - \frac{1}{4}x^2 + \frac{1}{2}x$$

gives $D = \{(1, 3)\}$, because f_1 and f_2 are redundant and $T(3)T(4) = T(3, 4)$, such that neither $(1, 4)$ nor $(2, 4)$ nor $(3, 4)$ is inserted into D. f_3 is not redundant. Therefore $G = \{f_3, f_4\}$.

The only choice for the next (I, J) is $(1, 3)$. Then

$$f_5 := NF(S(f_1, f_3), G) = y^4x + 4x^2y^2 + \frac{1}{4}y^2 + 2x + \frac{1}{2}$$

gives $D = \{(4, 5)\}$, because again f_1 and f_2 are redundant and $T(3)T(5) = T(3, 5)$, such

that neither (1, 5) nor (2, 5) nor (3, 5) but (4, 5) is inserted into D. We also get $G = \{f_3, f_4, f_5\}$.

The only choice for the next (I, J) is (4, 5). Then

$$f_6 := NF(S(f_4, f_5), G) = y^4 + \frac{1}{2}y^2x + 2x^3 + \frac{1}{2}x^2$$

gives $D = \{(5, 6)\}$ by the same arguments as before and in addition by $M(4, 6)$. We also get $G\{f_3, f_4, f_6\}$ because of $T(5, 6) = T(5)$.

The only choice for the next (I, J) is (5, 6). Then

$$f_7 := NF(S(f_5, f_6), G) = x^2y^2 + \frac{1}{14}y^2 - \frac{4}{7}x_4 - \frac{1}{7}x^3 + \frac{4}{7}x + \frac{1}{7}$$

gives $D = \{(4, 7), (6, 7)\}$ by similar arguments as before and $G\{f_3, f_6, f_7\}$ because of $T(4, 7) = T(4)$.

The next (I, J) is (4, 7). Then

$$f_i := NF(S(f_4, f_7), G) = y^2x + 14y^2 - 8x^5 - 58x^4 + \frac{9}{2}x^2 + 9x$$

gives $D = \{(6, 8), (7, 8)\}$ because of $T(3)T(8) = T(3, 8)$ and $B_8(6, 7)$ and $G = \{f_3, f_6, f_8\}$ because of $T(7, 8) = T(7)$. Then

$$f_9 := NF(S(f_7, f_8), G) = y^2 + \frac{112}{2745}x^6 - \frac{84}{305}x^5 - \frac{1264}{305}x^4 - \frac{13}{549}x^3 + \frac{84}{305}x^2 + \frac{1772}{2745}x + \frac{2}{2745}$$

gives $D = \{(6, 9), (8, 9)\}$ because of $B_9(6, 8)$ and $G = \{f_3, f_9\}$ because of $T(6, 9) = T(6)$ and $T(8, 9) = T(8)$. Then

$$f_{10} := NF(S(f_8, f_9), G) = x^7 + \frac{29}{4}x^6 - \frac{17}{16}x^4 - \frac{11}{8}x^3 + \frac{1}{32}x^2 + \frac{15}{16}x + \frac{1}{4}$$

gives $D = \{(6, 9)\}$ because of $T(9)T(10) = T(9, 10)$ and $T(3)T(10) = T(3, 10)$ and $G = \{f_3, f_9, f_{10}\}$. Then

$$NF(S(f_6, f_9), G) = 0.$$

Now $D = \emptyset$ and the algorithm terminates giving the Groebner basis

$$G = \{f_3, f_9, f_{10}\}.$$

5.2. The following statistics compare the algorithms 4.2 and 4.4. All examples can be found in Gebauer (1985).

								Algorithm 4.2				Algorithm 4.4			
Example	*a*	*b*	*c*	*d*	*e*	*f*	*g*	*h*	*k*	*l*	*m*	*h*	*k*	*l*	*m*
Ex1	7	6	*l*	*RN*	3	2	6	8/3	59	15	1·68	8/3	2	7	0·96
Ex5	6	6	*l*	*RN*	3	10	6	16/7	151	22	16·32	15/2	3	6	8.51
Ex27	7	7	*g*	*RN*	3	2	6	12/15	139	19	5·58	12/12	11	12	2·66
Ex12	6	6	*g*	*RN*	3	3	13	10/19	62	16	28·18	10/17	11	13	11·03
Ex2	3	3	*l*	*RN*	3	7	3	7/3	38	10	0·60	7/1	2	3	0·56
Ex8	3	3	*g*	*RN*	3	4	6	3/5	12	6	0·51	3/5	5	6	0·56
Ex3	4	4	*l*	*RN*	2	7	5	13/16	66	17	6·98	13/9	6	6	3·19
Ex10	4	4	*g*	*RN*	2	4	7	6/8	31	10	5·34	6/5	5	7	2·10
Ex4	5	5	*l*	*RN*	2	16	5	106/126	2392	111	5749·13	106/100	29	17	542·38
Ex11	5	5	*g*	*RN*	2	5	13	10/21	75	15	52·69	10/20	16	13	22·27
Ex14	6	6	*g*	*RFI*	3	5	13	13/12	120	19	203·13	13/9	7	13	60·04
Ex28	6	5	*g*	*RFI*	7	0	1	38/66	746	44	167·99	38/65	33	25	51·88
Ex9	3	3	*g*	*RN*	9	10	19	18/21	178	21	41·11	18/21	13	19	27·73
Ex29	6	6	*g*	*RN*	2	6	22	18/53	191	24	904·41	18/50	34	22	237·21

a Number of input polynomials.
b Number of variables.
c Lexicographical (*l*) or graduated (*g*) term ordering.
d Coefficient field of rational numbers (*RN*) or of rational functions over the integers (*RFI*).
e Maximal degree of input polynomials.
f Maximal degree of output polynomials.
g Length of Groebner basis.
h Number of *NF* computations: number of non-vanishing/vanishing *NF*'s.
k Maximal cardinality of set *B* or *D* respectively.
l Maximal cardinality of *G*.
m Computing time in seconds on an IBM 3090 mainframe.

References

Bayer, D. A. (1982). *The Division Algorithm and the Hilbert Scheme*. Ph.D. Thesis, Harvard University.

Bayer, D. A. (1986). Private communication.

Buchberger, B. (1965). *Ein Algorithmus zum Auffinden der Basis-elemente des Restklassenrings nach einem nulldimensionalen Polynomideal*. Ph.D. Thesis, Universität Innsbruck.

Buchberger, B. (1979). A criterion for detecting unnecessary reductions in the construction of Groebner bases. *Proc. EUROSAM 79, Springer L.N. in Comp. Sci.* **72**, 3–21.

Buchberger, B. (1985). Groebner Bases: An Algorithmic Method in Polynomial Ideal Theory. In: (ed. N. K. Bose) *Multidimensional Systems Theory*. D. Reidel Publ. Comp. Pp. 184–232.

Gebauer, R. (1985). *A collection of examples for Groebner calculations*. IBM Thomas J. Watson Research Center, Yorktown Heights, NY 10598.

Gebauer, R. & Möller, H. M. (1987). Groebner Bases, to appear in *SCRATCHPAD II Newsletter*, Vol. 2, No. 1.

Hearn, A. C. (1987). *REDUCE User's Manual*: Version 3.3. The Rand Corporation, Santa Monica, CA 90406.

Möller, H. M. (1985). A reduction strategy for the Taylor resolution. *Proc. EUROCAL 85, Springer L.N. in Comp. Sci.* **162**, 526–534.

Möller, H. M. & Mora, F. (1986). New constructive methods in classical ideal theory. *J. of Algebra*, **100**, 138–178.

Taylor, D. K. (1966). *Ideals Generated by Monomials in an R-sequence*. Ph.D. Thesis. University of Chicago.