JSC (P2)

Received by
B. Buchberger:
1987 -01- 26

A NEW IMPLEMENTATION OF BUCHBERGER'S ALGORITHM

Rüdiger Gebauer H. Michael Möller

ABSTRACT: Buchberger's algorithm for calculating Groebner bases of polynomial ideals is already implemented in some Computer Algebra Systems. Our new implementation differs from existing ones mainly by the criteria for omitting superfluous reductions. Buchberger (1985) recommended two criteria. The more important one can be interpreted as criterion for detecting redundant elements in a basis of a module of syzygies. We present a procedure for constructing a minimal basis of such module and a simple but effective method for obtaining a reduced, nearly minimal basis. The criteria based on the latter method are incorporated in a new variant of Buchberger's algorithm. The resulting implementation is compared with an existing one. The paper concludes with statistics stressing the good computational qualities of this new implementation.

This research was supported by IBM Germany and it was written while the first author was at IBM Thomas J. Watson Research Center Yorktown Heights.

A New Implementation of Buchberger's Algorithm

Rüdiger Gebauer
Springer Verlag Inc.
175, Fifth Avenue
New York, NY 10010
USA

H. Michael Möller
FB Mathematik u. Inf.
Fernuniversität Hagen
D-5800 Hagen 1

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, such that a lesser number of S-polynomial reductions has to be performed in fact. 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), but it does not hold as often as the first one and in most cases when it holds, also a criterion of the first type holds. 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 criterion 2 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 like e.g. 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 already stated by Moeller (1985). In this paper, we present two reduction strategies. The first one gives only a reduced basis of the module of syzygies (proposition 3.5), but the detection of redundant elements is very effective. The second one (see 3.9) gives a minimal basis of the module. Using the one to one correspondence of Taylor basis elements and pairs for the S-polynomial computation, pairs satisfying a criterion of the first type correspond to redundant Taylor basis elements. Hence the second reduction strategy (presented in 3.8) gives theoretically the best possible criterion of type 1.

The first strategy is applied to develop a variant of Buchberger's algorithm. Redundant Taylor basis elements are detected here by three simple criteria. It may happen, that not all redundant syzygies are detected. But as the comparison to the second strategy shows, this happens only in exceptional cases. 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 pair for the S-polynomial is no more needed for forthcoming 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. Very important for a fast variant of Buchberger's algorithm is also 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 canceled. 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 Jenks (1986), and REDUCE (release 3.2), see Hearn (1986). 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

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

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

For $f = \sum_{i=1}^{m} c(f,\varphi_i)\,\varphi_i$ with $\varphi_1 <_T \varphi_2 <_T \ldots <_T \varphi_m$

and $c(f,\varphi_i) \in K \setminus \{0\}$, we define as in Moeller & Mora (1986)

$$\text{Hcoeff}(f) := c(f,\varphi_m),\ \text{Hterm}(f) := \varphi_m$$

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

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. $\text{Hcoeff}(f_i) = 1$, $i=1,\ldots,r$. Mainly for avoiding tedious notations, we define

$$T(i) := \text{Hterm}(f_i),$$

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

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

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

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

which means

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

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

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

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

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

2.4 <u>Definition</u>. $F = \{f_1,\ldots,f_r\} \subset P \setminus \{0\}$ is called a Groebner basis of Ideal $(F) := \{\sum_{i=1}^{r} g_i f_i \,/\, g_i \in P\}$, 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 $S(f_i,f_j) \xrightarrow[F]{}^{+} 0$, $1 \le i < j \le r$.

- 6 -

(Buchberger gives in his publications a different definition for Groebner bases, but he showed already in his thesis (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 Moeller & Mora (1986). In the following, we need only three equivalent characterizations:

2.5 Theorem. Let $F = \{f_1,\ldots,f_r\} \subset P \setminus \{0\}$ and $I = \mathrm{Ideal}(F)$. Then the following conditions are equivalent.

C1) F is a Groebner basis of I.

C2) $M_T(F) = \{T(1),\ldots,T(r)\}$ generates $M_T(I)$, the least ideal containing $M_T(f)$ for all $0 \neq f \in I$.

C3) Let L be a basis of the module of syzygies $S_1 := \{(h_1,\ldots,h_r) \in P^r \,/\, \sum_{i=1}^{r} h_i\, T(i) = 0\}$. 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 $\Longleftrightarrow$ C2 can be found in Moeller & Mora (1986). C1 $\Longleftrightarrow$ C3 is shown for instance by Moeller (1985).

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

Ideal(F'). If Ideal(F) = Ideal(F') and F is a Groebner basis, then by C2, F' is a Groebner basis too, if and only if T(j) divides T(i), i.e.

$$T(i,j) = T(i) \quad \text{for a} \quad j \neq i .$$

For testing Ideal(F) = 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 $\text{Hterm}(S(f_i,f_j)) <_T \text{Hterm}(f_i)$,

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

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 of Syzygies

3.1 The main tools in this section are the resolution of Diana Taylor (1966) and methods for reducing the bases contained in this resolution. In Moeller & 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 $T(1),\dots,T(r)$, we call $(g_1,\dots,g_r) \in P^r$ homogeneous of degree $\varphi \in T$, if for every $i \in \{1,\dots,r\}$ a $c_i \in K$ exists, such that $g_i\ T(i) = c_i\ \varphi$.
Then

$$S^{(1)} := \{(g_1,\dots,g_r) \in P^r \ / \sum_{i=1}^{r} g_i\ T(i) = 0\}$$

has the Taylor basis $L^{(1)} := \{S_{ij}\ /\ 1 \le i < j \le r\}$
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 k-th canonical unit vector of P^r. Using this specific basis, C3 $\Longrightarrow$ 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 $<_1$,

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

Using this order, we do not denote the canonical k-th unit vector in $P^{r(r-1)/2}$ by e_k but by e_{ij}, if S_{ij} is the k-th 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

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

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

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

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 $1 \le i < j \le r$ 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.

$$MS(i,j,k) := \max \{ S_{ij}, S_{ik}, S_{jk} \} \; .$$

Then S_{ijk} contains a nonzero constant coefficient if the syzygies S_{ijk} and $MS(i,j,k)$ are homogeneous of the same degree.

3.4 Using the Taylor basis $L^{(2)}$, we can detect redundant elements in the basis $L^{(1)}$ of $S^{(1)}$ as we will show in the proof of the next proposition. These tests for reduction do not need an explicit knowledge of elements of $L^{(2)}$, because we are able to formulate these tests in the following simple way using only divisibility properties 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 $\{S_{lk} \,/\, \text{degree } S_{lk} = T(i,k),\ 1 \leq l < k\}$ the First w.r.t. $<_1$ is different from S_{ik}.)

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 <u>Proposition</u>. The module of syzygies $S^{(1)}$ is generated by

$$L^{*} := \{S_{ij} \,/\, 1 \leq i < j \leq r\ , \neg M(i,j), \neg F(i,j),$$

$$\neg B_k(i,j) \quad \text{for all } k > j\}\ .$$

Proof. $M(i,k)$ means, that a syzygy S_{ijk} or S_{jik} exists with 1 or -1 as coefficient of e_{ik} and a nonconstant coefficient for e_{jk}. This gives for $i < j$

$$(*) \qquad 0 = \frac{T(i,j,k)}{T(i,j)} S_{ij} - S_{ik} + \frac{T(i,j,k)}{T(j,k)} S_{jk} .$$

Since S_{ik} is homogeneous of degree $T(i,j,k) = T(i,k)$ but S_{jk} is of degree $T(j,k) <_T T(i,k)$, we have $S_{jk} <_1 S_{ik}$. Since $T(i,j)$ divides $T(i,j,k)$, we have $T(i,j) \leq_T T(i,k)$ but $\max\{i,j\} < k$, hence $MS(i,j,k) = S_{ik}$. Therefore equation (*) shows, that S_{ik} can be expressed in terms of syzygies of lower order, i.e. S_{ik} is redundant. For $j < i$ replace in (*) S_{ij} by $-S_{ji}$. The same arguments as before give also that S_{ik} is redundant.

Similarly, $F(i,k)$ means

$$(**) \qquad 0 = \frac{T(j,i,k)}{T(j,i)} S_{ji} - S_{jk} + S_{ik} ,$$

with $j < i < k$ and $MS(j,i,k) = S_{ik}$. As before (**) shows, that S_{ik} can be expressed in terms of lower order syzygies.

Finally, $B_k(i,j)$ means

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

where the coefficients of S_{ik} and S_{jk} are no constants displaying the fact, that their degrees are less than the degree of S_{ij}, i.e. $MS(i,j,k) = S_{ij}$. Hence S_{ij} can be expressed here in terms of lower order syzygies.

3.6 The reduced module basis L^* is not always a minimal basis. It may happen, that there are some syzygies S_{uv} of the same degree, such that there are some S_{ijk} containing more than one nonvanishing constant coefficient (as in criterion F). The criteria cancel MS(i,j,k) and ignore that equivalently an other S_{uv} could have been canceled. Sometimes it is more favourable not to cancel MS(i,j,k) but an other S_{uv} as the following example shows.

Example. Let r = 4 and $T(1) = x^2 y^2, T(2) = y^2 z$, $T(3) = x^2 z$, $T(4) = xyz$. The order $<_T$ is fixed arbitrarily as in 2.1. Then

by S_{123} : $0 = S_{12} - S_{13} + S_{23}$
$\Rightarrow$ S_{23} is canceled by F(23)

by S_{124} : $0 = S_{12} - S_{14} + x\, S_{24}$
$\Rightarrow$ S_{14} is canceled by M(14)

by S_{134} : $0 = S_{13} - S_{14} + y\, S_{34}$
$\Rightarrow$ S_{14} is canceled by M(14)

by S_{234} : $0 = S_{23} - x\, S_{24} + y\, S_{34}$
$\Rightarrow$ S_{23} is canceled by $B_4(23)$

No other S_{ij} is canceled, because the proof of prop. 3.5 shows, that any M(i,j) or F(i,j) or $B_k(i,j)$ leads to a syzygy S_{uvw} having that S_{ij} for MS(u,v,w). This means, that the reduced basis L^* consists of the four elements S_{12}, S_{13}, S_{24}, S_{34}. However, let us use S_{123} for cancelling S_{13}.

(This means, we do not cancel in $\{S_{v3} \mid 1 \le v < 3$, $T(v,3) = x^2 y^2 z\}$ all except the first, but all except the last, such that we use a criterion L(ast) instead of criterion F(irst).) Then we obtain also a reduced basis for $S^{(1)}$ but it consists only of the elements S_{12}, S_{23}, S_{34}.
Obviously the latter reduced basis is a minimal one for $S^{(1)}$.

3.7 For obtaining the reduced basis L^*, all elements of the set

$$S_\varphi := \{S_{ik} \mid i \in \{1,\dots,k-1\}, T(i,k) = \varphi\}$$

are canceled by criterion F except the first one. But as (**) and the example show, this decision is quite voluntary, and it sometimes results, that a redundant element is not detected. In order to detect all redundant elements, it is more reasonable to collect for fixed k all S_{ik}, $1 \le i < k$, of same degree. If one of them is redundant by a criterion B, also the remaining S_{ik} are redundant because each of them can be expressed by the assigned one and a lower order syzygy as the corresponding equation (**) shows.

3.8 A consequent use of this idea gives the following procedure for reducing $S^{(1)}$:

Assume, we have already constructed disjoint subsets U'_s of $\{S'_{ij} \mid 1 \le i < j < r\}$, $s = 1,\dots,S$, where the prime denotes, that we are dealing with (sets of) (r-1)-tuples, such that for any choice of $u'_s \in U'_s$, $s = 1,\dots,S$, $\{u'_1,\dots,u'_S\}$ is an minimal basis of $\{g_1,\dots,g_{r-1})/\Sigma\, g_i\, T(i) = 0\}$.

S_{ij} differs from S'_{ij} only by a last additional (zero) component, $1 \leq i < j < r$, and analogously U_s differs from U'_s.

Consider each S_{ir}, $1 \leq i < r$. If $M(i,r)$ holds, take the least j, such that $T(j,r)$ divides properly $T(i,r)$. If $T(i,j) = T(i,r)$ and $S_{ij} \in U_s$, then assign S_{ir} to U_s, otherwise skip S_{ir}. If $M(i,r)$ does not hold, collect all S_{jr} of degree $T(i,r)$, $1 \leq j < r$, into a new set U_s. Finally test all sets U_s. If $B_r(i,j)$ holds for a $S_{ij} \in U_s$, then cancel U_s.

3.9 <u>Proposition</u>. The construction in 3.8 gives a finite number of disjoint subsets U_s of $\{S_{ij} / 1 \leq i < j \leq r\}$, such that for any choice of $u_s \in U_s$ the set of all u_s constitutes a minimal basis of $S^{(1)}$.

Proof. Since all syzygies are homogeneous, minimality means irreducibility, i.e. we have to show, that the procedure in 3.8 detects all redundant elements S_{ij}. Some simple considerations, like for instance in Moeller & Mora (1986), show, that we find all redundant elements by considering all syzygies S_{uvw} where at least one of the three nonzero coefficients is a constant (1 or -1). Obviously, we have only to consider syzygies S_{uvw} which constitute a reduced basis of $S^{(2)}$. Therefore, we order the S_{uvw} by $<_2$:

$$S_{uvw} <_2 S_{ijk} \quad \text{if } T(u,v,w) <_T T(i,j,k)$$
$$\text{or if } T(u,v,w) = T(i,j,k),\ MS(u,v,w) <_1 MS(i,j,k)$$

and syzygies of same degree with same MS are ordered inverse lexicographically:

$S_{uvw} <_2 S_{ijk}$ if $T(u,v,w) = T(i,j,k)$,
$MS(u,v,w) = MS(i,j,k)$, $w \le k$, $w = k \Rightarrow v \le j$,
$(w = k,\ v = j) \Rightarrow u < i$.

For detecting redundant syzygies S_{ijk}, we use the dependence relations

$$0 = \frac{T(t,u,v,w)}{T(t,u,v)} S_{tuv} - \frac{T(t,u,v,w)}{T(t,u,w)} S_{tuw}$$

$$+ \frac{T(t,u,v,w)}{T(t,v,w)} S_{tvw} - \frac{T(t,u,v,w)}{T(u,v,w)} S_{uvw} .$$

(These relations arise from the Taylor basis of the next module of syzygies.) A syzygy S_{ijk} is redundant, if it is contained in such relation having as power product factor 1 or -1 and if it is maximal w.r.t. $<_2$ among all four involved syzygies.

The syzygies S_{ijk} with $k < r$ are already used for constructing an irreducible basis of $\{(g_1,\ldots,g_{r-1}) \ / \ \Sigma\ g_i\ T(i) = 0\}$. Therefore we have only to consider the syzygies of type S_{ijr} and among them only those where S_{ijr} and $MS(i,j,r)$ have the same degree, because otherwise S_{ijr} has no nonzero constant component.

Let us consider first syzygies of type S_{ijr} with $T(i,r) = T(j,r)$.

Then

$$S_{ijr} = \frac{T(i,j,r)}{T(i,j)} e_{ij} - e_{ir} + e_{jr} .$$

In this case we will call S_{ir} equivalent to S_{jr}. If $T(i,r) = T(j,r) = T(k,r) =: \tau$, $i < j < k$, then also $T(i,j,k,r) = \tau$ and we get the dependence relation

$$0 = \frac{\tau}{T(i,j,k)} S_{ijk} - S_{ijr} + S_{ikr} - S_{jkr} .$$

S_{jkr} is maximal w.r.t. $<_2$. Hence it is redundant. This means, that each syzygy of type

$$S_{ijr} = \frac{T(i,j,r)}{T(i,j)} e_{ij} - e_{ir} + e_{jr}$$

is redundant if S_{ir} is the not first element of all S_{jr} of the same degree.

Let us consider now two syzygies of degree τ , S_{ijr} or S_{jir} with $T(i,r) = \tau \neq T(j,r)$ and S_{ikr} or S_{kir} with $T(k,r) \neq \tau$. There is one dependence relation, which contains both syzygies. But we have to distinguish six different cases depending on the ordering of i,j,k. Let $i < j < k$. Then

$$0 = \frac{\tau}{T(i,j,k)} S_{ijk} - S_{ijr} + S_{ikr} - \frac{\tau}{T(j,k,r)} S_{jkr} .$$

If $MS(j,k,r)$ has degree τ , then $MS(j,k,r) = S_{jk} <_1 S_{ir} = MS(i,j,r) = MS(i,k,r)$. Therefore $S_{jkr} <_2 S_{ijr} <_2 S_{ikr}$. (This is obvious, if the degree of $MS(j,k,r)$ is less than τ .) Analogously $S_{ijk} <_2 S_{ijr} <_2 S_{ikr}$. Therefore, S_{ikr} is redundant. The same arguments show in the remaining five cases that always the greatest (w.r.t. $<_2$) of the two syzygies S_{ijr} (or S_{jir}) and S_{ikr} (or S_{kir}) is redundant. Therefore a syzygy S_{ijr} of degree τ with $T(i,r) = \tau \neq T(j,r)$ or $T(j,r) = \tau \neq T(i,r)$ is redundant, if $T(j,r)$ or $T(i,r)$ resp. is not the uniquely determined proper divisor $T(v,r)$ of τ with minimal v.

For detecting more redundant syzygies S_{uvw} , we have finally to consider the mixed case, two syzygies of degree τ , S_{ijr} or S_{jir} with $T(i,r) = T(j,r) (= \tau)$ and S_{kir} or S_{ikr} with $T(k,r) \neq \tau$ and we may exclude cases, where one of these syzygies is already detected to be redundant. Hence k is the minimal v, such that $T(v,r)$ divides properly τ , and i or j is the minimal v, such that $T(v,r) = \tau$. Let $\{u,v,w\} = \{i,j,k\}$, $u < v < w$. Then we have the dependence relation

$$0 = \frac{\tau}{T(u,v,w)} S_{uvw} - S_{uvr} + S_{uwr} - S_{vwr} .$$

Because of $MS(u,v,w) <_1 \min\{S_{ir}, S_{jr}\} <_1 \max\{S_{ir}, S_{jr}\} = MS(v,w,r)$, S_{vwr} is redundant. This means, if $k < \min\{l \,/\, T(l,r) = \tau\}$, then all syzygies S_{ijr} of degree τ with $T(i,r) = T(j,r) = \tau$ are redundant. And in case $v := \min\{l \,/\, T(l,r) = \tau\} < k$ it means, that for all $j > v$ with $T(j,r) = \tau$ the syzygy S_{jkr} (or S_{kjr} if $k < j$) is redundant.

We consider now the remaining syzygies S_{ijr} in order to show that the procedure in 3.8 gives a reduced basis for the module $S^{(1)}$.

If $T(i,r) = T(j,r) = \tau$, then $T(i,j,r) = \tau$ and

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

showing, that S_{ir} and S_{jr} are equivalent, i.e. if one is taken to be a basis element, the other one is redundant. Since S_{ijr} is a remained syzygy, i is the minimal v with $T(v,r) = \tau$ and there is at most a $k > i$, such that $T(k,r)$ divides properly τ. In that case $M(j,r)$ holds for all S_{jr} of degree τ and S_{ikr} is also a remaining syzygy. Then

$$0 = \frac{\tau}{T(i,k)} S_{ik} - S_{ir} + \frac{\tau}{T(k,r)} S_{kr} ,$$

showing, that S_{ir} (and hence each S_{jr} of the same degree) is redundant in the case $\tau \neq T(i,k)$ or S_{ik} redundant, i.e. S'_{ik} in no U'_s .

In case S_{ijr} is a remaining syzygy of degree τ with $T(i,r) \neq \tau = T(j,r)$, then i is the minimal v , such that $T(v,r)$ divides properly τ and the same conclusion as before shows, that S_{jr} is redundant if $T(i,j) \neq \tau$ and equivalent to S_{ij} otherwise, i.e. it may be inserted into the same U_s as S_{ij}.

The case S_{ikr} of degree τ with $T(i,r) = \tau \neq T(k,r)$ is already considered. If $T(i,r)$ and $T(k,r)$ are both different from τ , then $T(k,r) = \tau$ is equivalent to $B_r(i,k)$. In that case S_{ik} (and every syzygy in the same U_s) is redundant. In any other case S_{ikr} is redundant or has no component 1 or -1.

This shows at the one hand, that the construction of 3.8 gives in fact bases $\{u_1,...,u_S\}$ of $S^{(1)}$ with $u_s \in U_s$, and at the other hand, that there is no S_{ijr} with a component 1 or -1 left, i.e. no further redundant syzygy in the basis.

3.10 In most examples known to the authors, the sets U_s are singletons or consist sometimes of two or three elements. Therefore the time consuming construction of the minimal basis by means of the sets U_s has to be balanced against the simple construction of the reduced basis by prop. 3.5. The construction in 3.8 is of theoretical interest. Since we never needed the characteristic of the field K, the length of a minimal basis of $S^{(1)}$ is independent of char (K). This is surprizing, because an example of Reisner (1976) showed, that the length of a minimal basis of the next module of syzygies (displaying the dependence relations among the elements of a minimal basis of $S^{(1)}$) depends in fact on char (K). For practical reasons however, we expect that the construction of Groebner bases using prop. 3.5 is to be prefered. We will describe and discuss this construction in the next section.

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). In forthcoming papers, Buchberger refined and adapted it for finding reduced Groebner bases, i.e. Groebner bases G, in which every $g \in G$ is irreducible w.r.t. $G \setminus \{g\}$. 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: $\{f_1, \ldots, f_r\} \subset P \setminus \{0\}$.

INITIALIZATION: $B := \{\{i,j\} \,/\, 1 \le i < j \le r\}$;

$G := \{f_1, \ldots, f_r\}$; $R := r$.

ITERATION: <u>while</u> $\{I,J\} \in B$ <u>repeat</u>

<u>if</u> $\neg$ criterion 1 <u>and</u> $T(I)T(J) \neq T(I,J)$ <u>then</u>

$h := S(f_I, f_J)$;

$h := NF(h,G)$;

<u>if</u> $h \neq 0$ <u>then</u>

$h := f_{R+1}$; $G := G \cup \{f_{R+1}\}$;

$B := B \cup \{\{i,R+1\} \,/\, 1 \le i \le R\}$;

$R := R+1$;

$B := B \setminus \{\{I,J\}\}$.

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

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 $K \in \{1,\dots,R\}\setminus\{I,J\}$ 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 Buchberger's algorithm is usually shown by means of definition 2.4 and some special arguments for the use of the criteria, see for instance Buchberger (1979).

Let us prove the correctness using 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. $\{I,K\} \notin B$, $\{J,K\} \notin B$, $T(I,J) = T(I,J,K)$, then let for simplicity of notation $I < J < K$. The syzygy S_{IJK} shows

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

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 $T(I)T(J) = T(I,J)$

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

as already shown in Buchberger (1965), and otherwise

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

Therefore at termination $B = \emptyset$, we have $S(f_I,f_J) \xrightarrow[G]{}{}^{+} 0$ for all 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 section 3 gives the following modification of Buchberger's algorithm.

```
INPUT:            {f_1,...,f_r} ⊂ P \ {0}.

INITIALIZATION: G := {f_1}; D := ∅ ;
                for t := 2 to r
                   D := syzBas(D,t);
                   G := G ∪ {f_t};
                R := r.

ITERATION:      while (I,J) ∈ D repeat
                   h := S(f_I,f_J);
                   h := NF(h,G);
                   if h ≠ 0 then
                      f_{R+1} := h;
                      D := syzBas(D,R+1);
                      G := G ∪ {f_{R+1}}; R := R+1;
                   D := D \ {(I,J)}.
```

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

Here the subalgorithm syzBas(D,t) calculates a set of pairs (i,j), $1 \leq i < j \leq t$, such that the corresponding syzygies S_{ij} constitute by proposition 3.5 together with some syzygies $S_{kl}, 1 \leq k < l \leq t$, satifying $T(k)T(l) = T(k,l)$ a reduced basis of

$$\{(g_1,...,g_t) \in P^t / \sum_{i=1}^{t} g_i \; T(i) = 0\}.$$

This subalgorithm works in the following way. Consider the sets $D_\tau := \{(i,t) \mid 1 \leq i \leq t, \; T(i,t) = \tau\}$. Call such set superfluous, if it is empty or if for one of its elements (i,t)(and hence for all of its elements) M(i,t) holds, or if it contains an (i,t) with $T(i)T(t) = T(i,t)$. Take from each non-superfluous D_τ the element (i,t) with minimal i and assign (i,t) to D. (The other $(j,t) \in D_\tau$ are redundant by F(j,t).) Cancel in D all elements (i,j) in the case $B_t(i,j)$ holds.

This is exactly the iterative construction of proposition 3.5 with $(i,t) \in D_\tau \iff S_{it} \in S_\tau$ but with the exception, that the first element of S_τ is not used if $\neg$ M(i,t) holds for $S_{it} \in S_\tau$ and $T(j)T(t) = T(j,t)$ for an $S_{jt} \in S_\tau$. As remarked in 3.7, we could use in place of the first in S_τ this S_{jt} as well and in that case $S(f_j,f_t) \xrightarrow[G]{}^{+} 0$ holds.

4.5 The correctness of the alg. 4.4 is shown in analogy to 4.3. Its termination results from the same arguments as the termination of alg. 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. The modification of alg. 4.4 is based on the following idea.

If the input elements $f_1,\ldots,f_r$ are ordered, such that $T(1) \geq_T \ldots \geq_T T(r)$, 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 $i \leq r$ 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}. Thus, when $T(i,j) = T(i)$, then f_i is removed from the actual G and in the forthcoming calls of syzBas(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 alg. 4.2 or faster applications of syzBas in alg. 4.4 resp. However, for several reasons it is to be expected that alg. 4.4 is faster than alg. 4.2, as the statistics in section 5 will confirm,

- 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 syzBas all possible tests are already done, before pairs (i,j) are assigned to D.

- If in the iteration of alg. 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 syzBas.

- Following a recommendation of Buchberger, in alg. 4.2 the pair $\{I,J\} \in B$ 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. syzBas selects among all (i,t) with $1 \le i < t$ 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 alg. 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 alg. 4.4 than in alg. 4.2.

4.8 The more general reduction strategy described in 3.8 gives minimal bases for the module of syzygies. By a different handling of the sets D in alg. 4.4 this reduction strategy could be employed. In contrast to the existing installation of alg. 4.4, it would require, that the elements of D are no more pairs but sets of equivalent pairs, as described in 3.8. If one element (i,j) of such set satisfies $B_t(i,j)$ or $T(i)T(j) = T(i,j)$, then the complete set can be removed from D. This modification producing a minimal basis of syzygies overlooks no application of a criterion 1 and 2. But in all examples we analyzed carefully, we obtained already by syzBas sets D, such that $\{S_{ij} / (i,j) \in D\}$ is a minimal basis. Therefore we have the impression, that for standard problems the additional amount of computations for guaranteeing all possible applications of the criteria is not justified. For a final discussion however, more experiences are needed.

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 alg. 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

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

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

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

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

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

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

$$f_8 := NF(S(f_4, f_7), G) = y^2x + 14y^2 - 8x^5 - 58x^4 + \frac{9}{2}x^2 + 9x$$

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			
Exple	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	.96
Ex5	6	6	l	RN	3	10	6	16/7	151	22	16.32	15/2	3	6	8.51
Ex27	7	6	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	.60	7/1	2	3	.56
Ex8	3	3	g	RN	3	4	6	3/5	12	6	.51	3/5	5	6	.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 (RF I)

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 resp.

l: maximal cardinality of G

m: computing time in seconds on a IBM 3090 mainframe

References

Bayer, D.A. (1982). The division algorithm and the Hilbert scheme, Ph.D. Thesis, Havard university.

Buchberger, B. (1965). Ein Algorithmus zum Auffinden der Basiselemente 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, pp. 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.

Hearn, A.C. (1986). REDUCE User's Manual: Version 3.2 The Rand Corporation, Santa Monica, CA 90406.

Jenks, R.D. (1986). Scratchpad II Computer Algebra System. IBM Thomas J. Watson Research Center, Yorktown Heigths, NY 10598.

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

Moeller, H.M. & Mora, F. (1986). New constructive methods in classical ideal theory. J. of Algebra 100, No. 1, pp. 138 - 178.

Reisner, G.A. (1976). Cohen-Macaulay quotients of polynomial rings. Adv. math. 21, pp. 30 -49.

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