On the Construction of Gröbner Bases Using Syzygies

H. MICHAEL MÖLLER

FB Mathematik und Informatik, Fern Universität, Lützowstr. 125, D-5800 Hagen, Fed. Rep. of Germany

(Received 21 October 1986)

Gröbner bases are useful for analysing multivariate polynomial ideals. For different coefficient domains $R$, it is shown how to construct (weak) Gröbner bases using bases of modules of syzygies, and under constructibility conditions on $R$ an algorithm for finding the required module bases is given. These methods are described in detail for principal ideal rings $R$. This leads to strong Gröbner bases and in case of fields $R$ the construction is the known Buchberger algorithm.

1. Introduction

For multivariate polynomials over fields, the concept of Gröbner bases was introduced by Buchberger (1965) and up to now solutions using Gröbner bases have been developed for many problems connected with polynomial ideals. For a survey, see Buchberger (1985). In Möller and Mora (1986) some of the properties characterising Gröbner bases are summarised and some connections with syzygies are pointed out.

An ordering in the set of polynomials and a simplification procedure (reduction) w.r.t. this ordering by a finite set $F$ of polynomials are two essential notions in this context. The algorithm of Buchberger for constructing a Gröbner basis uses the fact that it is sufficient to test only so-called $S$-polynomials for being reducible to zero. Here, each $S$-polynomial depends on exactly two polynomials of $F$.

Gröbner bases are generalised by some authors to polynomials over rings $R$. Buchberger (1983) introduced reduction rings $R$, such that in $R[X_1,\ldots,X_n]$ the Buchberger algorithm can be easily adopted. These rings and the Buchberger algorithm have also been studied by Winkler (1984) and Stifter (1985). If $R$ is a Euclidean ring, Kandri-Rody & Kapur (1984) extended Gröbner bases to $R[X_1,\ldots,X_n]$ using the natural ordering in the Euclidean ring. Considering principal ideal rings $R$ with a special ordering, Pan (1985) generalised Gröbner bases to polynomial rings over such $R$.

For commutative Noetherian rings $R$ (with additional conditions concerning constructibility and uniqueness of some elements), Gröbner bases are introduced in $R[X_1,\ldots,X_n]$ by Trinks (1978), Zacharias (1978) and Schaller (1979), partially based on papers of Spear (1977) and Lauer (1976). By means of an explicit or implicit use of syzygies, they interpreted $S$-polynomials anew. Here, $S$-polynomials depend in general on more than two polynomials. Also, the reduction had to be generalised to what we will call weak reduction (and consequently we will call the reduction of Buchberger et al. strong reduction and the respective Gröbner bases weak and strong Gröbner bases). Weak Gröbner bases and weak reductions are studied in a broader context by Robbiano (1986). For non-commutative rings $R$, see Mora (1986).
The intention of this paper is to show the systematic use of syzygies in order to construct Gröbner bases starting with arbitrary commutative rings and ending with a presentation of Buchberger’s algorithm for polynomials over Euclidean rings. If $R$ is a commutative Noetherian ring, we give in terms of syzygies some equivalent conditions for weak Gröbner bases, show the connection with the different concepts of Trinks (1978), Zacharias (1978) and Schaller (1979) and give a new recursive procedure for constructing bases of modules of syzygies. This procedure allows a very efficient algorithm for constructing weak Gröbner bases.

Considering only unique factorisation rings, we show that Buchberger’s algorithm works with $S$-polynomials depending on only two polynomials for arbitrary finite sets of input polynomials exactly if $R$ is a principal ideal ring (with suitable constructibility conditions). This is an easy consequence of proposition 1 and the following example and shows that the concept of reduction rings is naturally restricted to principal ideal rings. Also strong reductions exist in general only if $R$ is a principal ideal ring, as elementary arguments show. Therefore there is only sense to define strong Gröbner bases in rings $R[X_1, \ldots, X_n]$ with a principal ideal ring $R$.

In section 4 we specify the results on weak Gröbner bases and weak reductions to polynomials over PIR’s and introduce the strong Gröbner bases and reductions. Strategies are presented for keeping the bases of the modules of syzygies restricted. This leads to a new Buchberger algorithm for polynomials over principal ideal rings, where, as with the criteria of Buchberger (1979) for detecting unnecessary $S$-polynomials, many $S$-polynomials have not to be considered. An installation of this algorithm already exists in SCRATCHPAD II for polynomials over Euclidean rings, see Gebauer & Möller (1987). An example concludes the paper.

In contrast with many of the articles quoted above, we did not deal with questions of uniqueness of special Gröbner bases in order to concentrate on the role of syzygies.

2. Characterisation of Weak Gröbner Bases

Let $R$ be a commutative ring with identity, $\mathcal{P} := R[X_1, \ldots, X_n]$, and $T$ the set of terms (power products) $\varphi = X_1^{i_1} \ldots X_n^{i_n}$ with $i_1, \ldots, i_n \in \mathbb{N}_0$. As usual, $T$ is ordered by $\prec_T$ such that

\[ 1 = X_1^0 \ldots X_n^0 \preceq_T \varphi \quad \text{for all } \varphi, \varphi_1, \varphi_2 \in T. \]

For

\[ f = \sum_{i=1}^r c_i \varphi_i \]

with $c_i \in R \setminus \{0\}$, $\varphi_1 <_T \ldots <_T \varphi_r$, let

\[ \text{lc}(f) := c_r, \quad \text{lt}(f) := \varphi_r, \quad M_T(f) := c_r \varphi_r \]

be the leading coefficient, the leading term and the maximal part of $f$ respectively. For avoiding a separate treatment of the zero polynomial, we define

\[ \text{lc}(0) := \text{lt}(0) := M_T(0) := 0 \]

and extend $<_T$ to $T \cup \{0\}$ by $0 <_T \varphi$ for all $\varphi \in T$. 

DEFINITION. Let $I$ be an ideal in $\mathcal{P}$. Then $F = \{f_1, \ldots, f_r\} \subset I$ is called a weak Gröbner basis of $I$ if the ideal

$$M_T(I) := \left\{ \sum_{k=1}^m M_T(g_k) \mid m \in \mathbb{N}, g_k \in I \right\}$$

is generated by $\{M_T(f_1), \ldots, M_T(f_r)\}$.

In theorem 1 we will show that weak Gröbner bases are, in fact, ideal bases. Hence, if every ideal in $\mathcal{P}$ has a weak Gröbner basis, then $\mathcal{P}$ and its subring $R$ are Noetherian. Conversely, if $R$ is Noetherian, every ideal in $\mathcal{P}$ has a weak Gröbner basis, because $\mathcal{P}$ is in this case Noetherian by the Hilbert Basis Theorem and then any ideal $M_T(I)$ has a finite basis $\{M_T(f_1), \ldots, M_T(f_r)\}$. Thus, in the following, $R$ will always denote a (commutative) Noetherian ring with identity.

DEFINITION. Let $I = (f_1, \ldots, f_r)$, i.e. $f_1, \ldots, f_r \in I$ and for all $f \in I$ polynomials $g_1, \ldots, g_r \in \mathcal{P}$ exist, such that $f$ has the representation

$$f = \sum_{i=1}^r g_i f_i.$$ 

We call this representation a weak Gröbner representation of $f$ (in terms of $f_1, \ldots, f_r$) if

$$\lt(f) = \max_{i=1}^r \lt(g_i) \lt(f_i).$$

DEFINITION. For a preassigned tuple $M := (M_T(f_1), \ldots, M_T(f_r))$, we call $G = (g_1, \ldots, g_r) \in \mathcal{P}^r$ a syzygy w.r.t. $M$, if

$$\sum_{i=1}^r g_i M_T(f_i) = 0,$$

and call $G$ is homogeneous of degree $\phi$, if $\phi \in T$ and $g_i = 0$ or $g_i = M_T(g_i)$, $\lt(g_i) \lt(f_i) = \phi$, $i = 1, \ldots, r$.

The set $S = S(M)$ of all syzygies with respect to the same tuple $M = (M_T(f_1), \ldots, M_T(f_r))$ is called the module of syzygies (w.r.t. $M$). Clearly, $S$ is homogeneous, i.e. any $G \in S$ splits into a sum of homogeneous $r$-tuples, all of them being in $S$, too.

DEFINITION. Let $F = \{f_1, \ldots, f_r\} \subset \mathcal{P}$ and $f, g \in \mathcal{P}$. We say $f$ reduces weakly to $g$ modulo $F$, for short $f \preceq_T g$, if $\lt(g) <_T \lt(f)$ and $f - g$ has a weak Gröbner representation in terms of $F$. $\preceq_T$ denotes the reflexive transitive closure of $\preceq_T$. The reduction $\preceq_T$ is Noetherian, because

$$g_1 \preceq_T g_2 \preceq_T \ldots$$

we have $\lt(g_1) >_T \lt(g_2) >_T \ldots$ and hence no $\lt(g_i)$ is a multiple of a preceding $\lt(g_j), j < i$.

This gives an ascending chain of ideals

$$(\lt(g_1)) \subset (\lt(g_1), \lt(g_2)) \subset (\lt(g_1), \lt(g_2), \lt(g_3)) \subset \ldots$$

which is finite because $\mathcal{P}$ is Noetherian.

THEOREM 1. Let

$$F = \{f_1, \ldots, f_r\} \subset \mathcal{P}, \quad I = (f_1, \ldots, f_r) \quad \text{and} \quad M = (M_T(f_1), \ldots, M_T(f_r)).$$

Then the following conditions are equivalent:

(C1) $F$ is a weak Gröbner basis of $I$.
(C2) Every $f \in I$ has a weak Gröbner representation in terms of $F$.
(C3) Let $G_1, \ldots, G_m$ be a basis of $S(M)$, $G_i = (g_{i1}, \ldots, g_{ir})$ homogeneous of degree $\phi_i, i = 1, \ldots, m$. Then any so-called $S$-polynomial $\sum_{j=1}^{r} g_{ij} f_j$ has a weak Gröbner representation in terms of $F$.
(C4) $f^w F^w + 0$ for every $f \in I$.
(C5) With $G_1, \ldots, G_m$ as in C3

$$\sum_{j=1}^{r} g_{ij} f_j^w F^w + 0, \quad i = 1, \ldots, m.$$

PROOF. C1$\Rightarrow$C2: Let $f \in I$ and let a weak Gröbner representation already exist for all $g \in I$, $lt(g) <_T lt(f)$. Then, by C1

$$M_T(f) = \sum_{i=1}^{r} h_i M_T(f_i), \quad h_i \text{ homogeneous},$$

and w.l.o.g. $lt(h_i)lt(f_i) = lt(f)$ or $h_i = 0, i = 1, \ldots, r$. Using a weak Gröbner representation for

$$f' := f - \sum_{i=1}^{r} h_i f_i$$

(by construction $lt(f') <_T lt(f)$!),

$$f' = \sum_{i=1}^{r} g_i f_i, \quad lt(g_i)lt(f_i) \leq_T lt(f') <_T lt(f),$$

we get for $f$ the weak Gröbner representation

$$f = \sum_{i=1}^{r} (h_i + g_i) f_i.$$

C2$\Rightarrow$C3: Each $S$-polynomial is in $I$.

C3$\Rightarrow$C1: Let $f \in I$. We will show $M_T(f) \in (M_T(f_1), \ldots, M_T(f_r))$. Consider an arbitrary representation

$$f = \sum_{i=1}^{r} g_i f_i, \quad \phi := \max lt(g_j)lt(f_j).$$

If $lt(f) = \phi$, we have

$$M_T(f) = \sum_{j \in J} M_T(g_j) M_T(f_j) \quad \text{with} \quad J := \{j | lt(g_j)lt(f_j) = \phi\},$$

i.e. $M_T(f) \in (M_T(f_1), \ldots, M_T(f_r))$. Else $lt(f) <_T \phi$. But then

$$0 = \sum_{j \in J} M_T(g_j) M_T(f_j).$$

Hence

$$G := \sum_{j \in \phi} M_T(g_j) e_j \in S(M),$$

where $e_j$ denotes the $j$th unit vector. Using the basis \{G_1, \ldots, G_m\} of $S(M)$ and the weak Gröbner representations

$$\sum_{j=1}^{r} g_{ij} f_j^w F^w + 0, \quad i = 1, \ldots, m,$$
we get
\[ G = \sum_{i=1}^{n} u_i G_i, \quad u_i = 0 \quad \text{or} \quad \text{l}_t(u_i) \phi_i = \phi \]
and
\[
\sum_{j \in J} M_T(g_j) f_j = \sum_{i=1}^{n} u_i \sum_{j=1}^{r} g_{ij} f_j = \sum_{j=1}^{r} \left\{ \sum_{i=1}^{n} u_i h_{ij} \right\} f_j.
\]

The maximal term on the left-hand side is \( \phi \), on the right-hand side \( <_T \phi \). Therefore, replacing in \( f = \sum g_i f_i \) the summand
\[
\sum_{j \in J} M_T(g_j) f_j \quad \text{by} \quad \sum_{j=1}^{r} \left\{ \sum_{i=1}^{n} u_i h_{ij} \right\} f_j,
\]
we obtain a representation for \( f \) with a maximal term \( <_T \phi \). An iterative application of this procedure gives finally a weak Gröbner representation of \( f \) and, as shown above, the maximal terms in this representation imply
\[ M_T(f) \in (M_T(f_1), \ldots, M_T(f_r)). \]

C1 \( \Rightarrow \) C4 is proved as C1 \( \Rightarrow \) C2. C4 \( \Rightarrow \) C5 is obvious. For C5 \( \Rightarrow \) C3 take in
\[
\begin{align*}
\phi := & \sum_{j=1}^{r} g_{ij} f_j \forall \ f_1 \forall \ f_2 \ldots \forall \ f_s \quad h_0 := 0
\end{align*}
\]
the weak Gröbner representations of \( h_0 - h_1, h_1 - h_2, \ldots, h_{s-1} - h_s \) and sum it up obtaining a weak Gröbner representation for \( h_0 \). \( \square \)

In theorem 1 we expressed the conditions characterising weak Gröbner bases in terms of \( \mathcal{O} \), the ring of polynomials over \( R \). This parallels the result known for polynomials over fields as in Möller & Mora (1986). The definitions and results for polynomials over commutative rings by Trinks (1978), Zacharias (1978) and Schaller (1979) are mostly given in terms of \( R \). The relationship with these results is easily established. Consider, for instance, the weak reduction. A given \( f \in \mathcal{O} \) is weakly reducible modulo \( F = \{f_1, \ldots, f_r\} \) to a polynomial \( g \), if \( f - g \) has a weak Gröbner representation in terms of \( F \). Because of \( \text{l}_t(g) <_T \text{l}_t(f) \), the maximal part of \( f \) and \( f - g \) coincide. This means that \( \text{l}_t(f) = \text{l}_t(f - g) \) and that
\[
\text{l}_c(f) = \sum_{j \in J} d_j \text{l}_c(f_j) \quad \text{with} \quad J = \{j \mid \text{l}_t(f_j) / \text{l}_t(f)\}
\]
holds for suitable \( d_j \in R \). But (1) is already sufficient for \( f \) to be weakly reducible modulo \( F \),
\[
f \forall f \quad f - \sum_{j \in J} d_j \frac{\text{l}_t(f)}{\text{l}_t(f_j)} f_j.
\]
Admitting only these reductions, Zacharias used C4 for defining (weak) Gröbner bases, and Trinks called a sequence of such reductions "D-Folge".

The connection with syzygies is mentioned by all three authors, but only Zacharias used the notion syzygy. We observe that in a homogeneous syzygy w.r.t. \( M = (M_T(f_1), \ldots, M_T(f_r)) \), all components can be divided by a term, such that \( (c_1 \phi_1, \ldots, c_r \phi_r) \), a syzygy w.r.t. \( M \) of degree \( \phi \), is obtained with
\[
\phi = \text{lcm} \{ \text{l}_t(f_j) \mid c_i \neq 0 \},
\]
and necessary and sufficient for being a syzygy of degree \( \phi \) is
\[
0 = \sum_{i=1}^{r} c_i \text{l}_c(f_j).
\]
Obviously at most $2^r$ different $\phi$'s satisfying (2) exist. Considering only homogeneous syzygies with $\phi$ as in (2), and using that all such syzygies of the same degree $\phi$ constitute a linear space $V(\phi)$, Trinks remarked that instead of requiring $f \neq 0$ for all $f \in I$ it suffices to consider only $S$-polynomials depending on syzygies which belong to a basis of one $V(\phi)$, i.e. he used $C5$ implicitly for defining (weak) Gröbner bases. Schaller used the notion "complete basis" for weak Gröbner bases and "simple representation" for weak Gröbner representation and $C2$ for defining weak Gröbner bases. Whereas Zacharias proposed a construction of a basis of $S(M)$ similar to Trinks, Schaller showed that a basis of $S(M)$ is obtained by constructing the module of syzygies $S \subset R^r$,

$$\left\{(c_1, \ldots, c_r) \in R^r \mid \sum_{i=1}^r c_i lc(f_i) = 0\right\}$$

say $C_1, \ldots, C_m$ with $C_i = (c_{i1}, \ldots, c_{ir})$, $i = 1, \ldots, m$, and then a basis of $S(M)$ is given by $G_1, \ldots, G_m$ with $G_i = (g_{i1}, \ldots, g_{ir})$,

$$g_{ij} = c_{ij} \frac{lcm(|lt(f_h)|)}{lt(f_j)} \quad j = 1, \ldots, r, \quad i = 1, \ldots, m.$$ 

### 3. An Iterative Construction of Weak Gröbner Bases

To construct weak Gröbner bases using $C3$ or $C5$ of theorem 1, some bases of modules of syzygies have to be considered until a weak Gröbner basis is found. Therefore it is more practical not to calculate each single module basis separately but to construct the basis of the next module by using the previous one.

Denoting

$$M_k := (M(f_1, \ldots, M(f_k)), \quad k = 1, 2, \ldots,$$

we will construct a basis for $S(M_k)$ using a basis of $S(M_{k-1})$. The initialisation of this procedure is easy because $S(M_1)$ is generated by $\{e \in R \mid e lc(f_1) = 0\}$, which is $\{0\}$ in case $R$ is an integral domain and $f_1 \neq 0$. For convenience of notation we write

$$c_i := lc(f_i), \quad \phi_i := lt(f_i), \quad i = 1, \ldots, r.$$ 

Our main tool in this paragraph will be the mapping

$$\pi_r : S(M_r) \to R, \quad \pi_r : (g_1, \ldots, g_r) \to lc(g_r).$$

We have

$$im\pi_r = (c_1, \ldots, c_{r-1}) : (c_r)$$

and

$$ker \pi_r = (S(M_{r-1}), 0) = \{(g_1, \ldots, g_{r-1}, 0) \mid (g_1, \ldots, g_{r-1}) \in S(M_{r-1})\}.$$ 

(The representation for the kernel is obvious, the identity for $im\pi_r$ will be clear from the following theorem.)

**Definition.** For $J \subseteq \{1, \ldots, r\}$ let $\phi(J) := lcm\{\phi_j \mid j \in J\}$ and $J$ is maximal for $\phi \in T$ if $\phi_j/\phi \Leftrightarrow j \in J$. We call a set $J \subseteq \{1, \ldots, r\}$ basic, if $r \in J$ and $J$ is maximal for $\phi(J)$. If $J$ is basic, $J^* := J \setminus \{r\}$ and $b_r \in (\phi_j \mid j \in J^*) : (c_r)$, i.e.

$$\sum_{j \in J^*} b_j c_j + b_r c_r = 0 \quad \text{for suitable } b_j \in R,$$

then

$$\sum_{j \in J^*} b_j \frac{\phi(J)}{\phi_j} e_j + b_r \frac{\phi(J)}{\phi_r} e_r.$$
where \( e_i \) denotes the \( i \)th unit vector, is a homogeneous syzygy of \( S(M_r) \) of degree \( \phi(J) \), which we call associated to \( b \) and \( J \).

**Theorem 2.** For any basic \( J \) let \( \{b(1, J), \ldots, b(s_J, J)\} \) with \( b(i, J) \neq 0 \) for \( i = 1, \ldots, s_J \), be a basis of \( (e_j \mid j \in J \setminus \{r\}) : (e_r) \). Let \( B(i, J) \) be associated to \( b(i, J) \) and \( J, i = 1, \ldots, s_J \). If \( \{A_1, \ldots, A_m\} \) is a homogeneous basis of \( S(M_{r-1}) \), then

\[
\{(A_1, 0), \ldots, (A_m, 0)\} \cup \bigcup_{j \in J_{\text{basic}}} \{B(i, J) \mid 1 \leq i \leq s_J\}
\]

is a homogeneous basis of \( S(M_r) \).

**Proof.** Let \( G = (g_1, \ldots, g_r) \in S(M_r) \), \( g_r \neq 0 \) and w.l.o.g. \( G \) homogeneous of degree \( \phi \). Let \( J_1 := \{j \mid g_j \neq 0\} \). By homogeneity \( j \in J_1 \Rightarrow \phi_j / \phi_j \), i.e. \( \phi(J_1) / \phi \). Let \( J = \{j \mid \phi_j / \phi(J_1)\} \). Then by construction \( \phi(J_1) / \phi(J) \) but \( J_1 \subseteq J \), i.e. \( \phi(J_1) = \phi(J) \). Since \( r \in J_1 \subseteq J \), \( J \) is basic.

Since \( G \) is homogeneous of degree \( \phi \),

\[
g_j = lc(g_j) \cdot \frac{\phi}{\phi_j} \quad \text{for } j \in J_1 \quad \text{and} \quad g_j = 0 \quad \text{for } j \notin J_1.
\]

\( G \in S(M_r) \) means

\[
\sum_{j \in J} lc(g_j) \cdot \frac{\phi}{\phi_j} \cdot c_j \phi_j = 0.
\]

This gives \( lc(g_r) \in (e_j \mid j \in J \setminus \{r\}) \) or, equivalently,

\[
lc(g_r) \in (e_j \mid j \in J \setminus \{r\}) : (e_r).
\]

Hence, a representation

\[
lc(g_r) = \sum_{j=1}^{s_J} u_j b(i, J) \quad \text{with } u_j \in R
\]

exists. The syzygies \( B(i, J) \) are homogeneous of degree \( \phi(J) \). Therefore

\[
G = \sum_{i=1}^{s_J} u_i \cdot \frac{\phi}{\phi(J)} B(i, J) \in S(M_r)
\]

is homogeneous of degree \( \phi \) and belongs to \( \ker \pi_r \). Hence,

\[
G = \sum_{i=1}^{s_J} u_i \cdot \frac{\phi}{\phi(J)} B(i, J) + \sum_{i=1}^{m} h_i (A_i, 0)
\]

with appropriate \( h_i \in \mathcal{P} \). Since \( G \) was arbitrary, the assertion is proven. \( \square \)

In the basis of \( S(M_r) \) as given in theorem 2, only syzygies occur which are homogeneous of a degree \( \phi(J) \), \( J \subseteq [1, \ldots, r] \). But usually some of them are redundant. This is caused by two reasons.

First, there may be some \( (A_i, 0) \) of degree \( \phi(J) \), \( J \subseteq [1, \ldots, r-1] \), and \( \phi_r \) divides \( \phi(J) \), such that in the basis of \( S(M_r) \) also some \( B(j, J_1) \) of degree \( \phi(J) \) exist \( (J \subseteq J_1, r \in J_1, \phi(J_1) = \phi(J)) \). These \( (A_i, 0) \) and \( B(j, J_1) \) may be linearly dependent.

Second, if \( J_1 \) and \( J_2 \) are maximal but \( J_1 \neq J_2 \), then \( \phi(J_1) / \phi(J_2) \) and

\[
(c_j \mid j \in J_1) : (c_r) \subseteq (c_j \mid j \in J_2) : (c_r).
\]

Therefore, \( B(i, J_1) \phi(J_2) / \phi(J_1) \) is associated to \( b \) and \( J_2 \) if \( B(i, J_1) \) is associated to \( b \) and \( J_1 \). Hence, enlarging a basis of \( (c_j \mid j \in J_1) : (c_r) \), say \( b(1, J_1), \ldots, b(s_{J_1}, J_1) \), to a basis of \( (c_j \mid j \in J_2) : (c_r) \) and taking the corresponding \( B(i, J_1) \phi(J_2) / \phi(J_1) \) associated to \( b(i, J_2) \) and \( J_2 \) for \( B(i, J_2) \), then \( B(i, J_2) \) being a multiple of \( B(i, J_1) \) is redundant in the basis of \( S(M_r) \).
If in the basis of $S(M_r)$ one element is an $r$-tuple with exactly one non-zero component, say the $j$th one, then $f_j = 0$ or $c_j$ is a zero divisor. For excluding these trivial cases, we assume $f_j \neq 0, j = 1, \ldots, r$, and $R$ is an integral domain. Then the sparsest elements are those with two non-zero components.

**Definition.** We call a homogeneous basis of $S(M_r)$ a principal basis if every basis element has exactly two non-zero components.

**Proposition 1.** If $R$ is a principal ideal ring and if

$$M_r := (M_r(f_1), \ldots, M_r(f_r)) \in (\mathbb{P} \setminus \{0\})^r,$$

then $S(M_r)$ has a principal basis.

**Proof.** With respect to theorem 2 it is sufficient to show that for any basic $J$ a basis $\{b(1, J), \ldots, b(s, J)\}$ of $(c_j | j \in J, j \neq r) : (c_r)$ exists, such that there are associated $B(i, J), i = 1, \ldots, s$, having exactly two non-vanishing components. Let $J^* := J \setminus \{r\}$.

Since $R$ is a principal ideal ring,

$$(c_j | j \in J^*) = (gcd\{c_j | j \in J^*\}),$$

$$(c_j) \cap (c_r) = (lcm\{c_j, c_r\}) \quad \text{for } j \in J^*$$

holds. In particular, $R$ is a unique factorisation ring. Therefore,

$$(lcm\{gcd\{c_j | j \in J^*\}, c_r\}) = (gcd\{lcm\{c_j, c_r\} | j \in J\})$$

holds. This gives

$$(c_j | j \in J^*) \cap (c_r) = \sum_{j \in J^*} (c_j) \cap (c_r),$$

or equivalently

$$(c_j | j \in J^*) : (c_r) = \sum_{j \in J^*} (c_j) : (c_r).$$

Hence, if $u_j$ generates $(c_j) : (c_r)$, then $\{u_j | j \in J^*\}$ is a basis of $(c_j | j \in J^*) : (c_r)$. Associated to $u_j$ and $\{j\}$ and hence to $u_j$ and $J$ is

$$B_j := -\frac{u_j c_j \phi(j, r)}{\phi_j} e_j + \frac{u_j \phi(j, r)}{\phi_r} e_r. \tag{3}$$

If $R$ is a unique factorisation ring (and if no $f_i$ is zero), we can show that each module $S(M_r)$ has a principal basis only if $R$ is a principal ideal ring. For this converse of proposition 1, it is sufficient to give an example of an $R$-module $S(M_3)$ which has no principal basis, and $R$ is a unique factorisation ring but not a principal ideal ring.

In that case, $c_1, c_2 \in R$ exist, such that $(c_1, c_2)$ is not the principal ideal $(gcd\{c_1, c_2\})$. Dividing out common factors and denoting the remainders again $c_1, c_2$, we have $c_1, c_2 \in R$ without common divisor and $1 \notin (c_1, c_2)$. Let $c_3 := c_1 + c_2$. Then $c_3$ has no divisor in common with $c_1$ and no one with $c_2$. Let $\varphi \in T$ be arbitrary and

$$M_3 := (c_1 \varphi, c_2 \varphi, c_3 \varphi).$$

If $(g_1, 0, g_3)$ and $(0, h_2, h_3)$ are homogeneous basis elements of $S(M_3)$, then

$$\pi_3(g_1, 0, g_3) = g_3 \in (c_1) : (c_3) = (c_1),$$

$$\pi_3(0, h_2, h_3) = h_3 \in (c_2) : (c_3) = (c_2).$$
Hence, for any \( G \in S(M_3) \) with
\[
G = \sum u_1(g_{11}, 0, g_{21}) + \sum u_2(0, h_{21}, h_{31}) + \sum w(k_{11}, k_{21}, 0),
\]
we have \( \pi_3(G) \in (c_1, c_2) \). But \((-1, -1, 1) \in S(M_3) \) and
\[
\pi_3(-1, -1, 1) \neq (c_1, c_2).
\]
Hence, this \( S(M_3) \) has no principal basis.

For the computation of a basis of \( S(M_r) \) by theorem 2 it is sufficient to be able to compute syzygies associated to a \( b \in R \) and a \( J \subseteq \{1, \ldots, r\} \). This is guaranteed by the following two computability requirements:

1. Ideals in \( R \) are detachable. That is there exists an algorithm, which, given \( c \in R \) and a finite set \( \{c_1, \ldots, c_r\} \subseteq R \), decides whether \( c \in (c_1, \ldots, c_r) \) and if so, produces \( u_1, \ldots, u_r \in R \) such that \( c = u_1c_1 + \ldots + u_rc_r \).

2. Ideal quotients in \( R \) are computable. That is, there exists an algorithm, which, given \( c \in R \) and a finite set \( \{c_1, \ldots, c_r\} \subseteq R \), produces a (finite) basis of the ideal \((c_1, \ldots, c_r) : (c) = \{d \in R \mid dc \in (c_1, \ldots, c_r)\}\).

These two conditions are essentially due to Zacharias (1978) who required in place of our second condition, that syzygies in \( R \) are solvable. Our condition, together with theorem 2, gives her second condition, but conversely using the projection \( \pi \), we see whenever syzygies in \( R \) are solvable, then also ideal quotients are computable, i.e. both second conditions are equivalent by theorem 2.

For Noetherian rings \( R \) with the two computability conditions the weak reduction can be performed too, because by the first condition, \( h_1, \ldots, h_r \) can be found, such that \( M_r(f) = \Sigma h_iM_r(f_i) \) and hence \( f \subseteq f - \Sigma h_if_i \). Then condition C5 of theorem 1 gives an algorithm for computing \( \text{Gröbner bases} \):

If an \( S \)-polynomial \( \sum g_i f_j \) is not weakly reducible to 0 modulo \( F = \{f_1, \ldots, f_r\} \), its 0-reducibility can be forced by enlarging \( F \). Let \( \sum g_i f_j w^+h_i \neq 0 \). Then \( \sum g_i f_j \) is weakly reducible to 0 modulo \( F' := F \cup \{h_i\} \),
\[
\sum_{j=1}^r g_i f_j w^+h_i \neq 0.
\]

Then the \( S \)-polynomials corresponding to a basis of \( S(M_r(f_1), \ldots, M_r(f_r), M_r(f_{r+1})) \) with \( f_{r+1} := h_i \) have to be weakly reduced. Some of the new \( S \)-polynomials may weakly reduce to 0 mod. \( F' \), but when a reduction to an \( h \neq 0 \) occurs, \( F' \) is enlarged again. The procedure indicated here is the translation of Buchberger's algorithm, which was given by Buchberger (1965) for polynomials over fields. Trinks (1978), Zacharias (1978) and Schaller (1979) elaborated this procedure to algorithms for obtaining weak \( \text{Gröbner bases} \) in polynomial rings over computable commutative Noetherian rings. However, none of these authors mentioned a recursive computation of the module bases as in theorem 2. Such recursion increases the efficiency of the computation: Since a basis element \( A_i \) in \( S(M_{r-1}) \) and the basis element \( (A_i, 0) \) in \( S(M_r) \) have the same \( S \)-polynomial, it is sufficient to test the \( S \)-polynomials once and not for each basis separately. Hence, if the polynomial set \( F \) is enlarged, the only new \( S \)-polynomials are those corresponding to the basis elements denoted by \( B(i, J) \) in theorem 2. In addition, as indicated in the remark following theorem 2, not all \( S \)-polynomials corresponding to the \( B(i, J) \) and \( (A_i, 0) \) have to be used. We will study this in more detail in the next paragraph for polynomials over principal ideal rings.
4. Gröbner Bases in Principal Ideal Rings

In the following, $R$ is always a principal ideal ring and $F$ a finite set of polynomials $f_i \neq 0$ in $\mathcal{P} = R[X_1, \ldots, X_n]$ with $c_i = \text{lcm}(f_i)$, $\phi_i = \text{lcm}(f_i)$, $i = 1, 2, \ldots$. For any subset $\{f_j | j \in J\} \subseteq F$, let

\[ c_j = \text{lcm}(c_j | J), \quad \phi(J) = \text{lcm}(\phi_j | j \in J), \quad T(J) = c_j \phi(J). \]

Using \((c_j) : (c_i) = (c_j / c_i)\), proposition 1 shows that $S(M_r)$ with

\[ M_r = (M_r(f_1), \ldots, M_r(f_i)) \]

has the principal basis $\{B_{ij} | 1 \leq j < k \leq r\}$,

\[ B_{ij} = \frac{T(j, k)}{T(j)} e_j - \frac{T(i, k)}{T(k)} e_k. \]

If $R$ is a field, $T(j, k) = \phi(j, k)$ because of $c_k = 1$, and then the $S$-polynomial corresponding to $B_{jk}$ is

\[ \frac{1}{c_j} \frac{\phi(j, k)}{\phi_j} f_j = \frac{1}{c_k} \frac{\phi(j, k)}{\phi_k} f_k. \]

This is the original $S$-polynomial $S(f_j, f_k)$ of Buchberger (1965).

As we have already remarked, the basis for $S(M_r)$ as constructed in theorem 2 (possibly) contains redundant elements. In the special instance considered here, we can detect such elements using the identity

\[ T(i, j) = T(i, k) B_{ik} + B_{jk} = 0, \quad (4) \]

which holds for arbitrary $i, j, k \in \{1, \ldots, r\}$. In case one coefficient, say $T(i, j, k)/T(i, j)$, is 1 we see using (4), that $B_{ij}$ is a redundant basis element and $T(i, k)$ and $T(j, k)$ both divide $T(i, j)$.

**Definition.** We say criterion $B$ holds for $(i, j)$ if $i < j < r$, $T(r)/T(i, j)$ and

\[ T(i, r) \neq T(i, j) \neq T(j, r). \]

We say criterion $M$ holds for $(i, r)$ if $i < r$ and

\[ \exists j < r: T(j, r)/T(i, r) \neq T(j, r). \]

We say criterion $F$ holds for $(i, r)$ if $i < r$ and

\[ \exists j < i: T(j, r) = T(i, r). \]

We also write briefly in these cases $B_i(i, j)$, $M_i(r)$, or $F(i, r)$ respectively.

These criteria were formulated by Gebauer & Möller (1988) for polynomials over fields and used for removing redundant elements in the principal basis $\{B_{ij} | 1 \leq i < j \leq r\}$. We state explicitly that these criteria require only lcm computations of ring elements and terms.

**Theorem 3.** A basis of $S(M_r)$ is given by

\[ \{B_{ij} | 1 \leq i < j \leq r, \neg M(i, j), \neg F(i, j), \forall k > j: \neg B_{k(i, j)}\}. \]
PROOF. We order the basis \( \{B_{ij} \mid 1 \leq i < j \leq r \} \) partially by \( B_{ij} < B_{kl} \) if

\[
T(i, j)/T(k, l) \neq T(i, j)
\]

or if \( T(i, j) = T(k, l) \) and \( j < l \) or if \( T(i, j) = T(k, l), j = l \) and \( i < k \).

If \( B_k(i, j) \) holds, then in any basis representation

\[
G = \sum g_{m} B_{mv}, \quad g_{m} \in \mathcal{P},
\]

\( B_{ij} \) can be replaced using (4) by \( B_{ik} \) and \( B_{j} \), and \( B_{ik} < B_{ij} \) holds. This can be done for arbitrary \( B_{ij} \) satisfying a criterion \( B_k \), i.e. for all \( G \in S(M_i) \) basis representations exist where no such \( B_{ij} \) occurs. The same arguments hold for criteria \( M \) and \( F \). \( \square \)

**Definition.** Let \( f, g \in \mathcal{P} \). We say \( f \) reduces strongly to \( g \) modulo \( F \), for short \( f \stackrel{S}{\sim} g \), if

\[
\text{lt}(g) <_{r} \text{lt}(f) \quad \text{and} \quad \exists f_i \in F, \exists h \in \mathcal{P}: g = f - h f_i.
\]

The reflexive transitive closure of \( \stackrel{S}{\sim} \) is denoted by \( \stackrel{S}{\sim} \).

The same arguments as for \( \stackrel{S}{\sim} \) give that \( \stackrel{S}{\sim} \) is also Noetherian. Since \( h f_i \) is already a weak Gröbner representation in terms of \( F \), a polynomial \( f \) reduces weakly (to another polynomial) modulo \( F \), if it reduces strongly.

A polynomial \( f \) reduces strongly if and only if \( M_F(f) \) is a multiple of an \( M_F(f_i) \), \( f_i \in F \). In that case

\[
f \stackrel{S}{\sim} f - \frac{M_F(f)}{M_F(f_i)} f_i.
\]

This criterion is considerably simpler than the corresponding one for the weak reduction as the derivation of equation (1) shows. But there are more polynomials weakly reducible than strongly. For instance, let \( \mathcal{P} = \mathbb{Z}[x, y], F = \{2x, 3y\}, f = xy \). Then \( f \not\equiv 0 \), because \( f - 0 \) has the weak Gröbner representation \( 2y \cdot 2x - x \cdot 3y \), and \( f \) does not reduce strongly modulo \( F \).

In order to be able to reduce strongly all polynomials which are weakly reducible mod. \( F \), we enlarge \( F \) to a set \( C(F) \) and use \( f \not\equiv 0 \) A similar procedure was used by Schaller (1979) in simplification rings by introducing the set of kernel polynomials.

**Definition.** Let \( F = \{f_1, \ldots, f_r\} \) and \( I \) the ideal generated by \( F \). We call a set \( M \) a completion of \( F \), briefly \( C(F) \), if it contains for every \( J \), maximal for \( \phi(J) \), a polynomial \( f_j \in I \) with \( \text{lt}(f_j)/\phi(J) \) and \( \text{lcm}(f_j)/\gcd\{c_j \mid j \in J\} \) and \( f_j \) has a weak Gröbner representation in terms of \( F \).

If no \( \text{lt}(f_j) \) is a multiple of another \( \text{lt}(f_j) \), then we see by considering the singletons \( J \), that we may assume \( F \subset C(F) \). So we have \( C(F) = \{2x, 3y, xy\} \) in the above-mentioned instance.

A completion of \( F = \{f_1, \ldots, f_r\} \) can be computed easily, similar to the basis construction in theorem 2. If for \( F^* := F \setminus \{f_r\} \) a completion \( C(F^*) \) is known, we may take for each maximal \( J \) not containing \( r \) the corresponding \( f \in C(F^*) \) for element \( f_j \) in \( C(F) \). Hence, let \( J \) be maximal and contain \( r \), i.e. \( J \) a basic set. Then \( J^* = J \setminus \{r\} \) is maximal w.r.t. \( F^* \) and \( \phi(J^*)/\phi(J) \). Let \( f^* \in C(F^*) \) correspond to \( J^* \), i.e.

\[
\text{lcm}(f^*)/\gcd\{c_j \mid j \in J^*\}, \text{lt}(f^*)/\phi(J^*).
\]

Let

\[
u_1 \text{lcm}(f^*) + u_2 c_r = \gcd\{\text{lcm}(f^*), c_r\}, \quad u_1, u_2 \in R.
\]
Then the so-called $T$-polynomial
\[ T(f^x, f_1) := u_1 \frac{\phi(J)}{\text{lt}(f^x)} f^x + u_2 \frac{\phi(J)}{\phi_1} f_1 \]
satisfies
\[ \text{lc}(T(f^x, f_1)) = \gcd(\text{lc}(f^x), c_0) \frac{\gcd(c_j | j \in J)}{\text{lt}(f^x, f_1)} = \phi(J) \]
and inserting the weak Gröbner representation of $f^x$ in terms of $\{f_1, \ldots, f_{r-1}\}$ into the definition $T(f^x, f_1)$ we read off the weak Gröbner representation in terms of $F$. Hence, we may take it for $f_1$.

Therefore, a completion $C(F)$ is obtained by taking
\[ C(F) = \{ f \in C(F) \} \]
and for every basic set the corresponding $T$-polynomial. An element $f \in C(F)$ can be cancelled if a $g \in C(F)$ exists, s.t. $\text{lt}(g)/\text{lt}(f)$ and $\text{lc}(g)/\text{lt}(f)$. This allows a reduction of the just constructed completion $C(F)$. An instance of this construction is contained in the final example.

**PROPOSITION 2.** Let $C(F)$ be a completion of $F = \{f_1, \ldots, f_r\}$ and $f, g \in \mathcal{P}$. If $f \stackrel{\text{w}}{\rightarrow} g$, then $f \stackrel{\text{w}}{\rightarrow} f'$ for a $g' \in \mathcal{P}$. If $f \stackrel{\text{w}}{\rightarrow} g$, then $f \stackrel{\text{w}}{\rightarrow} f'$ for a $g' \in \mathcal{P}$.

**PROOF.** Equation (1) shows that $f \stackrel{\text{w}}{\rightarrow} g$ implies
\[ \text{lc}(f) = \sum_{j \in J} d_j \text{lc}(f_j) \]
with $d_j \in \mathbb{R}$ and $J$ maximal for $\text{lt}(f)$. Then $\text{lc}(f) \in \langle c_j | j \in J \rangle$. This ideal in $\mathbb{R}$ is generated by
\[ c \cdot \text{lc}(f_j) = \gcd(c_j | j \in J). \]

By construction $\phi(J)/\text{lt}(f)$. Hence,
\[ f \stackrel{\text{w}}{\rightarrow} g \quad \text{for a } J \quad \text{and } \quad J \stackrel{\text{w}}{\rightarrow} f'. \]

Conversely, $f \stackrel{\text{w}}{\rightarrow} g$ implies $M_T(f_j)/M_T(f)$ for a maximal $J$. Using the weak Gröbner representation $f_j = \Sigma h_i f_i$, we get
\[ f \stackrel{\text{w}}{\rightarrow} f \quad \text{for a } J \quad \text{and } \quad J \stackrel{\text{w}}{\rightarrow} f'. \]

**DEFINITION.** Let $I$ be an ideal in $\mathcal{P}$. Then $F = \{f_1, \ldots, f_r\} \subset I$ is called a strong Gröbner basis of $I$, if for each $f \in I$ an $f \in F$ exists, such that $M_T(f_j)/M_T(f)$.

**THEOREM 4.** Let $I$ be generated by $F = \{f_1, \ldots, f_r\}$. Then the following conditions are equivalent.

1. $F$ is a strong Gröbner basis of $I$.
2. $f \stackrel{\text{w}}{\rightarrow} 0$ for every $f \in I$.
3. Let $\{G_1, \ldots, G_m\}$ be a basis of $S(M_T(f_1), \ldots, M_T(f_r))$ and each $G_i = (g_{i1}, \ldots, g_{im})$ be homogeneous. Then
\[ \sum_{j=1}^{r} g_{ij} f_j \stackrel{\text{w}}{\rightarrow} 0, \quad i = 1, \ldots, m. \]

**PROOF.** $C1' \Rightarrow C4'$: Let $f \in I$ and $M_T(f_j)$ divide $M_T(f)$. Then
\[ f \stackrel{\text{w}}{\rightarrow} \frac{M_T(f)}{M_T(f_k)} f_k = f'. \]
Because of \( f' \in I \) and \( \text{l}(f') < \text{l}(f) \) we may use an inductive argument.

C4' \( \Rightarrow \) C5': Clear because of \( \sum g_j f_j \in I \).

C5' \( \Rightarrow \) C1': Essentially like C5 \( \Rightarrow \) C3 \( \Rightarrow \) C1 in theorem 1.

We have only to replace weak Gröbner representations by representations

\[
\sum_{i=1}^{r} g_i f_i
\]

with \( k \in \{1, \ldots, r\} \), such that

\[
\text{l}(f) = \text{l}(g_k f_k) > \text{l}(g_i f_i)
\]

for all \( i \neq k \).

**COROLLARY.** \( F \) is a weak Gröbner basis of \( I \) if and only if a completion \( C(F) \) is a strong Gröbner basis of \( I \).

**PROOF.** Proposition 2 shows that \( f \) is weakly irreducible mod. \( F \) if and only if \( f \) is strongly irreducible mod \( C(F) \). Condition C4 and C4' mean that 0 is the only irreducible element of \( I \) in the respective setting. □

The algorithm sketched at the end of section 3 for computing weak Gröbner bases can be modified to obtain also strong Gröbner bases.

**ALGORITHM.** Input: \( \{f_1, \ldots, f_r\} \subset R[X_1, \ldots, X_n] \), \( R \) a principal ideal ring.

Step 1: Calculate

\[
D := \{(i, j) \mid 1 \leq i < j \leq r, \quad \text{l}(i, j) \neq 0, \quad \forall \ k \neq 0, \quad \text{l}(B_k(i, j)) \neq 0 \}.
\]

calculate a \( C(F) \) for \( F := \{f_1, \ldots, f_r\} \) and define \( R := r \).

Step 2: Let \( (i, j) \in D \). Calculate \( h \), such that

\[
\frac{\text{lcm}\{M_T(f_i), M_T(f_j)\}}{M_T(f_j)} f_i = \frac{\text{lcm}\{M_T(f_i), M_T(f_j)\}}{M_T(f_j)} f_j \text{ in } \mathbb{Z}^r \text{,}
\]

and \( h \) is no longer strongly reducible modulo \( C(F) \). Remove \( (i, j) \) from \( D \).

Step 3: If \( h \neq 0 \) enlarge \( F \) by \( f_{R+1} = h \), \( D \) by

\[
\{(k, R+1) \mid 1 \leq k \leq R, \quad \text{l}(M(k, R+1)) \neq 0 \}
\]

remove all \( (k, l) \) with \( B_{R+1}(k, l) \) from \( D \), calculate a \( C(F) \) for this new \( F \) and enlarge finally \( R \) by 1.

Step 4: If \( D \neq \emptyset \) go to step 2.

Output: \( F \), a weak Gröbner basis of \( \{f_1, \ldots, f_r\} \),

\( C(F) \), a strong Gröbner basis of \( \{f_1, \ldots, f_r\} \).

Since by construction of \( h \), each \( R > r \), is no multiple of an \( M_T(f), f \in C(f_1, \ldots, f_{R-1}) \), or equivalently as shown in proposition 2,

\[
M_T(f_R) \notin (M_T(f_1), \ldots, M_T(f_{R-1})),
\]

the algorithm produces a strictly increasing chain of ideals

\[
(M_T(f_1), \ldots, M_T(f_r)) \subset (M_T(f_1), \ldots, M_T(f_{r+1})) \subset \ldots .
\]
This chain is finite because \( \mathcal{P} \) is Noetherian. Therefore only finitely many \( h \neq 0 \) are produced in the algorithm. This shows termination.

For the correctness, we remark that when step 2 is performed, \( \{B_i\}_{(k, l) \in D} \) is a basis of \( S(M_T(f_j), \ldots, M_T(f_R)) \) by theorem 3. At termination, condition CS' holds for \( C(F) \), i.e. \( C(F) \) is a strong Gröbner basis and by the last corollary \( F \) is a weak one.

For the computation of weak and strong Gröbner bases by means of this algorithm, we need that in the principal ideal ring \( R \) all ring operations can be performed and that an algorithm exists which, given \( r_1, r_2 \in R \setminus \{0\} \), produces an \( \text{lcm} \) of \( r_1, r_2 \) and elements \( u_1, u_2 \in R \) with

\[
u_1 r_1 + u_2 r_2 = \text{gcd}\{r_1, r_2\} = \frac{r_1 r_2}{\text{lcm}\{r_1, r_2\}}.\]

The most time and space consuming parts of the algorithm are the reduction in step 2 and the calculation of the next \( C(F) \), even if the latter is computed as proposed by enlarging the previous \( C(F) \), by \( T \)-polynomials. Superfluous \( C(F) \) computations are made, when the new \( M_T(f_{R+1}) \) is a multiple of an \( M_T(f_i) \), \( i > R + 1 \), appearing later in the algorithm. This happens, for instance, when, as proposed by some authors, \( T \)-polynomials are also inserted into \( F \). (They are needed only for the strong reduction!)

To avoid unnecessary reductions in step 2, we also do not enlarge \( F \) by \( T \)-polynomials and keep the module basis restricted by the criteria \( M, F \) and \( B \). The decision not to take a pair \( (i, j) \) for reduction, when \( M(i, j) \) or \( F(i, j) \) or \( B_k(i, j) \) for \( k > j \) holds, parallels criteria of Buchberger (1979) for the case of polynomials over fields.

The algorithm is with minor modifications installed in the computer algebra system SCRATCHPAD II for polynomials in \( x_1, \ldots, x_n \) over Euclidean rings \( R \) and tested by various examples, see Gebauer & Möller (1987).

**Example.** Let \( R \) be the ring of integers, \( \mathcal{P} = R[x, y] \), \( \prec_T \) the graduated lexicographical ordering

\[
1 \prec_T x \prec_T y \prec_T x^2 \prec_T xy \prec_T y^2 \prec_T x^3 \prec_T x^4 \ldots
\]

and \( F = \{f_1, f_2\} \),

\[
f_1 = 2x^2y - 17y, \quad f_2 = 5xy^2 - 3x.
\]

The algorithm gives first \( D = \{(1, 2)\} \) and \( C(F) = \{f_1, f_2, f_{12}\} \),

\[
f_{12} = 3y f_1 - x f_2 = x^2 y^2 - 51y^2 + 3x^2.
\]

Taking the pair \( (1, 2) \) for reduction in step 2,

\[
f_3 = 5y f_1 - 2x f_2 = -85y^2 + 6x^2.
\]

Then, because of \( M(1, 3) \) we have \( D = \{(2, 3)\} \) and \( C(F) = \{f_1, f_2, f_3, f_{12}\} \), because we may take \( f_{12} \) for \( f_{123} \) and \( f_2 \) for \( f_{23} \). The pair \( (2, 3) \) gives

\[
f_4 = -17f_2 - xf_3 = -6x^3 + 51x.
\]

Because of \( M(2, 4) \) and \( M(3, 4) \), we have \( D = \{(1, 4)\} \), and \( C(F) = \{f_1, f_2, f_3, f_4, f_{12}\} \), because we may take \( f_1 \) for \( f_{14} \) and \( f_{12} \) for \( f_{1234} \). The pair \( (1, 4) \) gives

\[
-3x f_1 - y f_4 = 0.
\]

Thus, the algorithm terminates giving the weak Gröbner basis \( \{f_1, f_2, f_3, f_4\} \) and the strong Gröbner basis \( \{f_1, f_2, f_3, f_4, f_{12}\} \).
References

Sci. 204, 526–534.
Madison.
Conference, pp. 369–376.
Univ. Linz.
Theory 10, 475–488.
Winkler, F. (1984). The Church–Rosser property in computer algebra and special theorem proving/An
Comp. Sci.