Efficiently Computing Minimal Sets of Critical Pairs

M. Caboara [a,*], M. Kreuzer [b], L. Robbiano [a]

[a] *Department of Mathematics, University of Genoa, Italy*

[b] *Fachbereich Mathematik, Universität Dortmund, Germany*

Abstract

In the computation of a Gröbner basis using Buchberger's algorithm, a key issue for improving the efficiency is to produce techniques for avoiding as many unnecessary critical pairs as possible. A good solution would be to avoid *all* non-minimal critical pairs, and hence to process only a *minimal set of generators* of the module generated by the critical syzygies. In this paper we show how to obtain that desired solution in the homogeneous case while retaining the same efficiency as with the classical implementation. As a consequence, we get a new Optimized Buchberger Algorithm.

Key words: Critial Pairs, Buchberger Algorithm

1 Introduction

Ever since practical implementations of Buchberger's famous algorithm for computing Gröbner bases became feasible (Buchberger, 1965), it has been clear that, in order to improve the efficiency of this algorithm, one needs to avoid the treatment of as many critical pairs as possible. Buchberger (1979) studied this problem for the first time, and later in (Buchberger, 1985) and (Gebauer and Möller, 1987) his results were substantially improved and expanded. Nevertheless, Gebauer and Möller (1987) showed that their method did not always produce a minimal set of generators of the module generated by the critical syzygies. However, their method was very efficient and yielded an *almost*

* Corresponding author.

Email addresses: `caboara@dima.unige.it` (M. Caboara), `Martin.Kreuzer@mathematik.uni-dortmund.de` (M. Kreuzer), `robbiano@dima.unige.it` (L. Robbiano).

minimal set of critical pairs. Since then, many kinds of optimizations of Buchberger's algorithm have been found, in particular by implementers of computer algebra systems. But the problem of efficiently minimalizing the critical pairs has gone largely unnoticed and seems to be overdue for a solution. Indeed, that is the main objective of this paper.

To achieve our goal, we proceed as follows. Foremost, we need a detailed understanding of the entire process of computing Gröbner bases, in particular in the homogeneous case. An algorithm for simultaneously computing a Gröbner basis and a minimal system of generators contained in it is fine-tuned when the input is a reduced Gröbner basis. Then this result is applied to critical syzygies, using the fact that we show how the old criteria $M(i,j)$ and $F(i,j)$ of (Gebauer and Möller, 1987) yield a reduced Gröbner basis of the module of syzygies of the leading terms. Besides, when applied to this special case, the algorithm admits many subtle optimizations. In the end, we really achieve the goal of minimalizing the critical pairs efficiently.

Now, why do we think that what we achieved is important?

The first reason is theoretical curiosity. It is common knowledge among the implementers of Buchberger's algorithm that the criteria of Gebauer and Möller *almost* produce a minimal set of critical pairs. We wanted to see whether that *vox populi* is really true. Of course one could use a standard minimalization process to produce minimal sets of critical pairs, but this method could only handle small examples. Instead, we observed that, after applying two of the criteria of Gebauer and Möller, a *reduced Gröbner basis* of the module of syzygies of the leading terms is obtained. Then we were able to see the difference between the reduced Gröbner basis and a minimal set of generators of this module, and how this difference depends on the size of the example.

Another important reason is that we wanted to be able to compute a minimal set of generators of this module with the *same efficiency* as the usual application of the Gebauer-Möller criteria. And we wanted to do it while computing a Gröbner basis, so that we can replace the Gebauer-Möller criteria by our procedure. As we show in the last sections, we achieved this goal.

A third reason is that our results hold in full generality, namely for Gröbner bases of modules over positively (multi-) graded rings. Other optimizations of Buchberger's algorithm, e.g. ideas using trivial syzygies (see for instance Faugere (2002)), do not hold in this generality. Moreover, we would like to point out that the pairs we discard are truly useless, whereas pairs between elements in a reduced Gröbner bases which reduce to zero can still be useful for the computation of syzygies.

Finally, the readers should know that the basic terminology is taken from the book of the second and third authors (Kreuzer and Robbiano, 2000).

2 Some Background Material

Since we are interested in optimizing Buchberger's algorithm in the homogeneous case, we start by saying which gradings we consider. From now on let K be a field and $P = K[x_1, \dots, x_n]$ a polynomial ring over K. Moreover, let $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$ be an $m \times n$-matrix with integer entries. Then there exists exactly one $\mathbb{Z}^m$-grading on P such that every term $t = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ is homogeneous of degree $\deg_W(t) = W \cdot (\alpha_1, \dots, \alpha_n)^{\mathrm{tr}}$. We say that P is **(multi-) graded** by W. The matrix W is called the **degree matrix** and its rows are called the **weight vectors**.

For instance, the grading on P given by $W = (1, \dots, 1)$ is the standard grading. For every $d \in \mathbb{Z}^m$, the homogeneous component of degree d of P is $P_{W,d} = \oplus_{\deg_W(t)=d} K \cdot t$. Given $\delta_1, \dots, \delta_r \in \mathbb{Z}^m$, the graded free P-module $F = \oplus_{i=1}^r P(-\delta_i)$ inherits a $\mathbb{Z}^m$-grading from P in the natural way. Again we say that F is **graded by** W.

In order to be able to use these gradings in our algorithms, we need some positivity assumptions.

Definition 1 Let P be graded by W, and let $w_1, \dots, w_m$ be the rows of W.

a) The grading given by W is called **weakly positive** if there exist integers $a_1, \dots, a_m$ such that $a_1 w_1 + \cdots + a_m w_m$ has all entries strictly positive.
b) The grading given by W is called **positive** if $\mathrm{rk}(W) = m$, if no column of W is zero, and if the first non-zero entry in each column of W is positive.

Proposition 2 *Let P be weakly positively graded by W, and let M be a finitely generated graded P-module.*

a) We have $P_{W,0} = K$ and $\dim_K(M_{W,d}) < \infty$ for every $d \in \mathbb{Z}^m$.
b) The graded version of Nakayama's lemma holds: homogeneous elements $v_1, \dots, v_s \in M$ generate the module M if and only if their residue classes $\overline{v}_1, \dots, \overline{v}_s$ generate the K-vector space $M/(x_1, \dots, x_n)M$. In particular, every homogeneous system of generators of M contains a minimal one, and all irredundant homogeneous systems of generators of M have the same number of elements which is denoted by $\mu(M)$.

The proof of this proposition uses standard computer algebra methods and is contained in (Kreuzer and Robbiano, in preparation). For practical computations we need the somewhat stronger notion of a positive grading. The usefulness of positive gradings is illustrated by the following characterizations.

Recall that a module ordering σ on the set of terms $\mathbb{T}^n\langle e_1,\ldots,e_r\rangle$ of the graded free module F is called **degree compatible** or **compatible with** $\deg_W$ if the inequality $\deg_W(te_i) >_{\mathtt{Lex}} \deg_W(t'e_j)$ implies $te_i >_\sigma t'e_j$ for all $t,t' \in \mathbb{T}^n$ and all $i,j \in \{1,\ldots,r\}$.

Proposition 3 *Let P be graded by W, where W has $\mathbb{Z}$-linearly independent rows and non-zero columns. Then the following conditions are equivalent.*

- *a) The grading on P given by W is positive.*
- *b) The restriction of* `Lex` *to the monoid $\Gamma = \{d \in \mathbb{Z}^m \mid P_{W,d} \neq 0\}$ is a well-ordering, i.e. every non-empty subset of Γ has a minimal element with respect to* `Lex`*.*
- *c) The restriction of* `Lex` *to the monoid $\Gamma = \{d \in \mathbb{Z}^m \mid P_{W,d} \neq 0\}$ is a term ordering, i.e. every element $d \in \Gamma$ satisfies $d >_{\mathtt{Lex}} 0$.*
- *d) There exists a term ordering τ on $\mathbb{T}^n$ which is compatible with $\deg_W$.*
- *e) There exists a module term ordering σ on $\mathbb{T}^n\langle e_1,\ldots,e_r\rangle$ which is compatible with the grading given by W.*

Again we refer to (Kreuzer and Robbiano, in preparation) for a proof of this proposition. As a consequence, it follows that positive gradings are weakly positive. Moreover, in a positively graded setting, we can prove the finiteness of various algorithms in the usual way, i.e. by using the fact that there is no infinite sequence of homogeneous elements of strictly decreasing degrees.

In the remaining part of this section, we use truncated Gröbner bases to prove two very important technical tools, namely Corollary 8 and Corollary 10. We shall from now on assume that P is positively graded by $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$. Moreover, we let $\delta_1,\ldots,\delta_r \in \mathbb{Z}^m$, we let M be a finitely generated graded submodule of the graded free P-module $F = \oplus_{i=1}^r P(-\delta_i)$, and we let σ be a module term ordering on $\mathbb{T}^n\langle e_1,\ldots,e_r\rangle$, the set of terms in F.

The following notation will turn out to be convenient. Given a subset S of a graded P-module and $d \in \mathbb{Z}^m$, we let $S_{\leq d} = \{v \in S \mid v \text{ homogeneous}, \deg_W(v) \leq_{\mathtt{Lex}} d\}$ and $S_d = \{v \in S \mid v \text{ homogeneous}, \deg_W(v) = d\}$.

Definition 4 Assume that $G = \{g_1,\ldots,g_s\}$ is a homogeneous σ-Gröbner basis of M, and let $d \in \mathbb{Z}^m$. Then the set $G_{\leq d}$ is called a **d-truncated Gröbner basis** of M, or a Gröbner basis of M which has been **truncated in degree** d.

For truncated Gröbner bases, we now prove a characterization which is analogous to the Buchberger criterion in the usual case. To this end, we need to explain what we mean by critical pairs and critical syzygies.

Given homogeneous elements $g_1, \ldots, g_s \in M \setminus \{0\}$, we let $d_i = \deg_W(g_i)$ for $i = 1, \ldots, s$, and we let F' be the graded free P-module $\oplus_{i=1}^s P(-d_i)$. The canonical basis of F' will be denoted by $\{\varepsilon_1, \ldots, \varepsilon_s\}$. Notice that we have $\deg_W(\varepsilon_i) = d_i$ for $i = 1, \ldots, s$. Moreover, we write $\mathrm{LM}_\sigma(g_i) = c_i t_i e_{\gamma_i}$, where $c_i \in K \setminus \{0\}$, where $t_i \in \mathbb{T}^n$, and where $\gamma_i \in \{1, \ldots, r\}$.

Definition 5 A pair $(i,j) \in \{1, \ldots, s\}$ such that $1 \le i < j \le s$ and $\gamma_i = \gamma_j$ is called a **critical pair** of $(g_1, \ldots, g_s)$. The set of all critical pairs of $(g_, \ldots, g_s)$ is denoted by $\mathbb{B}$. For every critical pair $(i,j) \in \mathbb{B}$, the element $\sigma_{ij} = \frac{\mathrm{lcm}(t_i,t_j)}{c_i t_i}\,\varepsilon_i - \frac{\mathrm{lcm}(t_i,t_j)}{c_j t_j}\,\varepsilon_j$ is a syzygy of the pair $(\mathrm{LM}_\sigma(g_i), \mathrm{LM}_\sigma(g_j))$. It is called the **critical syzygy** associated to the critical pair (i,j). The set of all critical syzygies is denoted by Σ.

Clearly, a critical syzygy σ_{ij} is a homogeneous element of F' whose degree is precisely $\deg_W(\sigma_{ij}) = \deg_W(\mathrm{lcm}(t_i,t_j)) + \delta_{\gamma_i}$. This degree equals the degree of the corresponding S-vector $S_{ij} = \frac{\mathrm{lcm}(t_i,t_j)}{c_i t_i}\, g_i - \frac{\mathrm{lcm}(t_i,t_j)}{c_j t_j}\, g_j$ in F.

For every critical pair $(i,j) \in \mathbb{B}$, we call $\deg_W(\sigma_{ij})$ the **degree of the critical pair**. Then it makes sense to consider the set $\mathbb{B}_{\le d}$ for every given $d \in \mathbb{Z}^m$, and we observe that $\deg_W(\sigma_{ij}) \ge_{\mathtt{Lex}} \max\{d_i, d_j\}$ for all $(i,j) \in \mathbb{B}$. Finally, we remind the reader that $\mathrm{NR}_{\sigma,\mathcal{G}}(v)$ denotes normal remainder, i.e. the result of the division algorithm, as in (Kreuzer and Robbiano, 2000), Definition 1.6.7. At this point, we are ready to formulate and prove the following characterization of truncated Gröbner bases.

Proposition 6 (Characterization of Truncated Gröbner Bases) *Let P be positively graded by $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$, let $G = \{g_1, \ldots, g_s\}$ be a set of non-zero homogeneous vectors which generates a graded submodule M of $\oplus_{i=1}^r P(-\delta_i)$, and let $d \in \mathbb{Z}^m$. Then the following conditions are equivalent.*

a) The set $G_{\le d}$ is a d-truncated σ-Gröbner basis of M.
b) For every homogeneous element $v \in M_{\le d} \setminus \{0\}$, we have the relation $\mathrm{LT}_\sigma(v) \in \langle \mathrm{LT}_\sigma(g) \mid g \in G_{\le d} \rangle$.
c) For all pairs $(i,j) \in \mathbb{B}_{\le d}$, we have $\mathrm{NR}_{\sigma,\mathcal{G}_{\le d}}(S_{ij}) = 0$, where $\mathcal{G}_{\le d}$ is the tuple obtained from $\mathcal{G} = (g_1, \ldots, g_s)$ by deleting the elements of degree greater than d.

Proof. Without loss of generality, we may assume that $G_{\le d} = \{g_1, \ldots, g_{s'}\}$ for some $s' \le s$. It is clear that a) implies both b) and c). Now we show that b) implies a). By the assumption, we can find terms $t'_{s'+1}, \ldots, t'_{s''}$ of degree greater than d such that the set $\{\mathrm{LT}_\sigma(g_1), \ldots, \mathrm{LT}_\sigma(g_{s'})\} \cup \{t'_{s'+1}, \ldots, t'_{s''}\}$ is a system of generators of $\mathrm{LT}_\sigma(M)$. We choose homogeneous elements $h_{s'+1}, \ldots, h_{s''}$ in M such that $\mathrm{LT}_\sigma(h_i) = t'_i$ for $i = s'+1, \ldots, s''$. Then the set $\{g_1, \ldots, g_{s'}, h_{s'+1}, \ldots, h_{s''}\}$ is a homogeneous σ-Gröbner basis of M with truncation $G_{\le d}$.

It remains to prove that c) implies b). Let $v \in M_{\leq d}$ be a homogeneous non-zero element. Since $\{g_1, \ldots, g_{s'}\}$ generates $\langle M_{\leq d} \rangle$, we can represent v as $v = \sum_{i=1}^{s'} f_i g_i$, where f_i is homogeneous of degree $\deg_W(v) - \deg_W(g_i) \leq_{\texttt{Lex}} d$. In order to prove $\mathrm{LT}_\sigma(v) \in \langle \mathrm{LT}_\sigma(g_1), \ldots, \mathrm{LT}_\sigma(g_{s'}) \rangle$, it is enough to proceed as in the proof of Proposition 2.3.12 of (Kreuzer and Robbiano, 2000), replacing $\mathcal{G}$ by $\mathcal{G}_{\leq d}$. □

This characterization has several useful applications.

Corollary 7 *Let $G = \{g_1, \ldots, g_s\}$ be a homogeneous σ-Gröbner basis of the module M, and let $d \in \mathbb{Z}^m$. Then $G_{\leq d}$ is a d-truncated σ-Gröbner basis of the module $\langle M_{\leq d} \rangle$.*

Proof. Since G is a set of generators of M, the set $G_{\leq d}$ generates the module $\langle M_{\leq d} \rangle$. From Buchberger's Criterion we know that $\mathrm{NR}_{\sigma,\mathcal{G}}(S_{ij}) = 0$, for all pairs $(i,j) \in \mathbb{B}$. If we have $\deg_W(S_{ij}) \leq_{\texttt{Lex}} d$ here, the elements of G involved in the reduction steps $S_{ij} \xrightarrow{G} 0$ all have degrees less than or equal to d. Hence we see that $\mathrm{NR}_{\sigma,\mathcal{G}_{\leq d}}(S_{ij}) = 0$, and the proposition yields the claim. □

Corollary 8 *Let $d \in \mathbb{Z}^m$, let the elements of the tuple $\mathcal{G} = (g_1, \ldots, g_s)$ form a d-truncated σ-Gröbner basis of M, and let $g_{s+1} \in F$ be a homogeneous element of degree d such that $\mathrm{LT}_\sigma(g_{s+1}) \notin \langle \mathrm{LT}_\sigma(g_1), \ldots, \mathrm{LT}_\sigma(g_s) \rangle$. Then $\{g_1, \ldots, g_{s+1}\}$ is a d-truncated Gröbner basis of $M + \langle g_{s+1} \rangle$.*

Proof. In order to prove the claim, we check condition c) of the proposition. For $1 \leq i < j \leq s$ such that $\deg_W(S_{ij}) \leq_{\texttt{Lex}} d$, we have $\mathrm{NR}_{\sigma,\mathcal{G}}(S_{ij}) = 0$ by the assumption and by Proposition 6. For $i \in \{1, \ldots, s\}$ such that $\deg_W(S_{i\,s+1}) = d$, the fact that the pair $(i, s+1)$ has degree d implies that $\mathrm{LT}_\sigma(g_{s+1})$ is a multiple of $\mathrm{LT}_\sigma(g_i)$, in contradiction to the hypothesis. □

In the last part of this section, we prove an analogue of the preceding corollary for minimal generators. Recall that Proposition 2.b guarantees that all minimal systems of generators have the same length in the positively graded situation.

Proposition 9 *Let P be positively graded by $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$, let M be a graded P-module generated by homogeneous elements $\{g_1, \ldots, g_s\}$, and assume that $\deg_W(g_1) \leq_{\texttt{Lex}} \deg_W(g_2) \leq_{\texttt{Lex}} \cdots \leq_{\texttt{Lex}} \deg_W(g_s)$.*

- *a) The set $\{g_1, \ldots, g_s\}$ is a minimal system of generators of M if and only if we have $g_i \notin \langle g_1, \ldots, g_{i-1} \rangle$ for $i = 1, \ldots, s$.*
- *b) The set $\{g_i \mid i \in \{1, \ldots, s\},\ g_i \notin \langle g_1, \ldots, g_{i-1} \rangle\}$ is a minimal system of generators of M.*

Proof. First we prove a). If $\{g_1, \ldots, g_s\}$ is a minimal set of generators of M, then no relation of type $g_i \in \langle g_1, \ldots, g_{i-1} \rangle$ holds, since otherwise we would have $M = \langle g_1, \dots, g_{i-1}, g_{i+1}, \dots, g_s \rangle$. Conversely, if $\{g_1, \dots, g_s\}$ is not a minimal set of generators of M, then there exists an index $i \in \{1, \dots, s\}$ such that $g_i \in \langle g_1, \dots, g_{i-1}, g_{i+1}, \dots, g_s \rangle$. Using Corollary 1.7.11 of (Kreuzer and Robbiano, 2000), we obtain a representation $g_i = \sum_{j \neq i} f_j g_j$, where $f_j \in P$ is homogeneous of degree $\deg_W(g_i) - \deg_W(g_j)$ for $j \in \{1, \dots, i-1, i+1, \dots, s\}$.

Since $\deg_W(f_j) \geq_{\texttt{Lex}} 0$ for $f_j \neq 0$, we see that $\deg_W(g_i) <_{\texttt{Lex}} \deg_W(g_j)$ implies $f_j = 0$. Thus there are two possibilities. Either we have $\deg_W(g_i) >_{\texttt{Lex}} \deg_W(g_j)$ for all j such that $f_j \neq 0$ or there exist some indices j such that $\deg_W(g_j) = \deg_W(g_i)$. In the first case, those indices j satisfy $j < i$ by the assumption that the multidegrees of $g_1, \dots, g_s$ are ordered increasingly, and therefore we get $g_i \in \langle g_1, \dots, g_{i-1} \rangle$. In the second case, the f_j corresponding to those indices j are in $K \setminus \{0\}$. Let $j_{\max} = \max\{j \in \{1, \dots, s\} \mid f_j \in K \setminus \{0\}\}$. We get the relation $g_{j_{\max}} \in \langle g_1, \dots, g_{j_{\max}-1} \rangle$. In both cases, we arrive at a contradiction to our hypothesis.

Now let us show b). The set $S = \{g_i \mid i \in \{1, \dots, s\},\ g_i \notin \langle g_1, \dots, g_{i-1} \rangle\}$ is a system of generators of M, because an element g_i such that $g_i \in \langle g_1, \dots, g_{i-1} \rangle$ is also contained in $\langle g_j \in S \mid 1 \leq j \leq i-1 \rangle$. The fact that this system of generators is minimal follows from a). □

The following version is an immediate consequence of part a) of the proposition.

Corollary 10 *Let N be a graded P-module, let M be a submodule of N, let $\{g_1, \dots, g_s\}$ be a minimal homogeneous system of generators of M, and let $g_{s+1} \in N \setminus M$ be a homogeneous vector whose degree satisfies the inequality $\deg_W(g_{s+1}) \geq_{\texttt{Lex}} \max\{\deg_W(g_i) \mid i = 1, \dots, s\}$. Then $\{g_1, \dots, g_{s+1}\}$ is a minimal system of generators of the module $M + \langle g_{s+1} \rangle$. In particular, we have $\mu(M + \langle g_{s+1} \rangle) = \mu(M) + 1$.*

3 Minimal Generators in a Reduced Gröbner Basis

¿From here on we use the following assumptions. Let K be a field, and let $P = K[x_1, \dots, x_n]$ be a polynomial ring over K which is positively graded by a matrix $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$. Then let $r \geq 1$, let $\delta_1, \dots, \delta_r \in \mathbb{Z}^m$, and let M be a graded submodule of $F = \oplus_{i=1}^r P(-\delta_i)$ which is generated by a set of non-zero homogeneous vectors $\{v_1, \dots, v_s\}$. Furthermore, we choose a module term ordering σ on the monomodule of terms $\mathbb{T}^n \langle e_1, \dots, e_r \rangle$ in F, and we let $\mathcal{V} = (v_1, \dots, v_s)$.

Our first goal is to describe an algorithm which computes a homogeneous σ-Gröbner basis of M degree-by-degree and a variant of this algorithm which also yields a minimal system of generators of M contained in $\mathcal{V}$. This part is classical and more or less "well-known". Then we make good use of it in Theorem 15 for minimalizing reduced Gröbner bases.

To ease the notation, we shall use the following convention: whenever a vector g_i appears, we write $\mathrm{LM}_\sigma(g_i) = c_i t_i e_{\gamma_i}$, where $c_i \in K\setminus\{0\}$, where $t_i \in \mathbb{T}^n$, and where $\gamma_i \in \{1,\dots,r\}$. For two indices i,j such that $\gamma_i = \gamma_j$, we let $\sigma_{ij} = \frac{\mathrm{lcm}(t_i,t_j)}{c_i t_i}\,\varepsilon_i - \frac{\mathrm{lcm}(t_i,t_j)}{c_j t_j}\,\varepsilon_j$ and $S_{ij} = \frac{\mathrm{lcm}(t_i,t_j)}{c_i t_i}\,g_i - \frac{\mathrm{lcm}(t_i,t_j)}{c_j t_j}\,g_j$.

Theorem 11 (The Homogeneous Buchberger Algorithm)
In the above situation, consider the following instructions.

1) *Let $B = \emptyset$, $\mathcal{W} = \mathcal{V}$, $\mathcal{G} = \emptyset$, and let $s' = 0$.*
2) *Let d be the smallest degree with respect to* `Lex` *of an element of B or of $\mathcal{W}$. Form B_d and $\mathcal{W}_d$, and delete their entries from B and $\mathcal{W}$, respectively.*
3) *If $B_d = \emptyset$, continue with step 6). Otherwise, chose a pair $(i,j) \in B_d$ and remove it from B_d.*
4) *Compute the S-vector S_{ij} and its normal remainder $S'_{ij} = \mathrm{NR}_{\sigma,\mathcal{G}}(S_{ij})$. If $S'_{ij} = 0$, continue with step 3).*
5) *Increase s' by one, append $g_{s'} = S'_{ij}$ to the tuple $\mathcal{G}$, and append the set $\{(i,s') \mid 1 \le i < s',\, \gamma_i = \gamma_{s'}\}$ to the set B. Continue with step 3).*
6) *If $\mathcal{W}_d = \emptyset$, continue with step 9). Otherwise, choose a vector $v \in \mathcal{W}_d$ and remove it from $\mathcal{W}_d$.*
7) *Compute $v' = \mathrm{NR}_{\sigma,\mathcal{G}}(v)$. If $v' = 0$, continue with step 6).*
8) *Increase s' by one, append $g_{s'} = v'$ to the tuple $\mathcal{G}$, and append the set $\{(i,s') \mid 1 \le i < s',\, \gamma_i = \gamma_{s'}\}$ to the set B. Continue with step 6).*
9) *If $B = \emptyset$ and $\mathcal{W} = \emptyset$, return the tuple $\mathcal{G}$ and stop. Otherwise, continue with step 2).*

This is an algorithm which returns a σ-Gröbner basis $\mathcal{G}$ of M, where the tuple $\mathcal{G}$ consists of homogeneous vectors having non-decreasing multidegrees.

The proof of this theorem is standard Computer Algebra and is for instance contained in (Kreuzer and Robbiano, in preparation).

Remark 12 Let us add some observations about this algorithm.

a) If we interrupt its execution after some degree d_0 is finished, the tuple $\mathcal{G}$ is a d_0-truncated Gröbner basis of M. Consequently, we can compute truncated Gröbner bases efficiently. Moreover, in this case it suffices to append only the pairs $\{(i,s') \mid 1 \le i < s',\, \gamma_i = \gamma_{s'},\, \deg_W(\sigma_{is'}) \le_{\mathtt{Lex}} d_0\}$ to the set B in steps 5) and 8). The reason is that pairs of higher degree are never processed anyway, since we stop the computation after finishing degree d_0.

b) It is not required that σ is a degree compatible module term ordering. The reason is that, during the computation of the Gröbner basis, only comparisons of terms in the support of a homogeneous vector are performed. Thus these terms have the same degree, and it does not matter whether σ is degree compatible or not.

c) The Homogeneous Buchberger Algorithm can also be viewed as a special version of the usual Buchberger Algorithm where we use a suitable selection strategy.

The following variant of the Homogeneous Buchberger Algorithm computes a minimal system of generators of M contained in the given set of generators while computing a Gröbner basis. It provides an efficient method for finding minimal systems of generators.

Corollary 13 (Buchberger Algorithm with Minimalization)
In the situation of the theorem, consider the following instructions.

1') Let $B = \emptyset$, $\mathcal{W} = \mathcal{V}$, $\mathcal{G} = \emptyset$, $s' = 0$, and $\mathcal{V}_{\min} = \emptyset$.
2) Let d be the smallest degree with respect to `Lex` of an element of B or of $\mathcal{W}$. Form B_d and $\mathcal{W}_d$, and delete their entries from B and $\mathcal{W}$, respectively.
3) If $B_d = \emptyset$, continue with step 6). Otherwise, chose a pair $(i,j) \in B_d$ and remove it from B_d.
4) Compute the S-vector S_{ij} and its normal remainder $S'_{ij} = \mathrm{NR}_{\sigma,\mathcal{G}}(S_{ij})$. If $S'_{ij} = 0$, continue with step 3).
5) Increase s' by one, append $g_{s'} = S'_{ij}$ to the tuple $\mathcal{G}$, and append the set $\{(i,s') \mid 1 \le i < s',\, \gamma_i = \gamma_{s'}\}$ to the set B. Continue with step 3).
6) If $\mathcal{W}_d = \emptyset$, continue with step 9). Otherwise, choose a vector $v \in \mathcal{W}_d$ and remove it from $\mathcal{W}_d$.
7) Compute $v' = \mathrm{NR}_{\sigma,\mathcal{G}}(v)$. If $v' = 0$, continue with step 6).
8') Increase s' by one, append $g_{s'} = v'$ to the tuple $\mathcal{G}$, append v to the tuple $\mathcal{V}_{\min}$, and append $\{(i,s') \mid 1 \le i < s',\, \gamma_i = \gamma_{s'}\}$ to the set B. Continue with step 6).
9') If $B = \emptyset$ and $\mathcal{W} = \emptyset$, return the pair $(\mathcal{G}, \mathcal{V}_{\min})$ and stop. Otherwise, continue with step 2).

This is an algorithm which returns a pair $(\mathcal{G}, \mathcal{V}_{\min})$ such that $\mathcal{G}$ is a tuple of homogeneous vectors which are a σ-Gröbner basis of M, and $\mathcal{V}_{\min}$ is a subtuple of $\mathcal{V}$ of homogeneous vectors which are a minimal system of generators of M.

Proof. In view of the theorem, we only have to show that the elements in $\mathcal{V}_{\min}$ are a minimal set of generators of M. Since the algorithm is finite, it operates in only finitely many degrees d. Therefore it suffices to prove by induction on d that $\mathcal{V}_{\min}$ contains a minimal system of generators of $\langle M_{\le d}\rangle$ after the algorithm has finished working on elements of degree d.

This is clearly the case at the outset. Suppose it is true for the last degree treated before d. Inductively, we can show that the elements of $\mathcal{G}$ continue to be contained in the module $\langle M_{<d}\rangle$ while we are looping through steps 3), 4), and 5) of the algorithm. Namely, every time an element of the form $\mathrm{NF}_{\sigma,\mathcal{G}}(S_{ij})$ is added to $\mathcal{G}$, it is clearly contained in the module generated by the previous elements of $\mathcal{G}$. Furthermore, by part a) of the remark following Theorem 11, the elements of the tuple $\mathcal{G}$ form a d-truncated Gröbner basis of $\langle M_{<d}\rangle$ after we have finished looping through steps 3), 4), and 5), i.e. when we have treated all pairs of degree d.

Now let $\mathcal{W}_d = (w_1, \ldots, w_\ell)$, and let the numbering of these vectors correspond to the order in which they are chosen in step 6). We show that, for each application of steps 6), 7), and 8'), the elements of $\mathcal{V}_{\min}$ continue to be a minimal system of generators of the module they generate, and that this module always agrees with the one generated by the elements of $\mathcal{G}$. Furthermore, the elements of $\mathcal{G}$ are always a d-truncated σ-Gröbner basis of that module.

When a new vector $v = w_i$ is chosen in step 6), there are two possibilities. If $v' = 0$ in step 7), then v is already contained in the module M' generated by the elements of $\mathcal{V}_{\min}$. Otherwise, the vector v' is not contained in M', since the elements of $\mathcal{G}$ are a d-truncated σ-Gröbner basis and we can apply the Submodule Membership Test (see (Kreuzer and Robbiano, 2000), Proposition 2.4.10.a). In that case, the elements of $\mathcal{V}_{\min}$, together with v, form a minimal system of generators of the module $M' + \langle v\rangle = M' + \langle v'\rangle$ by Corollary 10. Moreover, the elements of $\mathcal{G}$, together with v', form a d-truncated σ-Gröbner basis of $M' + \langle v'\rangle$ by Corollary 8.

Altogether, it follows that, after degree d is finished, the elements of $\mathcal{V}_{\min}$ are a minimal system of generators of $\langle M_{\le d}\rangle$, as we wanted to show. □

Remark 14 Let us collect some observations about this algorithm.

a) If we are only interested in a minimal system of generators of M (and not in a Gröbner basis), we can stop the algorithm after we have completed degree $d_{\max} = \max\{\deg(v_i) \mid 1 \le i \le s\}$. In this case it suffices to append only the pairs $\{(i, s') \mid 1 \le i < s',\ \gamma_i = \gamma_{s'},\ \deg_W(\sigma_{is'}) \le_{\mathtt{Lex}} d_{\max}\}$ to the set B in steps 5) and 8').
b) In addition, we could alter step 8') and append the vector v' instead of v to the list $\mathcal{V}_{\min}$. Then $\mathcal{V}_{\min}$ would still contain a minimal homogeneous set of generators of M when the computation ends. These generators would not be contained in the initial tuple $\mathcal{V}$ anymore, but they would

have the additional property that each vector is fully reduced against the previous ones.

The final part of the section is devoted to a result which will be essential for our discussion of the minimalization of the critical pairs. Namely, we are going to apply the algorithm of Corollary 13 to a reduced Gröbner basis and improve it significantly in that case. The main differences between both algorithms occur in step 7), where it suffices to compare terms instead of computing normal remainders, and in step 8), where we append v to both $\mathcal{G}$ and $\mathcal{V}_{\min}$.

Theorem 15 (Minimal Generators in a Reduced Gröbner Basis)
In the situation of Theorem 11, let $\mathcal{V} = (v_1, \dots, v_s)$ be the reduced σ-Gröbner basis of M. Consider the following instructions.

1) *Let $B = \emptyset$, $\mathcal{W} = \mathcal{V}$, $\mathcal{G} = \emptyset$, $s' = 0$, and $\mathcal{V}_{\min} = \emptyset$.*
2) *Let d be the smallest degree with respect to* `Lex` *of an element of B or of $\mathcal{W}$. Form B_d and $\mathcal{W}_d$, and delete their entries from B and $\mathcal{W}$, respectively.*
3) *If $B_d = \emptyset$, continue with step 6). Otherwise, choose a pair $(i,j) \in B_d$ and remove it from B_d.*
4) *Compute $S'_{ij} = \mathrm{NR}_{\sigma,\mathcal{G}}(S_{ij})$. If $S'_{ij} = 0$, continue with step 3).*
5) *Increase s' by one, append $g_{s'} = S'_{ij}$ to the tuple $\mathcal{G}$, append the following set $\{(i,s') \mid 1 \le i < s',\, \gamma_i = \gamma_{s'}\}$ to B, and continue with step 3).*
6) *If $\mathcal{W}_d = \emptyset$, continue with step 9). Otherwise, choose $v \in \mathcal{W}_d$ and remove it from $\mathcal{W}_d$.*
7) *If $\mathrm{LT}_\sigma(v) = \mathrm{LT}_\sigma(g)$ for some $g \in \mathcal{G}$, then replace the element g in $\mathcal{G}$ by v. Continue with step 6).*
8) *Increase s' by one, append $g_{s'} = v$ to the tuples $\mathcal{G}$ and $\mathcal{V}_{\min}$, and append $\{(i,s') \mid 1 \le i < s',\, \gamma_i = \gamma_{s'}\}$ to the set B. Continue with step 6).*
9) *If $B = \emptyset$ and $\mathcal{W} = \emptyset$, return $\mathcal{V}_{\min}$ and stop. Otherwise, continue with step 2).*

This is an algorithm which computes a subtuple $\mathcal{V}_{\min}$ of $\mathcal{V}$ such that $\mathcal{V}_{\min}$ is a minimal system of generators of M.

Proof. It suffices to show that this procedure has the same effect as running the algorithm of Corollary 13 on $\mathcal{V}$.

First we use induction on d to show that, after we have finished some degree d, the tuple $\mathcal{G}$ has the same elements as $\mathcal{V}_{\le d}$. Every element of $\mathcal{V}_d$ is appended to $\mathcal{G}$ at some point in step 7) or 8). On the other hand, if an element $g_{s'}$ is put into $\mathcal{G}$ in step 5), it has a leading term which is not a multiple of an element of $\mathcal{V}_{<d}$. Hence it is swapped out of $\mathcal{G}$ at some point in step 7).

Next we note that, after we have finished cycling through steps 3), 4), and 5) in degree d, the tuple $\mathcal{G}$ is a d-truncated minimal σ-Gröbner basis of $M_{<d}$.

Now we turn our attention to the loop described in steps 6), 7) and 8). Notice that the effect of steps 7) and 8) is independent of the order in which we choose the elements $v \in \mathcal{W}_d$ in step 6). Hence we can assume for the purposes of this proof that we always choose the vector v in $\mathcal{W}_d$ which has the minimal leading term with respect to σ. With this assumption, we show inductively that when we run steps 7) and 8) for some element $v \in \mathcal{W}_d$, at each point the elements in $\mathcal{G}$ are a minimal σ-Gröbner basis of the module they generate, and the elements of $\mathcal{V}_{\min}$ are a minimal system of generators of that module.

For the induction step, we have to consider two cases: either v is swapped into $\mathcal{G}$ in step 7) or appended to both $\mathcal{G}$ and $\mathcal{V}_{\min}$ in step 8). In the first case, it suffices to show that the module generated by the elements of $\mathcal{G}$ does not change when we perform the swap, i.e. that the difference $v - g$ is contained in this module. This follows from the observations that $\mathrm{LT}_\sigma(v-g) <_\sigma \mathrm{LT}_\sigma(v)$ and all elements $\tilde{v}$ in $\mathcal{V}$ such that $\mathrm{LT}_\sigma(\tilde{v}) <_\sigma \mathrm{LT}_\sigma(v)$ are already in $\mathcal{G}$. Since $v-g \xrightarrow{\mathcal{V}} 0$, we have $v-g \xrightarrow{\mathcal{G}} 0$. In the second case, it is clear that $\mathcal{G}$ continues to be a minimal Gröbner basis of the module it generates by Corollary 8, and $\mathcal{V}_{\min}$ continues to be a minimal system of generators of that module by Corollary 10.

Finally, we note that in step 8) we can append v to $\mathcal{G}$ without passing to the normal remainder, since v is an element of a reduced Gröbner basis and thus irreducible. □

Remark 16 Let us make some observations about the preceding algorithm.

a) The proof of the proposition shows that the algorithm reconstructs the given reduced Gröbner basis inside $\mathcal{G}$, and that $\mathcal{G}_{\leq d}$ has the same elements as $\mathcal{V}_{\leq d}$ after some degree d is finished.
b) Moreover, we note that in step 4) it is not necessary to compute the normal remainder $\mathrm{NR}_{\sigma,\mathcal{G}}(S_{ij})$. Rather, it suffices to perform a full leading term reduction.
c) The different elements $\mathrm{NR}_{\sigma,\mathcal{G}}(S_{ij})$ computed in step 4) and the elements $v \in \mathcal{V}_d$ which are swapped into $\mathcal{G}$ by step 7) are in $1-1$ correspondence, since every new element computed in step 4) must have a new leading term in the leading term module of M. This new leading term must be the leading term of an element in the reduced Gröbner basis, hence it is swapped.

4 Minimalizing the Critical Syzygies

In this section we continue to use the assumptions and notation of the previous section. If we look at Theorem 11 and its proof, we can see that instead of treating all pairs (i,j) such that σ_{ij} is contained in the set of critical syzygies Σ, it would be enough to treat those pairs corresponding to a subset $\Theta \subseteq \Sigma$ which is a minimal system of generators of $\mathrm{Syz}_P(c_1 t_1 e_{\gamma_1}, \ldots, c_s t_s e_{\gamma_s})$.

In order to find Θ, we observe that the application of two of the rules for killing critical pairs given in (Gebauer and Möller, 1987) produces a minimal Gröbner basis of the module $\mathrm{Syz}_P(c_1 t_1 e_{\gamma_1}, \ldots, c_s t_s e_{\gamma_s})$ contained in the set Σ. From this we derive the idea to find Θ by applying Theorem 15. We need the following definition.

Definition 17 On the set of terms $\mathbb{T}^n\langle \varepsilon_1, \ldots, \varepsilon_s\rangle$ in $\oplus_{i=1}^s P(-d_i)$ we define a relation τ by letting

$$t\,\varepsilon_i \geq_\tau t'\,\varepsilon_j \;\Leftrightarrow\; \begin{cases} t\,t_i\,e_{\gamma_i} >_\sigma t'\,t_j\,e_{\gamma_j}, & \text{or} \\ t\,t_i\,e_{\gamma_i} = t'\,t_j\,e_{\gamma_j} & \text{and} \quad i \geq j \end{cases}$$

for $t, t' \in \mathbb{T}^n$ and $i,j \in \{1,\ldots,s\}$. As in (Kreuzer and Robbiano, 2000), Lemma 3.1.2, it follows that τ is a module term ordering. It is called the term ordering **induced** by the tuple $(t_1 e_{\gamma_1}, \ldots, t_s e_{\gamma_s})$ and by σ.

By (Kreuzer and Robbiano, 2000), Proposition 3.1.3, the set Σ is a τ-Gröbner basis of the module $\mathrm{Syz}_P(c_1 t_1 e_{\gamma_1}, \ldots, c_s t_s e_{\gamma_s})$. Moreover, σ_{ij} is a homogeneous element of $\oplus_{i=1}^s P(-d_i)$ of degree $\deg_W(\sigma_{ij}) = \deg(\mathrm{lcm}(t_i,t_j)) + \delta_{\gamma_i}$. For all $i,j \in \{1,\ldots,s\}$, we let $t_{ij} = \frac{\mathrm{lcm}(t_i,t_j)}{t_i}$. Now the main result of Gebauer and Möller (1987) reads as follows.

Proposition 18 *Consider the following instructions.*

Rule 1. *Delete in Σ all elements σ_{jk} such that there exists an index i in the set $\{1,\ldots,j-1\}$ such that t_{ki} divides t_{kj}. Call the resulting set Σ'.*

Rule 2. *Delete in Σ' all elements σ_{ik} such that there exists an index j in the set $\{i+1,\ldots,k-1\}$ such that t_{kj} properly divides t_{ki}. Call the resulting set Σ''.*

Rule 3. *Delete in Σ'' all elements σ_{ij} such that there exists an index k in the set $\in \{j+1,\ldots,s\}$ such that t_{ik} properly divides t_{ij} and t_{jk} properly divides t_{ji}. Call the resulting set Σ'''.*

Then the set Σ''' still generates $\mathrm{Syz}_P(c_1 t_1 e_{\gamma_1}, \ldots, c_s t_s e_{\gamma_s})$.

Remark 19 Let us interpret the previous proposition in another way. For $1 \leq i < j \leq s$ such that $\gamma_i = \gamma_j$, we have $\mathrm{LT}_\tau(\sigma_{ij}) = t_{ji}\varepsilon_j$. Hence Rules 1 and 2 can be restated as follows.

RULE 1'. Delete in Σ all elements σ_{ij} such that there exists an element $\sigma_{i'j}$ such that $\mathrm{LT}_\tau(\sigma_{ij})$ is a proper multiple of $\mathrm{LT}_\tau(\sigma_{i'j})$.

RULE 2'. If, among the remaining elements, there are elements σ_{ij}, $\sigma_{i'j}$ such that $\mathrm{LT}_\tau(\sigma_{ij}) = \mathrm{LT}_\tau(\sigma_{i'j})$, then delete the one having the larger index $\max\{i, i'\}$.

¿From Rules 1' and 2' it follows that the set Σ'' is a minimal τ-Gröbner basis of the module $\mathrm{Syz}_P(c_1t_1e_{\gamma_1}, \ldots, c_st_se_{\gamma_s})$, i.e. the leading terms of the elements of Σ'' minimally generate the leading term module.

In general, it is not true that Σ'' is a minimal system of generators of the module $\mathrm{Syz}_P(c_1t_1e_{\gamma_1}, \ldots, c_st_se_{\gamma_s})$, as our next example shows. (For another example, see (Gebauer and Möller, 1987), 3.6.)

Example 20 Let $P = \mathbb{Q}[x, y, z]$ be standard graded, let $r = 1$, $s = 4$ and $t_1 = x^3z^2$, $t_2 = x^3y^4$, $t_3 = y^5z^2$, $t_4 = x^2y^5z$. Then we get $\sigma_{12} = y^4\varepsilon_1 - z^2\varepsilon_2$, $\sigma_{13} = y^5\varepsilon_1 - x^3\varepsilon_3$, $\sigma_{14} = y^5\varepsilon_1 - xz\varepsilon_4$, $\sigma_{23} = yz^2\varepsilon_2 - x^3\varepsilon_3$, $\sigma_{24} = yz\varepsilon_2 - x\varepsilon_4$, and $\sigma_{34} = x^2\varepsilon_3 - z\varepsilon_4$. By applying Rules 1 and 2, we get the minimal τ-Gröbner basis $\Sigma'' = \{\sigma_{12}, \sigma_{24}, \sigma_{34}, \sigma_{13}\}$ of $\mathrm{Syz}_P(t_1, t_2, t_3, t_4)$, since $\mathrm{LT}_\tau(\sigma_{23}) = \mathrm{LT}_\tau(\sigma_{13})$ and $\mathrm{LT}_\tau(\sigma_{14}) = z \cdot \mathrm{LT}_\tau(\sigma_{24})$. Now we use Rule 3 and find $\Sigma''' = \Sigma''$, but Σ''' is not a minimal system of generators of $\mathrm{Syz}_P(t_1, t_2, t_3, t_4)$, since we have $\sigma_{13} = y\sigma_{12} + z\sigma_{24} - x\sigma_{34}$.

Before continuing, let us introduce a new notion. If we have an element σ_{ij} and perform a reduction step $\sigma_{ij} \xrightarrow{ct\sigma_{i'j}} c't'\varepsilon_i + c''t''\varepsilon_{i'}$, where $c, c', c'' \in K$ and $t, t', t'' \in \mathbb{T}^n$, we call this a **head reduction step**. (Notice that the j-indices have to match!) Similarly, we can define a **tail reduction step** as follows: $\sigma_{ij} \xrightarrow{ct\sigma_{i'i}} c't'\varepsilon_{i'} + c''t''\varepsilon_j$. It is clear that a tail reduction step does not change the leading term of the element.

Proposition 21 *The set* $\widetilde{\Sigma} = \{-c_j \cdot \sigma_{ij} \mid \sigma_{ij} \in \Sigma''\}$ *is the reduced* τ*-Gröbner basis of the module* $\mathrm{Syz}_P(c_1t_1e_{\gamma_1}, \ldots, c_st_se_{\gamma_s})$.

Proof. Since passing from Σ'' to $\widetilde{\Sigma}$ is equivalent to normalizing the leading coefficients, and since Σ'' is a minimal τ-Gröbner basis, it remains to show that no tail reductions are possible among the elements of $\widetilde{\Sigma}$. But if we perform a tail reduction on some element of $\widetilde{\Sigma}$, we get an element of the form $\tilde{c}\,\tilde{t}\,\sigma_{i'j}$ such that $i' < i$. Here we have to have $\tilde{t} = 1$, since σ_{ij} is part of a minimal Gröbner basis. Now we obtain a contradiction to the minimality of i in Rule 2'. $\square$

Remark 22 Let us apply the algorithm of Theorem 15 to the set $\widetilde{\Sigma}$. We make the following observations.

a) A *pair of pairs*, i.e. a critical pair between two elements σ_{ij}, $\sigma_{i'j'}$ yields an S-vector $S_{((i,j),(i',j'))} = c\,t\,\sigma_{ij} - c'\,t'\,\sigma_{i'j'}$ such that $c, c' \in K$ and $t, t' \in \mathbb{T}^n$ and $j = j'$, since the two leading terms have to cancel. Without loss of generality, let $i < i'$. Then the result is $\tilde{c}\,\tilde{t}\,\sigma_{ii'}$ for some $\tilde{c} \in K$ and $\tilde{t} \in \mathbb{T}^n$. The degree of such a pair of pairs is

$$\begin{aligned}\deg_W(S_{((i,j),(i',j))}) &= \deg_W(\tilde{t}) + \deg_W(\sigma_{ii'}) \\ &= \deg_W(\tfrac{\mathrm{lcm}(t_i,t_{i'},t_j)}{t_j}) + \deg_W(\varepsilon_j) \\ &= \deg_W(\mathrm{lcm}(t_i,t_{i'},t_j)) + \delta_{\gamma_j}\end{aligned}$$

b) During the course of the algorithm, a new Gröbner basis element can only be obtained from a pair of pairs if $\tilde{t} = 1$. This is equivalent to $\gcd(t_{ij}, t_{i'j}) = 1$.

Now we are ready to optimize the minimalization of the critical syzygies. To ease the notation, we shall minimalize the set Σ'' instead of $\widetilde{\Sigma}$. The lack of the normalization of the leading coefficients is clearly of no consequence. We need the following lemma.

Lemma 23 *Let $1 \le i < j < m \le s$ and $i' \in \{1,\dots,j-1\} \setminus \{i\}$. Suppose there are terms $t, t', t'' \in \mathbb{T}^n \setminus \{1\}$ such that $\sigma_{ij} = \sigma_{ii'} + t\,\sigma_{i'j} = t'\,\sigma_{im} - t''\,\sigma_{jm}$ and $\sigma_{i'm} = t\,\sigma_{i'j} + t''\,\sigma_{jm}$. Then t, t', and t'' are pairwise coprime.*

More precisely, given $\kappa \in \{1,\dots,n\}$, we define $\alpha = \deg_{x_\kappa}(t_i)$, $\alpha' = \deg_{x_\kappa}(t_{i'})$, $\beta = \deg_{x_\kappa}(t_j)$, and $\gamma = \deg_{x_\kappa}(t_m)$. Then one of the following four cases occurs.

1) *We have $\alpha = \gamma > \beta$ and $\alpha > \alpha'$.*
2) *We have $\alpha' = \beta > \gamma$ and $\alpha' > \alpha$.*
3) *We have $\alpha = \alpha' > \beta$ and $\alpha > \gamma$.*
4) *We have $\alpha = \alpha' = \beta > \gamma$ or $\alpha = \beta = \gamma > \alpha'$ or $\alpha' = \beta = \gamma > \alpha$.*

Proof. Comparing coefficients in the given equations yields the following equalities $\mathrm{lcm}(t_i,t_j) = \mathrm{lcm}(t_i,t_{i'}) = \mathrm{lcm}(t_{i'},t_m) = t\,\mathrm{lcm}(t_{i'},t_j) = t'\,\mathrm{lcm}(t_i,t_m) = t''\,\mathrm{lcm}(t_j,t_m)$. Thus the exponent of x_κ in these terms satisfies $\max\{\alpha,\beta\} = \max\{\alpha,\alpha'\} = \max\{\alpha',\gamma\} = \deg_{x_\kappa}(t) + \max\{\alpha',\beta\} = \deg_{x_\kappa}(t') + \max\{\alpha,\gamma\} = \deg_{x_\kappa}(t'') + \max\{\beta,\gamma\}$. We distinguish the following four cases.

Case 1: Suppose that x_κ divides t. In this case, $\max\{\alpha,\alpha'\} > \max\{\alpha',\beta\}$ yields $\alpha > \alpha'$ and $\alpha > \beta$. Then $\alpha = \max\{\alpha,\alpha'\} = \max\{\alpha',\gamma\}$ shows $\alpha = \gamma$, i.e. we have the inequalities stated in case 1) of the claim. Furthermore, it follows that $\gamma = \max\{\alpha,\gamma\} = \max\{\beta,\gamma\}$, i.e. that x_κ divides neither t' nor t''.

Case 2: Suppose that x_κ divides t'. In this case, $\max\{\alpha,\alpha'\} > \max\{\alpha,\gamma\}$ yields $\alpha' > \alpha$ and $\alpha' > \gamma$. Then $\max\{\alpha,\beta\} = \max\{\alpha,\alpha'\}$ shows $\alpha' = \beta$, i.e. we have the inequalities stated in case 2) of the claim. Furthermore, it follows that $\beta = \max\{\alpha',\beta\} = \max\{\beta,\gamma\}$, i.e. that x_κ divides neither t nor t''.

Case 3: If x_κ divides t'', we argue analogously and obtain the inequalities stated in 3) as well as the fact that x_κ divides neither t nor t'.

Case 4: If x_κ divides neither t nor t' nor t'', an easy case-by-case argument yields the possibilities listed in 4). $\square$

Proposition 24 (Minimalization of the Critical Syzygies)
Let Σ'' be the τ-Gröbner basis of $\mathrm{Syz}_P(c_1t_1e_{\gamma_1},\dots,c_st_se_{\gamma_s})$ defined in Proposition 18. Consider the following instructions.

1) *Let $\mathcal{B}^* = \emptyset$, $\mathcal{W} = \Sigma''$, $\mathcal{A} = \emptyset$, and $\Theta = \emptyset$.*
2) *For all $\sigma_{ij}, \sigma_{i'j} \in \Sigma''$ such that $1 \le i < i' < j \le s$, form the S-vector $S_{((i,j),(i',j))} = \tilde{t}\,\sigma_{ii'}$, where $\tilde{t} \in \mathbb{T}^n$. If $\tilde{t} = 1$, append $\sigma_{ii'}$ to $\mathcal{B}^*$.*
3) *Let d be the smallest degree with respect to* `Lex` *of an element of $\mathcal{B}^*$ or $\mathcal{W}$. Form $\mathcal{B}^*_d$ and $\mathcal{W}_d$, and delete their entries from $\mathcal{B}^*$ and $\mathcal{W}$, respectively.*
4) *If $\mathcal{B}^*_d = \emptyset$, continue with step 11). Otherwise, choose an element $\sigma_{ij} \in \mathcal{B}^*_d$ and remove it from $\mathcal{B}^*_d$.*
5) *If $\mathrm{LT}_\tau(\sigma_{ij}) \in \mathrm{LT}_\tau(\mathcal{A}_d)$, then continue with step 4).*
6) *If $\mathrm{LT}_\tau(\sigma_{ij}) = \mathrm{LT}_\tau(\sigma_{i'j})$ for some element $\sigma_{i'j} \in \mathcal{W}_d$, then remove $\sigma_{i'j}$ from $\mathcal{W}_d$, append it to $\mathcal{A}$, and continue with step 4).*
7) *Find $\sigma_{i'j} \in \mathcal{A}_{<d}$ such that t_{ji} is a multiple of $t_{ji'}$. Then perform the head reduction step $\sigma_{ij} \xrightarrow{\sigma_{i'j}} \tilde{t}\,\sigma_{k\ell}$, where $\tilde{t} \in \mathbb{T}^n$, where $k = \min\{i,i'\}$, and where $\ell = \max\{i,i'\}$. If $\tilde{t} \ne 1$, continue with step 4).*
8) *If $\mathrm{LT}_\tau(\sigma_{k\ell}) \in \mathrm{LT}_\tau(\mathcal{A}_d)$, then continue with step 4).*
9) *If $\mathrm{LT}_\tau(\sigma_{k\ell}) = \mathrm{LT}_\tau(\sigma_{k'\ell})$ for some element $\sigma_{k'\ell} \in \mathcal{W}_d$, then remove the element $\sigma_{k'\ell}$ from $\mathcal{W}_d$, append it to $\mathcal{A}$, and continue with step 4).*
10) *If $\sigma_{k\ell} \in \mathcal{B}^*_d$, then delete $\sigma_{k\ell}$ in $\mathcal{B}^*_d$ and continue with step 7), applied to this element. Otherwise continue with step 4).*
11) *Append $\mathcal{W}_d$ to $\mathcal{A}$ and to Θ.*
12) *If $\mathcal{B}^* = \emptyset$ and $\mathcal{W} = \emptyset$, return Θ and stop. Otherwise, continue with step 3).*

This is an algorithm which computes a subset $\Theta \subseteq \Sigma''$ such that Θ is a minimal system of generators of $\mathrm{Syz}_P(c_1t_1e_{\gamma_1},\dots,c_st_se_{\gamma_s})$.

Proof. It suffices to show that the given instructions define an optimization of the application of Theorem 15 to the set Σ''. The tuple $\mathcal{A}$ corresponds to $\mathcal{G}$

there, Θ corresponds to $\mathcal{V}_{\min}$, and $\mathcal{B}^*$ corresponds to B.

The first significant difference occurs in step 2). Instead of producing the pairs of pairs inductively each time we find a new Gröbner basis element, we precompute them all at once. This is possible, since we know from Theorem 15 that we are merely recomputing the Gröbner basis Σ''. Moreover, we do not store the pairs of pairs, but the S-vectors they generate, and we do not store S-vectors which are clearly useless by part b) of the remark following Proposition 21.

The main difference occurs in steps 5) through 10). Instead of computing the normal remainder of the S-vector, we perform leading term reductions only and check the result after each reduction step. When we choose an element σ_{ij} in step 4), it is not contained in $\mathcal{A}_d$, since if an element $\sigma_{k\ell}$ is appended to $\mathcal{A}$ in step 11) and cannot be contained in $\mathcal{B}_d^*$ by step 10). But the element σ_{ij} could have a leading term in $\mathrm{LT}_\sigma(\mathcal{A}_d)$ without being contained in $\mathcal{A}_d$. We claim that, in this case, we know $\sigma_{ij} \xrightarrow{\mathcal{A}} 0$, i.e. that σ_{ij} produces no new Gröbner basis element.

To prove this claim, we first note that clearly $\mathcal{A}$ is a subtuple of $\mathcal{W}$ at all times. Since the elements of $\mathcal{W}$ are fully interreduced, the tail of σ_{ij} cannot be a leading term of an element of $\mathcal{A}_d$. On the other hand, if $\mathrm{LT}_\tau(\sigma_{ij}) = \mathrm{LT}_\tau(\sigma_{i'j})$ for $\sigma_{i'j} \in \mathcal{A}_d$, then the leading term of the result of the reduction of σ_{ij} by $\sigma_{i'j}$ is the tail of σ_{ij}. Hence σ_{ij} can be tail reduced using $\mathcal{A}_{<d}$. By applying the same argument to the result of this tail reduction step, we conclude that after several tail reductions using $\mathcal{A}_{<d}$, we reach an element of $\mathcal{A}_d$, and the claim follows.

The next possibility for σ_{ij} is that it is head irreducible with respect to $\mathcal{A}$. In this case its leading term is equal to $\mathrm{LT}_\tau(\sigma_{i'j})$ for some $\sigma_{i'j} \in \mathcal{W}_d$. Now Theorem 15 says that we should put $\mathrm{NR}_{\tau,\mathcal{A}}(\sigma_{ij})$ into $\mathcal{A}$ and later swap it for $\sigma_{i'j}$. But, as we just saw, we can tail reduce σ_{ij} using $\mathcal{A}_{<d}$ until we reach $\sigma_{i'j}$. Thus the normal remainder is $\sigma_{i'j}$ and is put into $\mathcal{A}$ immediately, i.e. without actually performing the tail reductions and without a later swap.

The last possibility for $\mathrm{LT}_\tau(\sigma_{ij})$ is that it can be reduced using $\mathcal{A}_{<d}$. This reduction step is performed in step 7). Let us discuss the possible outcomes.

If the result is of the form $\tilde{t}\,\sigma_{k\ell}$ with $\tilde{t} \in \mathbb{T}^n \setminus \{1\}$, then $\sigma_{k\ell}$ has a lower degree and satisfies $\sigma_{k\ell} \xrightarrow{\mathcal{A}} 0$, because $\mathcal{A}$ contains a truncated Gröbner basis. Consequently, we have $\sigma_{ij} \xrightarrow{\mathcal{A}} 0$ and step 4) of 15 tells us to try the next S-vector.

If the result of the head reduction step has one of the new leading terms provided by the elements of $\mathcal{W}_d$, we notice this in step 8) or 9). In the first case, the element of $\mathcal{V}_d$ has already been swapped into $\mathcal{A}$ and nothing needs to be done. In the second case, we perform the swap in step 9).

If the result is an element $\sigma_{k\ell}$ of degree d which can be further head reduced, we check in step 10) whether $\sigma_{k\ell} \in \mathcal{B}_d^*$. In that case σ_{ij} and $\sigma_{k\ell}$ have the same reductions and it suffices to treat $\sigma_{k\ell}$ in step 7). Otherwise, we claim that $\sigma_{k\ell}$ is one of the elements of B_d^* which has been dealt with already, i.e. that we can go back to step 4) and treat the next element of $\mathcal{B}_d^*$.

To prove this claim, we first use $\sigma_{ij} \in \mathcal{B}_d^*$ in order to write $\sigma_{ij} = t' \sigma_{im} + t'' \sigma_{jm}$ with $t', t'' \in \mathbb{T}^n \setminus \{1\}$ and $j < m \leq s$. Secondly, by step 7), we have the equality $\sigma_{ij} = t\, \sigma_{i'j} \pm \sigma_{k\ell}$, where $\sigma_{k\ell} = \pm\sigma_{i'i}$ and $t \in \mathbb{T}^n \setminus \{1\}$. By looking at the coefficient of e_j in the equation $\sigma_{ii'} = t'\, \sigma_{im} - t\, \sigma_{i'j} - t''\, \sigma_{jm}$, we see that $t\ \mathrm{lcm}(t_{i'}, t_j) = t''\ \mathrm{lcm}(t_j, t_m)$. This term is a multiple of $t_{i'}$ and of t_m. Hence it is of the form $\tilde{t}\ \mathrm{lcm}(t_{i'}, t_m)$ for some $\tilde{t} \in \mathbb{T}^n$, and we have $\sigma_{ii'} = t'\, \sigma_{im} - \tilde{t}\, \sigma_{i'm}$. If $\tilde{t} \neq 1$, then $\sigma_{k\ell}$ is a pair of pairs, i.e. it is either in B_d^* or it is one of the elements of B_d^* treated before. Hence the claim follows if we can show that $\tilde{t} = 1$ does not happen.

Suppose that $\tilde{t} = 1$. Then we are in the situation of the lemma. Since the conditions of steps 8) and 9) did not apply, it follows that $\sigma_{k\ell}$ can be further head reduced using $\mathcal{A}_{<d}$. Hence there exist $u, u' \in \mathbb{T}^n$ and $j' < \max\{i, i'\}$ such that $\sigma_{i'i} = u\, \sigma_{i'j'} + u'\, \sigma_{j'i}$ and $u \neq 1$ or $u' \neq 1$, depending on whether $i > i'$ or $i < i'$.

Now we show that $u' \neq 1$ is impossible. We use the notation of the lemma and let $\delta = \deg_{x_\kappa}(t_{j'})$, where x_κ is one of the indeterminates occurring in t, i.e. where case 1) of the lemma holds. Then the equation $\mathrm{lcm}(t_{i'}, t_i) = u\ \mathrm{lcm}(t_{i'}, t_{j'}) = u'\ \mathrm{lcm}(t_i, t_{j'})$ shows $\max\{\alpha, \alpha'\} > \max\{\alpha, \delta\}$. This implies $\alpha' > \alpha$ and $\alpha' > \delta$, in contradiction to case 1) of the lemma. Similarly, we can show that $u \neq 1$ is impossible. This concludes the proof of the claim.

Altogether, it follows that steps 5) – 10) implement the full reduction of σ_{ij} together with the swapping procedure of step 7) of 15. Hence the remaining elements of $\mathcal{W}_d$ are precisely the minimal generators of degree d we are looking for, and they have to be appended to Θ in step 11). □

Let us apply this algorithm in the situation of Example 20.

Example 25 Our task is to minimalize $\mathcal{W} = \Sigma'' = \{\sigma_{12}, \sigma_{13}, \sigma_{24}, \sigma_{34}\}$, where we have $\deg_W(\sigma_{12}) = 9$, $\deg_W(\sigma_{13}) = 10$, and $\deg_W(\sigma_{24}) = \deg_W(\sigma_{34}) = 9$.

In step 2), the algorithm constructs the set $\mathcal{B}^*$. The pair of pairs $((2,4),(3,4))$ yields $S_{((2,4),(3,4))} = z\sigma_{24} - x\sigma_{34} = -yz^2\varepsilon_2 + x^3\varepsilon_3 = \sigma_{23}$, and this is the only element of $\mathcal{B}^*$. Notice that it has degree 10.

In step 3), the algorithm starts to operate in degree $d = 9$. Since $\mathcal{B}_9^* = \emptyset$, it appends σ_{12}, σ_{24}, and σ_{34} to $\mathcal{A}$ and Θ in step 11).

Next we process degree 10. In step 4), we choose $\sigma_{23} \in \mathcal{B}_{10}^*$ and set $\mathcal{B}_{10}^* = \emptyset$. Then, in step 6), we find $\mathrm{LT}_\tau(\sigma_{23}) = x^3\varepsilon_3 = \mathrm{LT}_\tau(\sigma_{13})$, where $\sigma_{13} \in \mathcal{W}_{10}$. Hence σ_{13} is removed from $\mathcal{W}_{10}$ and appended to $\mathcal{A}$ in step 6).

Thus we have $\mathcal{B}^* = \emptyset$ and $\mathcal{W} = \emptyset$ at this point, and step 12) returns the set $\Theta = \{\sigma_{12}, \sigma_{24}, \sigma_{34}\}$. We note that this is the correct answer, and there is an improvement over the application of Proposition 18 coming from the fact that in step 6) we merely check $\mathrm{LT}_\tau(\sigma_{ij}) \in \mathrm{LT}_\tau(\mathcal{W}_d)$ rather than $\sigma_{ij} \in \mathcal{W}_d$.

The following example provides a case where it is actually necessary to do one head reduction step in 7) in order to find a previously undiscovered non-minimal critical syzygy.

Example 26 Let $P = \mathbb{Q}[x_1, \ldots, x_5]$ be standard graded, let $r = 1$ and $s = 4$. The terms $t_1 = x_2^2x_3^6x_4x_5^2$, $t_2 = x_1^8x_2x_4x_5^4$, $t_3 = x_1^8x_2^2x_3^6$, and $t_4 = x_1^8x_3^6x_5^4$ yield the critical syzygies $\sigma_{12} = x_1^8x_5^2\varepsilon_1 - x_2x_3^6\varepsilon_2$, $\sigma_{13} = x_1^8\varepsilon_1 - x_4x_5^2\varepsilon_3$, $\sigma_{14} = x_1^8x_5^2\varepsilon_1 - x_2^2x_4\varepsilon_4$, $\sigma_{23} = x_2x_3^6\varepsilon_2 - x_4x_5^4\varepsilon_3$, $\sigma_{24} = x_3^6\varepsilon_2 - x_2x_4\varepsilon_4$, and $\sigma_{34} = x_5^4\varepsilon_3 - x_2^2\varepsilon_4$. Here steps 1) and 2) of Proposition 18 discard σ_{23} and σ_{14}, because we have $\mathrm{LT}_\tau(\sigma_{23}) = x_4x_5^4\varepsilon_3 = x_5^2\,\mathrm{LT}_\tau(\sigma_{13})$ and $\mathrm{LT}_\tau(\sigma_{14}) = x_2^2x_4\varepsilon_4 = x_2\,\mathrm{LT}_\tau(\sigma_{24})$. Thus we have $\Sigma'' = \{\sigma_{12}, \sigma_{13}, \sigma_{24}, \sigma_{34}\}$. We note that we have $\deg_W(\sigma_{12}) = 21$, $\deg_W(\sigma_{13}) = 19$, and $\deg_W(\sigma_{24}) = \deg_W(\sigma_{34}) = 20$. But Σ'' is not minimal, since we have $\sigma_{12} = x_5^2\sigma_{13} - x_2\sigma_{24} + x_4\sigma_{34}$.

Now we apply our algorithm. In step 2), we have to compute $S_{((2,4),(3,4))} = x_2\sigma_{24} - x_4\sigma_{34} = x_2x_3^6\varepsilon_2 - x_4x_5^4\varepsilon_3 = \sigma_{23}$. Thus σ_{23} is appended to $\mathcal{B}^*$. It has degree $\deg_W(\sigma_{23}) = 21$. No further pairs of pairs are found.

In step 3), the algorithm starts to operate in degree $d = 19$. We have $\mathcal{B}_{19}^* = \emptyset$ and $\mathcal{W}_{19} = (\sigma_{13})$. Thus we append σ_{13} to $\mathcal{A}$ and Θ in step 11). Next we pass to degree $d = 20$. We still have $\mathcal{B}_{20}^* = \emptyset$, but now we get $\mathcal{W}_{20} = (\sigma_{24}, \sigma_{34})$. In step 11), σ_{24} and σ_{34} are put into $\mathcal{A}$ and Θ.

When we start processing degree $d = 21$, we have to choose $\sigma_{23} \in \mathcal{B}_{21}^*$ and set $\mathcal{B}_{21}^* = \emptyset$ in step 4). The leading term $\mathrm{LT}_\tau(\sigma_{23}) = x_4x_5^4\varepsilon_3$ is not equal to one of the leading terms of the elements of $\mathcal{A}_{21}$ or $\mathcal{W}_{21}$. But we can perform a head reduction step in 7), namely $\sigma_{23} \xrightarrow{\sigma_{13}} -\sigma_{12}$. Here step 8) does not apply, but in step 9) we have $\mathrm{LT}_\tau(\sigma_{12}) \in \mathrm{LT}_\tau(\mathcal{W}_{21})$. Thus we continue by removing σ_{12} from $\mathcal{W}_{21}$ and appending it to $\mathcal{A}$.

Finally, we get $\mathcal{B}^* = \emptyset$ and $\mathcal{W} = \emptyset$. The algorithm returns $\Theta = \{\sigma_{13}, \sigma_{24}, \sigma_{34}\}$. As mentioned above, the non-minimal critical syzygy σ_{12} was discovered after one head reduction step in 7).

5 An Optimized Buchberger Algorithm

In this section we combine the results obtained so far. We continue to use the notation and conventions of the previous sections. In particular, we let $P = K[x_1, \ldots, x_n]$ be a polynomial ring over a field K which is positively graded by a matrix $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$, and we let M be a graded submodule of a graded free P-module $F = \oplus_{i=1}^r P(-\delta_i)$ which is generated by a tuple $\mathcal{V} = (v_1, \ldots, v_s)$ of homogeneous vectors. Furthermore, we let σ be a module term ordering on $\mathbb{T}^n\langle e_1, \ldots, e_r\rangle$.

In the following theorem the sets of critical pairs corresponding to the sets of critical syzygies considered earlier are denoted by the normal letters corresponding to their calligraphic versions.

Theorem 27 (Optimized Buchberger Algorithm)
In the above situation, consider the following sequence of instructions.

1) *Let $\mathcal{W} = \mathcal{V}$, $A = \emptyset$, $B = \emptyset$, $B^* = \emptyset$, $\mathcal{G} = \emptyset$, and let $s' = 0$.*
2) *Let d be the smallest degree w.r.t.* `Lex` *of an element of B or $\mathcal{W}$. Form B_d, B_d^*, $\mathcal{W}_d$, and delete their entries from B, B^*, and $\mathcal{W}$, respectively.*
3) *Apply* `MinPairs`(A, B_d, B_d^*).
4) *If $B_d = \emptyset$, then continue with step 7). Otherwise, choose a pair (i,j) in B_d, delete it from B_d, and append it to A.*
5) *Compute S_{ij} and $S'_{ij} = \mathrm{NR}_{\sigma,\mathcal{G}}(S_{ij})$. If $S'_{ij} = 0$, then continue with 4).*
6) *Increase s' by one, append $g_{s'} = S'_{ij}$ to $\mathcal{G}$, perform* `Update`$(B, B^*, g_{s'})$, *and continue with step 4).*
7) *If $\mathcal{W}_d = \emptyset$ then continue with 10). Otherwise, choose $v \in \mathcal{W}_d$ and delete it in $\mathcal{W}_d$.*
8) *Compute $v' = \mathrm{NR}_{\sigma,\mathcal{G}}(v)$. If $v' = 0$, continue with step 7).*
9) *Increase s' by one, append $g_{s'} = v'$ to $\mathcal{G}$ and perform* `Update`$(B, B^*, g_{s'})$. *Then continue with step 7).*
10) *If $B = \emptyset$ and $\mathcal{W} = \emptyset$, then return $\mathcal{G}$ and stop. Otherwise, continue with step 2).*

Here the procedure `Update`$(B, B^*, g_{s'})$ *is defined as follows.*

U1) *Form the set $C = \{(i, s') \mid 1 \le i < s',\ \gamma_i = \gamma_{s'}\}$.*
U2) *Delete from C all pairs (j, s') for which there exists an index i in the set $\{1, \ldots, j-1\}$ such that $t_{s'i}$ divides $t_{s'j}$.*
U3) *Delete from C all pairs (i, s') for which there exists an index j in the set $\{i+1, \ldots, s'-1\}$ such that $t_{s'j}$ properly divides $t_{s'i}$.*
U4) *Find in C all pairs (i, s') and (j, s') such that $1 \le i < j < s'$ and such that $\gcd(t_{is'}, t_{js'}) = 1$. For each of these, check if (i,j) is already contained in B^* and append it if necessary.*

U5) Append the elements of C to B and stop.

Furthermore, the procedure $\texttt{MinPairs}(A, B_d, B_d^*)$ *is defined as follows.*

M1) If $B_d^* = \emptyset$, then stop. Otherwise, choose a pair (i,j) in B_d^* and remove it from B_d^*.
M2) If $t_{ji} = t_{ji'}$ for some pair $(i',j) \in A$, then continue with step M1).
M3) If $t_{ji} = t_{ji'}$ for some pair $(i',j) \in B_d$, then remove this pair from B_d and append it to A. Continue with step M1).
M4) Find $(i',j) \in A$ such that $t_{ji'}$ divides t_{ji}. Let $k = \min\{i,i'\}$, and let $\ell = \max\{i,i'\}$. If $\gcd(t_{ij}, t_{i'j}) \neq 1$, then continue with M1).
M5) If $t_{\ell k} = t_{\ell k'}$ for some pair $(k',\ell) \in A$, then continue with M1).
M6) If $t_{\ell k} = t_{\ell k'}$ for some pair $(k',\ell) \in B_d$, then delete this pair in B_d, append it to A, and continue with M1).
M7) If $(k,\ell) \in B_d^*$, then delete (k,ℓ) in B_d^* and continue with M4), applied to this pair.
M8) Continue with step M1).

Altogether, we obtain an algorithm which computes a tuple $\mathcal{G}$ whose elements form a homogeneous σ-Gröbner basis of M. Moreover, the set of pairs which are treated at some time in steps 4) – 6) of the algorithm corresponds to a minimal system of generators of the module $\mathrm{Syz}_P(c_1t_1e_{\gamma_1}, \ldots, c_{s'}t_{s'}e_{\gamma_{s'}})$.

Proof. The main algorithm of this theorem agrees with the Homogeneous Buchberger Algorithm (see Theorem 11), except for the introduction of the procedure $\texttt{MinPairs}(A, B_d, B_d^*)$ in step 3) and the alteration of the enlargement of B in steps 5) and 8) of Theorem 11 which is now performed by the procedure $\texttt{Update}(B, B^*, g_{s'})$.

The foundation for these changes is the material presented above, especially Proposition 24. In steps 4) – 6) we want to treat only those pairs (i,j) for which the corresponding elements σ_{ij} are contained in the minimal system of generators Θ of the graded P-module $\mathrm{Syz}_P(c_1t_1e_{\gamma_1}, \ldots, c_{s'}t_{s'}e_{\gamma_{s'}})$.

Procedure $\texttt{Update}(B, B^*, g_{s'})$ applies Rules 1) and 2) of Gebauer-Möller in steps U2) and U3), respectively. Moreover, notice that step U4) computes all pairs of pairs which satisfy the condition of part b) of Remark 22, and stores the pairs corresponding to the resulting S-vectors in B^*.

Thus, in order to minimalize the critical pairs we process, we need to apply Proposition 24 to the set of critical syzygies corresponding to the set of critical pairs B, where we can refrain from computing the pairs of pairs, because they have already been generated and stored in B^*. This task is performed by the procedure $\texttt{MinPairs}(A, B_d, B_d^*)$. Its steps M1) – M8) are easy translations of steps 4) – 10) of Proposition 24 into the language of pairs. Notice that we have $\mathrm{LT}_\tau(\sigma_{ij}) = \mathrm{LT}_\tau(\sigma_{k\ell})$ if and only if $j = \ell$ and $t_{ji} = t_{\ell k}$. Altogether, $\mathtt{Update}(B, B^*, g_{s'})$ and $\mathtt{MinPairs}(A, B_d, B_d^*)$ make sure that only the pairs corresponding to Θ are treated at some point in steps 3) – 6).

Finally, we remark that A is used to keep track of the pairs (i,j) for which σ_{ij} is in that part of the minimal τ-Gröbner basis Σ'' of $\mathrm{Syz}_P(c_1 t_1 e_{\gamma_1}, \dots, c_{s'} t_{s'} e_{\gamma_{s'}})$ which has been computed so far. Thus it is updated when a non-minimal element of Σ'' is found in step M3) or step M6), and when a pair corresponding to an element of Θ is chosen for treatment in step 3). $\square$

Let us illustrate the performance of this algorithm by a simple example. It shows that cases like Example 20 occur naturally during actual Gröbner basis computations.

Example 28 Let $P = \mathbb{Q}[x,y,z]$ be standard graded, let $\sigma = \mathtt{DegLex}$, let $r = 1$, and let $M \subseteq P$ be the homogeneous ideal generated by the polynomials $v_1 = x^3z^2 + x^2y^2z$, $v_2 = x^3y^8$, and $v_3 = y^{10}z^2$. Then the leading terms are $t_1 = x^3z^2$, $t_2 = x^3y^8$, and $t_3 = y^{10}z^2$. Let us follow the steps of the Optimized Buchberger Algorithm.

The first degree is $d = 5$. Since $B_5 = \emptyset$, the first actions are to choose $v_1 \in \mathcal{W}_5$ in step 7) and append $g_1 = v_1$ to $\mathcal{G}$ in step 9). Then we continue with $d = 11$ and choose $v_2 \in \mathcal{W}_{11}$ in step 7). Since $v' = \mathrm{NR}_{\sigma,\mathcal{G}}(v_2) = v_2$, we append $g_2 = v_2$ to $\mathcal{G}$ in step 9) and update the set of pairs. The result is $B = \{(1,2)\}$ and $B^* = \emptyset$. Now we have to treat the degree $d = 12$. Notice that the degree of the pair $(1,2)$ is 13. Hence $B_{12} = \emptyset$ and we have to choose $v_3 \in \mathcal{W}_{12}$ in step 7). Since $v' = \mathrm{NR}_{\sigma,\mathcal{G}}(v_3) = v_3$, we append $g_3 = v_3$ to $\mathcal{G}$ in step 9) and update the set of pairs. In step U1), we form $C = \{(1,3),(2,3)\}$. In step U2), we obtain $t_{31} = x^3 = t_{32}$, and therefore $(2,3)$ is deleted in C. The result is $B = \{(1,2),(1,3)\}$ and $B^* = \emptyset$. This completes degree 12, and we continue with degree 13.

We choose the pair $(1,2)$ in step 4) and append it to A. Then we compute $S_{12} = y^8 g_1 - z^2 g_2 = x^2y^{10}z$ and $S'_{12} = \mathrm{NR}_{\sigma,\mathcal{G}}(S_{12}) = x^2y^{10}z$. Thus we have a new Gröbner basis element $g_4 = x^2y^{10}z$ and need to update the pairs again. In step U1), we form $C = \{(1,4),(2,4),(3,4)\}$. Step U2) does not apply, but in step U3) we remove the pair $(1,4)$ from C, since $t_{42} = x$ properly divides $t_{41} = xz$. Now we check that $t_{24} = y^2z$ properly divides $t_{23} = y^2z^2$ and $t_{34} = x^2$ properly divides $t_{32} = x^3$. Hence the pair $(2,3)$ is appended to B^*.

At this point we have finished degree 13, and we have the following situation: $A = \{(1,2)\}$, $B = \{(1,3),(2,4),(3,4)\}$, $B^* = \{(2,3)\}$, $\mathcal{G} = \{g_1,\dots,g_4\}$, and $s' = 4$. The next degree is $d = 14$, where we have to deal with the pairs in $B_{14} = \{(2,4),(3,4)\}$. Since $B_{14}^* = \emptyset$, we choose $(2,4)$ in step 4) and append it to A. Then we compute $S_{24} = 0$ and continue by choosing $(3,4)$ in B_{14}

and adding it to A. Again $S_{34} = 0$, and degree 14 is finished.

Now we start degree 15 by performing `MinPairs`(A, B_{15}, B^*_{15}), where we have $A = \{(1,2),(2,4),(3,4)\}$, $B_{15} = \{(1,3)\}$ and $B^*_{15} = \{(2,3)\}$. In step M1), we choose $(2,3)$. In step M3), we discover $t_{32} = x^3 = t_{31}$, where $(3,1) \in B_{15}$. Hence $(1,3)$ is deleted in B_{15} and appended to A. Then the procedure is finished, and the facts that $B_{15} = \emptyset$ as well as $\mathcal{W}_{15} = \emptyset$ allow us to return $\mathcal{G}$ and stop.

As in Example 20, we have found one useless pair, namely the pair $(1,3)$ in degree 15, which would not have been discovered by the Gebauer-Möller Installation, and which we were able to discard by a simple combinatorial check.

Remark 29 Let us discuss the efficiency of the algorithm of Theorem 27.

a) Steps U2) and U3) of this algorithm correspond to Rules 1) and 2) of the Gebauer-Möller installation. However, Rule 3 is not performed by the procedure `Update`$(\ldots)$, but by step M2) of the procedure `MinPairs`$(\ldots)$. In fact, step M2) gets rid of more pairs than Rule 3, because Rule 3 requires $(i,j) \in B^*_d \cap B_d$, whereas we only need a pair $(i,j) \in B^*_d$ such that $\mathrm{LT}_\tau(\sigma_{ij}) = \mathrm{LT}_\tau(\sigma_{i'j})$ for some $(i',j) \in B_d$.
b) A potential drawback of our approach is that the number of pairs of pairs considered in step U4) is quadratic in the number of elements of C surviving steps U2) and U3). But that number is usually fairly small. Hence the cost of U4) and the cardinality of B^* tend to be rather small. On the other hand, we do not need to check Rule 3 for all elements of the list B which is usually rather long. Our experiments suggest that, on average, the overhead of the two approaches is comparable.
c) Our procedure `MinPairs`$(\ldots)$ is very efficient in treating the elements of B^*_d. Each time we loop through steps M2) – M8), we delete one pair in B^*_d, and B^*_d is never enlarged. In practice, we find that the lists B^*_d are generally small. Hence our algorithm harnesses the full power and efficiency of the Gebauer-Möller installation, while it simultaneously kills *all* unnecessary pairs at a comparatively small cost.

6 Experimental Data and Conclusions

In this section we want to provide the reader with some experimental numerical data which illustrate the performance of the Optimized Buchberger Algorithm 27 as well as technical observations coming from an implementation in an experimental version of the "CoCoA 5" library in C++.

In the following table, we compare the application of Rules 1) – 3) of Proposition 18 to our procedures `Update`(...) and `Minpairs`(...) in Theorem 27, i.e. to the algorithm of Proposition 24. Let us point out that our procedure always minimalizes the critical pairs, independent of the order of the underlying terms. (Non-minimal critical pairs are recognized at different steps, though.) For the Gebauer-Möller installation, however, the number of undiscovered non-minimal critical pairs depends strongly on this order.

To aid the reader in understanding this table, let us explain the meaning of the symbols.

- $\#(G)$ is the cardinality of the reduced Gröbner basis of the corresponding ideal.
- $\#(\Sigma)$ is the total number of pairs, i.e. $\#(\Sigma) = \binom{\#(G)}{2}$.
- $\#(\Sigma'')$ is the number of pairs surviving Rules 1) and 2), i.e. the cardinality of the reduced Gröbner basis of pairs.
- B is the number of pairs killed by Rule 3), the Gebauer-Möller "Backwards" criterion.
- $M23$ is the number of pairs killed by steps M2) and M3) in Theorem 27.
- $M48$ is the number of pairs killed by steps M4) – M8) in Theorem 27.
- **Gain** $= M23 + M48 - B$, i.e. the number of newly discovered non-minimal critical pairs.
- $\#(\Theta)$ is the cardinality of a minimal system of generators of the syzygies of the leading terms. Hence we have $\#(\Theta) = \#(\Sigma'') - M23 - M48$

	$\#(G)$	$\#(\Sigma)$	$\#(\Sigma'')$	B	$M23$	$M48$	**Gain**	$\#(\Theta)$
T^51	83	3,403	250	7	7	0	**0**	243
Twomat3	109	5,886	741	15	26	1	**12**	714
Alex3	211	22,155	684	54	56	1	**3**	627
Gaukwa4	267	35,511	1,772	101	113	3	**15**	1,656
Kin1	306	46,665	3,411	70	172	0	**102**	3,239
Wang (Lex)	317	50,086	1,457	60	61	7	**8**	1,389
Cyclic 7	443	97,903	2,651	17	17	0	**0**	681
Hairer-2	506	127,765	5,305	150	152	4	**6**	5,149
Hom-Gonnet	854	364,231	11,763	587	648	27	**88**	11,088
Mora-9	4,131	8,530,515	46,395	1,930	1,914	23	**7**	44,458

The rows of this table correspond to standard examples of Gröbner basis computations. A file containing a description of every example can be downloaded at `ftp://cocoa.dima.unige.it/papers/CaboaraKreuzerRobbiano03.cocoa`

Moreover, a file containing the list of leading terms of the reduced Gröbner basis for each example can be downloaded at

`ftp://cocoa.dima.unige.it/papers/CaboaraKreuzerRobbiano03_2.cocoa`

Technical note: In the well-known example "Cyclic 7" we have homogenized using a new *smallest* indeterminate (see the file mentioned above).

For the reader who would like to run his own tests, we note that $\#(G)$, $\#(\Sigma)$, and $\#(\Theta)$ are invariants of the reduced Gröbner basis. But the effect of both the Gebauer-Möller installation and our Optimized Buchberger Algorithm depend strongly on the order in which the elements of Σ are produced during a Gröbner basis computation. For instance, this means that it depends on the chosen selection strategy. In our implementation pairs are kept ordered in increasing `DegLex` ordering, reductors are kept in the same order they are produced, reductors of the same degree are kept interreduced, and the reduction strategy is full reduction.

The following table shows some timings. It compares Singular 2.0.0 with the current experimental version of CoCoA 5 using the GM and CKR pair handling algorithms. Timings are in seconds for Linux running on an Athlon 2000+ CPU with 1.5GB RAM. All computations are over the rationals where the timings of the base field operations in Singular and CoCoA seem to be comparable.

Technical note: The reason why we include a comparison with Singular is an explicit request made by a referee, who suggested comparing our timings with "another efficient implementation". The table below indicates that both Singular and CoCoA 5 have efficient implementations of the Buchberger algorithm, and that our new algorithm has at least the same efficiency.

	Singular 2.0.0	CoCoA5 GM	CoCoA5 CKR
Tˆ51 (Lex)	149.32	7.28	7.14
Twomat3	1.21	8.66	8.50
Alex3	$<<1$	0.54	0.56
Gaukwa4	80.30	99.31	98.57
Kin1	407.09	89.25	87.41
Wang (Lex)	>1200	382.86	379.31
Cyclic 7	>1200	76.61	76.65
Hairer-2	79.36	141.83	139.76
Hom-Gonnet	3.97	4.55	4.95
Mora-9	30.53	86.17	89.75

Conclusions

First of all, let us collect some technical observations based on our implementation of the Optimized Buchberger Algorithm.

a) When we apply Rules 1 and 2 of Proposition 18, the remaining set of pairs Σ'' is usually almost a minimal system of generators of the module $\mathrm{Syz}_P(c_1 t_1 e_{\gamma_1}, \ldots, c_{s'} t_{s'} e_{\gamma_{s'}})$. Thus both Rule 3 and our algorithm kill comparatively few pairs. Nonetheless, over the rationals (or other costly fields), the saving is worthwhile because the treatment of each single pair can take a long time.

b) Steps M5) – M7) in the Optimized Buchberger Algorithm are independent. Hence it is possible to order them in such a way that the computational cost is minimized. This may be important if there is a large number of elements in B_d^* to be processed, since the operations may have substantially different computational costs.

c) All operations in our procedures `Update(...)` and `MinPairs(...)` have been greatly eased by memorizing the terms t_{ij}, t_{ji} and $\mathrm{lcm}(t_i, t_j)$ directly in the pair data type.

d) When a search is performed on the pairs in A, B, or B_d, full advantage can be taken of the fact that we may rely on data structures which allow logarithmic search costs.

Looking at the timings above, we see that, on average and with comparable implementations, our new algorithm is faster than the Gebauer-Möller installation. In some examples, the gains are relatively small, and in exceptional cases, the structure of the combinatorial data produces a larger overhead for our algorithm than for the Gebauer-Möller installation.

Acknowledgments

The third author is grateful to the organizers of the First International Congress of Mathematical Software (Beijing 2002) for their hospitality and the possibility to present his work to a wide audience. An extended abstract of this paper was published in the proceedings of the congress (see (Caboara, Kreuzer and Robbiano, 2002)).

References

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 LNCS **72**, 3–21.

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

Caboara, M., Kreuzer, M. and Robbiano, L. (2002) Minimal sets of critical pairs. In: (A. Cohen, X. Gao and N. Takayama, Eds.) *Mathematical Software, Proc. Conf. Beijing 2002.* World Scientific. Pp. 390–404

CoCoA (2001). A system for doing *Co*mputations in *Co*mmutative *A*lgebra. Available via anonymous ftp from `cocoa.dima.unige.it`

Faugère, J.C. (2002). A new efficient algorithm for computing Gröbner bases without reduction to zero (F5). In: (T. Mora, Ed.) *Symbolic and Algebraic Computation, Proc. Conf. ISSAC 2002.* ACM Press. Pp. 75–83

Gebauer, R. and Möller, H.M. (1987). On an installation of Buchberger's algorithm. *J. Symbolic Computation*, 6: 257–286.

Kreuzer, M. and Robbiano, L. (2000). *Computational Commutative Algebra 1.* Springer, Heidelberg.

Kreuzer, M. and Robbiano, L. (In preparation). *Computational Commutative Algebra 2.* Springer, Heidelberg.