Detecting Unnecessary Reductions in an Involutive Basis Computation

Joachim Apel
Mathematisches Institut
Universität Leipzig
D-04109 Leipzig, Germany
apel@mathematik.uni-leipzig.de

Ralf Hemmecke
Research Institute for Symbolic Computation
Johannes Kepler Universität
A-4040 Linz, Austria
ralf@hemmecke.de

October 30, 2002

Abstract

We consider the check of the involutive basis property in a polynomial context. In order to show that a finite generating set F of a polynomial ideal I is an involutive basis one must confirm two properties. Firstly, the set of leading terms of the elements of F has to be complete. Secondly, one has to prove that F is a Gröbner basis of I. The latter is the time critical part but can be accelerated by application of Buchberger's criteria including the many improvements found during the last two decades.

Gerdt and Blinkov (Involutive Bases of Polynomial Ideals. *Mathematics and Computers in Simulation* **45**, pp. 519–541, 1998) were the first who applied these criteria in involutive basis computations. We present criteria which are also transfered from the theory of Gröbner bases to involutive basis computations. We illustrate that our results exploit the Gröbner basis theory slightely more than those of Gerdt and Blinkov. Our criteria apply in all cases where those of Gerdt/Blinkov do, but we also present examples where our criteria are superior.

Some of our criteria can be used also in algebras of solvable type, e. g., Weyl algebras or enveloping algebras of Lie algebras, in full analogy to the Gröbner basis case.

We show that the application of criteria enforces the termination of the involutive basis algorithm independent of the prolongation selection strategy.

1 Introduction

This article contributes to an improvement of Janet's involutive basis algorithm in the context of polynomial ideals by adding criteria to avoid needless reductions. Since the involutive basis algorithm is similar to Buchberger's Gröbner basis algorithm [Buc65], it is quite natural to ask whether one can adapt the improvements such as the use of criteria as described in [Buc79] in order to speed up the algorithm. A first attempt has already been given by Gerdt and Blinkov [GB98]. Although many useless prolongations are detected by their criterion, we found examples where our more general criteria detect additional unnecessary reductions. Two such examples are given in Section 8. In fact, our criteria are as strong as in the Gröbner basis case in the sense that if three polynomials form a Buchberger triple, cf. [BW93, p. 229], one S-pair is avoided.

We start by recalling some standard notions and clarify our notation in Section 2. Our main theorem is presented and proved in Section 3. In Section 4, we extract from the main theorem some criteria. Furthermore we present an algorithm to test the involutive basis property which incorporates these criteria. The following Section 5 compares our criteria with Buchberger's criteria. The application of our criteria to the computation of involutive bases is treated in Section 6.

Up to now any implementation of the involutive basis algorithm is bound to a normal selection strategy, i. e., one must choose the next prolongation such that its leading term is minimal with respect to the divisibility semiorder. Apel [Ape98a] proved that the involutive basis algorithm (without usage of criteria) will terminate if the division refines the Thomas division in each step and a normal selection strategy is used. We give an example in Section 7 where the involutive basis algorithm does not terminate if one deviates from a normal strategy. In the same section we show, however, that termination is guaranteed even independent of the selection strategy if our criteria are applied.

We conclude our article with two examples that demonstrate the power of our criteria.

2 Preliminaries

As a reference we give here our notation in tabular form.

X	set of variables $X = \{x_1, \ldots, x_n\}$
$\mathbb{K}$	field
$\mathbb{K}[X]$	polynomial ring over $\mathbb{K}$ in the variables X
$\mathrm{Id}(G)$	ideal of $G \subseteq \mathbb{K}[X]$ in $\mathbb{K}[X]$
T	monoid of all power products of $\mathbb{K}[X]$
$u \trianglelefteq v$	divisibility relation on T: 'u divides v'
$u \triangleleft v$	divisibility relation on T: 'u divides v properly'
$\langle U \rangle$	monoid in T generated by $U \subseteq T$
$t\,\langle Y \rangle$	cone with vertex t, $t\,\langle Y \rangle = \{tu \mid u \in \langle Y \rangle\}$
$\prec$	admissible term order on T
$\operatorname{supp} f$	set of all terms of f
$\operatorname{lt} f$	leading term of f with respect to $\prec$
$\operatorname{lc} f$	leading coefficient of f with respect to $\prec$

$\operatorname{lm} f$	leading monomial of f with respect to $\prec$, $\operatorname{lm} f = \operatorname{lc}(f)\operatorname{lt}(f)$
$[g_1, g_2]$	abbreviation for $\operatorname{lcm}(\operatorname{lt} g_1, \operatorname{lt} g_2)$
$\operatorname{spol}(f, g)$	S-polynomial of f and g
$a \trianglelefteq_G g$	'ancestor of' relation wrt G: 'a is an ancestor of g'
$\operatorname{anc} g$	ancestor polynomial a with $a \trianglelefteq_G g$
$\operatorname{wanc} g$	weak ancestor polynomial w with $\operatorname{lt} w \trianglelefteq \operatorname{lt} g$
$\mathfrak{F}_t^G$	$\left\{ \sum_{g\in G} h_g g \,\middle|\, \forall_{g\in G}\, h_g \in \mathbb{K}[X] \wedge (h_g = 0 \vee \operatorname{lt}(h_g g) \preceq t) \right\}$
$\hat{\mathfrak{F}}_t^G$	abbreviation for $\bigcup_{s\prec t} \mathfrak{F}_s^G$
$S(f, g)$	abbreviation for the relation $\operatorname{spol}(f, g) \in \hat{\mathfrak{F}}^G_{[f,g]}$
$R(x, g, f)$	abbreviation for '$\mathrm{NF}_{\mathcal{M}}(xg, G)$ was computed' where xg was involutively top-reduced using f

We denote by $\mathbb{K}[X]$ the polynomial ring over a field $\mathbb{K}$ in the variables $X = \{x_1, \ldots, x_n\}$. The monoid of power products of $\mathbb{K}[X]$ is denoted by T. Since we are not interested in this article in computations with respect to different term orders we fix an arbitrary admissible[1] term order $\prec$ on T. For $0 \neq g \in \mathbb{K}[X]$ we denote by $\operatorname{supp} g$ ($\subset T$) the set of terms of g that appear with a non-zero coefficient and by $\operatorname{lt} g$ the biggest term of $\operatorname{supp} g$ with respect to the term order. Furthermore, if $G \subseteq \mathbb{K}[X]$, let $\operatorname{lt}(G) := \{\operatorname{lt} g \mid 0 \neq g \in G\}$. Divisibility and proper divisibility of two terms $u, v \in T$ is written as $u \trianglelefteq v$ and $u \triangleleft v$, respectively. By $[g_1, g_2]$ we abbreviate the least common multiple of the leading terms of two polynomials $g_1, g_2 \in \mathbb{K}[X]$.

Definition 2.1 *[Ape98b, p. 54] Let $G = \{g_1, \ldots, g_r\} \subseteq \mathbb{K}[X]$ and $\prec$ be an admissible term order on T. For $t \in T$, let $\mathfrak{F}_t^{G,\prec}$ be the additive subgroup of $I := \operatorname{Id}(G)$ consisting of all polynomials $h \in I$ which can be represented in the form $h = \sum_{\varrho=1}^{r} h_\varrho g_\varrho$ where $h_\varrho \in \mathbb{K}[X]$ and either $h_\varrho = 0$ or $\operatorname{lt}(h_\varrho g_\varrho) \preceq t$ for all $\varrho = 1, \ldots, r$. The family $\left(\mathfrak{F}_t^{G,\prec}\right)_{t\in T}$ is a $\mathbb{K}[X]$-module filtration of I, the so-called* ***Gröbner filtration*** *of I. By $\hat{\mathfrak{F}}_t^{G,\prec}$ we denote the union $\bigcup_{s\prec t} \mathfrak{F}_s^{G,\prec}$.*

Since we have fixed a term order, we omit the upper index $\prec$ throughout the rest of the article.

The proof of our main theorem is based on the following characterisation of Gröbner bases.

Theorem 2.2 *[Ape98b, Theorem 5.4] Let $G = \{g_1, \ldots, g_r\} \subseteq \mathbb{K}[X]$. G is a Gröbner basis of $I := \operatorname{Id}(G)$ if and only if $\mathfrak{F}_t^G = \{h \in I \mid h = 0 \vee \operatorname{lt} h \preceq t\}$ for all $t \in T$.*

Definition 2.3 *Let $g_1, g_2 \in \mathbb{K}[X]$. We define the* ***S-polynomial*** *of g_1 and g_2 by*

$$\operatorname{spol}(g_1, g_2) := \frac{t_1 g_1}{\operatorname{lc}(t_1 g_1)} - \frac{t_2 g_2}{\operatorname{lc}\,(t_2 g_2)}$$

where $t_1, t_2 \in T$ are such that $\operatorname{lt}(t_1 g_1) = \operatorname{lt}(t_2 g_2) = [g_1, g_2]$.

[1] An order on T is admissible if it is a well-order and compatible with the monoid structure of T.

Definition 2.4 *Let $G \subseteq \mathbb{K}[X]$ and $f, g \in \mathbb{K}[X]$. We define by $S^G(f,g)$ the binary predicate* $\operatorname{spol}(f,g) \in \hat{\mathfrak{F}}^G_{[f,g]}$. *In places where G is clear from the context, we omit the upper index and simply write $S(f,g)$.*

The notation $S(f,g)$ is just a short hand for saying that the S-polynomial has a 'good' representation. Note that the following lemma is just Buchberger's chain criterion.

Lemma 2.5 *[Buc79] Let $G \subseteq \mathbb{K}[X]$ be a finite set of non-zero polynomials. For any $f, g, p \in G$ it holds*

$$S(f,p) \wedge S(p,g) \wedge \operatorname{lt} p \trianglelefteq [f,g] \implies S(f,g).$$

Definition 2.6 *Let $G = \{g_1, \ldots, g_r\} \subset \mathbb{K}[X]$ be a set of non-zero polynomials. We define a quasi order $\trianglelefteq_G$ on G by $f \trianglelefteq_G g$ if and only if there exist $c \in \mathbb{K}$ and $t \in T$ such that $g - ctf \in \hat{\mathfrak{F}}^G_{\operatorname{lt} g}$. If $f \trianglelefteq_G g$, we say that f is an* ***ancestor*** *of g.*

The quasi order $\trianglelefteq_G$ is a partial order if all leading terms of G are pairwise distinct.

Note that $f \trianglelefteq_G g$ implies $\operatorname{lt} f \trianglelefteq \operatorname{lt} g$ and $S(f,g)$.

Janet [Jan20] introduced an algorithm to compute passive complete systems of PDEs. His algorithm was translated by Wu [Wu91] and Zharkov and Blinkov [ZB93] into the world of polynomials where it turned out to be another method to compute Gröbner bases that possess an additional structure. Such a structure comes from a separation of the variables into multiplicative and non-multiplicative. Janet used a certain rule for the separation of variables (nowadays known as Janet division). Gerdt and Blinkov [GB98] realised that such a separation can be generalised and came up with the concept of 'involutive division'. A second approach of generalising Janet's method is due to Apel [Ape98a]. Although there are now two slightly differing notions of involutive division, our main theorem will be shown to hold in both situations. We will explicitly state the necessary assumptions that must additionally be made.

Since an involutive division can be seen as a restriction of the ordinary divisibility relation on terms, Apel [Ape98b] used the term 'admissible partial division' instead.

Definition 2.7 *Let $(Y_t)_{t \in T}$ be a family of subsets of X. The family $\mathcal{M} = (t\langle Y_t \rangle)_{t \in T}$ is called a* ***partial division****. If $v \in u\langle Y_u \rangle$, then v is called an* ***$\mathcal{M}$-multiple*** *of u, and u is an* ***$\mathcal{M}$-divisor*** *of v. The* ***ordinary division*** *$(t\langle X \rangle)_{t \in T}$ is denoted by $\mathcal{O}$.*

Let $U \subseteq T$. Each family $\mathcal{N} = (u\langle Y_u \rangle)_{u \in U}$ ***induces*** *a partial division $\mathcal{M} = (t\langle Y_t \rangle)_{t \in T}$ by setting $Y_t := X$ for $t \notin U$. We also call $\mathcal{N}$ a partial division and mean its induced partial division. Let $\sqsubset$ be an irreflexive linear order on $U \subseteq T$. A partial division $\mathcal{M} = (t\langle Y_t \rangle)_{t \in T}$ is called* ***admissible on*** *$(U, \sqsubset)$ if for all $u, v \in U$ with $u \sqsubset v$, one of the conditions*

$$u\langle X \rangle \cap v\langle Y_v \rangle = \emptyset \text{ or} \tag{1}$$

$$u\langle Y_u \rangle \subset v\langle Y_v \rangle \tag{2}$$

holds. $\mathcal{M}$ *is* ***admissible on*** U *or* U***-admissible*** *if there exists an irreflexive linear order* $\sqsubset$ *on* U *such that* $\mathcal{M}$ *is admissible on* $(U, \sqsubset)$.

Let $\mathcal{M} = (t\langle Y_t\rangle)_{t\in T}$ *be a partial division. The set* $U \subseteq T$ *is called* $\mathcal{M}$***-complete*** *if* $\mathcal{M}$ *is admissible on* U *and*

$$\bigcup_{t\in U} t\langle Y_t\rangle = \bigcup_{t\in U} t\langle X\rangle .$$

The set U *is called* ***complete*** *if* U *is* $\mathcal{M}$*-complete for some partial division* $\mathcal{M}$.

The following definition introduces a partial order on the set of all partial divisions.

Definition 2.8 *[Ape98a] Let* $\mathcal{M}$ *and* $\mathcal{N}$ *be two partial divisions. If* $\mathcal{M}_t \subseteq \mathcal{N}_t$ *for all* $t \in T$ *we say that* $\mathcal{N}$ ***refines*** $\mathcal{M}$.

The Thomas division [Tho37] is a particular admissible partial division and mainly of theoretical interest. Apel [Ape98a] showed that the involutive basis algorithm will terminate if one chooses in each iteration a partial division which refines the Thomas division.

Definition 2.9 (Thomas Division) *Let* $U \subseteq T$ *be a set of power products. Define* $Y_t = X$ *for all* $t \notin U$ *and* $Y_t := \{x \in X \mid \forall u \in U : \deg_x u \leq \deg_x t\}$ *for all* $t \in U$*. The division* $(t\langle Y_t\rangle)_{t\in T}$ *is called* ***Thomas division on*** U.

Definition 2.10 *Let* $G \subseteq \mathbb{K}[X]$ *be a set of polynomials.* G *is called an* ***involutive basis*** *if* G *is a Gröbner basis and* $\operatorname{lt} G$ *is complete. An involutive basis* G *is an* $\mathcal{M}$***-involutive basis*** *if* $\operatorname{lt} G$ *is* $\mathcal{M}$*-complete for some partial division* $\mathcal{M}$.

Definition 2.11 *Let* $G \subseteq \mathbb{K}[X]$ *be a set of non-zero polynomials and* $\mathcal{M}$ *be a partial division.* G *is called* $\mathcal{M}$***-minimal*** *(resp.* $\mathcal{M}$***-reduced****) if* $\operatorname{lt} g \notin \mathcal{M}_{\operatorname{lt} g'}$ *(resp.* $\operatorname{supp} g \cap \mathcal{M}_{\operatorname{lt} g'} = \emptyset$ *and* $\operatorname{lc} g = 1$*) for all* $g, g' \in G$ *with* $g \neq g'$.

Theorem 2.12 *[Ape98a, Theorem 5.1] Let* $G = \{g_1, \ldots, g_r\} \subseteq \mathbb{K}[X]$ *be a set of non-zero monic polynomials and let* $\sqsubset$ *be an irreflexive linear order on* T*. Let* $\mathcal{M} = (t\langle Y_t\rangle)_{t\in T}$ *be a partial division which is admissible on* $(\operatorname{lt} G, \sqsubset)$*. Furthermore assume that* G *is* $\mathcal{M}$*-minimal. Then the following statements are equivalent.*

(i) G *is an* $\mathcal{M}$*-involutive basis.*

(ii) $\operatorname{lt} G$ *is* $\mathcal{M}$*-complete and* G *is a Gröbner basis.*

(iii) $\operatorname{lt} G$ *is* $\mathcal{M}$*-complete and* $S(g_i, g_j)$ *for all* $1 \leq i < j \leq r$.

(iv) For all $1 \leq i \leq r$ *and* $x \in X \setminus Y_{\operatorname{lt} g_i}$ *there exist* $j \in \{1, \ldots, r\}$ *and* $t \in \langle Y_{\operatorname{lt} g_j}\rangle$ *such that* $xg_i - tg_j \in \hat{\mathfrak{F}}^G_{\operatorname{lt}(xg_i)}$.

(v) For all $1 \leq i \leq r$ *and* $x \in X \setminus Y_{\operatorname{lt} g_i}$ *there exist* $j \in \{1, \ldots, r\}$ *and* $t \in \langle X\rangle$ *such that* $xg_i - tg_j \in \hat{\mathfrak{F}}^G_{\operatorname{lt}(xg_i)}$ *and* $\operatorname{lt}(g_j) \sqsubset \operatorname{lt}(g_i)$.

Proof. The implications (i) $\iff$ (ii) $\iff$ (iii) $\implies$ (iv) are trivial. The implication (iv) $\implies$ (v) follows by admissibility of $\mathcal{M}$ on $(\operatorname{lt} G, \sqsubset)$. And (v) $\implies$ (ii) follows from Theorem 5.1 in [Ape98a]. $\square$

3 Main Theorem

Our main theorem will add another equivalent condition to those presented in Theorem 2.12. We are going to present the theorem first and use in the proof some lemmata that will follow. Let us emphasise the fact, that the lemmata are pure Gröbner business without any reference to a partial division.

Theorem 3.1 *Let $G \subseteq \mathbb{K}[X]$ be a set of non-zero monic polynomials, let $\sqsubset$ be an irreflexive linear order on $\operatorname{lt} G$, and let $\mathcal{M} = (t\,\langle Y_t\rangle)_{t\in T}$ be an admissible partial division on $(\operatorname{lt} G, \sqsubset)$ such that G is $\mathcal{M}$-minimal. Moreover, let $\blacktriangleleft$ be an arbitrary linear order on G.*

For all $g \in G$ and $x \in X \setminus Y_{\operatorname{lt} g}$ let there exists $f \in G$ such that $\operatorname{lt}(xg) \in \mathcal{M}_{\operatorname{lt}(f)}$ and one of the following conditions holds.

1. $xg - \frac{\operatorname{lt}(xg)}{\operatorname{lt} f} f \in \hat{\mathfrak{F}}^G_{\operatorname{lt}(xg)}$.
2. *There exist $g', f' \in G$ such that*

$$\operatorname{lt} g' \trianglelefteq \operatorname{lt} g, \quad \operatorname{lt} f' \trianglelefteq \operatorname{lt} f, \quad [g', f'] = \operatorname{lt}(g'f') \tag{3}$$

   and either

   (a) $\operatorname{lt} f \lhd [g, f]$ *or*

   (b) $\operatorname{lt} f = [g, f] \wedge \exists f'' \in G : f'' \trianglelefteq_G f \wedge [f'', f'] \lhd [g, f]$.

3. *There exist $g', f', p \in G$ such that*

$$\operatorname{lt} g' \trianglelefteq \operatorname{lt} g, \quad \operatorname{lt} f' \trianglelefteq \operatorname{lt} f, \quad [p, g'] \lhd [g, f], \quad [p, f'] \lhd [g, f] \tag{4}$$

   and either

   (a) $\operatorname{lt} f \lhd [g, f]$ *or*

   (b) $\operatorname{lt} f = [g, f] \wedge \exists f'' \in G : f'' \trianglelefteq_G f \wedge [f'', f'] \lhd [g, f]$.

4. *There exist $g', h, h' \in G$, $y \in X \setminus Y_{\operatorname{lt} h}$ such that*

$$\operatorname{lt} g' \trianglelefteq \operatorname{lt} g, \quad \operatorname{lt} h' \trianglelefteq \operatorname{lt} h, \quad [g', h'] \lhd \operatorname{lt}(xg) = \operatorname{lt}(yh), \quad h \blacktriangleleft g. \tag{5}$$

Then G is an $\mathcal{M}$-involutive basis of $I = \operatorname{Id}(G)$.

Proof. Since for all $g \in G$ and $x \in X \setminus Y_{\operatorname{lt} g}$ the monomial $\operatorname{lt}(xg)$ is contained in the involutive cone of $\operatorname{lt} f$ for some $f \in G$, the set $\operatorname{lt} G$ is $\mathcal{M}$-complete. Hence, it remains to show that G is a Gröbner basis of I. This is equivalent to show $p \in \mathfrak{F}^G_{\operatorname{lt} p}$ for all $p \in I \setminus \{0\}$. Suppose there exists $p \in I \setminus \{0\}$ with $p \notin \mathfrak{F}^G_{\operatorname{lt} p}$. Let $t \in T$ be the minimal (w.r.t. $\prec$) term such that there exists $p \in I$ satisfying $p \in \mathfrak{F}^G_t \setminus \hat{\mathfrak{F}}^G_t$ and $\operatorname{lt} p \prec t$. We call $L = ((h_i, g_i))_{i=1,\ldots,k}$ a t-representation if $h_i \in K[X] \setminus \{0\}$, $g_i \in G$, $\operatorname{lt}(h_i g_i) \preceq t$, and $\operatorname{lt} g_i \neq \operatorname{lt} g_j$ for all $i, j \in \{1, \ldots, k\}$ with $i \neq j$. Let $\Sigma(L) := \sum_{i=1}^k h_i g_i$ and $\Gamma(L) := \{g_i \,|\, \operatorname{lt}(h_i g_i) = t,\, t \notin \mathcal{M}_{\operatorname{lt} g_i},\, 1 \leq i \leq k\}$. We also say that L is a t-representation of p if $p = \Sigma(L)$. If L is a t-representation, $\Sigma(L) \in \mathfrak{F}^G_t \setminus \hat{\mathfrak{F}}^G_t$, and $\operatorname{lt} \Sigma(L) \prec t$ then $\Gamma(L) \neq \emptyset$. Among all t-representations choose $L = ((h_i, g_i))_{i=1,\ldots,k}$ such that $p := \Sigma(L) \in \mathfrak{F}_t^G \setminus \hat{\mathfrak{F}}_t^G$, $\operatorname{lt} p \prec t$, and $\max_{\blacktriangleleft} \Gamma(L)$ is minimal with respect to $\blacktriangleleft$.

So, w.l.o.g. let g_1 be the maximal element of $\Gamma(L)$ with respect to $\blacktriangleleft$. From the definition of $\Gamma(L)$ it follows that there exists $x \in X \setminus Y_{\operatorname{lt} g_1}$ such that x divides $\operatorname{lt} h_1$. By $\mathcal{M}$-completeness there exists $f \in G$ such that $\operatorname{lt}(xg_1) \in \mathcal{M}_{\operatorname{lt}(f)}$. The polynomial $g = g_1$, its non-multiplicative variable x, and the polynomial f must satisfy one of the assumptions 1–4. We are going to show that each of these assumptions implies $\operatorname{spol}(g_1, f) \in \hat{\mathfrak{F}}^G_{\operatorname{lt}(xg_1)}$. For the first assumption this is obvious. For conditions 2 and 3 we apply Lemma 3.4 and 3.5, respectively, in order to show $S(g_1, f)$. Finally, if assumption 4 applies to $g = g_1$ and x then we must have $S(h, f)$ for the element h from condition 4 since by construction of L we conclude $\operatorname{spol}(h, f) = yh - \frac{\operatorname{lt}(yh)}{\operatorname{lt} f} f \in \mathfrak{F}^G_{\operatorname{lt}(yh)}$. Application of Lemma 3.6 shows $S(g_1, f)$.

It follows $\operatorname{lt}(h_1)g_1 = \frac{\operatorname{lt}(h_1 g_1)}{\operatorname{lt} f} f + \hat{h}$ for a suitable polynomial $\hat{h} \in \hat{\mathfrak{F}}_t^G$. Substituting the left hand side of the above equation in the sum $\sum_{i=1}^k h_i g_i$ by the right hand side yields a new t-representation $L' = ((h'_i, g'_i))_{i=1,\ldots,k'}$ of p.

Moreover, $\Gamma(L') \subseteq (\Gamma(L) \setminus \{g_1\}) \cup \{f\}$. Neither $t \in \mathcal{M}_{\operatorname{lt} f}$ nor $f \blacktriangleleft g_1$ can hold, since then L' would contradict the minimality assumptions on L.

If $t \notin \mathcal{M}_{\operatorname{lt} f}$ and $g_1 \blacktriangleleft f$ we can assume, w.l.o.g., $g'_1 = f$ and repeat the above arguments. For $x' \in X \setminus Y_{\operatorname{lt} g'_1}$ such that $x' \trianglelefteq \operatorname{lt} h'_1$ there exist $f' \in G$ and $\hat{h}' \in \hat{\mathfrak{F}}_t^G$ satisfying $\operatorname{lt}(x'g'_1) \in \mathcal{M}_{\operatorname{lt} f'}$ and $\operatorname{lt}(h'_1)g'_1 = \frac{\operatorname{lt}(h'_1 g'_1)}{\operatorname{lt} f'} f' + \hat{h}'$. Hence, again we can construct a representation L'' of p where now f' instead of g'_1 appears in the set $\Gamma(L'')$.

Iteration of the above process will eventually terminate with a t-representation L^* of p, which contradicts the minimality assumptions on L since the sequence $\operatorname{lt} g_1, \operatorname{lt} f, \operatorname{lt} f', \ldots$ is decreasing with respect to $\sqsubset$ according to the admissibility of $\mathcal{M}$ and finite because there are only finitely many elements in G whose leading term divides t. In summary, the supposition of the existence of $p \in I$ satisfying $p \neq 0$ and $p \notin \mathfrak{F}^G_{\operatorname{lt} p}$ must have been wrong and the assertion of the theorem follows. □

Remark 3.2 *We introduced the additional order $\blacktriangleleft$ for use in condition 4 in order to achieve more flexibility in view of an application of the Theorem to the completion procedure. Of course, one could simply use $g \blacktriangleleft g' :\Longleftrightarrow \operatorname{lt} g \sqsubset \operatorname{lt} g'$ or $g \blacktriangleleft g' :\Longleftrightarrow \operatorname{lt} g \prec \operatorname{lt} g'$. But having in mind not only the involutive basis check but also the involutive basis completion algorithm, it is preferable to use the 'age' or 'index relation' for $\blacktriangleleft$, i. e., $g_i \blacktriangleleft g_j :\Longleftrightarrow i < j$, where the elements of G are enumerated according to insertion time in G.*

The freedom to choose $\blacktriangleleft$ allows to circumvent the following situation. During a completion process it may happen that a non-multiplicative prolongation xg is explicitly reduced because its reduction preventing basis polynomial h is not yet part of the basis at this time. A good criterion could and should avoid this situation by preventing the reduction of yh instead. This behaviour is ensured by using the age relation as $\blacktriangleleft$ in a criterion derived from condition 4.

Obviously, the theorem still remains valid if the linear order $\blacktriangleleft$ is replaced by a family $(\blacktriangleleft_t)_{t \in T}$ of linear orders on G and the condition $h \blacktriangleleft_{\operatorname{lt}(xg)} g$ is used in *assumption 4. In our implementation we do not exploit this fact so far. But a possible improvement based on this observation would be to deviate from the age relation by making elements h small with respect to $\blacktriangleleft_{\mathrm{lt}\,(yh)}$ in case the reduction of the non-multiplicative prolongation yh can be avoided according to one of the other criteria 2 or 3.*

Remark 3.3 *The statements of Theorem 3.1 and the corresponding Lemmata are not only valid for partial divisions $\mathcal{M}$ which are admissible on $(\mathrm{lt}\, G, \sqsubset)$ but an analogous statement including conditions 2–4 holds also for arbitrary continuous involutive division in the sense of [GB98].*

This is obvious for Lemmata 3.4–3.6 none of them depends on the partial division $\mathcal{M}$.

There are two critical points in the proof of Theorem 3.1 where replacing the admissibility of $\mathcal{M}$ on $\mathrm{lt}\, G$ by the weaker condition $u\,\langle Y_u\rangle \cap v\,\langle Y_v\rangle = \emptyset$ for all $u, v \in \mathrm{lt}\, G$ turns out to be insufficient. The first place is the deduction of $\mathcal{M}$-completeness from $\mathrm{lt}\,(xg) \in \bigcup_{h\in G} \mathcal{M}_{\mathrm{lt}\, h}$ for all $x \in X$ and $g \in G$. But this statement remains true for arbitrary continuous involutive divisions.

The second critical place is the proof of the termination of the iteration process transforming the representation $\sum_{i=1}^{k} h_i g_i$ of p into a representation where the largest summand $h_1 g_1$ is replaced by $\frac{\mathrm{lt}\,(h_1 g_1)}{\mathrm{lt}\, f} f + \hat{h}$, where $\hat{h} \in \hat{\mathfrak{F}}_t^G$, $f \in G$, and $\mathrm{lt}\, f$ is the involutive divisor of $\mathrm{lt}\,(h_1 g_1)$. Obviously, this process terminates if for each $t \in T$ and each $U \subseteq T$ any sequence $(y_1, u_1), (y_2, u_2), \ldots$ of pairs from $X \times U$ satisfying $y_i u_i \trianglelefteq t$ and $y_i u_i \in \mathcal{M}_{u_{i+1}} \setminus \mathcal{M}_{u_i}$ for all $i = 1, 2, \ldots$ is finite. Again, this condition holds for all continuous involutive divisions.

Lemma 3.4 *Let $G \subseteq \mathbb{K}[X]$ be a set of non-zero monic polynomials with distinct leading terms. Let $g, f \in G$. For each $s \prec [g, f]$ and each $h \in \mathrm{Id}(G) \setminus \{0\}$ assume $h \in \mathfrak{F}_s^G \implies h \in \mathfrak{F}_{\mathrm{lt}\, h}^G$. Furthermore, assume condition 2 of Theorem 3.1. Then $S(g, f)$ holds.*

PROOF. Let $g, f, g', f' \in G$ be such that (3) holds. From $[g, g'] \prec [g, f]$ it follows $S(g, g')$. In addition $S(f', f)$ by $[f, f'] \prec [g, f]$ in subcase 2a and $S(f', f'')$ due to $[f', f''] \prec [g, f]$ and $S(f'', f)$ because $f'' \trianglelefteq_G f$ in subcase 2b. Moreover, $S(g', f')$ according to Buchberger's coprime criterion. By repeated application of Lemma 2.5 we conclude $S(g, f)$. □

Lemma 3.5 *Let $G \subseteq \mathbb{K}[X]$ be a set of non-zero monic polynomials with distinct leading terms. Let $g, f \in G$. For each $s \prec [g, f]$ and each $h \in \mathrm{Id}(G) \setminus \{0\}$ assume $h \in \mathfrak{F}_s^G \implies h \in \mathfrak{F}_{\mathrm{lt}\, h}^G$. Furthermore, assume condition 3 of Theorem 3.1. Then $S(g, f)$ holds.*

PROOF. Let $g, f, g', f', p \in G$ be such that (4) holds. From $[g, g'], [g', p], [p, f'] \prec [g, f]$ follows $S(g, g')$, $S(g', p)$, and $S(p, f')$. While we deduce $S(f', f)$ from $[f', f] \prec [g, f]$ in subcase 3a we obtain $S(f', f'')$ from $[f', f''] \prec [g, f]$ and $S(f'', f)$ by the assumption $f'' \trianglelefteq_G f$ in subcase 3b. Finally, repeated application of Lemma 2.5 yields $S(g, f)$. □

Lemma 3.6 *Let $G \subseteq \mathbb{K}[X]$ be a set of non-zero monic polynomials with distinct leading terms. Let $t \in T$ be a term and for each $s \prec t$ and each $h \in \mathrm{Id}(G) \setminus \{0\}$ assume $h \in \mathfrak{F}_s^G \implies h \in \mathfrak{F}_{\mathrm{lt}\, h}^G$. Let $g, g', h, h' \in G$ be such that $\mathrm{lt}\, g' \trianglelefteq \mathrm{lt}\, g$, $\mathrm{lt}\, h' \trianglelefteq \mathrm{lt}\, h$, and $[g', h'] \lhd [g, f] = [h, f] = t$.*

If $S(h, f)$ holds then $S(g, f)$ holds, too.

Proof. From $[g, g'], [g', h'], [h', h] \prec t$ follows $S(g, g')$, $S(g', h')$, and $S(h', h)$. By Lemma 2.5, we deduce $S(g, h)$. Moreover, $S(h, f)$ by assumption. We conclude $S(g, f)$ by Lemma 2.5. □

Remark 3.7 *Lemmata 3.5, and 3.6 and their proofs remain valid almost literally for left ideals generated by G of algebras of solvable type. Lemma 3.4 is based upon Buchberger's coprime criterion and, therefore, cannot be transfered.*

Hence, after removing Condition 2 also Theorem 3.1 including its proof holds in the more general situation of left ideals generated by G of algebras of solvable type. Only a few standard adaptions, cf. [AL88] or [KRW90], are necessary in the proof.

4 Check of the Involutive Basis Property

In this section we will present an algorithm which checks the $\mathcal{M}$-involutive basis property of a given finite set G with respect to a given partial division $\mathcal{M}$. This algorithm is based upon Theorem 3.1. Conditions 2–4 of the theorem are used in order to create criteria for omitting the reduction of certain non-multiplicative prolongations. In the presented algorithms we use the following assumptions and notations. Let $G = \{g_1, \ldots, g_r\} \subseteq \mathbb{K}[X]$ with $\mathrm{lt}\, g \neq \mathrm{lt}\, g'$ for all $g, g' \in G$ and let $\mathcal{M} = (t \langle Y_t \rangle)_{t \in T}$ be an admissible partial division on $\mathrm{lt}\, G$. Let $H \subseteq G$ be minimal with the property $\langle \mathrm{lt}\, H \rangle = \langle \mathrm{lt}\, G \rangle$. Let $\mathrm{anc}, \mathrm{wanc} : G \to G$ be two functions such that $\mathrm{anc}\, g \trianglelefteq_G g$, $\mathrm{lt}(\mathrm{wanc}\, g) \trianglelefteq \mathrm{lt}(\mathrm{anc}\, g) \trianglelefteq \mathrm{lt}\, g$, and $\mathrm{wanc}\, g \in H$ for all $g \in G$. Both functions are combined to define a family of functions $\mathrm{anc}_s : G \to G$ by

$$\mathrm{anc}_s\, g := \begin{cases} \mathrm{wanc}\, g & \text{if } \mathrm{lt}\,(\mathrm{anc}\, g) \lhd s \\ \mathrm{anc}\, g & \text{otherwise} \end{cases}$$

for all $s \in T$ and $g \in G$. By $\mathrm{anc}\, g$ and $\mathrm{wanc}\, g$ we abbreviate the notions 'ancestor' and 'weak ancestor' of g, respectively. Usually, s will be equal to $[g, f]$ when calling $\mathrm{anc}_s\, f$ or $\mathrm{anc}_s\, g$ during the investigation of a non-multiplicative prolongation xg which is involutively top-reducible by $f \in G$.

Under the made assumption that the leading term of the weak ancestor divides the leading term of the ancestor, the objects $\mathrm{anc}_s\, f$ and $\mathrm{anc}_s\, g$ can always serve as f' and g' in Conditions 2–4 of Theorem 3.1. The above definition of anc_s even incorporates a generalisation of Theorem 3.1 whose justification is covered by the forthcoming Remark 4.1.

Let idx be a function which assigns to each element $g_i \in G$ its index i. The function $\mathrm{NF}_{\mathcal{M}}$ assigns to each polynomial $h \in \mathbb{K}[X]$ an $\mathcal{M}$-involutive normal form of h modulo G. $\mathrm{NF}_{\mathcal{M}}(0, G) = 0$ and h' is an $\mathcal{M}$-involutive normal form of $h \neq 0$ modulo G if $h \to^*_{G,\mathcal{M}} h'$ and $h' = 0$ or $\operatorname{lt} h' \notin \bigcup_{t \in \operatorname{lt} G} \mathcal{M}_t$. The symbol $\to^*_{G,\mathcal{M}}$ denotes the reflexive, transitive closure of the involutive reduction relation which is defined for $h \neq 0$ by $h \to_{G,\mathcal{M}} h'$ iff

$$\exists g \in G, t \in \langle Y_{\operatorname{lt} g} \rangle, c \in \mathbb{K} \setminus \{0\} : h' = h + ctg \wedge \operatorname{lt}(tg) \in \operatorname{supp} h \setminus \operatorname{supp} h'.$$

If we have $h \to^*_{G,\mathcal{M}} h'$ and $\operatorname{lt} h \in \mathcal{M}_{\operatorname{lt} g} \setminus \operatorname{supp} h'$ for $h \in \mathbb{K}[X] \setminus \{0\}$ and $g \in G$ then we say that h **is involutively top-reducible by** g (with respect to $\mathcal{M}$) and h **is involutively top-reduced using** g during the $\mathcal{M}$-reduction of h to h'.

We write NF, $\to_G$, and $\to^*_G$ as abbreviations for $\mathrm{NF}_{\mathcal{O}}$, $\to_{G,\mathcal{O}}$, and $\to^*_{G,\mathcal{O}}$, respectively, where $\mathcal{O} = (t \langle X \rangle)_{t \in T}$ denotes the ordinary division.

Algorithm 1 INVOLUTIVEBASISCHECK

Call: $h = \text{INVOLUTIVEBASISCHECK}(G, \mathcal{M})$

Input: $G \subset K[X] \setminus \{0\} \cdots$ finite set of polynomials with pairwise distinct leading terms

$\mathcal{M} = (t \langle Y_t \rangle)_{t \in \operatorname{lt} G} \cdots$ admissible partial division on $\operatorname{lt} G$

Output: If G is an $\mathcal{M}$-involutive basis then $h = 0$, otherwise $h \in \operatorname{Id}(G)$ and $\operatorname{lt} h \notin \bigcup_{t \in \operatorname{lt} G} \mathcal{M}_t$.

$Q := \{ g \in G \mid \exists g' \in G \setminus \{g\} : \operatorname{lt} g \in \mathcal{M}_{\operatorname{lt}(g')} \}$
$G := G \setminus Q$
$C := \{ (x, g) \mid g \in G \wedge x \in X \setminus Y_{\operatorname{lt} g} \} \cup \{ (1, g) \mid g \in Q \}$
<u>while</u> $C \neq \emptyset$ <u>do</u>
  Choose smallest (t, g) from C; $C := C \setminus \{(t, g)\}$
  <u>if</u> not USELESS(t, g) <u>then</u>
    $h := \mathrm{NF}_{\mathcal{M}}(tg, G)$
    <u>if</u> $h \neq 0$ <u>then</u> <u>return</u> h
<u>return</u> 0

The subroutine USELESS is presented as Algorithm 2 where non-specified objects are inherited from Algorithm 1. It checks if a prolongation can be omitted according to Conditions 2–4 of Theorem 3.1 which we encoded in the following predicates.

$$\begin{aligned}
C_1(g, f, s) :&\Longleftrightarrow [\operatorname{anc}_s g, \operatorname{anc}_s f] \neq s \\
C_2(g, f, s) :&\Longleftrightarrow \operatorname{lt}(\operatorname{anc}_s g) \cdot \operatorname{lt}(\operatorname{anc}_s f) = s \\
C_3(g, f, s, H) :&\Longleftrightarrow \exists h \in H : \operatorname{lt} h \lhd s \wedge [h, \operatorname{anc}_s f] \neq s \wedge [h, \operatorname{anc}_s g] \neq s \\
C_4(g, s, G, \mathcal{M}) :&\Longleftrightarrow \exists h \in G, y \in X \setminus Y_{\operatorname{lt} h} : [\operatorname{anc}_s g, \operatorname{anc}_s h] \lhd s = \operatorname{lt}(yh) \\
&\qquad \wedge \operatorname{idx}(h) < \operatorname{idx}(g)
\end{aligned}$$

Remark 4.1 *Note, that the correctness of Algorithm 1 essentially follows from Theorem 3.1. However, the algorithm works also for inputs G which are not $\mathcal{M}$-minimal. Let $Q \subseteq G$ be as defined in Algorithm 1. It is easy to see that G is an $\mathcal{M}$-involutive basis of* $\operatorname{Id}(G)$ *if and only if $G \setminus Q$ satisfies the assumptions of Theorem 3.1 and $\mathrm{NF}_{\mathcal{M}}(q, G \setminus Q) = 0$ for all $q \in Q$. It is easy to observe that*

Algorithm 2 USELESS

Call: $b = \text{USELESS}(t, g)$

Input: $t = 1 \vee t \in X \setminus Y_{\operatorname{lt} g}$
$g \in G$

Output: $b = \underline{\mathsf{true}}$ if tg need not be reduced and
$b = \underline{\mathsf{false}}$ otherwise

1: Let $H \subseteq G$ be minimal with the property $\langle \operatorname{lt} H \rangle = \langle \operatorname{lt} G \rangle$.
2: $s := \operatorname{lt}(tg)$
3: $\underline{\mathsf{if}}$ $\nexists f \in G : s \in \mathcal{M}_{\operatorname{lt}(f)}$ $\underline{\mathsf{then}}$ $\underline{\mathsf{return}}$ $\underline{\mathsf{false}}$
4: Let f be such that $s \in \mathcal{M}_{\operatorname{lt}(f)}$.
5: $\underline{\mathsf{return}}$ $C_1(g, f, s) \vee C_2(g, f, s) \vee C_3(g, f, s, H) \vee C_4(g, s, G, \mathcal{M})$

the criteria implemented in Algorithm 2 remain valid also for prolongations of type $(1, g)$*.*

Algorithm 2 does not fully exploit Theorem 3.1. Instead of using a deterministic function anc_s *one could test all possible pairs* $(g', f') \in G \times G$ *fitting to the specification of* $\operatorname{anc}_s g$ *or* $\operatorname{anc}_s f$*, respectively. However, it seems that the overhead caused by the tests is larger than the effect gained by the criterion. Nevertheless, this question remains open for further investigation.*

5 Involutive Criteria vs. Buchberger's Criteria

With $s = [g, f]$ the expression $C_1(g, f, s)$ reflects a particular case of Condition 3 of Theorem 3.1, namely, when $p = \operatorname{anc}_s g$ or $p = \operatorname{anc}_s f$. It follows the ideas of [GB98]. While Gerdt and Blinkov refer to elements $f', g' \in G$ such that $\operatorname{lt} f' \trianglelefteq \operatorname{lt} f$, $\operatorname{lt} g' \trianglelefteq \operatorname{lt} g$ and $\operatorname{NF}_{\mathcal{M}}(\frac{\operatorname{lt} f}{\operatorname{lt} f'} \cdot f') = \operatorname{NF}_{\mathcal{M}}(\frac{\operatorname{lt} g}{\operatorname{lt} g'} \cdot g') = 0$ we use $f' = \operatorname{anc}_s f$ and $g' = \operatorname{anc}_s g$. Therefore, f' and g' need to satisfy only the weaker assumptions $\operatorname{lt} f' \trianglelefteq \operatorname{lt} f$ and $\operatorname{lt} g' \trianglelefteq \operatorname{lt} g$ in most cases. In the exceptional case $\operatorname{lt} f = \operatorname{lt}(xg)$ the additional assumption $f' \trianglelefteq_G f$ is made. Even this additional condition is still weaker than $\operatorname{NF}_{\mathcal{M}}(\frac{\operatorname{lt} f}{\operatorname{lt} f'} \cdot f') = 0$ unless the non-multiplicative prolongations are processed by increasing leading term, i. e., if the normal strategy is used, where both conditions become equivalent.

In order to compare the involutive criteria to Buchberger's criteria applied in the Gröbner basis algorithm we need to explain the meaning of the explicit reduction of an S-polynomial in the involutive algorithm. Consider two elements $g', f' \in G$. By convention, we say that the S-polynomial $\operatorname{spol}(g', f')$ is **explicitly reduced** during the involutive algorithm if there are polynomials $g, f \in G$ and a variable $x \in X \setminus Y_{\operatorname{lt} g}$ such that $g' \trianglelefteq_G g$, $f' \trianglelefteq_G f$, $\operatorname{lt}(xg) = [g', f'] \in \mathcal{M}_{\operatorname{lt}(f)}$ and the reduction of the prolongation xg could not be omitted by one of our criteria. Note, the reduction step cancelling the leading term $\operatorname{lt}(xg)$ will be performed using f in this situation. The above convention shows that C_1 reflects the fact that the explicit reduction of non-trivial multiples of S-polynomials can be avoided also in the involutive algorithm. Consider two elements $g', f' \in G$ such that $\operatorname{spol}(g', f')$ can be skipped during Buchberger's algorithm using the coprime criterion, i. e., $[g', f'] = \mathrm{lt}\,(g'f')$. If there exist $g, f \in G$ and a variable $x \in X \setminus Y_{\mathrm{lt}\,g}$ such that $g' \trianglelefteq_G g$, $f' \trianglelefteq_G f$, $\mathrm{lt}(xg) = [g', f'] \in \mathcal{M}_{\mathrm{lt}\,f}$ then the reduction of the non-multiplicative prolongation xg is omitted by criterion C_2. If such objects $g, f \in G$ and $x \in X \setminus Y_{\mathrm{lt}\,g}$ do not exist then the explicit reduction of $\mathrm{spol}(g', f')$ is impossible by convention. The correctness of the use of C_2 follows from Condition 2 of Theorem 3.1. Now, consider three basis elements $f', g', h' \in G$ such that $\mathrm{lt}\,h' \trianglelefteq [g', f']$. In this case at most two of the three S-polynomials $\mathrm{spol}(g', f'), \mathrm{spol}(g', h')$ and $\mathrm{spol}(f', h')$ need to be reduced in Buchberger's algorithm according to the chain criterion. If there is no $p \in G$ such that $[g', f'] \in \mathcal{M}_{\mathrm{lt}\,p}$ and either $f' \trianglelefteq_G p$ or $g' \trianglelefteq_G p$ then $\mathrm{spol}(g', f')$ will not be reduced explicitly by the involutive algorithm. W.l.o.g it suffices to consider in addition the case that there exists $f \in G$ such that $[g', f'] \in \mathcal{M}_{\mathrm{lt}\,f}$ and $f' \trianglelefteq_G f$. If $[h', g'] = [f', g']$ then the reduction of $\mathrm{spol}(h', g')$ is automatically omitted by the involutive algorithm, even without application of criteria. So consider the final case of $[h', g'] \triangleleft [f', g']$. If also $[h', f'] \triangleleft [f', g']$ then criterion C_3 applies in order to cancel any possible non-multiplicative prolongations xg of some $g \in G$ such that $g' \trianglelefteq_G g$ and $\mathrm{lt}\,(xg) = [f', g']$. Hence, $\mathrm{spol}(g', f')$ is not reduced explicitly. Finally, assume $[h', f'] = [f', g']$. If there exist elements $g, h \in G$ and non-multiplicative prolongations xg and yh such that $g' \trianglelefteq_G g$, $h' \trianglelefteq_G h$, and $\mathrm{lt}\,(xg) = \mathrm{lt}\,(yh) = [f', g']$ then one of these prolongations is skipped by criterion C_4, i. e., either $\mathrm{spol}(g', f')$ or $\mathrm{spol}(h', f')$ is not reduced explicitly. But if not both prolongations xg and yh of the above type exist then the reduction of at least one of the S-polynomials $\mathrm{spol}(g', f')$ and $\mathrm{spol}(h', f')$ cannot be reduced explicitly by convention. In summary, Algorithm 1 will never reduce more than two out of the three S-polynomials $\mathrm{spol}(g', f'), \mathrm{spol}(g', h')$ and $\mathrm{spol}(f', h')$ explicitly. The theoretical justification of criteria C_3 and C_4 consists in Conditions 3 and 4 of Theorem 3.1, respectively. In summary, we observed whenever the reduction of an S-polynomial can be avoided in Buchberger's algorithm our Algorithm 1 will omit the explicit reduction of the S-polynomial of two elements from H, too.

6 Involutive Basis Completion Algorithm

Until now we discussed the check algorithm for the involutive basis property. The computation of an involutive basis from an arbitrary given finite generating set can be done by application of a completion algorithm. Each time the check algorithm fails for the actual basis, the basis is enlarged by the failure causing element and the check algorithm is repeated until it ends successfully. But, in general, some of the prolongations tg treated previously need re-reduction due to the necessary changes of the partial division caused by the basis enlargements. This, however, involves reductions of prolongations that have already been explicitly reduced in a previous run of the check algorithm and it is a natural wish to avoid such repeated reductions as much as possible.

Total avoidance of repeated reductions is possible if an order $\sqsubset$ is fixed during the whole computation, i. e., each subset U of terms is ordered by the restriction of a fixed order $\sqsubset$ of T to U, and after each enlargement of the basis, a partial division is chosen which is admissible on $(U, \sqsubset)$, cf. [Ape98a]. Studying why multiple reduction of the same prolongation can be avoided one observes that Apel's proof relies on Buchberger's chain criterion.

Before we are going to present the INVOLUTIVEBASIS algorithm, let us deal with the question of avoiding repeated reductions of a prolongation. From Theorem 2.12, Condition (iv), we learn that the reduction of a prolongation (x, g), $g \in G$, $x \in X \setminus Y_{\mathrm{lt}\, g}$ during the involutive basis check serves for the verification of two conditions, namely, first the existence of $f \in G$ such that $\mathrm{lt}\,(xg) \in \mathcal{M}_{\mathrm{lt}\, f}$ and second the validity of $S(g, f)$.

Let G be an intermediate basis and $\mathcal{M}$ the corresponding $\mathrm{lt}(G)$-admissible partial division. Suppose in the $\mathcal{M}$-involutive basis check we encounter a prolongation (t, g), with $g \in G' \subset G$, $t \in X \cup \{1\}$ which has already been explicitly reduced using $h \in G'$, i. e., $\mathrm{lt}\,(xg) \in \mathcal{M}'_{\mathrm{lt}\, h}$, where G' was the basis at the time when this reduction took place (a previous involutive basis check) and $\mathcal{M}'$ the corresponding $\mathrm{lt}(G')$-admissible partial division. Furthermore suppose that now we find $f \in G$ with $\mathrm{lt}(tg) \in \mathcal{M}_{\mathrm{lt}\, f}$. This is exactly the situation where tg will repeatedly be reduced if the reduction cannot be avoided by means of criteria. The $\mathcal{M}$-involutive basis check requires the verification of $S^G(g, f)$. Provided $S^G(h, f)$ holds we can deduce $S^G(g, f)$ from $S^G(g, h)$ and Buchberger's chain criterion. Since the property $S^{G'}(g, h)$ is independent of the partial division and preserved under enlargement of the basis, we can conclude $S^G(g, h)$ from the explicit reduction of tg in the $\mathcal{M}'$-involutive basis check. If $h = f$ or $h = \mathrm{anc}\, f$, the relation $S(g, f)$ follows immediately. Let us describe this case by the predicate

$$C_0(t, g, G) :\Longleftrightarrow \exists f \in G : \mathrm{lt}(tg) \in \mathcal{M}_{\mathrm{lt}(f)} \wedge (R(t, g, f) \vee R(t, g, \mathrm{anc}\, f))$$

where $R(t, g, f)$ expresses that (t, g), $t \in X \cup \{1\}$ and $g \in G$, was reduced explicitly and top-reduced using $f \in G$ during the reduction process. It defines an effective version of Condition 1 of Theorem 3.1. Let $s := [g, f] = \mathrm{lt}\,(tg)$. Also in cases where $[\mathrm{anc}_s\, h, \mathrm{anc}_s\, f] \lhd s$, we easily conclude $S(g, f)$. In fact, this situation can effectively be tested by a slightly generalised version of our criterion C_3 which takes advantage of the knowledge of $R(t, g, h)$. Even the case $[\mathrm{anc}_s\, h, \mathrm{anc}_s\, f] = s = \mathrm{lt}\,(\mathrm{anc}_s\, h) \cdot \mathrm{lt}\,(\mathrm{anc}_s\, f)$ can be handled by a generalised version of C_3 incorporating C_2. In the remaining case, we have to ensure that a (perhaps multiple) non-multiplicative prolongation of h is either explicitly reduced starting with f or the reduction is omitted by another reason than application of a Buchberger like criterion involving g.

Recall the proposals of [Ape98a], i. e., to fix the order $\sqsubset$ and to apply Buchberger's criterion only in the restricted sense that each non-multiplicative prolongation is reduced only once during the completion process. In this situation we easily deduce $\mathrm{lt}\, f \sqsubset \mathrm{lt}\, h \sqsubset \mathrm{lt}\, g$ and, further, that $\mathrm{lt}\, g$ can never be an involutive divisor of $[h, f]$. Hence, the treatment of the S-pair (h, f) is definitely not omitted by reference to g.

Our discussion makes clear that our criteria, in particular C_0 and (a generalised version of) C_3, will avoid multiple reductions of a prolongation in a huge number of cases by exploiting the knowledge of previously performed reductions.

Another aspect of a 'good' dynamical property of the criteria has already been given in Remark 3.2. We propose to use the index function as stated in the definition of C_4 in order to let the history of reductions decide which of several potential prolongations need not be reduced.

So in contrast to the multiple reduction avoidance rule from [Ape98a] we still do not lose the freedom of changing $\sqsubset$ during the completion process.

Algorithm 3 INVOLUTIVEBASIS

Call: $G = \text{INVOLUTIVEBASIS}(F)$

Input: $F \subset K[X] \setminus \{0\} \cdots$ finite set of polynomials with pairwise distinct leading terms

Output: $G \cdots$ involutive basis of the ideal of F in $K[X]$

1: $G := F$
2: $\mathcal{M} := (t\,\langle Y_t \rangle)_{t\in \operatorname{lt}(G)} := \text{PARTIALDIVISION}(\operatorname{lt} G)$
3: $Q := \left\{ g \in G \,\middle|\, \exists f \in G \setminus \{g\} : \operatorname{lt} g \in \mathcal{M}_{\operatorname{lt}(f)} \right\}$
4: $C := \left\{ (x, g) \,|\, g \in G \setminus Q \wedge x \in X \setminus Y_{\operatorname{lt} g} \right\} \cup \left\{ (1, q) \,|\, q \in Q \right\}$
5: <u>while</u> $C \neq \emptyset$ <u>do</u>
6: Choose (t, g) from C; $C := C \setminus \{(t, g)\}$
7: <u>if</u> not $(C_0(t, g, G) \vee \text{USELESS}(t, g))$ <u>then</u>
8: $h := \mathrm{NF}_{\mathcal{M}}(tg, G \setminus Q)$
9: <u>if</u> $h \neq 0$ <u>then</u>
10: $G := G \cup \{h\}$
11: $\mathcal{M} := (t\,\langle Y_t \rangle)_{t\in \operatorname{lt}(G)} := \text{PARTIALDIVISION}(\operatorname{lt} G)$
12: $Q := \left\{ g \in G \,\middle|\, \exists f \in G \setminus \{g\} : \operatorname{lt} g \in \mathcal{M}_{\operatorname{lt}(f)} \right\}$
13: $C := \left\{ (x, g) \,|\, g \in G \setminus Q \wedge x \in X \setminus Y_{\operatorname{lt} g} \right\} \cup \left\{ (1, q) \,|\, q \in Q \right\}$
14: <u>return</u> G

The function call PARTIALDIVISION$(\operatorname{lt} G)$ in lines 2 and 11 computes a partial division which is admissible on the monomial set $\operatorname{lt} G$ and refines the Thomas division on $\operatorname{lt} G$.

The correctness of Algorithm 3 follows from Theorem 3.1 and Remark 4.1.

Remark 6.1 *The functions* anc *and* wanc *reflect parts of the history of the algorithm. They are initialised by* $\operatorname{anc} g := g$ *and* $\operatorname{wanc} g := h$ *where* $h \in G$ *is such that* $\operatorname{lt} h$ *is a* $\trianglelefteq$*-minimal divisor of* $\operatorname{lt} g$*. The values* $\operatorname{anc} g$ *and* $\operatorname{wanc} g$ *are updated during the run of the algorithm in the following situations.*

1. *Assume that a pair* $(1, q)$ *was chosen in line 6 and* q *was involutively top-reduced using some polynomial* $f \in G$ *in line 8. Then for all* $g \in G$ *with* $\operatorname{anc} g = q$ *set* $\operatorname{anc} g := \operatorname{anc} f$ *and* $\operatorname{wanc} g := \operatorname{wanc} f$*.*

   Moreover, if $\operatorname{lt}(\operatorname{anc} f) \prec \operatorname{lt}(\operatorname{anc} q) \neq \operatorname{lt} q$*, set* $\operatorname{anc} q := \operatorname{anc} f$ *and* $\operatorname{wanc} q := \operatorname{wanc} f$*.*

2. *Assume that a pair* (x, g) *was chosen in line 6 and involutively top-reduced by some polynomial* $f \in G$ *with* $\operatorname{lt}(xg) = \operatorname{lt} f$ *in line 8. If* $\operatorname{anc} f = f$ *then for all* $h \in G$ *with* $\operatorname{anc} h = f$ *set* $\operatorname{anc} h := \operatorname{anc} g$ *and* $\operatorname{wanc} h := \operatorname{wanc} g$*. If* $\operatorname{lt}(\operatorname{anc} g) \prec \operatorname{lt}(\operatorname{anc} f) \neq \operatorname{lt} f$*, set* $\operatorname{anc} f := \operatorname{anc} g$ *and* $\operatorname{wanc} f := \operatorname{wanc} g$*.*

3. *Assume that the prolongation* tg *was involutively top-irreducible in line 8. Then its remainder* h *gets* $\operatorname{anc} h := \operatorname{anc} g$ *and* $\operatorname{wanc} h := \operatorname{wanc} g$*.*

4. *Assume that the prolongation tg was involutively top-reducible in line 8. If the remainder h is non-zero then assign* $\operatorname{anc} h := h$ *and* $\operatorname{wanc} h := f$ *where $f \in G \cup \{h\}$ is such that* $\operatorname{lt} f$ *is a $\trianglelefteq$-minimal divisor of* $\operatorname{lt} h$. *Note, if the normal strategy is used in Algorithm 3, it always holds $f = h$.*

The updates of anc *and* wanc *described in 1 and 2 analogously apply to Algorithm 1.*

The idx *function is updated so that each new element h in line 10 gets a bigger index than any of the elements in G in order to simulate the age of a polynomial.*

7 Selection Strategy vs. Termination

In [Ape98a] it was proved that Algorithm 3 without application of criteria will always terminate if a normal selection strategy is applied. Indeed, without the assumption of using a normal selection strategy there are non-terminating examples. Also the assumption of a fair selection strategy, i. e., no prolongation stays in C forever, is insufficient for ensuring termination of the criteria free algorithm from [Ape98a].

Let us give a simple example of how it can happen that the involutive basis algorithm (without criteria) does not terminate if one deviates from a normal strategy.

Example 7.1 *We use the lexicographical term order refining $u \succ v \succ w \succ x \succ y$. For the readers convenience we write the multiplicative variables in curly brackets behind each polynomial. The division refines the Thomas division in each iteration. Let the following 7 polynomials be given and consider Algorithm 3 without application of criteria and with a selection of the next prolongation as given below.*

$$g_1 = x\ \{x\}, \quad g_2 = y\ \{y\}, \quad g_3 = u^2\ \{u\}, \quad g_4 = v^2\ \{v\}, \quad g_5 = w^2\ \{w\},$$
$$g_6 = ux - wy\ \{w, x\}, \quad g_7 = vy - wx\ \{w, y\}$$

First we reduce the prolongation ug_1 by g_6 and obtain $g_8 := wy\ \{w, y\}$. Then we reduce vg_8 by wg_7 and obtain $g_9 := w^2x\ \{w, y\}$. Now y is the only multiplicative variable for g_8. Then we add $g_{10} := ug_9 - w^2g_7 = w^3y\ \{w, y\}$. All variables are now non-multiplicative for g_5. We go on by adding $g_{11} := vg_{10} - w^3g_6 = w^4x\ \{w, y\}$, $g_{12} := ug_{11} - w^4g_7 = w^5y\ \{w, y\}$, etc. Each time a polynomial g_{i+1} $(i > 7)$ is added to the basis, the variable w becomes non-multiplicative for g_i. Obviously, this process is infinite by adding the polynomials $g_{2i+6} = w^{2i-1}y$, $g_{2i+7} = w^{2i}x$ $(i > 0)$.

Note that in the previous example the reduction step $vg_8 - wg_7$ would not be performed in Algorithm 3, because $\operatorname{wanc} g_8 = \operatorname{wanc} g_7 = g_2 = y \lhd [g_8, g_7] = vwy$ and, hence, $C_1(g_8, g_7, vwy)$ is true.

This is the key-observation which led to Theorem 7.2. The criteria tested in line 7 make Algorithm 3 terminating even independent of the selection strategy used in line 6.

Theorem 7.2 *Algorithm 3 terminates for all inputs fulfilling its specification, independent of the selection strategy applied in line 6.*

Proof. Let us sketch the proof idea. We first show that there can be only finitely many explicit involutive top-reductions during any run of the algorithm because many of the potential top-reductions are avoided due to criterion C_1. Then, by the properties of a partial division which refines the Thomas division, there can be only finitely many top-irreducible prolongations.

By G^i and $\mathcal{M}^i$ we denote the value of G and $\mathcal{M}$, respectively, before the i-th iteration of the while loop starting in line 5 of Algorithm 3. Moreover, $G^\infty = \left\{h \,\middle|\, \exists i \in \mathbb{N} : h \in G^i\right\}$ denotes the set of all polynomials which eventually belong to the basis G. We have the sequence of inclusions $G^1 \subseteq G^2 \subseteq \cdots$ and the resulting sequence $\left\langle \operatorname{lt} G^1 \right\rangle \subseteq \left\langle \operatorname{lt} G^2 \right\rangle \subseteq \cdots$ must become stationary, let us say $\left\langle \operatorname{lt} G^k \right\rangle = \left\langle \operatorname{lt} G^i \right\rangle$ for all $i \geq k$. Note, that after each iteration the weak ancestors of all elements $h \in G^\infty$ satisfy $\operatorname{wanc} h \in G^k$. Until the k-th iteration this is obvious and later this follows easily since the leading term of any element of $G^\infty \setminus G^k$ has a proper divisor in $\operatorname{lt} G^k$. Hence, also after the k-iteration no element of $G^\infty \setminus G^k$ may become a weak ancestor according to the specification of wanc.

Let $G^* := \left\{h \in G^\infty \,\middle|\, \operatorname{lt} h \trianglelefteq \operatorname{LCM}(\operatorname{lt} G^k)\right\}$. Furthermore, let $X' := X \cup \{1\}$ and $R := \{h \in G^\infty \mid \exists t \in X',\, g \in G^* : tg \to^*_{G^\infty} h\}$. Note that for the definition of R we use the ordinary reduction relation with respect to the fix set G^∞.

Suppose there exist $l \in \mathbb{N}$ and $h \in G^\infty$ such that

$$G^{l+1} \setminus G^l = \{h\}\,,\; h \notin R, \text{ and } \operatorname{anc} h = h$$

at creation time of h. Choose l to be minimal with the above property.

First of all, we must have $l \geq k$ since $G^k \subseteq R$ by construction of R. In order to satisfy $\operatorname{anc} h = h$ and $h \notin G^k$, the polynomial h must result from a top-reduction of some prolongation, i.e., there exist $g, f \in G^l$ and $t \in X'$ such that $\operatorname{lt}(tg) \in \mathcal{M}^l_{\operatorname{lt} f}$ and $\left(tg - \frac{\operatorname{lm}(tg)}{\operatorname{lm} f} f\right) \to^*_{G^\infty} h$. Next, we deduce $g \notin G^*$ since otherwise it will follow $h \in R$ because of $tg \to^*_{G^\infty} h$. Hence, $s := \operatorname{lt}(tg) \ntrianglelefteq \operatorname{LCM}(\operatorname{lt} G^k)$.

If $\operatorname{anc} g = g$ then $g \in R$ by minimality of l. We must have $t \neq 1$ in this case since otherwise $g \to^*_{G^\infty} h$ leads to the contradiction $h \in R$. Hence, in any case we obtain $\operatorname{lt}(\operatorname{anc} g) \lhd s$ and, therefore, $\operatorname{anc}_s g = \operatorname{wanc} g \in G^k$.

The equality $\operatorname{lt}(\operatorname{anc} f) = \operatorname{lt} f = s$ is impossible since we would obtain $f \in R$ by minimality of l and, consequently, $h \in R$ because of $f \to^*_{G^\infty} h$ in this situation. Therefore, $\operatorname{lt}(\operatorname{anc} f) \lhd s$ and $\operatorname{anc}_s f = \operatorname{wanc} f \in G^k$.

In summary we proved $\operatorname{anc}_s g, \operatorname{anc}_s f \in G^k$ and $s \ntrianglelefteq \operatorname{LCM}(\operatorname{lt} G^k)$. Consequently, $[\operatorname{anc}_s g, \operatorname{anc}_s f] \lhd s$ and $C_1(g, f, s)$. But this means our algorithm would have omitted the reduction of the prolongation tg during the l-th iteration, a contradiction.

In conclusion, the supposition of the existence of $h \in G^\infty$ such that $\operatorname{anc} h = h$ and $h \notin R$ must have been wrong.

Since the elements of G^∞ have pairwise distinct leading terms the set G^* must be finite. Furthermore it follows that the number of polynomials h which can be obtained as the result of a single Gröbner reduction step of a fixed polynomial f modulo G^∞ is finite. Noetherianity of $\prec$ ensures that the number of polynomials h resulting from f by an arbitrary number of Gröbner reduction steps modulo G^∞ is still finite. Finally, finiteness of G^* and X implies finiteness of R.

Hence, there exists k' such that anc $h \neq h$ for all $h \in G^\infty \setminus G^{k'}$, i. e., all elements added to G after the k'-th iteration result from top-irreducible prolongations. But, now, the properties of an involutive division refining the Thomas division ensure $\mathrm{LCM}(\mathrm{lt}\, G^{k'}) = \mathrm{LCM}(\mathrm{lt}\, G^l)$ for all $l \geq k'$. Hence, only a finite number of elements is added to $G^{k'}$. Therefore, there exists $k'' \geq k'$ such that $G^{k''} = G^l$ for all $l \geq k''$. Since $G^{k''}$ possesses only a finite number of prolongations, there are only finitely many iterations left. Hence, the algorithm terminates. □

Remark 7.3 *Again, let us explain the connection to the method due to Gerdt and Blinkov. Our Algorithm 3 will work correctly and terminate for any continuous involutive division $\mathcal{L}$ as defined in [GB98] which refines the Thomas division in the following sense. If U is a set of terms and $u \in U$ has maximal degree in the variable $x \in X$ among all elements of U then x is multiplicative for u with respect to $\mathcal{L}$ and U, i. e., each 'layer' of $\mathcal{L}$ refines the Thomas division.*

8 Examples

In this section we give two detailed examples which demonstrate that our criteria C_3 and C_4 are not covered by the other criteria. It is clear that the application of criteria becomes more powerful the longer the polynomials are that would be involved in a reduction. Nevertheless, for the purpose of demonstration, we have chosen monomial examples. In both examples we use the Janet division which is an admissible partial division and defined as follows.

Definition 8.1 *Let $U \subseteq T$ be a finite set of power products. Define $Y_t = X$ for all $t \notin U$ and*

$$Y_t := \left\{ x_i \in X \,\middle|\, \nexists u \in U : \left(\deg_{x_i} u > \deg_{x_i} t \wedge \forall\, 1 \leq j < i : \deg_{x_j} u = \deg_{x_j} t \right) \right\}$$

*for all $t \in U$. The division $(t \langle Y_t \rangle)_{t \in T}$ is called **Janet division on** U.*

We use a degree lexicographical term order refining $x \succ y \succ z \succ t$ and apply the normal strategy in Algorithm 3.

Example 8.2 (Application of C_3) *The polynomials $f_1 = x^2 z$, $f_2 = xyzt$, and $f_3 = xy^2 t$ form already a reduced Gröbner basis. We want to compute a Janet basis of the the ideal generated by $\{f_1, f_2, f_3\}$. At the beginning the above polynomials have $\{x, y, z, t\}$, $\{z, t\}$, and $\{y, z, t\}$ as their respective Janet-multiplicative variables. The next 2 prolongations, namely yf_2 and xf_2 reduce to zero by zf_3 and ytf_1, respectively. The remaining prolongation $f_4 := xf_3 = x^2 y^2 t$ is irreducible. After adding f_4 to the basis, y becomes non-multiplicative for f_1 and the other multiplicative variables remain unchanged. We have to* *check all prolongations again. According to the normal strategy, the next prolongation is* $f_5 := yf_1$, *which is irreducible. Again we have to consider all prolongations. Because of* $C_1(f_1, f_5, x^2yz)$ *the prolongation* yf_1 *need not be reduced. Since* $R(y, f_2, f_3)$ *and the multiplicative variables of* f_3 *have not changed, the (repeated) reduction of* yf_2 *is avoided. We can also avoid to reduce* xf_2, *because* $C_0(x, f_2, \{f_1, \ldots, f_5\})$ *follows from the fact that* $R(x, f_2, f_1)$ *and* $f_1 = \operatorname{anc} f_5$ *are true, and* $\operatorname{lt} f_5$ *is a Janet-divisor of* $\operatorname{lt}(xf_2)$ *with respect to the set* $\{f_1, \ldots f_5\}$. *The reduction of the prolongation* xf_3 *is avoided, because* $f_4 = \operatorname{anc} f_3$ *and, thus,* $C_1(f_3, f_4, x^2y^2t)$ *holds. There is only one prolongation left, namely* $f_6 := yf_5 = x^2y^2z$ *which is irreducible and thus added to the basis. All prolongations that have been considered before are again avoided by the same reasons as above. The prolongation* yf_5 *will not be reduced, because* $f_5 = \operatorname{anc} f_6$ *and, thus,* $C_1(f_5, f_6, x^2y^2z)$ *holds. The prolongation* zf_4 *reduces to zero by* tf_6, *but its reduction cannot be avoided by the Gerdt/Blinkov version of Buchberger's chain criterion, cf. [GB98]. Let* $s := x^2y^2zt = \operatorname{lt}(zf_4)$. *Also* $C_1(f_4, f_6, s)$ *and* $C_2(f_4, f_6, s)$ *are false. However,* $\operatorname{anc} f_4 = f_3$ *and* $\operatorname{anc} f_6 = f_1$, *and there is a polynomial, namely* f_2, *with* $[f_1, f_2] = x^2yzt \lhd s$, $[f_3, f_2] = xy^2zt \lhd s$. *Therefore,* $C_3(f_4, f_6, s, \{f_1, \ldots, f_6\})$ *is true and the reduction of* zf_4 *can be avoided.*

Example 8.3 (Application of C_4) *Let us check the Janet basis property for the polynomials* $f_1 = xyz$, $f_2 = yt$, $f_3 = zt$, $f_4 = xf_2 = xyt$ *and* $f_5 = xf_3 = xzt$. *The Janet-multipliers are then* $\{x, y, z, t\}$, $\{y, z, t\}$, $\{z, t\}$, $\{x, y, t\}$, *and* $\{x, z, t\}$, *respectively. The prolongations* yf_3, xf_3, xf_2, *all reduce to zero. Consider the prolongations* zf_4 *and* yf_5. *Both are involutively top-reducible by* f_1. *Now, for* f_4 *and* f_5 *the only proper divisibility relations are* $f_2 \lhd f_4$ *and* $f_3 \lhd f_5$, *but for any* $i > 1$ *we have* $[f_1, f_i] = xyzt$. *Therefore, neither of the criteria* C_1, C_2, *and* C_3 *is applicable for* zf_4 *or for* yf_5. *However, by application of criterion* C_4 *we need only reduce* zf_4 *but not* yf_5.

9 Conclusion

In Theorem 3.1, we have presented a new characterisation of the involutive basis property. From this theorem we extracted four criteria and applied them in check and completion algorithms for involutive bases. We also showed that the application of criteria even enforces a termination of Algorithm 3 independent of the selection strategy that is used to choose the next prolongation. This opens a new field for further investigation on connections to Buchberger's algorithm. In particular sugar strategy [GMN+91] should be revisited in the context of involutive bases.

Acknowledgements

This work was supported by the Austrian Science Foundation (FWF), SFB F013, project 1304 and the Naturwissenschaftlich-Theoretisches Zentrum (NTZ) of the University of Leipzig, Germany.

References

[AL88] Joachim Apel and Wolfgang Laßner. An extension of Buchberger's algorithm and calculations in enveloping fields of Lie algebras. *Journal of Symbolic Computation*, 6(2–3):361–370, October–December 1988.

[Ape98a] Joachim Apel. The theory of involutive divisions and an application to Hilbert function computations. *Journal of Symbolic Computation*, 25(6):683–704, June 1998.

[Ape98b] Joachim Apel. *Zu Berechenbarkeitsfragen der Idealtheorie*. Habilitationsschrift, Universität Leipzig, Fakultät für Mathematik und Informatik, Augustusplatz 10–11, 04109 Leipzig, 1998.

[Buc65] Bruno Buchberger. *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal*. PhD thesis, Univ. Innsbruck, Dept. of Math., Innsbruck, Austria, 1965.

[Buc79] Bruno Buchberger. A criterion for detecting unnecessary reductions in the construction of Gröbner bases. In Edward W. Ng, editor, *Proc. EUROSAM '79*, volume 72 of *Lecture Notes in Computer Science*, pages 3–21, Berlin, 1979. Springer Verlag.

[BW93] Thomas Becker and Volker Weispfenning. *Gröbner Bases. A Computational Approach to Commutative Algebra*, volume 141 of *Graduate Texts in Mathematics*. Springer Verlag, New York, 1993.

[GB98] Vladimir P. Gerdt and Yuri A. Blinkov. Involutive bases of polynomial ideals. *Mathematics and Computers in Simulation*, 45:519–541, 1998.

[GMN+91] Alessandro Giovini, Teo Mora, Gianfranco Niesi, Lorenzo Robbiano, and Carlo Traverso. 'One sugar cube, please' or Selection strategies in the Buchberger algorithm. In Stephen M. Watt, editor, *ISSAC'91: Proceedings of the 1991 International Symposium on Symbolic and Algebraic Computation, July 15–17, Bonn, Germany*, pages 49–54, New York, NY 10036, USA, 1991. ACM Press.

[Jan20] Maurice Janet. Les systèmes d'équations aux dérivées partielles. *Journal de Mathematique. 8^e^ série*, 3:65–151, 1920.

[KRW90] A. Kandri-Rody and Volker Weispfenning. Non-Commutative Gröbner Bases in Algebras of Solvable Type. *Journal of Symbolic Computation*, 9(1):1–26, January 1990.

[Tho37] Joseph Miller Thomas. *Differential Systems*. American Mathematical Society, New York, 1937.

[Wu91] Wen-Tsün Wu. On the construction of Groebner basis of a polynomial ideal based on Riquier-Janet theory. *Systems Science and Mathematical Sciences*, 4(3):193–207, 1991.

[ZB93] A. Yu. Zharkov and Yuri A. Blinkov. Involution approach to solving systems of algebraic equations. In G. Jacob, N. E. Oussous, and S. Steinberg, editors, *Proceedings of the 1993 International IMACS Symposium on Symbolic Computation*, pages 11–16. IMACS, Laboratoire d'Informatique Fondamentale de Lille, France, 1993.