J. Symbolic Computation (1997) **11**, 1–000

The Theory of Involutive Divisions and an Application to Hilbert Function Computations †

JOACHIM APEL

Institut für Informatik, Universität Leipzig, Germany

(Received 27 June 1996)

Generalising the divisibility relation of terms we introduce the lattice of so-called involutive divisions and define the admissibility of such an involutive division for a given set of terms. Based on this theory we present a new approach for building up a general theory of involutive bases of polynomial ideals. In particular, we give algorithms for checking the involutive basis property and for completing an arbitrary basis to an involutive one. It turns out that our theory is more constructive and more flexible than the axiomatic approach to general involutive bases due to Gerdt and Blinkov.

Finally, we show that an involutive basis contains more structural information about the ideal of leading terms than a Gröbner basis and that it is straight forward to compute the (affine) Hilbert function of an ideal I from an arbitrary involutive basis of I.

1. Introduction

The observation that the theory of involutive bases of polynomial ideals (c.f. (ZB93)) provides an alternative method for the computation of Gröbner bases made the involutive bases a frequently investigated subject during the last two years. Experimental implementations showed that the involutive method is fast and storage saving (c.f. (GB96), (Ni96)). There are different types of involutive divisions originating from the theory of partial differential equations (c.f. (Ja29), (Th37),(Po78)).

The advantage of the Pommaret division consists in the fact that the divisibility of terms is independent on the leading terms of the ideal generators. Moreover, involutive divisions of Pommaret type can be considered as divisions of homogeneous elements in associated graded rings of polynomial rings with respect to natural non-commutative gradings (see (Ap95)). Unfortunately, there are polynomial ideals having no finite Pommaret basis. This drawback motivated to investigate also other involutive divisions. It turned out that any polynomial ideal has got a finite Janet basis as well as a finite Thomas basis and that the construction of them is algorithmic. Within the PoSSo project, Nischke studied the different involutive bases and implemented a software package named InvBase in the PoSSo library. His computing tests related to Janet bases indicated a very promising way for the computation of Gröbner bases ((Ni96)).

Recently, Gerdt and Blinkov presented an axiomatic approach specifying the essential

† This work was partially supported by the ESPRIT-BRA project PoSSo, Contract No. 6846

0747–7171/90/000000 + 00 $03.00/0

properties of involutive divisions (see (GB96)). In Section 3 we will introduce another characterisation of involutive divisions which is more constructive and more flexible than that of (GB96). We will discuss the relationships between generalised involutive divisions and sets of terms. The involutive divisions introduced in this paper form a lattice. There will be presented algorithms for the computation of the set of all involutive divisions which are admissible for a given finite set of terms and for the computation of maximal admissible refinements of involutive divisions.

In Section 4 we analyse the classical involutive divisions, i.e. Pommaret, Janet and Thomas division, in terms of our theory.

Section 5 deals with the theory of involutive bases of polynomial ideals. In particular, there are presented algorithms for checking the involutive basis property and for the completion of an arbitrary basis to an involutive one.

In Section 6 we discuss possible improvements of the involutive basis completion algorithm. In particular, we discuss selection strategies for choosing the admissible involutive division and show that the costs of the completion process are related to the partial ordering belonging to the lattice of involutive divisions. Furthermore, we will close some logical gaps in the proofs of (GB96). Finally, we discuss similarities and differences between the involutive method and the theory of Gröbner bases.

It is well-known that Gröbner bases are a powerful tool for the computation of Hilbert functions. Already Buchberger discussed this relationship in his famous thesis (Bu65) where the theory of Gröbner bases was invented. Moreover, from the theory of partial differential equations it is well-known that finite involutive bases of Pommaret type provide direct access to Hilbert polynomials (c.f. (Po78), (Se94)). In Section 7 we will present an explicit formula for the (affine) Hilbert function of an ideal in terms of an arbitrary finite involutive basis. Especially in situations where the involutive algorithm is faster than Buchberger's algorithm we obtain an excellent algorithm for the computation of Hilbert functions. In some sense one can say that the structural information of a monomial ideal becomes better accessible if it is given by an involutive basis. The experimental observation that the involutive method provides a fast algorithm for computing Gröbner bases was the original heuristical motivation for studying involutive bases in the context of polynomial ideals. The close relationship between Hilbert functions and involutive bases gives a second, a theoretical, motivation.

Since, all crucial investigations rely only on the monoid T of terms it is an easy exercise to generalise the results to algebras of solvable type. But, in order to not overload the paper with technical details we will formulate the theory in terms of polynomial rings.

Acknowledgement: The author is grateful to V.P. Gerdt, H.M. Möller and K. Nischke for valuable discussions and hints. Moreover, he wants to thank the referees for helpful comments.

2. Preliminaries

In this section we will set up some definitions and discuss some aspects of the theory of Gröbner bases. However, it is not our intention to present a complete introduction to the theory of Gröbner bases, for this we refer to (Bu85) and (BW93). Only selected facts motivating the ideas of involutive bases will be reported here.

Throughout this paper the notion ordering (of a set) stands for total irreflexive ordering. The reflexive closure of an ordering will be marked by underlining the corresponding ordering symbol in the usual way. If we need to consider reflexive or partial orderings we will emphasise this fact explicitly.

Let $R = \mathbb{K}[X]$ be the polynomial ring in the indeterminates $X = \{x_1, \dots, x_n\}$ over the field $\mathbb{K}$. By T we denote the set $\{x_1^{i_1} \cdots x_n^{i_n} \mid i_j = 0, 1, \dots\}$ of terms of R. As usual, the total degree $\sum_{j=1}^{n} i_j$ of the term $t = x_1^{i_1} \cdots x_n^{i_n} \in T$ will be denoted by $\deg t$. Furthermore, $\deg_j t$ refers to the degree i_j of t in the indeterminate x_j. We introduce the denotation $T(x_{i_1}, \dots, x_{i_l})$, or alternatively $T(\{x_{i_1}, \dots, x_{i_l}\})$, for the set $T \cap \mathbb{K}[x_{i_1}, \dots, x_{i_l}]$ of terms in the indeterminates $\{x_{i_1}, \dots, x_{i_l}\} \subseteq X$.

T together with the multiplication obtained by restricting the multiplication of R is an abelian monoid. The monoid ideal $\{s \in T \mid \exists u \in U, v \in T : s = vu\}$ generated by the set $U \subseteq T$ will be denoted by $Id_T(U)$. We will write also shortly $Id_T(u)$ for the principal monoid ideal generated by $u \in T$. Furthermore, we introduce the denotation $\langle U \rangle$ for the submonoid $\{t \in T \mid \exists u_1, \dots, u_m \in U : t = u_1 u_2 \cdots u_m\}$ of T generated by $U \subseteq T$. By definition the product of $m = 0$ terms is 1, in particular, $\langle \emptyset \rangle = \{1\}$.

T is a vector space basis of the polynomial ring R, i.e. every polynomial $f \in R$ can be uniquely represented as a linear combination $f = \sum_{u \in T} c_u u$, where $c_u \in \mathbb{K}$ and only a finite number of coefficients c_u is unequal 0, in terms of T. The set $\operatorname{supp} f = \{u \in T \mid c_u \neq 0\}$ of all terms appearing with non-zero coefficient in the above linear combination is called the *support* of f. From now, let us fix an admissible term ordering, i.e. a multiplication compatible well-ordering, $\prec$ of T. If $f \neq 0$ then we call the maximal element of $\operatorname{supp} f$ with respect to $\prec$ the *leading term* of f with respect to $\prec$ (denotation $\operatorname{lt} f$). By definition $\operatorname{lt} F := \{\operatorname{lt} f \mid 0 \neq f \in F\}$ for sets $F \subseteq R$ of polynomials. Furthermore, we define the *leading coefficient* $\operatorname{lc} f := c_{\operatorname{lt} f}$ of $f \neq 0$ with respect to $\prec$ as the coefficient of the leading term of f.

Let $F \subset R$ be a set of non-zero polynomials. A polynomial $g \in R$ satisfying $\operatorname{supp} g \cap Id_T(\operatorname{lt} F) = \emptyset$ is called *Gröbner-irreducible* modulo F and $\prec$. Let $h, h' \in R$, $f \in F$, $u, v \in T$, and $c \in \mathbb{K}$ be such that $h' = h + cvf$, $u \in \operatorname{supp} h \setminus \operatorname{supp} h'$, and $u = v \operatorname{lt} f$. Then we say that h can be *reduced* to h' modulo F and $\prec$. Iterated reduction of h modulo F and $\prec$ will terminate after finitely many steps since $\prec$ is a well-ordering. The result of such a reduction process, which in general depends on various decisions made during the reduction, is called a *Gröbner normal form* of h modulo F and $\prec$. Any *Gröbner normal form* of h modulo F and $\prec$ is Gröbner-irreducible modulo F and $\prec$ and congruent to h modulo the ideal generated by F.

If every $h \in R$ has a uniquely determined Gröbner normal form modulo F and $\prec$ then F is called a *Gröbner basis* of the ideal I generated by F with respect to $\prec$. We have the well-known equivalences (c.f. (Bu85), (BW93)):

i) F is a Gröbner basis of I with respect to $\prec$.
ii) $Id_T(\operatorname{lt} I) = Id_T(\operatorname{lt} F) = \bigcup_{f \in F} Id_T(\operatorname{lt} f)$.
iii) Every $g \in I$ has Gröbner normal form 0 modulo F and $\prec$.
iv) For all $f, g \in F$ the S-polynomial $Spol(f, g) = \operatorname{lc}(g)\; uf - \operatorname{lc}(f)\; vg$, where by definition $u, v \in T$ are such that $u \cdot \operatorname{lt} f = v \cdot \operatorname{lt} g = lcm(\operatorname{lt} f, \operatorname{lt} g)$, has Gröbner normal form 0 modulo F and $\prec$.

While the conditions *ii)* and *iii)* are used in various generalisations of the theory of Gröbner bases the importance of condition *iv)* consists in the fact that it is constructive and illustrates the main idea of Buchberger's algorithm.

3. The Lattice of Involutive Divisions

Consider the family $\mathcal{T} = (T_u)_{u\in T}$ of subsets $T_u \subseteq T$, where $T_u = Id_T(u)$ is the principal monoid ideal of T generated by u. Then u is multiple of v if and only if $u \in T_v$ and u is divisor of v if and only if $v \in T_u$. This idea of characterising multiple and divisor relations can be generalised in the following way:

Definition 3.1. *Let $(Y_u)_{u\in T}$ be a family of subsets $Y_u \subseteq X$ of indeterminates. The family $\mathcal{M} = (u\cdot\langle Y_u\rangle)_{u\in T}$ is called the* involutive division *generated by $(Y_u)_{u\in T}$. The elements $u \in v\cdot\langle Y_v\rangle$ are called the $\mathcal{M}$*-multiples *of v and v is called a $\mathcal{M}$*-divisor *of $u \in v\cdot\langle Y_v\rangle$.*

Let $V \subseteq T$ be a set of terms and $\sqsubset$ an ordering of V. The involutive division $\mathcal{M} = (M_u)_{u\in T}$ is called admissible for $(V,\sqsubset)$ *if for all $v,w \in V$ such that $w \sqsubset v$ it holds one of the conditions $M_w \subset M_v$ or $M_v \cap Id_T(w) = \emptyset$. The short cut $\mathcal{M}$* is admissible for V *will express the existence of $\sqsubset$ such that $\mathcal{M}$ is admissible for $(V,\sqsubset)$.*

We remark, that the notion "involutive division" follows Zharkov/Gerdt/Blinkov, the elements of Y_u are the so-called "multiplicative variables" and those of $X\setminus Y_u$ the "non-multiplicative variables" for u in the sense of Zharkov/Gerdt/Blinkov (c.f. (ZB93), (GB96)). Let $\mathbb{M}_{(V,\sqsubset)}$ denote the set of all involutive divisions $\mathcal{M}$ which are admissible for $(V,\sqsubset)$. In accordance with the above definition we set $\mathbb{M}_V := \bigcup_{\sqsubset}\mathbb{M}_{(V,\sqsubset)}$, where $\sqsubset$ ranges over the set of all orderings of V. It is easy to verify the relationship $\mathbb{M}_{(V,\sqsubset)} \subseteq \mathbb{M}_{(W,\sqsubset|_W)}$ for any sets $W \subseteq V$ of terms and orderings $\sqsubset$ of V. Furthermore, $\mathbb{M}_\emptyset$ is the set of all involutive divisions. If $u \sqsubset v$ for some $u,v \in V$ satisfying $u \mid v$ then $\mathbb{M}_{(V,\sqsubset)} = \emptyset$ since $v \in M_v \cap Id_T(u) \neq \emptyset$ and $u \notin M_v \not\supseteq M_u$.

Definition 3.2. *Let $\mathcal{M} = (M_u)_{u\in T}$ and $\mathcal{N} = (N_u)_{u\in T}$ be two involutive divisions and $V \subseteq T$ a set of terms.*
If $M_v = N_v$ for all $v \in V$ then $\mathcal{M}$ and $\mathcal{N}$ are called V-equivalent *(denotation $\mathcal{M} \equiv_V \mathcal{N}$).*
If $M_u \subseteq N_u$ for all $u \in T$ then we say that $\mathcal{N}$ refines *$\mathcal{M}$ (denotation $\mathcal{M} \leq \mathcal{N}$).*

Obviously, $\equiv_V$ is an equivalence relation and $\leq$ is a reflexive partial ordering on the set $\mathbb{M}_\emptyset$ of all involutive divisions. For the rest of this paper all notions referring to an ordering of involutive division will be understood with respect to the refinement relation $\leq$. The set of all maximal elements of a set $\mathbb{M}$ of involutive divisions will be denoted by $\max(\mathbb{M})$. Any set $\mathbb{M}$ of involutive divisions has an infimum $\inf(\mathbb{M})$ and a supremum $\sup(\mathbb{M})$ with respect to $\leq$, hence, $(\mathbb{M}_\emptyset,\leq)$ forms a lattice.

Let us fix a set $V \subseteq T$ and consider the quotient space $\mathbb{M}_\emptyset/\equiv_V$. By $\bar{\mathcal{M}}$ we denote the equivalence class of $\mathcal{M}$ modulo $\equiv_V$. For any $\mathcal{M} \in \mathbb{M}_\emptyset$ we have $\sup(\bar{\mathcal{M}}) \in \bar{\mathcal{M}}$ and the quotient structure forms a lattice together with the induced refinement relation $\bar{\mathcal{M}} \leq \bar{\mathcal{N}} :\Longleftrightarrow \sup(\bar{\mathcal{M}}) \leq \sup(\bar{\mathcal{N}})$. Note, that the subset $\mathbb{M}_V/\equiv_V \subseteq \mathbb{M}_\emptyset/\equiv_V$ is closed under the inf-operation but, in general, it is not closed under the sup-operation.

Next, we are looking for necessary and sufficient conditions for the admissibility of an involutive division $\mathcal{M} = (M_u)_{u\in T}$ generated by $(Y_u)_{u\in T}$ for a given ordered set $(V,\sqsubset)$ of terms. Admissibility implies $M_u \subset M_v$, and hence $Y_u \subseteq Y_v$, for any terms $u,v \in V$ such that $u \sqsubset v$ and $u \in M_v$. Therefore, the set

$$A_u := \{x_i \in X \mid \exists v \in V : (u \sqsubset v \wedge u \in M_v \wedge x_i \notin Y_v)\} \qquad (3.1)$$

associated to u contains only indeterminates not belonging to Y_u. To each $u \in V$ we assign the subsets

$$B_u := \{v \in V \mid v \sqsubset u, v \notin Id_T(u)\} \text{ and } \tag{3.2}$$

$$C_u := \{v \in V \mid v \sqsubset u, M_v \not\subseteq u \cdot \langle Y_u \cup \{x_i \in X \mid \deg_i u < \deg_i v\}\rangle\} \tag{3.3}$$

of V. B_u consists of all terms $v \in V$ which are smaller than u with respect to $\sqsubset$ and for which the admissibility condition $M_v \subset M_u$ is unsatisfiable because of $M_v \ni v \notin Id_T(u) \supseteq M_u$. Therefore, if $\mathcal{M}$ is admissible for $(V, \sqsubset)$ we must have $M_u \cap Id_T(v) = \emptyset$ for all $v \in B_u$, i.e. each term $\frac{lcm(u,v)}{u}$, where $v \in B_u$, must contain at least one indeterminate which does not belong to the set Y_u. Note, if there exist $u, v \in V$ such that $v \sqsubset u$ and $v \mid u$ then we have $v \in B_u$ and $\frac{lcm(u,v)}{u} = 1$ which confirms our above observation $\mathbb{M}_{(V,\sqsubset)} = \emptyset$.

The set C_u is constructed in such a way that for any refinement $\mathcal{N}$ of $\mathcal{M}$ obtained by enlarging Y_u there is always satisfied one of the admissibility conditions $N_v \subset N_u$ or $N_u \cap Id_T(v) = \emptyset$ for all $v \in V \setminus C_u$ such that $v \sqsubset u$.

In the following theorem we consider monomial ideals of the polynomial ring $Q = \mathbb{K}[X]$. Note, the equality $Q = R$ in the settings of this paper. But for the sake of extendibility to algebras of solvable type R we emphasise that, in general, Q and R need not to coincide. Furthermore, we remark that the results presented in this section are independent on the choice of the field $\mathbb{K}$.

THEOREM 3.1. *Let $\mathcal{M} = (M_u)_{u \in T}$ be the involutive division generated by $(Y_u)_{u \in T}$. Furthermore, let $(V, \sqsubset)$ be an ordered set of terms. For each $u \in V$ let A_u, B_u and C_u be the sets defined in Equations 3.1–3.3. Then the following conditions are equivalent:*

i) $\mathcal{M}$ is admissible for $(V, \sqsubset)$.
ii) Y_u is independent set of the monomial ideal $(A_u) + (B_u) : (u)$ for every $u \in V$.
iii) Y_u is independent set of the monomial ideal $(A_u) + (C_u) : (u)$ for every $u \in V$.

Furthermore, if Y_u is maximal independent set for $(A_u) + (B_u) : (u)$ for every $u \in V$ and $Y_u = X$ for all $u \notin V$ then $\mathcal{M}$ is maximal in the set of all involutive division which are admissible for $(V, \sqsubset)$. In contrary, if $\mathcal{M}$ is a maximal element of the set of all involutive division admissible for $(V, \sqsubset)$ then for all $u \in V$ the set Y_u is a maximal independent set for $(A_u) + (C_u) : (u)$.

PROOF. *i) ⇒ iii)* Let $\mathcal{M}$ be admissible for $(V, \sqsubset)$. Assume that there exist $u \in V$ and $t \in T$ such that $t \in ((A_u) + (C_u) : (u)) \cap \mathbb{K}[Y_u]$, in particular $ut \in M_u$. If $t \in (A_u)$ then there exists $v \in V$ such that $u \sqsubset v$, $u \in M_v$ and $t \notin \langle Y_v \rangle$. Hence, $ut \in M_u \backslash M_v$. Consequently, neither $M_u \subseteq M_v$ nor $M_v \cap Id_T(u) = \emptyset$ in contradiction to Definition 3.1. It remains to consider the case $t \in (C_u) : (u)$. Then it follows the existence of $v \in V$ satisfying the conditions $v \sqsubset u$, $M_v \not\subseteq u \cdot \langle Y_u \cup \{x_i \in X \mid \deg_i u < \deg_i v\}\rangle \supseteq M_u$ and $ut \in M_u \cap Id_T(v)$ which again contradicts Definition 3.1. In conclusion, $((A_u) + (C_u) : (u)) \cap \mathbb{K}[Y_u] = \{0\}$ for all $u \in V$.
iii) ⇒ ii) Trivial, since $B_u \subseteq C_u$ for all $u \in V$.
ii) ⇒ i) Let $((A_u) + (B_u) : (u)) \cap \mathbb{K}[Y_u] = \{0\}$ for all $u \in V$. Let $v, u \in V$ be arbitrary elements of V satisfying $v \sqsubset u$ and consider the intersection $M_u \cap Id_T(v)$. We start with the case $v \notin Id_T(u)$. Then $v \in B_u$ and $\frac{lcm(u,v)}{u} \in (B_u) : (u)$. Hence, $\frac{lcm(u,v)}{u} \notin \langle Y_u \rangle$,

Figure 1. Computation of $\mathbb{M}_V/\equiv_V$

```
Input: V = {v_1, v_2, ..., v_m} ⊂ T
Output: M_V / ≡_V

function LIFT(π, Y, j)
      if j > m then
            M_{v_i} := v_i · ⟨Y[i]⟩ ,   (i = 1, ..., m)
            M_u := u · ⟨X⟩ ,   (u ∉ V)
            return({M})
      end if
      L := ∅
      l := j − 1
      while l > 0 and v_{π(j)} ∉ v_{π(l)} · ⟨Y[π(l)]⟩ do l := l − 1 end while
      if l > 0 then A := X\Y[π(l)] else A := ∅ end if
      B := { lcm(v_{π(i)}, v_{π(j)}) / v_{π(j)}  |  j < i ∧ v_{π(j)} ∤ v_{π(i)} }
      for each independent set Z of (A) + √(B) do
            Y[π(j)] := Z
            L := L∪ LIFT (π, Y, j + 1)
      end for
      return(L)
end LIFT
M := ∅
Y := array[1 ... m]
for each permutation π of {1, ..., m} do
      M := M∪ LIFT(π, Y, 1)
end for
return(M)
```

consequently, $lcm(u,v) \notin M_u$. It follows $w \notin M_u$ for all $w \in Id_T(lcm(u,v))$. In conclusion $M_u \cap Id_T(v) = \emptyset$.

Now, consider the case $v \in Id_T(u)$. Assume $M_u \cap Id_T(v) \neq \emptyset$ and let $w \in M_u \cap Id_T(v)$. Then $\frac{v}{u} \in \langle Y_u \rangle$ since $\frac{w}{u} \in \langle Y_u \rangle$ and $\frac{v}{u} \mid \frac{w}{u}$. Hence, $v \in M_u$ and $X \backslash Y_u \subseteq A_v$. Consequently, $Y_v \subseteq Y_u$ which implies $M_v \subseteq M_u$.

We come to the proof of the sufficient and the necessary condition presented in the second part of the theorem. Let the involutive division $\mathcal{M} = (M_u)_{u \in T}$ generated by $(Y_u)_{u \in T}$ satisfy $Y_u = X$ for all $u \notin V$ and have the property that all the sets Y_u, $u \in V$, are maximal independent sets for the corresponding monomial ideals $(A_u) + (B_u) : (u)$. Assume there exists an involutive division $\mathcal{N} = (N_u)_{u \in T}$ which is admissible for $(V, \sqsubset)$ and satisfies $\mathcal{M} < \mathcal{N}$. Let $\mathcal{N}$ be generated by $\left(Y_u^{\mathcal{N}}\right)_{u \in T}$ and let $A_v^{\mathcal{N}}$ and $B_v^{\mathcal{N}}$ be the sets defined in 3.1 and 3.2 which correspond to $\mathcal{N}$. Since definition 3.2 does not depend on the generating family $(Y_u)_{u \in T}$ we have $B_w = B_w^{\mathcal{N}}$ for all $w \in V$. Let $v \in V$ be of minimal possible degree such that $Y_v \subset Y_v^{\mathcal{N}}$. Then for any proper divisor $w \mid v$ we have $Y_w = Y_w^{\mathcal{N}}$ and, hence, $A_v = A_v^{\mathcal{N}}$. Consequently, $(A_v) + (B_v) : (v) = (A_v^{\mathcal{N}}) + (B_v^{\mathcal{N}}) : (v)$. Since, Y_v is assumed to be a maximal independent set of $(A_v) + (B_v) : (v)$ the larger set $Y_v^{\mathcal{N}}$ must be a dependent set of $(A_v^{\mathcal{N}}) + (B_v^{\mathcal{N}}) : (v)$. According to the first part of the theorem this contradicts the assumption that $\mathcal{N}$ is admissible for $(V, \sqsubset)$ and, consequently, $\mathcal{M} \in \max\left(\mathbb{M}_{(V,\sqsubset)}\right)$.

Let $\mathcal{M}$ be maximal in the set of all involutive division which are admissible for $(V, \sqsubset)$. We have to show that $Y_u \cup \{y\}$ is dependent set of the monomial ideal $(A_u) + (C_u) : (u)$ for any $u \in V$ and $y \in X \backslash Y_u$.

Figure 2. Computing submaximal admissible refinements

Input: $V = \{v_1, v_2, \dots, v_m\} \subset T$, ordered by $v_m \sqsubset \cdots \sqsubset v_1$
  $Y = [Y[1], \dots, Y[m]]$ generating[a] $\mathcal{M} \in \mathbb{M}_{(V,\sqsubset)}$

Output: $\mathcal{N} \in \operatorname{submax}\left(\mathbb{M}_{(V,\sqsubset)}\right)$ satisfying $\mathcal{M} \le \mathcal{N}$

$N_u := u \cdot \langle X \rangle\,, \quad (u \notin V)$
for $i := 1$ **to** m **do**
  $j := i - 1$
  while $j > 0$ and $v_i \notin N_{v_j}$ **do** $j := j - 1$ **end while**
  if $j > 0$ **then** $A := X \setminus Y[j]$ **else** $A := \emptyset$ **end if**
  $C := \left\{ \frac{lcm(v_i, v_j)}{v_i} \;\middle|\; i < j \le m \;\wedge\; v_j \cdot \langle Y[j] \rangle \not\subset v_i \cdot \langle Y[i] \cup \{x_l \mid \deg_l v_i < \deg_l v_j\} \rangle \right\}$
  while $Y[i]$ is not maximal independent for $(A) + \sqrt{(C)}$ **do**
    compute a maximal independent set $Z \supset Y[i]$ of $(A) + \sqrt{(C)}$
    $Y[i] := Z$
    $C := \left\{ \frac{lcm(v_i, v_j)}{v_i} \;\middle|\; i < j \le m \;\wedge\; v_j \cdot \langle Y[j] \rangle \not\subset v_i \cdot \langle Y[i] \cup \{x_l \mid \deg_l v_i < \deg_l v_j\} \rangle \right\}$
  end while
  $N_{v_i} := v_i \cdot \langle Y[i] \rangle$
end for
return($\mathcal{N}$)

[a] up to V-equivalence

Assume there exist $w \in V$ and $y \in X \setminus Y_w$ such that $((A_w) + (C_w) : (w)) \cap \mathbb{K}[Y_w \cup \{y\}] = \{0\}$. Let $\mathcal{N} = (N_v)_{v \in T}$ be the involutive division defined by $N_w := w \cdot \langle Y_w \cup \{y\} \rangle$ and $N_u := M_u$ for all $u \ne w$. Consider arbitrary $u, v \in V$ such that $v \sqsubset u$. If $w \notin \{u, v\}$ then the condition $N_v \subseteq N_u$ or $N_u \cap Id_T(v) = \emptyset$ carries over from $\mathcal{M}$.

Consider the case $v = w$. Obviously, $M_u \cap Id_T(w) = \emptyset$ implies $M_u \cap Id_T(w) = N_u \cap Id_T(w) = \emptyset$. So, let us check the case $M_w \subseteq M_u$. From $X \setminus Y_u \subseteq A_w$ and $(A_w) \cap \mathbb{K}[Y_w \cup \{y\}] = \{0\}$ we deduce $y \in Y_u$. Hence, $N_w \subseteq N_u = M_u$.

Finally, we have to consider $u = w$. Obviously, if $M_v \subseteq M_w$ then $M_v = N_v \subseteq M_w \subset N_w$. Hence, it remains the case $M_w \cap Id_T(v) = \emptyset$ where we will distinguish two subcases.

a) We start with the case $v \in C_w$. From $(C_w) : (w) \cap \mathbb{K}[Y_w \cup \{y\}] = \{0\}$ it follows $wt \notin (C_w) \supseteq (v)$ for all $t \in \langle Y_w \cup \{y\} \rangle$ and we deduce $N_w \cap Id_T(v) = \emptyset$.

b) Let $v \notin C_w$. If $N_w \cap Id_T(v) \ne \emptyset$ then it follows $\{x_i \mid \deg_i w < \deg_i v\} \subseteq Y_w \cup \{y\}$ and we deduce $N_v = M_v \subseteq w \cdot \langle Y_w \cup \{x_i \mid \deg_i w < \deg_i v\} \rangle \subseteq w \cdot \langle Y_w \cup \{y\} \rangle = N_w$.

In conclusion, it follows that $\mathcal{N}$ is admissible for $(V, \sqsubset)$. By construction we have $\mathcal{M} < \mathcal{N}$ in contradiction to the assumed maximality of $\mathcal{M}$. $\square$

An involutive division $\mathcal{M} \in \mathbb{M}_{(V,\sqsubset)}$ generated by a family $(Y_u)_{u \in T}$ satisfying the necessary maximality condition presented in Theorem 3.1, i.e. Y_u is a maximal independent set for the monomial ideal $(A_u) + (C_u) : (u)$ for all $u \in V$, will be called a *submaximal* involutive division admissible for $(V, \sqsubset)$. The set of all submaximal involutive division which are admissible for $(V, \sqsubset)$ will be denoted by $\operatorname{submax}(\mathbb{M}_{(V,\sqsubset)})$.

Figure 1 presents an algorithm for the computation of the set of equivalence classes modulo $\equiv_V$, given by their maximal representants, of all involutive divisions which are admissible for a fixed finite set $V \subset T$. Termination is obvious. Correctness follows immediately from the equivalence of conditions *i)* and *ii)* in Theorem 3.1 and some well-known facts on monomial ideals.

Let $\mathcal{M}$ be a given involutive division which is admissible for $(V,\sqsubset)$. Using the algorithm presented in Figure 2 it is possible to compute a submaximal involutive division $\mathcal{N}$ admissible for $(V,\sqsubset)$ which refines $\mathcal{M}$. The termination of Algorithm 2 is trivial. In the proof of Theorem 3.1 it was shown that enlarging $Y[i]$ to another independent set $Z \supset Y[i]$ of the ideal $(A)+\sqrt{(C)}$ preserves the admissibility of the involutive division generated by Y for $(V,\sqsubset)$. In particular, it is an invariant of Algorithm 2 that for every $1 \le j \le m$ the set $Y[j]$ is independent for the corresponding ideal $(A_{v_j})+(C_{v_j}):(v_j)$ defined in Theorem 3.1. Furthermore, if $Y[i]$ is enlarged in Algorithm 2 then for any $1 \le j < i$ the ideal $(A_{v_j})+(C_{v_j}):(v_j)$ becomes larger or equal, hence, also the maximality of all previously considered sets $Y[j]$ is maintained. In conclusion, it follows the correctness of the algorithm.

Note, the necessity of the **while**-loop repeating the refinement of the involutive division at $Y[i]$. The set C may become smaller after $Y[i]$ is enlarged to a maximal independent set $Z \supseteq Y[i]$. Therefore, in general, Z needs not to be maximal for the possibly smaller ideal $(A_{v_i})+(C_{v_i}):(v_i)$ corresponding to the refined involutive division.

As a byproduct we obtain an algorithm for checking the submaximality of an admissible involutive division. Since for any finite set V the set $\mathbb{M}_V/\equiv_V$ is finite, too, it is also possible to check maximality or to compute maximal refinements in an algorithmic way. In this case it is advisable to start with the computation of a submaximal refinement using Algorithm 2 and then to look for its maximal refinements using combinatorics. Algorithm 2 is fast and starting the combinatorical search from a submaximal admissible refinement often shrinks the costs drastically.

Let us summarise. For any given finite set V we are able to construct the set of all involutive divisions which are admissible for V. Furthermore, for an arbitrary given $\mathcal{M} \in \mathbb{M}_{(V,\sqsubset)}$ we can construct $\mathcal{N} \in \operatorname{submax}\left(\mathbb{M}_{(V,\sqsubset)}\right)$ satisfying $\mathcal{M} \le \mathcal{N}$. Spending more combinatorical efforts we can also achieve $\mathcal{N} \in \max\left(\mathbb{M}_{(V,\sqsubset)}\right)$.

In Section 6 we will show the importance of submaximal and maximal involutive divisions for the theory of involutive bases of polynomial ideals. Hence, from the point of view of constructivity, here we are in a better situation than in (GB96).

4. Classical Involutive Divisions

In this section we will justify our definition of involutive divisions by showing that the classical involutive divisions, i.e. Pommaret, Janet and Thomas division, can be described in terms of our theory. The reverse lexicographical ordering on T will prove to be a suitable ordering $\sqsubset$ for the classical involutive divisions. By $\lhd$ we denote the reverse lexicographical ordering extending $x_1 \lhd x_2 \lhd \cdots \lhd x_n$, i.e. $x_1^{i_1}\cdots x_n^{i_n} \lhd x_1^{j_1}\cdots x_n^{j_n}$ iff the first non-zero component of the integer vector $(i_1-j_1,\ldots,i_n-j_n)$ is positive. For the sake of simplicity we will denote any restriction $\lhd|_V$ of the reverse lexicographical ordering to a subset $V \subset T$ also by $\lhd$.

4.1. Pommaret Division

Definition 4.1. (c.f. (Po78), (ZB93),(GB96)) *$u \in T$ is called a* Pommaret divisor *of $v \in T$ if $u \mid v$ and, in addition, there exists $1 \le i \le n$ such that $u \in T(x_1,\ldots,x_i)$ and $\frac{v}{u} \in T(x_i,\ldots,x_n)$. Under the same conditions we call v a* Pommaret multiple *of u. The* *family* $\mathcal{P} = (P_v)_{v \in T}$, *where* P_v *denotes the set of all Pommaret multiples of* v, *is called the* Pommaret division *(corresponding to* $\lhd$*).*

If $v \notin T(x_1)$, then the set of all Pommaret multiples of v can be represented in the form $P_v = v \cdot \langle Y_{\mathcal{P},v} \rangle$, where $Y_{\mathcal{P},v} = \{x_i, \ldots, x_n\}$ and $1 \le i \le n$ is such that $v \in T(x_1, \ldots, x_i)$ but $v \notin T(x_1, \ldots, x_{i-1})$. For $v = x_1^\alpha$ we have $P_v = v \cdot \langle Y_{\mathcal{P},v} \rangle$, where $Y_{\mathcal{P},v} = X$.

LEMMA 4.1. *For every* $v \in T$ *the set* $Y_{\mathcal{P},v}$ *is maximal independent set for the monomial ideal* $(A_v) + (B_v) : (v)$ *defined in Theorem 3.1.*

PROOF. The case $v = 1$ is trivial since $A_1 = B_1 = \emptyset$. Consider $v \neq 1$ and let $1 \le i \le n$ be such that $\deg_i v > 0$ and $\deg_j v = 0$ for all $i < j \le n$. Then $A_v \subseteq \{x_1, \ldots, x_{i-1}\}$ since $Y_{\mathcal{P},u} \supseteq \{x_i, \ldots, x_n\}$ for all divisors u of v.

For any $T \ni w \lhd v$ there exists $1 \le k \le n$ such that $\deg_k w > \deg_k v$ and $\deg_j w = \deg_j v$ for all $1 \le j < k$. If, in addition, $v \not| w$ then $k < i$. Hence, $(B_v) : (v) \subseteq (x_1, \ldots, x_{i-1})$. From $\{\frac{x_k v}{x_i} \mid k < i\} \subseteq B_v$ we obtain equality.

The final observation that $Y_{\mathcal{P},v} = \{x_i, \ldots, x_n\}$ is a maximal independent set for $(A_v) + (B_v) : (v) = (x_1, \ldots, x_{i-1})$ completes the proof. $\Box$

COROLLARY 4.1. *The Pommaret division* $\mathcal{P}$ *is admissible for* $(T, \lhd)$ *and maximal in the set* $\mathbb{M}_{(T,\lhd)}$.

The corollary follows immediately from Lemma 4.1 and Theorem 3.1. The next two theorems emphasise the outstanding position of the Pommaret division in the class of all involutive divisions which are admissible on the entire monoid T.

THEOREM 4.1. *Let* $\sqsubset$ *be an ordering of* T *satisfying* $x_1 \sqsubset x_2 \sqsubset \cdots \sqsubset x_n$ *and* $u \sqsubset v \iff uw \sqsubset vw$ *for all* $u, v, w \in T$. *The Pommaret division* $\mathcal{P}$ *refines any involutive division* $\mathcal{M}$ *which is admissible for* $(T, \sqsubset)$.

PROOF. Assume there exists $u \in T$ such that $M_u \not\subseteq P_u$. Then there exist $1 \le j < i \le n$ such that $x_j \cdot u \in M_u$ and $x_i \mid u$. From the properties of $\sqsubset$ it follows $v := x_j \cdot \frac{u}{x_i} \sqsubset x_i \cdot \frac{u}{x_i} = u$. Obviously, $u \not| v$. Hence, $M_u \cap Id_T(v) = \emptyset$ according to Definition 3.1. This contradicts $x_i \cdot v = x_j \cdot u \in M_u$. $\Box$

THEOREM 4.2. *The Pommaret division is a maximal element of the set* $\mathbb{M}_T$ *of all involutive divisions admissible on the entire monoid* T.

PROOF. We have to prove that $\mathcal{P} \not< \mathcal{M}$ for any involutive division $\mathcal{M} \in \mathbb{M}_{(T,\sqsubset)}$, where $\sqsubset$ is an arbitrary order of T.

Assume, there exists an involutive division $\mathcal{M} = (M_u)_{u \in T} \in \mathbb{M}_T$ satisfying $\mathcal{P} < \mathcal{M}$. Let $\mathcal{M}$ be generated by $(Y_u)_{u \in T}$ and let $v \in T$ be a term of minimal possible degree such that $P_v \neq M_v$. Obviously, we have $v \notin \mathbb{K}[x_1]$. Let $1 < j \le n$ be such that $v \in \mathbb{K}[x_1, \ldots, x_j]$ and $v \notin \mathbb{K}[x_1, \ldots, x_{j-1}]$. It follows $v \in P_{\frac{v}{x_j}} = M_{\frac{v}{x_j}}$. Hence, $Y_v \subseteq Y_{\frac{v}{x_j}} = Y_{\mathcal{P},\frac{v}{x_j}}$. Let $1 \le i < j$ be minimal with the property $x_i \in Y_v$. It follows $\frac{v}{x_j} \in \mathbb{K}[x_1, \ldots, x_i]$. Set $u := \frac{v x_i}{x_j}$. From $u x_j = v x_i \in M_v \cap Id_T(u) \neq \emptyset$ it follows $v \sqsubset u$. But since $u \in \mathbb{K}[x_1, \ldots, x_i]$ we have also $\{x_i, \ldots, x_n\} \subseteq Y_{\mathcal{P},u} \subseteq Y_u$ leading to the contradiction $v x_i = u x_j \in M_u \cap Id_T(v) \neq \emptyset$. $\Box$

Note, that the $n!$ Pommaret divisions corresponding to the reverse lexicographical orderings extending a permutation of the indeterminates are not the only maximal involutive divisions admissible on T. But according to Theorem 4.1 all other maximal involutive divisions admissible for T require exotic term orderings $\sqsubset$. Let us consider an example. For $X = \{x, y\}$ let $T = T_y \cup T_x \cup T_{xy}$ be the partition of the set $T = T(x, y)$ of terms defined by $T_y := T(y)$, $T_x := x \cdot T(x)$, and $T_{xy} := Id_T(xy)$. Furthermore, let $\lhd$ denote the reverse lexicographical term ordering extending $x \lhd y$ and $\sqsubset$ the ordering of T having the following properties:

i) $\sqsubset|_{T_s} = \lhd|_{T_s}$ for $s \in \{y, x, xy\}$,
ii) $T_{xy} \sqsubset T_x \sqsubset T_y$, where $T_s \sqsubset T_{s'} :\Longleftrightarrow \forall u \in T_s, v \in T_{s'} \ : \ u \sqsubset v$.

Finally, let $\mathcal{P}$ be the Pommaret division corresponding to $\lhd$ and define: $Y_1 := Y_x := \{x, y\}$, $Y_u := \{y\}$ for all $1 \neq u \in T_y$, $Y_u := \{x\}$ for all $x \neq u \in T_x$, and $Y_u := Y_{\mathcal{P}, \frac{u}{xy}}$ for all $u \in T_{xy}$. It is easy to verify that the involutive division $\mathcal{M}$ generated by $(Y_u)_{u \in T}$ is admissible for T and not refined by any of the two Pommaret divisions. Moreover, $\mathcal{M}$ is a maximal element of $\mathbb{M}_T$.

4.2. Janet Division

In contrast to the Pommaret division the notion Janet division stands for a function $\iota : Pow(T) \to \mathbb{M}_\emptyset$, where $Pow(T)$ is the set of all subsets of T, which assigns to each subset $V \subseteq T$ an involutive division $\iota(V) = \mathcal{J}^{(V)} \in \mathbb{M}_V$ which is admissible for V.

Definition 4.2. (c.f. (Ja29),(GB96)) *Let $V \subseteq T$ be a set of terms. Furthermore, let $Y_{\mathcal{J}^{(V)}, u} := X$ for all $u \notin V$ and*

$$Y_{\mathcal{J}^{(V)}, v} := \left\{ x_i \ \mid \ \neg \exists u \in V \ \left(\deg_i u > \deg_i v \wedge \forall 1 \leq j < i \ \deg_j u = \deg_j v \right) \right\}$$

for all $v \in V$. The involutive division $\mathcal{J}^{(V)} = \left(J_u^{(V)} \right)_{u \in T}$, where $J_u^{(V)} := u \cdot \langle Y_{\mathcal{J}^{(V)}, u} \rangle$ for all $u \in T$, is called the Janet division (corresponding to $\lhd$) supported on V.

In the case of Janet divisions we will also use the notions *Janet divisor* and *Janet multiple* instead of $\mathcal{J}^{(V)}$-involutive divisor and $\mathcal{J}^{(V)}$-involutive multiple, respectively.

Lemma 4.2. *The Janet division supported on $V \subseteq T$ is admissible for $(V, \lhd)$. Furthermore, the sets $J_v^{(V)}$, $v \in V$, are pairwise disjoint.*

Proof. Let A_v and B_v be as defined in Equations 3.1 and 3.2. It is easy to observe the equality

$$J_v^{(V)} \cap V = \{v\} \ , \text{ for all } v \in V \quad . \tag{4.1}$$

Hence, we have $A_v = \emptyset$ for all $v \in V$. Fix an arbitrary $v \in V$. For any term $u \in T$ which is smaller than v with respect to the reverse lexicographical ordering there exists $1 \leq i_u \leq n$ such that $\deg_{i_u} u > \deg_{i_u} v$ and $\deg_j u = \deg_j v$ for all $1 \leq j < i_u$. Hence, $u \in B_v$ implies $x_{i_u} \notin Y_{\mathcal{J}^{(V)}, v}$. Consequently, $t \notin \langle Y_{\mathcal{J}^{(V)}, v} \rangle$ for all $t \in (B_v) : (v)$ and it follows that $Y_{\mathcal{J}^{(V)}, v}$ is an independent set for the monomial ideal $(A_v) + (B_v) : (v)$. This proves the admissibility of $\mathcal{J}^{(V)}$ for $(V, \lhd)$ and according to (4.1) the sets $J_v^{(V)}$, $v \in V$, are pairwise disjoint. $\square$

We cannot hope that $\mathcal{J}^{(V)}$ is maximal admissible for any set V, e.g. $\mathcal{J}^{(T)} \le \mathcal{P}$ according to Theorem 4.1 and the refinement is proper since $J_v^{(T)} = J_v^{(T)} \cap T = \{v\}$ for all $v \in T$. Actually, $V = T$ is an extreme case which is not of great interest in the case of Janet divisions. So, let us discuss the situation slightly more detailed. It is easy to observe that $Y_{\mathcal{J}^{(V)},u}$ is an independent set of the monomial ideal $(D_u) : (u)$, where $D_u := \{v \in V \mid v \lhd u\}$, for all $u \in V$. We have the relationship $(A_u) + (B_u) : (u) = (B_u) : (u) \subseteq (A_u) + (C_u) : (u) = (C_u) : (u) \subseteq (A_u) + (D_u) : (u) = (D_u) : (u)$, where A_u, B_u and C_u are the sets defined in 3.1–3.3. Obviously, an independent set of $(D_u) : (u)$ is also an independent set of $(C_u) : (u)$. However, a maximal independent set of $(D_u) : (u)$ needs not to be maximal for $(C_u) : (u)$. There are many sets V such that $Y_{\mathcal{J}^{(V)},u}$ is maximal independent set of the monomial ideal $(D_u) : (u)$ for all $u \in V$. If, nevertheless, we have $\mathcal{J}^{(V)} \notin \max\left(\mathbb{M}_{(V,\lhd)}\right)$ we can consider the non-maximality as a consequence of the property of Janet divisions that all elements of V have to be pairwise not Janet divisor of each other. But the following example shows that there exist also sets V for which even the maximality of $Y_{\mathcal{J}^{(V)},u}$ for $(D_u) : (u)$ does not hold for any $u \in V$. E.g., consider the set $V = \{x_1x_3, x_1x_2^2x_4, x_1^2x_2^2\}$ in four indeterminates. We have $Y_{\mathcal{J}^{(V)},x_1x_3} = \{x_3, x_4\}$. But $\{x_1, x_3, x_4\} \supset Y_{\mathcal{J}^{(V)},x_1x_3}$ is independent for $(D_{x_1x_3}) : (x_1x_3) = (x_1x_2^2, x_2^2x_4) = (x_1, x_4) \cap (x_2^2)$, too.

4.3. Thomas Division

Similar as the Janet division also the Thomas division is a function $\tau : Pow(T) \to \mathbb{M}_\emptyset$ assigning to each subset $V \subseteq T$ an involutive division $\tau(V) = \mathcal{T}^{(V)} \in \mathbb{M}_V$ which is admissible for V.

Definition 4.3. (c.f. (Th37),(GB96)) *Let $V \subseteq T$ be a set of terms. For each $v \in V$ define $Y_{\mathcal{T}^{(V)},v} := \{x_i \mid \forall u \in V \ \deg_i u \le \deg_i v\}$. The involutive division $\mathcal{T}^{(V)} = \left(T_u^{(V)}\right)_{u \in T}$, where $T_u^{(V)} = u \cdot \langle Y_{\mathcal{T}^{(V)},u}\rangle$ for all $u \in V$ and $T_u^{(V)} = Id_T(u)$ for all $u \notin V$, is called the* Thomas division supported on V.

Theorem 4.3. *Let $V \subseteq T$ be a set of terms and $\sqsubset$ an ordering of V satisfying $u \sqsubseteq v$ for all $u, v \in V$ such that $v \mid u$. Then :*

i) $\mathcal{T}^{(V)}$ is admissible for $(V, \sqsubset)$,
ii) the sets $T_v^{(V)}$, $v \in V$, are pairwise disjoint, and
iii) $\mathcal{T}^{(V)} \le \mathcal{M}$ for any $\mathcal{M} \in$ submax $(\mathbb{M}_{(V,\sqsubset)})$.

Proof. Let A_v and B_v be the sets defined in 3.1 and 3.2. Similar to the case of Janet divisions we have $T_v^{(V)} \cap V = \{v\}$. Again, it follows $A_v = \emptyset$ for all $v \in V$. Consider arbitrary $x_i \in X$ and $v \in V$ such that $x_i \in Y_{\mathcal{T}^{(V)},v}$. Then $x_i \nmid \frac{lcm(u,v)}{v}$ for all $u \in V$ according to Definition 4.3. The assumption on $\sqsubset$ ensures that $u \nmid v$ for all $u \in B_v$, hence, $1 \notin (B_v) : (v)$ for all $v \in V$. In summary, we deduce $Y_{\mathcal{T}^{(V)},v} \subseteq Z$ for any maximal independent set Z of $(A_v) + (B_v) : (v)$ and the properties *i)* and *ii)* follow immediately.

iii) Let $\mathcal{M} \in \operatorname{submax}(\mathbb{M}_{(V,\sqsubset)})$ be generated by $(Y_u)_{u\in T}$ and let $A_v^{\mathcal{M}}$ and $C_v^{\mathcal{M}}$ be the sets defined in 3.1 respectively 3.3 which belong to $\mathcal{M}$. Furthermore, define $D_v^{\mathcal{M}} := \{u \in V \mid u \sqsubset v\}$ for all $v \in V$. Applying the same arguments as above we observe $Y_{\mathcal{T}^{(V)},v} \subseteq Z$ for all $v \in V$ and all maximal independent sets Z of $(D_v^{\mathcal{M}}) : (v) \supseteq (C_v^{\mathcal{M}}) : (v)$. Let $x_i \in A_v^{\mathcal{M}}$. There exists $u \in V$ such that $v \sqsubset u$, $v \in M_u$ and $x_i \notin Y_u$. It follows $u \mid v$ and $\deg_i u = \deg_i v$. Since v has only finitely many divisors there must exist a with respect to $\sqsubset$ maximal term u satisfying the above conditions. For this maximal term u we have $x_i \notin A_u^{\mathcal{M}}$, consequently, $Y_u \cup \{x_i\}$ is independent set for $(A_u^{\mathcal{M}})$. $Y_u \cup \{x_i\}$ is dependent set for $(A_u^{\mathcal{M}}) + (C_u^{\mathcal{M}}) : (u)$ because of the submaximality of $\mathcal{M}$. Hence, $Y_u \cup \{x_i\}$ is dependent for $(C_u^{\mathcal{M}}) : (u)$. Consequently, $x_i \notin Y_{\mathcal{T}^{(V)},u}$ and it follows $x_i \notin Y_{\mathcal{T}^{(V)},v}$ since $\deg_i u = \deg_i v$. In conclusion, $Y_{\mathcal{T}^{(V)},v} \cap A_v^{\mathcal{M}} = \emptyset$.

In summary, we have $Y_{\mathcal{T}^{(V)},v} \subseteq Z$ for any $v \in V$ and any maximal independent set Z of $(A_v^{\mathcal{M}}) + (C_v^{\mathcal{M}}) : (v)$, in particular, $Y_{\mathcal{T}^{(V)},v} \subseteq Y_v$. □

Note the following property of the Thomas division.

LEMMA 4.3. *Let $\mathcal{M}$ be the involutive division generated by $(Y_u)_{u\in T}$ and $V \subset T$ a non-empty, finite set of terms. If $\mathcal{T}^{(V)} \leq \mathcal{M}$ then $x_i v \mid lcm(V)$ for all $v \in V$ and $x_i \in X\backslash Y_v$, where $lcm(V)$ denotes the least common multiple of all elements of V.*

PROOF. $x_i \in X\backslash Y_v \subseteq X\backslash Y_{\mathcal{T}^{(V)},v}$ implies the existence of $u \in V$ such that $\deg_i v < \deg_i u$ and the claim follows immediately. □

Any permutation π of X extends to a reverse lexicographical ordering $\lhd_\pi$ and analogously to Definition 4.2 we can define the Janet division $\mathcal{J}^{(V,\pi)}$ corresponding to $\lhd_\pi$ supported on V. We have the equality

$$\mathcal{T}^{(V)} = \inf_{\pi} \mathcal{J}^{(V,\pi)} \quad ,$$

where π ranges over all permutations of X.

5. Involutive Bases

In the following we repeat the ideas of Section 2 for building up the theory of Gröbner bases. But now, we allow only $\mathcal{M}$-multiples and $\mathcal{M}$-divisors.

DEFINITION 5.1. *Let $\prec$ be an admissible term order, $F \subseteq R$ a set of polynomials, and $\mathcal{M} = (M_u)_{u\in T}$ an involutive division which is admissible for* lt F. *The polynomial $h \in R$ is called* $\mathcal{M}$-irreducible *modulo F and $\prec$ if*

$$\operatorname{supp} h \cap \bigcup_{0\neq f\in F} M_{\operatorname{lt} f} = \emptyset \quad .$$

We say that h $\mathcal{M}$-reduces to h' modulo F and $\prec$ if there exist $v \in T$, $c \in \mathbb{K}$ and $f \in F$ such that $h' = h + cvf$ and $v \cdot \operatorname{lt} f \in M_{\operatorname{lt} f} \cap (\operatorname{supp} h \backslash \operatorname{supp} h')$. A $\mathcal{M}$-irreducible polynomial g obtained by iterated $\mathcal{M}$-reduction of h modulo F and $\prec$ is called a $\mathcal{M}$-normal form *of h modulo F and $\prec$.*

Under the assumption that $M_{\operatorname{lt} f} \cap M_{\operatorname{lt} g} = \emptyset$ for all polynomials $f \neq g$ from F it is easy to observe that every polynomial $h \in R$ has a uniquely determined $\mathcal{M}$-normal form modulo F and $\prec$. Moreover, the mapping assigning each polynomial its $\mathcal{M}$-normal form modulo F and $\prec$ is a linear function.

Definition 5.2. *Let $\prec$ be an admissible term ordering, $F \subseteq R$ a set of polynomials, and $\mathcal{M} = (M_u)_{u\in T}$ an involutive division which is admissible for* $\operatorname{lt} F$.

The set F is called $\mathcal{M}$-reduced *with respect to $\prec$ if $0 \notin F$ and all sets $M_{\operatorname{lt} f}$, $f \in F$, are pairwise disjoint. If, in addition,* $\operatorname{lc} f = 1$ *and* $\operatorname{supp} f \cap \bigcup_{f\neq g\in F} M_{\operatorname{lt} g} = \emptyset$ *for all $f \in F$ then F is called* totally $\mathcal{M}$-reduced *with respect to $\prec$.*

If for every non-zero polynomial $g \in I$ there exists $f \in F$ such that $\operatorname{lt} g \in M_{\operatorname{lt} f}$ *then F is called a* $\mathcal{M}$-involutive basis with respect to $\prec$ *of the ideal I generated by F. A $\mathcal{M}$-involutive basis F of I with respect to $\prec$ which is (totally) $\mathcal{M}$-reduced with respect to $\prec$ is called a* (totally) reduced $\mathcal{M}$-involutive basis *of I with respect to $\prec$.*

Remark 5.1. *Let F be a set of non-zero polynomials, $I \subseteq R$ the ideal generated by F, and $\prec$ an admissible term ordering. Furthermore, let $\mathcal{M}$ be an involutive division which is admissible for* $\operatorname{lt} F$. *Note the following obvious but useful facts:*

- *i) If F is $\mathcal{M}$-involutive basis of I with respect to $\prec$ then it is also a Gröbner basis of I with respect to $\prec$.*
- *ii) If F is a $\mathcal{N}$-involutive basis of I with respect to $\prec$ for some $\mathcal{N} \leq \mathcal{M}$ then it is also a $\mathcal{M}$-involutive basis of I with respect to $\prec$.*
- *iii) F is a $\mathcal{M}$-involutive basis of I with respect to $\prec$ if and only if each polynomial $g \in I$ has $\mathcal{M}$-normal form 0 modulo F and $\prec$.*
- *iv) If F is $\mathcal{M}$-involutive basis of I with respect to $\prec$ then there exists a subset $G \subseteq F$ which is reduced $\mathcal{M}$-involutive basis of I with respect to $\prec$. Moreover, if there exists a $\mathcal{M}$-involutive basis of I with respect to $\prec$ then there exists a uniquely determined totally reduced $\mathcal{M}$-involutive basis of I with respect to $\prec$. Furthermore, all reduced $\mathcal{M}$-involutive bases of I with respect to $\prec$ contain the same number of elements and have the same sets of leading terms with respect to $\prec$.*
- *v) F is a $\mathcal{M}$-involutive basis of I with respect to $\prec$ if and only if*

$$Id_T(\operatorname{lt} I) = \bigcup_{f\in F} M_{\operatorname{lt} f} \quad .$$

  If, in addition, F is $\mathcal{M}$-reduced with respect to $\prec$ then the union on the right hand side of the equation is disjoint.

A main problem in the theory of Gröbner bases consists in the fact that a given term $u \in Id_T(\operatorname{lt} F)$ can have more than only one divisor in $\operatorname{lt} F$. In the case of involutive divisions we are faced with the opposite problem, namely, that it is possible that $u \in Id_T(\operatorname{lt} F)$ has no $\mathcal{M}$-divisors in $\operatorname{lt} F$. The philosophy of the Gröbner test algorithm is to check that the least common multiples of elements of $\operatorname{lt} F$ have uniquely determined normal forms. Analogously, the test for the $\mathcal{M}$-involutive basis property consists in checking the existence of involutive divisors for minimal critical terms belonging to $Id_T(\operatorname{lt} F)$.

Theorem 5.1. *Let F be a set of non-zero polynomials, $I \subseteq R$ the ideal generated by F, and $\prec$ an admissible term order. Furthermore, let the involutive division $\mathcal{M} = (M_u)_{u\in T}$ generated by $(Y_u)_{u\in T}$ be such that* $\operatorname{lt} F$ *is $\mathcal{M}$-reduced with respect to $\prec$ and let $\sqsubset$ be an arbitrary ordering of* $\operatorname{lt} F$ *for which $\mathcal{M}$ is admissible for* $(\operatorname{lt} F, \sqsubset)$. *Then the following conditions are equivalent:*

i) F *is a* $\mathcal{M}$*-involutive basis of* I *with respect to* $\prec$.

ii) *For all* $f \in F$ *and* $x \in X \backslash Y_{\mathrm{lt} f}$ *the product* xf *has* $\mathcal{M}$*-normal form* 0 *modulo* F *and* $\prec$.

iii) *For every* $f \in F$ *and every* $x \in X \backslash Y_{\mathrm{lt} f}$ *there exists* $f' \in F$ *such that the following conditions are satisfied:* $\mathrm{lt}\, f' \sqsubset \mathrm{lt}\, f$, $\mathrm{lt}\, f' \mid x \cdot \mathrm{lt}\, f$, *and the S-polynomial of* f *and* f' *has a representation* $Spol(f,f') = \sum_{i=1}^{m} h_i f_i$, *where* $0 \neq h_i \in R$, $f_i \in F$, *and* $\mathrm{lt}(h_i f_i) \prec x \cdot \mathrm{lt}\, f$ *for all* $i = 1, \ldots, m$.

iv) F *is a Gröbner basis of* I *with respect to* $\prec$ *and* $X \cdot \mathrm{lt}\, F \subseteq \bigcup_{f \in F} M_{\mathrm{lt} f}$.

Proof. The implications *i)* $\Rightarrow$ *ii)* $\Rightarrow$ *iii)* are trivial.

iii) $\Rightarrow$ *i)* For $u \in T$ let I_u be the additive subgroup of I consisting of all polynomials $g \in I$ which can be represented in the form $g = \sum_{i=1}^{m} h_i f_i$, where $0 \neq h_i \in R$, $f_i \in F$, and $\mathrm{lt}(h_i f_i) \prec u$ for all $i = 1, \ldots, m$. We remark that the family $(I_u)_{u \in T}$ is a R-module filtration of I. Without loss of generality let us assume $\mathrm{lc}\, f = 1$ for all $f \in F$.

For each term $t \in Id_T(\mathrm{lt}\, F)$ we define the set $G_t := \{g \in F \ : \ \mathrm{lt}\, g \mid t\}$. Since F is $\mathcal{M}$-reduced with respect to $\prec$ the leading terms of the elements of F are pairwise different and, hence, each G_t is a non-empty finite subset of F containing a uniquely determined element g_t of minimal leading term with respect to $\sqsubset$. Set $v_t := \frac{t}{\mathrm{lt}\, g_t}$.

Assume $v_t \notin \langle Y_{\mathrm{lt}(g_t)} \rangle$. Then there exists $y \in X \backslash Y_{\mathrm{lt}(g_t)}$ dividing v_t. From *iii)* it follows the existence of $g \in F$ such that $\mathrm{lt}\, g \sqsubset \mathrm{lt}\, g_t$ and $\mathrm{lt}\, g \mid y \cdot \mathrm{lt}\, g_t \mid t$ in contradiction to the choice of g_t. In conclusion,

$$v_t \in \langle Y_{\mathrm{lt}(g_t)} \rangle \quad . \tag{5.1}$$

Next, we will show

$$uf - v_t g_t \in I_t \tag{5.2}$$

for all $f \in G_t$ and $u = \frac{t}{\mathrm{lt}\, f}$. The finiteness of G_t allows induction on $\mathrm{lt}\, f$ with respect to $\sqsubset$. If $\mathrm{lt}\, f$ is minimal with respect to $\sqsubset$ then $f = g_t$ and the membership (5.2) is obvious. Otherwise, there exists $y \in X \backslash Y_{\mathrm{lt} f}$ dividing u since F is $\mathcal{M}$-reduced. Condition *iii)* implies the existence of f' such that $\mathrm{lt}\, f' \sqsubset \mathrm{lt}\, f$, $\mathrm{lt}\, f' \mid y \cdot \mathrm{lt}\, f \mid t$, and $Spol(f,f') = yf - wf' \in I_{y \cdot \mathrm{lt}\, f}$, where $w \in T$ satisfies $y \cdot \mathrm{lt}\, f = w \cdot \mathrm{lt}\, f'$. We have $\frac{u}{y} wf' - v_t g_t \in I_t$ according to the induction hypothesis. Hence, $uf - v_t g_t = \frac{u}{y} wf' - v_t g_t + \frac{u}{y} Spol(f,f') \in I_t$.

Now, consider an arbitrary non-zero element $h \in I$ and let $d \in T$ be the uniquely determined term such that $h \in I_d$ and $h \notin I_s$ for all $s \prec d$. Then $h = \sum_{i=1}^{m} c_i u_i f_i$, where $0 \neq c_i \in \mathbb{K}$, $u_i \in T$, $f_i \in F$, and $u_i \cdot \mathrm{lt}\, f_i \prec d$ for all $i = 1, \ldots, m$. Let $t \in T$ be the maximal term among $u_i \cdot \mathrm{lt}\, f_i$, $i = 1, \ldots, m$. Define $J \subseteq \{1, \ldots, m\}$ such that $u_i \cdot \mathrm{lt}\, f_i = t$ if $i \in J$ and $u_i \cdot \mathrm{lt}\, f_i \prec t$ if $i \notin J$. By construction $h - \sum_{i \in J} c_i u_i f_i \in I_t$ and application of (5.2) to $u_i f_i$, $i \in J$, yields $h - \sum_{i \in J} c_i v_t g_t \in I_t$. From $h \notin I_t$ we deduce $\sum_{i \in J} c_i \neq 0$ and $\mathrm{lt}\, h = v_t \cdot \mathrm{lt}\, g_t$. Finally, using (5.1) we observe $\mathrm{lt}\, h \in M_{\mathrm{lt} g_t}$. In conclusion, F is a $\mathcal{M}$-involutive basis of I with respect to $\prec$.

The trivial observations *i)* $\Rightarrow$ *iv)* $\Rightarrow$ *iii)* complete the proof. □

The equivalence of the conditions *i)* and *ii)* is the fundamental idea for the construction of involutive bases. Note, that this equivalence fails if we require only that the sets $M_{\mathrm{lt} f}$ are pairwise disjoint instead of the stronger condition that F has to be $\mathcal{M}$-reduced which additionally implies that $\mathcal{M}$ is admissible for $\mathrm{lt}\, F$. Figure 3 presents an algorithm for testing whether a finite generating set F is a $\mathcal{M}$-involutive basis with respect to $\prec$.

Figure 3. Algorithm for checking the $\mathcal{M}$-basis property

<u>Input:</u>
  F $\cdots$ finite set of non-zero polynomials generating the ideal $I \subseteq R$
  $\mathcal{M} = (u \cdot \langle Y_u \rangle)_{u \in T}$ $\cdots$ involutive division admissible for $(\operatorname{lt} F, \sqsubset)$
  $\prec$ $\cdots$ admissible term ordering
<u>Output:</u>
  $g \in I$ $\cdots$ a polynomial which is $\mathcal{M}$-irreducible modulo F and $\prec$
  and $g = 0$ if and only if F is $\mathcal{M}$-involutive basis of I

compute a minimal subset $K \subseteq F$ such that $\operatorname{lt} K = \operatorname{lt} F$
$H := \left\{ g \in K \mid \forall f \in K \backslash \{g\} : \operatorname{lt} g \notin M_{\operatorname{lt} f} \right\}$
$L := \{(1,h) \mid h \in F \backslash H\} \cup \{(y,h) \mid h \in H, y \in X \backslash Y_{\operatorname{lt} h}\}$
while $L \neq \emptyset$ *do*
  choose $(u,h) \in L$ such that $u \cdot \operatorname{lt} h$ is minimal with respect to $\prec$
  $L := L \backslash \{(u,h)\}$
  $g := \mathcal{M}$-normal_form(uh) modulo H with respect to $\prec$
  if $g \neq 0$ **then** return(g) **end if**
end while
return(0)

It follows a sketch of the termination and correctness proofs. Termination follows from finiteness of L. So, let us consider correctness. By construction H is a maximal subset of F such that the sets $M_{\operatorname{lt} g}$, $g \in H$, are pairwise disjoint. H generates a subideal J of I. If the algorithm returns $g \neq 0$ then $g \in I$ is $\mathcal{M}$-irreducible modulo H and $\prec$. By construction of H the polynomial g is also $\mathcal{M}$-irreducible modulo F, hence, the answer is correct. Assume the result is 0. Then H is a $\mathcal{M}$-involutive basis of J with respect to $\prec$ according to Theorem 5.1. Furthermore, $J = I$ and it follows correctness.

Lemma 5.1. *Let $H \subset R$, $\prec$ an admissible term ordering, f a non-zero polynomial, and $\mathcal{M}$ the involutive division generated by $(Y_u)_{u \in T}$. Assume that $\mathcal{M}$ is admissible for $(\operatorname{lt} H, \sqsubset)$, H is $\mathcal{M}$-reduced and that for every $h \in H$ and every $y \in X \setminus Y_{\operatorname{lt} h}$ satisfying $y \cdot \operatorname{lt} h \preceq \operatorname{lt} f$ there exists $h' \in H$ such that $\operatorname{lt} h' \mid y \cdot \operatorname{lt} h$ and $\operatorname{lt} h' \sqsubset \operatorname{lt} h$. Then the $\mathcal{M}$-normal form g of f modulo H and $\prec$ is also a Gröbner normal form of f modulo H and $\prec$.*

Proof. It is sufficient to show that g is Gröbner-irreducible modulo H and $\prec$. Assume there exists $u \in \operatorname{supp} g \cap Id_T(\operatorname{lt} H)$ and let $h \in \{h' \in H \mid \operatorname{lt} h' \mid u\}$ be such that $\operatorname{lt} h$ is minimal with respect to $\sqsubset$. Since g is $\mathcal{M}$-irreducible modulo H and $\prec$ it follows $\frac{u}{\operatorname{lt} h} \notin \langle Y_{\operatorname{lt} h} \rangle$. So, let $y \in X \backslash Y_{\operatorname{lt} h}$ be a divisor of $\frac{u}{\operatorname{lt} h}$. We have $y \cdot \operatorname{lt} h \preceq u \preceq \operatorname{lt} g \preceq \operatorname{lt} f$. Hence, by assumption there exists $h' \in H$ such that $\operatorname{lt} h' \mid y \cdot \operatorname{lt} h \mid u$ and $\operatorname{lt} h' \sqsubset \operatorname{lt} h$ in contradiction to the minimal choice of h. Hence, $\operatorname{supp} g \cap Id_T(\operatorname{lt} H) = \emptyset$ and the claim follows. □

Corollary 5.1. *Let g be the polynomial returned by Algorithm 3 for input F,$\mathcal{M}$,$\prec$. If $g \neq 0$ then either $\operatorname{lt} g \notin (\operatorname{lt} F)$ or there exist $h \in F$ and $y \in X \backslash Y_{\operatorname{lt} h}$ such that $\operatorname{lt} g = y \cdot \operatorname{lt} h$.*

Proof. We use the notations of Algorithm 3. Let $(u,h) \in L$ be the pair considered last before termination, i.e g is $\mathcal{M}$-normal form of uh modulo F and $\prec$. In the case $u \cdot \operatorname{lt} h = \operatorname{lt} g$ it must hold $u \neq 1$ and the assertion is obvious.

Figure 4. Computation of involutive bases

```
Input:
      F   ···  finite generating set of the ideal I ⊆ R
      ≺   ···  admissible term ordering
Output:
      G and M such that G is M-involutive basis of I with respect to ≺
G :=GAUSS(F)
choose M ∈ 𝕄_{lt G} such that T^(lt G) ≤ M
while g :=CHECK(G, M, ≺) ≠ 0 do
      G := G ∪ {g}
      choose M ∈ 𝕄_{lt G} such that T^(lt G) ≤ M
end while
return(G, M)
```

Otherwise, $\operatorname{lt} g \prec u \cdot \operatorname{lt} h$. From Lemma 5.1 and the assumptions on the selection strategy for choosing the elements from L it follows that the $\mathcal{M}$-normal form of g modulo H and $\prec$ is also a Gröbner normal form of g modulo H and $\prec$. But g is $\mathcal{M}$-irreducible modulo H and $\prec$, hence, $\operatorname{lt} g \notin (\operatorname{lt} H) = (\operatorname{lt} F)$. $\square$

Let F,$\mathcal{M}$ and $\prec$ satisfy the input specification of Algorithm 3. Assume that the algorithm returns $g \neq 0$. The natural approach to force the zero-reduction of g is to add the polynomial g to the generating set F. However, in general $\mathcal{M}$ will not be admissible for $\operatorname{lt}(F \cup \{g\})$.

One possible solution is to choose $\mathcal{M}$ such that it is admissible for a set $V \subseteq T$ which is large enough to contain all leading terms of polynomials added to F during the completion process, e.g. the Pommaret method is of this type. In general, there is no essentially better a priori choice than $V = T$. It is well-known that an ideal needs not to have a finite Pommaret basis and according to Remark 5.1 and Theorem 4.1 the same is true at least for any $\mathcal{M} \in \mathbb{M}_{(T,\sqsubset)}$, where $\sqsubset$ is a multiplication compatible ordering. Hence, we learned that a completion process based on a fixed involutive division admissible for T will not terminate, in general. Note, however, that finite parametrizations of Pommaret bases can be computed in an algorithmic way (see (Ap96)).

An alternative approach consists in the generalisation of the ideas beyond the theories of Janet and Thomas bases, i.e. in adjusting the involutive division in each step to the enlarged generating set. Figure 4 presents the global structure of such a completion algorithm. The function CHECK calls Algorithm 3. The function GAUSS performs Gaussian autoreduction on the elements of F considered as elements of the $\mathbb{K}$-vector space $R = \mathbb{K}[X]$, i.e. G is a triangular system generating the same subvector space as F. The preparatory Gaussian autoreduction is optional and does not effect correctness or termination, but by this means we ensure that the leading terms of elements of G will be pairwise different during the whole run of the algorithm, in particular, $K = G$ for each execution of the CHECK-function.

The correctness of the method presented in Figure 4 is obvious. Let us consider the question of termination. Let G_ν be the value of G before the ν-th run of the while loop. The increasing polynomial ideal sequence $(\operatorname{lt} G_1) \subseteq (\operatorname{lt} G_2) \subseteq \cdots \subseteq (\operatorname{lt} G_\nu) \subseteq \cdots$ must become stationary since R is a Noetherian ring. Let ν_0 be such that $(\operatorname{lt} G_\nu) = (\operatorname{lt} G_{\nu_0})$ for all $\nu > \nu_0$. From Lemma 4.3 and Corollary 5.1 we deduce $lcm(\operatorname{lt} G_\nu) = lcm(\operatorname{lt} G_{\nu_0})$ for all $\nu > \nu_0$ and it follows that the sequence $G_{\nu_0} \subset G_{\nu_0+1} \subset \cdots$ must be finite. Hence, Algorithm 4 terminates.

6. Improvements and Heuristics

It is well-known that time and space behaviour of Buchberger's algorithm are very sensitive against selection strategies and applications of criterions (c.f. (Bu85) and (G&91)). Certainly, the same applies to the involutive basis algorithm and a lot of computer experiments will be necessary in order to tune Algorithm 4.

The strategies proposed in (ZB93) and (GB96), which proved to be fast in the experiments reported there, can be found as instantiation of our theory in the following way. If we choose always $\mathcal{M} = \mathcal{J}^{(\,\mathrm{lt}\, G)}$ or $\mathcal{M} = \mathcal{T}^{(\,\mathrm{lt}\, G)}$, respectively, then we obtain the Janet and Thomas methods as instantiations of our algorithm. The Pommaret method is not covered directly. This is not surprising since the Pommaret method is known to be non-terminating, in general. But we will indicate that there are variants of our algorithm which for arbitrary input F and $\prec$ are at least not worse than the Pommaret method.

We will discuss some of the freedoms contained in the Algorithms 3 and 4. Most of them appear in Buchberger's algorithm in a similar way and will be discussed only briefly. We aim our intention mainly at an absolute new question, namely, the choice of the involutive division. The central results are summarised in the Remarks 6.1 and 6.2. They are based widely on an exact cost analysis and improve the average behaviour of Algorithm 4 drastically.

6.1. Selection of $\mathcal{M}$

We will discuss a selection strategy for $\mathcal{M}$ from the point of view of keeping the number of reductions small and avoiding multiple reductions. But similar to selection problems in the theory of Gröbner bases also here we will not be able to present a general strategy which is optimal for all inputs. For any part of our strategy there are particular counter examples for which alternative strategies would be faster. So, in order to justify our strategy it is necessary to perform further investigations and tests which give an impression on the average behaviour of our strategy.

First of all, let us consider the statical dependencies on the generating set G of I and ask for an involutive division $\mathcal{M}$ refining the Thomas division supported on $\mathrm{lt}\, G$ such that the chance for G being a $\mathcal{M}$-involutive basis of I is high and the costs for the involutive basis check are low.

Let $\mathcal{M}$ and $\mathcal{N}$ be two involutive divisions admissible for $\mathrm{lt}\, G$ satisfying $\mathcal{T}^{(\,\mathrm{lt}\, G)} \leq \mathcal{N} < \mathcal{M}$. Then by condition *ii)* of Remark 5.1 it follows that the probability for G being a $\mathcal{M}$-involutive basis is higher than for G being a $\mathcal{N}$-involutive basis. Let $H_{\mathcal{M}}$ and $H_{\mathcal{N}}$ be the maximal subsets of G which are $\mathcal{M}$-reduced or $\mathcal{N}$-reduced, respectively. If $H_{\mathcal{M}} = H_{\mathcal{N}}$, e.g. if $H_{\mathcal{M}} = G$, then the set L appearing in Algorithm 3 for input $\mathcal{M}$ is a subset of that for input $\mathcal{N}$. Hence, in case of success, the check for $\mathcal{M}$ is performed faster. Now, consider the case $H_{\mathcal{N}} \neq H_{\mathcal{M}}$, i.e. $H_{\mathcal{M}} \subset H_{\mathcal{N}}$. We observe that the number of elements contained in L is smaller for $\mathcal{M}$ than for $\mathcal{N}$. Furthermore, any $\mathcal{N}$-reduction sequence is also a $\mathcal{M}$-reduction sequence and, hence, $\mathcal{N}$-reduction can be considered as a particular $\mathcal{M}$-reduction strategy. Applying this strategy the situation becomes similar to the case $H_{\mathcal{N}} = H_{\mathcal{M}}$. Next, let us consider the problem of deciding between $\mathcal{M}$ and $\mathcal{N}$ from a dynamic point of view. If G is not a $\mathcal{M}$-involutive basis then the decision for $\mathcal{M}$ or $\mathcal{N}$, respectively, will influence the future behaviour of the completion algorithm. There is a certain similarity between this behaviour and that based on the question whether or not to consider a critical pair which could be skipped according to Buchberger's second criterion. In the latter case it turned out that the application of the criterion is strongly advisable in most cases. In summary , we propose to choose $\mathcal{M}$ only among the submaximal involutive divisions admissible for $\operatorname{lt} G$. Since, at least using the algorithms discussed in this paper, the computation of maximal refinements is much more costly than that of submaximal ones it needs experimental calculations in order to decide whether a further restriction to only maximal involutive divisions is preferable. One should also estimate how often Algorithm 2 produces already a maximal refinement and would be followed only by a costly confirmation procedure.

In the following we deal with another dynamic feature, namely, the dependency of the choice of $\mathcal{M}$ from the history of the completion process. The changes of the involutive divisions should be "smooth" in order to carry over as many as possible zero-reductions from one intermediate basis check to a succeeding one. Let G be the generating set of I and $\mathcal{M}$ the corresponding involutive division at some intermediate state of Algorithm 4. Assume that uh, where $(u,h) \in L$, had $\mathcal{N}$-normal form 0 modulo G' and $\prec$ for a previous intermediate generating set $G' \subset G$ and the corresponding involutive division $\mathcal{N}$ admissible for $\operatorname{lt} G'$. Then the polynomial uh needs not to have $\mathcal{M}$-normal form 0 modulo G and $\prec$. There are counter examples even in the classical cases of Janet or Thomas division. So, it needs more than only condition *ii)* of Theorem 5.1 in order to prove that it is sufficient to consider a pair (u,h) only once during an involutive completion process.

Remark 6.1. *Fix a term ordering $\sqsubset$ satisfying $u \mid v \Rightarrow v \sqsubseteq u$, e.g. $\sqsubset = \lhd$. We modify the algorithm presented in Figure 4 by considering only such involutive divisions which are admissible for $(\operatorname{lt} G, \sqsubset)$. Furthermore, we modify the* check*-subroutine by removing all pairs (u,h) from L which have been considered previously.*

Let us consider termination and correctness of the modified algorithm. Termination follows in the same way as for the original algorithm since the assumptions of Lemma 5.1 remain valid and, hence, the validity of Corollary 5.1 is maintained. Let G and $\mathcal{M}$ be the result returned by the modified algorithm for input F and $\prec$. Furthermore, let H be the maximal $\mathcal{M}$-reduced subset of G. In order to show correctness we start with the proof that any element $f \in G\backslash H$ can be represented in the form

$$f = \sum_{i=1}^{k} h_i g_i \quad , \text{ where } h_i \in R\backslash\{0\}, g_i \in H, \text{ and } \operatorname{lt}(h_i g_i) \preceq \operatorname{lt} f. \tag{6.1}$$

The modified algorithm ensures that $(1,f)$ has been considered during a run of the check-subroutine. The reduction yields a representation $f = \sum_{i=1}^{k} h_i g_i$, where $0 \neq h_i \in R$, $g_i \in G$, $\operatorname{lt}(h_i g_i) \preceq \operatorname{lt} f$. Suppose $\operatorname{lt} f = \operatorname{lt} g_i$ for some $1 \leq i \leq k$ then $f = g_i$ since G is Gaussian autoreduced. But in contradiction to $(1,f) \in L$ this would mean that f was involutively irreducible at check time. Hence, $\operatorname{lt} g_i \prec \operatorname{lt} f$ for all $i = 1,2,\ldots,k$. If the leading term of f is minimal with respect to $\prec$ among all leading terms of elements of $G\backslash H$ then the above representation is already of type (6.1). Applying induction on $\operatorname{lt} f$ with respect to $\prec$ proves the existence of representations of type (6.1) for arbitrary $f \in G\backslash H$.

Next let us show that H satisfies condition *iii)* of Theorem 5.1. Let $f \in H$ and $x \in X\backslash Y_{\operatorname{lt} f}$. The modified algorithm ensures that there exist G' and $\mathcal{N}$ such that a $\mathcal{N}$-normal form of xf modulo G' and $\prec$ has been computed during the execution of

CHECK(G',$\mathcal{N}$,$\prec$). If $\mathrm{lt}(xf)$ is $\mathcal{N}$-irreducible modulo G' and $\prec$ then $\mathrm{lt}\ g = x \cdot \mathrm{lt}\ f$, where g is the result of CHECK(G',$\mathcal{N}$,$\prec$). Hence, $g \in G$, $\mathrm{lt}\ g \mid x \cdot \mathrm{lt}\ f$, and $\mathrm{lt}\ g \sqsubset \mathrm{lt}\ f$. Otherwise, there exists $g \in G'$ such that $x \cdot \mathrm{lt}\ f \in N_{\mathrm{lt} g}$ and $\mathrm{lt}\ g \notin N_{\mathrm{lt} g'}$ for all $g' \in G' \backslash \{g\}$. Again, we have $g \in G$, $\mathrm{lt}\ g \mid x \cdot \mathrm{lt}\ f$, and $\mathrm{lt}\ g \sqsubset \mathrm{lt}\ f$. In any case, keeping track of the $\mathcal{N}$-reduction of xf modulo G' and $\prec$ provides a representation $Spol(f, g) = \sum_{i=1}^{k} h_i g_i$, where $0 \neq h_i \in R$, $g_i \in G$, and $\mathrm{lt}(h_i g_i) \prec x \cdot \mathrm{lt}\ f$, of the S-polynomial of f and g in terms of G'. Finally, substituting the elements $g_i \notin H$ according to (6.1) shows that H, $\mathcal{M}$, $\prec$, and $\sqsubset$ satisfy condition *iii)* of Theorem 5.1. In conclusion, H and G are $\mathcal{M}$-involutive bases of $(H) = (G) = I$ with respect to $\prec$. □

So, we observed that we can avoid a lot of multiple reductions using the modified algorithm described in Remark 6.1. As a byproduct the costs for choosing the involutive division $\mathcal{M}$ are reduced drastically. Note, however, the price we have to pay for the above advantages is that we can miss a fast way of completion or even do not realise that an intermediate basis is already a $\mathcal{M}$-involutive basis for some $\mathcal{M}$ which is admissible only for another ordering $\sqsubset$.

In order to benefit from the possibility to remove previously considered pairs from L we have to ensure that the considered pairs (u, h) will be contained in L also in the succeeding checks.

In the classical involutive situations described in Section 4 the involutive division $\mathcal{M}$ is chosen according to a function $\varphi : Pow(T) \to \mathbb{M}_{\emptyset}$ satisfying $\varphi(V) \in \mathbb{M}_{(V,\sqsubset)}$. We have $\varphi(V) = \mathcal{P}$ for all $V \subseteq T$ in the Pommaret case and $\varphi = \iota$ respectively $\varphi = \tau$ in the Janet or Thomas case. In all three situations the function φ is descending in the sense that $\varphi(V) \leq \varphi(W)$ for all $W \subseteq V \subseteq T$. Also the involutive divisions investigated by Gerdt and Blinkov are of this type. The descending property ensures that any pair (x_i, h) contained in L for some intermediate check will be also a member of L for any succeeding check in which $\mathrm{lt}\ h$ is involutively irreducible modulo $\mathrm{lt}(G \backslash \{h\})$ and $\sqsubset$. But, in general, the selection strategy $\mathcal{M} = \varphi(\mathrm{lt}\ G)$ will not be optimal since $\varphi(\mathrm{lt}\ G)$ needs not to be (sub-)maximal.

REMARK 6.2. *Let G and $\mathcal{N}$ be the values of G and $\mathcal{M}$ before the execution of the instruction computing a new $\mathcal{M}$ in Algorithm 4 modified according to Remark 6.1. We propose to choose $\mathcal{M}$ in such a way that $\mathcal{M} \in$ submax $(\mathbb{M}_{(\mathrm{lt}\ G,\sqsubset)})$ and, in addition, $\inf(\mathcal{M}, \mathcal{N})$ takes a maximal possible value.*

Let $\varphi : Pow(T) \to \mathbb{M}_{\emptyset}$, where $\varphi(V) \in \mathbb{M}_{(V,\sqsubset)}$, be an arbitrary fixed descending function, e.g. one belonging to one of the classical involutive divisions discussed in Section 4. Then the additional property $\varphi(\mathrm{lt}\ G) \leq \mathcal{M}$ can be ensured for all involutive divisions used during the completion process. In particular, we are able to simulate the classical situations. Nevertheless it is an interesting open question how to apply the whole freedom left by Remark 6.2 in order to utilise as much as possible information from a specific leading term ideal.

Let $u = x^2y^2z, v = xyz^2, s = xy^3z$, and $t = x^3z$. There are exactly two submaximal involutive divisions which are admissible for $(\{u, v\}, \lhd)$ and exactly one submaximal involutive division which is admissible for $(\{u, v, s\}, \lhd)$ or $(\{u, v, t\}, \lhd)$, respectively. It is easy to check that any function $\varphi : Pow(T) \to \mathbb{M}_{\emptyset}$, where $\varphi(V) \in$ submax $\left(\mathbb{M}_{(V,\lhd)}\right)$ for all $V \subseteq T$, can satisfy only one of the conditions $\varphi\{u, v, s\} \leq \varphi\{u, v\}$ or $\varphi\{u, v, t\} \leq \varphi\{u, v\}$. Hence, there does not exist any descending function φ of this type. Consequently, it is impossible to find a selection strategy for $\mathcal{M}$ which depends only on $\operatorname{lt} G$ and ensures submaximality of $\mathcal{M}$ as well as the total exploitation of all previously computed reductions.

The above investigations show that our concept is more flexible and more general than the restriction to descending functions φ.

6.2. Miscellaneous

There are a lot of similarities between the theories of involutive and Gröbner bases. So, it is natural to ask whether we can make use of at least some of the improvements well-known from the theory of Gröbner bases.

Full versa head reduction

If we apply head $\mathcal{M}$-reduction, i.e. there are allowed only such reduction steps which cancel the leading term, then we have to consider weak $\mathcal{M}$-normal forms g of f modulo H and $\prec$, i.e. g has to satisfy only $\operatorname{lt} g \notin \bigcup_{h \in H} M_{\operatorname{lt} h}$ instead of $\operatorname{supp} g \cap \bigcup_{h \in H} M_{\operatorname{lt} h} = \emptyset$. Neglecting the details we remark that Algorithm 4 with head reduction has to perform at least all the work which has to be done in a particular variant of Buchberger's algorithm for the same input F and $\prec$. Hence, such a version of the involutive basis algorithm cannot improve Buchberger's algorithm. Moreover, the tests reported in (G&91) indicate that the simulated version of Buchberger's algorithm is not advisable in most cases.

Autoreduction of intermediate bases

Let us discuss the question which type of autoreduction should be applied on intermediate generating sets G during Algorithm 4. Gaussian autoreduction, i.e. the weakest possible autoreduction, should be applied to the input generating set in a preparatory step. Then any subsequent intermediate basis will be automatically Gaussian autoreduced. Any other kind of autoreduction, e.g. $\mathcal{M}$-autoreduction, has to be checked for its compatibility with the used function for choosing the involutive divisions since redundance of leading terms is not invariant under changing the involutive division. There are counter examples which show that intermediate $\mathcal{M}$-autoreduction can destroy the termination of our method. Only at the end when we have computed already a $\mathcal{M}$-involutive basis then we can be sure that $\mathcal{M}$-autoreduction leads to a $\mathcal{M}$-reduced set, which is even a reduced $\mathcal{M}$-involutive basis of the input ideal. Besides the above theoretical reasons there are also experimental indications showing that intermediate autoreduction should be avoided (see (G&91)).

Selection of the reduction polynomial

In the case of involutive bases this problem is much less important than in Buchberger's algorithm. For $\mathcal{M}$-reduced sets G the question is even irrelevant since any term $t \in T$ will have at most one involutive divisor in $\operatorname{lt} G$.

Selection of $(u, h) \in L$

The use of the standard selection strategy, i.e. choosing the pairs such that $u \cdot \operatorname{lt} h$ is minimal with respect to $\prec$, in Algorithm 3 is essential for the termination property of the completion procedure. So, we guess that the practical importance of the involutive method is restricted to degree compatible term orderings $\prec$ until also other termination preserving selection strategies will be known.

Removing unnecessary pairs from L

There are presented criterions for detecting useless prolongations in (GB96) which should be checked in our context. Partial answers to this question can be found also in Section 6.1 of this paper.

6.3. Comparison with Buchberger's algorithm

Finally, let us discuss the author's conjecture on the major advantage of the involutive basis method in comparison to Buchberger's algorithm. According to (G&91) it is advisable to perform full reduction on S-polynomials and to avoid post reduction of old ideal generators. We have the following background. Let $f \in F$ be such that $\mathrm{lt}\, f \notin Id_T\,(\,\mathrm{lt}(F\backslash\{f\})\,)$ and let g be a polynomial obtained from f by application of some reduction steps modulo $F\backslash\{f\}$. The question is whether f or g should be applied in subsequent S-polynomial reductions. An argument for f is that it often contains less terms and has smaller coefficients than g. An argument against f is that the reductions not performed on f may cause the necessity of many additional subsequent reductions during a Gröbner basis calculation. However, there exist also counter examples showing the opposite behaviour for both arguments.

The strategy proposed in (G&91) is a compromise justified by computing experiments. But it seems that the same strategy, i.e. full reduction of new polynomials and no post reduction of old polynomials, applied in the involutive method provides the better compromise. The generating sets appearing in the involutive algorithm contain certain redundant higher degree ("younger") polynomials of an intermediate reduction state. Moreover, due to this redundancy we need to consider only the S-polynomials of a special simple type according to Theorem 5.1. It seems that the involutive strategy reduces the growth of the length of the intermediate polynomials as well as of their coefficient size.

Similar considerations as Mall's comparison of involutive and Gröbner method for homogeneous ideals (see (Ma95)) and the fact that a full $\mathcal{M}$-reduction of a S-polynomial is always also a full Gröbner reduction according to Lemma 5.1 indicate that the phenomenons explained above remains as the only possible advantage of the involutive method in comparison to Buchberger's algorithm.

7. Application to the Computation of Hilbert Functions

First of all, recall some well-known facts about Hilbert functions (c.f. (Re76) or any other textbook on commutative algebra). Let $S = \mathbb{K}[Y]$ be the polynomial ring in $Y \subseteq X$ over the field $\mathbb{K}$. Furthermore, let $Y = \{y_1, \ldots, y_k\}$, where the y_i are pairwise different. We extend the notion of binomial coefficients to arbitrary integers by defining $\binom{-1}{-1} := 1$ and $\binom{r}{s} := 0$ for all r, s such that $r < s$ or $r < 0$ or $s < 0$ but $(r,s) \neq (-1,-1)$. † Then S contains exactly

$$\Delta(m;k) = \binom{m+k-1}{k-1} \tag{7.1}$$

† The unusual setting $\binom{-1}{-1} = 1$ proves to be useful in the exceptional case $k = 0$, i.e. $S = \mathbb{K}$.

terms of total degree m. Let $I \subseteq S$ be a homogeneous polynomial ideal and $A_m \subseteq S/I$ the $\mathbb{K}$-vector space of all residue classes $[f]_I \in S/I$ of m-forms f modulo I. The function $\mathcal{H}(\,\cdot\,; I) : \mathbb{N} \to \mathbb{N}$ defined by $\mathcal{H}(m; I) = dim_{\mathbb{K}}(A_m)$ is called the Hilbert function of I. Furthermore, we define the volume function of I by

$$\mathcal{V}(m; I) := \Delta(m; k) - \mathcal{H}(m; I) \quad , m = 0, 1, \ldots \quad .$$

Let $L(I)$ be the monomial ideal generated by the set $\operatorname{lt} I$ of leading terms of elements of I with respect to an arbitrary total degree compatible term ordering $\prec$. I and $L(I)$ have the same Hilbert function. Furthermore, we have the connection

$$\mathcal{H}^a(m; I) = \sum_{i=0}^{m} \mathcal{H}(i; L(I)) \quad , m = 0, 1, \ldots \quad , \tag{7.2}$$

to the affine Hilbert function $\mathcal{H}^a$ of I. Note, that (7.2) is also valid for inhomogeneous ideals I and more general definitions of leading forms.

THEOREM 7.1. *Let $\mathcal{M}$ be the involutive division generated by $(Y_u)_{u \in T}$ and $V \subset T$ a finite $\mathcal{M}$-reduced set of terms. By k_v we denote the number of indeterminates contained in Y_v. If V is a $\mathcal{M}$-involutive basis of the ideal $I = (V) \subseteq R$ (with respect to an arbitrary admissible term ordering $\prec$) then we have*

$$\mathcal{V}(m; I) = \sum_{v \in V} \Delta\left(m - \deg v; k_v\right) = \sum_{v \in V} \binom{m - \deg v + k_v - 1}{k_v - 1}, \quad m \in \mathbb{N} \quad .$$

PROOF. According to *v)* of Remark 5.1 we have $Id_T(V) = \bigcup_{v \in V} M_v$, where the union on the right hand side is disjoint. The submonoid generated by Y_v contains $\Delta\left(m; k_v\right)$ terms of degree m. Taking into account the degree shift caused by the factor v it follows that $v \cdot \langle Y_v \rangle = M_v$ contains exactly $\Delta\left(m - \deg v; k_v\right)$ terms of degree m. In conclusion, we observed the first equality and the second follows immediately by Equation (7.1). □

Using the relationships listed above we obtain explicit formulaes and fast algorithms for the computation of the Hilbert function of homogeneous and the affine Hilbert function of arbitrary polynomial ideals I.

References

Apel, J. (1995). A Gröbner Approach to Involutive Bases. *J.Symb.Comp.* **19**/5, pp. 441–457.

Apel, J. (1996). The Computation of Gröbner Bases Using an Alternative Algorithm. To appear in Proc. Workshop on Symbolic Rewriting Techniques, Monte-Verita 1995.

Becker, T., Weispfenning, V., in cooperation with Kredel, H. (1993). Gröbner Bases, A Computational Approach to Commutative Algebra. Springer, New York, Berlin, Heidelberg.

Buchberger, B. (1965). Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal. PhD Thesis, Univ. of Innsbruck, Austria.

Buchberger, B. (1985). An Algorithmic Method in Polynomial Ideal Theory. Chapter 6 in: Recent Trends in Multidimensional System Theory (ed.: N.K. Bose), D. Reidel Publ. Comp.

Gerdt, V.P., Blinkov, Yu.A. (1996). Involutive Bases of Polynomial Ideals. Preprint 01/96, Naturwissenschaftlich-Theoretisches Zentrum, University of Leipzig.

Giovini, A., Mora, T., Niesi, G., Robbiano, L., Traverso, C. (1991). "One sugar cube, please," or Selection Strategies in the Buchberger Algorithm. In: Watt, S.M. (ed.), Proc. ISSAC'91, ACM Press, New York, pp. 49–54.

Janet, M. (1929). Lecons sur les systèmes d'equations aux dérivées partielles. Gauthier-Villars, Paris.

Mall, D. (1995). A Note on Pommaret Bases. submitted to J.Symb.Comp.

Nischke, K. Private communication about an implementation of involutive bases.

Pommaret, J.F. (1978). Systems of Partial Differential Equations and Lie Pseudogroups. Gordan and Breach, New York.

Renschuch, B. (1976). Elementare und praktische Idealtheorie. Deutscher Verlag der Wissenschaften, Berlin.

Seiler, W. (1994). On the arbitrariness of the general solution of an involutive partial differential equation. *J.Math.Phys.* **35**, pp. 486–498.

Thomas, J. (1937). Differential Systems. American Mathematical Society, New York.

Zharkov, A.Yu., Blinkov, Yu.A. (1993). Involution Approach to Solving Systems of Algebraic Equations. Proc. IMACS'93, pp. 11–16.