ОБЪЕДИНЕННЫЙ
ИНСТИТУТ
ЯДЕРНЫХ
ИССЛЕДОВАНИЙ

Дубна

E5-98-150

V.P.Gerdt[1], M.Berth[2], G.Czichowski[2]

INVOLUTIVE DIVISIONS IN *MATHEMATICA*: IMPLEMENTATION AND SOME APPLICATIONS

Submitted to the Sixth Rhein Workshop on Computer Algebra,
March 31–April 3, 1998, Sankt-Augustin, Germany

---

[1]E-mail: gerdt@jinr.ru
[2]Department of Mathematics and Informatics, University of Greifsward, Germany;
E-mail: berth@rz.uni-greifswald.de;
E-mail: czicho@rz.uni-greifswald.de

1998

1 Introduction

In paper [1] a concept of involutive monomial division was invented which forms the foundation of algorithms [1, 2] for the construction of Gröbner bases [3, 4, 5] of a special form called involutive. Given a finite monomial set, an involutive division satisfying the axiomatic properties proposed in [1] leads to a self-consistent separation of variables for any monomial in the set into disjoined subsets of so-called multiplicative and nonmultiplicative variables. Thereby an involutive division defines the separation as a function of a monomial set and an element in the set. For a polynomial set the separation is assigned to the set of the leading monomials.

The idea of the separation of variables into multiplicative and nonmultiplicative goes back to classical papers of Janet [6] and Thomas [7]. They used particular separations of independent variables for completion of orthonomic systems of partial differential equations (PDEs) to an involutive form. Later on one of the separations already considered by Janet [6] was used intensively by Pommaret [8] for involutivity analysis of general systems of partial differential equations.

An involutive form of a system of PDEs is its interreduced completion by the differential consequences such that all integrability conditions are incorporated into the system. These conditions play the same role in the completion procedure for PDEs as nontrivial S-polynomials in the Buchberger algorithm for construction of Gröbner bases. By a well-known correspondence between polynomials and linear homogeneous partial differential equations, the notion of an involutive system can be transferred to systems of algebraic equations [9].

The separation of variables into multiplicative and nonmultiplicative allows one to generate the integrability conditions by means of multiplicative reductions of nonmultiplicative prolongations. In the language of monomials: if a leading monomial is multiplied by its multiplicative variables only, it is an involutive divisor of the resulting power product. Thus, in the course of involutive reduction polynomials are allowed to be multiplied by only multiplicative power products. Then an involutive basis of a polynomial ideal is defined [1] as a generating set such that any prolongation of any element is involutively (multiplicatively) reduced to zero modulo the set. Any involutive basis is a Gröbner one, though, generally, it may be redundant.

If an involutive division satisfies some extra conditions: noetherity, continuity and constructivity [1], then an involutive basis may be constructed algorithmically by sequential examination of single nonmultiplicative prolongations only. The uniqueness properties of involutive bases are investigated in [2] where a special form of an algorithm is proposed for construction of a minimal involutive basis which is unique much like to a reduced Gröbner basis. In addition to the above mentioned classical divisions, in paper [2] two more divisions were introduced which satisfy all the extra conditions.

In paper [10] it is shown that one can also construct different possible separations of variables for a fixed monomial set. These separations can not be considered, generally, as functions of a set and its element defined in [1]. Nevertheless, the results of paper [10] demonstrate for a wide class of divisions how one can change the division dynamically in the course of the completion. This increases the flexibility of the involutive technique and may also increase the efficiency of computations.

Computation of Janet bases relying upon the original Janet algorithm was implemented in Reduce and used for finding the size of a Lie symmetry group for PDEs [11] and for classification of ordinary differential equations admitting nontrivial Lie symmetries [12]. The study of algorithmic aspects of the general completion procedure for Pommaret division and implementation in Axiom was done in [13]. The completion to Pommaret polynomial bases was algorithmized and implemented in Reduce, first, in [14], and then with algorithmic improvements in [1].

In this paper we present first results of an implementation in *Mathematica* of involutive divisions introduced and studied in [1, 2] and also a new class of divisions the theoretical study of which including the proof of noetherity, continuity and constructivity will be presented elsewhere [15]. We discuss some built-in facilities of *Mathematica* which allow one to easily implement different involutive divisions as well as the algorithm for completion of a monomial set to involution [1, 2]. Some computer experiments and their analysis are also described. They reveal not only specific features of particular involutive divisions but also some general computational aspects of completion to involution important for the extension of the technique to polynomial and differential bases. The computational efficiency issues are also discussed, and some future improvements are shortly outlined.

As an application of the algorithms implemented we consider computation of Hilbert function and Hilbert polynomial for monomial ideals. Already Janet [6] showed how to compute these objects for a monomial ideal generated by an involutive monomial set. In particular, he wrote an explicit formula for the projective Hilbert polynomial in terms of Cartan characters. This representation is also used in [8, 13]. In paper [10] it was noticed that a Hilbert function can be written in a simple and elegant way as a certain sum over the elements of an involutive basis. We use this formula and the corresponding compact formula for the Hilbert polynomial which follows from the former. These explicit formulas allow to compute easily the index of regularity of an ideal [5], and we demonstrate this by explicit examples.

2 Involutive Monomial Division. General Properties

In this section, we give the definition of involutive divisions and describe their basic properties. The presentation follows [1, 2] where one can find more details and proofs.

Let $\mathbb{N}$ be a set of non-negative integers, and $\mathbb{M} = \{x_1^{d_1} \cdots x_n^{d_n} \mid d_i \in \mathbb{N}\}$ be a set of monomials in the polynomial ring $K[x_1, \ldots, x_n]$ over a field K of characteristic zero.

By $deg(u)$ and $deg_i(u)$ we denote the total degree of $u \in \mathbb{M}$ and the degree of variable x_i in u, respectively. For the least common multiple of two monomials $u, v \in \mathbb{M}$ we shall use the conventional notation $lcm(u, v)$. If monomial u divides monomial v we shall write $u|v$.

An admissible monomial ordering is denoted by $\succ$, and throughout this paper we shall assume that

$$x_1 \succ x_2 \succ \cdots \succ x_n. \qquad (1)$$

Definition 2.1 An *involutive division* L on $\mathbb{M}$ is given, if for any finite monomial set $U \subset \mathbb{M}$ and for any $u \in U$ there is given a submonoid $L(u, U)$ of $\mathbb{M}$ satisfying the conditions:

(a) If $w \in L(u, U)$ and $v|w$, then $v \in L(u, U)$.
(b) If $u, v \in U$ and $uL(u, U) \cap vL(v, U) \neq \emptyset$, then $u \in vL(v, U)$ or $v \in uL(u, U)$.
(c) If $v \in U$ and $v \in uL(u, U)$, then $L(v, U) \subseteq L(u, U)$.
(d) If $V \subseteq U$, then $L(u, U) \subseteq L(u, V)$ for all $u \in V$.

Elements of $L(u, U)$ are called *multiplicative* for u. If $w \in uL(u, U)$ we shall write $u|_L w$ and call u *(L−)involutive divisor* of w. The monomial w in its turn is called *(L−)involutive multiple* of u. In such an event the monomial $v = w/u$ is *multiplicative* for u and the equality $w = uv$ will be written as $w = u \times v$. If u is a conventional divisor of w but not an involutive one we shall write, as usual, $w = u \cdot v$. Then v is said to be *nonmultiplicative* for u.

Definition 2.2 We shall say that an involutive division L is *globally defined* if for any $u \in \mathbb{M}$ its multiplicative monomials are defined irrespective of the monomial set $U \ni u$; that is, if $L(u, U) = L(u)$.

Definition 2.1 for every $u \in U$ provides the separation

$$\{x_1, \ldots, x_n\} = M_L(u, U) \cup NM_L(u, U), \quad M_L(u, U) \cap NM_L(u, U) = \emptyset \qquad (2)$$

of the set of variables into two subsets: *multiplicative* $M_L(u, U) \subset L(u, U)$ and *non-multiplicative* $NM_L(u, U) \cap L(u, U) = \emptyset$. Conversely, if for any finite set $U \subset \mathbb{M}$ and any $u \in U$ the separation (2) is given such that the corresponding submonoid $L(u, U)$ of monomials in variables in $M_L(u, U)$ satisfies the conditions (b)-(d), then the partition generates an involutive division. The conventional monomial division, obviously, satisfies condition (b) only in the univariate case.

In what follows monomial sets are assumed to be finite.

Definition 2.3 A monomial set $U \in \mathbf{M}$ is *involutively autoreduced* or *L−autoreduced* if the condition $uL(u, U) \cap vL(v, U) = \emptyset$ holds for all distinct $u, v \in U$.

Definition 2.4 Given an involutive division L, a monomial set U is *involutive* with respect to L or L−involutive if

$$(\forall u \in U)\ (\forall w \in \mathbf{M})\ (\exists v \in U)\ \ [\, uw \in vL(v, U)\,].$$

Definition 2.5 An L–involutive monomial set $\tilde{U}$ is called L–*completion* of a set $U \subseteq \tilde{U}$ if

$$(\forall u \in U)\ (\forall w \in \mathbf{M})\ (\exists v \in \tilde{U})\ \ [\ uw \in vL(v,\tilde{U})\ ].$$

If there exists a finite L–completion $\tilde{U}$ of a finite set U, then the latter is *finitely generated* with respect to L. The involutive division L is *noetherian* if every finite set U is finitely generated with respect to L.

Proposition 2.6 *[1] If an involutive division L is noetherian, then every monomial ideal has a finite involutive basis $\bar{U}$.*

Proposition 2.7 *[2] If U is a finitely generated monomial set, then so is the set obtained by autoreduction of U in the sense of the conventional monomial division.*

Definition 2.8 A monomial set U is called *locally involutive* with respect to the involutive division L if

$$(\forall u \in U)\ (\forall x_i \in NM_L(u,U))\ (\exists v \in U)\ \ [\ v|_L(u \cdot x_i)\ ].$$

Definition 2.9 A division L is called *continuous* if for any finite set $U \in \mathbf{M}$ and for any finite sequence $\{u_i\}_{(1\leq i\leq k)}$ of elements in U such that

$$(\forall i < k)\ (\exists x_j \in NM_L(u_i,U))\ \ [\ u_{i+1}|_L u_i \cdot x_j\ ] \tag{3}$$

the inequality $u_i \neq u_j$ for $i \neq j$ holds.

Theorem 2.10 *[1] If an involutive division L is continuous then local involutivity of any monomial set U implies its involutivity.*

Definition 2.11 A continuous involutive division L is *constructive* if for any $U \subset \mathbf{M}$, $u \in U$, $x_i \in NM_L(u,U)$ such that $u \cdot x_i$ has no involutive divisors in U and

$$(\forall v \in U)\ (\forall x_j \in NM_L(v,U))\ (v \cdot x_j | u \cdot x_i,\ v \cdot x_j \neq u \cdot x_i)\ \ [\ v \cdot x_j \in \cup_{u \in U}\, u\, L(u,U)\ ]$$

the following condition holds:

$$(\forall w \in \cup_{u \in U}\, u\, L(u,U))\ \ [\ u \cdot x_i \notin wL(w, U \cup \{w\})\ ]. \tag{4}$$

3 Examples of Involutive Divisions and Completion Algorithm

We give, first, examples of the involutive divisions defined by Janet, Thomas and Pommaret and two new divisions proposed in [2]. For the proof of validity of properties (b)-(d) in Definition 2.1 for these divisions we refer to [1, 2].

Example 3.1 Thomas division [7]. Given a finite set $U \subset \mathbf{M}$, the variable x_i is considered as multiplicative for $u \in U$ if $deg_i(u) = max\{deg_i(v) \mid v \in U\}$, and nonmultiplicative, otherwise.

Example 3.2 Janet division [6]. Let the set $U \subset \mathbf{M}$ be finite. For each $1 \leq i \leq n$ divide U into groups labeled by non-negative integers $d_1, \ldots, d_i$:

$$[d_1, \ldots, d_i] = \{\ u\ \in U \mid d_j = deg_j(u),\ 1 \leq j \leq i\ \}.$$

A variable x_i is multiplicative for $u \in U$ if $i = 1$ and $deg_1(u) = max\{deg_1(v) \mid v \in U\}$, or if $i > 1$, $u \in [d_1, \ldots, d_{i-1}]$ and $deg_i(u) = max\{deg_i(v) \mid v \in [d_1, \ldots, d_{i-1}]\}$.

Example 3.3 Pommaret division [8]. For a monomial $u = x_1^{d_1} \cdots x_k^{d_k}$ with $d_k > 0$ the variables $x_j, j \geq k$ are considered as multiplicative and the other variables as nonmultiplicative. For $u = 1$ all the variables are multiplicative.

Example 3.4 Division I. [2] Let U be a finite monomial set. The variable x_i is nonmultiplicative for $u \in U$ if there is $v \in U$ such that

$$x_{i_1}^{d_1} \cdots x_{i_m}^{d_m} u = lcm(u,v), \quad 1 \leq m \leq [n/2], \quad d_j > 0\ \ (1 \leq j \leq m).$$

and $x_i \in \{x_{i_1}, \ldots, x_{i_m}\}$.

Example 3.5 Division II. [2] For monomial $u = x_1^{d_1} \cdots x_k^{d_n}$ the variable x_i is multiplicative if $d_i = d_{max}(u)$ where $d_{max}(u) = max\{d_1, \ldots, d_n\}$.

All these divisions are continuous and constructive, and except Pommaret division they are also noetherian [1, 2].

Now we consider a new class of involutive divisions induced by admissible monomial orderings (cf. [10]).

Example 3.6 Induced division. Given an admissible monomial ordering $\succ$ a variable x_i is nonmultiplicative for $u \in U$ if there is $v \in U$ such that $v \prec u$ and $deg_i(u) < deg_i(v)$.

The proof that this separation gives a noetherian, continuous and constructive involutive division for any admissible ordering is given in [15] together with some additional theoretical analysis of the listed divisions.

To distinguish these divisions, the abbreviations T, J, P, I, II, D will be used. In the implementation described below, three orderings are used to induce involutive divisions: lexicographical, degree-lexicographical and degree-reverse-lexicographical. To distinguish these three orderings we shall use the subscripts L, DL, DRL, respectively.

We note that

- Thomas division, Divisions I and II do not depend on the ordering on the variables. Janet and Pommaret divisions, as defined, are based on the ordering given in (1). Generally, the ordering $\succ$ defining an Induced division implies some variable ordering which is not compatible with (1). However, below we assume that lexicographical, degree-lexicographical and degree-reverse-lexicographical orderings are compatible with (1).

- Pommaret division and Division II are globally defined in accordance with Definition 2.1.

There are the following relations between separations generated by those divisions.

Proposition 3.7 *[1, 2, 15] For any U, $u \in U$ and $\succ$ the inclusions $M_T(u,U) \subseteq M_J(u,U)$, $M_T(u,U) \subseteq M_I(u,U)$, $M_T(u,U) \subseteq M_{D_\succ}(u,U)$ hold. If U is autoreduced with respect to Pommaret division, then also $M_P(u,U) \subseteq M_J(u,U)$.*

The following simple example explicitly shows that all eight divisions we use in this paper are different. In the table we list the multiplicative variables for every division.

Example 3.8 *Multiplicative variables for elements in the set $U = \{x^2y, xz, y^2, yz, z^3\}$* $(x \succ y \succ z)$ for different divisions.

Monomial	Multiplicative variables							
	T	J	P	I	II	D_L	D_{DL}	D_{DRL}
x^2y	x	x,y,z	y,z	x	x	x	x	x
xz	—	y,z	z	x	x,z	x	x,z	x,z
y^2	y	y,z	y,z	y	y	x,y	x,y	y
yz	—	z	z	—	y,z	x,y	x,y,z	x,y,z
z^3	z	z	z	z	z	x,y,z	z	z

If U is a finitely generated monomial set with respect to the involutive division L, then its finite completion gives an involutive basis of the monomial ideal generated by U. There may be different involutively autoreduced bases of the same monomial ideal. For

instance, from the definitions given in Examples 3.1 and 3.2 it is easy to see that any finite monomial set is Thomas and Janet autoreduced. Therefore, enlarging a Tomas or Janet basis by a prolongation of any its element and then completing the enlarged set leads to another Thomas and Janet basis, respectively. Similarly, Division I and an Induced division do not provide uniqueness of involutively autoreduced bases whereas Pommaret division and Division II do, as well as any globally defined division [2].

Definition 3.9 Let L be an involutive division, and $Id(U)$ be a monomial ideal. Then its L–involutive basis $\bar{U}$ will be called *minimal* if for any other involutive basis $\bar{V}$ of the same ideal the inclusion $\bar{U} \subseteq \bar{V}$ holds.

Proposition 3.10 *[2] If $U \subset \mathbb{M}$ is a finitely generated set with respect to a constructive involutive division, then the monomial ideal $Id(U)$ has a unique minimal involutive basis.*

If L is constructive, then to compute the minimal involutive basis for an ideal generated by a given finite monomial set one can use the following algorithm [2].

Algorithm **MinimalInvolutiveMonomialBasis:**

Input: U, a finite monomial set
Output: $\bar{U}$, the minimal involutive basis of $Id(U)$

```
1  begin
2    Ū := Autoreduce(U)
3    choose any admissible monomial ordering ≺
4    while exist u ∈ Ū and x ∈ NM_L(u, Ū) s.t.
5      u · x has no involutive divisors in Ū do
6      choose such u, x with the lowest u · x w.r.t. ≺
7      Ū := Ū ∪ {u · x}
8    end
9  end
```

Here *Autoreduce*(U) stands for the conventional (non-involutive) autoreduction.

Remark 3.11 With line 2 omitted the algorithm produces the minimal completion of a finitely generated set for any admissible ordering in line 3 [1] which we shall call *selection ordering.*

Remark 3.12 Given a constructive division L and a finitely generated L–autoreduced monomial set U, the number of monomials added in the course of completing the set as well as the number of reducible nonmultiplicative prolongations checked do not depend on the completion ordering in line 3 of the above algorithm.

Let $\succ_1$ and $\succ_2$ be two different completion orderings of U to $\bar{U}$, and N_1 and N_2 be the corresponding numbers of the reducible prolongations in the course of the completion procedure. Assume that $N_1 > N_2$. As proved in [1] (c.f. the proof of Theorem 4.14) the number of irreducible prolongations is invariant on the completion ordering. Therefore, there are reducible nonmultiplicative prolongations at completion with $\succ_1$ which are not considered at completion with $\succ_2$. Let $u \cdot x = v \times w,\ u, v \in \tilde{U}_1 \subseteq \bar{U}$ be the first such prolongation in the course of the first completion procedure with $\tilde{U}_1$ being the current monomial set. Then, by admissibility of both orderings, for the second completion procedure we obtain $u \times x = v \times w,\ u, v \in \tilde{U}_2$ which contradicts the property (b) in Definition 2.1.

We would like to stress that just the first computer experiments with the package directed our attention to this property of the completion procedure.

Example 3.13 (Continuation of Example 3.8). The minimal involutive bases of the ideal generated by the set $U = \{x^2y, xz, y^2, yz, z^3\}$ $(x \succ y \succ z)$ are given by

$$\begin{aligned}
\bar{U}_T &= \{x^2y^2z^3, x^2y^2z^2, x^2y^2z, x^2y^2, x^2yz^3, x^2yz^2, x^2yz, x^2y, x^2z^3,\\
&\quad x^2z^2, x^2z, xy^2z^3, xy^2z^2, xy^2z, xy^2, xyz^3, xyz^2, xyz, xz^3, xz^2,\\
&\quad xz, y^2z^3, y^2z^2, y^2z, y^2, yz^3, yz^2, yz, z^3\},\\
\bar{U}_J &= \{x^2y, x^2z, xy^2, xyz, xz, y^2, yz, z^3\},\\
\bar{U}_P &= \{x^2y, x^2z, xy^2, xyz, xz, y^2, yz, z^3, \ldots, x^ky, \ldots, x^lz, \ldots\},\\
\bar{U}_I &= \{x^2y^2z^3, x^2y^2z^2, x^2y^2z, x^2y^2, x^2yz^3, x^2yz^2, x^2yz, x^2y, xy^2z^3,\\
&\quad xy^2z^2, xy^2z, xy^2, xyz^3, xyz^2, xyz, xz^3, xz^2, xz, y^2z^3, y^2z^2,\\
&\quad y^2z, y^2, yz^3, yz^2, yz, z^3\},\\
\bar{U}_{II} &= \{x^2y^2, x^2y, xy^2, xyz, xz, y^2, yz, z^3\},\\
\bar{U}_L &= \{x^2y, xz^2, xz, y^2, yz^2, yz, z^3\},\\
\bar{U}_{DL} &= \{x^2y, xz, y^2, yz, z^3\},\\
\bar{U}_{DRL} &= \{x^2y, xy^2, xz, y^2, yz, z^3\},
\end{aligned}$$

where $k, l \in \mathbb{N}$ $(k, l > 2)$, and subscripts in the left-hand sides stand for different involutive divisions considered in Section 3. This example explicitly shows that Pommaret division is not noetherian, since it leads to an infinite monomial basis.

4 Implementation in *Mathematica*

Our goal was to produce a package for exploring different involutive divisions. In doing so, we have not paid much attention to efficiency issues, but rather tried to allow for high flexibility and easy extensibility.

In this section we will also describe some observations that allow to speed up the steps of the algorithm **MinimalInvolutiveMonomialBasis** significantly. The basic operations on monomial sets are the same for the computation of involutive bases of polynomial [1, 2] and differential systems [9], so the improvements described here can be used in these cases, too.

Language dependent optimizations were only made where they were straightforward and promised a big gain in speed. For example, we use compiled versions of the functions which implement term orderings.

Monomials are represented as multiindices, i.e. the monomial $x_1^{i_1} \cdot \ldots \cdot x_n^{i_n}$ is represented as the list of its exponents $\{i_1, \ldots, i_n\}$. Thus, the set $U = \{u_1, \ldots, u_m\}$ can be considered as a $m \times n-$ matrix of integers. For every monomial u, we use two additional lists of length n: a list giving the separation of the variables for u, and a similar list containing notes about the prolongations that have already been done.

In the following, we will apply functions like *lcm* also to multiindices, with the obvious meaning. The set notation will be used for lists, assuming that the order of the elements is given somehow.

Building a flexible and extensible system is helped by some features of *Mathematica*. We used a functional style of programming, making extensive use of high level functions – such as `Sort`, `Select`, `Map` – for manipulating lists.

We pass the term ordering function as a parameter to functions like `minimalInvolutiveMonomialBasis`. The parameter is just the name of the ordering function. In the following example, the built-in function `Sort` is used to sort a list U of monomials with respect to lexicographic ordering:

```
U = Sort[U, lexOrder]
```

The function `lexOrder` when called for two multiindices a, b gives `True` if $a \succeq_{lex} b$, `False` otherwise. To add a new term order called `ord`, one would only have to write a corresponding function similar to `lexOrder`. Then the symbol `ord` can be passed to other functions without the need to change any part of the package.

We chose to pass the involutive division as a parameter, too. The function `separation` computes the separation of a monomial u w.r.t. a monomial set U and an involutive division. For example,

```
separation[Janet][u, U]
```

returns a list $\{s_1, \ldots, s_n\}$ where $s_j = 1$ if $x^j \in M(u, U)$, and $s_j = 0$ otherwise.

The following statement returns the minimal involutive basis of U with respect to Janet division and with lexicographic selection ordering:

```
minimalInvolutiveMonomialBasis[Janet][U, lexOrder]
```

An induced division like D_L is given by the expression: `inducedDivision[lexOrder]`. Using a parameter to specify the involutive division makes it easy to program a general version of some operation now, and supplement it by more optimized versions for specific divisions later. For example, the table that gives the separation for each $u \in U$ is by default computed using the function `sepationsOneByOne` which takes each $u_i \in U$ and determines $M_L(u_i, U)$ or $NM_L(u_i, U)$ according to the definition of the involutive division given in the parameter:

```
separations[div_][U_List] := separationsOneByOne[div][U]

separationsOneByOne[div_][U_List] := Map[separation[div][#,U]&,U];
```

We use the pattern div_ here to mean "any division". Of course, there are often more efficient ways to compute separations, based on special properties of a particular division. As a simple example, consider Thomas division (Example 3.1), where one has to compute the maximal degrees only once. We added a specialized version of separations which computes the maximal degrees and then separates the variables for each $u \in U$ accordingly (this is done in the function thmult):

```
separations[Thomas][U_List] := Module[{maxima},
  maxima = Map[Max, U//Transpose];
  Return[
    Map[thmult[#,maxima]&,U]
  ]
]
```

The point here is that *Mathematica* will automatically dispatch to the specialized version, because the argument Thomas is more specific than the general pattern div_ [16]. A similar behavior is known in other programming languages as "overloading" or "polymorphism". To extend the package for a new involutive division (called, say, newDivision), one would only have to write the specific version of the function separation:

```
separation[newDivision][u_, U_List] := ...
```

All the other steps in the algorithm would then be executed by functions that are generically defined for any involutive division. When it is needed, a more efficient version of separations can be added, like in the following fragment:

```
separations[newDivision][U_List] := ...
```

This incremental development, starting with few generic functions that are then supplemented by more efficient ones for special cases, helps to find the right balance between "program efficiency" i.e. the time your program spends on computing, and "programmer efficiency", i.e. the time you spend on programming.

We will now describe observations that can be used to make some operations of the algorithm **MinimalInvolutiveMonomialBasis** faster. In the following we will consider the list $U = \{u_1, \ldots, u_n\}$ of monomials, and u is always an element of U.

The first step is to compute the separation for each of the input monomials. For globally defined divisions, this is done irrespective of the other monomials in U. The implementation for Thomas division was shown above, the only improvement over separationsOneByOne being that we compute $lcm\{u|u \in U\}$ only once. For Janet division (Example 3.2), we made use of the following remark:

Remark 4.1 When the list U is sorted lexicographically in decreasing order, the groups $[d_1, \ldots, d_i]$ mentioned in the definition are grouped together. These groups are sorted lexicographically with respect to their labels of any fixed length i. The sorted list starts with the group labeled $[d_{1\,max}]$, $d_{1\,max} = max\ deg_1 u$, the monomials in $[d_{1\,max}]$ have x_1 as a multiplicative variable. We can then split the list into groups given by labels of length 1 and proceed recursively within each of them, next considering degrees in the second variable x_2, and so on.

For a division $D_\succ$ (Example 3.6) that is induced by some ordering $\succ$, we can use an auxiliary list:

Remark 4.2 Let the monomials be sorted in descending order: $u_1 \succ \ldots \succ u_n$. We call the elements of the list $\mathrm{cm}(U) := \{m_1, \ldots, m_n | m_i = \mathrm{lcm}(u_i, \ldots, u_n), i = n, \ldots, 1\}$ *the cumulated multiples* of U. By definition, variable x_j is nonmultiplicative for u_i if and only if it has a higher degree in m_i: $deg_j u_i < deg_j m_i$. Thus, all we have to do is compute the list $\mathrm{cm}(U)$ of cumulated multiples and then compare each $u \in U$ against its corresponding entry in $cm(U)$.

For Division I, we are not aware of any property that would allow us to accelerate the computation of separations in a manner similar to Janet or Induced divisions.

The following observation can be used to speed up the process of finding a minimal nonmultiplicative prolongation (line 6 of the algorithm). Let us denote the minimal (w.r.t. the chosen ordering $\succ$) nonmultiplicative prolongation by a given variable x with $P_\succ(x)$.

Remark 4.3 Let U be sorted w.r.t. the completion ordering: $u_1 \succ \ldots \succ u_n$. Let u_i *and* x be fixed such that $u_i \cdot x$ is a minimal nonmultiplicative prolongation w.r.t. $\succ$. Then $u_i \cdot x$ is an element of the set $\{P_\succ(x_1), \ldots, P_\succ(x_n)\}$. This follows directly from the minimality of $u_i \cdot x$. Furthermore, u_i is the minimal monomial having x as a nonmultiplicative variable, because $v \cdot x \succ u \cdot x$ implies $v \succ u$.

The remark obviously extends to the more general situation of the algorithm, where some of the nonmultiplicative prolongations have already been considered.
The next step in the algorithm is to search for an involutive divisor w of a nonmultiplicative prolongation $v = u \cdot x$. In the polynomial case, the efficiency of this search can be even more important, since we may want to involutively reduce every term of a prolonged polynomial. Recall that for an involutively reduced set U, there can be at most one such w. We present now some optimizations that apply to increasingly specialized situations.

An involutive divisor is also a conventional one: $w|_L v \Rightarrow w|v$, and thus $w \preceq v$ w.r.t any admissible term ordering. Consequently, we can keep the list U sorted in descending order w.r.t. $\succ$, and use binary search to find the greatest $u_j \in U$ such that $u_j \preceq v$. All candidates for an involutive divisor are then among $u_j, \ldots, u_m$.

The binary search technique does not make much use of the properties of involutive divisions, in fact it is already applicable to finding conventional divisors of v. We have implemented this technique but found that it did not give improved timings. This is due to the overhead involved in the binary search that we had to program in the *Mathematica* language as opposed to the very fast built-in function `Select` for linear searching. The advantage of using binary search will surely realize for very large lists, or when used in an implementation in some other programming language.

The following remark uses a special property of involutive divisions, taking into account that v is a nonmultiplicative prolongation of an element of U.

Remark 4.4 Let U be an involutively autoreduced set of monomials and $v = u \cdot x$ a nonmultiplicative prolongation of some $u \in U$. If a monomial $w \in U$ is an involutive divisor of v then $deg_x w = deg_x v$. Since $u \cdot x$ should be involutively reducible by w, we can write $u \cdot x = w \times (u \cdot x/w)$. If $w = v = u \cdot x$, we are done. If $w \neq u \cdot x$ and $w|u$, then $u = w \times (u/w)$, which contradicts our assumption that U is involutively autoreduced.

One can gain even more by considering particular divisions.

Remark 4.5 Let us assume that we want to compute a minimal involutive Janet basis, and that we search for an involutive divisor w of some nonmultiplicative prolongation $v = u \cdot x_j$. Then, w is in the class $[deg_1 u, \ldots, deg_{j-1} u, deg_j u + 1]$ because w has to divide $u \cdot x_j$ and thus $deg_k w \leq deg_k u$ for $k = 1, \ldots, j-1$. In fact, these degrees have to be equal, because $deg_k w < deg_k u$ would mean that x_k is nonmultiplicative for w. Furthermore, $deg_j w = deg_j u + 1$ according to Remark 4.4.

Consequently, there holds $u \cdot x \succeq_{lex} w \succ_{lex} u$, which can also be used to narrow the search range for an involutive divisor.[1] There are similar relations for Pommaret and induced divisions. Namely, for Pommaret division, w is reverse lexicographically greater than u, and for a division that is induced by $\succ$, either $u \cdot x = w$ or $u \succ w$ holds.

These properties together with Remark 3.12 suggest that one should keep the monomials sorted with respect to some order that is most suitable for finding involutive divisors, and use this order as completion order, too.

Finally, when we find no involutive divisor, we have to add the prolongation to the set and adjust separations accordingly.

Remark 4.6 For all divisions discussed so far, the following holds for a monomial $u \in U$: $\mathrm{NM}(u, U \cup \{v\}) = \mathrm{NM}(u, U) \cup \mathrm{NM}(u, \{u, v\})$.

A detailed discussion of this fact can be found in [15]. So, after adding a monomial v to U, we have to compute the separation of v, and then only "pairwise" separations for every $u \in U$.

Again, for special divisions, we can make more improvements.

[1] Here $\succ_{lex}$ denotes the lexicographical ordering compatible with (1).

Remark 4.7 Let $v = u \cdot x_j$ be some nonmultiplicative prolongation, and assume that v has no involutive divisor in the Janet-autoreduced set U. Then, the separation may only change for monomials in the class $[deg_1 u, \ldots, deg_{j-1} u, deg_j u + 1]$.

Remark 4.8 Consider the same situation but with some induced division $D_\succ$. Only the variable x_j can change from multiplicative to nonmultiplicative, and it can do so only for monomials $s \succ v$ satisfying $deg_j s = deg_j v - 1$.

Of all the improvements mentioned above, only Remark 4.4 is implemented in the current version of the package.

We have applied the package to examples taken from various sources. For each polynomial system, we computed the degree reverse lexicographical Gröbner basis and took the resulting set of leading monomials as input to the algorithm **MinimalInvolutiveMonomialBasis**. As we will describe in the following section, the output can then be used to compute the Hilbert function, the Hilbert polynomial and the index of regularity of the corresponding polynomial ideal.

Example 4.9 [5, p. 455] $U = \{x^3yz^5, xy^3z^2\}$.

Example 4.10 [17] Consider a $n \times n$ matrix $A = (\alpha_{ij})_{n,n}$ with unspecified entries. The condition $A^2 = 0$ leads to a system of n^2 polynomial equations in the variables $\alpha_{11}, \ldots, \alpha_{1n}, \alpha_{21}, \ldots, \alpha_{nn}$. We treated the leading monomials of the degree reverse lexicographic Gröbner basis, where the variables are ordered according to $\alpha_{11} \succ \ldots \succ \alpha_{1n} \succ \alpha_{21} \succ \ldots \succ \alpha_{nn}$.

Example 4.11 The system of "n -th cyclic roots" is a well known example. For $n = 4$, it is given by:

$$\begin{aligned}
x_1 + x_2 + x_3 + x_4 &= 0\\
x_1x_2 + x_2x_3 + x_3x_4 + x_4x_1 &= 0\\
x_1x_2x_3 + x_2x_3x_4 + x_3x_4x_1 + x_4x_1x_2 &= 0\\
x_1x_2x_3x_4 - 1 &= 0
\end{aligned}$$

The following table shows the results of applying the algorithm **MinimalInvolutiveMonomialBasis** to our examples. In the first three columns, the size of the input is given where m is the number of monomials, n is the number of variables, and d is the maximum total degree of the input monomials. The divisions are indicated by the abbreviations used above. For each division, we give the length of the minimal involutive monomial basis, the number of prolongations considered during completion, and the portion of reducible prolongations. Thus, 100% reducible prolongations means that the input is already an involutive basis. An empty entry in the column for Pommaret division means that we did not compute a minimal Pommaret basis because the ideal is not zero dimensional. For the other divisions, it means that the timing is larger than 9999 seconds at our computer[2].

Input	*Size*			*Division*							
	m	n	d	J	T	P	I	II	D_L	D_{DRL}	D_{DL}
Ex. 3.8	5	3	3	**8** 11 73%	**29** 55 57%	–	**26** 47 55%	**8** 11 73%	**7** 9 78%	**6** 8 88%	**5** 6 100%
Ex. 4.9	2	3	9	**5** 4 25%	**14** 19 37%	–	**3** 2 50%	**12** 17 41%	**3** 2 50%	**3** 2 50%	**3** 2 50%
Ex. 4.10 $n = 2$	5	4	3	**5** 7 100%	**25** 49 59%	–	**25** 49 59%	**12** 21 67%	**10** 18 72%	**5** 7 100%	**5** 7 100%
Ex. 4.10 $n = 3$	25	9	4	**56** 239 87%	–	–	–	**612** 2972 80%	**531** 2920 83%	**1711** 9362 82%	**1479** 8044 82%
Ex. 4.10 $n = 4$	161	16	6	**1324** 11836 90%	–	–	–	–	–	–	–
Ex. 4.11 $n = 4$	7	4	6	**7** 14 100%	**98** 242 62%	–	**98** 242 62%	**25** 55 67%	**41** 92 63%	**9** 20 90%	**7** 14 100%
Ex. 4.11 $n = 5$	20	5	8	**23** 76 96%	**1010** 3544 72%	**23** 76 96%	–	**93** 297 75%	**154** 488 72%	**135** 548 79%	**106** 419 79%
Ex. 4.11 $n = 6$	45	6	9	**46** 194 99%	–	**46** 194 99%	–	**201** 807 81%	**385** 1527 78%	**841** 4230 81%	**972** 4899 81%

For some examples, bases for two different divisions may coincide. For Example 3.8, all bases are different, the input is already a basis for the division D_{DL}. For the system of Example 4.9, bases for Division I, D_L, D_{DRL}, and D_{DL} coincide. The bases for Thomas and Division I coincide in Example 4.10 with $n = 2$, also the input is a base for Janet division and for the Induced divisions D_{DRL} and D_{DL}. For the fourth cyclic roots (Example 4.11), the bases for Thomas division and Division I, as well as those for Janet division and the induced division D_{DL} coincide, respectively.

The computations with monomial sets should give at least some hint to the performance of different divisions in the polynomial and differential cases. From our experience, Janet division, generally, and Induced divisions, sometimes, seem to be

[2] a 200 MHz 586 running Linux

the most promising in terms of prolongations that have to be considered. Pommaret division – even though it is not noetherian – deserves further investigation, because it is globally defined and rather "compact", too.

5 Computation of Hilbert Function, Hilbert Polynomial and Index of Regularity

Analysis of arbitrariness of the solution space for systems of PDEs was just one of the basic motivations for the development of the Janet-Riquier theory of involutivity [6, 18] and the corner stone for the following research activity related with completion to involution (c.f. [8, 11, 13, 19, 22, 23]). Already Janet [6] relying on the concept of an involutive system and taking into account the uniqueness of involutive divisors, gave explicit expressions for the number of monomials which have no divisors among the leading terms of the system. Janet's formulas are written in terms of the Cartan characters σ_k^q. They are defined for an involutive basis of (maximal total) degree q as a number of monomials in $\mathbb{M}$ of the total degree q and with k Pommaret multiplicative variables which have no involutive divisors among the leading monomials of the basis. Janet obtained, in particular, the following presentation of the Hilbert polynomial of an ideal $I = Id(U)$ generated by a set U of monomials of degree q, which was later used in [8, 13, 19]:

$$HP_I(s) = \sum_{k=1}^{n} \binom{s+k-1}{k-1} \sigma_q^k. \quad (5)$$

Recently in paper [10] it was observed that the affine Hilbert function for a monomial ideal $I \subset K[x_1, \ldots, x_n)$, given its $L-$*reduced* involutive basis U can be written in the following simple and elegant way:

$$^aHF_I(s) = \binom{n+s}{s} - \sum_{i=0}^{s} \sum_{u \in U} \binom{i - deg(u) + m(u) - 1}{m(u) - 1}, \quad (6)$$

where $m(u)$ is a number of multiplicative variables of u. This formula is an easy consequence of the fact that any monomial $w \in I$ has a unique involutive divisor in U which implies the equality $w = u \times (w/u)$. The first term in (6) stands for the total number of monomials in $\mathbb{M}$ of degree less or equal s and the double sum counts the number of such monomials which have involutive divisors in U. Though this presentation, for a Pommaret basis, is completely equivalent to Janet's explicit formulas, it is more compact, valid for arbitrary involutive divisions and more directable for computation of Hilbert functions.

If $s \geq s_m$, where

$$s_m = max\{deg(u) \mid u \in U\}, \quad (7)$$

then one can rewrite

$$\sum_{i=0}^{s}\binom{i-deg(u)+m(u)-1}{m(u)-1}=\sum_{i=deg(u)}^{s}\binom{i-deg(u)+m(u)-1}{m(u)-1}=\binom{s-deg(u)+m(u)}{m(u)}$$

and thereby obtain from (6) the following compact formula for the affine Hilbert polynomial of I represented by its involutive basis:

$$^{a}HP_I(s)=\binom{n+s}{s}-\sum_{u\in U}\binom{s-deg(u)+m(u)}{m(u)}. \qquad (8)$$

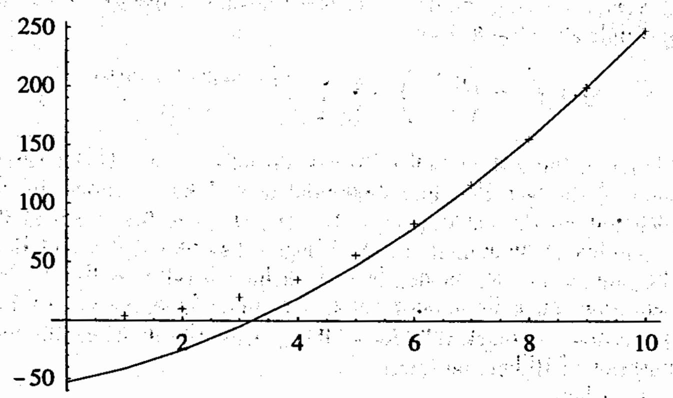
Much like (6), this formula not only generalizes (5) to arbitrary involutive divisions, but also gives a simpler representation for the Hilbert polynomial.

The above introduced s_m gives an upper bound for the index of regularity [5] of ideal I, that is, such minimal integer $s_0 \geq 0$ that for all $s \geq s_0$ the following equality holds

$$^{a}HP_I(s)={}^{a}HF_I(s) \qquad (9)$$

The index of regularity can be easily found numerically from the explicit formulas (6-8) by starting at the bound (7) and checking the equality (9) for decreasing integer values of s.

For illustrative purposes consider Example 4.9. The generated ideal is two-dimensional, and its affine Hilbert polynomial computed by formula (8) for any involutive division is $2s^2+10s-53$. The values of this polynomial for integer arguments together with ones of the affine Hilbert function computed by formula (6) are plotted at Fig.1. The index of regularity is 8.



As a more nontrivial example consider now the polynomial ideal generated by squaring a 4×4 matrix in Example 4.10 all the elements of which are considered as variables. The reduced degree reverse lexicographical Gröbner basis computed with *Mathematica* in about 5 minutes at our 200 MHz 586 computer contains 161 elements. Janet basis of the monomial ideal generated by leading monomials of the Gröbner basis contains 1324 elements, and gives the following affine Hilbert polynomial

$$\frac{1}{1440}s^8+\frac{1}{72}s^7+\frac{8}{45}s^6+\frac{113}{144}s^5+\frac{3259}{1440}s^4+\frac{617}{144}s^3+\frac{607}{120}s^2+\frac{41}{12}s+3$$

with 2 as index of regularity. The current first implementation in *Mathematica*, as we discuss in Sect.4, does not take into account many specific properties of the involutive technique which, we expect, will drastically decrease the timings. By this reason the computation of the Janet basis took about 2 hours whereas computation of the Hilbert polynomial took only 2 seconds.

6 Conclusion

The practical efficiency of the algorithm **MinimalInvolutiveMonomialBasis** depends on the efficiency of the following basic operations, given a monomial set U and its separation:

1. Selection of a minimal nonmultiplicative prolongation $u \times x$ in the current monomial set U with respect to the completion ordering.

2. Search for an involutive divisor in U.

3. Recomputing the separation for $U \cup \{u \cdot x\}$.

As we have noted, the first implementation described in Sect.4 is far from being optimal. In the next version we shall improve, first of all, the implementation of the above mentioned operations taking into account both specific algorithmic features of involutive divisions and related programming in *Mathematica*.

The basic operations remain of great importance for the implementation of the polynomial involutive algorithm of paper [2] which we plan to do as a next step. Then we want to extend the polynomial *Mathematica* code to linear PDEs. This class of differential equations is of interest by its own, and also for the Lie symmetry analysis of nonlinear differential equations. The most nontrivial step here is integration of the determining systems of linear PDEs for the symmetry generators [20]. These systems are overdetermined and just the completion to involution is the most universal algorithmic scheme for their explicit solving. The completion of nonlinear PDE systems to involution involves, generally, their splitting into a finite number of subsystems as was shown already by Thomas [7]. The subsystems contain not only equations but also inequalities much like regular systems produced by the Rosenfeld-Gröbner algorithm [21].

The separation of independent variables into multiplicative and nonmultiplicative allows one to obtain the integrability conditions of PDEs from their nonmultiplicative prolongations. There is also another method of computation of integrability conditions which does not use the separation [22]. The related simplified form of PDEs called reduced involutive form is a generalization to nonlinear cases of a standard form [23]. The standard form was proved to be a differential Gröbner basis for linear PDEs in [24].

We believe that the implementation of the involutive division algorithms for differential equations together with its experimental and theoretical comparison with other computer algebra packages available for general analysis of PDEs [13, 21, 22, 25] will allow one to improve the algorithms and implementations. The latter is necessary for solving real problems with PDEs which is significantly harder than algebraic equations with corresponding numbers of independent variables and of degree. The notable progress in efficiency of algebraic Gröbner basis algorithms over the last years, and application to real problems may exert influence on their counterparts in PDEs: characteristic sets, differential Gröbner bases, involutive systems, etc.

7 Acknowledgement

The research described in this paper was conducted during a stay of the first author at the University of Greifswald which was supported by the German Academic Exchange Service.

References

[1] Gerdt, V.P., Blinkov, Yu.A. (1996). Involutive Bases of Polynomial Ideals. Preprint-Nr.1/1996, Naturwissenschaftlich-Theoretisches Zentrum, University of Leipzig; *Math. Comp. Simul.* **45**, 1998, 519-542.

[2] Gerdt, V.P., Blinkov, Yu.A. (1997). Minimal Involutive Bases. Preprint JINR E5-4-1997, Dubna; *Math. Comp. Simul.* **45**, 1998, 543-560.

[3] Buchberger, B. (1985). Gröbner Bases: an Algorithmic Method in Polynomial Ideal Theory. In: *Recent Trends in Multidimensional System Theory,* Bose, N.K. (ed.), Reidel, Dordrecht, pp.184-232.

[4] Becker, T., Weispfenning, V., Kredel, H. (1993). *Gröbner Bases. A Computational Approach to Commutative Algebra.* Graduate Texts in Mathematics **141**, Springer-Verlag, New York.

[5] Cox, D., Little, J., O'Shea, D. (1996). *Ideals, Varieties and Algorithms. An Introduction to Computational Algebraic Geometry and Commutative Algebra.* 2nd Edition, Springer-Verlag, New-York.

[6] Janet, M. (1920). Sur les Systèmes d'Equations aux Dérivées Partielles. *J. Math. Pure et Appl.* **3**, 65-151.

[7] Thomas, J. (1937). *Differential Systems.* American Mathematical Society, New York.

[8] Pommaret, J.F. (1978). *Systems of Partial Differential Equations and Lie Pseudogroups*, Gordon & Breach, New York.

[9] Gerdt, V.P. (1995). Gröbner Bases and Involutive Methods for Algebraic and Differential Equations. In: *Computer Algebra in Science and Engineering*, Fleischer, J., Grabmeier, J., Hehl, F.W., Küchlin, W. (eds.), World Scientific, Singapore, pp.117-137; *Math. Comput. Modelling* **25**, No.8/9, 1997, 75-90.

[10] Apel, J. (1997). Theory of Involutive Divisions and an Application to Hilbert Function. To appear in *J. Symb. Comp.*

[11] Schwarz, F. (1992). An Algorithm for Determining the Size of Symmetry Groups. *Computing* **49**, 95-115.

[12] Schwarz, F. (1996). Janet Bases of 2^{nd} Order Ordinary Differential Equations. In: *Proceedings of the ISSAC'96*, Lakshman Y.N. (ed.), ACM Press, pp.179-188.

[13] Seiler, W.M. (1994) *Analysis and Application of the Formal Theory of Partial Differential Equations.* PhD Thesis, Lancaster University.

[14] Zharkov, A.Yu., Blinkov, Yu.A. (1993). Involutive Approach to Investigating Polynomial Systems. In: Proceedings of "SC 93", International IMACS Symposium on Symbolic Computation: New Trends and Developments (Lille, June 14-17, 1993). *Math. Comp. Simul.* **42** (1996), 323-332.

[15] Gerdt, V.P. (1998). Involutive Division Technique: Some Generalizations and Optimizations. Submitted to International Conference "Computer Algebra in Scientific Computing" (St.Petersburg, Russia, April 20-24, 1998).

[16] Wolfram, S. (1996) *The Mathematica Book*, Third Edition, Wolfram Media, Inc. and Cambridge University Press

[17] Bayer, D., Stillman, M. (1992). Computation of Hilbert Functions. *J. Symb. Comp.* 14, 31-50.

[18] Riquier, C. (1910) *Les Systèmes d'Equations aux Dérivées Partielles*, Gauthier-Villars, Paris.

[19] Seiler, W.M. (1994) On the Arbitrariness of the General Solution of an Involutive Partial Differential Equation. *J. Math. Phys.* 35, 486-498.

[20] Hereman, W. (1995). Symbolic software for the computation of Lie symmetry analysis. In: CRC Handbook of Lie Group Analysis of Differential Equations, Volume 3: New Trends in Theoretical Developments and Computational methods, Ibragimov, N.H. et al. (eds.), CRC Press, Boca Raton, pp.367-413.

[21] Boulier, F., Lazard, D., Ollivier, F., Petitot, M. Representation for the Radical of a Finitely Generated Differential Ideal. In: *Proceedings of the ISSAC'95*, Levelt, A.H.M. (ed.), ACM Press, pp.158-166.

[22] Reid, G.J., Wittkopf, A.D., Boulton, A. (1996). Reduction of Systems of Nonlinear Partial Differential Equations to Simplified Involutive Form. *Euro. J. Appl. Maths.* **7**, 635-666.

[23] Reid, G.J. (1992) Algorithms for Reducing a System of PDEs to Standard Form, Determining the Dimension of its Solution Space and Calculating its Taylor Series Solution. *Euro. J. Appl. Maths.* **2**, 293-318.

[24] Czichowski, G., Thiede, M. (1992). Standard forms of differential equations and symmetry computation. *Seminar Sophus Lie* (now: Journal of Lie Theory) 2, 223-233.

[25] Mansfield, E.L., Fackerell, E.D. (1992). Differential Gröbner bases. Preprint of School of Mathematics, Physics, Computer Science and Electronics. Macquarie University, Sydney.

Received by Publishing Department
on June 1, 1998.