Passive Complete Orthonomic Systems of PDEs and Involutive Bases of Polynomial Modules

Joachim Apel

Universität Leipzig, Mathematisches Institut
Augustusplatz 10–11,
04109 Leipzig, Germany
apel@mathematik.uni-leipzig.de

Abstract. The objective of this article is to enlighten the relationship between the two classical theories of passive complete orthonomic systems of PDEs on the one hand and Gröbner bases of finitely generated modules over polynomial rings on the other hand. The link between both types of canonical forms are the involutive bases which are both, a particular type of Gröbner bases which carry some additional structure and a natural translation of the notion of passive complete orthonomic systems of linear PDEs with constant coefficients into the language of polynomial modules.
We will point out some desirable applications which a "good" notion of involutive bases could provide. Unfortunately, these desires turn out to collide and we will discuss the problem of finding a reasonable compromise.

1 Introduction

Our objective is to discuss a general framework of involutive bases of finitely generated modules over polynomial rings which on the one hand still provides a uniform algorithmic treatment but on the other hand includes useful instances for some natural applications.

First of all, we will shortly introduce the two major pillars of involutive bases which consist in the passive complete orthonomic form of systems of partial differential equations (PDEs) and the Gröbner bases of polynomial modules. Passive complete orthonomic systems of PDEs are the main idea behind Riquier's existence theorems (c.f. Riquier (1910); Thomas (1929)) and the corresponding algorithms for solving systems of PDEs due to Janet (1929). Gröbner bases and Buchberger's algorithm (c.f. (Buchberger , 1965, 1985)) for their computation, nowadays, have countless applications in commutative and non-commutative algebra as well as in algebraic geometry. Moreover, both methods are fundamental for lots of applications in- and outside mathematics due to their impact on respective solution methods for systems of differential or algebraic equations. Riquier's and Buchberger's theories are related to each other by the fact that the translation of the passive complete orthonomic form of systems of linear PDEs with constant coefficients into the language of polynomial modules provides a particular type of Gröbner bases carrying an additional structure which can be roughly described by saying that in addition to the direct access to the initial module $\mathrm{in}_{\prec}(M)$, which is characteristic for all Gröbner bases of a module M, an involutive basis of M provides a decomposition of $\mathrm{in}_{\prec}(M)$ into a certain direct sum of finitely many free modules. Indeed, the overlapping area of both theories is larger than only linear PDEs with constant coefficients on the one hand and polynomial modules on the other hand side. In Section 4 we will discuss the connection a little more detailed.

The notion *involutive bases* for the Gröbner bases with the additional initial ideal decomposition property was introduced by Gerdt and Blinkov, who were inspired by the modern terminology used in the theory of PDEs. We follow this notion since it is well-established in the community of people working in this field. But a warning might be helpful at this place. In the theory of PDEs the adjective 'involutive' describes intrinsic geometric properties of the system and its meaning is coordinate free. In contrast, Riquier's normal forms as well as Buchberger's Gröbner bases are defined within a given coordinate system. Therefore, 'involutive bases' is a coordinate free notion assigned to a coordinate dependent object. This fact can cause heavy confusion unless one forgets about the intrinsic meaning of the adjective 'involutive' when working in ideal theory. The classical meaning of 'involutive' suggests the distinction of a property of ideals rather than a property of particular generating sets.

Riquier's theory leaves some freedom in choosing the multipliers for each of the equations in order to complete an orthonomic system of PDEs (see Section 2). Depending on what application is concerned different ways of defining the sets of multipliers have been introduced in the past. Janet suggested a very sophisticated assignment rule leading to an efficient algorithm (see (Janet , 1929)). In Section 6 we will explain the advantage of Janet's assignments for algorithmic purposes but we will also show how to further improve them. The main objective of Thomas was to give a most elegant and easy understandable presentation of Riquier's existence theorems. This aim is fulfilled best by concentrating on only the principal algorithmic aspects and disregarding any efficiency issues (see (Thomas , 1929, 1937)). Yet another objective can be found in Pommaret's coordinate free studies of systems of PDEs, where a multiplier notion optimal for systems of PDEs in generic coordinates is applied (see (Pommaret , 1978)).

The use of different multiplier notions for different applications was motivation for Gerdt and Blinkov (1998) to think about a general framework for fixing the multipliers. In this article we will discuss and motivate the ideas which stand behind the alternative concept introduced in (Apel , 1998).

Sometimes it might seem that the presented examples are not characteristic since many of them consider only the most simple case of monomial ideals. However, the situation is not much different for general modules M because after fixing an admissible term order $\prec$ the main algorithmic part takes place only in the initial module $\mathrm{in}_{\prec}(M)$, which indeed is monomial. Also the second restriction to ideals is not essential. If M, and consequently also $\mathrm{in}_{\prec}(M)$, are submodules of a module F of higher rank k then we can decompose $\mathrm{in}_{\prec}(M)$ in a direct sum of k monomial submodules of modules of rank 1, i.e. ideals, and treat each of them separately.

2 Orthonomic Systems of Partial Differential Equations

Let $x_1, \ldots, x_n$ denote the independent variables, $u_1, \ldots, u_k$ the unknown functions and $\mathcal{D}$ the set of all differential operators of the form

$$\frac{\partial^{i_1+\cdots+i_n}}{\partial x_1^{i_1} \cdots \partial x_n^{i_n}} . \tag{1}$$

Furthermore, let the set $\mathcal{DU} = \{Du_j \mid D \in \mathcal{D}, 1 \leq j \leq k\}$ of all formal derivatives of the unknown functions by differential operators from $\mathcal{D}$ be ordered by a well-order $\prec$ which is compatible with differentiation in the sense $\frac{\partial}{\partial x_i} D_1 u_{j_1} \prec \frac{\partial}{\partial x_i} D_2 u_{j_2}$ for all $i \in \{1, \ldots, n\}$ and $D_1 u_{j_1}, D_2 u_{j_2} \in \mathcal{DU}$ such that $D_1 u_{j_1} \prec D_2 u_{j_2}$. Usually, the additional assumption that $\prec$ has to be compatible with the order of derivation is made, i.e. $D_1 u_{j_1} \prec D_2 u_{j_2}$ holds for all $j_1, j_2 \in \{1, \ldots, k\}$ and $D_1 = \frac{\partial^{i_1+\cdots+i_n}}{\partial x_1^{i_1} \cdots \partial x_n^{i_n}}, D_2 = \frac{\partial^{i'_1+\cdots+i'_n}}{\partial x_1^{i'_1} \cdots \partial x_n^{i'_n}} \in \mathcal{D}$ such that $i_1 + \cdots + i_n < i'_1 + \cdots + i'_n$.

Consider a system of finitely many partial differential equations which are all of the form

$$D_i u_{j_i} = G_i , \tag{2}$$

where $D_i u_{j_i} \in \mathcal{DU}$ and G_i is a function of the independent variables and the derivatives which are less than $D_i u_{j_i}$ with respect to $\prec$, and the left hand sides of the equations are pairwise distinct. Then we call $Du_j \in \mathcal{DU}$ a *principal* derivative of the system if it can be obtained by differentiation from the left hand side of one of the equations and we call it a *parametric* derivative of the system, otherwise. A system of PDEs is called *orthonomic* if it satisfies the above conditions, no right hand side contains any principal derivative, and each right hand side can be developed in a Taylor series in the region under consideration. Let us illustrate the notions introduced so far by an example.

Example 1 (Part 1). Consider the system

$$u_{xx} = y v_x \tag{3}$$
$$u_{yy} = -x^2 u \tag{4}$$

of two partial differential equations in the unknown functions $u = u(x, y)$ and $v = v(x, y)$ in two independent variables x and y. As usual, subscripts at the unknown functions indicate partial derivatives, e.g. $u_{xy} = \frac{\partial^2}{\partial x \partial y} u$. This system is in orthonomic form with respect to any order $\prec$ which is compatible with the order of derivation. Obviously, the right hand sides considered as functions in x, y and the occurring derivatives of u and v have Taylor series expansions everywhere. Since the derivatives on the right hand side of the equations are of lower order than the derivatives on the left hand side, the derivatives on the right hand side are smaller than the left hand sides with respect to $\prec$, in particular, no derivative on the right hand side can be obtained by differentiation of a left hand side.

All derivatives of v are parametric. The parametric derivatives of u are u, u_x, u_y and u_{xy}. The remaining derivatives of u are principal.

Let $D_1 u_{j_1} = G_1$ and $D_2 u_{j_2} = G_2$ be two equations of the system such that differentiation of the left hand sides by $\Delta_1, \Delta_2 \in \mathcal{D}$, respectively, leads to the same principal derivative $\Delta_1(D_1 u_{j_1}) = \Delta_2(D_2 u_{j_2})$. In particular we must have $j_1 = j_2$ and any solution of our system of PDEs has to satisfy also the equation $\Delta_1 G_1 - \Delta_2 G_2 = 0$ which is called an *integrability condition* for the system. The system is called *passive* if the left hand side of any of its integrability conditions becomes identical zero after replacement of all principal derivatives in an obvious way. In what follows by calling a system passive we will subsume that it is also orthonomic.

In general, replacing all principal derivatives in the left hand side of an integrability condition yields a function depending on the independent variables and the parametric derivatives. Obviously, the system of PDEs is incompatible if for some integrability condition this function is non-zero and depends only on the independent variables. If neither such an integrability condition exists nor the system is passive we can solve the non-zero integrability conditions for their highest derivative, write them in form (2) and add them to the system of PDEs. Repeating this process eventually we will produce a passive system or will encounter that the system is incompatible.

Example 1 (Part 2). Differentiating Equation (3) twice by y and Equation (4) twice by x yields the integrability condition

$$y v_{xyy} + 2 v_{xy} + x^2 u_{xx} + 4 x u_x + 2u = 0$$

Replacing the principal derivative u_{xx} by the right hand side of Equation (3) yields

$$y v_{xyy} + 2 v_{xy} + x^2 y v_x + 4 x u_x + 2u = 0 \ .$$

Hence, the system is neither passive nor *proved* to be incompatible. We solve the equation for the highest occurring derivative v_{xyy} and add the new equation

$$v_{xyy} = -2 \frac{v_{xy} + 2 x u_x + u}{y} - x^2 v_x \tag{5}$$

to our system. The system formed by Equations (3), (4) and (5) is passive since there are no further (essential) integrability conditions. For the new system we have

$$\mathcal{PR} = \left\{ \frac{\partial^{i+j}}{\partial x^i \partial y^j} u \;\middle|\; i \geq 2 \text{ or } j \geq 2 \right\} \cup \left\{ \frac{\partial^{i+j}}{\partial x^i \partial y^j} v \;\middle|\; i \geq 1 \text{ and } j \geq 2 \right\}$$

$$\mathcal{PA} = \left\{ u, \frac{\partial}{\partial x} u, \frac{\partial}{\partial y} u, \frac{\partial^2}{\partial x \partial y} u, v \right\} \cup \left\{ \frac{\partial^i}{\partial y^i} v, \frac{\partial^i}{\partial x^i} v, \frac{\partial^{i+1}}{\partial x^i \partial y} v \;\middle|\; i = 1, 2, \ldots \right\}$$

The observation that any compatible system of PDEs can be transformed in passive orthonomic form is due to Tresse (1894). Riquier surpassed this result by showing that any system of this particular form has a unique holomorphic solution for arbitrary given initial determinations of a certain type prescribed by the system (see (Riquier , 1910)). Riquier's result makes use of decompositions of each of the sets $\mathcal{PR}$ of principal and $\mathcal{PA}$ of parametric derivatives, and hence also of $\mathcal{DU}$, in finitely many pairwise disjoint cones. Such a cone is given by its vertex which is a derivative $Du_j \in \mathcal{DU}$ and a subset $Y \subseteq \{x_1, \ldots, x_n\}$, where $\Delta(Du_j)$ belongs to the cone if and only if $\Delta \in \mathcal{D}$ is a differential operator involving only variables from Y. We will use the denotation $[Du_j, Y]$ for this cone. The elements of Y are called the *multipliers* and the remaining independent variables the *non-multipliers* for Du_j. Such a decomposition of the set $\mathcal{DU}$ allows to prove the existence of a convergent power series solution for the unknown functions u_j, $j \in \{1, \ldots, k\}$, at an arbitrary given point $(\widehat{x}_1, \ldots, \widehat{x}_n) \in \mathbb{C}^n$ belonging to a region where the system is orthonomic. The particular importance of the cones forming $\mathcal{PA}$ is the description of the initial determinations, more precisely, each cone $[Du_j, Y]$ belonging to $\mathcal{PA}$ provides an initial condition of the form $Du_j|_{\forall x_i \notin Y : x_i = \widehat{x}_i} = \varphi(y_1, \ldots, y_r)$, where $Y = \{y_1, \ldots, y_r\}$ and φ can be chosen as an arbitrary holomorphic function. We will call an orthonomic system of PDEs *complete* if there exists a disjoint decomposition of $\mathcal{PR}$ into cones such that each vertex is the left hand side of an equation of the system (see (Thomas , 1929)).

Example 1 (Part 3). We have the disjoint decompositions

$$\begin{aligned}
\mathcal{PR} &= [u_{xx}, \{x\}] \cup [u_{xxy}, \{x\}] \cup [u_{yy}, \{x, y\}] \cup [v_{xyy}, \{x, y\}] \\
\mathcal{PA} &= [u, \emptyset] \cup [u_x, \emptyset] \cup [u_y, \emptyset] \cup [u_{xy}, \emptyset] \cup [v, \{y\}] \cup [v_x, \{x\}] \cup [v_{xy}, \{x\}]
\end{aligned}$$

Hence, we can extend our system of PDEs to the passive complete form

$$\begin{aligned}
u_{xx} &= y v_x \\
u_{xxy} &= y v_{xy} + v_x \\
u_{yy} &= -x^2 u \\
v_{xyy} &= -2 \frac{v_{xy} + 2x u_x + u}{y} - x^2 v_x \ .
\end{aligned}$$

The system has a uniquely determined holomorphic solution for an arbitrary initial determination $u|_{x=x_0,y=y_0} = c_1, u_x|_{x=x_0,y=y_0} = c_2, u_y|_{x=x_0,y=y_0} = c_3, u_{xy}|_{x=x_0,y=y_0} = c_4, v|_{x=x_0} = \varphi_1(y), v_x|_{y=y_0} = \varphi_2(x)$ and $v_{xy}|_{y=y_0} = \varphi_3(x)$, where $x_0, y_0, c_1, c_2, c_3, c_4$ are complex numbers, $y_0 \neq 0$, and $\varphi_1, \varphi_2, \varphi_3$ are holomorphic functions.

Finally, we can distinguish two aspects of passive (complete) orthonomic systems of PDEs. Firstly, there is a dynamic aspect which consists in the algorithmic transformation of an arbitrary system of PDEs into passive (complete) orthonomic form. Secondly, there is a static aspect consisting in the determination of the solution space of a system of PDEs in passive (complete) orthonomic form. Janet was the first who investigated the dynamic part from the point of view of efficiency and a crucial property of his algorithm is that it directly computes a complete system of PDEs (see (Janet , 1929)).

For an excellent overview on the basic ideas of the Riquier/Janet theory we refer to the article (Thomas , 1929) by Joseph M. Thomas.

3 Gröbner Bases of Polynomial Modules

Let $R = \mathbb{K}[X]$ be the polynomial ring over the field $\mathbb{K}$ in the variables $X = \{x_1, \ldots, x_n\}$, F a free R-module of rank k with basis $\{e_1, \ldots, e_k\}$ and $M \subseteq F$ an arbitrary submodule of F. An *R-term* is a monomial $x_1^{i_1} \cdots x_n^{i_n}$ without coefficient. By *F-term* we denote a module element te_i, where t is an R-term and e_i one of the basis elements of F. If no confusion is possible we will simply speak of terms instead of R- or F-terms. An admissible term order $\prec$ of F is a well-order of the set of all F-terms which is compatible with the multiplication by R-terms. By $\mathrm{lt}_\prec(f)$ we denote the leading term of a non-zero element $f \in F$ with respect to $\prec$, i.e. the largest (w.r.t. $\prec$) term appearing in f with non-zero coefficient. $\mathrm{in}_\prec(f)$ denotes the *initial term* of $f \in F$ with respect to $\prec$, that is $\mathrm{in}_\prec(f) = 0$ in case $f = 0$ and $\mathrm{in}_\prec(f) = c\ \mathrm{lt}_\prec(f)$, where c is the coefficient of $\mathrm{lt}_\prec(f)$ in f, otherwise. For arbitrary subsets $V \subseteq F$ we extend these notions by $\mathrm{lt}_\prec(V) = \{\mathrm{lt}_\prec(v) \mid v \in V \setminus \{0\}\}$ and $\mathrm{in}_\prec(V)$ to be the submodule of F which is generated by all initial terms of elements of V.

Then a (finite) subset $V \subset M$ is called a *Gröbner basis* of M with respect to $\prec$ if and only if $\mathrm{in}_\prec(V) = \mathrm{in}_\prec(M)$. One way to compute a Gröbner basis of M from an arbitrary given finite generating set of M is the application of Buchberger's famous algorithm (see (Buchberger , 1965, 1985); for the module case see also Möller and Mora (1986)). We will illustrate the notions and methods by an example.

Example 2 (Part 1). Consider the polynomial ring $R = \mathbb{C}[x, y]$ and the free R-module F with basis $\{e_1, e_2\}$. Moreover, let $\prec$ be the degreewise lexicographical order of the multiplicative monoid of R-terms which is defined by $x^\alpha y^\beta \prec x^{\alpha'} y^{\beta'}$ iff the first non-zero component of the integer vector $((\alpha + \beta) - (\alpha' + \beta'), \beta - \beta', \alpha - \alpha')$ is negative. $\prec$ is extended to F-terms by $te_i \prec se_j :\Leftrightarrow t \prec s$ or $t = s$ and $i < j$.

Consider the module elements $p = x^2ye_1 - 2xy^2e_2 + x^3e_2$ and $q = 2x^2ye_1 + xye_1 + x^2ye_2$. Then $\mathrm{in}_\prec(p) = -2xy^2e_2$ since $x^3 \prec x^2y \prec xy^2$ and, hence, $x^3e_2 \prec x^2ye_1 \prec xy^2e_2$. Similarly, $\mathrm{in}_\prec(q) = x^2ye_2$ because $xy \prec x^2y$ and $x^2ye_1 \prec x^2ye_2$. Consequently, $\mathrm{in}_\prec(V) = R\ (-2xy^2e_2, x^2ye_2) \subset F$ is the initial module of the set $V = \{p, q\}$. By M we denote the submodule of F generated by V. Then we have $r := xp + 2yq = 4x^2y^2e_1 + x^3ye_1 + x^4e_2 + 2xy^2e_1 \in M$ and since $\mathrm{in}_\prec(r) = 4x^2y^2e_1 \notin \mathrm{in}_\prec(V)$ we deduce that V is not a Gröbner basis of M with respect to $\prec$. (p, q) was the only critical pair of V (see Buchberger (1985)) and since the initial term of the new element r belongs to a different module generator also the extended set $V \cup \{r\}$ has no additional critical pairs. Hence, $\mathrm{in}_\prec(M) = R\ (-2xy^2e_2, x^2ye_2, 4x^2y^2e_1)$, i.e. $\{p, q, r\}$ is a Gröbner basis of M with respect to $\prec$.

For a comprehensive introduction to the theory of Gröbner bases we refer to the survey article Buchberger (1985) or one of the textbooks Adams and Loustaunau (1994); Becker and Weispfenning (1993); Eisenbud (1995).

4 Relationships Between Gröbner Bases and Passive Systems

The idea behind passive complete systems of PDEs can be translated in terms of distinguished Gröbner bases of submodules of a free module F of rank k over the polynomial ring $R = \mathbb{C}[X]$, the so-called involutive bases of polynomial modules. For this purpose let us consider the special case of systems of linear PDEs with constant coefficients. Then in view of the natural isomorphisms between the monoid $\mathcal{D}$ with differentiation, the multiplicative monoid $T = \langle X \rangle$ of R-terms, and the additive monoid $\mathbb{N}^n$, there is a natural isomorphism between the ring $\mathbb{C}[\mathcal{D}]$ of polynomial differential operators and the polynomial ring $R = \mathbb{C}[X]$. The left hand side of a linear partial differential equation $G = 0$ with constant coefficients can be considered as an element of the $\mathbb{C}[\mathcal{D}]$-(left)module $\mathcal{F}$ which is freely generated by the unknown functions $u_1, \ldots, u_k$ and scalar multiplication of $m \in \mathcal{F}$ by $\Delta \in \mathbb{C}[\mathcal{D}]$ means application of the differential operator Δ to m. The modules $\mathcal{F}$ and $F = R^k$ are isomorphic. There is a natural bijection between the equivalence classes of systems of PDEs of the form $G = 0$ with left hand sides in $\mathcal{F}$ and the submodules of F. Moreover, a passive system of PDEs is mapped to a Gröbner basis and vice versa, where the corresponding orders $\prec$ are the same under the natural isomorphism between $\mathcal{D}$ and T.

Let us outline the overlapping area of both theories a little more detailed. First of all, note, none of the theories is completely covered by the other. On the one hand the translation from systems of PDEs to R-modules over some ring R is restricted to linear PDEs. Nevertheless, the condition of constant coefficients can be omitted if one allows so-called D-modules as algebraic counterpart. On the other hand also Gröbner bases can be considered in a much more general context than polynomial modules, see e.g. Apel (2000) and the references therein for huge classes of rings allowing a generalized Gröbner theory. But PDE-analogues to the corresponding Gröbner bases can be considered only for graded structures originating from an $\mathbb{N}^n$-filtration of a ring of functions.

Example 1 (Part 4). The system considered in Example 1 does not fit in the above concept due to the non-constant coefficients. However, it has a natural algebraic translation in a free left module F of rank 2 over the Weyl algebra W_2 in the indeterminates $x, y, \partial_x, \partial_y$, where $\partial_x\, x = x\partial_x + 1, \partial_y\, y = y\partial_y + 1$ and all other pairs of indeterminates commute.

The input translates in the module elements $\partial_x^2 e_1 - y\partial_x\, e_2$ and $\partial_y^2 e_1 + x^2 e_1$, where e_1 and e_2 are the free generators of F. By M we denote the left submodule of F generated by these two elements. Applying the Gröbner basis techniques for finitely generated left modules over Weyl algebras (see Apel and Laßner (1988)) we obtain the left Gröbner basis $\{\partial_x^2 e_1 - y\partial_x\, e_2, \partial_y^2 e_1 + x^2 e_1, y\partial_x\partial_y^2\, e_2 +$

$2\partial_x\partial_y\, e_2 + x^2y\partial_x\, e_2 + 4x\partial_x\, e_1 + 2e_1\}$. Using the methods introduced in (Apel , 1998) it is also possible to compute involutive bases in F (for the notion of an involutive basis see the forthcoming Definition 1). One particular such basis can be obtained by adding the element $\partial_x^2\partial_y\, e_1 - y\partial_x\partial_y\, e_2 - \partial_x\, e_2$ to the above Gröbner basis. Retranslation in the language of PDEs confirms the analogy to our previous results. There remains one difference, namely the division by y appearing in Equation 5 cannot take place in the context of the Weyl algebra W_2. But we could extend W_2 by allowing division by x and y and apply the Gröbner theory developed in (Apel , 2000) which does not require the variables and coefficients to commute.

Example 2 (Part 2). The module elements p and q from Example 2 correspond to the following system of linear PDEs with constant coefficients

$$\begin{aligned} u_{xxy} - 2v_{xyy} + v_{xxx} &= 0 \\ 2u_{xxy} + u_{xy} + v_{xxy} &= 0 \end{aligned}$$

in unknown functions u and v and independent variables x and y. Transformation into orthonomic form yields

$$\begin{aligned} v_{xyy} &= \frac{1}{2}\left(u_{xxy} + v_{xxx}\right) \\ v_{xxy} &= -2u_{xxy} - u_{xy} \end{aligned}$$

Differentiating the first equation by x and the second by y leads to a non-contradicting integrability condition and adding the resulting equation

$$u_{xxyy} = -\frac{1}{4}\left(u_{xxxy} + v_{xxxx} + 2u_{xyy}\right)$$

makes the system passive. Moreover, the system is already complete as the decomposition

$$\mathcal{PR} = [v_{xyy}, \{x, y\}] \cup [v_{xxy}, \{x\}] \cup [u_{xxyy}, \{x, y\}] \tag{6}$$

of the set of principal derivative shows. The decomposition

$$\mathcal{PA} = [v, \{y\}] \cup [v_x, \{x\}] \cup [v_{xy}, \emptyset] \cup [u, \{y\}] \cup [u_x, \{y\}] \cup [u_{xx}, \{x\}] \cup [u_{xxy}, \{x\}]$$

of the set of parametric derivatives implies that the system has a unique holomorphic solution for an arbitrary initial determination of the type
$v_{xy}|_{x=x_0,y=y_0} = c, v|_{x=x_0} = \varphi_1(y), v_x|_{y=y_0} = \varphi_2(x),\ u|_{x=x_0} = \varphi_3(y), u_x|_{x=x_0} = \varphi_4(y), u_{xx}|_{y=y_0} = \varphi_5(x), u_{xxy}|_{y=y_0} = \varphi_6(x)$.

Recall, that the basic property of a Gröbner basis V of the submodule $M \subset F$ with respect to $\prec$ consists in the equality $\mathrm{in}_\prec(M) = \mathrm{in}_\prec(V)$ or, equivalently, in the sum representation

$$\mathrm{in}_\prec(M) = \sum_{v\in V} R\, \mathrm{in}_\prec(v)\ . \tag{7}$$

In case V is the image of a minimal passive complete system of PDEs in F we have the stronger condition

$$\mathrm{in}_\prec(M) = \bigoplus_{v \in V} \mathbb{C}[Y_v]\mathrm{in}_\prec(v) \, . \tag{8}$$

Example 2 (Part 3). From Equation (6) we deduce that $\{p, q, r\}$ is not only a Gröbner basis but even an involutive basis providing the direct sum decomposition $\mathrm{in}_\prec(M) = \mathbb{C}[x, y]\ xy^2e_2 \oplus \mathbb{C}[x]\ x^2ye_2 \oplus \mathbb{C}[x, y]\ x^2y^2e_1$ of the initial module $\mathrm{in}_\prec(M) = \mathrm{in}_\prec(\{p, q, r\})$.

Equation (8) is a good starting point for the definition of an involutive basis of the submodule $M \subset F$ with respect to $\prec$ which we wish to be the analogous notion to a passive complete system of PDEs. In fact, if we restrict our interests to only the static aspect then this equation would be already the correct analogue. However, it is slightly too general in order to reflect also Janet's dynamical aspects in a satisfactory way.

One method for the computation of a passive complete system is to first compute a passive system and to complete it in a subsequent step. Translated to the language of polynomial modules, that is, first to compute a Gröbner basis and afterwards to decompose the initial module in a direct sum of the required type. Actually, this is the idea which is implicitly suggested by Thomas' paper (Thomas , 1929). In contrast, the most important feature of Janet's algorithm consists in the fact, that it combines the completion of the set of principal derivatives and the transformation into passive form (see Janet (1929)). Also alternative definitions of multipliers and non-multipliers introduced in the past, e.g. by Thomas (Thomas , 1929, 1937) or by Pommaret (1978), show the nice behavior that an orthonomic system of PDEs is passive and complete if and only if replacing all principal derivatives in $\frac{\partial}{\partial x}(D_i u_{j_i} - G_i)$ yields zero for all equations $D_i u_{j_i} = G_i$ of the system and all non-multipliers x of $D_i u_{j_i}$.

In fact, this is the crucial condition which enables the application of a Janet like algorithm, see also Figure 1 and the explanations in Section 5.

5 Involutive Bases of Polynomial Modules

In what follows we will consider arbitrary coefficient fields $\mathbb{K}$. The only reason we had to restrict ourselves to the field $\mathbb{K} = \mathbb{C}$ of complex numbers in the previous section was the relation to systems of PDEs. Here we will also switch to the more frequently used right module notation. In our setting of a module over a commutative polynomial ring this makes of course no difference. Note, however, in the general case of PDEs or non-commutative algebraic situations such as the Weyl algebra case considered in Part 4 of Example 1 we would have to take care about the correct sides.

The demands on the notion of involutive basis as a "good" module theoretical analogue to passive complete systems resulting from the investigations made in the previous section can be summarized in two conditions:

1. a minimal involutive basis V of M has to satisfy Equation (8) and
2. there should exist a Janet type algorithm (see Figure 1) which transforms an arbitrary finite generating set of M in an involutive basis V of M.

Two different approaches satisfying both conditions have been introduced by Gerdt and Blinkov (1998) and by Apel (1998). While the Gerdt/Blinkov method saves almost all classical dynamic features our approach maintains only the principal idea behind Janet's algorithm explained at the end of the previous section.

Definition 1. *Let F be a free module of rank k over the polynomial ring $R = \mathbb{K}[X]$ in the indeterminates $X = \{x_1, \ldots, x_n\}$ and M a submodule of F. Moreover, let $\prec$ be an admissible term order of F. Then a subset $V \subset M \setminus \{0\}$ is called a* minimal involutive basis *of M with respect to $\prec$ if there exists a linear order $\sqsubset$ of $\mathrm{lt}_\prec(V)$ and a family $(Y_v)_{v\in V}$ of subsets of X such that*

1. $\mathrm{in}_\prec(M) = \bigoplus_{v\in V} \mathrm{in}_\prec(v)\mathbb{K}[Y_v]$ *and*
2. $\mathrm{in}_\prec(v')\mathbb{K}[X] \cap \mathrm{in}_\prec(v)\mathbb{K}[Y_v] = \{0\}$ *for all $v, v' \in V$ such that* $\mathrm{lt}_\prec(v') \sqsubset \mathrm{lt}_\prec(v)$.

A subset $V' \subseteq M$ containing a subset V which is a minimal involutive basis of M w.r.t. $\prec$ is called an involutive basis *of M w.r.t. $\prec$.*

It is an immediate consequence of Definition 1 that the initial terms of the elements of a minimal involutive basis are pairwise distinct. We will call a family $(Y_v)_{v\in V}$ of subsets of X *admissible* for the ordered set $(\mathrm{lt}_\prec(V), \sqsubset)$ if for all $v, v' \in V \setminus \{0\}$ such that $\mathrm{lt}_\prec(v') \sqsubseteq \mathrm{lt}_\prec(v)$ it holds one of the conditions $\mathrm{in}_\prec(v')\mathbb{K}[Y_{v'}] \subseteq \mathrm{in}_\prec(v)\mathbb{K}[Y_v]$ or $\mathrm{in}_\prec(v)\mathbb{K}[Y_v] \cap \mathrm{in}_\prec(v')\mathbb{K}[X] = \{0\}$. Moreover, by writing that $(Y_v)_{v\in V}$ is admissible for $\mathrm{lt}_\prec(V)$ we express the existence of a linear order $\sqsubset$ on $\mathrm{lt}_\prec(V)$ such that $(Y_v)_{v\in V}$ is admissible for $(\mathrm{lt}_\prec(V), \sqsubset)$. Note, in the language of Apel (1998) a family $(Y'_s)_{s\in S}$ defines an involutive division $\mathcal{M} = (s \cdot \langle Y'_s\rangle)_{s\in S}$. If $S = \mathrm{lt}_\prec(V)$ and $Y_v = Y'_{\mathrm{lt}_\prec(v)}$ for all $v \in V$ then the family $(Y_v)_{v\in V}$ of multiplier sets is admissible for $(\mathrm{lt}_\prec(V), \sqsubset)$ if and only if the involutive division $\mathcal{M} = (s \cdot \langle Y'_s\rangle)_{s\in S}$ is admissible for $(S, \sqsubset)$.

Using the admissibility notion we can say that $V \subset M$ is an involutive basis of M with respect to $\prec$ if and only if there exists a family $(Y_v)_{v\in V}$ of multiplier sets which is admissible for $\mathrm{lt}_\prec(V)$ and satisfies $\mathrm{in}_\prec(M) = \sum_{v\in V} \mathrm{in}_\prec(v)\mathbb{K}[Y_v]$.

Note, there is a close relationship between the notions of minimal involutive bases and *reduced* Gröbner bases. However, since we did not assume that the elements of a minimal involutive basis are tail reduced, the better analogue are the Gröbner bases which are minimal with respect to set inclusion. The following two examples will illustrate Definition 1.

Example 3 (Part 1). Consider the polynomial ring $R = \mathbb{K}[x, y, z, w]$ as a free R-module F of rank 1 and let M be the submodule of F, i.e. the ideal of R, which is generated by the set $V = \{xz, xw, yz, yw\}$ of monomials.

If we order V by $xz \sqsubset xw \sqsubset yz \sqsubset yw$ then there is a unique admissible family of maximal multiplier sets, namely, $Y_{xz} = \{x, y, z, w\}, Y_{xw} = \{x, y, w\}, Y_{yz} = \{y, z, w\}$ and $Y_{yw} = \{y, w\}$. It is easy to verify that the so-defined family $(Y_v)_{v\in V}$

is admissible for $(V, \sqsubset)$. That each of the sets Y_v, $v \in V$, is the only maximal set of multipliers which v can take follows immediately by the observation that for any $v \in V$ and any variable $s \notin Y_v$ there exists $v' \in V$ such that $v' \sqsubset v$ and $v\mathbb{K}[s] \cap v'R \supsetneq \{0\}$ in contradiction to the admissibility conditions. Moreover, one easily observes $M = \mathrm{in}_\prec(M) = xz\mathbb{K}[x,y,z,w] \oplus xw\mathbb{K}[x,y,w] \oplus yz\mathbb{K}[y,z,w] \oplus yw\mathbb{K}[y,w]$ and, therefore, V is an involutive basis of M.

Example 4. In general, the situation is more complicated even for monomial ideals of polynomial rings. Let us consider another example of this type with $R = \mathbb{K}[x,y,z,w]$ and $F = R$ being as in the previous example and $V = \{xy, xz, w\}$.

If V is ordered according to $xy \sqsubset xz \sqsubset w$ then there are two maximal admissible families of multipliers. In both cases we have $Y_{xy} = \{x,y,z,w\}$ and $Y_{xz} = \{x,z,w\}$. But there are two ways to fix a maximal set of multipliers for w, namely either $Y_w = \{y,z,w\}$ or $Y_w = \{x,w\}$. In both cases we have only the inclusion $xy\mathbb{K}[Y_{xy}] \oplus xz\mathbb{K}[Y_{xz}] \oplus w\mathbb{K}[Y_w] \subsetneq M$, hence, none of the two multiplier assignments makes V an involutive basis.

Nevertheless, V is an involutive basis of M. We just need to reorder V according to $w \sqsubset xy \sqsubset xz$. Then $Y_w = \{x,y,z,w\}$, $Y_{xy} = \{x,y,z\}$ and $Y_{xz} = \{x,z\}$ is the one and only maximal admissible choice of the sets of multipliers and one easily verifies the direct sum decomposition $M = w\mathbb{K}[x,y,z,w] \oplus xy\mathbb{K}[x,y,z] \oplus xz\mathbb{K}[x,z]$.

We remind that there are also sets V of monomials, e.g. $V = \{x^2, y^2\}$, which by no linear order $\sqsubset$ and by no admissible family of multiplier sets can be made an involutive basis. Also the question whether there is exactly one way to define a maximal admissible family of multiplier sets for a monomial set V is not related to V being an involutive basis or not. At the first glance Definition 1 seems to have no dynamical part. However, the following theorem shows that Condition 2, which is slightly more restrictive than the property $\mathrm{in}_\prec(v)\mathbb{K}[Y_v] \cap \mathrm{in}_\prec(v')\mathbb{K}[Y_{v'}] = \{0\}$ for all $v, v' \in V$ following already from Condition 1 of Definition 1 alone, enables the application of a Janet like algorithm for the computation of the so-defined involutive bases.

Theorem 1. *Let F be a free module of rank k over the polynomial ring $R = \mathbb{K}[X]$ in the variables $X = \{x_1, \ldots, x_n\}$ and $M \subset F$ a submodule with generating set V, where all elements of V are monic and have pairwise distinct leading terms. Moreover, let $\prec$ be an admissible term order of F, $\sqsubset$ a linear order of $\mathrm{lt}_\prec(V)$ and $(Y_v)_{v \in V}$ a family of multiplier sets which is admissible for the ordered set $(\mathrm{lt}_\prec(V), \sqsubset)$.*

Then with $V' = \{v' \in V \mid \mathrm{in}_\prec(v') \notin \mathrm{in}_\prec(v)\mathbb{K}[Y_v] \text{ for all } v \in V \setminus \{v'\}\}$ the following conditions are equivalent:

1. $\mathrm{in}_\prec(M) = \sum_{v \in V} \mathrm{in}_\prec(v)\mathbb{K}[Y_v]$,
2. $\mathrm{in}_\prec(M) = \bigoplus_{v' \in V'} \mathrm{in}_\prec(v')\mathbb{K}[Y_{v'}]$,
3. *V is a Gröbner basis of M with respect to $\prec$ and for all $w \in V$ and all variables $x \notin Y_w$ it holds* $\mathrm{in}_\prec(xw) = x\,\mathrm{in}_\prec(w) \in \sum_{v \in V} \mathrm{in}_\prec(v)\mathbb{K}[Y_v]$,
4. $(V \setminus V') \subset \sum_{v' \in V'} v'\mathbb{K}[Y_{v'}]$ *and for all $w \in V'$ and all variables $x \notin Y_w$ it holds* $xw \in \sum_{v' \in V'} v'\mathbb{K}[Y_{v'}]$.

Moreover, any of the above conditions implies that V is an involutive basis of M with respect to $\prec$.

Proof. Before we start to prove the equivalences let us make some remarks concerning the last statement. Obviously, V is an involutive basis of M with respect to $\prec$ if Conditions 1. or 2. are satisfied. But one might wonder why the opposite direction should fail to hold. The reason is simply that V could be an involutive basis according to the definition introduced here but the considered family $(Y_v)_{v\in V}$ is not suitable for providing the representations stated in 1. and 2. This problem can be avoided by defining the notion of an involutive basis V with respect to a given order $\sqsubset$ and a given family $(Y_v)_{v\in V}$ in the way it was done in (Apel , 1998).

In what follows, $\langle Y\rangle$ denotes the commutative monoid which is freely generated by some subset $Y \subseteq X$.

The equivalence of 1. and 2. follows immediately from the admissibility of $(Y_v)_{v\in V}$. The implication 1. $\to$ 3. is trivial. Let us sketch the main ideas behind the proof direction 3. $\to$ 1. The essential part consists in proving that for all $w \in V$ and all terms $t \in \langle X\rangle$ there is a representation $tw = a + b$, where $a = \sum_{v\in V} f_v v$ and $b = \sum_{v\in V} g_v v$ such that $f_v, g_v \in R$, only finitely many of the f_v and g_v are non-zero, $f_v \in \mathbb{K}[Y_v]$ for all $v \in V$, and $\mathrm{lt}_\prec(g_v v) \prec \mathrm{lt}_\prec(tw)$ for all $v \in V$ such that $g_v \neq 0$. In case $t \in \langle Y_w\rangle$ this is obvious, so let $x \in X \setminus Y_w$ be a non-multiplier occurring in t. Then by condition 3. we have $\mathrm{in}_\prec(xw) = x\,\mathrm{in}_\prec(w) \in \sum_{v\in V} \mathrm{in}_\prec(v)\mathbb{K}[Y_v]$ and, hence, there exist $w' \in V$ and $s \in \mathbb{K}[Y_{w'}]$ such that $\mathrm{lt}_\prec(xw) = \mathrm{lt}_\prec(sw')$. Since V is a Gröbner basis it follows the existence of a representation $xw - sw' = \sum_{v\in V} g'_v v$, where only finitely many g'_v are non-zero and $\mathrm{lt}_\prec(g'_v v) \prec \mathrm{lt}_\prec(xw)$ for all v such that $g'_v \neq 0$. Consequently, if one can show that $\frac{t}{x} sw'$ has a required representation $a' + b'$ then also $tw = \frac{t}{x} sw' + \sum_{v\in V} \frac{t}{x} g'_v v$ can be represented in the desired way. An obvious idea seems to be to repeat the process recursively and conclude termination by induction on the number of non-multipliers contained in t. But this approach will not work since a non-multiplier for w does not need to be also a non-multiplier for w'. Moreover, relaxing the admissibility condition of $(Y_v)_{v\in V}$ in such a way that only Condition 1 but not necessarily Condition 2 of Definition 1 holds can actually result in an infinite process. Note, there are simple counter examples showing that the implication 3. $\to$ 1. need not to hold in the relaxed case, cf. the forthcoming Example 3 (Part 2). However, the stronger notion of admissibility used here implies $\mathrm{lt}_\prec(w') \sqsubset \mathrm{lt}_\prec(w)$ which indeed ensures termination. Note, that by the finiteness of the number of terms dividing $t\,\mathrm{in}_\prec(w)$ this is even true if V is infinite and $\sqsubset$ is not a well-order. Application of simple inductive arguments on finite representations $m = \sum_{v\in V} h_v v$ of arbitrary elements $m \in M$ finishes the proof of direction 3. $\to$ 1.

The implication 3. $\to$ 4. is obvious and it remains to consider the branch 4. $\to$ 3. An arbitrary element $m \in M$ can be represented in the form $m = \sum_{v\in V} h_v v$, where only finitely many of the $h_v \in R$ are non-zero. According to the first part of 4. we can assume w.l.o.g. $h_v = 0$ for all $v \notin V'$. A rewriting process which successively replaces products of the form xv, where x is a non-multiplier for

$v \in V'$, finally ends up with a finite representation $m = \sum_{v' \in V'} f_{v'} v'$, where $f_{v'} \in \mathbb{K}[Y_{v'}]$. Note, that here the strong definition of admissibility of $(Y_v)_{v \in V}$ is again essential. Now, we can deduce $\mathrm{lt}_\prec(f_{v'} v') \preceq \mathrm{lt}_\prec(m)$ for all $v' \in V'$ such that $f_{v'} \neq 0$ since no initial parts of the summands on the right hand side can cancel out[1]. This proves that V is a Gröbner basis and the second part of 3. follows easily by considering the special case $m = xw$ in our above investigations. □

Fig. 1. Involutive basis construction method of Janet type

Input:
- V ··· finite set of non-zero elements of a $\mathbb{K}[X]$-module M
- $\prec$ ··· admissible term ordering

Output:
- W ··· minimal involutive basis of M with respect to $\prec$

$U :=$ minimal subset of V such that $\mathrm{lt}_\prec(U) = \mathrm{lt}_\prec(V)$
$(Y_v)_{v \in U} :=$ admissible family for $\mathrm{lt}_\prec(U)$
$W := \left\{ w \in U \mid \mathrm{in}_\prec(w) \notin \bigoplus_{v \in U \setminus \{w\}} \mathrm{in}_\prec(v)\mathbb{K}[Y_v] \right\}$
$L := \{(1, v) \mid v \in V \setminus W\} \cup \{(y, w) \mid w \in W, y \in X \setminus Y_w\}$
while $L \neq \emptyset$ *do*
  choose $(t, u) \in L$
  $L := L \setminus \{(t, u)\}$
  $w :=$ involutive normal form of tu modulo W w.r.t. $(Y_v)_{v \in W}$ and $\prec$
  if $w \neq 0$ **then**
    $V := V \cup \{w\}$
    $U :=$ minimal subset of V such that $\mathrm{lt}_\prec(U) = \mathrm{lt}_\prec(V)$
    $(Y_v)_{v \in U} :=$ admissible family for $\mathrm{lt}_\prec(U)$
    $W := \left\{ w \in U \mid \mathrm{in}_\prec(w) \notin \bigoplus_{v \in U \setminus \{w\}} \mathrm{in}_\prec(v)\mathbb{K}[Y_v] \right\}$
    $L := \{(1, v) \mid v \in V \setminus W\} \cup \{(y, w) \mid w \in W, y \in X \setminus Y_w\}$
  end if
end while
return(W)

Figure 1 sketches the global structure of a Janet like method for computing an involutive basis of a given R-module. Some further details are necessary in order to make the presented frame algorithmic. A couple of ways to achieve this will be mentioned below.

First of all, we will explain the meaning of some objects used in our method. According to the specification it is allowed that various elements of the input basis V have the same leading term. U is a maximal subset of elements of V whose leading terms are pairwise distinct. The family $(Y_v)_{v \in U}$ of multiplier sets which is admissible for $\mathrm{lt}_\prec(V) = \mathrm{lt}_\prec(U)$ is indexed by the subset $U \subseteq V$ since

[1] Note, by the same argument it will follow immediately that the sum $\sum_{v' \in V'} v'\mathbb{K}[Y_{v'}]$ is direct, i.e. $\sum_{v' \in V'} v'\mathbb{K}[Y_{v'}] = \bigoplus_{v' \in V'} v'\mathbb{K}[Y_{v'}]$.

$Y_v = Y_{v'}$ must hold for all $v, v' \in V$ such that $\mathrm{lt}_\prec(v) = \mathrm{lt}_\prec(v')$ according to the admissibility property. After fixing $(Y_v)_{v\in U}$ we construct the set W as a maximal subset of U such that the sum $\sum_{v\in W} \mathrm{in}_\prec(v)\mathbb{K}[Y_v]$ is direct, i.e. $\mathrm{lt}_\prec(tv) \neq \mathrm{lt}_\prec(t'v')$ for all $v, v' \in W$, $t \in \langle Y_v\rangle$, $t' \in \langle Y_{v'}\rangle$. L is a set consisting of two types of critical pairs (t, u), where all of them have the characteristic property $\mathrm{in}_\prec(tu) \in \bigoplus_{v\in W} \mathrm{in}_\prec(v)\mathbb{K}[Y_v]$, i.e. tu is involutively reducible modulo W with respect to the admissible family $(Y_v)_{v\in W}$.

The global structure of the method displayed in Figure 1 is this of a critical element/completion algorithm. The main type of critical elements are the so-called *non-multiplicative prolongations* $(y, w) \in (X \setminus Y_w) \times W$. A second type are the pairs $(1, v)$, where the leading term of $v \in V$ is involutively reducible by some other element of V. Note, the second type of critical pairs does not occur when the leading terms of the input basis elements are pairwise distinct and Janet's definition of multipliers is used. In case the reduction of the polynomial tu resulting from the critical pair (t, u) yields a non-zero remainder w the basis is extended by w and the check is repeated. We remark the fact that completion of W by non-zero reduction remainders of non-multiplicative prolongations (and if applicable elements of $V \setminus W$) does not only complete the set of leading terms of W but at the same time completes W to a Gröbner basis of M without explicitly computing Buchberger's S-polynomials as the distinguishing feature of a Janet like algorithm.

If tu has involutive remainder 0 modulo W for all pairs $(t, u) \in L$ then W is an involutive basis of M according to Condition 4 of Theorem 1. Hence, the method displayed in Figure 1 works correctly provided that it terminates. A series of further restrictions is necessary in order to ensure termination for arbitrary inputs satisfying the specification.

The extension of V, and hence U, during the completion process requires the adaption of the admissible family $(Y_v)_{v\in U}$ of multiplier sets. Janet solved this problem by giving a general rule how to adapt the sets of multipliers and proved termination for his particular multiplier choice. But it turns out that the process will also terminate if one chooses the sets of multipliers in each step completely new, taking care only that the multiplier sets are "sufficiently large". More precisely, "sufficiently large" means $x \in Y_v$ for all $v \in U$ and $x \in X$ such that $\deg_x \mathrm{lt}_\prec(v) \geq \deg_x \mathrm{lt}_\prec(v')$ for all $v' \in U$. In the language of Apel (1998) these admissible families correspond exactly to the involutive divisions refining the *Thomas division on* $\mathrm{lt}_\prec(U)$, which is defined by the multiplier sets $Y_v^T = \{x \in X \mid \forall v' \in U : \deg_x v \geq \deg_x v'\}$, $v \in U$. The advantage of such an approach is the possibility of a better adjustment of the admissible family $(Y_v)_{v\in U}$ to the concrete intermediate basis. However, this freedom in choice causes a large overhead and some heuristical restrictions are advisable in order to find a compromise. A detailed analysis how to compute the families $(Y_v)_{v\in U}$ and a detailed discussion of the algorithm which completes an arbitrary finite generating set of M to a finite (minimal) involutive basis of M can be found in (Apel , 1998). Nowadays, in view of the possibility to use Hemmecke's *sliced divisions* for initializing and adapting the family $(Y_v)_{v\in U}$ (see Hemmecke (2001)) in connection with the application of the criteria introduced by Apel and Hemmecke (2002) parts of the heuristics from (Apel , 1998) appear in a new light. In particular, the overhead caused by multiple reductions of non-multiplicative prolongations seems to be rather small for the sliced divisions strategy though the order $\sqsubset$ is changed during the adaption of the involutive division, or equivalently the admissible family of multiplier sets, to the intermediate basis.

Another generalization of Janet's method is the Gerdt/Blinkov approach which follows the classical method of fixing a priori all sets of multipliers, i.e. of fixing the families $(Y_s)_{s\in S}$ for all finite sets S of monomials. In this context a series of technical restrictions is necessary in order to ensure the termination of the algorithm. In (Apel , 1998) it is proved that there does not exist any family of multiplier assignments satisfying all conditions of Gerdt and Blinkov (1998) and having the additional property that for all finite sets of monomials the corresponding multiplier family is maximal. However, the Gerdt/Blinkov approach is also not subsumed by the method discussed here since it might include assignments of multiplier sets which violate Condition 2 of our Definition 1. It is an open question whether there are situations where one can take advantage of this fact.

Note, all methods discussed so far have in common that, in addition, the critical pairs $(u, h) \in L$ have to be processed according to the *normal selection strategy*, i.e. $\mathrm{lt}_{\prec}(uh)$ must be minimal with respect to $\prec$, in order to ensure termination for any specified input. Experiments show that the normal selection strategy is not preferable in Buchberger's algorithm for the computation of Gröbner bases. State of the art implementations frequently use *sugar strategy* instead (see Giovini et al. (1991)). In (Gerdt and Blinkov , 1998) Gerdt and Blinkov where the first who transfered Buchberger's criteria for detecting unnecessary critical pairs to the involutive method. Recently it could be shown by Apel and Hemmecke (2002) that the involutive basis algorithm terminates independent of the pair selection strategy if a series of criteria including those of Gerdt and Blinkov are applied in order to avoid the treatment of certain pairs $(u, h) \in L$.

6 "Good" Involutive Bases

There are theoretical as well as computational issues which pose further conditions on a "good" choice of an involutive basis V of a module $M \subset F$. Some of them are related to questions of the following type:

1. What is the minimal value of the sum $\sum_{v\in V} |X \setminus Y_v|$ which an involutive basis V of M can take?
2. What is the minimal number of elements of an involutive basis V of M?
3. What is the minimal highest degree of the elements of an involutive basis of M?
4. What is the maximal number d for which exist $V \subset M$ and a multiplier family $(Y_v)_{v\in V}$ making V an involutive basis of M such that $|Y_v| \geq d$ for all $v \in V$?

In case of generic coordinates and a degreewise reverse lexicographical term order $\prec$ Questions 1. - 3. have simple answers in terms of well-known algebraic invariants. In this case Bayer and Stillman (1987) could show that the crucial invariants of the module M coincide with those of its generic initial module, some generalizations of their results which are required here are due to Eisenbud (1995), and Mall (1998) proved that, under the same conditions, any set V such that $\mathrm{lt}_\prec(V)$ consists of the minimal monomial generators of $\mathrm{in}_\prec(M)$ becomes an involutive basis of M when the multipliers are assigned in a Pommaret like way. In case $rank\, F = 1$ the results of Bayer/Stillman, Eisenbud, and Mall answer also Question 4.

Let us consider the much more delicate but also much more interesting case of non-generic coordinates. We start with the investigation of involutive bases which are "good" in the sense that they can be computed in a minimal number of steps. The importance of the first three questions for a complexity analysis of the completion algorithm is obvious. In particular, the first question is highly interesting since the number $\sum_{v\in V}|X \setminus Y_v|$ provides an estimate for the costs of the involutive basis verification algorithm. In case of homogeneous modules M and the input generating set V' being a minimal homogeneous generating set of M the completion algorithm to involutive form has the same costs under the additional assumption that we have an oracle which tells us how to define the multipliers for the intermediate generating sets in the same way as they will appear in the final output. Note, the complexity analysis is harder than in the case of Buchberger's algorithm where analogous statements hold without an oracle. We can offer a heuristics for the multiplier assignment which in some sense is a static approximation of the oracle. While, in general, Question 1 is difficult to answer it is always easy to find a family $(Y_v)_{v\in V}$ of admissible multiplier assignments such that $\sum_{v\in V}|X \setminus Y_v|$ is minimal for a given finite set V, a given term order $\prec$, and a given linear order $\sqsubset$ of $\mathrm{lt}_\prec(V)$. Note, we neither require $M = \sum_{v\in V} v\mathbb{K}[Y_v]$ (which clearly would be unfulfillable in general) nor that $\sqsubset$ and $\prec$ are optimal in whatsoever sense. Let us discuss the objective of minimizing $\sum_{v\in V}|X \setminus Y_v|$ a little more detailed. In order to have a trivial intersection $v\mathbb{K}[Y_v] \cap v'\mathbb{K}[Y_{v'}] = \{0\}$ it is necessary and sufficient to ensure $\mathrm{lcm}(v, v') \notin v\mathbb{K}[Y_v] \cap v'\mathbb{K}[Y_{v'}]$, which is exactly the case if at least one of the conditions $\frac{\mathrm{lcm}(v,v')}{v} \notin \mathbb{K}[Y_v]$ or $\frac{\mathrm{lcm}(v,v')}{v'} \notin \mathbb{K}[Y_{v'}]$ holds. How this property is achieved by the different approaches applied in the past? Thomas uses the most rigid way which consists in requiring that for any distinct elements $v, v' \in V$ no variable of $\frac{\mathrm{lcm}(v,v')}{v}$ belongs to Y_v and no variable of $\frac{\mathrm{lcm}(v,v')}{v'}$ belongs to $Y_{v'}$. The method due to Janet is much more sophisticated. It enumerates the variables and requires that for any two distinct elements $v, v' \in V$ the first variable x in which v and v' have distinct degrees, without loss of generality let us assume $\deg_x v < \deg_x v'$, is not contained in Y_v and, therefore, Janet's method ensures $\frac{\mathrm{lcm}(v,v')}{v} \notin \mathbb{K}[Y_v]$ by introducing a single condition $x \notin Y_v$ for the pair (v, v'). Janet's approach sounds already very promising but still can be improved for two reasons. Firstly, it does not make any use of inclusions $v'\mathbb{K}[Y_{v'}] \subset v\mathbb{K}[Y_v]$ which might allow to waive the condition $x \notin Y_v$ for the pair (v, v') in case $v \mid v'$

and $Y_{v'} \subseteq Y_v \cup \{x\}$. Secondly, it always poses a condition on the first variable x in which v and v' have different degrees. But it can happen that the consideration of v and a third basis element $v'' \in V$ yields a condition $y \notin Y_v$ in such a way that by chance also $\deg_y v < \deg_y v'$. In this case the single condition $y \notin Y_v$ ensures already $v\mathbb{K}[Y_v] \cap v'\mathbb{K}[Y_{v'}] = v\mathbb{K}[Y_v] \cap v''\mathbb{K}[Y_{v''}] = \{0\}$ and the condition $x \notin Y_v$ can be refused again. By removing redundant admissibility conditions one obtains an admissible refinement of the Janet division. See (Apel , 1998, Figure 2) for an algorithm which computes a (sub-)maximal refinement for an arbitrary given admissible family of multiplier sets.

Example 5. Consider the ideal M generated by $V = \{x_2x_3^2, x_2^2x_3, x_1x_2^2\}$ in $F = R = \mathbb{K}[x_1, x_2, x_3]$. Janet's sets of multipliers are $Y_{x_2x_3^2} = \{x_3\}$, $Y_{x_2^2x_3} = \{x_2, x_3\}$ and $Y_{x_1x_2^2} = \{x_1, x_2, x_3\}$. A better assignment is $Y'_{x_2x_3^2} = \{x_1, x_3\}$, $Y'_{x_2^2x_3} = \{x_2, x_3\}$ and $Y'_{x_1x_2^2} = \{x_1, x_2, x_3\}$. Not only that $\sum_{v\in V} |X \setminus Y'_v| = 2 < 3 = \sum_{v\in V} |X \setminus Y_v|$, we have even the proper inclusion $\{xv \mid v \in V \text{ and } x \in X \setminus Y'_v\} \subset \{xv \mid v \in V \text{ and } x \in X \setminus Y_v\}$ of the sets of elements which have to be reduced to zero during an involutive basis check. Hence, the running time in case of success is not only heuristically but provably faster for the second family of multipliers. Finally, we observe that the family $\left(Y'_{x_2x_3^2}, Y'_{x_2^2x_3}, Y'_{x_1x_2^2}\right)$ yields the decomposition $M = x_2x_3^2\mathbb{K}[x_1, x_3] \oplus x_2^2x_3\mathbb{K}[x_2, x_3] \oplus x_1x_2^2\mathbb{K}[x_1, x_2, x_3]$ showing that V is an involutive basis of M. In contrast the original Janet assignment fails the check since $x_1x_2x_3^2 \in M \setminus \left(x_2x_3^2\mathbb{K}[x_3] \oplus x_2^2x_3\mathbb{K}[x_2, x_3] \oplus x_1x_2^2\mathbb{K}[x_1, x_2, x_3]\right)$, i.e. V is not a Janet basis of M.

A mild variation of the above static approach which includes also dynamic features without essentially increasing the costs is to look for an admissible multiplier assignment $(Y_v)_{v\in V}$ such that the sum $\sum_{v\in V} |X \setminus (Y_v \cup Z_v)|$, where $Z_v \subseteq X$ denotes the set of all variables x for which xv had been reduced already during the previous completion process, becomes minimal. If a fixed linear order $\sqsubset$ of the set of all terms is used during the completion algorithm then this number is the better approximation for the remaining costs of the completion process since no repeated reductions are necessary under these conditions (see (Apel , 1998)). The basic idea behind the strategy suggested in (Apel , 1998, Remark 6.2) is to choose the multipliers according to this heuristics.

Now let us consider another notion of "good" involutive bases, namely, such which provide the maximal value d introduced in Question 4. The search for involutive bases which are "good" in such a sense is strongly related to the solution of combinatorial problems and the computation of invariants of the module. There is the following open conjecture due to Stanley (1982): an arbitrary monomial module M can be decomposed in the form (8) such that $|Y_v| \geq \mathit{depth}\, M$ for all $v \in V$. In (Apel , 2001 a) this conjecture could be proved for some huge classes of modules in the case $\mathit{rank}\, F = 1$ by proving the existence of "good" involutive bases, i.e. such which for a suitable multiplier definition satisfy $d \geq \mathit{depth}\, M$. This property is even more restrictive than conjectured by Stanley since the additional Condition 2 of Definition 1 holds. So it is not surprising that the class of involutive bases defined in Definition 1 is not rich enough to prove Stanley's conjecture in general. The following simple counter examples illustrates that no definition of involutive bases allowing a Janet type algorithm need to provide the maximal possible d.

Example 3 (Part 2). In Part 1 we observed that $V = \{xz, xw, yz, yw\}$ is an involutive basis and one easily verifies that the largest element of V with respect to any linear order $\sqsubset$ will have at most two multipliers. However, M can be decomposed also in the form $M = xz\mathbb{K}[x,z,w] \oplus xw\mathbb{K}[x,y,w] \oplus yz\mathbb{K}[x,y,z] \oplus yw\mathbb{K}[y,z,w] \oplus xyzw\mathbb{K}[x,y,z,w]$ with vertices from the larger generating set $V' = \{xz, xw, yz, yw, xyzw\}$ of M. While the corresponding multiplier sets satisfy Equation (8) they do not allow a Janet like algorithm. Note, that V' and the above family of multipliers satisfy the last two but violate the first two conditions of Theorem 1. One easily observes that Condition 2 of Definition 1 is not satisfied for any linear order $\sqsubset$ of V'.

The above example shows that even in the case that the minimal generators of a monomial module M can be used as the vertices of a direct sum decomposition (8) of M such a decomposition need not be the "best" possible with respect to Question 4. Consequently, "good" in the sense of the first three questions can be quite distinct from "good" in the sense of the last question. The difficulties one meets in the study of Stanley's conjecture make clear that a relaxation of the assignment rules for the multipliers will not only disable Janet's algorithm but will have also impact on the costs of the alternative method which consists in first computing a Gröbner basis and doing the direct sum decomposition of the initial module subsequently. In fact, this shows that the sometimes underestimated task of computing an involutive basis of a given monomial module is not easy if additional conditions are posed on the decomposition. Note, there is an obvious but infeasible algorithm for solving this problem which is based on the simple observation that the number of decompositions of type (8) in maximal direct summands is finite. During the search for suitable initial determinations of a system of PDEs the demands on the decomposition of the set $\mathcal{PA}$ of parametric derivatives in disjoint cones are often similar to those of Stanley. Therefore, the investigation of Stanley's conjecture for modules R/I (see (Apel , 2001 b)) can contribute to this part of the Riquier/Janet theory which seems to be much less investigated in the past.

7 Concluding Remarks

The observation of Zharkov and Blinkov (1993) that there is something interesting at the junction of passive complete orthonomic systems of PDEs and Gröbner bases of polynomial ideals was the starting point of the investigation of involutive bases. Zharkov and Blinkov's motivation was to find a fast alternative algorithm for the computation of Gröbner bases in polynomial rings and a series of remarkable results and computer experiments in this direction have been reported in the past (c.f. Gerdt et al. (2001), Hemmecke (2001)). Each comparison depends strongly on the used implementations since Buchberger's algorithm for the computation of Gröbner bases and Janet's algorithm for the computation of involutive bases are of the same complexity order. Though, Gerdt/Blinkov/Yanovich compared to todays state of the art implementations of Buchberger's algorithm there still remains a little danger that at some day the original justification of (polynomial) involutive bases might disappear, for instance, when an essentially improvement in the strategies of Buchberger's algorithm will be found. This is the reason why one should also have in mind theoretical justifications resulting from the additional structure of involutive bases. This additional structure consists in a direct sum decomposition of the initial module and allows, for instance, to give a closed formula for the Hilbert function (see (Apel , 1998)) or to compute Stanley decompositions (see (Apel , 2001 a,b)).

The quite different approaches due to Gerdt and Blinkov (1998) and Apel (1998), respectively, show that there is no canonical generalization of Riquier's ideas to rings and modules. An objective of this article is to convince the reader that there is certainly no "best" algebraic generalization and that there is still a wide open field in finding "good" ones depending on the application one has in mind. The application might be one of the previously investigated as well as some completely new which probably will be discovered in the future.

Bibliography

W. W. Adams, P. Loustaunau. An Introduction to Gröbner Bases, *Graduate Studies in Mathematics*, Vol. **3**, AMS Press, Providence, (1994).

J. Apel. The Theory of Involutive Divisions and an Application to Hilbert Function Computations. *J. Symb. Comp.* **25**, 683-704 (1998).

J. Apel. Computational Ideal Theory in Finitely Generated Extension Rings. *Theoretical Computer Science*, **244/1-2**, 1–33 (2000).

J. Apel. On a Conjecture of R. P. Stanley; Part I – Monomial Ideals. *MSRI Preprint* 2001-004 (2001).

J. Apel. On a Conjecture of R. P. Stanley; Part II – Quotients modulo Monomial Ideals. *MSRI Preprint* 2001-009 (2001).

J. Apel. Stanley Decompositions and Riquier Bases. Talk presented at the Conference on Applications of Computer Algebra (ACA'01), Albuquerque (2001).

J. Apel, R. Hemmecke. Detecting Unnecessary Reductions in an Involutive Basis Computation. Work in Progress.

J. Apel, W. Laßner. An Extension of Buchberger's Algorithm and Calculations in Enveloping Fields of Lie Algebras. *J. Symb. Comp.* **6**, 361–370 (1988).

D. Bayer, M. Stillman. A Criterion for Detecting m-Regularity. *Invent. math.* **87**, 1–11 (1987).

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

B. Buchberger. Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal, *Ph.D. Thesis*, University of Innsbruck, (1965).

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

D. Eisenbud. Commutative Algebra. With a view toward algebraic geometry. Graduate Texts in Mathematics, **150**. *Springer-Verlag*, New York, (1995).

V. P. Gerdt, Yu. A. Blinkov. Involutive Bases of Polynomial Ideals. *Mathematics and Computers in Simulation* **45**, 519–542 (1998).

V. P. Gerdt, Yu. A. Blinkov, D. A. Yanovich. Fast Computation of Polynomial Janet Bases. Talk presented at the Conference on Applications of Computer Algebra (ACA'01), Albuquerque (2001).

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.

R. Hemmecke. Dynamical Aspects of Involutive Bases Computations. SNSC'01, Linz (2001), This Volume.

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

D. Mall, On the Relation Between Gröbner and Pommaret Bases. *AAECC* **9**/2, 117–123 (1998).

H. M. Möller, T. Mora. New Constructive Methods in Classical Ideal Theory, *J.Algebra* **100**, 138–178, (1986).

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

C. H. Riquier. Les systémes d'equations aux dérivées partielles. *Gauthier-Villars*, Paris (1910).

R. P. Stanley. Linear Diophantine Equations and Local Cohomology. *Invent. math.* **68**, 175–193 (1982).

J. M. Thomas. Riquier's Existence Theorems. *Annals of Mathematics* **30/2**, 285–310 (1929).

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

A. R. Tresse. Sur les invariants différentials des groupes continus de transformations. *Acta Mathematica* **18**, 1–8 (1894).

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