Some Approaches to Construction of Standard Bases in Commutative and Differential Algebra

E.V. Pankratiev

Department of Mechanics and Mathematics
Moscow State University
Vorobyovy Gory, Moscow, Russia
pankrat@shade.msu.ru

Abstract. In this talk I would like to present the directions of research and some results obtained by the Moscow team involved in INTAS grant 99-1222 related to the theory of standard bases in polynomial and differential rings and modules.

The concept of the Gröbner basis introduced by B. Buchberger is a basic one in the constructive theory of polynomial ideals and is studied in detail by numerous researchers. To introduce this notion we must endow the set of monomials with an admissible order, e.g., lexicographic, or total degree then lexicographic, or total degree then inverse lexicographic [6, p. 71]. Then, for any polynomial, we can define its leading monomial, for any pair of polynomials $f, g \in K[x_1, \ldots, x_n]$ we define a relation of reduction $f \underset{g}{\rightarrow} f'$ (an analogue of polynomial remainder), and for any $f \in K[x_1, \ldots, x_n]$ and a set $G = \{g_1, \ldots, g_k\}$, $g_i \in K[x_1, \ldots, x_n]$, $i = 1, \ldots, k$, we define a relation of reduction $f \overset{*}{\underset{G}{\rightarrow}} f'$, and, for any pair $f_1, f_2 \in K[x_1, \ldots, x_n]$, we can define their S-polynomial $S(f_1, f_2)$. The exact definitions can be found in any paper on Gröbner bases, in particular, one can find in [19] a rather long list of definitions of Gröbner bases; some of them are presented below. Although the Gröbner basis of a polynomial ideal is not uniquely defined, one can distinguish among all the Gröbner bases of the ideal an autoreduced Gröbner basis which is defined uniquely up to multiplication of its elements by elements of the field K. Remember that a set G of polynomials is called autoreduced if, for any $f, g \in G$, no monomial which is present in f with nonzero coefficient is divisible by the leading monomial of g.

The following conditions on an autoreduced subset $\mathcal{A}$ of a polynomial ideal I are each equivalent to the requirement that $\mathcal{A}$ is the autoreduced Gröbner basis of I:

1. the leading monomials of the elements of $\mathcal{A}$ generate the set of leading monomials of the elements of I;
2. the reduction relation $\overset{*}{\underset{\mathcal{A}}{\rightarrow}}$ satisfies the following property: for any $f_1, f_2 \in K[x_1, \ldots, x_n]$ and for irreducible $r_1, r_2 \in K[x_1, \ldots, x_n]$ such that $f_i \overset{*}{\underset{\mathcal{A}}{\rightarrow}} r_i$, $i = 1, 2$,

$$f_1 - f_2 \in I \iff r_1 = r_2$$

   (in this case, we say that $\overset{*}{\underset{\mathcal{A}}{\rightarrow}}$ is a canonical simplifier);
3. the reduction relation $\overset{*}{\underset{\mathcal{A}}{\rightarrow}}$ satisfies the following property:

$$f \overset{*}{\underset{\mathcal{A}}{\rightarrow}} 0 \iff f \in I;$$

   (in this case, we say that $\overset{*}{\underset{\mathcal{A}}{\rightarrow}}$ is a normal simplifier);
4. $\mathcal{A}$ is the autoreduced subset of I of minimal rank (we call such a set the characteristic set of the ideal);
5. $\mathcal{A}$ generates I and is any S-polynomial $S(g_1, g_2)$, $g_1, g_2 \in \mathcal{A}$, is reducible to zero (we call such a set coherent).

There is a well-known algorithm for constructing the autoreduced Gröbner basis of an ideal specified by an arbitrary finite system of generators $I = (g_1, \ldots, g_k)$. This algorithm is called the *completion* algorithm or *Buchberger's* algorithm. Its simplest form is the following:

Completion algorithm

input: a set of polynomials $G = \{g_1, \ldots, g_l\}$.
output: the Gröbner basis $G = \{g_1, \ldots, g_k\}$ of the ideal (G).

begin any pair $g_i, g_j \in G$
reduce the S-polynomial $S(g_i, g_j)$ (compute the normal form $NF(S(g_i, g_j))$)
if $NF(S(g_i, g_j)) \neq 0$ **then**
$G = G \cup \{NF(S(g_i, g_j))\}$
autoreduce G
end

Note that there are several "degrees of freedom" in this algorithm that can be employed for making it more efficient. First, certain criteria can be applied for eliminating some pairs (g_i, g_j) from consideration, in particular, "the triangle rule". Second, different strategies can be used for choosing the current pair (g_i, g_j) and different normal form algorithms can be applied. The autoreduction procedure can be run at different stages.

Moreover, in some cases it is expedient to find the Gröbner basis with respect to an ordering (total degree then inverse lexicographic) and to use this basis as the initial data for determining the Gröbner basis with respect to the lexicographic ordering (the Gröbner walk procedure).

For a polynomial ideal I, property (1) of Gröbner bases allows one to construct the so-called G-representation for any element $f \in I$

$$f = \sum_j m_j g_{i(j)},$$

where m_j are monomials, $g_i = g_{i(j)} \in G$, G is the Gröbner basis of I, and $\mathrm{lm}(m_j g_{i(j)}) > \mathrm{lm}(m_{j+1} g_{i(j+1)})$ for any j (lm stands for "leading monomial"). Note that this property can be used as another equivalent definition of Gröbner bases. This representation is in general not unique. To obtain a unique G-representation, we must specify a one-value mapping from the set of all leading monomials of polynomials from the ideal I onto the set of leading monomials of polynomials from the set G (in [18], [15] such representations are called the normal G-representations).

A very important class of Gröbner bases, for which the uniqueness of a special form of G-representation holds, is the class of involutive bases. The theory of involutive bases was developed by Zharkov, Blinkov, Gerdt, Apel [25], [8], [1]. The relations between the Gröbner and involutive bases are studied by different researchers (see, e.g., [2]). To define an involutive basis of a polynomial ideal, we must specify, along with an admissible ordering of monomials, an involutive division on the monomials. The most widely used involutive divisions are called the Janet division, the Pommaret division, and the Thomas division. An axiomatic definition of involutive division is given, e.g., in [8]. It seems to be rather general, and "good" involutive divisions should satisfy some additional conditions. Some such conditions are presented in [8] and in [1]. A. Semenov compared admissible involutive divisions introduced by J. Apel [1] with continuous involutive divisions considered in [8] and introduced a property of *strong continuity* [23]. Similarly to the case of Gröbner bases, the problem of passing from one involutive basis to another one can be considered. An algorithm for its solution is proposed by Golubitsky [11].

The situation in differential algebra is much more complicated. For describing differential equations by algebraic tools, two kinds of algebraic objects are used. Linear partial differential equations are described in terms of modules over the rings of differential operators. The theory of Gröbner bases can be extended to submodules of free differential modules almost completely.

The ring of differential polynomials used for investigating algebraic differential equations is a much more complicated object. There are several approaches to constructing the theory of differential Gröbner bases [4], [20], [17].

F. Ollivier [20] endows the set of differential monomials with an admissible order and defines derivation operations on the set of differential monomials (note that a derivation operation applied to a differential monomial in the ring of differential polynomials gives a differential polynomial). Then, he defines a standard basis of a differential ideal as a set satisfying property 1 for differential ideals. The main deficiency of this definition is that, as a rule, such a basis is infinite. For example, the standard basis in this sense for the differential ideal $[y^2]$ in the ring of ordinary differential polynomials $C\{y\}$ is infinite.

The existence of infinitely generated differential polynomial ideals (which have no finite systems of generators) prevents us from attempts to construct a theory of (finite) differential Gröbner bases applicable for all differential ideals. First of all, we must restrict the set of ideals under consideration. To satisfy the ascending chain condition, we restrict ourselves by consideration of perfect (radical) differential ideals. However, it is unbelievable that one can construct a constructive theory of perfect differential ideals.

Considering the ring of differential polynomials $\mathcal{R} = \mathcal{F}\{y_1, \ldots, y_n\}$ over a differential field $\mathcal{F}$ with a set of derivation operators $\Delta = \{\delta_1, \ldots, \delta_m\}$ we introduce an admissible order on the set of derivatives $\Theta = \{\delta_1^{i_1} \ldots \delta_m^{i_m} y_j\}$, where $i_1, \ldots, i_m \geq 0$, $1 \leq j \leq n$. For any differential polynomial $f \in \mathcal{R}$, the highest derivative $\theta \in \Theta$ present in f is called the *leader* of f (we write $\theta = L_f$). By $S_f = \partial f / \partial L_f$ we denote the *separant* of f and by I_f we denote the *initial* of f (the leading coefficient of f considered as a polynomial in L_f), and we denote $H_f = S_f I_f$. The relation of differential reduction $f \underset{g}{\rightarrow} f_1$ allows one to eliminate form f the proper derivatives of L_g as well as the powers of L_g higher than or equal to those present in g. However, in this process, we should multiply f by some powers of S_g and I_g; hence, we cannot obtain in this way a relation satisfying property (2).

The main tool used for the investigation of differential ideals is the theory of autoreduced (characteristic) sets developed by J. Ritt [21] and E. Kolchin [13]. It is known that, for a prime differential ideal I, if an autoreduced set $\mathcal{A}$ satisfies property (4), then properties (3) and (5) are also fulfilled. The problem is how to construct the primary decomposition of a perfect differential ideal $I = \{\mathcal{A}\}$? This problem is very hard.

For example, consider a perfect differential ideal $I = \{\mathcal{A}\}$ generated (as a perfect differential ideal) by one irreducible ordinary differential polynomial $\mathcal{A} = \{f\}$. The primary decomposition of I consists in this case of a general component, for which $\mathcal{A}$ is the minimal autoreduced set, and, possibly, singular components. As a rule, f does not generate the general component as the differential ideal $\{\mathcal{A}\}$. M.V. Kondratieva proposed a partial method for determining the generators of this prime differential ideal and for constructing the primary decomposition [14]. She also obtained the following sufficient condition for the perfect differential ideal $I = \{\mathcal{A}\}$ to be prime.

Theorem 1. *Let* $f = y^{(k)} y^{(s)} + y^{(k+1)} + y^{(k)} * g(y, y', \ldots y^{(s+1)})$, *where* $s > k+1$. *Then,* $[f] : H_f^{\infty} = \{f\}$.

There are several generalizations of the Buchberger algorithm to the differential case which are called by different authors the Ritt–Kolchin algorithms. Remember that Ritt and Kolchin considered primary decompositions of perfect differential ideals. It is very difficult to develop an algorithm for constructing this decomposition. Thus, the Ritt–Kolchin algorithms give only a partial solution of the problem.

It was noted above that the solution is complete for linear partial differential systems. Constructing the theory of differential Gröbner bases, E. Mansfield [17] considers autoreduced differential systems

satisfying some additional conditions, namely, CNI (Coherent with Null Intersection), SPR ($S(G)$ is Pseudo-Reduced), and GAC (G is Almost Complete).

Other generalizations of the Buchberger algorithm deal with some classes of differential ideals different from the prime ones. The most fruitful algorithm used in constructive differential algebra is proposed by Boulier, Lazard, Ollivier, and Petitot [3], and is known as the Rosenfeld–Gröbner algorithm. This algorithm represents a perfect differential ideal as an intersection of *regular* differential ideals. In contrast to the primary decomposition, this representation depends on the ranking of differential indeterminates. In a series of numerical experiments, the systems of Euler equations in two and three space variables were considered for different rankings [16]. It was found out that not only the computation time and the memory used depend on the ranking, but also the number of components is different for different rankings. For some rankings, we did not succeed in determining the regular representation. The most interesting fact is that, for all cases where we did not succeed in determining the regular representation for three space variables, we did not also succeed in determining such a representation for two space variables.

Another class of differential ideal was introduced by E. Hubert [12]. It is known that, for prime differential ideals, the conditions 3 and 4 are equivalent. Hubert proposed to consider the differential ideals for which these conditions are equivalent. She called such ideals characterizable. Note that the definition of a characterizable ideal depends on the ranking of differential polynomials (there are differential ideal characterizable for one ranking and noncharacterizable for another one). In particular, it is important to know how to pass from a characteristic set with respect to a ranking of the differential polynomials to the characteristic set with respect to another ranking. A method for solving this problem is proposed by O. Golubitsky [10]. This is a generalization of the algorithm for passing from the Gröbner basis of a polynomial ideal with respect to an admissible ordering of monomials to the Gröbner basis of the same ideal with respect to another ordering [5].

Although the involutive methods came into computer algebra from the theory of partial differential equations, the theory of involutive bases is well developed only for polynomial ideals. Only the first steps are made in the direction of its generalization to differential algebra [9, 7].

Acknowledgements

The work was supported by INTAS (grant 99-1222) and the Russian Foundation for Basic Research (grant 02-01-01033).

References

1. Apel, J.: The Theory of Involutive Divisions and an Application to Hilbert Function Computations. *J. Symb. Comp.* **25** (1998) 683–704
2. Astrelin, A.V., Golubitsky, O. D., Pankratiev, E.V.: Groebner Bases and Involutive Bases. In: *Algebra. Proceedings of the International Algebraic Conference on the Occasion of the 90th Birthday of A.G. Kurosh. Moscow, Russia, May 25-30, 1998.* Walter de Gruyter, Berlin (2000) 49–55
3. Boulier, F., Lazard, D., Ollivier, F., Petitot, M.: Representation for the Radical of a Finitely Generated Differential Ideal. In: *Proc. ISSAC'95* (1995) 158–166
4. Carra' Ferro, G.: Differential Gröbner Bases in One Variable and in the Partial Case. Algorithms and Software for Symbolic Analysis of Nonlinear Systems. *Math. Comput. Modelling* **25** (1997) 1–10
5. Collart, S., Kalkbrener, M., Mall, D.: Converting Bases with the Gröbner Walk. *J. Symb. Comp.* **24** (1997) 465–469
6. Davenport, J.H., Siret, Y., Tournier, E.:
Computer Algebra. Systems and Algorithms for Algebraic Computation, Academic Press, London (1988)
7. Chen, Y.-F., Gao, X.-S.: Involutive Directions and New Involutive Divisions, *Computers and Mathematics with Applications* **41** (2001) 945–956
8. Gerdt, V.P., Blinkov, Yu.A.: Involutive Bases of Polynomial Ideals. *Mathematics and Computers in Simulation* **45** (1998) 519–541
9. Gerdt, V.P.: Completion of Linear Differential Systems to Involution. In: *Proc. CASC'99*, Springer-Verlag, Berlin (1999) 115–138
10. Golubitsky, O.D.: Differential Gröbner Walk. In: *Proc. 5th International Workshop on Computer Algebra and its Application in Physics. CAAP-01,* JINR E5, 11-2001-279, Dubna (2002) 114–126
11. Golubitsky, O.D.: Involutive Gröbner Walk, *Fundamental and Applied Mathematics* (in print).
12. Hubert, E.: Factorization-Free Decomposition Algorithms in Differential Algebra. *J. Symb. Comp.* (2000) **29** 641–662
13. Kolchin, E.: *Differential Algebra and Algebraic Groups*, Academic Press, New York, London (1973)
14. Kondratieva, M.V.: Examples of Computation of Generators of a Differential Ideal by Its Characteristic Set. *Programming and Computer Software* **28** (2002), no. 2, 81–83
15. Kondratieva, M.V., Levin, A.B., Mikhalev, A.V., Pankratiev, E.V.: *Differential and Difference Dimension Polynomials.* Kluwer Academic Publishers, Dordrecht (1999)
16. Makarevich, N.A.: Computation of the Characteristic Sets for the Euler Equations for Different Rankings. In: *Proc. 5th International Workshop on Computer Algebra and its Application in Physics. CAAP-01,* JINR E5, 11-2001-279, Dubna (2002) 196–202
17. Mansfield, E.: *Differential Gröbner Bases.* Ph. D. Thesis. University of Sydney (1991)
18. Mikhalev, A.V., Pankratiev, E.V.: *Computer Algebra. Computations in Differential and Difference Algebra.* Moscow Univ. Press, Moscow (1989)
19. Möller, H.M., Mora, F.: New Constructive Methods in Classical Ideal Theory. *J. Algebra* **100** (1986) 138–178
20. Ollivier, F.: Standard Bases of Differential Ideals. In *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes (Tokyo, 1990)*, Lect. Notes Comput. Sci. **508**, Springer-Verlag, Berlin (1991) 304–321
21. Ritt, J.F.: *Differential Algebra.* Amer. Math. Soc. Colloq. Publ., Vol. 33. Amer. Math. Soc., New York (1950)
22. Seiler, W.M.: Computer Algebra and Differential Equations. An Overview, *MathPAD* **7/1** (1997) 34–49
23. Semenov, A.S.: Static Properties of Involutive Divisions. In: *Proc. Workshop on Under- and Overdetermined Systems of Algebraic or Differential Equations. March 18–19, 2002, Karlsruhe, Germany*, J. Calmet, M. Hausdorf, and W.M. Seiler (Eds.) (2002) 151–155
24. Strukova, T.A.: *Differential Gröbner bases.* Diploma. Moscow State Univ., Moscow (1999)
25. Zharkov, A.Yu., Blinkov, Yu.A.: Involution Approach to Solving Systems of Algebraic Equations. In: *Proc. 1993 International IMACS Symposium on Symbolic Computations,* G. Jacob, N.E. Oussous, and S. Steinberg (Eds.), IMACS, Laboratoire d'Informatique Fondamentale de Lille, France (1993) 11–16