

STANDARD BASES IN DIFFERENTIAL ALGEBRA

E.V. PANKRATIEV

APRIL 14, 2007

- Gröbner bases of polynomial ideals
- Characteristic sets of perfect differential ideals
- Involutive bases of linear differential ideals and differential modules
- Differential standard bases of finitely generated differential ideals

Gröbner bases of polynomial ideals

- *Monomial ordering* plays the key role in definition of Gröbner bases
- There are many *equivalent* definitions of Gröbner bases
- There is a *distinguished* Gröbner basis (autoreduced)
- For *any* finite system of generators of a polynomial ideal I , its Gröbner basis (autoreduced) may be determined in a finite number of steps (the same is true for any submodule of a finitely generated polynomial module) *for any admissible monomial ordering*.

Let $R = k[x_0, \dots, x_m]$ be the polynomial ring over a field k . By $T = T(X)$ we denote the semigroup of monomials generated by elements of $X = \{x_0, \dots, x_m\}$. Then, T forms a basis of R ; i.e., any $a \in R$ may be represented as a finite linear combination of monomials with nonzero coefficients from k , and this representation is *unique*.

Admissible monomial orderings

Suppose that the monomials are ordered so that $\forall \theta \in T$

$$1 \preceq \theta, \tag{1}$$

$$\theta_1 \prec \theta_2 \implies \theta\theta_1 \prec \theta\theta_2. \tag{2}$$

A monomial ordering given, we can distinguish the *leading monomial* $\text{lm}(a)$ in any polynomial $a \in R$. A set G of generators of an ideal $I \subset k[x_0, \dots, x_m]$ is a *Gröbner basis* of I if the monomial ideal generated by $\{\text{lm}(g) \mid g \in G\}$ coincides with the monomial ideal generated by $\{\text{lm}(g) \mid g \in I\}$. This means that, for any $f \in I$, there exists $g \in G$ (maybe not unique!) such that $\text{lm}(g)$ divides $\text{lm}(f)$.

A polynomial set G is *monic* if any $g \in G$ is monic, i.e., its leading coefficient is equal to one.

A polynomial set G is *autoreduced* if, for any $g_1, g_2 \in G$ such that $g_1 \neq g_2$, none of monomials present in g_1 (with nonzero coefficients) is divisible by the leading monomial of g_2 (and vice versa).

The set of all monic autoreduced subsets of ideal I may be ordered in such a way that the minimal monic autoreduced subset of I is its Gröbner basis (uniquely defined). This basis is minimal (contains the minimal number of elements).

Differential algebra

Let $R = \mathcal{F}\{y_1, \dots, y_n\}$ be the ring of differential polynomials in *differential indeterminates* y_i over a partial differential field \mathcal{F} with a basic set of derivation operators $\Delta = \{\delta_1, \dots, \delta_m\}$. Similar to the polynomial case, we may consider *admissible orderings* on the set of *derivatives* $\Theta = \{\delta_1^{i_1} \dots \delta_m^{i_m}\}$ and *autoreduced sets* of differential polynomials. The set of autoreduced sets may be ordered. In any differential ideal I , there exists a minimal autoreduced subset, we refer to it as a *characteristic set of I* ; however, it is not unique.

Ritt and Kolchin demonstrated that characteristic sets of *prime* differential ideals possess many properties of Gröbner bases. Later, the theory of characteristic sets was extended to a larger class of *perfect* differential ideals.

Linear differential equations

In the case of *linear systems of partial differential equations*, the theory of characteristic sets of differential ideals may be reduced to the theory of Gröbner bases of differential modules (modules over the (noncommutative) ring of differential polynomials). In this case, all principal properties of Gröbner bases hold. If \mathcal{F} is a differential field of constants, then differential modules are isomorphic to polynomial modules, and we deal with Gröbner bases of polynomial modules.

Involutive bases

Consider the ring of polynomials $k[x_1, \dots, x_n]$ with monomial ordering `degrevlex`. Let $G = \{g_1, \dots, g_m\}$ be a system of generators of an ideal I ordered lexicographically decreasing order of leading monomials (we suppose that all leading monomials of elements g_i are distinct). For each $i \geq 2$, we find the minimal monomial t_i such that the leading monomial of $t_i g_i$ is divisible by at least one of $\text{lm}(g_j)$, $j < i$, and reduce the polynomial $t_i g_i$ with respect to $\{g_1, \dots, g_{i-1}\}$. If the result is nonzero, we add it to the set G preserving the lexicographic ordering of leading monomials. Moreover, we perform the multiplication of g_i by t_i in several steps such that, at each step, the polynomial is multiplied by a variable x_l . The results of the intermediate multiplications are also added to the set G . After completion of this procedure, we obtain a Gröbner basis of I , which is known as Janet's basis.

This method came into commutative algebra from the theory of differential equations. It was axiomatized and generalized by Zharkov, Blinkov, Gerdt, and others. The corresponding theory is known as the theory of involutive bases.

Differential standard bases of finitely generated differential ideals

We consider finitely generated differential ideals in the ring of ordinary differential polynomials in one differential indeterminate over a differential field of constants. The theory is nontrivial even in the case of one generator.

Example 1. Consider the differential polynomial $A = (y')^2 + y \in \mathcal{F}\{x\}$ (F is an ordinary differential field). This polynomial is absolutely irreducible. However the differential ideal $[A]$ is not prime. It is not even perfect. In particular, one can prove that $y''' \notin [A]$, but $y''' \in \{A\}$. The radical of $[A]$ is not a prime ideal. It can be represented as $\{A\} = [y] \cap \mathfrak{p}$, where the differential ideal \mathfrak{p} is defined by the condition $f \in \mathfrak{p}$ iff $f \cdot (y')^k \in [A]$ for some $k \in \mathbb{N}$.

Differential G -bases by Ollivier and Carra–Ferro

A set $G \subset I$ is a differential G -basis of a differential ideal I if the leading monomials of G and their derivatives generate the set of leading monomials of I .

To use this approach we have to order the set of differential monomials and to differentiate the differential monomials (e.g., lexicographically).

The differential ideal $[y^2] \subset \mathcal{F}\{y\}$ has no differential G -basis (under the lexicographic ordering).

It has a differential G -basis (consisting of one element) for *degrevlex* ordering [Zobnin].

- An *ordinary differential ring* \mathcal{R} is a commutative ring with a derivative operator δ .
- $\Theta := \{\delta^k : k \geq 0\}$.
- An ideal I of \mathcal{R} is *differential* iff $\delta I \subset I$.
- $[F]$ denotes the differential ideal generated by F .
- \mathcal{F} is a differential *field of constants* of characteristic zero.
- $\mathcal{F}\{y\} := \mathcal{F}[y, \delta y, \delta^2 y, \dots]$ — a ring of differential polynomials.
- $y_i := \delta^i y$.
- \mathbb{M} — the set of all differential monomials.
- $\text{lm}_{\prec} f$ — the *leading monomial* of a polynomial $f \notin \mathcal{F}$ w.r.t. \prec .

Admissible orderings

An *admissible ordering* on the set of differential monomials \mathbb{M} must satisfy the following axioms:

- $M \prec N \implies MP \prec NP \quad \forall M, N, P \in \mathbb{M};$
- $1 \preceq P \quad \forall P \in \mathbb{M};$
- $y_i \prec y_j \iff i < j.$

These properties are sufficient to guarantee that any admissible ordering well orders \mathbb{M} (Zobnin, 2003).

Examples: **lex, deglex, wt-lex, degrevlex, wt-revlex,**

It is well known that any monomial ordering can be specified by an $m \times (k + 1)$ *monomial matrix* \mathcal{M} with real entries and lexicographically positive columns such that $\text{Ker}_{\mathbb{Q}} \mathcal{M} = \{0\}$:

$$\mathcal{M} \begin{pmatrix} \alpha_0 \\ \vdots \\ \alpha_k \end{pmatrix} \prec_{\text{lex}} \mathcal{M} \begin{pmatrix} \beta_0 \\ \vdots \\ \beta_k \end{pmatrix} \iff y_0^{\alpha_0} \cdots y_k^{\alpha_k} \prec y_0^{\beta_0} \cdots y_k^{\beta_k}.$$

Definition 1. A set of monomial matrices $\{\mathcal{M}_k\}$ is called *concordant* if the matrix \mathcal{M}_{k-1} can be obtained from \mathcal{M}_k by deleting the rightmost column and then by deleting a row of zeroes, if such a row exists.

Theorem. Any admissible ordering on differential monomials can be specified by a concordant set of monomial matrices or, equivalently, by an infinite monomial matrix.

Examples of orderings (ctd.)

DegRevLex

$$(\mathbf{1}), \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix} \dots$$

$$\begin{pmatrix} 1 & 1 & 1 & 1 & \dots \\ & 1 & 1 & 1 & \dots \\ & & 1 & 1 & \dots \\ & & & 1 & \dots \\ \dots & \dots & \dots & \dots & \dots \end{pmatrix}$$

WtRevLex

$$(\mathbf{1}), \begin{pmatrix} 1 & \mathbf{2} \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & \mathbf{2} & \mathbf{3} \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & \mathbf{2} & \mathbf{3} & \mathbf{4} \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix} \dots$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & \dots \\ & 1 & 1 & 1 & \dots \\ & & 1 & 1 & \dots \\ & & & 1 & \dots \\ \dots & \dots & \dots & \dots & \dots \end{pmatrix}$$

δ -stability

An admissible ordering \prec is called

- δ -stable, if $\boxed{M \preceq N} \implies \boxed{\text{lm}_{\prec} \delta M \preceq \text{lm}_{\prec} \delta N}$;
- strictly δ -stable, if $\boxed{M \prec N} \implies \boxed{\text{lm}_{\prec} \delta M \prec \text{lm}_{\prec} \delta N}$.

Example. **Lex** and **deglex** are strictly δ -stable.

Degrevlex and **wtrevlex** are δ -stable, but not strictly δ -stable, since $y_i^2 \succ y_{i-1}y_{i+1}$, but $\text{lm} \delta y_i^2 = \text{lm} \delta y_{i-1}y_{i+1}$.

δ -lexicographic and β -orderings

For \prec the following are equivalent:

- $\text{lm}_{\prec} \delta M = \text{lm}_{\text{lex}} \delta M$ for any monomial M ;
- $y_i y_j \prec y_{i-1} y_{j+1}$ for all $0 < i \leq j$,
i.e., \prec is lexicographic on isobaric monomials of degree 2;

We call such orderings δ -lexicographic.

Example. The orderings **lex**, **deglex** and **wt-lex** are δ -lexicographic.

If, in contrast, all summands in $\delta^k M$ are compared reverse lexicographically then we call \prec a β -ordering.

Example. **Degrevlex** and **wt-degrevlex** are β -orderings.

δ -fixedness

Definition 2. An admissible ordering \prec is δ -fixed if

$$\forall f \in \mathcal{F}\{y\} \setminus \mathcal{F} \quad \exists M \in \mathbb{M}; \quad \exists k_0, r \in \mathbb{N} :$$

$$\text{lm}_{\prec} \delta^k f = My_{r+k} \quad \text{for all } k \geq k_0.$$

Example. Any δ -lexicographic ordering is δ -fixed.

Concordance with quasi-linearity

Let \prec be an admissible ordering.

A polynomial $f \in \mathcal{F}\{x\} \setminus \mathcal{F}$ is \prec -quasi-linear if $\deg \text{lm}_{\prec} f = 1$.

Example. $f = y_1 + y_0^2$ is quasi-linear w.r.t. **lex**, but not **deglex**.

We say that \prec is concordant with quasi-linearity if the derivative of any \prec -quasi-linear polynomial is quasi-linear too.

Example. **Lex**, **deglex**, **degrevlex** are concordant with quasi-linearity, as well as any δ -lexicographic ordering.

Relations between orderings

lex, deglex, wt-lex



Strict δ -stable orderings



δ -lexicographic
orderings



δ -fixed orderings

degrevlex, wt-revlex



δ -stable orderings



Orderings that are concordant
with quasi-linearity



Differential standard bases

Fix an admissible ordering \prec . Consider a differential ideal I of $\mathcal{F}\{x\}$.

A set $G \subset I$ is a differential standard basis of I if ΘG is an algebraic Gröbner basis of I in $\mathcal{F}[y_0, y_1, y_2, \dots]$ (possibly, infinite).

A DSB is reduced if every $g \in G$ is reduced w.r.t. $\Theta (G \setminus \{g\})$.

Example. Any linear ideal has a **finite** differential standard basis.

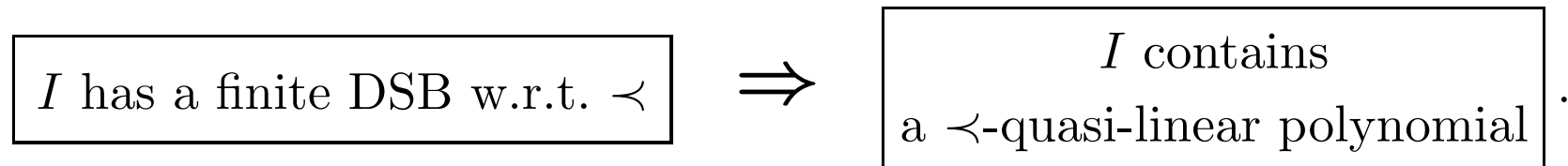
Unfortunately, differential standard bases are often **infinite**:

Example. The ideal $[y^2]$ does not have finite DSB w.r.t. **lex**.

Finiteness criterion

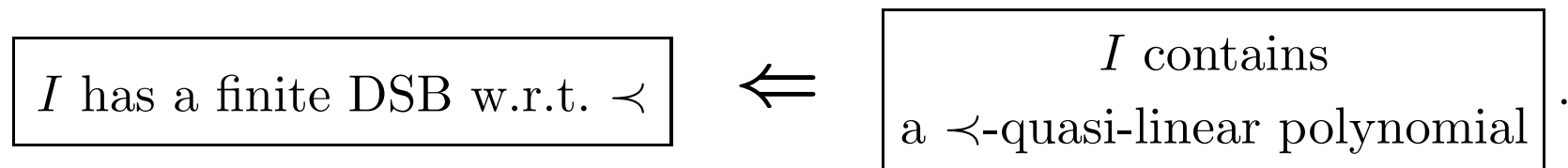
Let I be a proper differential ideal of $\mathcal{F}\{y\}$.

Necessary condition. For a δ -fixed ordering \prec



Sufficient condition.

For a **concordant with quasi-linearity** ordering \prec



Corollary. For δ -lexicographic orderings the condition is necessary and sufficient.

Corollaries

GENERALIZATIONS OF G. CARRÀ FERRO'S THEOREMS:

Corollary. Let \prec be **δ -fixed**.

If the degree of each monomial in f_1, \dots, f_n is greater than 1 then $[f_1, \dots, f_n]$ has no finite DSB w.r.t. \prec .

Corollary. Let \prec be **strictly δ -stable**. The reduced DSB of $[f]$ w.r.t. \prec consists of f itself $\iff f$ is \prec -quasi-linear.

KEY ROLE OF **lex**:

A DSB w.r.t. a **δ -fixed**
ordering is finite



A **lex** DSB is also finite .

Finite bases: an example

Fix the **pure lexicographic** ordering.

Consider the DSB of the ideals $[y_1^n + y]$, $n \geq 3$:

- $y_1^n + y_0$;
- $n y_0 y_2 - y_1^2$;
- $n y_1^{n-2} y_2^2 + y_2 = y_2 (n y_1^{n-2} y_2 + 1)$;
- $y_3 - n(n-2) y_1^{n-3} y_2^3$.

The DSB are finite, since $[y_1^n + y]$ contains a quasi-linear polynomial.

By the way, one can prove that these ideals are radical.

$\underbrace{\text{lex, deglex, wt-lex}}$

Strict δ -stability



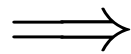
δ -lexness



δ -fixedness



Necessity of criterion



$\underbrace{\text{degrevlex, wt-revlex}}$

δ -stability



Concordance with
quasi-linearity



Sufficiency of criterion

$\underbrace{\text{any ordering for an ideal
containing linear polynomials}}$

Finite DSB and radical ideals

Let \prec be a δ -fixed and concordant with quasi-linearity ordering.

Theorem (M. V. Kondratieva, A. Zobnin).

Let $f \in \mathcal{F}\{y\}$ be a first-order differential polynomial not in \mathcal{F} .

The ideal $[f]$ has a finite DSB w.r.t. \prec (i.e., $[f]$ contains a \prec -quasi-linear polynomial) iff $[f]$ is radical.

Example.

Let $f_{m,n} = (y_1 + 1)^m - cy^n$, $c \in \mathcal{F}$, $c \neq 0$.

Then $[f_{m,n}]$ is radical and has a finite lex-DSB iff $n \mid m$.

Other orderings: a conjecture

Conjecture (M. V. Kondratieva, A. Zobnin). A proper ideal I has a finite DSB w.r.t. a concordant with quasi-linearity β -ordering \prec iff either

- I contains a \prec -quasi-linear polynomial, or
- $I = [f^p]$, where f is \prec -quasi-linear and $p \geq 1$.

The sufficiency (\implies) is easy to prove

The necessity (\impliedby) is still an open problem.

References

- [1] A.V. ASTRELIN, O.D. GOLUBITSKY, E.V. PANKRATIEV Gröbner Bases and Involutive Bases, In: *Algebra: Proceedings of the International Algebraic Conference*, Moscow, Russia, May 25-30, 1998 Berlin: Walter de Gruyter, 2000, pp. 49-55.
- [2] Becker T. and Weispfenning W., *Groebner Bases. A Computational Approach to Commutative Algebra*, Graduate Texts in Mathematics, Springer-Verlag, New York, 1993.
- [3] Boulier F., Lazard D., Ollivier F., Petitot M., *Representation for the Radical of a Finitely Generated Differential Ideal*, in Proceedings of 1995 International Symposium on Symbolic and Algebraic Computation, 158–166, ACM Press, 1995.
- [4] BUCHBERGER B. Gröbner bases: An algorithmic method in polynomial ideal theory. *Recent Trends in Multidimensional Systems Theory*, chapter 6 (1985), 184–232.
- [5] Carrà Ferro G., *Groebner Bases and Differential Algebra*, Lecture Notes in Computer Science, vol. 356, 141–150, 1989.

- [6] Carrà Ferro G., *Differential Gröbner Bases in One Variable and in the Partial Case*, Math. Comput. Modelling, Pergamon Press, vol. 25, 1–10, 1997.
- [7] Cox D., Little J., O’Shea D., *Ideals, Varieties and Algorithms. An Introduction to Computational Algebraic Geometry and Commutative Algebra*, New York, NY: Springer, 1998.
- [8] Cox D., Little J., O’Shea D., *Using Algebraic Geometry*, Springer-Verlag, New-York – Berlin – Heidelberg, 1998.
- [9] Gallo G., Mishra B., Ollivier F., *Some Constructions in Rings of Differential Polynomials*, Lecture Notes in Computer Science, vol. 539, 171–182, 1991.
- [10] Hong H., *Groebner Basis Under Composition I*, The Journal of Symbolic Computation, 643-663, 25 (5), 1998.
- [11] Hong H. and Weispfenning V., *Algorithmic Theory of Admissible Term Orders*, preprint, 1999.
- [12] Hubert E., *Essential Components of an Algebraic Differential Equation*, Journal of Symbolic Computation (1999), vol. 28, 4–5, pp. 657–680.

- [13] Hubert E., *Factorization-free Decomposition Algorithm in Differential Algebra*, J. Symb. Comp. (29), no. 2, 641–662 (2000).
- [14] Hubert E., *Notes on triangular sets and triangulation-decomposition algorithms I: Polynomial Systems*, Symbolic and Numerical Scientific Computing 2001, 1–40, 2003.
- [15] Hubert E., *Notes on triangular sets and triangulation-decomposition algorithms II: Differential Systems*, Symbolic and Numerical Scientific Computing 2001, 40–87, 2003.
- [16] E. R. Kolchin. *On the exponents of differential ideals*, Annals of Mathematics, 42:740–777, 1941.
- [17] Kolchin E.R., *Differential Algebra and Algebraic Groups*, 1973.
- [18] Kondratieva M.V., Levin A.B., Mikhalev A.V., Pankratiev E.V., *Differential and Difference Dimension Polynomials*, Kluwer Academic Publisher, 1999.
- [19] Levi H., *On the Structure of Differential Polynomials and on Their Theory of Ideals*, Trans. AMS, vol. 51, 532–568, 1942.
- [20] Mead D.G., *A Necessary and Sufficient Condition for Membership in $[uv]$* , Proc. AMS, vol. 17, 470–473, 1966.

- [21] Mead D.G., Newton M.E., *Syzygies in $[y^p z]$* , Proc. AMS, vol. 43 (2), 301–305, 1974.
- [22] Ollivier F., *Le problème de l'identifiabilité structurelle globale*, Doctoral Dissertation, Paris, 1990.
- [23] Ollivier F., *Standard Bases of Differential Ideals*, Lecture Notes in Computer Science, 304–321, 508, 1990.
- [24] O'Keefe K.B., *A Property of the Differential Ideal $[y^p]$* , Trans. AMS, vol. 94, 483–497, 1960.
- [25] Pankratiev E.V., *Some Approaches to Construction of Standard Bases in Commutative and Differential Algebra*, in Proceedings of CASC-2002, V.G. Ganzha, E.W. Mayr, E.V. Vorozhtsov (Eds.), 265–268, 2002.
- [26] Pankratiev E.V., *Some approaches to construction of the differential Groebner bases*, Calculemus 2002. Marseille, France, July 3-5, 2002.
- [27] Ritt J.F., *Differential Algebra*, volume XXXIII of Colloquium Publications. New York, American Mathematical Society, 1950.
- [28] Robbiano L., *Term Orderings on the Polynomial Ring*, in Proceedings of EUROCAL 85, Lecture Notes in Computer Science 204, 513-517, 1985.

- [29] Robbiano L., *On the Theory of Graded Structures*, J. Symb. Comp., **2**, 139–170 (1986).
- [30] Rust C., Reid G.J., *Rankings of Partial Derivatives*, in Proceedings of the 1997 International Symposium on Symbolic and Algebraic Computation, 9–16, ACM Press, New York, 1997.
- [31] Rust C., *Rankings of Derivatives for Elimination Algorithms and Formal Solvability of Analytic Partial Differential Equations*, Ph.D. dissertation, Chicago, Illinois, 1998.
- [32] Sit W.Y., *The Ritt-Kolchin Theory for Differential Polynomials*, Differential Algebra and Related Topics, Proceedings of the International Workshop, NJSU, 2–3 November 2000, Eds. Li Guo, William F. Keigher, Phyllis J. Cassidy, William Y. Sit.
- [33] Weispfenning V., *Admissible Orders and Linear Forms*, in ACM SIGSAM Bulletin, 21 / 2, 16-18, 1987
- [34] Weispfenning V., *Differential Term-Orders*, in Proceedings of ISSAC-93, 245–253, ACM press, Kiev, 1993.

- [35] Zobnin A., *Essential Properties of Admissible Orderings and Rankings*, Contributions to General Algebra 14, 205–221, 2004.
- [36] Zobnin A., *Generalized Reduction in Rings of Differential Polynomials*, Programming and Computer Software, 30 (2), 2004.
- [37] Zobnin A., *On Testing the Membership to Differential Ideals*, in Proceedings of CASC-2004, pages 485–496. Technische Universität München, 2004.
- [38] Zobnin A., *Admissible Orderings and Finiteness Criteria for Differential Standard Bases*, in Proceedings of ISSAC-2005, pages 365–372. M. Kauers, editor. ACM Press, 2005.