タイトル：Generic Grobner basis in $\mathcal{D}$-announcement

著者：Bahloul, Rouchdi

引用：数理解析研究所講究録 (2004), 1395: 31-37

発行日：2004-10

URL：http://hdl.handle.net/2433/25923

タイプ：Departmental Bulletin Paper

出版：Kyoto University
Generic Gröbner basis in $\hat{\mathcal{D}}$ - announcement

Rouchdi BAHLOUL
Department of Mathematics, Kobe University *

Abstract

Many authors have studied parametric Gröbner bases. Here we develop this notion in the case of ring of differential operators in the formal case where the ring of coefficients $\mathcal{C}$ is the most general as possible. This gives rise to the notion of generic Gröbner basis on an irreducible affine scheme of Spec$(\mathcal{C})$. Our goal here is to state existence theorems of generic Gröbner bases and comprehensive Gröbner bases for local orders, these will use truncated divisions in the Buchberger algorithm. We will emphasize the difference between nonreduced and reduced generic Gröbner bases by seeing that truncated divisions are not applicable to reduced ones in general. Finally, we will propose applications to comprehensive standard bases, local Bernstein polynomials and Gröbner fans.

Introduction

This short note is related to the talk given, under the same title, in the workshop "Computer Algebra - Design of Algorithms, Implementations and Applications" given at the RIMS (Kyoto university) on december 2003. This talk was based on the preprint [Ba03]. New results have been discovered since this preprint so this note shall be an extended abstract and an announcement of a paper (in preparation) which shall be an improvement of the first part of [Ba03].

Parametric Gröbner bases have been studied by several authors and is now a further developed subject: P. Gianni [Gi89], M. Lejeune-Jalabert and A. Philippe [LP89], T. Becker [Be94], V. Weispfenning [We92] with the existence a comprehensive Gröbner basis and more recently [We03] with the notion of a canonical comprehensive Gröbner basis. There also exists an alternative approach to the construction of a comprehensive Gröbner basis by T. Sato and A. Suzuki [SS03].

All these constructions are concerned with ideals in polynomial rings. In 1997, T. Oaku [Oa97] studied parametric Gröbner bases in rings of algebraic differential operators in a work concerning (among others) the study of the local or global Bernstein polynomial for a polynomial with parameters. This work enables A. Leykin [Le01] to obtain a constructibility result concerning the (global) Bernstein polynomial for a polynomial with parameters. In the same spirit, U. Walther [Wa03] made a study of algebraic de Rham cohomology groups.

rouchdi@math.kobe-u.ac.jp
Now concerning the local situation, in a recent paper, A. Frühbis-Krüger [Fr03] makes use of a parametric approach to standard bases for the study of singularities of analytic functions with parameters, but it seems that no general construction have been made.

The purpose of this note is an exposition and a announcement concerning a general study of parametric standard bases. We will be concerned by all the local situations: local algebraic, analytic, formal. This will take place in rings of differential operators but will, of course, cover the commutative situations.

Here we will be concerned mainly by local orderings but our interest lies both in algebraic, analytic or formal cases.

Moreover we will emphasize the difference between reduced and nonreduced standard bases. For this, let us see a trivial but instructive example in the commutative case.

Let us consider $f(a,x,y) = ay - xy + x$ and consider a local order on $\mathbb{N}^2$ (i.e. on the $x,y$ monomials) such that the leading monomial of $f$ is $y$ (here $a$ is a parameter).

Consider the ideal $I$ in $\mathbb{C}[a][x,y]$ and $\hat{I}$ in $\mathbb{C}[a][[x,y]]$ both generated by $f$. It is trivial to say that $f$ is standard bases of $\text{Frac}(\mathbb{C}[a])[x,y] \cdot I$ so that $f$ is a generic Gröbner basis of $I$ on $\mathbb{C} \simeq \text{Specm}(\mathbb{C}[a])$ (the maximal spectrum). Indeed, for any $a_0 \neq 0$, $f(a_0, x, y)$ is a standard basis of $I_{|a=a_0}$ or of $\hat{I}_{|a=a_0}$ and the leading monomial is constant (of course in this trivial example, $f(0, x, y)$ is also a standard basis of $I_{|a=0}$). But $f$ is not a reduced generic standard basis, i.e. its specialization into $a_0 \neq 0$ is not reduced. So let us reduce $f$. The reduction of $f$ (which is unique up to a factor in $\mathbb{C}[a]$) is

$$g = ay + x + x^2/a + x^3/a^2 + x^4/a^3 + \cdots .$$

As one can see, this is not in the ring of the begining $\mathbb{C}[a][x,y]$ nor in $\mathbb{C}[a][[x,y]]$ but in an extension of the latest and one can not take off the denominators. The idea in this case shall be to “control” these denominators.

The plan is the following. In the first section we shall introduce the objects and state the main results. By using a notion of truncated division, in the nonreduced case, we shall thus be able to simplify the results of [Ba03]. In the second section, we shall state and announce applications: existence of comprehensive standard bases, application to the (local) generic Bernstein polynomial (work in progress), application to a constructibility result (see [Ba03]) for Gröbner fans (and in project to GKZ-hypergeometric systems).

This paper contains no proofs. Some of them can be found in [Ba03] but in a subsequent paper, we shall prove all the results of the present note.

I wish to thank N. Takayama for fruitful discussions that helped to make things more clear to me.

This work was made under the support of the FY2003 JSPS Postdoctoral Fellowship.

1. Main results

To be as more general as possible, we shall work in $\mathcal{D}_n(k)(z)$ and $\mathcal{D}_n(z)$ but every thing said in this section will work for any other (usual) ring if one dispose of a division theorem.
Let $n \geq 1$ be an integer and $k$ be a field of characteristic zero. Let $x_1, \ldots, x_n$ be variables and set $x = (x_1, \ldots, x_n)$. Define $\mathcal{D}_n(k)(z)$ as the $k[[x]]$ (resp. $\mathbb{C}\{x\}$) algebra generated by the $\partial_{x_i}$'s and $z$ with the relations:

$$\forall i, j \forall u, v, [u, z] = [\partial_{x_i}, z] = [u, v] = [\partial_{x_i}, \partial_{x_j}] = 0 \text{ and } [\partial_{x_i}, u] = \frac{\partial u}{\partial x_i} z,$$

here $u$ and $v$ are in $k[[x]]$ (resp. $\mathbb{C}\{x\}$). The obtained ring is a homogenized version of the ring $\mathcal{D}_n(k)$ (resp. $\mathcal{D}_n$) of differential operators with formal (resp. analytic) power series as the coefficient ring. The ring $\mathcal{D}_n(k)(z)$ is much more convenient than $\mathcal{D}_n(k)$ for we can deal with more orders (the technique of homogenizing, computing and dehomogenizing is usual).

Let $<$ be an order on $\mathbb{N}^{n+1}$ compatible with sums and for which the following notions are well defined (for example the order $<_k$ defined in [ACG01] and used in [Ba03]).

An operator $P \in \mathcal{D}_n(k)(z)$ can be written uniquely as $P = \sum c_{\alpha, \beta, k} x^\alpha \partial_z^\beta z^k$ (here $x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$). We define its Newton diagram $\mathrm{ND}(P)$ as the set of $(\alpha, \beta, k) \in \mathbb{N}^{n+1}$ such that $c_{\alpha, \beta, k} \neq 0$. Then we define the
- leading exponent $\exp_<(P) = \max_\prec \mathrm{ND}(P)$,
- leading monomial $\mathrm{lm}_<(P) = (x, \partial_x, z)^{\exp_<(P)}$,
- leading coefficient $\mathrm{lc}_<(P) = \exp_<(P) \in k$ (or in $\mathbb{C}$ for $P \in \mathcal{D}_n(z)$).

Note that since the order $<$ is compatible with sums, we have $\exp_<(PQ) = \exp_<(P) + \exp_<(Q)$ for any $P, Q \in \mathcal{R}(z)$ (which is one of $\mathcal{D}_n(k)(z)$ and $\mathcal{D}_n(z)$). Now, let us recall the division theorem of [ACG01]. For $e_1, \ldots, e_r \in \mathbb{N}^{n+1}$, define the partition of $\mathbb{N}^{n+1}$:
- $\Delta_1 = e_1 + \mathbb{N}^{n+1}$
- For $j = 2, \ldots, r$, $\Delta_j = (e_j + \mathbb{N}^{n+1}) \setminus (\Delta_1 \cup \cdots \cup \Delta_{j-1})$
- $\bar{\Delta} = \mathbb{N}^{n+1} \setminus (\Delta_1 \cup \cdots \cup \Delta_r)$.

**Theorem 1.** ([ACG01] th.7) For any $P, Q_1, \ldots, Q_r \in \mathcal{R}(z)$ with $Q_j \neq 0$, there exists a unique $(q_1, \ldots, q_r, R) \in \mathcal{R}(z)^{r+1}$ such that $P = q_1 Q_1 + \cdots + q_r Q_r + R$ and

1. for any $j$ such that $q_j \neq 0$, $\exp_<(Q_j) + \mathrm{ND}(q_j) \subset \Delta_j$,
2. $\mathrm{ND}(R) \subset \bar{\Delta}$ if $R \neq 0$, where the partition $\mathbb{N}^{n+1} = \Delta_1 \cup \cdots \cup \Delta_r \cup \bar{\Delta}$ is associated with the $\exp_<(Q_i)$'s. $R$ is called a remainder of the division of $P$ by $Q_1, \ldots, Q_r$ (with respect to $<$).

As a consequence:

$$\exp_<(P) \geq \max_\prec \{\exp_<(q_1 Q_1), \ldots, \exp_<(q_r Q_r), \exp_<(R)\}.$$

Let us recall the idea of the proof, this will be useful in the sequel.

- **Put** $(P^0, q_1^0, \ldots, q_r^0, R^0) = (P, 0, \ldots, 0, 0)$.
- For $i \geq 0$, if $P^i = 0$ then put $(P^{i+1}, q_1^{i+1}, \ldots, q_r^{i+1}, R^{i+1}) = (P^i, q_1^i, \ldots, q_r^i, R^i)$.
- if $\exp_<(P^i) \in \bar{\Delta}$ then
  $$(P^{i+1}, q_1^{i+1}, \ldots, q_r^{i+1}, R^{i+1}) = (P^i - \mathrm{lt}_<(P^i), q_1^i, \ldots, q_r^i, R^i + \mathrm{lt}_<(P^i)),$$
- if not, then let $j = \min \{k \in \{1, \ldots, r\}, \exp_<(P^i) \in \Delta_k\}$ and put
  $$P^{i+1} = P^i - \frac{\mathrm{lc}_<(P^i)}{\mathrm{lc}_<(Q_j)} \cdot (x, \partial_x, z)^{\exp_<(P^i) - \exp_<(Q_j)} \cdot Q_j,$$
  $$q_j^{i+1} = q_j^i + \frac{\mathrm{lc}_<(P^i)}{\mathrm{lc}_<(Q_j)} \cdot (x, \partial_x, z)^{\exp_<(P^i) - \exp_<(Q_j)},$$
  and for $l \neq j$, $q_l^{i+1} = q_l^i$.  

V-3
\[ R^{i+1} = R^i. \]

With this process, we obtain \( (r + 2) \) sequences \( P^i, q^i_1, \ldots, q^i_r \) and \( R^i \) with \( i \in \mathbb{N} \) satisfying \( P = \sum_j q^i_j Q_j + R^i + P^i \). The first point consists in showing that these sequences converge for the \((x_1, \ldots, x_n)\)-adic topology, by considering \( \hat{D}_n(k)(\rho) \) as a free \( k[[x]] \)-module (in particular the limit of \( P^i \) is 0). The second point which is much harder is to prove that if the inputs are in \( D_n(\rho) \) then the limits (which are in \( \hat{D}_n(\mathbb{C})(\rho) \)) are indeed in \( D_n(\rho) \). Now, as a consequence, we have:

**Lemma 2.** Let \( C \) be a commutative integral ring and let \( F = \text{Frac}(C) \) denotes its fraction field. Let \( P, Q_1, \ldots, Q_r \) be in \( \hat{D}_n(\mathbb{C})(\rho) \) (i.e. the coefficients are in \( C \)). Now let us consider the division of \( P \) by the \( Q_j \)'s in \( D_n(F)(\rho) \) with respect to \( \prec \): \( P = q_1 Q_1 + \cdots + q_r Q_r + R \). We claim that the coefficients of \( R \) and of the \( q_j \)'s are of the following form:

\[
\frac{c}{\prod_{j=1}^{r} \text{lc}_{\prec}(Q_j)^{d_j}} \text{ where } c \in C, \ d_j \in \mathbb{N}.
\]

**Truncated divisions.** Let us keep the notations of the division process. If the remainder is not zero then there exists an \( i_0 \) (that we suppose minimal) such that \( \exp_{\prec}(P^{i_0}) \) is not divisible by any \( Q_j \) so we can stop the division process at this point: \( P = \sum_j q^i_j Q_j + R \) where \( R = P^{i_0} \) and \( q_j = q^i_j \) are “algebraic” (in the sense that they are obtained by a finite number of algebraic operations). This truncated division does not satisfy (in general) conditions (1) and (2) of theorem 1 but it satisfies (*) and it is enough for constructing Gröbner bases.

**Gröbner bases** We still denote by \( R(\rho) \) one of \( D_n(\rho) \), \( \hat{D}_n(k)(\rho) \) and let \( J \) be an ideal in \( R(\rho) \). Consider the set of leading exponents of \( J \) (with respect to \( \prec \)): \( \exp_{\prec}(J) = \{ \exp_{\prec}(P), P \in J \setminus \{0\} \}. \)

This is a subset of \( \mathbb{N}^{2n+1} \) which is stable by sums. By the usual Dickson lemma, we have that:

**Definition.** There exists \( Q_1, \ldots, Q_r \in J \) such that

\[
\exp_{\prec}(J) = \bigcup_{j=1}^{r} (\exp_{\prec}(Q_j) + \mathbb{N}^{2n+1}).
\]

Such a set \( \{Q_1, \ldots, Q_r\} \) is called a Gröbner basis of \( J \) with respect to \( \prec \).

A consequence of the division theorem is the following: Let \( J \subset R(\rho) \) be an ideal and \( Q_1, \ldots, Q_r \in J \). Let \( P \in R(\rho) \) then these two points are equivalent:

- \( P \in J \Rightarrow \) the remainder \( R \) of the division of \( P \) by the \( Q_j \)'s (with respect to \( \prec \)) is zero.
- \( Q_1, \ldots, Q_r \) form a \( \prec \)-Gröbner basis.

There also exists a criterion for a subset of \( J \) to be a Gröbner basis. It makes use of \( S \)-operators (see the definition in [Ba03] for example).

**Proposition 3.** (see for example [CG97]) Let \( \{Q_1, \ldots, Q_r\} \) be a set of generators of \( J \) in \( R(\rho) \). Then this set is a \( \prec \)-Gröbner basis of \( J \) if and only if the following holds: for any \( j, j' \), the remainder of the division of \( S(Q_j, Q_{j'}) \) by \( Q_1, \ldots, Q_r \) is zero.

As a consequence, one can construct a Gröbner basis by using the Buchberger algorithm [Bu70] which consists in adding to a set of generators of an ideal all the nonzero
reminders of the division of \( S(P, Q) \) for \( P, Q \) in this set, and to continue until the remainders are zero (see [Ba03] for a more precise statement).

**Remark on finiteness.** Now if we use truncated divisions, then we can claim that each element of Gröbner basis can be obtained after a finite number of algebraic operations (which does not mean that a finite number of steps is enough to construct a Gröbner basis since we don’t know in advance if the remainder of a division will be zero or not).

**Generic Gröbner bases.** Now let \( \mathcal{C} \) be a commutative unitary ring for which we denote by \( \mathcal{F} \) the fraction field and \( \text{Spec}(\mathcal{C}) \) the spectrum. For any \( \mathcal{P} \) in \( \text{Spec}(\mathcal{C}) \) and \( c \in \mathcal{C} \), denote by \([c]_\mathcal{P}\) the class of \( c \) in \( \mathcal{C}/\mathcal{P} \) and \((c)_\mathcal{P}\) this class viewed in the fraction field \( \mathcal{F}(\mathcal{P}) \) of \( \mathcal{C}/\mathcal{P} \). The element \((c)\mathcal{P}\) is called the specialization of \( c \) into \( \mathcal{P} \).

Now we can easily extend this notation to elements of \( \hat{\mathcal{D}}_n(\mathcal{C})\langle z \rangle \) and of \( \hat{\mathcal{D}}_n(\mathcal{F})\langle z \rangle \) for which the denominator of the coefficients are not in \( \mathcal{P} \).

Now given an ideal \( \mathcal{J} \) in \( \hat{\mathcal{D}}_n(\mathcal{C})\langle z \rangle \), we define \( (\mathcal{J})_\mathcal{P} \subset \hat{\mathcal{D}}_n(\mathcal{F}(\mathcal{P}))\langle z \rangle \) as the ideal generated by all the \((\mathcal{P})_\mathcal{P}\) for \( \mathcal{P} \in J \).

**Localization.** Let \( \mathcal{C} = \{c_1, \ldots, c_r\} \) be a subset of \( \mathcal{C} \) and let \( M(\mathcal{C}) \) be the set of monomials \( c_1^{d_1} \cdots c_r^{d_r} \) where \( d_i \in \mathbb{N} \), then \( M(\mathcal{C}) \) is a multiplicative subset of \( \mathcal{C} \). Then we denote by \( \hat{\mathcal{D}}_n(M(\mathcal{C}))\langle z \rangle \) be the localization of \( \hat{\mathcal{D}}_n(\mathcal{C})\langle z \rangle \) w.r.t. \( M(\mathcal{C}) \). We view this localization as the set of the operators in \( \hat{\mathcal{D}}_n(\mathcal{F})\langle z \rangle \) with denominators in \( M(\mathcal{C}) \).

**Construction of a generic Gröbner basis on an irreducible affine scheme.**

Fix a prime ideal \( \mathcal{Q} \) in \( \mathcal{C} \). Let \( \mathcal{J} \) be an ideal in \( \hat{\mathcal{D}}_n(\mathcal{C})\langle z \rangle \).

(a) Since \( (\mathcal{J})_\mathcal{Q} \) is generated by \( \{(\mathcal{J})_\mathcal{Q}; f \in \mathcal{J} \} \) and \( \hat{\mathcal{D}}_n(\mathcal{F}(\mathcal{Q}))\langle z \rangle \) is noetherian, there exists a finite system \( \{f_1, \ldots, f_s\} \) of \( \mathcal{J} \) such that \( \{(f_1)\mathcal{Q}, \ldots, (f_s)\mathcal{Q}\} \) generates \( (\mathcal{J})_\mathcal{Q} \). Let \( f_1, \ldots, f_s \) be such a system.

(b) Let \( g_1 = (f_1)\mathcal{Q}, \ldots, g_s = (f_s)\mathcal{Q}, g_{s+1}, \ldots, g_r \) be a \( \prec \)-Gröbner basis of \( (\mathcal{J})_\mathcal{Q} \) constructed using the Buchberger algorithm starting from \( \{(f_1)\mathcal{Q}, \ldots, (f_s)\mathcal{Q}\} \).

By multiplying \( g_j \) by a suitable coefficient, we may assume that for any \( j = 1, \ldots, r \), the leading coefficient of \( g_j \) has the following form:

\[
\frac{[c_j]_\mathcal{Q}}{[1]_\mathcal{Q}}.
\]

(c) For each \( j \), lift \( g_j \) to \( Q_j \in \hat{\mathcal{D}}_n(\mathcal{F})\langle z \rangle \) in a way that \( \text{ND}(g_j) = \text{ND}(Q_j) \). Put \( \mathcal{G} = \{Q_1, \ldots, Q_r\} \).

Such a set \( \mathcal{G} \) is called a generic Gröbner basis of \( \mathcal{J} \) on \( V(\mathcal{Q}) \subset \text{Spec}(\mathcal{C}) \).

**Remarks.**

(i) Denote by \( \text{lc}(\mathcal{G}) \) the set of the leading coefficients of the elements of \( \mathcal{G} \). We have \( \text{lc}(\mathcal{G}) \subset \mathcal{C} \setminus \mathcal{Q} \). A priori, by lemma 2, \( \mathcal{G} \) is contained in \( \hat{\mathcal{D}}_n(\mathcal{C})\langle z \rangle \). We can be more precise and say that \( \mathcal{G} \subset \hat{\mathcal{D}}_n(\mathcal{C})\langle z \rangle \cdot \mathcal{J} + \hat{\mathcal{D}}_n(\mathcal{C})\langle z \rangle \).

(ii) By using truncated divisions, the elements of \( \mathcal{G} \) shall have denominators with bounded multiplicities so by multiplying them by an element in \( \text{lc}(\mathcal{G}) \), we have: \( \mathcal{G} \subset \hat{\mathcal{D}}_n(\mathcal{C})\langle z \rangle \cdot \mathcal{J} + \hat{\mathcal{D}}_n(\mathcal{Q})\langle z \rangle \).

(iii) However, if one wants to compute a reduced generic Gröbner basis, that is a generic Gröbner basis which specializes (generically) to the (up to a factor) reduced Gröbner basis.
(see [Ba03]) then one may not be able to avoid unbounded denominators multiplicities as in (ii). Indeed, see the trivial example given in the introduction.

Now, the main result concerning a generic Gröbner basis is

**Theorem 4.** Take $Q \subset C$ prime and $J \subset \hat{D}_n(C)\langle z \rangle$. Let $G$ be a generic Gröbner basis of $J$ on $V(Q)$. Take

$$h = \prod_{Q \in G} \text{lcm}(Q)$$

which can be seen in $C \setminus Q$ (indeed, the leading coefficient of each $Q$ has this form: $\xi$, see step (b) in the construction above), then for any $P \in V(Q) \setminus V(h)$:

(i) $(G)_P \subset (J)_P$,

(ii) $\text{Exp}_{\prec}((J)_P) = \bigcup_{Q \in G} (\text{Exp}_{\prec}((Q)_P) + \mathbb{N}^{2n+1})$.

In other words, $(G)_P$ is a Gröbner basis of $(J)_P$ for a generic $P \in V(Q)$ and the leading exponents are (generically) constant.

The proof consists in considering the divisions of the $S$-operators of $(G)_Q$, then to lift these divisions from $F(Q)$ to $F$ and then to specialize into $P$ (see the detailed proof in [Ba03]).

2. Applications

- This is more a remark than an application. Concerning standard bases in the polynomial case:

  Given a ideal in $k[x_1, \ldots, x_n]$ and any order, thanks to the truncated divisions (this item is independant on generic Gröbner bases), one can show the existence of a standard bases without using any homogenization technique or the division with écart.

- Existence of comprehensive standard bases:

  Given an ideal $J$ in $C\{a, x\}$ with parameters $a = (a_1, \ldots, a_m)$ and variables $x = (x_1, \ldots, x_n)$ and given a local order on $\mathbb{N}^n$, then there exists a comprehensive standard basis $G \subset J$, that is for any $a_0$ in a small neighborhood of 0 in $C^m$, $G|_{a=a_0}$ is a standard basis of $J|_{a=a_0}$. This can be shown also for ideals in $C\{a, x\}\langle \partial_x \rangle$.

  The proof will be made in details in a subsequent paper.

- Application to the local generic Bernstein polynomial:

  In a work in progress, we prove a constructibility result concerning the local Bernstein polynomial associated with an analytic germ depending on parameters, which is a local version of A. Leykin's main one [Le01]. This makes a full use of generic standard bases in rings of analytic and formal differential operators. This application was, firstly, the main motivation for the study of generic Gröbner bases in the local case.

- In [Ba03], we showed that given an ideal $I$ in $A_n(k) \otimes k[a]$ or in $D_n \otimes C\{a\}$, then the set of $a \in k^m$ (resp. $a \in (C^m, 0)$) is stratified (constructible) by the algebraic (resp. analytic) Gröbner fan. Note that the proof makes use of reduced generic Gröbner bases. We think that this constructibility result can be applied to the study of Gutz hypergeometric systems with parameters using the results in [SST00] (this remark comes from N. Takayama). This application is a joint project work with N. Takayama.
References


