

On F5 Algorithm for Weyl Algebras over Fields with Valuations

Ari Dwi Hartanto | ari@ugm.ac.id
(Universitas Gadjah Mada, Indonesia;
PhD Student at Kanazawa University)

Prof. Katsuyoshi Ohara
(Kanazawa University)

2022.12.21: Computer Algebra – Foundations and Applications

K : a field with valuation

$K[x]$: polynomial ring $K[x_1, \dots, x_n]$

$D_n(K)$: Weyl algebra $K\langle x_1, \dots, x_n, \partial_{x_1}, \dots, \partial_{x_n} \rangle$

Definition 1

A valuation on K is a function $\text{val} : K^* \rightarrow \mathbb{R}$ satisfying

$$\text{val}(ab) = \text{val}(a) + \text{val}(b) \quad \text{and} \quad \text{val}(a + b) \geq \min(\text{val}(a), \text{val}(b)).$$

Example.

Let $K = \mathbb{Q}$, and p be a prime number.

- For $q = p^m \frac{a}{b} \in \mathbb{Q}^*$ where p does not divide both a and b , we can define $\text{val}(q) = m$.
- It is known as p -adic valuation.

Previous results by other researchers

■ Groebner bases over fields with valuations

(A.W.Chan and D.Maclagan: 2019)

- ▶ $<_c$: tropical term ordering on $K[x]$
 $ax^\alpha <_c bx^\beta$ if $\text{val}(a) + u \cdot \alpha > \text{val}(b) + u \cdot \beta$; using a monomial order (lex,...,etc.) as tie breaker.
- ▶ using a 'special' division algorithm (a modified Mora's algorithm)

■ On affine tropical F5 algorithms

(Tristan Vaccon, T.Verron, K.Yokoyama (2021))

- ▶ $<_v$: tropical term ordering on $K[x]$
 $ax^\alpha <_v bx^\beta$ if $\deg(x^\alpha) < \deg(x^\beta)$; using $<_c$ as tie breaker.
- ▶ using the tropical LUP algorithm

■ On tropical Groebner bases for rings of differential operators $D_n(K)$

(Ari Dwi Hartanto and K.Ohara: presented on Risa/Asir Conference 2022)

Tropical term ordering for $D_n(K)$

Definition 2 (presented on Risa/Asir Conference 2022)

$u, v \in \mathbb{R}^n$

$<_1$: a monomial ordering on $\mathcal{M} \subset D_n(K)$.

For $ax^\alpha \partial^\beta, bx^{\alpha'} \partial^{\beta'} \in \mathcal{T} \subset D_n(K)$, we write:

(1) $ax^\alpha \partial^\beta < bx^{\alpha'} \partial^{\beta'}$ if:

- $|\beta| < |\beta'|$; or
- $|\beta| = |\beta'|$ and $\text{val}(a) + (u, v) \cdot (\alpha, \beta) > \text{val}(b) + (u, v) \cdot (\alpha', \beta')$; or
- $|\beta| = |\beta'|$ and $\text{val}(a) + (u, v) \cdot (\alpha, \beta) = \text{val}(b) + (u, v) \cdot (\alpha', \beta')$ and $x^\alpha \partial^\beta <_1 x^{\alpha'} \partial^{\beta'}$.

(2) $ax^\alpha \partial^\beta = bx^{\alpha'} \partial^{\beta'}$ if $\text{val}(a) = \text{val}(b)$ and $(\alpha, \beta) = (\alpha', \beta')$.

and call \leq a tropical term order on \mathcal{T} .

We generalize Definition 2

Definition 3

$w, \omega \in \mathbb{R}^{2n}$ s.t. $w_i \geq 0$ and $\max_{1 \leq j \leq n} w_j < w_{n+i}$ for all $i = 1, \dots, n$,
 $<_1$: a monomial ordering on $\mathcal{M} \subset D_n(K)$.

For $ax^\alpha \partial^\beta, bx^{\alpha'} \partial^{\beta'} \in \mathcal{T} \subset D_n(K)$, we write $ax^\alpha \partial^\beta < bx^{\alpha'} \partial^{\beta'}$ if:

- (i) $w \cdot (\alpha, \beta) < w \cdot (\alpha', \beta')$; or
- (ii) $w \cdot (\alpha, \beta) = w \cdot (\alpha', \beta')$ and $-\text{val}(a) + \omega \cdot (\alpha, \beta) < -\text{val}(b) + \omega \cdot (\alpha', \beta')$; or
- (iii) $w \cdot (\alpha, \beta) = w \cdot (\alpha', \beta')$ and $-\text{val}(a) + \omega \cdot (\alpha, \beta) = -\text{val}(b) + \omega \cdot (\alpha', \beta')$ and $x^\alpha \partial^\beta <_1 x^{\alpha'} \partial^{\beta'}$.

Moreover, we write $ax^\alpha \partial^\beta = bx^{\alpha'} \partial^{\beta'}$ if $\text{val}(a) = \text{val}(b)$ and $(\alpha, \beta) = (\alpha', \beta')$.

Remark.

If we restrict our ring to $K[x] \subset D_n(K)$, we can say that

\leq is more general than \leq_c and \leq_v .

■ $\leq \Leftrightarrow \leq_c$ when $w = (0, \dots, 0, w_{n+1}, \dots, w_{2n})$ and $(\omega_1, \dots, \omega_n) = -1 \cdot u$.

■ $\leq \Leftrightarrow \leq_v$ when $w = (1, \dots, 1, w_{n+1}, \dots, w_{2n})$ and $(\omega_1, \dots, \omega_n) = -1 \cdot u$.

Division Algorithm w.r.t. \leq ?

- adopting the division algorithm as in A.W.Chan (2019)
- the algorithm only work in homogeneous polynomials

$$D_n^{(h)}(K) := K[h]\langle x_1, \dots, x_n, \partial_1, \dots, \partial_n \rangle$$

- ▶ h : the homogenization variable
- ▶ h commutes with x_i and ∂_i
- ▶ multiplication: $\partial_i x_i = x_i \partial_i + h^2$

Definition 4 (Term order with valuation on $D_n^{(h)}(K)$)

$w, \omega \in \mathbb{R}^{2n}$ s.t. $0 \leq w_i$ and $\max_{1 \leq j \leq n} w_j < w_{n+i}$ for all $i = 1, \dots, n$

We write $ax^\alpha \partial^\beta h^\gamma <_h bx^{\alpha'} \partial^{\beta'} h^{\gamma'}$ **if:**

- (i) $\deg(x^\alpha \partial^\beta) + \gamma < \deg(x^{\alpha'} \partial^{\beta'}) + \gamma'$; or
- (ii) $\deg(x^\alpha \partial^\beta) + \gamma = \deg(x^{\alpha'} \partial^{\beta'}) + \gamma'$ and $ax^\alpha \partial^\beta < bx^{\alpha'} \partial^{\beta'}$.

We write $ax^\alpha \partial^\beta h^\gamma =_h bx^{\alpha'} \partial^{\beta'} h^{\gamma'}$ **if** $\text{val}(a) = \text{val}(b)$ and $(\alpha, \beta, \gamma) = (\alpha', \beta', \gamma')$.

(Input/Output) Division Algorithm w.r.t. \leq_h

Input: A homogeneous polynomial $f \in D_n^{(h)}(K)$,

$G = \{g_1, \dots, g_N\} \subset D_n^{(h)}(K)$ a finite set of homogeneous polynomials.

Output: $H_1, \dots, H_N, r \in D_n^{(h)}(K)$ satisfying

$$f = \left(\sum_{i=1}^N H_i g_i \right) + r$$

where:

- (i) $\text{LT}(f) \geq_h \text{LT}(H_i g_i)$ for all i
- (ii) no term of r is divisible by any $\text{LM}(g_i)$.

Module of syzygies

For simplicity, let us denote $R := D_n^{(h)}(K)$.

$F := \{f_1, \dots, f_N\}$ a generating set of a left ideal $I \subset R$

We assume that they are ordered increasingly by \leq_h on their leading terms.

R^N : the free R -module generated by e_1, \dots, e_N

$\mathbb{T} := \{te_i \mid t \in \mathcal{T}, i = 1, \dots, N\}$ the set of all module terms in R^N

Define the (surjective) R -module homomorphism:

$$\begin{aligned} \nu : R^N &\longrightarrow I \\ e_i &\mapsto f_i. \end{aligned}$$

$\Rightarrow \text{Syz}(F) := \ker(\nu)$ the **module of syzygies** of F

$\Rightarrow R^N / \text{Syz}(F) \cong I$ (by the fundamental theorem of module homomorphism)

Module Term Ordering

Definition 5

\leq_h : a term order on $\mathcal{T} \subset R$ with valuation.

\prec_h denotes the module term order on $\mathbb{T} \subset R^N$, defined as follows:

$$\begin{aligned} ax^\alpha \partial^\beta h^\gamma e_i \prec_h bx^{\alpha'} \partial^{\beta'} h^{\gamma'} e_j &:\iff i < j \text{ or} \\ & i = j \text{ and } ax^\alpha \partial^\beta h^\gamma <_h bx^{\alpha'} \partial^{\beta'} h^{\gamma'} \end{aligned}$$

$$ax^\alpha \partial^\beta h^\gamma e_i =_h bx^{\alpha'} \partial^{\beta'} h^{\gamma'} e_j \quad :\iff i = j \text{ and } ax^\alpha \partial^\beta h^\gamma =_h bx^{\alpha'} \partial^{\beta'} h^{\gamma'}$$

Natural Signatures \mathfrak{s}_η

- For $f \in I$, denote \mathbf{f} an element of R^N s.t. $\nu(\mathbf{f}) = f$.
- $R^N/\text{Syz}(F) \cong I$
Let $\psi : I \longrightarrow R^N/\text{Syz}(F)$ be the (unique) module isomorphism.
 $f \mapsto \mathbf{f} + \text{Syz}(F)$
- For a function $\eta : R^N/\text{Syz}(F) \longrightarrow R^N$ defined by $\mathbf{f} + \text{Syz}(F) \mapsto \mathbf{f}$, we define a function

$$\begin{aligned} \mathfrak{s}_\eta : I \setminus \{0\} &\longrightarrow \mathbb{T} \setminus \{0\} \\ f &\mapsto \mathfrak{s}_\eta(f) := \text{LT}((\eta \circ \psi)(f)). \end{aligned}$$

10

22

Property of \mathfrak{s}_η

- $\text{LT}(\text{Syz}(F)) \subset \mathbb{T}$ the set of leading module terms of $\text{Syz}(F)$
- $\text{NS}(\text{Syz}(F)) := \mathbb{T} \setminus \text{LT}(\text{Syz}(F))$ the normal set of $\text{Syz}(F)$

Lemma 6

Let $f \in I \setminus \{0\}$ and $t \in \mathbb{T} \setminus \{0\}$.

Then:

1. $\mathfrak{s}_\eta(tf) =_h \text{LT}(t \mathfrak{s}_\eta(f)) \iff \text{LT}(t \mathfrak{s}_\eta(f)) \in \text{NS}(\text{Syz}(F))$
2. $\mathfrak{s}_\eta(tf) \prec_h \text{LT}(t \mathfrak{s}_\eta(f)) \iff \text{LT}(t \mathfrak{s}_\eta(f)) \in \text{LT}(\text{Syz}(F))$

11

22

Definition 7 (top ♯-reduction)

$f, g \in I \setminus \{0\}$, and $h \in I$

We say that f (top) ♯-reduces to h by g w.r.t. $\mathfrak{s}_\eta(f)$ if there exists $t \in \mathcal{T}$ s.t.:

- (i) $f - tg = h$ and $\text{LT}(tg) = \text{LT}(f)$,
- (ii) $\mathfrak{s}_{\eta'}(tg) \prec_p \mathfrak{s}_\eta(f)$.

The polynomial g is called ♯-reductor for f

Remark.

Performing consecutively a sequence of ♯-reduction steps $f \xrightarrow{g_1} f_{(1)} \xrightarrow{g_2} f_{(2)} \xrightarrow{g_3} \dots$ might not stop. (\prec_h is not well-order)

Algorithm 1: Sig-Top-Reduction

Input: $f \in D_n^{(h)}(K)$ homogeneous, $\mathfrak{s}_\eta(f)$,
 $G = \{g_1, \dots, g_N\} \subset D_n^{(h)}(K)$ homogeneous
Output: $H_1, \dots, H_N, r \in D_n^{(h)}(K)$ s.t.

$$f = \left(\sum_{i=1}^N H_i g_i \right) + r$$

where:

- (i) $\text{LT}(f) \geq_h \text{LT}(H_i g_i)$
- (ii) no ♯-reductor in G for $\text{LT}(r)$
- (iii) $\mathfrak{s}_\eta(f) \succ_h \text{LT}(H_i \mathfrak{s}_{\eta_i}(g_i))$.
 (This implies $\mathfrak{s}_{\eta'}(r) =_h \mathfrak{s}_\eta(f)$)

1 Initialize

2 $T \leftarrow G$
 3 $q_0 \leftarrow f, \quad j \leftarrow 0,$
 $h_{1,0} \leftarrow 0, \dots, h_{N,0} \leftarrow 0$

4 While $q_j \neq 0$ do

5 If there is no a sig-reductor in T for $\text{LT}(q_j)$
 then

6 Return: $r := q_j; \quad H_i = h_{i,j}$

7 else

8 Choose a ♯-reductor $g \in T$ for $\text{LT}(q_j)$
 with $E(q_j, m_\alpha g)$ min. among all choices.

9 Update $T \leftarrow T \cup \{q_j\}$ if $E(q_j, m_\alpha g) > 0$

10 $q' \leftarrow q_j - c_\alpha m_\alpha g$ (canceling $\text{LT}(q_j)$)

11 If $g \in G$ then

12 $q_{j+1} \leftarrow q'$
 13 \dots

14 If $g \notin G$ then

15 $q_{j+1} \leftarrow \frac{1}{1 - c_\alpha} q'$
 16 \dots

17 $j = j + 1$

18 Return $r := q_j; \quad H_i = h_{i,j}$

Definition 8

We say that $f \in I$ is \mathfrak{s} -irreducible w.r.t. $\mathfrak{s}_\eta(f)$ if:

- $f = 0$; or
- **there is no** $g \in I$ which (top) \mathfrak{s} -reduces f . (\Leftrightarrow there is no \mathfrak{s} -reductor for $\text{LT}(f)$)

Definition 9

We say that an \mathfrak{s} -irreducible $f \in I \setminus \{0\}$ is **primitive \mathfrak{s} -irreducible** w.r.t. $\mathfrak{s}_\eta(f)$ if **there is no** \mathfrak{s} -irreducible $g \in I \setminus \{0\}$ and $t \in \mathcal{T} \setminus \{1\}$ s.t.:

- (i) $\text{LT}(tg) = \text{LT}(f)$; and
- (ii) $\mathfrak{s}_{\eta'}(tg) =_h \mathfrak{s}_\eta(f)(f)$.

Proposition 10

Let $f \in I \setminus \{0\}$. Then, $\min_\eta \mathfrak{s}_\eta(f)$ exists.

We define the function

$$\begin{aligned} \text{sig} : I \setminus \{0\} &\longrightarrow \text{NS}(\text{Syz}(F)) \\ f &\mapsto \min_\eta (\mathfrak{s}_\eta(f)). \end{aligned}$$

Theorem 11

Let $f \in I$ such that f is \mathfrak{s} -irreducible with respect to $\sigma = \mathfrak{s}_\eta(f)$, and f is of the form $f = \nu(\sigma + \text{lower terms})$.

Then,:

- (i) $f = 0 \Leftrightarrow \sigma \in \text{LT}(\text{Syz}(F))$.
- (ii) $f \neq 0 \Leftrightarrow \sigma \in \text{NS}(\text{Syz}(F)) \Leftrightarrow f \neq 0$ and $\sigma = \mathfrak{s}_\eta(f) =_h \text{sig}(f)$.

Definition 12

We say that $G \subset I$ is an \mathfrak{s} -Groebner basis if for each \mathfrak{s} -irreducible $f \in I \setminus \{0\}$ w.r.t. $\text{sig}(f)$, there exist $g \in G$ and $t \in \mathcal{T}$ s.t.:

- (i) $\text{LT}(tg) = \text{LT}(f)$ and
- (ii) $\text{sig}(tg) =_h \text{sig}(f)$.

Proposition 13

If G is an \mathfrak{s} -Groebner basis w.r.t. \preceq_h , then G is a Groebner basis w.r.t. \leq_h .

Normal Pairs

Definition 14

$g_1, g_2 \in I \setminus \{0\}$.

Let $\text{spoly}(g_1, g_2) = u_1g_1 - u_2g_2$.

We say that (g_1, g_2) is a **normal pair** if:

- (i) g_i is a primitive \mathfrak{s} -irreducible w.r.t. $\mathfrak{s}_{\eta_i}(g_i)$, $i = 1, 2$;
- (ii) $\mathfrak{s}_{\eta_i}(u_i g_i) =_h \text{LT}(u_i \mathfrak{s}_{\eta_i}(g_i))$ $i = 1, 2$;
- (iii) $\mathfrak{s}_{\eta_1}(u_1 g_1) \neq_h \mathfrak{s}_{\eta_2}(u_2 g_2)$.

Theorem 15 (conjecture)

Let G be a set of \mathfrak{s} -irreducible polynomials of I s.t.:

- (i) for each $i = 1, \dots, N$ s.t. $\mathbf{e}_i \notin \text{LT}(\text{Syz}(F))$, there exists $g_i \in G$ s.t. $\mathfrak{s}(g_i) = \mathbf{e}_i$;
- (ii) for any $g_1, g_2 \in G$ s.t. (g_1, g_2) is normal, there exist $g \in G$ and $t \in \mathcal{T}$ s.t. tg is \mathfrak{s} -irreducible and $\mathfrak{s}(tg) =_h \mathfrak{s}(\text{spoly}(g_1, g_2))$.

Then G is a \mathfrak{s} -Groebner basis of I .

A problem when checking condition (ii) of normal pair definition:

$$\mathfrak{s}_\eta(tf) =_h \text{LT}(t \mathfrak{s}_\eta(f)) \quad \Leftrightarrow \quad \text{LT}(t \mathfrak{s}_\eta(f)) \notin \text{LT}(\text{Syz}(F))$$

(we do not know $\text{LT}(\text{Syz}(F))$ beforehand)

Solution?

→ Introduce a new variable S , a set of known leading terms of syzygies.

→ At the beginning, $S \leftarrow \emptyset$.

→ We enlarge S when performing sig-top-reduction algorithm on $\text{spoly}(g_1, g_2)$ yields 0.

In commutative case, we have principal syzygies $f_i \mathbf{e}_j - f_j \mathbf{e}_i$;
but not in non-commutative case: $D_n^{(h)}(K)$.

Algorithm 2: Main framework

Input: $F = \{f_1, \dots, f_N\} \subset R$ homogeneous,
 ordered in increasing tdegree
 \leq_h : term ordering on $\mathcal{T} \subset R$ with val.
Output: G : a Groebner basis
 of the left ideal I generated by F

```

1  $S \leftarrow \emptyset$ ;  $G_1 \leftarrow \{(f_1, \mathbf{e}_1)\}$ ;  $i \leftarrow 1$ ;
2 for  $j = 2, \dots, N$  do
3    $r \leftarrow \text{DIV}(f_j, \text{poly}(G_i))$ 
4   if  $r \neq 0$  then
5      $i \leftarrow i + 1$ 
6      $G_i, S \leftarrow \text{SigGr}((r, \mathbf{e}_i), G_{i-1}, S, j)$ 
7 Return:  $G := \text{poly}(G_i)$ 

```

Algorithm 3: SigGr()

Input: $(r, \mathbf{e}_i), G_{i-1}, S, j$
Output: G_i : a \mathfrak{s} -Groebner basis of the left ideal I
 generated by f_1, \dots, f_j
 S : leading terms of syzygies

```

1  $[P, S] \leftarrow \text{UpdateNPairs}(\emptyset, (r, \mathbf{e}_i), G_{i-1}, S)$ 
2  $G_i \leftarrow G_{i-1} \cup \{(r, \mathbf{e}_i)\}$ 
3 while  $P \neq \emptyset$  then
4   Prune  $P$  by  $S$ 
5   Prune  $P$  from rewritable polynomials
6   Pick  $(f, \sigma) \in P$  with minimal  $\sigma$ 
7    $(f, \sigma) \leftarrow \mathfrak{s}\text{-reduce}((f, \sigma), G)$ 
8   if  $f \neq 0$  then
9      $[P, S] \leftarrow \text{UpdateNPairs}(P, (f, \sigma), G_i, S)$ 
10     $G_i \leftarrow G_i \cup \{(f, \sigma)\}$ 
11  else
12     $S \leftarrow S \cup \{\sigma\}$ 
13 Return:  $G_i, S$ 

```

Implementation: Risa/Asir

Settings: $R = D_3^{(h)}(\mathbb{Q})$, 3-adic valuation, deglex \prec
 $w = (0, 0, 0, 1, 1, 1)$ and $\omega = (-1, -1, -1, 1, 1, 1)$

F	Buchberger Alg.			F5 Alg.*		
	CPU time (s)	#Spoly	#ZeroReds.	CPU time (s)	#N.pairs	#ZeroReds.
$x^2 + 4x\partial_y$ $z\partial_x + 4y\partial_z$	0.2969	113	99	0.2344	71	15
$3x^2 + 2x\partial_y$ $3y\partial_x^2 + 2xy\partial_z$ $\partial_x\partial_y\partial_z + 4y^2\partial_z$	12.75	1202	1154	4.484	713	56
$3y\partial_y^2 + 2z^2\partial_z$ $2\partial_x^3\partial_z + 3x^2z\partial_y$	174.2	5047	4947	13.98	742	22

Specs.:

ThinkPad X1 Nano Gen 1
 Intel® Core™ i7-1180G7 Processor (2.20 GHz up to 4.60 GHz)
 16 GB LPDDR4X-4266MHz
 Windows 11 Pro 64bit; Risa/Asir 20220403

Some References

- [1] A. Arri and J. Perry, The F5 criterion revised. *J. Symb. Computation* 46 (2011) 1017–1029.
- [2] A. Giovini, T. Mora, et al., “One sugar cube, please,” or selection strategies in the buchberger algorithm, *Proceedings of the 1991 International Symposium on Symbolic and Algebraic Computation* (1991) 49–54.
- [3] A. W. Chan and D. Maclagan, Groebner bases over fields with valuations, *Mathematics of Computation* 88 (2019) 467–483. Providence, RI, 2015.
- [4] J.C. Faugère, A new efficient algorithm for computing Gröbner bases without reduction to zero (F5). In: *ISSAC '02: Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation*. ACM Press, New York, NY, USA, pp. 75–83.
- [5] T. Hibi, *Groebner Bases: Statistics and Software Systems*, Springer, 2013.
- [6] T. Vaccon, T. Verron, K. Yokoyama, On Affine Tropical F5 Algorithms, *Journal of Symbolic Comp.* 102 (2021) 132–152
- [7] S. Coutinho, *A Primer of Algebraic D-Modules*, Cambridge University Press, 1995.

Thank You