Stafford theorem: algorithms and applications

Alban Quadrat

INRIA Sophia Antipolis, APICS Project, 2004 route des lucioles, BP 93, 06902 Sophia Antipolis cedex, France.

Alban.Quadrat@sophia.inria.fr

http://www-sop.inria.fr/members/Alban.Quadrat/index.html

KIAS Winter School on Algebraic Systems Theory

KIAS, Seoul, 15/12/08

Monge problem (1784)

- Let D be a ring of differential operators (e.g., $D = A_n(k)$).
- Let $\mathcal{F}$ be a left D-module (e.g., $k[x_1, \ldots, x_n]$, $\mathcal{F} = C^\infty(\mathbb{R}^n)$):

$$\forall\, P_1,\, P_2 \in D,\; \forall\, y_1,\, y_2 \in \mathcal{F}: \;\; P_1\, y_1 + P_2\, y_2 \in \mathcal{F}.$$

Let us consider $R \in D^{q \times p}$ and the linear system of PDEs:

$$\ker_{\mathcal{F}}(R.) \triangleq \{\eta \in \mathcal{F}^p \mid R\, \eta = 0\}.$$

- Question: When does $Q \in D^{p \times m}$ exist such that:

$$\ker_{\mathcal{F}}(R.) = \mathrm{im}_{\mathcal{F}}(Q.) \triangleq Q\, \mathcal{F}^m?$$

$\Rightarrow$ Q is called a parametrization of $\ker_{\mathcal{F}}(R.)$.

Example

- Example: $D = B_1(\mathbb{R}) = \mathbb{R}(t)\left[\partial; \mathrm{id}, \frac{d}{dt}\right]$, $\mathcal{F} = C^{\infty}(\mathbb{R})$, $\alpha \in \mathbb{R}(t)$,

$$R = \left(\partial^2 + \alpha(t)\,\partial + 1,\ -\partial - \alpha(t)\right) \in D^{1\times 2}.$$

$$\ddot{y}(t) + \alpha(t)\,\dot{y}(t) + y(t) - \dot{u}(t) - \alpha(t)\,u(t) = 0 \quad (\star)$$

$$\Leftrightarrow \left\{ \begin{array}{l} y(t) = \dot{\xi}(t) + \alpha(t)\,\xi(t), \\ u(t) = \ddot{\xi}(t) + \alpha(t)\,\dot{\xi}(t) + (\dot{\alpha}(t) + 1)\,\xi(t). \end{array} \right. \qquad (\star\star)$$

$(\star\star)$ is an injective parametrization of $(\star)$ because $\xi = -\dot{y} + u$.

- Example: $D = \mathbb{R}[\partial_1, \partial_2, \partial_3]$, $\quad \partial_i = \partial/\partial x_i$, $\quad \mathcal{F} = C^{\infty}(\mathbb{R}^3)$,

$$\begin{array}{rcl} \mathrm{div}\,\vec{A} = 0 & \Leftrightarrow & \exists\,\vec{B} \in \mathcal{F}^3 :\ \vec{A} = \mathrm{curl}\,\vec{B}, \\ \mathrm{curl}\,\vec{B} = \vec{0} & \Leftrightarrow & \exists\,f \in \mathcal{F} :\ \vec{B} = \mathrm{grad}\,f. \end{array}$$

Involution & formal adjoint

- Let k be a field, $\mathrm{char}(k) > 0$, and $D = A_n(k)$ or $B_n(k)$.
- Let θ be the involution of D defined by:

$$\theta(\partial_i) = -\partial_i, \quad \theta(x_i) = x_i, \quad \theta(a) = a, \quad \forall\, a \in k.$$

$$(\theta : D \longrightarrow D \ k\text{-linear map}, \quad \theta(P\,Q) = \theta(Q)\,\theta(P),\ \theta^2 = \mathrm{id}).$$

- If $R \in D^{q \times p}$, then the formal adjoint of R is defined by:

$$\theta(R) = (\theta(R_{ij}))^T \in D^{p \times q}.$$

- $\widetilde{N} = D^{1 \times q}/(D^{1 \times p}\,\theta(R))$ is adjoint left D-module of the finitely presented left D-module $M = D^{1 \times p}/(D^{1 \times q}\,R)$.
- If $\mathcal{F}$ is a left D-module, then we have:

$$\ker_{\mathcal{F}}(R.) = \{\eta \in \mathcal{F}^p \mid R\,\eta = 0\} \cong \hom_D(M, \mathcal{F}).$$

Definitions

- Definition: 1. M is free if $\exists\, r \in \mathbb{Z}_+$ such that $M \cong D^r$.

2. M is stably free if $\exists\, r, s \in \mathbb{Z}_+$ such that $M \oplus D^s \cong D^r$.

3. M is projective if $\exists\, r \in \mathbb{Z}_+$ and a D-module P such that:

$$M \oplus P \cong D^r.$$

4. M is reflexive if $\varepsilon : M \longrightarrow \hom_D(\hom_D(M, D), D)$ is an isomorphism, where:

$$\varepsilon(m)(f) = f(m), \quad \forall\, m \in M, \quad \forall\, f \in \hom_D(M, D).$$

5. M is torsion-free if:

$$t(M) = \{m \in M \,|\, \exists\, 0 \neq P \in D : P\, m = 0\} = 0.$$

6. M is torsion if $t(M) = M$.

Classification of modules

- Theorem:

1. We have the following implications:

$$\text{free} \Rightarrow \text{stably free} \Rightarrow \text{projective} \Rightarrow \text{reflexive} \Rightarrow \text{torsion-free.}$$

2. If D is a principal domain (e.g., $B_1(\mathbb{Q}) = \mathbb{Q}(t)\left[\partial; \mathrm{id}, \frac{d}{dt}\right]$), then:

$$\text{torsion-free} = \text{free}.$$

3. If D is a hereditary ring (e.g., $A_1(\mathbb{Q}) = \mathbb{Q}[t]\left[\partial; \mathrm{id}, \frac{d}{dt}\right]$), then:

$$\text{torsion-free} = \text{projective}.$$

4. If $D = k[\partial_1, \ldots, \partial_n]$, k is a field of constants, then:

$$\text{projective} = \text{free} \qquad \text{(Quillen-Suslin theorem)}.$$

Module M	**Homological algebra**	$\mathcal{F}$ **injective cogenerator**
with torsion	$t(M) \cong \mathrm{ext}^1_D(\widetilde{N}, D)_\theta$	$\emptyset$
torsion-free	$\mathrm{ext}^1_D(\widetilde{N}, D) = 0$	$\ker_{\mathcal{F}}(R.) = Q\, \mathcal{F}^{l_1}$
reflexive	$\mathrm{ext}^i_D(\widetilde{N}, D) = 0$ $i = 1,\, 2$	$\ker_{\mathcal{F}}(R.) = Q_1\, \mathcal{F}^{l_1}$ $\ker_{\mathcal{F}}(Q_1.) = Q_2\, \mathcal{F}^{l_2}$
projective = stably free	$\mathrm{ext}^i_D(\widetilde{N}, D) = 0$ $1 \leq i \leq n = \mathrm{gld}(D)$	$\ker_{\mathcal{F}}(R.) = Q_1\, \mathcal{F}^{l_1}$ $\ker_{\mathcal{F}}(Q_1.) = Q_2\, \mathcal{F}^{l_2}$ $\ldots$ $\ker_{\mathcal{F}}(Q_{n-1}.) = Q_n\, \mathcal{F}^{l_n}$
free	?	$\ker_{\mathcal{F}}(R.) = Q\, \mathcal{F}^m$ $\exists\; T :\;\; T\, Q = I_m$

Computation bases

- $V = \{(x \quad y \quad z)^T \in k^3 \mid 2\,x + 3\,y + 5\,z = 0\}, \quad k = \mathbb{Q},\, \mathbb{R},\, \mathbb{C}.$

$$2\,x+3\,y+5\,z = 0 \Rightarrow x = -\frac{3}{2}\,y - \frac{5}{2}\,z \Rightarrow \begin{cases} x = \frac{3}{2}\,y - \frac{5}{2}\,z, \\ y = y, \\ z = z, \end{cases} \quad \forall\, y,\, z \in k.$$

$$\Rightarrow V = k\left(-\frac{3}{2} \quad 1 \quad 0\right)^T + k\left(-\frac{5}{2} \quad 0 \quad 1\right)^T$$ basis of V.

- $M = \{(x \quad y \quad z)^T \in \mathbb{Z}^3 \mid 2\,x + 3\,y + 5\,z = 0\}.$

$$M = \mathbb{Z}\,(\alpha_1 \quad \beta_1 \quad \gamma_1)^T + \mathbb{Z}\,(\alpha_2 \quad \beta_2 \quad \gamma_2)^T \Leftrightarrow \begin{cases} x = \alpha_1\,t_1 + \alpha_2\,t_2, \\ y = \beta_1\,t_1 + \beta_2\,t_2, \quad t_i \in \mathbb{Z}, \\ z = \gamma_1\,t_1 + \gamma_2\,t_2, \qquad (\star) \end{cases}$$

$\Rightarrow \{(\alpha_i \quad \beta_i \quad \gamma_i)^T\}_{i=1,\,2}$ is a basis of M iff $(\star)$ is injective, i.e.:

$$\exists\; a_{ij} \in \mathbb{Z}, \quad i = 1,\, 2: \qquad t_i = a_{i1}\,x + a_{i2}\,y + a_{i3}\,z.$$

Stafford's results

- Theorem: Let us consider $a_1, a_2, a_3 \in D$ and the left ideal:

$$I = D\,a_1 + D\,a_2 + D\,a_3.$$

$$\Rightarrow \; \exists \; c_1, c_2 \in D : \; I = D\,(a_1 + c_1\,a_3) + D\,(a_2 + c_2\,a_3).$$

- Two constructive proofs have been developed in:

⋆ A. Hillebrand, W. Schmale, "Towards an effective version of a theorem of Stafford", *J. Symbolic Computation*, 32 (2001), 699-716.

⋆ A. Leykin, "Algorithmic proofs of two theorems of Stafford", *J. Symbolic Computation*, 38 (2004), 15 35-1550.

- Implementation in the package Stafford of OreModules.

- Corollary: A stably free left D-module M with $\mathrm{rank}_D(M) \geq 2$ is free, i.e., M admits a finite basis over D.

Elementary operations

- Definition: 1. The general linear group $\mathrm{GL}_m(D)$ is the group of invertible matrices with entries in D:

$$\mathrm{GL}_m(D) = \{\, U \in D^{m \times m} \mid \exists\, V \in D^{m \times m} : \; U\,V = V\,U = I_m \,\}.$$

2. The elementary group $\mathrm{EL}_m(D)$ is the subgroup of $\mathrm{GL}_m(D)$ generated by all matrices of the form

$$I_m + r\,E_{ij}, \quad r \in D, \quad i \neq j,$$

E_{ij} is the matrix defined by 1 at the position (i, j) and 0 else.

3. $a = (a_1 \; \ldots \; a_m)^T \in D^m$ is called unimodular if:

$$\exists\, b = (b_1 \; \ldots \; b_m) \in D^{1 \times m} : \; b\,a = \sum_{i=1}^{m} b_i\,a_i = 1.$$

We denote by $\mathrm{U}_m(D)$ the set of unimodular vectors of D^m.

• Theorem: Let $m \geq 3$ and $a = (a_1 \ \ldots \ a_m)^T \in \mathrm{U}_m(D)$. Then, there exists $E \in \mathrm{EL}_m(D)$ which satisfies:

$$E\,a = (1 \quad 0 \ \ldots \ 0)^T.$$

• Using Stafford's result, there exist $c_1, c_2 \in D$ such that:

$$a' = (a_1 + c_1\,a_m \quad a_2 + c_2\,a_m \quad a_3 \ \ldots \ a_{m-1})^T \in \mathrm{U}_{m-1}(D).$$

• $a'_1 = a_1 + c_1\,a_m, \quad a'_2 = a_2 + c_2\,a_m, \quad a'_i = a_i, \quad i \geq 3,$

$$E_1 = \begin{pmatrix} 1 & 0 & 0 & \ldots & 0 & c_1 \\ 0 & 1 & 0 & \ldots & 0 & c_2 \\ 0 & 0 & 1 & \ldots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 1 & 0 \\ 0 & 0 & 0 & \ldots & 0 & 1 \end{pmatrix} \in \mathrm{EL}_m(D).$$

Then, we have $E_1\,a = (a'_1 \quad a'_2 \ \ldots \ a'_{m-1} \quad a_m)^T$.

- $a' \in \mathrm{U}_{m-1}(D) \Rightarrow \exists\, b_1, \ldots, b_{m-1} \in D$ such that:

$$\sum_{i=1}^{m-1} b_i\, a'_i = 1 \Rightarrow \sum_{i=1}^{m-1} (a'_1 - 1 - a_m)\, b_i\, a'_i = (a'_1 - 1 - a_m).$$

- Let us define $a''_i = (a'_1 - 1 - a_m)\, b_i, \quad i \geq 1$, and:

$$E_2 = \begin{pmatrix} 1 & 0 & 0 & \ldots & 0 & 0 \\ 0 & 1 & 0 & \ldots & 0 & 0 \\ 0 & 0 & 1 & \ldots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 1 & 0 \\ a''_1 & a''_2 & a''_3 & \ldots & a''_{m-1} & 1 \end{pmatrix} \in \mathrm{EL}_m(D).$$

Using $\sum_{i=1}^{m-1} a''_i\, a'_i = a'_1 - 1 - a_m$, we then have:

$$E_2\, (a'_1 \ \ldots \ a'_{m-1} \quad a_m)^T = (a'_1 \ \ldots \ a'_{m-1} \quad a'_1 - 1)^T.$$

• If we define by

$$E_3 = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 & -1 \\ 0 & 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & 0 \\ 0 & 0 & 0 & \dots & 0 & 1 \end{pmatrix} \in \mathrm{EL}_m(D),$$

then we have:

$$E_3 \, (a'_1 \; \dots \; a'_{m-1} \quad a'_1 - 1)^T = (1 \quad a'_2 \; \dots \; a'_{m-1} \quad a'_1 - 1)^T.$$

- Finally, if we denote by

$$E_4 = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 & 0 \\ -a'_2 & 1 & 0 & \dots & 0 & 0 \\ -a'_3 & 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ -a'_{m-1} & 0 & 0 & \dots & 1 & 0 \\ -a'_1 + 1 & 0 & 0 & \dots & 0 & 1 \end{pmatrix} \in \mathrm{EL}_m(D),$$

then we finally get:

$$E_4 \, (1 \quad a'_2 \; \dots \; a'_{m-1} \quad a'_1 - 1)^T = (1 \quad 0 \; \dots \; 0)^T.$$

- Hence, if we denote by $E = E_4 \, E_3 \, E_2 \, E_1 \in \mathrm{EL}_m(D)$, then:

$$E \, (a_1 \; \dots \; a_m)^T = (1 \quad 0 \; \dots \; 0)^T.$$

Computation of basis

• Let $R \in D^{q \times p}$ be a matrix such that $p \geq q+2$ and which admits a right-inverse $S \in D^{p \times q}$.

$$0 \longrightarrow D^{1\times q} \xrightarrow{.R} D^{1\times p} \xrightarrow{\pi} M \longrightarrow 0.$$

$\Rightarrow$ M is a stably free left D-module with:

$$\mathrm{rank}_D(M) = p - q \geq 2.$$

• Compute the formal adjoint $\widetilde{R} = \theta(R) \in D^{p \times q}$:

$$0 \longleftarrow D^{1\times q} \xleftarrow{.\widetilde{R}} D^{1\times p} \longleftarrow \ker_D(.\widetilde{R}) \longleftarrow 0.$$

• If we denote by $\widetilde{S} = \theta(S)$, then we have $\widetilde{S}\,\widetilde{R} = I_q$.

- Compute $\widetilde{E_1} \in \mathrm{EL}_p(D)$ such that:

$$\widetilde{E_1}\,\widetilde{R} = \begin{pmatrix} 1 & \star \\ 0 & \\ \vdots & \widetilde{R_2} \\ 0 & \end{pmatrix}, \quad \widetilde{R_2} \in D^{(p-1)\times(q-1)}.$$

- Compute $\widetilde{E_2} \in \mathrm{EL}_{p-1}(D)$ such that:

$$\widetilde{E_2}\,\widetilde{R_2} = \begin{pmatrix} 1 & \star \\ 0 & \\ \vdots & \widetilde{R_3} \\ 0 & \end{pmatrix}, \quad \widetilde{R_3} \in D^{(p-2)\times(q-2)}.$$

$$\widetilde{E_2}' = \begin{pmatrix} 1 & 0 \\ 0 & \widetilde{E_2} \end{pmatrix} \quad \Rightarrow \quad (\widetilde{E_2}'\,\widetilde{E_1})\,\widetilde{R} = \begin{pmatrix} 1 & \star & \star \\ 0 & 1 & \star \\ \vdots & 0 & \\ \vdots & \vdots & \widetilde{R_3} \\ 0 & 0 & \end{pmatrix}.$$

- By induction, we obtain $\widetilde{U} \in \mathrm{EL}_n(D)$ such that:

$$\widetilde{T} = \widetilde{U}\,\widetilde{R} = \begin{pmatrix} 1 & \star & \star & \star & \star \\ 0 & 1 & \star & \star & \star \\ 0 & 0 & 1 & \star & \star \\ 0 & 0 & 0 & 1 & \star \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 \\ 0 & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

- We easily check that we have:

$$\ker_D(.\widetilde{T}) = D^{1\times(p-q)}\,(0 \quad I_{p-q}).$$

• If we denote by $\widetilde{P} = (0 \quad I_{p-q}) \in D^{(p-q) \times p}$, then we obtain the commutative exact diagram:

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & & & \\
 & & \uparrow & & \uparrow & & & & \\
0 & \longleftarrow & D^{1\times q} & \xleftarrow{.\widetilde{R}} & D^{1\times p} & \longleftarrow & \ker_D(.\widetilde{R}) & \longleftarrow & 0 \\
 & & \| & & \uparrow .\widetilde{U} & & & & \\
0 & \longleftarrow & D^{1\times q} & \xleftarrow{.\widetilde{T}} & D^{1\times p} & \xleftarrow{.\widetilde{P}} & D^{1\times (p-q)} & \longleftarrow & 0. \\
 & & \uparrow & & \uparrow & & & & \\
 & & 0 & & 0 & & & &
\end{array}$$

• In particular, we obtain:

$$\ker_D(.\widetilde{R}) = D^{1\times(p-q)} \, (\widetilde{P} \, \widetilde{U}) \cong D^{1\times(p-q)}.$$

Therefore, we have the split exact sequence:

$$0 \longleftarrow D^{1\times q} \xleftarrow{.\widetilde{R}} D^{1\times p} \xleftarrow{.(\widetilde{P}\ \widetilde{U})} D^{1\times(p-q)} \longleftarrow 0.$$

- By duality, we obtain the split exact sequence

$$0 \longrightarrow D^{1\times q} \xrightarrow{.R} D^{1\times p} \xrightarrow{.(U\ P)} D^{1\times(p-q)} \longrightarrow 0,$$

where $U = \theta(\widetilde{U})$, which proves

$$M = \operatorname{coker}_D(.R) \cong D^{1\times p}\,(U\ \ P) = D^{1\times(p-q)},$$

i.e., M is a free left D-module of rank $p-q$.

- Let $Q = U\,P \in D^{p\times(p-q)}$ be formed by the last $p-q$ columns of U and $T \in D^{(p-q)\times p}$ the left-inverse of Q, i.e., $T\,Q = I_{p-q}$.

Bases of free modules

- We have the following exact commutative diagram

$$
\begin{array}{ccccccc}
 & \xleftarrow{.S} & & \xleftarrow{.T} & & & \\
D^{1\times q} & \xrightarrow{.R} & D^{1\times p} & \xrightarrow{.Q} & D^{1\times (p-q)} & \longrightarrow & 0 \\
\| & & \| & & \uparrow \phi & & \\
D^{1\times q} & \xrightarrow{.R} & D^{1\times p} & \xrightarrow{\pi} & M & \longrightarrow & 0,
\end{array}
$$

where the isomorphism ϕ is defined by:

$$
\begin{array}{cccc}
\phi : M & \longrightarrow & D^{1\times (p-q)} \\
\pi(\lambda) & \longmapsto & \lambda\, Q,
\end{array}
\qquad
\begin{array}{ccc}
\phi^{-1} : D^{1\times (p-q)} & \longrightarrow & M \\
\mu & \longmapsto & \pi(\mu\, T).
\end{array}
$$

- If we denote by $\{h_k\}_{k=1,\ldots,p-q}$ the standard basis of $D^{1\times (p-q)}$, then $\{\phi^{-1}(h_k) = \pi(h_k\, T) = \pi(T_{k\bullet})\}_{k=1,\ldots,(p-q)}$ is a basis of M

$\Rightarrow$ the residue classes of the rows of T in M define a basis of M.

Injective parametrizations

- Let $\{f_j\}_{j=1,\ldots,p}$ the standard basis of D^p and $\{y_j = \pi(f_j)\}_{j=1,\ldots,p}$ a family of generators of $M = D^{1\times p}/(D^{1\times q}\,R)$.

- For $j = 1, \ldots, p$, we have

$$y_j = \phi^{-1}(\phi(y_j)) = \phi^{-1}(f_j\,Q) = \phi^{-1}\left(\sum_{k=1}^{p-q} Q_{jk}\,h_k\right) = \sum_{k=1}^{p-q} Q_{jk}\,z_k, \;(\star)$$

which shows that Q defines a parametrization of M.

- The elements $z_k = \phi^{-1}(h_k) = \pi(T_{k\bullet})$ of the basis of M satisfy

$$z_k = \pi\left(\sum_{j=1}^{p} T_{kj}\,f_j\right) = \sum_{j=1}^{p} T_{kj}\,\pi(f_j) = \sum_{j=1}^{p} T_{kj}\,y_j,$$

which proves that $(\star)$ is an injective parametrization of M.

Example

- Let us consider the time-varying linear control system:

$$\left\{ \begin{array}{l} \dot{x}_2 - u_2 = 0, \\ \dot{x}_1 - t\, u_1 = 0, \end{array} \right. \quad (\star) \quad \Rightarrow \quad R = \left(\begin{array}{cccc} 0 & \partial & 0 & -1 \\ \partial & 0 & -t & 0 \end{array} \right).$$

- $(\star)$ admits the injective parametrization of over the second Weyl algebra $B_1(\mathbb{Q}) = \mathbb{Q}(t) \left[\partial; \mathrm{id}, \frac{d}{dt}\right]$:

$$\left\{ \begin{array}{l} x_1 = \xi_1, \\ x_2 = \xi_2, \\ u_1 = \frac{1}{t}\, \dot{\xi}_1, \\ u_2 = \dot{\xi}_2. \end{array} \right. \quad (\star\star)$$

- But, the parametrization $(\star\star)$ is singular at $t = 0$.
- $M = B_1(\mathbb{Q})^{1\times 4}/(B_1(\mathbb{Q})^{1\times 2}\, R)$ is free with basis $\{x_1, x_2\}$.

- Let $D = A_1(\mathbb{Q}) = \mathbb{Q}[t]\left[\partial; \mathrm{id}, \frac{d}{dt}\right]$ and $P = D^{1\times 4}/(D^{1\times 2}\,R)$.
- P is a stably free D-module as R admits the right-inverse:

$$S = \begin{pmatrix} 0 & 0 & 0 & -1 \\ t & 0 & \partial & 0 \end{pmatrix}^T.$$

- Computing $\mathrm{ext}^1_D(\widetilde{N}, D)$, we obtain the parametrization of $(\star)$:

$$\begin{cases} x_1 = -t^2\,\xi_1 + t\,\dot{\xi}_2 - \xi_2, \\ x_2 = -\xi_3, \\ u_1 = -t\,\dot{\xi}_1 - 2\,\xi_1 + \ddot{\xi}_2, \\ u_2 = -\dot{\xi}_3. \end{cases} \qquad (\star\star\star)$$

$(\star\star\star)$ is clearly non-injective because $\mathrm{rank}_D(P) = 2$.

- P is a stably free left D-module of $\mathrm{rank}_D(P) = 2$, i.e., free.

- The formal adjoint of R is $\widetilde{R} = \begin{pmatrix} 0 & -\partial & 0 & -1 \\ -\partial & 0 & -t & 0 \end{pmatrix}^T$.
- We have the following equality of left ideals of D:

$$D\,0 + D\,(-\partial) + D\,(-1) = D\,(0 - (-1)) + D\,(-\partial + 0 \times (-1)).$$

Taking $c_1 = -1$ and $c_2 = 0$, we define the elementary matrices:

$$\widetilde{E_1} = \begin{pmatrix} 1 & 0 & 0 & -1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad \widetilde{E_2} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix},$$

$$\widetilde{E_3} = \begin{pmatrix} 1 & 0 & 0 & -1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad \widetilde{E_4} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ \partial & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

- Defining $\widetilde{E} = \widetilde{E_4}\,\widetilde{E_3}\,\widetilde{E_2}\,\widetilde{E_1}$, we get:

$$\widetilde{E}\,\widetilde{R} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & -t & -\partial \end{pmatrix}^T.$$

- We have the following equality of left ideals of D:

$$D\,0 + D\,(-t) + D\,(-\partial) = D\,(0 - \partial) + D\,(-t + 0 \times (-\partial)).$$

Taking $c_1' = 1$ and $c_2' = 0$, we define the elementary matrices:

$$\widetilde{F_1} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \widetilde{F_2} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -t & \partial & 1 \end{pmatrix},$$

$$\widetilde{F_3} = \begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \widetilde{F_4} = \begin{pmatrix} 1 & 0 & 0 \\ t & 1 & 0 \\ \partial + 1 & 0 & 1 \end{pmatrix}.$$

- If we define $\widetilde{F} = \widetilde{F_4}\,\widetilde{F_3}\,\widetilde{F_2}\,\widetilde{F_1}$ and $\widetilde{G} = \mathrm{diag}(1, \widetilde{F})$, then we get:

$$(\widetilde{G}\,\widetilde{E})\,\widetilde{R} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

• Taking the last two columns of the formal adjoint of $\widetilde{G}\,\widetilde{E}$, we obtain the matrix defining a parametrization of $(\star)$:

$$Q = \begin{pmatrix} t^2 & -t\,\partial + 1 \\ t\,(t+1) & -(t+1)\,\partial + 1 \\ t\,\partial + 2 & -\partial^2 \\ t\,(t+1)\,\partial + 2\,t + 1 & -(t+1)\,\partial^2 \end{pmatrix}$$

• The matrix Q defines an injective parametrization of $(\star)$ because

$$T = \begin{pmatrix} 0 & 0 & t+1 & -1 \\ t+1 & -t & 0 & 0 \end{pmatrix}$$

is a left-inverse of Q, i.e., $T\,Q = I_2$.

- Equivalently, time-varying linear control system

$$\begin{cases} \dot{x}_2 - u_2 = 0, \\ \dot{x}_1 - t\, u_1 = 0, \end{cases}$$

is injectively parametrized by

$$(\star) \;\Leftrightarrow\; \begin{cases} x_1 = t^2\, \xi_1 - t\, \dot{\xi}_2 + \xi_2, \\ x_2 = t\,(t+1)\, \xi_1 - (t+1)\, \dot{\xi}_2 + \xi_2, \\ u_1 = t\, \dot{\xi}_1 + 2\, \xi_1 - \ddot{\xi}_2, \\ u_2 = t\,(t+1)\, \dot{\xi}_1 + (2\,t+1)\, \xi_1 - (t+1)\, \ddot{\xi}_2, \end{cases}$$

and $\{\xi_1,\, \xi_2\}$ is a basis of the free left D-module P because:

$$\begin{cases} \xi_1 = (t+1)\, u_1 - u_2, \\ \xi_2 = (t+1)\, x_1 - t\, x_2. \end{cases}$$

Example

- Let $D = A_3(\mathbb{Q})$ and $R = -(\partial_1 - x_3 \quad \partial_2 \quad \partial_3) \in D^{1\times 3}$.
- We define the left D-module $M = D^{1\times 3}/(D\,R)$ defining:

$$\partial_1\, y_1 + \partial_2\, y_2 + \partial_3\, y_3 - x_3\, y_1 = 0. \quad (\star)$$

- Does $(\star)$ admit an injective parametrization?
- $S = (-\partial_3 \quad 0 \quad \partial_1 - x_3)^T$ satisfies $R\,S = 1$, i.e., M is stably free of rank 2, and thus, free.
- The formal adjoint $\widetilde{R}$ of R is defined by

$$\widetilde{R} = (\partial_1 + x_3 \quad \partial_2 \quad \partial_3)^T$$

is unimodular because we have $\widetilde{S}\,\widetilde{R} = 1$.

• An constructive version of Stafford's result gives

$$D\,(\partial_1+x_3)+D\,\partial_2+D\,\partial_3=D\,(\partial_1+x_3)+D\,(\partial_2+\partial_3),$$

because we have the relations

$$\left\{\begin{array}{l} \partial_2=(\partial_2\,(\partial_2+\partial_3))\,P_1-(\partial_2\,(\partial_1+x_3))\,P_2,\\ \partial_3=(\partial_3\,(\partial_2+\partial_3))\,P_1-(\partial_3\,(\partial_1+x_3))\,P_2,\end{array}\right.$$

where $P_1=\partial_1+x_3$ and $P_2=\partial_2+\partial_3$.

• Taking $c_1=0$ and $c_2=1$, we can define

$$\widetilde{E_1}=\left(\begin{array}{ccc} 1 & 0 & 0\\ 0 & 1 & 1\\ 0 & 0 & 1\end{array}\right),\quad \widetilde{E_2}=\left(\begin{array}{ccc} 1 & 0 & 0\\ 0 & 1 & 0\\ Q_1 & Q_2 & 1\end{array}\right),$$

where:

$$\left\{\begin{array}{l} Q_1=(\partial_1+x_3-1-\partial_3)\,(\partial_2+\partial_3),\\ Q_2=-(\partial_1+x_3-1-\partial_3)\,(\partial_1+x_3),\end{array}\right.$$

$$\widetilde{E_3} = \begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \widetilde{E_4} = \begin{pmatrix} 1 & 0 & 0 \\ -(\partial_2 + \partial_3) & 0 & 1 \\ -(\partial_1 + x_3 - 1) & 0 & 1 \end{pmatrix}.$$

- Defining $\widetilde{E} = \widetilde{E_4}\,\widetilde{E_3}\,\widetilde{E_2}\,\widetilde{E_1}$, we get:

$$\widetilde{E}\,(\partial_1 + x_3 \quad \partial_2 \quad \partial_3)^T = (1 \quad 0 \quad 0)^T.$$

- Taking the last two columns of $\theta(\widetilde{E})$, we obtain:

$$\begin{cases} y_1 = (1 - L_1)\,(\partial_2 + \partial_3)\,\xi_1 + ((1 - L_1)\,(\partial_1 - x_3) + 1)\,\xi_2, \\ y_2 = (-L_2\,(\partial_2 + \partial_3) + 1)\,\xi_1 - L_2\,(\partial_1 - x_3)\,\xi_2, \\ y_3 = (-(1 + L_2)\,(\partial_2 + \partial_3) + 1)\,\xi_1 - (1 + L_2)\,(\partial_1 - x_3)\,\xi_2, \end{cases}$$

$$\text{where} \begin{cases} L_1 = (\partial_2 + \partial_3)\,(\partial_1 - \partial_3 - x_3 + 1), \\ L_2 = (-\partial_1 + x_3)\,(\partial_1 - \partial_3 - x_3 + 1). \end{cases}$$

$$\begin{cases} y_1 = (1 - L_1)\,(\partial_2 + \partial_3)\,\xi_1 + ((1 - L_1)\,(\partial_1 - x_3) + 1)\,\xi_2, \\ y_2 = (-L_2\,(\partial_2 + \partial_3) + 1)\,\xi_1(x) - L_2\,(\partial_1 - x_3)\,\xi_2, \\ y_3 = (-(1 + L_2)\,(\partial_2 + \partial_3) + 1)\,\xi_1 - (1 + L_2)\,(\partial_1 - x_3)\,\xi_2, \end{cases}$$

is an injective parametrization of the system

$$\partial_1\, y_1 + \partial_2\, y_2 + \partial_3\, y_3 - x_3\, y_1 = 0, \quad (\star)$$

as we have:

$$\begin{cases} \xi_1 = (-\partial_1^2 + \partial_1\,\partial_3 - x_3\,\partial_3 + (2\,x_3 - 1)\,\partial_1 - x_3^2 + x_3 + 1)\,y_2 \\ \qquad + (\partial_1^2 - \partial_1\,\partial_3 + x_3\,\partial_3 - (2\,x_3 - 1)\,\partial_1 + x_3^2 - x_3)\,y_3, \\ \xi_2 = y_1 + (-\partial_3^2 + \partial_1\,\partial_2 - \partial_2\,\partial_3 + \partial_1\,\partial_3 + \partial_2 - (x_3 - 1)\,\partial_3 - x_3 - 2)\,y_2 \\ \qquad + (\partial_3^2 - \partial_1\,\partial_2 + \partial_2\,\partial_3 - \partial_1\,\partial_3 + (x_3 - 1)\,\partial_3 + (x_3 - 1)\,\partial_2 + 2)\,y_3. \end{cases}$$

- $\{\xi_1, \xi_2\}$ is a basis of the left D-module defined by $(\star)$.

Stable unimodular vectors

- Notation: $\mathrm{U}_m(D) = \{\text{unimodular vectors of } D^m\}$.
- Definition: $a = (a_1 \ \ldots \ a_m)^T \in \mathrm{U}_m(D)$ is stable if there exist $c_1, \ldots, c_{m-1} \in D$ such that:

$$(a_1 + c_1\, a_m \ \ldots \ a_{m-1} + c_{m-1}\, a_m)^T \in \mathrm{U}_{m-1}(D).$$

- $a = (a_1 \ \ldots \ a_m)^T$ is stable iff there exist $c_1, \ldots, c_{m-1} \in D$ and $b_1, \ldots, b_{m-1} \in D$ such that:

$$\sum_{i=1}^{m-1} b_i\,(a_i + c_i\, a_m) = 1 \Leftrightarrow \left(b_1 \ \ldots \ b_{m-1} \quad \sum_{i=1}^{m-1} b_i\, c_i\right) \begin{pmatrix} a_1 \\ \vdots \\ a_m \end{pmatrix} = 1,$$

$$\text{i.e., } b_m \triangleq \sum_{i=1}^{m-1} b_i\, c_i \in b_1\, D + \ldots + b_{m-1}\, D.$$

Examples

• Example: Let $D = \mathbb{Q}[x]$ and $a = (x^2 + 1 \quad x)^T \in D^2$. The vector a is unimodular because:

$$(1 \quad -x) \begin{pmatrix} x^2 + 1 \\ x \end{pmatrix} = 1.$$

Moreover, a is stable because $(x^2 + 1) - x\,x = 1 \in \mathrm{U}_1(D)$.

The vector $a' = (x \quad x^2 + 1)^T$ is also unimodular but not stable:

$$\forall\, c \in D, \quad \deg(x + c(x)\,(x^2 + 1)) \geq 1.$$

• Example: Let $D = A_3(\mathbb{Q})$ and $a = (\partial_1 + x_3 \quad \partial_2 \quad \partial_3)^T \in D^3$. The vector a is unimodular because $b = (\partial_3 \quad 0 \quad -(\partial_1 + x_3))$ is a left-inverse of a over D. Moreover, we have:

$$(\partial_2 + \partial_3 \quad -(\partial_1 + x_3)) \begin{pmatrix} \partial_1 + x_3 + 0\,\partial_3 \\ \partial_2 + \partial_3 \end{pmatrix} = 1.$$

Stable rank

- Definition: The stable rank of D, denoted by $\mathrm{sr}(D)$ is the least integer m such that every element of $\mathrm{U}_{m+1}(D)$ is stable.

- Example: $\mathrm{sr}(D) = 2$

$$\Rightarrow \left\{ \begin{array}{l} \forall \, (a_1 \quad a_2 \quad a_3)^T \in \mathrm{U}_3(D), \; \exists \; c_1, \, c_2 \in D : \\ \qquad\qquad\qquad\qquad (a_1 + c_1 \, a_3 \quad a_2 + c_2 \, a_3)^T \in \mathrm{U}_2(D), \\ \exists \, (a_1 \quad a_2)^T \in \mathrm{U}_2(D) : \; \forall \; c \in D, \; a_1 + c \, a_2 \notin \mathrm{U}_1(D). \end{array} \right.$$

- Example: $\mathrm{sr}(D) = 1 \; \Rightarrow \; \forall \, (a_1 \quad a_2)^T \in \mathrm{U}_2(D), \; \exists \; c \in D$:

$$a_1 + c \, a_2 \in \mathrm{U}_1(D) \; \Leftrightarrow \; (a_1 + c \, a_2)^{-1} \in D.$$

- Example: According to Stafford theorem ($D = A_n(k)$ or $B_n(k)$, $\mathrm{char}(k) > 0$), for all $a_1, \, a_2, \, a_3 \in D$, there exist c_1 and $c_2 \in D$ s.t.:

$$D \, a_1 + D \, a_2 + D \, a_3 = D \, (a_1 + c_1 \, a_3) + D \, (a_2 + c_2 \, a_3) \; \Rightarrow \; \mathrm{sr}(D) = 2.$$

Examples

- Example: If k is a field of characteristic 0, then $\mathrm{sr}(A_n(k)) = 2$.

- Example: If k is a field of characteristic 0, then $\mathrm{sr}(B_n(k)) = 2$.

- Example: If D is a a commutative noetherian ring of Krull dimension d, then $\mathrm{sr}(D) \leq d + 1$.

- Example: If D is an integral domain (e.g., $\mathbb{Z}$, $k[x]$, k a field), then $\mathrm{sr}(D) \leq 2$.

- Example: $\mathrm{sr}(\mathbb{R}[x_1, \ldots, x_n]) = n + 1$.

Generalization I

• Proposition: If $a = (a_1 \ \ldots \ a_m)^T$ is a stable element of $\mathrm{U}_m(D)$, then there exists $E \in \mathrm{EL}_m(D)$ such that:

$$E \begin{pmatrix} a_1 \\ \vdots \\ a_m \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

More precisely, let $c_1, \ldots, c_{m-1} \in D$ such that

$$a' = (a_1 + c_1\, a_m \quad a_2 + c_2\, a_m \ \ldots \ a_{m-1} + c_{m-1}\, a_m)^T \in \mathrm{U}_{m-1}(D),$$

and $b_1, \ldots, b_{m-1} \in D$ satisfying $\sum_{i=1}^{m-1} b_i\, a'_i = 1$. Let us introduce

$$a''_i = (a'_1 - 1 - a_m)\, b_i, \quad i = 1, \ldots, m-1,$$

and following matrices $E_i \in \mathrm{EL}_m(D)$:

Generalization I

$$E_1 = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 & c_1 \\ 0 & 1 & 0 & \dots & 0 & c_2 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & c_{m-1} \\ 0 & 0 & 0 & \dots & 0 & 1 \end{pmatrix}, \quad E_2 = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & 1 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & 0 \\ a''_1 & a''_2 & a''_3 & \dots & a''_{m-1} & 1 \end{pmatrix},$$

$$E_3 = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 & -1 \\ 0 & 1 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & 0 \\ 0 & 0 & 0 & \dots & 0 & 1 \end{pmatrix}, \quad E_4 = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 & 0 \\ -a'_2 & 1 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ -a'_{m-1} & 0 & 0 & \dots & 1 & 0 \\ -a'_1 + 1 & 0 & 0 & \dots & 0 & 1 \end{pmatrix}.$$

Then, we have $(E_4\, E_3\, E_2\, E_1)\, a = (1 \quad 0 \, \dots \, 0)^T$.

Generalization II

• Theorem: Let D be a ring (admitting an involution θ) and M a stably free left D-module defined by the finite free resolution:

$$0 \longrightarrow D^{1\times q} \xrightarrow{.R} D^{1\times p} \xrightarrow{\pi} M \longrightarrow 0.$$

If $\mathrm{rank}_D(M) = p - q \geq \mathrm{sr}(D)$, then M is a free left D-module.

• The proof of the theorem is similar as for the Stafford thm.

We can apply the previous proposition till the last column

$$E\,\theta(R) = \begin{pmatrix} 1 & \star & \dots & \dots & \star \\ 0 & 1 & \star & \dots & \star \\ \vdots & \vdots & \vdots & \vdots & \star \\ 0 & 0 & 0 & \vdots & L \end{pmatrix}$$

because we have $L \in D^{(p-(q-1))\times 1}$ and $p - q + 1 \geq \mathrm{sr}(D) + 1$.

Conclusion

• We have given a constructive algorithm for computing bases of free modules over the Weyl algebras $D = A_n(k)$ and $B_n(k)$, when k is a field of $\mathrm{char}(k) > 0$.

• This algorithm and the Stafford theorem on the generation of left ideals over the Weyl algebras are implemented in the package STAFFORD for $k = \mathbb{Q}$ (Q.-Robertz):

http://wwwb.math.rwth-aachen.de/OreModules/

• Algorithms for the computation of projective dimensions and shortest free resolutions are also available in OREMODULES.

A. Q, D. Robertz, *Computation of bases of free modules over the Weyl algebras*, Journal of Symbolic Computation, 42 (2007), 1113-1141.