Quillen-Suslin 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

Introduction

• In Talk 1, we have shown how to check whether or not a left module $M = D^{1\times p}/(D^{1\times q} R)$ over a certain Ore algebra D was:

1. torsion,
2. admits non-trivial torsion elements,
3. torsion-free,
4. reflexive,
5. projective.

• In this talk, we study stably free and free modules.

• We shall focus on the so-called Quillen-Suslin theorem proving that projective modules over $D = k[x_1, \ldots, x_n]$ (k a field) are free.

1. Constructive computation of bases of free D-modules:

   package QuillenSuslin.

2. Applications in mathematical systems theory.

Shorter free resolutions

- Theorem: Let us consider a finite free resolution of M:

$$0 \longrightarrow D^{1\times p_m} \xrightarrow{.R_m} D^{1\times p_{m-1}} \xrightarrow{.R_{m-1}} \ldots \xrightarrow{.R_2} D^{1\times p_1} \xrightarrow{.R_1} D^{1\times p_0} \xrightarrow{\pi} M \longrightarrow 0.$$

1. If $m \geq 3$ and there exists $S_m \in D^{p_{m-1}\times p_m}$ such that $R_m\, S_m = I_{p_m}$, then we have the finite free resolution of M:

$$0 \longrightarrow D^{1\times p_{m-1}} \xrightarrow{.T_{m-1}} D^{1\times (p_{m-2}+p_m)} \xrightarrow{.T_{m-2}} D^{1\times p_{m-3}} \xrightarrow{.R_{m-3}} \ldots \xrightarrow{\pi} M \longrightarrow 0, \quad (1)$$

$$\text{where} \quad T_{m-1} = (R_{m-1} \quad S_m), \quad T_{m-2} = \begin{pmatrix} R_{m-2} \\ 0 \end{pmatrix}.$$

2. If $m = 2$ and there exists $S_2 \in D^{p_1\times p_2}$ such that $R_2\, S_2 = I_{p_2}$, then we have the finite free resolution

$$0 \longrightarrow D^{1\times p_1} \xrightarrow{.T_1} D^{1\times (p_0+p_2)} \xrightarrow{\tau} M \longrightarrow 0, \quad (2)$$

where $T_1 = (R_1 \quad S_2)$ and $\tau = \begin{pmatrix} \pi \\ 0 \end{pmatrix}$.

Example: annihilator of $\dot{\delta}$

- $\dot{\delta}$ satisfies the system: $\quad t^2\, y(t) = 0, \quad t\, \dot{y}(t) + 2\, y(t) = 0.$
- We consider $D = \mathbb{Q}[t]\left[\partial; \mathrm{id}, \frac{d}{dt}\right]$ and the left D-module:

$$M = D/\left(D\, t^2 + D\,(t\,\partial + 2)\right).$$

- M admits the following finite free resolution of M:

$$0 \longrightarrow D \xrightarrow{.R_2} D^{1\times 2} \xrightarrow{.R_1} D \xrightarrow{\pi} M \longrightarrow 0,$$

$$R_1 = \begin{pmatrix} t^2 & t\,\partial + 2 \end{pmatrix}^T, \quad R_2 = \begin{pmatrix} \partial & -t \end{pmatrix}.$$

- $S_2 = \begin{pmatrix} t & \partial \end{pmatrix}^T$ is a right-inverse of R_2, and thus, we get:

$$0 \longrightarrow D^{1\times 2} \xrightarrow{.T_1} D^{1\times 2} \xrightarrow{\tau} M \longrightarrow 0, \quad T_1 = \begin{pmatrix} t^2 & t \\ t\,\partial + 2 & \partial \end{pmatrix}.$$

Example: contact transformations

- $D = A_3(\mathbb{Q}) = \mathbb{Q}[x_1, x_2, x_3]\left[\partial_1; \mathrm{id}, \frac{\partial}{\partial x_1}\right]\left[\partial_2; \mathrm{id}, \frac{\partial}{\partial x_2}\right]\left[\partial_3; \mathrm{id}, \frac{\partial}{\partial x_3}\right]$,

$$R_1 = \begin{pmatrix} \frac{1}{2}\,x_2\,\partial_1 & x_2\,\partial_2 + 1 & x_2\,\partial_3 + \frac{1}{2}\,\partial_1 \\ -\frac{1}{2}\,x_2\,\partial_2 - \frac{3}{2} & 0 & \frac{1}{2}\,\partial_2 \\ -\partial_1 - \frac{1}{2}\,x_2\,\partial_3 & -\partial_2 & -\frac{1}{2}\,\partial_3 \end{pmatrix} \in D^{3\times 3}.$$

- If $R_2 = (\partial_2 \quad -(\partial_1 + x_3\,\partial_3) \quad x_2\,\partial_2 + 2)$, then the left D-module $M = D^{1\times 3}/(D^{1\times 3}\,R_1)$ admits the finite free resolution:

$$0 \longrightarrow D \xrightarrow{.R_2} D^{1\times 3} \xrightarrow{.R_1} D^{1\times 3} \xrightarrow{\pi} M \longrightarrow 0.$$

- $S_2 = (-x_2 \quad 0 \quad 1)^T$ is a right-inverse of R_2 and we get:

$$0 \longrightarrow D^{1\times 3} \xrightarrow{.T_1} D^{1\times 4} \xrightarrow{\tau} M \longrightarrow 0,$$

$$T_1 = \begin{pmatrix} \frac{1}{2}\,x_2\,\partial_1 & x_2\,\partial_2 + 1 & x_2\,\partial_3 + \frac{1}{2}\,\partial_1 & -x_2 \\ -\frac{1}{2}\,x_2\,\partial_2 - \frac{3}{2} & 0 & \frac{1}{2}\,\partial_2 & 0 \\ -\partial_1 - \frac{1}{2}\,x_2\,\partial_3 & -\partial_2 & -\frac{1}{2}\,\partial_3 & 1 \end{pmatrix}.$$

Projective dimensions

• Definition: A projective resolution of a left D-module M is an exact sequence of the form

$$0 \longrightarrow P_n \xrightarrow{\delta_n} P_{n-1} \xrightarrow{\delta_{n-1}} \ldots \xrightarrow{\delta_1} P_0 \xrightarrow{\delta_0} M \longrightarrow 0, \quad (\star)$$

where the $P_i's$ are projective left D-modules.

• Definition: We call left projective dimension of a left D-module M, denoted by $\mathrm{lpd}_D(M)$, the smallest n such that there exists a projective resolution of the form $(\star)$.

• Proposition: $\mathrm{lpd}_D(M) = n$ iff there exists a finite projective resolution $(\star)$ of M, where δ_n is nonsplit, i.e., there exists no D-morphism $\tau_n : P_{n-1} \longrightarrow P_n$ such that $\tau_n \circ \delta_n = \mathrm{id}_{P_n}$, with the convention $P_{-1} = M$.

Computation of left projective dimensions

- Algorithm: 1. Compute a finite free resolution of M.

2. Set $j = m$ and $T_j = R_m$.

3. Check if R_j admits a right-inverse S_j over D.

$\Rightarrow$ If not, then exit and $\mathrm{lpd}_D(M) = j$.

$\Rightarrow$ If yes and:

(a) If $j = 1$, then exit with $\mathrm{lpd}_D(M) = 0$.
(b) If $j = 2$, then compute (2) and return to 3 with $j \leftarrow j - 1$.
(c) If $j \geq 3$, then compute (1) and return to 3 with $j \leftarrow j - 1$.

- Example: The left $A_1(\mathbb{Q})$-module M associated with the annihilator of $\dot{\delta}$ has $\mathrm{lpd}_D(M) = 1$.

- Example: The left $A_3(\mathbb{Q})$-module M associated with the contact transformations has $\mathrm{lpd}_D(M) = 0$.

Shortest free resolutions

- If M is a projective left D-module, then $\mathrm{lpd}_D(M) = 0$.
- Moreover, if M admits a finite free resolution

$$0 \longrightarrow D^{1\times p_m} \xrightarrow{.R_m} D^{1\times p_{m-1}} \xrightarrow{.R_{m-1}} \dots \xrightarrow{.R_2} D^{1\times p_1} \xrightarrow{.R_1} D^{1\times p_0} \xrightarrow{\pi} M \longrightarrow 0,$$

then the previous algorithm returns a matrix $R \in D^{q\times p}$ such that

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

is a split finite free resolution of M, i.e., $(\star)$ is exact and R admits a right-inverse $S \in D^{p\times q}$, i.e., $R\,S = I_q$.

In particular, we have $D^{1\times p} \cong M \oplus D^{1\times q}$, which proves that M is a stably free left D-module (Serre's theorem).

- The matrix R will be called a minimal presentation matrix of M.

Example: contact transformations

- We consider the left $D = A_3(\mathbb{Q})$-module $M = D^{1\times 3}/(D^{1\times 3}\, R_1)$:

$$R_1 = \begin{pmatrix} \frac{1}{2}\, x_2\, \partial_1 & x_2\, \partial_2 + 1 & x_2\, \partial_3 + \frac{1}{2}\, \partial_1 \\ -\frac{1}{2}\, x_2\, \partial_2 - \frac{3}{2} & 0 & \frac{1}{2}\, \partial_2 \\ -\partial_1 - \frac{1}{2}\, x_2\, \partial_3 & -\partial_2 & -\frac{1}{2}\, \partial_3 \end{pmatrix}.$$

- M is a stably free left D-module defined by the minimal presentation matrix T_1: $\quad 0 \longrightarrow D^{1\times 3} \xrightarrow{.T_1} D^{1\times 4} \xrightarrow{\tau} M \longrightarrow 0$,

$$T_1 = \begin{pmatrix} \frac{1}{2}\, x_2\, \partial_1 & x_2\, \partial_2 + 1 & x_2\, \partial_3 + \frac{1}{2}\, \partial_1 & -x_2 \\ -\frac{1}{2}\, x_2\, \partial_2 - \frac{3}{2} & 0 & \frac{1}{2}\, \partial_2 & 0 \\ -\partial_1 - \frac{1}{2}\, x_2\, \partial_3 & -\partial_2 & -\frac{1}{2}\, \partial_3 & 1 \end{pmatrix},$$

$$S_1 = \begin{pmatrix} 0 & -1 & 0 \\ 1 & 0 & x_2 \\ 0 & -x_2 & 0 \\ \partial_2 & -\partial_1 - x_2\, \partial_3 & x_2\, \partial_2 + 2 \end{pmatrix}, \quad T_1\, S_1 = I_3.$$

Existence of finite free resolutions

• Theorem: Let A be a left noetherian ring of finite left projective dimension $\mathrm{lgld}(A)$ and whose finitely generated projective left A-module are stably free. Let $D = A[\partial_1; \alpha_1, \beta_1] \dots [\partial_m; \alpha_m, \beta_m]$ be an Ore algebra where the α_i's are automorphisms. Then, we have:

1. Every finitely generated left D-module admits a finite free resolution of length $\mathrm{lpd}(D) + 1$.
2. Every finitely generated projective left D-module is stably free.

• Example: $D = A[x_1, \dots, x_n]$, where A is a principal ideal domain (e.g., $A = \mathbb{Z}$, $A = k$ a field).

• Example: The Weyl algebras $D = A_n(k)$ and $B_n(k)$.

Characterization of free modules

- Let M be a stably free left D-module defined by a minimal presentation matrix R:

$$0 \longrightarrow D^{1\times q} \xrightarrow{.R} D^{1\times p} \xrightarrow{\pi} M \longrightarrow 0, \quad R\,S = I_q.$$

- $\mathrm{GL}_p(D) = \{U \in D^{p\times p} \mid \exists\, V \in D^{p\times p} : \; U\,V = V\,U = I_p\}$.

- Theorem: Let $R \in D^{q\times p}$ be a matrix admitting a right-inverse over D. Then, the left D-module $M = D^{1\times p}/(D^{1\times q}\,R)$ is free of rank $p-q$ iff there exists $U \in \mathrm{GL}_p(D)$ satisfying:

$$R\,U = (I_q \quad 0).$$

Then, $U^{-1} = \begin{pmatrix} R \\ T \end{pmatrix}$, where $T \in D^{(p-q)\times p}$, and the family $\{\pi(T_{i\bullet})\}_{i=1,\dots,p-q}$ forms a basis of the free left D-module M.

Proof

- Let us suppose that there exists $U \in \mathrm{GL}_p(D)$ such that:

$$R\,U = (I_q \quad 0).$$

- We obtain the following commutative exact diagram

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & & & \\
 & & \downarrow & & \downarrow & & & & \\
0 & \longrightarrow & D^{1\times q} & \xrightarrow{.R} & D^{1\times p} & \xrightarrow{\pi} & M & \longrightarrow & 0 \\
 & & \| & & \downarrow .U & & & & \\
0 & \longrightarrow & D^{1\times q} & \xrightarrow{.(I_q \quad 0)} & D^{1\times p} & \xrightarrow{.\left(\begin{array}{c} 0 \\ I_{p-q} \end{array}\right)} & D^{1\times(p-q)} & \longrightarrow & 0, \\
 & & \downarrow & & \downarrow & & & & \\
 & & 0 & & 0 & & & &
\end{array}$$

which proves that $M \cong D^{1\times(p-q)}$, i.e., M is a free of rank $p-q$.

Proof

- Let M be a free left D-module, i.e., $\phi : M \xrightarrow{\cong} D^{1\times(p-q)}$.
- We have the following exact commutative diagram $(.Q = \phi \circ \pi)$

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

where the first horizontal exact sequence splits, namely:

$$R\,Q = 0, \quad R\,S = I_q, \quad T\,Q = I_{p-q}, \quad T\,S = 0, \quad S\,R + Q\,T = I_p,$$

i.e., $\begin{pmatrix} R \\ T \end{pmatrix} (S \quad Q) = \begin{pmatrix} I_q & 0 \\ 0 & I_{p-q} \end{pmatrix} = I_p, \quad (S \quad Q) \begin{pmatrix} R \\ T \end{pmatrix} = I_p.$

Proof

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

The isomorphism ϕ is defined by:

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

• 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 $\{f_j\}_{j=1,\ldots,p}$ be the standard basis of $D^{1\times p}$ 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.

Injective parametrizations

- Let $M = D^{1\times p}/(D^{1\times q}\, R)$ be a torsion-free left D-module.
- From the vanishing of $\mathrm{ext}_D^1(N, D)$, where $N = D^q/(R\, D^p)$ is the Auslander transpose of M, we obtain $Q \in D^{p\times m}$ such that

$$\begin{array}{ccccccccc} & & D^{1\times q} & \xrightarrow{.R} & D^{1\times p} & \xrightarrow{\pi} & M & \longrightarrow 0 \\ 0 \longleftarrow N & \xleftarrow{\kappa} & D^q & \xleftarrow{R.} & D^p & \xleftarrow{Q.} & D^m & \\ & & D^{1\times q} & \xrightarrow{.R} & D^{1\times p} & \xrightarrow{.Q} & D^{1\times m}, & \end{array}$$

$\mathrm{ext}_D^1(N, D) = \ker_D(.Q)/(D^{1\times q}\, R) = 0 \Leftrightarrow M \cong D^{1\times p}\, Q \subseteq D^{1\times m}$.

- If $.Q : D^{1\times p} \longrightarrow D^{1\times m}$ is surjective, i.e, Q admits a left-inverse $T \in D^{m\times p}$, i.e., $T\, Q = I_m$, then we have

$$M \cong D^{1\times p}\, Q = D^{1\times m},$$

i.e., M is a free left D-module of rank m, $\{\pi(T_{k\bullet})\}_{k=1,\dots,m}$ is a basis and Q an injective parametrization of M.

Example: contact transformations

- We consider the left $D = A_3(\mathbb{Q})$-module $M = D^{1\times 3}/(D^{1\times 3}\, R)$:

$$R = \begin{pmatrix} \frac{1}{2}\, x_2\, \partial_1 & x_2\, \partial_2 + 1 & x_2\, \partial_3 + \frac{1}{2}\, \partial_1 \\ -\frac{1}{2}\, x_2\, \partial_2 - \frac{3}{2} & 0 & \frac{1}{2}\, \partial_2 \\ -\partial_1 - \frac{1}{2}\, x_2\, \partial_3 & -\partial_2 & -\frac{1}{2}\, \partial_3 \end{pmatrix}.$$

- Checking the vanishing of $\operatorname{ext}^1_D(\widetilde{N}, D) = 0$, we obtain that

$$Q = (-\partial_2 \quad x_2\, \partial_3 + \partial_1 \quad -(x_2\, \partial_2 + 2))^T$$

defines a parametrization of M, i.e., $M \cong D^{1\times 3}\, Q \subseteq D$.

- Q admits the left-inverse $T = \frac{1}{2}\,(x_2 \quad 0 \quad -1)$, which proves that $M \cong D^{1\times 3}\, Q = D$ and $z = \pi(T)$ is a basis of M.

- The generators $\{y_i = \pi(f_j)\}_{j=1,2,3}$ of M satisfying the relations $R\, y = 0$, where $y = (y_1,\, y_2,\, y_3)^T$, satisfy $y = Q\, z$ and $z = T\, y$:

$$y_1 = -\partial_2\, z, \quad y_2 = (x_2\, \partial_3 + \partial_1)\, z, \quad y_3 = -(x_2\, \partial_2 + 2)\, z,$$

$$z = \frac{1}{2}\,(x_2\, y_1 - y_3).$$

Minimal parametrizations

- We generally have $m \geq \mathrm{rank}_D(M)$ (e.g., $\ker_D(Q.) \neq 0$).

- Theorem: Let $M = D^{1\times p}/(D^{1\times q}\, R)$ be a torsion-free left D-module. Then, there exists a parametrization $P \in D^{p\times l}$ of M such that $l = \mathrm{rank}_D(M)$, i.e., $L = D^{1\times l}/(D^{1\times p}\, P)$ is torsion.

- P is called a minimal parametrization of M.

- Algorithm: P can be obtained by selecting $\mathrm{rank}_D(M)$ right D-linearly independent columns of a parametrization Q of M.

- Heuristic method for computing basis of a free left D-modules:

1. Compute $Q \in D^{p\times m}$ such that $\ker_D(R.) = Q\, D^m$.
2. Define $P \in D^{p\times \mathrm{rank}_D(M)}$ by selecting $\mathrm{rank}_D(M)$ right D-linearly independent columns of Q.
3. Check whether or not P admits a left-inverse over D.

Example

We consider the $D = \mathbb{Q}[x_1, x_2]$-module $M = D^{1\times 3}/(D\,R)$, where:

$$R = (x_1\,x_2^2 + 1 \quad 3\,x_2/2 + x_1 - 1 \quad 2\,x_1\,x_2), \quad \mathrm{rank}_D(M) = 2.$$

- Checking $\mathrm{ext}^1_D(D/(D^{1\times 3}\,R^T), D) = 0$, we obtain that

$$Q = \begin{pmatrix} -4\,x_1 - 6\,x_2 + 4 & 6\,x_2^2 - 4\,x_2 & 0 \\ 4 & -4\,x_2 & 4\,x_1\,x_2 \\ 2\,x_1\,x_2 + 3\,x_2^2 - 2\,x_2 & -3\,x_2^3 + 2\,x_2^2 + 2 & -2\,x_1 - 3\,x_2 + 2 \end{pmatrix},$$

is a parametrization of M, i.e., $M \cong D^{1\times 3}\,Q \subseteq D^{1\times 3}$.

- Selecting the first two columns of Q, we obtain that

$$P = \begin{pmatrix} -4\,x_1 - 6\,x_2 + 4 & 6\,x_2^2 - 4\,x_2 \\ 4 & -4\,x_2 \\ 2\,x_1\,x_2 + 3\,x_2^2 - 2\,x_2 & -3\,x_2^3 + 2\,x_2^2 + 2 \end{pmatrix},$$

is a minimal parametrization of M, i.e.:

$$M \cong D^{1\times 3}\,Q \subseteq D^{1\times 2} = D^{1\times \mathrm{rank}_D(M)}.$$

Example

- The parametrization P of M admits a left-inverse defined by:

$$T = \frac{1}{4} \left(\begin{array}{ccc} x_2^2 & 1 & 2\,x_2 \\ x_2 & 0 & 2 \end{array} \right).$$

- The set of generators $\{y_j = \pi(f_j)\}_{j=1,2,3}$ of M satisfies

$$(x_1\,x_2^2 + 1)\,y_1 + (3\,x_2/2 + x_1 - 1)\,y_2 + 2\,x_1\,x_2\,y_3 = 0,$$

and a basis $\{z_1, z_2\}$ of M is defined by:

$$\left\{ \begin{array}{l} z_1 = \frac{1}{4}\,(x_2^2\,y_1 + y_2 + 2\,x_2\,y_3), \\ z_2 = \frac{1}{4}\,(x_2\,y_1 + 2\,y_3). \end{array} \right.$$

- The generators $\{y_1, y_2, y_3\}$ can be written in the basis $\{z_1, z_2\}$:

$$\left\{ \begin{array}{l} y_1 = (-4\,x_1 - 6\,x_2 + 4)\,z_1 + (6\,x_2^2 - 4\,x_2)\,z_2, \\ y_2 = 4\,z_1 - 4\,x_2\,z_2, \\ y_3 = (2\,x_1\,x_2 + 3\,x_2^2 - 2\,x_2)\,z_1 + (-3\,x_2^3 + 2\,x_2^2 + 2)\,z_2. \end{array} \right.$$

Computation of bases of general free modules

- Let $P \in D^{p\times m}$ and $D^{1\times p} \xrightarrow{.P} D^{1\times m}$.

1. If $U = D^{1\times p}\, P$ is free, then compute $R \in D^{q\times p}$ such that:

$$0 \longrightarrow D^{1\times q} \xrightarrow{.R} D^{1\times p} \xrightarrow{.P} D^{1\times m} \quad \text{is exact.}$$

$$\Rightarrow \begin{array}{ccccccccc} 0 & \longrightarrow & D^{1\times q} & \xrightarrow{.R} & D^{1\times p} & \xrightarrow{.P} & D^{1\times p}\,P & \longrightarrow & 0 \\ & & \| & & \| & & \uparrow \psi & & \\ 0 & \longrightarrow & D^{1\times q} & \xrightarrow{.R} & D^{1\times p} & \xrightarrow{\pi} & M & \longrightarrow & 0, \end{array}$$

where $\psi(\pi(\lambda)) = \lambda\, P$, $\forall\, \lambda \in D^{1\times p}$. We get $U = \psi(M)$ and:

$$\Rightarrow \; U = D^{1\times (p-q)}\,(T\,P), \quad \text{where} \quad \left(\begin{array}{c} R \\ T \end{array}\right) (S \quad Q) = I_p.$$

2. If $V = \ker_D(.P)$ is free, then compute $R \in D^{q\times p}$ such that $\ker_D(.P) = D^{1\times q}\, R$ and go to 1 with $V = D^{1\times p}\, R$.

3. If $W = D^{1\times p}/\ker_D(.P)$, then $W = D^{1\times p}/(D^{1\times q}\, R) = M$.

Quillen-Suslin theorem

• Theorem: Every finitely generated projective module over the ring $D = k[x_1, \ldots, x_n]$, where k is a field, is free.

• Corollary: For every stably free D-module $M = D^{1\times p}/(D^{1\times q}\, R)$ defined by a minimal presentation matrix $R \in D^{q\times p}$, there exists $U \in \mathrm{GL}_p(D)$, i.e., $\det U \in k \setminus \{0\}$, such that:

$$R\, U = (I_q \quad 0).$$

• Corollary: For every stably free D-module $M = D^{1\times p}/(D^{1\times q}\, R)$ defined by a minimal presentation matrix $R \in D^{q\times p}$, there exists $T \in D^{(p-q)\times p}$ such that:

$$\det\left(\left(\begin{array}{c} R \\ T \end{array}\right)\right) \in k \setminus \{0\}.$$

• Constructive proofs of the Quillen-Suslin have been given in the literature (e.g., Logar-Sturmfels, Park, Lombardi-Yengui).

Particular case: principal ideal domain D

- Let D be a principal ideal domain D (e.g., $D = k[x]$, k a field).
- Computing a Smith normal form of $R \in D^{q \times p}$ satisfying $R\,S = I_q$, we obtain $F \in \mathrm{GL}_q(D)$ and $G \in \mathrm{GL}_p(D)$ satisfying:

$$R = F\,(I_q \quad 0)\,G = F\,(I_q \quad 0)\begin{pmatrix} G_1 \\ G_2 \end{pmatrix} = F\,G_1 \;\Leftrightarrow\; G_1 = F^{-1}\,R.$$

$$\begin{pmatrix} F^{-1}\,R \\ G_2 \end{pmatrix} G^{-1} = I_p \;\Rightarrow\; \begin{pmatrix} F^{-1} & 0 \\ 0 & I_{p-q} \end{pmatrix}\begin{pmatrix} R \\ G_2 \end{pmatrix} G^{-1} = I_p,$$

$$\Rightarrow \begin{pmatrix} R \\ G_2 \end{pmatrix} G^{-1} \begin{pmatrix} F^{-1} & 0 \\ 0 & I_{p-q} \end{pmatrix} = I_p.$$

Then, the matrix $U = G^{-1}\begin{pmatrix} F^{-1} & 0 \\ 0 & I_{p-q} \end{pmatrix} \in \mathrm{GL}_p(D)$ satisfies:

$$R\,U = (I_q \quad 0).$$

Particular case: $R \in D^{(p-1)\times p}$

- Let D be a commutative ring and $R \in D^{(p-1)\times p}$ admitting a right-inverse $S \in D^{p\times(p-1)}$.
- Let us denote by m_i the $(p-1)\times(p-1)$-minor of R obtained by removing the i^{th} column of R.
- The m_i's satisfy a Bézout identity $\sum_{i=1}^{p} n_i\, m_i = 1$, with $n_i \in D$.
- Then, we can check that the matrix

$$V = \begin{pmatrix} & R & \\ (-1)^{p+1}\, n_1 & \dots & (-1)^{2\,p}\, n_p \end{pmatrix} \in D^{p\times p}$$

is such that $\det V = 1$ and its inverse $U = V^{-1} \in D^{p\times p}$ satisfies:

$$R\,U = (I_{p-1} \quad 0).$$

Reduction to the case of a single row

- Let $R \in D^{q \times p}$ a matrix admitting a right-inverse $S \in D^{p \times q}$.

- The computation of $U \in \mathrm{GL}_p(D)$ satisfying $R\,U = (I_q \quad 0)$ can be reduced to the case of row vectors with entries in D:

Let $U_1 \in \mathrm{GL}_p(D)$ be such that $R_{1\bullet}\,U_1 = (1 \quad 0 \; \ldots \; 0)$

$$\Rightarrow R\,U_1 = \left(\begin{array}{cc} 1 & 0 \\ C_1 & R_2 \end{array}\right).$$

$R\,S = I_q \;\Leftrightarrow\; (R\,U_1)\,(U_1^{-1}\,S) = I_q$

$$\Leftrightarrow \left(\begin{array}{cc} 1 & 0 \\ C_1 & R_2 \end{array}\right)\left(\begin{array}{cc} W & X \\ Y & Z \end{array}\right) = \left(\begin{array}{cc} 1 & 0 \\ 0 & I_{q-1} \end{array}\right) \Leftrightarrow \left\{\begin{array}{l} W = 1, \\ X = 0, \\ C_1 + R_2\,Y = 0, \\ R_2\,Z = I_{q-1}, \end{array}\right.$$

$$\Rightarrow U_2 = \left(\begin{array}{cc} 1 & 0 \\ Y & I_{p-1} \end{array}\right) \in \mathrm{GL}_p(D): \; R\,(U_1\,U_2) = \left(\begin{array}{cc} 1 & 0 \\ 0 & R_2 \end{array}\right) \ldots$$

Particular case: one invertible entry in R

- Let $R \in D^{1\times p}$ a row vector admitting a right-inverse $S \in D^{p\times 1}$.
- If one entry of R is invertible over D, e.g., $R_1 \in \mathrm{U}(D)$, then

$$(R_1 \; \ldots \; R_p) \overbrace{\begin{pmatrix} R_1^{-1} & 0 \\ 0 & I_{p-1} \end{pmatrix}}^{W} = (1 \quad R_2 \; \ldots \; R_p),$$

and $\det W = R_1^{-1} \in D$. Denoting by $L = (R_2 \; \ldots \; R_p)$, we get:

$$(1 \quad L) \begin{pmatrix} 1 & -L \\ 0 & I_{p-1} \end{pmatrix} = (1 \quad 0 \; \ldots \; 0).$$

Then, the matrix $U = \begin{pmatrix} R_1^{-1} & 0 \\ 0 & I_{p-1} \end{pmatrix} \begin{pmatrix} 1 & -L \\ 0 & I_{p-1} \end{pmatrix} \in \mathrm{GL}_p(D)$ satisfies:

$$R\,U = (1 \quad 0 \; \ldots \; 0).$$

Particular case: 2 entries of R generate D

- Let D be a commutative ring.
- Let $R \in D^{1 \times p}$ a row vector admitting a right-inverse $S \in D^{p \times 1}$.
- We suppose that two entries of R, e.g., R_1 and R_2 generate D: there exist X_1 and $X_2 \in D$ such that $R_1\, X_1 + R_2\, X_2 = 1$.
- The matrix defined by

$$W = \begin{pmatrix} X_1 & -R_2 & 0 \\ X_2 & R_1 & 0 \\ 0 & 0 & I_{p-2} \end{pmatrix}$$

satisfies $\det W = 1$ and $R\, W = (1 \quad 0 \quad R_3 \ \ldots \ R_p)$.

- Denoting by $L = (R_3 \ \ldots \ R_p)$, we finally obtain:

$$(1 \quad 0 \quad L) \begin{pmatrix} 1 & 0 & -L \\ 0 & 1 & 0 \\ 0 & 0 & I_{p-2} \end{pmatrix} = (1 \quad 0 \ \ldots \ 0).$$

H. A. Park's example

- Let us consider $D = \mathbb{Q}[x, y]$ and $R = (1 - x\,y \quad x^2 \quad y^2)$.
- R admits the right-inverse $S = (x\,y + 1 \quad y^2 \quad 0)$ over D.
- In particular, the first two entries $R_1 = 1 - x\,y$ and $R_2 = x^2$ of R generate D: $R_1\,X_1 + R_2\,X_2 = 1$, where $X_1 = x\,y + 1$ and $X_2 = y^2$.
- Then, the unimodular matrices defined by

$$W = \begin{pmatrix} x\,y + 1 & -x^2 & 0 \\ y^2 & 1 - x\,y & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 & -y^2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

satisfy $\det W = 1$, $R\,W = (1 \quad 0 \quad y^2)$ and $R\,(W\,Z) = (1 \quad 0 \quad 0)$.

$$W\,Z = \begin{pmatrix} x\,y + 1 & -x^2 & -(x\,y + 1)\,y^2 \\ y^2 & 1 - x\,y & -y^4 \\ 0 & 0 & 1 \end{pmatrix} \in \mathrm{GL}_3(D).$$

Particular case: one entry of R is 0

- Let D be a commutative ring.
- Let $R \in D^{1 \times p}$ a row vector admitting a right-inverse $S \in D^{p \times 1}$.
- We suppose that one entry of R (e.g., R_1) is 0, $\sum_{i=2}^{p} S_i \, R_i = 1$.
- The matrix defined by

$$W = \begin{pmatrix} 1 & & & \\ (1 - R_1) \, S_2 & 1 & & \\ \vdots & & \ddots & \\ (1 - R_1) \, S_p & & & 1 \end{pmatrix}$$

satisfies $\det W = 1$ and:

$$R \, W = (R_1 + (1 - R_1) \sum_{i=2}^{p} S_i \, R_i = 1 \quad R_2 \ \ldots \ R_p).$$

The row vector $R \, W = (1 \quad R_2 \ \ldots \ R_p)$ can then be reduced to $(1 \quad 0 \ \ldots \ 0)$ by means of elementary operations.

Particular case: first condition on the right-inverse

- Let D be a commutative ring.
- Let $R \in D^{1 \times p}$ a row vector admitting a right-inverse $S \in D^{p \times 1}$.
- Let us suppose that one entry of S, e.g., S_1 is invertible.
- The matrix defined by

$$W = \begin{pmatrix} S_1 & & & \\ S_2 & 1 & & \\ \vdots & & \ddots & \\ S_p & & & 1 \end{pmatrix}$$

satisfies $\det W = S_1 \in \mathrm{U}(D)$ and $R\,W = (1 \quad R_2 \; \ldots \; R_p)$.

The row vector $R\,W = (1 \quad R_2 \; \ldots \; R_p)$ can then be reduced to $(1 \quad 0 \; \ldots \; 0)$ by means of elementary operations.

Particular case: second condition on the right-inverse

- Let D be a commutative ring.
- Let $R \in D^{1\times p}$ a row vector admitting a right-inverse $S \in D^{p\times 1}$.
- Let us suppose that two entries of S, e.g., S_1 and S_2 generate D: there exist X_1 and $X_2 \in D$ such that $X_1\,S_1 + X_2\,S_2 = 1$.
- The matrix defined by

$$W = \begin{pmatrix} S_1 & -X_2 & & & \\ S_2 & X_1 & & & \\ S_3 & & 1 & & \\ \vdots & & & \ddots & \\ S_p & & & & 1 \end{pmatrix}$$

satisfies $\det W = 1$ and $R\,W = (1 \quad \star \quad R_3 \; \ldots \; R_p)$, which can be reduced to $(1 \quad 0 \; \ldots \; 0)$ by means of elementary operations.

Example: locally free modules

- Let us consider the $D = \mathbb{Q}[x_1, x_2]$-module $M = D^{1\times 3}/(D\,R)$:

$$R = (x_1^2 - x_2^2 - 1 \quad x_1^2 + x_2^2 - 1 \quad x_1 - x_2).$$

- The matrix $S = (-1 \quad 0 \quad x_1 + x_2)$ is a right-inverse of R, a fact proving that M is a projective, i.e., free D-module of rank 2.

- Checking that $\mathrm{ext}^1_D(D/(D^{1\times 3}\,R^T), D) = 0$, we obtain that

$$Q = \left(\begin{array}{ccc} x_1 - x_2 & -x_1 + x_2 & x_1^2 + x_2^2 - 1 \\ -x_1 + x_2 & -x_1 + x_2 & -x_1^2 + x_2^2 \\ 2\,x_2^2 & 2\,x_1^2 - 2 & 0 \end{array}\right)$$

defines a parametrization of M, i.e., $M \cong D^{1\times 3}\,Q \subseteq D^{1\times 3}$.

- The parametrization Q is not injective because $\mathrm{rank}_D(M) = 2$.

Example: locally free modules

- We have the following 3 minimal parametrizations of M:

$$Q_1 = \begin{pmatrix} -x_1 + x_2 & x_1^2 + x_2^2 - 1 \\ -x_1 + x_2 & -x_1^2 + x_2^2 \\ 2\,x_1^2 - 2 & 0 \end{pmatrix}, \quad Q_2 = \begin{pmatrix} x_1 - x_2 & x_1^2 + x_2^2 - 1 \\ -x_1 + x_2 & -x_1^2 + x_2^2 \\ 2\,x_2^2 & 0 \end{pmatrix},$$

$$Q_3 = \begin{pmatrix} x_1 - x_2 & -x_1 + x_2 \\ -x_1 + x_2 & -x_1 + x_2 \\ 2\,x_2^2 & 2\,x_1^2 - 2 \end{pmatrix}.$$

None of them admits a left-inverse over D.

- The annihilators of the torsion D-modules $L_i = D^{1\times 2}/(D^{1\times 3}\,Q_i)$

$$\begin{cases} \mathrm{ann}_D(L_1) = (x_1^2 - 1), \\ \mathrm{ann}_D(L_2) = (x_2^2), \\ \mathrm{ann}_D(L_3) = (x_1 - x_2). \end{cases}$$

satisfy the Bézout identity $-p_1 + p_2 + (x_1 + x_2)\,p_3 = 1$, where:

$$p_1 = x_1^2 - 1, \quad p_2 = x_2^2, \quad p_3 = x_1 - x_2.$$

Example: locally free modules

• Over the localizations $D_{p_i} = \{a/p_i^r \mid a \in D,\ r \in \mathbb{N}\}$ of D, the minimal parametrizations Q_i's admit the following left-inverses:

$$T_1 = \frac{1}{2\,(x_1^2 - 1)} \left(\begin{array}{ccc} 0 & 0 & 1 \\ 1 & -1 & 0 \end{array}\right), \quad T_2 = \frac{1}{2\,x_2^2} \left(\begin{array}{ccc} 0 & 0 & 1 \\ 1 & 1 & 0 \end{array}\right),$$

$$T_3 = -\frac{1}{2\,(x_1 - x_2)} \left(\begin{array}{ccc} -1 & 1 & 0 \\ 1 & 1 & 0 \end{array}\right),$$

i.e., satisfy $T_i\, Q_i = I_2$, $i = 1, 2, 3$.

• Projective D-modules are locally free.

• Computation of minimal parametrizations gives us local bases.

A constructive proof of the Quillen-Suslin theorem

• We shortly explain the idea of a constructive proof of the Quillen-Suslin theorem (Logar and Sturmfels).

• Normalization step: Let us consider $a \in k[y_1, \ldots, y_n]$ and let us denote by $m = \deg a + 1$, where $\deg a$ is the total degree of a. Using the following reversible transformation

$$\begin{cases} x_n = y_n, \\ x_i = y_i - y_n^{m^{n-i}}, \end{cases} \Leftrightarrow \begin{cases} y_n = x_n, \\ y_i = x_i + x_n^{m^{n-i}}, \quad i = 1, \ldots, n-1, \end{cases}$$

we obtain $a(y_1, \ldots, y_n) = c\, b(x_1, \ldots, x_n)$, where $0 \neq c \in k$ and b is a monic polynomial in x_n, i.e., the leading coefficient of $b \in E[x_n]$ is 1, where $E = k[x_1, \ldots, x_{n-1}]$.

• If k is a infinite field, then we can obtain this result by means of a simpler transformation.

A constructive proof of the Quillen-Suslin theorem

• A ring A is called local if it contains only one maximal ideal $\mathfrak{m}$, namely, a proper ideal $\mathfrak{m}$ of A which is not properly contained in any ideal of A other than A itself.

• Computation of local bases (Horrock's theorem): Let A be a commutative local ring and R a row vector admitting a right-inverse over $A[x]$. If one of the components R_i of R is monic, then there exists $U \in \mathrm{GL}_p(A[x])$, satisfying:

$$R\,U = (1 \quad 0 \; \ldots \; 0).$$

• Constructive proof of Horrock's theorem can easily be obtained and implemented (QuillenSuslin).

A constructive proof of the Quillen-Suslin theorem

- Main algorithm:
  - **Input:** $R \in D^{1 \times p}$ a row vector which admits a right-inverse over D and a monic component in the last variable x_n.
  - **Output:** A finite number of maximal ideals $\{\mathfrak{m}_i\}_{i \in I}$ of the ring $E = k[x_1, \ldots, x_{n-1}]$ and unimodular matrices $\{H_i\}_{i \in I}$ over the ring $E_{\mathfrak{m}_i}[x_n]$, i.e., $H_i \in \mathrm{GL}_p(E_{\mathfrak{m}_i}[x_n])$, satisfying

$$R\, H_i = (1,\ 0,\ \ldots,\ 0),$$

and such that the ideal defined by the denominators of the matrices H_i's, $i \in I$, generates E.

A constructive proof of the Quillen-Suslin theorem

1. Let $\mathfrak{m}_1$ be an arbitrary maximal ideal of the ring E. Using Horrocks' theorem, compute a unimodular matrix H_1 over $E_{\mathfrak{m}_1}[x_n]$ which satisfies that $R\,H_1 = (1 \quad 0 \;\ldots\; 0)$.
2. Let $d_1 \in E$ be the common denominator of all the entries of H_1 and J the ideal of E generated by d_1. Set $i = 1$.
3. While $J \neq E$, do:
   1. For $i \longleftarrow i+1$, compute a maximal ideal $\mathfrak{m}_i$ of E such that:
   $$J \subset \mathfrak{m}_i.$$
   2. Using Horrocks' theorem, compute a matrix H_i over the ring $E_{\mathfrak{m}_i}[x_n]$ such that det H_i is invertible in $E_{\mathfrak{m}_i}[x_n]$ and:
   $$R\,H_i = (1 \quad 0 \;\ldots\; 0).$$
   3. Let d_i be the denominator of the matrix H_i and consider the ideal $J = (d_1, \ldots, d_i)$.
4. Return $\{\mathfrak{m}_i\}_{i \in I}$, $\{H_i\}_{i \in I}$ and $\{d_i\}_{i \in I}$.

A constructive proof of the Quillen-Suslin theorem

- Patching the local bases: Let $R \in D^{1 \times p}$ be a vector admitting a right-inverse over $D = k[x_1, \ldots, x_n]$ and $U \in \mathrm{GL}_p(E_{\mathfrak{m}}[x_n])$, where $\mathfrak{m}$ is a maximal ideal of $E = k[x_1, \ldots, x_{n-1}]$, which satisfies:

$$R\,U = (1 \quad 0 \ \ldots \ 0).$$

Let $d \in E \setminus \mathfrak{m}$ be a common denominator of the entries of U.

Then, the matrix defined by

$$\Delta(\bullet, x_n, z) = U(\bullet, x_n)\, U^{-1}(\bullet, x_n + z) \in \mathrm{GL}_p(E_{\mathfrak{m}}[x_n, z])$$

is such that

$$\forall\, z \in D, \quad R(\bullet, x_n)\, \Delta(\bullet, x_n, z) = R(\bullet, x_n + z),$$

d^p is a common denominator of the entries of $\Delta(\bullet, x_n, z)$ and:

$$\Delta(\bullet, x_n, d^p\, z) \in \mathrm{GL}_p(E[x_n, z]).$$

A constructive proof of the Quillen-Suslin theorem

- Let $\{\mathfrak{m}_i\}_{i\in I}$, $\{H_i\}_{i\in I}$ and $\{d_i\}_{i\in I}$ be the output of the main algorithm, where $I = \{1, \ldots, m\}$. Let us define the matrices:

$$\Delta_i(\bullet, x_n, z) = H_i(\bullet, x_n)\, H_i^{-1}(\bullet, x_n + z), \quad i = 1, \ldots, m.$$

Let $a_n \in k$. We have $(d_1, \ldots, d_m) = E = k[x_1, \ldots, x_{n-1}]$

$$\Rightarrow\ \exists\, c_i \in E,\ i = 1, \ldots, m, \quad \sum_{i=1}^{m} c_i\, d_i^p = 1.$$

$$R(\bullet, x_n)\, \Delta_1(\bullet, x_n, (a_n - x_n)\, c_1\, d_1^p) = R(\bullet, x_n + (a_n - x_n)\, c_1\, d_1^p),$$

$$R(\bullet, x_n + (a_n - x_n)\, c_1\, d_1^p)\, \Delta_2(\bullet, x_n + (a_n - x_n)\, c_1\, d_1^p, (a_n - x_n)\, c_2\, d_2^p)$$

$$= R\left(\bullet, x_n + (a_n - x_n)\left(\textstyle\sum_{i=1}^{2} c_i\, d_i^p\right)\right),$$

$$\ldots$$

$$R\left(\bullet, x_n + (a_n - x_n)\left(\textstyle\sum_{i=1}^{m-1} c_i\, d_i^p\right)\right)$$

$$\Delta_l\left(\bullet, x_n + (a_n - x_n)\left(\textstyle\sum_{i=1}^{m-1} c_i\, d_i^p\right), (a_n - x_n)\, c_l\, d_l^p\right) = R(\bullet, a_n).$$

A constructive proof of the Quillen-Suslin theorem

- We finally obtain that the matrix

$$U(\bullet, x_n) = \Delta_1(\bullet, x_n, (a_n - x_n)\, c_1\, d_1^p)\, \Delta_2(\bullet, x_n + (a_n - x_n)\, c_1\, d_1^p, (a_n - x_n)\, c_2\, d_2^p) \\ \ldots \Delta_l\left(\bullet, x_n + (a_n - x_n)\left(\sum_{i=1}^{l-1} c_i\, d_i^p\right), (a_n - x_n)\, c_l\, d_l^p\right) \in \mathrm{GL}_p(D)$$

satisfies $R(\bullet, x_n)\, U(\bullet, x_n) = R(\bullet, a_n)$.

- Theorem: Let $D = k[x_1, \ldots, x_n]$ be a commutative polynomial ring over a field k and $R \in D^{1\times p}$ a row vector admitting a right-inverse over D. Then, for all $a_n \in k$, there exists $U \in \mathrm{GL}_p(D)$ s.t.:

$$R(\bullet, x_n)\; U(\bullet, x_n) = R(\bullet, a_n).$$

- Implementation of the previous theorem was done in the package QuillenSuslin (Fabiańska, Aachen University):

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

Example

- We consider the $D = \mathbb{Q}[x_1, x_2]$-module $M = D^{1\times 3}/(D\,R)$, where:

$$R = (x_1\,x_2^2 + 1 \quad 3\,x_2/2 + x_1 - 1 \quad 2\,x_1\,x_2).$$

- Normalized entry $3\,x_2/2 + x_1 - 1$ over $D = E[x_2]$ ($E = \mathbb{Q}[x_1]$).
- We consider the maximal ideal $\mathfrak{m}_1 = (x_1)$ of E. Using an effective version of Horrocks' theorem, we get that the matrix

$$H_1 = \frac{1}{d_1}\begin{pmatrix} 4 & -2\,(3\,x_1 + 2\,x_2 - 2) & 4\,x_1\,(3\,x_1 - 2) \\ 2\,x_1\,(3\,x_1 - 2\,x_2 - 2) & 4\,(x_1\,x_2^2 + 1) & -4\,x_1\,(3\,x_1^2\,x_2 - 2\,x_1\,x_2 + 2) \\ 0 & 0 & 9\,x_1^3 - 12\,x_1^2 + 4\,x_1 + 4 \end{pmatrix},$$

where $d_1 = 9\,x_1^3 - 12\,x_1^2 + 4\,x_1 + 4 \notin \mathfrak{m}_1$, is such that:

$$\begin{cases} \det H_1 = 4/d_1 \;\Rightarrow\; H_1 \in \mathrm{GL}_3(E_{\mathfrak{m}_1}[x_2]), \\ R\,H_1 = (1 \quad 0 \quad 0). \end{cases}$$

Example

- We have $J = (d_1) \subsetneq E$. Then, we consider another maximal ideal $\mathfrak{m}_2$ such that $J \subseteq \mathfrak{m}_2$, e.g., $\mathfrak{m}_2 = (9\,x_1^3 - 12\,x_1^2 + 4\,x_1 + 4)$.
- Using an effective version of Horrocks' theorem, we obtain that

$$H_2 = \frac{1}{d_2} \begin{pmatrix} 0 & 0 & 4\,x_1\,(3\,x_1 - 2) \\ 8\,x_1 & -8\,x_1\,x_2 & -4\,x_1\,(3\,x_1^2\,x_2 - 2\,x_1\,x_2 + 2) \\ -4 & 2\,(3\,x_1 + 2\,x_2 - 2) & 9\,x_1^3 - 12\,x_1^2 + 4\,x_1 + 4 \end{pmatrix},$$

where $d_2 = 4\,x_1\,(3\,x_1 - 2) \notin \mathfrak{m}_2$, is such that:

$$\begin{cases} \det H_2 = -1/(x_1\,(3\,x_1 - 2)) \;\Rightarrow\; H_2 \in \mathrm{GL}_3(E_{\mathfrak{m}_2}[x_2]), \\ R\,H_2 = (1 \quad 0 \quad 0). \end{cases}$$

- We have the Bézout identity

$$c_1\,d_1 + c_2\,d_2 = 1, \quad c_1 = 1/4, \quad c_2 = -(3\,x_1 - 2)/16,$$

i.e., $(d_1, d_2) = E$ and the main algorithm stops.

Example

- The matrix defined by

$$\Delta_1(x_1, x_2, -c_1\, d_1\, x_2) = H_1(x_1, x_2)\, H_1^{-1}(x_1, x_2 - c_1\, d_1\, x_2),$$

$$\left(\begin{array}{ccc} (9\,x_1^4/4 - 3\,x_1^3 + x_1^2)\,x_2^2 + (3\,x_1^2/2 - x_1)\,x_2 + 1 & -x_2 & -2\,x_1\,x_2 \\ -(18\,x_1^4 - 24\,x_1^3 + 8\,x_1^2)\,x_1\,x_2^3/8 + (27\,x_1^5 - 54\,x_1^4 + 36\,x_1^3 - 20\,x_1^2 + 8\,x_1)\,x_1\,x_2^2/8 - x_1\,x_2 & x_1\,x_2^2 + (-3\,x_1^2/2 + x_1)\,x_2 + 1 & 2\,x_1^2\,x_2^2 - x_1^2\,(3\,x_1 - 2)\,x_2 \\ 0 & 0 & 1 \end{array}\right),$$

satisfies:

$$\left\{\begin{array}{l} \Delta_1(x_1, x_2, -c_1\, d_1\, x_2) \in \mathrm{GL}_3(D), \\ R(x_1, x_2)\, \Delta_1(x_1, x_2, -c_1\, d_1\, x_2) = R(x_1, x_2 - c_1\, d_1\, x_2). \end{array}\right.$$

Example

- The matrix defined by

$$\Delta_2(x_1, x_2 - c_1\, d_1\, x_2, -c_2\, d_2\, x_2) = H_2(x_1, x_2 - c_1\, d_1\, x_2)\, H_2(x_2, 0)^{-1},$$

$$\left(\begin{array}{ccc} 1 & 0 & 0 \\ 0 & (3\, x_1^2/2 - x_1)\, x_2 + 1 & x_1^2\, (3\, x_1 - 2)\, x_2 \\ (9\, x_1^2 - 12\, x_1 + 4)\, x_1\, x_2/8 & (-3\, x_1 + 2)\, x_2/4 & (-3\, x_1^2/2 + x_1)\, x_2 + 1 \end{array}\right),$$

satisfies:

$$\left\{\begin{array}{l} \Delta_2(x_1, x_2 - c_1\, d_1\, x_2, -c_2\, d_2\, x_2) \in \mathrm{GL}_3(D), \\ R(x_1, x_2 - c_1\, d_1\, x_2)\, \Delta_2(x_1, x_2 - c_1\, d_1\, x_2, -c_2\, d_2\, x_2) = R(x_1, 0). \end{array}\right.$$

$$U_1 = \Delta_1(x_1, x_2, -c_1\, d_1\, x_2)\, \Delta_2(x_1, x_2 - c_1\, d_1\, x_2, -c_2\, d_2\, x_2) \in \mathrm{GL}_3(D),$$

$$R(x_1, x_2)\, U_1 = R(x_1, 0) = (1 \quad 3\, x_1/2 - 1 \quad 0).$$

Example

- We easily check that the matrix

$$U_2 = \begin{pmatrix} 1 & -3\,x_1/2+1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \in \mathrm{GL}_3(D)$$

satisfies $R(x_1, 0)\, U_2 = (1 \quad 0 \quad 0)$.

- Finally, if we define the matrix $U = U_1\, U_2 \in \mathrm{GL}_3(D)$, namely,

$$U = \begin{pmatrix} (3\,x_1^2/2 - x_1)\,x_2 + 1 & (-9\,x_1^3/4 + 3\,x_1^2 - x_1 - 1)\,x_2 - 3\,x_1/2 + 1 & -2\,x_1\,x_2 \\ (-3\,x_1^3/2 + x_1^2)\,x_2^2 - x_1\,x_2 & (9\,x_1^4/4 - 3\,x_1^3 + x_1^2 + x_1)\,x_2^2 + (3\,x_1^2/2 - x_1)\,x_2 + 1 & 2\,x_1^2\,x_2^2 \\ (9\,x_1^2 - 12\,x_1 + 4)\,x_1\,x_2/8 & (-27\,x_1^4/16 + 27\,x_1^3/8 - 9\,x_1^2/4 - x_1/4 + 1/2)\,x_2 & (-3\,x_1^2/2 + x_1)\,x_2 + 1 \end{pmatrix},$$

we obtain $R\,U = (1 \quad 0 \quad 0)$!

Application: flat linear OD time-delay control system

- Let us consider the following OD time-delay linear system:

$$\begin{cases} \dot{y}_1(t) - y_1(t-h) + 2\,y_1(t) + 2\,y_2(t) - 2\,u(t-h) = 0, \\ \dot{y}_1(t) + \dot{y}_2(t) - \dot{u}(t-h) - u(t) = 0. \end{cases} \qquad (\star)$$

- We consider $D = \mathbb{Q}(a)\left[\partial; \mathrm{id}, \frac{d}{dt}\right][\delta; \sigma, 0]$ and the two matrices:

$$R = \begin{pmatrix} \partial - \delta + 2 & 2 & -2\,\delta \\ \partial & \partial & -\partial\,\delta - 1 \end{pmatrix}, \quad S = \begin{pmatrix} 0 & 0 \\ \frac{1}{2}\,(\partial\,\delta + 1) & -\delta \\ \frac{1}{2}\,\partial & -1 \end{pmatrix}.$$

- We can easily check that $R\,S = I_2$, which proves that the D-module $M = D^{1\times 3}/(D^{1\times 2}\,R)$ is free (Quillen-Suslin theorem), and thus, $(\star)$ admits an injective parametrisation.

Application: flat linear OD time-delay control system

- We have the following system equivalence

$$\left\{\begin{array}{l} \dot{y}_1(t) - y_1(t-h) + 2\,y_1(t) + 2\,y_2(t) - 2\,u(t-h) = 0,\\ \dot{y}_1(t) + \dot{y}_2(t) - \dot{u}(t-h) - u(t) = 0. \end{array}\right.$$

$$\Leftrightarrow \left\{\begin{array}{l} \dot{z}_1(t) + 2\,z_1(t) + 2\,z_2(t) = 0,\\ \dot{z}_1(t) + \dot{z}_2(t) - v(t) = 0, \end{array}\right.$$

defined by the following reversible transformations:

$$\left\{\begin{array}{ll} y_1(t) = & z_1(t),\\ y_2(t) = & \frac{1}{2}\left(\dot{z}_1(t-2\,h) + z_1(t-h)\right) + z_2(t) + v(t-h),\\ u(t) = & \frac{1}{2}\,\dot{z}_1(t-h) + v(t). \end{array}\right.$$

$$\Leftrightarrow \left\{\begin{array}{l} z_1(t) = y_1(t),\\ z_2(t) = -\frac{1}{2}\,y_1(t-h) + y_2(t) - u(t-h),\\ v(t) = -\frac{1}{2}\,\dot{y}_1(t-h) + u(t), \end{array}\right.$$

Application: flat linear OD time-delay control system

- Moreover, we have the following system equivalence

$$\left\{\begin{array}{l} \dot{z}_1(t) + 2\, z_1(t) + 2\, z_2(t) = 0, \\ \dot{z}_1(t) + \dot{z}_2(t) - v(t) = 0, \end{array}\right. \quad \Leftrightarrow \quad \left\{\begin{array}{l} 2\, x_1(t) + 2\, x_2(t) = 0, \\ -w(t) = 0, \end{array}\right.$$

defined by the following reversible transformations:

$$\left\{\begin{array}{l} z_1(t) = x_1(t), \\ z_2(t) = x_2(t) - \frac{1}{2}\, \dot{x}_1(t), \\ v(t) = w(t) - \frac{1}{2}\, \ddot{x}_1(t) + \dot{x}_1(t) + \dot{x}_2(t), \end{array}\right. \quad \Leftrightarrow \quad \left\{\begin{array}{l} x_1(t) = z_1(t), \\ x_2(t) = z_2(t) + \frac{1}{2}\, \dot{z}_1(t), \\ w(t) = v(t) + \dot{z}_1(t) + \dot{z}_2(t). \end{array}\right.$$

- We finally obtain the following injective parametrisation:

$$\left\{\begin{array}{l} y_1(t) = x_1(t), \\ y_2(t) = \frac{1}{2}\, (-\ddot{x}_1(t-h) + \dot{x}_1(t-2\,h) - \dot{x}_1(t) + x_1(t-h) - 2\, x_1(t)), \\ u(t) = \frac{1}{2}\, (\dot{x}_1(t-h) - \ddot{x}_1(t)). \end{array}\right.$$

Application: δ-flat linear OD time-delay systems

- Flexible rod with a mass:

$$\left\{ \begin{array}{l} \sigma^2 \dfrac{\partial^2 q(\tau,x)}{\partial \tau^2} - \dfrac{\partial^2 q(\tau,x)}{\partial x^2} = 0, \\ \dfrac{\partial q}{\partial x}(\tau,0) = -u(\tau), \\ \dfrac{\partial q}{\partial x}(\tau,L) = -J\,\dfrac{\partial^2 q}{\partial \tau^2}(\tau,L), \\ y(\tau) = q(\tau,L). \end{array} \right. \qquad (\star)$$

- $q(\tau,x) = \phi(\tau + \sigma\,x) + \psi(\tau - \sigma\,x)$, $t = (\sigma/J)\,\tau$, $v = (2\,J/\sigma^2)\,u$,

$$(\star) \;\Rightarrow\; \ddot{y}(t+1) + \ddot{y}(t-1) + \dot{y}(t+1) - \dot{y}(t-1) = v(t)$$

$$\Leftrightarrow \left\{ \begin{array}{l} y(t) = \xi(t-1), \\ v(t) = \ddot{\xi}(t) + \ddot{\xi}(t-2) + \dot{\xi}(t) - \dot{\xi}(t-2). \end{array} \right.$$

- If y_r is a desired trajectoire, then $\xi_r(t) = y_r(t+1)$ and:

$$v_r(t) = \ddot{y}_r(t+1) + \ddot{y}_r(t-1) + \dot{y}_r(t+1) - \dot{y}_r(t-1).$$

Application: π-flat linear OD time-delay systems

- Wind tunnel model (Manitius, IEEE TAC 84):

$$\left\{\begin{array}{l} \dot{x}_1(t) + a\,x_1(t) - k\,a\,x_2(t-h) = 0, \\ \dot{x}_2(t) - x_3(t) = 0, \\ \dot{x}_3(t) + \omega^2\,x_2(t) + 2\,\zeta\,\omega\,x_3(t) - \omega^2\,u(t) = 0, \end{array}\right.$$

$$\Leftrightarrow \left\{\begin{array}{l} x_1(t) = \omega^2\,a\,k\,\xi(t-h), \\ x_2(t) = \omega^2\,\dot{\xi}(t) + \omega^2\,a\,\xi(t), \qquad \xi(t) = x_1(t+h)/(\omega^2\,a), \\ x_3(t) = \omega^2\,\ddot{\xi}(t) + \omega^2\,a\,\dot{\xi}(t), \\ u(t) = \xi^{(3)}(t) + (2\,\zeta\,\omega + a)\,\ddot{\xi}(t) + (\omega^2 + 2\,a\,\zeta\,\omega)\,\dot{\xi}(t) + a\,\omega^2\,\xi(t). \end{array}\right.$$

- Simple network model (Fliess-Mounier, IFAC TDS98):

$$\left\{\begin{array}{l} \dot{x}_1(t) + u_1(t) - u_2(t-h_1) = 0, \\ \dot{x}_2(t) - u_1(t-h_2) = 0, \end{array}\right. \quad \Leftrightarrow \quad \left\{\begin{array}{l} x_1(t) = \xi_1(t-h_1) - \xi_2(t), \\ x_2(t) = \xi_2(t-h_2), \\ u_1(t) = \dot{\xi}_2(t), \\ u_2(t) = \dot{\xi}_1(t). \end{array}\right.$$

$$\xi_1(t) = x_1(t+h_1) + x_2(t+h_1+h_2), \; \xi_2(t) = x_2(t+h_2).$$

Conclusion

- We have studied stably free and free modules.
- We have briefly explained the Quillen-Suslin theorem.

1. Constructive computation of bases of free D-modules can be obtained by means of the package QuillenSuslin:

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

2. More applications in mathematical systems theory: constructive solutions of the Lin-Bose's conjectures, effective computation of (weakly) coprime factorizations of rational transfer matrices, reduction and decomposition problems...

   A. Fabiańska, A. Quadrat, "Applications of the Quillen-Suslin theorem to multidimensional systems theory", in *Gröbner Bases in Control Theory and Signal Processing*, H. Park and G. Regensburger, Radon Series on Computation and Applied Mathematics 3, de Gruyter publisher, 2007, 23-106.