

An Introduction to Computer Algebra System SINGULAR. Part III, Modules and Beyond

Viktor Levandovskyy

4th SCIENCE Training School in Symbolic Computation

10.07.2009, RISC, Hagenberg

Modules in a Constructive Way

Let A be a polynomial ring. Consider the submodules of A^n . We use $\{e_1, \dots, e_n\}$, $e_i = (0, \dots, 1, \dots, 0)$ as canonical basis of A^n as of A -module of rank n . Then a vector $v \in A^n$ is uniquely defined

$$A^n \ni v = \sum_{i=1}^n v_i e_i = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}, \quad v_i \in A.$$

A submodule $S \subset A^n$ is generated by a set of vectors and hence, can be alternatively given by the columns of $m \times n$ matrix.

There is a type casting between the data types `module` and `matrix`.

Lemma

Let M be an A -module. M is finitely generated if and only if $M \cong A^n/L$ for a suitable $n \in \mathbb{N}$ and a suitable submodule $L \subset A^n$.

Modules in a Constructive Way: Finite Presentation

Definition

Let M be an A -module. M is called of *finite presentation* if there exists an $n \times m$ -matrix φ such that M is isomorphic to the cokernel of the map $A^m \xrightarrow{\varphi} A^n$. φ is called a *presentation matrix* of M . We write $A^m \xrightarrow{\varphi} A^n \rightarrow M \rightarrow 0$ to denote a presentation of M .

Operations with finitely presented modules can be constructively done with presentation matrices.

Module Orderings

- Position-over-Term (c, dp) resp. Term-over-Position (dp, C)
- descending ("C") resp. ascending ("c") order of components

The Trinity of Gröbner basis

a.k.a. Gröbner engine: `std`, `syz`, `lift`.

Suppose we are given $I = \{\bar{f}_1, \dots, \bar{f}_k\} \subset A^r$ and let F be a matrix with \bar{f}_i as columns.

$$\begin{pmatrix} \bar{f}_1 & \dots & \bar{f}_k \\ 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix} \xrightarrow{GB} \left(\begin{array}{ccc|ccc} \bar{0} & \dots & \bar{0} & \bar{h}_1 & \dots & \bar{h}_t \\ \hline & \mathbf{S} & & & \mathbf{T} & \end{array} \right).$$

Let H be a matrix with columns \bar{h}_i . Then

- $\{\bar{h}_1, \dots, \bar{h}_t\}$ is a Gröbner basis of I
- columns of \mathbf{S} generate $\text{syz}(\{\bar{f}_1, \dots, \bar{f}_k\})$
- \mathbf{T} is a left transition matrix between two bases of F , i.e. $H = F \cdot \mathbf{T}$

Applications: Solving inhomogeneous problem

Task

Let $R = K[x_1, \dots, x_n]$.

- (a) Describe a method for obtaining all the solutions $\xi \in R^m$ of the system $A\xi = f$, where $A \in R^{1 \times m}$ and $f \in R$ are given.

Hint: consider first a homogeneous system $A\xi = 0$.

- (b) Apply your method on the following equation:

$$[x^2 - yz - 1, y^2 - xz - 1, z^2 - xy - 1]\xi = x^2 + y^2 + z^2 - 2.$$

Applications: Solving inhomogeneous problem

A solution exists if and only if $f \in_R \langle A_1, \dots, A_m \rangle$. Constructively speaking $\text{NormalForm}(f, \text{GroebnerBasis}(A_1, \dots, A_m)) = 0$ must hold true. If $\xi, \eta \in R^m$ are two different solutions, that is $A\xi = f$ and $A\eta = f$, then $A(\xi - \eta) = 0 \Leftrightarrow \xi - \eta \in \text{syz}(A)$.

So it suffices to find

- 1 one solution ξ_0 of the inhomogeneous equation $A\xi_0 = f$ (since $f \in_R \langle A_1, \dots, A_m \rangle$, there exists an admissible presentation w.r.t. a Gröbner basis of $\{A_i\}$, hence there exists a presentation w.r.t $\{A_i\}$) and
- 2 the generating system of the syzygy module of A , $\text{syz}(A) = \{\eta \in R^m \mid A\eta = 0\} \subset R^m$.

Then all the solutions are $\xi_0 + \text{syz}(A)$.

Concrete solution

Consider the \mathbb{D}_P (deglex) ordering. Then $A_1 = x^2 - yz - 1$, $A_2 = y^2 - xz - 1$, $A_3 = -xy + z^2 - 1$ and the Gröbner basis of A is $\{g_1 = x + y + z, g_2 = y^2 + yz + z^2 - 1\}$. Since $f = (x - y - z) \cdot (x + y + z) + 2 \cdot (y^2 + yz + z^2 - 1)$ is an admissible presentation, $f \in A$ and hence there exist solutions.

Since $x + y + z = -z \cdot A_1 - x \cdot A_2 - y \cdot A_3$ and $y^2 + yz + z^2 - 1 = -z^2 \cdot A_1 + (-xz + 1) \cdot A_2 - yz \cdot A_3$, it follows that $f = (-xz + yz - z^2) \cdot A_1 + (-xz - x^2 + xy + 2) \cdot A_2 + (-xy + y^2 - yz) \cdot A_3$

Hence $\xi_0 = [-xz + yz - z^2, -xz - x^2 + xy + 2, -xy + y^2 - yz]^T$.

Concrete solution: syzygy module

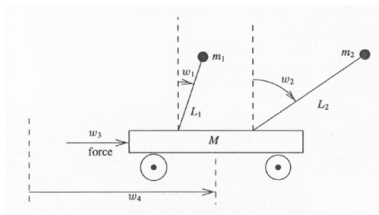
$$S = \left\langle \begin{bmatrix} y - z \\ -x + z \\ x - y \end{bmatrix}, \begin{bmatrix} -xz + z^2 - 1 \\ -x^2 + xz \\ -xy + yz + 1 \end{bmatrix}, \begin{bmatrix} -y^2 + xz + 1 \\ x^2 - yz - 1 \\ 0 \end{bmatrix} \right\rangle$$

Now we can reduce ξ_0 modulo syzygies and obtain

$$\xi'_0 = [-z^2 + 1, -xz + 1, -yz]^T = \xi_0 + yS_1 + S_3.$$

Concrete: Two pendula, mounted on a cart

Polderman, Willems "Introduction to Mathematical Systems Theory".



Denote $\partial := \frac{d}{dt}$. A linearized system becomes $\mathbf{S} \cdot \bar{\mathbf{w}} = \mathbf{0}$, where \mathbf{S} is

$$\begin{pmatrix} m_1 L_1 \partial^2 & m_2 L_2 \partial^2 & -1 & (m_1 + m_2 + M) \partial^2 \\ m_1 L_1^2 \partial^2 - m_1 g L_1 & 0 & 0 & m_1 L_1 \partial^2 \\ 0 & m_2 L_2^2 \partial^2 - m_2 g L_2 & 0 & m_2 L_2 \partial^2 \end{pmatrix}$$

Two pendula: Computations

The underlying ring $R = \mathbb{K}(m_1, m_2, m, g, L_1, L_2)[\frac{d}{dt}]$ is commutative. Define the submodule $T \subset R^3$, generated by the columns of S and the module $U = R^3/T$.

```
LIB "poly.lib";
ring R = (0,m1,m2,M,g,L1,L2), Dt, dp;
module T =
    [m1*L1*Dt^2, m2*L2*Dt^2, -1, (M+m1+m2)*Dt^2],
    [m1*L1^2*Dt^2-m1*L1*g, 0, 0, m1*L1*Dt^2],
    [0, m2*L2^2*Dt^2-m2*L2*g, 0, m2*L2*Dt^2];
T = transpose(T);
option(redSB); option(redTail);
module W = groebner(T);
module L = lift(T,W);
number n2 = content(L[2]);
number n3 = content(L[3]);
```

Two pendula: Conclusion

Since the ring $R = \mathbb{K}(m_1, m_2, m, g, L_1, L_2)[\frac{d}{dt}]$ is commutative principal ideal domain, torsion-free modules are free modules. Hence, a system S is **controllable** if and only if the Gröbner basis of the adjoint system module (presented as S^T) is the identity matrix.

This is true **generically**, namely for all values of parameters but a set of measure (or probability) 0. We have computed the set of obstructions, it is $\{L_1 - L_2\}$.

Non-generic Autonomy

If $L_1 = L_2 = L$, the system is not controllable but it has torsion submodule, which gives rise to **autonomous** elements.

Namely, such elements ω (e.g. $\omega = w_1 - w_2$) satisfy an autonomous ODE $\frac{d(\omega)}{dt^2} = \frac{g}{L} \cdot \omega$, whereas the annihilator of torsion submodule is $\langle L\partial^2 - g \rangle$.

Playground time

Consider the Bipedulum problem with parameters g, ℓ_1, ℓ_2 :

$$\begin{bmatrix} \ell_1 \partial^2 + g & 0 & -g\ell_2 \\ 0 & \ell_2 \partial^2 + g & -g\ell_1 \end{bmatrix}$$

```
ring r = (0,g,l1,l2),Dt,dp;  
module RR = [l1*Dt^2+g,0,-g*l2], [0, l2*Dt^2+g, -g*l1]  
module R = transpose(RR);
```

Task for participants

- recover generic and nongeneric properties of this problem, depending on parameters

Generating Finite Difference Schemes

What can be done symbolically?

Given a linear system of PDE with, say, constant coefficients, we are able to compute systematically different finite difference schemes symbolically.

Moreover, there are symbolic methods for testing the obtained scheme for von Neumann stability and check the dispersion.

For getting a particular scheme we need the equations together with fixed approximation rules for each differential expression in unknown function(s) u (like u_{xx} , u_{tx}), involved in the system of equations.

Difference Approximations

Notation: difference operators $T_x : f(t, x, y, z) \rightarrow f(t, x + \Delta x, y, z)$.

Taylor Expansion

$$u(x \pm \Delta x) = u(x) \pm \Delta x u_x(x) + \frac{\Delta x^2}{2} u_{xx}(x) + \mathcal{O}(\Delta x^3).$$

$$u_x(x) = \frac{u(x + \Delta x) - u(x)}{\Delta x} + \mathcal{O}(\Delta x) \text{ (forward difference)}$$

$$u_x(x) = \frac{u(x) - u(x - \Delta x)}{\Delta x} + \mathcal{O}(\Delta x) \text{ (backward difference)}$$

$$u_x(x) = \frac{u(x + \Delta x) - u(x - \Delta x)}{2\Delta x} + \mathcal{O}(\Delta x^2) \text{ (central 1st order diff.)}$$

$$\frac{u(x + \Delta x) - 2u(x) + u(x - \Delta x))}{\Delta x^2} = u_{xx}(x) + \mathcal{O}(\Delta x^2)$$

Forward difference

$$(T_x - 1) \bullet u = \Delta x \bullet u_x \Leftrightarrow (\Delta x, 1 - T_x) \cdot (u_x, u)^T = 0.$$

Difference Approximations: Rules

Approximation Rules

- **Forward difference** $(\Delta x, 1 - T_x) \cdot (u_x, u)^T = 0$
- **Backward difference** $(\Delta x \cdot T_x, 1 - T_x) \cdot (u_x, u)^T = 0$
- **A 1st order central appr.** $(2\Delta x \cdot T_x, 1 - T_x^2) \cdot (u_x, u)^T = 0$
- **A 2nd order central appr.** $(-\Delta x^2 \cdot T_x, (1 - T_x)^2) \cdot (u_{xx}, u)^T = 0$
- **Trapezoid rule** $(\frac{1}{2}\Delta x \cdot (T_x + 1), 1 - T_x) \cdot (u_x, u)^T = 0$
- **Midpoint rule** $(2\Delta x \cdot T_x, 1 - T_x^2) \cdot (u_x, u)^T = 0$.
- **Pyramid rule** $(\frac{1}{3}\Delta x \cdot (T_x^2 + T_x + 1), T_x(1 - T_x^2)) \cdot (u_x, u)^T = 0$

Computing Finite Difference Schemes I

The equation $u_{tt} - \lambda^2 u_{xx} = 0$

We approximate x via trapezoid rule and t via backward difference. We obtain the matrix formulation

$$\begin{pmatrix} -\lambda^2 & 0 & 1 & 0 & 0 \\ \Delta x/2 \cdot (T_x + 1) & 1 - T_x & 0 & 0 & 0 \\ 0 & \Delta x/2 \cdot (T_x + 1) & 0 & 0 & 1 - T_x \\ 0 & 0 & \Delta t \cdot T_t & 1 - T_t & 0 \\ 0 & 0 & 0 & \Delta t \cdot T_t & 1 - T_t \end{pmatrix} \cdot \begin{pmatrix} u_{xx} \\ u_x \\ u_{tt} \\ u_t \\ u \end{pmatrix}$$

Computational Task

Let M be a submodule of a free module, generated by the rows of the matrix above. We look for a submodule $N \subset M$, involving only u .

Elimination of module components

Suppose there is a monomial well-ordering \prec_A on a ring A .

The ordering \prec_m on a free left module $A^r = \bigoplus_{i=1}^r Ae_i$ is the

position-over-term ordering with $e_1 \succ e_2 \succ \dots$, defined as follows:

$$x^\alpha e_i \prec_m x^\beta e_j \Leftrightarrow j < i \text{ or } j = i \text{ and } x^\alpha \prec_A x^\beta.$$

Lemma

Let $M \subseteq A^r$ be a submodule. Let $G = \{g_1, \dots, g_m\}$ be a Gröbner basis of M with respect to \prec_m as before.

Then $\forall 1 \leq s \leq r \quad G \cap \bigoplus_{i=s}^r Ae_i$ is a Gröbner basis of $M \cap \bigoplus_{i=s}^r Ae_i$.

Computing Finite Difference Schemes II

Continue with the example before. Gröbner basis computation gives us the submodule, generated by the difference polynomial

$$\begin{aligned} & \frac{4\lambda^2 \Delta t^2}{\Delta h^2} (T_x^2 T_t^2 - 2T_x T_t^2 + T_t^2) = \\ &= T_x^2 T_t^2 - 2T_x^2 T_t + 2T_x T_t^2 + T_x^2 - 4T_x T_t + T_t^2 + 2T_x - 2T_t + 1 \end{aligned}$$

Written in the nodes of the mesh, it looks as follows

$$\begin{aligned} & \frac{4\lambda^2 \Delta t^2}{\Delta h^2} \cdot (u_{j+2}^{n+2} - 2u_{j+1}^{n+2} + u_j^{n+2}) = \\ &= (u_{j+2}^{n+2} - 2u_{j+2}^{n+1} + u_{j+2}^n) + 2(u_{j+1}^{n+2} - 2u_{j+1}^{n+1} + u_{j+1}^n) + \\ & \quad + (u_j^{n+2} - 2u_j^{n+1} + u_j^n) \end{aligned}$$

One can easily see that this scheme is consistent. END OF STORY.

Task for participants

- Experiment with other monomial module orderings and see the differences
- What can be changed (ring and ordering), such that you will still get the scheme?

Aftermath or Background: Introduction to Modules

Introduction to Modules

Definition

Let A be a ring. A set M with two operations $+$: $M \times M \rightarrow M$ (*addition*) and \cdot : $A \times M \rightarrow M$ (*scalar multiplication*) is called *A -module* if

① $(M, +)$ is an abelian group.

② $(a + b) \cdot m = a \cdot m + b \cdot m$

$$a \cdot (m + n) = a \cdot m + a \cdot n$$

$$(ab) \cdot m = a \cdot (b \cdot m)$$

$$1 \cdot m = m \quad \text{for all } a, b \in A \text{ and } m, n \in M.$$

Examples of Modules Around Us

- 1 Let A be a ring, then A is an A -module with the ring operation.
- 2 If $A = \mathbb{K}$ is a field, then A -modules are just \mathbb{K} -vector spaces.
- 3 Every abelian group is a \mathbb{Z} -module with scalar multiplication

$$n \cdot x := x + \cdots + x.$$

- 4 Let $I \subset A$ be an ideal, then I and A/I are A -modules with the obvious addition and scalar multiplication.
- 5 Let A be a ring and $A^n = \{(x_1, \dots, x_n) \mid x_i \in A\}$ the n -fold Cartesian product of A , then A^n is an A -module (with the component-wise addition and scalar multiplication).
- 6 Let $\varphi : A \rightarrow B$ be a ring map, and set $a \cdot b := \varphi(a) \cdot b$ for $a \in A$ and $b \in B$. This defines an A -module structure on B . The ring B together with this structure is called an A -algebra.

Homomorphisms of Modules

Definition

- ➊ Let M, N be A -modules. A map $\varphi : M \rightarrow N$ is called *A -module homomorphism* if, for all $a \in A$ and $m, n \in M$,
 - ➊ $\varphi(am) = a\varphi(m)$,
 - ➋ $\varphi(m + n) = \varphi(m) + \varphi(n)$.
- ➌ The set of all A -mod hom's from M to N is $\text{Hom}_A(M, N)$.
- ➍ A bijective A -module homomorphism is called *isomorphism*.
- ➎ Let $\varphi : M \rightarrow N$ be an A -module homomorphism. The *kernel* of φ is defined by $\text{Ker}(\varphi) := \{m \in M \mid \varphi(m) = 0\}$. The *image* of φ is defined by $\text{Im}(\varphi) := \{\varphi(m) \mid m \in M\}$.
- ➏ (Lemma) $\text{Ker}(\varphi)$ and $\text{Im}(\varphi)$ are submodules of M , respectively N .
- ➐ Let M be an A -module and $N \subset M$ be a submodule. We define the *factor module* M/N by $M/N := \{m + N \mid m \in M\}$.
- ➑ Let $\varphi : M \rightarrow N$ be an A -module homomorphism, then $\text{Coker}(\varphi) := N / \text{Im}(\varphi)$ is called the *cokernel* of φ .

Lemma

- ① *With the canonical operations, by choosing representatives,*

$$(m + N) + (n + N) := (m + n) + N, \quad a \cdot (m + N) := am + N$$

the set M/N is an A -module. N , the equivalence class of $0 \in M$ is the 0-element in M/N . The map $\pi : M \rightarrow M/N$, $\pi(m) := m + N$ is a surjective A -module homomorphism.

- ② *Let $\varphi : M \rightarrow N$ be an A -module homomorphism, then*

$$\text{Im}(\varphi) \cong M / \text{Ker}(\varphi).$$

Definition

- ① An A -module M is called *finitely generated* if $M = \sum_{i=1}^n A \cdot m_i$ for suitable $m_1, \dots, m_n \in M$. We then write $M = \langle m_1, \dots, m_n \rangle$, and m_1, \dots, m_n are called *generators* of M .
- ② Let M be an A -module. The *torsion submodule* is defined by

$$\text{Tors}(M) := \{m \in M \mid \exists \text{ a non-zero-divisor } a \in A \text{ with } am = 0\}.$$

A module M is called *torsion free* if $\text{Tors}(M) = 0$.

M itself is called a *torsion module* if $\text{Tors}(M) = M$.

- ③ The *annihilator* of M is $\text{Ann}_A(M) := \{a \in A \mid aM = 0\}$.
- ④ An A -module. M is called *free* if $M \cong \bigoplus_{i \in I} A$. The cardinality of the index set I is called the *rank* of M . A subset $S \subset M$ is called a *basis* of M if every $m \in M$ can be written in a unique way as a finite linear combination $m = a_1 m_1 + \dots + a_n m_n$ with $m_i \in S$ and $a_i \in A$, for some n (depending on m).