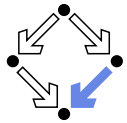
Converting matrices of Ore polynomials from Popov form to Hermite form using the FGLM algorithm

Johannes Middeke



Research Institute for Symbolic Computation (RISC),
Johannes Kepler University,
Linz, Austria

ACA 2010
24th of June, 2010

* *This work was supported by the Austrian Science Foundation (FWF) under the project DIFFOP (P20 336–N18).*

Motivation/Overview

Ore polynomials are a **generalisation of** ordinary polynomials, linear **differential operators** and linear **difference operators**.

Matrices are used to represent linear systems of operators.

Normal forms capture important properties of matrices and the systems they represent.

We will present in this talk:

- Normal forms are connected to Gröbner bases (generalising [Kojima et al., 2007]).
- The FGLM algorithm can be used to convert normal forms into each other.

Motivation/Overview

Ore polynomials are a generalisation of ordinary polynomials, linear differential operators and linear difference operators.

Matrices are used to represent linear systems of operators.

Normal forms capture important properties of matrices and the systems they represent.

We will present in this talk:

- Normal forms are connected to Gröbner bases (generalising [Kojima et al., 2007]).
- The FGLM algorithm can be used to convert normal forms into each other.

Motivation/Overview

Ore polynomials are a generalisation of ordinary polynomials, linear differential operators and linear difference operators.

Matrices are used to represent linear systems of operators.

Normal forms capture important properties of matrices and the systems they represent.

We will present in this talk:

- Normal forms are connected to Gröbner bases (generalising [Kojima et al., 2007]).
- The FGLM algorithm can be used to convert normal forms into each other.

Motivation/Overview

Ore polynomials are a generalisation of ordinary polynomials, linear differential operators and linear difference operators.

Matrices are used to represent linear systems of operators.

Normal forms capture important properties of matrices and the systems they represent.

We will present in this talk:

- Normal forms are connected to **Gröbner bases** (generalising [Kojima et al., 2007]).
- The **FGLM algorithm** can be used to convert normal forms into each other.

Ore polynomials

Let K be a skew field with automorphism $\sigma\colon K \to K$ and (σ-) derivative $\vartheta\colon K \to K$.

Ore polynomials are expressions

$$a_n\partial^n + \ldots + a_1\partial + a_0 \quad \text{with } a_0, \ldots, a_n \in K.$$

We denote the set of all Ore polynomials by $R = K[\partial; \sigma, \vartheta]$.

Addition is as usual and multiplication is given by the commutation rule

$$\partial a = \sigma(a)\partial + \vartheta(a) \quad \text{for all } a \in K.$$

Examples are

- ordinary (commutative) polynomials ($\sigma = \mathrm{id}$ and $\vartheta = 0$),
- differential operators ($\sigma = \mathrm{id}$), and
- difference operators ($\vartheta = 0$).

Ore polynomials

Let K be a skew field with automorphism $\sigma\colon K \to K$ and (σ-) derivative $\vartheta\colon K \to K$.

Ore polynomials are expressions

$$a_n\partial^n + \ldots + a_1\partial + a_0 \quad \text{with } a_0, \ldots, a_n \in K.$$

We denote the set of all Ore polynomials by $R = K[\partial; \sigma, \vartheta]$.

Addition is as usual and multiplication is given by the commutation rule

$$\partial a = \sigma(a)\partial + \vartheta(a) \quad \text{for all } a \in K.$$

Examples are

- ordinary (commutative) polynomials ($\sigma = \mathrm{id}$ and $\vartheta = 0$),
- differential operators ($\sigma = \mathrm{id}$), and
- difference operators ($\vartheta = 0$).

Ore polynomials

Let K be a skew field with automorphism $\sigma\colon K \to K$ and (σ-) derivative $\vartheta\colon K \to K$.

Ore polynomials are expressions

$$a_n\partial^n + \ldots + a_1\partial + a_0 \quad \text{with } a_0, \ldots, a_n \in K.$$

We denote the set of all Ore polynomials by $R = K[\partial; \sigma, \vartheta]$.

Addition is as usual and multiplication is given by the **commutation rule**

$$\partial a = \sigma(a)\partial + \vartheta(a) \quad \text{for all } a \in K.$$

Examples are

- ordinary (commutative) polynomials ($\sigma = \mathrm{id}$ and $\vartheta = 0$),
- differential operators ($\sigma = \mathrm{id}$), and
- difference operators ($\vartheta = 0$).

Ore polynomials

Let K be a skew field with automorphism $\sigma\colon K \to K$ and (σ-) derivative $\vartheta\colon K \to K$.

Ore polynomials are expressions

$$a_n\partial^n + \ldots + a_1\partial + a_0 \quad \text{with } a_0, \ldots, a_n \in K.$$

We denote the set of all Ore polynomials by $R = K[\partial; \sigma, \vartheta]$.

Addition is as usual and multiplication is given by the commutation rule

$$\partial a = \sigma(a)\partial + \vartheta(a) \quad \text{for all } a \in K.$$

Examples are

- ordinary (commutative) polynomials ($\sigma = \mathrm{id}$ and $\vartheta = 0$),
- differential operators ($\sigma = \mathrm{id}$), and
- difference operators ($\vartheta = 0$).

Matrices

We denote the ring of $m \times n$ **matrices** over R by ${}^mR^n$.

An important notion will be the degree of a matrix $M \in {}^mR^n$

$$\deg M = \max\{\deg M_{i,j} \mid 1 \leqslant i \leqslant m \text{ and } 1 \leqslant j \leqslant n\}.$$

Matrices

We denote the ring of $m \times n$ matrices over R by ${}^mR^n$.

An important notion will be the **degree** of a matrix $M \in {}^mR^n$

$$\deg M = \max\{\deg M_{i,j} \mid 1 \leqslant i \leqslant m \text{ and } 1 \leqslant j \leqslant n\}.$$

Hermite normal form

A matrix in **Hermite normal form** is essentially in **upper row echelon form** with some restrictions on the degrees.

For example is the matrix

$$H = \begin{pmatrix} 1 & \partial & x\partial - 1 \\ 0 & \partial^2 - 1 & x + 1 \end{pmatrix} \in {}^2\mathbb{Q}(x)[\partial; \mathrm{id}, d/dx]^3$$

in Hermite normal form.

The left-most non-zero entries of each row are called pivots.

Every matrix can be brought to a unique Hermite normal form by elementary row operations.

Hermite normal form

A matrix in Hermite normal form is essentially in upper row echelon form with some restrictions on the degrees.

For example is the matrix

$$H = \begin{pmatrix} 1 & \partial & x\partial - 1 \\ 0 & \partial^2 - 1 & x + 1 \end{pmatrix} \in {}^2\mathbb{Q}(x)[\partial; \mathrm{id}, d/dx]^3$$

in Hermite normal form.

The left-most non-zero entries of each row are called pivots.

Every matrix can be brought to a unique Hermite normal form by elementary row operations.

Hermite normal form

A matrix in Hermite normal form is essentially in upper row echelon form with some restrictions on the degrees.

For example is the matrix

$$H = \begin{pmatrix} 1 & \partial & x\partial - 1 \\ 0 & \partial^2 - 1 & x + 1 \end{pmatrix} \in {}^2\mathbb{Q}(x)[\partial; \mathrm{id}, d/dx]^3$$

in Hermite normal form.

The **left-most non-zero entries** of each row are called **pivots**.

Every matrix can be brought to a unique Hermite normal form by elementary row operations.

Hermite normal form

A matrix in Hermite normal form is essentially in upper row echelon form with some restrictions on the degrees.

For example is the matrix

$$H = \begin{pmatrix} 1 & \partial & x\partial - 1 \\ 0 & \partial^2 - 1 & x + 1 \end{pmatrix} \in {}^2\mathbb{Q}(x)[\partial; \mathrm{id}, d/dx]^3$$

in Hermite normal form.

The left-most non-zero entries of each row are called pivots.

Every matrix can be brought to a unique Hermite normal form by elementary **row operations**.

Popov normal form

A matrix in **Popov normal form** has its (left-most) **entries of highest degree in different columns**.

For example is the matrix

$$P = \begin{pmatrix} 1 & \partial & x\partial - 1 \\ \frac{1}{x}\partial & \frac{1}{x} & \partial^2 - \frac{x+1}{x} \end{pmatrix} \in {}^2\mathbb{Q}(x)[\partial; \mathrm{id}, d/dx]^3$$

in Popov normal form.

The left-most highest degree entries of each row are called pivots.

Every matrix can be brought to a unique Popov normal form by elementary row operations.

Matrices in Popov normal form are **row-reduced**.

Popov normal form

A matrix in Popov normal form has its (left-most) entries of highest degree in different columns.

For example is the matrix

$$P = \begin{pmatrix} 1 & \partial & x\partial - 1 \\ \frac{1}{x}\partial & \frac{1}{x} & \partial^2 - \frac{x+1}{x} \end{pmatrix} \in {}^2\mathbb{Q}(x)[\partial; \mathrm{id}, d/dx]^3$$

in Popov normal form.

The left-most highest degree entries of each row are called pivots.

Every matrix can be brought to a unique Popov normal form by elementary row operations.

Matrices in Popov normal form are row-reduced.

Popov normal form

A matrix in Popov normal form has its (left-most) entries of highest degree in different columns.

For example is the matrix

$$P = \begin{pmatrix} 1 & \partial & x\partial - 1 \\ \frac{1}{x}\partial & \frac{1}{x} & \partial^2 - \frac{x+1}{x} \end{pmatrix} \in {}^2\mathbb{Q}(x)[\partial; \mathrm{id}, d/dx]^3$$

in Popov normal form.

The **left-most highest degree entries** of each row are called **pivots**.

Every matrix can be brought to a unique Popov normal form by elementary row operations.

Matrices in Popov normal form are **row-reduced**.

Popov normal form

A matrix in Popov normal form has its (left-most) entries of highest degree in different columns.

For example is the matrix

$$P = \begin{pmatrix} 1 & \partial & x\partial - 1 \\ \frac{1}{x}\partial & \frac{1}{x} & \partial^2 - \frac{x+1}{x} \end{pmatrix} \in {}^2\mathbb{Q}(x)[\partial; \mathrm{id}, d/dx]^3$$

in Popov normal form.

The left-most highest degree entries of each row are called pivots.

Every matrix can be brought to a unique Popov normal form by elementary **row operations**.

Matrices in Popov normal form are **row-reduced**.

Popov normal form

A matrix in Popov normal form has its (left-most) entries of highest degree in different columns.

For example is the matrix

$$P = \begin{pmatrix} 1 & \partial & x\partial - 1 \\ \frac{1}{x}\partial & \frac{1}{x} & \partial^2 - \frac{x+1}{x} \end{pmatrix} \in {}^2\mathbb{Q}(x)[\partial; \mathrm{id}, d/dx]^3$$

in Popov normal form.

The left-most highest degree entries of each row are called pivots.

Every matrix can be brought to a unique Popov normal form by elementary row operations.

Matrices in Popov normal form are **row-reduced**.

Gröbner bases of modules

There is a theory of (left) **Gröbner bases for Ore polynomials** that looks **"almost identical" to** that of **ordinary polynomials**.

Also the extension to modules is as in the commutative case.

In particular, are Monomials of the form

$$\partial^i \mathfrak{e}_j, \qquad \text{where } 0 \leqslant i \text{ and } 1 \leqslant j \leqslant n$$

and where $\mathfrak{e}_j$ is the j^{th} canonical basis vector.

With this notion of monomial, reduction, Gröbner bases, etc. are defined as in the usual case.

Gröbner bases of modules

There is a theory of (left) Gröbner bases for Ore polynomials that looks "almost identical" to that of ordinary polynomials.

Also the **extension to modules** is **as in the commutative case**.

In particular, are Monomials of the form

$$\partial^i \mathfrak{e}_j, \qquad \text{where } 0 \leqslant i \text{ and } 1 \leqslant j \leqslant n$$

and where $\mathfrak{e}_j$ is the j^{th} canonical basis vector.

With this notion of monomial, reduction, Gröbner bases, etc. are defined as in the usual case.

Gröbner bases of modules

There is a theory of (left) Gröbner bases for Ore polynomials that looks "almost identical" to that of ordinary polynomials.

Also the extension to modules is as in the commutative case.

In particular, are **Monomials** of the form

$$\partial^i \mathfrak{e}_j, \qquad \text{where } 0 \leqslant i \text{ and } 1 \leqslant j \leqslant n$$

and where $\mathfrak{e}_j$ is the j^{th} **canonical basis vector**.

With this notion of monomial, reduction, Gröbner bases, etc. are defined as in the usual case.

Gröbner bases of modules

There is a theory of (left) Gröbner bases for Ore polynomials that looks "almost identical" to that of ordinary polynomials.

Also the extension to modules is as in the commutative case.

In particular, are Monomials of the form

$$\partial^i \mathfrak{e}_j, \qquad \text{where } 0 \leqslant i \text{ and } 1 \leqslant j \leqslant n$$

and where $\mathfrak{e}_j$ is the j^{th} canonical basis vector.

With this notion of monomial, reduction, Gröbner bases, etc. are defined as in the usual case.

Monomial orderings

There are two important **admissible monomial orderings**:

Definition (position over term ordering)

$$\partial^i \mathfrak{e}_j <_{\mathrm{POT}} \partial^s \mathfrak{e}_t \iff j > t \vee (j = t \wedge i < s)$$

For $n = 2$ this yields

$$(0,1) < (0,\partial) < (0,\partial^2) < \ldots < (1,0) < (\partial,0) < (\partial^2,0) < \ldots$$

Definition (term over position ordering)

$$\partial^i \mathfrak{e}_j <_{\mathrm{TOP}} \partial^s \mathfrak{e}_t \iff i < s \vee (i = s \wedge j > t)$$

For $n = 2$ this yields

$$(0,1) < (1,0) < (0,\partial) < (\partial,0) < (0,\partial^2) < (\partial^2,0) < \ldots$$

Monomial orderings

There are two important admissible monomial orderings:

Definition (position over term ordering)

$$\partial^i \mathfrak{e}_j <_{\mathrm{POT}} \partial^s \mathfrak{e}_t \iff j > t \vee (j = t \wedge i < s)$$

For $n = 2$ this yields

$$(0,1) < (0,\partial) < (0,\partial^2) < \ldots < (1,0) < (\partial,0) < (\partial^2,0) < \ldots$$

Definition (term over position ordering)

$$\partial^i \mathfrak{e}_j <_{\mathrm{TOP}} \partial^s \mathfrak{e}_t \iff i < s \vee (i = s \wedge j > t)$$

For $n = 2$ this yields

$$(0,1) < (1,0) < (0,\partial) < (\partial,0) < (0,\partial^2) < (\partial^2,0) < \ldots$$

Monomial orderings

There are two important admissible monomial orderings:

Definition (position over term ordering)

$$\partial^i \mathfrak{e}_j <_{\mathrm{POT}} \partial^s \mathfrak{e}_t \iff j > t \vee (j = t \wedge i < s)$$

For $n = 2$ this yields

$$(0,1) < (0,\partial) < (0,\partial^2) < \ldots < (1,0) < (\partial,0) < (\partial^2,0) < \ldots$$

Definition (term over position ordering)

$$\partial^i \mathfrak{e}_j <_{\mathrm{TOP}} \partial^s \mathfrak{e}_t \iff i < s \vee (i = s \wedge j > t)$$

For $n = 2$ this yields

$$(0,1) < (1,0) < (0,\partial) < (\partial,0) < (0,\partial^2) < (\partial^2,0) < \ldots$$

Monomial orderings

There are two important admissible monomial orderings:

Definition (position over term ordering)

$$\partial^i \mathfrak{e}_j <_{\mathrm{POT}} \partial^s \mathfrak{e}_t \iff j > t \vee (j = t \wedge i < s)$$

For $n = 2$ this yields

$$(0,1) < (0,\partial) < (0,\partial^2) < \ldots < (1,0) < (\partial,0) < (\partial^2,0) < \ldots$$

Definition (term over position ordering)

$$\partial^i \mathfrak{e}_j <_{\mathrm{TOP}} \partial^s \mathfrak{e}_t \iff i < s \vee (i = s \wedge j > t)$$

For $n = 2$ this yields

$$(0,1) < (1,0) < (0,\partial) < (\partial,0) < (0,\partial^2) < (\partial^2,0) < \ldots$$

Monomial orderings

There are two important admissible monomial orderings:

Definition (position over term ordering)

$$\partial^i \mathfrak{e}_j <_{\mathrm{POT}} \partial^s \mathfrak{e}_t \iff j > t \vee (j = t \wedge i < s)$$

For $n = 2$ this yields

$$(0,1) < (0,\partial) < (0,\partial^2) < \ldots < (1,0) < (\partial,0) < (\partial^2,0) < \ldots$$

Definition (term over position ordering)

$$\partial^i \mathfrak{e}_j <_{\mathrm{TOP}} \partial^s \mathfrak{e}_t \iff i < s \vee (i = s \wedge j > t)$$

For $n = 2$ this yields

$$(0,1) < (1,0) < (0,\partial) < (\partial,0) < (0,\partial^2) < (\partial^2,0) < \ldots$$

Example

Let $v = (\partial^2 + 1, x - \partial) \in \mathbb{Q}(x)[\partial; \mathrm{id}, d/dx]^2$.

The term over position leading term is $(\partial^2, 0)$.

Let $w = (x\partial, 1)$ with leading term $(x\partial, 0)$.

Then v is reducible by $\{w\}$ and

$$v \longrightarrow_{\{w\}} v - \frac{1}{x}\partial \cdot w = (1 - \tfrac{1}{x}\partial, x - (1 + \tfrac{1}{x})\partial).$$

But v is not reducible by $\{(1, x - \partial^2)\}$ since the leading term is $-(0, \partial^2)$.

Example

Let $v = (\partial^2 + 1, x - \partial) \in \mathbb{Q}(x)[\partial; \mathrm{id}, d/dx]^2$.

The **term over position leading term** is $(\partial^2, 0)$.

Let $w = (x\partial, 1)$ with leading term $(x\partial, 0)$.

Then v is reducible by $\{w\}$ and

$$v \longrightarrow_{\{w\}} v - \frac{1}{x}\partial \cdot w = (1 - \tfrac{1}{x}\partial, x - (1 + \tfrac{1}{x})\partial).$$

But v is not reducible by $\{(1, x - \partial^2)\}$ since the leading term is $-(0, \partial^2)$.

Example

Let $v = (\partial^2 + 1, x - \partial) \in \mathbb{Q}(x)[\partial; \mathrm{id}, d/dx]^2$.

The term over position leading term is $(\partial^2, 0)$.

Let $w = (x\partial, 1)$ with **leading term** $(x\partial, 0)$.

Then v is reducible by $\{w\}$ and

$$v \longrightarrow_{\{w\}} v - \frac{1}{x}\partial \cdot w = (1 - \tfrac{1}{x}\partial, x - (1 + \tfrac{1}{x})\partial).$$

But v is not reducible by $\{(1, x - \partial^2)\}$ since the leading term is $-(0, \partial^2)$.

Example

Let $v = (\partial^2 + 1, x - \partial) \in \mathbb{Q}(x)[\partial; \mathrm{id}, d/dx]^2$.

The term over position leading term is $(\partial^2, 0)$.

Let $w = (x\partial, 1)$ with leading term $(x\partial, 0)$.

Then v is **reducible** by $\{w\}$ and

$$v \longrightarrow_{\{w\}} v - \frac{1}{x}\partial \cdot w = (1 - \tfrac{1}{x}\partial, x - (1 + \tfrac{1}{x})\partial).$$

But v is not reducible by $\{(1, x - \partial^2)\}$ since the leading term is $-(0, \partial^2)$.

Example

Let $v = (\partial^2 + 1, x - \partial) \in \mathbb{Q}(x)[\partial; \mathrm{id}, d/dx]^2$.

The term over position leading term is $(\partial^2, 0)$.

Let $w = (x\partial, 1)$ with leading term $(x\partial, 0)$.

Then v is reducible by $\{w\}$ and

$$v \longrightarrow_{\{w\}} v - \frac{1}{x}\partial \cdot w = (1 - \tfrac{1}{x}\partial, x - (1 + \tfrac{1}{x})\partial).$$

But v is **not reducible** by $\{(1, x - \partial^2)\}$ since the **leading term** is $-(0, \partial^2)$.

Normal forms & Gröbner bases

We may generalise [Kojima et al., Prop. 2 and 4] to Ore polynomials

Theorem

*A matrix $H \in {}^mR^n$ is in **Hermite normal form** if and only if its rows form a **reduced position over term Gröbner basis** for $R^m H$.*

Theorem

A matrix $P \in {}^mR^n$ is in Popov normal form if and only if its rows form a reduced term over position Gröbner basis for $R^m P$.

In both cases do the pivots correspond to the leading terms.

Normal forms & Gröbner bases

We may generalise [Kojima et al., Prop. 2 and 4] to Ore polynomials

Theorem

A matrix $H \in {}^mR^n$ is in Hermite normal form if and only if its rows form a reduced position over term Gröbner basis for $R^m H$.

Theorem

*A matrix $P \in {}^mR^n$ is in **Popov normal form** if and only if its rows form a **reduced term over position Gröbner basis** for $R^m P$.*

In both cases do the pivots correspond to the leading terms.

Normal forms & Gröbner bases

We may generalise [Kojima et al., Prop. 2 and 4] to Ore polynomials

Theorem

A matrix $H \in {}^mR^n$ is in Hermite normal form if and only if its rows form a reduced position over term Gröbner basis for $R^m H$.

Theorem

A matrix $P \in {}^mR^n$ is in Popov normal form if and only if its rows form a reduced term over position Gröbner basis for $R^m P$.

In both cases do the **pivots** correspond to the **leading terms**.

The FGLM algorithm

The FGLM algorithm may be used to **convert Gröbner bases from one monomial ordering to another one**.

The original algorithm was created for ideals of commutative polynomials having a finite dimensional quotient.

It translates the algebraic problem to a linear algebra problem.

In our case, the FLGM algorithm needs to work in the K-vector space

$$\frac{R^n}{R^m M} \quad \text{where } M \in {}^m R^n.$$

Unfortunately, this space is in general not finite dimensional.

The FGLM algorithm

The FGLM algorithm may be used to convert Gröbner bases from one monomial ordering to another one.

The original algorithm was created for **ideals of commutative polynomials** having a **finite dimensional quotient**.

It translates the algebraic problem to a linear algebra problem.

In our case, the FLGM algorithm needs to work in the K-vector space

$$\frac{R^n}{R^m M} \quad \text{where } M \in {}^m R^n.$$

Unfortunately, this space is in general not finite dimensional.

The FGLM algorithm

The FGLM algorithm may be used to convert Gröbner bases from one monomial ordering to another one.

The original algorithm was created for ideals of commutative polynomials having a finite dimensional quotient.

It **translates** the **algebraic problem** to a **linear algebra problem**.

In our case, the FLGM algorithm needs to work in the K-vector space

$$\frac{R^n}{R^m M} \quad \text{where } M \in {}^m R^n.$$

Unfortunately, this space is in general not finite dimensional.

The FGLM algorithm

The FGLM algorithm may be used to convert Gröbner bases from one monomial ordering to another one.

The original algorithm was created for ideals of commutative polynomials having a finite dimensional quotient.

It translates the algebraic problem to a linear algebra problem.

In our case, the FLGM algorithm needs to work in the **K-vector space**

$$\frac{R^n}{R^m M} \quad \text{where } M \in {}^m R^n.$$

Unfortunately, this space is in general not finite dimensional.

The FGLM algorithm

The FGLM algorithm may be used to convert Gröbner bases from one monomial ordering to another one.

The original algorithm was created for ideals of commutative polynomials having a finite dimensional quotient.

It translates the algebraic problem to a linear algebra problem.

In our case, the FLGM algorithm needs to work in the K-vector space

$$\frac{R^n}{R^m M} \quad \text{where } M \in {}^m R^n.$$

Unfortunately, this space is in general **not finite dimensional**.

Degree bounds

We can generalise [Giesbrecht et al., 2009] to non-square matrices of Ore polynomials

Theorem

If H is the Hermite normal form of a matrix $M \in {}^{m}R^{n}$ then

$$\deg H \leqslant m \deg M.$$

Similarly, we obtain

Theorem

If P is the Popov normal form of a matrix $M \in {}^{m}R^{n}$ then

$$\deg P \leqslant \deg M.$$

Degree bounds

We can generalise [Giesbrecht et al., 2009] to non-square matrices of Ore polynomials

Theorem

If H is the Hermite normal form of a matrix $M \in {}^{m}R^{n}$ then

$$\deg H \leqslant m \deg M.$$

Similarly, we obtain

Theorem

If P is the Popov normal form of a matrix $M \in {}^{m}R^{n}$ then

$$\deg P \leqslant \deg M.$$

The FGLM revisited

Using the **degree bounds**, for FGLM we only need to consider a **finite dimensional subspace** of $R^n/R^m M$.

Given a matrix $P \in {}^mR^n$ in Popov normal form, we want to compute the corresponding Hermite normal form H.

With FGLM, we test a monomials in ascending position over term order for whether they are

- leading monomial of a position over term Gröbner basis element, or
- element of a basis of $R^n/R^m P$.

The checks are done using the Gröbner basis P.

We can ignore all those monomials of degree larger than $m \deg P$.

The complexity (in field operations) amounts to $\mathcal{O}((mn \deg P)^4)$ —which drops to $\mathcal{O}((m \deg P)^4)$ if P is square.

The FGLM revisited

Using the degree bounds, for FGLM we only need to consider a finite dimensional subspace of $R^n/R^m M$.

Given a matrix $P \in {}^mR^n$ in Popov normal form, we want to compute the corresponding Hermite normal form H.

With FGLM, we test a monomials in ascending position over term order for whether they are

- leading monomial of a position over term Gröbner basis element, or
- element of a basis of $R^n/R^m P$.

The checks are done using the Gröbner basis P.

We can ignore all those monomials of degree larger than $m \deg P$.

The complexity (in field operations) amounts to $\mathcal{O}((mn \deg P)^4)$ —which drops to $\mathcal{O}((m \deg P)^4)$ if P is square.

The FGLM revisited

Using the degree bounds, for FGLM we only need to consider a finite dimensional subspace of $R^n/R^m M$.

Given a matrix $P \in {}^m R^n$ in Popov normal form, we want to compute the corresponding Hermite normal form H.

With FGLM, we **test a monomials in ascending position over term order** for whether they are

- **leading monomial** of a position over term Gröbner basis element, or
- **element of a basis** of $R^n/R^m P$.

The checks are done using the Gröbner basis P.

We can ignore all those monomials of degree larger than $m \deg P$.

The complexity (in field operations) amounts to $\mathcal{O}((mn \deg P)^4)$ —which drops to $\mathcal{O}((m \deg P)^4)$ if P is square.

The FGLM revisited

Using the degree bounds, for FGLM we only need to consider a finite dimensional subspace of $R^n/R^m M$.

Given a matrix $P \in {}^m R^n$ in Popov normal form, we want to compute the corresponding Hermite normal form H.

With FGLM, we test a monomials in ascending position over term order for whether they are

- leading monomial of a position over term Gröbner basis element, or
- element of a basis of $R^n/R^m P$.

The checks are done using the Gröbner basis P.

We can **ignore** all those **monomials of degree larger than** $m \deg P$.

The complexity (in field operations) amounts to $\mathcal{O}((mn \deg P)^4)$ —which drops to $\mathcal{O}((m \deg P)^4)$ if P is square.

The FGLM revisited

Using the degree bounds, for FGLM we only need to consider a finite dimensional subspace of $R^n/R^m M$.

Given a matrix $P \in {}^mR^n$ in Popov normal form, we want to compute the corresponding Hermite normal form H.

With FGLM, we test a monomials in ascending position over term order for whether they are

- leading monomial of a position over term Gröbner basis element, or
- element of a basis of $R^n/R^m P$.

The checks are done using the Gröbner basis P.

We can ignore all those monomials of degree larger than $m \deg P$.

The **complexity** (in field operations) amounts to $\mathcal{O}((mn \deg P)^4)$ —which drops to $\mathcal{O}((m \deg P)^4)$ if P is **square**.

Example

Consider the matrix

$$M = \begin{pmatrix} 1 & \partial & x\partial - 1 \\ \frac{1}{x}\partial & \frac{1}{x} & \partial^2 - \frac{x+1}{x} \end{pmatrix} \in {}^2\mathbb{Q}(x)[\partial; \mathrm{id}, d/dx]^3.$$

The degree bound is 4 and we work in the space generated by the irreducible monomials of degree less or equal to 4

$$\overline{\mathfrak{e}_1}, \overline{\partial\mathfrak{e}_1}, \overline{\partial^2\mathfrak{e}_1}, \overline{\partial^3\mathfrak{e}_1}, \overline{\partial^4\mathfrak{e}_1}, \ \overline{\mathfrak{e}_2}, \ \overline{\mathfrak{e}_3}, \overline{\partial\mathfrak{e}_3}.$$

The smallest position over term monomials are

$$\mathfrak{e}_3, \partial\mathfrak{e}_3, \partial^2\mathfrak{e}_3, \partial^3\mathfrak{e}_3, \partial^4\mathfrak{e}_3,$$

and their residue classes are linearly independent.

Since we reached the degree bound, the next elements are $\mathfrak{e}_2, \partial\mathfrak{e}_2$ whose residue classes are still linearly independent.

Example

Consider the matrix

$$M = \begin{pmatrix} 1 & \partial & x\partial - 1 \\ \frac{1}{x}\partial & \frac{1}{x} & \partial^2 - \frac{x+1}{x} \end{pmatrix} \in {}^2\mathbb{Q}(x)[\partial; \mathrm{id}, d/dx]^3.$$

The **degree bound** is 4 and we work in the space generated by the **irreducible monomials of degree less or equal to** 4

$$\overline{\mathfrak{e}_1}, \overline{\partial\mathfrak{e}_1}, \overline{\partial^2\mathfrak{e}_1}, \overline{\partial^3\mathfrak{e}_1}, \overline{\partial^4\mathfrak{e}_1}, \ \overline{\mathfrak{e}_2}, \ \overline{\mathfrak{e}_3}, \overline{\partial\mathfrak{e}_3}.$$

The smallest position over term monomials are

$$\mathfrak{e}_3, \partial\mathfrak{e}_3, \partial^2\mathfrak{e}_3, \partial^3\mathfrak{e}_3, \partial^4\mathfrak{e}_3,$$

and their residue classes are linearly independent.

Since we reached the degree bound, the next elements are $\mathfrak{e}_2, \partial\mathfrak{e}_2$ whose residue classes are still linearly independent.

Example

Consider the matrix

$$M = \begin{pmatrix} 1 & \partial & x\partial - 1 \\ \frac{1}{x}\partial & \frac{1}{x} & \partial^2 - \frac{x+1}{x} \end{pmatrix} \in {}^2\mathbb{Q}(x)[\partial; \mathrm{id}, d/dx]^3.$$

The degree bound is 4 and we work in the space generated by the irreducible monomials of degree less or equal to 4

$$\overline{\mathfrak{e}_1}, \overline{\partial\mathfrak{e}_1}, \overline{\partial^2\mathfrak{e}_1}, \overline{\partial^3\mathfrak{e}_1}, \overline{\partial^4\mathfrak{e}_1}, \ \overline{\mathfrak{e}_2}, \ \overline{\mathfrak{e}_3}, \overline{\partial\mathfrak{e}_3}.$$

The **smallest** position over term **monomials** are

$$\mathfrak{e}_3, \partial\mathfrak{e}_3, \partial^2\mathfrak{e}_3, \partial^3\mathfrak{e}_3, \partial^4\mathfrak{e}_3,$$

and their **residue classes are linearly independent**.

Since we reached the degree bound, the next elements are $\mathfrak{e}_2, \partial\mathfrak{e}_2$ whose residue classes are still linearly independent.

Example

Consider the matrix

$$M = \begin{pmatrix} 1 & \partial & x\partial - 1 \\ \frac{1}{x}\partial & \frac{1}{x} & \partial^2 - \frac{x+1}{x} \end{pmatrix} \in {}^2\mathbb{Q}(x)[\partial; \mathrm{id}, d/dx]^3.$$

The degree bound is 4 and we work in the space generated by the irreducible monomials of degree less or equal to 4

$$\overline{\mathfrak{e}_1}, \overline{\partial\mathfrak{e}_1}, \overline{\partial^2\mathfrak{e}_1}, \overline{\partial^3\mathfrak{e}_1}, \overline{\partial^4\mathfrak{e}_1}, \ \overline{\mathfrak{e}_2}, \ \overline{\mathfrak{e}_3}, \overline{\partial\mathfrak{e}_3}.$$

The smallest position over term monomials are

$$\mathfrak{e}_3, \partial\mathfrak{e}_3, \partial^2\mathfrak{e}_3, \partial^3\mathfrak{e}_3, \partial^4\mathfrak{e}_3,$$

and their residue classes are linearly independent.

Since we **reached the degree bound**, the next elements are $\mathfrak{e}_2, \partial\mathfrak{e}_2$ whose residue classes are still **linearly independent**.

Example (cont.)

The residue class of the next monomial $\partial^2 \mathfrak{e}_2$ **depends linearly** on the previous ones.

We have

$$\partial^2 \mathfrak{e}_2 \equiv \mathfrak{e}_2 - (x+1)\mathfrak{e}_3 \pmod{P}.$$

Thus the first position over term Gröbner basis element is

$$(0, \partial^2 - 1, x+1).$$

Continuing in this manner we obtain the Hermite normal form of

$$\begin{pmatrix} 1 & \partial & x\partial - 1 \\ \frac{1}{x}\partial & \frac{1}{x} & \partial^2 - \frac{x+1}{x} \end{pmatrix}$$

to be

$$\begin{pmatrix} 1 & \partial & x\partial - 1 \\ 0 & \partial^2 - 1 & x+1 \end{pmatrix}.$$

Example (cont.)

The residue class of the next monomial $\partial^2 \mathfrak{e}_2$ depends linearly on the previous ones.

We have

$$\partial^2 \mathfrak{e}_2 \equiv \mathfrak{e}_2 - (x+1)\mathfrak{e}_3 \pmod{P}.$$

Thus the **first position over term Gröbner basis element** is

$$(0, \partial^2 - 1, x+1).$$

Continuing in this manner we obtain the Hermite normal form of

$$\begin{pmatrix} 1 & \partial & x\partial - 1 \\ \frac{1}{x}\partial & \frac{1}{x} & \partial^2 - \frac{x+1}{x} \end{pmatrix}$$

to be

$$\begin{pmatrix} 1 & \partial & x\partial - 1 \\ 0 & \partial^2 - 1 & x+1 \end{pmatrix}.$$

Example (cont.)

The residue class of the next monomial $\partial^2 \mathfrak{e}_2$ depends linearly on the previous ones.

We have

$$\partial^2 \mathfrak{e}_2 \equiv \mathfrak{e}_2 - (x+1)\mathfrak{e}_3 \pmod{P}.$$

Thus the first position over term Gröbner basis element is

$$(0, \partial^2 - 1, x+1).$$

Continuing in this manner we obtain the **Hermite normal form** of

$$\begin{pmatrix} 1 & \partial & x\partial - 1 \\ \frac{1}{x}\partial & \frac{1}{x} & \partial^2 - \frac{x+1}{x} \end{pmatrix}$$

to be

$$\begin{pmatrix} 1 & \partial & x\partial - 1 \\ 0 & \partial^2 - 1 & x+1 \end{pmatrix}.$$

Summary

In this talk we have considered **matrices of Ore polynomials**.

We connected the Hermite normal form and the Popov normal form to Gröbner bases.

We adapted the FGLM algorithm to convert between Popov normal form and Hermite normal form.

Summary

In this talk we have considered matrices of Ore polynomials.

We connected the **Hermite normal form** and the **Popov normal form** to **Gröbner bases**.

We adapted the FGLM algorithm to convert between Popov normal form and Hermite normal form.

Summary

In this talk we have considered matrices of Ore polynomials.

We connected the Hermite normal form and the Popov normal form to Gröbner bases.

We adapted the FGLM algorithm to convert between Popov normal form and Hermite normal form.

Thank you very much!

Bibliography

Mark Giesbrecht and Myung Sub Kim.
Computer Algebra in Scientific Computing, volume 5743 of *Lecture Notes in Computer Science*, chapter On Computing the Hermite Form of a Matrix of Differential Polynomials, pages 118–129.
Springer, Berlin / Heidelberg, 2009.

Chiaki Kojima, Paolo Rapisarda, and Kiyotsugu Takaba.
Canonical forms for polynomial and quadratic differential operators.
System & Control Letters, pages 678–684, 2007.

Hermite normal form

Definition (Hermite form)

A matrix $M \in {}^mR^n$ is in **Hermite form** if there exist column indices $j_1 > j_2 > \ldots > j_m$ which we call **pivot indices** such that

1. $M_{i,k} = 0$ if $k < j_i$,
2. the entries M_{i,j_i} are monic, and
3. $\deg M_{i,j_i} > M_{i,k}$ for all $k \neq j_i$.

Popov normal form

Definition (Popov form)

A matrix $M \in {}^{m}R^{n}$ is said to be in **Popov form**, if

1. M is row-reduced and $\operatorname{rdeg}_i M \leqslant \operatorname{rdeg}_{i+1} M$ for all i.
2. for the i^{th} row there exists a column index j_i (the **pivot index**) such that
   - 2.1 M_{i,j_i} is monic and $\deg M_{i,j_i} = \operatorname{rdeg}_i M$;
   - 2.2 $\deg M_{i,k} < \operatorname{rdeg}_i M$ if $k < j_i$;
   - 2.3 $\deg M_{k,j_i} < \operatorname{rdeg}_i M$ if $k \neq i$; and
   - 2.4 if $\operatorname{rdeg}_i M = \operatorname{rdeg}_k M$ and $i < k$ then $j_i < j_k$ (i. e., pivot indices are ordered increasingly).

Row-reducedness

Definition (Leading row coefficient matrix)

Let $M \in {}^mR^n$. The **leading row coefficient matrix** of M is defined by

$$\mathrm{LC}_{\mathrm{row}}(M) = \left(\sigma^{\deg M - \deg M_{i,\bullet}}(\mathrm{coeff}(\deg M_{i,\bullet}, M_{i,j}))\right)_{i,j} \in {}^mK^n.$$

Definition (Row-reducedness)

A matrix $M \in {}^mR^n$ is row-reduced if $\mathrm{LC}_{\mathrm{row}}(M)$ has left row-rank m.

Row-reducedness

Definition (Leading row coefficient matrix)

Let $M \in {}^mR^n$. The leading row coefficient matrix of M is defined by

$$\mathrm{LC}_{\mathrm{row}}(M) = \left(\sigma^{\deg M - \deg M_{i,\bullet}}(\mathrm{coeff}(\deg M_{i,\bullet}, M_{i,j}))\right)_{i,j} \in {}^mK^n.$$

Definition (Row-reducedness)

A matrix $M \in {}^mR^n$ is **row-reduced** if $\mathrm{LC}_{\mathrm{row}}(M)$ has left row-rank m.