Difference Equations, Inverse Systems and Gröbner Bases

Franz Pauer

Institut für Mathematik, Universität Innsbruck

2006-05-15

The inverse system of a polynomial ideal

Let F be a field,
$F[s] := F[s_1, \ldots, s_n]$ the algebra of n-variate polynomials over F,
I an ideal in $F[s]$.

The **inverse system** of I is

$$I^{\perp} := \{f \in Hom_F(F[s], F) \mid f|_I = 0\} \ .$$

An F-basis of $I^{\perp}$ is a **dual basis** of I .

(Related: Implicit form of a subspace of a vector-space).

Advantage of a dual basis e.g.:
decide "$f \in I$?" for $f \in F[s]$.

Note that

$$I^{\perp} \cong Hom_F(F[s]/I, F) \ .$$

$I^{\perp}$ is a finite-dimensional F-vectorspace iff the ideal I is zero-dimensional.

History

- Macaulay(1915): inverse system

- Gröbner(1938): differential operators associated to I

- Oberst(1990): in the context of multidimensional linear system theory

- Marinari, Möller, Mora(1991,1993,1996); Möller, Tenberg(1999): Gauß-basis (set of zeroes of I is known and contained in F^n)

- Mourrain(1997); Mourrain, Ruatta(2002): local inverse system (set of zeroes of I is known and contained in F^n), application to interpolation

- Heiß, Oberst, Pauer (2002, 2006): application to square-free decomposition of zero-dimensional ideals

Representation of elements of $I^\perp$

Let $\leq$ be a term order on $\mathbb{N}^n$ and

$$\Gamma := \mathbb{N}^n \setminus deg(I) \ .$$

Then

$$F[s] = I \oplus \bigoplus_{\gamma\in\Gamma} Fs^\gamma \ , \qquad h = (h - \mathsf{nf}(h)) + \mathsf{nf}(h).$$

($\mathsf{nf}(h)$ is the normal form of h with respect to I and $\leq$).

Describe $\varphi \in I^\perp$ by:

$$(\varphi(s^\gamma))_{\gamma\in\Gamma} \quad \text{and} \quad \varphi|_I = 0 \ .$$

Let $h \in F[s]$ and $\mathsf{nf}(h) = \sum_{\gamma\in\Gamma} c_\gamma s^\gamma$. Then

$$\varphi(h) = \varphi(\mathsf{nf}(h)) = \sum_{\gamma\in\Gamma} c_\gamma \varphi(s^\gamma) \ .$$

An F-Basis of $I^{\perp}$ (if Γ is finite):

Let $e_\gamma \in I^{\perp}$ be defined by

$$\begin{aligned} e_\gamma(s^\gamma) &= 1 \\ e_\gamma(s^\alpha) &= 0 \quad \text{if } \alpha \in \Gamma, \alpha \neq \gamma \\ e_\gamma|_I &= 0 \end{aligned}$$

The family $(e_\gamma)_{\gamma\in\Gamma}$ is an F-basis of $I^{\perp}$.

For $\varphi \in I^{\perp}$ we have:

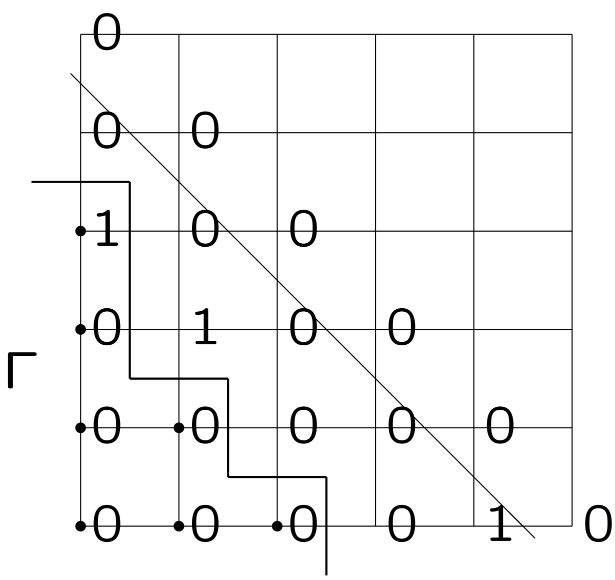
$$\varphi = \sum_{\gamma\in\Gamma} \varphi(s^\gamma)e_\gamma \ .$$

If we identify $I^{\perp}$ and $Hom_F(F[s]/I, F)$, then the basis $(e_\gamma)_{\gamma\in\Gamma}$ is dual to the F-basis $(\overline{s}^\gamma)_{\gamma\in\Gamma}$.

Example 1

$$
\begin{aligned}
I &:= {}_{\mathbb{Q}[s_1,s_2]} < s_2^4, -s_2^3 + s_1 s_2^2, \\
&\quad s_2 s_1^2, s_1^3 - s_2^2 + s_2 s_1 > \\
&\quad \leq \text{ gr. lex. term-order, } s_1 > s_2 \\
\Gamma &= \{(0,0),(1,0),(0,1), \\
&\quad (2,0),(1,1),(0,2),(0,3)\} \\
I^\perp &:= {}_{\mathbb{Q}} < e_\gamma \mid \gamma \in \{(0,0),(1,0),(0,1), \\
&\quad (2,0),(1,1),(0,2),(0,3)\} >
\end{aligned}
$$

The values of $e_{(0,3)}$:



Example 2

$$
\begin{aligned}
I \quad &:= \quad < 6s_1^2 s_2 + s_1 s_2^2 - s_2^3, \\
& \quad\; 3s_1 s_2^3 + 2s_1 s_2^2 - 2s_2^3, \\
& \quad\; 12s_1^3 - 12s_2^2 + 12s_2 s_1 - 5s_2^3 + 5s_1 s_2^2, \\
& \quad\; 3s_2^4 - 4s_1 s_2^2 + 4s_2^3 > \subseteq \mathbb{Q}[s_1, s_2]
\end{aligned}
$$

$$
\begin{aligned}
\Gamma \quad &= \quad \{(0,0),(1,0),(0,1), \\
& \quad\; (2,0),(1,1),(0,2),(1,2),(0,3)\}
\end{aligned}
$$

Computation of the normal forms nf(s^α) for $\alpha \in \mathbb{N}^2 \setminus \Gamma, |\alpha| = \alpha_1 + \alpha_2 \leq 4$ yields

s^α	s_1^3	$s_1^2 s_2$	s_2^4	s_1^4	$s_1^3 s_2$	$s_1^2 s_2^2$	$s_1 s_2^3$
$e_{(0,0)}(s^\alpha)$	0	0	0	0	0	0	0
$e_{(1,0)}(s^\alpha)$	0	0	0	0	0	0	0
$e_{(0,1)}(s^\alpha)$	0	0	0	0	0	0	0
$e_{(2,0)}(s^\alpha)$	0	0	0	0	0	0	0
$e_{(1,1)}(s^\alpha)$	-1	0	0	0	0	0	0
$e_{(0,2)}(s^\alpha)$	1	0	0	0	0	0	0
$e_{(1,2)}(s^\alpha)$	$\frac{3}{4}$	$\frac{-1}{6}$	$\frac{4}{3}$	$\frac{3}{4}$	$\frac{-1}{6}$	$\frac{1}{3}$	$\frac{-2}{3}$
$e_{(0,3)}(s^\alpha)$	$\frac{1}{4}$	$\frac{1}{6}$	$\frac{-4}{3}$	$\frac{1}{4}$	$\frac{1}{6}$	$\frac{-1}{3}$	$\frac{2}{3}$

$I^{\perp}$ as $F[s]$-module

$Hom_F(F[s], F)$ is an $F[s]$-module by

$$(f \circ \varphi)(g) := \varphi(fg) \text{ , where } f, g \in F[s],$$
$$\varphi \in Hom_F(F[s], F).$$

I is an ideal, hence $I^{\perp}$ is an $F[s]$-submodule.

Let $R := Rad(I)$. Compute $V \leq_F I^{\perp}$ with $V \oplus Rad(I) \circ I^{\perp} = I^{\perp}$.

If I is primary and F-rational: each F-basis of V is a system of $F[s]$-generators of $I^{\perp}$ of minimal length (Nakayama's Lemma).

If the primary decomposition of I is known, we can compute a system of $F[s]$-generators of $I^{\perp}$ of minimal length for any zero-dimensional ideal I.

Example 3

$I :=_{\mathbb{Q}[s]} < s_2 s_1 - s_2,$

$s_1^5 - 5s_1^4 + 10s_1^3 - 10s_1^2 + 5s_1 - 1, s_2^2 >$

$Rad(I) = < s_2, s_1 - 1 >$

$\mathbb{Q}$-basis of $I^\perp$:
$\{e_{(0,0)}, e_{(1,0)}, e_{(0,1)}, e_{(2,0)}, e_{(3,0)}, e_{(4,0)}\}$

$\mathbb{Q}$-basis of $Rad(I) \circ I^\perp$:
$\{e_{(0,0)} - e_{(4,0)}, e_{(1,0)} + 4e_{(4,0)},$
$e_{(2,0)} - 6e_{(4,0)}, e_{(3,0)} + 4e_{(4,0)}\}$

$\mathbb{Q}$-basis of V:
$E = \{e_{(0,0)}, e_{(0,1)}\}$

Linear Systems of Partial Difference Equations with Constant Coefficients

Given:

- a family
$$(R(\mu))_{\mu\in\mathbb{N}^n}$$
of columns $R(\mu) := (R_i(\mu))_{1\le i\le k}$, in $F^{k\times 1}$, where only finitely many $R(\mu)$ are $\neq 0$

- a map $v = (v_1,\ldots,v_k) : \mathbb{N}^n \to F^{k\times 1}$,

where k, n are positive integers.

Wanted:

all maps (signal vectors) $w : \mathbb{N}^n \to F$ such that
$$\sum_{\mu\in\mathbb{N}^n} R(\mu)w(\mu+\nu) = v(\nu) \quad \text{for all } \nu\in\mathbb{N}^n . \tag{1}$$

("system of k partial difference equations with constant coefficients for 1 unknown w")

Questions

- How can we decide whether system (1) is solvable or not?

- How can we find a *canonical subset* $\Gamma \subseteq \mathbb{N}^n$ such that for every *initial condition* $x : \Gamma \to F$ there is exactly one solution w with $w|\Gamma = x$?

- If w is such a solution, how can we compute $w(\mu)$ for any $\mu \in \mathbb{N}^n$?

Represent data by polynomials

$F[s] := F[s_1, \dots, s_n]$, $s^\mu := s_1^{\mu_1} s_2^{\mu_2} \cdots s_n^{\mu_n}$.

For $\mu \in \mathbb{N}^n$ and $w : \mathbb{N}^n \to F$, $\nu \mapsto w(\nu)$, let

$$(s^\mu \circ w)(\nu) := w(\mu + \nu), \quad \text{for all } \nu \in \mathbb{N}^n$$

(left shift action).

By $w(s^\mu) := w(\mu)$ we consider $w : \mathbb{N}^n \longrightarrow F$ as an F-linear map $w : F[s] \longrightarrow F$.
Then $(s^\mu \circ w)(\nu) = w(\mu + \nu) = w(s^\mu s^\nu)$.

Hence

$$\sum_{\mu \in \mathbb{N}^n} R_i(\mu) w(\mu + \nu) = \sum_{\mu \in \mathbb{N}^n} R_i(\mu) w(s^\mu s^\nu) =$$

$$= w\Big(\sum_{\mu \in \mathbb{N}^n} R_i(\mu) s^\mu s^\nu\Big) = w(s^\nu R_i)\,,$$

where

$$R_i := \sum_{\mu \in \mathbb{N}^n} R_i(\mu) s^\mu \in F[s]\,.$$

Thus equation (1) gets the simple form

$$w(s^\nu R_i) = v_i(\nu) \qquad \text{for } i = 1, \cdots, k \text{ and all } \nu \in \mathbb{N}^n \ . \tag{2}$$

or

$$R_i \circ w = v_i \, , 1 \leq i \leq k.$$

In the homogeneous case ($v = 0$) this means

$$w \in I^\perp \ ,$$

where I is the ideal generated by $R_1, \ldots, R_k$.

Example 4

(compare Example 2)

Find $w : \mathbb{N}^2 \longrightarrow \mathbb{Q}$ such that for all $\nu \in \mathbb{N}^2$:

$$6w((2,1)+\nu) + w((1,2)+\nu) - w((0,3)+\nu) = 0$$

$$3w((1,3)+\nu) + 2w((1,2)+\nu) - 2w((0,3)+\nu) = 0$$

$$12w((3,0)+\nu)) - 12w((0,2)+\nu) + 12w((1,1)+\nu) -$$
$$-5w((0,3)+\nu) + 5w((1,2)+\nu) = 0$$

$$3w((0,4)+\nu) - 4w((1,2)+\nu) + 4w((0,3)+\nu) = 0$$

A canonical subset is $\Gamma :=$
$= \{(0,0),(1,0),(0,1),(2,0),(1,1),(0,2),(1,2),(0,3)\}$

For $\mu \in \mathbb{N}^2$:

$$w(\mu) := w(\mathsf{nf}(s^{\mu}))$$

(see Example 2).

Non-homogeneous Case

Existence of Solutions

Compute a system of generators $L_1, \ldots, L_p$ of the $F[s]$-submodule

$$\{u \in F[s]^k \mid \sum_{i=1}^{k} u_i R_i = 0\} \leq F[s]^k \ .$$

Then: A solution of (1) exists iff

$$\sum_{j=1}^{k} L_{ij} \circ v_j = 0 \ , \ 1 \leq i \leq p \ .$$

Solutions

If solutions w exist:
$w(\mu)$ can be chosen arbitrarily, if $\mu \in \Gamma$.
For $\mu \neq \Gamma$ compute
$\mathsf{nf}(s^\mu) = \sum_{\alpha \in \Gamma} c_\alpha s^\alpha$ and
$s^\mu - \mathsf{nf}(s^\mu) = \sum_{\nu,i} d_{\nu,i} s^\nu R_i$.
Then

$$w(\mu) = \sum_{\alpha \in \Gamma} c_\alpha w(\alpha) + \sum_{\nu,i} d_{\nu,i} v_i(\nu) \ .$$

Represent signal vectors by power series

Let $F[[z]] := F[[z_1, \ldots, z_n]]$ be the F-algebra of n-variate formal power-series over F, $z^\mu := z_1^{\mu_1} z_2^{\mu_2} \cdots z_n^{\mu_n}$.

We now write maps $w : \mathbb{N}^n \longrightarrow F$ in the form

$$w = \sum_{\nu \in \mathbb{N}^n} w(\nu) z^\nu \in F[[z]],$$

then $s^\mu \circ w = \sum_{\nu \in \mathbb{N}^n} w(\nu + \mu) z^\nu$.
In particular, $s^\mu \circ z^\pi = z^{\pi - \mu}$, if $\pi - \mu \in \mathbb{N}^n$, and $s^\mu \circ z^\pi = 0$, otherwise.

Example 5 $F = \mathbb{Q}$, $n = 2$, $k = 2$.

$$R := \begin{pmatrix} 2s_1^2 s_2 + 1 \\ 3s_1 s_2^2 + 2 \end{pmatrix}$$

$$v := \begin{pmatrix} 13z_2^2 + 5z_1^2 z_2^3 \\ 6z_2^2 + 10z_1^2 z_2^3 + 15z_1 z_2 \end{pmatrix} \; .$$

Here $p = 1$ and
$L = (-R_2, R_1) = (-3s_1 s_2^2 - 2, 2s_1^2 s_2 + 1)$,
$L \circ v = 0$, hence the system $R \circ w = v$ is solvable.

A Gröbner basis of the ideal

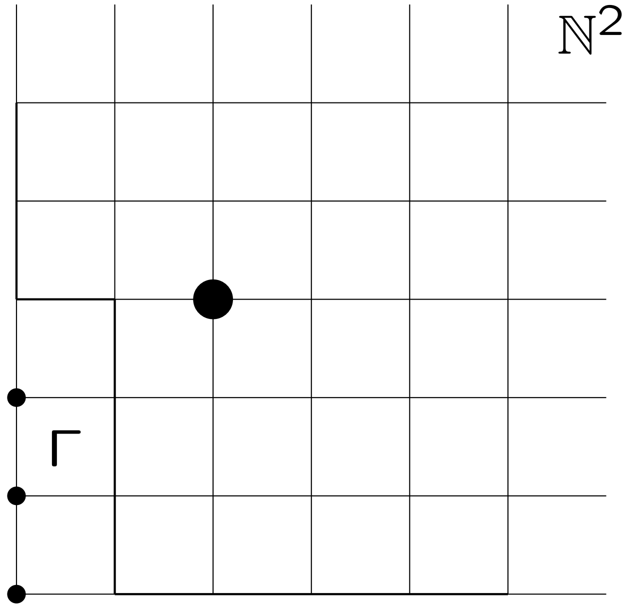
$$U := \langle R_1, R_2 \rangle = \langle 2s_1^2 s_2 + 1,\, 3s_1 s_2^2 + 2 \rangle$$

in $F[s_1, s_2]$ with respect to the graded lexicographic order ($s_1 > s_2$) is

$$\{4s_1 - 3s_2, 9s_2^3 + 8\}$$

and hence

$$\Gamma = \{(0,0), (0,1), (0,2)\} \; .$$



Let $\mu := (2,3)$. Then

$$s_1^2 s_2^3 = -\frac{1}{2}s_2^2 + (-\frac{3}{4}s_1 s_2^4)R_1 + (\frac{1}{2}s_1^2 s_2^3 + \frac{1}{4}s_2^2)R_2 \ .$$

Hence

$$w(2,3) =$$

$$= -\frac{1}{2}x(0,2) - \frac{3}{4}v_1(1,4) + \frac{1}{2}v_2(2,3) + \frac{1}{4}v_2(0,2) =$$

$$= -\frac{1}{2}x(0,2) + \frac{13}{2} \ .$$

Convergent power series

Let

$$\mathbb{C}\langle z\rangle := \mathbb{C}\langle z_1, \ldots, z_n\rangle$$

be the algebra of (locally) convergent power series (i.e. power series $\sum_\mu a(\mu)z^\mu$ such that there are $C > 0$ and $d_1 > 0, \ldots, d_n > 0$ with $|a(\mu)| \leq Cd^\mu$ for all $\mu \in \mathbb{N}^n$).

Consider signal vectors as vectors of power series. Then the solution of

$$R_i \circ w = v_i\,, 1 \leq i \leq k,\ \ w|\Gamma = x$$

is convergent if the data x and $v_i, 1 \leq i \leq k$, are so.

Differential equations

For $\mu \in \mathbb{N}^n,\ a \in F[[z]]$ consider

$$s^\mu \bullet a := \partial^\mu a = \frac{\partial^{|\mu|} a}{\partial z_1^{\mu_1} \cdots \partial z_n^{\mu_n}} \ .$$

The map

$$(\mathbb{C}[[z]], \circ) \to (\mathbb{C}[[z]], \bullet)$$

$$\sum_\mu a(\mu) z^\mu \mapsto \sum_\mu \frac{a(\mu)}{\mu!} z^\mu$$

is an isomorphism of the $F[s]-$modules $(F[[z]], \circ)$ and $(F[[z]], \bullet)$ (*Borel-isomorphism*).

Let

$$O(\mathbb{C}^r; \mathrm{exp})$$

be the algebra of entire holomorphic functions of *exponential type* (i.e. holomorphic functions $b = \sum_{\mu \in \mathbb{N}^n} b(\mu) z^\mu$ on $\mathbb{C}^n$ such that there are $C > 0$ and $d_1 > 0, \ldots, d_n > 0$ with $|b(\mu)| \leq C \, \mathrm{exp}(\sum_{i=1}^r d_i |\mu_i|)$ for all $\mu \in \mathbb{N}^n$).
The Borel isomorphism induces the isomorphism

$$(\mathbb{C}\langle z \rangle, \circ) \cong (O(\mathbb{C}^n; \mathrm{exp}), \bullet) \ .$$

Thus results for the discrete case can be translated to the continuous case.

Extension to F[s]-Modules

Let U be an $F[s]$-submodule of $F[s]^\ell$.

The inverse system of U is

$$U^\perp := \{f \in Hom_F(F[s]^\ell, F) \mid f|_U = 0\} \ .$$

A system of k difference equations in ℓ unknowns is given by a family of $k \times \ell$-matrices

$$(R(\mu))_{\mu \in \mathbb{N}^n}$$

where only finitely many matrices $R(\mu) \in F$ are $\neq 0$, and a map

$$(v_1, \ldots, v_k) : \mathbb{N}^n \to F^{k \times 1} \ ,$$

where k, ℓ, n are positive integers.

Wanted: all ℓ-columns w of functions (signal vectors) $w_i : \mathbb{N}^n \to F$, $1 \leq i \leq \ell$ such that

$$\sum_{j=1}^{\ell} \sum_{\mu \in \mathbb{N}^n} R_{ij}(\mu) w_j(\mu + \nu) = v_i(\nu) \ ,$$

for $i = 1, \cdots, k$ and all $\nu \in \mathbb{N}^n$.

Consider w as F-linear map $w := F[s]^\ell \longrightarrow F$ by $w(0, \ldots, 0, \underbrace{s^\mu}_{i}, 0, \ldots, 0) := w_i(\mu)$.

Use Gröbner bases for modules (instead of ideals).

Extension to signal vectors defined on (a submonoid of) $\mathbb{Z}^n$

Consider signal vectors $w : M \longrightarrow F$, where M is a finitely generated submonoid of $\mathbb{Z}^n$ (instead of $M = \mathbb{N}^n$), e.g. $M = \mathbb{Z}^n$.
Then w induces

$$w : F[M] \longrightarrow F\,,$$

where $F[M]$ is a finitely generated subalgebra of the algebra $F[s, s^{-1}]$ of Laurentpolynomials, e.g. $F[M] = F[s, s^{-1}]$.

Hence: extend theory of Gröbner bases to Laurent polynomials.

Pauer, F., Unterkircher, A.: Groebner Bases for Ideals in Laurent Polynomial Rings and their Application to Systems of Difference Equations. AAECC 9/4 (1999), 271-291.

Zerz,E., Oberst, U.: Acta Applicandae Mathematicae 31 (1993), 249-273.

References

Riquier, C.: Les Systèmes d'Équations aux Dérivées Partielles. Gauthier-Villars, Paris: 1910.

Oberst, U.: Multidimensional Constant Linear Systems. Acta Appl. Math. 20 (1990), 1-175.

Oberst, U., Pauer, F.: The Constructive Solution of Linear Systems of Partial Difference and Differential Equations with Constant Coefficients.
Multidim. Systems and Signal Processing 12 (2001), 253-308.