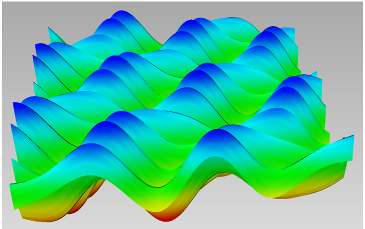
From moments to sparse representations, a geometric, algebraic and algorithmic viewpoint

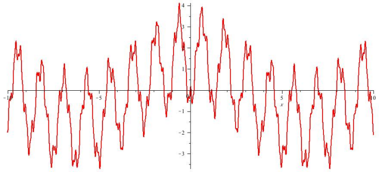
Bernard Mourrain
Inria Méditerranée, Sophia Antipolis
Bernard.Mourrain@inria.fr

Part I



Sparse representation of signals

Given a function or signal $f(t)$:



decompose it as

$$f(t) = \sum_{i=1}^{r'} (a_i cos(\mu_i t) + b_i sin(\mu_i t)) e^{\nu_i t} = \sum_{i=1}^{\mathbf{r}} \omega_{\mathbf{i}} e^{\zeta_{\mathbf{i}} t}$$

Prony's method (1795)

For the signal $f(t) = \sum_{i=1}^{\mathbf{r}} \omega_{\mathbf{i}} e^{\zeta_{\mathbf{i}} t}$, $(\omega_i, \zeta_i \in \mathbb{C})$,

- Evaluate f at $2\,r$ regularly spaced points: $\sigma_0 := f(0), \sigma_1 := f(1), \ldots$
- Compute a non-zero element $\mathbf{p} = [\mathbf{p_0}, \ldots, \mathbf{p_r}]$ in the kernel:

$$\begin{bmatrix} \sigma_0 & \sigma_1 & \ldots & \sigma_r \\ \sigma_1 & & & \sigma_{r+1} \\ \vdots & & & \vdots \\ \sigma_{r-1} & \ldots & \sigma_{2r-1} & \sigma_{2r-1} \end{bmatrix} \begin{bmatrix} p_0 \\ p_1 \\ \vdots \\ p_r \end{bmatrix} = 0$$

- Compute the roots $\xi_{\mathbf{1}} = \mathbf{e}^{\zeta_1}, \ldots, \xi_{\mathbf{r}} = \mathbf{e}^{\zeta_r}$ of $p(x) := \sum_{i=0}^{r} p_i x^i$.
- Solve the system

$$\begin{bmatrix} 1 & \ldots & \ldots & 1 \\ \xi_1 & & & \xi_r \\ \vdots & & & \vdots \\ \xi_1^{r-1} & \ldots & \ldots & \xi_r^{r-1} \end{bmatrix} \begin{bmatrix} \omega_{\mathbf{1}} \\ \omega_{\mathbf{2}} \\ \vdots \\ \omega_{\mathbf{r}} \end{bmatrix} = \begin{bmatrix} \sigma_0 \\ \sigma_1 \\ \vdots \\ \sigma_{r-1} \end{bmatrix}.$$

Symmetric tensor decomposition and Waring problem (1770)

Symmetric tensor decomposition problem:

Given a homogeneous polynomial ψ of degree d in the variables $\overline{\mathbf{x}} = (x_0, x_1, \ldots, x_n)$ with coefficients $\in \mathbb{K}$:

$$\psi(\overline{\mathbf{x}}) = \sum_{|\alpha|=d} \sigma_\alpha \binom{d}{\alpha} \overline{\mathbf{x}}^\alpha,$$

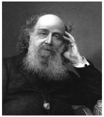
find a minimal decomposition of ψ of the form

$$\psi(\overline{\mathbf{x}}) = \sum_{i=1}^{r} \omega_i (\xi_{i,0}x_0 + \xi_{i,1}x_1 + \cdots + \xi_{i,n}x_n)^d$$

with $\xi_i = (\xi_{i,0}, \xi_{i,1}, \ldots, \xi_{i,n}) \in \overline{\mathbb{K}}^{n+1}$ spanning disctint lines, $\omega_i \in \overline{\mathbb{K}}$.

The minimal r in such a decomposition is called the **rank** of ψ.

Sylvester approach (1851)



Theorem

The binary form $\psi(x_0, x_1) = \sum_{i=0}^{d} \sigma_i \binom{d}{i} x_0^{d-i} x_1^i$ *can be decomposed as a sum of* r *distinct powers of linear forms*

$$\psi = \sum_{k=1}^{r} \omega_k (\alpha_{\mathbf{k}} x_0 + \beta_{\mathbf{k}} x_1)^d$$

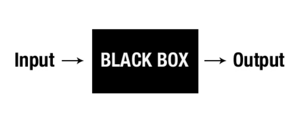
iff there exists a polynomial $p(x_0, x_1) := p_0 x_0^r + p_1 x_0^{r-1} x_1 + \cdots + p_r x_1^r$ *s.t.*

$$\begin{bmatrix} \sigma_0 & \sigma_1 & \dots & \sigma_r \\ \sigma_1 & & & \sigma_{r+1} \\ \vdots & & & \vdots \\ \sigma_{d-r} & \dots & \sigma_{d-1} & \sigma_d \end{bmatrix} \begin{bmatrix} p_0 \\ p_1 \\ \vdots \\ p_r \end{bmatrix} = 0$$

and of the form $p = c \prod_{k=1}^{r} (\beta_{\mathbf{k}} x_0 - \alpha_{\mathbf{k}} x_1)$ *with* $(\alpha_k : \beta_k)$ *distinct.*

Sparse interpolation

Given a black-box polynomial function $f(x)$



find what are the terms inside from output values.

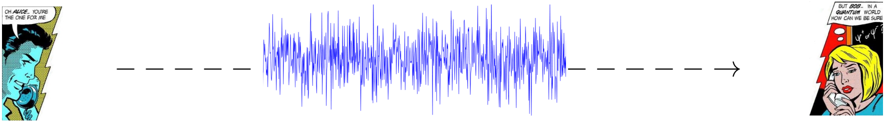
☞ Find $r \in \mathbb{N}, \omega_i \in \mathbb{C}, \alpha_i \in \mathbb{N}$ such that $f(x) = \sum_{i=1}^{r} \omega_i \, x^{\alpha_i}$.

- Choose $\varphi \in \mathbb{C}$
- Compute the sequence of terms $\sigma_0 = f(1), \ldots, \sigma_{2r-1} = f(\varphi^{2r-1})$;
- Construct the matrix $H = [\sigma_{i+j}]$ and its kernel $p = [p_0, \ldots, p_r]$ s.t.

$$\begin{bmatrix} \sigma_0 & \sigma_1 & \ldots & \sigma_r \\ \sigma_1 & & & \sigma_{r+1} \\ \vdots & & & \vdots \\ \sigma_{r-1} & \ldots & \sigma_{2r-1} & \sigma_{2r-1} \end{bmatrix} \begin{bmatrix} p_0 \\ p_1 \\ \vdots \\ p_r \end{bmatrix} = 0$$

- Compute the roots $\xi_{\mathbf{1}} = \varphi^{\alpha_1}, \ldots, \xi_{\mathbf{r}} = \varphi^{\alpha_{\mathbf{r}}}$ of $p(x) := \sum_{i=0}^{r} p_i x^i$ and deduce the exponents $\alpha_{\mathbf{i}} = \log_\varphi(\xi_{\mathbf{i}})$.
- Deduce the weights $W = [\omega_i]$ by solving $V_\Xi W = [\sigma_0, \ldots, \sigma_{r-1}]$ where V_Ξ is the Vandermonde system of the roots $\xi_1, \ldots, \xi_r$.

Decoding



An algebraic code:

$$E = \{c(f) = [f(\xi_1), \dots, f(\xi_m)] \mid f \in \mathbb{K}[x]; \deg(f) \le d\}.$$

Encoding messages using the dual code:

$$C = E^{\perp} = \{\mathbf{c} \mid \mathbf{c} \cdot [f(\xi_1), \dots, f(\xi_l)] = 0 \ \forall f \in V = \langle \mathbf{x}^{\mathbf{a}} \rangle \subset \mathbb{F}[\mathbf{x}]\}$$

Message received: $r = m + e$ for $m \in C$ where $e = [\omega_1, \dots, \omega_m]$ is an error with $\omega_j \neq 0$ for $j = i_1, \dots, i_r$ and $\omega_j = 0$ otherwise.

☞ **Find the error e.**

Berlekamp-Massey method (1969)

- Compute the syndrome $\sigma_k = c(x^k) \cdot r = c(x^k) \cdot e = \sum_{j=1}^{r} \omega_{i_j} \xi_{i_j}^k$.
- Compute the matrix

$$\begin{bmatrix} \sigma_0 & \sigma_1 & \dots & \sigma_r \\ \sigma_1 & & & \sigma_{r+1} \\ \vdots & & & \vdots \\ \sigma_{r-1} & \dots & \sigma_{2r-1} & \sigma_{2r-1} \end{bmatrix} \begin{bmatrix} p_0 \\ p_1 \\ \vdots \\ p_r \end{bmatrix} = 0$$

  and its kernel $p = [p_0, \dots, p_r]$.
- Compute the roots of the error locator polynomial $p(x) = \sum_{i=0}^{r} p_i \, x^i = p_r \prod_{j=1}^{r} (x - \xi_{i_j})$.
- Deduce the errors ω_{i_j}.

Simultaneous decomposition

Simultaneous decomposition problem

Given symmetric tensors $\psi_1, \dots, \psi_m$ of order $d_1, \dots, d_m$, find a simultaneous decomposition of the form

$$\psi_l = \sum_{i=1}^{r} \omega_{l,i} (\xi_{i,0} x_0 + \xi_{i,1} x_1 + \cdots + \xi_{i,n} x_n)^{d_l}$$

where $\xi_i = (\xi_{i,0}, \dots, \xi_{i,n})$ span distinct lines in $\overline{\mathbb{K}}^{n+1}$ and $\omega_{l,i} \in \overline{\mathbb{K}}$ for $l = 1, \dots, m$.

Proposition (One dimensional decomposition)

Let $\psi_l = \sum_{i=0}^{d_l} \sigma_{1,i} \binom{d_l}{i} x_0^{d_l - i} x_1^i \in \mathbb{K}[x_0, x_1]_{d_l}$ *for* $l = 1, \ldots, m$.
If there exists a polynomial $p(x_0, x_1) := p_0 x_0^r + p_1 x_0^{r-1} x_1 + \cdots + p_r x_1^r$ *s.t.*

$$\left[\begin{array}{cccc} \sigma_{1,0} & \sigma_{1,1} & \cdots & \sigma_{1,r} \\ \sigma_{1,1} & & & \sigma_{1,r+1} \\ \vdots & & & \vdots \\ \sigma_{1,d_1-r} & \cdots & \sigma_{1,d_1-1} & \sigma_{1,d_1} \\ \hline \vdots & & & \vdots \\ \hline \sigma_{m,0} & \sigma_{m,1} & \cdots & \sigma_{m,r} \\ \sigma_{m,1} & & & \sigma_{r+1} \\ \vdots & & & \vdots \\ \sigma_{m,d_m-r} & \cdots & \sigma_{m,d_m-1} & \sigma_{m,d_m} \end{array}\right] \left[\begin{array}{c} p_0 \\ p_1 \\ \vdots \\ p_r \end{array}\right] = 0$$

of the form $p = c \prod_{k=1}^{r} (\beta_k x_0 - \alpha_k x_1)$ *with* $[\alpha_k : \beta_k]$ *distinct, then*

$$\psi_l = \sum_{i=1}^{r} \omega_{i,l} (\alpha_l x_0 + \beta_l x_1)^{d_l}$$

for $\omega_{i,l} \in \overline{\mathbb{K}}$ *and* $l = 1, \ldots, m$.

Sequences, series, duality (1D)

Sequences: $\sigma = (\sigma_k)_{k\in\mathbb{N}} \in \mathbb{K}^{\mathbb{N}}$ indexed by $k \in \mathbb{N}$.

Formal power series:

$$\sigma(y) = \sum_{k=0}^{\infty} \sigma_k \frac{y^k}{k!} \in \mathbb{K}[[y]] \qquad \sigma(\mathbf{z}) = \sum_{\mathbf{k}=\mathbf{0}}^{\infty} \sigma_{\mathbf{k}} \, \mathbf{z}^{\mathbf{k}} \in \mathbb{K}[[\mathbf{z}]]$$

Linear functionals: $\mathbb{K}[x]^* = \{\Lambda : \mathbb{K}[x] \to \mathbb{K} \text{ linear}\}$.

Example:

- $p \mapsto$ coefficient of x^i in $p = \frac{1}{i!}\partial^i(p)(0)$
- $\mathfrak{e}_\zeta : p \mapsto p(\zeta)$.

Series as linear functionals: For $\sigma(y) = \sum_{k=0}^{\infty} \sigma_k \frac{y^k}{k!} \in \mathbb{K}[[y]]$ or $\sigma(z) = \sum_{k=0}^{\infty} \sigma_k z^k \in \mathbb{K}[[z]]$,

$$\sigma : p = \sum_k p_k x^k \mapsto \langle \sigma | p \rangle = \sum_k \sigma_k p_k$$

$(\frac{y^k}{k!})$ **(resp.** (z^k)**)** is the dual basis of the monomial basis $(x^k)_{k \in \mathbb{N}}$.

Example:

$$\mathfrak{e}_\zeta(y) = \sum_{k=0}^{\infty} \zeta^k \frac{y^k}{k!} = e^{\zeta y} \in \mathbb{K}[[y]] \quad \mathfrak{e}_\zeta(\mathbf{z}) = \sum_{k=0}^{\infty} \zeta^{\mathbf{k}} \mathbf{z}^{\mathbf{k}} = \frac{1}{1-\zeta \mathbf{z}} \in \mathbb{K}[[\mathbf{z}]]$$

Structure of $\mathbb{K}[x]$-module: $p \star \Lambda : q \mapsto \Lambda(p\, q)$.

$$\begin{aligned} x \star \sigma(y) &= \sum_{k=1}^{\infty} \sigma_k \frac{y^{k-1}}{(k-1)!} = \partial(\sigma(y)) \\ p(x) \star \sigma(y) &= p(\partial)(\sigma(y)) \end{aligned}$$

$$\mathbf{p}(\mathbf{x}) \star \sigma(\mathbf{z}) = \pi_+(\mathbf{p}(\mathbf{z}^{-1})(\sigma(\mathbf{z})))$$

Sequences, series, duality (nD)

Multi-index sequences: $\sigma = (\sigma_\alpha)_{\alpha\in\mathbb{N}^n} \in \mathbb{K}^{\mathbb{N}^n}$ indexed by $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$.

Taylor series:

$$\sigma(\mathbf{y}) = \sum_{\alpha\in\mathbb{N}^n} \sigma_\alpha \frac{\mathbf{y}^\alpha}{\alpha!} \in \mathbb{K}[[y_1, \ldots, y_n]] \qquad \sigma(\mathbf{z}) = \sum_{\alpha\in\mathbb{N}^n} \sigma_\alpha \mathbf{z}^\alpha \in \mathbb{K}[[\mathbf{z}_1, \ldots, \mathbf{z}_n]]$$

where $\alpha! = \prod \alpha_i!$ for $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}$.

Linear functionals: $\sigma \in R^* = \{\sigma : R \to \mathbb{K}, \textbf{ linear}\}$

$$\sigma : p = \sum_\alpha p_\alpha \mathbf{x}^\alpha \mapsto \langle \sigma | p \rangle = \sum_\alpha \sigma_\alpha p_\alpha$$

The coefficients $\langle \sigma | \mathbf{x}^\alpha \rangle = \sigma_\alpha \in \mathbb{K}$, $\alpha \in \mathbb{N}^n$ are called the **moments** of σ.

Structure of R-module: $\forall p \in R, \sigma \in R^*$, $p \star \sigma : q \mapsto \langle \sigma | p\, q \rangle$:

$$p \star \sigma = p(\partial_1, \ldots, \partial_n)(\sigma)(\mathbf{y}) \qquad \mathbf{p} \star \sigma = \pi_+(\mathbf{p}(\mathbf{z}_1^{-1}, \ldots, \mathbf{z}_n^{-1})\sigma(\mathbf{z}))$$

Symmetric tensor and apolarity

Apolar product: For $f = \sum_{|\alpha|=d} f_\alpha \binom{d}{\alpha} \overline{\mathbf{x}}^\alpha$, $g = \sum_{|\alpha|=d} g_\alpha \binom{d}{\alpha} \overline{\mathbf{x}}^\alpha \in \mathbb{K}[\overline{\mathbf{x}}]_d$,

$$\langle f, g \rangle_d = \sum_{|\alpha|=d} f_\alpha \, g_\alpha \binom{d}{\alpha}.$$

Property: $\langle f, (\xi_0 x_0 + \cdots + \xi_n x_n)^d \rangle = f(\xi_0, \ldots, \xi_n)$

Duality: For $\psi \in S_d$, we define $\psi^* \in S_d^* = \mathrm{Hom}_{\mathbb{K}}(S_d, \mathbb{K})$ as

$$\begin{aligned} \psi^* : S_d &\to \mathbb{K} \\ p &\mapsto \langle \psi, p \rangle_d \end{aligned}$$

Example: $((\xi_0 x_0 + \cdots + \xi_n x_n)^d)^* = \mathfrak{e}_\xi : p \in S_d \mapsto p(\xi)$ (evaluation at ξ)

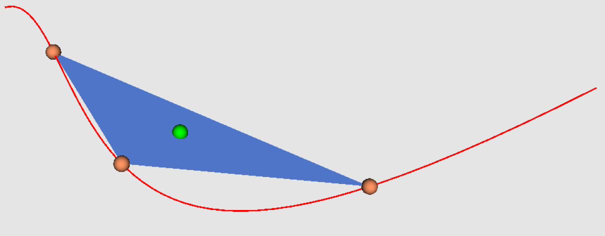
Dual symmetric tensor decomposition problem:

Given $\psi^* \in S_d^*$, find a decomposition of the form $\psi^* = \sum_{i=1}^r \omega_i \mathfrak{e}_{\xi_i}$ where $\xi_i = (\xi_{i,0}, \xi_{i,1}, \ldots, \xi_{i,n})$ span distinct lines in $\overline{\mathbb{K}}^{n+1}$, $\omega_i \in \overline{\mathbb{K}}$ ($\omega_i \neq 0$).

Symmetric tensors and secants

The evaluation $\mathfrak{e}_\xi \in S_d^*$ at $\xi \in \overline{\mathbb{K}}^{n+1}$ represented by the vector $(\xi^\alpha)_{|\alpha|=d}$ defines a point of the **Veronese** variety $\mathcal{V}_d^n \subset \mathbb{P}(S_d^*)$.

$\psi^* = \sum_{i=1}^r \omega_i \mathfrak{e}_{\xi_i}$ iff the corresponding point $[\psi^*]$ in $\mathbb{P}(S_d^*)$ is in the linear span of the evaluations $[\mathfrak{e}_{\xi_i}] \in \mathcal{V}_d^n$.



Let $S_r^o(\mathcal{V}_d^n) = \{[\psi^*] \in \mathbb{P}(S_d^*) \mid \psi^* = \sum_{i=1}^r \omega_i e_i \text{ with } [e_i] \in \mathcal{V}_d^n, \omega_i \in \mathbb{K}\}$.

The closure $S_r(\mathcal{V}_d^n) = \overline{S_r^o(\mathcal{V}_d^n)}$ is the **r^{th}-secant** of $\mathcal{V}_d^n$.

Dehomogeneization (aparté)

$$S = \mathbb{K}[x_0, \ldots, x_n] \qquad R = \mathbb{K}[x_1, \ldots, x_n]$$

$$\begin{array}{rcl} \iota_0 : p(x_0, \ldots, x_n) & \mapsto & p(1, x_1, \ldots, x_n) \\ x_0^{\deg(p)} p(\frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0}) & \leftarrow & p(x_1, \ldots, x_n) : h_0 \end{array}$$

Dual action

- $h_0^* : \sigma \in S_d^* \mapsto \sigma \circ h_0 \in R_{\leq d}^*$
- $\iota_0^* : \sigma \in R_{\leq d}^* \mapsto \sigma \circ \iota \in S_d^*$

$$\iota_0^*(\sigma(\mathbf{y}) + \mathcal{O}(\mathbf{y})^d) = [\mathfrak{e}_0\, \sigma(\mathbf{y})]_d$$

where $\mathfrak{e}_0 = \sum_i \frac{y_0^k}{k!}$.

For $I \subset R$, let $[\mathfrak{e}_0\, I^{\perp}]_*$ be the vector space of homogeneous components of $\mathfrak{e}_0\, \sigma(\mathbf{y})$ for $\sigma \in I^{\perp} \subset R^*$, then

$$[\mathfrak{e}_0\, I^{\perp}]_* = (J : x_0^*)^{\perp}$$

for any J such that $\iota_0(J) = I$ (e.g. $J = (I^{h_0})$).

Inverse systems

For I an ideal in $R = \mathbb{K}[\mathbf{x}]$,

$$I^{\perp} = \{\sigma \in R^* \mid \forall p \in I,\ \langle \sigma | p \rangle = 0\}.$$

- In $\mathbb{K}[[\mathbf{y}]]$, $I^{\perp}$ is stable by **derivations** with respect to y_i.
- **In $\mathbb{K}[[\mathbf{z}]]$, $I^{\perp}$ is stable by "division" by variables z_i.**

Inverse system generated by $\omega_1, \ldots, \omega_r \in \mathbb{K}[\mathbf{y}]$

$$\langle\langle \omega_1, \ldots, \omega_r \rangle\rangle = \langle \partial_{\mathbf{y}}^{\alpha}(\omega_i), \alpha \in \mathbb{N}^n \rangle \quad \text{resp. } \langle \pi_+(\mathbf{z}^{-\alpha}\omega_{\mathbf{i}}(\mathbf{z})), \alpha \in \mathbb{N}^{\mathbf{n}} \rangle$$

Example: $I = (x_1^2, x_2^2) \subset \mathbb{K}[x_1, x_2]$

$$I^{\perp} = \langle 1, y_1, y_2, y_1 y_2 \rangle = \langle\langle y_1 y_2 \rangle\rangle \quad \text{resp. } \langle \mathbf{1}, \mathbf{z_1}, \mathbf{z_2}, \mathbf{z_1 z_2} \rangle = \langle\langle \mathbf{z_1 z_2} \rangle\rangle$$

Dual of quotient algebra: for $\mathcal{A} = R/I$, $\mathcal{A}^* = I^{\perp}$.

Hankel operators

Hankel operator: For $\sigma = (\sigma_1, \ldots, \sigma_m) \in (R^*)^m$,

$$\begin{array}{rcl} H_\sigma : R & \to & (R^*)^m \\ p & \mapsto & (p \star \sigma_1, \ldots, p \star \sigma_m) \end{array}$$

σ is the **symbol** of H_σ.

Truncated Hankel operator: $V, W_1, \ldots, W_m \subset R$,

$$H_\sigma^{W,V} : p \in V \to ((p \star \sigma_i)_{|W_i})$$

Example: $V = \langle \mathbf{x}^\alpha, \alpha \in A\rangle = \langle \mathbf{x}^A\rangle, W = \langle \mathbf{x}^\beta, \beta \in B\rangle = \langle \mathbf{x}^B\rangle \subset R$, $\sigma \in R^*$,

$$H_\sigma^{A,B} = [\langle \sigma | \mathbf{x}^\alpha \mathbf{x}^\beta\rangle]_{\alpha \in A, \beta \in B} = [\sigma_{\alpha+\beta}]_{\alpha \in A, \beta \in B}.$$

Ideal:

$$\begin{aligned} I_\sigma = \ker H_\sigma &= \{p \in \mathbb{K}[\mathbf{x}] \mid p \star \sigma = 0\}, \\ &= \{p = \sum_\alpha p_\alpha \mathbf{x}^\alpha \mid \forall \beta \in \mathbb{N}^n \sum_\alpha p_\alpha \sigma_{\alpha+\beta} = 0\} \end{aligned}$$

Linear recurrence relations on the sequence $\sigma = (\sigma_\alpha)_{\alpha \in \mathbb{N}^n}$.

Quotient algebra: $\mathcal{A}_\sigma = R/I_\sigma$ ☞ **Studied case:** $\dim \mathcal{A}_\sigma < \infty$

Structure of an Artinian algebra $\mathcal{A}$

Definition: $\mathcal{A} = \mathbb{K}[\mathbf{x}]/I$ is **Artinian** if $\dim_{\mathbb{K}} \mathcal{A} < \infty$.

Hilbert nullstellensatz: $\mathcal{A} = \mathbb{K}[\mathbf{x}]/I$ Artinian $\Leftrightarrow \mathcal{V}_{\overline{\mathbb{K}}}(I) = \{\xi_1, \ldots, \xi_r\}$ is finite.

Assuming $\mathbb{K} = \overline{\mathbb{K}}$ is algebraically closed, we have

- $I = Q_1 \cap \cdots \cap Q_r$ where Q_i is m_{ξ_i}-primary where $\mathcal{V}_{\overline{\mathbb{K}}}(I) = \{\xi_1, \ldots, \xi_r\}$.
- $\mathcal{A} = \mathbb{K}[\mathbf{x}]/I = \mathcal{A}_1 \oplus \cdots \oplus \mathcal{A}_r$, with
  - $\mathcal{A}_i = \mathbf{u}_i\, \mathcal{A} \sim \mathbb{K}[x_1, \ldots, x_n]/Q_i$,
  - $\mathbf{u}_i^2 = \mathbf{u}_i$, $\mathbf{u}_i\, \mathbf{u}_j = 0$ if $i \neq j$, $\mathbf{u}_1 + \cdots + \mathbf{u}_r = 1$.
- $\dim R/Q_i = \mu_i$ is the multiplicity of ξ_i.

Structure of the dual $\mathcal{A}^*$

Sparse series:

$$\mathcal{P}ol\mathcal{E}xp = \left\{ \sigma(\mathbf{y}) = \sum_{i=1}^{r} \omega_i(\mathbf{y})\, \mathfrak{e}_{\xi_i}(\mathbf{y}) \mid \omega_i(\mathbf{y}) \in \mathbb{K}[\mathbf{y}], \right\}$$

where $\mathfrak{e}_{\xi_i}(\mathbf{y}) = e^{\mathbf{y}\cdot\xi_i} = e^{y_1\xi_{1,i}+\cdots+y_n\xi_{n,i}}$ with $\xi_{i,j} \in \mathbb{K}$.

Inverse system generated by $\omega_1, \ldots, \omega_r \in \mathbb{K}[\mathbf{y}]$

$$\langle\langle \omega_1, \ldots, \omega_r \rangle\rangle = \langle \partial_{\mathbf{y}}^{\alpha}(\omega_i), \alpha \in \mathbb{N}^n \rangle$$

Theorem

For $\mathbb{K} = \overline{\mathbb{K}}$ algebraically closed,

$$\mathcal{A}^* = \oplus_{i=1}^{r} \mathcal{D}_i\, \mathfrak{e}_{\xi_i}(\mathbf{y}) \quad \subset \quad \mathcal{P}ol\mathcal{E}xp$$

- $\mathcal{V}_{\overline{\mathbb{K}}}(I) = \{\xi_1, \ldots, \xi_r\}$
- $\mathcal{D}_i = \langle\langle \omega_{i,1}, \ldots, \omega_{i,l_i} \rangle\rangle$ *with* $\omega_{i,j} \in \mathbb{K}[\mathbf{y}]$, $Q_i^{\perp} = \mathcal{D}_i \mathfrak{e}_{\xi}$ *where* $I = Q_1 \cap \cdots \cap Q_r$
- $\mu(\omega_{i,1}, \ldots, \omega_{i,l_i}) := \dim_{\mathbb{K}}(\mathcal{D}_i) = \mu_i$ *multiplicity of* ξ_i.

The roots by eigencomputation

Hypothesis: $\mathcal{V}_{\mathbb{K}}(I) = \{\xi_1, \ldots, \xi_r\} \Leftrightarrow \mathcal{A} = \mathbb{K}[\mathbf{x}]/I$ Artinian.

$$\begin{array}{rcl} \mathcal{M}_a : \mathcal{A} & \to & \mathcal{A} \\ u & \mapsto & a\,u \end{array} \qquad \begin{array}{rcl} \mathcal{M}_a^{\mathsf{t}} : \mathcal{A}^* & \to & \mathcal{A}^* \\ \Lambda & \mapsto & a \star \Lambda = \Lambda \circ \mathcal{M}_a \end{array}$$

Theorem

- *The eigenvalues of $\mathcal{M}_a$ are $\{a(\xi_1), \ldots, a(\xi_r)\}$.*
- *The eigenvectors of all $(\mathcal{M}_a^{\mathsf{t}})_{a \in \mathcal{A}}$ are (up to a scalar) $\mathbf{e}_{\xi_i} : p \mapsto p(\xi_i)$.*

Proposition

If the roots are simple, the operators $\mathcal{M}_a$ are diagonalizable. Their common eigenvectors are, up to a scalar, interpolation polynomials $\mathbf{u}_i$ at the roots and idempotent in $\mathcal{A}$.

Example

Roots of polynomial systems

$$\left\{ \begin{array}{lcl} f_1 & = & x_1^2 x_2 - x_1^2 \\ f_2 & = & x_1 x_2 - x_2 \end{array} \right. \qquad I = (f_1, f_2) \subset \mathbb{C}[\mathbf{x}]$$

$$\mathcal{A} = \mathbb{C}[\mathbf{x}]/I \equiv \langle 1, x_1, x_2 \rangle \quad I = (x_1^2 - x_2, x_1 x_2 - x_2, x_2^2 - x_2)$$

$$M_1 = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix}, \quad M_2 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 1 & 1 \end{pmatrix} \quad \begin{array}{c} \text{common} \\ \text{eigvecs of} \\ M_1^t, M_2^t \end{array} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$$

$$I = Q_1 \cap Q_2 \quad \text{where} \quad Q_1 = (x_1^2, x_2), \quad Q_2 = \mathbf{m}_{(1,1)} = (x_1 - 1, x_2 - 1)$$

$$I = Q_1^\perp \oplus Q_2^\perp \quad Q_1^\perp = \langle 1, y_1 \rangle = \langle 1, y_1 \rangle\, \mathfrak{e}_{(0,0)}(\mathbf{y}) \quad Q_2^\perp = \langle 1 \rangle\, \mathfrak{e}_{(1,1)}(\mathbf{y}) = \langle e^{y_1 + y_2} \rangle$$

Solution of partial differential equations (with constant coeff.)

$$\left\{ \begin{array}{lcl} \partial_{y_1}^2 \partial_{y_2} \sigma - \partial_{y_1}^2 \sigma & = & 0 \\ \partial_{y_1} \partial_{y_2} \sigma - \partial_{y_2} \sigma & = & 0 \end{array} \right. \qquad \begin{array}{l} f_1 \star \sigma = 0 \\ f_2 \star \sigma = 0 \end{array} \quad \Rightarrow \quad \sigma \in I^\perp = Q_1^\perp \oplus Q_2^\perp$$

$$\sigma = a + b\, y_1 + c\, e^{y_1 + y_2} \quad a, b, c \in \mathbb{C}$$

References

Gaspard Riche Baron de Prony.
Essai expérimental et analytique: Sur les lois de la dilatabilité de fluides élastiques et sur celles de la force expansive de la vapeur de l'alcool, à différentes températures.
J. Ecole Polyt., 1:24–76, 1795.

Michael Ben-Or and Prasoon Tiwari.
A deterministic algorithm for sparse multivariate polynomial interpolation.
In *Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing*, pages 301–309. ACM, 1988.

Elwyn R. Berlekamp.
Nonbinary BCH decoding.
IEEE Transactions on Information Theory, 14(2):242–242, 1968.

Leopold Kronecker.
Zur Theorie der Elimination Einer Variabeln aus Zwei Algebraischen Gleichungen.
Monatsber. Königl. Preussischen Akad. Wies. (Berlin), pages 535–600., 1881.

James Massey.
Shift-register synthesis and BCH decoding.
IEEE transactions on Information Theory, 15(1):122–127, 1969.

James Joseph Sylvester.
Essay on Canonical Form.
The collected mathematical papers of J. J. Sylvester, Vol. I, Paper 34, Cambridge University Press. 1909 (XV und 688). G. Bell, London, 1851.

Richard Zippel.
Probabilistic Algorithms for Sparse Polynomials.
In *Proceedings of the International Symposiumon on Symbolic and Algebraic Computation*, EUROSAM '79, pages 216–226, London, UK, 1979. Springer-Verlag.