Solving and bonding 0-dimensional ideals: Moeller Algorithm and Macaulay Bases

ACA2018

Santiago de Compostela

Duality

Notation

$\mathcal{P} := k[X_1, \ldots, X_n]$,

$\mathcal{T} := \{X_1^{a_1} \cdots X_n^{a_n} : (a_1, \ldots, a_n) \in \mathbb{N}^n\}$, $<$ term-order on $\mathcal{T}$,

$f = \sum_{\tau \in \mathcal{T}} c(f, \tau)\tau \in \mathrm{Span}_k(\mathcal{T}) = \mathcal{P}$,

$\mathbf{T}(f) := \max_{<}\{\tau \in \mathcal{T} : c(f, \mathbf{T}(f)) \neq 0\}$, $\mathrm{lc}(f) := c(f, \mathbf{T}(f))$.

$\mathsf{I} \subset \mathcal{P}$ a (zero)-dimensional ideal,

$\mathbf{T}(\mathsf{I}) := \{\mathbf{T}(f) : f \in \mathsf{I}\}$ a monomial ideal,

$\mathbf{N}(\mathsf{I}) := \mathcal{T} \setminus \mathbf{T}(\mathsf{I})$ an order ideal,

$k[\mathbf{N}(\mathsf{I})] := \mathrm{Span}_k(\mathbf{N}(\mathsf{I}))$.

It holds

1. $\mathcal{P} \cong \mathsf{I} \oplus k[\mathbf{N}(\mathsf{I})]$;
2. $\mathcal{P} \setminus \mathsf{I} \cong k[\mathbf{N}(\mathsf{I})]$;
3. for each $f \in \mathcal{P}$, there is a unique

$$g := \mathrm{Can}(f, \mathsf{I}, <) = \sum_{t \in \mathbf{N}(\mathsf{I})} \gamma(f, t, <) t \in k[\mathbf{N}(\mathsf{I})]$$

   such that $f - g \in \mathsf{I}$.

$\mathcal{P}^* := \mathrm{Hom}(\mathcal{P}, k)$ is made a $\mathcal{P}$-module defining
$\forall \ell \in \mathcal{P}^*, f \in \mathcal{P}$, $\ell \cdot f \in \mathcal{P}^*$ as

$$(\ell \cdot f)(g) := \ell(fg), \ \forall g \in \mathcal{P}.$$

$\mathbb{L} = \{\ell_1, \ldots, \ell_r\} \subset \mathcal{P}^*$ and $\mathbf{q} = \{q_1, \ldots, q_s\} \subset \mathcal{P}$ are said to

- **triangular** if

  $r = s$ and $\ell_i(q_j) = 0$, for each $i < j$;

- **biorthogonal** if

  $$r = s \text{ and } \ell_i(q_j) = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \neq j. \end{cases}$$

For each k-vector subspace $L \subset \mathcal{P}^*$, let

$$\mathfrak{P}(L) := \{g \in \mathcal{P} : \ell(g) = 0, \forall \ell \in L\}$$

and, for each k-vector subspace $P \subset \mathcal{P}$, let

$$\mathfrak{L}(P) := \{\ell \in \mathcal{P}^* : \ell(g) = 0, \forall g \in P\}.$$

$\rightarrow$ **duality between $\mathfrak{P}$ and $\mathfrak{L}$!**

$\mathbb{L} := \{\ell_1, \ldots, \ell_r\} \subset \mathcal{P}^*$ a linearly independent set of k-linear functionals such that

$L := \mathrm{Span}_k(\mathbb{L})$ $\mathcal{P}$-**module** so that $\mathsf{I} := \mathfrak{P}(L)$ **0-dim. ideal**;

$\mathbf{N}(\mathsf{I}) := \{t_1, \ldots, t_r\}$,

$\mathbf{q} := \{q_1, \ldots, q_r\} \subset k(\mathbf{N}(\mathsf{I})) \subset \mathcal{P}$ the set triangular to $\mathbb{L}$, obtained via Moeller's Algorithm;

$\left(q_{ij}^{(h)}\right) \in k^{r^2}, 1 \leq k \leq r$ the matrices defined by

$$X_h q_i = \sum_j q_{ij}^{(h)} q_j \text{ mod } \mathsf{I}$$

$\Lambda := \{\lambda_1, \ldots, \lambda_r\}$ the set biorthogonal to $\mathbf{q}$, which can be trivially deduced by Gaussian reduction

Then

$$X_h \lambda_j = \sum_{i=1}^{r} q_{ij}^{(h)} \lambda_i, \forall i, j, h.$$

Closure

Let

$\mathrm{m} := (X_1, \ldots, X_n)$ be the maximal at the origin;

$\mathrm{I} \subset \mathcal{P}$ an ideal;

the m-**closure** of I is the ideal $\bigcap_d \mathrm{I} + \mathrm{m}^d$;

I is m-**closed** iff $\mathrm{I} = \bigcap_d \mathrm{I} + \mathrm{m}^d$;

For each $\tau \in \mathcal{T}$, denote $M(\tau) : \mathcal{P} \to k$ the morphism defined by

$$M(\tau) = c(f, \tau), \forall f = \sum_{t \in \mathcal{T}} c(f, t) t \in \mathcal{P}.$$

Denoting $\mathbb{M} := \{M(\tau) : \tau \in \mathcal{T}\}$ for all

$$f := \sum_{t \in \mathcal{T}} a_t t \in \mathcal{P} \text{ and } \ell := \sum_{\tau \in \mathcal{T}} c_\tau M(\tau) \in k[[\mathbb{M}]] \cong \mathcal{P}^*$$

it holds $\ell(f) = \sum_{t \in \mathcal{T}} a_t c_t$.

Macaulay Bases

Let $<$ be a standard ordering on $\mathcal{T}$ and let $\mathsf{I} \subset \mathcal{P}$ an m-closed ideal. Denoted $\mathrm{Can}(t, \mathsf{I}, <) =: \sum_{\tau \in \mathbf{N}_<(\mathsf{I})} \gamma(t, \tau, <)\tau \in k[[\mathbf{N}_<(\mathsf{I})]]$ and, $\forall \tau \in \mathbf{N}_<(\mathsf{I})$ $\ell(\tau) := M(\tau) + \sum_{t \in \mathbf{T}_<(\mathsf{I})} \gamma(t, \tau, <) M(t) \in k[\mathbb{M}]$, then

$$\mathfrak{M}(\mathsf{I}) = \mathrm{Span}_k\{\ell(\tau), \tau \in \mathbf{N}_<(\mathsf{I})\}.$$

The set $\{\ell(\tau), \tau \in \mathbf{N}_<(\mathsf{I})\}$ is called the **Macaulay Basis** of I. There is an algorithm which, given a finite basis (not necessarily Gröbner/standard) of an m-primary ideal I, computes its Macaulay Basis. It becomes an *infinite procedure* which, given a finite basis of an ideal $\mathsf{I} \subset \mathsf{m}$, returns the infinite Macaulay Basis of its m-closure.

Moeller's algorithm

→ Moeller algorithm vs Buchberger–Moeller algorithm

- B-M is iterative on terms; Moeller iterates on functionals
- Moeller is claimed to be more efficient
- in particular (Lundqvist) B-M pays the need of testing monomial divisions
- M is iterative (thus is extending the ideal when new functionals are considered)
- the classical version (soft-M) applies to a set of functionals
- under a suitable assumption with the same complexity a stronger version (hard-M) returns infos for a *Macaulay chain* of ideals

soft-Moeller

Let $\mathbb{L} = \{\ell_1, \ldots, \ell_s\} \subset \mathcal{P}^*$ be a (not necessarily linearly indipendent) set of k-linear functionals such that $L := \mathrm{Span}_k(\mathbb{L})$ is a $\mathcal{P}$-module, and let us denote, for each $f \in \mathcal{P}$,

$$v(f, \mathbb{L}) := (\ell_1(f), \ldots, \ell_s(f)) \in k^s.$$

Since $\dim_k(L) < \infty$ then $\mathsf{I} := \mathfrak{P}(L)$ is a zero-dimensional ideal and

$$\#(\mathbf{N}(\mathsf{I})) = \deg(\mathsf{I}) = \dim_k(L) =: r \leq s.$$

Denote $\mathbf{N}(\mathsf{I}) = \{t_1, \ldots, t_r\}$, and let us consider the $s \times r$ matrix $\ell_i(t_j)$ *whose columns* are the vectors $v(t_j, \mathbb{L})$ and *are linearly independent*, since any relation $\sum_j c_j v(t_j, \mathbb{L}) = 0$ would imply

$$\ell_i(\sum_j c_j t_j) = \sum_j c_j \ell_i(t_j) = 0 \text{ and } \sum_j c_j t_j \in \mathfrak{P}(L) = \mathsf{I}$$

contradicting the definition of $\mathbf{N}(\mathsf{I})$.

The matrix $\ell_i(t_j)$ has rank $r \leq s$ and it is possible to extract an ordered subset

$$\Lambda := \{\lambda_1, \dots, \lambda_r\} \subset \mathbb{L}, \quad \mathrm{Span}_k\{\Lambda\} = \mathrm{Span}_k\{\mathbb{L}\}$$

and to re-enumerate the terms in $\mathbf{N}(\mathsf{I})$ in such a way that *each principal minor* $\lambda_i(t_j), 1 \leq i, j \leq \sigma \leq r$ *is invertible*.

Therefore, if we consider a set $\mathbf{q} := \{q_1, \ldots, q_r\} \subset \mathcal{P}$ which is *triangular* w.r.t. Λ, and (a_{ij}) denotes the invertible matrix s.t.

$$q_i = \sum_{j=1}^{r} a_{ij} t_j, \forall i \leq r,$$

then for each $\sigma \leq r$

- $\{q_1, \ldots, q_\sigma\}$ and $\{\lambda_1, \ldots, \lambda_\sigma\}$ are triangular;
- $\mathrm{Span}_k\{t_1, \ldots, t_\sigma\} = \mathrm{Span}_k\{q_1, \ldots, q_\sigma\}$;
- (a_{ij}) is lower triangular.

hard-Moeller

If we now further assume that

1. $\dim_k(L) = r = s$ and
2. each sub-vector space $L_\sigma := \mathrm{Span}_k(\{\ell_1, \dots, \ell_\sigma\})$ is a $\mathcal{P}$-module

so that

3. each $\mathsf{I}_\sigma = \mathfrak{P}(L_\sigma)$ is a zero-dimensional ideal

   and

4. there is a *Macaulay chain* $\mathsf{I}_1 \supset \mathsf{I}_2 \supset \cdots \supset \mathsf{I}_s = \mathsf{I}$,

then

- $\lambda_\sigma = \ell_\sigma, \forall\sigma$
- $\mathbf{N}(\mathsf{I}_\sigma) = \{t_1, \dots, t_\sigma\}$ is an order ideal $\forall\sigma$
- $\mathsf{I}_\sigma \oplus \mathrm{Span}_k\{q_1, \dots, q_\sigma\} = \mathcal{P}, \forall\sigma$
- $\mathbf{T}(q_\sigma) = t_\sigma, \forall\sigma.$

Theorem (soft-Möller)

Let $\mathcal{P} := k[X_1, \ldots, X_n]$, *and* $<$ *be any termordering. Let* $\mathbb{L} = \{\ell_1, \ldots, \ell_s\} \subset \mathcal{P}^*$ *be a set of* k*-linear functionals such that* $\mathfrak{P}(\mathrm{Span}_k(\mathbb{L}))$ *is a zero-dimensional ideal. Then there are*

- *an integer* $r \in \mathbb{N}$,
- *an order ideal* $\mathbf{N} := \{t_1, \ldots, t_r\} \subset \mathcal{T}$,
- *an ordered subset* $\Lambda := \{\lambda_1, \ldots, \lambda_r\} \subset \mathbb{L}$,
- *an ordered set* $\mathbf{q} := \{q_1, \ldots, q_r\} \subset \mathcal{P}$,

such that, denoting $L := \mathrm{Span}_k(\mathbb{L})$ *and* $\mathsf{I} := \mathfrak{P}(L)$, *it holds:*

- $r = \deg(\mathsf{I}) = \dim_k(\mathbb{L})$,
- $\mathbf{N}(\mathsf{I}) = \mathbf{N}$,
- $\mathrm{Span}_k(\Lambda) = \mathrm{Span}_k(\mathbb{L})$,
- $\mathrm{Span}_k\{t_1, \ldots, t_\sigma\} = \mathrm{Span}_k\{q_1, \ldots, q_\sigma\}, \forall \sigma \leq r$,
- $\{q_1, \ldots, q_\sigma\}$, $\{\lambda_1, \ldots, \lambda_\sigma\}$ *are triangular,* $\forall \sigma \leq r$.

Theorem (hard-Möller)

If, moreover, denoting $L := \mathrm{Span}_k(\mathbb{L})$ *and* $\mathsf{I} := \mathfrak{P}(L)$, *we have*

- $\dim_k(L) = r = s$ *and*
- $L_\sigma := \mathrm{Span}_k(\{\ell_1, \dots, \ell_\sigma\})$ *is a* $\mathcal{P}$*-module,* $\forall \sigma$,

then it further holds

- $\lambda_\sigma = \ell_\sigma$,
- $\mathbf{N}(\mathsf{I}_\sigma) = \{t_1, \dots, t_\sigma\}$ *is an order ideal,*
- $\mathsf{I}_\sigma \oplus \mathrm{Span}_k\{q_1, \dots, q_\sigma\} = \mathcal{P}$,
- $\mathbf{T}(q_\sigma) = t_\sigma$.

for each $\sigma \leq r$, *where* $\mathsf{I}_\sigma = \mathfrak{P}(L_\sigma)$.

DeGroebnerization

Yes of course the computation returns also the *irrelevant Grobner basis* of each I_σ which is the worst-way to compute normal-form. Lundqvist gave 4 approaches with good complexity for computing normal form of the finite radical 0-dimensional ideal given by a set of points

1. through a family of separators deduced by a witness matrix
2. introducing an *allgemaine* coordinate Y and represent the ideal as

$$g(Y), X_1 - g_1(Y), \cdots, X_n - g_n(Y), \deg(g_i) < \deg(g)$$

   better to use RUR
3. using the monomial basis deduced by Lex-Game/Bar-Code ($\rightarrow$ Ceria)
4. apply the preliminary steps of Moeller algorithm to deduce (á la Auzinger-Stetter) a partition of the variables as

$$\{X_1, \ldots, X_n\} = \{Z_1, \ldots, Z_\nu\} \sqcup \{Y_1, \ldots, Y_{n-\nu}\}$$

   and polynomial

$$h_i \in k[Y_1, \ldots, Y_{n-\nu}], 1 \leq i \leq \nu : Z_i - h_i \in \mathsf{I}$$

Robbiano in St.Petersburg: what for a 0-dimensional non-radical ideal?

1. via Marinari-M. formulation of Cerlienco-Mureddu to this case
2. hopefully we can use an *allgemaine* coordinate w.r.t. which each primary is curvilinear
3. via Marinari-M. formulation of Cerlienco-Mureddu to this case
4. Moeller algorithm is still available

For each $\mathsf{a} \in \mathsf{Z} := \mathcal{Z}(\mathsf{I})$

- $\lambda_{\mathsf{a}} : \mathcal{P} \mapsto \mathcal{P}$ the translation $\lambda_{\mathsf{a}}(X_i) = X_i + a_i, \forall i$,
- $\mathfrak{m}_{\mathsf{a}} = (X_1 - a_1, \ldots, X_n - a_n)$,
- $\mathfrak{q}_{\mathsf{a}}$ the $\mathfrak{m}_{\mathsf{a}}$-primary component of I,
- $\Lambda_{\mathsf{a}} := \mathfrak{M}(\lambda_{\mathsf{a}}(\mathfrak{q}_{\mathsf{a}})) \subset \mathrm{Span}_k(\mathbb{M})$,
- $\{\ell_{\upsilon\mathsf{a}} : \upsilon \in \mathbf{N}_<(\lambda_{\mathsf{a}}(\mathfrak{q}_{\mathsf{a}}))\}$ is the enumerated Macaulay basis of Λ_{a},

$\pi_m(\ell(\tau)) = (\sigma_{X_m^{d_m}\cdots X_n^{d_n}}(\ell(\tau)))(X_1^{-1},\ldots,X_m^{-1},0,\ldots,0) \in k[X_1,\ldots,X_m]$.
$\lambda_{\mathsf{a}} : \mathcal{P} \mapsto \mathcal{P}$ the translation $\lambda_{\mathsf{a}}(X_i) = X_i + a_i, \forall i$
For $\lambda = \ell_{\upsilon\mathsf{a}}\lambda_{\mathsf{a}}$ we set

$$\pi_m(\lambda) := \pi_m(\ell_{\upsilon\mathsf{a}}\lambda_{\mathsf{a}}) := \pi_m(\ell_{\upsilon\mathsf{a}})\lambda_{\pi_m(\mathsf{a})}.$$

with

$$\sigma_j(M(\tau)) := \sigma_{X_j}(M(\tau)) = \begin{cases} M(\omega) \text{ if } \tau = X_j\omega \\ 0 \text{ if } X_j \nmid \tau \end{cases} \qquad \forall\ \tau \in \mathcal{T};$$

Degré zéro de Moeller

Roland Barthes
Le Degré zéro de l'écriture,
Éditions du Seuil, 1953

Degré zéro

A reformulation of Möller algorithm removing all irrelevant political *décombres*:

- V a $\mathbb{K}$-vectorspace
- $v_1, v_2, v_3, \ldots$ an ordered basis of V
- $V^\star := \mathrm{Hom}_\mathbb{K}(V, \mathbb{K})$
- $\lambda_1, \lambda_2, \lambda_3, \ldots,$ an ordered sequence of *functionals* in $V^\star$ not necessarily linearly independent.
- $L_k := \{v \in V : \lambda_i(v) = 0, i \leq k\}$

Produce a set $w_1, w_2, \ldots \in V$ which is *triangular* w.r.t. $\{\lambda_i, i \leq k\}$ and at least a vector $u \in L_k$

$$\begin{array}{c|cccc|c} & \lambda_1 & \lambda_2 & \cdots & \lambda_k & \lambda_{k+1} \\ \hline w_1 & 1 & \star & \cdots & \star & \star \\ w_2 & 0 & 1 & \ddots & \vdots & \vdots \\ \vdots & \vdots & \ddots & \ddots & \star & \star \\ w_k & 0 & \cdots & 0 & 1 & \star \\ \hline u_1 & 0 & \cdots & \cdots & 0 & ? \\ \vdots & \vdots & \ddots & \ddots & \vdots & \vdots \\ u_r & 0 & \cdots & \cdots & 0 & ? \end{array}$$

If all ? are 0

- pick the next vector,
- evaluate it,
- reduce it via $w_1, \dots, w_k$ obtaining v
- if $\lambda_{k+1}(v) \neq 0$ set $w_{k+1} := v$ else set $u_{r+1} := v$

until $\lambda_{k+1}(v) \neq 0$.

How to grant termination?

Consider n linear operators $\mathfrak{X}_1, \ldots, \mathfrak{X}_n \in \mathrm{Hom}_{\mathbb{K}}(V, V)$ and to each functional $\lambda : V \to \mathbb{K}$ and each i associates the functional

$$\lambda^{(i)} \in \mathrm{Hom}_{\mathbb{K}}(V, \mathbb{K}) = V^\star : V \xrightarrow{\mathfrak{X}_i} V \xrightarrow{\lambda} \mathbb{K}$$

Thus each $\mathfrak{X}_i$ defines a lin. op. $\mathfrak{X}_i \in \mathrm{Hom}_{\mathbb{K}}(V^\star, V^\star)$

$$\mathfrak{X}_i : V^\star \to V^\star : \lambda \mapsto \lambda^{(i)}$$

Moreover $\mathfrak{X}_1, \ldots, \mathfrak{X}_n$ generate a (not necessarily commutative) $\mathbb{K}-$algebra $\mathfrak{A}$ $\mathbb{K}\langle \mathfrak{X}_1, \ldots, \mathfrak{X}_n \rangle \twoheadrightarrow \mathfrak{A} \subset \mathrm{Hom}_{\mathbb{K}}(V, V)$

Under these definitions

- V is a left $\mathfrak{A}$-module;
- $V^\star$ is a right $\mathfrak{A}$-module.

Mourrain: B-connection

- $B := \mathrm{Span}_{\mathbb{K}}(b_1, \ldots, b_s) \subset V$ a subvectorspace
- $\bar{B} := \{b_1, \ldots, b_s\} \cup \{\mathfrak{X}_j(b_i) 1 \leq j \leq n, 1 \leq i \leq s\}$
- $B_0 := B$
- $B_{i+1} := \{v_0 + \sum_{j=1}^{n} \mathfrak{X}_j(v_j) : v_j \in B_i, 0 \leq j \leq n\}$ for each $i \in \mathbb{N}$

A subvectorspace $W \subset V$ is *B-connected* if

$$\forall w \in W \exists i : w \in B_i$$

If V is B-connected then
$\lambda(v) = 0 \forall v \in \bar{B} \implies \lambda(v) = 0 \forall v \in V$

$$\mathfrak{X}_1(\lambda_{8x+a}) = (-1)^a \lambda_{8x+a+1},\ 0 \le a \le 7$$

$$\mathfrak{X}_2(\lambda_{8x+4a+b}) = (-1)^a \lambda_{8x+4a+4+b},\ 0 \le a \le 3,\ 0 \le b \le 1$$

$$\mathfrak{X}_3(\lambda_{8x+a}) = \begin{cases} \lambda_{8x+a+2},\ a \in \{0,1,4,5\}, \\ -\lambda_{8x+a-2},\ a \in \{2,3,6,7\} \end{cases}$$

$$\mathfrak{X}_4(\lambda_{8x+a}) = \lambda_{8x+a+8},\ 0 \le a \le 7$$

$$\mathfrak{X}_1(\lambda_{8x+a}) = (-1)^a \lambda_{8x+a+1},\ 0 \leq a \leq 7$$

$$\mathfrak{X}_2(\lambda_{8x+4a+b}) = (-1)^a \lambda_{8x+4a+4+b},\ 0 \leq a \leq 3,\ 0 \leq b \leq 1$$

$$\mathfrak{X}_3(\lambda_{8x+a}) = \begin{cases} \lambda_{8x+a+2},\ a \in \{0,1,4,5\}, \\ -\lambda_{8x+a-2},\ a \in \{2,3,6,7\} \end{cases}$$

$$\mathfrak{X}_4(\lambda_{8x+a}) = \lambda_{8x+a+8},\ 0 \leq a \leq 7$$

$\mathbb{O}[x]$

Next episode: The Revenge of Macaulay