Next episode:
Möller vs Buchberger

Spear's Theorem

$$\mathcal{B} := \{\omega \in \langle \overline{\mathbf{V}} \rangle : \mathcal{I}_\omega \neq R\} \subset \left\{ v\omega : v \in \langle \overline{\mathbf{v}} \rangle, \omega \in \langle \overline{\mathbf{V}} \rangle \right\}$$

$$\mathbf{T}(\cdot) : \mathcal{A}^u \mapsto \mathcal{B}^{(u)} : f \to \mathbf{T}(f)$$

$$(\Gamma, \circ), \mathcal{B} \subset \Gamma \subset \langle \overline{\mathbf{V}} \rangle,$$

The associated Γ-graded ring $\mathcal{G} = G(\mathcal{A})$ coincides as a **set** with $\mathcal{A}$ and this is sufficient to smoothly export Buchberger test/completion. **But** $\mathcal{G} = G(\mathcal{A})$ and $\mathcal{A}$ do not coincide as **rings**: the multiplication $\star$ of $\mathcal{A}$ does not coincide with $*$, the one of $\mathcal{G}$. However an old slogan stated that in order to provide a Buchberger Algorithm on $\mathcal{A}$, one **just needs to modify, in the algorithm for $\mathcal{G}$, the multiplication procedure!**

$\mathcal{A} = \mathcal{Q}/\mathcal{I}$ is an effectively given left R-module, endowed with its natural Γ-pseudovaluation $\mathbf{T}(\cdot)$ where the semigroup $(\Gamma, \circ)$ satisfies

- $\mathcal{B} \subset \Gamma \subset \langle \overline{\mathbf{V}} \rangle$ and
- the restriction of $<$ on Γ is a semigroup ordering.

We denote:

- $\mathcal{G} = G(\mathcal{A})$,
- $\star$ the multiplication of $\mathcal{A}$,
- $*$ the one of $\mathcal{G}$.

Arithmetics of $\mathcal{A}$ and $G(\mathcal{A})$

Denote $\mathcal{G} = G(\mathcal{A})$, $\star$ the multiplication of $\mathcal{A}$, $*$ the one of $\mathcal{G}$.

1. For each term $\tau \in \mathcal{B} \subset \Gamma$ there are an automorphism $\alpha_\tau : R \to R$ and an α_τ-derivation $\theta_\tau : R \to R$ so that for each $r \in R$, $t \star r = \alpha_t(r)t + \theta_t(r)$ and $t * r = \alpha_t(r)t$.
2. For two terms $\tau_1, \tau_2 \in \mathcal{B} \subset \Gamma$, there are elements $\varpi(\tau_2, \tau_1) \in R$ and $\Delta(\tau_2, \tau_1) \in \mathcal{A}, \mathbf{T}(\Delta(\tau_2, \tau_1)) < \tau_2 \circ \tau_1$ such that $\tau_2 \star \tau_1 = \varpi(\tau_2, \tau_1)\tau_2 \circ \tau_1 + \Delta(\tau_2, \tau_1)$ and $\tau_2 * \tau_1 = \mathcal{L}(\tau_2 \star \tau_1) = \varpi(\tau_2, \tau_1)\tau_2 \circ \tau_1$.
3. $c_u\tau_u * c_v\tau_v = c_u\alpha_{\tau_u}(c_v)\varpi(\tau_u, \tau_v)\tau_u \circ \tau_v$.

Arithmetics of $\mathcal{A}$ and $G(\mathcal{A})$

Pesch, Nguefack–Pola

$$\mathcal{A} = \mathcal{R}\langle X_1, \dots, X_n, Y_1, \dots, Y_m\rangle / \mathcal{I}$$

$$X_j * X_i = a_{ij} X_i X_j, \quad Y_l * X_j = b_{jl} X_j^{e_i - 1} X_j Y_l, \; Y_k * Y_l = c_{lk} Y_l Y_k$$

where a_{ij}, b_{jl}, c_{lk} are invertible elements in $\mathcal{R}$, $e_i \in \mathbb{N}^*$.

3. $c_u\tau_u * c_v\tau_v = c_u\alpha_{\tau_u}(c_v)\varpi(\tau_u, \tau_v)\tau_u \circ \tau_v$.
4. $\alpha_{\tau_u} = \mathrm{Id}$
5. $\tau_u \circ \tau_v = \Upsilon(\tau_u, \tau_v)\tau_u\tau_v$,
   $\Upsilon(\tau_u, \tau_v) \in \{X_1^{d_1} \cdots X_n^{d_n} \mid (d_1, \dots, d_n) \in \mathbb{N}^n\}$;
6. $c_u\tau_u * c_v\tau_v = c_u\alpha_{\tau_u}(c_v)\varpi(\tau_u, \tau_v)\Upsilon(\tau_u, \tau_v)\tau_u\tau_v =$
   $\varpi(\tau_u, \tau_v)\Upsilon(\tau_u, \tau_v) \cdot c_u\tau_u \cdot c_v\tau_v$.

BUCHBERGER

Some Buchberger Theory

For any set $F \subset \mathcal{A}^m$ we denote, in function of $<$:

- $\mathbb{I}_2(F) \subset \mathcal{A}^m$ the twosided ideal generated by F,
- $\mathbf{T}\{F\} := \{\mathbf{T}(f) : f \in F\} \subset \mathcal{B}^{(m)}$;
- $\mathbf{M}\{F\} := \{\mathbf{M}(f) : f \in F\} \subset \mathrm{M}(\mathcal{A}^m)$.
- $\mathbf{T}_2(F) := \mathbb{I}_2(\mathbf{T}\{F\}) = \{\mathbf{T}(\lambda \star f \star \rho) : \lambda, \rho \in \mathcal{B}, f \in F\} = \{\lambda \circ \mathbf{T}(f) \circ \rho : \lambda, \rho \in \mathcal{B}, f \in F\} \subset \mathcal{B}^{(m)}$;
- $\mathbf{M}_2(F) := \{\mathbf{M}(a\lambda \star f \star b\rho) : a \in R_\lambda \setminus \{0\}, b \in R_\rho \setminus \{0\}, \lambda, \rho \in \mathcal{B}, f \in F\} = \{m * \mathbf{M}(f) * n : m, n \in \mathrm{M}(\mathcal{A}), f \in F\} \subset \mathrm{M}(\mathcal{A}^m)$,

In general Buchberger Theory of left, right, $\mathcal{A}$-bilateral (or: twosided), restricted Gröbner bases is formulated stating notations, definitions and properties and proving results only for the twosided case leaving to the reader the task of **adapting** them properly specializing some data and trivially simplifying the argument.
Alternatively, one could state and prove the theory only in the left case, since right, twosided and restricted Gröbner bases can be considered, respectively, as left Gröbner basis in the **opposite algebra** $\mathcal{A}^{\mathrm{op}}$, in the enveloping algebras $\mathcal{A} \otimes_R \mathcal{A}^{\mathrm{op}}$ and $R \otimes_R \mathcal{A}^{\mathrm{op}}$.
We follow the former approach.
Further **restricted** bases can be seen as **left** bases in the algebra $\mathcal{A}$ endowed with the multiplication $\diamond$, thus giving a strong improvement on my algorithm.

We specialize each

TWOSIDED EXPRESSION

$$a\lambda \star f \star b\rho : a \in R_\lambda \setminus \{0\}, b \in R_\rho \setminus \{0\}, \lambda, \rho \in \mathcal{B}, f \in F$$

to the other cases by setting

LEFT EXPRESSION $b = 1, \rho = 1$, obtaining

$$a\lambda \star f : a \in R_\lambda \setminus \{0\}, \lambda \in \mathcal{B}, f \in F$$

RIGHT EXPRESSION $a = 1, \lambda = 1$, obtaining

$$f \star b\rho : b \in R_\rho \setminus \{0\}, \rho \in \mathcal{B}, f \in F$$

RESTRICTED EXPRESSION $b = 1, \lambda = 1$, obtaining

$$af \star \rho = a\rho \diamond f : a \in R \setminus \{0\}, \rho \in \mathcal{B}, f \in F.$$

Gröbner Bases

$$f = \sum_{i=1}^{s} c(f, t_i)t_i : c(f, t_i) \in \mathbb{Z} \setminus \{0\}, t_i \in \langle \overline{\mathbf{z}} \rangle, t_1 > \cdots > t_s.$$

Gröbner Bases

$$f = \sum_{i=1}^{s} c(f, t_i)t_i : c(f, t_i) \in \mathbb{Z} \setminus \{0\}, t_i \in \langle \overline{\mathbf{Z}} \rangle, t_1 > \cdots > t_s.$$

$$\mathbf{T}(f) := t_1, \mathrm{lc}(f) := c(f, t_1), \mathbf{M}(f) := c(f, t_1)t_1.$$

Gröbner Bases

$$f = \sum_{i=1}^{s} c(f, t_i)t_i : c(f, t_i) \in \mathbb{Z} \setminus \{0\}, t_i \in \langle \overline{\mathbf{Z}} \rangle, t_1 > \cdots > t_s.$$

$$\mathbf{T}(f) := t_1, \mathrm{lc}(f) := c(f, t_1), \mathbf{M}(f) := c(f, t_1)t_1.$$

Pan: $XY = 3X \cdot Y - X \cdot 2Y \in \mathbb{I}(3X, 2Y)$

Let M $\subset \mathcal{A}^m$ be a (left, right, bilateral) $\mathcal{A}$-module. $F \subset$ M will be called

Gröbner Bases

$$f = \sum_{i=1}^{s} c(f, t_i)t_i : c(f, t_i) \in \mathbb{Z} \setminus \{0\}, t_i \in \langle \overline{\mathbf{Z}} \rangle, t_1 > \cdots > t_s.$$

$$\mathbf{T}(f) := t_1, \mathrm{lc}(f) := c(f, t_1), \mathbf{M}(f) := c(f, t_1)t_1.$$

Pan: $XY = 3X \cdot Y - X \cdot 2Y \in \mathbb{I}(3X, 2Y)$

Let M $\subset \mathcal{A}^m$ be a (left, right, bilateral) $\mathcal{A}$-module. $F \subset$ M will be called

a (left, right, bilateral) *Gröbner basis* of M if F satisfies the following condition:

- for each $f \in$ M, there are $g_i \in F$, $\lambda_i, \rho_i \in \mathcal{B}, a_i \in R_{\lambda_i} \setminus \{0\}, b_i \in R_{\rho_i} \setminus \{0\}$ such that
  - $\mathbf{T}(f) = \lambda_i \circ \mathbf{T}(g_i) \circ \rho_i$ for all i,
  - $\mathbf{M}(f) = \sum_i a_i\lambda_i * \mathbf{M}(g_i) * b_i\rho_i$;

Gröbner Bases

$$f = \sum_{i=1}^{s} c(f, t_i)t_i : c(f, t_i) \in \mathbb{Z} \setminus \{0\}, t_i \in \langle \overline{\mathbf{Z}} \rangle, t_1 > \cdots > t_s.$$

$$\mathbf{T}(f) := t_1, \mathrm{lc}(f) := c(f, t_1), \mathbf{M}(f) := c(f, t_1)t_1.$$

Pan: $XY = 3X \cdot Y - X \cdot 2Y \in \mathbb{I}(3X, 2Y)$

Let M $\subset \mathcal{A}^m$ be a (left, right, bilateral) $\mathcal{A}$-module. $F \subset$ M will be called

a (left, right, bilateral) *strong Gröbner basis* of I if F satisfies the following equivalent conditions

- for each $f \in$ M there is $g \in F$ such that $\mathbf{M}(g) \mid \mathbf{M}(f)$,
- for each $f \in$ M there are $g \in F$, $\lambda, \rho \in \mathcal{B}, a \in R_\lambda \setminus \{0\}, b \in R_\rho \setminus \{0\}$, such that

$$\mathbf{T}(f) = \lambda \circ \mathbf{T}(g) \circ \rho \text{ and } \mathbf{M}(f) = a\lambda * \mathbf{M}(g) * b\rho.$$

FIGURE: Twosided Normal Form Algorithms

$(g, \sum_{i=1}^{\mu} a_i\lambda_i \star g_i \star b_i\rho_i)$:= **BilateralNormalForm**(f, F)

where

$f \in \mathcal{A}^m$, $F \subset \mathcal{A}^m$,

$g \in \mathcal{A}^m$ is a twosided **normal form** of f w.r.t. F.

$g_i \in F$, $\lambda_i, \rho_i \in \mathcal{B}$, $a_i \in R_{\lambda_i} \setminus \{0\}$, $b_i \in R_{\rho_i} \setminus \{0\}$,

$f - g = \sum_{i=1}^{\mu} a_i\lambda_i \star g_i \star b_i\rho_i$ is a twosided **Gröbner representation** in terms of F,

$g := f, \mu := 0$,

While $\mathbf{M}(g) \in \mathbf{M}\{\mathbb{I}_2(\mathbf{M}\{F\})\}$ **do**

Choose $g_i \in F, \lambda_i, \rho_i \in \mathcal{B}, a_i \in R_{\lambda_i} \setminus \{0\}, b_i \in R_{\rho_i} \setminus \{0\}$:

$\mathbf{T}(g) = \lambda_i \circ \mathbf{T}(g_i) \circ \rho_i, \mu < i \leq \nu$,

$\mathbf{M}(g) = \sum_{i=\mu+1}^{\nu} a_i\lambda_i * \mathbf{M}(g_i) * b_i\rho_i$,

- $g := g - \sum_{i=\mu+1}^{\nu} a_i\lambda_i \star g_i \star b_i\rho_i$, $\mu := \nu$.

Denote $F := \{g_1, \ldots, g_u\} \subset \mathcal{A}^m$, $g_i = \mathbf{M}(g_i) - p_i =: c_i\tau_i\mathbf{e}_{\iota_i} - p_i$; since $a\lambda * c\tau * b\rho = a\alpha_\lambda(c)\varpi(\lambda,\tau)\alpha_{\lambda\circ\tau}(b)\varpi(\lambda\circ\tau,\rho)\lambda\circ\tau\circ\rho$, the computations to be performed for the monomial $\mathbf{M}(f) = d\omega$ are

WEAK TWOSIDED CASE

- compute finite triples $(\lambda_i, g_i, \rho_i) : \lambda_i \circ \tau_i \circ \rho_i = \omega$,
- compute elements d_i, e_i :

$$c = \sum_i d_i\Big(\alpha_\lambda(c_i)\varpi(\lambda_i,\tau_i)\varpi(\lambda_i\circ\tau_i,\rho_i)\Big)e_i$$

- set $a_i := d_i, b_i := \alpha^{-1}_{\lambda_i\circ\tau_i}(e_i)$

STRONG TWOSIDED CASE

- compute $i, 1 \le i \le u$, $\lambda, \rho : \lambda \circ \tau_i \circ \rho = \omega$,
- compute

  $d, e : c = d\Big(\alpha_\lambda(c_i)\varpi(\lambda,\tau_i)\varpi(\lambda\circ\tau_i,\rho)\Big)e$
- set $a := d, b := \alpha^{-1}_{\lambda\circ\tau_i}(e)$

MÖLLER

Moeller Lifting Theorem

Given a finite set

$$F := \{g_1, \ldots, g_u\} \subset \mathcal{A}^m, g_i = \mathbf{M}(g_i) - p_i =: a_i \tau_i \mathbf{e}_{\iota_i} - p_i,$$

we denote M the module $M := \mathbb{I}(F)$ endowed with its natural pseudovaluation.

Buchberger

A generating set F is a Gröbner basis if and only if each S-polynomial has 0 as normal form.

Möller

A generating set F is a Gröbner basis if and only if each element in a *Gebauer–Möller set* i.e. minimal basis of the syzygies among the leading monomials $\{\mathbf{M}(f_\alpha) : f_\alpha \in F\}$ lifts, via Buchberger reduction, to a syzygy among the elements of F.

$\hat{R} := \{a \in R : ah = a \star h = h \star a, \text{ for each } h \in \mathcal{A}\}$

We impose on the twosided $\mathcal{A}$-module $\left(\mathcal{A} \otimes_{\hat{R}} \mathcal{A}^{\mathrm{op}}\right)^u$, with canonical basis denoted by $\{e_1, \ldots, e_u\}$ and whose generic element has the shape

$\sum_i a_i \lambda_i e_{l_i} b_i \rho_i, \lambda_i, \rho_i \in \mathcal{B}, a_i \in R_{\lambda_i} \setminus \{0\}, b_i \in R_{\rho_i} \setminus \{0\}, l_i \leq u$, the $\Gamma^{(m)}$-*pseudovaluation* $w : \left(\mathcal{A} \otimes_{\hat{R}} \mathcal{A}^{\mathrm{op}}\right)^u \to \Gamma^{(m)}$ which, on each element $\sigma := \sum_i a_i \lambda_i e_{l_i} b_i \rho_i \in \left(\mathcal{A} \otimes_{\hat{R}} \mathcal{A}^{\mathrm{op}}\right)^u \setminus \{0\}$ is defined as $w(\sigma) := \max_{<}\{\lambda_i \circ \mathbf{T}(g_{l_i}) \circ \rho_i\} = \max_{<}\{\lambda_i \circ \tau_{l_i} \circ \rho_i \mathbf{e}_{\iota_{l_i}}\} =: \delta\epsilon$, $\epsilon \in \{\mathbf{e_1}, ..., \mathbf{e_m}\}$, $\delta \in \Gamma$, so that $G\left(\left(\mathcal{A} \otimes_{\hat{R}} \mathcal{A}^{\mathrm{op}}\right)^u\right) = \left(G\left(\mathcal{A} \otimes_{\hat{R}} \mathcal{A}^{\mathrm{op}}\right)\right)^u = \left(\mathcal{G} \otimes_{\hat{R}} \mathcal{G}^{\mathrm{op}}\right)^u$ and its corresponding $\Gamma^{(m)}$-homogeneous *leading form* is

$$\mathcal{L}_2(\sigma) := \sum_{h \in H} a_h \lambda_h e_{l_h} b_h \rho_h \in \left(\mathcal{G} \otimes_{\hat{R}} \mathcal{G}^{\mathrm{op}}\right)^u$$

where $H := \{h : \lambda_h \circ \tau_{l_h} \circ \rho_h \mathbf{e}_{\iota_{l_h}} = v(\sigma) = \delta\epsilon\}$.

We also denote, for each set $S \subset \left(\mathcal{A} \otimes_{\hat{R}} \mathcal{A}^{\mathrm{op}}\right)^u$,

$$\mathcal{L}_2\{S\} := \{\mathcal{L}(g) : g \in S\} \subset \left(\mathcal{A} \otimes_{\hat{R}} \mathcal{A}^{\mathrm{op}}\right)^u.$$

We can therefore consider the morphisms

$$\mathfrak{s}_2 : \left(\mathcal{G} \otimes_{\hat{R}} \mathcal{G}^{\mathrm{op}}\right)^u \to \mathcal{G}^m \textbf{ and } \mathfrak{S}_2 : \left(\mathcal{A} \otimes_{\hat{R}} \mathcal{A}^{\mathrm{op}}\right)^u \to \mathcal{A}^m$$

defined as

$$\begin{aligned} \mathfrak{s}_2\left(\sum_i a_i\lambda_i e_{l_i} b_i\rho_i\right) &:= \sum_i a_i\lambda_i * \mathbf{M}(g_{l_i}) * b_i\rho_i, \\ \mathfrak{S}_2\left(\sum_i a_i\lambda_i e_{l_i} b_i\rho_i\right) &:= \sum_i a_i\lambda_i \star g_{l_i} \star b_i\rho_i. \end{aligned}$$

If $u \in \ker(\mathfrak{s}_2)$ is $\Gamma^{(m)}$-homogeneous and $U \in \ker(\mathfrak{S}_2)$ is such that $u = \mathcal{L}_2(U)$, we say that u *lifts* to U, or U is a *lifting* of u, or simply u *has a lifting*.

A twosided *Gebauer–Möller set* for F is any $\Gamma^{(m)}$-homogeneous basis of $\ker(\mathfrak{s}_2)$.

A set $B \subset M$ is called a *standard basis* of M if $\mathbb{I}(\mathcal{L}\{B\}) = \mathbb{I}(\mathcal{L}\{M\})$.

Statement of Lifting Theorem

With the present notation and denoting $\mathfrak{GM}(F)$ any Gebauer–Möller set for F, the following conditions are equivalent:

1. F is a Gröbner basis of $M := \mathbb{I}_2(F)$;
2. $f \in M \iff f$ has a Gröbner representation in terms of F;
4. each $\sigma \in \mathfrak{GM}(F)$ has a lifting $\mathrm{lift}(\sigma_2)$;
5. each $\Gamma^{(m)}$-homogeneous element $u \in \ker(\mathfrak{s})$ has a lifting $\mathrm{lift}(u)$;

and implies

6. $\{\mathrm{lift}(\sigma) : \sigma \in \mathfrak{GM}(F)\}$ is a standard basis of $\ker(\mathfrak{S}_2)$.

Gebauer–Möller set vs. Buchberger Criteria

Preserving and ordering the S-pairs to be processed is the main problem of Buchberger Algorithm; it is well extablished that substituting Gebauer–Möller set in place of Buchberger Criteria is a must. In a non trivial case-study, where 3 binomials $\{g_1, g_2, g_3\}$ in 5 variables produce up to 5 more elements, next g_9 kills 2 redundant bases elements; g_{11} kills 2 redundant bases elements more and finally g_{12} removes g_{10}, the required basis being thus

$$\{g_1, g_2, g_3, g_4, g_9, g_{11}, g_{12}\},$$

Buchberger criteria approach requires to store up to **23** elements, while the Gebauer–Möller set approach stores at most **8** elements (in the crucial loop introducing g_9; note that Buchberger criteria approach **stores always at least 8 elements after the third loop** introducting g_6).

	2	3	4	5	6	7	8	9	10	11	12		26
useful			1	2	3	4	5	6	7	8	9		9
crit1									5	15	16	24	24
crit2				2		3		4	5		6	11	11
useless					1		2		6	9	11	17	17
S-pairs			2	1	4	6	11	15	12	7	12	0	
S-pairs			5	5	**9**	**12**	**18**	**23**	**21**	**17**	**23**		
	2	3	4	5	6	7	8	9	10	11	12		27
useful			1	2	3	4	5	6	7	8	9		9
redundant								1		3			3
useless				1		2		3	7	10	12	18	18
S-pairs		0	1	1	3	4	5	4	3	0	2	0	
S-pairs	0	2	3	4	6	6	7	**8**	6	5	6		