Oracle-supported drawing of the Groebner *escalier*

Maria Emilia Alonso, Maria Grazia Marinari, Teo Mora

Oracle-supported drawing of the Gröbner *escalier*

Maria Emilia Alonso
Depto. Algebra. Fac.CC. Matemáticas
Universidad Complutense de Madrid
m_alonso@mat.ucm.es

Maria Grazia Marinari
DIMA
Università di Genova
marinari@dima.unige.it

Teo Mora
DISI
Università di Genova
theomora@disi.unige.it

June 16, 2010

The aim of this note is to discuss the following quite queer

Problem 1 *Given*

- *the free non-commutative polynomial ring,* $\mathcal{P} := \mathbb{F}\langle X_1, \ldots, X_n\rangle$ (public),
- *a bilateral ideal* $\mathsf{I} \subset \mathbb{F}\langle X_1, \ldots, X_n\rangle$ (private),
- *a finite set* $G := \{g_1, \ldots, g_l\} \subset \mathsf{I}$ *of elements of the ideal* I (public),
- *a noetherian semigroup term-ordering* $\prec$, (private), *on the word semigroup* $\mathcal{T} := \langle X_1, \ldots, X_n\rangle$,

compute

> *a finite subset* $H \subset \Gamma(\mathsf{I})$ *of the Gröbner basis* $\Gamma(\mathsf{I})$ *of* I *w.r.t.* $\prec$ *s.t., for each* $g_i \in G$ *its* normal form $NF(g_i, H)$ *w.r.t.* H *is zero,*

by means of a finite number of queries to an oracle, which

> *given a term* $\tau \in \mathcal{T}$ *returns its* canonical form $\mathrm{Can}(\tau, \mathsf{I}, \prec)$ *w.r.t. the ideal* I *and the term-ordering* $\prec$. □

This queer problem has been suggested to us by [2] where a similar problem, but with stronger assumptions, is faced in order to set up a chosen-cyphertext attack against the cryptographic system proposed in [10][1].

The formulation of Problem 1 is partially due to the underlying application but is also due to the structure of the Gröbner bases in the non-commutative

[1] Though we will breefly report on this application in Appendix we are not interested in dealing with it, preferring to refer to the recent survey [7].

setting, which in general are infinite; however, even if we restrict to the noetherian setting of the (commutative) polynomial ring $\mathcal{P} := \mathbb{F}[X_1, \ldots, X_n]$, we are unable (as we will show through easy counterexamples) to produce an algorithm which allows to return the (while finite) Gröbner basis of I, unless we have some further informations allowing to bound such basis; the best we can do is to solve the following reformulation:

Problem 2 *Given*

- *the commutative polynomial ring,* $\mathcal{P} := \mathbb{F}[X_1, \ldots, X_n]$,
- *an ideal* $\mathsf{I} \subset \mathbb{F}[X_1, \ldots, X_n]$,
- *a noetherian semigroup term-ordering* $\prec$ *on the set of terms*

$$\mathcal{T} := \{X_1^{a_1} \ldots X_n^{a_n}, (a_1, \ldots, a_n) \in \mathbb{N}^n\},$$

- *a degree bound of the elements of the Gröbner basis* $\Gamma(\mathsf{I})$ *of* I *w.r.t.* $\prec$, i.e. *a value* $D \in \mathbb{N}$ *satisfying* $D \geq d(\mathsf{I}) := \max\{\deg(\gamma_i) : \gamma_i \in \Gamma(\mathsf{I})\}$,

compute

- *the Gröbner basis* $\Gamma(\mathsf{I})$ *of* I *w.r.t.* $\prec$,

by means of a finite number of queries to an oracle, which

- *given a term* $\tau \in \mathcal{T}$ *returns its* canonical form $\mathrm{Can}(\tau, \mathsf{I}, \prec)$ *w.r.t. the ideal* I *and the term-ordering* $\prec$. □

After recalling the basic notions and set up the notation (Section 1) we solve first Problem 1 (Section 2) and next Problem 2 (Section 3) for which we propose a different, more combinatiorial, solution.

We want to thank T. Moriarty and R.F. Ree for their precious apport.

1 Notation and recalls on Gröbner Bases

We consider a (non-necessarily commutative) monoid $\mathcal{T}$ generated by the set of variables $\{X_1, \ldots, X_n\}$, a field $\mathbb{F}$ and the monoid-ring $\mathcal{P} := \mathrm{Span}_{\mathbb{F}}(\mathcal{T})$.
For any set $F \subset \mathcal{P}$ we denote $\mathsf{I} \subset \mathcal{P}$ the (bilateral) ideal generated by F.
Each $f \in \mathcal{P}$ can be uniquely expressed as

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

and we call *support* of f the set $\mathrm{supp}(f) := \{\tau \in \mathcal{T} : c(f, \tau) \neq 0\}$.
Moreover, fixing a noetherian semigroup ordering $\prec$ on $\mathcal{T}$, the *leading term*, *leading coefficient* and *leading monomial* of f are ordinately:

$$\mathbf{T}(f) := \max_{\prec}\{\tau \in \mathrm{supp}(f)\},\ \mathrm{lc}(f) := c(f, \mathbf{T}(f))\ \text{ and }\ \mathbf{M}(f) := \mathrm{lc}(f)\mathbf{T}(f).$$

For each ideal $\mathsf{I} \subset \mathcal{P}$, we also consider

- the *semigroup ideal* $\mathbf{T}(\mathsf{I}) := \{\mathbf{T}(f) : f \in \mathsf{I}\}$,
- the *Gröbner sous-escalier* $\mathbf{N}(\mathsf{I}) := \mathcal{T} \setminus \mathbf{T}(\mathsf{I})$,
- the vector-space $\mathbb{F}[\mathbf{N}(\mathsf{I})] := \mathrm{Span}_{\mathbb{F}}(\mathbf{N}(\mathsf{I}))$,
- $\mathbf{G}(\mathsf{I}) \subset \mathbf{T}(\mathsf{I})$ the unique minimal basis of $\mathbf{T}(\mathsf{I})$.

We recall that for $f \in \mathcal{P}$ and $G \subset \mathcal{P}$,

- f has *Gröbner representation* in terms of G if

$$f = \sum_{i=1}^{\mu_f} c_i \lambda_i g_{j_i} \rho_i, \ c_i \in \mathbb{F} \setminus \{0\}, \lambda_i, \rho_i \in \mathcal{T}, g_{j_i} \in G, \mu_f \in \mathbb{N}$$

  with $\mathbf{T}(f) = \lambda_1 \mathbf{T}(g_{j_1})\rho_1 \succ \cdots \succ \lambda_i \mathbf{T}(g_{j_i})\rho_i \succ \cdots$.

- $h := NF(f, G, \prec) \in \mathcal{P}$ is a *normal form* of f w.r.t. G, if
  - $f - h \in \mathbb{I}(G)$ has a Gröbner representation in terms of G and
  - $h \neq 0 \implies \mathbf{T}(h) \notin \{\lambda \mathbf{T}(g)\rho : \lambda, \rho \in \mathcal{T}, g \in G\} =: \mathbf{T}(G)$.
- For each $f \in \mathcal{P}$, there is a unique *canonical form*

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

  s.t. $f - g \in \mathsf{I}$.
- A Gröbner basis of I is any set $\Gamma \subset \mathsf{I}$ s.t. $\{\mathbf{T}(\gamma) : \gamma \in \Gamma\}$ generates $\mathbf{T}(\mathsf{I})$.
- The *reduced Gröbner basis* of I is the set

$$\{\tau - \mathrm{Can}(\tau, \mathsf{I}, \prec) : \tau \in \mathbf{G}(\mathsf{I})\}.$$

2 Oracle-supported Approximation of $\Gamma(\mathsf{I})$

Let us now specialize $\mathcal{T}$ to be the word semigroup $\mathcal{T} := \langle X_1, \ldots, X_n \rangle$ so that in particular the following holds:

- for each term $v \in \mathcal{T}$ and variables X_l, X_r we have by definition

$$X_l v X_r \in \mathbf{G}(\mathsf{I}) \iff X_l v \in \mathbf{N}(\mathsf{I}), v X_r \in \mathbf{N}(\mathsf{I}), X_l v X_r \in \mathbf{T}(\mathsf{I}); \quad (1)$$

- for each term $v \in \mathcal{T}$ and each variable X we have

$$\omega = vX \in \mathbf{N}(\mathsf{I}) \implies v \in \mathbf{N}(\mathsf{I}), \ \omega = Xv \in \mathbf{N}(\mathsf{I}) \implies v \in \mathbf{N}(\mathsf{I}). \quad (2)$$

If we ask our oracle the value of $\mathrm{Can}(\tau, \mathsf{I}, \prec)$[2] for any term $\tau \in \mathcal{T}$, we can deduce whether

1. $\tau \in \mathbf{T}(\mathsf{I})$ in which case we obtain also $\mathrm{Can}(\tau, \mathsf{I}, \prec)$, or
2. $\tau \in \mathbf{N}(\mathsf{I})$ *i. e.* $\tau = \mathrm{Can}(\tau, \mathsf{I}, \prec)$.

Procedure 3 *We are assuming of having the sets*

$$\mathrm{supp}(g_j), g_j \in G,$$

so that, without needing to know the term-ordering $\prec$, we can deduce the sets

$$T_j := \{\tau \in \mathrm{supp}(g_j) : \tau \nmid \omega, \forall \omega \in \mathrm{supp}(g_j)\}.$$

Since for each j, there are $\tau \in T_j, \lambda, \rho \in \mathcal{T} : \tau = \lambda \mathbf{T}(f)\rho$ for some $f \in \Gamma(\mathsf{I})$ e.g. $\tau := \mathbf{T}(g_j) \in \mathbf{T}(\mathsf{I})$*, we can produce a scheme, based on Equation (1), which in a finite number of steps produces an element of $\Gamma(\mathsf{I})$; we choose the most suitable set T_j then repeatedly we*

- *pick an element $\tau \in T_j$, if $\tau \notin \mathbf{T}(\mathsf{I})$, simply remove it, otherwise:*
- *for $\tau = X_l\omega \in \mathbf{T}(\mathsf{I})$ we test whether $\omega \in \mathbf{T}(\mathsf{I})$ in which case we set $\tau := \omega$ and repeat until we have an element $\tau = X_l\omega \in \mathbf{T}(\mathsf{I})$ for which $\omega \in \mathbf{N}(\mathsf{I})$;*
- *now, for $\omega = \upsilon X_r \in \mathbf{N}(\mathsf{I})$ we test whether $X_l\upsilon \in \mathbf{T}(\mathsf{I})$, in which case we set $\omega := \upsilon \in \mathbf{N}(\mathsf{I})$ and repeat until we have an element $X_l\upsilon X_r$ for which*

  $$X_l\upsilon \in \mathbf{N}(\mathsf{I}), \upsilon X_r \in \mathbf{N}(\mathsf{I}), X_l\upsilon X_r \in \mathbf{T}(\mathsf{I})$$

  id est $X_l\upsilon X_r \in \mathbf{G}(\mathsf{I})$.

Remarking that we also have

$$\mathbf{G}(\mathsf{I}) \ni X_l\upsilon X_r \mid \tau \in \mathrm{supp}(g_j),$$

we can solve Problem 1 by a repeated application of the scheme above as follows: set $H := \emptyset$ and repeatedly

- *apply the scheme above thus obtaining an element $\tau \in \mathbf{G}(\mathsf{I})$ and the polynomial* $\mathrm{Can}(\tau, \mathsf{I}, \prec)$*,*
- *set $H := H \cup \{\tau - \mathrm{Can}(\tau, \mathsf{I}, \prec)\}$, $G := \{NF(g, H) : g \in G\}$*

until $G = \{0\}$.

At termination, which is granted by noetherianity, the set H satisfies the conditions required in Problem 1.

Clearly, in the non-commutative case, where in general Gröbner bases are infinite, we can not hope to produce the whole basis of I.

[2] Or, in order to mask our question — see the discussion on Bulygin assumption (B2) in the Appendix, — the values of $\mathrm{Can}(l_\iota \tau r_\iota, \mathsf{I}, \prec)$ where $l_\iota, r_\iota \in \mathcal{P}$ satisfy $\tau = \sum_\iota l_\iota \tau r_\iota$, so that

$$\mathrm{Can}(\tau, \mathsf{I}, \prec) = \sum_\iota \mathrm{Can}(l_\iota \tau r_\iota, \mathsf{I}, \prec).$$

3 Oracle-supported Deduction of $\Gamma(\mathsf{I})$ (commutative case)

We begin by observing that also in the commutative case $\mathcal{P} = \mathbb{F}[X_1, \ldots, X_n]$, with $\deg(X_i) = 1, \forall\, 1 \leq i \leq n$, a strong solution returning the complete basis of an ideal $\mathsf{I} \subset \mathcal{P}$ can not be produced, unless further knowledge is assumed: in fact, given $\mathsf{I} \subset \mathbb{F}[X_1, \ldots, X_n]$ and a value $\delta \in \mathbb{N}, \delta < d(\mathsf{I})$, in general there are smaller ideals (see Remark 5) $\mathsf{J} \subsetneqq \mathsf{I}$ which satisfy

$$\{f \in \mathsf{I} : \deg(f) \leq \delta\} = \{f \in \mathsf{J} : \deg(f) \leq \delta\}.$$

We recall the following definitions and facts:

- For any $\tau \in \mathcal{T}, 1 \leq i \leq n$ the *X_i-th predecessor of τ* is $\frac{\tau}{X_i}$ if $X_i \mid \tau$, otherwise we say that τ does not have X_i-th predecessor.
- $\mathbf{B}(\mathsf{I}) \subset \mathbf{T}(\mathsf{I})$, the *border of the ideal*, is defined by
  $\mathbf{B}(\mathsf{I}) := \{\tau \in \mathbf{T}(\mathsf{I}) \,:\, \exists\, 1 \leq i \leq n, \frac{\tau}{X_i} \in \mathbf{N}(\mathsf{I})\}$,
- $\mathbf{J}(\mathsf{I}) \subset \mathbf{T}(\mathsf{I})$ the *interior of the ideal*, is defined by
  $\mathbf{J}(\mathsf{I}) := \{\tau \in \mathbf{T}(\mathsf{I}) \,:\, \forall\, 1 \leq i \leq n, \frac{\tau}{X_i} \in \mathbf{T}(\mathsf{I})\}$, and
- the unique minimal basis of $\mathbf{T}(\mathsf{I})$, $\mathbf{G}(\mathsf{I}) \subset \mathbf{B}(\mathsf{I})$, is characterized as
  $\mathbf{G}(\mathsf{I}) := \{\tau \in \mathbf{B}(\mathsf{I}) \,:\, \forall\, 1 \leq i \leq n, \frac{\tau}{X_i} \in \mathbf{N}(\mathsf{I})\}$.
- For each $f_1, f_2 \in \mathcal{P}$, the *S-polynomial of f_1 and f_2* is

  $$S(f_1, f_2) := \mathrm{lc}(f_2)^{-1} \frac{\delta(f_1, f_2)}{\mathbf{T}(f_2)} f_2 - \mathrm{lc}(f_1)^{-1} \frac{\delta(f_1, f_2)}{\mathbf{T}(f_1)} f_1,$$

  where $\delta := \delta(f_1, f_2) := \mathrm{lcm}(\mathbf{T}(f_1), \mathbf{T}(f_2))$.
- A set $G = \{g_1, \ldots, g_s\}$ is a Gröbner basis of $\mathbb{I}(G)$ iff for each $i < j$ the S-polynomial $S(g_i, g_j)$ has a Gröbner representation in terms of G.
- (Buchberger's Second Criterion)
  For each $f, g, h \in \mathcal{P} : \mathbf{T}(h) \mid \mathrm{lcm}(\mathbf{T}(f), \mathbf{T}(g))$, if both $S(f, h)$ and $S(g, h)$ have a Gröbner representation in terms of G, the same is true for $S(f, g)$.
- We also set $d(\mathsf{I}) := \max\{\deg(\zeta) : \zeta \in \mathsf{G}(\mathsf{I})$.

Let then $\mathsf{J} \subset \mathbb{F}[X_1, \ldots, X_n] := \mathcal{P}$ be an ideal, $\prec$ a noetherian semigroup term-ordering, $\Gamma(\mathsf{J}) = \{\gamma_1, \ldots, \gamma_s\}$ the Gröbner basis of J w.r.t. $\prec$ and $\delta \in \mathbb{N}$ any degree value s.t. $\delta \geq d(\mathsf{J}) + 1$.

Enumerate the variables and the Gröbner basis elements in such a way that $X_1 \prec X_2 \prec \ldots \prec X_n$ and

$$i < j \iff \text{either } \begin{cases} \deg(\gamma_i) > \deg(\gamma_j) \text{ or} \\ \deg(\gamma_i) = \deg(\gamma_j) \text{ and } \mathbf{T}(\gamma_i) \succ \mathbf{T}(\gamma_j). \end{cases}$$

Denoting

$$\Omega := \min_{\prec}\{\tau \in \mathbf{T}(\mathsf{I}), \deg(\tau) = \delta + 1\}$$

and $d_i := \deg(\gamma_i) < \delta$, we necessarily have

$$\Omega = X_1^{\delta+1-d_s}\mathbf{T}(\gamma_s).$$

We also let $h_0 := \Omega - \mathrm{Can}(\Omega, \mathsf{J}, \prec)$, so that $\mathrm{lc}(h_0) = 1, \mathbf{T}(h_0) = \Omega = X_1^{\delta-d_s}\mathbf{T}(\gamma_s)$, and $h_i := X_2\gamma_i, 1 \leq i \leq s$. We obtain[3]:

Proposition 4 *With the above notation it holds $H := \{h_0, h_1, \ldots, h_s\}$ is a Gröbner basis w.r.t. $\prec$ of the ideal $\mathbb{I}(H) = X_2\mathsf{J} + (h_0)$.*

Proof Clearly if $S(\gamma_i, \gamma_j), 1 \leq i < j \leq s$, has the Gröbner representation in terms of $\Gamma(\mathsf{J}), S(\gamma_i, \gamma_j) = \sum_{\alpha=1}^{\mu_{ij}} c_\alpha\tau_\alpha\gamma_{\ell_\alpha}$, then $S(h_i, h_j) = X_2 \sum_{\alpha=1}^{\mu_{ij}} c_\alpha\tau_\alpha\gamma_{\ell_\alpha} = \sum_{\alpha=1}^{\mu_{ij}} c_\alpha\tau_\alpha h_{\ell_\alpha}$ is a Gröbner representation in terms of H.
Moreover, since $\Omega = \mathbf{T}(h_0)$ and $\mathbf{T}(h_s) = X_2\mathbf{T}(\gamma_s) \mid \mathrm{lcm}(\mathbf{T}(h_j), \Omega), 0 \leq j \leq s$, as a direct consequence of Buchberger's Second Criterion, in order to prove the claim it is sufficient to show that the S-polynomial $S(h_s, h_0)$ between h_0 and h_s has a Gröbner representation in terms of H.

By assumption there $\exists\, \mu = \mu_{h_0}, \alpha \in \mathbb{N}, 1 \leq \alpha \leq s, c_\alpha \in \mathbb{F} \setminus \{0\}, \tau_\alpha \in \mathcal{T}$, s.t. we have a Gröbner representation

$$\mathsf{J} \ni \mathsf{h_0} = \Omega - \mathrm{Can}(\Omega, \mathsf{J}, \prec) = \mathrm{lc}(\gamma_\mathsf{s})^{-1}\mathsf{X_1^{D-d_s}}\gamma_\mathsf{s} + \sum_{\alpha=1}^{\mu} \mathsf{c}_\alpha\tau_\alpha\gamma_{\ell_\alpha}$$

where $\gamma_{\ell_\alpha} \in \Gamma(\mathsf{J})$ and

$$\Omega = X_1^{D-d_s}\mathbf{T}(\gamma_s) \succ \tau_1\mathbf{T}(\gamma_{\ell_1}) \succ \tau_2\mathbf{T}(\gamma_{\ell_2}) \succ \cdots;$$

thus we trivially obtain the required Gröbner representation

$$\begin{aligned} S(h_s, h_0) &= \mathrm{lc}(h_0)^{-1}\frac{\delta(h_s, h_0)}{\mathbf{T}(h_0)}h_0 - \mathrm{lc}(h_s)^{-1}\frac{\delta(h_s, h_0)}{\mathbf{T}(h_s)}h_s = \\ &= X_2h_0 - \mathrm{lc}(\gamma_s)^{-1}X_1^{D-d_s}(X_2\gamma_s) \\ &= X_2\sum_{\alpha=1}^{\mu} c_\alpha\tau_\alpha\gamma_{\ell_\alpha} = \sum_{\alpha=1}^{\mu} c_\alpha\tau_\alpha h_{\ell_\alpha}. \end{aligned}$$

□

Remark 5 *For any ideal $\mathsf{J} \subset \mathcal{P}$, noetherian semigroup term-ordering $\prec$, and degree value $\delta \in \mathbb{N}$ s.t. $\delta \geq d(\mathsf{J}) + 1$, the two ideals $\mathsf{I}_\delta := \mathbb{I}(H)$ and $\mathsf{I} := X_2\mathsf{J}$ satisfy both:*

$$\{f \in \mathsf{I}_\delta : \deg(f) \leq \delta\} = \{f \in \mathsf{I} : \deg(f) \leq \delta\} \text{ and } \mathsf{I} \subset \mathsf{I}_\delta,$$

[3]Of course, our construction is indebted to the counterexample to Cardinal's Conjecture proposed in [9].

with

$$d(\mathsf{I}_\delta) > \delta \geq \mathsf{d}(\mathsf{J}) + 1 = \mathsf{d}(\mathsf{I}).$$

Thus, the algorithm we are going to sketch below applied to the (unknown) ideal I_δ *returns the correct answer* I_δ *if the input data satisfy* $D \geq \delta + 1$*, but returns the wrong answer* I *if* $\delta \geq D \geq d(\mathsf{J}) + 1$.
That is, we actually need to assume to know an upper bound D *for* $d(\mathsf{I})$ *and only deal with terms belonging to the* box

$$\mathcal{B}(D) := \{X_1^{a_1} \cdots X_n^{a_n} \in \mathbb{T} : \, 0 \leq a_i \leq D, \forall\, 1 \leq i \leq n\}.$$

□

We now give a combinatorial algorithm to solve Problem 2.

Let $\omega = X_1 \cdot \ldots \cdot X_n$, as $\omega^0 = 1 \in \mathbf{N}(\mathsf{I})$, we take iteratively $\omega^{i+1}, i \in \mathbb{N}$, until either we find $j \in \mathbb{N}, j \leq D$, such that $\omega^{j-1} \in \mathbf{N}(\mathsf{I})$ and $\omega^j \in \mathbf{T}(\mathsf{I})$ or $\omega^D \in \mathbf{N}(\mathsf{I})$. In this last case we can deduce that $\mathsf{I} = (0)$[4], otherwise, for the found $j \in \mathbb{N}$ we begin deciding which of the following cases arises:

Case 1 $\omega^j \in \mathbf{G}(\mathsf{I})$ (i.e. all the predecessors of ω^j are in $\mathbf{N}(\mathsf{I})$),

Case 2 $\omega^j \in \mathbf{B}(\mathsf{I}) \setminus \mathbf{G}(\mathsf{I})$ (i.e. at most $n-1$ predecessors of ω^j are in $\mathbf{N}(\mathsf{I})$),

Case 3 $\omega^j \in \mathbf{J}(\mathsf{I})$ (i.e. all the predecessors of ω^j are in $\mathbf{T}(\mathsf{I})$).

To visualize the situation we identify $\mathcal{T}$ with $\mathbb{N}^n$ thought as

$$\{\underline{x} = (x_1, \ldots, x_n) \in \mathbb{R}^n : x_i \in \mathbb{N}, 1 \leq i \leq n\};$$

by 'line' (and one should better say 'half-line') of $\mathcal{T}$ we mean a set of aligned points of $\mathbb{N}^n \subset \mathbb{R}^n$ and similarly for 'plane', 'hyperplane', 'simplicial complex' etc..

We point out that :

- for $n = 2$, $\mathbf{B}(\mathsf{I})$ is a 'piecewise linear curve' $\mathcal{C}(\mathsf{I})$ consisting of contiguous horizontal and vertical 'segments' from which all the 'convex' vertices are removed and possibly the leftmost vertical segment and the bottom horizontal one are 'half-lines'[5];
- for $n \geq 3$, $\mathbf{B}(\mathsf{I})$ is a 'simplicial complex'[6], consisting of contiguous shares of 'hyperplanes' each of them parallel to a 'coordinate hyperplane' (the closest to a coordinate one possibly being infinite) from which all the 'protruding' i-th facets with $i \leq n-2$ are removed;

[4] In fact each term τ with $\deg(\tau) \leq D$ trivially satisfies $\tau \mid \omega^D$, i.e. $\omega^D \in \mathbf{N}(\mathsf{I})$ implies $\mathbf{G}(\mathsf{I}) = \emptyset$.

[5] As $\mathbf{B}(\mathsf{I}) \cup \{\text{all the convex vertices}\}$ looks like the profile of a stair A. Galligo introduced the term *escalier*.

[6] Still called *escalier*.

– $\mathbf{J}(\mathsf{I})$ is the set of points lying above the *escalier*;

– $\mathbf{G}(\mathsf{I})$ consists of the 'concave vertices' of the *escalier*;

– $\mathbf{N}(\mathsf{I})$ is the set of points below the *escalier* (for this named *sous-escalier*).

We will also call '0-*dimensional*', ..., '$n-1$-*dimensional' point of the* escalier a point lying on a vertex , ..., on a $(n-1)$-facet (and not in a lower dimensional one) noticing that the elements of $\mathbf{G}(\mathsf{I})$ are particular '0-dimensional' points.

From now on we will assume that $\exists j \in \mathbb{N}, j \leq D$, such that $\omega^{j-1} \in \mathbf{N}(\mathsf{I})$ and $\omega^j \in \mathbf{T}(\mathsf{I})$.

3.1 Two variables

We distinguish between the three possible cases for $\omega^j := X^jY^j$ and, through several steps, we construct $\mathbf{G}(\mathsf{I})$:

case 1 $\omega^j \in \mathbf{G}(\mathsf{I})$ (the 'line' $x = y$ meets $\mathbf{T}(\mathsf{I})$ in a 'concave vertex' of the *escalier*),

I step: $t_1 := \omega^j = X^jY^j \in \mathbf{G}(\mathsf{I})$ and we store it (it could be the only generator)

II step: starting from $t_1 = \omega^j \in \mathbf{G}(\mathsf{I})$ (found in step I), we need to consider X^jY^{j+n} and $X^{j+m}Y^j$ as $n, m \in \mathbb{N}^*$:

a) examine X^jY^{j+n}:

(i) if $\forall\, n \leq D-j$, $X^{j-1}Y^{j+n} \in \mathbf{N}(\mathsf{I})$, then there is no generator in $\mathbf{G}(\mathsf{I})$ with X-exponent $< j$;

(ii) if $\exists\, \tilde{n} = \min\{n : 0 < n \leq D-j, X^{j-1}Y^{j+n} \in \mathbf{T}(\mathsf{I})\}$, we let $b_2 := j + \tilde{n}$ and
- if $Y^{b_2} \in \mathbf{T}(\mathsf{I})$ then we set $\alpha_2 := 0$
- otherwise we set $\alpha_2 := \max\{\alpha \leq j-1 : X^{\alpha-1}Y^{b_2} \in \mathbf{N}(\mathsf{I})\}$, so that $t_{22} := X^{\alpha_2}Y^{b_2}$, with $0 \leq \alpha_2 < j, b_2 > j$, is a new generator and we store it;

b) examine $X^{j+m}Y^j$:

(i) if $\forall\, m \leq D-j$, $X^{j+m}Y^{j-1} \in \mathbf{N}(\mathsf{I})$, then there is no generator in $\mathbf{G}(\mathsf{I})$ with Y-exponent $< j$;

(ii) if $\exists\, \tilde{m} = \min\{0 < m \leq D-j : X^{j+m}Y^{j-1} \in \mathbf{T}(\mathsf{I})\}$, we let $a_2 := j + \tilde{m}$ and
- if $X^{a_2} \in \mathbf{T}(\mathsf{I})$ then we set $\beta_2 := 0$
- otherwise we set $\beta_2 := \max\{\beta \leq j-1 : X^{a_2}Y^{\beta-1} \in \mathbf{N}(\mathsf{I})\}$, so that $t_{21} := X^{a_2}Y^{\beta_2}$, with $0 \leq \beta_2 < j, a_2 > j$ is a new generator and we store it ;

t_1 is the only generator of $\mathbf{T}(\mathsf{I})$ iff at step II hold both $a)(i)$ and $b)(i)$, otherwise at least one further generator is found.

case 2 $\omega^j \in \mathbf{B}(\mathsf{I}) \setminus \mathbf{G}(\mathsf{I})$: have to distinguish whether the 'line' $x = y$ meets $\mathbf{T}(\mathsf{I})$ in a 'vertical' or 'horizontal side' of the *escalier*:

a) $X^{j-1}Y^j \in \mathbf{N}(\mathsf{l}), X^jY^{j-1} \in \mathbf{T}(\mathsf{l})$ ('vertical side' case),

I step : - if $X^j \in \mathbf{T}(\mathsf{l})$ then we set $\bar{\beta}_1 := 0$
- otherwise we set

$$\bar{\beta}_1 := \max\{\beta < j : X^jY^{\beta-1} \in \mathbf{N}(\mathsf{l})\},$$

so that $\bar{t}_1 := X^jY^{\bar{\beta}_1} \in \mathbf{G}(\mathsf{l})$ and we store it (possibly the only generator);

II step :

(j) starting from $\bar{t}_1 := X^jY^{\bar{\beta}_1} \in \mathbf{G}(\mathsf{l})$, if $j < D$ we repeat the procedure described in case 1, step $II\,b)(i),(ii)$ possibly finding a new generator $\bar{t}_{21} := X^{\bar{a}_2}Y^{\bar{\beta}_2} \in \mathbf{G}(\mathsf{l})$ with $0 \le \bar{\beta}_2 < \bar{\beta}_1 < j, D \ge \bar{a}_2 > j$;

(jj) starting from ω^j we repeat the procedure described in case 1 step $IIa)(i),(ii)$ possibly finding a new generator $\bar{t}_{22} := X^{\bar{\alpha}_2}Y^{\bar{b}_2} \in \mathbf{G}(\mathsf{l})$ with $0 \le \bar{\alpha}_2 < j, D \ge \bar{b}_2 > j$;

b) $X^jY^{j-1} \in \mathbf{N}(\mathsf{l}), X^{j-1}Y^j \in \mathbf{T}(\mathsf{l})$ ('horizontal side' case),

I step : - if $Y^j \in \mathbf{T}(\mathsf{l})$ then we set $\tilde{\alpha}_1 := 0$
- otherwise we set $\tilde{\alpha}_1 := \max\{\alpha < j : X^{\alpha-1}Y^j \in \mathbf{N}(\mathsf{l})\}$,

so that $\tilde{t}_1 := X^{\tilde{\alpha}_1}Y^j \in \mathbf{G}(\mathsf{l})$ and we store it (possibly the only generator);

II step :

(j) starting from $\tilde{t}_1 := X^{\tilde{\alpha}_1}Y^j \in \mathbf{G}(\mathsf{l})$, if $j < D$ we repeat the procedure described in case 1, step $II\,a)(i),(ii)$ possibly finding a new generator $\tilde{t}_{22} := X^{\tilde{\alpha}_2}Y^{\tilde{b}_2} \in \mathbf{G}(\mathsf{l})$ with $0 \le \tilde{\alpha}_2 < \tilde{\alpha}_1 < j, D \ge \tilde{b}_2 > j$;

(jj) starting from ω^j we repeat the procedure described in case 1 step $IIb),(i),(ii)$ possibly finding a new generator $\tilde{t}_{21} := X^{\tilde{\alpha}_2}Y^{\tilde{b}_2} \in \mathbf{G}(\mathsf{l})$ with $0 \le \tilde{\alpha}_2 < j, D \ge \tilde{b}_2 > j$;

$\bar{t}_1$ (resp. $\tilde{t}_1$) is the only generator of $\mathbf{T}(\mathsf{l})$ iff at step $II\,a)$ (resp. $II\,b)$) hold both $a)(i)$ and $b)(i)$ of case 1 step II, otherwise at least one further generator is added.

case 3 $\omega^j \in \mathbf{J}(\mathsf{l})$ (the 'line' $x = y$ meets $\mathbf{T}(\mathsf{l})$ in a 'convex vertex' of the *escalier*),

I step : by construction $\omega^{j-1} \in \mathbf{N}(\mathsf{l})$, thus $X^{j-1}Y^j, X^jY^{j-1} \in \mathbf{B}(\mathsf{l})$ (the first one in a 'horizontal' and the second one in a 'vertical side' of the *escalier*), operating on them respectively like in case 2 $b)$ step I and case 2 $a)$ step I, we get two generators:

- $\breve{t}_{12} := X^{\breve{\alpha}_1}Y^j$, $0 \le \breve{\alpha}_1 < j$,
- $\breve{t}_{11} := X^jY^{\breve{\beta}_1}$, $0 \le \breve{\beta}_1 < j$;

II step :

– operating on $\breve{t}_{12}$ like in case 1, step $II\,a)(i),(ii)$ we possibly find a new generator $\breve{t}_{22} := X^{\breve{\alpha}_2}Y^{\breve{b}_2}$ with $0 \leq \breve{\alpha}_2 < \breve{\alpha}_1 < j, D \geq \breve{b}_2 > j$
– operating on $\breve{t}_{11}$ like in case 1, step $II\,b)(i),(ii)$ we possibly find a new generator $\breve{t}_{21} := X^{\breve{a}_2}Y^{\breve{\beta}_2}$ with $0 \leq \breve{\beta}_2 < \breve{\beta}_1 < j, D \geq \breve{a}_2 > j$;

$\breve{t}_{11}$ and $\breve{t}_{12}$ are the only generators of I iff at step II hold both $a)(i)$ and $b)(i)$ of case 1 step II, otherwise at least one further generator is added.

all cases III and further steps

starting from the previous step generators (all of type $t_{i2} := X^{\alpha_i}Y^{b_i}$ with $0 \leq \alpha_i < \ldots < j, D \geq b_i > \ldots > j$ or $t_{i1} := X^{a_i}Y^{\beta_i}$ with $0 \leq \beta_i < \ldots < j, D \geq a_i > \ldots > j$) we operate like in case 2 step $II(j)$ while $D > b_i$ and $D > a_i$

The procedure stops because our possible degrees do not exceed the fixed bound D and we don't miss any generator since we are following the *escalier* point by point.

Example 6 Let $\mathcal{P} = \mathbb{F}[X, Y]$, $\omega = XY$.

1. $\mathsf{I} = (X^2Y^2, XY^3, X^4Y, Y^8), D = 8$.

   We have $\omega^1 \in \mathbf{N}(\mathsf{I}), \omega^2 \in \mathbf{T}(\mathsf{I})$ and $XY^2, X^2Y \in \mathbf{N}(\mathsf{I})$, thus $\omega^2 \in \mathbf{G}(\mathsf{I})$; considering $X^{2+m}Y, m \leq D-2$ and $XY^{2+n}, n \leq D-2$ we see that:

   $\min\{n : XY^{2+n} \in \mathbf{T}(\mathsf{I})\} = 1$, with $Y^3, XY^2 \in \mathbf{N}(\mathsf{I})$, thus $XY^3 \in \mathbf{G}(\mathsf{I})$;

   $\min\{m : X^{2+n}Y \in \mathbf{T}(\mathsf{I})\} = 2$, with $X^3Y, X^4 \in \mathbf{N}(\mathsf{I})$ thus $X^4Y \in \mathbf{G}(\mathsf{I})$.

   Starting from XY^3 we see that $\min\{n : Y^{3+n} \in \mathbf{T}(\mathsf{I})\} = 5$ thus $Y^8 \in \mathbf{G}(\mathsf{I})$; while, starting from X^4Y we see that $X^{4+m} \in \mathbf{N}(\mathsf{I}), \forall\, m \leq D-4$, so that do not exist generators with null Y-exponent.

2. $\mathsf{I} = (X^3Y^2), D = 5$.

   We have $\omega^1, \omega^2 \in \mathbf{N}(\mathsf{I})$, $\omega^3 \in \mathbf{T}(\mathsf{I})$ with $X^2Y^3 \in \mathbf{N}(\mathsf{I})$ and $X^3Y^2 \in \mathbf{T}(\mathsf{I})$ thus we have to consider $X^3Y^{3-q}, 0 < q \leq 3$, as $X^3Y^2 \in \mathbf{B}(\mathsf{I}), X^3Y \in \mathbf{N}(\mathsf{I})$ we have $X^3Y^2 \in \mathbf{G}(\mathsf{I})$; moreover as $X^{3+m}Y \in \mathbf{N}(\mathsf{I}), \forall\, m \leq D-3$ and $X^2Y^{2+n} \in \mathbf{N}(\mathsf{I}), \forall\, n \leq D-2$ we have that X^3Y^2 is the unique generator.

3. $\mathsf{I} = (X^2Y^4, X^4Y^3), D = 7$.

   We have $\omega^1, \omega^2, \omega^3 \in \mathbf{N}(\mathsf{I})$, $\omega^4 \in \mathbf{T}(\mathsf{I})$ with $X^3Y^4, X^4Y^3 \in \mathbf{B}(\mathsf{I})$ thus we have to consider $X^{4-p}Y^4, X^4Y^{4-q}, p, q \leq 4$, and we see that $X^4Y^3 \in \mathbf{G}(\mathsf{I}), X^2Y^4 \in \mathbf{G}(\mathsf{I})$ are the only generators of I.

3.2 $n \geq 3$ variables

Using the 2-variables case as a first inductive step, we consider X_n as n^{th} variable, added to $X_1, \ldots, X_{n-1}$. Assuming we are able to find all the minimal generators (up to the degree bound) of a monomial ideal in $n-1$ variables, we will slice $\mathcal{T}$ in 'hyperplanes' $x_n = j, j \leq D$, and we will argue by considering

the intersection E_j of the *escalier* with each one of them. One of the following cases occurs:

- E_j has dimension $i \leq n-2$, so it does not contain any element of $\mathbf{G}(\mathsf{I})$,
- E_j is $n-1$-dimensional and so it contains some element of $\mathbf{G}(\mathsf{I})$,
- $E_j = \emptyset$.

Remark 7 *We point out explicitly that for any* $\mathsf{I} \neq (0)$ *there must exist at least one* $j \in \mathbb{N}$ *with* E_j *hyperplanar.*

Moreover, as we already remarked, $\omega^D \in \mathbf{N}(\mathsf{I}) \implies \mathsf{I} = (0)$ *and* $\mathbf{N}(\mathsf{I}) = \emptyset$. *If, instead, for some* $j \leq D, \omega^j \in \mathbf{T}(\mathsf{I})$ *then, necessarily, there is a* $\tau \in \mathbf{G}(\mathsf{I}), \tau \mid \omega^j$ *and thus* $E_{j-h_1^-} \cap \mathbf{G}(\mathsf{I}) \neq \emptyset$ *for some* $h_1^-, 0 \leq h_1^- \leq j$.

It is however possible that for some $j \leq D$, $\omega^j \in \mathbf{T}(\mathsf{I})$ *and* $E_{j+h} \cap \mathbf{G}(\mathsf{I}) = \emptyset$ *for each* $h, 0 \leq h \leq D-j$. *This simply means that all generators of* $\mathbf{T}(\mathsf{I})$ *have* X_n-*degree bounded by* j *and that* $E_j = E_{j+h}$ *for each* $h \in \mathbb{N}$. □

Step I: By applying the $n-1$-variables algorithm to ω^j (on the 'hyperplane' $x_n = j$) we find a set of terms $\widetilde{\mathbf{G}}(\mathsf{I})_1$ from which, after cancelling all the terms σ such that $\frac{\sigma}{X_n} \in \mathbf{T}(\mathsf{I})$, we get a set of terms $\mathbf{G}(\mathsf{I})_{j\dots j}$ for which two possibilities arise:

(i) $\mathbf{G}(\mathsf{I})_{j\dots j} \neq \emptyset$ and we set $\mathbf{G}(\mathsf{I})_1 := \mathbf{G}(\mathsf{I})_{j\dots j}$,

(ii) otherwise, $\mathbf{G}(\mathsf{I})_{j\dots j} = \emptyset$ means that E_j is $i \leq n-2$-dimensional and we have to iteratively consider $\omega_n^{+h} := X_1^j \cdots X_{n-1}^j X_n^{j+h}, \forall\ h \leq D-j$, and $\omega_n^{-h} := X_1^j \cdots X_{n-1}^j X_n^{j-h}, \forall\ h \leq j$, until we find necessarily an E_{j-h} which is 'hyperplanar' and possibly also an E_{j+h}, which is 'hyperplanar'; we then set[7]:
   - $h_1^+ := \min\{h \leq D-j, E_{j+h}$ 'hyperplanar'$\}$ (if it exists),
   - $h_1^- := \min\{h \leq j, E_{j-h}$ 'hyperplanar'$\}$.

By applying the $n-1$-variables algorithm on both 'hyperplanes' $x_n = j + h_1^+$ and $x_n = j - h_1^-$(noticing that by assumption $X_1^j \cdots X_{n-1}^j X_n^{j+h_1^+}$, $X_1^j \cdots X_{n-1}^j X_n^{j-h_1^-} \in \mathbf{T}(\mathsf{I})$), after the above cancellation procedure, we get new sets of terms $\mathbf{G}(\mathsf{I})_{j\dots j}^{h_1^+}$ and $\mathbf{G}(\mathsf{I})_{j\dots j}^{h_1^-}$. As we observed in Remark 7 it can not happen $E_{j-h} \cap \mathbf{G}(\mathsf{I}) = \emptyset, \forall\, h \leq j$, i.e. at least $\mathbf{G}(\mathsf{I})_{j\dots j}^{h_1^-} \neq \emptyset$ so that, setting : $\mathbf{G}(\mathsf{I})_1^+ := \mathbf{G}(\mathsf{I})_{j\dots j}^{+h_1^+}$ and $\mathbf{G}(\mathsf{I})_1^- := \mathbf{G}(\mathsf{I})_{j\dots j}^{+h_1^-}$[8], we get

$$\emptyset \neq \mathbf{G}(\mathsf{I})_1 := \mathbf{G}(\mathsf{I})_1^+ \cup \mathbf{G}(\mathsf{I})_1^-,$$

[7]Notice that if $\mathbf{G}(\mathsf{I})_{j\dots j} \neq \emptyset$ we must think of $h_1^+ = h_1^- = 0$.

[8]Of course if $\nexists\, h_1^+$ we set $\mathbf{G}(\mathsf{I})_1^+ := \emptyset$ noticing that if $\mathbf{G}(\mathsf{I})_1^+ := \emptyset$ do not exist generators with X_n-exponent $\geq j$. We also note that if $\mathbf{G}(\mathsf{I})_{j\dots j} \neq \emptyset$ we can think $\mathbf{G}(\mathsf{I})_1 = \mathbf{G}(\mathsf{I})_1^-$.

Step II a) $\forall\ \sigma = X_1^{a_1}\cdots X_{n-1}^{a_{n-1}}X_n^{j-h_1^-} \in \mathbf{G}(\mathsf{I})_1^-$ we move along the 'line'

$$\begin{cases} x_1 - a_1 = x_2 - a_2 \\ x_1 - a_1 = x_3 - a_3 \\ \vdots \\ x_n = j - h_1^- - 1, \end{cases},$$

with the following two possible issues:

(i) for all $X_1^{a_1+l}\cdots X_{n-1}^{a_{n-1}+l}X_n^{j-h_1^-} \in \mathbf{G}(\mathsf{I})_1^-$ and $l \leq \max\{D - a_i\}$ it holds

$$X_1^{a_1+l}\cdots X_{n-1}^{a_{n-1}+l}X_n^{j-h_1^- -1} \in \mathbf{N}(\mathsf{I}),$$

that is the whole share of the 'hyperplane' $x_n = j - h_1^-$ lying on $\mathbf{T}(\mathsf{I})$ actually belongs to $\mathbf{B}(\mathsf{I})$ (i.e. do not exist generators having X_n-exponent $< j - h_1^-$).

(ii) $\exists\, X_1^{a_1}\cdots X_{n-1}^{a_{n-1}}X_n^{j-h_1^-} \in \mathbf{G}(\mathsf{I})_1^-$ and

$$l_{a_1\ldots a_{n-1}} := \min\left\{l \in \mathbb{N}^* : X_1^{a_1+l}\cdots X_{n-1}^{a_{n-1}+l}X_n^{j-h_1^- -1} \in \mathbf{T}(\mathsf{I})\right\},$$

that is the *escalier* does not exhaust $\mathbf{T}(\mathsf{I})\cap\{\underline{x} \in \mathbb{R}^n : x_n = j - h_1^-\}$ (i.e. some $X_1^{\alpha_1}\cdots X_{n-1}^{\alpha_{n-1}}X_n^{j-h_1^-} \in \mathbf{J}(\mathsf{I})$ and do exist generators having X_n-exponent $< j - h_1^-$). In this case we consider iteratively

$$X_1^{a_1+l_{a_1\ldots a_{n-1}}}\cdots X_{n-1}^{a_{n-1}+l_{a_1,\ldots,a_{n-1}}}X_n^{j-h_1^- -h}, h \leq j - h_1^-$$

until either we find $h^-_{a_1\ldots a_{n-1}}, 0 < h^-_{a_1\ldots a_{n-1}} < j - h_1^-$ with

$$X_1^{a_1+l_{a_1\ldots a_{n-1}}}\cdots X_{n-1}^{a_{n-1}+l_{a_1\ldots a_{n-1}}}X_n^{j-h_1^- -1-h^-_{a_1\ldots a_{n-1}}} \in \mathbf{N}(\mathsf{I})$$

(so that $E_{j-h_1^- -h^-_{a_1,\ldots,a_{n-1}}}$ is 'hyperplanar' thus containing some generators of I) or $X_1^{a_1+l_{a_1\ldots a_{n-1}}}\cdots X_{n-1}^{a_{n-1}+l_{a_1\ldots a_{n-1}}} \in \mathbf{T}(\mathsf{I})$ in which case we set $h^-_{a_1\ldots a_{n-1}} = j - h_1^-$ (so that $j - h_1^- - h_{a_1\ldots a_{n-1}} = 0$ and still $E_0 = E_{j-h_1^- -h^-_{a_1\ldots a_{n-1}}}$ is 'hyperplanar' thus containing some generators of I).
We then set

$$h_2^- := \min_{X_1^{a_1}\cdots X_{n-1}^{a_{n-1}}X_n^{j-h_1^-} \in \mathbf{G}(\mathsf{I})_1^-} \{h^-_{a_1\ldots a_{n-1}} \text{ as above}\}.$$

By applying the $n-1$-variables algorithm on the 'hyperplane' $x_n = j - h_1^- - h_2^-$ (the nearest-below which is $\parallel$ to $x_n = j - h_1^-$

and contains generators of l) we find a set of terms $\widetilde{\mathbf{G}}(\mathsf{l})^{-h_2^-}$ from which we must erase all the terms whose X_n-predecessor lie in $\mathbf{T}(\mathsf{l})$, getting, by construction, a non-empty:

$$\mathbf{G}(\mathsf{l})^{-h_2^-} := \widetilde{\mathbf{G}}(\mathsf{l})^{-h_2^-} \setminus \{\sigma \in \widetilde{\mathbf{G}}(\mathsf{l})^{-h_2^-} \ : \frac{\sigma}{X_n} \in \mathbf{T}(\mathsf{l})\},$$

which contains all the generators lying on the 'hyperplane' $x_n = j - h_1^- - h_2^-$

and we let $\mathbf{G}(\mathsf{l})_2^- := \begin{cases} \emptyset & \text{in case (i)} \\ \mathbf{G}(\mathsf{l})^{-h_2^-} & \text{in case (ii)} \end{cases}$.

b) If $\mathbf{G}(\mathsf{l})_1^+ \neq \emptyset$, we fix any $X_1^{a_1} \cdots X_{n-1}^{a_{n-1}} X_n^{j+h_1^+} \in \mathbf{G}(\mathsf{l})_1^+$: by iteratively applying (on each 'hyperplane' $x_n = j + h_1^+ + h$) the $n-1$-variables algorithm to $X_1^{a_1} \cdots X_{n-1}^{a_{n-1}} X_n^{j+h_1^+ + h}, j + h_1^+ + h \leq D$ we find a set of terms $\widetilde{\mathbf{G}}(\mathsf{l})_2^{+h}$ from which, after cancelling all the terms σ such that $\frac{\sigma}{X_n} \in \mathbf{T}(\mathsf{l})$, we get a set $\mathbf{G}(\mathsf{l})_2^{+h}$ and two possibilities arise:

(i) for all $h, j + h_1^+ + h \leq D, \mathbf{G}(\mathsf{l})_2^{+h} = \emptyset$ which means that do not exist generators having X_n-exponent $> j + h_1^+$;

(ii) $\exists\, h_2^+ = \min\{h, j + h_1^+ + h \leq D : \mathbf{G}(\mathsf{l})_2^{+h} \neq \emptyset\}$ and $\mathbf{G}(\mathsf{l})_2^{+h_2^+}$ gives all the generators contained in the 'hyperplane' $x_n = j + h_1^+ + h_2^+$ (the upper-nearest $\parallel$ to $x_n = j + h_1^+$ which contains generators).

Then we let $\mathbf{G}(\mathsf{l})_2^+ := \begin{cases} \emptyset & \text{in case (i)} \\ \mathbf{G}(\mathsf{l})^{+h_2^+} & \text{in case (ii)} \end{cases}$

We finally set $\mathbf{G}(\mathsf{l})_2 := \mathbf{G}(\mathsf{l})_2^+ \cup \mathbf{G}(\mathsf{l})_2^-$.

Further Steps : Starting from $\mathbf{G}(\mathsf{l})_{i-1} = \mathbf{G}(\mathsf{l})_{i-1}^+ \cup \mathbf{G}(\mathsf{l})_{i-1}^-$, $\forall\ i \geq 3$, we repeat:

- if $\mathbf{G}(\mathsf{l})_{i-1}^- \neq \emptyset$ for a fixed $\sigma \in \mathbf{G}(\mathsf{l})_{i-1}^-$ all the procedures of Step II a), possibly finding a non-empty $\mathbf{G}(\mathsf{l})_i^-$ and the relative X_n-exponent $j - h_1^- - \cdots - h_i^-$.
- if $\mathbf{G}(\mathsf{l})_{i-1}^+ \neq \emptyset$, for each $\sigma \in \mathbf{G}(\mathsf{l})_{i-1}^+$ all the procedures of Step II b), possibly finding a non-empty $\mathbf{G}(\mathsf{l})_i^+$.

The procedure stops because our possible degrees do not exceed the fixed bound $D \in \mathbb{N}^*$ that is we find an $n_D(\mathsf{l}) \in \mathbb{N}$ such that

$$\mathbf{G}(\mathsf{l})_{\leq D} = \bigcup_{i=1}^{n_D(\mathsf{l})} \mathbf{G}(\mathsf{l})_i$$

and we don't miss any generator since we have controlled the situation at each x_n-level.

Example 8 Let $\mathcal{P} = \mathbb{F}[X, Y, Z]$, $\omega = XYZ$.
$\mathsf{I} = (XY^3Z^4, Y^5Z^3, X^3Y^2Z^2, X^4Z), D = 8$.
We have $\omega^2 \in \mathbf{N}(\mathsf{I}), \omega^3 \in \mathbf{T}(\mathsf{I})$ with $X^3Y^3Z^2, X^3Y^2Z^3 \in \mathbf{T}(\mathsf{I}), X^2Y^3Z^3 \in \mathbf{N}(\mathsf{I})$.

Step I We apply in the 'plane' $z = 3$ the 2-variables algorithm to $\omega^3 = X^3Y^3(Z^3)$: as $X^2Y^3(Z^3) \in \mathbf{N}(\mathsf{I})$ and $X^3Y^2(Z^3) \in \mathbf{T}(\mathsf{I})$ we consider $X^3Y^{3-q}(Z^3)$, $q \leq 3$ until $X^3Y^{3-q}(Z^3) \in \mathbf{B}(\mathsf{I})$ and $X^3Y^{2-q}(Z^3) \in \mathbf{N}(\mathsf{I})$ or $q = 3$. Since $X^3Y^2(Z^3) \in \mathbf{B}(\mathsf{I})$ and $X^3Y(Z^3) \in \mathbf{N}(\mathsf{I})$ we take $X^3Y^2(Z^3)$ and we store it (recalling that $\omega^2 \in \mathbf{N}(\mathsf{I})$). Starting from $X^3Y^2(Z^3)$ we consider $X^{3+m}Y(Z^3), m \leq 5$, and, since $X^4Y(Z^3), X^4(Z^3) \in \mathbf{B}(\mathsf{I})$, we store $X^4(Z^3)$. Starting from $X^3Y^3(Z^3)$ we look whether

$$\exists\, \nu := \min\{n :\ X^2Y^{3+n}(Z^3) \in \mathbf{T}(\mathsf{I}), 3 + n \leq 8\}$$

and we find $\nu = 2$ as $X^2Y^5(Z^3) \in \mathbf{B}(\mathsf{I})$ from which, by considering $X^{2-p}Y^5(Z^3), p \leq 2$ until $X^{2-p}Y^5(Z^3) \in \mathbf{B}(\mathsf{I})$ and $X^{1-p}Y^5(Z^3) \in \mathbf{N}(\mathsf{I})$ or $p = 2$, we obtain $Y^5(Z^3) \in \mathbf{T}(\mathsf{I})$ and we store it. We stop here as the 2-variables algorithm on the 'plane' $z = 3$ does not produce other elements. Dividing by Z each $\sigma \in \{X^3Y^2Z^3, X^4Z^3, Y^5Z^3\}$ we get $\mathbf{G}(\mathsf{I})_1 = \{Y^5Z^3\}$ (as $X^3Y^2Z^3, X^4Z^2 \in \mathbf{T}(\mathsf{I})$).

Step II
a) We look whether $\exists\, l_{0,5} := \min\{l :\ X^{0+l}Y^{5+l}Z^2 \in \mathbf{T}(\mathsf{I}), l \leq 8)\}$ and we get $l_{0,5} = 3$ (as $X^3Y^8Z^2 \in \mathbf{T}(\mathsf{I})$ and $X^2Y^7Z^2 \in \mathbf{N}(\mathsf{I})$), we then consider $X^3Y^8(Z^2)$ on the 'plane' $z = 2$ and, by applying the 2-variables algorithm, we get $X^3Y^2Z^2 \in \mathbf{T}(\mathsf{I})$ and $X^4Z^2 \in \mathbf{T}(\mathsf{I})$ to be stored and, since dividing by Z, we get $X^3Y^2Z \in \mathbf{N}(\mathsf{I})$ while $X^4Z \in \mathbf{T}(\mathsf{I})$, we have $\mathbf{G}(\mathsf{I})_2^- = \{X^3Y^2Z^2\}$.

b) Let's now look to what happens on the 'planes' $z = 3 + h, h \leq 5$. Knowing that $X^3Y^3Z^4 \in \mathbf{T}(\mathsf{I})$ we must apply the 2-variables algorithm to $X^3Y^3(Z^4)$ on the 'plane' $z = 4$ obtaining as output the set

$$\{XY^3(Z^4), X^3Y^2(Z^4), X^4(Z^4)\}$$

and, as we have $X^3Y^2Z^3, X^4Z^3 \in \mathbf{T}(\mathsf{I})$ but $XY^3Z^3 \in \mathbf{N}(\mathsf{I})$ we set $\mathbf{G}(\mathsf{I})_2^+ = \{XY^3Z^4\}$ and finally $\mathbf{G}(\mathsf{I})_2 = \{XY^3Z^4, X^3Y^2Z^2\}$.

Step III
a) We look whether $\exists\, l_{3,2} := \min\{l :\ X^{3+l}Y^{2+l}Z \in \mathbf{T}(\mathsf{I}), l \leq 6\}$ and we find $l_{3,2} = 1$ (as $X^4Y^3Z \in \mathbf{T}(\mathsf{I})$ and $X^3Y^2Z \in \mathbf{N}(\mathsf{I})$), we then apply the 2-variables algorithm to $X^4Y^3(Z)$ on the 'plane' $z = 1$ finding only $X^4Z \in \mathbf{B}(\mathsf{I})$ to be stored and divided by Z and, as $X^4 \in \mathbf{N}(\mathsf{I})$, we set $\mathbf{G}(\mathsf{I})_3^- = \{X^4Z\}$.

b) Let's now look to what happens on the 'planes' $z = 4 + h, h \leq 4$, knowing that $XY^3Z^{4+h} \in \mathbf{T}(\mathsf{I})$ we apply the 2-variables algorithm to $XY^3(Z^{4+h}), h \leq 4$; at each step we get

$$\{XY^3(Z^{4+h}), X^3Y^2(Z^{4+h}), X^4(Z^{4+h}), Y^5(Z^{4+h})\}$$

and since all elements are trivially to be discarded we get $\mathbf{G}(\mathsf{I})_3^+ = \emptyset$.

Further Steps Finally, since $X^{4+l}Y^{0+l} \in \mathbf{N}(\mathsf{I}), \forall\, l \leq 8$, we deduce that there is no generator with null Z-exponent, i.e. $\mathbf{G}(\mathsf{I})_4^- = \emptyset$. Since we also have $\mathbf{G}(\mathsf{I})_3^+ = \emptyset$, the algorithm terminates and we can conclude that $\mathbf{G}(\mathsf{I}) = \{XY^3Z^4, X^3Y^2Z^2, X^4Z, Y^5Z^3\}$.

4 A cryptographic application

The survey [7] reports on a class of cryptosystems whose scheme has been independently proposed by B. Barkee *et al.* [1] and by Fellows–Koblitz [3, 4, 5, 6]. Such schemes are defined on the commutative polynomial ring $\mathcal{P} = \mathbb{F}[X_1, \ldots, X_n]$ and consist in:

1. writing down an easy-to-produce Gröbner basis $\Gamma = \{\gamma_1, \ldots, \gamma_s\}$ generating an ideal $\mathsf{I} := \mathbb{I}(\Gamma) \subset \mathcal{P}$ and
2. publishing a set $G := \{g_1, \ldots, g_l\} \subset \mathsf{I}$ of polynomials in $\mathcal{P}$ and a set
$$T := \{\tau_1, \ldots, \tau_m\} \subset \mathbf{N}(\mathsf{I}) = \mathcal{T} \setminus \mathbf{T}(\mathsf{I})$$
of *normal terms* belonging to the Gröbner *sous-escalier* of I;
3. in order to send a message $M := \sum_{i=1}^m c_i\tau_i \in \mathrm{Span}_k(T)$, Bob (the sender) produces random polynomials $p_j \in \mathcal{P}, 1 \leq j \leq l, \deg(p_j) = \mathfrak{d}_j$, and encrypts M as $C := M + \sum_{j=1}^l p_j g_j$;
4. Alice (the receiver), possessing the Gröbner basis of I, applies Buchberger's reduction to obtain $\mathrm{Can}(C, \mathsf{I}, \prec) = M = \sum_{i=1}^m c_i\tau_i$.

Rai [10] proposed essentially the same system in the setting of the non-commutative polynomial ring $\mathcal{P} = \mathbb{F}\langle X_1, \ldots, X_n\rangle$: in his example the bilalteral ideal I is principal:
$$\mathsf{I} := \mathbb{I}(\Gamma) \subset \mathcal{P},\ \Gamma = \{\gamma\}$$
and the published set $G := \{g_1, \ldots, g_l\} \subset \mathsf{I}$ is defined as $g_i := h_i\gamma l_i$ for random elements $h_i, l_i \in \mathcal{P}$.

We now describe a Bulygin-like (see [2]) chosen-cyphertext attack on Barkee's cryptosystems under the assumption of knowing

(B.1). the set $\mathbf{G}(\mathsf{I}) := \{\mathbf{T}(\gamma_i) : 1 \leq i \leq s\}$ and

(B.2). for each $\gamma_i \in \Gamma$, a set of pairs (s_i, t_i) of terms s.t. $s_i w t_i \notin \mathbf{T}(\mathsf{I})$ for each $w \in \mathrm{supp}(\gamma_i)$.

Assuming the cryptoanalyst has temporary access to the decryption black box, according Bulygin's attack, he then builds fake cyphertexts
$$C_i := s_i\mathbf{T}(\gamma_i)t_i + \sum_j p_j g_j q_j;$$

the decripted version of this message being

$$\mathrm{Can}(C_i, \mathsf{I}, \prec) = \mathrm{Can}(s_i \mathbf{T}(g_i) t_i, \mathsf{I}, \prec) = s_i \, \mathrm{Can}(\mathbf{T}(g_i), \mathsf{I}, \prec) t_i$$

thus the attack allows him to read $\gamma_i = \mathbf{T}(\gamma_i) - \mathrm{Can}(\mathbf{T}(\gamma_i), \mathsf{I}, \prec)$.

Before discussing the relation between Bulygin's assumption (B.1) and our oracle-based algorithm, let us consider the queer assumption (B.2); it is justified by Bulygin as a tool for masking his attacks: *Polynomial t_i, s_i are chosen for masking the "fake" cyphertext* ([2], pg.2)

Assumption (B.2) is however completely useless: this "masking" in fact can be performed simply by choosing any set of polynomials $l_{i\iota}, r_{i\iota} \in \mathcal{P}$ satisfying $\mathbf{T}(\gamma_i) = \sum_\iota l_{i\iota} \mathbf{T}(\gamma_i) r_{i\iota}$, thus we obtain

$$\mathrm{Can}(\mathbf{T}(\gamma_i), \mathsf{I}, \prec) = \sum_\iota \mathrm{Can}(l_{i\iota} \mathbf{T}(\gamma_i) r_{i\iota}, \mathsf{I}, \prec)$$

and we thus succeed in crashing the system via the fake cyphertexts $l_{i\iota} \mathbf{T}(\gamma_i) r_{i\iota}$.

As regards assumption (B1), our investigation on the presented procedures was suggested by the aim of providing a tool to produce the set $\mathbf{G}(\mathsf{I})$ and thus showing that assumption (B1) was unnecessary; however this is not true, except in the commutative case where we can cryptoanalyse a Barkee's scheme via our solution to Problem 2, provided we know a bound for the degrees.

In fact we must stress that our solution of Problem 1 does not allow to reconstruct the set $\mathbf{G}(\mathsf{I})$, thus satysfying the necessary request (B1) by Bulygin, nor to cryptoanalyse a non-commutative Barkee's scheme: all we can do is to produce a subset $H = \{h_1, \ldots, h_m\} \subset \mathbf{G}(\mathsf{I})$ of the Gröbner basis $\Gamma(\mathsf{I}) = \{\gamma_1, \ldots, \gamma_s\}$ — used by Alice, via Buchberger's reduction, in order to read any message M encrypted as $C = M + \sum_{j=1}^{l} p_j g_j q_j$ — sufficient to produce a Gröbner representation

$$g_j = \sum_i c_{ij} \lambda_{ij} h_{\iota_{ij}} \rho_{ij}, \mathbf{T}(g_j) = \lambda_{1j} \mathbf{T}(h_{\iota_{1j}}) \rho_{1j} \succ \lambda_{2j} \mathbf{T}(h_{\iota_{2j}}) \rho_{2j} \succ \ldots$$

of each public element $g_j \in G$. Is this sufficient to obtain a Gröbner representation of $C - M$? Of course no: in fact after we distribute the expression $C - M = \sum_{j=1}^{l} p_j g_j q_j$ we obtain

$$C - M = \sum_{j=1}^{L} \sum_i c_j \lambda_j g_{\kappa_j} \rho_j, \lambda_j, \rho_j \in \mathcal{T}, c_j \in \mathbb{F} \setminus \{0\};$$

if we substitute each instance of g_{κ_j} with its Gröbner representation deduced by our algorithm we simply have:

$$C - M = \sum_{j=1}^{L} \sum_i c_j c_{i\kappa_j} \lambda_j \lambda_{i\kappa_j} h_{\iota_{i\kappa_j}} \rho_{i\kappa_j} \rho_j;$$

thus if we properly reenumerate the summands we obtain a representation

$$C - M = \sum_{k=1}^{K} d_k \lambda_k h_{\iota_k} \rho_k, \;\; \lambda_1 \mathbf{T}(h_{\iota_1})\rho_1 \succeq \lambda_2 \mathbf{T}(h_{\iota_2})\rho_2 \succeq \dots$$

but we can not rule out equalities; thus we don't obtain

$$\mathbf{T}(C - M) = \lambda_1 \mathbf{T}(h_{\iota_1})\rho_1 \succ \lambda_2 \mathbf{T}(h_{\iota_2})\rho_2 \succ \dots$$

and we cannot hope to successfully apply Buchberger reduction.

In fact, we can trivially build a theoretical counter-example by argueing as follows: assume that

$$\Omega := \lambda_1 \mathbf{T}(h_{\iota_1})\rho_1 = \lambda_2 \mathbf{T}(h_{\iota_2})\rho_2 \succ \lambda_3 \mathbf{T}(h_{\iota_3})\rho_3 \;\text{ and }\; d_1 \operatorname{lc}(h_{\iota_1}) + d_2 \operatorname{lc}(h_{\iota_2}) = 0;$$

as a consequence, $l := d_1 \lambda_1 h_{\iota_1} \rho_1 + d_2 \lambda_2 h_{\iota_2} \rho_2 \in \mathsf{I}$ necessarily satisfies $\mathbf{T}(l) \prec \Omega$ and has a Gröbner representation

$$l = \sum_{i=1}^{I} \bar{d}_i \bar{\lambda}_i \gamma_{\iota_i} \bar{\rho}_i, \qquad \mathbf{T}(l) = \bar{\lambda}_1 \mathbf{T}(\gamma_{\iota_1})\bar{\rho}_1 \succ \cdots$$

in terms of Γ but not necessarily of H. Therefore, we can not discard the possibility that both

$$\bar{\lambda}_1 \mathbf{T}(\gamma_{\iota_1})\bar{\rho}_1 = \mathbf{T}(l) \succ \lambda_3 \mathbf{T}(h_{\iota_3})\rho_3 \text{ and } \mathbf{T}(l) \notin \mathbb{I}(\mathbf{T}(h) : h \in H),$$

so that $\gamma_{\iota_1} \notin H$. In this unhappy, but realistic, situation we have the representation

$$C - M = \sum_{k=1}^{K} d_k \lambda_k h_{\iota_k} \rho_k = l + \sum_{k=3}^{K} d_k \lambda_k h_{\iota_k} \rho_k = \sum_{k=1}^{I} \bar{d}_i \bar{\lambda}_i \gamma_{\iota_i} \bar{\rho}_i + \sum_{k=3}^{K} d_k \lambda_k h_{\iota_k} \rho_k$$

where

$$\bar{\lambda}_1 \mathbf{T}(\gamma_{\iota_1})\bar{\rho}_1 \succ \bar{\lambda}_i \mathbf{T}(\gamma_{\iota_i})\bar{\rho}_i \text{ and } \bar{\lambda}_1 \mathbf{T}(\gamma_{\iota_1})\bar{\rho}_1 \succ \lambda_3 \mathbf{T}(h_{\iota_3})\rho_3 \succeq \lambda_k \mathbf{T}(h_{\iota_k})\rho_k, \forall\; i, k,$$

so that necessarily $\mathbf{T}(C - M) = \bar{\lambda}_1 \mathbf{T}(\gamma_{\iota_1})\bar{\rho}_1 \notin \mathbb{I}(\{\mathbf{T}(h) : h \in H\})$ and we can not perform Bucheberger reduction.

On the other side, in the commutative case, each potential message C necessarily satisfies

$$\deg(C) \leq \Delta := \max\{\deg(\tau_i), \deg(g_j) + \eth, \tau_i \in T, g_j \in G\}$$

and thus $D := \Delta$ is a 'reasonable' guess for degree bound $d(\mathsf{I})$. Of course the degree bound Δ on the messages does not necessarily satisfy $\Delta \geq d(\mathsf{I})$, so that our solution of Problem 2 would not cryptoanalyse Barkee's scheme using $D := \Delta$; however an implementation of Barkee's scheme in order to be protected against it must assure $\Delta \ll d(\mathsf{I})$.

While cryptoanalysing Barkee's schemes is an irrelevant task[9] we would like to briefly point to a connected problem, which is equally irrelevant but at least is a combinatorial amusement. The technical tool used by the Barkee's scheme in order to *write down an easy-to-produce Gröbner basis* was later revealed in [8] and simply consists into a combinatorial trick allowing, given any set of terms $\Upsilon := \{v_1, \ldots, v_s\} \subset \mathcal{T}$, to produce a polynomial set $\Gamma := \{\gamma_1, \ldots, \gamma_s\}$, satisfying $\mathbf{T}(\gamma_i) = v_i$, and giving a Gröbner basis of the ideal it generates.

In principle, a Barkee's scheme could write down a term set Υ and the related easy-to-produce Gröbner basis Γ, fix a value $D_0 \ll d(\mathbb{I}(\Gamma))$, extract from Γ the subset

$\Gamma' := \{\gamma \in \Gamma : \deg(\gamma) \leq D_0\}$ with the corresponding term set

$\Upsilon' := \{\mathbf{T}(\gamma) : \gamma \in \Gamma'\} = \{v \in \Upsilon : \deg(v) \leq D_0\} \subset \Upsilon$

and then produce the public set G just using the elements belonging to Γ' with

$$D_0 < \Delta := \max\{\deg(\tau_i), \deg(g_j) + \eth, \tau_i \in T, g_j \in G\} < d(\mathbb{I}(\Gamma)).$$

Recalling that our commutative procedure only deals with terms into the *box*

$$\mathcal{B}(D) := \{X_1^{a_1} \cdots X_n^{a_n} \in \mathbb{T} : 0 \leq a_i \leq D, \forall\, 1 \leq i \leq n\},$$

and informally calling D_0-*badly-connected* a set of terms Υ such that, if we apply our procedure to it with the value $D := D_0 < \max\{\deg(v) : v \in \Upsilon\}$ we are unable to produce the set $\Upsilon' := \{v \in \Upsilon : \deg(v) \leq D_0\}$, we remark that if Υ is D_0-badly connected, then in a Barkee's scheme, it would be nearly sufficient to make public a set $G \subset \mathbb{I}(\Gamma')$ in order to dwarf the use of our procedure in order to cryptoanalyse it.

The question, then, becomes the existence of badly connected sets of terms; we have the strong impression that the answer is negative[10]. Nevertheless, as we said above, we consider irrelevant to devote some time to this task.

References

[1] B. Barkee, D.C. Can, J. Ecks, T. Moriarty, R.F. Ree, Why you can not even hope to use Gröbner Bases in Public Key Cryptography. *J. Symb.Comp.* **18** (1994), 497–501.

[2] S. Bulygin, *Chosen-cyphertext attack on noncommutative Polly Cracker*, Manuscript, (2005) `http://arxiv.org/abs/cs/0508015v2`

[9] Barkee's scheme was just a provocation aimed to address research towards sparse systems like the ones independently investigated, at the same time, by Fellows-Koblitz. As for their non-commutative generalizations, we simply wonder how it was possible that they have attracted attention, though an algorithm providing their cryptoanalysis [[11], Th. 13] was already available since 1996.

[10] Consider the 2-variable case; in a minimal Gröbner basis Γ, for any two elements $X^aY^b, X^cY^d \in \mathbf{G}(\Gamma)$ $a < c$ imples $b > d$.

Thus, if $X^aY^b, X^cY^d \in \mathbf{G}(\Gamma)$ are D_0-badly connected, there must be an element $X^eY^f \notin \mathcal{B}(D)$ and which satisfyes $a < e < c, b > f > d$. For such elements necessarily either $D_0 < e < a$ or $D_0 < f < b$, contradicting the assumption that $\deg(X^aY^b), \deg(X^cY^d) \leq D_0$.

[3] M.R. Fellows, N. Koblitz, Kid krypto. Advances in Cryptography – Crypto'92, *Lect. N. Comp. Sci.* **740** (1993) 371–389

[4] M.R. Fellows, N. Koblitz, Combinatorially based cryptography for children (and adults). *Congressus Numerantium* **99** (1994) 9–41

[5] M.R. Fellows, N. Koblitz, Combinatorial cryptosystems galore! *Contemporary Math.* **168** 51–61 (1994)

[6] N. Koblitz, Algebraic Aspects of Cryptography, Springer (1998)

[7] F. Levy-dit-Vehel, M.G. Marinari, L. Perret, C. Traverso, *A Survey on Polly Cracker Systems* in [12] (2009) 285–305

[8] T. Mora, *The Nugis Groebnerialium 2: Applying Macaulay's Trick in Order to easily Write Down a Gröbner Basis* J. AAECC. **13** (2003), 437-4446.

[9] B.Mourrain, *Bezoutian and quotient ring structure* J. Symb. Comp. **39** (2005), 397-415

[10] T.S. Rai, *Infinite Gröbner bases and Noncommutative Polly Cracker Cryptosystems* PhD Thesis, Virginia Polytechnique Institute and State Univ. (2004)

[11] F.L. Prittchard, *The Ideal Membership Problem in Noncommutative Polynomial Rings* J. Symb. Comp. (1996) 27–48.

[12] M. Sala et al. (Ed.) *Gröbner bases, Coding, Cryptography*, Springer Risc XVI, (2009).