

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

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

$<$ a term-ordering on \mathcal{T} ,

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

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

$$\text{lc}(f) := c(f, \mathbf{T}(f)).$$

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

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

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

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

It holds

$$1. \mathcal{P} \cong I \oplus k[\mathbf{N}(I)];$$

$$2. \mathcal{P} \setminus I \cong k[\mathbf{N}(I)];$$

3. for each $f \in \mathcal{P}$, there is a unique

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

such that $f - g \in I$.

Moreover:

$$(a) \text{Can}(f_1, I) = \text{Can}(f_2, I) \iff f_1 - f_2 \in I;$$

$$(b) \text{Can}(f, I) = 0 \iff f \in I.$$

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

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

$<$ a term-ordering on \mathcal{T} ,

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

$\mathcal{P}^* := \text{Hom}_k(\mathcal{P}, k)$ the k -vector space of all k -linear functionals $\ell : \mathcal{P} \mapsto k$.

$$f \in \mathcal{P}, \ell \in \mathcal{P}^* \implies \ell(f) = \sum_{\tau \in \mathcal{T}} c(f, \tau) \ell(\tau).$$

\mathcal{P}^* is made a \mathcal{P} -module defining $\forall \ell \in \mathcal{P}^*, f \in \mathcal{P}$

$$\ell \cdot f \in \mathcal{P}^* \text{ as } (\ell \cdot f)(g) := \ell(fg) \forall g \in \mathcal{P}.$$

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

- *triangular* if

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

- *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

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

For each k -vector subspaces $P, P_1, P_2 \subset \mathcal{P}$ and each k -vector subspaces $L, L_1, L_2 \subset \mathcal{P}^*$ it holds

- P is an ideal iff $\mathfrak{L}(P)$ is a \mathcal{P} -module.
- L is a \mathcal{P} -module iff $\mathfrak{P}(L)$ is an ideal.
- $P_1 \subset P_2 \implies \mathfrak{L}(P_1) \supset \mathfrak{L}(P_2)$;
- $L_1 \subset L_2 \implies \mathfrak{P}(L_1) \supset \mathfrak{P}(L_2)$;
- $\mathfrak{L}(P_1 \cap P_2) \supset \mathfrak{L}(P_1) + \mathfrak{L}(P_2)$;
- $\mathfrak{P}(L_1 \cap L_2) \supset \mathfrak{P}(L_1) + \mathfrak{P}(L_2)$;
- $\mathfrak{L}(P_1 + P_2) = \mathfrak{L}(P_1) \cap \mathfrak{L}(P_2)$;
- $\mathfrak{P}(L_1 + L_2) = \mathfrak{P}(L_1) \cap \mathfrak{P}(L_2)$.
- $P = \mathfrak{P}\mathfrak{L}(P)$.
- $L \subset \mathfrak{L}\mathfrak{P}(L)$;
- $\dim_k(L) < \infty \implies L = \mathfrak{L}\mathfrak{P}(L)$.

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

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

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

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

Denote $\mathbf{N}(I) = \{t_1, \dots, t_r\}$, 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

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

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

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

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

and to re-enumerate the terms in $\mathbf{N}(I)$ 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

$$\mathfrak{q} := \{q_1, \dots, q_r\} \subset \mathcal{P}$$

which is triangular w.r.t. \mathbb{L} , and (a_{ij}) denotes the invertible matrix such that

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

then for each $\sigma \leq r$

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

If we now further assume that

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

so that

3. each $\mathfrak{l}_\sigma = \mathfrak{P}(L_\sigma)$ is a zero-dimensional ideal and
4. there is a chain $\mathfrak{l}_1 \supset \mathfrak{l}_2 \supset \dots \supset \mathfrak{l}_s = \mathfrak{l}$,

then

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

Theorem 1 (Möller) *Let $\mathcal{P} := k[X_1, \dots, X_n]$, and $<$ be any termordering. Let $\mathbb{L} = \{\ell_1, \dots, \ell_s\} \subset \mathcal{P}^*$ be a set of k -linear functionals such that $\mathfrak{P}(\text{Span}_k(\mathbb{L}))$ is a zero-dimensional ideal.*

Then there are

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

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

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

Theorem 1 (cont.) Let $\mathcal{P} := k[X_1, \dots, X_n]$, and $<$ be any termordering. Let $\mathbb{L} = \{\ell_1, \dots, \ell_s\} \subset \mathcal{P}^*$ be a set of k -linear functionals such that $\mathfrak{P}(\text{Span}_k(\mathbb{L}))$ is a zero-dimensional ideal.

Then there are

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

If, moreover, denoting $L := \text{Span}_k(\mathbb{L})$ and $\mathfrak{l} := \mathfrak{P}(L)$, we have

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

then it further holds

- $\lambda_\sigma = \ell_\sigma$,
- $\mathbb{N}(\mathfrak{l}_\sigma) = \{t_1, \dots, t_\sigma\}$ is an order ideal,
- $\mathfrak{l}_\sigma \oplus \text{Span}_k\{q_1, \dots, q_\sigma\} = \mathcal{P}$,
- $\mathbf{T}(q_\sigma) = t_\sigma$.

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

Corollary 1 (Lagrange Interpol. Formula)

Let

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

$<$ be any termordering.

$\mathbb{L} = \{\ell_1, \dots, \ell_s\} \subset \mathcal{P}^*$ be a set of k -linear functionals such that $I := \mathfrak{P}(\text{Span}_k(\mathbb{L}))$ is a 0-dim. ideal.

There exists a set $\mathfrak{q} = \{q_1, \dots, q_s\} \subset \mathcal{P}$ such that

1. $q_i = \text{Can}(q_i, I) \in \text{Span}_k(\mathbf{N}(I))$;
2. \mathbb{L} and \mathfrak{q} are triangular;
3. $\mathcal{P}/I \cong \text{Span}_k(\mathfrak{q})$.

There exists a set $\mathfrak{q}' = \{q'_1, \dots, q'_s\} \subset \mathcal{P}$ such that

1. $q'_i = \text{Can}(q'_i, I) \in \text{Span}_k(\mathbf{N}(I))$;
2. \mathbb{L} and \mathfrak{q}' are biorthogonal;
3. $\mathcal{P}/I \cong \text{Span}_k(\mathfrak{q}')$.

Let $c_1, \dots, c_s \in k$ and let $q := \sum_i c_i q'_i \in \mathcal{P}$. Then, if $\{g_1, \dots, g_t\}$ denotes a Gröbner basis of I , one has

1. q is the unique polynomial in $\text{Span}_k(\mathbf{N}(I))$ such that $\ell_i(q) = c_i$, for each i ;
2. for each $p \in \mathcal{P}$ it is equivalent
 - (a) $\ell_i(p) = c_i$, for each i ,
 - (b) $q = \text{Can}(p, I)$,
 - (c) exist $h_j \in \mathcal{P}_t$ such that

$$p = q + \sum_{j=1}^t h_j g_j, \mathbf{T}(h_j) \mathbf{T}(g_j) \leq \mathbf{T}(p - q).$$

Let

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

$<$ be any termordering;

$\mathbb{L} = \{\ell_1, \dots, \ell_r\} \subset \mathcal{P}^*$ be a set of linearly independent k -linear functionals such that $I := \mathfrak{P}(\text{Span}_k(\mathbb{L}))$ is a zero-dimensional ideal

and let

$$\mathbf{N} := \{t_1, \dots, t_r\} \subset \mathcal{T},$$

$$\mathbf{q} := \{q_1, \dots, q_r\} \subset \mathcal{P},$$

$$G := \{g_1, \dots, g_t\} \subset \mathcal{P},$$

be such that

- \mathbf{N} is an order ideal,
- $\text{Span}_k\{t_1, \dots, t_r\} = \text{Span}_k\{q_1, \dots, q_r\}$,
- $\{q_1, \dots, q_r\}$ and $\{\ell_1, \dots, \ell_r\}$ are triangular,
- $\ell(g) = 0$ for each $g \in G$ and each $\ell \in \mathbb{L}$,
- $\mathbf{N} \sqcup \mathbf{T}_{<}(G) = \mathcal{T}$,
- for each $g \in G$, $g - \text{lc}(g)\mathbf{T}_{<}(g) \in \text{Span}_k(\mathbf{N})$,

then G is a reduced Gröbner basis of $\mathfrak{P}(\text{Span}_k(\mathbb{L}))$ w.r.t. $<$.

$\mathbb{L} = \{\ell_1, \dots, \ell_s\} \subset \mathcal{P}^*$ is s.t.

$$L_\sigma := \text{Span}_k(\{\ell_1, \dots, \ell_\sigma\})$$

is a \mathcal{P} -module, for each $\sigma \leq s$,

$$I_\sigma = \mathfrak{P}(L_\sigma), \text{ for each } \sigma \leq s,$$

$G_\sigma \subset I_\sigma$ is the red. Gröbner basis of $I_\sigma, \forall \sigma \leq s$,

$\mathbf{N} := \{t_1, \dots, t_s\}$ is an order ideal,

$\mathbf{q} := \{q_1, \dots, q_s\} \subset \mathcal{P}$ is a set triangular to \mathbb{L} ,

$$\mathbf{N}_\sigma := \{t_1, \dots, t_\sigma\} = \mathbf{N}(I_\sigma), \forall \sigma \leq s,$$

$$q_\sigma \in \text{Span}_k\{\mathbf{N}_\sigma\}, \text{ and } \mathbf{T}(q_\sigma) = t_\sigma, \forall \sigma \leq s,$$

$$\text{Span}_k\{t_1, \dots, t_\sigma\} = \text{Span}_k\{q_1, \dots, q_\sigma\}, \forall \sigma \leq s,$$

$\{q_1, \dots, q_\sigma\}$ and $\{\ell_1, \dots, \ell_\sigma\}$ are triangular $\forall \sigma$.

$$\sigma := 1, t_1 := 1, \mathbf{N} := \{t_1\}, q_1 := \ell_1(1)^{-1}(t_1)t_1,$$

$$\mathbf{q} := \{q_1\}, G_1 := \{X_h - \ell_1(X_h), 1 \leq h \leq n\},$$

$$\% \% \mathbf{N}_\sigma \sqcup \mathbf{T}(G_\sigma) = \mathcal{T}.$$

$$\% \% \ell_j(f) = 0 \text{ for all } f \in G_\sigma, 1 \leq j \leq \sigma.$$

For $\sigma := 2..s$ **do**

$$t := \min\{\mathbf{T}(f) : f \in G_\sigma, \ell_\sigma(f) \neq 0\},$$

$$\text{Let } f \in G_\sigma : \mathbf{T}(f) = t,$$

$$t_\sigma := t, q_\sigma := \ell_\sigma^{-1}(f)f,$$

$$\mathbf{N} := \mathbf{N} \cup \{t_\sigma\}, \mathbf{q} := \mathbf{q} \cup \{q_\sigma\},$$

$$G_\sigma := \{f - \ell_\sigma(f)q_\sigma : f \in G_{\sigma-1}\}.$$

For each $h = 1..n : X_{ht} \notin \mathbf{T}(G_\sigma)$ **do**

$$p := X_{ht},$$

$$\text{For } i = 1..\sigma \text{ do } p := p - \ell_i(p)q_i,$$

$$G_\sigma := G_\sigma \cup \{p\};$$

$$\% \% \mathbf{N}_\sigma \sqcup \mathbf{T}(G_\sigma) = \mathcal{T},$$

$$\% \% \ell_j(f) = 0 \text{ for all } f \in G_\sigma, 1 \leq j \leq \sigma.$$

$\mathbb{L} = \{\ell_1, \dots, \ell_s\} \subset \mathcal{P}^*$ is s.t. $I := \mathfrak{P}(\text{Span}_k(\mathbb{L}))$ is a zero-dimensional ideal;

$G \subset I$ is the reduced Gröbner basis of I w.r.t. $<$;

$r = \deg(I) = \dim_k(\text{Span}_k(\mathbb{L}))$;

$\mathbf{N} := \{t_1, \dots, t_r\} = \mathbf{N}(I)$;

$1 = t_1 < t_2 < \dots < t_i < t_{i+1} < \dots < t_r$,

$\Lambda := \{\lambda_1, \dots, \lambda_r\} \subset \mathbb{L}$, is a linearly independent basis of $\text{Span}_k(\mathbb{L})$;

$\mathbf{q} := \{q_1, \dots, q_r\} \subset \mathcal{P}$ is a set triangular to Λ ;

$q_i \in \text{Span}_k\{t_1, \dots, t_i\}$, $\mathbf{T}(q_i) = t_i$, for each $i \leq r$;

$\text{Span}_k\{t_1, \dots, t_i\} = \text{Span}_k\{q_1, \dots, q_i\}$, for each $i \leq r$;

$\{q_1, \dots, q_i\}$ and $\{\lambda_1, \dots, \lambda_i\}$ are triangular, for each $i \leq r$.

$G := \emptyset, r := 1, t_1 := 1, \mathbf{N} := \{t_1\},$

$v := (\ell_1(t_1), \dots, \ell_s(t_1)),$

$\mu := \min\{j : \ell_j(1) \neq 0\},$

$\lambda_1 := \ell_\mu, \Lambda := \{\lambda_1\},$

$q_1 := \lambda_1(1)^{-1}t_1, \mathbf{q} := \{q_1\}, \text{vect}(1) := \lambda_1(1)^{-1}v,$

$\% \text{ vect}(1) = (\ell_1(q_1), \dots, \ell_s(q_1)),$

While $\mathbf{N} \sqcup \mathbf{T}(G) \neq \mathcal{T}$ **do**

$t := \min_{<} \{\tau \in \mathcal{T}, \tau \notin \mathbf{N} \sqcup \mathbf{T}(G)\},$

$q := t, v := (\ell_1(q), \dots, \ell_s(q))$

For $j = 1..r$ **do**

$v := v - \lambda_j(q) \text{vect}(j), q := q - \lambda_j(q)q_j,$

$\% \text{ } v = (\ell_1(q), \dots, \ell_s(q)).$

If $v = 0$ **then**

$G := G \cup \{q\},$

else

$r := r + 1$

$t_r := t, \mathbf{N} := \mathbf{N} \cup \{t_r\},$

$\mu := \min\{j : \ell_j(q) \neq 0\},$

$\lambda_r := \ell_\mu, \Lambda := \Lambda \cup \{\lambda_r\},$

$q_r := \lambda_r(q)^{-1}q, \mathbf{q} := \mathbf{q} \cup \{q_r\}, \text{vect}(r) := \lambda_r(q)^{-1}v$

$\% \text{ vect}(i) = (\ell_1(q_i), \dots, \ell_s(q_i))$ for each $i, 1 \leq i \leq r$

$G, r, \mathbf{N}, \Lambda, \mathbf{q}$

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

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

$<$ a term-ordering on \mathcal{T} ,

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

Block orderings on $k[X_1, \dots, X_\nu][X_{\nu+1}, \dots, X_n]$

$$X_1^{a_1} \cdots X_\nu^{a_\nu} < X_i, \forall (a_1, \dots, a_\nu) \in \mathbb{N}^\nu, i > \nu$$

have the elimination property:

- $G \cap k[X_1, \dots, X_\nu]$ is the Gröbner basis of $I \cap k[X_1, \dots, X_\nu]$.

The **lex ordering** induced by $X_1 < \dots < X_n$ has the elimination property on $k[X_1][X_2] \cdots [X_{n-1}][X_n]$:

- $G \cap k[X_1, \dots, X_\nu]$ is the Gröbner basis of $I \cap k[X_1, \dots, X_\nu], \forall \nu < n$

The **degrevlex ordering** $<$ induced by $X_1 < \dots < X_n$ is the ordering obtained by reversing the result of the lex ordering \prec induced by $X_n \prec \dots \prec X_1$ on homogeneous components of \mathcal{T} :

$$\tau < \omega \iff \begin{cases} \deg(\tau) < \deg(\omega) & \text{or} \\ \deg(\tau) = \deg(\omega) & \tau \succ \omega \end{cases}$$

For its elimination property, the *lex* is a good tool for solving [Gianni–Kalkbener, Lazard’s triangular sets] or for applications [see the CRHT-like algorithms in BCH codes] but both practical experience and theoretical argument show that, in general, *lex* is a very bad choice for applying Buchberger Algorithm.

On the other side the *degrevlex ordering* is the *optimal* choice for applying Buchberger Algorithm

- Bayer D., Stillman M., A Theorem on Refining Division Orders by the Reverse Lexicographic Order, *Duke J. Math.* **55** (1987), 321–328.

This suggests the

Problem 1 (FGLM Problem) *Given*

- a termordering $<$ on the polynomial ring $\mathcal{P} := k[X_1, \dots, X_n]$,
- a zero-dimensional ideal $I \subset \mathcal{P}$ and
- its reduced Gröbner basis G_{\prec} w.r.t. the term-ordering \prec ,

to deduce the Gröbner basis $G_{<}$ of I w.r.t. $<$.

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

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

\prec a term-ordering on \mathcal{T} ,

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

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

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

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

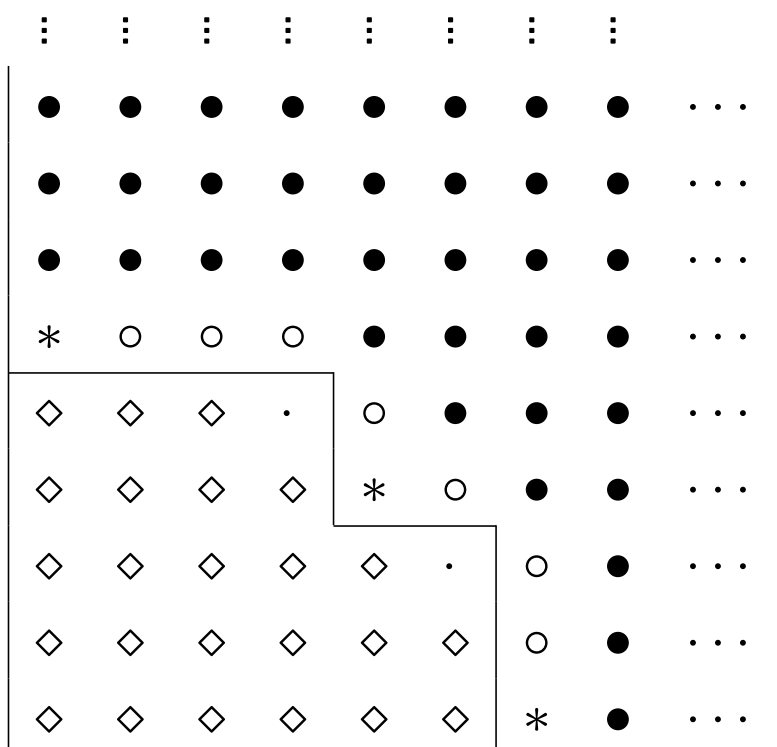
◇ $\mathbf{N}(I) := \mathbf{N}_{\prec}(I) = \mathcal{T} \setminus \mathbf{T}_{\prec}(I)$ an order ideal,

○ $\mathbf{B}_{\prec}(I) := \{X_h \tau : 1 \leq h \leq n, \tau \in \mathbf{N}_{\prec}(I)\} \setminus \mathbf{N}_{\prec}(I)$,

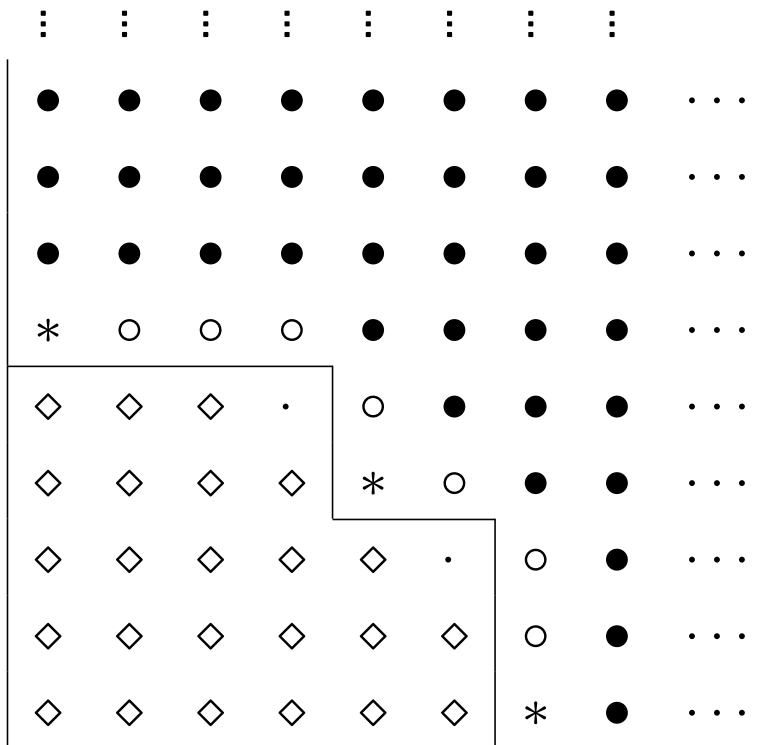
● $\mathbf{I}_{\prec}(I) := \mathbf{T}_{\prec}(I) \setminus \mathbf{B}_{\prec}(I)$,

* $\mathbf{G}_{\prec}(I) \subset \mathbf{B}_{\prec}(I)$ the unique minimal basis of $\mathbf{T}_{\prec}(I)$,

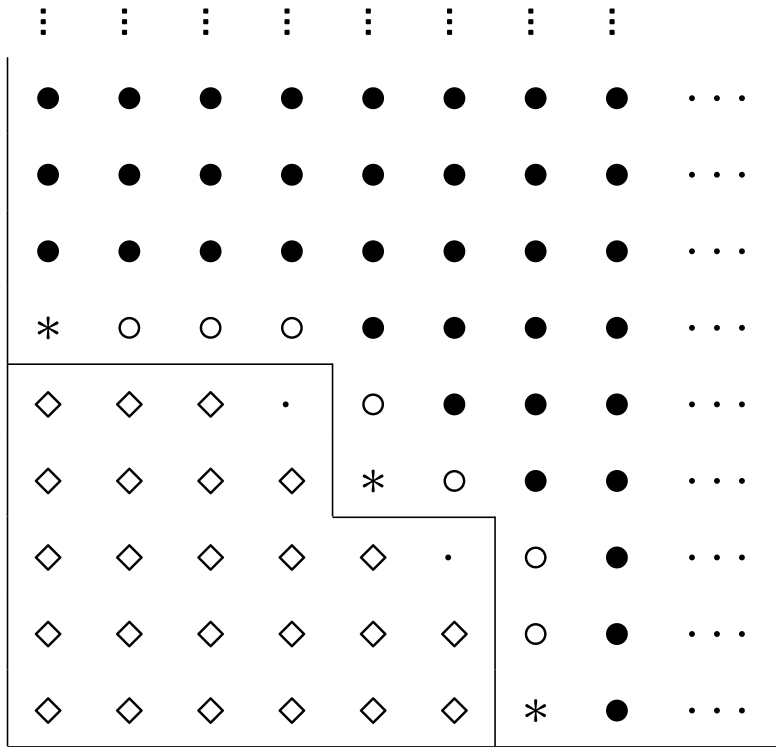
· $\mathbf{C}_{\prec}(I) := \{\tau \in \mathbf{N}_{\prec}(I) : X_h \tau \in \mathbf{T}_{\prec}(I), \forall h\}$.



- $\mathbf{T}_{\prec}(\mathfrak{I}) = \{\tau \in \mathcal{T} : \exists g \in \mathfrak{I} : \mathbf{T}_{\prec}(g) = \tau\}$;
- $\mathbf{I}_{\prec}(\mathfrak{I}) = \{\tau \in \mathbf{T}_{\prec}(\mathfrak{I}) : X_i \mid \tau \implies \frac{\tau}{X_i} \in \mathbf{T}_{\prec}(\mathfrak{I})\}$;
- $\mathbf{B}_{\prec}(\mathfrak{I}) = \{\tau \in \mathbf{T}_{\prec}(\mathfrak{I}) : \exists X_i \mid \tau, \frac{\tau}{X_i} \in \mathbf{N}_{\prec}(\mathfrak{I})\}$;
- $\mathbf{G}_{\prec}(\mathfrak{I}) = \{\tau \in \mathbf{T}_{\prec}(\mathfrak{I}) : \forall X_i \mid \tau, \frac{\tau}{X_i} \in \mathbf{N}_{\prec}(\mathfrak{I})\}$;
- $\mathbf{C}_{\prec}(\mathfrak{I}) = \{\tau \in \mathbf{N}_{\prec}(\mathfrak{I}) : \forall i, X_i \tau \in \mathbf{B}_{\prec}(\mathfrak{I})\}$;
- $\mathbf{N}_{\prec}(\mathfrak{I}) = \{\tau \in \mathcal{T} : \nexists g \in \mathfrak{I} : \mathbf{T}_{\prec}(g) = \tau\}$;
- $\mathbf{C}_{\prec}(\mathfrak{I}) \cup \mathbf{T}_{\prec}(\mathfrak{I})$ is a monomial ideal;
- $\mathbf{N}_{\prec}(\mathfrak{I}) \cup \mathbf{G}_{\prec}(\mathfrak{I})$ and $\mathbf{N}_{\prec}(\mathfrak{I}) \cup \mathbf{B}_{\prec}(\mathfrak{I})$ are order ideals.



- $\tau \in \mathbf{I}_{\prec}(\mathbb{I}) \iff \forall X_i \mid \tau, \frac{\tau}{X_i} \in \mathbf{T}_{\prec}(\mathbb{I});$
- $\tau \in \mathbf{B}_{\prec}(\mathbb{I}) \setminus \mathbf{G}_{\prec}(\mathbb{I}) \iff \exists h, H : \frac{\tau}{X_h} \in \mathbf{N}_{\prec}(\mathbb{I}), \frac{\tau}{X_H} \in \mathbf{B}_{\prec}(\mathbb{I}) \subset \mathbf{T}_{\prec}(\mathbb{I});$
- $\tau \in \mathbf{B}_{\prec}(\mathbb{I}) \setminus \mathbf{G}_{\prec}(\mathbb{I}) \implies \forall X_i \mid \tau, \frac{\tau}{X_i} \in \mathbf{N}_{\prec}(\mathbb{I}) \cup \mathbf{B}_{\prec}(\mathbb{I});$
- $\tau \in \mathbf{N}_{\prec}(\mathbb{I}) \cup \mathbf{G}_{\prec}(\mathbb{I}) \iff \forall X_i \mid \tau, \frac{\tau}{X_i} \in \mathbf{N}_{\prec}(\mathbb{I});$
- $\tau \in \mathbf{T}_{\prec}(\mathbb{I}) \cup \mathbf{C}_{\prec}(\mathbb{I}) \iff \forall X_i \mid \tau, \frac{\tau}{X_i} \in \mathbf{T}_{\prec}(\mathbb{I});$
- $\tau \in \mathbf{N}_{\prec}(\mathbb{I}) \setminus \mathbf{C}_{\prec}(\mathbb{I}) \iff \exists h : X_h \tau \in \mathbf{N}_{\prec}(\mathbb{I}).$



Macaulay(1913-16), FGLM, Traverso(\approx 1982-3)

The *border basis* of I w.r.t. \prec is the set

$$\{\tau - \text{Can}(\tau, I, \prec) : \tau \in \mathbf{B}_{\prec}(I)\}.$$

A *Gröbner representation* of I is the assignement of

- a linearly independent set $\mathbf{q} = \{q_1, \dots, q_s\}$,

$$q_1 = 1 : \mathcal{P}/I = \text{Span}_k(\mathbf{q}),$$

- the set

$$\mathcal{M} = \mathcal{M}(\mathbf{q}) := \left\{ \left(a_{lj}^{(h)} \right) \in k^{s^2}, 1 \leq h \leq n \right\}$$

of the square matrices $\left(a_{lj}^{(h)} \right)$ defined by the equalities

$$X_h q_l = \sum_j a_{lj}^{(h)} q_j, \forall l, j, h, 1 \leq l, j \leq s, 1 \leq h \leq n$$

in $\mathcal{P}/I = \text{Span}_k(\mathbf{q})$.

For each $f \in \mathcal{P}$ the *Gröbner description* of f in terms of a Gröbner representation $(\mathbf{q}, \mathcal{M})$ is the unique vector

$$\mathbf{Rep}(f, \mathbf{q}) := (\gamma(f, q_1, \mathbf{q}), \dots, \gamma(f, q_s, \mathbf{q})) \in k^s$$

such that $f - \sum_j \gamma(f, q_j, \mathbf{q}) q_j \in I$.

The *linear representation* of I w.r.t. \prec is the Gröbner representation

$$(\mathbf{N}_{\prec}(I), \mathcal{M}(\mathbf{N}_{\prec}(I))), \mathbf{q} = \mathbf{N}_{\prec}(I).$$

With these definitions, if \prec is a termordering and $\mathbf{N}_{\prec}(I) = \{\tau_1, \dots, \tau_s\}$, the *Gröbner description*

$$\mathbf{Rep}(f, \mathbf{N}_{\prec}(I)) := (\gamma(f, \tau_1, \mathbf{N}_{\prec}(I)), \dots, \gamma(f, \tau_s, \mathbf{N}_{\prec}(I)))$$

of f in terms of the linear representation of I w.r.t. \prec is a convoluted synonymous of the notion of the canonical form

$$\text{Can}(f, I, \prec) = \sum_{j=1}^s \gamma(f, \tau_j, \prec) \tau_j = \sum_{j=1}^s \gamma(f, \tau_j, \mathbf{N}_{\prec}(I)) \tau_j$$

of f in terms of \prec .

Let \prec be a termordering and $\mathbf{N}_\prec(\mathbb{I}) = \{\tau_1, \dots, \tau_s\}$; in order to apply Möller Algorithm to the FGLM Problem, we just need to choose as functionals $\mathbb{L} := \{\ell_1, \dots, \ell_s\}$ the coefficients of the canonical forms

$$\ell_i(\cdot) := \gamma(\cdot, \tau_i, \mathbf{N}_\prec(\mathbb{I}))$$

so that we need to compute

$$\mathbf{Rep}(f, \mathbf{N}_\prec(\mathbb{I})) := (\gamma(f, \tau_1, \mathbf{N}_\prec(\mathbb{I})), \dots, \gamma(f, \tau_s, \mathbf{N}_\prec(\mathbb{I})))$$

for each $f \in \mathbb{B} := \{X_i \tau_j, 1 \leq i \leq n, 1 \leq j \leq s\}$.

Such elements being treated by \prec -increasing ordering, when the **While**-loop is treating a term $X_h \tau_l$, we have previously managed the term τ_l so that we previously computed $\mathbf{Rep}(\tau_l, \mathbf{N}_\prec(\mathbb{I}))$ which satisfies the relation

$$\tau_l - \sum_{j=1}^s \gamma(\tau_l, \tau_j, \prec) \tau_j = \tau_l - \text{Can}(\tau_l, \mathbb{I}, \prec) \in \mathbb{I},$$

so that

$$X_h \tau_l - \sum_{j=1}^s \gamma(\tau_l, \tau_j, \prec) X_h \tau_j \in \mathbb{I},$$

and

$$\begin{aligned} \text{Can}(X_h \tau_l, \mathbb{I}, \prec) &= \sum_{j=1}^s \gamma(\tau_l, \tau_j, \prec) \text{Can}(X_h \tau_j, \mathbb{I}, \prec) \\ &= \sum_{i=1}^s \left(\sum_{j=1}^s \gamma(\tau_l, \tau_j, \prec) \gamma(X_h \tau_j, \tau_i, \prec) \right) \tau_i. \end{aligned}$$

For the \prec -minimal $\omega := X_h \tau_l \in B$ we have

- if $\omega \notin \mathbf{T}_{\prec}(I)$ then $\omega \in \mathbf{N}_{\prec}(I)$, so that we add ω to \mathbf{N} and $\{\omega X_h : 1 \leq h \leq n\}$ to B ;
- if there is $g \in G_{\prec}$ such that $\mathbf{T}_{\prec}(g) = \omega$ and $g = \omega - \sum_{\tau \in \mathbf{N}_{\prec}(I)} \gamma(\omega, \tau, \prec) \tau$, since the procedure iterates on \prec -increasing values of ω , we have

$$\gamma(\omega, \tau, \prec) \neq 0 \implies \tau \prec \omega \implies \tau \in \mathbf{N};$$

- if there is $H, 1 \leq H \leq n, \tau \in \mathbf{T}_{\prec}(I)$ such that $\omega = X_H \tau$; thus $\tau \prec \omega$ has been already treated so that we have obtained a representation $\text{Can}(\tau, I, \prec) = \sum_{j=1}^s \gamma(\tau, \prec, \tau_j) \tau_j$; since in such representation we have

$$\gamma(\tau, \prec, \tau_j) \neq 0 \implies \tau_j \prec \tau \implies \tau_j \in \mathbf{N}, X_H \tau_j \prec X_H \tau = \omega,$$

we also have the representation

$$\text{Can}(X_H \tau, I, \prec) = \sum_{j=1}^s \gamma(\tau, \prec, \tau_j) \text{Can}(X_H \tau_j, I, \prec)$$

and we can use the same formula as above to derive

$$\begin{aligned} \gamma(X_h \tau_l, \tau_i, \prec) &= \gamma(X_H \tau, \tau_i, \prec) \\ &= \sum_{j=1}^s \gamma(\tau, \tau_j, \prec) \gamma(X_H \tau_j, \tau_i, \prec) \\ &= \sum_{j=1}^s \gamma(X_h \tau_l, \tau_j, \prec) \gamma(X_H \tau_j, \tau_i, \prec). \end{aligned}$$

$(\mathbf{N}_{\prec}, \mathcal{M}) := \mathbf{FGLM}\text{-Matrix}(G_{\prec})$ where

$G_{\prec} \subset I$ is the reduced Gröbner basis of I w.r.t. \prec ;

$s = \deg(I)$,

$\mathbf{N}_{\prec} := \{\tau_1, \dots, \tau_s\} = \mathbf{N}_{\prec}(I)$,

$1 = \tau_1 \prec \tau_2 \prec \dots \prec \tau_j \prec \tau_{j+1} \prec \dots \prec \tau_s$,

$\mathcal{M} = \mathcal{M}(\mathbf{N}_{\prec}) = \left\{ \left(a_{lj}^{(h)} \right) \in k^{s^2}, 1 \leq h \leq n \right\}$ is the set of the square matrices defined by the equalities $X_h \tau_l = \sum_j a_{lj}^{(h)} \tau_j$ in $\mathcal{P}/I = \text{Span}_k(\mathbf{N}_{\prec})$;

$r := 1, \tau_1 := 1, \mathbf{N}_{\prec} := \{\tau_1\}, \mathbf{B} := \{X_h : 1 \leq h \leq n\}$,

While $\mathbf{B} \neq \emptyset$ **do**

$\omega := \min_{\prec}(\mathbf{B}), \mathbf{B} := \mathbf{B} \setminus \{\omega\}$,

$h, l : \omega := X_h \tau_l$

If $\omega \notin \mathbf{T}_{\prec}(I)$ **then**

$r := r + 1$

$\tau_r := \omega, \mathbf{N}_{\prec} := \mathbf{N}_{\prec} \cup \{\tau_r\}, \mathbf{B} := \mathbf{B} \cup \{X_h \tau_r : 1 \leq h \leq n\}$,

$a_{lr}^{(k)} := 1$;

else

if $\exists g := \mathbf{T}_{\prec}(g) - \sum_{j=1}^r \gamma(\omega, \tau_j, \prec) \tau_j \in G_{\prec} : \mathbf{T}_{\prec}(g) = \omega = X_h \tau_l$ **then**

For $j = 1..r$ **do** $a_{lj}^{(h)} := \gamma(\omega, \tau_j, \prec)$

else

Let $H, \iota : 1 \leq H \leq n, 1 \leq \iota \leq r : X_H \tau_{\iota} \in \mathbf{T}_{\prec}(G_{\prec}), \tau_{\iota} = X_H \tau_{\iota}$;

For $i = 1..r$ **do** $a_{li}^{(h)} := \sum_{j=1}^r a_{lj}^{(h)} a_{ji}^{(H)}$

For each $H, i : X_H \tau_i = \omega$ **do**

For $j = 1..r$ **do** $a_{ij}^{(H)} := a_{lj}^{(h)}$;

$\mathbf{N}_{\prec}, \mathcal{M}$

$(\mathbf{N}_{\prec}, \mathcal{M}) := \mathbf{FGLM}\text{-Matrix}(G_{\prec})$

$G := \emptyset, r := 1, t_1 := 1, \mathbf{N} := \{t_1\}, q_1 := 1, \mathbf{q} := \{q_1\},$

$\mathbf{B} := \{X_h, 1 \leq h \leq n\}$

$\text{vect}(1) := (1, 0, \dots, 0), \mu(1) := 1,$

$\% \text{ vect}(1) = \mathbf{Rep}(q_1, \mathbf{N}_{\prec}), \mu(1) = \min\{j : \gamma(q_1, \tau_j, \prec) \neq 0\}$

Let $\mathbf{B} := \{(X_h, h, 1), 1 \leq h \leq n\}$

While $\mathbf{B} \neq \emptyset$ **do**

$t := \min_{\prec}(\mathbf{B}), \mathbf{B} := \mathbf{B} \setminus \{t\},$

$l, h : t = X_{htl} = X_h \mathbf{T}_{\prec}(q_l)$

If $t \notin \mathbf{T}_{\prec}(G)$ **then**

$q := X_h q_l$

For $i = 1..s$ **do** $v_i := \sum_{j=1}^s \gamma(q_l, \tau_j, \prec) a_{ji}^{(h)};$

$v := (v_1, \dots, v_s)$

$\% \text{ } v = \mathbf{Rep}(q, \mathbf{N}_{\prec})$

For $j = 1..r$ **do**

$v := v - \gamma(q, \tau_{\mu(j)}, \prec) \text{vect}(j), q := q - \gamma(q, \tau_{\mu(j)}, \prec) q_j,$

$\% \text{ } v = \mathbf{Rep}(q, \mathbf{N}_{\prec})$

If $v = 0$ **then**

$G := G \cup \{q\},$

else

$r := r + 1$

$t_r := t, \mathbf{N} := \mathbf{N} \cup \{t_r\},$

$\mu(r) := \min\{j : \gamma(q, \tau_j, \prec) \neq 0\},$

$q_r := \gamma(q, \tau_{\mu(r)}, \prec)^{-1} q, \text{vect}(r) := \gamma(q, \tau_{\mu(r)}, \prec)^{-1} v$

$\% \text{ vect}(i) = \mathbf{Rep}(q_i, \mathbf{N}_{\prec}), \forall i, 1 \leq i \leq r$

$\mathbf{q} := \mathbf{q} \cup \{q_r\},$

$\mathbf{B} := \mathbf{B} \cup \{X_h t_r, 1 \leq h \leq n\},$

$G, \mathbf{N}, \mathbf{q}$

Berlekamp-Massey-Sakata a sort of FGLM on modules with functionals depending on the state of the computation.

- J. Todd, H. Coxeter, A practical method for enumerating cosets of a finite abstract group. *Proc. Edinburgh Math. Soc.*, **5**(1936)

Verbatim FGLM-Matrix over groups view as quotient of non-comm. polynomial rings modulo bimonomial ideals.

- Buchberger B., Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal, *Ph. D. Thesis, Innsbruck*, (1965)
- Buchberger B., Ein algorithmisches Kriterium für die Lösbarkeit eines algebraischen Gleichungssystem, *Aeq. Math.* **4** (1970), 374–383

Solved the FGLM Problem essentially by the FGLM Algorithm

- Möller H.M., Buchberger B., The construction of multivariate polynomials with preassigned zeros, *L. N. Comp. Sci.* **144** (1982), 24–31, Springer

Interpolation on multivariate points

- P. Gianni, Algebraic solution of systems of polynomial equations using Gröbner bases, *L. N. Comp. Sci.* **356** (1989), 247–257

FGLM-like Algorithm for effectively perform generic change of coordinate

- Sasaki T. , Some algebraic algorithms based on head term elimination over polynomial ring *L. N. Comp. Sci.* **378** (1987), 24–31, Springer

Iteratively compute

$$I_i := \mathbb{I}(G_i) \subset k[X_1, \dots, X_{i-1}][X_i], G_{i-1} := G_i \cap k[X_1, \dots, X_{i-1}].$$

- Faugère J.C., Gianni P., Lazard D., Mora T. Efficient Computation of Zero-dimensional Gröbner Bases by Change of Ordering. *J. Symb. Comp.* **16** (1993), 329–344.

FGLM-Problem, FGLM-Matrix, FGLM-Algorithm, FGLM-complexity

- Marinari M.G., Möller H.M. Gröbner Bases of Ideals Defined by Functionals with an Application to Ideals of Projective Points. *J AAECC* (1993), **4**, 103–145.

Generalizing Möller and FGLM Algorithm to general functional evaluation

Implementation via p -modular evaluation and CRT interpolation

- Alonso M.E., Marinari M.G., The big Mother of all Dualities: Möller Algorithm, *Comm. Alg.* (2003), 374–383

A survey with further applications to canonical modules

- S. Licciardi, Implicitization of hypersurfaces and curves by the Primbasissatz and basis conversion, *Proc. IS-SAC'94* (1994) 191-196

Generalizing FGLM to the higherdim. case. Not effective.

- Collard S., Mall D., Kalkbrener M., *The Gröbner Walk* (1993)

Solves the FGLM-Problem via performing small changes within the Gröbner Fan. A loser: zillion slower even of the original FGLM.

- Traverso C., Hilbert function and the Buchberger algorithm, *J. Symb. Comp.* **22** (1996), 355–376

Until yesterday, the most efficient solution for the FGLM-Problem. Wlog assume the ideal homogeneous and use the knowledge of its Hilbert Function to predict how many new generators of a fixed degree are needed in the G-bases; when such generators are produced, all other S-pairs of same degree are discarded; the Hilbert function is re-evaluated and the computation is performed in higher degree.

- Basiri A., Faugère J.-C., Changing the ordering of Gröbner Bases with LLL: Case of Two Variables, *Proc. IS-SAC'03* (2003) 23-28

“The worst case complexity [...] is not better than the complexity of the FGLM algorithm; but also give the theoretical complexity with some parameters depending on the size of the output. When the output is small the algorithm is more efficient.”

- Sala M. , Personal communication (2005)

For a random suitable weight, the weight-compatible ordering $<$ has the property that $G_{<} \cap k[X_1, \dots, X_{n-1}]$ is a G-basis of $I \cap k[X_1, \dots, X_{n-1}]$. Thus, one

- iteratively computes, $i = n - 1..1$, the G-basis G_i of $I_i := I \cap k[X_1, \dots, X_i]$
- $H_1 := G_1$
- iteratively , $i = 1..n - 1$, applies Buchberger algorithm to $H_i \cup G_{i+1}$ in order to obtain the lex G-basis $H_{i+1} \subset k[X_1, \dots, X_{i+1}]$ for I_{i+1} .

- Lakshman Y.N., *A Single Exponential Bound on the Complexity of Computing Gröbner Bases of Zero Dimensional Ideals* , Progress in Mathematics **94** (1990), 227–234, Birkhäuser

FGLM as a good-complexity tool for intersecting 0-dim. ideals

- Abbott J.; Bigatti A.; Kreuzer M.; Robbiano L. Computing Ideals of Points. *J. Symb.Comp.* , **30** (2000), 341–356.

Extending Marinari–Möller to projective spaces

- Reinhert B., Madlener K., A Note on Nielsen Reduction and Coset Enumeration. *Proc. ISSAC'98* , (1998), 171–178.

Rereeding Todd-Coxeter in terms of non-commut. FGLM

- Borges-Trenard M.A., Borges-Quintana M., Computing Gröbner Bases by FGLM Techniques in a Noncommutative Settings. *J. Symb.Comp.* , **30** (2000), 429–449.

FGLM Algorithm in non-commutative setting

- M. Borges-Quintana, M. A. Borges-Trenard, E. Martinez-Moro A general framework for applying FGLM techniques to linear codes
- M. Borges-Quintana, M.A. Borges-Trenard, P. Fitzpatrick, E. Martinez-Moro Groebner bases and combinatorics for binary codes
- M. Borges-Quintana, M. Borges-Trenard, E. Martinez-Moro On a Grobner bases structure associated to linear codes

Structure of the FGLM-Matrix for a binomial ideal.

Application to linear codes

Binomial ideals: each basis element has the shape $\tau_1 - \tau_2, \tau_i$ terms.

Let

$I \subset \mathbb{Z}_2[X_1, \dots, X_n]$, a binomial 0-dim. ideal,

$$\mathbf{N}(I) = \{\tau_0 = 1, \tau_1, \dots, \tau_s\}$$

Then

1. $\forall \ell, 1 \leq \ell \leq s \exists! h, l, 1 \leq h \leq n, 0 \leq l < s, : h := \min\{i : X_i \mid \tau_\ell, \} \tau_\ell = X_h \tau_l$
2. $\forall h, l, 1 \leq h \leq n, 1 \leq l \leq s, \exists! \ell : \text{Can}(X_h \tau_l, I) = \tau_\ell$

Therefore encoding a linear $[n, k]$ -code by encoding the generating matrix (a_{ij}) by the polynomial ideal

$$I = \left\{ \prod_{j=1}^n X_j^{a_{ij}} - 1, 1 \leq i \leq k \right\}$$

and each codeword $(a_1, \dots, a_n) \in \mathbb{Z}_2^n$ as $\prod_{j=1}^n X_j^{a_j}$, for any codeword $\tau \in \mathcal{T}$, the maximum likelihood decoding error is $\text{Can}(\tau, I)$.

Thus

- use an improved version of the FGLM algorithm for binomial ideals to deduce the data above
- decoding codewords using such data

For the code whose parity check matrix is

$$H^T := \begin{vmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 \end{vmatrix}$$

we have $N(I) = \{1, X_1, X_2, X_3, X_4, X_5, X_6, X_1X_6\}$, which we encode as

$$\tau_\ell = X_h \tau_l \text{ in the table } \begin{array}{c|cccccccc} \ell & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ \hline h & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ l & 1 & 2 & 3 & 4 & 5 & 6 & 6 \end{array}$$

and whose corresponding FGLM-matrix is

$$\text{Can}(X_h \tau_l, I) = \tau_\ell \begin{array}{c|cccccccc} & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ \hline 1 & 1 & 0 & 5 & 4 & 3 & 2 & 7 & 6 \\ 2 & 2 & 5 & 0 & 7 & 6 & 1 & 4 & 3 \\ 3 & 3 & 4 & 7 & 0 & 1 & 6 & 5 & 2 \\ 4 & 4 & 3 & 6 & 1 & 0 & 7 & 2 & 5 \\ 5 & 5 & 2 & 1 & 6 & 7 & 0 & 3 & 4 \\ 6 & 6 & 7 & 4 & 5 & 2 & 3 & 0 & 1 \\ 7 & 7 & 6 & 3 & 2 & 5 & 4 & 1 & 0 \end{array}$$

When arrives the message (eg.: $X_2X_5X_6$)

- read it and run on the second matrix getting the encoded error:

$$0 \xrightarrow{2} 2 \xrightarrow{5} 1 \xrightarrow{6} 7$$

- run on the first matrix decoding the encoded error, while at the same time rewriting the message

$$1 \xrightarrow{\boxed{1}} X_1 \xrightarrow{2} X_1X_2 \xrightarrow{3} X_1X_2 \xrightarrow{4} X_1X_2 \xrightarrow{5} X_1X_2X_5 \xrightarrow{\boxed{6}} X_1X_2X_5$$