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

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

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

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

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

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

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

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

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

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

It holds

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

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

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

Moreover:

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

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

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

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

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

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

$\mathcal{P}^* := \mathsf{Hom}_k(\mathcal{P}, k)$ 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 $\forall \ell \in \mathcal{P}^*, f \in \mathcal{P}$

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

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

- *triangular* if

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

- *biorthogonal* if

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

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

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

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

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

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

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

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

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

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

Therefore, if we consider a set

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

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

If we now further assume that

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

so that

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

then

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

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

Then there are

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

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

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

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

Then there are

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

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

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

then it further holds

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

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

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* $\mathsf{I} := \mathfrak{P}(\mathsf{Span}_k(\mathbb{L}))$ *is a 0-dim. ideal.*

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

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

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

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

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* $\mathsf{Span}_k(\mathbf{N}(\mathsf{I}))$ *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) $q = \mathsf{Can}(p, \mathsf{I})$,
   (c) *exist* $h_j \in \mathcal{P}_t$*such that*
$$p = q + \sum_{j=1} h_j g_j, \mathbf{T}(h_j)\mathbf{T}(g_j) \leq \mathbf{T}(p - q).$$

Let

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

$<$ be any termordering;

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

and let

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

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

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

be such that

- $\mathbf{N}$ is an order ideal,
- $\mathsf{Span}_k\{t_1, \ldots, t_r\} = \mathsf{Span}_k\{q_1, \ldots, q_r\}$,
- $\{q_1, \ldots, q_r\}$ and $\{\ell_1, \ldots, \ell_r\}$ 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 $g \in G, g - \mathsf{lc}(g)\mathbf{T}_<(g) \in \mathsf{Span}_k(\mathbf{N})$,

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

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

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

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

$\mathsf{I}_\sigma = \mathfrak{P}(L_\sigma)$, for each $\sigma \leq s$,

$G_\sigma \subset \mathsf{I}_\sigma$ is the red. Gröbner basis of $\mathsf{I}_\sigma, \forall\sigma \leq s$,

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

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

$\mathbf{N}_\sigma := \{t_1, \ldots, t_\sigma\} = \mathbf{N}(\mathsf{I}_\sigma)$, $\forall\sigma \leq s$,

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

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

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

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

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

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

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

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

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

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 $h = 1..n : X_h t \notin \mathbf{T}(G_\sigma)$ **do**

$p := X_h t$,

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

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

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

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

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

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

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

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

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

$\Lambda := \{\lambda_1, \ldots, \lambda_r\} \subset \mathbb{L}$, is a linearly indipendent basis of $\mathsf{Span}_k(\mathbb{L})$;

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

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

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

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

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

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

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

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

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

%% $\mathrm{vect}(1) = (\ell_1(q_1), \ldots, \ell_s(q_1)),$

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

> $t := \min_<\{\tau \in \mathcal{T}, \tau \notin \mathbf{N} \sqcup \mathbf{T}(G)\},$
>
> $q := t, v := (\ell_1(q), \ldots, \ell_s(q))$
>
> **For** $j = 1..r$ **do**
>
>> $v := v - \lambda_j(q)\,\mathrm{vect}(j), q := q - \lambda_j(q) q_j,$
>>
>> %% $v = (\ell_1(q), \ldots, \ell_s(q)).$
>
> **If** $v = 0$ **then**
>
>> $G := G \cup \{q\},$
>
> **else**
>
>> $r := r + 1$
>>
>> $t_r := t, \mathbf{N} := \mathbf{N} \cup \{t_r\},$
>>
>> $\mu := \min\{j : \ell_j(q) \neq 0\},$
>>
>> $\lambda_r := \ell_\mu, \Lambda := \Lambda \cup \{\lambda_r\},$
>>
>> $q_r := \lambda_r(q)^{-1} q, \mathbf{q} := \mathbf{q} \cup \{q_r\}, \mathrm{vect}(r) := \lambda_r(q)^{-1} v$
>>
>> %% $\mathrm{vect}(i) = (\ell_1(q_i), \ldots, \ell_s(q_i))$ for each $i, 1 \leq i \leq r$

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

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

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

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

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

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

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

have the elimination property:

- $G \cap k[X_1, \ldots, X_\nu]$ is the Gröbner basis of $\mathsf{I} \cap k[X_1, \ldots, X_\nu]$.

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

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

The **degrevlex ordering** $<$ induced by $X_1 < \ldots X_n$ is the ordering obtained by reversing the result of the lex ordering $\prec$ induced by $X_n \prec \ldots \prec X_1$ on homogeneus 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 trianglar sets] or for applications [see the CRHT-like algoithms 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* $\mathcal{P} := k[X_1, \ldots, X_n]$,
- *a zero-dimensional ideal* I $\subset \mathcal{P}$ *and*
- *its reduced Gröbner basis* $G_\prec$ *w.r.t. the termordering* $\prec$,

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

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

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

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

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

$\mathbf{T}(f) := \mathsf{max}_{<}\{\tau \in \mathcal{T} : c(f, \tau) \neq 0\}$.

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

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

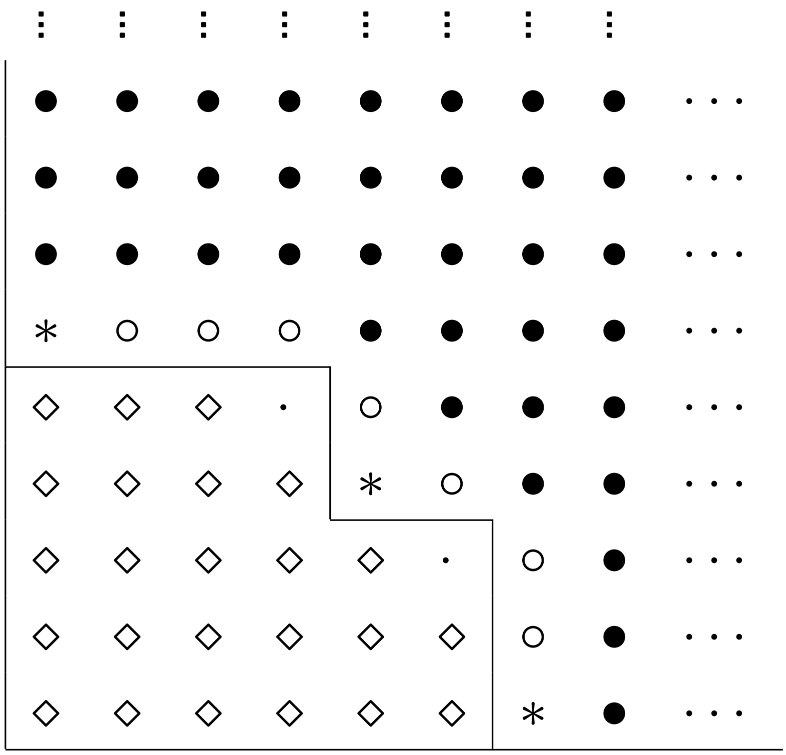
$\diamond$ $\mathbf{N}(\mathsf{I}) := \mathbf{N}_{<}(\mathsf{I}) = \mathcal{T} \setminus \mathbf{T}_{<}(\mathsf{I})$ an order ideal,

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

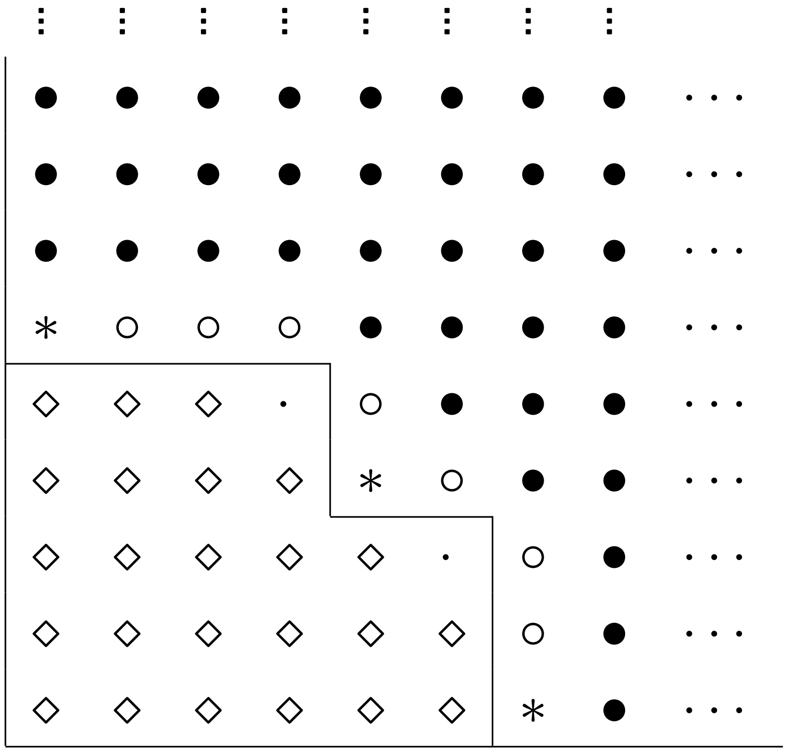
$\bullet$ $\mathbf{I}_{\prec}(\mathsf{I}) := \mathbf{T}_{\prec}(\mathsf{I}) \setminus \mathbf{B}_{\prec}(\mathsf{I})$,

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

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



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



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

$$
\begin{array}{ccccccccc}
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \\
\bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \cdots \\
\bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \cdots \\
\bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \cdots \\
* & \circ & \circ & \circ & \bullet & \bullet & \bullet & \bullet & \cdots \\
\diamond & \diamond & \diamond & \cdot & \circ & \bullet & \bullet & \bullet & \cdots \\
\diamond & \diamond & \diamond & \diamond & * & \circ & \bullet & \bullet & \cdots \\
\diamond & \diamond & \diamond & \diamond & \diamond & \cdot & \circ & \bullet & \cdots \\
\diamond & \diamond & \diamond & \diamond & \diamond & \diamond & \circ & \bullet & \cdots \\
\diamond & \diamond & \diamond & \diamond & \diamond & \diamond & * & \bullet & \cdots
\end{array}
$$

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

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

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

A *Gröbner representation* of I is the assignement of

- a linearly independent set $\mathbf{q} = \{q_1, \ldots, q_s\}$,
$$q_1 = 1 : \mathcal{P}/\mathsf{I} = \mathsf{Span}_k(\mathbf{q}),$$
- the set
$$\mathcal{M} = \mathcal{M}(\mathbf{q}) := \left\{ \left(a_{lj}^{(h)}\right) \in k^{s^2}, 1 \le h \le n \right\}$$
of the square matrices $\left(a_{lj}^{(h)}\right)$ defined by the equalities
$$X_h q_l = \sum_j a_{lj}^{(h)} q_j, \forall l, j, h, 1 \le l, j \le s, 1 \le h \le n$$
in $\mathcal{P}/\mathsf{I} = \mathsf{Span}_k(\mathbf{q})$.

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

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

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

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

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

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

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

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

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

of f in terms of $\prec$.

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

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

so that we need to compute

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

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

Such elements being treated by $\prec$-incresing 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 $\mathbf{Rep}(\tau_l, \mathbf{N}_\prec(\mathsf{I}))$ which satisfies the relation

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

so that

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

and

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

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

- if $\omega \notin \mathbf{T}_\prec(\mathsf{I})$ then $\omega \in \mathbf{N}_\prec(\mathsf{I})$, so that we add ω to $\mathbf{N}$ and $\{\omega X_h : 1 \le h \le n\}$ to B;

- if there is $g \in G_\prec$ such that $\mathbf{T}_\prec(g) = \omega$ and $g = \omega - \sum_{\tau\in\mathbf{N}_\prec(\mathsf{I})} \gamma(\omega,\tau,\prec)\tau$, since the procedure iterates on $\prec$-increasing values of ω, we have

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

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

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

we also have the representation

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

and we can use the same formula as above to derive

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

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

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

$s =$ deg(I),

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

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

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

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

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

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

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

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

$r := r + 1$

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

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

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

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

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

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

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

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

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

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

vect(1) $:= (1, 0, \ldots, 0), \mu(1) := 1$,

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

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

While B $\neq \emptyset$ **do**

  $t := \min_<(\mathrm{B})$, B $:=$ B $\setminus \{t\}$,

  $l, h : t = X_h t_l = X_h \mathbf{T}_<(q_l)$

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

    $q := X_h q_l$

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

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

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

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

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

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

    If $v = 0$ **then**

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

    else

      $r := r + 1$

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

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

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

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

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

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

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

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, Innsbruch*, (1965)
- Buchberger B., Ein algorithmisches Kriterium für die Lösbarkeit eines algebraischen Gleischunssystem, *Aeq. Math.* **4** (1970), 374–383

Solved the FGLM Problem essentially by the FGLM Algorthm

- 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 effetively 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

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

- 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. ISSAC'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 changements within the Gröbner Fan. A looser: 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. ISSAC'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 paremementers 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 $G_< \cap k[X_1, \ldots, X_{n-1}]$ is a G-basis of $\mathsf{I} \cap k[X_1, \ldots, X_{n-1}]$. Thus, one

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

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

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. $\forall h, l, 1 \leq h \leq n, 1 \leq l \leq s, \exists! \ell :$ Can$(X_h \tau_l, \mathsf{I}) = \tau_\ell$

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

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

and each codeword $(a_1, \dots, a_n) \in \mathbb{Z}_2^n$ as $\prod_{j=1}^n X_j^{a_j}$, for any codewoord $\tau \in \mathcal{T}$, the maximum likelyhood decoding error is Can(τ, 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 $\mathbf{N}(\mathsf{I}) = \{1, X_1, X_2, X_3, X_4, X_5, X_6, X_1X_6\}$, which we encode as

$\tau_\ell = X_h \tau_l$ in the table

ℓ	1	2	3	4	5	6	7
h	0	0	0	0	0	0	1
l	1	2	3	4	5	6	6

and whose corresponding FGLM-matrix is

$\mathrm{Can}(X_h \tau_l, \mathsf{I}) = \tau_\ell$

	0	1	2	3	4	5	6	7
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

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

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

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

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

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