\( \mathcal{P} := k[X_1, \ldots, X_n], \)
\( \mathcal{T} := \{X_1^{a_1} \cdots X_n^{a_n} : (a_1, \ldots, a_n) \in \mathbb{N}^n\}, \)
\(< \) a term-ordering on \( \mathcal{T}, \)
\( f = \sum_{\tau \in \mathcal{T}} c(f, \tau) \tau \in \text{Span}_k(\mathcal{T}) = \mathcal{P}, \)
\( T(f) := \max_{<}\{\tau \in \mathcal{T} : c(f, T(f)) \neq 0\}, \)
\( \text{lct}(f) := c(f, T(f)). \)

\( \mathfrak{l} \subset \mathcal{P} \) a (zero)-dimensional ideal,
\( \mathcal{T}(l) := \{T(f) : f \in \mathfrak{l}\} \) a monomial ideal,
\( \mathcal{N}(l) := \mathcal{T} \setminus \mathcal{T}(l) \) an order ideal,
\( k[\mathcal{N}(l)] := \text{Span}_k(\mathcal{N}(l)). \)

It holds
1. \( \mathcal{P} \cong \mathfrak{l} \oplus k[\mathcal{N}(l)]; \)
2. \( \mathcal{P} \setminus \mathfrak{l} \cong k[\mathcal{N}(l)]; \)
3. for each \( f \in \mathcal{P}, \) there is a unique
\[
g := \text{Can}(f, l, <) = \sum_{t \in \mathcal{N}(l)} \gamma(f, t, <) t \in k[\mathcal{N}(l)]\]
such that \( f - g \in \mathfrak{l}. \)

Moreover:

(a) \( \text{Can}(f_1, l) = \text{Can}(f_2, l) \iff f_1 - f_2 \in \mathfrak{l}; \)
(b) \( \text{Can}(f, l) = 0 \iff f \in \mathfrak{l}. \)
\( \mathcal{P} := k[X_1, \ldots, X_n], \)

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

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

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

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

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

\( \mathbb{L} = \{\ell_1, \ldots, \ell_r\} \subset \mathcal{P}^* \) and \( \mathbb{q} = \{q_1, \ldots, q_s\} \subset \mathcal{P} \) 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
\[ \mathcal{P}(L) := \{ g \in \mathcal{P} : \ell(g) = 0, \forall \ell \in L \} \]
and, for each $k$-vector subspace $P \subset \mathcal{P}$, let
\[ \mathcal{L}(P) := \{ \ell \in \mathcal{P}^* : \ell(g) = 0, \forall g \in P \}. \]

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
\begin{itemize}
  \item $P$ is an ideal iff $\mathcal{L}(P)$ is a $\mathcal{P}$-module.
  \item $L$ is a $\mathcal{P}$-module iff $\mathcal{P}(L)$ is an ideal.
  \item $P_1 \subset P_2 \implies \mathcal{L}(P_1) \supset \mathcal{L}(P_2)$;
  \item $L_1 \subset L_2 \implies \mathcal{P}(L_1) \supset \mathcal{P}(L_2)$;
  \item $\mathcal{L}(P_1 \cap P_2) \supset \mathcal{L}(P_1) + \mathcal{L}(P_2)$;
  \item $\mathcal{P}(L_1 \cap L_2) \supset \mathcal{P}(L_1) + \mathcal{P}(L_2)$;
  \item $\mathcal{L}(P_1 + P_2) = \mathcal{L}(P_1) \cap \mathcal{L}(P_2)$;
  \item $\mathcal{P}(L_1 + L_2) = \mathcal{P}(L_1) \cap \mathcal{P}(L_2)$.
  \item $P = \mathcal{P}\mathcal{L}(P)$.
  \item $L \subset \mathcal{L}\mathcal{P}(L)$;
  \item $\dim_k(L) < \infty \implies L = \mathcal{L}\mathcal{P}(L)$.
\end{itemize}
Let $\mathbb{L} = \{\ell_1, \ldots, \ell_s\} \subset \mathcal{P}^*$ 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 $f \in \mathcal{P}$,

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

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

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

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

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

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

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

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

and to re-enumerate the terms in $\mathcal{N}(I)$ 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
\[ q := \{q_1, \ldots, q_r\} \subset P \]
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 \( \sigma \leq r \)

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

If we now further assume that
1. \( \dim_k(L) = r = s \) and
2. each subvectorspace \( L_\sigma := \text{Span}_k(\{\ell_1, \ldots, \ell_\sigma\}) \) is a \( P \)-module
so that
3. each \( I_\sigma = \mathfrak{P}(L_\sigma) \) is a zero-dimensional ideal and
4. there is a chain \( I_1 \supset I_2 \supset \cdots \supset I_s = I \),
then
- \( \lambda_\sigma = \ell_\sigma, \forall \sigma \)
- \( \mathcal{N}(I_\sigma) = \{t_1, \ldots, t_\sigma\} \) is an order ideal \( \forall \sigma \)
- \( I_\sigma \oplus \text{Span}_k\{q_1, \ldots, q_\sigma\} = P, \forall \sigma \)
- \( T(q_\sigma) = t_\sigma, \forall \sigma. \)
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 $\wp(\text{Span}_k(\mathbb{L}))$ is a zero-dimensional ideal.

Then there are

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

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

- $r = \deg(\mathfrak{p}) = \dim_k(\mathbb{L}),$
- $\mathcal{N}(\mathfrak{p}) = \mathcal{N},$
- $\text{Span}_k(\Lambda) = \text{Span}_k(\mathbb{L}),$
- $\text{Span}_k\{t_1, \ldots, t_\sigma\} = \text{Span}_k\{q_1, \ldots, q_\sigma\}, \forall \sigma \leq r,$
- $\{q_1, \ldots, q_\sigma\}, \{\lambda_1, \ldots, \lambda_\sigma\}$ 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 $\mathfrak{P}(\text{Span}_k(\mathbb{L}))$ is a zero-dimensional ideal.

Then there are

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

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

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

then it further holds

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

for each $\sigma \leq r$, where $I_\sigma = \mathfrak{P}(L_\sigma)$. 
Corollary 1 (Lagrange Interpol. Formula)

Let
\[ P := k[X_1, \ldots, X_n], \]
be any termordering.

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

There exists a set \( q = \{q_1, \ldots, q_s\} \subset P \) such that
1. \( q_i = \text{Can}(q_i, I) \in \text{Span}_k(\mathcal{N}(I)); \)
2. \( \mathbb{L} \) and \( q \) are triangular;
3. \( P/I \cong \text{Span}_k(q). \)

There exists a set \( q' = \{q'_1, \ldots, q'_s\} \subset P \) such that
1. \( q'_i = \text{Can}(q'_i, I) \in \text{Span}_k(\mathcal{N}(I)); \)
2. \( \mathbb{L} \) and \( q' \) are biorthogonal;
3. \( P/I \cong \text{Span}_k(q'). \)

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

1. \( q \) is the unique polynomial in \( \text{Span}_k(\mathcal{N}(I)) \) such that \( \ell_i(q) = c_i, \) for each \( i; \)
2. for each \( p \in P \) it is equivalent
   (a) \( \ell_i(p) = c_i, \) for each \( i, \)
   (b) \( q = \text{Can}(p, I), \)
   (c) exist \( h_j \in P \) such that
   \[ p = q + \sum_{j=1} h_j g_j, \quad T(h_j)T(g_j) \leq T(p - q). \]
Let
\[ P := k[X_1, \ldots, X_n], \]
be any termordering;
\[ \mathbb{L} = \{\ell_1, \ldots, \ell_r\} \subset P^* \]
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
\[ N := \{t_1, \ldots, t_r\} \subset T, \]
\[ q := \{q_1, \ldots, q_r\} \subset \mathcal{P}, \]
\[ G := \{g_1, \ldots, g_t\} \subset \mathcal{P}, \]
be such that
\begin{itemize}
  
  \item \( N \) is an order ideal,
  \item \( \text{Span}_k\{t_1, \ldots, t_r\} = \text{Span}_k\{q_1, \ldots, q_r\} \),
  \item \( \{q_1, \ldots, q_r\} \) and \( \{\ell_1, \ldots, \ell_r\} \) are triangular,
  \item \( \ell(g) = 0 \) for each \( g \in G \) and each \( \ell \in \mathbb{L} \),
  \item \( N \sqcup T_<(G) = T \),
  \item for each \( g \in G, g - \text{lcm}(g)T_<(g) \in \text{Span}_k(N) \),
\end{itemize}
then \( G \) is a reduced Gröbner basis of \( \mathfrak{p}(\text{Span}_k(\mathbb{L})) \) w.r.t. \( < \).
\[ L = \{ \ell_1, \ldots, \ell_s \} \subset \mathcal{P}^{\ast} \text{ is s.t.}\]
\[ L_{\sigma} := \text{Span}_k(\{\ell_1, \ldots, \ell_s\}) \]

\[ \text{is a } \mathcal{P}\text{-module, for each } \sigma \leq s,\]
\[ l_{\sigma} = \mathfrak{P}(L_{\sigma}), \text{ for each } \sigma \leq s,\]
\[ G_{\sigma} \subset l_{\sigma} \text{ is the red. Gröbner basis of } l_{\sigma}, \forall \sigma \leq s,\]
\[ N := \{ t_1, \ldots, t_s \} \text{ is an order ideal,}\]
\[ q := \{ q_1, \ldots, q_s \} \subset \mathcal{P} \text{ is a set triangular to } L,\]
\[ N_{\sigma} := \{ t_1, \ldots, t_\sigma \} = N(l_{\sigma}), \forall \sigma \leq s,\]
\[ q_\sigma \in \text{Span}_k(N_{\sigma}), \text{ and } T(q_\sigma) = t_\sigma, \forall \sigma \leq s,\]
\[ \text{Span}_k(t_1, \ldots, t_\sigma) = \text{Span}_k(q_1, \ldots, q_\sigma), \forall \sigma \leq s,\]
\[ \{ q_1, \ldots, q_\sigma \} \text{ and } \{ \ell_1, \ldots, \ell_\sigma \} \text{ are triangular } \forall \sigma.\]

\[ \sigma := 1, t_1 := 1, N := \{ t_1 \}, q_1 := \ell_1(1)^{-1}(t_1)t_1,\]
\[ q := \{ q_1 \}, G_1 := \{ X_h - \ell_1(X_h), 1 \leq h \leq n \},\]
\[ \text{for } \sigma := 2..s \text{ do}\]
\[ t := \min\{ T(f) : f \in G_\sigma, \ell_\sigma(f) \neq 0 \},\]
\[ \text{Let } f \in G_\sigma : T(f) = t,\]
\[ t_\sigma := t, q_\sigma := \ell_\sigma^{-1}(f)f,\]
\[ N := N \cup \{ t_\sigma \}, q := q \cup \{ q_\sigma \},\]
\[ G_\sigma := \{ f - \ell_\sigma(f)q_\sigma : f \in G_{\sigma-1} \}.\]
\[ \text{For each } h = 1..n : X_h t \notin T(G_\sigma) \text{ do}\]
\[ p := X_h t,\]
\[ \text{For } i = 1..\sigma \text{ do } p := p - \ell_i(p)q_i,\]
\[ G_\sigma := G_\sigma \cup \{ p \};\]
\[ \text{for } \sigma := 2..s \text{ do}\]
\[ t := \min\{ T(f) : f \in G_\sigma, \ell_\sigma(f) \neq 0 \},\]
\[ \text{Let } f \in G_\sigma : T(f) = t,\]
\[ t_\sigma := t, q_\sigma := \ell_\sigma^{-1}(f)f,\]
\[ N := N \cup \{ t_\sigma \}, q := q \cup \{ q_\sigma \},\]
\[ G_\sigma := \{ f - \ell_\sigma(f)q_\sigma : f \in G_{\sigma-1} \}.\]
\[ \text{For each } h = 1..n : X_h t \notin T(G_\sigma) \text{ do}\]
\[ p := X_h t,\]
\[ \text{For } i = 1..\sigma \text{ do } p := p - \ell_i(p)q_i,\]
\[ G_\sigma := G_\sigma \cup \{ p \};\]
\[ \text{for } \sigma := 2..s \text{ do}\]
\[ t := \min\{ T(f) : f \in G_\sigma, \ell_\sigma(f) \neq 0 \},\]
\[ \text{Let } f \in G_\sigma : T(f) = t,\]
\[ t_\sigma := t, q_\sigma := \ell_\sigma^{-1}(f)f,\]
\[ N := N \cup \{ t_\sigma \}, q := q \cup \{ q_\sigma \},\]
\[ G_\sigma := \{ f - \ell_\sigma(f)q_\sigma : f \in G_{\sigma-1} \}.\]
\( \mathbb{L} = \{ \ell_1, \ldots, \ell_s \} \subset \mathcal{P}^* \) is s.t. \( I := \wp(\text{Span}_k(\mathbb{L})) \) is a zero-dimensional ideal;

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

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

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

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

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

\( q := \{q_1, \ldots, q_r\} \subset \mathcal{P} \) is a set triangular to \( \Lambda \);

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

\( \text{Span}_k\{t_1, \ldots, t_i\} = \text{Span}_k\{q_1, \ldots, q_i\} \), for each \( i \leq r \);

\( \{q_1, \ldots, q_i\} \) and \( \{\lambda_1, \ldots, \lambda_i\} \) are triangular, for each \( i \leq r \).
\( G := \emptyset, r := 1, t_1 := 1, N := \{t_1\}, \) 

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

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

\( \lambda_1 := \ell_{\mu}, \Lambda := \{\lambda_1\}, \) 

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

\( \text{While } N \sqcup T(G) \neq T \text{ do} \)

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

\( q := t, v := (\ell_1(q), \ldots, \ell_s(q)) \) 

\( \text{For } j = 1 \ldots r \text{ do} \)

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

\( \text{If } v = 0 \text{ then} \)

\( G := G \cup \{q\}, \) 

\( \text{else} \)

\( r := r + 1 \) 

\( t_r := t, N := N \cup \{t_r\}, \) 

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

\( \lambda_r := \ell_{\mu}, \Lambda := \Lambda \cup \{\lambda_r\}, \) 

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

\( \text{If } v = 0 \text{ then} \)

\( G := G \cup \{q\}, \) 

\( \text{else} \)
\( \mathcal{P} := k[X_1, \ldots, X_n], \)

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

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

\( I \subset \mathcal{P} \) 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 \( I \cap k[X_1, \ldots, X_\nu] \).

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 \( I \cap k[X_1, \ldots, X_\nu], \forall \nu < n \)

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

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


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 term-ordering $\prec$,

**to deduce the Gröbner basis $G_\prec$ of $I$ w.r.t. $\prec$.**
\[ \mathcal{P} := k[X_1, \ldots, X_n], \]
\[ \mathcal{T} := \{X_1^{a_1} \cdots X_n^{a_n} : (a_1, \ldots, a_n) \in \mathbb{N}^n\}, \]
\[ \prec \text{ a term-ordering on } \mathcal{T}, \]
\[ f = \sum_{\tau \in \mathcal{T}} c(f, \tau) \tau \in \text{Span}_k(\mathcal{T}) = \mathcal{P}, \]
\[ \mathcal{T}(f) := \max_{\prec} \{\tau \in \mathcal{T} : c(f, \tau) \neq 0\}. \]

Let \( I \subset \mathcal{P} \) a (zero)-dimensional ideal,
\[ \mathcal{T}(I) := \{\mathcal{T}(f) : f \in I\} \text{ a monomial ideal}, \]
\[ \diamond \mathcal{N}(I) := \mathcal{N}_\prec(I) = \mathcal{T} \setminus \mathcal{T}_\prec(I) \text{ an order ideal}, \]
\[ \circ \mathcal{B}_\prec(I) := \{X_h \tau : 1 \leq h \leq n, \tau \in \mathcal{N}_\prec(I)\} \setminus \mathcal{N}_\prec(I), \]
\[ \bullet \mathcal{I}_\prec(I) := \mathcal{T}_\prec(I) \setminus \mathcal{B}_\prec(I), \]
\[ * \mathcal{G}_\prec(I) \subset \mathcal{B}_\prec(I) \text{ the unique minimal basis of } \mathcal{T}_\prec(I), \]
\[ \cdot \mathcal{C}_\prec(I) := \{\tau \in \mathcal{N}_\prec(I) : X_h \tau \in \mathcal{T}_\prec(I), \forall h\}. \]
• $T_<(l) = \{ \tau \in T : \exists g \in l : T_<(g) = \tau \}$;
• $I_<(l) = \{ \tau \in T_<(l) : X_i \mid \tau \implies X_i \in T_<(l) \}$;
• $B_<(l) = \{ \tau \in T_<(l) : \exists X_i \mid X_i \tau \in N_<(l) \}$;
• $G_<(l) = \{ \tau \in T_<(l) : \forall X_i \mid X_i \tau \in N_<(l) \}$;
• $C_<(l) = \{ \tau \in N_<(l) : \forall i, X_i \tau \in B_<(l) \}$;
• $N_<(l) = \{ \tau \in T : \forall g \in l : T_<(g) = \tau \}$;
• $C_<(l) \cup T_<(l)$ is a monomial ideal;
• $N_<(l) \cup G_<(l)$ and $N_<(l) \cup B_<(l)$ are order ideals.

<table>
<thead>
<tr>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>...</td>
</tr>
<tr>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>...</td>
</tr>
<tr>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>...</td>
</tr>
<tr>
<td>*</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>...</td>
</tr>
<tr>
<td>◊</td>
<td>◊</td>
<td>◊</td>
<td>◊</td>
<td>○</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>...</td>
</tr>
<tr>
<td>◊</td>
<td>◊</td>
<td>◊</td>
<td>◊</td>
<td>◊</td>
<td>*</td>
<td>○</td>
<td>●</td>
<td>●</td>
<td>...</td>
</tr>
<tr>
<td>◊</td>
<td>◊</td>
<td>◊</td>
<td>◊</td>
<td>◊</td>
<td>◊</td>
<td>○</td>
<td>●</td>
<td>●</td>
<td>...</td>
</tr>
<tr>
<td>◊</td>
<td>◊</td>
<td>◊</td>
<td>◊</td>
<td>◊</td>
<td>◊</td>
<td>○</td>
<td>●</td>
<td>●</td>
<td>...</td>
</tr>
<tr>
<td>◊</td>
<td>◊</td>
<td>◊</td>
<td>◊</td>
<td>◊</td>
<td>◊</td>
<td>◊</td>
<td>*</td>
<td>●</td>
<td>...</td>
</tr>
</tbody>
</table>
• $\tau \in I_<(l) \iff \forall X_i \mid \tau, \frac{\tau}{X_i} \in T_<(l)$;

• $\tau \in B_<(l) \setminus G_<(l) \iff \exists h, H : \frac{\tau}{X_h} \in N_<(l), \frac{\tau}{X_H} \in B_<(l) \subset T_<(l)$;

• $\tau \in B_<(l) \setminus G_<(l) \implies \forall X_i \mid \tau, \frac{\tau}{X_i} \in N_<(l) \cup B_<(l)$;

• $\tau \in N_<(l) \setminus G_<(l) \iff \forall X_i \mid \tau, \frac{\tau}{X_i} \in N_<(l)$;

• $\tau \in T_<(l) \cup C_<(l) \iff \forall X_i \mid \tau, \frac{\tau}{X_i} \in T_<(l)$;

• $\tau \in N_<(l) \setminus C_<(l) \iff \exists h : X_h \tau \in N_<(l)$.
Macaulay (1913-16), FGLM, Traverso (≈ 1982-3)

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

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

A *Gröbner representation* of $I$ is the assignement of

- a linearly independent set $q = \{q_1, \ldots, q_s\}$,
  $$q_1 = 1 : P / I = \text{Span}_k(q),$$
- the set
  $$M = M(q) := \left\{ \left( a_{lj}^{(h)} \right) \in k^{s^2}, 1 \leq h \leq n \right\}$$
  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 $P / I = \text{Span}_k(q)$.

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

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

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

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

$$(N_{\prec}(I), M(N_{\prec}(I))), \ q = N_{\prec}(I).$$

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

$$\text{Rep}(f, N_{\prec}(I)) := (\gamma(f, \tau_1, N_{\prec}(I)), \ldots, \gamma(f, \tau_s, N_{\prec}(I)))$$

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

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

of $f$ in terms of $\prec$.  

18
Let \( \prec \) be a termordering and \( N \prec (I) = \{\tau_1, \ldots, \tau_s\} \); in order to apply Möller Algorithm to the FGLM Problem, we just need to choose as functionals \( \mathbb{L} := \{\ell_1, \ldots, \ell_s\} \) the coefficients of the canonical forms

\[
\ell_i(\cdot) := \gamma(\cdot, \tau_i, N \prec (I))
\]

so that we need to compute

\[
\text{Rep}(f, N \prec (I)) := (\gamma(f, \tau_1, N \prec (I)), \ldots, \gamma(f, \tau_s, N \prec (I)))
\]

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

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 \( \tau_l \) so that we previously computed \( \text{Rep}(\tau_l, N \prec (I)) \) which satisfies the relation

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

so that

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

and

\[
\text{Can}(X_h \tau_l, I, \prec) = \sum_{j=1}^{s} \gamma(\tau_l, \tau_j, \prec) \text{Can}(X_h \tau_j, I, \prec)
\]

\[
= \sum_{i=1}^{s} \left( \sum_{j=1}^{s} \gamma(\tau, \tau_j, \prec) \gamma(X_h \tau_j, \tau_i, \prec) \right) \tau_i.
\]
For the $\prec$-minimal $\omega := X_h\tau_l \in B$ we have

- if $\omega \notin T_{\prec}(l)$ then $\omega \in N_{\prec}(l)$, so that we add $\omega$ to $N$ and $
\omega X_h : 1 \leq h \leq n}$ to $B$
;

- if there is $g \in G_{\prec}$ such that $T_{\prec}(g) = \omega$ and $g = \omega - \sum_{\tau \in N_{\prec}(l)} \gamma(\omega, \tau, \prec)\tau$, since the procedure iterates on $\prec$-increasing values of $\omega$, we have
\[ \gamma(\omega, \tau, \prec) \neq 0 \implies \tau \prec \omega \implies \tau \in N; \]

- if there is $H, 1 \leq H \leq n, \tau \in T_{\prec}(l)$ such that $\omega = X_H\tau$; thus $\tau \prec \omega$ has been already treated so that we have obtained a representation $\text{Can}(\tau, l, \prec) = \sum_{j=1}^{s} \gamma(\tau, \prec, \tau_j)\tau_j$; since in such representation we have
\[ \gamma(\tau, \prec, \tau_j) \neq 0 \implies \tau_j \prec \tau \implies \tau_j \in N, X_H\tau_j \prec X_H\tau = \omega, \]
we also have the representation
\[ \text{Can}(X_H\tau, l, \prec) = \sum_{j=1}^{s} \gamma(\tau, \prec, \tau_j) \text{Can}(X_H\tau_j, l, \prec) \]
and we can use the same formula as above to derive
\[ \gamma(X_h\tau_l, \tau_i, \prec) = \gamma(X_H\tau, \tau_i, \prec) = \sum_{j=1}^{s} \gamma(\tau, \tau_j, \prec)\gamma(X_H\tau_j, \tau_i, \prec) = \sum_{j=1}^{s} \gamma(X_h\tau_l, \tau_j, \prec)\gamma(X_H\tau_j, \tau_i, \prec). \]
\((N_\prec, M) := \text{FGLM-Matrix}(G_\prec)\) where

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

\(s = \deg(I),\n\)

\(N_\prec := \{\tau_1, \ldots, \tau_s\} = N_\prec(I),\n\)

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

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

\(r := 1, \tau_1 := 1, N_\prec := \{\tau_1\}, B := \{X_h : 1 \leq h \leq n\},\)

While \(B \neq \emptyset\) do

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

\(h, l : \omega := X_h \tau_l\)

If \(\omega \notin T_\prec(I)\) then

\(r := r + 1\)

\(\tau_r := \omega, N_\prec := N_\prec \cup \{\tau_r\}, B := B \cup \{X_h \tau_r : 1 \leq h \leq n\},\)

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

else

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

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

else

Let \(H, \iota : 1 \leq H \leq n, 1 \leq \iota \leq r : X_h \tau_i \in T_\prec(G_\prec), \tau_i = X_H \tau_i;\)

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 \(a_{lj}^{(H)} := a_{lj}^{(h)};\)

\(N_\prec, M\)
(N, M) := FGLM-Matrix(G)

G := ∅, r := 1, t_1 := 1, N := \{t_1\}, q_1 := 1, q := \{q_1\},
B := \{X_h, 1 \leq h \leq n\}

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

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

While B ≠ ∅ do

\[ t := \min_<(B), B := B \setminus \{t\}\]
\[ l, h : t = X_h t_l = X_h T_<(q_l) \]

If t \notin 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 = Rep(q, N)

For j = 1..r do

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

%% v = Rep(q, N)

If v = 0 then

G := G ∪ \{q\},

else

r := r + 1
\[ t_r := t, N := N \cup \{t_r\}, \]
\[ \mu(r) := \min\{j : \gamma(q, \tau_j, \prec) \neq 0\}, \]
\[ q_r := \gamma(q, \tau_{\mu(r)}, \prec)^{-1}q, vect(r) := \gamma(q, \tau_{\mu(r)}, \prec)^{-1}v \]

%% vect(i) = Rep(q_i, N), \forall i, 1 \leq i \leq r
\[ q := q \cup \{q_r\}, \]
B := B ∪ \{X_h t_r, 1 \leq h \leq n\},

G, N, q
**Berlekamp-Massey-Sakata** a sort of FGLM on modules with functionals depending on the state of the computation.


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


Solved the FGLM Problem essentially by the FGLM Algorithm


Interpolation on multivariate points


FGLM-like Algorithm for effeectively perform generic change of coordinate


Iteratively compute

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


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


Generalizing Möller and FGLM Algorithm to general functional evaluation

Implementation via \(p\)-modular evaluation and CRT interpolation


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.


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.


“The worst case complexity [...] is not better than the complexity of the FGLM algorithm; but also give the theoretical complexity with some parementers 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 $G_\prec \cap k[X_1, \ldots, X_{n-1}]$ is a G-basis of $I \cap k[X_1, \ldots, X_{n-1}]$. Thus, one

- iteratively computes, $i = n - 1..1$, the G-basis $G_i$ of $l_i := l \cap k[X_1, \ldots, X_i]$
- $H_1 := G_1$
- 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 $l_{i+1}$.

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


Extending Marinari–Möller to projective spaces


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


FGLM Algorithm in non-commutative setting

• M. Borges-Quintana, M. A. Borges-Trenard, E. Martínez-Moro A general framework for applying FGLM techniques to linear codes

• M. Borges-Quintana, M.A. Borges-Trenard, P. Fitzpatrick, E. Martínez-Moro Grobner bases and combinatorics for binary codes

• M. Borges-Quintana, M. Borges-Trenard, E. Martínez-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

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

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

Then

1. $\forall \ell, 1 \leq \ell \leq s \exists! h, l, 1 \leq h \leq n, 0 \leq l < s, : h := \min\{i : X_i | \tau_\ell, } \tau_\ell = X_h \tau_l$

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 $(a_1, \ldots, a_n) \in \mathbb{Z}_2^n$ as $\prod_{j=1}^{n} X_j^{a_{ij}}$, for any codeword $\tau \in T$, 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
\[
H^T := \begin{bmatrix}
1 & 1 & 0 & 1 & 0 & 0 \\
1 & 0 & 1 & 0 & 1 & 0 \\
1 & 1 & 1 & 0 & 0 & 1
\end{bmatrix}
\]
we have \(N(l) = \{1, X_1, X_2, X_3, X_4, X_5, X_6, X_1X_6\}\), which we encode as
\[
\tau_l = X_h \tau_l \text{ in the table}
\begin{array}{c|ccccccccc}
\ell & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\
h & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
l & 1 & 2 & 3 & 4 & 5 & 6 & 6
\end{array}
\]
and whose corresponding FGLM-matrix is
\[
\text{Can}(X_h \tau_l, l) = \tau_l
\begin{array}{cccccccc}
0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\
1 & 1 & 0 & 5 & 4 & 3 & 2 & 7 & 6 \\
2 & 2 & 5 & 0 & 7 & 6 & 1 & 4 & 3 \\
3 & 3 & 4 & 7 & 0 & 1 & 6 & 5 & 2 \\
4 & 4 & 3 & 6 & 1 & 0 & 7 & 2 & 5 \\
5 & 5 & 2 & 1 & 6 & 7 & 0 & 3 & 4 \\
6 & 6 & 7 & 4 & 5 & 2 & 3 & 0 & 1 \\
7 & 7 & 6 & 3 & 2 & 5 & 4 & 1 & 0
\end{array}
\]
When arrives the message (eg.: \(X_2X_5X_6\))

- read it and run on the second matrix getting the encoded error:
  \[
  0 \overset{2}{\rightarrow} 2 \overset{5}{\rightarrow} 1 \overset{6}{\rightarrow} 7
  \]
- run on the first matrix decoding the encoded error, while at the same time rewriting the message
  \[
  1 \overset{1}{\rightarrow} X_1 \overset{2}{\rightarrow} X_1X_2 \overset{3}{\rightarrow} X_1X_2 \overset{4}{\rightarrow} X_1X_2 \overset{5}{\rightarrow} X_1X_2X_5 \overset{6}{\rightarrow} X_1X_2X_5
  \]