# Faugère's F4 Algorithm Formalization

Dongwook Cheon

July 24, 2025

# Chapter 1

# Gröbner Basis

Here we fix a field $k$ of coefficients, and a monomial order $\leq$ on $k[x_1, \cdots, x_n]$. Let $f \in k[x_1, \cdots, x_n] \setminus \{0\}$.

**Definition 1** (Monomial order)**.** A **monomial order** on $k[x_1, \cdots, x_n]$ is a total order $<$ on $\mathbb{Z}_{\geq 0}^n$ satisfying:

(i) if $\alpha < \beta$, then $\alpha + \gamma < \beta + \gamma$ for any $\gamma \in \mathbb{Z}_{\geq 0}^n$;

(ii) $<$ is a well-ordering.

**Definition 2** (Leading monomial, leading coefficient, and leading term)**.** The **leading monomial** $\mathrm{LM}(f)$ of $f$ is the monomial in $f$ maximum under the fixed monomial order. The **leading coefficient** $\mathrm{LC}(f)$ of $f$ is the coefficient of $\mathrm{LM}(f)$ in $f$. The **leading term** of $f$ is then simply the $\mathrm{LC}(f)$-multiple of $\mathrm{LM}(f)$.

**Definition 3** (Monomial ideal)**.** An ideal $I \trianglelefteq k[x_1, \cdots, x_n]$ is a **monomial ideal** if there exists a subset of exponents $A \subseteq \mathbb{Z}_{\geq 0}^n$ such that

$$I = \langle x^\alpha : \alpha \in A \rangle.$$

**Definition 4** (Gröbner basis)**.** A finite subset $G = \{g_1, \cdots, g_t\} \neq \{0\}$ of $I \trianglelefteq k[x_1, \cdots, x_n]$ is said to be a **Gröbner basis** of $I$ if

$$\langle \mathrm{LM}(I) \rangle = \langle \mathrm{LM}(G) \rangle = \langle \mathrm{LM}(g_1), \cdots, \mathrm{LM}(g_t) \rangle.$$

# Chapter 2

# Buchberger's Criterion

**Definition 5** (Multivariate division algorithm)**.**

Input: divisor set $\{f_1, \cdots, f_s\}$ and dividend $f$
Output: quotients $q_1, \cdots, q_s$ and remainder $r$

$\forall\, i,\ q_i := 0;\ r := 0$

$p := f$

while $p \neq 0$:

  $i := 1$

  $DivisionOccured := False$

  while $i \leq s$ and not $DivisionOccured$:

    if $\mathrm{LT}(f_i) \mid \mathrm{LT}(p)$:

      $q_i := q_i + \mathrm{LT}(p)/\mathrm{LT}(f_i)$

      $p := p - (\mathrm{LT}(p)/\mathrm{LT}(f_i))f_i$

    else:

      $i := i + 1$

  if not $DivisionOccured$:

    $r := r + \mathrm{LT}(p)$

    $p := p - \mathrm{LT}(p)$

return $q_1, \cdots, q_s, r$

**Definition 6** (S-polynomial)**.** Define the **least common multiple** $\gamma = \mathrm{lcm}(\alpha, \beta)$ of two monomials $\alpha, \beta$ as $\gamma_i = \max(\alpha_i, \beta_i)$. The **S-polynomial** of two polynomials $f$ and $g$, given a monomial order, is

$$S(f, g) = \frac{\mathrm{lcm}(\mathrm{LM}(f), \mathrm{LM}(g))}{\mathrm{LT}(f)} f - \frac{\mathrm{lcm}(\mathrm{LM}(f), \mathrm{LM}(g))}{\mathrm{LT}(g)} g.$$

We say each part of above, i.e.

$$\frac{\mathrm{lcm}(\mathrm{LM}(f), \mathrm{LM}(g))}{\mathrm{LT}(f)} f \quad \text{and} \quad \frac{\mathrm{lcm}(\mathrm{LM}(f), \mathrm{LM}(g))}{\mathrm{LT}(g)} g,$$

the **S-pair** of $f$ and $g$.

**Theorem 7** (Buchberger's criterion)**.** *Let $I \trianglelefteq k[x_1, \cdots, x_n]$. Then a basis $G = \{g_1, \cdots, g_t\}$ is a Gröbner basis of $I$ iff the remainder of each $S(g_i, g_j) (i \neq j)$ in long division by $G$ is zero.*

**Definition 8** (Standard representation)**.** For $G = \{g_1, \cdots, g_t\} \subseteq k[x_1, \cdots, x_n]$ and $f \in k[x_1, \cdots, x_n]$, a **standard representation** of $f$ by $G$ is, if exists, an equality

$$f = \sum_{k=1}^{t} A_k g_k, \quad A_k \in k[x_1, \cdots, x_n],$$

where $A_k g_k = 0$ or $\mathrm{LM}(f) \geq \mathrm{LM}(A_k g_k)$ for every $1 \leq k \leq t$. If such a standard representation exists, we say $f$ **reduces to zero modulo** $G$ and notate it as

$$f \to_G 0.$$

**Theorem 9** (Refinement of Buchberger's criterion)**.** *Let $I \trianglelefteq k[x_1, \cdots, x_n]$. Then a basis $G = \{g_1, \cdots, g_t\}$ is a Gröbner basis of $I$ iff $S(g_i, g_j) \to_G 0$ for each pair of $i \neq j$.*

# Chapter 3

# Faugère's F4 Algorithm

**Definition 10** (Monomial set)**.** The **monomial set** of a polynomial $f$ is the set of monomials with nonzero coefficient in $f$, and is denoted by $\mathrm{Mon}(f)$. For $K \subseteq k[x_1, \cdots, x_n]$, we define as

$$\mathrm{Mon}(K) = \bigcup_{f \in K} \mathrm{Mon}(f).$$

**Definition 11** (Symbolic preprocessing)**.**

Input: $L$, $G = \{f_1, \cdots, f_t\}$ (two finite sets of polynomials)
Output: $H$ (a finite set of polynomial containing $L$)

$H := L$

$done := \mathrm{LM}(H)$

while $done \neq \mathrm{Mon}(H)$:

$x^\beta := \max_<(\mathrm{Mon}(H) \setminus done)$
$done := done \cup \{x^\beta\}$
if $\exists g \in G$ such that $\mathrm{LM}(g) \mid x^\beta$:
$g :=$ one such choice of $g$
$H := H \cup \left\{\frac{x^\beta}{\mathrm{LM}(g)} g\right\}$

return $H$

**Theorem 12** (Result of symbolic preprocessing)**.** *The algorithm above with input $L$ and $G$ terminates and obtains as an output a set of polynomials $H$ satisfying the following two properties:*

*(i)* $L \subseteq H$, *and*

*(ii)* *whenever $x^\beta$ is a monomial in some $f \in H$, and for some $g \in G$ its leading monomial* $\mathrm{LM}(g)$ *divides $x^\beta$, then* $\frac{x^\beta}{\mathrm{LM}(g)} g \in H$.

**Definition 13** (Faugère's F4 algorithm)**.**

Input: $F = \{f_1, \cdots, f_s\}$ (a generating set of polynomials of an ideal)
Output: $G$ (a Gröbner basis of the ideal, containing $F$)

$G := F$

$t := s$

$B := \{\{i, j\} \mid 1 \leq i < j \leq s\}$

while $B \neq \emptyset$:

$B' :=$ a nonempty subset of $B$

$B := B \setminus B'$

$L := \left\{ \frac{\mathrm{lcm}(\mathrm{LM}(f_i), \mathrm{LM}(f_j))}{\mathrm{LT}(f_i)} f_i \mid \{i, j\} \in B' \right\}$

$H := SymbolicPreprocessing(L, G)$

$M := (\mathrm{coeff}(h_k, x^{\alpha_\ell}))_{k,\ell}$
(the matrix of coefficients of H; $x^{\alpha_\ell}$ sorted under monomial order)

$N :=$ row reduced echelon form of $M$

$N^+ := \{n \in \mathrm{rows}(N) \mid \mathrm{LM}(n) \notin \langle \mathrm{LM}(\mathrm{rows}(N)) \rangle\}$

for $n \in N^+$:

$t := t + 1$

$f_t :=$ the polynomial form of $n$

$G := G \cup \{f_t\}$

$B := B \cup \{\{i, t\} \mid 1 \leq i < t\}$

return $G$

**Theorem 14** (Result of F4)**.** *The output $G'$ of Faugère's F4 algorithm is a Gröbner basis of the ideal generated by the input polynomial set $G$. In particular, the output satisfies the refined Buchberger criterion; i.e. every S-polynomial within $G'$ reduces to zero over $G'$.*