Faugère's F4 Algorithm Formalization

Dongwook Cheon

May 23, 2025

Here we fix a field k of coefficients, and a monomial order $\leq$ on $k[x_1, \cdots, x_n]$.

Chapter 1

Gröbner Basis

Let $f \in k[x_1, \cdots, x_n] \setminus \{0\}$.

Definition 1 (Leading monomial & leading term)**.** The **leading monomial** $\mathrm{LM}(f)$ of f is the monomial in f maximum under the fixed monomial order. The **leading term** $\mathrm{LT}(f)$ of f is the multiple of $\mathrm{LM}(f)$ by its coefficient in f.

Definition 2 (Monomial ideal)**.** An ideal $I \trianglelefteq k[x_1, \cdots, x_n]$ is a **monomial ideal** if for some subset of exponents $A \subseteq \mathbb{Z}^n_{\geq 0}$,

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

Theorem 3 (Dickson's lemma)**.** *For any monomial ideal $I = \langle x^\alpha : \alpha \in A \rangle \trianglelefteq k[x_1, \cdots, x_n]$, there exists a finite subset $A' \subseteq A$ such that $I = \langle x^\alpha : \alpha \in A' \rangle$.*

Definition 4 (Ideal of leading terms)**.** Let $I \trianglelefteq k[x_1, \cdots, x_n]$ a nontrivial ideal. The **ideal of leading terms** of I is the ideal generated by leading terms of each $f \in I \setminus \{0\}$. Namely,

$$\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(f) : f \in I \setminus \{0\} \rangle.$$

This is equivalent to being generated by leading monomials, i.e. the above ideals are equal to

$$\langle \mathrm{LM}(I) \rangle = \langle \mathrm{LM}(f) : f \in I \setminus \{0\} \rangle.$$

Definition 5 (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

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

Definition 6 (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

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

Chapter 2

Buchberger's Criterion

Definition 7 (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 $p \neq 0$:
  - $i := 1$
  - $\mathit{DivisionOccured} := False$
  - while $i \leq s$ and not $\mathit{DivisionOccured}$:
    - if $\mathrm{LT}(f_i) | \mathrm{LT}(p)$:
      - $q_i := q_i + \mathrm{LT}(p)/\mathrm{LT}(f_i)$
      - $p := p - (\mathrm{LT}(p)/\mathrm{LT}(f_i))f_i$
    - else:
      - $i := i + 1$
  - if not $\mathit{DivisionOccured}$:
    - $r := r + \mathrm{LT}(p)$
    - $p := p - \mathrm{LT}(p)$

return $q_1, \cdots, q_s, r$

Definition 8 (S-polynomial)**.** Define the **least common multiple** $\gamma = \mathrm{lcm}(\alpha, \beta)$ of two monomials α, β 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 9 (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 10 (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 11 (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 12 (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 $\mathrm{LM}(g) | x^\beta$:
    - $g :=$ one such choice of g
    - $H := H \cup \left\{ \frac{x^\beta}{\mathrm{LM}(g)} g \right\}$

  return H

Theorem 13 (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^β is a monomial in some $f \in H$, and for some $g \in G$ its leading monomial $\mathrm{LM}(g)$ divides x^β, then $\frac{x^\beta}{\mathrm{LM}(g)} g \in H$.*

Definition 14 (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^{α_ℓ} 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 15 (Result of F4)**.** *The output of Faugère's F4 algorithm is a Gröbner basis of the ideal generated by the input polynomials.*

The proof needs an refined version of Buchberger criterion.