Faugère's F4 Algorithm Formalization

Dongwook Cheon

May 9, 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 $f \in k[x_1, \cdots, x_n] \quad \{0\}$.

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 $f \in I \quad \{0\}$. Namely,

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

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

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

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

Faugère F4 Algorithm

Definition 7 (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 $done \neq \mathrm{Mon}(H)$:
    – $x^\beta := \max_<(\mathrm{Mon}(H)\ \ done)$
    – $done := done \cup \{x^\beta\}$
    – 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 $H$
```

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 $done \neq \mathrm{Mon}(H)$:
    – $x^\beta := \max_<(\mathrm{Mon}(H)\ \ done)$
    – $done := done \cup \{x^\beta\}$
    – 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 8 (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 $\frac{x^\beta}{\mathrm{LM}(g)} g \in H$.*