Faugère's F5 algorithm–Criterion

Hojin Lee

Dec 2024

Outline

1. Preliminaries
2. Gröbner Bases
3. Tuples of polynomials
4. Signature
5. The Criterion
6. Formalization

Preliminaries

We follow *A New Attempt On The F5 Criterion* by Christian Eder.

Definition

Fix a monomial order. If $f \in k[x_1, \ldots, x_n]$, define

1. $\mathrm{HM}(f) = c_\alpha x^\alpha$
2. $\mathrm{HT}(f) = x^\alpha$
3. $\mathrm{HC}(f) = c_\alpha$

where α is the maximal element among the monomials of f.

Preliminaries

Definition

Let f and g be nonzero polynomials in $k[x_1, \ldots, x_n]$. The S-polynomial is defined as

$$\mathrm{Spol}(f,g) = \mathrm{HC}(g)\frac{\tau}{\mathrm{HT}(f)}f - \mathrm{HC}(f)\frac{\tau}{\mathrm{HT}(g)}g$$

where $\tau = \mathrm{lcm}(\mathrm{HT}(f), \mathrm{HT}(g))$.

Preliminaries

Definition

Let $P \subset k[x_1, \ldots, x_n]$ be a finite set, f a nonzero polynomial, and t a term. A representation

$$f = \sum_{p \in P} \lambda_p p$$

where the λ_p are in the polynomial ring, $p \in P$, is called a t-representation of f wrt P, if for all $p \in P$ such that $\lambda_p \neq 0$, we have $HT(\lambda_p p) \leq t$.

If $t = \mathrm{HT}(f)$, then a t-representation of f is called a standard representation.

Gröbner Bases

Here is the Gröbner basis characterization we use:

Theorem

Let $G = \{g_1, \ldots, g_N\}$ *be a finite subset of* $k[x_1, \ldots, x_n]$ *with* $0 \notin G$*. If for all* $f \in I = \langle G \rangle$*,* f *has a standard representation, then* G *is a Gröbner basis of* I*.*

Tuples of polynomials

We will work with m-tuples of polynomials in $k[x_1, \dots, x_n]$, rather than single polynomials. This is because we want to define the *signature* of a polynomial.

Tuples of polynomials

Consider the free module $k[x_1, \ldots, x_n]^{\oplus m}$. For the sake of brevity, we will denote this as $k[\mathbf{x}]^m$.

Definition

Let $\mathbf{g} = \sum_{k=1}^{m} g_k \mathbf{e}_k \in k[\mathbf{x}]^m$, where the $\mathbf{e}_k$ are unit vectors. The index of $\mathbf{g}$ is the smallest i such that $g_i \neq 0$. We do not consider the case $\mathbf{g} = 0$, so the index is defined.

Tuples of polynomials

We extend our monomial ordering to m-tuples of polynomials.

Definition

If $\mathbf{g}$ and $\mathbf{h}$ are elements of $k[\mathbf{x}]^m$ with index i and j, then define the order $\mathbf{g} < \mathbf{h}$ if and only if $i > j$ or $i = j$ and $\mathrm{HT}(g_i) < \mathrm{HT}(h_i)$ where g_i and h_i are obvious. As the zero tuple does not have an index, we define $0 < \mathbf{g}$ for any nonzero $\mathbf{g}$.

Tuples of polynomials

Definition

We define the module head term MHT of nonzero $\mathbf{g} \in k[\mathbf{x}]^m$ to be

$$\mathrm{MHT}(\mathbf{g}) = \mathrm{HT}(g_i)\mathbf{e}_i,$$

where i is the index of $\mathbf{g}$.

Tuples of polynomials

Lemma

The module ordering $<$ on $k[\mathbf{x}]^m$ is well-founded, i.e., every nonempty subset has a minimal element.

Proof.

Let P be a nonempty subset of $k[\mathbf{x}]^m$. If $0 \in P$, we are done. If $0 \notin P$, then for $\mathbf{p} \in P$ its index is defined and is bounded by m. Thus $i_{\max} = \max\{\mathrm{index}(\mathbf{p}|\mathbf{p} \in P\}$ and $t_{\min} = \min\{\mathrm{HT}(p_k)|\mathbf{p} \in P, \mathrm{index}(\mathbf{p}) = k\}$ are defined, and the set of $\mathbf{p}$ such that the index is $i_{\max}$ and the head term of $p_{i_{\max}}$ is $t_{\min}$ is the set of minimal elements of P. $\square$

Signature

Definition

A labeled polynomial r is a pair $(u\mathbf{e}_k, p)$ where u is a term of $k[\mathbf{x}]$ and $p \in k[\mathbf{x}]$.
Given such r, its signature is defined as $\mathcal{S}(r) = u\mathbf{e}_k$ and the polynomial is defined as p, its index is k.
A labeled polynomial r is admissible with respect to an m-tuple F if there exists a nonzero m-tuple $\mathbf{g}$ such that $v_F(\mathbf{g}) = p$ and $\mathrm{MHT}(\mathbf{g}) = \mathcal{S}(r)$.

The Criterion

Need a lot more definitions: Normalized pairs etc...
Will not cover, as even the most basic lemmas were challenging to formalize. Anyways, here is the statement:

Theorem (F5 criterion)

Suppose we are given an m-tuple $F = (f_i)$ *of polynomials, and a set* $G = (r_i)$ *of labeled polynomials admissible wrt* F*, containing all elements of the form* $(\mathbf{e}_i, f_i)$*. If for all pairs* (r_i, r_j) *normalized wrt* G, $\mathrm{Spol}(r_i, r_j)$ *has a t-representation where* $t < \mathrm{lcm}(\mathrm{HT}(p_i), \mathrm{HT}(p_j))$*, then* p_i *form a Gröbner basis of* $I = \langle p_1, \ldots, p_{n_G} \rangle$ *where the* p_i *are the polynomial parts of the* r_i*.*

Formalization

See code

References

On the criteria of the F5 algorithm, Christian Eder