On the Criteria of Faugère's F_5 Algorithm

Christian Eder

Technische Universität Kaiserslautern

July 08, 2008

Overview of the Talk

Table of Contents

The main problem

Given an ideal I we want to compute a Gröbner basis G of I.

The main problem

Given an ideal I we want to compute a Gröbner basis G of I.

- We want to do this **fast** and without much **memory usage**.

The main problem

Given an ideal I we want to compute a Gröbner basis G of I.

- We want to do this **fast** and without much **memory usage**.
- We do not want to compute **zero-reductions of S-Polynomials** as they do not give us any new information about G, but cost time and memory.

The main problem

Given an ideal I we want to compute a Gröbner basis G of I.

- We want to do this **fast** and without much **memory usage**.
- We do not want to compute **zero-reductions of S-Polynomials** as they do not give us any new information about G, but cost time and memory.

$\Rightarrow$ How do we detect such useless critical pairs/S-Polynomials?

Faugère's Idea

(a) Connect the polynomials in $\mathbb{K}[\underline{x}]$ with module elements in $\mathbb{K}[\underline{x}]^m$.

Faugère's Idea

(a) Connect the polynomials in $\mathbb{K}[\underline{x}]$ with module elements in $\mathbb{K}[\underline{x}]^m$.

(b) Add **new data** received from this connection to each polynomial investigated.

Faugère's Idea

(a) Connect the polynomials in $\mathbb{K}[\underline{x}]$ with module elements in $\mathbb{K}[\underline{x}]^m$.

(b) Add **new data** received from this connection to each polynomial investigated.

(c) Use this data to detect useless critical pairs/S-Polynomials and delete them **before** they are reduced.

Faugère's Idea

(a) Connect the polynomials in $\mathbb{K}[\underline{x}]$ with module elements in $\mathbb{K}[\underline{x}]^m$.

(b) Add **new data** received from this connection to each polynomial investigated.

(c) Use this data to detect useless critical pairs/S-Polynomials and delete them **before** they are reduced.

This is what the Gröbner basis algorithm called F_5 is all about.

What this talk is about

(a) Understand the connection between polynomials and module elements.

What this talk is about

(a) Understand the connection between polynomials and module elements.

(b) Understand the way new data is added to a polynomial.

What this talk is about

(a) Understand the connection between polynomials and module elements.
(b) Understand the way new data is added to a polynomial.
(c) State Faugère's Criteria to detect useless critical pairs using this new data.

What this talk is about

(a) Understand the connection between polynomials and module elements.
(b) Understand the way new data is added to a polynomial.
(c) State Faugère's Criteria to detect useless critical pairs using this new data.
(d) Understand why these criteria work in a small example.

Table of Contents

Polynomial Basics

- $\mathbb{K}$ always denotes a field, $\mathbb{K}[\underline{x}]$ is the polynomial ring over $\mathbb{K}$ in the variables $\underline{x} = (x_1, \ldots, x_n)$, $\leq$ denotes a well-ordering on $\mathbb{K}[\underline{x}]$, $\mathcal{T}$ denotes the monoid of power products of $\underline{x}$.

Polynomial Basics

- $\mathbb{K}$ always denotes a field, $\mathbb{K}[\underline{x}]$ is the polynomial ring over $\mathbb{K}$ in the variables $\underline{x} = (x_1, \dots, x_n)$, $\leq$ denotes a well-ordering on $\mathbb{K}[\underline{x}]$, $\mathcal{T}$ denotes the monoid of power products of $\underline{x}$.
- If $p = \sum_{k=1}^{m} a_i p_i$, $a_k \in \mathbb{K}, p_k \in \mathcal{T}$ for all $k \in \{1, \dots, m\}$ where $a_1 p_1 < \dots < a_m p_m$ then we denote
  - the **head term** of p $\mathrm{HT}(p) = p_m$,
  - the **head coefficient** of p $\mathrm{HC}(p) = a_m$,
  - the **head monom** of p $\mathrm{HM}(p) = a_m p_m$.

Polynomial Basics

- $\mathbb{K}$ always denotes a field, $\mathbb{K}[\underline{x}]$ is the polynomial ring over $\mathbb{K}$ in the variables $\underline{x} = (x_1, \ldots, x_n)$, $\leq$ denotes a well-ordering on $\mathbb{K}[\underline{x}]$, $\mathcal{T}$ denotes the monoid of power products of $\underline{x}$.
- If $p = \sum_{k=1}^{m} a_i p_i$, $a_k \in \mathbb{K}, p_k \in \mathcal{T}$ for all $k \in \{1, \ldots, m\}$ where $a_1 p_1 < \ldots < a_m p_m$ then we denote
  - the **head term** of p $\mathrm{HT}(p) = p_m$,
  - the **head coefficient** of p $\mathrm{HC}(p) = a_m$,
  - the **head monom** of p $\mathrm{HM}(p) = a_m p_m$.
- Let $p_1, p_2 \in \mathbb{K}[\underline{x}]$,

$$u_k = \frac{\mathrm{LCM}(\mathrm{HT}(p_1), \mathrm{HT}(p_2))}{\mathrm{HT}(p_k)} \text{ for } k \in \{1, 2\},$$

  then we denote the **S-Polynomial** of p_1, p_2

$$\mathrm{Spol}(p_1, p_2) = \mathrm{HC}(p_2) u_1 p_1 - \mathrm{HC}(p_1) u_2 p_2.$$

Polynomial Basics

- $F = (f_1, \ldots, f_m)$ with $f_i \neq 0 \in \mathbb{K}[\underline{x}]$ always denotes a **sequence of homogeneous polynomials**.

Polynomial Basics

- $F = (f_1, \ldots, f_m)$ with $f_i \neq 0 \in \mathbb{K}[\underline{x}]$ always denotes a **sequence of homogeneous polynomials**.
- Let $p \in \mathbb{K}[\underline{x}]$ be a polynomial and $\mathcal{P} := \{p_1, \ldots, p_m\}$ be a set of polynomials in $\mathbb{K}[\underline{x}]$. Then we say that

$$p = \sum_{i=1}^{n} \lambda_i p_i \quad \lambda_i \in \mathbb{K}[\underline{x}]$$

is an t-**representation of** p **w.r.t.** $\mathcal{P}$ if $\mathrm{HT}(\lambda_i p_i) < t$ for all $i \in \{1, \ldots, m\}$.

Example

Consider the polynomial ring $\mathbb{K}[x, y]$, $\leq$ a degree reverse lexicographical ordering. Let $p_1 = 3x^2 + y$, $p_2 = 2xy + 1$. Then $\mathrm{LCM}\big(\mathrm{HT}(p_1), \mathrm{HT}(p_2)\big) = x^2y$, $u_1 = y$ and $u_2 = x$. We get

$$
\begin{aligned}
\mathrm{Spol}(p_1, p_2) &= 2yp_1 - 3xp_2 \\
&= \mathbf{6x^2y^2} + 2y^2 - \mathbf{6x^2y^2} - 3x \\
&= 2y^2 - 3x.
\end{aligned}
$$

Characterization of Gröbner Bases

Theorem

Let $G \supset \{f_1, \ldots, f_m\}$. If for all $p_i, p_j \in G$ $Spol(p_i, p_j)$ has a t-representation for $t = LCM\big(HT(p_i), HT(p_j)\big)$ or $Spol(p_i, p_j)$ reduces to zero w.r.t. G then G is a Gröbner basis of $I = \langle f_1, \ldots, f_m \rangle$.

Characterization of Gröbner Bases

Theorem

Let $G \supset \{f_1, \ldots, f_m\}$. If for all $p_i, p_j \in G$ $Spol(p_i, p_j)$ has a t-representation for $t = LCM\big(HT(p_i), HT(p_j)\big)$ or $Spol(p_i, p_j)$ reduces to zero w.r.t. G then G is a Gröbner basis of $I = \langle f_1, \ldots, f_m \rangle$.

Proof.

See [BeWe]. □

Table of Contents

Module Basics

Let $\mathbb{K}[\underline{x}]^m$ be an m-dimensional module with generators $\mathbf{e}_1, \ldots, \mathbf{e}_m$

- We define the **evaluation map** $v_F : \mathbb{K}[\underline{x}]^m \to \mathbb{K}$ such that $v_F(\mathbf{e}_i) = f_i$ for all $i \in \{1, \ldots, m\}$.

Module Basics

Let $\mathbb{K}[\underline{x}]^m$ be an m-dimensional module with generators $\mathbf{e}_1, \ldots, \mathbf{e}_m$

- We define the **evaluation map** $v_F : \mathbb{K}[\underline{x}]^m \to \mathbb{K}$ such that $v_F(\mathbf{e}_i) = f_i$ for all $i \in \{1, \ldots, m\}$.
- We define a **module term ordering** $\prec_{\mathrm{F}}$ on $\mathbb{K}[\underline{x}]^m$:

$$t_i\mathbf{e}_i \prec_{\mathrm{F}} t_j\mathbf{e}_j :\Leftrightarrow \begin{array}{ll} \text{(a)} & i > j, \text{ or} \\ \text{(b)} & i = j \text{ and } t_i < t_j. \end{array}$$

where $t_i, t_j \in \mathcal{T}$. We denote the highest term of an element $\mathbf{g} \in \mathbb{K}[\underline{x}]^m$ w.r.t. $\prec_{\mathrm{F}}$ the **module head term** $\mathrm{MHT}(\mathbf{g})$.

Module Basics

Let $\mathbb{K}[\underline{x}]^m$ be an m-dimensional module with generators $\mathbf{e}_1, \ldots, \mathbf{e}_m$

- We define the **evaluation map** $v_F : \mathbb{K}[\underline{x}]^m \to \mathbb{K}$ such that $v_F(\mathbf{e}_i) = f_i$ for all $i \in \{1, \ldots, m\}$.
- We define a **module term ordering** $\prec_{\mathrm{F}}$ on $\mathbb{K}[\underline{x}]^m$:

$$t_i\mathbf{e}_i \prec_{\mathrm{F}} t_j\mathbf{e}_j :\Leftrightarrow \quad \begin{array}{ll} \text{(a)} & i > j, \text{ or} \\ \text{(b)} & i = j \text{ and } t_i < t_j. \end{array}$$

  where $t_i, t_j \in \mathcal{T}$. We denote the highest term of an element $\mathbf{g} \in \mathbb{K}[\underline{x}]^m$ w.r.t. $\prec_{\mathrm{F}}$ the **module head term** $\mathrm{MHT}(\mathbf{g})$.
- For an element $\mathbf{g} = \sum_{i=1}^m g_i\mathbf{e}_i \in \mathbb{K}[\underline{x}]^m$ we define the **index of g** to be the lowest number k such that $g_k \neq 0$ and denote it by $\mathrm{index}(\mathbf{g})$. Thus we write $\mathbf{g} = \sum_{i=k}^m g_i\mathbf{e}_i$ in the following.

Example

Assume the sequence $F = (f_1, \ldots, f_m)$, $\leq$ the degree reverse lexicographical ordering, $\underline{x} = (x, y)$.
Let

$$\begin{aligned}
\mathbf{g}_1 &= (x^2 + xy)\mathbf{e}_2 + x^7 y\mathbf{e}_4, \\
\mathbf{g}_2 &= x^2 y\mathbf{e}_2 + y\mathbf{e}_3, \\
\mathbf{g}_3 &= \mathbf{e}_1 + x\mathbf{e}_2.
\end{aligned}$$

Example

Assume the sequence $F = (f_1, \ldots, f_m)$, $\leq$ the degree reverse lexicographical ordering, $\underline{x} = (x, y)$.
Let

$$\begin{aligned}\mathbf{g}_1 &= (x^2 + xy)\mathbf{e}_2 + x^7 y\mathbf{e}_4, \\ \mathbf{g}_2 &= x^2 y\mathbf{e}_2 + y\mathbf{e}_3, \\ \mathbf{g}_3 &= \mathbf{e}_1 + x\mathbf{e}_2.\end{aligned}$$

(a) $\mathrm{index}(\mathbf{g}_1) = \mathrm{index}(\mathbf{g}_2) = 2$, $\mathrm{index}(\mathbf{g}_3) = 1$.

Example

Assume the sequence $F = (f_1, \dots, f_m)$, $\leq$ the degree reverse lexicographical ordering, $\underline{x} = (x, y)$.
Let

$$\begin{aligned} \mathbf{g}_1 &= (x^2 + xy)\mathbf{e}_2 + x^7 y \mathbf{e}_4, \\ \mathbf{g}_2 &= x^2 y \mathbf{e}_2 + y \mathbf{e}_3, \\ \mathbf{g}_3 &= \mathbf{e}_1 + x \mathbf{e}_2. \end{aligned}$$

(a) $\mathrm{index}(\mathbf{g}_1) = \mathrm{index}(\mathbf{g}_2) = 2$, $\mathrm{index}(\mathbf{g}_3) = 1$.

(b) $\mathrm{MHT}(\mathbf{g}_1) = x^2\mathbf{e}_2$ as $2 < 4$ and $x^2 > xy$. Similar we receive $\mathrm{MHT}(\mathbf{g}_2) = x^2 y \mathbf{e}_2$ and $\mathrm{MHT}(\mathbf{g}_3) = \mathbf{e}_1$.

Example

Assume the sequence $F = (f_1, \ldots, f_m)$, $\leq$ the degree reverse lexicographical ordering, $\underline{x} = (x, y)$.
Let

$$\begin{aligned} \mathbf{g}_1 &= (x^2 + xy)\mathbf{e}_2 + x^7 y\mathbf{e}_4, \\ \mathbf{g}_2 &= x^2 y\mathbf{e}_2 + y\mathbf{e}_3, \\ \mathbf{g}_3 &= \mathbf{e}_1 + x\mathbf{e}_2. \end{aligned}$$

(a) $\mathrm{index}(\mathbf{g}_1) = \mathrm{index}(\mathbf{g}_2) = 2$, $\mathrm{index}(\mathbf{g}_3) = 1$.
(b) $\mathrm{MHT}(\mathbf{g}_1) = x^2\mathbf{e}_2$ as $2 < 4$ and $x^2 > xy$. Similar we receive $\mathrm{MHT}(\mathbf{g}_2) = x^2 y\mathbf{e}_2$ and $\mathrm{MHT}(\mathbf{g}_3) = \mathbf{e}_1$.
(c) $\mathrm{MHT}(\mathbf{g}_1) \prec_{\mathrm{F}} \mathrm{MHT}(\mathbf{g}_2)$ as both have the same index and $x^2 < x^2 y$. $\mathrm{MHT}(\mathbf{g}_2) \prec_{\mathrm{F}} \mathrm{MHT}(\mathbf{g}_3)$ as $\mathrm{index}(\mathbf{g}_3) < \mathrm{index}(\mathbf{g}_2)$.

Labeling of a Polynomial

- A polynomial p is called **admissible (w.r.t. F)** if there exists an element $\mathbf{g} \in \mathbb{K}[\underline{x}]^m$ such that $v_F(\mathbf{g}) = p$.

Labeling of a Polynomial

- A polynomial p is called **admissible (w.r.t. F)** if there exists an element $\mathbf{g} \in \mathbb{K}[\underline{x}]^m$ such that $v_F(\mathbf{g}) = p$.
- An **admissible, labeled polynomial** r is an element of $\mathbb{K}[\underline{x}]^m \times \mathbb{K}[\underline{x}]$ defined by $r = \big(\mathcal{S}(r), \mathrm{poly}(r)\big)$ where

Labeling of a Polynomial

- A polynomial p is called **admissible (w.r.t. F)** if there exists an element $\mathbf{g} \in \mathbb{K}[\underline{x}]^m$ such that $v_F(\mathbf{g}) = p$.
- An **admissible, labeled polynomial** r is an element of $\mathbb{K}[\underline{x}]^m \times \mathbb{K}[\underline{x}]$ defined by $r = \big(\mathcal{S}(r), \mathrm{poly}(r)\big)$ where
  - $\mathrm{poly}(r) \in \mathbb{K}[\underline{x}]$ is the polynomial part,

Labeling of a Polynomial

- A polynomial p is called **admissible (w.r.t. F)** if there exists an element $\mathbf{g} \in \mathbb{K}[\underline{x}]^m$ such that $v_F(\mathbf{g}) = p$.
- An **admissible, labeled polynomial** r is an element of $\mathbb{K}[\underline{x}]^m \times \mathbb{K}[\underline{x}]$ defined by $r = \big(\mathcal{S}(r), \mathrm{poly}(r)\big)$ where
  - $\mathrm{poly}(r) \in \mathbb{K}[\underline{x}]$ is the polynomial part,
  - $\mathcal{S}(r) = \mathrm{MHT}(\mathbf{g})$ such that $v_F(\mathbf{g}) = \mathrm{poly}(r)$ is the **signature of** r.

Labeling of a Polynomial

- A polynomial p is called **admissible (w.r.t. F)** if there exists an element $\mathbf{g} \in \mathbb{K}[\underline{x}]^m$ such that $v_F(\mathbf{g}) = p$.
- An **admissible, labeled polynomial** r is an element of $\mathbb{K}[\underline{x}]^m \times \mathbb{K}[\underline{x}]$ defined by $r = \big(\mathcal{S}(r), \mathrm{poly}(r)\big)$ where
  - $\mathrm{poly}(r) \in \mathbb{K}[\underline{x}]$ is the polynomial part,
  - $\mathcal{S}(r) = \mathrm{MHT}(\mathbf{g})$ such that $v_F(\mathbf{g}) = \mathrm{poly}(r)$ is the **signature of** r.
- The **index of** r is defined to be $\mathrm{index}(r) = \mathrm{index}\big(\mathcal{S}(r)\big)$.

Labeling of a Polynomial

- A polynomial p is called **admissible (w.r.t. F)** if there exists an element $\mathbf{g} \in \mathbb{K}[\underline{x}]^m$ such that $v_F(\mathbf{g}) = p$.
- An **admissible, labeled polynomial** r is an element of $\mathbb{K}[\underline{x}]^m \times \mathbb{K}[\underline{x}]$ defined by $r = \big(\mathcal{S}(r), \mathrm{poly}(r)\big)$ where
  - $\mathrm{poly}(r) \in \mathbb{K}[\underline{x}]$ is the polynomial part,
  - $\mathcal{S}(r) = \mathrm{MHT}(\mathbf{g})$ such that $v_F(\mathbf{g}) = \mathrm{poly}(r)$ is the **signature of** r.
- The **index of** r is defined to be $\mathrm{index}(r) = \mathrm{index}\big(\mathcal{S}(r)\big)$.
- For an admissible labeled polynomial r with $\mathcal{S}(r) = t\mathbf{e}_k$ we denote the **term of the signature** of r to be

$$\Gamma\big(\mathcal{S}(r)\big) = t \in \mathcal{T}.$$

Labeling of a Polynomial

- If r_1, r_2 are admissible labeled polynomials such that $u_2\mathcal{S}(r_2) \prec_{\mathrm{F}} u_1\mathcal{S}(r_1)$ then

$$\mathrm{Spol}(r_1, r_2) = \Big(u_1\mathcal{S}(r_1), \mathrm{Spol}\big(\mathrm{poly}(r_1), \mathrm{poly}(r_2)\big)\Big).$$

Labeling of a Polynomial

- If r_1, r_2 are admissible labeled polynomials such that $u_2\mathcal{S}(r_2) \prec_{\mathrm{F}} u_1\mathcal{S}(r_1)$ then

$$\mathrm{Spol}(r_1, r_2) = \Big(u_1\mathcal{S}(r_1), \mathrm{Spol}\big(\mathrm{poly}(r_1), \mathrm{poly}(r_2)\big)\Big).$$

- If $r = \big(\mathcal{S}(r), \mathrm{poly}(r)\big)$ is an admissible labeled polynomial and $\mathcal{R} := \{r_1, \ldots, r_m\}$ is a set of admissible labeled polynomials then we say that

$$\mathrm{poly}(r) = \sum_{i=1}^{n} \lambda_i \mathrm{poly}(r_i) \quad \lambda_i \in \mathbb{K}[\underline{x}]$$

  is an **admissible** t**-representation of** r **w.r.t.** $\mathcal{R}$ if $\mathrm{HT}\big(\lambda_i \mathrm{poly}(r_i)\big) < t$ and $\mathrm{HT}(\lambda_i)\mathcal{S}(r_i) \preceq_{\mathrm{F}} \mathcal{S}(r)$ for all i and $t = \mathrm{HT}\big(\mathrm{poly}(r)\big)$.

Example

Assume the sequence $F = (f_1, \ldots, f_m)$.

(a) Let $p = f_1$. Then $r = (\mathbf{e}_1, f_1)$ is an admissible labeled polynomial as $v_F(\mathbf{e}_1) = f_1$.

Example

Assume the sequence $F = (f_1, \ldots, f_m)$.

(a) Let $p = f_1$. Then $r = (\mathbf{e}_1, f_1)$ is an admissible labeled polynomial as $v_F(\mathbf{e}_1) = f_1$.

(b) Again let $p = f_1$. Then $r' = (\mathrm{HT}(f_2)\mathbf{e}_1, f_1)$ is also an admissible labeled polynomial. For this consider the module element $\mathbf{g} = (f_2 + 1)\mathbf{e}_1 - f_1\mathbf{e}_2$. It holds that $v_F(\mathbf{g}) = f_2 f_1 + f_1 - f_1 f_2 = f_1$ and $\mathrm{MHT}(\mathbf{g}) = \mathrm{HT}(f_2)\mathbf{e}_1$.

Example

Assume the sequence $F = (f_1, \ldots, f_m)$.

(a) Let $p = f_1$. Then $r = (\mathbf{e}_1, f_1)$ is an admissible labeled polynomial as $v_F(\mathbf{e}_1) = f_1$.

(b) Again let $p = f_1$. Then $r' = (\mathrm{HT}(f_2)\mathbf{e}_1, f_1)$ is also an admissible labeled polynomial. For this consider the module element $\mathbf{g} = (f_2 + 1)\mathbf{e}_1 - f_1\mathbf{e}_2$. It holds that $v_F(\mathbf{g}) = f_2 f_1 + f_1 - f_1 f_2 = f_1$ and $\mathrm{MHT}(\mathbf{g}) = \mathrm{HT}(f_2)\mathbf{e}_1$.

Remark

For a polynomial p there can exist infinitely many different admissible labeled polynomials r such that $\mathrm{poly}(r) = p$. In the case of F being a **regular sequence** the admissible labeled polynomial r corresponding to a polynomial p computed by F_5 is uniquely defined.

Table of Contents

New Characterization of Gröbner Bases

Notations

In the following we use a shorter notation for $r = \big(\mathcal{S}(r), \mathrm{poly}(r)\big)$ denoting $\mathrm{poly}(r)$ by p. $G = \{r_1, \ldots, r_m\}$ denotes a set of admissible labeled polynomials such that $\mathrm{poly}(G) := \{p_i \mid r_i \in G\} \supset \{f_1, \ldots, f_m\}$.

New Characterization of Gröbner Bases

Notations

In the following we use a shorter notation for $r = \big(\mathcal{S}(r), \mathrm{poly}(r)\big)$ denoting $\mathrm{poly}(r)$ by p. $G = \{r_1, \ldots, r_m\}$ denotes a set of admissible labeled polynomials such that $\mathrm{poly}(G) := \{p_i \mid r_i \in G\} \supset \{f_1, \ldots, f_m\}$.

Theorem (Admissible Representation Characterization)

If for all $r_i, r_j \in G$ $Spol(r_i, r_j)$ has an admissible t-representation for $t = LCM\big(HT(p_i), HT(p_j)\big)$ or $Spol(p_i, p_j)$ reduces to zero w.r.t. G then $poly(G)$ is a Gröbner basis of $I = \langle f_1, \ldots, f_m \rangle$.

New Characterization of Gröbner Bases

Notations

In the following we use a shorter notation for $r = \big(\mathcal{S}(r), \mathrm{poly}(r)\big)$ denoting $\mathrm{poly}(r)$ by p. $G = \{r_1, \ldots, r_m\}$ denotes a set of admissible labeled polynomials such that $\mathrm{poly}(G) := \{p_i \mid r_i \in G\} \supset \{f_1, \ldots, f_m\}$.

Theorem (Admissible Representation Characterization)

If for all $r_i, r_j \in G$ $Spol(r_i, r_j)$ has an admissible t-representation for $t = LCM\big(HT(p_i), HT(p_j)\big)$ or $Spol(p_i, p_j)$ reduces to zero w.r.t. G then $poly(G)$ is a Gröbner basis of $I = \langle f_1, \ldots, f_m \rangle$.

Proof

If r is an admissible labeled polynomial with admissible t-representation then p has a t-representation for $t = \mathrm{HT}(p)$.

Faugère's Criteria

F_5 Criterion

$\mathrm{Spol}(r_i, r_j)$ is **not normalized** iff for $u_k r_k$ ($k = i$ or $k = j$) there exist $r_{\mathrm{prev}} \in G$ such that

$$\begin{aligned} \mathrm{index}(r_{\mathrm{prev}}) &> \mathrm{index}(r_k) \\ \mathrm{HT}(p_{\mathrm{prev}}) &\mid u_k \Gamma\big(\mathcal{S}(r_k)\big). \end{aligned}$$

This Criterion is stated explicitly in Faugère's description of the F_5 Algorithm, but it is **not** the only one.

Faugère's Criteria

F_5 Criterion

$\mathrm{Spol}(r_i, r_j)$ is **not normalized** iff for $u_k r_k$ ($k = i$ or $k = j$) there exist $r_{\mathrm{prev}} \in G$ such that

$$\begin{aligned} \mathrm{index}(r_{\mathrm{prev}}) &> \mathrm{index}(r_k) \\ \mathrm{HT}(p_{\mathrm{prev}}) &\mid u_k \Gamma\big(\mathcal{S}(r_k)\big). \end{aligned}$$

This Criterion is stated explicitly in Faugère's description of the F_5 Algorithm, but it is **not** the only one.

Remark

This criterion would delete the element $r' = (\mathrm{HT}(f_2)\mathbf{e}_1, f_1)$ as the element $r_2 = (\mathbf{e}_2, f_2)$ has $\mathrm{index}(r_2) = 2 > 1$ and clearly $\mathrm{HT}\big(\mathrm{poly}(r_2)\big) \mid \mathrm{HT}(f_2)$.

Faugère's Criteria

Rewritten Criterion

$\mathrm{Spol}(r_i, r_j)$ is **rewritable** iff for $u_k r_k$ ($k = i$ or $k = j$) there exist $r_v, r_w \in G$ such that

$$\begin{aligned} \mathrm{index}(r_k) &= \mathrm{index}\big(\mathrm{Spol}(r_v, r_w)\big) \\ \Gamma\Big(\mathcal{S}\big(\mathrm{Spol}(r_v, r_w)\big)\Big) &\mid u_k \Gamma\big(\mathcal{S}(r_k)\big). \end{aligned}$$

This Criterion is not stated explicitly, but it is part of the pseudocode.

Using the Criteria to compute Gröbner Bases

Theorem (New Characterization using Faugère's Criteria)

Let $\mathcal{L} \subset G \times G$ such that for every element $(r_i, r_j) \in \mathcal{L}$ $\mathcal{S}pol(r_i, r_j)$ is

(a) *normalized, and*

(b) *not rewritable.*

If each such $\mathcal{S}pol(r_i, r_j)$ has a t-representation with $t = LCM\big(HT(p_i), HT(p_j)\big)$ or reduces to zero, then $poly(G)$ is a Gröbner basis of $I = \langle f_1, \ldots, f_m \rangle$.

Using the Criteria to compute Gröbner Bases

Theorem (New Characterization using Faugère's Criteria)

Let $\mathcal{L} \subset G \times G$ such that for every element $(r_i, r_j) \in \mathcal{L}$ $\mathcal{S}pol(r_i, r_j)$ is

(a) *normalized, and*

(b) *not rewritable.*

If each such $\mathcal{S}pol(r_i, r_j)$ has a t-representation with $t = \mathcal{LCM}\big(\mathcal{HT}(p_i), \mathcal{HT}(p_j)\big)$ or reduces to zero, then $poly(G)$ is a Gröbner basis of $I = \langle f_1, \ldots, f_m \rangle$.

Remark

The idea is to only investigate on S-Polynomials with generators being elements of $\mathcal{L}$. We need to show that all other S-Polynomials have a t-representation or reduce to zero.

Using the Criteria to compute Gröbner Bases

Idea of the Proof

If $\mathrm{Spol}(r_i, r_j)$ is not normalized and/or rewritable then we can assume w.l.o.g. that $u_i r_i$ with $\mathrm{index}(r_i) = k$ is not normalized and/or rewritable. It follows that there exists a (not necessarily principal) syzygy with the element $u_i \Gamma\big(\mathcal{S}(r)\big)\mathbf{e}_k$. From this syzygy we can compute a *rewriter* r_{rew} such that we get the following relationship:

$$\mathrm{Spol}(r_i, r_j) = \lambda_1 \mathrm{Spol}(r_i, r_{\mathrm{rew}}) + \lambda_2 \mathrm{Spol}(r_{\mathrm{rew}}, r_j).$$

Both, $\mathrm{Spol}(r_i, r_{\mathrm{rew}})$ and $\mathrm{Spol}(r_{\mathrm{rew}}, r_j)$ were already or will be investigated in F_5. This leads to an admissible t-representation of $\mathrm{Spol}(r_i, r_j)$ where $t = \mathrm{LCM}\big(\mathrm{HT}(p_i), \mathrm{HT}(p_j)\big)$.

Example of the Rewritten Criterion

In [Fa] Faugère computes the Gröbner basis of $I = \langle f_1, f_2, f_3 \rangle$ where

$$\begin{aligned} f_1 &= yz^3 - x^2t^2 \\ f_2 &= xz^2 - y^2t \\ f_3 &= x^2y - z^2t \end{aligned}$$

in $\mathbb{Q}[x, y, z, t]$ with degree reverse lexicographical ordering $x > y > z > t$. During these computations $\mathrm{Spol}(r_1, r_3) = (x^2\mathcal{S}(r_1), x^2f_1 - z^3f_3)$ is detected to be rewritable by the element $r_6 = (x\mathbf{e}_1, y^3zt - x^3t^2)$ as both have the same index and $x\Gamma\big(\mathcal{S}(r_6)\big) = x^2\Gamma\big(\mathcal{S}(r_1)\big)$. r_6 was computed from $\mathrm{Spol}(r_1, r_2)$ such that we have a syzygy $\mathbf{s}_6 = x\mathbf{e}_1 - yz\mathbf{e}_2 - \mathbf{e}_6$, for r_1 we have the trivial syzygy $\mathbf{s}_1 = \mathbf{e}_1 - \mathbf{e}_1$.

Example of the Rewritten Criterion

If we compute

$$\begin{aligned} x^2\mathbf{s}_1 + x\mathbf{s}_6 &= x^2\mathbf{e}_1 - x^2\mathbf{e}_1 + x^2\mathbf{e}_1 - xyz\mathbf{e}_2 - x\mathbf{e}_6 \\ &= x^2\mathbf{e}_1 - xyz\mathbf{e}_2 - x\mathbf{e}_6. \end{aligned}$$

From this we receive that $xyz\mathrm{HT}(p_2) = x^2\mathrm{HT}(p_1)$ and $xyz\mathrm{HT}(p_2) = z^3\mathrm{HT}(p_3)$. Thus we can rewrite $\mathrm{Spol}(r_1, r_3) = x\mathrm{Spol}(r_1, r_2) + z\mathrm{Spol}(r_2, r_3)$.
Thus $\mathrm{Spol}(r_1, r_3)$ can be deleted from further investigations as it does not give us new information about the Gröbner basis of I.

Table of Contents

Facts about the F_5 Algorithm

Faugère's F_5 Algorithm

- ... is one of the fastest known Gröbner bases algorithms.

Facts about the F_5 Algorithm

Faugère's F_5 Algorithm

- ... is one of the fastest known Gröbner bases algorithms.
- ... uses two criteria, the F_5 Criterion and the Rewritten Criterion.

Facts about the F_5 Algorithm

Faugère's F_5 Algorithm

- ... is one of the fastest known Gröbner bases algorithms.
- ... uses two criteria, the F_5 Criterion and the Rewritten Criterion.
- ... does not compute any zero-reduction in the case of F being a regular sequence.

Facts about the F_5 Algorithm

Faugère's F_5 Algorithm

- ... is one of the fastest known Gröbner bases algorithms.
- ... uses two criteria, the F_5 Criterion and the Rewritten Criterion.
- ... does not compute any zero-reduction in the case of F being a regular sequence.
- ... cannot be combined with other known criteria, e.g. the Buchberger Criteria.

Facts about the F_5 Algorithm

Faugère's F_5 Algorithm

- ... is one of the fastest known Gröbner bases algorithms.
- ... uses two criteria, the F_5 Criterion and the Rewritten Criterion.
- ... does not compute any zero-reduction in the case of F being a regular sequence.
- ... cannot be combined with other known criteria, e.g. the Buchberger Criteria.
- ... should not be implemented as stated in [Fa]. The code needs lots of optimizations to be fast.

Table of Contents

References

T. Becker, V. Weispfenning and H. Kredel.
Gröbner Bases
Springer Verlag, 1993

J.-C. Faugère.
A new efficient algorithm for computing Gröbner bases without reduction to zero F_5
Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation ISSAC, pages 75 - 83, 2002

G.-M. Greuel, G. Pfister and H. Schönemann.
SINGULAR 3-0-4. *A computer algebra system for polynomial computations*, TU Kaiserslautern, 2008, `http://www.singular.uni-kl.de`.