Computer Science Journal of Moldova, vol.**16**, no.1(46), 2008

A New Attempt On The F_5 Criterion

Christian Eder

Abstract

Faugère's criterion used in the F_5 algorithm is still not understand and thus there are not many implementations of this algorithm. We state its proof using syzygies to explain the normalization condition of a polynomial. This gives a new insight in the way the F_5 criterion works.

1 Introduction

In 2002 Faugère published a new algorithm for computing Gröbner bases [2]. He found a new criterion defining when a set is a Gröbner basis. This criterion can be used to compute Gröbner bases of ideals generated by arbitrary finite sequences of polynomials.

In the F_5 algorithm additional data on the polynomials is used to detect redundant critical pairs in advance to avoid computations of zero. In this paper we give a proof of the F_5 criterion with some easier and more general arguments.

The plan of the paper is as follows: In section 2 we give briefly the basic definitions for Gröbner basis computations as well as the main terminology for the F_5 criterion. In section 3 we prove the main theorem of this paper, the F_5 criterion.

2 Basic Notations

Throughout this paper ring always means a commutative ring with identity, $\mathbb{N}$ is the set of non-negative integers. $\mathbb{K}$ denotes the ground field, $\mathbb{K}[\underline{x}]$ the polynomial ring over $\mathbb{K}$ in the finite sequence of n variables $\underline{x} = (x_1, \dots, x_n)$. $\mathcal{T}$ denotes the set of terms of $\mathbb{K}[\underline{x}]$. Furthermore let $<$ be a total order on $\mathbb{K}[\underline{x}]$.

2.1 Gröbner basics

We briefly give the main definitions needed to define a Gröbner basis in a characterization useful for our purposes.

Definition 2.1. Let $t = x_1^{\alpha_1} \cdots x_n^{\alpha_n} \in \mathcal{T}$ where $\alpha_i \in \mathbb{N}$ for $i \in \{1, \dots, n\}$. The *total degree of* t is defined to be $\deg(t) = \sum_{i=1}^{n} \alpha_i$.

Let

$$f = \sum_{\alpha} c_{\alpha_1, \dots, \alpha_n} x_1^{\alpha_1} \cdots x_n^{\alpha_n} = \sum_{\alpha} c_\alpha x^\alpha \in \mathbb{K}[\underline{x}] \backslash \{0\}$$

where $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{N}^n$, $c_\alpha \in \mathbb{K}$, and only finitely many $c_\alpha \neq 0$. The *total degree of* f is defined as $\deg(f) = \max\{\alpha_1 + \cdots + \alpha_n \mid c_{\alpha_1, \dots, \alpha_n} \neq 0\}$. Furthermore writing $f = c_\alpha x^\alpha + c_\beta x^\beta + \cdots + c_\gamma x^\gamma$, $x^\alpha > x^\beta > \cdots > x^\gamma$ in a unique way as a sum of non-zero terms we define

(a) the head monomial of f: $\mathrm{HM}(f) = c_\alpha x^\alpha$,

(b) the head term of f: $\mathrm{HT}(f) = x^\alpha$,

(c) the head coefficient of f: $\mathrm{HC}(f) = c_\alpha$.

Definition 2.2. Let $f, g \in \mathbb{K}[\underline{x}] \backslash \{0\}$. The *S-polynomial* of f and g is defined to be

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

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

Definition 2.3. Let $P \subset \mathbb{K}[\underline{x}]$ be a finite set, $0 \neq f \in \mathbb{K}[\underline{x}]$, and $t \in \mathcal{T}$. A representation

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

where $\lambda_p \in \mathbb{K}[\underline{x}]$, $p \in P$ is called a *t-representation of f w.r.t. P* if for all $p \in P$ such that $\lambda_p \neq 0$ $\mathrm{HT}(\lambda_p p) \leq t$.

For $t = \mathrm{HT}(f)$ a t-representation of f is called a *standard representation*

There are a lot of equivalent characterizations of Gröbner bases, see for example [1]. The one we need in this paper is stated next.

Theorem 2.4. *Let $G = \{g_1, \ldots, g_{n_G}\}$ be a finite subset of $\mathbb{K}[\underline{x}]$ with $0 \notin G$. If for all $f \in I = \langle g_1, \ldots, g_{n_G} \rangle$ f has a standard representation, then G is a Gröbner basis of I.*

Proof. See [1]. □

2.2 F_5 basics

We extend given definitions and state new terminology needed to understand Faugère's F_5 criterion.

In the following let $F = (f_1, \ldots, f_m)$ be a sequence of polynomials in $\mathbb{K}[\underline{x}]$, $\mathbb{K}[\underline{x}]^m$ denotes the free $\mathbb{K}[\underline{x}]$-module of rank m.

Definition 2.5. Let $\mathbf{g} = \sum_{k=1}^m g_k \mathbf{e}_k \in \mathbb{K}[\underline{x}]^m$ where $\mathbf{e}_k$ denotes the k-th standard vector in $\mathbb{K}[\underline{x}]^m$. We define the evaluation map w.r.t. F $v_F : \mathbb{K}[\underline{x}]^m \to \mathbb{K}[\underline{x}]$ such that

$$v_F\left(\sum_{k=1}^m g_k \mathbf{e}_k\right) = \sum_{k=1}^m g_k f_k$$

An element $\mathbf{s} \in \mathbb{K}[\underline{x}]^m$ is called a syzygy w.r.t. F if $v_F(\mathbf{s}) = 0$. For $m \geq 2$ for each pair f_i, f_j with $1 \leq i < j \leq m$ we have a so-called principal syzygy w.r.t. F, $\pi_{i,j} = f_j \mathbf{e}_i - f_i \mathbf{e}_j$.

The set of all syzygies w.r.t. F is denoted $\mathrm{Syz}(F) = \ker(v_F)$ and generates an $\mathbb{K}[\underline{x}]$-module. The submodule generated by all principal syzygies w.r.t. F is denoted $\mathrm{PSyz}(F)$.

Next we define an ordering of $\mathbb{K}[\underline{x}]^m$.

Definition 2.6. Let $\mathbf{g} = \sum_{k=1}^m g_k \mathbf{e}_k \in \mathbb{K}[\underline{x}]^m$. The index of $\mathbf{g}$, denoted by $\mathrm{index}(\mathbf{g})$, is the smallest $i \in \{1, \ldots, m\}$ such that $g_i \neq 0$.

Suppose that $\mathbf{g}$ and $\mathbf{h} \in \mathbb{K}[\underline{x}]^m$ with $\mathrm{index}(\mathbf{g}) = i$ and $\mathrm{index}(\mathbf{h}) = j$. Then we can write $\mathbf{g} = \sum_{k=i}^m g_k \mathbf{e}_k$ and $\mathbf{h} = \sum_{k=j}^m h_k \mathbf{e}_k$.

$$\mathbf{g} \prec \mathbf{h} :\Leftrightarrow \begin{cases} i > j, \text{ or} \\ i = j \text{ and } \mathrm{HT}(g_i) < \mathrm{HT}(h_i) \end{cases}$$

For any $\mathbf{g} \in \mathbb{K}[\underline{x}]^m \backslash \{0\}$ it holds that $0 \prec \mathbf{g}$.

This leads to an extension of the terminology of head terms.

Definition 2.7. Let $\mathbf{g} \in \mathbb{K}[\underline{x}]^m \backslash \{0\}$ with $\mathrm{index}(\mathbf{g}) = i$. The module head term MHT of $\mathbf{g}$ is defined to be $\mathrm{MHT}(\mathbf{g}) = \mathrm{HT}(g_i)\mathbf{e}_i$.

Lemma 2.8. *The module ordering $\prec$ is well-founded.*

Proof. Let $\emptyset \neq P \subset \mathbb{K}[\underline{x}]^m$. The index of any element $\mathbf{p} = \sum_{i=1}^m p_i \mathbf{e}_i \in P$ is bounded by m, and $\leq$ is a well-ordering on the head terms of polynomials in $\mathbb{K}[\underline{x}]$. Thus

$$\begin{aligned} i_{\max} &:= \max\{\mathrm{index}(\mathbf{p}) \mid \mathbf{p} \in P\} \\ t_{\min} &:= \min\{\mathrm{HT}(p_k) \mid \mathbf{p} \in P, \mathrm{index}(\mathbf{p}) = k\} \end{aligned}$$

are well-defined. Then

$$\emptyset \neq M := \{\mathbf{p} \in P \mid \mathrm{index}(\mathbf{p}) = i_{\max}, \mathrm{HT}(p_{i_{\max}}) = t_{\min}\}$$

is the set of minimal elements of P. $\square$

Next we define a connection between polynomials in $\mathbb{K}[\underline{x}]$ and module elements in $\mathbb{K}[\underline{x}]^m$. These are the main concepts for the F_5 criterion.

Definition 2.9.

(a) A *labeled polynomial* r is an element $r = (u\mathbf{e}_k, p)$ such that $u \in \mathcal{T}$, $p \in \mathbb{K}[\underline{x}]$.

(b) The *signature of* r is defined by $\mathcal{S}(r) := u\mathbf{e}_k$, the *polynomial of* r by $\mathrm{poly}(r) := p$, and the *index of* r by $\mathrm{index}(r) := k$. For a finite set G of labeled polynomials we define $\mathrm{poly}(G) := \{\mathrm{poly}(r) | r \in G\}$.

(c) If $t \in \mathcal{T}$ then $tr := (tu\mathbf{e}_k, tp)$, if $c \in \mathbb{K}$ then $cr := (u\mathbf{e}_k, cp)$.

(d) r is called *admissible w.r.t.* F if there exists a $\mathbf{g} \in \mathbb{K}[\underline{x}]^m \backslash \{0\}$ such that $v_F(\mathbf{g}) = p$ and $\mathrm{MHT}(\mathbf{g}) = \mathcal{S}(r)$.

(e) Let G be a finite set of labeled admissible w.r.t. F polynomials. r is called *normalized w.r.t.* G if $u \notin \mathrm{HT}(\langle\{p_i \in \mathrm{poly}(G) \mid \mathrm{index}(r_i) > \mathrm{index}(r)\}\rangle)$.

(f) Let (r_1, r_2) be a pair of labeled polynomials with $\tau = \mathrm{lcm}\big(\mathrm{HT}(\mathrm{poly}(r_1)), \mathrm{HT}(\mathrm{poly}(r_2))\big)$, $\tau_i = \frac{\tau}{\mathrm{HT}(\mathrm{poly}(r_i))}$ for $i \in \{1, 2\}$. Then (r_1, r_2) is called normalized if $\tau_1 r_1$, $\tau_2 r_2$ are normalized and $\mathcal{S}(\tau_2 r_2) \prec \mathcal{S}(\tau_1 r_1)$. For a pair of labeled polynomials (r_1, r_2) where r_1, r_2 are admissible to $\mathbf{g}_1, \mathbf{g}_2$ respectively, we define the S-polynomial to be

$$\mathrm{Spol}(r_1, r_2) := \big(\mathrm{MHT}(\tau_1\mathbf{g}_1 - \tau_2\mathbf{g}_2), c_2\tau_1\mathrm{poly}(r_1) - c_1\tau_2\mathrm{poly}(r_2)\big),$$

where $c_i = \mathrm{HC}(\mathrm{poly}(r_i))$ for $i \in \{1, 2\}$.

Corollary 2.10. *If r_1 and r_2 are admissible labeled polynomials w.r.t. F then Spol(r_1, r_2) is an admissible labeled polynomial w.r.t. F.*

3 F_5 criterion

Next we prove the F_5 criterion stated in [2]. For this purpose we need some lemmata and more notations.

Convention 3.1. In the following let $F = (f_1, \ldots, f_m)$, $f_i \in \mathbb{K}[\underline{x}]$, $G = \{r_1, \ldots, r_{n_G}\}$ a set of labeled admissible w.r.t. F polynomials such that

$$\{(\mathbf{e}_1, f_1), \ldots, (\mathbf{e}_m, f_m)\} \subset G.$$

Let $p_i = \operatorname{poly}(r_i)$ for all $i \in \{1, \ldots, n_G\}$, $\operatorname{poly}(G) = \{p_1, \ldots, p_{n_G}\}$.

When we write *admissible* we always mean *admissible w.r.t. F*.

Lemma 3.2. *If an admissible labeled polynomial $r = (u\mathbf{e}_k, p)$ with $\mathbf{g} \in \mathbb{K}[\underline{x}]^m$ such that $MHT(\mathbf{g}) = u\mathbf{e}_k$ and $v_F(\mathbf{g}) = p$ is non-normalized w.r.t. G then there exists $\mathbf{s} \in PSyz(F)$ with $index(\mathbf{s}) = k$ such that $MHT(\mathbf{g} - \mathbf{s}) \prec MHT(\mathbf{g})$.*

Proof. If $r = (u\mathbf{e}_k, p)$ is non-normalized then there exists $r_i \in G$ with $p_i = \sum_{\ell=k_0}^{m} \lambda_\ell f_\ell \in G$ where $\lambda_\ell \in \mathcal{K}[\underline{x}]$ such that $\operatorname{index}(r_i) = k_0 > k$ and $\operatorname{HT}(p_i) \mid u$. So there exists $t \in \mathcal{T}$ such that $t\operatorname{HT}(p_i) = u$. Let $\mathbf{z} := p_i\mathbf{e}_k - f_k \sum_{\ell=k_0}^{m} \lambda_\ell \mathbf{e}_\ell \in \operatorname{Syz}(F)$. Now we can rewrite

$$\begin{aligned}
p_i\mathbf{e}_k - f_k \sum_{\ell=k_0}^{m} \lambda_\ell \mathbf{e}_\ell &= \left(\sum_{\ell=k_0}^{m} \lambda_\ell f_\ell\right) \mathbf{e}_k - f_k \sum_{\ell=k_0}^{m} \lambda_\ell \mathbf{e}_\ell \\
&= \lambda_{k_0} f_{k_0} \mathbf{e}_k - \lambda_{k_0} f_k \mathbf{e}_{k_0} + \lambda_{k_0+1} f_{k_0+1} \mathbf{e}_k - \\
&\quad - \lambda_{k_0+1} f_k \mathbf{e}_{k_0+1} + \cdots + \lambda_m f_m \mathbf{e}_k - \lambda_m f_k \mathbf{e}_m \\
&= \lambda_{k_0} \pi_{k,k_0} + \lambda_{k_0+1} \pi_{k,k_0+1} + \cdots + \lambda_m \pi_{k,m} \\
&= \sum_{\ell=k_0}^{m} \lambda_\ell \pi_{k,\ell}
\end{aligned}$$

where $\pi_{v,w}$ denotes the principal syzygy $f_w\mathbf{e}_v - f_v\mathbf{e}_w \in \operatorname{PSyz}(F)$ for $v < w \in \{1, \ldots, m\}$. Set $\mathbf{s} = t\mathbf{z} \in \operatorname{PSyz}(F)$. By construction $\operatorname{index}(\mathbf{s}) = k$, $\operatorname{MHT}(\mathbf{g} - \mathbf{s}) \prec \operatorname{MHT}(\mathbf{g})$ and $v_F(\mathbf{g} - \mathbf{s}) = v_F(\mathbf{g})$. □

Lemma 3.3. *Let $r = (u\mathbf{e}_k, p)$ and let $\tau_1, \tau_2 \in \mathcal{T}$. If $\tau_2\tau_1 r$ is normalized w.r.t. $G \Rightarrow \tau_1 r$ is normalized w.r.t. G.*

Proof. Let $\tau_2\tau_1 r = (\tau_2\tau_1 u e_k, \tau_2\tau_1 p)$ be normalized w.r.t. G.

Assume for contradiction that $\tau_1 r = (\tau_1 u e_k, \tau_1 p)$ is non-normalized w.r.t. G. Then there exists $r_0 \in G$ such that $\operatorname{index}(r_0) > k$ and $\operatorname{HT}(p_0) \mid \tau_1 u$. Then $\operatorname{HT}(p_0) \mid \tau_2\tau_1 u$ and it follows that $\tau_2\tau_1 r$ is non-normalized w.r.t. G, which contradicts our assumption that $\tau_2\tau_1 r$ is normalized w.r.t. G. $\square$

The following definition of the ordering $\lessdot$ for representations of a labeled polynomials is similar to the one Faugère has stated in [2]. For a deeper insight we refer to [3].

Definition 3.4. Let $f \in I = \langle g_1, \ldots, g_{n_G}\rangle$. Then we define

$$\mathcal{R}_f := \Big\{(\lambda,\sigma) \in \mathbb{K}[\underline{x}]^{n_G} \times \operatorname{Sym}_{n_G} \mid f = \sum_{i=1}^{n_G} \lambda_i p_{\sigma(i)}, \mathcal{S}(\lambda_1 r_{\sigma(1)}) \succeq \ldots \\ \cdots \succeq \mathcal{S}(\lambda_{n_G} r_{\sigma(n_G)})\Big\}$$

to be the set of *labeled representations of* f *w.r.t.* G where Sym_{n_G} denotes the symmetric group on $\{1,\ldots,n_G\}$. Next we define the ordering $\lessdot$ on labeled representations of f w.r.t. G.

For two labeled representations of f w.r.t. G, (λ,σ) and (λ',σ'), we define

$$\begin{aligned} \omega &= \big(\mathcal{S}(\operatorname{HT}(\lambda_1) r_{\sigma(1)}), \ldots, \mathcal{S}(\operatorname{HT}(\lambda_{n_G}) r_{\sigma(n_G)})\big), \\ \omega' &= \big(\mathcal{S}(\operatorname{HT}(\lambda'_1) r_{\sigma'(1)}), \ldots, \mathcal{S}(\operatorname{HT}(\lambda'_{n_G}) r_{\sigma'(n_G)})\big), \end{aligned}$$

respectively.
$(\lambda,\sigma) \lessdot (\lambda',\sigma')$ iff one of the following conditions holds:

(a) $\exists i$ such that $\forall 1 \le j < i \le n_G$: $\omega_j = \omega'_j$ and $\omega_i \prec \omega'_i$,

(b) $\forall j$: $\omega_j = \omega'_j$ and
$\max_{\ell=1,\ldots,n_G} \operatorname{HT}(\lambda_\ell p_{\sigma(\ell)}) < \max_{\ell'=1,\ldots,n_G} \operatorname{HT}(\lambda'_{\ell'} p_{\sigma'(\ell')})$,

(c) $\forall j$: $\omega_j = \omega'_j$,
$\max_{\ell=1,\ldots,n_G} \operatorname{HT}(\lambda_\ell p_{\sigma(\ell)}) = \max_{\ell'=1,\ldots,n_G} \operatorname{HT}(\lambda'_{\ell'} p_{\sigma'(\ell')}) =: t$
and $\#\{\ell \mid \operatorname{HT}(\lambda_\ell p_{\sigma(\ell)}) = t\} < \#\{\ell' \mid \operatorname{HT}(\lambda_{\ell'} p_{\sigma(\ell')}) = t\}$.

Lemma 3.5. *The ordering $\lessdot$ is well-founded.*

Proof. See [3], Lemma 3.17. $\square$

Lemma 3.6. *Let $f \in I = \langle g_1, \ldots, g_{n_G} \rangle$. Let (λ, σ) be a minimal labeled representation for f w.r.t. G. Then for all indices $v \in \{1, \ldots, m\}$:*

$$\#\{k \mid (\lambda_k, \sigma(k)) \in (\lambda, \sigma), \lambda_k \neq 0, \mathit{index}(r_{\sigma(k)}) = v\} \leq 1.$$

Proof. We can assume σ to be the identity by renumbering G, $f = \sum_{i=1}^{m} \lambda_i g_i$. Choose $v \in \{1, \ldots, m\}$ arbitrarily. Denote

$$\begin{aligned} I &= \{k \mid (\lambda_k, \mathrm{id}(k)) \in (\lambda, \mathrm{id}), \mathrm{index}(r_k) = v\}, \\ I_< &= \{k \mid (\lambda_k, \mathrm{id}(k)) \in (\lambda, \mathrm{id}), \mathrm{index}(r_k) < v\} \text{ and} \\ I_> &= \{k \mid (\lambda_k, \mathrm{id}(k)) \in (\lambda, \mathrm{id}), \mathrm{index}(r_k) > v\}. \end{aligned}$$

Assume that $\#I > 1$.
Each $r_k \in G$ is admissible w.r.t. F, i.e. $g_k = \sum_{j=v}^{m} \eta_{k,j} f_j$ with $\eta_{k,j} \in \mathbb{K}[\underline{x}]$.
Thus we get a new representation of f:

$$\begin{aligned} f &= \sum_{i=1}^{m} \lambda_i g_i = \sum_{i \in I} \lambda_i g_i + \sum_{j \notin I} \lambda_j g_j \\ &= \sum_{i \in I_<} \lambda_i g_i + \left(\sum_{j \in I} \lambda_j \eta_{j,v} \right) f_v + \sum_{j \in I} \lambda_j \sum_{k=v+1}^{m} \eta_{j,k} f_k + \sum_{\ell \in I_>} \lambda_\ell g_\ell \end{aligned}$$

This new labeled representation $(\lambda', \sigma') \prec_{\mathrm{lex}} (\lambda, \mathrm{id})$: The first $\#I_<$ components remained unchanged, then there is one component $\lambda'_v f_v$ where $\lambda'_v = \sum_{j \in I} \lambda_j \eta_{j,v}$. By construction

$$\begin{aligned} &\mathcal{S}(\mathrm{HT}(\lambda'_v) r_{\sigma'(v)}) = \\ &= \max\{\mathcal{S}(\mathrm{HT}(\lambda_k) r_k) \mid (\lambda_k, \mathrm{id}(k)) \in (\lambda, \mathrm{id}), \mathrm{index}(r_k) = v\}, \end{aligned}$$

where $\mathrm{poly}(r_{\sigma'(v)}) = f_v$. So the signatures of the first $\#I_< + 1$ components of both labeled representations are equal. But the $\#I_< + 2$th component of (λ, id) has index v, as we assumed that there are at least two such components, whereas the $\#I_< + 2$th component of (λ', σ') has an index $< v$.

Thus we received a contradiction of the minimality of (λ, id) w.r.t. $\lessdot$. $\square$

Remark 3.7. Note that a labeled representation w.r.t. G does not restrict the number of possible representations of an element $f \in I$. A labeled representation w.r.t. G just orders the components of the corresponding representation of f so that representations can be compared w.r.t. $\lessdot$.

Definition 3.8. Let $t \in \mathcal{T}$, (λ, σ) be a labeled representation w.r.t. G of a labeled polynomial r. W.l.o.g. we can assume $\sigma = \mathrm{id}$. Then (λ, id) is called a *t-representation of r* if

$$p = \sum_{\ell=1}^{n_G} \lambda_\ell p_\ell$$

such that for all components $\mathrm{HT}(\lambda_\ell p_\ell) \leq t$ and $\mathcal{S}(\mathrm{HT}(\lambda_\ell) r_\ell) \preceq \mathcal{S}(r)$.

Theorem 3.9. *If for all pairs (r_i, r_j) normalized w.r.t. G Spol(r_i, r_j) has a t-representation where $t < lcm\big(HT(p_i), HT(p_j)\big)$ then poly(G) is a Gröbner basis of $I = \langle p_1, \ldots, p_n \rangle$.*

Proof. Let $f \in I$. Then f has a labeled representation (λ, σ) w.r.t. G. W.l.o.g. we can assume $\sigma = \mathrm{id}$ such that $f = \sum_{\ell=1}^{n_G} \lambda_\ell p_\ell$. By Lemma 3.5 let us assume (λ, id) to be a minimal labeled representation of f w.r.t. G.

If there is a component $(\lambda_k, \mathrm{id}(k)) \in (\lambda, \mathrm{id})$ such that $\lambda_k r_k$ is not normalized w.r.t. G then there exists a principal syzygy $\mathbf{s}$ by Lemma 3.2. $\lambda_k r_k$ is admissible, i.e. there exists $\mathbf{g} \in \mathbb{K}[\underline{x}]^m$ such that $\mathrm{MHT}(\mathbf{g}) = \mathcal{S}(\mathrm{HT}(\lambda_k) r_k)$ and $v_F(\mathbf{g}) = \lambda_k p_k$. So we can construct $\mathbf{g} - \mathbf{s}$ with $\mathrm{MHT}(\mathbf{g} - \mathbf{s}) \prec \mathrm{MHT}(\mathbf{g})$ and $\lambda_k r_k$ admissible to $\mathbf{g} - \mathbf{s}$. This gives a labeled representation (λ', σ') of f w.r.t. G such that $(\lambda', \sigma') \lessdot (\lambda, \mathrm{id})$. This contradicts the minimality of (λ, id) w.r.t. $\lessdot$, so every $\lambda_k r_k$ such that $(\lambda_k, \mathrm{id}(k)) \in (\lambda, \mathrm{id})$ is normalized w.r.t. G.

By Lemma 3.6 there are no two components with the same index in (λ, id), i.e. all $\lambda_k r_k$ have different signatures.

Assume that there exist components $(\lambda_k, \mathrm{id}(k))$ such that $\mathrm{HT}(\lambda_k p_k) = t'$ where $t' \geq \mathrm{HT}(f)$. Note that $\#\{\ell \mid \mathrm{HT}(\lambda_\ell p_\ell) = t'\} \geq 2$. Choose two such components $(\lambda_i, \mathrm{id}(i))$, $(\lambda_j, \mathrm{id}(j))$.

Let $\tau = \mathrm{lcm}\big(\mathrm{HT}(p_i), \mathrm{HT}(p_j)\big)$, $\tau_i = \frac{\tau}{\mathrm{HT}(p_i)}$, and $\tau_j = \frac{\tau}{\mathrm{HT}(p_j)}$. Then $\tau \mid t'$, $\tau_i \mid \mathrm{HT}(\lambda_i)$, and $\tau_j \mid \mathrm{HT}(\lambda_j)$.

Define $m_i = \mathrm{HM}(\lambda_i)$ and $m_j = \frac{\mathrm{HC}(\lambda_i)}{\mathrm{HC}(\lambda_j)}\mathrm{HM}(\lambda_j)$. Now we compute

$$\begin{aligned}
m_i p_i - m_j p_j &= \mathrm{HC}(\lambda_i)\mathrm{HT}(\lambda_i)p_i - \mathrm{HC}(\lambda_i)\mathrm{HT}(\lambda_j)p_j \\
&= \mathrm{HC}(\lambda_i)\left(\frac{\tau_i t'}{\tau}p_i - \frac{\tau_j t'}{\tau}p_j\right) \\
&= \mathrm{HC}(\lambda_i)\frac{t'}{\tau}\mathrm{Spol}(p_i, p_j).
\end{aligned}$$

Since $\lambda_i r_i$ and $\lambda_j r_j$ are normalized w.r.t. G it follows with Lemma 3.3 that also $\tau_i r_i$ and $\tau_j r_j$ are normalized w.r.t. G.

Thus we get a new labeled representation (λ'', σ'') of f w.r.t. G:

$$\begin{aligned}
f &= \sum_{\ell=1}^{n_G} \lambda_\ell p_\ell = \lambda_i p_i + \lambda_j p_j + \sum_{\substack{\ell=1 \\ \ell \neq i,j}}^{n_G} \lambda_\ell p_\ell \\
&= m_i p_i + \big(\lambda_i - \mathrm{HT}(\lambda_i)\big)p_i - m_j p_j - \frac{\mathrm{HC}(\lambda_i)}{\mathrm{HC}(\lambda_j)}\big(\lambda_j - \mathrm{HT}(\lambda_j)\big)p_j \\
&\quad + \left(1 + \frac{\mathrm{HC}(\lambda_i)}{\mathrm{HC}(\lambda_j)}\right)\lambda_j p_j + \sum_{\substack{\ell=1 \\ \ell \neq i,j}}^{n_G} \lambda_\ell p_\ell.
\end{aligned}$$

As $\mathrm{Spol}(r_i, r_j)$ has a t-representation $\mathrm{Spol}(p_i, p_j) = \sum_{\ell=1}^{n_G} \eta_\ell p_\ell$ such that

$$\mathrm{HT}(\eta_\ell p_\ell) < \mathrm{HT}(\mathrm{lcm}(\mathrm{HT}(p_i), \mathrm{HT}(p_j))) \quad \text{and}$$
$$\mathcal{S}(\mathrm{HT}(\eta_\ell) r_\ell) \preceq \mathcal{S}(\mathrm{Spol}(r_i, r_j)).$$

It follows that $(\lambda'', \sigma'') \lessdot (\lambda, \mathrm{id})$. This contradicts the minimality of (λ, id). □

Acknowledgement. I would like to thank John Perry for many useful discussions.

References

[1] T.Becker, V.Weispfennig, and H.Kredel. *Gröbner Bases.* Springer Verlag, 1993.

[2] J.C. Faugère. *A new efficient algorithm for computing Gröbner bases without reduction to zero(F5).* Symbolic and Algebraic Computation, Proc. Conferenz ISSAC 2002, pp. 75–83, 2002.

[3] Stegers, Till. *Faugère's F5 Algorithm Revisited.* Thesis for the degreee of Diplom-Mathematiker, 2005.

Christian Eder,

Received November 7, 2007

Fachbereich Mathematik, TU Kaiserslautern,
Postfach 3049, 67653
Kaiserslautern, Germany
E–mail: *ederc@rhrk.uni − kl.de*