On the Complexity of the Gröbner-Bases Algorithm over $K[x,y,z]$[1)]

Franz Winkler
Johannes Kepler Universität Linz, Austria

Abstract

In /Bu65/, /Bu70/, /Bu76/ B. Buchberger presented an algorithm which, given a basis for an ideal in $K[x_1,...,x_n]$ (the ring of polynomials in n indeterminates over the field K), constructs a so-called Gröbner-basis for the ideal. The importance of Gröbner-bases for effectively carrying out a large number of construction and decision problems in polynomial ideal theory has been investigated in /Bu65/, /Wi78/, /WB81/, /Bu83b/. For the case of two variables B. Buchberger /Bu79/, /Bu83a/ gave bounds for the degrees of the polynomials which are generated by the Gröbner-bases algorithm. However, no bound has been known until now for the case of more than two variables. In this paper we give such a bound for the case of three variables.

1. Introduction

In /Bu65/, /Bu70/, /Bu76/ B. Buchberger presented an algorithm which, given a basis F for an ideal in $K[x_1,...,x_n]$ (the ring of polynomials in n indeterminates over the field K), constructs a so-called Gröbner-basis G for ideal(F), the ideal generated by F. A Gröbner-basis G can be characterized by the fact that every polynomial has a unique normal form w.r.t. a certain reduction relation induced by G. A large number of construction and decision problems in polynomial ideal theory can be solved easily once a Gröbner-basis for the ideal has been constructed (see /Bu65/, /Wi78/, /WB81/, /Bu83b/).

However, for a long time no bound was known for the complexity of the Gröbner-bases algorithm, especially for the degrees of the polynomials which are constructed by the Gröbner-bases algorithm. In 1979 B. Buchberger /Bu79/ gave such a bound, which was improved in /Bu83a/, for the case of two variables.

1) The work for this paper was supported by the Austrian Research Fund under grant Nr. 4567.

Lazard /La83/ makes some remarks on this problem but he considers a special class of ideals. In this paper we give a bound for the case of three variables, where absolutely no special properties are required of the ideal.

The problem to be solved is the following:

(P) given a basis F for a polynomial ideal in $K[x,y,z]$ construct a bound b such that the degree of every polynomial which is constructed during the execution of the Gröbner-bases algorithm on F is less than or equal to b.

(P) is solved in the subsequent chapters. Expressed only in D and d, the maximal and minimal degree of the polynomials in F, respectively, we get the bound $(8D + 1)\cdot 2^d$. For proofs of the various lemmata we refer to /Wi83/.

2. Reduction of the problem

Throughout this paper, we let the linear ordering $<_t$ on the set of power products be the graduated lexicographical ordering, i.e. power products are ordered according to their degrees and lexicographically within the same degree.

By the "overlap lemma" /KB78/, /Bu79/, /BW79/ it suffices to consider only "essential" pairs of polynomials during the execution of the Gröbner-bases algorithm, where a pair f,g in F is essential if there is no sequence $f=h_1,\dots,h_l=g$ in F such that

$lpp(h_i)$ divides $lcm(lpp(f),lpp(g))$ for all $1<i<l$,

$deg(lcm(lpp(h_i),lpp(h_{i+1}))) < deg(lcm(lpp(f),lpp(g)))$ for all $1\leq i\leq l-1$,

where lpp(f) denotes the leading power product of f w.r.t. $<_t$ and lcm(p,q) the least common multiple of the power products p,q. So every polynomial h which is added to the basis during the execution of the Gröbner-bases algorithm satisfies the following two conditions:

(i) lpp(h) is not a multiple of lpp(f) for every f, which is already in the basis,

(ii) deg(h) is not greater than the maximal degree of the least common multiples of essential pairs of polynomials in the basis.

We call a sequence of polynomials $h_1,\dots,h_s$ admissible w.r.t. F if h_i satisfies these two conditions w.r.t. $F\cup\{h_1,\dots,h_{i-1}\}$ for all i. Then it is clear that the following theorem holds.

Theorem 2.1: Let F be a finite set of polynomials in $K[x_1,\dots,x_n]$. Then every polynomial which is either in F or is generated during the execution of the Gröbner-bases algorithm on F has degree less than or equal to $\max\{\max\{\deg(h) \mid h\in H\} \mid H=F\cup\{h_1,\dots,h_s\},\ h_1,\dots,h_s \text{ admissible w.r.t. } F\}$.

So if we have a bound for the maximal degree of the polynomials in $F\cup\{h_1,\dots,h_s\}$, where $h_1,\dots,h_s$ are admissible w.r.t. F, then we have solved problem (P). Such a bound is constructed in the next chapter. Actually the notion of "admissibility" depends only on the leading power products of the involved polynomials. So instead of sets of polynomials F we consider sets of power products P.

3. A bound for admissible sequences of power products

Let $V:=\{x,y,z\}$ denote the set of variables or indeterminates.
By pp3 we denote the set of power products in x,y and z.
If $p=x^a y^b z^c$ is a power product then $\deg(p,x)=a$, $\deg(p,y)=b$, $\deg(p,z)=c$ and $\deg(p)=a+b+c$.
By $\mathrm{lcm}(p,q)$ we denote the least common multiple of the two power products p,q.
We write $p\preceq q$ for "p divides q".
If $P\subseteq pp3$, $v\in V$ and $d\in\mathbb{N}$ then $P^* := \{q \in pp3 \mid p\preceq q \text{ for some } p \in P\}$,
$\mathrm{mind}(P,v) := \min\{\deg(p,v) \mid p \in P\}$, and $\mathrm{sect}(P,d) := \{p \in P \mid \deg(p)=d\}$.

Def.: Let $d\in\mathbb{N}$, P a nonempty subset of sect(pp3,d). Then
$\mathrm{int}(P) := \{p \in \mathrm{sect}(pp3,d) \mid \deg(p,v)\geq \mathrm{mind}(P,v) \text{ for all } v\in V\} - P$.
$\mathrm{ext}(P) := \mathrm{sect}(pp3,d) - (P\cup \mathrm{int}(P))$.

An important notion in /Bu83a/ is the "essentiality" of pairs of polynomials in some basis F. Since this notion depends only on the leading power products of the polynomials in F, we can define it for sets of power products.

Def.: Let P be a finite subset of pp3. Then
$\mathrm{ess}(P) := \{(p,q) \mid p,q\in P,\ p\neq q$, and there are no $r_1,\dots,r_l$ in P such that
$p=r_1,\ r_l=q,$
$r_i \preceq \mathrm{lcm}(p,q)$ for all $1\leq i\leq l$, and
$\deg(\mathrm{lcm}(r_i,r_{i+1})) < \deg(\mathrm{lcm}(p,q))$ for all $1\leq i\leq l-1\}$.

(Essential pairs in P.)

Def.: Let P be a finite subset of pp3. Then the maximal degree of essential least common multiples of P is defined as
$mdel(P) := max\{deg(lcm(p,q)) \mid (p,q) \in ess(P)\}$.

Example 3.1: Let $P = \{x^2yz^6, x^3y^2z^5, xy^3z^5, x^4y^2z^3, xy^5z^3, x^4y^4z, x^3y^5z\}$.
$ess(P) = \{(p_1,p_2),(p_1,p_3),(p_2,p_3),(p_2,p_4),(p_3,p_5),(p_4,p_6),(p_5,p_7),(p_6,p_7)\}$.
For instance (p_1,p_6) is not in ess(P), since $r_1=p_1$, $r_2=p_2$, $r_3=p_4$, $r_4=p_6$ satisfy the condition in the definition of "ess".
So $mdel(P)=11$.

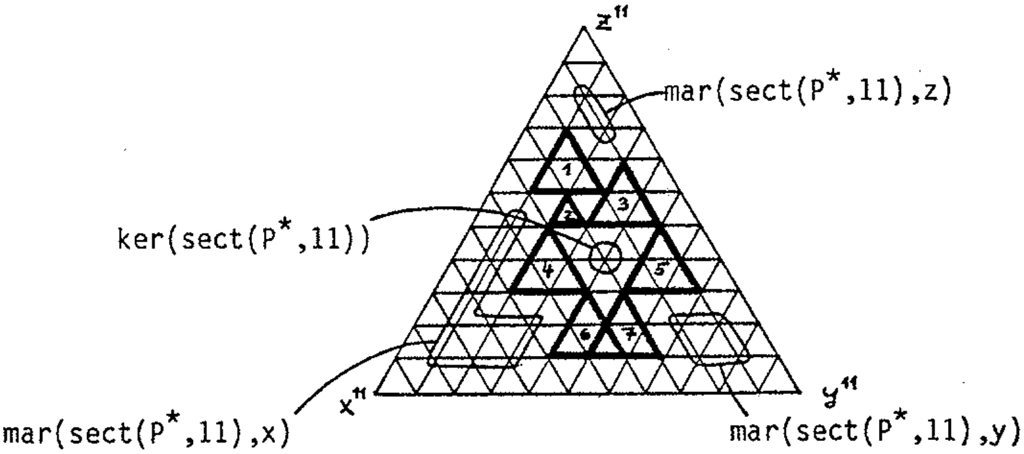
Def.: Let $P \subseteq pp3$. Then the width of P is defined as
$w(P) := \sum_{v \in V} mind(P,v)$.

Lemma 3.1: Let P be a finite subset of pp3, $m \geq mdel(P)$, $p \in int(sect(P^*,m))$, $v \in V$.
If $p.v^k \notin P^*$ for all $k \in \mathbb{N}$,
then for all $w \in V-\{v\}$ there is a $k \in \mathbb{N}$ such that $p.w^k \in P^*$.

So $int(sect(P^*,m))$ $(m \geq mdel(P))$ can be decomposed into the following four parts.

Def.: Let P be a finite subset of pp3, $m \geq mdel(P)$.
$ker(sect(P^*,m)) := \{p \mid p \in int(sect(P^*,m))$ and for all $v \in V$ there is a $k \in \mathbb{N}$ such that $p.v^k \in P^*\}$.
(Kernel of $sect(P^*,m)$.)
For $v \in V$:
$mar(sect(P^*,m),v) := \{p \mid p \in int(sect(P^*,m))$ and for all $k \in \mathbb{N}$ $p.v^k \notin P^*\}$.
(Margin of $sect(P^*,m)$ at v.)

Example 3.2:
Let P be as in example 3.1,
m=11 ($\geq mdel(P)$).



The triangles symbolize the multiples of the indicated power products.

Corollary to lemma 3.1: Let P be a finite subset of pp3, m≥mdel(P).
Then
int(sect(P^*,m)) is the disjunct union of ker(sect(P^*,m)), mar(sect(P^*,m),x), mar(sect(P^*,m),y) and mar(sect(P^*,m),z).

In order to investigate the increase of "mdel" if an "admissible" power product p is added to the set of power products P, we need some means of measuring the "distance" between p and P. The goal, of course, is to specify this "distance" dist(p,P) in such a way that mdel(P ∪ {p}) can easily be expressed in terms of mdel(P) and dist(p,P).

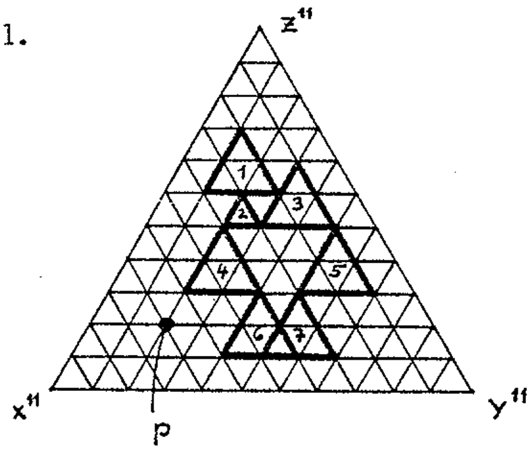
Def.: Let P ⊆ pp3, p ε pp3.
dist(p,P) := max{deg(r) | p.r ε P^* and p.s ∉ P^* for all s<r}.
(Distance between p and P.)

Lemma 3.2: Let P be a finite subset of pp3, p ε sect(pp3-P^*,mdel(P)).
Then mdel(P ∪ {p}) = mdel(P) + dist(p,P).

Example 3.3: Let P be as in example 3.1.

Suppose p = p_8 = $x^7y^2z^2$ is added to P.

dist(p,P)=2



The new essential pairs are (4,8) and (6,8).
So mdel(P ∪ {p}) = 13 = mdel(P) + dist(p,P).

During the execution of the Gröbner-bases algorithm it is well possible that a polynomial h is added to the basis F such that, for p=lpp(h), deg(p) < mdel({q ε pp3 | there is a polynomial f ε F with lpp(f)=q}. Lemma 3.2 can be extended to deal also with this case.

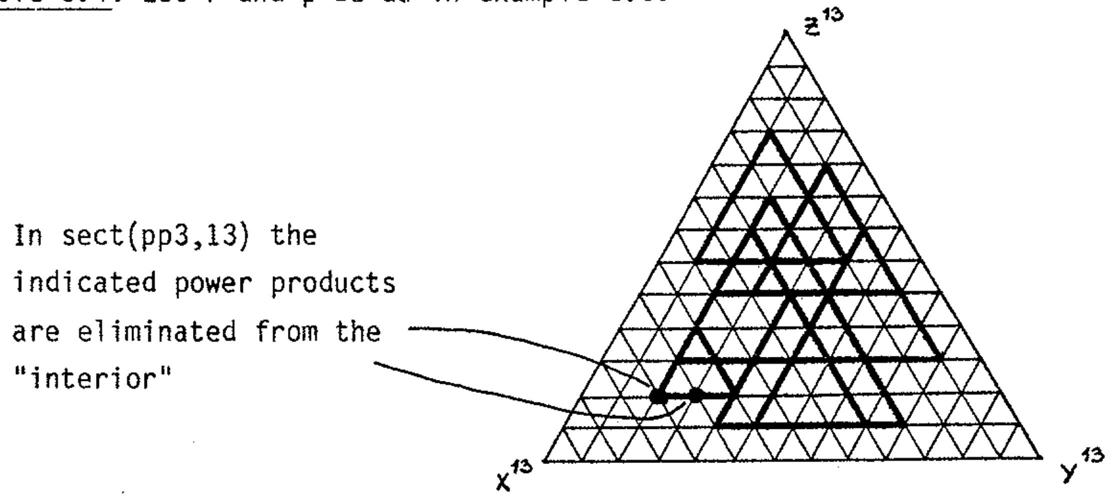
Lemma 3.3: Let P be a finite subset of pp3, p ε pp3, deg(p)<mdel(P).
Then mdel(P ∪ {p}) ≤ mdel(P) + max{dist(p',P) | p<p' and deg(p')=mdel(P)}.

While "mdel" increases if a new power product p is added to P, one notices a decrease of the "interior" and (or) the "width" of P. This phenomenon is investigated in detail in the next few lemmata.

Lemma 3.4: Let P be a finite subset of pp3, $p \in \mathrm{int}(\mathrm{sect}(P^*,\mathrm{mdel}(P)))$.
Then

$$|\mathrm{int}(\mathrm{sect}((P \cup \{p\})^*,\mathrm{mdel}(P)+\mathrm{dist}(p,P)))| < |\mathrm{int}(\mathrm{sect}(P^*,\mathrm{mdel}(P)))| - \mathrm{dist}(p,P).$$

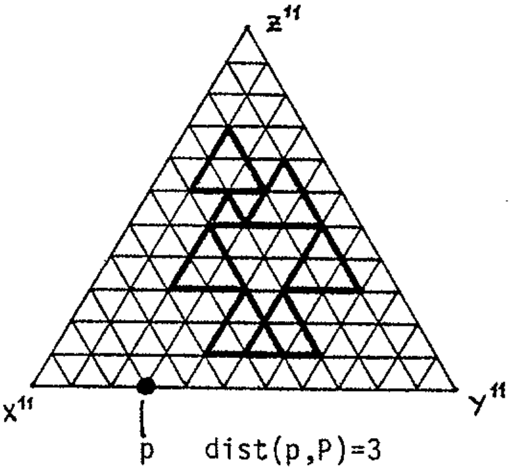
Example 3.4: Let P and p be as in example 3.3.

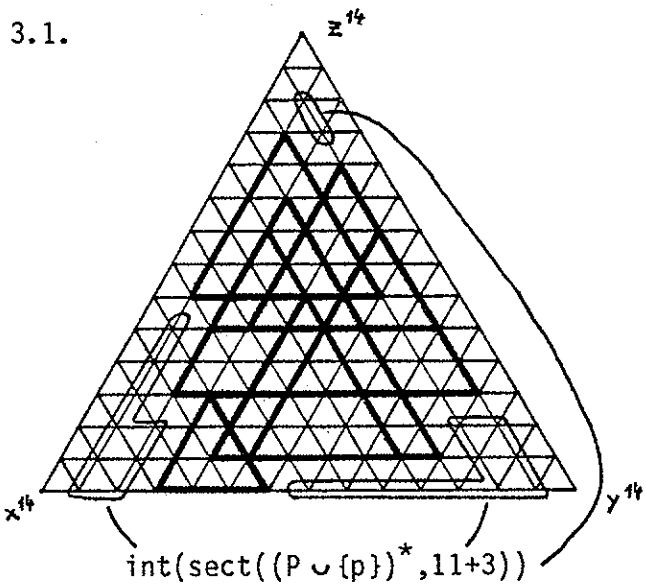


Lemma 3.5: Let P be a finite subset of pp3, $p \in \mathrm{ext}(\mathrm{sect}(P^*,\mathrm{mdel}(P)))$,
$t = w(P) - w(P \cup \{p\})$.
Then

$$|\mathrm{int}(\mathrm{sect}((P \cup \{p\})^*,\mathrm{mdel}(P)+\mathrm{dist}(p,P)))| <$$
$$|\mathrm{int}(\mathrm{sect}(P^*,\mathrm{mdel}(P)))| + t.\mathrm{mdel}(P) - (\mathrm{dist}(p,P)-t).$$

Example 3.5: Let P be as in example 3.1.





Now we are ready for constructing a bound for the degrees in "admissible" sequences of power products w.r.t. some starting set P. We achieve this bound in two steps. First we construct a bound for such "admissible" sequences, where every element of the sequence has degree as high as possible. In a second step we prove that this bound holds for arbitrary "admissible" sequences.

Def.: Let P be a finite subset of pp3. Then

a sequence $(p_1,\dots,p_s)$ in pp3 is called maximal w.r.t. P

$:\Longleftrightarrow$ for all $1 \leq i \leq s$:

$$\deg(p_i) = \mathrm{mdel}(P \;\; \{p_1,\dots,p_{i-1}\}) \text{ and}$$
$$p_i \in (P \cup \{p_1,\dots,p_{i-1}\})^*.$$

Lemma 3.6: Let P be a finite subset of pp3, $(p_1,\dots,p_s)$ maximal w.r.t. P,

$t = w(P) - w(P \cup \{p_1,\dots,p_s\})$,

$k = | \mathrm{int}(\mathrm{sect}((P \cup \{p_1,\dots,p_s\})^*, \mathrm{mdel}(P \cup \{p_1,\dots,p_s\}))) |$.

Then

$$\mathrm{mdel}(P \cup \{p_1,\dots,p_s\}) \leq (\dots(((\mathrm{mdel}(P) + | \mathrm{int}(\mathrm{sect}(P^*,\mathrm{mdel}(P))) |)\underbrace{\cdot 2+1)\cdot 2+1)\cdot \;\dots)\cdot 2+1}_{t \text{ times}} - k.$$

Proof: By induction on t.

If t=0 then by lemma 3.4

$$\mathrm{mdel}(P \cup \{p_1,\dots,p_s\}) \leq \mathrm{mdel}(P) + | \mathrm{int}(\mathrm{sect}(P^*,\mathrm{mdel}(P))) | - k.$$

Now let $t > 0$.

We choose s' such that

$w(P \cup \{p_1,\dots,p_{s'-1}\}) = w(P) - t' > w(P) - t$ and

$w(P \cup \{p_1,\dots,p_{s'}\}) = w(P) - t$.

Let

$k' := | \mathrm{int}(\mathrm{sect}((P \cup \{p_1,\dots,p_{s'-1}\})^*, \mathrm{mdel}(P \cup \{p_1,\dots,p_{s'-1}\}))) |$.

Then by induction hypothesis

$$\mathrm{mdel}(P \cup \{p_1,\dots,p_{s'-1}\}) \leq \underbrace{(\dots(((\mathrm{mdel}(P) + | \mathrm{int}(\mathrm{sect}(P^*,\mathrm{mdel}(P))) |)\underbrace{\cdot 2+1)\cdot 2+1)\cdot \;\dots)\cdot 2+1}_{t' \text{ times}}}_{:= c} - k'.$$

So

$$\mathrm{mdel}(P \cup \{p_1,\dots,p_{s'}\}) \leq c - k' + \underbrace{\mathrm{dist}(p_{s'}, P \cup \{p_1,\dots,p_{s'-1}\})}_{:= d}.$$

By lemma 3.5

$I := | \mathrm{int}(\mathrm{sect}((P \cup \{p_1,\dots,p_{s'}\})^*, \mathrm{mdel}(P \cup \{p_1,\dots,p_{s'}\}))) | \leq$

$\quad k' + (t-t').\mathrm{mdel}(P \cup \{p_1,\dots,p_{s'-1}\}) - (d - (t-t'))$.

Now we get from lemma 3.4

$\mathrm{mdel}(P \cup \{p_1,\dots,p_s\}) \leq c - k' + d + (I - k) \leq$

$c - k' + d + k' + (t-t').\underbrace{\mathrm{mdel}(P \cup \{p_1,\dots,p_{s'-1}\})}_{\leq c} - d + (t-t') - k \leq$

$(\dots((c\cdot \underbrace{2 + 1)\cdot 2 + 1)\cdot \dots)\cdot 2 + 1}_{(t-t')\text{ times}} - k \leq$

$(\dots(((\mathrm{mdel}(P) + | \mathrm{int}(\mathrm{sect}(P^*,\mathrm{mdel}(P))) |)\cdot \underbrace{2 + 1)\cdot 2 + 1)\cdot \dots)\cdot 2 + 1}_{t\text{ times}} - k.$ ●

Def: Let P be a finite subset of pp3.

$b(P) := \max\{\mathrm{mdel}(P \cup \{p_1,\dots,p_s\}) \mid (p_1,\dots,p_s) \text{ maximal w.r.t. } P\}$.

(Bound for P.)

Theorem 3.1: Let P be a finite subset of pp3.

Then

$b(P) \leq (\dots(((\mathrm{mdel}(P) + | \mathrm{int}(\mathrm{sect}(P^*,\mathrm{mdel}(P))) |)\cdot \underbrace{2 + 1)\cdot 2 + 1)\cdot \dots)\cdot 2 + 1}_{w(P)\text{ times}}.$

Proof: The assertion follows from lemma 3.6 if we set $t=w(P)$ and $k=0$. ●

Corollary to theorem 3.1: Let P be a finite subset of pp3.

Then

$$b(P) \leq (\mathrm{mdel}(P) + | \mathrm{int}(\mathrm{sect}(P^*,\mathrm{mdel}(P))) | + 1)\cdot 2^{w(P)}.$$

Theorem 3.1 gives a bound for the degrees of the power products in a sequence $(p_1,\dots,p_t)$ which is maximal w.r.t. P. But during the execution of the Gröbner-bases algorithm this maximality usually does not hold. So what remains to be done is to show that b(P) is an upper bound for $\mathrm{mdel}(P \cup \{q_1,\dots,q_s\})$, where the sequence $(q_1,\dots,q_s)$ is admissible w.r.t. P.

Lemma 3.7: Let $P,Q \subseteq$ pp3, $P^* \subseteq Q^*$, $\mathrm{mdel}(P) > \mathrm{mdel}(Q)$, $q \in \mathrm{sect}(pp3,\mathrm{mdel}(Q))$.
Then there is a $p \in \mathrm{sect}(pp3,\mathrm{mdel}(P))$ such that

$\quad$(*) $q \leq p$ and $\mathrm{dist}(q,Q) + \mathrm{mdel}(Q) \leq \mathrm{dist}(p,P) + \mathrm{mdel}(P)$.

Theorem 3.2: Let P be a finite subset of pp3, $q_1,\dots,q_s \in$ pp3 such that $\deg(q_i) \leq \mathrm{mdel}(P \cup \{q_1,\dots,q_{i-1}\})$ for all $1 \leq i \leq s$.
Then there is a maximal sequence $(p_1,\dots,p_t)$ w.r.t. P such that

$\mathrm{mdel}(P \cup \{q_1,\dots,q_s\}) \leq \mathrm{mdel}(P \cup \{p_1,\dots,p_t\})$ and

$(P \cup \{p_1,\dots,p_t\})^* \subseteq (P \cup \{q_1,\dots,q_s\})^*$.

Proof: By induction on s.

s=1: If $\mathrm{mdel}(P \cup \{q_1\}) \leq \mathrm{mdel}(P)$ then the assertion holds with t=0.

If $\mathrm{mdel}(P \cup \{q_1\}) > \mathrm{mdel}(P)$ then by lemma 3.3 there is a p_1 such that

$\deg(p_1)=\mathrm{mdel}(P)$, $q_1 \leq p_1$, $p_1 \notin P^*$ and

$\mathrm{mdel}(P \cup \{q_1\}) \leq \mathrm{mdel}(P) + \mathrm{dist}(p_1,P) = \mathrm{mdel}(P \cup \{p_1\})$.

↑ lemma 3.2

Obviously $(P \cup \{p_1\})^* \subseteq (P \cup \{q_1\})^*$ holds.

s>1: By induction hypothesis there are $p_1,\dots,p_{t'}$ maximal w.r.t. P such that

$\mathrm{mdel}(P \cup \{q_1,\dots,q_{s-1}\}) \leq \mathrm{mdel}(P \cup \{p_1,\dots,p_{t'}\})$ and

$(P \cup \{p_1,\dots,p_{t'}\})^* \subseteq (P \cup \{q_1,\dots,q_{s-1}\})^*$.

By lemma 3.7 for every $q \in \mathrm{sect}(\mathrm{pp3},\mathrm{mdel}(P \cup \{q_1,\dots,q_{s-1}\}))$ there is a $p \in \mathrm{sect}(\mathrm{pp3},\mathrm{mdel}(P \cup \{p_1,\dots,p_{t'}\}))$ such that

$q \leq p$ and

(*) $\mathrm{mdel}(P \cup \{q_1,\dots,q_{s-1}\}) + \mathrm{dist}(q,P \cup \{q_1,\dots,q_{s-1}\}) \leq \mathrm{mdel}(P \cup \{p_1,\dots,p_{t'}\}) + \mathrm{dist}(p,P \cup \{p_1,\dots,p_{t'}\})$.

So

$\mathrm{mdel}(P \cup \{q_1,\dots,q_s\}) \leq$
↑ lemma 3.3

$\mathrm{mdel}(P \cup \{q_1,\dots,q_{s-1}\}) + \max\{\mathrm{dist}(q',P \cup \{q_1,\dots,q_{s-1}\}) \mid q_s \leq q'$ and $\deg(q')=\mathrm{mdel}(P \cup \{q_1,\dots,q_{s-1}\})\} \leq$
↑ (*)

$\mathrm{mdel}(P \cup \{p_1,\dots,p_{t'}\}) + \max\{\mathrm{dist}(p',P \cup \{p_1,\dots,p_{t'}\}) \mid q_s \leq p'$ and $\deg(p')=\mathrm{mdel}(P \cup \{p_1,\dots,p_{t'}\})\}$.

If $\mathrm{sect}(\{q_s\}^*,\mathrm{mdel}(P \cup \{p_1,\dots,p_{t'}\})) \subseteq (P \cup \{p_1,\dots,p_{t'}\})^*$ then the assertion holds for t=t'.

If $A := \mathrm{sect}(\{q_s\}^*,\mathrm{mdel}(P \cup \{p_1,\dots,p_{t'}\})) - (P \cup \{p_1,\dots,p_{t'}\})^* \neq \emptyset$ then we choose $p_{t'+1}$ in A such that

$\mathrm{dist}(p_{t'+1},P \cup \{p_1,\dots,p_{t'}\}) = \max\{\mathrm{dist}(p',P \cup \{p_1,\dots,p_{t'}\}) \mid p' \in A\}$.

Then we have

$\text{mdel}(P \cup \{q_1,\dots,q_s\}) \leq \text{mdel}(P \cup \{p_1,\dots,p_{t'}\}) + \text{dist}(p_{t'+1}, P \cup \{p_1,\dots,p_{t'}\})$

$= \quad \text{mdel}(P \cup \{p_1,\dots,p_{t'},p_{t'+1}\})$

↑ lemma 3.2

and by the induction hypothesis

$(P \cup \{p_1,\dots,p_{t'},p_{t'+1}\}) \subseteq (P \cup \{q_1,\dots,q_s\})$. •

Corollary to theorem 3.2: Let P be a finite subset of pp3, $q_1,\dots,q_s$ such that $\deg(q_i) \leq \text{mdel}(P \cup \{q_1,\dots,q_{i-1}\})$ for all $1 \leq i \leq s$.
Then $\text{mdel}(P \cup \{q_1,\dots,q_s\}) \leq b(P)$.

Theorem 3.3: Let F be a finite set of polynomials in K[x,y,z],
$P = \{p \mid p = \text{lpp}(f) \text{ for some } f \in F\}$, $h_1,\dots,h_s$ admissible polynomials w.r.t. F.
Then

$$\max\{\deg(h) \mid h \in F \cup \{h_1,\dots,h_s\}\} \leq b(P).$$

Proof: The leading power products of $h_1,\dots,h_s$ satisfy the conditions of the corollary to theorem 3.2. So

$\max\{\deg(h) \mid h \in F \cup \{h_1,\dots,h_s\}\} \leq$

$\text{mdel}(P \cup \{\text{lpp}(h_1),\dots,\text{lpp}(h_s)\}) \leq$

↑ cor. to theorem 3.2

$b(P)$. •

4. Conclusion

Combining theorem 2.1 and the corollary to theorem 3.2 we get

Theorem 4.1: Let F be a finite set of polynomials in K[x,y,z],
$P = \{\text{lpp}(f) \mid f \in F\}$,
then every polynomial which is either in F or is generated during the execution of the Gröbner-bases algorithm on F has degree less than or equal to b(P).

From this bound for the degrees of the polynomials generated by the Gröbner-bases algorithm we can get one which only depends on the maximal and minimal degree of the given basis F. This bound is of course much coarser than the one given in the above theorems.

Corollary to theorem 4.1: Let F be a finite set of polynomials in K[x,y,z], $d = \min\{\deg(f) \mid f \in F\}$, $D = \max\{\deg(f) \mid f \in F\}$, then every polynomial which is either in F or is generated during the execution of the Gröbner-bases algorithm on F has degree less than or equal to

$$(8D + 1)\cdot 2^d.$$

Proof: $w(P) \leq d$, $\text{mdel}(P) \leq 2D$,

$$|\text{int}(\text{sect}(P^*,\text{mdel}(P)))| \leq |\text{sect}(pp3,2D)| = \binom{3 - 1 + 2D}{2D} =$$

$$= \frac{(2D+2). \ldots .3}{2D. \ldots .1} \leq 2D.3.$$

So by the corollary to theorem 3.1

$b(P) \leq$

$(\text{mdel}(P) + |\text{int}(\text{sect}(P^*,\text{mdel}(P)))| + 1)\cdot 2^{w(P)} \leq$

$(2D + 6D + 1)\cdot 2^d =$

$(8D + 1)\cdot 2^d$. ●

References

/Bu65/ B. Buchberger: Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal, Ph.D. Dissertation, Univ. Innsbruck, Austria, 1965.

/Bu70/ B. Buchberger: Ein algorithmisches Kriterium für die Lösbarkeit eines algebraischen Gleichungssystems, Aequ. Math., vol. 4/3, pp. 374-383, 1970.

/Bu76/ B. Buchberger: A Theoretical Basis for the Reduction of Polynomials to Canonical Forms, ACM SIGSAM Bull., vol. 39, pp. 19-29, 1976.

/Bu79/ B. Buchberger: A Criterion for Detecting Unnecessary Reductions in the Construction of Gröbner-Bases, Int. Symposium on Symbolic and Algebraic Manipulation, EUROSAM'79, Marseille, France, LNCS 72, Springer-Verlag, 1979.

/Bu83a/ B. Buchberger: A Note on the Complexity of Constructing Gröbner-Bases, EUROCAL'83, London, LNCS, Springer-Verlag, 1983.

/Bu83b/ B. Buchberger: Gröbner Bases: A Method in Symbolic Mathematics, V Intern. Conf. on Simulation, Programming and Mathematical Methods for Solving Physical Problems, Joint Inst. for Nuclear Research, Dubna, USSR, Sept. 20-23, 1983.

/BW79/ B. Buchberger, F. Winkler: Miscellaneous Results on the Construction of Gröbner-Bases for Polynomial Ideals, Techn. Rep. Nr. 137, Inst. für Math., Univ. Linz, Austria, 1979

/KB78/ C. Kollreider, B. Buchberger: An Improved Algorithmic Construction of Gröbner-Bases for Polynomial Ideals, Techn. Rep. Nr. 110, Inst. für Math., Univ. Linz, Austria, 1978.

/La83/ D. Lazard: Gröbner Bases, Gaussian Elimination and Resolution of Systems of Algebraic Equations, EUROCAL'83, London, LNCS, Springer-Verlag, 1983.

/Wi78/ F. Winkler: Implementierung eines Algorithmus zur Konstruktion von Gröbner-Basen, Diplomarbeit, Inst. für Math., Univ. Linz, Austria, 1978.

/Wi83/ F. Winkler: On the Complexity of the Gröbner-Bases Algorithm over K[x,y,z], Techn. Rep. Nr. CAMP 83-25.0, Inst. für Math., Univ. Linz, Austria, 1983.

/WB81/ F. Winkler, B. Buchberger, F. Lichtenberger, H. Rolletschek: An Algorithm for Constructing Canonical Bases (Groebner-Bases) of Polynomial Ideals, submitted for publication, 1981.