ACM SIGSAM Bulletin, Vol. 10, No. 4, Nov. 1976, pp. 19-24

SOME PROPERTIES OF GRÖBNER-BASES FOR POLYNOMIAL IDEALS

by

B. Buchberger
Universität Linz
A-4045 LINZ, Austria

Abstract

We give a uniqueness theorem for Gröbner-bases of polynomial ideals and show that it is effectively decidable whether a given basis is a (minimal normed) Gröbner-basis. Incidentally, we show how our methods may be applied to decide $\mathfrak{a} \leq \mathfrak{b}$ for given polynomial ideals $\mathfrak{a}$ and $\mathfrak{b}$.

Introduction

Resuming our former work on the reduction of polynomials, in [1], we introduced the notion of a Gröbner-basis for polynomial ideals and gave a characterization theorem for such bases which immediately leads to a solution of many computability and decidability results in the theory of polynomial ideals. Among them is the problem of effectively deciding $\mathfrak{a} \leq \mathfrak{b}$ for polynomial ideals $\mathfrak{a}$ and $\mathfrak{b}$. In our early papers on polynomial reduction we have not explicitly shown how this problem may be attacked by our methods. So we present a solution to this problem here (see section 2).

The main concern of the present paper is a uniqueness theorem for Gröbner-bases (see section 1) and two decidability results for such bases which solve the two "meta-problems" to decide whether a given basis is a Gröbner-basis and whether a given basis is a minimal normed Gröbner-basis (see section 3). We establish these results by proving some lemmas on Gröbner-bases which may be of independent interest. For instance, in 1.8 we show that two G-bases that generate the same ideal have the same set of M-terms. For a partial converse, see 3.1.

This paper immediately follows [1], where one can find all preparatory definitions, conventions on the use of variables and also references to the literature. A more tutorial presentation of the material given here is available from the author.

1. The uniqueness of minimal normed Gröbner-bases

1.1. Definition:

$$\mathrm{Delete}(F,i) := \begin{cases} (0), & \text{if } L(F)=1 \wedge i=1 \\ (F_1,\dots,F_{i-1},F_{i+1},\dots,F_{L(F)}), & \text{if } L(F)\geq 2 \wedge 1\leq i\leq L(F) \\ F, & \text{otherwise} \end{cases}$$

1.2. Example:

$F := (xy^2-x, 3x-2)$.
$G := \mathrm{Delete}(F,1) = (3x-2)$
$\mathrm{Delete}(G,1) = (0)$
$\mathrm{Delete}(F,2) = (xy^2-x)$.

1.3. Definition:

$$\mathrm{Normed}(F) :\longleftrightarrow F=(0) \vee (L(F)=1 \wedge \mathrm{Hcoef}(F_1)=1) \vee$$
$$\vee (L(F)>1 \wedge \bigwedge_{1\leq i\leq L(F)} (\mathrm{Hcoef}(F_i)=1 \wedge$$
$$\wedge \mathrm{Normalf}(F_i,\mathrm{Delete}(F,i))))$$

(F is normed).

1.4. Example:

$\mathrm{Normed}((0))$
$\mathrm{Normed}((x^2-x))$
$\neg \mathrm{Normed}((2x^2-x))$
$\mathrm{Normed}((x^2-x, xy+3))$
$\neg \mathrm{Normed}((x^2-x, x^2y+3))$
$\neg \mathrm{Normed}((x^2-x, y^3+3x^2))$.

1.5. Definition:

F is a minimal G-basis (for Ideal(F)) (abbreviated: Min-G-basis (F)) :$\longleftrightarrow$

$$L(F)=1 \vee$$
$$L(F)>1 \wedge \text{G-basis}(F) \wedge$$
$$\wedge \neg \bigvee_{1\leq i\leq L(F)} (\mathrm{Ideal}(\mathrm{Delete}(F,i)) =$$
$$= \mathrm{Ideal}(F) \wedge \text{G-basis}(\mathrm{Delete}(F,i)))$$

(deleting a polynomial in F destroys the property of being a G-basis for the same ideal).

Our goal is to proof the following theorem

1.6. Theorem:

Min-G-basis(F), Normed(F),
Min-G-basis(G), Normed(G),
Ideal(F) = Ideal(G) $\longrightarrow$

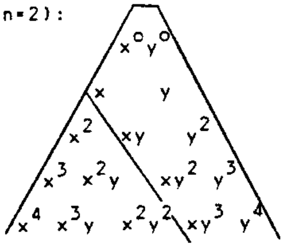
$$\bigvee_{\pi} (\pi : \{1,..,L(F)\} \xrightarrow[onto]{1-1} \{1,..,L(G)\} \wedge \bigwedge_{1 \leq i \leq L(F)} F_i = G_{\pi(i)})$$

(i.e. minimal normed Gröbner-bases for polynomial ideals are uniquely determined).

1.7. Sketch of the proof for Theorem 1.6.:

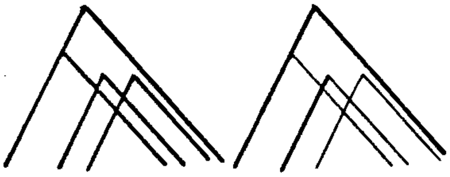
We establish the result of the theorem by proving a number of lemmas. For obtaining the intuitions necessary in the proofs the following graphical representation of the set of terms might be helpful: Arrange the terms of $K\langle\rangle_n$ in a schema like this

(example: n=2):



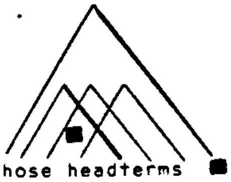
The multiples of some term t (for instance $t=x^2$) cover a region which intuitively may be conceived as the "shadow of t".
With this interpretation the lemmas may be visualized as follows:

ad Lemma 1.8.:



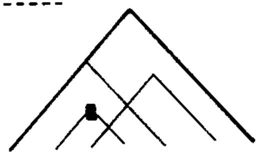
The M-terms of two G-bases of the same ideal cover the same region.

ad Lemma 1.10.:



Polynomials whose headterms ■ lie in the shadow of the headterms of other polynomials of the basis may be dropped from a G-basis. The basis obtained will still be a G-basis.

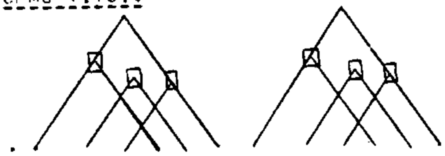
ad Lemma 1.14.:



No polynomial in a minimal G-basis may have a headterm ■ lying in the shadow of the headterm of other polynomials in the basis.

The Lemmas 1.8.,1.10.,1.12. and 1.14 lead to Lemma 1.16.

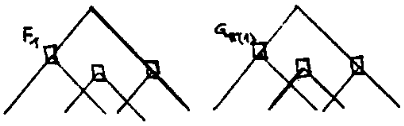
ad Lemma 1.16.:



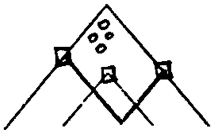
Two minimal G-basis of the same ideal have the same set of headterms.

From the graphical representation of the Lemmas 1.8. and 1.16. the proof of the theorem can easily be guessed:

Let two minimal normed G-basis be given for the same ideal. By Lemma 1.16. they will look like this:



Assume, for instance, $F_1 \neq G_{\pi(1)}$.
Then, by Lemma 1.8., the terms o that could occur in $g:=F_i-G_{\pi(i)} \in$ Ideal(F) would be distributed like this:



Such terms cannot exist because F and G are normed.

1.8. Lemma:

G-basis(F), G-basis(G),
Ideal(F) = Ideal(G) $\longrightarrow$

$$\bigwedge_{t} (\mathrm{Mterm}(t,F) \longleftrightarrow \mathrm{Mterm}(t,G)).$$

(i.e. G-basis for the same ideal have the same M-terms.)

1.9. Proof:

Assume
(1) Mterm(t,F) and
(2) $\neg$Mterm(t,G).
Then for somo s and $1 \leq i \leq L(F)$
(3) $t = s.\mathrm{Hterm}(F_i) \wedge F_i \neq 0$.

Now,
(4) $s.F_i \in \mathrm{Ideal}(F) = \mathrm{Ideal}(G)$

Construct g such that
(5) $s.F_i \underset{G}{>} \underset{\sim}{g}$

Because of (4) we have
(6) $g \in \mathrm{Ideal}(G)$

Because of $\mathrm{Hterm}(s.F_i)=t$ and (2) we have
(7) $g \neq 0$

Because of (5) we have
(8) $\mathrm{Normalf}(g,G)$

(6),(7),(8) contradict the fact that G is a G-basis.

1.10. Lemma:

$L(F) > 1,\ 1 \leq i \leq L(F),\ \text{G-basis}(F),\ \bigvee_{1 \leq j \leq L(F)} (j \neq i \wedge F_j \neq 0 \wedge \mathrm{Multiple}(\mathrm{Hterm}(F_i),\mathrm{Hterm}(F_j)))$

$\longrightarrow$

$\text{G-basis}(\mathrm{Delete}(F,i))$.

(i.e.: Deleting polynomials from a G-basis whose headterms are multiples of other polynomials in the basis does not affect the property of being a G-basis.)

1.11. Proof:

Assume for some g
(1) $g \in \mathrm{Ideal}(\mathrm{Delete}(F,i))$
(2) $g \neq 0$
(3) $\mathrm{Normalf}(g,\mathrm{Delete}(F,i))$

Then
(4) $g \in \mathrm{Ideal}(F)$
and
(5) $\mathrm{Normalf}(g,F)$
because assume
(6) $\mathrm{Occur}(t,g)$
(7) $F_k \neq 0 \wedge \mathrm{Multiple}(t,\mathrm{Hterm}(F_k))$ for some t and $1 \leq k \leq L(F)$

Case I: $k=i$

In this case because of the assumptions of the Lemma
(8) $\mathrm{Multiple}(t,\mathrm{Hterm}(F_j)) \wedge F_j \neq 0$ for some $j \neq i$.

(6) and (8) is a contradiction to (3).

Case II: $k \neq i$

In this case (6) and (7) are already a contradiction to (3).

Thus, (5) is established.

However, (2),(4) and (5) contradicts the fact that F is a G-basis. So we have to refuse assumptions (1)-(3).

1.12. Lemma:

$\text{Min-G-basis}(F) \longrightarrow$
$(L(F)=1 \wedge F_1=0) \vee \bigwedge_{1 \leq i \leq L(F)} F_i \neq 0.$

(i.e. in a non-zero minimal G-basis all F_i are non-zero.)

1.13. Proof:

Assume
(1) $(L(F) > 1 \vee F_1 \neq 0) \wedge \bigvee_{1 \leq i \leq L(F)} F_i = 0.$

Case I:
$L(F) > 1 \wedge \bigvee_{1 \leq i \leq L(F)} F_i = 0$

In this case consider
(2) $F' := \mathrm{Delete}(F,i)$.

Of course,
(3) $\mathrm{Ideal}(F') = \mathrm{Ideal}(F)$

in addition
(4) $\text{G-basis}(F')$
as is easily seen by using the fact that the definition of Mterm requires $F_i \neq 0$.

(3) and (4) contradict Min-G-basis(F).

Case II: $F_1 \neq 0 \wedge \bigvee_{1 \leq i \leq L(F)} F_i = 0$

In this case $L(F)=1$ is not possible.
If $L(F) > 1$ we have Case I again.

1.14. Lemma:

$\text{Min-G-basis}(F) \longrightarrow$
$\neg \bigvee_{1 \leq i,j \leq L(F)} (i \neq j \wedge \mathrm{Multiple}(\mathrm{Hterm}(F_i), ,\mathrm{Hterm}(F_j)))$

1.15. Proof:

Assume for some $1 \leq i,j \leq L(F)$ with $i \neq j$ and some s
(1) $\mathrm{Hterm}(F_i) = s.\mathrm{Hterm}(F_j)$

From Lemma 1.12. we know
(2) $F_j \neq 0$.

Case I: $F_i \in \mathrm{Ideal}(\mathrm{Delete}(F,i))$

In this case
(3) $\mathrm{Ideal}(F) = \mathrm{Ideal}(\mathrm{Delete}(F,i))$
and
(4) $\text{G-basis}(\mathrm{Delete}(F,i))$
because of Lemma 1.10.

(3) and (4) contradict to the premise Min-G-basis(F).

Case II: $F_i \notin \mathrm{Ideal}(\mathrm{Delete}(F,i))$

In this case construct a g such that

(5) $F_i \underset{\mathrm{Delete}(F,i)}{>} \underset{\sim}{g}$

Then,
(6) $g \neq 0$
because otherwise $F_i \in \mathrm{Ideal}(\mathrm{Delete}(F,i))$.

Further,
(7) $g \in \mathrm{Ideal}(F)$
because $F_i \in \mathrm{Ideal}(F)$ and $F_i \underset{F}{>} g$ (use (5)!).

Finally,
(8) $\mathrm{Normalf}(g,F)$ because
(9) $\mathrm{Occ}(t,g),\ F_k \neq 0,\ \mathrm{Multiple}(t,\mathrm{Hterm}(F_k))$

for $k \neq i$ is impossible by (5) and for $k=i$ is impossible by (5) and (1).
However (6),(7),(8) contradict to the premise that (F) is a G-basis.

So we obtained a contradiction in both cases, i.e. we have to refuse the assumption (1).

1.16. Lemma:

Min-G-basis(F),
Min-G-basis(G),
ideal(F) = ideal(G)

$$\longrightarrow$$

$$\bigvee_{\pi} (\pi: \{1,..,L(F)\} \xrightarrow[\text{onto}]{1-1} \{1,..,L(G)\} \wedge$$
$$\wedge \bigwedge_{1\le i\le L(F)} \text{Hterm}(F_i)=\text{Hterm}(G_{\pi(i)})).$$

(Two minimal G-bases of the same ideal have the same headterms.)

1.17. Proof:

By Lemma 1.12. we know that

(3) $(L(F)=1 \wedge F_1=0) \vee \bigwedge_{1\le i\le L(F)} F_i\ne 0$

(4) $(L(G)=1 \wedge G_1=0) \vee \bigwedge_{1\le j\le L(G)} G_j\ne 0$

So we have to consider four cases

Case I: $L(F)=1 \wedge F_1=0 \wedge L(G)=1 \wedge G_1=0$

In this case the conclusion of the Lemma is trivially true.

Case II: $L(F)=1 \wedge F_1=0 \wedge \bigwedge_{1\le j\le L(G)} G_j\ne 0$

This is not possible because in this case we would have $\text{ideal}(F)=\{0\}\ne\text{ideal}(G)$.

Case III: $(\bigwedge_{1\le i\le L(F)} F_i\ne 0) \wedge L(G)=1 \wedge G_1=0$

Not possible, as above.

Case IV: $\bigwedge_{1\le i\le L(F)} F_i\ne 0 \wedge \bigwedge_{1\le j\le L(G)} G_j\ne 0$

From Lemma 1.8. we have

(5) $\bigwedge_{t} (\text{Mterm}(t,F) \longleftrightarrow \text{Mterm}(t,G))$

(use the fact that Min-G-basis(F) implies G-basis(F): in the case L(F)=1 we always have G-basis(F) because of criterion (G2) in [1]).

In addition, by Lemma 1.14.

(6) $\neg \bigvee_{\substack{1\le i,j\le L(F)\\ i\ne j}} \text{Multiple}(\text{Hterm}(F_i), \text{Hterm}(F_j))$

and

(7) $\neg \bigvee_{\substack{1\le i,j\le L(G)\\ i\ne j}} \text{Multiple}(\text{Hterm}(G_i), \text{Hterm}(G_j))$

In particular, we have

(8) $\bigwedge_{\substack{1\le i,j\le L(F)\\ i\ne j}} \text{Hterm}(F_i) \ne \text{Hterm}(F_j)$

and

(9) $\bigwedge_{\substack{1\le i,j\le L(G)\\ i\ne j}} \text{Hterm}(G_i) \ne \text{Hterm}(G_j)$

Let $i_1,....,i_k$, $j_1,....,j_k$ be such that

(10) $\bigwedge_{1\le p,q\le k} (p\ne q \longrightarrow i_p\ne i_q \wedge j_p\ne j_q)$

(11) $\{\text{Hterm}(F_1),..,\text{Hterm}(F_{L(F)})\} \cap$
$\cap \{\text{Hterm}(G_1),..,\text{Hterm}(G_{L(G)})\} =$
$= \{\text{Hterm}(F_{i_1}),..,\text{Hterm}(F_{i_k})\} =$
$= \{\text{Hterm}(G_{j_1}),..,\text{Hterm}(G_{j_k})\}$,

(12) $\bigwedge_{1\le p\le k} \text{Hterm}(F_{i_p}) = \text{Hterm}(G_{j_p})$.

Define

(13) $\pi(i_1):=j_1,....,\pi(i_k):=j_k$.

If $\{1,..,L(F)\} = \{i_1,...,i_k\}$ and $\{1,..,L(G)\} = \{i_1,...,j_k\}$ then nothing is left to be proved. We show, that the assumption $\{1,..,L(F)\} \ne \{i_1,...,i_k\}$ leads to a contradiction. Similarly, we could prove the assumption $\{1,..,L(G)\} \ne \{j_1,...,i_k\}$ to be contradictory.

Of course, $\{i_1,...,i_k\} \subseteq \{1,..,L(F)\}$.

So let us assume that

(14) $\hat{i} \in \{1,..,L(F)\}$ but

(15) $\hat{i} \notin \{i_1,...,i_k\}$.

By (15) we have

(16) $\bigwedge_{1\le j\le L(G)} \text{Hterm}(F_{\hat{i}}) \ne \text{Hterm}(G_j)$

Since Mterm(Hterm($F_{\hat{i}}$),F), by (5), we obtain

(17) Mterm(Hterm($F_{\hat{i}}$),G)

i.e.

(18) $\text{Hterm}(F_{\hat{i}})=s.\text{Hterm}(G_{\hat{j}})$ for some $\hat{j} \in \{1,..,L(G)\}$ and some $s\ne x_1^0..x_n^0$.

($s=x_1^0..x_n^0$ would contradict (16)).

Since Mterm(Hterm($G_{\hat{j}}$),G), by (5), we obtain

(19) Mterm(Hterm($G_{\hat{j}}$),F)

i.e.

(20) $\text{Hterm}(G_{\hat{j}}) = t.\text{Hterm}(F_{\hat{\hat{i}}})$ for some $\hat{\hat{i}} \in \{1,..,L(F)\}$ and t.

Thus, from (18) and (20) we obtain

(21) $\text{Hterm}(F_{\hat{i}}) = s.t.\text{Hterm}(F_{\hat{\hat{i}}})$

where $s.t \ne x_1^0...x_n^0$ and therefore $\hat{\hat{i}} \ne \hat{i}$.

However (21) is contradictory to (6).

1.18. Proof of Theorem 1.6.:

By Lemma 1.16. we get a $\pi: \{1,..,L(F)\} \xrightarrow[\text{onto}]{1-1}$ $\xrightarrow[\text{onto}]{1-1} \{1,..,L(G)\}$ such that

(1) $\bigwedge_{1\le i\le L(F)} \text{Hterm}(F_i) = \text{Hterm}(G_{\pi(i)})$

Case I: F=G=(0)

In this case the conclusion of the Theorem is trivially true.

Case II: $F,G \neq (0)$

(The cases $F=(0) \wedge G \neq (0)$ and $F \neq (0) \wedge G=(0)$ are not possible because of the assumption $\text{Ideal}(F) = \text{Ideal}(G)$.)

From the assumption that F and G are normed we get

(2) $\bigwedge_{1 \leq i \leq L(F)} (\text{Hcoef}(F_i)=1, \text{Hcoef}(G_i)=1)$.

Now assume

(3) $F_i \neq G_{\pi(i)}$ for some $1 \leq i \leq L(F)$

and define

(4) $g := F_i - G_{\pi(i)}$.

We immediately have

(5) $g \neq 0$

and

(6) $g \in \text{Ideal}(F)$.

In addition,

(7) $\text{Normalf}(g,F)$.

To show this assume

(8) $\text{Occ}(t,g)$.

Then

(9) $t \neq \text{Hterm}(F_i) = \text{Hterm}(G_{\pi(i)})$

because of (1),(2) and (4).
From (8) it follows that $\text{Occ}(t,F_i) \vee \text{Occ}(t,G_{\pi(i)})$.

If $\text{Occ}(t,F_i)$ then $\neg \text{Mterm}(t,F)$ because of (9) and the assumption that F is normed.

If $\text{Occ}(t,G_{\pi(i)})$ then $\neg \text{Mterm}(t,F)$ because of (9) and the assumption that G is normed which leads to $\neg \text{Mterm}(t,G)$, wherefrom $\neg \text{Mterm}(t,F)$ may be concluded by Lemma 1.8.

(5),(6) and (7) contradict to the assumption that F is a G-basis. So (3) has to be refused.

2. The effectiveness of deciding ideal inclusion

In [1], 2.2, we have seen that there is an algorithm that constructs g such that $f > g$ for a given f, i.e. there is a function Compnormf which is computable and such that

(C1) $\bigwedge_f f \underset{F}{>} \text{Compnormf}(f,F)$

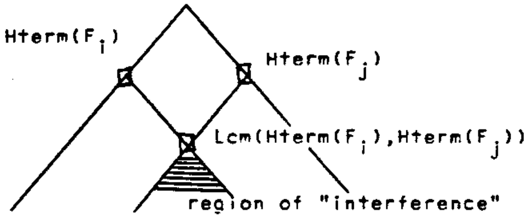
(computability (decidability) in this context means computability (decidability) relative to the arithmetic operations for K.)

In our early papers on polynomial reduction (see references in [1]) we have given an algorithm Comp-G-basis which constructs a minimal G-basis G from F, i.e.

(C2) $\bigwedge_F (\text{Ideal}(F) = \text{Ideal}(\text{Comp-G-basis}(F)) \wedge \text{Min-G-basis}(\text{Comp-G-basis}(F))$.

This algorithm is based on property (G2) of G-bases (see [1], 3.3), which shows that for forcing a basis to be a G-basis it suffices to add polynomials that guarantee that the S-polynomials can be M-reduced to 0.

Why S-polynomials are so important in our investigations can, again, be "seen" from the graphical presentation in 1.7.



The "region of interference" is the only region where something interesting may happen.

We now show how $\text{Ideal}(F) \subseteq \text{Ideal}(G)$ can be easily decided as soon as we have an algorithm Comp-G-basis which constructs minimal G-basis for given polynomial ideals.

We first show how to apply the algorithm Comp-G-basis to obtain an easy method for deciding $f \in \text{Ideal}(G)$:

1. $G' := \text{Comp-G-basis}(G)$
2. $g := \text{Compnormf}(f,G')$
3. $g = 0$?

   Yes: answer "$f \in \text{Ideal}(G)$"

   No : answer "$f \notin \text{Ideal}(G)$".

This algorithm is correct because of (G5) and (G6) in [1], Proposition 3.7.

Now $\text{Ideal}(F) \subseteq \text{Ideal}(G)$ can be decided by deciding $\bigwedge_i F_i \in \text{Ideal}(G)$ using the above method.

3. The effectiveness of deciding whether F is a minimal normed G-basis

For making the decision whether a given basis F is a G-basis proceed as follows

1. $G := \text{Comp-G-basis}(F)$
2. $\bigwedge_t (\text{Mterm}(t,F) \longleftrightarrow \text{Mterm}(t,G))$?

   Yes: answer "F is a G-basis"
   No : answer "F is not a G-basis".