1976-00-00-A

ACM
ASSOCIATION FOR COMPUTING MACHINERY · FOUNDED 1947 ·

SIGSAM Bulletin

A Quarterly Publication of the
Special Interest Group on Symbolic & Algebraic Manipulation

Volume 10, Number 3, August 1976, (Issue Number 39)

Contents:

Contributions

A THEORETICAL BASIS FOR THE REDUCTION OF POLYNOMIALS TO CANONICAL FORMS

by

B. Buchberger
Universität Linz
A-4045 LINZ, Austria

Abstract

We define a certain type of bases of polynomial ideals whose usefulness stems from the fact that a number of computability problems in the theory of polynomial ideals (e.g. the problem of constructing canonical forms for polynomials) is reducible to the construction of bases of this type. We prove a characterization theorem for these bases which immediately leads to an effective method for their construction.

Introduction

In [1] we gave an algorithm for effectively constructing a basis of the vector space $K[x_1,\ldots,x_n]/\mathfrak{a}$ where $\mathfrak{a}$ is some ideal of dimension 0 in the polynomial ring $K[x_1,\ldots,x_n]$. In [2] we showed that the same algorithm is correct in the case of arbitrary dimension, too, and demonstrated how it can be applied to solve a number of other computability and decidability problems in the theory of polynomial ideals.

Recently, M. Lauer, [4], has pointed out that this algorithm, as a byproduct, yields the solution to the problem of constructing canonical forms for polynomial expressions under side relations.

This problem has been raised at the EUROSAM conference 1974, see [6], where it has been conjectured that, in general, for polynomials canonical forms do not exist.

Our algorithm proceeds by constructing a new basis for a given ideal from which the answer to the computability and decidability problems may be easily read off.

In this paper we single out the characteristic property of such bases by a definition that is independent of the algorithm (see Definition 3.1). In this definition we use a new version of the concept of M-reduction, which, in fact, was the original one proposed by W. Gröbner, [4], in 1964, (see Definition 1.5). Formally, this version is more appealing than that used in [1] and [2]. However, it needs a totally new proof of the main theorem on which the algorithm in [1] and [2] is based.

After some preparations in sections 1 and 2, we present this proof in section 3 (see 3.3 to 3.6). In one of the next issues of this Bulletin we shall give a uniqueness theorem and some further decidability results for the bases defined in 3.1.

In this paper we emphasize the technical aspects of the proof. For the reader who whishes to have more examples and informal intuitions, we prepared a tutorial exposition of the material, see [3].

1. Basic Definitions

Throughout the paper, K denotes an arbitrary field. By $K[x_1,\ldots,x_n]$ (abbreviated $K[\,]_n$) we denote the ring of all polynomials over K in n indeterminates ($n \in N_+$). (N ... set of natural numbers including zero, $N_+ := N-\{0\}$.)

In the examples, K always will be the field of rational numbers and for naming concrete polynomials we use the usual notation. For example, by $3xy^2 + 5x - 1$ and $-x_1^3x_2 + \frac{3}{2}x_1x_3^2 - x_1x_2x_3$ we name certain polynomials in $K[x,y]$ and $K[x_1,x_2,x_3]$, respectively. Note, that these names are not unique. For instance, $3xy^2 + 5x - 1$; $-1 + 5x + 3xy^2$, and $0.x^2 + 3xy^2 + 5x - 1$ are names for the same polynomial. Ordinarily, also $xy^2 + 5x - 1 + 2xy^2$ would be accepted as a name for the same polynomial. If one wanted to think of the polynomial ring $K[x_1,\ldots,x_n]$ to be the set of expressions of the above kind, one had to norm these expressions by some rule (for instance,

(R1) combine equal terms
(R2) omit terms with zero coefficient
(R3) use a fixed order of terms).

One should carefully distinguish between the two meanings of the sign + in expressions like this

$$(5x^2 + 3y) + (2xy + 1)$$

separator between terms of the first polynomial

separator between terms

sign for addition of two polynomials

Otherwise, by the suggestive notations above, one is easily mislead to draw incorrect conclusions in reduction arguments for polynomials. So, if doubts appear about the nature of polynomials one should either take a set of axioms for the structures admitted as "polynomial rings over K in n indeterminates" or choose a fixed mathematical model rather than the ordinary "linguistic" one. For instance, a suitable model could be defined as follows:

The polynomial ring in n indeterminates over the field (K,+,.) is the structure $(K[]_n,[+],[.])$, where

$$K[]_n := \{f \mid f: N^n \longrightarrow K \text{ and } \{(i_1,\dots,i_n) \mid f(i_1,\dots,i_n) \neq 0\} \text{ is finite}\}$$

and for $f,g \in K[]_n$, $(i_1,\dots,i_n) \in N^n$

$$(f[+]g)(i_1,\dots,i_n) := f(i_1,\dots,i_n) + g(i_1,\dots,i_n)$$

$$(f[.]g)(i_1,\dots,i_n) := \sum_{\substack{(j_1,\dots,j_n) \in N^n \\ (k_1,\dots,k_n) \in N^n \\ j_1+k_1=i_1,\dots,j_n+k_n=i_n}} f(j_1,\dots,j_n).g(k_1,\dots,k_n)$$

However, in order not to blow up the formal apparatus of this paper we give all definitions below relative to the familiar "linguistic" model and encourage the critical reader to control that the dangerous ambiguities pointed out above do not go into the definitions.

1.1. Definition:

$K\langle\rangle_n := \{x_1^{i_1} \dots x_n^{i_n} \mid i_1,\dots,i_n \in N\}$
(set of terms in n indeterminates)

$Degree(x_1^{i_1} \dots x_n^{i_n}) := i_1+\dots+i_n$
(the degree of a term)

$x_1^{i_1}\dots x_n^{i_n} <_T x_1^{j_1}\dots x_n^{j_n} \ :\longleftrightarrow$
$Degree(x_1^{i_1}\dots x_n^{i_n}) < Degree(x_1^{j_1}\dots x_n^{j_n})$ or
$(Degree(x_1^{i_1}\dots x_n^{i_n}) = Degree(x_1^{j_1}\dots x_n^{j_n})$ and
$i_1=j_1,\dots,i_k=j_k, i_{k+1}>j_{k+1}$ for some k
with $1 \leq k+1 \leq n)$
(lexikographical ordering of terms)

The ordering $<_T$ plays an essential role in the reduction procedure defined below.

1.2. Convention:

To simplify notation we restrict the use of certain variables

- i,j,k,l,m... variables for natural numbers
- a,b,c,d ... variables for elements of K
- f,g,h ... variables for polynomials of $K[]_n$
- s,t ... variables for terms in $K\langle\rangle_n$
- F,G,H ... variables for finite, non-empty sequences of polynomials.

It is understood that all these variables (with the exeption of F,G,H) preserve their range when used with indices. Thus, f_1 is a variable ranging over $K[]_n$. On the other hand, F_i means the i-th component of the sequence F.

1.3. Definition:

$Coef(t,f)$:= Coefficient of term t in f

$Occ(t,f) :\longleftrightarrow Coef(t,f) \neq 0$ (term t occurs in f)

$Hterm(f) := \begin{cases} \text{the term that is maximal with respect to } <_T \text{ among the terms occuring in } f, \text{ if } f \neq 0 \\ x_1^0 \dots x_n^0, \text{ if } f = 0 \end{cases}$
(the head-term of f)

$Hcoef(f) := Coef(Hterm(f),f)$
(the head-coefficient of f)

$Head(f) := Hcoef(f).Hterm(f)$ (the head of f)

$Rest(f) := f - Head(f)$ (the rest of f)

1.4. Definition:

$Multiple(x_1^{i_1}\dots x_n^{i_n}, x_1^{j_1}\dots x_n^{j_n}) :\longleftrightarrow$
$i_1 \geq j_1,\dots,i_n \geq j_n$
($x_1^{i_1}\dots x_n^{i_n}$ is a multiple of $x_1^{j_1}\dots x_n^{j_n}$)

$Lcm(x_1^{i_1}\dots x_n^{i_n}, x_1^{j_1}\dots x_n^{j_n}) :=$
$:= x_1^{max(i_1,j_1)}\dots x_n^{max(i_n,j_n)}$
(the least common multiple of two terms)

$L(F)$:= length (i.e. number of components) in the sequence F

$Mterm(t,F) :\longleftrightarrow \bigvee_{1 \leq i \leq L(F)} F_i \neq 0 \wedge Multiple(t, Hterm(F_i))$
(t is an M-term with respect to F)

$Normalf(f,F) :\longleftrightarrow \bigwedge_t (Occ(t,f) \longrightarrow \neg Mterm(t,F))$
(f is in normal form with respect to F).

1.5. Definition:

$f \underset{F,t,i}{\overset{1}{\rightarrow}} g :\longleftrightarrow$
$1 \leq i \leq L(F)$,
$F_i \neq 0$,
$Occ(t,f)$,
$Multiple(t, Hterm(F_i))$,
$g = f - a.s.F_i$, where
$a = \dfrac{Coef(t,f)}{Hcoef(F_i)}$ and s is such that
$t = s.Hterm(F_i)$
(f M-reduces to g with respect to F in one step that involves t and F_i).

$$f \overset{1}{\underset{F}{\to}} g :\longleftrightarrow \bigvee_{t,i} f \overset{1}{\underset{F,t,i}{\to}} g$$

(f M-reduces to g with respect to F in one step)

$$f \underset{F}{\to} g :\longleftrightarrow \bigvee_{k\in N} \bigvee_{h_0,\ldots,h_k} \Big(f=h_0,\ g=h_k,\ \bigwedge_{0\le j<k} h_j \overset{1}{\underset{F}{\to}} h_{j+1}\Big)$$

(f M-reduces to g with respect to F)

$$f \underset{F}{\underset{\sim}{\to}} g :\longleftrightarrow f \underset{F}{\to} g \wedge \text{Normalf}(g,F)$$

(g is a normalform of f with respect to F)

$$f \underset{F}{\overset{succ}{\nabla}} g :\longleftrightarrow \bigvee_h (f \underset{F}{\to} h) \wedge (g \underset{F}{\to} h)$$

(f and g have a common $\to$-successor with respect to F).

1.6. Convention:

If F is clear from the context we write Mterm(t), Normalf(f), $\overset{1}{\underset{t,i}{\to}}$, $\overset{1}{\to}$, $\to$, $\underset{\sim}{\to}$, $\overset{succ}{\nabla}$ instead of Mterm(t,F), Normalf(f,F), $\overset{1}{\underset{F,t,i}{\to}}$, $\overset{1}{\underset{F}{\to}}$, $\underset{F}{\to}$, $\underset{F}{\underset{\sim}{\to}}$, $\underset{F}{\overset{succ}{\nabla}}$.

1.7. Example:

$F := (x_1^2x_2 - 3x_3,\ 2x_3^2 + 5x_1x_2,\ -5x_1x_3 - x_2)$.

Then, $\text{Hterm}(F_1) = x_1^2x_2$, $\text{Hterm}(F_2) = x_3^2$, $\text{Hterm}(F_3) = x_1x_3$, $\text{Mterm}(x_2x_3^4, F)$.

$$-3x_2x_3^4 + 3x_1^2x_2x_3 + x_1x_2 \overset{1}{\underset{F,x_2x_3^4,2}{\to}}$$

$$\frac{15}{2}x_1x_2^2x_3^2 + 3x_1^2x_2x_3 + x_1x_2 \overset{1}{\underset{F,x_1^2x_2x_3,1}{\to}}$$

$$\frac{15}{2}x_1x_2^2x_3^2 + 9x_3^2 + x_1x_2,$$

and, therefore

$$-3x_2x_3^4 + 3x_1^2x_2x_3 + x_1x_2 \underset{F}{\to}$$

$$\frac{15}{2}x_1x_2^2x_3^2 + 9x_3^2 + x_1x_2$$

Further,

$$2x_1^2x_2 - 2x_3^2 + 5 \overset{1}{\underset{F}{\to}} -2x_3^2 + 6x_3 + 5 \overset{1}{\underset{F}{\to}}$$

$$\overset{1}{\underset{F}{\to}} 5x_1x_2 + 6x_3 + 5, \text{ and therefore}$$

$$2x_1^2x_2 - 2x_3^2 + 5 \underset{F}{\to} \underset{\sim\sim\sim}{5x_1x_2 + 6x_3 + 5}$$

because Normalf$(5x_1x_2 + 6x_3 + 5, F)$.

Also

$$2x_3^2 + 10x_1x_2 + 6x_3 + 5 \underset{F}{\to} 5x_1x_2 + 6x_3 + 5,$$

and therefore,

$$2x_1^2x_2 - 2x_3^2 + 5 \underset{F}{\overset{succ}{\nabla}} 2x_3^2 + 10x_1x_2 + 6x_3 + 5.$$

1.8. Definition:

$$\text{Spol}(f,g) :=$$

$$:= \text{Hcoef}(g) \cdot \frac{\text{Lcm}(\text{Hterm}(f),\text{Hterm}(g))}{\text{Hterm}(f)} \cdot f -$$

$$- \text{Hcoef}(f) \cdot \frac{\text{Lcm}(\text{Hterm}(f),\text{Hterm}(g))}{\text{Hterm}(g)} \cdot g$$

(the S-polynomial of f and g, i.e. a polynomial which derives from f and g by a special type of subtraction), where

$$\frac{x_1^{i_1}\ldots x_n^{i_n}}{x_1^{j_1}\ldots x_n^{j_n}} := x_1^{i_1-j_1}\ldots x_n^{i_n-j_n}, \text{ which is}$$

considered to be defined only in case $i_1 \ge j_1, \ldots, i_n \ge j_n$.

1.9. Example:

Let $f := 5xy - 3x$, $g := 7y^2 + 2x$.

$\text{Lcm}(\text{Hterm}(f),\text{Hterm}(g)) = \text{Lcm}(xy, y^2) = xy^2$.

$$\text{Spol}(f,g) = 7 \cdot \frac{xy^2}{xy} \cdot f - 5 \cdot \frac{xy^2}{y^2} \cdot g =$$

$$= 7 \cdot y \cdot f - 5 \cdot x \cdot g =$$

$$= (35xy^2 - 21xy) - (35xy^2 + 10x^2) =$$

$$= -21xy - 10x^2.$$

Notice, that by the procedure of forming Spol(f,g) the highest term (in our example xy^2) disappears. The S-polynomials play a central role in Theorem 3.3 and the algorithms in [1] and [2].

1.10. Definition:

$$\text{Ideal}(F) :=$$

$$:= \{h_1 \cdot F_1 + \ldots + h_l \cdot F_l \mid l = L(F) \wedge h_1, \ldots, h_l \in K[\,]_n\}$$

(the ideal generated by F).

We now list some elementary facts about the notions introduced so far. We shall make constant and tacit use of these properties in the proofs in Section 3.

2. Elementary properties of the basic notions

2.1. Lemma:

(E1) Properties of $<_T$

$<_T$ is a linear ordering on $K\langle\rangle_n$ which is isomorphic to the ordering $<$ on N.

$x_1^0 \ldots x_n^0$ corresponds to the zero element in N, i.e. $x_1^0 \ldots x_n^0 \leq_T t$.

(E2) Properties of Occ, Hcoef, Hterm, Head, Rest

$f \neq 0 \longrightarrow \mathrm{Occ}(\mathrm{Hterm}(f), f)$

$f = \mathrm{Head}(f) + \mathrm{Rest}(f)$

$\mathrm{Hcoef}(0) = 0$, $\mathrm{Hterm}(0) = x_1^0 \ldots x_n^0$, $\mathrm{Head}(0) = 0$, $\mathrm{Rest}(0) = 0$

$\mathrm{Normalf}(f) \longrightarrow \mathrm{Normalf}(\mathrm{Rest}(f))$

$\mathrm{Hterm}(f) \neq x_1^0 \ldots x_n^0 \longrightarrow$

$\longrightarrow \mathrm{Hterm}(f) >_T \mathrm{Hterm}(\mathrm{Rest}(f))$.

(E3) Properties of $\to^1$

$f \to^1 g \longrightarrow f \neq 0$

$f \to^1_{t,i} g \longrightarrow \neg\mathrm{Occ}(t, g)$

$\mathrm{Hterm}(f) \neq x_1^0 \ldots x_n^0$, $f \to^1_{\mathrm{Hterm}(f), i} g \longrightarrow$

$\longrightarrow \mathrm{Hterm}(f) >_T \mathrm{Hterm}(g)$

$f \to^1 g \longrightarrow \mathrm{Hterm}(f) \geq_T \mathrm{Hterm}(g)$

$f \to^1_{t,i} g$, $\neg\mathrm{Occ}(t,h) \longrightarrow f+h \to^1 g+h$

$\mathrm{Rest}(f) \to^1 g \longrightarrow f \to^1 \mathrm{Head}(f) + g$

$\mathrm{Rest}(f) \to^1 \mathrm{Rest}(g)$, $\mathrm{Head}(f) = \mathrm{Head}(g) \longrightarrow$

$\longrightarrow f \to^1 g$

$f \to^1 g$, $a \neq 0 \longrightarrow a.t.f \to^1 a.t.g$.

(E4) Properties of $\to$

$\to$ is a quasi-ordering on $K[\,]_n$ (i.e. it is reflexive and transitive).

$f \to g \wedge f \neq g \longrightarrow \bigvee_h f \to^1 h$

$f \to g \wedge f \neq g \longrightarrow \neg\mathrm{Normalf}(f)$

$f \to g \longrightarrow \mathrm{Hterm}(f) \geq_T \mathrm{Hterm}(g)$

$\bigwedge_f \bigvee_g f \to \underset{\sim}{g}$

$\mathrm{Rest}(f) \to g \longrightarrow f \to \mathrm{Head}(f) + g$

$f \to g \longrightarrow a.t.f \to a.t.g$

$\neg\mathrm{Mterm}(\mathrm{Hterm}(h)) \wedge h \to h' \longrightarrow$

$\longrightarrow \mathrm{Head}(h) = \mathrm{Head}(h') \wedge \mathrm{Rest}(h) \to \mathrm{Rest}(h')$

$f \to g$, $\mathrm{Hterm}(f) = \mathrm{Hterm}(g) \longrightarrow$

$\longrightarrow \mathrm{Rest}(f) \to \mathrm{Rest}(g)$

(E5) Properties of $\to$ and Ideal

$f \to_F g \longrightarrow f - g \in \mathrm{Ideal}(F)$

$f \to_F g$, $f \in \mathrm{Ideal}(F) \longrightarrow g \in \mathrm{Ideal}(F)$

(E6) Properties of $\to$ and Normalf

$\mathrm{Normalf}(0)$

$\mathrm{Normalf}(f) \longrightarrow f \to \underset{\sim}{f}$

$\mathrm{Normalf}(f) \wedge f \to g \longrightarrow f = g$

$f \to \underset{\sim}{g} \longrightarrow \mathrm{Normalf}(g)$.

(E7) Properties of Spol

$f, g \in \mathrm{Ideal}(F) \longrightarrow \mathrm{Spol}(f,g) \in \mathrm{Ideal}(F)$

$\bigwedge_{1 \leq i, j \leq L(F)} \mathrm{Spol}(F_i, F_j) \in \mathrm{Ideal}(F)$

(E8) Properties of $\underset{\nabla}{\mathrm{succ}}$

$\underset{\nabla}{\mathrm{succ}}$ is reflexive and symmetric

$f \underset{\nabla}{\mathrm{succ}} g \longrightarrow \bigvee_h f \to \underset{\sim}{h}$, $g \to \underset{\sim}{h}$

$f \to g \longrightarrow f \underset{\nabla}{\mathrm{succ}} g$.

2.2. Proofs:

In general, the proofs for these properties are immediate.

ad (E4) $\bigwedge_f \bigvee_g f \to \underset{\sim}{g}$: There is a straightforward algorithm that constructs g such that $f \to \underset{\sim}{g}$ for a given f:

successively eliminate M-terms t from f by executing a step of the form $f \to^1_{F,t,i} g$ until no M-terms are left, i.e. a normal form is reached.

The termination of this algorithm is guaranteed by the fact that in each step g decreases with respect to the following wellfounded ordering (for the notion of a well-founded ordering and its role in termination proofs, see [7] ,pp. 185):

$g <_P g' :\longleftrightarrow W(g) < W(g')$, where

$W(g) := \sum_{Occ(t,g)} 2^{Nr(t)}$ and Nr is the order isomorphism between $(K<>_n, <_T)$ and $(N,<)$.

2.3. Remark:

One is easily tempted to believe that

$f \to^1 g \longrightarrow f+h \to^1 g+h$ or that

$f \to g \longrightarrow f+h \to g+h$. However, this is not the case and, in fact, this is one of the major reasons why the theorems on reductions of polynomials are relatively hard to prove. Instead, we have the following lemma.

2.4. Lemma:

(R1) $f \to^1 g \longrightarrow f+h \overset{succ}{\nabla} g+h$

(R2) $f-g \to^1 h \longrightarrow \bigvee_{f',g'} (h = f'-g',\ f \to f',\ g \to g')$

(R3) $f-g \to 0 \longrightarrow f \overset{succ}{\nabla} g$.

2.5. Proof:

ad (R1):

Assume $f \to^1_{t,i} g$, i.e. $g = f-a.s.F_i$ where

$a := \frac{Coef(t,f)}{Hcoef(F_i)}$ and

s is such that
$t = s.Hterm(F_i)$.

Case I: $Coef(t,h) = 0$.

In this case we have $f+h \to^1 g+h$ and therefore $f+h \overset{succ}{\nabla} g+h$.

Case II a: $Coef(t,h) \neq 0$,
$Coef(t,h) = -Coef(t,f)$.

In this case we have $g+h \to^1 f+h$ and therefore $f+h \overset{succ}{\nabla} g+h$.

Case II b: $Coef(t,h) \neq 0$,
$Coef(t,h) \neq -Coef(t,f)$.

In this case we define

$$\hat{h} := f + h - \frac{Coef(t,f+h)}{Hcoef(F_i)} . s . F_i$$

$$\hat{\hat{h}} := g + h - \frac{Coef(t,g+h)}{Hcoef(F_i)} . s . F_i .$$

Since $Occ(t,f+h)$ and $Occ(t,g+h)$, we have $f+h \to^1 \hat{h}$ and $g+h \to^1 \hat{\hat{h}}$. It is easy to check that $\hat{h} = \hat{\hat{h}}$. Thus, $f+h \overset{succ}{\nabla} g+h$.

ad (R2):

Assume $f-g \to^1_{t,i} h$, i.e. $h=f-g-a.s.F_i$, where

$a := \frac{Coef(t,f-g)}{Hcoef(F_i)}$ and s is

such that $t = s.Hterm(F_i)$.

Case I: $Occ(t,f)$, $\neg Occ(t,g)$.

Choose: $f' := f - a.s.F_i$,

$g' := g$,

Case II: $\neg Occ(t,f)$, $Occ(t,g)$.

Choose: $f' := f$,

$g' := g - (-a).s.F_i$.

Case III: $Occ(t,f)$, $Occ(t,g)$,
$Coef(t,f) \neq Coef(t,g)$.

(The case $Coef(t,f) = Coef(t,g) \neq 0$ is not possible, because of $Occ(t,f-g)$. By the same reason also $\neg Occ(t,f) \wedge \neg Occ(t,g)$ is not possible!)

Choose: $f' := f - \frac{Coef(t,f)}{Hcoef(F_i)} . s . F_i$,

$g' := g - \frac{Coef(t,g)}{Hcoef(F_i)} . s . F_i$.

ad (R3):

We give a proof by induction on the number of $\to^1$-steps necessary to M-reduce f-g to 0.

Induction basis:

$f-g = 0$ (i.e. the M-reduction is possible in zero steps).

In this case $f=g$ and therefore $f \overset{succ}{\nabla} g$.

Induction hypothesis:

For a fixed $t \in N$:

$f-g = h_0 \to^1 h_1 \to^1 \ldots \to^1 h_t = 0 \longrightarrow f \overset{succ}{\nabla} g$.

We now consider $f,g,h_0,\ldots,h_{t+1}$ such that

$f-g = h_0 \to^1 h_1 \to^1 \ldots \to^1 h_{t+1} = 0$.

Choose $f'-g'$ such that

$h_1 = f'-g'$, $f \to f'$, $g \to g'$ (use (R2)!) .

By induction hypothesis, $f' \overset{succ}{\nabla} g'$, and therefore $f \overset{succ}{\nabla} g$.

3. Gröbner-bases and characterization of Gröbner-bases

3.1. Definition:

A sequence F of polynomials from $K[\,]_n$ is a Gröbner-basis (abbreviated G-basis(F)) (for ideal (F)) : $\longleftrightarrow$

(G1) $\bigwedge_{g} (g \in \mathrm{Ideal}(F), \mathrm{Normalf}(g,F) \longrightarrow g=0)$

(i.e. in Ideal(F) there is no polynomial in normalform other than 0).

3.2. Example:

Let $F := (xy-x, x^2+y)$. F is not a G-basis, because $-y^2+y \in \mathrm{Ideal}(F)$, $-y^2+y \neq 0$, $\mathrm{Normalf}(-y^2+y, F)$.

Let $F' := (xy-x, x^2+y, -y^2+y)$. F' is a G-basis. This, too, can easily be seen after applying the algorithm given in [2]. For the moment notice that $\neg\mathrm{Normalf}(-y^2+y, F')$.

3.3. Theorem:

The following statements are equivalent:

(G1) F is a Gröbner-basis.

(G2) $\bigwedge_{1\le i,j\le L(F)} \mathrm{Spol}(F_i,F_j) \mathrel{\cdot\!>} \underset{\sim}{0}$.

(i.e. all the S-polynomials of polynomials F_i and F_j are M-reducible to 0)

(G3) $\bigwedge_{h,h_1,h_2} (h \mathrel{\cdot\!>} \underset{\sim}{h_1} \wedge h \mathrel{\cdot\!>} \underset{\sim}{h_2} \longrightarrow h_1=h_2)$

(i.e. all the M-reductions of a given polynomial h lead to the same normalform).

3.4. Proof of Theorem 3.3:

(G1) $\longrightarrow$ (G2):

Assume (G1), i.e.

(1) $\bigwedge_{g} (g \in \mathrm{Ideal}(F), \mathrm{Normalf}(g,F) \longrightarrow g=0)$

Take i,j such that $1\le i,j\le L(F)$. Then

(2) $\mathrm{Spol}(F_i,F_j) \in \mathrm{Ideal}(F)$

Let g be such that

(3) $\mathrm{Spol}(F_i,F_j) \mathrel{\cdot\!>} \underset{\sim}{g}$

Then,

(4) $g \in \mathrm{Ideal}(F)$.

So by (1), (4) and (3), $g=0$, i.e.

(5) $\mathrm{Spol}(F_i,F_j) \mathrel{\cdot\!>} \underset{\sim}{0}$.

(Note that we constantly use the "elementary properties" compiled in Lemma 2.1.)

3.5. Proof of Theorem 3.3.

(G2) $\longrightarrow$ (G3):

Sketch:

Use induction on the headterms of h with respect to the ordering $<_T$.
Lemma 2.4. will play a central role.
Compare also the graphical summary of the proof in [3].

Details:

Induction basis: $\mathrm{Hterm}(h) = x_1^0 \ldots x_n^0$.

Assume $h \mathrel{\cdot\!>} \underset{\sim}{h_1}$, $h \mathrel{\cdot\!>} \underset{\sim}{h_2}$.

Case I: $\bigvee_{1\le i\le L(F)} (\mathrm{Hterm}(F_i)=x_1^0\ldots x_n^0 \wedge F_i\neq 0)$.

Then $h_1=0$, $h_2=0$, i.e. $h_1=h_2$.

Case II: $\neg\bigvee_{1\le i\le L(F)} (\mathrm{Hterm}(F_i)=x_1^0\ldots x_n^0 \wedge F_i\neq 0)$.

Then Normalf(h), and therefore $h_1=h$, $h_2=h$, i.e. $h_1=h_2$.

Induction hypothesis: For some fixed t $t >_T x_1^0\ldots x_n^0$:

(1) $\bigwedge_{h} (\mathrm{Hterm}(h) <_T t \longrightarrow$

$\longrightarrow \bigwedge_{h_1,h_2} (h \mathrel{\cdot\!>} \underset{\sim}{h_1} \wedge h \mathrel{\cdot\!>} \underset{\sim}{h_2} \longrightarrow h_1=h_2))$.

Consider now an h with

(2) $\mathrm{Hterm}(h)=t$.

Case I:

$\neg\bigvee_{1\le i\le L(F)} (F_i\neq 0 \wedge \mathrm{Multiple}(\mathrm{Hterm}(h),\mathrm{Hterm}(F_i)))$.

Assume

(3) $h \mathrel{\cdot\!>} \underset{\sim}{h_1}$, $h \mathrel{\cdot\!>} \underset{\sim}{h_2}$. We have

(4) $h \mathrel{\cdot\!>} h_1$, $h \mathrel{\cdot\!>} h_2$ and therefore

(5) $\mathrm{Head}(h) = \mathrm{Head}(h_1) = \mathrm{Head}(h_2)$,

(6) $\mathrm{Rest}(h) \mathrel{\cdot\!>} \mathrm{Rest}(h_1)$, $\mathrm{Rest}(h) \mathrel{\cdot\!>} \mathrm{Rest}(h_2)$

(7) $\mathrm{Hterm}(\mathrm{Rest}(h)) <_T \mathrm{Hterm}(h)=t$

(8) $\mathrm{Normalf}(\mathrm{Rest}(h_1))$, $\mathrm{Normalf}(\mathrm{Rest}(h_2))$.

From (6) and (8)

(9) $\mathrm{Rest}(h) \mathrel{\cdot\!>} \underset{\sim}{\mathrm{Rest}(h_1)}$, $\mathrm{Rest}(h) \mathrel{\cdot\!>} \underset{\sim}{\mathrm{Rest}(h_2)}$.

Thus, from (7) and (9) by induction hypothesis

(10) $\mathrm{Rest}(h_1) = \mathrm{Rest}(h_2)$.

Finally, from (5) and (10)

(11) $h_1=h_2$, q.e.d.

Case II:

$\bigvee_{1\le i\le L(F)} (F_i\neq 0 \wedge \mathrm{Multiple}(\mathrm{Hterm}(h),\mathrm{Hterm}(F_i)))$.

Assume that $1\le m\le L(F)$,

$\bigwedge_{1\le k,k'\le m} (k\neq k' \longrightarrow i_k\neq i_{k'})$, $\bigwedge_{1\le k\le m} 1\le i_k\le L(F)$

and

(12) $F_{i_k} \neq 0 \wedge Multiple(Hterm(h), Hterm(F_{i_k}))$

for $1 \le k \le m$

and

(13) $F_i = 0 \vee \neg Multiple(Hterm(h), Hterm(F_i))$

for $i \notin \{i_1, \dots, i_m\}$.

Take $g_1, g_2, \bar h$ such that

(14) $Rest(h) \to \underset{\sim}{g_1}$

(15) $Head(h) \to^1_{Hterm(h),i_1} g_2$

(16) $g_2 + g_1 \to \underset{\sim}{\bar h}$. From (14)-(16) we obtain

(17) $h \to \underset{\sim}{\bar h}$. We show

(18) $\bigwedge_{h_2} (h \to \underset{\sim}{h_2} \longrightarrow h_2 = \bar h)$, wherefrom

(19) $\bigwedge_{h_1, h_2} (h \to \underset{\sim}{h_1} \wedge h \to \underset{\sim}{h_2} \longrightarrow h_1 = h_2)$

follows. Thus, let us assume

(20) $h \to \underset{\sim}{h_2}$.

Case II a: h is M-reduced to h_2 by an M-reduction of the following kind:

$h = Head(h) + Rest(h) \to$

$\to Head(h) + g_1' \to^1_{Hterm(h),i_1} g_2' + g_1' \to h_2$,

where

(21) $Rest(h) \to g_1'$

(22) $Head(h) \to^1_{Hterm(h),i_1} g_2'$

(23) $g_2' + g_1' \to \underset{\sim}{h_2}$.

For showing that in every case of this type $h_2 = \bar h$ we show somewhat more, namely:

for all $p, g, g_2', f_0, \dots, f_p$, if

(24) $Hterm(g) <_T Hterm(h)$

(25) $Head(h) \to^1_{Hterm(h),i_1} g_2'$

(26) $g = f_0$, $\bigwedge_{0 \le q < p} f_q \to^1 f_{q+1}$

then

(27) $g_2' + g \overset{succ}{\nabla} g_2' + f_p$.

Because if we have proven this we may proceed as follows: Assume (21) to (23) for some g_1', g_2' and h_2.

Consider an M-reduction that reduces g_1' to normalform, i.e. take $p \in N$, $f_0, \dots, f_p$ such that

(28) $g_1' = f_0$, $\bigwedge_{0 \le q < p} f_q \to^1 f_{q+1}$ and

(29) $Normalf(f_p)$.

Then on the one hand for some h_3

(30) $h = Head(h) + Rest(h) \to Head(h) + g_1' =$

$= Head(h) + f_0 \to^1 Head(h) + f_1 \to^1 \dots$

$\dots \to^1 Head(h) + f_p \to^1_{Hterm(h),i_1} g_2' + f_p \to \underset{\sim}{h_3}$.

On the other hand

(31) $h = Head(h) + Rest(h) \to$

$\to Head(h) + g_1' \to^1_{Hterm(h),i_1} g_2' + g_1' \to \underset{\sim}{h_2}$.

By (21), (28) and (29)

(32) $Rest(h) \to \underset{\sim}{f_p}$

and therefore, by induction hypothesis (1) and (14)

(33) $f_p = g_1$.

By (15) and (22),

(34) $g_2 = g_2'$.

By (16), (30), (33), (34) and induction hypothesis (1)

(35) $h_3 = \bar h$.

Now set $g := g_1'$. Then (24) holds because of (21), (25) holds because of (22) and (26) because of (28).

So by (27) for some $\hat h$

(36) $g_2' + g_1' \to \underset{\sim}{\hat h}$,

(37) $g_2' + f_p \to \underset{\sim}{\hat h}$.

From (30) and (37) by the induction hypothesis (1) and (35) we obtain

(38) $\hat h = h_3 = \bar h$.

Thus, by (23), (36), induction hypothesis (1) and (38) we, finally, obtain

(39) $h_2 = \hat h = \bar h$.

So let us show that from (24)-(26) we may infer (27). This is shown by induction on p.

First assume p=0, i.e. $g = f_0 = f_p$.

Then $g_2' + g = g_2' + f_p$, i.e. (27) is trivially true.

Induction hypothesis for p: For $p := \bar p$ and arbitrary $g, g_2', f_0, \dots, f_{\bar p}$: if (24)-(26) are satisfied then (27) is also true.

Now consider $p := \bar p + 1$ and arbitrary g, g_2', $f_0, \dots, f_{\bar p + 1}$. Assume (24)-(26).

By induction hypothesis on p we have

(40) $g_2' + g \overset{succ}{\nabla} g_2' + f_{\bar p}$.

Furthermore, of course, we have

(41) $f_{\bar p} \to^1 f_{\bar p + 1}$ and, by (24) and (26),

(42) $Hterm(g_2' + f_{\bar p}) <_T Hterm(h)$.

From (41) and Lemma 2.4, (R1) we get

(43) $g_2' + f_{\bar p} \overset{succ}{\nabla} g_2' + f_{\bar p + 1}$.

From (40) and (43) we have

(44) $g_2' + g \to \underset{\sim}{\hat h}$, $g_2' + f_{\bar p} \to \underset{\sim}{\hat h}$ and

(45) $g_2' + f_{\bar p} \to \underset{\sim}{\hat{\hat h}}$, $g_2' + f_{\bar p + 1} \to \underset{\sim}{\hat{\hat h}}$ for some $\hat h$, $\hat{\hat h}$.

Now, by (42), (44), (45) and the induction hypothesis (1)

(46) $\hat h = \hat{\hat h}$.

So, finally, we have

(47) $g_2'+g \overset{succ}{\nabla} g_2'+f_{\bar{p}+1}$.

Case II b: h is M-reduced to h_2 by an M-reduction of the following kind:

h = Head(h) + Rest(h) ->

$\rightarrow \mathrm{Head}(h)+g_1' \xrightarrow[\mathrm{Hterm}(h),i_k]{1} g_2''+g_1' \rightarrow h_2$

($2 \leq k \leq m$), where

(48) $\mathrm{Rest}(h) \rightarrow g_1'$,

(49) $\mathrm{Head}(h) \xrightarrow[\mathrm{Hterm}(h),i_k]{1} g_2''$,

(50) $g_2''+g_1' \rightarrow h_2$.

For showing that $h_2=\bar{h}$ consider the following M-reduction

h = Head(h) + Rest(h) ->

$\rightarrow \mathrm{Head}(h)+g_1' \xrightarrow[\mathrm{Hterm}(h),i_1]{1} g_2'+g_1' > h_3$, where

(51) $\mathrm{Head}(h) \xrightarrow[\mathrm{Hterm}(h),i_1]{} g_2'$,

(52) $g_2' + g_1' \rightarrow h_3$.

From Case IIa we know that

(53) $h_3 = \bar{h}$.

We now show that

(54) $g_2'' + g_1' \overset{succ}{\nabla} g_2' + g_1'$.

For this purpose we observe that

(55) $g_2'' + g_1' - (g_2' + g_1') = g_2'' - g_2' =$

$$= \left(\mathrm{Head}(h) - \frac{\mathrm{Hcoef}(h)}{\mathrm{Hcoef}(F_{i_k})} \cdot \frac{\mathrm{Hterm}(h)}{\mathrm{Hterm}(F_{i_k})} \cdot F_{i_k}\right) - \left(\mathrm{Head}(h) - \frac{\mathrm{Hcoef}(h)}{\mathrm{Hcoef}(F_{i_1})} \cdot \frac{\mathrm{Hterm}(h)}{\mathrm{Hterm}(F_{i_1})} \cdot F_{i_1}\right) =$$

$$= \frac{\mathrm{Hcoef}(h)}{\mathrm{Hcoef}(F_{i_1}).\mathrm{Hcoef}(F_{i_k})} \cdot \left(\mathrm{Hcoef}(F_{i_k}) \cdot \frac{\mathrm{Hterm}(h)}{\mathrm{Hterm}(F_{i_1})} \cdot F_{i_1} - \mathrm{Hcoef}(F_{i_1}) \cdot \frac{\mathrm{Hterm}(h)}{\mathrm{Hterm}(F_{i_k})} \cdot F_{i_k}\right) =$$

$$= \frac{\mathrm{Hcoef}(h)}{\mathrm{Hcoef}(F_{i_1}).\mathrm{Hcoef}(F_{i_k})} \cdot (\mathrm{Hcoef}(F_{i_k}) \cdot \frac{\mathrm{Hterm}(h)}{\mathrm{Lcm}(\mathrm{Hterm}(F_{i_1}),\mathrm{Hterm}(F_{i_k}))} \cdot \frac{\mathrm{Lcm}(\mathrm{Hterm}(F_{i_1}),\mathrm{Hterm}(F_{i_k}))}{\mathrm{Hterm}(F_{i_1})} \cdot F_{i_1} -$$

$$- \mathrm{Hcoef}(F_{i_1}) \cdot \frac{\mathrm{Hterm}(h)}{\mathrm{Lcm}(\mathrm{Hterm}(F_{i_1}),\mathrm{Hterm}(F_{i_k}))} \cdot \frac{\mathrm{Lcm}(\mathrm{Hterm}(F_{i_1}),\mathrm{Hterm}(F_{i_k}))}{\mathrm{Hterm}(F_{i_k})} \cdot F_{i_k}) =$$

$$= \frac{\mathrm{Hcoef}(h)}{\mathrm{Hcoef}(F_{i_1}).\mathrm{Hcoef}(F_{i_k})} \cdot \frac{\mathrm{Hterm}(h)}{\mathrm{Lcm}(\mathrm{Hterm}(F_{i_1}),\mathrm{Hterm}(F_{i_k}))} \cdot \mathrm{Spol}(F_{i_1},F_{i_k}).$$

Now, from the assumption (G2) we know

(56) $\mathrm{Spol}(F_{i_1},F_{i_k}) \rightarrow 0$.

Therefore

(57) $(g_2'' + g_1') - (g_2' + g_1') \rightarrow 0$

and from this, by Lemma 2.4, (R3) we get (54), i.e.

(58) $g_2'' + g_1' \rightarrow \hat{h}$, $g_2' + g_1' \rightarrow \hat{h}$ for some $\hat{h}$.

By the induction hypothesis (1) and (52), (53), (58) we get

(59) $\hat{h} = \bar{h}$,

and again by the induction hypothesis (1) and (50), (58), (59) we get

(60) $h_2 = \hat{h} = \bar{h}$, q.e.d.

3.6. Proof of Theorem 3.3.

(G3) $\longrightarrow$ (G1):

Sketch:

We show that every $g \in \mathrm{Ideal}(F)$ may be M-reduced to 0. Hence, there cannot exist a $g \neq 0$ in Ideal(F) that is in normalform.
The proof is carried out by induction (with respect to $<_T$) on terms that are maximal among the terms in $h_1.F_1, h_2.F_2, \ldots, h_l.F_l$ needed to represent some polynomial $g \in \mathrm{Ideal}(F)$ by $g=h_1.F_1+\ldots+h_l.F_l$ ($l=L(F)$).

Details:

Let $l := L(F)$.
Assume (G3). We shall show that

(1) $\bigwedge_t \bigwedge_{h_1,\ldots,h_l,g} \left(\bigwedge_{1\leq j\leq l} (h_j=0 \vee F_j=0 \vee \mathrm{Hterm}(h_j.F_j) <_T t) \text{ and } g=h_1.F_1+\ldots+h_l.F_l \longrightarrow g \rightarrow 0\right).$

From this it follows that

$\bigwedge_g (g \in \mathrm{Ideal}(F) \longrightarrow g \rightarrow 0)$

wherefrom (G1) is immediate.

For showing (1) we use induction on t.

Induction basis: $t := x_1^0 \ldots x_n^0$.

In this case $\mathrm{Hterm}(h_j.F_j) <_T t$ is not possible, i.e. the only possibility remaining in this case is that g has a representation $g = \sum_{1\leq j\leq l} h_j.F_j$ with $\bigwedge_{1\leq j\leq l} (h_j=0 \vee F_j=0)$,

i.e. $g=0$, and therefore $g \rightarrow 0$.

Induction hypothesis: For some fixed t:

(2) $\bigwedge_{h_1,\dots,h_l,g} \Big(\bigwedge_{1\le j\le l} (h_j=0 \vee F_j=0 \vee$
$\vee\, Hterm(h_j.F_j) <_T t)$
$g = \sum_{1\le j\le l} h_j.F_j \longrightarrow g \to 0\Big)$.

We shall show

(3) $\bigwedge_{h_1,\dots,h_l,g} \Big(\bigwedge_{1\le j\le l} (h_j=0 \vee F_j=0 \vee$
$\vee\, Hterm(h_j.F_j) \le_T t)$
$g = \sum_{1\le j\le l} h_j.F_j \longrightarrow g \to 0\Big)$.

by showing that for all $m, i_1,\dots,i_m$, $h_1,\dots,h_l,g$: if

(4) $1\le m\le l$, $\bigwedge_{1\le j\le m} 1\le i_j\le l$, $\bigwedge_{1\le j,k\le m} (j\ne k \longrightarrow i_j\ne i_k)$

(5) $\bigwedge_{1\le j\le m} (h_{i_j}\ne 0 \wedge F_{i_j}\ne 0 \wedge Hterm(h_{i_j}.F_{i_j}) = t)$

(6) $\bigwedge_{i\notin\{i_1,\dots,i_m\}} (h_i=0 \vee F_i=0 \vee$
$\vee\, Hterm(h_i,F_i) <_T t)$

(7) $g = \sum_{1\le j\le l} h_j.F_j$

then

(8) $g \to 0$.

We show this by induction on m.

Induction basis: $m=1$:

In this case we have

(9) $g = h_{i_1}.F_{i_1} + \sum_{\substack{1\le j\le l\\ j\ne i_1}} h_j.F_j \;\to^1_{t,i_1}$

$\to^1_{t,i_1}\; Rest(h_{i_1}).F_{i_1} + \sum_{j\ne i_1} h_j.F_j =: g'$

Since (by(5))

(10) $h_{i_1}\ne 0 \wedge F_{i_1}\ne 0 \wedge Hterm(h_{i_1},F_{i_1}) = t$

we have

(11) $Rest(h_{i_1})=0 \vee Hterm(Rest(h_{i_1}).F_{i_1}) <_T t$.

(Note that this is true also in case $t = x_1^0\dots x_n^0$.)

From (6) and (11) we see that the induction hypothesis (2) is applicable to g' so that $g \to g' \to 0$ and, therefore $g \to 0$.

Induction hypothesis: For all $m\le\bar m$ $(\bar m\ge 1)$ and all $i_1,\dots,i_m,h_1,\dots,h_l,g$: if (4)-(7) is satisfied then $g \to 0$.

Now we assume that for some $i_1,\dots,i_{\bar m+1}$, $h_1,\dots,h_l,g$

(12) $1\le \bar m+1\le l$, $\bigwedge_{1\le j\le \bar m+1} 1\le i_j\le l$, $\bigwedge_{\substack{1\le j,k\le \bar m+1\\ j\ne k}} i_j\ne i_k$

(13) $\bigwedge_{1\le j\le \bar m+1} (h_{i_j}\ne 0 \wedge F_{i_j}\ne 0 \wedge Hterm(h_{i_j}.F_{i_j}) = t)$

(14) $\bigwedge_{i\notin\{i_1,\dots,i_{\bar m+1}\}} (h_i=0 \vee F_i=0 \vee$
$\vee\, Hterm(h_i.F_i) <_T t)$

(15) $g = \sum_{1\le j\le l} h_j.F_j$.

Define

$$a := -\frac{Hcoef(h_{i_1}).Hcoef(F_{i_1}) + Hcoef(h_{i_2}).Hcoef(F_{i_2})}{Hcoef(F_{i_2})}$$

$$b := \frac{Hcoef(h_{i_1})}{Hcoef(F_{i_2})} \quad \text{and}$$

$$s := \frac{t}{Lcm(Hterm(F_{i_1}),Hterm(F_{i_2}))}$$

It is easy to check that

(16) $Head(h_{i_1}).F_{i_1} + (Head(h_{i_2}) + a.Hterm(h_{i_2})).$
$.F_{i_2} = b.s.Spol(F_{i_1},F_{i_2})$.

This yields the following representation of g

(17) $g = h_{i_1}.F_{i_1} + h_{i_2}.F_{i_2} + \sum_{\substack{j=1\\ j\ne i_1,i_2}}^{l} h_j.F_j =$

$= Head(h_{i_1}).F_{i_1} +$
$+ (Head(h_{i_2}) + a.Hterm(h_{i_2})).F_{i_2} + g'$

where

(18) $g' := Rest(h_{i_1}).F_{i_1} + Rest(h_{i_2}).F_{i_2} -$
$- a.Hterm(h_{i_2}).F_{i_2} + \sum_{\substack{j=1\\ j\ne i_1,i_2}}^{l} h_j.F_j$

g' has a representation that satisfies the requirements (4)-(7) of the induction hypothesis for some $m\le\bar m$ or even satisfies the premise in (2). So

(19) $g' \to 0$.

By (16), (17)

(20) $g - g' = b.s.Spol(F_{i_1},F_{i_2})$.

Now from (G3) we can deduce

(21) $\bigwedge_{1\le i,j\le l} Spol(F_i,F_j) \to 0$.

To show this take i,j with $1\le i,j\le l$. There exists an $\hat{h}$ such that

(22) $f_{left} :=$
$:= Hcoef(F_j).\dfrac{Lcm(Hterm(F_i),Hterm(F_j))}{Hterm(F_i)}.F_i \to^1$
$\to^1_{Lcm(Hterm(F_i),Hterm(F_j)),j}\; Spol(F_i,F_j) \to \hat{h}$

On the other hand,

(23) $f_{left\ Lcm(Hterm(F_i),Hterm(F_j)),i} \overset{1}{\to} \underset{\sim}{\hat{h}}$

So because of (G3)

(24) $\hat{h} = 0$

such that (21) may be seen from (22).

From (21) and (20) we have

(25) $g - g' \to 0$,

and, hence, using Lemma 2.4., (R3)

(26) $g \overset{succ}{\nabla} g'$.

Assume

(27) $g \to \underset{\sim}{\hat{h}},\ g' \to \underset{\sim}{\hat{h}}$

for some $\hat{h}$. Then

(28) $\hat{h} = 0$

by (19) and (G3), so by (27)

(29) $g \to 0$.

In the next proposition we list some easy consequences of Theorem 3.3. which give some further characterizations of G-bases.

3.7. Proposition:

The following statements are equivalent:

(G1) F is a Gröbner-basis.

(G4) $\bigwedge_{g,h} (g \in Ideal(F),\ g \to \underset{\sim}{h} \longrightarrow h=0)$
(i.e. all normalforms of polynomials in Ideal(F) are zero)

(G5) $\bigwedge_{g} (g \in Ideal(F) \longleftrightarrow \bigwedge_{h} (g \to \underset{\sim}{h} \longrightarrow h=0))$
(i.e. polynomials are in Ideal(F) iff all normalforms of them are zero)

(G6) $\bigwedge_{g} (g \in Ideal(F) \longleftrightarrow g \to 0)$
(i.e. polynomials are in Ideal(F) iff they are M-reducible to zero)

(G7) $\bigwedge_{1 \le i,j \le L(F)} \bigwedge_{g} (Spol(F_i,F_j) \to \underset{\sim}{g} \longrightarrow g=0)$
(i.e. all normalforms of all S-polynomials of F_i and F_j are zero).

3.8. Proof:

(G1) $\longrightarrow$ (G4):

From $g \in Ideal(F)$ and $g \to \underset{\sim}{h}$ we infer $h \in Ideal(F)$ and Normalf(h). Thus by (G1) $h=0$.

(G4) $\longrightarrow$ (G5):

" $\longrightarrow$ ": From $g \in Ideal(F)$ and $g \to \underset{\sim}{h}$ follows $h=0$ by (G4).

" $\longleftarrow$ ": Assume $\bigwedge_{h} (g \to \underset{\sim}{h} \longrightarrow h=0)$.
Take some $\hat{h}$ such that $g \to \underset{\sim}{\hat{h}}$ (at least one such $\hat{h}$ can always be constructed by the algorithm in 2.2.).
Then $\hat{h}=0$, i.e. $g \to 0$ and, therefore $g \in Ideal(F)$.

(G5) $\longrightarrow$ (G6):

" $\longrightarrow$ ": Take an $\hat{h}$ such that $g \to \underset{\sim}{\hat{h}}$. Then $\hat{h}=0$ by (G5). Thus, $g \to 0$.

" $\longleftarrow$ ": Immediate.

(G6) $\longrightarrow$ (G1):

Assume $g \in Ideal(F)$, Normalf(g). Then $g \to 0$ by (G6) and, therefore, $g=0$.

(G1) $\longrightarrow$ (G7):

By (G2) and (G3) in Theorem 3.3.

(G7) $\longrightarrow$ (G1):

Take some $\hat{g}$ such that $Spol(F_i,F_j) \to \underset{\sim}{\hat{g}}$. Then $\hat{g}=0$ by (G7). Thus, $Spol(F_i,F_j) \to 0$. (G1), then, follows by (G2) in Theorem 3.3.

4. Conclusions:

(G2) of Theorem 3.3 is the key to an effective method for constructing Gröbner-bases for an ideal generated by a basis F: in one step produce the S-polynomial of F_i and F_j and M-reduce this polynomial. If it is M-reduced to 0 proceed to the next combination of indices i,j. If not augment the basis by the result of the M-reduction. A detailed description of this method together with a termination proof is given in [2].
This algorithm has been programed several times, see [1] and [8]. No theoretical bounds on the number of steps are known so far, except in the case $K[x,y]$, where we know how to determine a bound for the highest degree of the terms appearing during the algorithm, see [1]. However, we think that one should first concentrate more on establishing criterions in the style of S1 and S2 in [2], which reduce the complexity of the algorithm rather than trying to obtain complexity estimations for crude versions of the algorithm.

Acknowledgement:

This paper had not been written without the encouragement of Prof.R.Loos (Kaiserslautern). My work on the problems discussed in this paper still profits by the personal instructions of my former teacher, Prof. W. Gröbner (Innsbruck). I express my sincere gratitude to both of them.

References:

[1] B. Buchberger, Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal, Dissertation, Universität Innsbruck, 1965.

[2] B. Buchberger, Ein algorithmisches Kriterium für die Lösbarkeit eines algebraischen Gleichungssystems, Aequationes mathematicae, Vol. 4/3,S. 374-383, 1970.

[3] B. Buchberger, On Certain Bases of Polynomial Ideals, Bericht Nr. 53, Institut für Mathematik, Universität Linz.

[4] W. Gröbner, Personal communication, Seminar d. Institutes für Mathematik, Universität Innsbruck, 1964.

[5] M. Lauer, Canonical Representatives for Residue Classes of a Polynomial Ideal, to appear in the Proceedings of the SIGSAM Conference 1976, ACM.

[6] R. Loos, Toward a Formal Implementation of Computer Algebra, SIGSAM Bulletin, 8, p. 9-16, 1974.

[7] Z. Manna, Mathematical Theory of Computation, Mc Graw Hill, 1974.

[8] R. Schrader, Diplomarbeit, Math. Institut, Universität Karlsruhe, 1976.

Editor's Note

You may want to memorize the next column before reading Korpela's paper.

The first 13 pages of this issue were prepared by the Conference Chairman Dr. James Griesmer. Thanks to him. The unexpected number of contributions to the conference is one reason for the size of 48 pages of this issue. The other reason is that I did not insist on retyping the ANALITIK contribution on ACM model paper because of the number of different alphabets (e.g.Cyrillic) involved. Since the former issue had only 32 pages I hope the size of this issue can be justified. We have a backlog of some 30 more abstracts and two contributions, 11 pages each. One from Marseille on symbolic integration via predicate logic.

Nevertheless I would like to encourage more contributions to the discussion section, to the problem section, more class room notes, more news on personal items and systems.

Please note also the change of my address on the first inside cover.

R. Loos

(Page 43 continued)

"ВЫПОЛНИТЬ"	execute, do
"ВЫЧИСЛИТЬ"	compute, evaluate
"ГДЕ"	where
"ГРАФИК"	graph
"ДЕЛИТЬ"	divide
"ДИФФЕРЕНЦИРОВАТЬ"	differentiate
"ДЛЯ"	for
"ДО"	until
"ДРОБИ"	fractions
"ЕСЛИ"	if
"ЗАГОЛОВКА"	heading
"ЗАПИСАТЬ"	write
"ЗНАЧЕНИЕ"	value
"И"	and
"ИДТИ", "ИТТИ"	go
"ИЛИ"	or
"ИНАЧЕ"	else
"ИНТЕГРИРОВАТЬ"	integrate
"КОНЕЦ"	end
"ЛЕВАЯ"	left
"МАССИВ"	array
"МАСШТАБ"	scale
"НА"	to, go to
"НАЗВАТЬ"	define
"НЕ"	not
"ОПИСАНИЕ"	description, definition
"ОЧИСТИТЬ"	clean
"ПОЛОЖИТЬ"	place, assign
"ПРАВАЯ"	right
"ПРИ"	at
"ПРИМЕНИТЬ"	apply
"ПРИВЕСТИ"	simplify
"ПРОБЕЛ"	blank
"ПРОЦЕДУРА"	procedure
"ПУСТЬ"	let
"РАЗРЯДНРСТЬ"	capacity, number of digits
"СРАВНИТЬ"	compare
"СТЕРЕТЬ"	erase
"СТОП"	stop
"СТРОКА"	line
"ТАБЛИЦА"	table
"ТО"	then
"ФОРМАТ"	format, line breadth
"ЧАСТЬ"	part, side
"ЧИСЛО"	number
"ШАГ"	step
"ЭКРАН"	screen