記 号 処 理 38－2
（1986. 9. 16）

加群のGröbner基底と連立線形方程式の多項式解

古川昭夫（都立大・数学）　佐々木建昭（理化学研究所）　小林英恒（日大・数学）

多項式を要素とする次元rのS個のベクトルを$\vec{f}_i = (f_{i1}, \cdots, f_{ir})$, $i=1,\cdots,s$, とする。ただし，Kを体とするとき，$f_{i1}, \cdots, f_{ir} \in K[x_1, \cdots, x_n]$ とする。$\vec{f}_1, \cdots, \vec{f}_s$ から生成される $K[x_1, \cdots, x_n]$ 上の加群を $\vec{I} = (\vec{f}_1, \cdots, \vec{f}_s)$ と表わす。すなわち，$\vec{I}$ の任意の要素 $\vec{f}$ は $\vec{f} = \sum_{i=1}^{s} h_i \vec{f}_i$, ただし $h_i \in K[x_1, \cdots, x_n]$, と表わされる。本論文では加群 $\vec{I}$ のGröbner基底の理論を構成する。この理論の応用の一つとして，未知数 $y_1, \cdots, y_s$ に対する連立線形方程式 $y_1 f_{1i} + \cdots + y_s f_{si} = f_{0i}$, $i=1, \cdots, r$, の多項式解 $y_1, \cdots, y_s \in K[x_1, \cdots, x_n]$ の効率的な計算法を提出する。

Gröbner Basis of a Module over $K[x_1,\ldots,x_n]$ and Polynomial Solutions of a System of Linear Equations

A. Furukawa*), T. Sasaki**), H. Kobayashi***)

*) Department of Mathematics, Tokyo Metropolitan University
**) The Institute of Physical and Chemical Research
***) Department of Mathematics, Nihon University

Abstract

Let $\vec{f}_i = (f_{i1},\ldots,f_{ir})$, $i=1,\ldots,s$, be r-dimensional vectors, where $f_{i1}, \ldots, f_{ir}$ are polynomials in $K[x_1,\ldots,x_n]$ with K a field. Let $\vec{I} = (\vec{f}_1,\ldots,\vec{f}_s)$ be a module over $K[x_1,\ldots,x_n]$ generated by $\vec{f}_1, \ldots, \vec{f}_s$, i.e., an element $\vec{f}$ of $\vec{I}$ is of the form $\vec{f} = \sum_{i=1}^{s} h_i \vec{f}_i$, with $h_i \in K[x_1,\ldots,x_n]$. This paper develops a theory of Gröbner basis of the module $\vec{I}$. As an application of the Gröbner basis theory for $\vec{I}$, we construct an efficient method for solving a system of linear equations $y_1 f_{1i} + \cdots + y_s f_{si} = f_{0i}$, $i=1,\ldots,r$, where unknowns $y_1, \ldots, y_s$ are in $K[x_1,\ldots,x_n]$.

§1. Introduction

In discussing polynomial ideals and related problems, the Gröbner bases are very useful ideal bases [1]. For example, ref. [2] lists many problems which can be solved by using Gröbner bases within reasonable computation steps. In this paper, we show that a simple generalization of the Gröbner basis for polynomial ideal allows us to solve the following system of linear equations efficiently:

$$\begin{cases} y_1 f_{11} + \cdots + y_s f_{s1} = f_{01}, \\ \quad \cdots \\ y_1 f_{1r} + \cdots + y_s f_{sr} = f_{0r}, \end{cases} \tag{1}$$

where $f_{ij} \in K[x_1,\ldots,x_n]$, $i=0,\ldots,s$, $j=1,\ldots,r$, and the solutions $y_1, \ldots, y_s$ are in $K[x_1,\ldots,x_n]$.

In the case of a single equation $y_1 f_1 + \cdots + y_s f_s = f_0$, $f_i \in K[x_1,\ldots,x_n]$, $i=0,\ldots,s$, an efficient method was found which we call the Gröbner basis method, because the method is closely related to the calculation of a Gröbner basis of the ideal $(f_1,\ldots,f_s)$, see [2,3]. Using this Gröbner basis method, we can solve the above system (1) iteratively by solving one equation and substituting the unknowns by the result in yet unsolved equations (successive substitution method).

However, as for a system of linear equations, we know the famous formula by Cramer for the solutions in $K(x_1,\ldots,x_n)$. Recently, one of the authors derived a determinant form formula for the solutions in $K(x_1,\ldots,x_{n-1})[x_n]$, see [4]. In these formulas, all the equations of the system are treated equally and the linear system is solved efficiently.

In this paper, we derive an efficient resolution method for the solutions in $K[x_1,\ldots,x_n]$, by treating all the equations of (1) simultaneously. Here, by an efficient method we mean a more efficient method than the successive substitution using the Gröbner basis. The new method is an analogue of the Gröbner basis method for a single equation, and it is obtained by extending the Gröbner basis theory to a module over $K[x_1,\ldots,x_n]$.

In §2, we define basic concepts. The Gröbner basis theory is extended to a module in §3, where we use a similar formulation of Gröbner basis as in our previous paper [5] because of its apparent simplicity. In §4, we describe an efficient resolution method for the linear system (1). A simple example and discussion are given in §5.

§2. Definitions of monoideal and order

Let $\mathbb{Z}_0$ be the set of nonnegative integers, and $\mathbb{Z}_0^n$ the Cartesian product of $\mathbb{Z}_0$ with n a positive integer. An element A of $\mathbb{Z}_0^n$ is written as $(\alpha_1,\ldots,\alpha_n)$ and we define $|A| = \alpha_1 + \cdots + \alpha_n$. We write $(0,\ldots,0)$ as 0. Let $K[x_1,\ldots,x_n]$ be the ring of polynomials in n variables $x_1, \ldots, x_n$ with coefficients in a field K. We abbreviate $K[x_1,\ldots,x_n]$ to $K[x]$. We express f in $K[x]$ as $f = \sum_A a_A x^A$, where $A = (\alpha_1,\ldots,\alpha_n)$, $a_A \in K$, and x^A is an abbreviation of $x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n}$. We call $\alpha_1 + \cdots + \alpha_n$ the degree of a term x^A, i.e., $\deg(x^A) = |A|$.

Let $(\mathbb{Z}_0^n)^r$ be the set of r-dimensional vectors with their components in $\mathbb{Z}_0^n$. We denote an element of $(\mathbb{Z}_0^n)^r$ as $\vec{A} = (A_1,\ldots,A_r)$. Similarly, by $(K[x])^r$ we mean the set of r-dimensional vectors with their components in $K[x]$. An element of $(K[x])^r$ is denoted as $\vec{f} = (f_1,\ldots,f_r)$, where

$f_i \in K[x]$, i=1,...,r. In particular, we write (0,...,0) as $\vec{0}$.

Let $\vec{S} = (S_1,...,S_r)$ and $\vec{T} = (T_1,...,T_r)$ be r-dimensional vectors of sets, i.e., S_1, ..., S_r, and T_1, ..., T_r are sets. In particular, we write $(\phi,...,\phi)$ as $\vec{\phi}$. Then, union and intersection of $\vec{S}$ and $\vec{T}$ are defined as

$$\vec{S} \cup \vec{T} = (S_1 \cup T_1, \ \ldots \ , S_r \cup T_r),$$

$$\vec{S} \cap \vec{T} = (S_1 \cap T_1, \ \ldots \ , S_r \cap T_r).$$

Furthermore, if $\vec{A} = (A_1,...,A_r)$ is such that $A_1 \in S_1$, ..., and $A_r \in S_r$, then we write $\vec{A} \in \vec{S}$.

Definition 1 [monoideal].

A subset I_M of $\mathbb{Z}_0^n$ is a monoideal if $I_M + \mathbb{Z}_0^n = I_M$. □

Proposition 1. (For the proof, see [5].)

A monoideal I_M is finitely generated. That is, there exist a finite number of elements A_1, ..., A_s in I_M satisfying

$$I_M = \bigcup_{i=1}^{s} (A_i + \mathbb{Z}_0^n). \ \square$$

Definition 2 [total-degree lexicographic order $\rhd$ in $\mathbb{Z}_0^n$].

For any elements $A = (\alpha_1,...,\alpha_n)$ and $B = (\beta_1,...,\beta_n)$ of $\mathbb{Z}_0^n$, we define $A \rhd B$ iff either $|A| > |B|$ or $|A| = |B|$ and there is an integer i, $1 \leq i \leq n$, such that $\alpha_j = \beta_j$ for all j, $1 \leq j < i$, and $\alpha_i > \beta_i$. We define $A \trianglerighteq$ iff $A \rhd B$ or $A = B$. □

Example 1. In $\mathbb{Z}_0^3$, $(0,0,4) \rhd (3,0,0) \rhd (2,1,0) \rhd (1,2,0) \rhd (1,1,1) \rhd (0,3,0) \rhd (0,2,1) \rhd (0,1,2) \rhd (0,0,3) \rhd (2,0,0)$, and so on.

Proposition 2. The order $\rhd$ is Noetherian in descending direction, i.e., any descending chain $A_1 \rhd A_2 \rhd A_3 \rhd \cdots$ is always finite.

Proof. Let A be any element of $\mathbb{Z}_0^n$ with $|A| = d$. Then, the number of elements in $\mathbb{Z}_0^n$ which are less than A in the order $\rhd$ is at most $(d+1)^n$. □

Proposition 3. The order $\rhd$ is consistent with addition of elements of $\mathbb{Z}_0^n$.

Proof. Let A, B, C, D be any elements of $\mathbb{Z}_0^n$ satisfying $A \rhd B$ and $C \trianglerighteq D$. Then, obviously $A + C \rhd B + D$. □

Note. The following theory is valid for other definitions of order $\rhd$ so far as Props. 2 and 3 hold. In particular, the lexicographic order is important in many practical calculations.

Definition 3 [exponent set, leading exponent, head term].

Let f be a nonzero element of K[x]. Exponent set of f, leading exponent of f, and head term of f, which are abbreviated to exs(f), lex(f), and ht(f), respectively, are defined as follows:

$$\mathrm{exs}(f) = \{A \in \mathbb{Z}_0^n \mid A \text{ in } f = \textstyle\sum a_A x^A, \ a_A \neq 0\},$$

$$\mathrm{lex}(f) \in \mathrm{exs}(f), \ \mathrm{lex}(f) \rhd \text{any other element of exs}(f),$$

$$\mathrm{ht}(f) = \text{a term } a_A x^A \text{ of f, where } A = \mathrm{lex}(f).$$

We define $\mathrm{exs}(0) = \phi$, $\mathrm{lex}(0) = \phi$, and $\mathrm{ht}(0) = 0$, and we consider for convenience that $\phi \lhd (0,...,0)$. □

Definition 4 [highest-order smallest-suffix component order $\rhd$ in $(\mathbb{Z}_0^n)^r$].

Let $\vec{A} = (A_1,...,A_r)$ and $\vec{B} = (B_1,...,B_r)$ be any elements of $(\mathbb{Z}_0^n)^r$. We reorder the components of $\vec{A}$ and define $\vec{A}' = (A_{i_1},...,A_{i_r})$ as follows: $\{i_1,...,i_r\} = \{1,...,r\}$ and $A_{i_1} \trianglerighteq A_{i_2} \trianglerighteq \cdots \trianglerighteq A_{i_r}$, where $\ell < m$ for any (ℓ,m) such that $A_{i_\ell} = A_{i_m}$. Similarly, we define $\vec{B}' = (B_{j_1},...,B_{j_r})$ by reordering the components of $\vec{B}$ as described above. Then, we define $\vec{A} \rhd \vec{B}$ iff there is an integer k, $1 \leq k \leq r$, such that $[A_{i_\ell} = B_{j_\ell}$ and $i_\ell = j_\ell$ for all ℓ, $1 \leq \ell < k]$ and [either $A_{i_k} \rhd B_{j_k}$ or $A_{i_k} = B_{j_k}$ with $i_k < j_k$]. We define

$\vec{A} \geqq \vec{B}$ iff $\vec{A} \rhd \vec{B}$ or $\vec{A} = \vec{B}$. □

Note. We called the above order the highest-order smallest-suffix component order because A_{i_1} and B_{j_1} are the leading components in determining the order.

Example 2. In $(\mathbb{Z}_0^3)^2$, $((1,1,1), (0,2,0)) \rhd ((2,0,0), (1,1,1)) \rhd$

$\rhd ((0,3,0), (0,2,1)) \rhd ((2,0,0), (1,1,0)) \rhd ((2,0,0), (0,0,1))$.

Notes. We can define an order in $(\mathbb{Z}_0^n)^r$ from the order $\rhd$ in $\mathbb{Z}_0^n$ variously, and the above definition is only one choice among many possible definitions. For example, we may define the nonzero smallest-suffix component to be the leading component of $\vec{A}$. When solving a system of linear equations, however, the efficiency of calculation depends crucially on choice of the order. The above definition is the most appropriate choice for solving the system of linear equations. We discuss this point again in §5.

Proposition 4. The order $\rhd$ in $(\mathbb{Z}_0^n)^r$ is Noetherian in descending direction, i.e., any descending chain $A_1 \rhd A_2 \rhd A_3 \rhd \cdots$ is always finite.

Proof. Let $\vec{A} = (A_1,\ldots,A_r)$ be any element of $(\mathbb{Z}_0^n)^r$ with $\max\{|A_1|,\ldots,|A_r|\} = d$. Then, the number of elements in $(\mathbb{Z}_0^n)^r$ which are less than $\vec{A}$ in the order $\rhd$ is at most $(d+1)^{nr}$. □

Proposition 5. The order $\rhd$ is consistent with addition of elements of $(\mathbb{Z}_0^n)^r$.

Proof. Let A, B, C, D be any elements of $(\mathbb{Z}_0^n)^r$ satisfying $A \rhd B$ and $C \geqq D$. Then, obviously $A + C \rhd B + D$. □

Definition 5 [head term, head position, and rest of $\vec{f}$].

Let $\vec{f} = (f_1,\ldots,f_r)$ be an element of $(K[x])^r$. Put $A_i = \mathrm{lex}(f_i)$, $i=1,\ldots,r$, and let A_k be the highest-order smallest-suffix component of $(A_1,\ldots,A_r)$, i.e., A_{i_1} in Def. 4. Then, head term of $\vec{f}$, head position of $\vec{f}$, and rest of $\vec{f}$, which are abbreviated to $\mathrm{ht}(\vec{f})$, $\mathrm{hp}(\vec{f})$, and $\mathrm{rest}(\vec{f})$, respectively, are defined as follows:

$$\mathrm{ht}(\vec{f}) = \mathrm{ht}(f_k),$$

$$\mathrm{hp}(\vec{f}) = k,$$

$$\mathrm{rest}(\vec{f}) = \vec{f} - (0,\ldots,0,\ \underset{\substack{\uparrow\\ k\text{-th component}}}{\mathrm{ht}(\vec{f})}\ ,0,\ldots,0). \quad \square$$

It is obvious that $\mathrm{lex}(\vec{f}) \rhd \mathrm{lex}(\mathrm{rest}(\vec{f}))$ if $\vec{f} \neq \vec{0}$. In the following, we say $\vec{f}$ is higher order than $\vec{g}$ if $\mathrm{lex}(\vec{f}) \rhd \mathrm{lex}(\vec{g})$.

Example 3. Let $\vec{f} = (xy^4-1,\ x^2y^2,\ xy^4-x)$, then $\mathrm{ht}(\vec{f}) = xy^4$ and $\mathrm{hp}(\vec{f}) = 1$.

Let $\vec{g} = (xy^4-y,\ x^2y^3-1,\ xy^4-1)$, then $\mathrm{ht}(\vec{g}) = x^2y^3$ and $\mathrm{hp}(\vec{g}) = 2$.

Definition 6 [exponent set, leading exponent, and lex-monoideal of $\vec{f}$].

With the notations in Def. 5, exponent set of $\vec{f}$, leading exponent of $\vec{f}$, and lex-monoideal of $\vec{f}$, which are r-dimensional vectors and abbreviated to $\mathrm{exs}(\vec{f})$, $\mathrm{lex}(\vec{f})$, and $\mathrm{lmo}(\vec{f})$, respectively, are defined as follows:

$$\mathrm{exs}(\vec{f}) = (\mathrm{exs}(f_1),\ldots,\mathrm{exs}(f_r)),$$

$$\mathrm{lex}(\vec{f}) = (0,\ldots,0,\ \mathrm{lex}(f_k)\ ,0,\ldots,0),$$

$$\mathrm{lmo}(\vec{f}) = (\phi,\ldots,\phi,\ \underset{\substack{\uparrow\\ k\text{-th component}}}{\mathrm{lex}(f_k)+\mathbb{Z}_0^n}\ ,\phi,\ldots,\phi). \quad \square$$

§3. Gröbner basis of a module over $K[x_1,\ldots,x_n]$

In this paper, by a module $\vec{I} = (\vec{f}_1,\ldots,\vec{f}_s)$ with $\vec{f}_i \in (K[x])^r$, $i=1,\ldots,s$,

we mean the set $\{h_1\vec{f}_1 + \cdots + h_s\vec{f}_s \mid h_i \in K[x],\ i=1,\ldots,s\}$.

Definition 7 [reducibility].

Let $F = \{\vec{f}_1,\ldots,\vec{f}_s\}$ be a subset of $(K[x])^r$, and put $\vec{E} = \bigcup_{i=1}^{s} \mathrm{lmo}(\vec{f}_i)$. An element $\vec{h}$ of $(K[x])^r$ is called reducible with respect to F if $\mathrm{exs}(\vec{h}) \cap \vec{E} \neq \vec{\phi}$, and $\vec{h}$ is called irreducible w.r.t. F if $\mathrm{exs}(\vec{h}) \cap \vec{E} = \vec{\phi}$. □

Definition 8 [reduction].

With the notations in Def. 7, let $\vec{h}' \in (K[x])^r$. The $\vec{h}'$ is called a reduction of $\vec{h}$ w.r.t. F and written as $\vec{h} \xrightarrow[F]{} \vec{h}'$ if one of the followings holds:

(a) $\vec{h}' = \vec{h}$ when $\vec{h}$ is irreducible w.r.t. F,

(b) $\vec{h}' = \vec{h} - c\cdot x^A\vec{f}_k$ when $\mathrm{exs}(\vec{h}) \cap \mathrm{lmo}(\vec{f}_k) \neq \vec{\phi}$,

where c and A are determined as follows: let $\mathrm{ht}(\vec{f}_k) = a_{A_k}x^{A_k}$, hence the $\mathrm{hp}(\vec{f}_k)$-th component of $\vec{h}$ contains a term proportional to x^{A_k} and let the term be $b_{A+A_k}x^{A+A_k}$ then $c = b_{A+A_k}/a_{A_k}$. In the case of (b), we call this reduction as genuine (one-step) reduction w.r.t. $\vec{f}_k$. □

Note. It is obvious that $\mathrm{lex}(\vec{h}) \geqq \mathrm{lex}(\vec{h}')$.

Definition 9 [normal form].

Suppose $\vec{h}$ in $(K[x])^r$ is reduced successively as $\vec{h} \xrightarrow[F]{} \vec{h}' \xrightarrow[F]{} \cdots \xrightarrow[F]{} \underline{\vec{h}}$, and if $\underline{\vec{h}}$ is irreducible w.r.t. F then $\underline{\vec{h}}$ is called a normal form of $\vec{h}$ w.r.t. F. We denote the above reduction sequence by $\vec{h} \xrightarrow[F]{*} \underline{\vec{h}}$. □

Example 4. Let $F = \{\vec{f}, \vec{g}\}$, where $\vec{f}$ and $\vec{g}$ are given in Example 3, and $\vec{h} = (xy^4, x^2y^3, xy^4)$. Then, $\vec{h}$ can be reduced w.r.t. F as follows:

$$\vec{h} \xrightarrow[F]{} (1,\ x^2y^3-x^2y^2,\ x) \quad \text{[reduction w.r.t. } \vec{f}\text{]}$$
$$\xrightarrow[F]{} (-xy^4+y+1,\ -x^2y^2+1,\ -xy^4+x+1) \quad \text{[reduction w.r.t. } \vec{g}\text{]}$$
$$\xrightarrow[F]{} (y,\ 1,\ 1) \quad \text{[reduction w.r.t. } \vec{f}\text{]}.$$

The last term (y, 1, 1) is irreducible w.r.t. F, and it is a normal form of $\vec{h}$.

Proposition 6. Let $F = \{\vec{f}_1,\ldots,\vec{f}_s\}$ be a subset of $(K[x])^r$. Given any element $\vec{h}$ of $(K[x])^r$, we can reduce $\vec{h}$ to a normal form $\underline{\vec{h}}$ w.r.t. F by a finite sequence of reductions.

Proof. We use induction on $\mathrm{lex}(\vec{h})$. When $\vec{h} = (0,\ldots,0)$, hence $\mathrm{lex}(\vec{h}) = (\phi,\ldots,\phi)$, $\vec{h}$ is already a normal form. Assume that the proposition is valid for any $\vec{g}$ such that $\mathrm{lex}(\vec{g}) \lhd \mathrm{lex}(\vec{h})$. Put $\vec{h} = \vec{h}_0 + \mathrm{rest}(\vec{h})$, and let

$$\text{(A)}: \vec{h} \xrightarrow[F]{} \vec{h}_1 \xrightarrow[F]{} \cdots \xrightarrow[F]{} \vec{h}_k \xrightarrow[F]{} \cdots$$

be a genuine reduction chain of $\vec{h}$ w.r.t. F, i.e., $\vec{h} \neq \vec{h}_1 \neq \cdots \neq \vec{h}_k \neq \cdots$. From definition of reduction, we get a descending chain

$$\text{(B)}: \mathrm{lex}(\vec{h}) = \mathrm{lex}(\vec{h}_0) \geqq \mathrm{lex}(\vec{h}_1) \geqq \mathrm{lex}(\vec{h}_2) \geqq \cdots$$

in $(\mathbb{Z}_0^n)^r$.

(Case 1). In the case that there exists an integer k such that $\mathrm{lex}(\vec{h}) \rhd \mathrm{lex}(\vec{h}_k)$. By induction assumption, the reduction chain (C): $\vec{h}_k \xrightarrow[F]{} \vec{h}_{k+1} \xrightarrow[F]{} \cdots$ is finite. Hence, chain (A) is also finite.

(Case 2). In the case that $\mathrm{lex}(\vec{h}_k) = \mathrm{lex}(\vec{h})$ for any k. Since the head term of $\vec{h}$, or $\vec{h}_0$, is not reduced in chain (A), we get a corresponding genuine reduction chain (D): $\mathrm{rest}(\vec{h}) \xrightarrow[F]{} \mathrm{rest}(\vec{h}_1) \xrightarrow[F]{} \cdots$. Since $\mathrm{lex}(\vec{h}) \rhd \mathrm{lex}(\mathrm{rest}(\vec{h}))$, the chain (D) is finite by induction assumption. Hence, the reduction chain (A) is also finite. □

Definition 10 [Gröbner basis].

Let $\vec{I} = (\vec{f}_1,\ldots,\vec{f}_s)$ be a module in $(K[x])^r$. A subset $G = (\vec{g}_1,\ldots,\vec{g}_t)$ of $(K[x])^r$ is called a Gröbner basis of $\vec{I}$ if the following conditions are satisfied:

(1) $(\vec{g}_1,\ldots,\vec{g}_t) = \vec{I}$.

(2) for any element $\vec{f}$ of $\vec{I}$, $\vec{f} \xrightarrow[G]{} \vec{0}$. □

Definition 11 [S-pair].

Let $\vec{f}$ and $\vec{g}$ be elements of $(K[x])^r$ and put $ht(\vec{f}) = a_A x^A$ and $ht(\vec{g}) = b_B x^B$. The S-pair of $\vec{f}$ and $\vec{g}$, to be abbreviated to $Sp(\vec{f},\vec{g})$, is defined by

$$Sp(\vec{f},\vec{g}) = \begin{cases} u\cdot\vec{f} - (a_A/b_B)v\cdot\vec{g} & \text{if } hp(\vec{f}) = hp(\vec{g}), \\ \vec{0} & \text{otherwise,} \end{cases}$$

where u and v are monomials satisfying $LCM(x^A,x^B) = u\cdot x^A = v\cdot x^B$, with LCM the least common multiple. □

Note. That $Sp(\vec{f},\vec{g}) = \vec{0}$ when $hp(\vec{f}) \neq hp(\vec{g})$ is essential in the Gröbner basis theory of $\vec{I}$, and it is quite reasonable from the viewpoint of general reduction theory.

Theorem 1. Let $G = \{\vec{g}_1,\ldots,\vec{g}_t\}$ be a Gröbner basis of a module $\vec{I}$ in $(K[x])^r$, and $\vec{h}$ an element of $(K[x])^r$. Let $\underline{\vec{h}}_1$ and $\underline{\vec{h}}_2$ be normal forms of $\vec{h}$ w.r.t. G, then $\underline{\vec{h}}_1 = \underline{\vec{h}}_2$.

Proof. Let $\vec{E} = \bigcup_{i=1}^{t} lmo(\vec{g}_i)$. By definition of normal form, we have $exs(\underline{\vec{h}}_i) \cap \vec{E} = \vec{\phi}$, i=1,2. On the other hand, $lex(\underline{\vec{h}}_1 - \underline{\vec{h}}_2) \in \vec{E}$ because $\underline{\vec{h}}_1 - \underline{\vec{h}}_2 \in \vec{I}$. Hence, if $\underline{\vec{h}}_1 - \underline{\vec{h}}_2 \neq \vec{0}$ then we have a contradiction. □

Theorem 2. Let $\vec{I} = (\vec{g}_1,\ldots,\vec{g}_t)$ be a module in $(K[x])^r$ and put $G = \{\vec{g}_1,\ldots,\vec{g}_t\}$. If $Sp(\vec{g}_i,\vec{g}_j) \xrightarrow[G]{} \vec{0}$ for any pair $(\vec{g}_i,\vec{g}_j)$, $i \neq j$, $1 \leq i,j \leq t$, then G is a Gröbner basis of $\vec{I}$.

Proof. Put $\vec{E} = \bigcup_{i=1}^{t} lmo(\vec{g}_i)$ and let $\vec{f}$ be any element of $\vec{I}$ with $lex(\vec{f}) = \vec{A}$. We have only to show $\vec{f} \xrightarrow[G]{} \vec{0}$. If $\vec{A} \in \vec{E}$ then $\vec{f}$ can be reduced directly and we can replace $\vec{f}$ by $\vec{f}'$, $lex(\vec{f}') \lhd \vec{A}$, so we have only to consider the case of $\vec{A} \notin \vec{E}$.

Since $\vec{f} \in \vec{I}$, there exist $h_1, \ldots, h_t$ in $K[x]$ satisfying

$$\vec{f} = h_1\vec{g}_1 + \cdots + h_t\vec{g}_t.$$

For i=1,...,t, put

$$ht(\vec{g}_i) = a_{A_i}x^{A_i}, \quad ht(h_i) = b_{B_i}x^{B_i},$$

hence $ht(h_i\vec{g}_i) = a_{A_i}b_{B_i}x^{A_i+B_i}$. Let $\vec{D}$ be the highest order element of $\{lex(h_i\vec{g}_i) \mid i=1,\ldots,t,\ h_i \neq 0\}$. Without loss of generality, we assume $\vec{D} = lex(h_1\vec{g}_1) = \cdots = lex(h_\tau\vec{g}_\tau)$, and $\vec{D} \rhd lex(h_i\vec{g}_i)$ for all $i > \tau$. Then, putting $h_i = b_{B_i}x^{B_i} + h_i'$, we decompose $\vec{f}$ as

$$\vec{f} = \vec{f}^{(1)} + \vec{f}^{(2)},$$

$$\vec{f}^{(1)} = \sum_{i=1}^{\tau} b_{B_i}x^{B_i}\vec{g}_i, \quad \vec{f}^{(2)} = \sum_{i=1}^{\tau} h_i'\vec{g}_i + \sum_{i=\tau+1}^{t} h_i\vec{g}_i.$$

We see $\vec{D} \rhd lex(h_i'\vec{g}_i)$, i=1,...,$\tau$. If $\tau = 1$ then $\vec{D} = \vec{A} \in \vec{E}$, contradicting to the assumption $\vec{A} \not\in \vec{E}$. Hence, $\tau > 1$ and we can rewrite $\vec{f}^{(1)}$ as

$$\begin{aligned} \vec{f}^{(1)} = {} & (a_{A_1}b_{B_1})\cdot(x^{B_1}\vec{g}_1/a_{A_1} - x^{B_2}\vec{g}_2/a_{A_2}) \\ & + (a_{A_2}b_{B_2} + a_{A_1}b_{B_1})\cdot(x^{B_2}\vec{g}_2/a_{A_2} - x^{B_3}\vec{g}_3/a_{A_3}) \\ & + \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ & + (a_{A_{\tau-1}}b_{B_{\tau-1}} + \cdots + a_{A_1}b_{B_1})\cdot(x^{B_{\tau-1}}\vec{g}_{\tau-1}/a_{A_{\tau-1}} - x^{B_\tau}\vec{g}_\tau/a_{A_\tau}) \\ & + (a_{A_\tau}b_{B_\tau} + \cdots + a_{A_1}b_{B_1})\cdot(x^{B_\tau}\vec{g}_\tau/a_{A_\tau}). \end{aligned}$$

We first note that the last term of this expression is $\vec{0}$. To see this, we consider $ht(\vec{f}^{(1)})$, which is

$$\sum_{i=1}^{\tau} a_{A_i}b_{B_i}x^{A_i+B_i} = (a_{A_1}b_{B_1} + \cdots + a_{A_\tau}b_{B_\tau})\cdot x^{A_1+B_1}.$$

If this expression is not zero then $\vec{A} = lex(\vec{f}) = (0,\ldots,0,\ A_1+B_1\ ,0\ldots,0)$, contradicting to the assumption $\vec{A} \not\in \vec{E}$. We next consider the j-th term, $j \leq \tau-1$, of the above r.h.s. expression. Recalling the definition of S-pair, we see [the j-th term] $= u\cdot Sp(\vec{g}_j,\vec{g}_{j+1})$ with u a monomial. By the assumption of theorem, $Sp(\vec{g}_j,\vec{g}_{j+1}) \xrightarrow[G]{} \vec{0}$. Hence, we find $\vec{f}^{(1)} \xrightarrow[G]{} \vec{0}$.

The $\vec{f}^{(2)}$ is of the same form as $\vec{f}$, so we can continue the above reduction, reaching $\vec{f} \xrightarrow[G]{} \cdots \xrightarrow[G]{} \vec{f}'$, $\mathrm{lex}(\vec{f}') \lhd \mathrm{lex}(\vec{g}_i)$, $i=1,\ldots,t$. That is $\vec{f} \xrightarrow[G]{} \vec{0}$. □

Note. The S-pairs $\mathrm{Sp}(\vec{g}_i,\vec{g}_j)$ with $\mathrm{hp}(\vec{g}_i) \neq \mathrm{hp}(\vec{g}_j)$ are unnecessary in the above proof, which shows the appropriateness of Def. 11.

An important problem in the Gröbner basis theory is how to construct the Gröbner basis, and Buchberger [1] found a simple procedure for the case of polynomial ideals. Buchberger's procedure, with a slight modification, applies to our case, too.

Procedure BUCHBERGER

input: a module $\vec{I} = (\vec{f}_1,\ldots,\vec{f}_s)$ in $(K[x])^r$.

output: a Gröbner basis $G = \{\vec{g}_1,\ldots,\vec{g}_t\}$ of $\vec{I}$.

```
G := {g1:=f1, ..., gs:=fs};
P := {(gi,gj) | gi,gj ε G, i ≠ j, hp(gi) = hp(gj)};
while P ≠ φ do begin
    pij := a pair (gi,gj) in P;
    P := P - {pij};
    g := a normal form of Sp(gi,gj) w.r.t. G;
    if g ≠ 0 then begin
        P := P ∪ {(gi,g) | hp(gi) = hp(g), gi ε G};
        G := G ∪ {g};
        end;
    end.
```

In the process of the above procedure, the size of G is increasing one by one, so we denote the G explicitly by G_0, G_1, G_2, ..., where $G_0 = F$ and $G_i = G_{i-1} \cup \{\vec{g}_i\}$, $i \geq 1$, with $\vec{g}_i$ the i-th generated S-pair in normal form. Writing $\vec{g}_i = \vec{g}_{s+i}$, so $G_i = \{\vec{g}_1,\ldots,\vec{g}_{s+i}\}$, we put $\vec{E}_i = \bigcup_{j=1}^{s+i} \mathrm{lmo}(\vec{g}_j)$.

Theorem 3. The procedure BUCHBERGER terminates in finite steps, and it gives us a Gröbner basis of the module $\vec{I}$.

Proof. We denote $\vec{E}_i$ as $(E_{i1},\ldots,E_{ir})$, where E_{ij}, $1 \leq j \leq r$, are monoideals in $\mathbb{Z}_0^n$. For every j, $1 \leq j \leq r$, $E_{1j} \subseteq E_{2j} \subseteq \cdots \subseteq E_{ij} \subseteq \cdots$ is an ascending chain of monoideals, so it must be a finite chain (see [5].). Therefore, there exists an integer k_j such that $E_{1j} \subseteq E_{2j} \subseteq \cdots \subseteq E_{k_j,j} = E_{k_j+1,j} = \cdots$. Let $k = \max\{k_1,\ldots,k_r\}$, then $\vec{E}_1 \subseteq \vec{E}_2 \subseteq \cdots \subseteq \vec{E}_k = \vec{E}_{k+1} = \cdots$, and every element of the module $\vec{I}$ is reducible w.r.t. G_k. This means that procedure BUCHBERGER terminates. Hence, Theorem 2 tells us that the procedure gives us a Gröbner basis of $\vec{I}$. □

§4. Polynomial solutions of a system of linear equations

Let us consider the system (1) given in §1. We rewrite (1) as

$$y_1\vec{f}_1 + \cdots + y_s\vec{f}_s = \vec{f}_0, \tag{1'}$$

where $\vec{f}_i = (f_{i1},\ldots,f_{ir})$, $i=0,\ldots,s$.

Before solving (1'), we consider the following homogeneous equations:

$$z_1\vec{g}_1 + \cdots + z_t\vec{g}_t = \vec{0}, \tag{2}$$

where $G = \{\vec{g}_1,\ldots,\vec{g}_t\}$ is a Gröbner basis of the module $\vec{I} = (\vec{f}_1,\ldots,\vec{f}_s)$.

Let $\vec{g}_i$ and $\vec{g}_j$ satisfy $\mathrm{hp}(\vec{g}_i) = \mathrm{hp}(\vec{g}_j)$, and put $\mathrm{ht}(\vec{g}_i) = a_{A_i}x^{A_i}$ and $\mathrm{ht}(\vec{g}_j) = b_{B_j}x^{B_j}$ with $a_{A_i}, b_{B_j} \in K$. Then, since G is a Gröbner basis, we have

$$\mathrm{Sp}(\vec{g}_i,\vec{g}_j) \xrightarrow[G]{} \vec{0}.$$

This reduction relation can be rewritten as

$$u_{ij}\vec{g}_i - (a_{A_i}/b_{B_j})\cdot v_{ij}\vec{g}_j = \sum_{k=1}^{t} w_{ij,k}\vec{g}_k,$$

where u_{ij} and v_{ij} are monomials satisfying $LCM(x^{A_i},x^{B_j}) = u_{ij}x^{A_i} = v_{ij}x^{B_j}$ and $w_{ij,k}$ satisfies $lex(w_{ij,k}\vec{g}_k) \lhd lex(u_{ij}\vec{g}_i) = lex(v_{ij}\vec{g}_j)$.

Proposition 7. With the above notations, let

$$\tilde{z}^{(ij)} = (w_{ij,1},\ldots, w_{ij,i}-u_{ij}, \ldots, w_{ij,j}+(a_{A_i}/b_{B_j})\cdot v_{ij}, \ldots, w_{ij,t}), \tag{3}$$

where we assume $i < j$. Then, $(z_1,\ldots,z_t) = \tilde{z}^{(ij)}$ is the lowest order solution of (2) satisfying

$$lex(z_i\vec{g}_i) = lex(z_j\vec{g}_j) \rhd lex(z_k\vec{g}_k) \text{ for all } k \neq i,j.$$

Proof. It is obvious because u_{ij} and v_{ij} are monomials of the lowest orders satisfying $lex(u_{ij}\vec{g}_i) = lex(v_{ij}\vec{g}_j)$. □

Theorem 4. With the above notations, $\{(z_1,\ldots,z_t) = \tilde{z}^{(ij)} \mid hp(\vec{g}_i) = hp(\vec{g}_j), i < j\}$ constitutes the set of generators of the polynomial solutions of (2).

Proof. Let $z_i = h_i$, with $h_i \in K[x]$, i=1,...,t, be any solution of (2) and put

$$\vec{f} = h_1\vec{g}_1 + \cdots + h_t\vec{g}_t.$$

We show, by subtracting multiples of the special solutions $\{\tilde{z}^{(ij)}\}$, we can reduce $\vec{f}$ to $\vec{0}$.

We use the same notations a_{A_i}, A_i, b_{B_i}, B_i, $\vec{D}$, and τ which were used in the proof of Theorem 2. We decompose $\vec{f}$ as

$$\vec{f} = \vec{f}^{(1)} + \vec{f}^{(2)},$$

$$\vec{f}^{(1)} = \sum_{i=1}^{\tau} b_{B_i}x^{B_i}\vec{g}_i, \quad \vec{f}^{(2)} = \sum_{i=1}^{\tau} h_i'\vec{g}_i + \sum_{i=\tau+1}^{t} h_i\vec{g}_i.$$

We see $\vec{D} \rhd lex(h_i'\vec{g}_i)$, i=1,...,$\tau$. If $\tau = 1$ then $\vec{f}$ can never be equal to $\vec{0}$. Hence, $\tau > 1$ and we can rewrite $\vec{f}^{(1)}$ as

$$\begin{aligned}\vec{f}^{(1)} &= (a_{A_1}b_{B_1})\cdot(x^{B_1}\vec{g}_1/a_{A_1} - x^{B_2}\vec{g}_2/a_{A_2})\\ &+ (a_{A_2}b_{B_2} + a_{A_1}b_{B_1})\cdot(x^{B_2}\vec{g}_2/a_{A_2} - x^{B_3}\vec{g}_3/a_{A_3})\\ &+ \cdots\cdots\\ &+ (a_{A_{\tau-1}}b_{B_{\tau-1}} + \cdots + a_{A_1}b_{B_1})\cdot(x^{B_{\tau-1}}\vec{g}_{\tau-1}/a_{A_{\tau-1}} - x^{B_\tau}\vec{g}_\tau/a_{A_\tau})\\ &+ (a_{A_\tau}b_{B_\tau} + \cdots + a_{A_1}b_{B_1})\cdot(x^{B_\tau}\vec{g}_\tau/a_{A_\tau}).\end{aligned}$$

We first note that the last term of this expression is $\vec{0}$ because $\sum_{i=1}^{\tau} a_{A_i}b_{B_i}$ is the coefficient of $ht(\vec{f})$. We next consider the j-th term, $j \leqq \tau-1$, of the above r.h.s. expression. Recalling the definition of S-pair, we see [the j-th term] = $u\cdot Sp(\vec{g}_j,\vec{g}_{j+1})$ with u a monomial. Hence, by subtracting $u\cdot\tilde{z}^{(j,j+1)}$, we can replace the term by $u\cdot\sum_{k=1}^{t} w_{j,j+1,k}\vec{g}_k$ which is less order than $Sp(\vec{g}_j,\vec{g}_{j+1})$. That is, subtracting multiples of special solutions $\tilde{z}^{(j,j+1)}$, j=1,...,τ-1, we can reduce $\vec{f}$ to $\vec{f}'$ such that $lex(\vec{f}) \rhd lex(\vec{f}')$. Continuing this subtraction, we obtain $\vec{f} \longrightarrow \vec{0}$ because of Prop. 7. □

Note. The above theorem is valid if some of the $z_1, \ldots, z_t$ are zero. For example, consider the case $g_{11} \neq 0$, $g_{21} = \cdots = g_{t1} = 0$. In this case, $hp(\vec{g}_1) = 1$ and $hp(\vec{g}_k) > 1$, k=2,...,t, so $Sp(\vec{g}_i,\vec{g}_j) = (0, \ldots)$ for any i and j, $1 \leqq i,j \leqq t$. Hence, $w_{ij,1} = 0$ for every pair (i,j) such that $hp(\vec{g}_i) = hp(\vec{g}_j)$, and $z_1 = 0$.

Now, let us consider the system (1'). Assume that $\{\vec{g}_1,\ldots,\vec{g}_t\}$ is a Gröbner basis of $\vec{I} = (\vec{f}_1,\ldots,\vec{f}_s)$, constructed by the procedure BUCHBERGER. Then, tracing the construction procedure, we can construct polynomials $q_{ji} \in K[x]$, j=1,...,t, i=1,...,s, such that

$$\vec{g}_j = \sum_{i=1}^{s} q_{ji}\vec{f}_i, \quad j=1,\ldots,t. \tag{4}$$

Conversely, tracing the reduction $\vec{f}_i \xrightarrow[G]{} \vec{0}$, we can construct polynomials $p_{ij} \in K[x]$, i=1,...,s, j=1,...,t, such that

$$\vec{f}_i = \sum_{j=1}^{t} p_{ij}\vec{g}_j, \quad i=1,...,s. \tag{5}$$

Using (5), we can transform the system (1') with $\vec{f}_0 = \vec{0}$ to (2), where

$$z_j = \sum_{i=1}^{s} p_{ij}y_i, \quad j=1,...,t. \tag{6}$$

Conversely, formula (4) allows us to calculate the solution $(y_1,...,y_s)$ of (1') from the solution $(z_1,...,z_t)$ of (2) by the formula

$$y_i = \sum_{j=1}^{t} q_{ji}z_j, \quad i=1,...,s. \tag{7}$$

Thus, we obtain the following algorithm.

Algorithm SOLVE

Input: linear system $y_1\vec{f}_1 + \cdots + y_s\vec{f}_s = \vec{f}_0$, $\vec{f}_i \in (K[x])^r$.

Output: generators of the solutions y_i, i=1,...,s, in K[x].

Step 1. By using procedure BUCHBERGER,

calculate a Gröbner basis of module $\vec{I} = (\vec{f}_1,...,\vec{f}_s)$,

and let the basis obtained be $G = \{\vec{g}_1,...,\vec{g}_t\}$;

Step 2. By reducing $\vec{f}_0$ w.r.t. G,

calculate polynomials $z_j^{(0)}$, j=1,...,t, such that

$\vec{f}_0 = \Sigma_{j=1}^{t} z_j^{(0)}\vec{g}_j + \underline{\vec{f}}_0$, $\underline{\vec{f}}_0$ is irreducible w.r.t. G;

If $\underline{\vec{f}}_0 \neq \vec{0}$ then return ϕ (no solution),

else let $\tilde{z}^{(0)} = (z_1^{(0)},...,z_t^{(0)})$ (particular solution);

Step 3. Calculate a set of polynomials $\{q_{ji}\}$ satisfying (4);

Step 4. For every pair $(\vec{g}_i,\vec{g}_j)$ in G such that $hp(\vec{g}_i) = hp(\vec{g}_j)$,

calculate the generator $\tilde{z}^{(ij)}$ by the formula (3);

Then, transform these generators and particular solution $\tilde{z}^{(0)}$

by the formula (7), and return the results.

§5. Example and discussion

In this section, we use Nf to denote the normal form w.r.t. $\{\vec{f}_1,\vec{f}_2,\vec{f}_3,\cdots\}$ for simplicity. Furthermore, the head terms are indicated by underlines.

Example 5. In $(Q[x,y])^2$, let $\vec{I} = (\vec{f}_1,\vec{f}_2,\vec{f}_3)$ with $\vec{f}_1 = (\underline{x^2}-1, y^2-1)$, $\vec{f}_2 = (xy-2, \underline{x^3}-y)$, and $\vec{f}_3 = (y^2+x, \underline{xy}-1)$.

We calculate a Gröbner basis of the module $\vec{I}$ given in Example 5. By using procedure BUCHBERGER, we get

$$\vec{f}_4 = Nf(Sp(\vec{f}_2,\vec{f}_3)) = (xy^2-y^3-xy-y^2-x-2y,\ \underline{y^4}+x^2-2y^2-x+y),$$

$$\vec{f}_5 = Nf(Sp(\vec{f}_2,\vec{f}_4))$$

$$= (\underline{y^6}+2xy^4+y^5+2xy^3-y^4+4xy^2-2y^3+2xy+y^2-x-2y-1,$$

$$-2y^3+2x^2-3y^2-x+3y+1),$$

$$\vec{f}_6 = Nf(Sp(\vec{f}_3,\vec{f}_4)) = (\underline{y^5}+2xy^3-y^3+2xy+y^2+2x+3y-1,\ -2y^3+x+y),$$

$$Nf(Sp(\vec{f}_1,\vec{f}_5)) = \vec{0},$$

$$Nf(Sp(\vec{f}_1,\vec{f}_6)) = \vec{0},$$

$$Nf(Sp(\vec{f}_5,\vec{f}_6)) = \vec{0}.$$

Since other pairs do not possess common head position, we get $\{\vec{f}_1,\vec{f}_2,...,\vec{f}_6\}$ as a Gröbner basis of $(\vec{f}_1,\vec{f}_2,\vec{f}_3)$.

The above computation is done with the highest-order smallest-suffix component order. In order to see how the efficiency of the resolution method depends on the choice of order, we consider another definition of order $\rhd$. It is easy to find that solving (1) with the order defined below is equivalent to solving (1) by the successive substitution method, where each single equation is solved by the Gröbner basis method.

Definition 4' [nonzero smallest-suffix component order $\rhd$ in $(\mathbb{Z}_0^n)^r$].

Let $\vec{A} = (A_1,\ldots,A_r)$ and $\vec{B} = (B_1,\ldots,B_r)$ be any elements of $(\mathbb{Z}_0^n)^r$. We define $\vec{A} \rhd \vec{B}$ iff there exists an integer k such that $A_i = B_i$ for all i, $1 \leq i < k$, and $A_k \rhd B_k$. We define $\vec{A} \trianglerighteq \vec{B}$ iff $\vec{A} \rhd \vec{B}$ or $\vec{A} = \vec{B}$. □

Example 6. In $(\mathbb{Z}_0^3)^2$, $((1,1,1), (0,0,0)) \rhd ((0,3,0), (1,1,0)) \rhd$

$\rhd ((0,0,1), (0,1,1)) \rhd ((0,0,0), (1,1,0)) \rhd (\phi, (1,1,1))$.

Calculating a Gröbner basis of the module given in Example 5 with the nonzero smallest-suffix component order, we obtain $\{\vec{f}_1,\vec{f}_2,\ldots,\vec{f}_{12}\}$ as a Gröbner basis of $(\vec{f}_1,\vec{f}_2,\vec{f}_3)$.

Using the above Gröbner bases, we can easily calculate the generators of the homogeneous system of linear equations

$$y_1\vec{f}_1 + y_2\vec{f}_2 + y_3\vec{f}_3 = \vec{0}.$$

With the highest-order smallest-suffix component order, the solutions are represented by 6 generators. On the other hand, with the nonzero smallest-suffix component order, 30 generators are necessary to represent the solutions. Hence, for the above problem, the highest-order smallest-suffix component order is much better than the order defined in Def. 4', from the viewpoint of not only the computation speed but also the smallness of the number of generators.

Note that solving (1) with the nonzero smallest-suffix component order is equivalent to solving (1) by the successive substitution method. Thus, the above example indicates the superiority of our method to the successive substitution method. This is quite reasonable because, as for a system of linear equations, the more the number of equations is, the narrower the solution space becomes. Therefore, generally speaking, we can solve the system more efficiently by treating all the equations simultaneously than solving each equation successively.

Note. The algorithm described so far can be extended easily to calculate the general solutions in $\mathbb{Z}[x_1,\ldots,x_n]$. In order to do so, we have only to define the order $\rhd$ by including the integer coefficients as described in [6].

References

[1] B. Buchberger, "An algorithm for finding a basis for the residue class ring of a zero-dimensional polynomial ideal (German)", Ph. D. Thesis, Univ. of Innsbruck (Austria), Math. Inst., 1965.

[2] G. Zacharias, "Generalized Gröbner basis in commutative polynomial rings", Bachelor Thesis, M.I.T., Dept. of Comp. Sci., 1978.

[3] B. Buchberger, "Basic features and development of the critical-pair/completion procedure", Proc. First Intern'l Conf. on "Rewriting Techniques and Applications", France, 1985, Springer Lecture Notes Comput. Sci..

[4] T. Sasaki, "Cramer-type formula for the polynomial solutions of coupled linear equations with polynomial coefficients", Publ. RIMS (Kyoto Univ.), 21 (1985), pp. 237-254.

[5] H. Kobayashi, A. Furukawa, T. Sasaki, "Gröbner basis of ideal of convergent power series", preprint, 20 pages, 1985.

[6] B. Buchberger, "A critical-pair/completion algorithm for finitely generated ideals in rings", Proc. of the Conf. "Rekursive Kombinatorik", (Eds. E. Borger, G. Hasenjager, and D. Rodding), Lecture Notes Comp. Sci., Springer-Verlag, 1983.