数理解析研究所講究録
第612巻 1987年 1-23

Gröbner-Bases について

都立大数学科　古川 昭夫
(Akio Furukawa)

近年，多項式イデアル論における有力な算法としてGröbner-Basesの方法が注目を浴び，それを利用してめざましい成果がでている。本稿ではそれを紹介すると共に，基本定理の別証明を与える論法を報告する。

体K上の多項式環 $R = K[x_1, x_2, \cdots, x_n]$ 上のイデアル $I = (f_1, f_2, \cdots, f_r)$ の剰余環 R/I における標準形を求めるためにBuchbergerによって理論が開発された算法が，Gröbner-Basesの方法であり，SAC1に実際にimplementされている。近年，1)多項式係数の不定方程式の生成元の求解，2)代数方程式の求解，3)素イデアルの判定，4)準素イデアル分解などの算法が次々とGröbner-Basesを利用して開発されている。本稿ではり，2)の算法と理論を紹介する。

§1 準備

まず，次の様に用語を定める。

$\mathbb{Z}_0^+ : \{ x \in \mathbb{Z} \mid x \geqslant 0 \}$

K ： 基礎体（係数体）

R ： $K[x_1, x_2, \cdots, x_n]$ 多項式環

項 ： $x_1^{e_1} x_2^{e_2} \cdots x_n^{e_n}$, $e_i \in \mathbb{Z}_0^+$

指数： $(e_1, e_2, \cdots, e_n) \in (\mathbb{Z}_0^+)^n$

単項式： 係数 × 項

多項式： 単項式の和。 但し，同類項は簡約されるものとする。

Gröbner-Bases（以下，G-Bases と略す）では，"順序" が本質的に重要な役割をはたす。

$\mathfrak{E} = (e_1, e_2, \cdots, e_n)$, $\mathfrak{f} = (f_1, f_2, \cdots, f_n) \in (\mathbb{Z}_0^+)^n$

に対して

Ⓛ lexicographic ordering $\triangleright$

$\mathfrak{E} \triangleright \mathfrak{f}$

$\Leftrightarrow e_1 > f_1 \ \vee \ (e_2, \cdots, e_n) \triangleright (f_1, \cdots, f_n)$

Ⓣ total degree ordering ▶

$\mathfrak{e} \blacktriangleright \mathfrak{f}$

$\Leftrightarrow e_1+e_2+\cdots+e_n > f_1+f_2+\cdots+f_n$

otherwise $\mathfrak{e} \triangleright \mathfrak{f}$

例 $(3,2,1) \triangleright (3,1,2) \triangleright (2,3,5)$

$(2,3,5) \blacktriangleright (3,2,1) \blacktriangleright (3,1,2)$

以下，順序としてはⓁを採用して話をする。但し，次の性質の成立する$(\mathbb{Z}_{\geq 0}^{+})^n$の全順序ならば同様の話ができる。

小性質Θ

① $\mathfrak{e}_1 \triangleright \mathfrak{f}_1$, $\mathfrak{e}_2 \triangleright \mathfrak{f}_2 \Rightarrow \mathfrak{e}_1 \cdot \mathfrak{e}_2 \triangleright \mathfrak{f}_1 \cdot \mathfrak{f}_2$

② 降下列は有限でとまる。

さて，Notationをさらに次の様に定める。

$\exp(t)$ ：項tの指数（exponent）。

$t_1 \triangleright t_2 \Leftrightarrow \exp(t_1) \triangleright \exp(t_2)$

$\mathrm{term}(m)$ ：単項式mの項（term）。

$\mathrm{coef}(m)$ ：単項式mの係数（coefficient）。

$m_1 \triangleright m_2 \Leftrightarrow \mathrm{term}(m_1) \triangleright \mathrm{term}(m_2)$

このようにして項，単項式にも順序が定められる。

$E(P)$ ：多項式 P に現われる項の指数の集合。

$\max\exp(P)$ ： $E(P)$ の最大元。

$\max(P)$ ： $\max\exp(P)$ に対応する項。

$\mathrm{head}(P)$: $\max(P)$ に対応する P 中の単項式。

$\mathrm{rest}(P)$: $P - \mathrm{head}(P)$

例 $P = 3x_1^2x_2 + 4x_1x_2 + 6 \in \mathbb{Q}[x_1, x_2]$ に対し

$E(P) = \{(2,1), (1,1), (0,0)\}$,

$\max\exp(P) = (2,1)$, $\max(P) = x_1^2x_2$

$\mathrm{head}(P) = 3x_1^2x_2$, $\mathrm{rest}(P) = 4x_1x_2 + 6$

次に多項式 P_1, P_2 に対して

$P_1 \rhd P_2 \iff \max(P_1) \rhd \max(P_2)$

$P_1 \trianglerighteq P_2 \iff \max(P_1) = \max(P_2) \vee P_1 \rhd P_2$

と順序を定める。 従って $P_1 \trianglerighteq P_2 \wedge P_2 \trianglerighteq P_1$ なる同じ order の多項式はたくさん存在する。

さらに，多項式の組 $F = (P_1, P_2, \ldots, P_\ell)$ に対し，

$$\max F = \max_{i=1}^{\ell} (\max P_i)$$

$$\overline{\max}\ F = \{P_i \mid \max P_i = \max F\}$$

と定める。 2つの多項式の組 $F_1 = (P_1, P_2, \ldots, P_\ell)$, $F_2 = (Q_1, Q_2, \ldots, Q_\ell)$ に対して，

$F_1 \rhd F_2 \iff \max F_1 \rhd \max F_2$

or $\# \overline{\max} F_1 = \# \overline{\max} F_2$

$F_1 \trianglerighteq F_2 \iff \max F_1 \trianglerighteq \max F_2$

or $\# \overline{\max} F_1 = \# \overline{\max} F_2$

(但し，$\#$ は集合の元の個数を表わす。)

として順序関係を定める。

§2 M-reduction と G-Basis

指数 $\mathfrak{e} = (e_1, e_2, \ldots, e_n)$，$\mathfrak{f} = (f_1, f_2, \ldots, f_n)$ に対し，別の順序関係 $\geqslant$ を

$$\mathfrak{e} \geqslant \mathfrak{f} \iff \forall i \quad e_i \geqslant f_i$$

として定める。 すると，

$$t_1 \mid t_2 \iff \exp(t_1) \leqslant \exp(t_2)$$

である。 多項式の組 $F = \{P_1, P_2, \ldots, P_k\}$ に対して

$$M(F) = \{\mathfrak{e} \in (\mathbb{Z}_0^+)^n \mid \exists P_i \quad \mathfrak{e} \geqslant \max \exp(P_i)\}$$

と定める。 一般に $(\mathbb{Z}_0^+)^n$ の部分集合 S は，

$$S + (\mathbb{Z}_0^+)^n = S$$

をみたすとき，monoideal といわれる。 $M(F)$ も monoideal の例である。

さて，このとき，

多項式 f が $F=\{P_1,\cdots,P_n\}$ について M-可約

$\Leftrightarrow M(F)\cap E(f)\neq\emptyset$

多項式 f が $F=\{P_1,\cdots,P_n\}$ について M-既約

(あるいは M-正規)

$\Leftrightarrow M(F)\cap E(f)=\emptyset$

多項式 f が one-step M-reducible to $f^{(1)}$

w.r.t. P_i [記号では $f \xrightarrow[i]{} f^{(1)}$ (F)]

$\Leftrightarrow \exists e\in E(f),\ \exists P_i\in F,\ \exists m$: 単項式

s.t. $e \geqslant \max\exp(P_i)$,

$f^{(1)} = f - m\cdot P_i$, $f^{(1)} \lhd f$

例 $P_1 = xy-1$, $P_2 = x^2-y$, $f = x^2y$, $g = y^2+x$

$F=\{P_1, P_2\}$ のとき,

f は F に関して M 可約で,

$x^2y \xrightarrow[1]{} x$ (F)

$x^2y \xrightarrow[2]{} y$ (F)

ここで, x, y は M-正規である。

g は F に関して M 既約で, M-正規である。

このとき,

$\mathrm{hcoef}(P)$: 多項式 P の $\mathrm{head}(P)$ の係数.

と定めると、上記の単項式 m は

$$m = (x^{\alpha}/\max(P_i)) \cdot (\mathrm{hcoef}(f)/\mathrm{hcoef}(P_i))$$

で表わされる。　文脈で、今考えている多項式の組 $F = \{P_1, \dots, P_k\}$ が固定して自明なとき、

$f \xrightarrow{i} f^{(1)}$ (F)　は単に　$f \xrightarrow{i} f^{(1)}$

と F を略してかく。

また、

$f \longrightarrow f^{(1)} \iff \exists P_i \in F,\ f \xrightarrow{} f^{(1)}$

$f \longrightarrow\!\!\!\!\!\rightarrow g \iff \exists f_0 = f, \exists f_1, \exists f_2, \dots, \exists f_m = g$

$$\text{s.t.}\quad f_0 \to f_1 \to f_2 \to \cdots \to f_m$$

と定める。　($\to\!\!\!\!\!\rightarrow$ は $\to$ の trasitive and reflexive closure に他ならない。)　このとき、f は g に M-可約であるといい、特に $g \neq f$ (従って、$g \lhd f$) のとき、f は g に真に M-可約であるという。

例　$F = \{xy - 1, x^2 - y\}$　のとき

$$x^2y^2 + xy \xrightarrow{1} 2xy \xrightarrow{1} 1$$

$$x^2y^2 + xy \xrightarrow{2} y^3 + xy \xrightarrow{1} y^3 + 1$$

なので、　$x^2y^2 + xy \twoheadrightarrow 1$,　$x^2y^2 + xy \twoheadrightarrow y^3 + 1$

$F = \{P_1, P_2, \cdots, P_k\}$ で生成されるイデアルとは

$$ideal(F) = \{h_1 P_1 + h_2 P_2 + \cdots + h_k P_k \mid h_i \in R\}$$

なる多項式の集合であり，

$$f \equiv g \pmod{ideal(F)}$$

とは，

$$f - g \in ideal(F)$$

のことであった。さて，ここで $(mod\ ideal(F))$ を単に，$(mod\ F)$ と略すことにすると次の性質が成立する。

性質1

(1) $f \longrightarrow g \Rightarrow f \equiv g\ (mod\ F) \wedge f \rhd g$

(2) $f \longrightarrow\!\!\!\!\!\rightarrow g \Rightarrow f \equiv g\ (mod\ F) \wedge f \trianglerighteq g$

これはイデアルの基本性質から明らかである。ただし，reductron の方法により，同じ f から派生する正規形でも一般には等しくならないことに注意しよう。

性質2

$$\left.\begin{array}{l} f_1 \longrightarrow\!\!\!\!\!\rightarrow g \quad (g\text{は正規}) \\ f_2 \longrightarrow\!\!\!\!\!\rightarrow g \quad (\quad\ \ ) \end{array}\right\} \Rightarrow f_1 \equiv f_2\ (mod\ F)$$

は当然に成立するが，$f_1 \equiv f_2$ でも，($f_1 = f_2$ でも) 両者の正規形は一致するとは限らない。

性質3

M-reduction は有限回の step で停止する。

これは順序 $\triangleright$ の Noether 性による。

さて，一般には $f \in ideal(F)$ でも，$f \twoheadrightarrow 0\ (F)$ とは言えない。しかし，Fがうまい条件をみたすとき，$f \in ideal(F) \Leftrightarrow f \twoheadrightarrow 0$ がいえることがある。このようなFが扱いやすい。

Gröbner-Basis の定義

F が G.Basis

$\Leftrightarrow$ " $f \in ideal(F),\ f \neq 0 \Rightarrow f$ はFに関して M可約

次の性質が容易に確められるので，G-Basis を構成する方法がわかれば，$K[x_1, x_2, \ldots, x_n] / ideal(F)$ における標準形の問題は解決できることになる。

性質4・G-Basis の性質

$F = \{P_1, P_2, \ldots, P_s\}$ が G-Basis ならば

1) $f \in ideal(F)$ $\quad f \twoheadrightarrow 0$ (reduction path によらず)

2) $f - g \in ideal(F)$

$\exists h \quad f \twoheadrightarrow h,\ g \twoheadrightarrow h$

さて，G-Basis は必ず存在する。　というのは，一般に

Lemma 1

monoideal $\subseteq (\mathbb{Z}_0^+)^n$　は有限生成

が成立するので，$S = \{ \max\exp(f) \mid f \in \mathrm{ideal}(F) \}$ も monoideal だ従って有限生成である。その生成元に対応する多項式（一意的には定まらない）の組を $G = \{Q_1, Q_2, \cdots, Q_l\}$ とすれば $E(G) = S$ なので，実際に G は G-Basis となる。

しかし，この存在証明は G-Basis の構成には役立たない。G-Basis の構成は多項式の組を多項式の項書換規則（term rewriting rule）とみなし Knuth-Bendix の Completion-Algorithm をこの M-reduction に適用することによって与えられる。

多項式 P, Q と生成元に含むイデアルでは $P=0$, $Q=0$ とみなせるので，P, Q は

$$\max P \longrightarrow -\frac{\mathrm{rest}(P)}{\mathrm{hcoef}(P)}, \quad \max Q \longrightarrow -\frac{\mathrm{rest}(Q)}{\mathrm{hcoef}(Q)}$$

なる書換則とみなせる。　すると，P と Q の両方の書換則を適用できる順序最小の項は L.C.M(P, Q) である。
$\mathrm{L.C.M}(P,Q)/P = t$, $\mathrm{LCM}(P,Q)/Q = S$ とするとき，

$$\left(tP,\ \frac{hcoef(P)}{hcoef(Q)}\ sQ\right)$$

を P, Q の critical-pair といい，

$$tP - \frac{hcoef(P)}{hcoef(Q)}\ sQ$$

を P と Q の S-polynomial といい $Sp(P,Q)$ と表わす。

例 $Sp(xy-1,\ x^2-y)$

$$= x(xy-1) - y(x^2-y) = -x+y^2,$$

$Sp(x^2-y,\ -x+y^2)$

$$= 1\cdot(x^2-y) - (-1)x(-x+y^2)$$

$$= xy^2 - y$$

性質5. S-polynomial と G-basis

$G = \{P_1, P_2, \cdots, P_k\}$ が G-basis

$\Leftrightarrow \forall P_i, \forall P_j \quad Sp(P_i, P_j) \longrightarrow\!\!\!\!\!\rightarrow 0$

この証明は簡単である。 M-reduction の

1) $f \longrightarrow\!\!\!\!\!\rightarrow g \Rightarrow t\cdot f \longrightarrow\!\!\!\!\!\rightarrow t\cdot g$

2) $g_1 \longrightarrow\!\!\!\!\!\rightarrow g_2 \Rightarrow f[t \leftarrow g_1] \downarrow f[t \leftarrow g_2]$

なる性質を用いるのが Buchberger の証明法である。本稿では性質6の証明の際，同様の証明ができることを後ほど示す。性質5を用いてG-basis構成の算法が可能となる。

算法 1　　G-basis

1° $G := F$　　(F: given set of polynomials)

2° G の中から2つの f, g をとりだし
$Sp(f, g)$ の正規形を G に加える。

3° すべて Check してなければ 2° へ。

但し，F は最初から reduce しておくのが良い。

この算法が必ず停止することは，次の lemma に基づく。

LEMMA 2

$\sum (\subseteq (\mathbb{Z}_0^+)^m)$ のどの元も $\geqq$ に関して比較できないならば，$\sum$ は有限集合。

さて，$F = \{P_1, P_2, \cdots, P_k\}$ とするとき，$f \xrightarrow{}_i g$ ということは，$f = g + m \cdot P_i$ なる単項式 m が存在することに他ならない。従って

$f \xrightarrow{}\!\!\!\!\rightarrow g$ ならば，$f = g + \sum_{i=1}^{k} h_i P_i$ ---- (*)

とかける。(*) で等号が成立するような多項式 h_i

は，unique ではないが，1つの reduction-path を定めれば，それに対応する h_i は unique となる。このようなとき，

$$f \Longrightarrow g \oplus h_1 P_1 \oplus \cdots \oplus h_k P_k$$

とかくことにする。すると，

性質 6 ・ M-reduction と付随多項式

$$f \Longrightarrow g \oplus h_1 f_1 \oplus \cdots \oplus h_e f_e \ , \ f * g$$

$$\Rightarrow f \trianglerighteq g \ , \ f \trianglerighteq h_i f_i$$

の成立することは明らかであろう。

§3 代数方程式への応用

G-basis と辞書式順序 (L) で構成すると，次の性質が成立する。

性質 7 ・ G-Basis と消去

F を G-Basis とするとき，

$$\mathrm{ideal}(F) \cap K[x_i, x_{i+1}, \cdots, x_n] = \mathrm{ideal}(F \cap K[x_i, x_{i+1}, \cdots, x_n])$$

ideal $F = (P_1, P_2, \cdots, P_k)$ は，連立方程式

$$P_1 = 0 \wedge P_2 = 0 \wedge \cdots \cdots P_k = 0 \qquad \cdots (*)$$

の零点集合と対応関係をもっている。(*) が基礎体 K の代数的閉体 $\overline{K}$ 上で解をもつとき，イデアル F のことを可解 (soluable) といい，その解を F の解ということにすると，性質7を利用して可解性の判定・有限個の解の非解のアルゴリズムが構成される。

算法2．方程式系の可解性の判定

イデアル $F = (P_1, P_2, \cdots, P_k)$ が与えられたとき，
F から，F の Gröbner-basis G を順序 Ⓛ で構成する。(これを，$G := GB(F)$ とかく。)

F が非可解 $\Leftrightarrow$ $1 \notin G$

但し，G-Basis の各多項式は hcoef を1に正規化しておくものとする。

算法3．無限可解性の判定

$G := GB(F)$, $F \subseteq K[x_1, x_2, \cdots, x_n]$
F が有限個の解をもつ。
$\Leftrightarrow$ $\forall_i (1 \leq i \leq n)$ $x_i^{j_i}$ を head term にもつ多項式が G に存在する。

算法4　代数方程式の全根の求解

- $F=(P_1, P_2, \ldots, P_k) \subseteq \mathbb{Q}[x_1, x_2, \ldots, x_m]$ given
- $G:=\{Q_1, Q_2, \ldots, Q_m\}:=GB(F)$,
  (但し，各Q_iは$(Q_1, Q_2, \ldots \check{Q_i} \ldots Q_m)$に関して既約になるよう，必要に応じて，$Q_i$を$(Q_1, \ldots \check{Q_i} \ldots Q_m)$に関する正規形$\widetilde{Q_i}$ととりかえておくものとする。
  このようなG-Basisはreduced-Gröbner-Basisといわれる。)
- $Q \in G \cap K[x_m]$　なる$Q(x_m) \in G$　ととる。
  (算法3より，有限個の解をもつならば，このような$Q(x_m) \in G$は必らず存在し，しかもreduced-G-Basisならば，このような$Q(x_m)$は唯一つである。)
- $Q(x_m)=0$を解き，解$x_m=a_m$を，$Q_1, Q_2, \ldots, Q_m$に代入して得られる多項式を$Q_1^{(m-1)}, \ldots\ldots, Q_m^{(m-1)}$とする。
- $Q(x_{m-1}) \in \{Q_1^{(m-1)}, \ldots\ldots, Q_m^{(m-1)}\} \cap K[x_{m-1}]$
  なる$Q(x_{m-1})$達をとり，それらの共通解$x_{m-1}=a_{m-1}$を$Q_1^{(m-1)}, \ldots, Q_m^{(m-1)}$に代入して得られる多項式を$Q_1^{(m-2)}, \ldots\ldots, Q_m^{(m-2)}$とし　以下，順次$x_{m-2}, x_{m-3}, \ldots$　を消去し，最終解を得る。

§4 線形不定方程式への応用

$P_1, P_2, \cdots, P_k \in K[x_1, \cdots, x_m]$, $f \in K[x_1, \cdots, x_m]$ のとき, 線形不定方程式

$$f_1P_1 + f_2P_2 + \cdots + f_kP_k = f \quad \cdots \text{Ⓐ}$$

の多項式解 $(f_1, f_2, \cdots, f_k)$ について考察しよう。

$F = \{P_1, P_2, \cdots, P_k\}$ から reduced G-Basis $G := GB(F) = \{Q_1, Q_2, \cdots, Q_m\}$ を作ると, 各 Q_i は

$$Q_i = g_1P_1 + g_2P_2 + \cdots + g_kP_k$$

とかけているので, Ⓐの解の構造を知るには

$$\begin{cases} h_1Q_1 + h_2Q_2 + \cdots + h_mQ_m = f \\ \{Q_1, Q_2, \cdots, Q_m\} \text{ は reduced G-Basis} \end{cases} \quad \cdots \text{Ⓑ}$$

の解の構造がわかればよい。 従って, 以下ではⒷの形の線形不定方程式を考えることにする。

算法5 特殊解の構成

f, $G = \{Q_1, Q_2, \cdots, Q_m\}$ (reduced G-Basis) が与えられたとき, Ⓑの特殊解 $(h_1, \cdots, h_m)$ は,

$f \longrightarrow 0$ のときのみ存在し,

このとき, $f \longrightarrow 0 \oplus h_1P_1 \oplus h_2P_2 \oplus \cdots \oplus h_mP_m$

$(h_1, h_2, \cdots, h_e)$ をとればよい。

従って特殊解を求めることができることがわかったので，

Ⓑの一般解を求めるには，

$$\begin{cases} h_1 Q_1 + h_2 Q_2 + \cdots + h_m Q_m = f \\ \{Q_1, Q_2, \cdots, Q_m\} \text{ is reduced G-Basis.} \end{cases} \quad \cdots \text{Ⓒ}$$

の一般解がわかればよいことになる。

算法6・一般解の構成

Ⓒの一般解は

$$Sp(Q_i, Q_j) = t_i Q_i - \frac{c_i}{c_i} t_j P_j$$

(c_i, c_j は Q_i, Q_j の head coefficients)

$$\Longrightarrow 0 \oplus \bar{h}_1 Q_1 \oplus \cdots \oplus \bar{h}_m Q_m$$

とするとき，

$$(\bar{h}_1, \bar{h}_2, \cdots, \bar{h}_i - t_i, \cdots, \bar{h}_j + \frac{c_i}{c_i} t_j, \cdots, \bar{h}_m) \quad \cdots \text{Ⓓ}$$

なる ${}_mC_2$ 個の生成元で生成される。

この算法はBuchberger氏によるものであるが，氏はその証明を公表していない。従って以下の証明は筆者によるものである。

(算法6の証明)

Ⓒの一般解 $(h_1, h_2, \cdots, h_m)$ が、Ⓓの形の生成元によって生成されることを $(h_1Q_1, h_2Q_2, \cdots, h_mQ_m)$ のorderに関する帰納法によって示す。

$(h_1Q_1, h_2Q_2, \cdots, h_mQ_m) = (0, 0, \cdots, 0)$ のとき、

たしかにⒹの元で生成されている。

$(h_1Q_1, h_2Q_2, \cdots, h_mQ_m)$ のorder $\sqcup$ 未満のⒸの解 $(h_1, h_2, \cdots, h_m)$ がⒹの元で生成されているとき、$(h_1Q_1, h_2Q_2, \cdots, h_mQ_m)$ のorderが $\sqcup$ のときも、Ⓒの解 $(h_1, h_2, \cdots, h_m)$ がⒹの元で生成されていることを示そう。

$(h_1, h_2, \cdots, h_m)$ はⒸの解で、$(h_1Q_1, h_2Q_2, \cdots, h_mQ_m)$ のorderが $\sqcup$ $(\rhd (0,0,0,\cdots 0))$ とする。

$$h_1Q_1 \trianglerighteq h_2Q_2 \trianglerighteq \cdots \trianglerighteq h_mQ_m \quad \cdots ①$$

と仮定しても一般性を失なわない。

h_iQ_i のorderを $\overline{\sqcup}_i$ とし、

h_iQ_i の head monomial を $e_i \cdot M_i$ $(e_i \in k)$

h_i の head monomial を $d_i \cdot m_i$ $(d_i \in k)$

Q_i の head monomial を $c_i \cdot q_i$ $(c_i \in k)$

とする。 (従って $M_i = m_i \cdot q_i$, $e_i = c_i \cdot d_i$)

$$h_1Q_1 + h_2Q_2 + \cdots + h_mQ_m = 0 \quad \cdots ②$$

の左辺に形式的に表われている項のうち最大のorderのものは、①の仮定より $M_1 = m_1 \cdot g_1$ である。一方、②の右辺を考えると、M_1 の係数の和は0でなければいけない。従って $h_i Q_i$ $(i=2, \cdots, m)$ の中には M_1 と head term にもつものが少なくとも1つある。①の仮定より $h_2 Q_2$ の head term M_2 は M_1 と一致する。

$$\left.\begin{aligned} h_1 Q_1 &= d_1 \cdot c_1 \cdot m_1 \cdot g_1 + R_1, & R_1 \lhd h_1 Q_1, \\ h_2 Q_2 &= d_2 \cdot c_2 \cdot m_2 \cdot g_2 + R_2, & R_2 \lhd h_2 Q_2, \\ h_3 Q_3 &= d_3 \cdot c_3 \cdot m_3 \cdot g_3 + R_3, & R_3 \lhd h_3 Q_3, \\ & & \\ h_m Q_m &= d_m \cdot c_m \cdot m_m \cdot g_m + R_m, & R_m \lhd h_m Q_m, \end{aligned}\right\} \quad ③$$

とおく。

$Sp(Q_1, Q_2)$ に対応する Ⓓ の解を

$$(\overline{h_1} - t_1, \overline{h_2} + \frac{c_2}{c_1} t_2, \overline{h_3}, \cdots, \overline{h_m}) \quad \cdots ④$$

但し、$g_1 = \max(Q_1)$, $g_2 = \max(Q_2)$, $G = G.C.D(g_1, g_2)$ とするとき、$t_1 = g_2/G$, $t_2 = g_1/G$。

とする。このとき、M-reductionの性質より

$$\forall_i \quad \max(t_1 Q_1) = \max(t_2 Q_2) \rhd \overline{h_i} \cdot Q_i \quad \cdots ⑤$$

特に、$t_1 \rhd \overline{h}_1$, $t_2 \rhd \overline{h}_2$

が成立している。（ここで $\trianglerighteq$ ではなく $\rhd$ に注意！）

さて、$M_1 = m_1 g_1 = m_2 g_2$ なので、m_1, m_2 は t_1, t_2

の倍数で，従って $m_1 g_1 = m_2 g_2 = s t_1 g_1 = s t_2 g_2$ とおける。

$$d_1 s \quad (\overline{h_1} - t_1,\ \overline{h_2} + \frac{c_2}{c_1} t_2,\ \overline{h_3},\ \cdots,\ \overline{h_m}) \qquad \cdots ⑥$$

は Ⓒ の解なので，$(\widetilde{h_1}, \widetilde{h_2}, \widetilde{h_3}, \cdots, \widetilde{h_m})$

$$= (h_1 - d_1 s \cdot t_1 + d_1 s \cdot \overline{h_1},\ h_2 + \frac{c_2}{c_1} d_1 s \cdot t_2 + d_1 s \cdot \overline{h_2},$$
$$h_3 + d_1 s \cdot \overline{h_3},\ h_4 + d_1 s \cdot \overline{h_4},\ \cdots) \qquad \cdots ⑦$$

も Ⓒ の解である。 ⑦ の order を考えると

$(h_1 - d_1 s \cdot t_1 + d_1 s \overline{h_1}) \cdot Q_1 \lhd M_1$

（∵ $h_1 = d_1 m_1$，$m_1 = s t_1$ より ～～ は 0 に等しく，

$s\overline{h_1} \lhd s t_1$ より $s\overline{h_1} g_1 \lhd s t_1 g_1 = M_1$）

$(h_2 + \frac{c_2}{c_1} d_1 s t_2 + d_1 s \overline{h_2}) \cdot Q_2 \trianglelefteq M_1$

（∵ $h_2 g_2 = M_1$，$s t_2 g_2 = M_1$，$s \overline{h_2} g_2 \lhd s t_2 g_2 \lhd M_1$）

$(h_3 + d_1 s \overline{h_3}) Q_3 \begin{cases} \trianglelefteq M_1 & (m_3 g_3 = M_1 \text{ のとき}) \\ \lhd M_1 & (m_3 g_3 \lhd M_1 \text{ のとき}) \end{cases}$

（∵ $s \overline{h_3} g_3 \lhd s t_1 g_1 = M_1$）

$(h_4 + d_1 s \overline{h_4}) Q_4 \begin{cases} \trianglelefteq M_1 & (m_4 g_4 = M_1 \text{ のとき}) \\ \lhd M_1 & (m_4 g_4 \lhd M_1 \text{ のとき}) \end{cases}$

が成立しているので，仮定① と order の定義より

$$(h_1 Q_1, h_2 Q_2, \cdots, h_m Q_m) \rhd \underbrace{(\widetilde{h_1} Q_1, \widetilde{h_2} Q_2, \cdots, \widetilde{h_m} Q_m)}_{⑦ \text{の解に対応}}$$

が成立する。 従って，帰納法の仮定により

$(\widetilde{h_1}, \widetilde{h_2}, \cdots, \widetilde{h_m})$ は Ⓓ の元で生成されている。

一方，今，

$$(h_1, h_2, \cdots, h_m) = (\widetilde{h_1}, \widetilde{h_2}, \cdots, \widetilde{h_m}) - d_1 S(\overline{h_1} - t_1, \overline{h_2} + \frac{c_2}{c_1} t_2, \overline{h_3}, \cdots, \overline{h_m})$$

（Ⓓ の元）

なので，$(h_1\Theta_1, h_2\Theta_2, \cdots, h_m\Theta_m)$ の order が L のときも題意は成立する。order $\triangleright$ は多項式の組 $(f_1, \cdots, f_m)$ に関して有限の降鎖列しかもたないので，従って，order についての帰納法により任意の order $(h_1\Theta_1, \cdots, h_m\Theta_m)$ に対応する任意の Ⓖ の解 $(h_1, h_2, \cdots, h_m)$ が Ⓓ の type の元で生成されることが示された。（証明おわり）

全く同じ論法で，$G = \{P_1, P_2, \cdots, P_k\}$ に関し，

"$\forall Sp(P_i, P_j) \Rightarrow 0 \oplus f_1 P_1 \oplus \cdots \oplus f_k P_k$

$\Rightarrow \forall (g_1, g_2, \cdots, g_k) \ \exists (h_1, h_2, \cdots, h_k)$

$g_1 P_1 + g_2 P_2 + \cdots + g_k P_k \Rightarrow 0 \oplus h_1 P_1 \oplus \cdots \oplus h_k P_k$"

（すなわち性質5）を $(g_1 P_1, g_2 P_2, \cdots, g_k P_k)$ の order $\triangleright$ に関する帰納法で示すことができる。また，この論法で Euclid 環上の G-Basis の存在と構成証明をすることができる。

[REFERENCES]

[1] B.Buchberger, Ein algorithmisches Kriterium fur die Losbarkeit eines algebraischen Gleichungsystems, Aequationes Mathematicae, Vol 4/3.S. 374-383, 1970.

[2] B.Buchberger, A Theoretical Basis for the reduction of polynomials to canonical forms, ACM SIGSAM Bulletin 39, 19-29, 1976.

[3] L.Bachmir and B.Buchberger, A Simplified Proof of the Characterization thorem for the Gröbner-bases, ACM SIGSAM Bulletin ,29-34, 1980. Vol 14 No 4.

[4] B.Buchberger and R.Loos, Algebraic Simplification in Computer Algebra, Springer, 11-43, 1982.

[5] C.Kollreider and B.Buchberger, An improved Algorithmic Construction of Gróbner bases for Polynomial ideals, Techn. Rep. Nr. 110, Inst. für MATH, Univ. Linz. Austria, 1979.

[6] B.Buchberger, A criterian for detecting unnecessary reductions in the construction of Groebner bases, Eurosam 79, Springer Lec.Note. in Comp.Sci. No 72, 3-21, 1979.

[7] B.Buchberger, Grobner Bases: An algorithmic method in Polynomial ideal Theory, CAMP-Publ-Nr83-29.0, Chap6, 1983.

[8] A.Kandri Rody and Deepak Kapur, Algorithms for computing Gröbner Bases of Polynomil ideals over various Euclidean rings, Proc. of EUROSAM84, 1984.

[9] A.Kandri Rody and B.D.Saunders, Primality of ideals in polynomial rings, Proc of MACSYMA USER'S CONFERENCE84, 1984.

[1], [2] は Gröbner-Basis に関するオリジナル論文であるが，両者とも記法・証明がわかりにくい。[3], [4] は証明もすっきりしていて読みやすい。Gröbner-Basis の構成の効率化については [5], [6] をみると良い。代数方程式の求解の算法とその理論の証明は [7] が詳しい。[7] は参考文献も豊富で Gröbner-Basis について詳しく調べたい人にはおすすめたい。Euclid 環を係数にする多項式イデアルについても同様の理論が成立することを示したのが [8] である。[9] はイデアルの既約性の判定と G-Basis の関連を示している。

Gröbner-Basis の implement は，Buchberger を中心に数式処理システム SAC1 上で行なわれている。このプログラムは東大センターにもある。日本では，藤瀬哲朗（電通大…当時，現三菱総研）が REDUCE 2.0 上に，筆者が muSIMP/muMATH 83 上に implement している。