数理解析研究所講究録
第520巻 1984年 23-35

Gröbner - Basis とその応用

東京都立大学理学部数学科
古川 昭夫 (Akio Furukawa)
日本大学理工学部数学科
小林 英恒 (Hidetsune Kobayashi)

1. 動機と導入

多項式環上でのイデアル・モジュールの計算は一般には困難とされていたが、計算機の発達と数式処理のアルゴリズムの研究の進歩に伴ない多少のことができるようになった。本稿においては、

(1) イデアル $I=(f_1, f_2, \cdots, f_s)$ と多項式 g が与えられたとき、 $g \in I$ or $g \notin I$ の判定法.

(2) $g \in \sqrt{I}$ or $g \notin \sqrt{I}$ の判定法.

について述べる。

2. Gröbner - basis の定義と構成

(1)の問題は、Buchbergerが 1970～1976 にかけて解決しているので、それを紹介する。

以下、次の様なNotationを用いる。

K： 体（四則演算に閉じている集合，乗法は可換）

$R = K[x_1, x_2, \ldots, x_n]$ ：K上のn変数多項式環

$I = (f_1, f_2, \ldots, f_s)$ ：n変数多項式 $f_1, f_2, \ldots, f_s$ で生成されるイデアル，すなわち

$$\{c_1 f_1 + \cdots + c_s f_s \mid c_1, c_2, \ldots, c_s \in R\}$$

$g \in I \Leftrightarrow g \equiv 0 \pmod{I}$ なので、剰余環R/Iについて考察しよう。 R/IはK上のベクトル空間となっている。$\dim_K(R/I) = \infty$ ではあるが、その無限個のbase を、explictに書くことが可能である。[Buc 2]

（Gröbner-basis の定義）

R/IをK上のベクトル空間とみたときのbaseが、有限個の多項式 $F_1, F_2, \ldots, F_\ell$ を用いて

$$\{mF_i \mid m \text{ は } n \text{ 変数単項式}, i = 1, \ldots, \ell\}$$

となっているとき、$\{F_1, F_2, \ldots, F_\ell\}$ をイデアルIのGröbner-basis（略して G-basis）という。

れば、イデアルIを生成する多項式に付随する reduction rule に、さらに（イデアルIに属する）適当な多項式に付随するruleを付加し、reduction system 全体を Church-Rosserにすることであるといえる。

定式化にはいくつかの定義が必要である。

（定義：単項式の順序）

$$x_1^{\alpha_1}\cdots x_n^{\alpha_n} <_T x_1^{\beta_1}\cdots x_n^{\beta_n}$$

$$\Leftrightarrow (\alpha_1+\cdots+\alpha_n < \beta_1+\cdots+\beta_n)$$

$$\text{or } (\alpha_1+\cdots+\alpha_n = \beta_1+\cdots+\beta_n \text{ and } \alpha_n<\beta_n)$$

$$\text{or } \left(\alpha_1+\cdots+\alpha_n = \beta_1+\cdots+\beta_n \text{ and } \alpha_n=\beta_n \text{ and } x_1^{\alpha_1}\cdots x_{n-1}^{\alpha_{n-1}} <_T x_1^{\beta_1}\cdots x_n^{\beta_{n-1}}\right)$$

つまり、全次数、辞書式順序

（例）$K[x,y,z]$ 上で、

$$1 <_T x <_T y <_T z <_T x^2 <_T xy <_T xz <\cdots$$

（定義；記法）

1) Hterm(f)：多項式f中の単項式で order が最大のもの
2) Hcoef(f)：Hterm(f)の係数
3) Head(f)：Hcoef(f)×Hterm(f)
4) rest(f)：f−Head(f)

数学的にはこの定義で十分なのであるが、この定義を直接利用してG-basisを構成するのは困難である。計算機科学的には、modの計算は“項書替のreduction”とみる方がわかりやすい。例えば、イデアル $I=(x^3-y^2-2, x^2y^2-2xy+1)$ が与えられたとき、各多項式を $x^3 \to y^2+2$, $x^2y^2 \to 2xy-1$ なる“項書替則”とみなすわけである。1変数の場合は、イデアルはすべて単項生成なので、このような操作で、$g \in I$ ならば必ず0にreduction可能であるが、多変数多項式環のイデアルは単項生成でないので、例えば、$f_3 = y^2\cdot(x^3-y^2-2)-x(x^2y^2-2xy+1) = -y^4+2x^2y-2y^2-x$ は、このイデアルIに属するにもかかわらず、2の規則 $x^3 \to y^2+2$, $x^2y^2 \to 2xy-1$ では0にreductionできない。また、例えば、x^3y^2 という多項式は、

$$x^3y^3 \longrightarrow (y^2+2)y^3 = y^5+2y^3$$

$$x^3y^2 \longrightarrow x(2xy-1) = 2x^2y-x$$

なる2通りのreductionによって結果が異ってしまう。あるreductionのsystemでこれ以上reductionできないものを正規形（normal form）といい、reductionのpathによらず、同一のnormal formをもつとき、そのreductionはChurch-Rosserであるといわれる。従ってmod Iでの標準形を定めるということは、別の見方からす

5) Coef(t,f) : f 中の項 t の係数

さて、このとき、多項式の組 $F=\{F_1, F_2, \cdots, F_s\}$ が与えられたとき、F に関する one-step M reduction は次の様に定義される。

(定義) $f \xrightarrow[F_i,t]{1} g$ f の項 t に対する F_i に関する reduction

すなわち、 $Coef(t,f) \neq 0$, $Hterm(F_i) | t$ のとき、

$$g = f - \frac{Coef(t,f)}{Hcoef(F_i)} \cdot \frac{t}{Hterm(F_i)} \cdot F_i$$

(定義) $f \xrightarrow{1} g \Leftrightarrow {}^{\exists}t, {}^{\exists}F_i \quad f \xrightarrow[F_i,t]{1} g$

$\xrightarrow{1}$ の transitive and reflexive closure を $\longrightarrow$ で表わす。すなわち

(定義) $f \longrightarrow g \Leftrightarrow {}^{\exists}k \geq 0, {}^{\exists}h_0, \cdots, {}^{\exists}h_k$

$(f = h_0 \xrightarrow{1} h_1 \xrightarrow{1} h_2 \longrightarrow \cdots \longrightarrow h_k = g)$

この reduction で、もう reduction できない多項式を normal form という。

(定義) $Normal(f,F) \Leftrightarrow \forall_t, \forall_{F_i}\ Coef(t,f) \neq 0 \Rightarrow Hterm(F_i) \nmid t$

(定義) $f \longrightarrow \underset{\sim}{g} \Leftrightarrow f \longrightarrow g \wedge Normal(g,F)$

さて、このとき、Knuth-Bendix の critical-pair に対応するものが、Spolynomial の概念である。

（定義：S-polynomial）

$h = GCD(Hterm(f), Hterm(g))$ とするとき，

$$Sp(f,g) = \frac{Head(g)}{h} \cdot f - \frac{Head(f)}{h} \cdot g$$

例　$f = 5xy - 3x$，$g = 7x^2 + 2x$

$Sp(f,g) = 7x \cdot f - 5y \cdot g = -21xy - 10x^2$

さて、このとき次の基本定理が成立する。

（G-BASIS の基本定理）

$F = \{F_1, F_2, \cdots, F_\ell\}$ を多項式の組とするとき，以下の条件は同値である。

(1) F が Gröbner-basis

(2) $\forall_{Fi} \forall_{Fj}$　$Sp(Fi, Fj) \longrightarrow 0$

(3) $\forall_h \forall_{h_1} \forall_{h_2}$　$(h \to \underline{h_1}, h \to \underline{h_2}) \Rightarrow \underline{h_1} = \underline{h_2}$

（証明）は［Buc 2］を見よ。

これから，次の様なアルゴリズムが構成できる。

Algorithm GO （Gröbner-basis の生成）

input ：イデアル I の生成元 $\cdot f_1, f_2, \ldots, f_r$

output：イデアル I の Gröbner-basis

$F = \{F_1, F_2, \ldots, F_\ell\}$

1° $F := \{f_1, f_2, \ldots, f_r\}$

2° $Sp(F_i, F_j)$ を作り、F について reduction する。

この normal form が 0 でなければ、

$F := F \cup \{\text{Normal form}(Sp(F_i, F_j))\}$

3° 2° をくりかえし、すべての F_i, F_j に関し、

$Sp(F_i, F_j) \longrightarrow 0$ となったら、F が求める

G-basis となる。

G-basis の基本定理は、このアルゴリズムが停止すれば、出力された F が求めるものであることを保証している。アルゴリズムの停止性は［Buc 1］を見よ。

3. 多項式gが、あるイデアルの根基に属すための判定法について

前で説明した通り、G-basisを用いるイデアル $I \subset \mathbb{Q}[x_1,\dots,x_n]$, $g \in \mathbb{Q}[x_1,\dots,x_n]$ が与えられたとき、fがIに属するか否かが$\mathbb{Q}$上判定できる。

そこで、代数独立なn個の多項式 $f_1,\dots,f_n$ によって生成されたイデアル $I=(f_1,\dots,f_n)$ が与えられたとき、Iのradical $\sqrt{I}=\{g \mid \exists m \in \mathbb{N} \quad g^m \in I\}$ に多項式gが属するか否かの判定を$\mathbb{Q}$上でできないかと考えてみる。

もし $g \in \sqrt{I}$ ならば、$g \in I$, $g^2 \in I$, $g^4 \in I$, $g^8 \in I$, …… を次々にIのG-basisによって判定していけば、いつかは $g^{2^\alpha} \in I$ となるはずであるが、何度やっても $g^{2^\alpha} \notin I$ でも、$g \notin \sqrt{I}$ とはいえない。逆に、$g^N \notin I \Rightarrow \forall m \geq N \quad g^m \notin I$ なる自然数Nの存在がいえれば、判定可能ということになる。

それには、次のBezoutの定理を用いればよい。

(Bezoutの定理) $f_1,\dots,f_n$ を $\mathbb{C}[x_1,\dots,x_n]$ 上の多項式で、それぞれ次数を d_i とし、$I=(f_1,\dots,f_n)$ とする。

$f_1,\dots,f_n$ が代数独立ならば、

$$\dim_{\mathbb{C}}(\mathbb{C}[x_1,\dots,x_n]/I) \leq d_1 \cdot d_2 \cdots d_n$$

これより、次の定理を得る。

(定理) $f_1, \cdots, f_m \in \mathbb{C}[x_1, \cdots, x_n]$ が代数独立な、
d_i 次の多項式, $N = d_1 \cdot d_2 \cdots d_n$, $I = (f_1, \cdots, f_m)$
とするとき、
$(\exists m \quad f^m \in I) \Leftrightarrow f^N \in I$

(証明) $V = \mathbb{C}[x_1, \cdots, x_n]/I$ を $\mathbb{C}$ 上のベクトル空間とみて、
積写像 $f : u \longrightarrow f \cdot u$ $(u, f \cdot u \in V)$ を考えると、
これは線形写像である。 従って、$d = \dim_{\mathbb{C}} V$ とすれば
$f^m = 0 \Leftrightarrow f^d = 0$ である。
線形写像として $f^d = 0$ となることと、$f^d \in I$ なることは同値であり、Bezout の定理より $N \geq d$ なので、
定理は成立する。 //

Bezout の定理は、代数的閉体 $\mathbb{C}$ 上での定理なので、
$\dim_{\mathbb{Q}}(\mathbb{Q}[x_1, \cdots, x_n]/I) \leq d_1 \cdots d_n$ を必ずしも直接的には保証しない。 我々は $\mathbb{Q}[x_1, \cdots, x_n]$ 上の多項式のイデアルの radical について判定したいので、$\mathbb{Q}$ 上でも上記の定理が成立することを示さねばならない。 次の lemma よりそれは保証される。

(lemma) $f, f_1, \cdots, f_n \in \mathbb{Q}[x_1, \cdots, x_n]$

$$f = \sum_{i=1}^{n} g_i f_i \quad , \quad g_i \in \mathbb{C}[x_1, \cdots, x_n]$$

ならば、$\exists h_i \in \mathbb{Q}[x_1, \cdots, x_n]$ が存在し

$$f = \sum_{i=1}^{n} h_i \cdot f_i$$ とかける。

(証明)

$f = \sum a_{i_1 \cdots i_n} x_1^{i_1} \cdots x_n^{i_n}$, $f_j = \sum a_{j i_1 \cdots i_n} x_1^{i_1} \cdots x_n^{i_n}$,

$g_j = \sum b_{j i_1 \cdots i_n} x_1^{i_1} \cdots x_n^{i_n}$ とおく。ここに、

$a_{i \cdots i_n}, a_{j i_1 \cdots i_n} \in \mathbb{Q}$, $b_{j i_1 \cdots i_n} \in \mathbb{C}$ である。

$f = \sum f_j g_j$ より

$$a_{\bullet} = \sum_{j} a_{j \bullet} b_{j \bullet}$$

の形の等式が得られるが、これは $b_{j\bullet}$ を変数とする線形方程式と考えれば、$\mathbb{C}$ 上での解が存在することから、係数のなす行列の階数その他に関する議論は $\mathbb{Q}$ 上でやれることだから、$\mathbb{Q}$ 上の解が存在することが分かる。 //

4. Examples

$F_1 = x^3 - y^2 - 2$ 1 : $\boxed{x^3 \longrightarrow y^2 + 2}$

$F_2 = x^2y^2 - 2xy + 1$ 2 : $\boxed{x^2y^2 \longrightarrow 2xy - 1}$

$Sp(F_1, F_2) = y^2 \cdot F_1 - xF_2$

$= -y^4 + 2x^2y - 2y^2 - x$ 3 : $\boxed{y^4 \longrightarrow 2x^2y - 2y^2 - x}$

↳ F_3とする

$Sp(F_1, F_3) \longrightarrow 0$

$Sp(F_2, F_3) \longrightarrow 0$

で、$I = (F_1, F_2)$ の G-basis は (F_1, F_2, F_3)

$g = (x^3 - y^2 - 2) - y^2(xy - 1)$

$= -xy^3 + x^3 - 2$

$g^2 = x^2y^6 - 2x^4y^3 + x^6 + 4xy^3 - 4x^3 + 4$

$\longrightarrow 0$

となるので、$g \in \sqrt{I}$ がわかる。

一般には $g, g^2, g^4, g^8, g^{16}, \cdots$ の Normal form を求めればよく、この場合 $d_1 = \deg(F_1) = 3$, $d_2 = \deg(F_2) = 4$ なので、$g^{12} = g^4 \cdot g^8$ の Normal form を求めればよい。

例えば、$g = x^3 - y - 2$ のときは、

$g \longrightarrow y^2 - y$

$g^2 \longrightarrow y^4 - 2y^3 + y^2$

$\longrightarrow 2x^2y - 2y^3 - y^2 - x$

3.

$g^4 \rightarrow -12xy^3 - 14x^2y + 6xy^2 - 4y^3 - 3x^2 + 12xy + 22y^2 + 7x + 4y - 8$

$g^8 \rightarrow 1092xy^3 - 688x^2y + 957xy^2 + 44y^3 + 309x^2 - 1536xy - 790y^2$

$+ 578x - 1536y + 252$

$g^{12} \rightarrow$ Not 0 !!

$\therefore g \notin \sqrt{I}$

参考文献

[BUC1] B.Buchberger, Ein Algorithmishes Kriteium fur die Losbarkeit eines algebraishen Gleichungsystems, Aequationes Mathematicae, vol 4,p374-383, 1970.

[BUC2] B.Buchberger, A theoritical basis for the reduction of polynomials to canonical forms, ACM SIGSAM Bulletin, No.40,p19-29, 1976.

[B&B] L.Bachmair and B.Buchberger, A simplified proof of the characterization theorem for Grobner basis, ACM SIGSAM Bulletin, No.52, p29-34, 1980.

[HER] G.Hermann, Die Frage der entlich vielen Schritte in der Theorie der Polynomideale, Math.Ann.95, p736-788, 1926

[LAU] M.Lauer, Cannonical representatives for residue classes of a polynomial ideal, Proc. ACM SYMSAC'76, p339-345, 1976.

[LAZ1] D.Lazard, Algebre lineaire sur $K[x, \ldots, x]$ et elimination, Bull.Soc.Math.France 105, p165-190, 1977

[LAZ2] D.Lazard, Resolution des systemes d'equation algebrique, Theo.Comp.Sci.15, p77-110, 1981

[SEI] A.Seidenberg, Construction in algebra, Trans.Amer.Math.Soc.No197, p273-313,1974 .

[SHA] I.R.Shafarevich, Basic Algebraic Geometry chapⅣ, Springer, 1977.

[S&F] T.Sasaki and A.Furukawa, On solutions of linear Diophantiine equations with polynomial coefficients, to appear.

[P&Y] M.E.Pohst and D.Y.Y.Yun, On solving systems of algebraic equations via ideal basis and elimination theory, Proc. Proc. ACM SYMSAC'81, p206-211,1981.

[VdW] Van der Werden, Moderne Algera, Springer, 1950.