記号処理 38－3
（1986. 9. 16）

Gröbner基底による代数的関係とGCDの計算法

佐々木建昭　　古川昭夫
（理化学研究所）　（都立大・数学）

m個の多項式 $P_1, P_2, \cdots, P_m$, ただし $P_i \in Q[x_1, \cdots, x_n]$, が与えられたとき, $P_1, P_2, \cdots, P_m$ 間に成立する代数的関係 $R(P_1, P_2, \cdots, P_m)$, ただし $R(y_1, \cdots, y_m) \in Q[y_1, \cdots, y_m]$, を計算することを考える。この問題は原理的には終結式を用いて解くことができるが, Gröbner基底の計算法を利用することにより, はるかに効率的に解くことができる。さらに, Gröbner基底の計算法を利用した, 多変数多項式のGCDの計算を論じる。

Computation of Algebraic Relations and GCD's

by Using Gröbner Basis Method

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

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

Abstract

Let $P_1, \ldots, P_m$ be polynomials in $Q[x_1,\ldots,x_n]$. We consider the calculation of algebraic relation $R(y_1,\ldots,y_m)$ in $Q[y_1,\ldots,y_m]$ such that $R(P_1,\ldots,P_m) = 0$. This problem can be solved by calculating resultants successively, but using the Gröbner basis method we can calculate the algebraic relation much more efficiently. We discuss, furthermore, the computation of GCD of multivariate polynomials by using the Gröbner basis method.

Gröbner基底による代数的関係とGCDの計算法

佐々木建昭（理研），石川昭夫（都立大・数学）

1．はじめに

本研究は1年前の理研シンポジウム「代数的計算法」における高橋正氏の講演[1]に啓発されて行ったものである。氏の問題提起はこうである：

> m個の多項式 $P_1, P_2, \cdots, P_m$，ただし $P_i \in Q(x_1, \cdots, x_n)$，が与えられたとき，$P_1, P_2, \cdots, P_m$ の間に代数的関係が成立すればそれを求めよ。ただし，代数関係とは，$R(y_1, y_2, \cdots, y_m)$ を $Q\{y_1, y_2, \cdots, y_m\}$ 内の多変数多項式とするとき，$R(P_1, P_2, \cdots, P_m) = 0$ なるQ上の多項式のことである。

このような代数的関係RはGröbner基底[2,3]の計算法を応用すれば簡単に計算することができる。

この計算法は多項式のGCD計算にも適用できる。本稿で提案するGCD計算法と従来の最も効率的な方法であるEZGCD法を比べて，どちらがより効率的かは現時点では明らかでないが，本稿の方法は互除法に基づく方法よりは効率的であろうと筆者らは考えている。

なお，本稿で述べる計算方法はGröbner基底の計算法を知っている者ならば誰でも考えつくものとみえて，上記の二つのideaともに調べてみると先駆者[4,5]が居たことを断っておく。

2．Euclidean消去とBuchberger消去

多項式の組 $P_1, P_2, \cdots, P_m$，ただし $P_i \in Q[x_1, \cdots, x_n]$，が与えられたとき，これらの多項式が0に等しいとみて，より簡単な多項式系に簡約することができる。その一つの方法は，どれか一つの変数，たとえば x_n，を主変数とみなして，主変数に関して最大次数の項（これを主項－leading term－という）を消去するよく知られた方法である。主項消去を連続して行うことはEuclidの互除法に他ならないので，この消去法をEuclidean消去と呼ぶことにする。

（例） $P_1(x_1, x_2) = \underline{(x_1^2+1)x_2^2} + (x_1^2+x_1+2)x_2 + x_1^2 - 2x_1 - 3,$

$P_2(x_1, x_2) = \underline{(x_1-1)x_2^2} + (x_1^2+3)x_2 + x_1^2 + x_1 - 3.$

下線は主項を表わす。主項を消去するには（l_c は主係数を表わす），

$$P_3 \leftarrow \{l_c(P_2)/g\} \cdot P_1 - \{l_c(P_1)/g\} \cdot P_2$$

ただし，$g = GCD(l_c(P_1), l_c(P_2))$

$$= \{(x_1-1)(x_1^2+x_1+2) - (x_1^2+1)(x_1^2+3)\}x_2 + \{(x_1-1)(x_1^2+x_1-3) - (x_1^2+1)(x_1^2-2x_1-3)\}.$$

一方，Gröbner基底の計算では，単項式に一意的な順序を導入し，各多項式の中で順序が最大の項（これを頭項－head term－という）を消去する。Gröbner

基底の発見者の名にちなんで，この方法をBuchberger消去と呼ぶことにする。

(例) $P_1(x_1,x_2)=\underline{x_1^2x_2^2}+x_1^2x_2+x_1^2+x_1x_2+x_2^2-2x_1+2x_2-3$,

$P_2(x_1,x_2)=\underline{x_1^2x_2}+x_1x_2^2+x_1^2-x_2^2+x_1+3x_2-3$.

これらの多項式は上例と同じものであるが，単項式にバラして，全次数辞書式順に各項を並べたものである($x_1>x_2$)。下線部は頭項を表わす。P_1とP_2の頭項(htで表わす)を消去するには

$$P_3 \leftarrow \{ht(P_2)/d\}\cdot P_1-\{ht(P_1)/d\}\cdot P_2$$

ただし，$d=GCD(ht(P_1),ht(P_2))$

$$=1\cdot(x_1^2x_2+x_1^2+x_1x_2+x_2^2-2x_1+2x_2-3)$$
$$-x_2\cdot(x_1x_2^2+x_1^2-x_2^2+x_1+3x_2-3).$$

今の場合，P_3はP_1をP_2でM-簡約したものに等しいが，上の定義式によれば，$d\neq ht(P_1)$かつ$d\neq ht(P_2)$の場合にはP_3はS-多項式を与える。

上記の二つの消去法を比較すると，Buchberger消去の方がきめ細かい消去法であることは自明である。実際，辞書式順序(前頁の例では$x_2>x_1$)でBuchberger消去を続ければEuclidean消去が実現できるが，その逆は成立しない。

3. 代数的関係の計算法

新しい不定元$t_1,t_2,\cdots,t_m$を導入し

$$\{P_1(x_1,\cdots,x_n)=t_1,\ P_2(x_1,\cdots,x_n)=t_2,\cdots,P_m(x_1,\cdots x_n)=t_m\}$$

とおく。代数的関係の定義によると，$P_1-t_1=0,\cdots,P_m-t_m=0$から変数$x_1,\cdots,x_n$を消去していき，最後にすべての変数が消去されて不定元$t_1,\cdots,t_m$だけの多項式が得られるならば，それが求める代数的関係であると言える。

変数$x_1,\cdots,x_n$の消去をEuclidean消去法で行う場合を考えよう。x_nを主変数に選び，x_nをすべて消去すると結果は終結式で表わすことができる。たとえば

$$P_2^{(1)}=res_{x_n}(P_1,P_2),\cdots,P_m^{(1)}=res_{x_n}(P_1,P_m)$$

はx_nを含まない。ここで，res_xは変数xに関する終結式を表わす。この変数消去を繰り返せば，うまく行けば代数的関係が計算できる。

終結式を用いる方法はほとんどの場合非常に効率が悪い。このことを高橋氏の例(〔1〕を見よ)でみよう。氏の例の一つは

$$P_1=(z_1^6+z_2^6)+522(z_1^5z_2-z_1z_2^5)-10005(z_1^4z_2^2+z_1^2z_2^4),$$
$$P_2=-(z_1^4+z_2^4)+228(z_1^3z_2-z_1z_2^3)-494(z_1^2z_2^2),$$
$$P_3=z_1z_2(z_1^2+11z_1z_2-z_2^2)^5,$$

である。これらP_1,P_2,P_3の間には次の代数的関係が存在する：

$$P_1^2+P_2^3-1728P_3^2=0.$$

この代数的関係は z_1, z_2 に関して12次である。しかしながら，

$p_1^{(1)} = res_{z_2}(p_2, p_1) = (z_1$ に関して32次以上，t_2 に関して6次の多項式)，
$p_3^{(1)} = res_{z_2}(p_2, p_3) = (z_1$ に関して44次以上，t_2 に関して11次の多項式)，
$p_3^{(2)} = res_{z_1}(p_1^{(1)}, p_3^{(1)}) = (t_2$ に関して32×11次以上の多項式)，

となってしまう。これではたまらない。

上記の高橋氏の例をBuchberger消去で計算してみよう。Buchberger消去は順序の選び方に任意性があり，目的によっては特定の順序を選ばなければならないが，今の場合には消去さえできればどんな順序でもよい（次節の理由づけを参照）。このような時は，計算量の観点からは全次数一斉書式順序を選ぶのが断然得である。以下は高橋氏の記号Eを用いて計算機で消去を実行した結果である。

{P1 ← p1 - T, P2 ← p2 - H, P3 ← p3 - F}.

Step 1. P1 ← P1のP2によるM-簡約，P3 ← P3のP2によるM-簡約，
P4 ← SPOL(P1, P2) ..... P1とP2のS-多項式：

```
P4 := 8179489500*Z1^3*Z2^4 - Z1^3*H - 17931004500*Z1^2*Z2^5 - 750*Z1^2*Z2*H -
      8259118500*Z1*Z2^6 - 160501*Z1*Z2^2*H - Z1*T - 36223500*Z2^7 -
      36223500*Z2^3*H
```

Step 2. P4 ← P4のP1によるM-簡約，P3 ← P3のP4, P2によるM-簡約，
P5 ← SPOL(P1, P4) ..... P1とP4のS-多項式：

```
P5 := 606841*Z1^4*H + 318102313*Z1^3*Z2*H - 20588477025000*Z1^2*Z2^6 -
      5372966109*Z1^2*Z2^2*H + 606841*Z1^2*T - 8270763525000*Z1*Z2^7 -
      11465478437*Z1*Z2^3*H - 137028437*Z1*Z2*T - 36224850000*Z2^8 -
      36225075700*Z2^4*H - 225700*Z2^2*T
```

Step 3. P5 ← P5のP4, P2によるM-簡約，P3 ← P3のP5, P1, P4によるM-簡約，
P6 ← SPOL(P4, P5) ... P4とP5のS-多項式：

```
P6 := 396751091982*Z1^4*Z2*H - 5645961748797*Z1^3*Z2^2*H + 529230388*Z1^3*T
      + 1625834365479*Z1^2*Z2^3*H - 120836227482*Z1^2*Z2*T +
      443132049375000*Z1*Z2^8 - 5871990816651*Z1*Z2^4*H + 300642169987*Z1*
      Z2^2*T - 529230388*Z1*H^2 + 1894123125000*Z2^9 + 1917381899175*Z2^5*H
      + 23258774175*Z2^3*T
```

Step 4. $P_6 \leftarrow P_6$ の P_2, P_5 による M－簡約，
$P_3 \leftarrow P_3$ の P_6, P_4, P_1, P_2, P_5 による M－簡約：

```
P36 := 583971589262*( - 1728*F + H^3 + T^2)
```

目出度く，最低次の代数的関係が非常に少ない手間で得られた。（上記では，分り易さのため，Buchberger 消去を M－簡約と S－多項式に区別して呼んだ。）
なお，上述の計算が簡単に行えたのは，問題そのものが簡単な代数的関係を有していることを除けば，全次数一斉書式が効いていることを再度強調したい。

4. 理論的裏付

前節で述べた方法がアルゴリズムとして成立するには，
① 手続きが有限回の手順で終了する，
② 代数的関係が存在する場合には関係式を生成する，
③ 代数的関係が存在しない場合にはそのことを判定できる，
の3条件が満たされる必要がある。以下，これらの点を証明しよう。

4.1. アルゴリズムの停止性

我々の方法は $Q(t_1, \cdots, t_m)[x_1, \cdots, x_n]$ 内のイデアル $(P_1 - t_1, P_2 - t_2 \cdots, P_m - t_m)$ の Gröbner 基底を計算していることに他ならない。したがって，Gröbner 基底の一般論から，我々の手順は有限回の回数で停止することが保障される。

4.2. 代数的関係が生成され得ること

イデアル $I = (P_1 - t_1, P_2 - t_2, \cdots, P_m - t_m)$ の Gröbner 基底を

$$\{\tilde{P}_1, \tilde{P}_2, \cdots, \tilde{P}_e\}, \quad \text{ただし } \tilde{P}_i \in Q[t_1, \cdots, t_m][x_1, \cdots, x_n],$$

とする。すなわち，Buchberger 消去においては $x_1, \cdots, x_n$ のみならず，$t_1, \cdots, t_m$ も多項式的に扱うのである。今，Gröbner 基底のどれかの要素，たとえば，$\tilde{P}_e$ が $x_1, \cdots, x_n$ を含まないとしよう。このとき

$$\alpha_1 \cdot (P_1 - t_1) + \alpha_2 \cdot (P_2 - t_2) + \cdots + \alpha_m (P_m - t_m) = \tilde{P}_e \in Q[t_1, \cdots, t_m]$$

なる多項式 $\alpha_1, \alpha_2, \cdots, \alpha_m$ が存在する。この式において $t_i = P_i$, $i = 1, \cdots, m$, とおくと $\tilde{P}_e = 0$ となる。すなわち $\tilde{P}_e$ は求める関係である。

4.3. 代数的関係の存在性の判定

さて，上記の Gröbner 基底のどの要素も変数 $x_1, \cdots, x_n$ のどれかを含むとし，この場合にも $P_1, P_2, \cdots, P_m$ の代数的関係 $\tilde{R}(P_1, \cdots, P_m) = 0$ が存在すると仮定してみよう。このとき，$\tilde{R}(P_1, \cdots, P_m) \equiv \tilde{R}(t_1, \cdots, t_m) \pmod{I}$ ゆえ，$\tilde{R}(t_1, \cdots, t_m) \equiv 0 \pmod{}$ となる。すなわち，$\tilde{R}(t_1, \cdots, t_m) \in I$ であるから，

$$\beta_1 \cdot \tilde{P}_1 + \beta_2 \cdot \tilde{P}_2 + \cdots + \beta_e \cdot \tilde{P}_e = \tilde{R} \in Q[t_1, \cdots, t_m]$$

を満たす多項式 $\beta_1, \cdots, \beta_e$ が存在しなければならない。Gröbner 基底の性質によると，任意の多項式は Gröbner 基底で M－簡約することにより，（基底の要素で展開できる部分）＋（一意的な正規形）の形に分解できる。ところが，$\tilde{R}$ は $x_1, \cdots, x_n$ を含まないから，これらの変数を含む $\tilde{p}_1, \cdots, \tilde{p}_e$ ではもはや M－簡約できない。すなわち，上記の線形方程式は多項式解をもたず，したがってこのような $\tilde{R}$ は存在しえず，代数的関係のないことがわかる。

4.2と4.3を合わせると②と③が主張できる。なお，Buchberger 消去に基づく方法は，計算量は別にしても，m と n の大小関係に依存しないという点でも終結式法より一般性がある。Buchberger 消去では，m と n の大小関係にかかわらず，代数的関係は，もし存在すれば，生成される。しかしながら，終結式法では $m > n$ の場合は問題ないが，$m \leqq n$ の場合には，原理的には $p_1, \cdots, p_m$ のあらゆる組合せについて終結式を作ってみなければ，代数的関係を見落とす可能性がある。

5．多変数多項式の GCD の計算

多変数多項式 P_1 と P_2 が与えられたとき，$GCD(P_1, P_2)$ の次数は P_1 と P_2 の次数のいずれよりも小さい。従って，全次数一辞書式順序で P_1 と P_2 の最高順位項から順に Buchberger 消去をしていけば，$GCD(P_1, P_2)$ が計算できるのではと予想される。この予想は実際は正しく，次の定理が成立する。

> 〔定理（〔5〕参照）〕 イデアル $(P_1, P_2, \cdots P_m)$，ただし $P_i \in Q\{x_1, \cdots x_n\}$，の Gröbner 基底を $\{\tilde{p}_1, \tilde{p}_2, \cdots, \tilde{p}_e\}$ とする。この基底において，全次数が最低の要素の中には $\tilde{p}_i = GCD(P_1, P_2, \cdots, P_m)$ なるものが存在する。

（本定理は最近の Springer Lecture Notes に載っている。しかし，筆者らが本テーマを思いついた時点ではこの本は入手不可能であった。）

以上より，残る問題は上記の GCD 計算法の効率化と他の方法との優劣の比較である。残念ながら筆者らはこの問題にまだ手をつけていないが，上記の方法には期待を抱いている。それは，一般的に言って，Buchberger 消去法は Euclidean 消去法より効率がよいし，変数の順序づけや消去順の選び方に任意性が多くあり，うまく消去を進めれば計算量を大巾に減らせる可能性があるからである。

〔1〕高橋正，理研シンポジウム「代数的計算法」講演録，昭和60年2月，p.10.
〔2〕B. Buchberger, Ph.D. Thesis, Univ. of Innsbruck (Austria), 1965
〔3〕B. Buchberger, "Gröbner bases", in Recent Trends in Multidimensional Systems Theory, N.K. Bose (ed), D. Reidel Publ. Comp. 1985
〔4〕D.S. Arnon & T.W. Sederberg, "Implicit equations for parametric surfaces by Gröbner basis", Proc. 1984 MACSYMA User's Conf. P.431
〔5〕G. Giani & B. Trager, "GCD's and factoring multivariate polynomials using Gröbner bases," Lect. Notes Comp. Sci. 204, P.409. 1985