数理解析研究所講究録 1395 巻 2004 年 8-15

8

パラメーターが指数部に現れる連立代数方程式について

横山 和弘
九州大学数理学研究院
福岡市東区箱崎 6-10-1
yokoyama@math.kyushu-u.ac.jp

1 はじめに

数学研究では、指数部や係数部にパラメーターを持つ代数方程式が現れることが多い。係数にパラメーターが現われる場合には、解の存在や安定性の計算等について、いくつかの興味深い研究 ([7, 8]) があるが、指数部の場合に関してはほとんど研究されていない。そこで、本論文では、指数部にパラメーターを持つ連立代数方程式の解のある種の計算可能性、安定性等を扱い、対応するイデアルの Gröbner 基底の計算可能性や安定性に置き換えて議論する。本研究は、高橋正 (神戸大学) による代数曲面の特異点の非退化条件の計算による証明 [6] に触発されたものである。以下に特徴的な例をあげておく。

例 1 $S_{k,0}$ *[1, 6]* の特異点を調べたい。ここで、

$$f = x^2z + yz^2 + y^{4k+1} + axy^{3k+1} + bzy^{2k+1}$$

であり、k は正整数、a, b は複素数である。この場合には、以下の連立代数方程式を考えることとなる。

$$f = \frac{\partial f}{\partial x} = \frac{\partial f}{\partial y} = \frac{\partial f}{\partial z} = 0.$$

パラメーター k は係数部にも現れるため、より複雑な問題となっている。

まず、本論文の問題設定と目標をあげる。

目標 有理数体 $\mathbb{Q}$ を係数体とする多項式環を考える。パラメーターを指数部に持つ有限個の多項式から生成されるイデアル $\mathcal{I}$ に対して、以下の性質を調べたい。ここで、各パラメーターに対して、その値を固定すれば、既約 Gröbner 基底 ([2, 3]) は固定された項順序に対して一意的に定まり、計算も可能であることに注意しておく。

(1) **安定性:** パラメーターの値が十分に大きい時、$\mathcal{I}$ の Gröbner 基底の形が安定するか？もしくは、その形がパラメーターの値に対して uniformly に決まるか？(イデアルではなく、解について考えたい場合には、イデアルの根基を考えることになろう。)

(2) **計算可能性:** $\mathcal{I}$ の Gröbner 基底の形がパラメーターの値が十分に大きい時に安定する場合には、それを計算するアルゴリズムがあるか？つまり、計算のステップ数がパラメーターの値によらないで有限回で停止するようなアルゴリズムがあるか？

一般論として、ランダムに指数部にパラメーターを持つような多項式を作り、それらによって生成されるイデアルを考えた場合、そのイデアルが安定性や uniformity を持つことは考えられない。しかし、確実に安定性や uniformity を持つような特殊なイデアルのクラスが存在する。そのようなクラスとして、より広範囲であり、より応用が可能なものを探すことは非常に重要であろう。本論文では、この難しい問題への最初の挑戦として、最も単純と考えられる一変数の場合を取り上げ、その場合に肯定的な結果が得られたことを示す。(多変数ではあるがイデアルとしては 0 次元になる場合にも同様になる。) 具体的には、より複雑な場合を捉えるために、この簡単な場合の考察により得られた知見をもとに単純ではあるが基本的と思われる定式化を行った。本論文では、詳しい証明等を省いているので、完全な内容のものとして、[10] を参照されたい。

一個のパラメーターを持つ問題への別のアプローチとして、Volker Weispfenning (Passau 大学) は、高橋に触発され、単項式と 2 項式から生成される場合を扱い、完全な結果を導出している ([9])。彼の手法は本論文での方法とは独立であり、複雑な問題を扱うためのステップとして、補間しあうものと考える。

2 定式化と計算技法

問題設定 多項式環 $\mathbb{Q}[X]$ を考える。ここで、$X = \{x_1, \ldots, x_n\}$ を変数の集合とする。ここでは、パラメーターを指数部に含む多項式をパラメーターが固定した値を持つ (しかし未知である) 普通の多項式として考える。つまり、パラメーターは変数として扱わないものとする。さらに、指数は必ず非負であるので、パラメーターには条件が付くが、適当な shift で パラメーターはすべての正整数を動くものと仮定しておく。

定義 1 (Ep-Power Product and Ep-Ideal) パラメーターを指数部に持つ *power product* を ep-power product と呼び、*ep-power product* を因子に持つ項 *(term)* を ep-term と呼ぶことにする。更に、*ep-term* を項に持つ多項式を ep-polynomial と呼ぶ。イデアルが *ep-polynomial* をその生成集合に持つ時、そのイデアルを ep-ideal と呼ぶ。*ep-polynomial*、*ep-ideals* と区別するため、*ep-term* を項に持たない多項式を ordinary polynomial と呼び、*ordinary polynomial* だけで生成されるイデアルを ordinary *ideal* と呼ぶ。

例 2 *例 1* の多項式

$$f = x^2z + yz^2 + y^{4k+1} + axy^{3k+1} + bzy^{2k+1}$$

は、*ep-polynomial* で $\mathbb{C}[x, y, z]$ に属する。ここで、a, b は固定しているものとする。y^{4k+1}、axy^{3k+1}、bzy^{2k+1} が *ep-terms* である。

例 2 では、y^k が本質的であろう。というのは、y^k を新しい変数 w で置き換えることにより、以下の ordinary polynomial に変換できるからである。

$$g = x^2z + yz^2 + w^4y + axw^3y + bzw^2y.$$

定義 2 (Essential Set) *ep-polynomial* f に対して、*ep-power product* の集合 $\{T_1, \ldots, T_s\}$ で、各 T_i を別の新しい変数 y_i に置き換えると *ordinary polynomial* が得られるときに、$\{T_1, \ldots, T_s\}$ を f の essential set と呼ぶ。さらに、イデアル $\mathcal{I}$ の生成集合 G に対して、*ep-power product* の集合 $\{T_1, \ldots, T_s\}$ がすべての G の元の *essential set* である時に、$\{T_1, \ldots, T_s\}$ を $\mathcal{I}$ の essential set と呼ぶ。*(f に対しては、いろいろな essential set が存在する。)* 余剰な元を取り除いたものを *essential set* と呼ぶこともできよう。

安定性を定義するために Gröbner 基底の形について議論する。以下、項順序 $\prec$ を固定して考える。$\mathcal{I}$ を ep-ideal とし、その生成集合 $\mathcal{F}$ には ep-polynomial が含まれているとする。さらに、$K = (k_1, \ldots, k_t)$ を $\mathcal{I}$ に現われるパラメーターの集合とする。(ここで、$\mathcal{I} = (\mathcal{F})$ と書く.) 各ベクトル $A = (a_1, \ldots, a_t) \in \mathbb{N}^t$、

ここで $\mathbb{N}$ を自然数全体の集合とする、に対して、$G(A)$ を A を K に代入したときの $\mathcal{I}$ の既約 Gröbner 基底とする。

定義 3 (Gröbner 基底の安定性) イデアル $\mathcal{I}$ が stable *Gröbner* 基底 を持つとは、あるベクトル $B = (b_1, \ldots, b_t) \in \mathbb{N}^t$ が存在して、以下のどれかが成り立つ時にいう。この B を bound と呼ぶことにする。

(1) ***Generic Form:*** $a_i \geq b_i$ となるすべてのベクトル $A = (a_1, \ldots, a_t)$ に対して、$G(A)$ の元の個数はパラメーター K の値 A によらずに一定であり、各元の個数もパラメーター K の値 A によらずに一定であり、さらに、*"comprehensive"* となる。つまり、各元は固定された *ep-terms* と *ordinary terms* の和で表され、パラメーター K の各固定値 A に対しては、既約 *Gröbner* 基底 $G(A)$ は、単純に、それらの *ep-term* の K に A を代入することで得られる。このような場合に、$G(A)$ は generic form であると言う.

(2) ***Periodic Form:*** あるベクトル $P = (p_1, \ldots, p_t) \in \mathbb{N}^t$ が存在して、$a_i \geq b_i$ なる各ベクトル $A = (a_1, \ldots, a_t)$ に対して、$G(A)$ は値 $(a_1 \bmod p_1, \ldots, a_s \bmod p_s)$ により一意的に定まる。この場合に、$G(A)$ を periodic form であると言い、P を period と呼ぶ。特別な場合として、$G(A)$ が値 A に依らず決る時に、$G(A)$ を completely stable form と呼ぶ。

(3) ***Bounded Form:*** $a_i \geq b_i$ であるベクトル $A = (a_1, \ldots, a_t)$ に対して、$G(A)$ が自明になる $(G(A) = \{1\})$。この場合に、$G(A)$ を bounded form であると言う。この場合は、 completely stable form の特別な場合でもある.

periodic form (bounded form を含む*)* を総称して finite form と呼ぶ。これは、すべての *Gröbner* 基底の元の次数がある固定した値で上から評価されているからである。

さらに、イデアル $\mathcal{I}$ が semi-stable *Gröbner* 基底を持つとは、$\mathcal{I}$ が *stable Gröbner* 基底を持ついくつかのイデアルの交わりとなっている時に言う。ここで、*ordinary ideal* は、いつでも *stable Gröbner* 基底を持つと考えることにする。

例 3 以下は自分自身で生成されるイデアルの *Gröbner* 基底になっている。ここで、項順序は辞書式順序 $x_1 \prec x_2 \prec x_3$ とする。このとき、それ自身は *generic form* となっている。

$$f_1 = x_1^{k+2} + 1,\ f_2 = x_2 - x_1^{k+1} - x_1 + 1,\ f_3 = x_3 - x_1^k - 1$$

例 4 *(1)* イデアル $\langle x^k - 1, x^2 + x + 1 \rangle$ は $k \equiv 0 \pmod 3$ の時に $\langle x^2 + x + 1 \rangle$ となり、それ意外の場合では、$\langle 1 \rangle$ となる。これは、*periodic case* となる。

(2) イデアル $\langle x^k - 5x + 2, x^2 + x - 6 \rangle$ は $k = 3$ の時だけ $\langle x - 2 \rangle$ となり、それ以外の場合には、$\langle 1 \rangle$ となる。これは、*bounded case* となる。

(3) イデアル $\langle x^{k+1} - x^k + x^2 - 1, x^2 + x - 2 \rangle$ は、すべての $k \geq 1$ に対して、$\langle x - 1 \rangle$ となる。これは *completely stable case* である。

2.1 適応可能な計算技法

指数部にパラメーターを含む連立代数方程式を解くこと、つまり対応する ep-ideal の Gröbner 基底を計算することに対して大変重要かつ有効な計算技法を二つ挙げる。以下では、$\mathcal{I}$ を ep-ideal とし、その与えられた生成集合を $\mathcal{F} = \{f_1, \ldots, f_r\}$ とする。また、$\mathcal{T} = \{T_1, \ldots, T_s\}$ を essential set とする。(elimination ideal については [4, 3] を、comprehensive Gröbner 基底については [7, 8] を参照。)

Slack Variables and Elimination: $\mathcal{I}$ の Gröbner 基底が finite form である時には、生成する多項式に現われるすべての ep-power product を消去することが有効であろう。

まず、生成集合 $\mathcal{F}$ において、ep-power product $T_1,\ldots,T_s$ を新たな slack variables $y_1,\ldots,y_s$ に置き換える。この操作により、新たな多項式集合 $\mathcal{F}_0$ (すべて ordinary polynomial) が得られる。つまり、各 f_i に対して、新たな多項式 $f_{i,0}(X,Y)$ が得られ、そこでは $f_{i,0}(X,T)=f_i(X)$ となっている。

$\mathcal{I}_0$ を $\mathbb{Q}[X,Y]$ における $\mathcal{F}_0$ で生成されるイデアルとする。ある elimination order $X \prec\prec Y$ を固定して、elimination ideal $\mathcal{J}=\mathcal{I}_0\cap\mathbb{Q}[X]$ を計算する。この時、すべての $\mathcal{J}$ に属する多項式は、ep-ideal $\mathcal{I}$ に属する ordinary polynomial である。そこで、H を $\mathcal{J}$ の Gröbner 基底とする。

補題 1 H は $\mathcal{I}$ に含まれる。つまり、$\mathcal{J}$ は $\mathcal{I}$ に含まれる。

定義 4 上記の *elimination ideal* $\mathcal{J}$ を finite subideal *of* $\mathcal{I}$ と呼ぶ。*($\mathcal{J}$ は $\mathcal{T}$ の選び方に依存する.)*

もし、finite subideal $\mathcal{J}$ が 0-dimensional であれば、$\mathcal{I}$ の Gröbner 基底は finite form であり、それを計算する方法が存在する。(詳細は後で述べる。)

一方、零点を計算したい場合には、単純に Gröbner 基底を計算するより効率的な方法がある。$\mathcal{J}\subset\mathcal{I}$ であるので、零点集合 $V(\mathcal{J})$ は $V(\mathcal{I})$ を含むことになる。したがって、すべての $\mathcal{I}$ の零点は、$\mathcal{J}$ の各零点に対して、それらが元来与えられた生成集合 F を満たすかどうかを検査すればよいからである。この方法は、$V(\mathcal{J})$ が有限集合の場合、すなわち $\mathcal{J}$ が 0-dimensional の場合には、極めて有効であろう。

さたに、$\mathcal{J}$ の素イデアル分解 (prime decomposition) を使う方法もある。(詳しい計算法については [3, 5] を参照.) $\mathcal{J}$ の 各素因子 $\mathcal{P}$ に対して、$\mathcal{I}+\mathcal{P}$ を計算すればよい。その後で、すべての素因子 $\mathcal{P}$ に対する $\mathcal{I}+\mathcal{P}$ らの結果を集めて、最終的な結果を得ることができる。

例 5 *例 1 の ep-polynomial* $S_{k,0}$ では、

$$f=x^2z+yz^2+y^{4k+1}+axy^{3k+1}+bzy^{2k+1}$$

とその偏微分が生成集合であるので、$\{y^k\}$ が *essential set* となる。そこで、y^k を新たな変数 w に置き換えて、4 変数の *ordinary ideal* f_0,f_1,f_2,f_3 を得る。*(ここでは、a,b,k を変数と考えて、つまり、ここでは係数のパラメーター a,b,k に対して "generic case" しか考えないこととする。)* 次に、*elimination ideal* $\mathcal{J}$ を計算する。つまり、多項式環 $\mathbb{Q}(a,b,k)[x,y,z,w]$ の中で、$\langle f_0,f_1,f_2,f_3\rangle$ から w を消去する。

辞書式順序 $w\succ z\succ y\succ x$ により、$\mathcal{J}$ を計算し、その素因子をすべて求める。結果、$\mathcal{J}$ は二つの素因子 $\langle x,y\rangle$、$\langle x,z\rangle$ を持つことが分かる。そこで、元の問題を $x=y=0$ の場合と $x=z=0$ の場合の二つの場合に分ける。結果として、

$$x=y=0\rightarrow z=0,\ x=z=0\rightarrow y=0$$

を得る。つまり、$\langle x,y,z\rangle$ が *ep-ideal* $\mathcal{I}$ の根基となることが示された。以上の計算は、*"generic case"* に対応するものであり、a,b,k は特定の代数方程式を満足しないと仮定した場合の結果であるが、実際の方程式は、$a\neq 0$ かつ $b\notin\{0,2,-2\}$ になる。*([6] を参照)*。このような係数にもパラメーターが現われる連立代数方程式を正確に解く方法として、*Chapter 6 Section 3 in [4]* もしくは、*comprehensive Gröbner basis computation [7, 8]* を参照されたい。

パラメーター付きのイデアルの Gröbner 基底の可能な形を分類したいのであれば、Comprehensive Gröbner Basis[7, 8] の概念を利用することができよう。単項式と 2 項式により生成される ep-ideals に対しての最近の結果 [9] を参考されたい。

Comprehensive Gröbner basis: Buchberger 算法 [2, 4, 3] をステップ毎に実行することで、計算が可能な場合も有り得る。ここでは、各ステップにおいて、どの項が leading term になるかを逐次判定しなくてはならない。つまり、各ステップにおいて、パラメーター の値により様々な場合に分岐して行く。

例 6 もし、2 個の *ep-term* y^{3k+2}、y^{2k+20} が途中の式に現われたとしよう。2 つの項の順番は k の値に依存して、以下のようになる。

$$k>6 \rightarrow y^{3k+2} \succ y^{2k+8},\ k<6 \rightarrow y^{3k+2} \prec y^{2k+8},\ k=6 \rightarrow \textit{we must merge } y^{3k+2} \textit{ and } y^{2k+8}.$$

最も本質的な問題は Buchberger 算法 (ここで、monomial reductions も含むとして) が有限回 (パラメーターの値に依存しない回数) の操作で終了するかである。もちろん、Buchberger 算法の計算量がパラメーターの値に依存する場合がある。

例 7 例えば、$f(x,y)=x^k-1,\ g(x,y)=xy-y-1$ を考えてみよう。ここで、辞書式順序 $y \succ x$ について、既約 *Gröbner* 基底は

$$\{x^{k-1}+x^{k-2}+\cdots+1, x^{k-2}+2x^{k-3}+\cdots+(k-1)+ky\}$$

となる。これは、*Buchberger* 算法は少なくとも k 回の *monomial reduction* を必要としている。

以下、一個のパラメーターがひとつの変数の指数部のみに現われる、つまり、唯一の essential set を持つという、最も単純な場合を考える。

3 一変数の場合の安定性

一変数多項式環 $\mathbb{Q}[x]$ の中で ep-ideal $\mathcal{I}$ を考え、$\{x^k\}$ が $\mathcal{I}$ の唯一の essential set とする。一般には、$\mathcal{I}$ が (semi-)stable Gröbner 基底を持つとは限らないが、この場合には、必ずそのような安定性を持つ。

問題設定 essential set $\{x^k\}$ を持つ $\mathbb{Q}$ 上の ep-polynomial $f(x), g(x)$ に対して、$\gcd(f(x),g(x))$ を計算したい。この多項式は $\mathcal{I}=\langle f(x),g(x)\rangle$ の Gröbner 基底に他ならない。(ここで、k は係数には現われないものとする。) さらに、簡単のために、$f(x)$ と $g(x)$ の定数は 0 でないとする。(因子 x を $f(x)$、$g(x)$ から前もって取り除いておく。)

定理 1 $f(x), g(x)$ より計算できる正の整数 P, B が存在し、以下を満たす。k の各値 $a \geq B$ に対して、$\gcd(f(x),g(x))$ は、*"generic form factor"* と *"finite form factor"* の積で表され、*finite form factor* は $a \bmod P$ の値により一意的に定まる。すなわち、*ep-ideal* $\mathcal{I}$ は *semi-stable Gröbner* 基底を持つ。

以下では、$\gcd(f(x),g(x))$ を計算する具体的な手続きを与える。まず、x^k を新しい変数 y に置き換え、f, g から 2 変数多項式 f_0, g_0 を構成する。つまり、$f(x)=f_0(x,x^k)$ であり、$g(x)=g_0(x,x^k)$ である。2 変数多項式として $\gcd(f_0(x,y),g_0(x,y))$ を計算し、それを $h_0(x,y)$ とおく。この時、$h(x)=h_0(x,x^k)$ は $f(x), g(x)$ の共通因子になる。そこで、$h(x)$ を *generic form factor* と呼ぶことにする。(もちろん、$h(x)$ 自身が ordinary polynomial であることもありうる。)

次に、$f'(x)=f(x)/h(x)$ と $g'(x)=g(x)/h(x)$ を考え、$\gcd(f'(x),g'(x))$ を計算する。f', g' で、再び x^k を新しい変数 y に置き換え、f', g' より、2 変数多項式 f_1, g_1 を構成する。つまり、$f'(x)=f_1(x,x^k)$ であり、$g'(x)=g_1(x,x^k)$ となる。$f_0=f_1h_0$ かつ $g_0=g_1h_0$ であるので、f_1 と g_1 は 2 変数として、共通因子を持たない。そこで、終結式 $\mathrm{res}_y(f_1,g_1)$ は 0 にはならず、変数 x に関する ordinary non-zero polynomial

となり、更に、$\langle f_1(x,y), g_1(x,y)\rangle$ に属する。finite subideal $\langle f_1(x,y), g_1(x,y)\rangle \cap \mathbb{Q}[x]$ を考えると、これは $\{0\}$ ではない。そこで、$m(x)$ をその生成元とする。$m(x)$ は $\langle f'(x), g'(x)\rangle$ に属することが補題 1 より示される。$m(x)$ が定数の時 (0 ではない) は、$\langle f'(x), g'(x)\rangle = 1$ となり、$f'(x), g'(x)$ には共通因子がないことがわかる。

以下、$m(x)$ が定数ではない場合を考える。$m(x)$ を $\mathbb{Q}$ 上で因数分解し、既約因子 $m_i(x)$ を計算する。

$$m(x) = \prod_{i=1}^{r} m_i(x)^{e_i}.$$

$m(x)$ はイデアル $\langle f'(x), g'(x)\rangle$ に属し、$m_i(x)^{e_i}$ らは互いに素であるので、

$$\gcd(f', g') = \gcd(f', g', m) = \prod_{i=1}^{r} \gcd(f', g', m_i(x)^{e_i}).$$

を得る。従って、gcd 計算は $\gcd(f', g', m_i(x)^{e_i})$ 計算に帰着される。(ここで、x を既約因子からは除いていることに注意しておく。) 既約因子 $m_i(x)$ を以下の二つの場合に分ける:

定義 5 ある正整数 p が存在して、$m_i(x)$ が $x^p - 1$ の因子の時、$m_i(x)$ を cyclotomic factor と呼ぶ。さらに、$m_i(x)$ が $x^p - 1$ を割るような最小の正整数 p を $m_i(x)$ の period と呼ぶ。(このとき、$m_i(x)$ は *cyclotomic polynomial* である。) そうでない時、$m_i(x)(\neq x)$ を non cyclotomic factor と呼ぶ。

$m_i(x)$ の period P_i は、$\deg(m_i) = \phi(P_i)$ であるので、$\deg(m_i)$ のある関数として上から評価されることに注意する。(簡単な例では、$P_i < 2\deg(m_i)^2$ となる。) よって、各 $m_i(x)$ が cyclotomic factor であるかどうか、そしてその場合の period P_i は、P_i の上からの評価を計算し、それ以下の各正整数 n において、$x^n - 1$ が m_i で割り切れるかどうかを調べればよいことが分かる。

Cyclotomic Case ここでは、$m_i(x)$ を period P_i とする cyclotomic factor とする。

命題 1 $\gcd(f'(x), g'(x), m_i(x))$ は $k \bmod P_i$ の値により一意的に定まる。

$\gcd(f(x), g(x))$ が $m_i(x)$ を因子として持つかどうかは単純に各 $a \in \{0, 1, \ldots, P_i - 1\}$ に対して、$f'_a(x)$ と $g'_a(x)$ を $m_i(x)$ で割ることで判定できる。($f'_a(x)$ と $g'_a(x)$ は、$f'(x)$ と $g'(x)$ において、a を k に代入することで得られる。) そこで、もし、$e_i = 1$ であれば、これで終了することになる。

$e_i > 1$ の場合には、$\gcd(f'(x), g'(x)) = m_i(x)^e$ となる指数 e の計算に、微分 "derivatives" を利用して、同様の操作を行なう。ここでは、例のみを示し、詳細を省略する。([10] を参照されたい。)

注意 1 微分 $\frac{d^e f'_a}{dx^e}$ と $\frac{d^e g'_a}{dx^e}$, に対して、すべての指数部は非負でなければならない。したがって、条件 $k \geq e_i$ が必要となり、代入計算においては、ある正整数 d を導入して、$a + dP_i$ を使うこともある。この変更により、小さい値 $k < e_i$ に対しては, $\gcd(f'(x), g'(x), m_i(x)^{e_i})$ を個別に計算することになる。

命題 2 ある正の整数 M_i が存在して、$k > M_i$ であれば、$\gcd(f'(x), g'(x), m_i(x)^{e_i})$ が $k \bmod P_i$ の値により一意的に定まる。さらに、M_i は $f(x), g(x), m_i(x)$ より計算される。

例 8 例として、以下を考える。

$$f(x) = x^{3k} - 2x^{k+6} + 1,\ g(x) = (x^k - 1)^2 + (x^2 + x + 1)^2$$

elimination ideal は $m(x) = (x^2 + x + 1)^2 m'(x)$ により生成され、$m'(x)$ は *non cyclotomic factor* である。また、$k \equiv 0 \pmod 3$ に対して、$f(x), g(x)$ は $x^2 + x + 1$ で割り切れる。さらに、微分を考えれば、

$$\frac{f(x)}{dx} = 3kx^{3k-1} - 2(k+6)x^{k+5},\ \frac{g(x)}{dx} = 2kx^{k-1}(x^k - 1) + 2(x^2 + x + 1)(2x + 1)$$

より、$k=3s$ とおいて ($s \geq 1$)、指数部の k に 3 を代入する。

$$\frac{f(x)}{dx} \to (3s-12)x^8, \quad \frac{g(x)}{dx} \to 2sx^2(x^3-1)+2(x^2+x+1)(2x+1).$$

終結式計算により、$k=12$ の時のみ, つまり $s=4$ の時のみ、$f(x), g(x)$ は $(x^2+x+1)^2$ で割り切れる。

Non Cyclotomic Case 各 non cyclotomic factor $m_i(x)(\neq x)$ に対して以下を得る。

命題 3 ある正の整数 B_i が存在して、$\gcd(f'(x), g'(x), m_i(x)^{e_i})$ は すべての $k > B_i$ に対して自明なものとなる。さらに、B_i は $f(x), g(x), m_i(x)$ より計算される。

実際の手続きは以下で与えられる。

PROCEDURE [NON CYCLOTOMIC CASE]

1. Compute a root α of $m_i(x)$ with rigorous error analysis and compute a correct bound A on $|\alpha|$ so that
   - $|\alpha| > A > 1$ if $|\alpha| > 1$, and
   - $|\alpha| < A < 1$ if $|\alpha| < 1$.
2. Compute $F(y), G(y)$ by
$$\begin{aligned} F(y) &= \mathrm{res}_x(f_1(x,y), m_i(x)) \\ G(y) &= \mathrm{res}_x(g_1(x,y), m_i(x)). \end{aligned}$$
3. If $F(y) \neq 0$, then compute a bound D on the absolute value of roots of $F(y)$ so that
   - $D > |\beta|$ for any root β of $F(y)$ if $|\alpha| > 1$, and
   - $0 < D < |\beta|$ for any non-zero root β of $F(y)$ if $|\alpha| < 1$.

   If $F(y) = 0$, then compute a bound D on the absolute value of roots of $G(y)$ so that
   - $D > |\beta|$ for any root β of $G(y)$ if $|\alpha| > 1$, and
   - $0 < D < |\beta|$ for any non-zero root β of $G(y)$ if $|\alpha| < 1$.
4. Compute the smallest positive integer B_i such that
   - if $|\alpha| > 1$, $A^{B_i} > D$, and
   - if $|\alpha| < 1$, $A^{B_i} < D$.

   Then, $\gcd(f'(x), g'(x), m_i(x))$ is trivial if $k > B_i$.
5. Substituting $1, ..., B_i$ for k, compute
$$\gcd(f'(x), g'(x), m_i(x))$$
   and return them. (B_i is updated to the largest integer $N \leq B_i$ such that $\gcd(f'(x), g'(x), m_i(x))$ is non-trivial. If it does not exist, we can set $B_i = 0$.)

例 9 以下の例を考える。

$$f(x) = x^{2k} + x^{2+k} + 2x^k + 2, \quad g(x) = x^2 + 2$$

$m(x) = x^2+2$ が *elimination ideal* の生成元となり、それ自身は既約である。$m(x)$ の根の絶対値は $\sqrt{2}$ となり、$F(y) = (y^2+2)^2$ の根の絶対値も同じく $\sqrt{2}$ となる。したがって、$A = \sqrt{2}$ かつ $U = \sqrt{2}$ を得、結果として、$B = 1$ を得る。これより、任意の $k \geq 2$ に対して、$\gcd(f(x), g(x)) = 1$ となる。また、$k = 1$ に対しては、$f(x) = x^3 + x^2 + 2x + 2$, $g(x) = x^2 + 2$ であったので、$\gcd(f(x), g(x)) = x^2 + 2$ を得る。

ここで、二つの場合、cyclotomic case と non-cyclotomic case を統合する。評価値 M_i, B_j と periods P_i を集めて、$P = \mathrm{LCM}(P_i \mid m_i$ is a cyclotomic factor), $B = \max\{M_i, B_j \mid m_i$ is a cyclotomic factor and m_j is a non-cyclotomic factor $\}$ とする。この P, B に対して定理 1 が成り立つ。

前節で行なった一変数での議論がそのまま適用できる場合として以下がある。

仮定 多変数多項式環 $\mathbb{Q}[x_1,\ldots,x_n]$ で、$\mathcal{F}=\{f_1,\ldots,f_r\}$ により生成される ep-ideal $\mathcal{I}$ が以下を満たす。

1. パラメーター は k のみで、essential set は唯一 $\{x_1^k\}$ とする。

2. SLACK VARIABLE AND ELIMINATION により計算される $\mathcal{I}$ の finite subideal $\mathcal{J}$ は 0次元である。

この時、一変数の場合と同様に、$\mathcal{I}$ の成分 (素因子) の Gröbner 基底を一変数の時と同様な方法で計算でき、結果として、以下を得る。

定理 2 仮定の下で、$\sqrt{\mathcal{I}}$ は *semi-stable な Gröbner* 基底を持つ。

4 まとめ

本研究では、指数部にパラメーターを持つイデアルの Gröbner 基底の安定性について、基本的と思われる概念を提示し、最も簡単な場合、すなわち、パラメーターが一つである一変数の場合と 0 次元の場合、に対して Gröbner 基底を計算する具体的な方法を提案した。しかしながら、提案した方法については、計算効率の解析も実例での計算機実験も行なっていない。そこで、次のステップとして、より精密な計算法を開発し、計算量解析と実例での計算機実験によりその有効性を確かめたい。また、安定性、計算可能性を持つ大きなクラスを見つけて行きたい。

謝辞 Passau 大学 Volker Weispfenning 教授、神戸大学高橋正教授とは、著者が文部科学省在外研究員として RISC-Linz 滞在中 (2003 年 7 月～9 月) に、パラメーターを指数部に持つイデアルの Gröbner 基底の安定性／計算可能性について非常に有益な議論を行ないました。この場を借りて、感謝の意を表します。さらに、RISC-Linz の Bruno Buchberger 教授には、RISC-Linz 滞在時の援助を深く感謝します。

参 考 文 献

[1] V.I. Arnol'd. Critical points of smooth functions and their normal forms. *Russian Math. Surveys* **30:5**:1-75, 1975.

[2] B. Buchberger. An algorithm for finding a basis for the residue class ring of a zero-dimensional polynomial ideal (German). PhD Thesis, University of Innsbruck, Institute for Mathematics, 1965.

[3] T. Becker, V. Weispfenning. *Gröbner Bases.* GTM **141**, Springer-Verlag, New York, 1993.

[4] D. Cox, J. Little, D. O'Shea. *Ideals, Varieties, and Algorithms.* UTM, Springer-Verlag, 1992.

[5] T. Shimoyama, K. Yokoyama. Localization and primary decomposition of polynomial ideals. *J. Symb. Comp.* **22**:247-277, 1996.

[6] T. Takahashi. An application of Gröbner bases for a hierarchical defining equation of singularity. preprint, 2003.

[7] V. Weispfenning. Comprehensive Gröbner bases. *J. Symb. Comput.*, **14**:1-29, 1992.

[8] V. Weispfenning. Canonical comprehensive Gröbner bases. In *ISSAC 2002*, pages 270-276. ACM Press, 2002.

[9] V. Weispfenning. Gröbner bases for binomials with parametric exponents, preprint, 2004.

[10] K. Yokoyama, On Systems of Algebraic Equations with Parametric Exponents. In *ISSAC 2004*, page 312-319. ACM Press, 2004.