

## real root counting に関する話題

九大・数理 木村欣司 (Kinji Kimura)

Faculty of Mathematics, Kyushu University

神奈川工科大・情報 平野照比古 (Teruhiko Hilano)

Faculty of Information Technology, Kanagawa Institute of Technology

早大・理工 荻田武史 (Takeshi Ogita)

Science and Engineering, Waseda University

京大・情報 山澤宏樹 (Hiroki Yamazawa)

Graduate School of Informatics, Kyoto University

東大・工学 曾我部知広 (Tomohiro Sogabe)

School of Engineering, The University of Tokyo

九大・数理 横山和弘 (Kazuhiro Yokoyama)

Faculty of Mathematics, Kyushu University

### 1 はじめに

Cylindrical Algebraic Decomposition を効率よく行うためには, 連立代数方程式系の実根の数を数える手法を確立する必要がある.[1] 我々は, 沢口一之が「古今算法記」(1671)の最後に出した遺題 15 問の中の第 14 問を題材に実根の数を数える手法の確立を試みる.[3] 沢口一之の問題を例題とする理由は, その難しさにある.

### 2 問題

平山諦著「関孝和 -その業績と伝記-」[4]の p.62 からは関孝和の著書「発微算法」について解説が書かれている. その平山の本の p.74-75 に以下の問題が紹介されている. しかし, 問題の起源は「発微算法」ではなく「古今算法記」である.

平面に 1 点を適当にとる. そのとき, 頂点からその 1 点にむかって線分をひく.

それぞれの辺の長さを文字で表す.

そのとき, 以下の関係式が成立することが知られている.

$$\begin{aligned}
 g_6 = & a^2d^2(b^2 + c^2 + e^2 + f^2) - a^2d^4 - a^4d^2 \\
 & + b^2e^2(a^2 + c^2 + d^2 + f^2) - b^2e^4 - b^4e^2 \\
 & + c^2f^2(a^2 + b^2 + e^2 + d^2) - c^2f^4 - c^4f^2 \\
 & - a^2b^2c^2 - a^2e^2f^2 - b^2f^2d^2 - c^2d^2e^2 = 0
 \end{aligned} \tag{1}$$

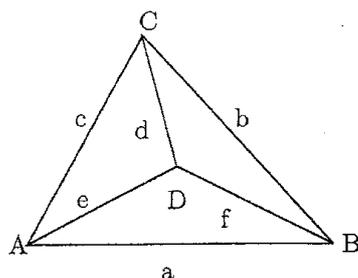


図 1: 問題の説明のための図

これは、グレブナー基底により定理自動証明できる。

これ以外にも以下の条件を課している。

$$g_1 = d^3 - b^3 - 271 = 0 \quad (2)$$

$$g_2 = b^3 - c^3 - 217 = 0 \quad (3)$$

$$g_3 = c^3 - a^3 - 60.8 = 0 \quad (4)$$

$$g_4 = a^3 - e^3 - 326.2 = 0 \quad (5)$$

$$g_5 = e^3 - f^3 - 61 = 0 \quad (6)$$

連立代数方程式系 (1)-(6) から  $f$  のみの式をもとめよ。というのが、沢口一之の問題である。しかし、この問題設定では現在の数式処理ソフト特に Risa/Asir では容易に計算できる問題である。参考までに、関孝和は解き方を説明しているのみであることを付け加える。[4]

そこで、東京理科大学数学科小松彦三郎教授により新たな問題設定が行われた。連立代数方程式系 (1)-(6) において、 $a, b, c, d, e, f$  が図形の長さを表しているという条件を課さない場合に実根の数を数えよ。この問題をこれから議論する。参考までに条件を課す場合も議論する。

### 3 $a, b, c, d, e, f$ に条件を課す場合

$a, b, c, d, e, f$  が図形の長さをあらわしているという条件すなわちすべての変数は非負の実数であるという条件を課す場合の議論をする。

#### 3.1 最小多項式

変数  $f$  についての最小多項式は

$$g_{11} = c_{1458}f^{1458} + c_{1455}f^{1455} + c_{1452}f^{1452} + \dots$$

と次数が 3 飛ばしになっている。すべての変数が対称に含まれていることも考慮すると、問題を書き換えることができる。

$$a' = a^3, \quad b' = b^3, \quad c' = c^3, \quad d' = d^3, \quad e' = e^3, \quad s = f^3 \quad (7)$$

$(x' = x^3$  は実数上 1 対 1 対応) とすると,

$$d' - b' = 271 \quad (8)$$

$$b' - c' = 217 \quad (9)$$

$$c' - a' = 60.8 \quad (10)$$

$$a' - e' = 326.2 \quad (11)$$

$$e' - s = 61 \quad (12)$$

$$g(s) = c_{1458}s^{486} + c_{1455}s^{485} + c_{1452}s^{484} + \dots = 0 \quad (13)$$

よって, 式 (13) のみを考えればよい. 残りの変数は,  $s$  に対して線形方程式 (8)-(12) を解くことで得られる.

なお, 最小多項式は Risa/Asir 上で構成した. アルゴリズムの詳細は, [6, pp.240,245-249] を参照されたい. さらに, 有限体上の G.C.D. より  $f$  が分離化元であることもわかる.

### 3.2 Fourier の定理と Laguerre の定理を $g(s)$ に適用

Fourier の定理 [2, pp.99-100] より,  $65 < s$  に根がないことがわかる.  $64 < s \leq 65$  の根の個数は 1 つまたはそれより偶数個少ない. よって, 1 つと確定する. さらに,  $24 < s \leq 64$  に根がないことがわかる. Laguerre の定理 [2, pp.101-102] より,  $0 < s < 33$  に根がないことがわかる. さらに,  $g(s)$  の定数項が 0 でないことも考慮すると  $0 \leq s \leq 64$  に根が存在しないことがわかる.

他の変数は, 上記の結果から線形方程式 (8)-(12) で計算する. 以上より, すべての変数は非負の実数であるという条件を課す場合実根は 1 つ.

これからは, Risa/Asir 上でおこなった計算の結果に対して定理を適応した.

## 4 $a, b, c, d, e, f$ に条件を課さない場合

$a, b, c, d, e, f$  が図形の長さをあらわしているという条件すなわちすべての変数の根は非負の実数であるという条件を課さない場合の議論をする. この場合は, もやは Fourier の定理と Laguerre の定理のみでは扱うことは困難である.

### 4.1 高階の導関数を利用する方法

数学的事実 [9, pp.39-64]

「与えられた関数  $f(x)$  の導関数  $f'(x)$  の隣り合う実数解の間では  $f(x)$  は単調な関数であり, その間には高々 1 つの解しか持たない」

この事実をもちいて real root counting をおこなうのが高階の導関数を利用する方法である.

定理 1

係数が実数の多項式  $f(x)$  に対して, 次のような多項式列

$$f_1(x), f_2(x), \dots, f_k(x)$$

をつくる.

1.  $f_1(x) = f(x)/\gcd(f(x), f'(x))$  とおく.

2.  $f_j(x)$  まで定義されていて  $f_j(x)$  の次数が 1 より大きいときは  $f_{j+1}(x) = f'_j(x)/\gcd(f'_j(x), f''_j(x))$  とおく.

3.  $f_{j+1}(x)$  の次数が 1 より大きいときは前の操作をくり返す.

この多項式列は次の条件を満たす.

- すべての  $f_j(x)$  は重複因子を持たない.  $f_1(x)$  と  $f(x)$  は同じ解を持つ.
- $f_j(x)$  と  $f_{j+1}(x)$  は共通解を持たない.
- $j = 1, 2, \dots, k-1$  に対して,  $\alpha, \beta$  を隣り合う  $f_{j+1}(x)$  の解とする.  $f_j(x)$  は区間  $(\alpha, \beta)$  に高々 1 つの解しか持たない. もしこの区間に  $f_j(x)$  が解を持てば  $f_j(\alpha)$  と  $f_j(\beta)$  は符号が異なる.

根の多重度は別途決定できるが, この問題では  $\gcd(g(s), g'(s)) = 1$  であるためそのような議論はここではしない. 詳しくは, [9, pp.39-64] を参照していただきたい.

## 4.2 結果

表 1:  $g(s)$  の実根の区間数表現

	$s$
1	[[640017148584, 10], [640017148585, 10]]
2	[[-9680216914656, 10], [-9680216914655, 10]]
3	[[-1093955121813, 10], [-1093955121812, 10]]
4	[[-8921900976700, 10], [-8921900976699, 10]]
5	[[-6795503392712, 10], [-6795503392711, 10]]
6	[[-6552320519219, 10], [-6552320519218, 10]]
7	[[-3730008868846, 10], [-3730008868845, 10]]
8	[[-4546250322124, 10], [-4546250322123, 10]]

高階の導関数を利用する方法をもちいて  $g(s)$  の実根を区間数で包み込むと, 表 1 のようになる. 表 1 における 10 は,  $\times 10^{-10}$  を意味する. 以上より, 連立代数方程式系 (1)-(6) の実根の個数は 8 つ. これらの計算は多倍長数のために pari をもちいて C 言語による独自実装によっておこなった.

## 4.3 Pederson と Roy の定理

詳細は, [6, pp.146] を参照されたい.

$$\begin{cases} f(x, y) = x^2 + y^2 - 4, \\ g(x, y) = xy - 1. \end{cases} \quad (14)$$

について考える.

全次数順序  $y \succ x$  でグレブナー基底は  $G = \{yx - 1, x^2 + y^2 - 4, x^3 - 4x + y\}$  となり, 剰余環の線形基底  $L(G) = \{1, x, x^2, y\}$  が計算できる. 以下では,  $t_1 = 1, t_2 = x, t_3 = x^2, t_4 = y$  とする.

倍写像の行列を計算すると,

$$M_{t_1} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad M_{t_2} = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 4 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \end{pmatrix},$$

$$M_{t_3} = \begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 4 & 0 & 1 \\ 1 & 0 & 4 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix}, \quad M_{t_4} = \begin{pmatrix} 0 & 1 & 0 & 4 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

となる.

2次形式の表現行列  $B$

$$B = (b_{i,j} = \text{trace}(M_{t_i} M_{t_j})), \quad i, j = 1, \dots, 4$$

$$= \begin{pmatrix} 4 & 0 & 8 & 0 \\ 0 & 8 & 0 & 4 \\ 8 & 0 & 28 & 0 \\ 0 & 4 & 0 & 8 \end{pmatrix}.$$

#### 4.3.1 Pederson と Roy の定理

定理 2

(Pederson と Roy の定理)

非線形連立代数方程式 (14) の実根の個数

= 対称行列  $B$  の正の実根の数 - 対称行列  $B$  の負の実根の数

= 0 固有値を持たないならば,  $2 \times$  対称行列  $B$  の正の実根の数 - 行列サイズ

対称行列  $B$  の固有方程式

$$C(z) = c_0 + c_1 z + \dots + c_{d-1} z^{d-1} + c_d z^d$$

が計算できると, Descartes 定理により対称行列  $B$  の正の実根の数 =  $\{c_0, c_1, \dots, c_d\}$  の符号変化の回数であるから連立代数方程式系 (1)-(6) の実根の数が数えられる.

#### 4.3.2 精度保証付き数値計算による高速化

精度保証付き数値計算を用いると対称行列  $B$  のすべての固有値の存在範囲を区間数により高速に評価できる. [8, pp.85] よって, 非線形連立代数方程式 (14) の実根の個数を計算することができる. ここで注意をする. 数式処理は有理数を用いて計算をおこなう. 一方で, 精度保証付き数値計算は浮動小数点 (double) をもちいて計算をおこなう. すなわち, 有理数から浮動小数点 (double) への変換のため精度保証付き数値計算は区間数対称行列に対しておこなわなければならないように思えるがそれは正しくない. 有理数から構成される区間数対称行列の要素は非常に狭い区間を持っている. その事実と以下の定理組み合わせることで, 精度保証付き数値計算の効率性を損なうことなく数式処理の高速化に利用できる.

## 定理 3

(Weyl の摂動定理)

$E = [e_{i,j}], F = [f_{i,j}]$  は共に実対称行列で、それぞれ固有値  $\lambda_1 \leq \dots \leq \lambda_n, \mu_1 \leq \dots \leq \mu_n$  をもつものとするれば

$$|\lambda_i - \mu_i| \leq \|E - F\| \quad (15)$$

ここで、行列のノルムは  $1, 2, \infty$ , フロベニウスノルムのすべてが許される。(対称行列なので、 $1$  ノルムと  $\infty$  ノルムは等しい)

詳しくは、[7, pp.100] を参照されたい。

この定理を利用する。まず、与えられた有理数の行列を区間幅の狭い区間数を要素とする行列  $E$  に変換する。区間数行列  $E$  の要素において下限すべてを取り出した行列を  $D$  して上限すべてを取り出した行列を  $U$  とする。次に、 $F = (D + U)/2$  によって点行列  $F$  をさだめる。よって、精度保証付き数値計算によって  $F$  の固有値を評価できたならば Weyl の摂動定理により  $E$  の固有値が評価できる。

## 4.3.3 B 行列の作り方

剰余環の線形基底  $L(G) = \{1, x, x^2, y\}$  が計算できたならば、多項式

$$F = 1 + x + x^2 + y$$

として、

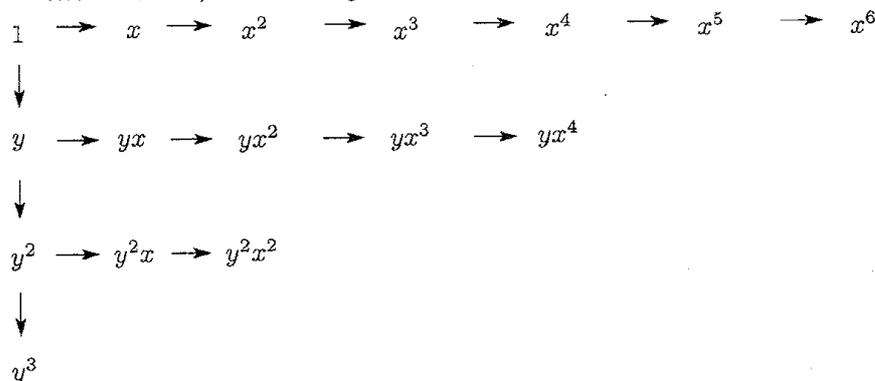
$$F^3 = x^6 + 3x^5 + 3x^4y + 6x^4 + 6x^3y + 3x^2y^2 + 7x^3 + 9x^2y + 3xy^2 + y^3 \\ + 6x^2 + 6xy + 3y^2 + 3x + 3y + 1$$

を計算する。このとき、係数を無視した単項式の集合

$$V = \{x^6, x^5, x^4y, x^4, x^3y, x^2y^2, x^3, x^2y, xy^2, y^3, x^2, xy, y^2, x, y, 1\}$$

をつくる。

この集合に対して、全次数順序  $y > x$  を考慮して次の木をつくる。



この木の順に正規簡約を計算する。

$$\text{normal}(1, G) = u_1,$$

$$\begin{aligned}
\text{normal}(x, G) &= \text{normal}(u_1x, G) = u_2, \\
\text{normal}(x^2, G) &= \text{normal}(u_2x, G) = u_3, \\
\text{normal}(x^3, G) &= \text{normal}(u_3x, G) = u_4, \\
\text{normal}(x^4, G) &= \text{normal}(u_4x, G) = u_5, \\
\text{normal}(x^5, G) &= \text{normal}(u_5x, G) = u_6, \\
\text{normal}(x^6, G) &= \text{normal}(u_6x, G) = u_7, \\
\text{normal}(y, G) &= \text{normal}(u_1y, G) = u_8, \\
\text{normal}(yx, G) &= \text{normal}(u_8x, G) = u_9, \\
\text{normal}(yx^2, G) &= \text{normal}(u_9x, G) = u_{10}, \dots
\end{aligned}$$

ここで,  $\text{normal}(A, X)$  は  $A$  の  $X$  による正規簡約をあらわす.

2次形式の表現行列  $B$

$$B = (b_{i,j} = \text{trace}(M_{t_i t_j})), \quad i, j = 1, \dots, 4$$

と書き直せるため,  $\text{normal}(t_i t_j t_k, G)$   $t_k \in L(G)$  が計算できたならばそのデータのみを用いて  $M_{t_i t_j}$  を構成できる.

以上より, 沢口一之の問題の行列  $B$  を構成できる. しかし,  $B$  行列の構成には 24 時間を必要とした. さらに, その対称行列  $B$  の要素は巨大な桁をもつ有理数となり浮動小数点 (double) で表現できる量ではない. いろいろな計算を試みたが対称行列  $B$  の正の固有値の数を確定することはできなかった.

## 5 まとめ

高階の導関数をもちいて実根を数える方法は, 十分に実用に耐えうる算法であることが確認できたので maple に実装し Cylindrical Algebraic Decomposition の高速化に活用していく方針である. Pederson と Roy の定理は, 理論的としてはとても美しいが効率の点で 1 変数代数方程式をつくり高階の導関数をもちいて実根を数える方法と比べると改良を必要とする算法である. 効率化をこれからの課題とする. また, 最近の研究で精度保証付き数値計算を積極的に活用してより効率的な算法を開発した. 別の機会に発表または論文等で報告することを約束する.

## 参 考 文 献

- [1] George E. Collins, H. Hong: Partial Cylindrical Algebraic Decomposition for Quantifier Elimination, *J. Symb. Comput.*, **12(3)**, 1991, pp. 299-328.
- [2] 高木貞治: 代数学講義 (改訂新版), 共立出版, 東京, 1965.
- [3] 竹之内脩: 古今算法記自問一十五好之答術, 近畿和算ゼミナール報告集 [6], 風草工房.
- [4] 平山諦: 関孝和 その業績と伝記, 恒星社版, 東京, 1974.
- [5] 広田良吾: 行列式とパフィアン (1), 日本応用数学会誌「応用数理」, **14(1)**, 2004, pp. 62-66.
- [6] 野呂正行, 横山和弘: グレブナー基底の計算 基礎篇, 東京大学出版会, 東京, 2003.
- [7] 山本哲郎: 数値解析入門 [増訂版], サイエンス社, 東京, 2003.

- [8] 大石進一: 精度保証付き数値計算, コロナ社, 東京, 2000.
- [9] 齋藤友克, 竹島卓, 平野照比古: グレブナー基底の計算 実践篇, 東京大学出版会, 東京, 2003.