パラメトリックな零次元イデアルのシェイプフォームについて

On the shape forms of zero-dimensinal ideals of parametric polynomial rings

東京理科大学・理学部応用数学科　　佐藤洋祐 [*1]
Yosuke Sato
Tokyo University of Science

Abstract

A quantifier elimination algorithm based on the computation of comprehensive Gröbner systems (CGS-QE algorithm) proposed in our paper of ISSAC2015 is based on the real root counting theorem. Though the algorithm works uniformly no matter whether the addressed parametric ideals are radical or not, it has a serious disadvantage that the output quantifier free formula often contains may unnecessary equations and inequalities. In this paper, we study an alternative naive quantifier elimination algorithm based on the computation of the shape forms of zero-dimensional parametric ideals.

1　はじめに

[1] で導入された限量子記号消去アルゴリズム (CGS-QE algorithm) は零次元イデアルの実零点の個数に関する real root counting theorem を利用している。このアルゴリズムの長所は、イデアルが根基であるかどうかにかかわらず、多変数版エルミートの 2 次形式によるイデアルの一様な計算が可能になることである。その一方、出力される論理式は不必要な式を多く含むため煩雑になってしまう欠点がある。岩根氏が開発した論理式の簡易化手法を用いて、ある程度の簡易化が可能ではあるが限界がある。本稿では、この方法とは全く異なる、零次元イデアルのシェイプフォームの計算に基づく素朴な方法について考察する。パラメーターを含む多項式環における計算なので、様々の考察が必要になる。シェイプフォームの計算に関して、現在までに得られた結果について報告する。

2　Comprehensive Gröbner System

包括的グレブナー基底系 (CGS) の定義を与える。

定義 1
イデアル $I \subset \mathbb{Q}[\bar{A}, \bar{X}]$ ($\bar{A} = A_1, \ldots, A_m$ はパラメーター, $\bar{X} = X_1, \ldots, X_n$ は主変数) の項順序 $>$ に関する CGS $\mathcal{G}$ とは、以下をみたす $\mathcal{G} = \{(\mathcal{S}_1, G_1), \ldots, (\mathcal{S}_l, G_l)\}$ のことである。

*1 E-mail: `ysato@rs.tus.ac.jp`

(1) $\mathcal{S}_i \subset \mathbb{C}^m, \mathcal{S}_1 \cup \cdots \cup \mathcal{S}_l = \mathbb{C}^m$, $\mathcal{S}_i \cap \mathcal{S}_j = \emptyset (i \neq j)$

(2) 各 i について、G_i は $\mathbb{Q}[\bar{A}, \bar{X}]$ の有限集合で、任意の $\bar{a} \in \mathcal{S}_i$ にたいして、$G_i(\bar{a}) = \{g(\bar{a}, \bar{X}) : g \in G_i\}$ は イデアル $I(\bar{a}) = \{f(\bar{a}, \bar{X}) : f \in I\}$ の $>$ に関するグレブナー基底である。

各 $\mathcal{S}_i$ は代数的多様体 V_1, V_2 にたいして $V_1 \setminus V_2$ の形をしている。$\mathcal{S}_i$ を $\mathcal{G}$ の *segment* とよぶ。言葉の乱用ではあるが $(\mathcal{S}_i, G_i)$ も $\mathcal{G}$ の *segment* とよぶことにする。

3 Real Root Counting Theorem に基づく CGS-QE

簡単な例を用いて Real Root Counting Theorem に基づく CGS-QE の概要を述べる。

$$\exists X, Y (Y^3 - XY - 1 = 0 \land X^2 - 2X + 1 - AY = 0) \qquad (\Leftrightarrow \phi(A))$$

の限量子記号記号は以下のように消去できる。

X, Y の全次数逆式項順序で $I = \langle Y^3 - XY - 1, X^2 - 2X + 1 - AY \rangle$ の CGS(A はパラメーター) は $\{(\mathbb{C}, \{Y^3 - XY - 1, X^2 - 2X + 1 - AY\})\}$ (生成元そのもの) なので、$\mathbb{R}[X, Y]/I$ の基底として $\{1, X, Y, Y^2, XY, XY^2\}$ がとれる. CGS を使ってこの基底にたいする (多変数版) エルミートの 2 次形式とよばれる以下のような対称行列 M_1^I を計算する。

$$M_1^I = \begin{pmatrix} 6 & 6 & 0 & 4 & 3A & 4 \\ 6 & 6 & 3A & 4 & 10A & 3A^2+6A+4 \\ 0 & 3A & 4 & 3A+6 & 4 & 10A+6 \\ 4 & 4 & 3A+6 & 4 & 10A+6 & 3A^2+9A+4 \\ 3A & 10A & 4 & 10A+6 & 3A^2+6A+4 & 21A+6 \\ 4 & 3A^2+6A+4 & 10A+6 & 3A^2+9A+4 & 21A+6 & 16A^2+28A+4 \end{pmatrix}$$

この固有多項式を $f(\chi)$ とすると Real Root Count Theorem から以下がなりたつ。

$\phi(\bar{A}) \Leftrightarrow f(\chi)$ の正の根の個数 $>$ $f(\chi)$ の負の根の個数 $\Leftrightarrow$ $f(\chi)$ の正の根の個数 $\neq$ $f(\chi)$ の負の根の個数

(根の個数は重複度を含めて数える。)

この固有多項式 $f(\chi)$ を計算すると以下のようになる。

$\chi^6 + (-28 - 34A - 19A^2)\chi^5 + (48 + 168A - 309A^2 + 90A^3 + 30A^4)\chi^4 +$
$(1472 + 2496A + 4736A^2 - 106A^3 + 1451A^4 + 378A^5 + 54A^6)\chi^3 +$
$(-11776A - 9664A^2 - 7660A^3 - 8036A^4 - 1782A^5 - 216A^6)\chi^2 +$
$(-2944A^2 + 10384A^3 - 6220A^4 - 1782A^5 - 189A^6)\chi +$
$33856A^3 + 43632A^4 + 8856A^5 + 729A^6$

$A0 = 33856A^3 + 43632A^4 + 8856A^5 + 729A^6$
$A1 = -2944A^2 + 10384A^3 - 6220A^4 - 1782A^5 - 189A^6$
$A2 = -11776A - 9664A^2 - 7660A^3 - 8036A^4 - 1782A^5 - 216A^6$
$A3 = 1472 + 2496A + 4736A^2 - 106A^3 + 1451A^4 + 378A^5 + 54A^6$
$A4 = 48 + 168A - 309A^2 + 90A^3 + 30A^4$
$A5 = -28 - 34A - 19A^2$

として、デカルトの符号法則を使った岩根氏の簡易化公式により以下の限量子記号を含まない同値な論理式が得られる。

$(A0 \geq 0 \land A1 \neq 0) \lor (A2 \geq 0 \land A3 \geq 0 \land A4 \geq 0 \land A5 > 0) \lor (A2 \geq 0 \land A3 \leq 0 \land A4 \geq 0 \land A5 < 0) \lor (A1 \geq 0 \land A2 \leq 0 \land A4 \geq 0 \land A5 < 0) \lor (A1 \geq 0 \land A2 \leq 0 \land A3 > 0 \land A4 \leq 0) \lor (A1 \leq 0 \land A2 \leq 0 \land A4 \geq 0 \land A5 > 0) \lor (A1 \leq 0 \land A2 \leq 0 \land A3 < 0 \land A4 \leq 0)$

この方法による CGS-QE には以下のような欠点がある。

- デカルトの符号法則を使っているので、一般に、出力される限量子記号を含まない論理式には不必要な式がたくさん含まれる。岩根氏が開発した論理式の簡易化公式を用いて、不必要な式はある程度削除できるが限界がある。
- $\mathbb{Q}[\bar{X}]/I$ の次元 (M_1^I のサイズ) の 2 乗に比例して、固有多項式の係数 (パラメーターの多項式) が複雑になる。

4 零次元イデアルのシェイプフォームを利用した素朴な方法

I の シェイプフォーム を使っても、限量子記号消去を行うことが可能である。

I の $X > Y$ なる辞書式順序の CGS は以下のようになる。

$$\{(\mathbb{C}, \{X - Y^5 + 2Y^3 + AY^2 + Y^2 - Y - 2, Y^6 - 2Y^4 - AY^3 - 2Y^3 + Y^2 + 2Y + 1\})$$

したがって、もとの式は以下の式と同値になる。

$$\exists Y(Y^6 - 2Y^4 - AY^3 - 2Y^3 + Y^2 + 2Y + 1 = 0)$$

これから、スツルムハビッチ列の計算による special QE を使って限量子記号消去が可能になる。

零次元イデアルの シェイプフォーム がいつも得られるとは限らないが、根基イデアルについては以下の定理がなりたつ。

定理 2 (Shape Lemma)
零次元の根基イデアル $I \subset K[X_1, \ldots, X_n]$ にたいして、

$$I + \langle Y - (X_1 + c_2X_2 + \cdots + c_nX_n)\rangle = \langle X_1 - g_1(Y), \ldots, X_n - g_n(Y), g(Y)\rangle$$

となるような自然数 $c_2, \ldots, c_n$ が存在して計算できる。

5 得られた理論結果と今後の課題

零次元イデアルの シェイプフォーム を利用して限量子記号消去を行うためには、パラメーターを含む多項式環における シェイプフォーム の計算が必要になる。シェイプフォーム の計算に関して得られた結果を以下に述べる。

定理 3 (Sato,Fukasaku)
イデアル $I \subset \mathbb{Q}[\bar{A}, \bar{X}]$ の *CGS* のある *segment* $\mathcal{S}$ において、I が零次元であるとき、エルミートの 2 次形式 M_1^I の行列式 $Det(M_1^I)$ は $\forall \bar{a} \in \mathcal{S}\ q(\bar{a}) \neq 0$ なる $\bar{A}$ の有理係数多項式 $p(\bar{A}), q(\bar{A})$ にたいして $Det(M_1^I)= p(\bar{A})/q(\bar{A})$ と表される。このとき、以下が成り立つ。

$$\bar{a} \in \mathcal{S} \text{ にたいして } I(\bar{a}) \text{ が根基である} \Leftrightarrow p(\bar{a}) \neq 0$$

定理 4 (Sato)
イデアル $I \subset \mathbb{Q}[\bar{A}, \bar{X}]$ がある *segment* $\mathcal{S}$ において零次元で根基であるとき、$\mathcal{S}$ を $\mathcal{S}_1 \cup \cdots \cup \mathcal{S}_l$ に分割し、各 $\mathcal{S}_i$ において I のパラメーター $\bar{A}$ に関して一様なシェイプフォームを計算できる。

I が根基でないけど零次元であるような segment にたいしても、一様に I の根基を計算できるので、理論的にはこの方法で限量子記号消去が可能である。
しかしながら、この方法によるシェイプフォームは一般に複雑な形になる。つまり、$g(Y)$ の係数が膨れ上がるのでスツルムハビッチ列の計算が重たくなる。前節で扱った例では $A = 0$ のとき根基ではない (実は $33856 + 43632A + 8856A^2 + 729A^3 = 0$ のときも根基ではない) が、一様な シェイプフォーム が得られている。このような場合、限量子記号消去のためには根基の計算は必要ない。今後の課題として、限量子記号消去のための効率的なシェイプフォームの計算法の研究が重要になる。その際、[2] で示した結果が重要になると考えている。

謝　辞

本研究は JSPS 科研費 JP21K03375 の助成を受けています.

参 考 文 献

[1] Fukasaku,R., Iwane,H., Sato,Y.: Real Quantifier Elimination by Computation of Comprehensive Gröbner Systems. Proc. ISSAC2015, pp. 173–180, 2015.

[2] Sato,Y., Fukasaku,R., Sekigawa,H.:On Continuity of the Roots of a Parametric Zero Dimensional Multivariate Polynomial Ideal. Proc.ISSAC2018, pp.359-365. 2018.