素朴なCGS-QEアルゴリズムについて

On a naive algorithm of CGS-QE

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 order to overcome it, we have developed an alternative way based on the computation of the shape forms of zero-dimensional parametric ideals last year. In this paper, we further improve the algorithm to compute the shape forms zero-dimensional parametric ideals and present an efficient CGS-QE algorithm.

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) の欠点を克服するため、零次元イデアルのシェイプフォームに関する理論を構築し、2024 年度の RIMS 共同研究 (公開型) において発表した [3]。しかしながら、その時点の理論には整備されていない部分が多々あり、新たな CGS-QE のアルゴリズムを構築するには至っていなかった。その後、理論を大幅に進歩させることができ、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 CGS-QE のアルゴリズムを構築した。本稿では、この結果について概要を報告する。[3] と重なる部分があるが、２章と３章で [1] の概要を述べ、４章で素朴な CGS-QE のアルゴリズムの基本となるアイデアと問題点を示す。５章と６章が本稿の主要部である。具体例を用いて零次元イデアルのシェイプフォームに関して整備した理論を紹介する。最後に素朴な CGS-QE のアルゴリズムについて、従来の方法では実時間以内に計算不能であるが、このアルゴリズムでは、瞬時に限量子消去が可能な例を１つ用いて紹介する。

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。

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

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。

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

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等による 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。

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 CGS-QE が可能であるが、以下のような問題点がある。

問題点
新たな変数 Y を導入するので、一般にシェイプフォームは複雑な形になる。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。

5　シェイプフォームを求めるための効率的アルゴリズム

上記の問題点を克服するために構築したアルゴリズムのよりどころとなる定理を述べる。

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、「$\bar{a} \in \mathcal{S}$ にたいして $I(\bar{a})$ が根基である $\Leftrightarrow p(\bar{a}) \neq 0$」が成り立つ。

この定理を用いて、最小限の CGS 計算でシェイプフォームを求めるアルゴリズムを構築した。
以下に SageMath で実装した CGS の計算プログラムによる簡単な計算例を用いてアルゴリズムの概要を紹介する。

イデアル $I = \langle x^2 + ay + y^2 + b, xy + cx + d\rangle$ (x, y が主変数、a, b, c, d がパラメーター) のシェイプフォームの計算例

I の CGS(項順序は $x > y$ の全次数逆辞書式) は以下のようになる。

```
sage: load('new_cgs.sage')
load('new_cgs.sage'))
sage: make_parametric_ring('x,y','a,b,c,d','degrevlex','degrevlex')
Defining x, y, a, b, c, d
sage: I=[x^2+a*y+y^2+b,x*y+c*x+d]
sage: newcgs(I)
[([[0], [1]],
  [y^3 + y^2*a + y^2*c - x*d + y*a*c + y*b + b*c,
   x^2 + y^2 + y*a + b,
   x*y + x*c + d])]
```

これから、すべてのパラメーター空間で $\mathbb{C}[x,y]/I$ の次元が 4 で基底として $\{y^2,y,x,1\}$ がとれることがわかる。$\{x-f(y),g(y)\}$ の形のシェイプフォームが得られるのは、$\mathbb{C}[x,y]/I$ の基底として $\{y^3,y^2,y,1\}$ がとれる場合である。
x_1,x_2,x_3,x_4 を変数として、$x_1y^3+x_2y^2+x_3y+x_4$ の上記のグレブナー基底による normal form を計算すると $(-(a+c)x_1+x_2)y^2+(-(ac+b)x_1+x_3)y+dx_1x+(-bcx_1+x_4)$ が得られる。したがって、$\{y^3,y^2,y,1\}$ が基底であるための必要十分条件は以下の斉次線形方程式が自明解しか持たないことがわかる。

$$\begin{pmatrix} -(a+c) & 1 & 0 & 0 \\ -(ac+b) & 0 & 1 & 0 \\ d & 0 & 0 & 0 \\ -bc & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

この行列式を計算すると d であるので、この形のシェイプフォームが存在するための必要十分条件は $d \neq 0$ であることがわかる。また、グレブナー基底を使って得られる線形方程式を解くことで、以下のシェイプフォームが計算される。

$$\{dx-y^3-(a+c)y^2-(ac+b)y-bc, y^4+(a+2c)y^3+(2ac+c^2+b)y^2+(ac^2+2bc)y+bc^2+d^2\}$$

$\{y-f(x),g(x)\}$ の形のシェイプフォームについても同様にして、この形のシェイプフォームが存在するための必要十分条件は $d \neq 0$ であり、以下のシェイプフォームが計算される。

$$\{dy-x^3+(ac-c^2-b)x+ad-cd, x^4+(-ac+c^2+b)x^2+(-ad+2cd)x+d^2\}$$

$d=0$ の場合は、シェイプフォームを得るためには新しい変数を導入する必要がある. 理論的には、イデアルの根基を計算すれば、シェイプフォームが計算できるが、以下のように根基の計算は必要最小限に抑えることができる。

この場合 M_1^I の行列式 $\mathrm{Det}(M_1^I)$ をグレブナー基底を用いて計算すると以下が得られる。

$$(M_1^I) = 2(-b+ac-c^2)(-4a^3bc+16ab^2c-2a^4c^2+12a^2bc^2-24b^2c^2+4a^3c^3-8abc^3-2a^2c^4)$$

したがって、$\mathrm{Det}(M_1^I) \neq 0$ の領域は空でなく、そこで I は根基なので、Shape Lemma により、新しい変数 k にたいして、$I+\langle x+my-k\rangle$ のシェイプフォームが $\{x-f(k),y-g(k),h(k)\}$ となるような自然数

m が必ず存在することがわかる。
k を辞書式に x, y より大きい項順序にたいして、$x + my - k$ を加えたものもグレブナー基底であるので、これを用いて、このような具体的な m にたいして、前の計算と同様に、シェイプフォームになる領域とシェイプフォームが計算できる。

$m = 1$ にたいして、以下が計算される。

$a - 2c \neq 0$、シェイプフォームは
$\{$
$(a-2c)y + k^2 + (a+1)k + b,$
$(a-2c)x + k^2 - ka + b,$
$k^4 - (a+2c)k^3 + (ac + 2c^2 + 2b)k^2 + (a^2c - 2ac^2 - ab - 2bc)k - abc + 2bc^2 + b^2$
$\}$

$a - 2c = 0$ でも $\mathrm{Det}(M_1^I) \neq 0$ であるような値がある ($\Leftrightarrow \mathrm{Det}(M_1^I) \notin \sqrt{\langle a - 2c \rangle}$ なので計算できる。) ので、$a - 2c = 0$ でも I が根基である領域が存在する。

$m = 3$ にたいして、同様の計算を行う ($a - 2c = 0$ も用いる) と以下が計算される。

$a - 2c = 0 \wedge c^2 - b \neq 0$、シェイプフォームは
$\{$
$6(c^2 - b)y - k^3 - 2k^2c - (11c^2 + b)k - 8bc,$
$3(c^2 - b)x + k^3 + 2k^2c + (8c^2 + 4b)k + 8bc,$
$k^4 + 8k^3c + (19c^2 + 5b)k^2 + (12c^3 + 20bc)k + 12bc^2 + 4b^2$
$\}$

$a - 2c = 0 \wedge c^2 - b = 0 \Rightarrow \mathrm{Det}(M_1^I) = 0$ なので、この領域のどんな値にたいしても I は根基でない。

I のグレブナー基底、及び $a - 2c = 0, c^2 - b = 0$ を用いて x と y の最小多項式を計算すると、
x^3、$y^3 + 3cy^2 + 3c^2y + c^3 = (y + c)^3$
が得られ、シェイプフォーム $\{x^3$、$y^3 + 3cy^2 + 3c^2y + c^3 = (y + c)^3\}$ が得られる。

一般のイデアルにたいしても同様に計算される。重要なポイントは以下の 3 点である。

(1) 任意の項順序に対する CGS を 1 つ計算しておけば、根基の計算が必要になるまで、それを用いてシェイプフォームの計算が可能である。

(2) 根基の計算は必要最小限に抑えることができる。

上記の例の場合だと、$2(-b+ac-c^2)(-4a^3bc+16ab^2c-2a^4c^2+12a^2bc^2-24b^2c^2+4a^3c^3-8abc^3-2a^2c^4) = 0$ なる領域にたいして、根基を計算する必要がなく、ずっと小さい領域 $a - 2c = 0 \wedge c^2 - b = 0$ における根基の計算のみで済む。

(3) この計算を可能にするのが定理３、すなわち $\mathrm{Det}(M_1^I)=0$ が I が根基でないことの必要十分条件になることである。

6　素朴な CGS-QE アルゴリズム

前章で述べた方法でシェイプフォームが計算されれば、スツルムハビッチ列の計算等による special QE を使って限量子記号消去が可能になる。しかし、大抵の場合はシェイプフォームまで求めなくても、一変数の最小多項式の計算だけで限量子記号消去が可能になる。以下にその概要を具体例を 1 つ用いて紹介する。

$\exists x,y(3axy+byz+xz+3=0\wedge 5xyz+ax+y+b=0\wedge xz+byz+az+by-7=0)$

にたいして、
$I=\langle 3axy+byz+xz+3,5xyz+ax+y+b,xz+byz+az+by-7\rangle$($x,y$ が主変数、a,b がパラメーター)の CGS($x>y>z$ の全次数逆辞書式) は前述の SageMath プログラムで瞬時に計算できる。グレグナー基底が $\{1\}$ でない segment は全部で５つあり、それぞれにたいして $\mathbb{Q}/I$ の次元と z の最小多項式は CGS を用いて以下のように計算される。

1. segment $\mathbb{V}(0)-\mathbb{V}(a^2b-5/3ab^2)$, 6 次元
$25ba^2z^6-500baz^5+(-15ba^4-15a^3+25b^2a^2-70ba+2500b)z^4+(3b^2a^4+249ba^3+(15b^2+258)a^2-250b^2a-5b^3+700b)z^3+(9a^5-6b^2a^4+(-30b^2+33b)a^3+(12b^3-990b)a^2+(-183b^2-1080)a)z^2+((-9b^2-126)a^4+24b^2a^3+(12b^3-213b)a^2)z+(54b^2+441)a^3$

2. segment $\mathbb{V}(b)-\mathbb{V}(a,b)$, 4 次元
$5a^2z^4-86az^3+(-3a^4+360)z^2+42a^3z-147a^2$

3. segment $\mathbb{V}(a-5/3b)-\mathbb{V}(b^3+5/2b^2+129/10b,a-5/3b)$, 5 次元
$375b^2z^5+(-375b^2-4500b)z^4+(-625b^4+375b^3+3870b+13500)z^3+(125b^5+625b^4+6075b^3-2277b^2-9720)z^2+(-375b^5-570b^4-5250b^3-14220b^2)z+1350b^4+11025b^2$

4. segment $\mathbb{V}(b^2+5/2b+129/10),a-5/3b)-\mathbb{V}(1)$, 4 次元
$-2773500z^4+(-2580000b-903000)z^3+(-11030950b-49190250)z^2+(-15115575b+92973267)z+24961500b+47260440$

5. segment $\mathbb{V}(a)-\mathbb{V}(b^3-140b,a)$, 1 次元
$z-1/500b^2+7/25$

いずれも最小多項式の次数と $\mathbb{Q}/I$ の次元が一致するので、シェイプフォームが存在することが保証される。限量子記号消去のためにはシェイプフォームを計算する必要がなく、与えられた論理式は以下の論理式と同値であることがわかる。

$\exists z\ (a^2b-5/3ab^2\neq 0\wedge 25ba^2z^6-500baz^5+(-15ba^4-15a^3+25b^2a^2-70ba+2500b)z^4+(3b^2a^4+249ba^3+(15b^2+258)a^2-250b^2a-5b^3+700b)z^3+(9a^5-6b^2a^4+(-30b^2+33b)a^3+(12b^3-990b)a^2+(-183b^2-1080)a)z^2+((-9b^2-126)a^4+24b^2a^3+(12b^3-213b)a^2)z+(54b^2+441)a^3=0)\vee$

$\exists z\ (b = 0 \wedge a \neq 0 \wedge 5a^2z^4 - 86az^3 + (-3a^4 + 360)z^2 + 42a^3z - 147a^2 = 0) \vee$
$(a - 5/3b = 0 \wedge b^3 + 5/2b^2 + 129/10b \neq 0) \vee$
$\exists z\ (b^2 + 5/2b + 129/10 = 0 \wedge a - 5/3b = 0 \wedge -2773500z^4 + (-2580000b - 903000)z^3 + (-11030950b - 49190250)z^2 + (-15115575b + 92973267)z + 24961500b + 47260440 = 0) \vee$
$(a = 0 \wedge b^3 - 140b \neq 0)$

special QE のプログラムで限量子記号 $\exists z$ を消去して以下の同値な論理式が計算される。

$(a - 5/3b = 0 \wedge b^3 + 5/2b^2 + 129/10b \neq 0) \vee (a = 0 \wedge b^3 - 140b \neq 0) \vee ((a < 0 \wedge (b < (3a)/5 \vee (3a)/5 < b < 0 \vee b > 0)) \vee (a > 0 \wedge (b < 0 \vee 0 < b < (3a)/5 \vee b > (3a)/5))) \vee (b = 0 \wedge (a < 0 \vee a > 0))$

因みに、もとの論理式を Mathematica の限量子記号消去プログラム `Reduce` や `Resolve` に入力しても手元の PC では計算は終了しないが、上記の限量子記号 $\exists z$ のみの論理式にたいしては上の最終的な論理式が瞬時に計算される。また、[1] のアルゴリズムを実装した Maple のプログラムでは、もとの論理式にたいして、瞬時に限量子記号は消去されるが、出力される論理式は途方もなく複雑なものになる。

謝　　辞

This work was supported by the Research Institute for Mathematical Sciences, an International Joint Usage/Research Center located in Kyoto University.

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.

[3] 佐藤洋祐: 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. RIMS Kôkyûroku No.2320 Computer Algebra – Foundations and Applications 2025.