数理解析研究所講究録
第1572巻 2007年 124-130

CGSのcanonical formに向けて

鈴木 晃
AKIRA SUZUKI*
神戸大学
KOBE UNIVERSITY

1 はじめに

CGS(comprehensive Gröbner system, 包括グレブナー系) はWeispfennigにより導入され[9]たパラメータを含んだイデアルに対するグレブナー基底の一種である. これを計算する実装はRedlog[1], DispGB[3, 2], ACGB[6, 7], SimpleCGB[8] 等が提唱・実装されてきたが, その標準形は未だ定義されていない. 通常のグレブナー基底の場合には簡約グレブナー基底がその標準形として存在し, 例えば同じイデアルかどうか判定するためにはその簡約グレブナー基底が文字列として一致するかを調べれば良い. 一方でパラメータを含んだイデアルに対してはその標準的な表現が存在しないため, 様々な実装による出力の評価や比較が困難であるが, 適切なCGSの標準形を定義できればこのような困難は克服できる. 今回は, CGSの部分的な標準形をそのアルゴリズムと共に提案したと同時に, 本質的な標準形の困難さについて報告した.

なお, 先行研究としてWeispfenningのCanonical CGB[10]やManubens-MontesのMinimal Canonical CGS[4]があるが, それらは同値類の意味で「canonical」であるに過ぎず, それらもまた完全な標準形とは言えない.

2 CGSの定義と例

本報告ではKを体, LをKの代数的閉包, $\bar{X}$を変数, $\bar{A}=\{A_1,\ldots,A_N\}$をパラメータとし, $\bar{X}\cap\bar{A}=\emptyset$とする. また, $\bar{X}$上の項全体の集合$T(\bar{X})$上の項順序$<_{\bar{X}}$を固定する. 同様に$T(\bar{A})$上の項順序$<_{\bar{A}}$も固定する. 各$\bar{a}\in L^{|\bar{A}|}$と各$f(\bar{X},\bar{A})\in K[\bar{X},\bar{A}]$に対して, $f(\bar{X},\bar{a})\in L[\bar{X}]$を$f$の$\bar{a}$による*specilization*と呼び$\sigma_{\bar{a}}(f)$と表す. 各$H\subseteq K[\bar{A}]$に対し, $V(H)\subseteq L^N$をHにより定義される代数的集合とする. つまり

$$V(H)=\{\bar{a}\in L^N\ :\ \sigma_{\bar{a}}(h)=0\quad(\forall h\in H)\}$$

とする. なおここでは$V(H)\subseteq L^N$であるのに対して$H\subseteq K[\bar{A}]$である点に注意したい.

先ずCGSと簡約CGSを定義する.

定義 1 (CGS) $\mathcal{G}=\{(S_1,G_1),\ldots,(S_l,G_l)\}$が$F\subseteq K[\bar{X},\bar{A}]$に対するCGSであるとは以下を満たす時に言う:

- $S_1\cup\cdots\cup S_l=L^N$であり,

*sakira@kobe-u.ac.jp

- 各 $i=1,\ldots,l$ と各 $\bar{a}\in S_i$ に対して $\sigma_{\bar{a}}[G_i]$ が $\langle\sigma_{\bar{a}}[F]\rangle$ の $L[\bar{X}]$ に於けるグレブナー基底である.

また各 (S_i,G_i) を $\mathcal{G}$ の**断片**と呼ぶ.

定義 2 *CGS* $\{(S_1,G_1),\ldots,(S_l,G_l)\}$ が**簡約**であるとは各 $i=1,\ldots,l$ と各 $\bar{a}\in S_i$ に対して $\sigma_{\bar{a}}[G_i]$ が簡約グレブナー基底である時に言う.

与えられた $F\subseteq K[\bar{X},\bar{A}]$ に対する簡約CGSは一意ではない. そこで更に簡約CGS $\{(S_1,G_1),\ldots,(S_l,G_l)\}$ が**強簡約**である事を, 各断片 (S_i,G_i) の各 $\bar{a}\in S$ と G に現れる多項式の $((K[\bar{A}])[\bar{X}]$ の意味での) 先頭係数 $c\in K[\bar{A}]$ に対して, $\sigma_{\bar{a}}(c)\neq 0$ と定義した. しかし強簡約 CGS ですら一意からはほど遠い事は以下の例からもわかる.

例 3 以下は a,b をパラメータとして $x\gg y\gg t$ の時の $\{bx-y,ay-x,x+y-t\}$ の強簡約 *CGS* の例である.

```
((b+1)(a+1)!=0,(b*a-1)=0)[(a+1)*y-t,(a+1)*x-a*t]
((b+1)!=0,(a+1)=0)[t,(-b-1)*y,x]
((b+1)=0,(a+1)=0)[t,x+y]
((a+1)!=0,(b+1)=0)[t,(a+1)*y,x]
((b+1)(a+1)(b*a-1)!=0)[(b*a-1)*t,(a+1)*y,(a+1)*x]
```

以下は同じパラメトリックイデアルに対する強簡約 *CGS* であるが, 断片の数が異なる.

```
((b+1)(a+1)!=0,(b*a-1)=0)[(a+1)*y-t,(a+1)*x-a*t]
((b+1)=0,(a+1)=0)[t,x+y]
((b+1)(b*a-1)!=0 or (a+1)(b*a-1)!=0)[(b*a-1)*t,y,x]
```

以下も同じパラメトリックなイデアルに対する強簡約 *CGS* の例であるが, 条件部分や基底部分の表現が異なる.

```
((a+1)!=0,(b*a-1)=0)[(a+1)*y-t,(a+1)*x-a*t]
((b+1)=0,(a+1)=0)[t,x+y]
((b*a-1)!=0)[t,y,x]
```

同じパラメトリックイデアルに対する表現であっても無数の表現が存在し得る事は容易にわかる. ただし上の例の内では一番読みやすいものは3番目のものであり, またこれ以上は簡約化できない (読みやすくできない) 事もわかる. 従って, 1番目の出力や2番目の出力が CGS 計算システムから出力されたとしてもそれを3番目の出力へ変換するアルゴリズムが望まれる訳である. しかしこのゴールに対しては多くの困難が存在する. 次節以降でそれらの困難及びその解決への方策について触れる.

3 意味のあるCGSの標準形とは

ただ「標準的である」というだけであるなら定義できる事は次のようにわかる.

先ず簡約 CGS の同値性は計算により判別可能である旨を注記しておく. ここで二つの簡約 CGS $\mathcal{G}$ と $\mathcal{G}'$ が**同値**であるとは, 任意の $\bar{a}\in L^{|\bar{A}|}$ に対し, 各々の断片 $(S,G)\in\mathcal{G}$ と $(S',G')\in\mathcal{G}'$ を $\bar{a}\in S\cap S'$ となるように取った場合に $\sigma_{\bar{a}}[G]=\sigma_{\bar{a}}[G']$ を満たす時に言う. この時, 以下のような手順で簡約 CGS 達 $\mathcal{G}$ と $\mathcal{G}'$ の同値性は計算できる:

1. 条件部分の同値性

   (a) 各 $(S,G)\in\mathcal{G}$, $(S',G')\in\mathcal{G}'$ に対して (S,G) を $(S\cap S',G),(S\setminus S',G)$ で置きかえ, (S',G') を $(S'\cap S,G'),(S'\setminus S,G')$ で置きかえるという作業を繰り返す.

   (b) この作業により $\mathcal{G}$ と $\mathcal{G}'$ の条件分割は一致する.

2. 多項式部分の同値性

   (a) $(S,G)\in\mathcal{G}$ と $(S,G')\in\mathcal{G}'$ に対して根基イデアル I を $V(I)$ が S のザリスキー閉包になるものとする.

   (b) $g\in G$ と $g'\in G'$ を比較するのであれば, g のある単項 $c\cdot t$ に対応する g' の単項を $c'\cdot t$ とした時に $c\cdot hc_{\bar{A}}(g')-c'\cdot hc_{\bar{A}}(g)\in I$ を満たせば S の上で g と g' が同値な多項式であると判断できる.

従って「文字列として最短であると同時に辞書式順序で最初のもの」などという定義を「CGS の標準形」に与える事は理論的には可能であり, この「標準形」を出力するアルゴリズムは以下のように与える事ができる. しかしこれは非現実的であると同時にユーザにとっても不便である.

アルゴリズム StupidCanonicalCGS

入力: $F\subseteq K[\bar{X},\bar{A}]$ 有限

1. F の簡約 CGS G_0 をとにかく計算する.
2. G_0 より長くない文字列の範囲内で、辞書式順序で小さい順から「CGS を表現していて G_0 と同値なもの」を順に調べる.
3. 最初に見つかった G を出力する.

少なくとも G_0 という上限があるので, このアルゴリズムは停止する事がわかる.

実際には, この StupidCanonicalCGS は現実的な時間内で停止しないとともに, 必ずしも数学的に意味のある出力が得られるとは限らない. そこでより妥当性の高い CGS の標準形の定義を与えたいが, ここでは以下のようなポリシーを採用したい.

1. 簡約 CGS を成している
2. 各断片は強簡約されている
3. 断片の数は最小
4. 各断片 (S,G) の条件部分 S の表現は一意かつ読みやすい
5. 各断片 (S,G) の基底部分 G の表現は一意かつ読みやすい
6. 計算するための現実的なアルゴリズムが存在する

これらのポリシーの中にはトレードオフの関係にあるものもあるため, どのようにバランスを取るべきなのかも熟慮する必要があろう. 特に条件 3 と条件 4-5 を同時に最適化するのは経験上困難である.

また, 種々のアルゴリズムの比較や検証のために用いるためには, 与えられた $F\subseteq K[\bar{X},\bar{A}]$ から「標準 CGS」を求められるだけではなく, 既に他の方法で F から計算された CGS を「標準 CGS」に変換する方法が望ましいであろう. 更にそれにかかる計算コストが低いのが望ましい. なお, Montes 達の MCCGS で

は与えられた F から上の 1.〜4. のみを満たす CGS を与えるアルゴリズムを目指しているが, 一意性は示されておらずあくまでも可能な限り簡約するに留まっている. 但し, 計算された CGS を「1.〜4. を満たす CGS」に変換する方法についても MCCGS[4] ではよく研究されており, 参考になるであろう.

注 4 これまでに「*canonical* な *CGS/CGB*」として *ACGB, CCGB, MCCGS* 等が提唱されてきたが, いずれも同値類の意味での *canonical* に留まり, 文字列としての一意性からはほど遠い.

4 断片数最小を目指して

強簡約された簡約 CGS $\mathcal{G} = \{(S_1, G_1), \ldots, (S_l, G_l)\}$ が与えられたとする. その断片 (S_i, G_i) を任意に固定した時, 各 $\bar{a} \in S_i$ に対して,$\sigma_{\bar{a}}[G_i]$ に含まれる先頭項の集合 $ht[\sigma_{\bar{a}}[G_i]]$ は一定である. 実際 $T_i := ht_{\bar{A}}[G_i]$ とした時, 任意の $\bar{a} \in S_i$ に対して $T_i = ht[\sigma_{\bar{a}}[G_i]]$ が成り立つ.

よって, 各 $T \in \mathcal{T}_{\mathcal{G}} := \{ht_{\bar{A}}[G_i] : i = 1, \ldots, l\}$ に対して, $\mathcal{G}_T = \{(S_i, G_i) \in \mathcal{G} : ht_{\bar{A}}[G_i] = T, i = 1, \ldots, l\}$ に含まれる断片達を一つにまとめる事が可能であれば, 強簡約された CGS として断片を最小のものを得る事ができ, これ以上断片の個数を減らす事はできない事がわかる. つまり (S_T, G_T) をうまく取る事で, $\{(S_T, G_T)\}$ と $\mathcal{G}_T$ を同値にできれば $\{(S_T, G_T) : T \in \mathcal{T}_{\mathcal{G}}\}$ は条件 1.〜3. を満たす. しかしそのような (S_T, G_T) がどのような条件下で取れるかは明らかになっていない.

例 5 (Montes 2007) $\{ax + b, cx + d\}$ *(*媒介変数は a, b, c, d*)* に対する簡約 *CGS* の断片の内, 先頭項集合として $\{x\}$ のものだけ取り出すと

$$\{(ad - bc = 0, a \neq 0)\{ax + b\}, (a = 0, b = 0, c \neq 0)\{cx + d\}\}$$

となるが, これらを一つの断片にまとめるために *Motes* は

$$(ad - bc = 0 \wedge (a \neq 0 \vee c \neq 0))\{ax + b, cx + d\}$$

という表現を許容する事を提案している.

但し, このような許容を以ってしても以下の様な例に対処できず, 一つの断片にまとめる事はできない.

例 6 (Wibmer 2006) $\{a^2x - a, ax^2 - x\}$ *(*媒介変数は a*)* に対する簡約 *CGS* は

$$\{(a = 0), \{x\}, (a \neq 0), \{ax - 1\}\}$$

と計算される.

本報告では, これらの例に対する解決案として余剰な媒介変数の導入を提案した. Motens の例に対しては e を余剰補助変数として,

$$(ad - bc = 0 \wedge ea + c \neq 0 \wedge (a \neq 0 \vee c \neq 0)) \quad \{(ea + c)x + (eb + d)\}$$

という一つの断片として, また Wibmer の例に対しては b を余剰媒介変数として,

$$(ab = 0 \wedge (a \neq 0 \vee b \neq 0)) \quad \{(a^2 + b)x - a\}$$

という一つの断片として表現できる. ただし, これらの解決案についても (1) CGS の定義を変更する必要がある, (2) 一意性をどう実現するか, などの問題が残されている.

5 条件部分及び基底部分の表現を一意かつ読みやく

条件部分の表現については2007年のRisaConで提案した方法を用いる事で実現できる. また, それ以外の方法での採用可能であり, どの定義を用いるかだけの問題となる. 従って問題は, 基底部分についても一意かつ読みやすい表現が存在するか否か, そしてもし存在すればそれを計算するにはどうするか, となる.

簡約CGSの断片 (S,G) が与えられた時, 多項式 $g \in G$ が標準的なものであって欲しい際に最低限満たして欲しい条件として以下を挙げる事ができる. 但し $g = c_1t_1 + \cdots + c_nt_n$ $(c_1,\ldots,c_n \in K[\bar{A}] \setminus \{0\}, t_1,\ldots,t_n \in T(\bar{X}), t_1 > \cdots > t_n)$ と書けているとし, 議論を容易にするために条件部分 S が $S = V(Z) \setminus V(N)$ と書けていて Z が素イデアルの簡約グレブナー基底であると仮定する.

1. 各 $i = 1,\ldots,n$ に対して $\mathrm{nf}_Z(c_i) = c_i$,
2. $\gcd(c_1,\ldots,c_n) = 1$.

しかしこれだけでは一意とならない事は以下の例からもわかる.

例 7 $S = V(a^2+b) \setminus V(a)$ の上で $f = ax^2 - (a+b)x$ と $g = x^2 + (a-1)x$ は同じ多項式を示す. *(つまり任意の $(a,b) \in S$ に対して $\sigma_{(a,b)}(f)$ を monic 化したものと $\sigma_{(a,b)}(g)$ (を monic 化したもの) は一致する.)*

この例では g の方が「読みやすい」ので S の上で f を g へ変換したいのだが, これは以下のようなアイディアに基き実現できる. 但し後で述べるように一般の断片に対して適用できない不完全なアイディアである旨注記しておく.

基本的なアイディアは, $K[a,b]$ に於いて $a+b \equiv a-a^2 \bmod \langle a^2+b\rangle$ である事から a を $\gcd_{K[a,b]/\langle a^2+b\rangle}(a, a+b)$ のようなものと考え, f の各係数を a で「割る」事で g を得るというものである. つまり上記の最低限満たして欲しい条件の「$\gcd(c_1,\ldots,c_n) = 1$」を「$\gcd_{K[\bar{A}]/\langle Z\rangle}(c_1,\ldots,c_n) = 1$」で置き替えられれば良い. 但し, $\gcd_{K[\bar{A}]/\langle Z\rangle}$ を定義できるための条件が明らかになっていない点に問題が残されている. どこに集中すれば良いのかという問題提起を以下に記す.

定義 8 $I \subseteq K[\bar{A}]$ を素イデアル, $a,b \in K[\bar{A}] \setminus I$ とする. この時 $d \in K[\bar{A}]$ が **I を法としての a と b の共通因子**であるとは、$a'd - a \in I$ かつ $b'd - b \in I$ となる $a', b' \in K[\bar{A}]$ が存在する時に言う.

問題 9 与えられた I, a, b に対し, *(「最大」とは限らない)* 極大共通因子を見つけたい. つまり

$$D = \{d \in K[\bar{A}] \ : \ d \text{は} I \text{を法としての} a \text{と} b \text{の共通因子}\}$$

とした時に、$\bar{d} \in D$ を $c\bar{d} \in D$ となる $c \in K[\bar{A}] \setminus K$ が存在しないように見つけたい.

注 10 $K[\bar{A}]/I$ が *UFD* であれば $\gcd(a,b)$ を $K[\bar{A}]/I$ で考えればいいが、一般には $K[\bar{A}]/I$ は *UFD* ではない。ただし、I を素としているので整域ではある。

ここで $\dim(I) = 0$ の時には I は極大イデアルなので $K[\bar{A}]/I$ は体となり, 何もする事はない. また $\dim(I) = 1$ の時には $\gcd_{K[\bar{A}]/I}(c_1,\ldots,c_n) = 1$ とする手続きの候補は以下のように与えられる. 実際, この手続きに従えば例7の f は g に変換できる事も確認できる.

ここで $I \subseteq K[\bar{A}]$ を1次元素イデアル, $a_1t_1 + \cdots + a_nt_n \in K[\bar{A}, \bar{X}]$ を与えられた多項式とする. 但し $a_i \in K[\bar{A}] \setminus I$, $t_i \in T(\bar{X})$ とする.

1. $\{B\} \subseteq \bar{A}$ を maximally independent modulo I とする.
2. 各 $i = 1,\ldots,n$ に対して,

(a) $I+\langle a_i\rangle$ は 0 次元なので $K[B]\cap(I+\langle a_i\rangle)$ の生成元 b_i を取れて,

(b) $c_i\in K[\bar{A}]$ を $\mathrm{nf}_I(c_ia_i)=b_i$ なるものとする.

3. $c:=\mathrm{lcm}(c_1,\ldots,c_n)$ とする.

4. 各 $i=1,\ldots,n$ に対して,

(a) $d_i=\mathrm{nf}_I((c/c_i)b_i)_{B\gg\bar{A}\setminus\{B\}}$ とする.

5. $d:=gcd(d_1,\ldots,d_n)_{K(\bar{A}\setminus\{B\})[B]}$ とおき,

6. $e_i=d_i/d\in K[\bar{A}]$ とおく.

7. $e_1t_1+\cdots+e_nt_n\in K[\bar{A},\bar{X}]$ を返す.

この時、各 i に対して $K[\bar{A}]/I$ にて $c_1c_id(a_1e_i-e_1a_i)=c_1c_i(a_1d_i-d_1a_i)=c_1c_i(a_1(c/c_i)b_i-(c/c_1)b_1a_i)=c(c_1a_1b_i-c_ib_1a_i)=0$ であり, I が素である事より $a_ie_1-e_1a_i\in I$ がわかる. つまり有理関数 a_i/a_1 と e_i/e_1 は $V(I)$ の上 (の定義される範囲) で一致する.

但しこの手続きを 2 次元以上に拡張する手法については議論の余地が多く残されている.

6 最後に

以上のように canonical な CGS の定義に向けて乗り越えるべき困難は多く残されている. 特に,

- 断片の数を減らす際にどこまで定義の拡張を許すか,
- 基底部分の標準形をヒューリスティックな手法に頼らず得る事ができるか,

という二点については互いに影響を与える点もあり, 克服までにはまだ研究が必要であると予想される.

参 考 文 献

[1] Dolzmann, A. and Sturm, T. (1997). Redlog: Computer algebra meets computer logic, ACM SIGSAM Bulletin, 31, 2, 2–9.

[2] Manubens, M. and Montes, A. (2004). Improving DISPGB Algorithm using the discriminant ideal, J. Symb. Comp., 41, 1245–1263.

[3] Montes, A. (2002). A new algorithm for discussing Gröbner basis with parameters, J. Symb. Comp. 33, 1-2, 183–208.

[4] Manubens, M. and Montes, A. (2006). Minimal Canonical Comprehensive Gröbner System, preprint MA2-IR-06-00015.

[5] Noro, M. and Takeshima, T. (1992). Risa/Asir – A Computer Algebra System. International Symposium on Symbolic and Algebraic Computation (ISSAC 92), Proceedings, 387–396.

[6] Suzuki, A. and Sato, Y. (2002). An Alternative approach to Comprehensive Gröbner Bases. International Symposium on Symbolic and Algebraic Computation (ISSAC 2002), Proceedings, 255–261.

[7] Suzuki, A. and Sato, Y. (2003). An Alternative approach to Comprehensive Gröbner Bases. J. Symb. Comp. 36/3-4, 649–667.

[8] Suzuki, A. and Sato. Y. (2006). A Simple Algorithm to Compute Comprehensive Gröbner Bases Using Gröbner Bases, International Symposium on Symbolic and Algebraic Computation (ISSAC 2006), Proceedings, 326–331.

[9] Weispfenning, V. (1992). Comprehensive Gröbner bases, J. Symb. Comp. 14/1, 1–29.

[10] Weispfenning, V. (2003). Canonical Comprehensive Gröbner bases, J. Symb. Comp. 36, 669-683.