数理解析研究所講究録
1514巻 2006年 132-137

グレブナー基底を用いた包括グレブナー基底計算

鈴木 晃
AKIRA SUZUKI
神戸大学 情報管理室
OFFICE OF INFORMATION MANAGEMENT, KOBE UNIVERSITY

Abstract
包括グレブナー系と包括グレブナー基底を計算する新しいアルゴリズムの概略について述べる。このアルゴリズムで必要とされるのは簡約グレブナー基底のみであり、実装は非常に容易である。

1 はじめに

包括グレブナー基底 (comprehensive Gröbner basis) と包括グレブナー系 (comprehensive Gröbner system) は Volker Weispfenning により 1992 年に導入され、[7] 同時にその存在と計算アルゴリズムが示された。近年、Montes による DispGB [1, 2], 鈴木-佐藤による ACGB [4, 5], Weispfenning による CCGB [8] など新しいアルゴリズムの導入が進んできた。これらのアルゴリズムはグレブナー基底を計算するためのブッフバーガーアルゴリズムへ、パラメータによる場合分けを組み合わせる事で拡張されたもの考えられ、各々独自の S-多項式や単項簡約 (monomial reduction) を必要としていた。(但し DispGB などでは既存アルゴリズムとの併用にて独自の単項簡約の使用量を削減している。) また、この独自な単項簡約の為の特殊なデータ構造をも必要とする。その重要性にも関わらず多くの数式処理システムに対する包括グレブナー基底の実装が遅れてきた理由は、これらの理由による影響も大きいだろうと筆者は考える。

本論文では新しい考え方に基く包括グレブナー系及び包括グレブナー基底のアルゴリズムをそのアイディアと共に紹介する。このアルゴリズムで必要とされるのは体係数の多項式環に対する簡約グレブナー基底 (reduced Gröbner basis) のみであり、特殊なデータ構造や単項簡約は必要とされない。また、簡約グレブナー基底を計算するアルゴリズムはどのようなものであっても構わない。アルゴリズム自身は簡易であり、その実装もこれまでのもの達よりも大幅に簡素であり、また多くの場合に計算が高速に行われる。

このアルゴリズムが高速である理由の代表として以下の二点を挙げることができるだろう。

1. 数式処理システムに内蔵された簡約グレブナー基底のルーチンを使用できる。
   多くの場合、内蔵ルーチンは最適・高速化がなされており、その使用は独自開発ルーチンより高速となる場合が多い。
2. 場合分けの場合達に共通部分を許した。
   これにより場合分け判定の大幅な単純化がもたらされた。この単純化は理論のみならず実装の簡素化や計算の高速化に繋がる。

特に 2 番目で触れられている場合分け判定の単純化は重要である。これまでのアルゴリズムの多くはこの判定をいかに効率よく行なうか、またはいかに全体での計算量を減らすよう判定を行なうかに注意が向けらてきた。一方で、今回のアルゴリズムでは実質的に条件分岐の判定は簡約グレブナー基底の計算に含まれるため包括グレブナー系の中では行なう必要がない。新しいアルゴリズムでも条件分岐は必要とされるものの、そのための計算を改めて行なう必要はない。

2 包括グレブナー系

以下、この論文では K を任意の体とし、その代数閉体を L とする。また、$\bar{X}=\{X_1,\ldots,X_n\}$ を変数、$\bar{A}=\{A_1,\ldots,A_m\}$ を媒介変数とし、$\bar{X}\cap\bar{A}\neq\emptyset$ と仮定する。また、$\bar{X}$ 上の項達 $T(\bar{X})$ 上の項順序 $<_{\bar{X}}$ を固定しておく。各 $F\subseteq K[\bar{A}]$ に対して $V(F)\subseteq K^m$ を $V(F)=\{\bar{a}\in L^m:(\forall f\in F)f(\bar{a})=0\}$ で定義し、特に $f\in K[\bar{A}]$ に対しては $V(f)=V(\{f\})$ とおく。この時、包括グレブナー系を以下のように定義する。

各 $\bar{a}\in L^m$ に対して特化準同型 (specialization homomorphism) $\sigma_{\bar{a}}:K[\bar{A}]\to L$ を各 A_i への a_i の代入により自然に定義し、更にこれを $\sigma_{\bar{a}}:K[\bar{X},\bar{A}]\to L[\bar{X}]$ へと自然に拡張する。

定義 1 F を $K[\bar{X},\bar{A}]$ の有限部分集合とする。$S\subseteq L^m$ を代数構成的集合とする。対達の有限集合 $\mathcal{G}=\{(S_1,G_1),\ldots,(S_l,G_l)\}$ が F に対する S 上の**包括グレブナー系**であるとは以下を満たす時に言う。

1. $S_1,\ldots,S_l$ は L^m の構成的部分集合、$G_1,\ldots,G_l$ は $K[\bar{X},\bar{A}]$ の有限部分集合であり、

2. $S_1\cup\cdots\cup S_l\supseteq S$ を満たし、

3. 各 $i=1,\ldots,l$ と各 $\bar{a}\in S_i$ に対して $\sigma_{\bar{a}}[G_i]$ が $\sigma_{\bar{a}}[F]$ の $L[\bar{X}]$ におけるグレブナー基底をなす。

特に F に対する L^m 上の包括グレブナー系を単に F に対する**包括グレブナー系**と呼ぶ。

この時、包括グレブナー基底は以下のように特徴付けられる。

定義 2 F と G を $K[\bar{X},\bar{A}]$ の有限部分集合とする。G が F の**包括グレブナー基底**であるとは、$\{(L^m,G)\}$ が F に対する包括グレブナー系である時に言う。

以下の定理が新しいアルゴリズムでの鍵となる。以降、各 $f\in K[\bar{X},\bar{A}]$ に対して $\mathrm{hc}_{\bar{A}}(f)\in K[\bar{A}]$ を $f\in(K[\bar{A}])[\bar{X}]$ と見た時の先頭係数とする。

定理 1 F を $K[\bar{X},\bar{A}]$ の有限部分集合とする。$\bar{X}\cup\bar{A}$ 上の項達 $T(\bar{X},\bar{A})$ 上の項順序 $<_{\bar{X},\bar{A}}$ は $<_{\bar{X}}$ を $\bar{X}\gg_{\bar{X},\bar{A}}\bar{A}$ を満たすように拡張したものであるとする。G を $K[\bar{X},\bar{A}]$ でのイデアル $\langle F\rangle$ の $<_{\bar{X},\bar{A}}$ に関するグレブナー基底とする。この時、全ての $g\in G\setminus K[\bar{A}]$ に対して $\mathrm{hc}_{\bar{A}}(g)(\bar{a})\neq 0$ なる $\bar{a}\in V(\langle F\rangle\cap K[\bar{A}])$ に対して、$L[\bar{X}]$ に於いて $\sigma_{\bar{a}}[G]$ は $\langle\sigma_{\bar{a}}[F]\rangle$ のグレブナー基底を成す。

証明についてはこれを省略するが、主単項のふるまいを考えれば自然な主張であると言える。つまり、定理の条件を満たす $\bar{a}$ に対しては $\{\mathrm{ht}_{\bar{A}}(g):g\in G\}\setminus\{0\}=\{\mathrm{ht}(g'):g'\in\sigma_{\bar{a}}[G]\}\setminus\{0\}$ となる事と $\sigma_{\bar{a}}[G]\subseteq\langle\sigma_{\bar{a}}[F]\rangle$ が $G\subseteq\langle F\rangle$ から導かれる事から推察できるであろう。

ここで与えられた有限部分集合 $F\subseteq K[\bar{X},\bar{A}]$ に対する $V(\langle F\rangle\cap K[\bar{A}])$ 上の包括グレブナー系を求める事を考える。まず G を $\bar{X}\gg\bar{A}$ なる項順序での $K[\bar{X},\bar{A}]$ におけるイデアル $\langle F\rangle$ の簡約グレブナー基底とする。更に $\{h_1,\ldots,h_l\}=\{\mathrm{hc}_{\bar{A}}(g):g\in G\setminus K[\bar{A}]\}$ とおき、$h=\mathrm{lcm}\{h_1,\ldots,h_l\}\in K[\bar{A}]$ とおく。この時、$\bar{a}\in V(\langle F\rangle\cap K[\bar{A}])\setminus V(h)$ は $h(\bar{a})\neq 0$ を満たすので、上記の定理により $\sigma_{\bar{a}}[G]$ が $\langle\sigma_{\bar{a}}[F]\rangle$ のグレブナー基底である事がわかる。つまり $\{(V(\langle F\rangle\cap K[\bar{A}])\setminus V(h),G)\}$ は F に対する $V(\langle F\rangle\cap K[\bar{A}])\setminus V(h)$ 上の包括グレブナー系をなす。よって $V(\langle F\rangle\cap K[\bar{A}])\setminus V(h)=V(\langle F\rangle\cap K[\bar{A}])\setminus V(\langle F\cup\{h\}\rangle\cap K[\bar{A}])$ の残りとして F に対する $V(\langle F\cup\{h\}\rangle\cap K[\bar{A}])$ 上の包括グレブナー系が計算できればよい。ここで $V(\langle F\cup\{h\}\rangle\cap K[\bar{A}])=V(\langle F\cup\{h_1\}\rangle\cap K[\bar{A}])\cup\cdots\cup V(\langle F\cup\{h_l\}\rangle\cap K[\bar{A}])$ に注意すると各 $V(\langle F\cup\{h_i\}\rangle\cap K[\bar{A}])$ $(i=1,\ldots,l)$ 上の包括グレブナー系が求まれば充分である。

各 $i=1,\ldots,l$ に対して G_i を再び $\bar{X}\gg\bar{A}$ なる項順序での $\langle F\cup\{h_i\}\rangle$ の簡約グレブナー基底とし、$h_i'=\mathrm{lcm}\{\mathrm{hc}_{\bar{A}}(g):g\in G_i\setminus K[\bar{A}]\}$ とおくと、再び定理により $\{(V(\langle F\cup\{h_i\}\rangle\cap K[\bar{A}])\setminus V(h_i'),G_i)\}$ が $F\cup\{h_i\}$ に対

する $V((\langle F\cup\{h_i\}\rangle\cap K[\bar{A}])\setminus V(h_i')$ 上の包括グレブナー系である事がわかるが、$\bar{a}\in V((\langle F\cup\{h_i\}\rangle\cap K[\bar{A}])\setminus V(h_i')$ に対しては $h_i(\bar{a})=0$ より $\sigma_{\bar{a}}[F]\setminus\{0\}=\sigma_{\bar{a}}[F\cup\{h_i\}]\setminus\{0\}$ であるので、$\{V((\langle F\cup\{h_i\}\rangle\cap K[\bar{A}])\setminus V(h_i'),G_i)\}$ は F に対する $V(F\cup\{h_i\})\setminus V(h_i')=V((\langle F\cup\{h_i\}\rangle\cap K[\bar{A}])\setminus V((\langle F\cup\{h_i,h_i'\}\rangle\cap K[\bar{A}])$ 上の包括グレブナー系である事がわかる。以下、各 $V((\langle F\cup\{h_i,h_i'\}\rangle\cap K[\bar{A}])$ に対してこの段落の議論を再帰的に繰り返し、もし停止すれば $\langle F\rangle\cap K[\bar{A}]$ 上の包括グレブナー系を得られる。一方で $\bar{a}\notin V(\langle F\rangle\cap K[\bar{A}])$ に対しては $\langle\sigma_{\bar{a}}[F]\rangle=\langle 1\rangle$ である事も容易にわかる。

しかしこの再帰は必ず有限の深さで停止する。実際、あるステップにて $\langle F\cup S\rangle$ の簡約グレブナー基底 G_S が計算され、$\{h_1^S,\ldots,h_{l'}^S\}=\{\mathrm{hc}_{\bar{A}}(g):g\in G_S\setminus K[\bar{A}]\}$ とおいたとするとその次の再帰レベルでは $\langle F\cup S\cup\{h_1^S\}\rangle,\ldots,\langle F\cup S\cup\{h_{l'}^S\}\rangle$ に対する計算が行なわれる。ここで G_S が簡約されている事に注意すると各 $i=1,\ldots,l'$ に対して $h_i^S\notin\langle F\cup S\rangle$ であるので $\langle F\cup S\rangle\subsetneq\langle F\cup S\cup\{h_i^S\}\rangle$ がわかる。$K[\bar{X},\bar{A}]$ はネーター環であるのでこの $\subsetneq$-列は有限である。更に各ステップで分岐数 l' は有限である事から König の補題により計算全体の停止性もわかる。

上記の計算が以下のアルゴリズム **CGSMain** で行なわれ、**CGSMain** のための前処理・後処理がアルゴリズム **CGS** にて行なわれる。従ってアルゴリズム **CGS** は与えられた有限 $F\subseteq K[\bar{X},\bar{A}]$ に対する包括グレブナー系を出力する事がわかる。

アルゴリズム CGSMain

入力：$F\subseteq K[\bar{X},\bar{A}]$ 有限

```
G := ReducedGB(F, <_{X̄,Ā});
if 1∈G then
 return ∅;
else
 {h_1,...,h_l} := {hc_Ā(g) : g∈G\K[Ā]};
 h := lcm{h_1,...,h_l};
 return {(V(G∩K[Ā])\V(h),G)}∪
   CGSMain(F∪{h_1})∪···∪CGSMain(F∪{h_l});
end if
end.
```

アルゴリズム CGS

入力：$F\subseteq K[\bar{X},\bar{A}]$ 有限, $<_{\bar{X}}$：$T(\bar{X})$ 上の項順序

```
<_{X̄,Ā} := T(X̄,Ā) 上の項順序で X̄ ≫ Ā を満たすよう <_X̄ を拡張したもの;
G := CGSMain(F);
S := ⋃{S' : (∃G')(S',G')∈G};
return {(L^m\S,{1})}∪G;
end.
```

3 包括グレブナー基底

現在までに包括グレブナー基底を直接計算する手法は提案されておらず、包括グレブナー基底の計算は包括グレブナー系を介して行なわれる。ただし一般に $\{(S_1,G_1),\ldots,(S_l,G_l)\}$ が F に対する包括グレブナー

系であったとしても $G_1 \cup \cdots \cup G_l$ が包括グレブナー基底をなすとは限らないが、以下の**誠実**(faithful) 包括グレブナー系の導入によりこの問題は回避できる。

定義 3 $F \subseteq K[\bar{X}, \bar{A}]$ に対する包括グレブナー系 $\{(S_1, G_1), \ldots, (S_l, G_l)\}$ が *(F に対して)* **誠実**であるとは $K[\bar{X}, \bar{A}]$ において $G_1 \cup \cdots \cup G_l \subseteq \langle F \rangle$ である時に言う。

ここで与えられた $F \subseteq K[\bar{X}, \bar{A}]$ に対する誠実包括グレブナー基底 $\{(S_1, G_1), \ldots, (S_l, G_l)\}$ が得られたとし、$\bar{a} \in L^m$ を任意に固定する。この時、誠実さにより $\sigma_{\bar{a}}[G_1 \cup \cdots \cup G_l] \subseteq \langle \sigma_{\bar{a}}[F] \rangle$ が成立する。一方で、$\bar{a} \in S_i$ なる $i = 1, \ldots, l$ が存在し、この時 $\sigma_{\bar{a}}[G_i]$ が $\langle \sigma_{\bar{a}}[F] \rangle$ のグレブナー基底となるので、特に $\sigma_{\bar{a}}[G_1 \cup \cdots \cup G_l]$ は $\langle \sigma_{\bar{a}}[F] \rangle$ のグレブナー基底をなす。つまり $G_1 \cup \cdots \cup G_l$ は F に対する包括グレブナー基底をなす。

誠実包括グレブナー系を得るための方法には以下の 2 通りがある。

i. 誠実さを保ったまま包括グレブナー系の計算を進める。
   これまでの方法では特殊なデータ構造を必要とし、その結果、包括グレブナー系の計算において、特別な単項簡約も必要となった。

ii. 包括グレブナー系を求めてからそれを誠実にする。
   この方法では包括グレブナー系の計算アルゴリズム自身は簡素にしやすいものの、その計算後に改めて誠実にするためのグレブナー基底計算が必要となった。

本論文では i. の方法を採用するが、これを前節で採用したアルゴリズムに適合させるためにダミー変数 U を導入すると同時に、$T(\bar{X}, \bar{A})$ 上の項順序 $<_{\bar{X},\bar{A}}$ を更に $T(U, \bar{X}, \bar{A})$ 上へ $U \gg \bar{X} \gg \bar{A}$ を満たすよう拡張し、それを $<_{U,\bar{X},\bar{A}}$ と記す。また各 $f \in K[U, \bar{X}, \bar{A}]$ に対して $\mathrm{hc}_{\bar{X},\bar{A}}(f) \in K[\bar{X}, \bar{A}]$ を $(K[\bar{X}, \bar{A}])[U]$ としての先頭係数とする。

また、各 $F \subseteq K[\bar{X}, \bar{A}]$ と $h \in K[U]$ に対して $h \cdot F = \{h \cdot f \in K[U, \bar{X}, \bar{A}] : f \in F\}$ とおく。また、特化準同型 $\sigma^* : K[U, \bar{X}, \bar{A}] \to K[\bar{X}, \bar{A}]$ を $\sigma^*(U) = 1$ で自然に定義する。この時、以下の事実は容易に得られる。

事実 1 任意の $F \subseteq K[\bar{X}, \bar{A}]$ と $S \subseteq K[\bar{A}]$ に対し、$K[U, \bar{X}, \bar{A}]$ において $G \subseteq \langle U \cdot F \cup (U-1) \cdot S \rangle$ であるとする。この時、$K[\bar{X}, \bar{A}]$ において $\sigma^*[G] \subseteq \langle F \rangle$ である。

また、前節と同様に以下の定理が成立する。証明はこれを省略するが、興味を持たれた方は [6] を参照されたい。

定理 2 F を $K[\bar{X}, \bar{A}]$ の有限部分集合、S を $K[\bar{A}]$ の有限部分集合とする。$U \cup \bar{X} \cup \bar{A}$ 上の項達 $T(U, \bar{X}, \bar{A})$ 上の項順序 $<_{U,\bar{X},\bar{A}}$ は $<_{\bar{X}}$ を $U \gg \bar{X} \gg_{\bar{X},\bar{A}} \bar{A}$ を満たすように拡張したものであるとする。G を $K[U, \bar{X}, \bar{A}]$ でのイデアル $\langle U \cdot F \cup (U-1) \cdot S \rangle$ の $<_{U,\bar{X},\bar{A}}$ に関する簡約グレブナー基底とする。この時、全ての $\mathrm{hc}_{\bar{X},\bar{A}}(g) \notin K[A]$ なる $g \in G \setminus K[\bar{X}, \bar{A}]$ に対して $\mathrm{hc}_{\bar{A}}(g)(\bar{a}) \neq 0$ となる $\bar{a} \in V(S) \cap V(\langle F \rangle \cap K[\bar{A}])$ に対して、$L[\bar{X}]$ に於いて $\sigma_{\bar{a}}[\sigma^*[G]]$ は $\langle \sigma_{\bar{a}}[F] \rangle$ のグレブナー基底を成す。

本質的には前節と同じ議論が成立する。但し、事実 1. により定理 2. の $\sigma^*[G]$ は誠実包括グレブナー系の一部を為す。以上により包括グレブナー基底を計算するアルゴリズムは以下のように記述できる。与えられた $F \subseteq K[\bar{X}, \bar{A}]$ に対して、**CGBMain**$(F, \emptyset)$ は誠実包括グレブナー系を、**CGB**(F) は包括グレブナー基底を出力する。

アルゴリズム **CGBMain**

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

G := ReducedGB($\langle U \cdot F \cup (U-1) \cdot S,\ <_{U,\bar{X},\bar{A}}\rangle$;
if $1 \in \langle S \rangle$ then
 return $\{(V(S), \sigma^*[G])\}$;
else
 $\{h_1, \ldots, h_l\} := \{\mathrm{hc}_{\bar{A}}(g) : g \in G \setminus K[\bar{X}, \bar{A}], \mathrm{hc}_{\bar{X},\bar{A}}(g) \notin K[\bar{A}]\}$;
 $h := \mathrm{lcm}\{h_1, \ldots, h_l\}$;
 return $\{(V(S) \setminus V(h), \sigma^*[G])\} \cup$
  CGBMain($F, S \cup \{h_1\}$)$\cup \cdots \cup$CGBMain($F, S \cup \{h_l\}$);
end if
end.

アルゴリズム **CGB**

入力: $F \subseteq K[\bar{X}, \bar{A}]$ 有限, $<_{\bar{X}} : T(\bar{X})$ 上の項順序

$<_{U,\bar{X},\bar{A}} := T(U, \bar{X}, \bar{A})$ 上の項順序で $U \gg \bar{X} \gg \bar{A}$ を満たすよう $<_{\bar{X}}$ を拡張したもの;
$\{(S_1, G_1), \ldots, (S_l, G_l)\}$:= CGBMain($F, \emptyset$);
return $G_1 \cup \cdots \cup G_l$;
end.

4 最後に

本論文では包括グレブナー系及び包括グレブナー基底を計算する新しいアルゴリズムの概略を紹介した。より詳細な内容については [6] を参照されたい。これらのアルゴリズムは記述や理論が単純というだけではなく、実装も簡易であり、実際に筆者は包括グレブナー系の実装を Risa/Asir [3] をはじめとした複数の数式処理システム上に実装した。また、計算実験を通じてこの新しいアルゴリズムは既存のものより多くの場合に高速である事もわかった。

全体の見通しが良くなった事から多くの最適化手法が考えられる事も新しいアルゴリズムの利点である。既に様々な最適化手法が提案され、それらの内のいくつかは実装済みである。どのような場合にどのような最適化手法が有効であるかといった調査は今後の課題として残されている。

参 考 文 献

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

[2] Manubens, M. and Montes, A. (2005). Improving DISPGB Algorithm Using the Discriminant Ideal, J. Symb. Comp., A3L 2005 special issue, to appear

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

[4] 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.

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

[6] 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, to appear

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

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