数理解析研究所講究録 第2104巻 2019年 65-77

疎な多変数多項式系の高速な変数消去法の探求

Towards Fast Method of Variable Elimination of Sparse Multivariate Polynomial Systems *

佐々木 建昭 (Tateaki Sasaki) †
筑波大学 名誉教授
(University of Tsukuba)

稲葉 大樹 (Daiju Inaba) ‡
(公財) 日本数学検定協会
(Japan Assoc. Math. Certification)

Abstract

Given $\{F_1, \ldots, F_{m+1}\} \subset \mathbb{K}[\boldsymbol{x}, \boldsymbol{u}]$, with $m \geq 2$, where $\mathbb{K}$ is a number field of characteristic 0, $(\boldsymbol{x}) = (x_1, \ldots, x_m)$ and $(\boldsymbol{u}) = (u_1, \ldots, u_n)$, we want to develop an efficient method of computing $\widehat{S}(\boldsymbol{u})$ which is the smallest polynomial of the elimination ideal $\langle F_1, \ldots, F_{m+1}\rangle \cap \mathbb{K}[\boldsymbol{u}]$, without computing the Gröbner basis but eliminating $\boldsymbol{x}$ with polynomial remainder sequences w.r.t. $\boldsymbol{x}$. Our targets are sparse multivariate polynomials of many sub-variables $\boldsymbol{u}$. Last year, we succeeded in finding such a method for $\{G, H\} \subset \mathbb{K}[x, \boldsymbol{u}]$. The method is much more efficient than the Gröbner basis method when $n \geq 3$. In this paper, we attack the case of $m \geq 2$. Contrary to the conventional triangularization method which converts the initial system to $\{G_1(x_1, \ldots, x_m, \boldsymbol{u}), G_2(x_2, \ldots, x_m, \boldsymbol{u}), \ldots, G_m(x_m, \boldsymbol{u}), H(\boldsymbol{u})\}$, our method computes $H_1(\boldsymbol{u}), \ldots, H_l(\boldsymbol{u})$. We will prove that each $H_i(\boldsymbol{u})$ $(i \in \{1, \ldots, l\})$ is a multiple of $\widehat{S}$, so we compute $H := \gcd(H_1, \ldots, H_l)$. H is a small multiple of $\widehat{S}$: $H = \widetilde{H}\widehat{S}$. We propose a method of deleting "extraneous factor" $\widetilde{H}$, by factorizing H.

Key words: elimination ideal of polynomial system, lowest-order element of elimination ideal, Gröbner basis, multivariate sparse polynomial remainder sequence, triangular system, extraneous factor

---

*本研究は科研費 (課題番号 15K00005) の支援で行われた.

†sasaki@math.tsukuba.ac.jp
‡d.inaba@su-gaku.net

1　はじめに

本稿では、与多項式はすべては標数 0 の数体 $\mathbb{K}$ 上の多項式とする。

多変数多項式系の変数消去は、数式処理の応用では最も基本的かつ重要なものである。その算法は、剰余列 (polynomial remainder sequence、**PRS** と略記) 法とグレブナー基底 (Gröbner basis、**GB** と略記) 法に大別される；細かく言えば、Sylvester 行列の行列式で定義される終結式 (resultant) を計算する方法もあるが、剰余列の最終要素は最大公約子 (GCD) あるいは終結式なので、この方法は剰余列法に含める。

与多項式が 3 個以上の場合、各消去変数 (これを**主変数**と呼ぶ) 毎に、一つの多項式と他の多項式たちとの剰余列を計算することで、多項式系を主変数に関して三角化できる。三角化された系は**三角系** (triangular system) と呼ばれる。一方、グレブナー基底の算法は、多項式を単項式の和と見なし、単項式全体を一意的に順序づける項順序を導入して、消去する多項式に最小の単項式を掛けることで先頭の項同士を可能な限り消去していく。グレブナー基底は広く使われるが、項順序として**辞書式順序** (各変数に順序をつける) を用いると、計算の進行につれて高位の変数から順に消去され、変数消去が行える。

二つの算法を比較すると、計算効率の点では剰余列法が遥かに優れているが、得られる多項式の数学的性質の点ではグレブナー基底法が優れている。たとえば、与多項式が消去変数に関して疎な場合、終結式は同じ因子を多重に含むことが多い。グレブナー基底法で主変数を消去すれば順序最低の多項式が得られるが、剰余列法で得られる多項式は大抵、**余計な因子** (extraneous factor) を含んでいる。上記二つの消去法は同じように見えるが、実は大きく異なるのである (これらの違いは筆者らも研究に取り掛かって初めて知った)。剰余列法は昔から有名で、グレブナー基底も誕生以来 50 年以上も経つので、両者の関係はよく解明されていると思うであろうが、全くそうでない。筆者らの知るところ、両者の関係を論じたのは文献 [17] だけだが、著者の Wang も同様なことを述べている。

このような状況下、筆者らは一昨年に**拡張ヘンゼル構成** (extended Hensel construction **EHC** と略記) 算法 [13] の効率化に取り掛かった。EHC はヘンゼル因子を主変数の消去後に残る変数たち (これを**従変数**と呼ぶ) の有理式の級数に展開する。従来は有理式の分母因子を**拡張互除法** (剰余列法の拡張) で計算していたが、疎な多項式に対して因子が多重に計算されることが多かった。一方、グレブナー基底法では簡潔な分母因子が得られた。だが、グレブナー基底法は従変数の個数が多いと計算がベラボウに重い。何とか剰余列法でグレブナー基底法と同じ簡潔な結果が得られないかと、あれこれ模索した。

EHC では、必要な変数消去は 2 多項式系 $\{G, H\} \subset \mathbb{K}[x, \boldsymbol{u}]$, $(\boldsymbol{u}) = (u_1, \ldots, u_n)$, に帰着される；$x$ が主変数で $\boldsymbol{u}$ が従変数。この簡単な系において、筆者らは非常に簡単で重要な関係式を発見した。互いに素な G と H を出発する剰余列の最終元を $P_k(\boldsymbol{u})$、その余因子の組を (A_k, B_k) とし (余因子については第 2 章で説明)、イデアル $\langle G, H\rangle$ の辞書式順序での簡約基底の最小元を $\widehat{S}(\boldsymbol{u})$ とすれば、『**定理：** (A_k, B_k) を第 2 章に述べるように規格化すれば、$P_k = c\widehat{S}$, $c \in \mathbb{K}$, となる』がそれである。この定理より、最小元 $\widehat{S}$ はグレブナー基底を用いずに剰余列法で計算できるので、従変数の個数が多い場合、$\widehat{S}$ の計算が革命的に速くなる。さらに、$\widehat{S}$ の余因子も高速に計算できる。

本稿では、前論文で扱った2多項式系の議論を3個以上の多・多項式系に拡張する。多・多項式系では上述の簡潔な定理は成立しないが、例外的場合を除き、主変数が消去された複数の多項式 $R_1, \ldots, R_l \in \mathbb{K}[\boldsymbol{u}]$ を計算できる (従来の三角系では1個しか計算しない)。すると、$R_1, \ldots, R_l$ の GCD として $\widehat{S}$ が計算できる場合が多い。本稿は他にも多くの結果を含み、従来の連立代数方程式の三角化法を一新するだろう。なお、本稿には改良・追加すべき箇所が少なからずあり、本稿は最終稿でないことを断っておく。

2　これまでの研究の簡単な復習

本章では、x は主変数、$(\boldsymbol{u}) = (u_1, \ldots, u_n)$ は従変数の組を表す。多項式 $G \in \mathbb{K}[x, \boldsymbol{u}]$ が $G = \sum_{i=0}^{l} g_i x^{d_i}$ $(g_i \in \mathbb{K}[\boldsymbol{u}],\ d_l > d_{l-1} > \cdots > d_0)$ のとき、主変数 x に関する G の 次数 d_l, 主係数 $g_l(\boldsymbol{u})$, 係因数 $\gcd(g_l, g_{l-1}, \ldots, g_0)$ (gcd は最大公約子演算) をそれぞれ $\deg(G), \mathrm{lc}(G), \mathrm{cont}(G)$ と表す。主変数 x に関して G を H で割った商と剰余をそれぞれ $\mathrm{quo}(G, H)$ と $\mathrm{rem}(G, H)$ と表す。H が G を割り切るとき $H \,|\, G$ と表す。

$G, H \in \mathbb{K}[x, \boldsymbol{u}]$ は互いに素で $\deg(G) \geq \deg(H)$ とする。G と H から始まる x に関する剰余列を $(P_1 = G,\ P_2 = H,\ P_3, \cdots, P_k)$, $0 \neq P_k \in \mathbb{K}[\boldsymbol{u}]$ とし、$\mathrm{lc}(P_i) = c_i$, $\deg(P_i) = d_i$ とおく。剰余列は $P_i \in \mathbb{K}[x, \boldsymbol{u}]$ を満たすべく生成するが、従来は擬除算が用いられていた：$P'_{i+1} := \mathrm{rem}(c_i^{d_{i-1}-d_i+1} P_{i-1}, P_i)$, $P_{i+1} := P'_{i+1}/\beta_i$。ここで P'_{i+1} が P_{i-1} の P_i による**擬剰余** (pseudo remainder (Prem)) で、$P'_{i+1} = \mathrm{Prem}(P_{i-1}, P_i)$ と表される。擬剰余列は i の増加につれて P'_{i+1} のサイズが指数関数的に増大するが、その係数の共通因子には c_j のべき乗, $j < i$, が系統的に含まれる。それを算法として除去するのが $\beta_i \in \mathbb{K}[\boldsymbol{u}]$ であり、理論的に β_i を決定しようと開発されたのが部分終結式理論である [5, 6, 2, 3]。終結式は剰余列の最終要素に対する係数行列式であるが、部分終結式理論はそれを剰余列の途中因子にまで拡張するものである。いずれも擬剰余算に基づいている。しかし、疎な多項式では $\deg(P_{i-1}) - \deg(P_i) \gg 1$ となる場合が頻繁にある。その場合には乗数 $c_i^{d_{i-1}-d_i+1}$ が大きくなるので非常に無駄である。乗数を可能な限り小さくした**疎擬剰余** (spsPrem と略記) を使うべきである。疎擬剰余は Loos [10] も定義したが、具体的算法では部分終結式理論を使っている；疎擬剰余に対する行列式理論を作れなかったのだろう。

筆者らも、昨年の論文 [16] では疎擬剰余に基づく剰余列を提唱したが、そこでは β_i を理論的に決定するには到らず、P'_{i+1} に含まれる $c_{j(<i)}$ 因子を Hearn の**試し除算法** (trial-division method)[9] で除去した。論文査読の過程で査読者から文献 [8] を教えられ、部分終結式理論に基づく擬剰余列の改良算法を知るとともに、疎擬剰余列に対する行列理論が未だ開発されていないことを知った。実は、Hearn の試し除算法は理論的裏付けがない。さらに、上記の PRS 算法は**中間式膨張**を引き起こしている (実際に必要なのは P_{i+1} だが、それを得るのに途中で大きな数式 P'_{i+1} を計算している) が、Ducos の算法でも中間式膨張は完全には抑えられていない。そこで、論文 [12] では、疎擬除算を基づく剰余列に対する行列理論を作って Hearn の試し除算法に理論的裏付けを与えるとともに、べき級数乗算を用いて P'_{i+1} の必要項だけを計算し、β_i による除算をべき級数除算で行って中間式膨張

を可能な限り抑える算法を提案した。なお、上述の剰余列の各因子 P_i に対しては余因子 (cofactor) $A_i, B_i \in \mathbb{K}[x, \boldsymbol{u}]$ が存在し、次の式を満足する。

$$A_i G + B_i H = P_i, \quad \deg(A_i) < \deg(H) - \deg(P_i), \quad \deg(B_i) < \deg(G) - \deg(P_i). \quad (2.1)$$

余因子は、剰余列と全く同じ算式で計算できる。$(P_1, A_1, B_1) := (G, 1, 0)$, $(P_2, A_2, B_2) := (G, 0, 1)$, $P_{i+1} = \mathrm{Prem}(P_{i-1}, P_i)/\beta_i = (\alpha_i P_{i-1} - Q_i P_i)/\beta_i$ とするとき、$(P_{i+1}, A_{i+1}, B_{i+1}) := \big(\alpha_i\,(P_{i-1}, A_{i-1}, B_{i-1}) - Q_i\,(P_i, A_i, B_i)\big)/\beta_i$.

$\succ_{\mathrm{el}}$ は $x \succ_{\mathrm{el}} u_1, \ldots, u_n$ を満たす項順序とし、イデアル $\langle G, H\rangle$ の順序 $\succ_{\mathrm{el}}$ に関する簡約グレブナー基底を $\mathrm{GB}(G, H)$ と表す (簡約基底とは、各要素が互いに簡約できない基底のことである)。$\boldsymbol{u}$ の順序はなんでもよいが、本稿の例題では辞書式順序を用いている。筆者らは第一論文 [14] では $\mathrm{GB}(G, H) \cap \mathbb{K}[\boldsymbol{u}] = \{\widehat{S}_1, \widehat{S}_2, \ldots\}$ と思っていた。その場合、EHC で分母因子の選び方が一意的でなくなり、嫌な気がしていた。だが、いくつか例題を試すうち $\widehat{S}_1$ だけしか出てこないので、逆に $\widehat{S}_2, \ldots$ がないのが正しいと思った。手元にあった複数の教科書を見たら、$(\boldsymbol{u}) = (u_1)$ の場合だけが終結式を用いて証明してあった。従変数が複数個の場合は自分で証明しようと模索するうち、多項式イデアルと代数多様体の間の基本的関係に思い到った。定理は基本的に第 3 章に述べる定理 1 と同じで、証明は第 3 章の定理 A をベースにし、定理 B の代りに終結式を用いて行った。

余因子はグレブナー基底の各要素にも定義できる：$\exists \widetilde{A}, \widetilde{B} \in \mathbb{K}[x, \boldsymbol{u]}$ s.t. $\widetilde{A} G + \widetilde{B} H = \widehat{S}$. $\widetilde{A}$ と $\widetilde{B}$ は、剰余列に対する余因子と同様な算法で計算できるが、その方法で計算すると大抵、次数条件は満足されないし、少し条件を変えて計算すると全く異なる余因子となることが多い。そのため、$\widehat{A}, \widehat{B}$ でなく $\widetilde{A}, \widetilde{B}$ と表した。

第 1 章で述べた「EHC のグレブナー基底による定式化」では $\widehat{S}$ のみならず $\widetilde{A}, \widetilde{B}$ も算法に必要だった。しかし、通常の算法で計算した $\widetilde{A}, \widetilde{B}$ は上述のように次数条件を満たさず大きな多項式になるが、算法ではそれぞれ H と G で可能な限り割り次数を低減していた。すると、用いた全例題で、それぞれ H と G の次数未満まで低減できた。そこで、次数低減はどんな場合にも成立するに違いないと思い、証明に着手した。以下、$g = \mathrm{lc}(G)$, $h = \mathrm{lc}(H)$ とおき、$\gamma = \gcd(g, h)$ とする。$\gamma = 1$ (1 以外の数値でもよい) の場合は容易に証明できたが、$1 \neq \gamma \in \mathbb{K}[\boldsymbol{u}]$ の場合には非常に手こずった。最終的に、(グレブナー基底計算用の) Buchberger の算法で主変数を消去して多項式 $\widetilde{P} \in \mathbb{K}[\boldsymbol{u}]$ を計算すれば、消去の進行とともに γ の因子が $\widetilde{P}$ の余因子 $\widetilde{A}$ と $\widetilde{B}$ に移動することを見出した。$\widehat{S}$ は多くの場合、Buchberger 算法をさらに $\widetilde{P}$ に適用して得られるが、その場合、$\widetilde{A}$ と $\widetilde{B}$ の高次項の全ての係数には γ が因子として含まれて高次項が H と G で次数低減できるのである。$\widetilde{A}$ と $\widetilde{B}$ が次数条件を満たさない場合、$\widehat{A}, \widehat{B}$ を $\widehat{A} := \mathrm{rem}(\widetilde{A}, H)$, $\widehat{B} := \mathrm{rem}(\widetilde{B}, G)$ と計算すれば、$\widehat{S}$ の次数条件を満たす余因子が得られる。これから、次式を導くのは容易である。

$$(P_k, A_k, B_k)/\gcd(\mathrm{cont}(A_k), \mathrm{cont}(B_k)) = c\,(\widehat{S}, \widehat{A}, \widehat{B}), \quad c \in \mathbb{K}. \quad (2.2)$$

筆者らは論文 [16] で、従変数の個数 n が 3~6 の例で、Mathematica によるグレブナー基底計算と GAL による上式を利用した $\widehat{S}$ 計算とを、計算時間の観点から比較してみた。

その結果、後者の方が $n=3$ では約 8.8 倍、$n=4$ では約 650 倍速く、$n\geq 5$ では後者が数百ミリ秒以下なのに前者は 1 時間半経っても計算が終了しなかった。

3 $\widehat{S}(\boldsymbol{u})$ に関する基本定理

主変数と従変数をそれぞれ $(\boldsymbol{x})=(x_1,\ldots,x_m)$, $(\boldsymbol{u})=(u_1,\ldots,u_n)$、与多項式の集合を $\mathcal{F}=\{F_1,F_2,\ldots,F_{m+1}\}\in\mathbb{K}[\boldsymbol{x},\boldsymbol{u}]$ とする；ここで $m\geq 2$。$\mathcal{F}$ が生成するイデアル $\langle F_1,\ldots,F_{m+1}\rangle$ を $\mathcal{I}(\mathcal{F})$ と表し、$\mathcal{I}(\mathcal{F})$ の消去順序 $\succ_{\rm el}$ に関する簡約グレブナー基底を $\mathrm{GB}(\mathcal{F})$ と表す。前章では $m=1$ だったで、暗黙裏に F_1 と F_2 ともに主変数 x を含むとしたが、本章では次のような場合も起こり得る：$\mathcal{F}'=\{F_1,\ldots,F_{m'}\}$ は $x_1,\ldots,x_{m'-1}$ のみを含み、$\mathcal{F}''=\{F_{m'+1},\ldots,F_{m+1}\}$ は $x_{m'},\ldots,x_m$ のみを含む。このような場合、$\mathcal{F}$ を一つの系と扱うよりも、二つの別々の系 $\mathcal{F}'$ と $\mathcal{F}''$ として扱うべきである。そこで、次の概念を導入して事態を簡単化する。さらに、$F_1,F_2,\ldots,F_{m+1}$ が非定数の共通因子 $C\in\mathbb{K}[\boldsymbol{x},\boldsymbol{u}]$ を含む場合も C を別に扱うべきである。

定義 1 [**variables-connected な系**] 多項式 F_j と $F_{j'}$ $(j\neq j')$ がともに変数 x_i を含むとき、F_j と $F_{j'}$ は x_i-**connected** であるという。系 $\mathcal{F}$ において、変数 x_{i_1} と m 変数の連鎖 $(x_{i_1},x_{i_2},\ldots,x_{i_m})$, ただし $\{i_1,i_2,\ldots,i_m\}=\{1,2,\ldots,m\}$, が存在し、$1\leq i\leq m$ なる各 i に対して F_{j_i} と $F_{j_{i+1}}$, ただし $\{j_1,j_2,\ldots,j_m,j_{m+1}\}=\{1,2,\ldots,m,m+1\}$, が x_i-connected であるならば、$\mathcal{F}$ は $(x_1,\ldots,x_m)$-**connected** であるという。 □

定理 1 $\mathcal{F}=\{F_1,\ldots,F_{m+1}\}\subset\mathbb{K}[\boldsymbol{x},\boldsymbol{u}]$, $m\geq 2$, は $(\boldsymbol{x})$-connected な系であり、$F_1,F_2,\ldots,F_{m+1}$ は共通因子を含まないとする。$\mathcal{I}$ は $\mathcal{F}$ の元で生成されるイデアルとする。$\mathcal{F}$ では主変数 $\boldsymbol{x}$ が消去可能であり、$\mathcal{I}\cap\mathbb{K}[\boldsymbol{u}]$ は正確に n 変数の非零多項式を含むとする。このとき、消去順序 $\succ_{\rm el}$, $x_i\succ_{\rm el}u_j$ $(\forall i,j)$, に関する $\mathcal{I}$ の簡約グレブナー基底を $\mathrm{GB}(\mathcal{F})$ とすれば、$\mathrm{GB}(\mathcal{F})\cap\mathbb{K}[\boldsymbol{u}]=\{\widehat{S}\}$ が成立する。ここで、$\widehat{S}$ は $\mathrm{GB}(\mathcal{F})$ の順序最低の要素である $(u_1,\ldots,u_n$ の順序はなんでもよい$)$。 □

証明に先だって、イデアルと多様体に関して復習しておく。

本稿では係数体 $\mathbb{K}$ を標数 0 に限定したから、多項式の**零点** (zero) を考えることができる。多項式系 $\mathcal{F}$ の零点とは $(\boldsymbol{\zeta},\boldsymbol{\eta})\in\mathbb{C}^{m+n}$, $(\boldsymbol{\zeta})=(\zeta_1,\ldots,\zeta_m)$, $(\boldsymbol{\eta})=(\eta_1,\ldots,\eta_n)$ で、$F_1(\boldsymbol{\zeta},\boldsymbol{\eta})=\cdots=F_{m+1}(\boldsymbol{\zeta},\boldsymbol{\eta})=0$ を満たすものである。零点のうち $\boldsymbol{u}$ に関する部分 $(\boldsymbol{\eta})$ は**部分零点** (partial zero) と言われる。多項式系 $\mathcal{F}$ の零点全体の集合 (代数多様体；多重零点は 1 個と数える) を $\mathcal{V}(\mathcal{F})$ と表す。多項式イデアルと代数多様体とは深い関係があり、教科書 [7] に解り易く解説されている。本章では次の二つの定理を利用する。『**定理 A:** $\mathcal{V}(\mathcal{F})$ の任意の要素は、$\mathcal{I}(\mathcal{F})$ の全要素の共通零点である』。この定理のため、$\mathcal{V}(\mathcal{F})$ を $\mathcal{V}(\mathcal{I})$ とも表す。『**定理 B**(閉包定理)**:** $\mathcal{I}_m$ を $\mathcal{I}(\mathcal{F})$ の $\mathbb{K}[\boldsymbol{u}]$ への写像、$\mathcal{I}_m=\mathcal{I}(\mathcal{F})\cap\mathbb{K}[\boldsymbol{u}]$、とすれば、$\mathcal{V}(\mathcal{I}_m)$ は $\mathcal{V}(\mathcal{I})$ の $\mathbb{C}^n$ 空間への写像を含む最小の代数多様体である。ここで、「含まれない部分」とは次元が n 未満で、$\mathcal{F}$ の零点には対応しない点である』。たとえば、多項式 $G(x,\boldsymbol{u})$ と $H(x,\boldsymbol{u})$ の終結式では $\langle \mathrm{lc}(G),\mathrm{lc}(H)\rangle$ の代数多様体が「含まれない部分」にあたる。

定理 1 の証明 定理の仮定より、系 $\mathcal{F}$ から $\boldsymbol{x}$ を消去して $\boldsymbol{u}$ だけの多項式が得られるので、$\mathrm{GB}(\mathcal{F}) \cap \mathbb{K}[\boldsymbol{u}] = \{\widehat{S}_1, \widehat{S}_2, \dots\}$, $\widehat{S}_1 \prec_{\mathrm{el}} \widehat{S}_2 \prec_{\mathrm{el}} \cdots$, とする。($\boldsymbol{x}$)-connected の仮定から、$\mathrm{GB}(\mathcal{F})$ が複数個のグレブナー基底の要素の集合和である場合は除かれる。つぎに、$\widehat{R}(\boldsymbol{u})$ はその零点として、$\mathcal{F}$ の零点には対応しない部分零点を除き、$\mathcal{F}$ の $\boldsymbol{u}$ に関する部分零点のみを多重度込みで全て含む多項式とする。そのような多項式の存在は、グレブナー基底が多項式のみを要素とし零点の多重度を保つことから保証される。
さて、消去イデアルは元のイデアルの部分集合であり、$\widehat{R}$ は部分零点を全て多重度込みで含むからイデアルの要素であり、部分零点しか含まないから消去イデアルの中で最小で $\widehat{R} = \widehat{S}$ である。また、定理 A から上記の $\{\widehat{S}_1, \widehat{S}_2, \dots\}$ で $\widehat{S}_2, \dots$ は $\widehat{R}$ の倍数であることがわかる。一方、$\mathrm{GB}(\mathcal{F})$ は簡約基底ゆえ、定理が導かれる。 □

系 1 $G, H, H_1, H_2 \in \mathbb{K}[x, \boldsymbol{u}]$ は 0 でない多項式とし、$H = H_1 H_2$ を満たすとする。$\widehat{S}(\boldsymbol{u}), \widehat{S}_1(\boldsymbol{u}), \widehat{S}_2(\boldsymbol{u})$ はそれぞれ、$\langle G, H\rangle$, $\langle G, H_1\rangle$, $\langle G, H_2\rangle$ の消去順序 $x \succ_{\mathrm{el}} u_1, \dots, u_n$ に関する簡約グレブナー基底の最小元とする。すると、$\widehat{S} = \widehat{S}_1\, \widehat{S}_2$ が成立する。
証明 $\widehat{R}(\boldsymbol{u}), \widehat{R}_1(\boldsymbol{u}), \widehat{R}_2(\boldsymbol{u})$ はそれぞれ系 $\{G, H\}$, $\{G, H_1\}$, $\{G, H_2\}$ の部分零点のみを多重度込みで全て含む多項式とすれば、系は定理 1 と同様に証明される。 □

注釈 1 定理 1 は [15] における定理 1 の拡張である。系 1 は [15] における定理 2 の拡張だが、証明が簡単である。 □

例 1 [簡約グレブナー基底の例] F_1, F_2, F_3 を下記の多項式とする。

$$\left\{\begin{array}{rcl} F_1 &=& x^4{\cdot}(y{+}u) + x^2{\cdot}(y{-}2w) + (2u{+}w), \\ F_2 &=& x^4{\cdot}(y{-}u) + x^2{\cdot}(2y{+}u) + (u{-}2w), \\ F_3 &=& x^4{\cdot}(\,yu\,) + x^2{\cdot}(y{+}2w) + (3u{-}w). \end{array}\right. \tag{3.3}$$

イデアル $\langle F_1, F_2, F_3\rangle$ の辞書式順序 $x \succ y \succ u \succ w$ に関する簡約グレブナー基底を Mathematica で計算すると、以下の 10 個の多項式が基底要素として得られる。

$$\begin{array}{rcl} G_1 &=& 407263383039911893119888740176\, x^4u + \cdots + 407263383039911893119888740176\, w, \\ G_2 &=& 162905353215964757247955496 0704\, x^4w + \cdots + 8145267660798237862397774803 52\, w, \\ &\vdots& \qquad\qquad\qquad\qquad\qquad \vdots \\ G_7 &=& 176158230110199363956632\, y^2w + \cdots + +10389388546346356009197680\, w^3, \\ G_9 &=& 48000\, yw^8 - 419640\, yw^7 - 769740\, yw^6 + \cdots + 18224352\, w^4 - 5430496\, w^3, \\ G_{10} &=& 33\, u^7 + 23\, u^6w - 126\, u^6 - 55\, u^5w^2 - 343\, u^5w + 316\, u^5 - 12\, u^4w^3 \\ &-& 130\, u^4w^2 + 544\, u^4w - 202\, u^4 + 32\, u^3w^4 + 218\, u^3w^3 + 548\, u^3w^2 - 128\, u^3w \\ &-& 144\, u^2w^4 + 428\, u^2w^3 - 420\, u^2w^2 + 144\, uw^4 - 256\, uw^3 - 32\, w^4. \end{array}$$

G_{10} が $\widehat{S}$ に対応する。$G_1, G_2, G_3, \dots, G_9, G_{10}$ の項数は $61, 62, 61, 58, 58, 57, 54, 58, 61, 20$ である。G_{10} は簡単だが多数の大きな多項式を経由して得られた。G_{10} の簡単さを見れば、グレブナー基底を経ずに $\widehat{S}$ を計算したくなるのは人情であろう。 □

4　剰余列による主変数の消去

本章では剰余列による主変数の消去を考察する。3 個以上の多項式系で $\widehat{S}$ を計算するには、2 多項式系の場合とは異なる困難を乗り越える必要があることが解るだろう。

定義 2 [Elim$(F_i, F_j; x_\ell)$, successful な消去, regular な消去]
ℓ 番以降の主変数の組を $(\boldsymbol{x}_\ell) = (x_\ell, , \ldots, x_m)$ とし、F_i と F_j は $\mathbb{K}[\boldsymbol{x}_\ell, \boldsymbol{u}]$ の多項式とする。x_ℓ が F_i と F_j の主変数のとき、F_i と F_j から x_ℓ に関する剰余列を計算して x_ℓ を消去する。剰余列最後の非零要素 P_k が x_ℓ を含まないとき**消去は successful** という。消去が successful なとき、余因子 A_k, B_k から P_k を $G := P_k/\gcd(\mathrm{cont}(A_k), \mathrm{cont}(B_k))$ と規格化することを含め、消去全体を $G := \mathrm{Elim}(F_i, F_j; x_\ell)$ と表す。P_k が $x_{\ell+1}$ を含む (resp. 含まない) とき、**消去は regular** (resp. **irregular**) という。 □

4.1　主変数消去のアウトライン

筆者らは、$\widehat{S}$ の計算を二つの段階で行う。(第二段階はまだ未完成である)。
　第一段階：主変数を消去し、一般に複数個の多項式 $\subset \mathbb{K}[\boldsymbol{u}]$ を生成する、
　第二段階：第一段階で得られた多項式たちから $\widehat{S}(\boldsymbol{u})$ を計算する。
第一段階は、概略、次のように実行される。

主変数と多項式の並べ替え： 定義 1 で m 個の変数の連鎖 $(x_{i_1}, x_{i_1}, \ldots, x_{i_m})$ を導入したが、この連鎖が $(x_1, x_2, \ldots, x_m)$ となるよう主変数を並べ替え、各変数 x_i $(1 \le i \le m)$ が F_i と F_{i+1} を結ぶように $m+1$ 個の多項式を並べ替える。これらにより、主変数に辞書式順序が設定される。

主変数の消去： 次に、主変数を $x_1 \to x_2 \to \cdots \to x_m$ と順に消去する (詳細は次項で)。なお次項では、変数 $x_1, \ldots, x_{i-1}$ を消去した直後の多項式には $\widetilde{F}_i, \widetilde{F}_{i+1}, \ldots$ のように $\widetilde{}$ をつけて区別する。

三つの場合： 主変数 x_i の消去は、次の三つの場合に分類できる。
場合-1) 主変数 x_i が j (≥ 2) 個の多項式 $\widetilde{F}_{i,1}, \ldots, \widetilde{F}_{i,j}$ に含まれ、かつ j 個の消去 $\mathrm{Elim}(\widetilde{F}_{i,1}, \widetilde{F}_{i,2}; x_i)$, $\mathrm{Elim}(\widetilde{F}_{i,2}, \widetilde{F}_{i,3}; x_i)$, $\ldots$, $\mathrm{Elim}(\widetilde{F}_{i,j}, \widetilde{F}_{i,1}; x_i)$ がすべて successful で regular な場合。これらすべての消去を実行する。
場合-2) $\mathrm{Elim}(\widetilde{F}_i, \widetilde{F}_{j>i}; x_i)$ が unsuccessful な場合。
この場合は剰余列の最終要素 P_k は x_i を含み、$\widetilde{F}_i$ と $\widetilde{F}_j$ は共通因子 $G := \gcd(\widetilde{F}_i, \widetilde{F}_j)$ を持つので、$\widetilde{F}'_i := \widetilde{F}_i/G$, $\widetilde{F}'_j := \widetilde{F}_j/G$ 計算し、系 $\{F_i, F_j\}$ を三つの系 $\{G, \widetilde{F}'_1\}$, $\{G, \widetilde{F}'_2\}$, $\{\widetilde{F}'_1, \widetilde{F}'_2\}$ に分けて、変数消去を続行する。
場合-3) $\mathrm{Elim}(\widetilde{F}_i, \widetilde{F}_{j>i}; x_i)$ が irregular な場合。
この場合は稀にしか起きないが、変数 x_i の消去後に変数 x_{i+1} を含む多項式の個数が 1 個または 0 個になる事態も起こり得る。いずれの事態でも、変数 x_{i+1} の主変数

間での順序を下げて、可能な限り主変数の消去を実行する。その過程で主変数全体の消去が行き詰まる場合も生じ得るが、それは主定理 1 に設定した仮定「主変数が全て消去できる」が満たされない場合である。

上記の方法の特徴は**場合-1)** である。変数の三角化法と比較すると、上記の方法は余計に剰余列を計算しているが、このことが $\widehat{S}$ の計算には非常に重要なのである。

定理 2 $\mathcal{F} = \{F_1, \ldots, F_{m+1}\} \subset \mathbb{K}[\boldsymbol{x}, \boldsymbol{u}]$ は定理 1 と同じ条件を満たすとし、$H(\boldsymbol{u})$ は $\mathcal{F}$ の主変数を全て消去して得られた任意の多項式とすれば、$H(\boldsymbol{u})$ は $\widehat{S}$ の定数倍である。

証明 定理 1 から直ちに得られる。 □

定理 2 は簡単だが、主変数の消去で $\boldsymbol{u}$ の複数個の多項式が得られるならば、非常に強力である。このことを $\mathcal{F}_3 = \{F_1, F_2, F_3\} \subset \mathbb{K}[x, y, \boldsymbol{u}]$ の系で具体的に見よう；ここで、x, y が主変数である。下記の例では、x と y を順に消去し、下記のように $\{G_1, G_2, G_3\} \subset \mathbb{K}[y, \boldsymbol{u}]$ と $\{H_1, H_2, H_3\} \subset \mathbb{K}[\boldsymbol{u}]$ を計算する。

$$\left\{ \begin{array}{lcl} (G_1, G_2, G_3) & := & (\,\mathrm{Elim}(F_1, F_2; x),\ \mathrm{Elim}(F_2, F_3; x),\ \mathrm{Elim}(F_3, F_1; x)), \\ (H_1, H_2, H_3) & := & (\,\mathrm{Elim}(G_1, G_2; y),\ \mathrm{Elim}(G_2, G_3; y),\ \mathrm{Elim}(G_3, G_1; y)). \end{array} \right. \tag{4.4}$$

例 2 [主変数の消去] 例 1 で与えた系で行う。
上記 (4.4) で定めた (G_1, G_2, G_3) と (H_1, H_2, H_3) は下記となる。

$$\begin{aligned} G_1 &= 3\,y^3u + 4\,y^3w + 15\,y^2u^2 + \cdots - 9\,u^2w^2 + 8\,uw^3, \\ G_2 &= 18\,y^2u^3 + 24\,y^2u^2w - 36\,y^2u^2 + \cdots + 64\,uw^2 + 32\,w^3, \\ G_3 &= -9\,y^2u^3 - 12\,y^2u^2w + 36\,y^2u^2 + \cdots + 20\,uw^2 - 32\,w^3. \end{aligned}$$

$$\begin{aligned} H_1 &= 661320\,u^{17} + 3750360\,u^{16}w + \cdots + 9216000\,uw^{10} + 663552\,w^{11}, \\ H_2 &= 2076\,u^{16} - 20412\,u^{15}w - \cdots - 32768\,uw^8 - 16384\,uw^7 + 4096\,w^8, \\ H_3 &= -40788\,u^{17} - 156864\,u^{16}w + \cdots + 172032\,uw^{10} + 262144\,w^{11}, \end{aligned}$$

参考までに、H_1, H_2, H_3 の項数はそれぞれ $98, 112, 98$ である。
定理 2 に基づき H_1, H_2, H_3 の最大公約子を計算すると、$\gcd(H_1, H_2) = \gcd(H_2, H_3) = \gcd(H_3, H_1) = G_{10}$ となる**:** G_{10} は例 1 で与えた多項式で、$\widehat{S}$ そのものである。
参考までに、$\widetilde{H}_i := H_i/\widehat{S}$ $(i = 1, 2, 3)$ を示す。

$$\begin{aligned} \widetilde{H}_1 &= 11\,u^{12} - 139\,u^{11}w - 388\,u^{11} + \cdots + 10848\,uw^8 - 1024\,w^9, \\ \widetilde{H}_2 &= -11583\,u^{13} + 17577\,u^{12}w + \cdots + 2720\,uw^8 - 208\,w^9, \\ \widetilde{H}_3 &= 704\,u^{12} + 1664\,u^{11}w - 3568\,u^{11} + \cdots + 23744\,uw^8 + 6448\,w^9. \end{aligned}$$

$\widetilde{H}_1, \widetilde{H}_2, \widetilde{H}_3$ は項数がそれぞれ $40, 50, 40$ の多項式で、G_{10} よりもかなり大きい。このことは、通常の方法では $\widehat{S}$ を計算するのが容易でないことを示している。 □

注釈 2 [三角化との違い] 多項式系 $\mathcal{F}$ の三角化は、たとえば変数 x_1 の消去では一つの多項式で他の全ての多項式の x_1 を消去する、すなわち $\mathrm{Elim}(F_1, F_j; x_1)$, $2 \leq \forall j \leq m{+}1$、を実行する。その結果、全ての主変数を消去したあとには、$\boldsymbol{u}$ の多項式が一つだけ残る。例 2 では $\{F_1(x,y,u), G_1(y,u), H_3(u)\}$ が $\mathcal{F}$ の三角系である。消去法には少しの違いしか見えないが、結果には大きな違いがある。 □

5 “余計な因子” とその除去法

前章の例 2 では、幸いにして $\widehat{S}(\boldsymbol{u})$ を剰余列計算と GCD 演算で計算することができた。しかし、一般には $\widehat{S}(\boldsymbol{u})$ を簡単には計算できない。多くの場合、次に述べる “余計な因子” が出現するからである。

定義 3 [余計な因子] 与えられた系 $\mathcal{F} = \{F_1, \ldots, f_{m+1}\} \subset \mathbb{K}[\boldsymbol{x}, \boldsymbol{u}]$ から、Elim 演算で主変数を消去して多項式 $H_1, \ldots, H_l \in \mathbb{K}[\boldsymbol{u}]$ を得たとして、$H = \gcd(H_1, \ldots, H_l)$ とする。H が $\widehat{S}$ の定数倍ではなく $H = \widetilde{H}\widehat{S}$ であるとき、$\widetilde{H}$ を H の**余計な因子**という。 □

本章では、第 5.1 節で $\widehat{S}$ が剰余列だけで (GCD 演算なしで) 決定できる最も簡単な場合を記述する。第 5.2 節では余計な因子の典型的な出現例を与え、出現のメカニズムを解明する。第 5.3 節では、前節で述べた典型的な余計因子の除去法を述べる。

5.1 最も簡単な場合

“最も簡単な場合” とはどんな場合かは、次の定理で記述する。

定理 3 本定理で扱う系 $\mathcal{F} = \{F_1, \ldots, F_{m+1}\}$ では、各変数 x_i $(i \in \{1, 2, \ldots, m\})$ が $\{???, F_i, F_{i+1}\}$ にだけ含まれるとする。ここで、“???” は F_j $(j < i)$ を含んでも含まなくてもよい。もしも $G_{i+1} = \mathrm{Elim}(G_i, F_{i+1}; x_i)$、ただし $G_1 = F_1$、が各 $i \in \{1, 2, \ldots, m\}$ に対して successful で regular ならば、G_{m+1} は $\widehat{S}$ の定数倍である。

証明 主変数の消去は $G_2 := \mathrm{Elim}(F_1, F_2; x_1)$ から始まる。仮定より、$G_2 \neq 0$ で G_2 は x_2 を含み、G_2 は $\langle F_1, F_2\rangle \cap \mathbb{K}[x_2, \ldots, x_m, \boldsymbol{u}]$ の順序最低の元 (の定数倍) であることがわかる。$\mathcal{I} = \langle\mathcal{F}\rangle$、$\mathcal{I}' = \langle G_2, F_3, \ldots, F_{m+1}\rangle$ とすれば、$\mathcal{I}' \subset \mathcal{I}$ なので $G_2 \prec_{\mathrm{el}} \widehat{S}$ はありえない。同様に、任意の $i \in \{2, \ldots, m\}$ に対し、$G_{i+1} := \mathrm{Elim}(G_i, F_{i+1}; x_i)$ はイデアル $\langle G_i, F_{i+1}, \ldots, F_{m+1}\rangle$ の最低順序の元であり、G_{m+1} が $\widehat{S}$ の定数倍であることがわかる。 □

例 3 [最も簡単な場合] F_1, F_2, F_3 を下記の多項式とする。

$$\left\{\begin{array}{rcl} F_1 &=& x^4{\cdot}(y{+}u) + x^2{\cdot}(y{-}2w) + (2u{+}w), \\ F_2 &=& x^4{\cdot}(y{-}u) + x^2{\cdot}(2y{+}u) + (u{-}2w), \\ F_3 &=& \big(y{\cdot}(3u{+}2w) + (u{-}2w)\big) \times \big(y{\cdot}(3u{+}2w) - (u{-}2w)\big). \end{array}\right. \tag{5.5}$$

主変数 x の消去は $G_2 := \mathrm{Elim}(F_1, F_2; x)$ だけで、y の消去は $H_3 := \mathrm{Elim}(G_2, F_3; y)$ だけで、下記となる。

$$\begin{aligned} G_2 &= y^3{\cdot}(3u{+}4w) + y^2{\cdot}(15u^2 + 31uw + 13w^2) \\ &+ y{\cdot}(5u^3 - 2u^2w - 12uw^2 - 8w^3) + 11u^4 - 7u^3w - 9u^2w^2 + 8uw^3, \\ H_3 &= (\,297u^7 + 405u^6w + 45u^6 - 225u^5w^2 - (18\text{ terms}) + 104w^5 - 32w^4) \\ &\times (\,297u^7 + 405u^6w - 45u^6 - 225u^5w^2 + (18\text{ terms}) + 104w^5 + 32w^4) \end{aligned}$$

G_2 も H_3 も原始的 (係因数が 1) で余計因子を持たず、$H_3 = \widehat{S}$ である。なお、H_3 の因数分解は系 1 による。 □

5.2 余計因子の現れ方

本節では余計因子が発生する典型的な例題を示し、剰余列法は本質的に余計因子を発生させる算法であることを指摘する。

例 4 [余計因子の発生] $\mathcal{F} = \{F_1, F_2, F_3\}$ を下記多項式で与える。

$$\left\{ \begin{array}{lcl} F_1 &=& x^4{\cdot}(y{+}u) + x^2{\cdot}(y{-}2u) + (2y{-}u), \\ F_2 &=& x^4{\cdot}(y{-}u) + x^2{\cdot}(2y{+}u) + (y{-}2u), \\ F_3 &=& x^4{\cdot}(\,yu\,) + x^2{\cdot}(y{+}u) + (y{-}u). \end{array} \right. \tag{5.6}$$

今の例では H_1, H_2, H_3 は次の多項式となる。

$$\begin{aligned} H_1 = {} & -54\,u^7{\times}(u+2){\times}(63\,u^3 + 62\,u^2 - 156\,u + 72){\times}(7\,u^3 - 208\,u^2 + 100\,u - 16), \\ H_2 = {} & 2\,u^7{\times}(u+2){\times}(63\,u^3 + 62\,u^2 - 156\,u + 72){\times}(9u+8){\times}(1183\,u^3 - \cdots + 736), \\ H_3 = {} & u^7{\times}(u+2){\times}(63\,u^3 + 62\,u^2 - 156\,u + 72) \\ & {\times}(207\,u^8 - 53\,u^7 - 2079\,u^6 + 406\,u^5 + \cdots - 2544\,u^2 - 32\,u + 512), \end{aligned}$$

これらより、$\gcd(H_1, H_2, H_3) = u^7{\times}(u+2){\times}(63\,u^3 + 62\,u^2 - 156\,u + 72)$ を得る。一方、上記の系のグレブナー基底からは $\widehat{S} = u{\times}(u+2){\times}(63\,u^3 + 62\,u^2 - 156\,u + 72)$ が得られ、u^6 が余計な因子であることが分かる。注意すべきは因子 u^7 のうち u だけ余計因子でないことである。これはどう判定すればいいのだろうか？ □

上記の例 4 では、入力多項式の x の係数項の多くが y と u の同次式であることに気付く。そのため、主変数 x を消去後の各多項式 $G_i := \mathrm{Elim}(F_{j_1}, F_{j_2}; x)$ は y と u のほぼ同次式となり、主変数 y の消去時に剰余列算法では除去しきれないほどに $H_i := \mathrm{Elim}(G_{j_1}, G_{j_2}; x)$ が u を因子として含むことになる。例 4 は、x の各係数が一つを除き全て y と u の同次式なので極端であるが、そうでなくても、入力多項式の主変数に関する項の指数が不揃いの場合などにも消去後の式に余計因子が現れることがある。すなわち、(疎) 擬除算に基ずく (疎) 剰余列計算では、たとえ主係数からくる係因数を (部分終結式あるいは類似の理論に基づく) 算法で除去しても、除去しきれない因子が余計因子として残る場合がある。

5.3 余因子による余計因子の除去法

2 多項式系 $\{G, H\} \subset \mathbb{K}[x, \boldsymbol{u}]$ でも剰余列の最終要素 P_k は余計因子を含む場合が多いが、第 2 章の式 (2.2) が示すように、余因子を使って除去可能である。そこで、本節では多・多項式系の余因子を使って余計因子の除去を試みる。

余因子の算式は 2 章の式 (2.1) の下に記したが、それが示すように余因子は Elim 演算毎に計算履歴に無関係に計算される。多項式系 $\mathcal{F}$ では Elim 演算は m 回連続し、各々の消去で得られた余因子を連結する必要がある。簡単のため式 (4.4) で与えた (G_1, G_2, G_3) と (H_1, H_2, H_3) で説明しよう。たとえば $G_1 = \mathrm{Elim}(F_1, F_2; x)$ に対しては $G_1 = A_{1,1}F_1 + A_{1,2}F_2$ を満たす $A_{1,1}$ と $A_{1,2}$ が計算されるが、初期多項式が 3 個あるのでこれを $G_1 = A_{1,1}F_1 + A_{1,2}F_2 + A_{1,3}F_3$、ただし $A_{1,3} = 0$、と表す。すると、各 G_i と各 H_i に対して次式を満たす 6 組の余因子が計算される。

$$\begin{cases} G_i = A_{i,1}F_1 + A_{i,2}F_2 + A_{i,3}F_3, & (i = 1, 2, 3), \\ H_i = B_{i,1}G_1 + B_{i,2}G_2 + B_{i,3}G_3, & (i = 1, 2, 3). \end{cases} \tag{5.7}$$

我々が欲しいのは、各 H_i を F_1, F_2, F_3 で次式のように表す余因子 $C_{i,1}, C_{i.2}, C_{i,3}$ である:

$$H_i = C_{i,1}F_1 + C_{i,2}F_2 + C_{i,3}F_3, \quad (i = 1, 2, 3). \tag{5.8}$$

式 (5.7) の余因子たちから $C_{i,j}$ を計算するのは容易である。

実際に計算すると分かるが、余因子 $A_{i,j}$ と $B_{i,j}$ は主変数と従変数の多項式で、それぞれ G_i と H_i より大きな多項式になる場合がほとんどである。しかも、例 4 の場合、H_1, H_2, H_3 が因子 u^7 を持つのに、余因子 $A_{i,j}$ と $B_{i,j}$ は因子として u さえ持たない。しかしながら、非常に幸いなことに、われわれが実際に必要なのは $A_{i,j}$ と $B_{i,j}$ そのものではなく、これらの余因子で主変数を 0 としたもので十分なことである。したがって、$C_{i,j}$ は具体的に計算する必要はなく、$a_{i,j} := A_{i,j}|_{x=y=0}$、$b_{i,j} := B_{i,j}|_{x=y=0}$ から $c_{i,j} := C_{i,j}|_{x=y=0}$ を計算しさえすればよい。これらのことを具体例でみよう。

例 5 [余計因子の除去] 例 4 の F_1, F_2, F_3 で余計因子の除去を試みよう。
上で定義した $c_{i,j} \in \mathbb{Q}[u]$ のうち、$i = 1$ だけを示す。

$$\begin{cases} c_{1,1} = & -383292\,u^{14} - 1192896\,u^{13} + \cdots + 1718144\,u^7 + 39936\,u^6, \\ c_{1,2} = & -479115\,u^{14} - 1491120\,u^{13} - \cdots - 680896\,u^7 - 867840\,u^6, \\ c_{1,3} = & 0. \end{cases} \tag{5.9}$$

$c_{2,j}$ と $c_{3,j}$ $(j = 1, 2, 3)$ も u^6 を因子として持つ。H_1, H_2, H_3 が u だけの多項式なので、$f_j := F_j|_{x=y=0}$ $(j = 1, 2, 3)$ とする: $f_1 = -u$, $f_2 = -2u$, $f_3 = -u$。このとき、$H_i = c_{i,1}f_1 + c_{i,2}f_2 + c_{i,3}f_3$ が成立する。各 $i \in \{1, 2, 3\}$ に対し、$c_{i,j}$ は u^6 で割り切れるが $(u{+}2)$ では割り切れないので、u^6 は余計な因子だが $(u{+}2)$ は余計な因子ではなさそうだ。実際、そのことは下記の補題で保証される。 □

補題に先だち、記号と重要な多項式を定義しておく。例5の中では主変数$\boldsymbol{x}$を消去して得られる多項式を$H_i(\boldsymbol{u})$とし、その余因子を$C_{i,j}$としたが、その記号は$m>2$でもそのまま使用する；ただし、i=1,...,lとする。そして、次の二つの多項式を定義する。

$$H_i = c_{i,1}f_1 + c_{i,1}f_2 + \cdots + c_{i,m+1}f_{m+1}, \tag{5.10}$$

$$\overline{H}_i = c_{i,1}F_1 + c_{i,2}F_2 + \cdots + c_{i,m+1}F_{m+1}. \tag{5.11}$$

$\boldsymbol{f} = (F_1,\ldots,F_{m+1})|_{\boldsymbol{x}=\boldsymbol{0}}$、$\boldsymbol{c}_i = (C_{i,1},\ldots,C_{i,m+1})|_{\boldsymbol{x}=\boldsymbol{0}}$と表す。$F_1,\ldots,F_{m+1}$は仮定より共通因子を持たないが、$f_1,\ldots,f_{m+1}$は持ち得ることに注意(例4,5がそうである)。$H_i$が余計因子$\widetilde{H}$を持てば、式(5.10)の右辺全体が$\widetilde{H}$を因子として持ち、大抵の場合は個々の$\boldsymbol{u}$-余因子$c_{i,j}$が$\widetilde{H}$で割り切れる必要がある。

補題1 系$\{F_1,\ldots,F_{m+1}\}\in\mathbb{K}[\boldsymbol{x},\boldsymbol{u}]$の主変数を消去して、$H_i(\boldsymbol{u})\in\mathbb{K}[\boldsymbol{u}]$ ($i\in\{1,\ldots,l\}$)と余因子たち$C_{i,1},\ldots,C_{i,m+1}\in\mathbb{K}[\boldsymbol{x},\boldsymbol{u}]$を得たとし、$c_{i,j}:=C_{i,j}|_{\boldsymbol{x}=\boldsymbol{0}}$ ($j\in\{1,\ldots,m+1\}$)とする。$H:=\gcd(H_1,\ldots,H_l)$とし、$\widetilde{H}$はHの真の因子とする。もしも各$i\in\{1,\ldots,l\}$に対して$\boldsymbol{c}_i$が$\widetilde{H}$の倍数ならば$\widetilde{H}$はHの余計因子である。ただし、上式で$\boldsymbol{f}$が$\widetilde{H}$で割り切れる場合は$\boldsymbol{f}$を$\boldsymbol{f}/\widetilde{H}$で置き換える。

証明 各iに対して$H_i = C_{i,1}F_1+\cdots+C_{i,m+1}F_{m+1}$であり、これを$\mathbb{K}[\boldsymbol{u}]$空間に射影したものが式(5.10)である。各$c_{i,j}$を$\widetilde{H}$で割り、$c_{i,j}=c'_{i,j}\widetilde{H}+r_{i,j}$とする；$r_{i,j}$は剰余である。もしも各$(i,j)$に対して$r_{i,j}=0$ならば、各$H_i$は$\widetilde{H}$で割り切れるが、$H_i/\widetilde{H}$がイデアル$\mathcal{I}(\mathcal{F})$の要素であるとは限らない。一方、式(5.11)の$\overline{H}_i$はイデアルの要素であり、補題の条件が満たされれば$\overline{H}_i/\widetilde{H}=c'_{i,1}F_1+\cdots+c'_{i,m+1}F_{i,m+1}$なので、$\widetilde{H}$が余計因子であることが解る。(なお、$r_{i,j}\neq 0$であっても$r_{i,1}f_1+\cdots+r_{i,m+1}f_{m+1}\equiv 0 \pmod{\widetilde{H}}$であれば$H_i$は$\widetilde{H}$で割り切れるが、(5.11)の右辺が割り切れることは稀である。この辺りのことはまだ解明していない。) □

定理4 系$\mathcal{F}=\{F_1,\ldots,F_{m+1}\}$の主変数を剰余列法で消去して得られた$H_1,\ldots,H_l\in\mathbb{K}[\boldsymbol{u}]$と各$H_i$ ($i\in\{1,\ldots,l\}$)に対する余因子、および$H:=\gcd(H_1,\ldots,H_l)$の既約因数分解から、GB($\mathcal{F}$)の項順序$\succ_{\rm el}$に関する最低元$\widehat{S}$を計算することができる。

証明 Hの異なる因子各々を$\widetilde{H}$だとして、補題1を順に適用すればよい。 □

参 考 文 献

[1] W.S. Brown: On Euclid's algorithm and the computation of polynomial greatest common divisors. JACM **18**(4), 478-504 (1971).

[2] W.S. Brown and J.F. Traub: On Euclid's algorithm and the theory of subresultants. JACM **18**(4), 505-515 (1971).

[3] W.S. Brown: The subresultant PRS algorithm. ACM TOMS **4**, 237-249 (1978).

[4] B. Buchberger: Gröbner bases: an algorithmic methods in polynomial ideal theory. in *Multidimensional Systems Theory*, Chap. 6. Reidel Publishing, 1985.

[5] G.E. Collins: Polynomial remainder sequences and determinants. Amer. Math. Monthly **71**, 708-712, 1966.

[6] G.E.Collins: Subresultants and reduced polynomial remainder sequences. JACM **14** 128-142 (1967).

[7] D. Cox, J. Little, D. O'Shea: *Ideals, Varieties, and Algorithms – An Introduction to Computational Algebraic Geometry and Commutative Algebra*, Second Edition, Chaps. 3 and 4, Springer-Verlag, 1997.

[8] L. Ducos: Optimizations of the subresultant algorithm. J. Pure Appl. Algebra **145**, 149-163, 2000.

[9] A.C. Hearn: Non modular computation of polynomial GCD using trial division. *Proceedings EUROSAM'79* (Springer LNCS **72**), 227-239 (1979).

[10] R. Loos: Generalized Polynomial Remainder Sequence. in *Computer Algebra (Computing Supplementum 4)*, 115-137, Springer-Verlag (1982).

[11] T. Sasaki: A subresultant-like Theory for Buchberger's procedure. JJIAM (Jap. J. Indust. Appl. Math.) **31**, 137-164, 2014.

[12] T. Sasaki: A theory and algorithm for computing sparse multivariate polynomial remainder sequence. preprint of Univ. Tsukuba, 14 pages (2018), submitted.

[13] T. Sasaki and D. Inaba: Hensel construction of $F(x, u_1, \ldots, u_\ell)$, $\ell \geq 2$, at a singular point and its applications. *ACM SIGSAM Bulletin*, **34**(1), 9-17 (2000).

[14] T. Sasaki and D. Inaba: Enhancing the extended Hensel construction by using Gröbner bases. *Proceedings of CASC2016 (Computer Algebra in Scientific Computing)*, Springer LNCS 9890, 457-472 (2016).

[15] T. Sasaki and D. Inaba: Various enhancements of extended Hensel construction for sparse multivariate polynomials. *Proceedings of SYNASC2016 (Symbolic and Numeric Algorithms for Scientific Computing)*, IEEE Computer Society, 83-86 (2017).

[16] T. Sasaki and D. Inaba: Simple relation between the lowest-order element of ideal $\langle G, H \rangle$ and the last element of polynomial remainder sequence. *Proceedings of SYNASC2017 (Symbolic and Numeric Algorithms for Scientific Computing)*, IEEE Computer Society, 2018 (in printing).

[17] D. Wang: On the connection between Ritt characteristic sets and Buchberger-Gröbner bases. Math. Comp. Sci., **10** (4), 479–492 (Dec. 2016).