ＴＥＳ (Term Elimination Sequence) について

On TES (Term Elimination Sequence)

筑波大学・数理物質系 名誉教授　　佐々木 建昭 *1

Tateaki Sasaki

Professor emeritus, University of Tsukuba

Abstract

In computer algebra, two kinds of polynomial representations are used. One is the recursive representation and another is the monomial representation; see Sect. 1 for details. The resultants were developed on the recursive representation, and the Gröbner bases are computed with the monomial representation. The key operation in Gröbner basis theory is the $\mathrm{Spol}(G,H)$ which is defined by canceling the leading-monomials of G and H by multiplying the lowest-order monomials to them respectively. Similarly, we can define "TrmElim(G,H)", Elim(G,H) in short, to be an operation which cancels the leading-terms of G and H by multiplying the lowest-order terms to them respectively. Both the $\mathrm{Spol}(G,H)$ and the $\mathrm{Elim}(G,H)$ are "critical-pair"s of Knuth-Bendix. In this paper, we study the Elim operation for $G,H\in\mathbb{K}[x,\boldsymbol{u}]$, where $(\boldsymbol{u})=(u_1,\ldots,u_n)$, with $x\succ u_1,\ldots,u_n$. The TES is a degree-decreasing sequence of Elim operations for relatively prime G and H, s.t. $\deg_x(G)\geq\deg_x(H)$, i.e., $(P_1:=G,\ P_2:=H,\ P_3:=\mathrm{Elim}(G,H),\ \ldots,\ P_k:=\mathrm{Elim}(P_{k-2},P_{k-1}))$, where $P_k\in\mathbb{K}[\boldsymbol{u}]$. Similarly, we can decrease the x-degree by computing an S-polynomial set, SpS in short. Let $\mathrm{Sylv}(G,H)$ denote Sylvester's determinant. We note that most multivariate resultants contain "extraneous factors". We can understand the TES by comparing $\mathrm{Sylv}(G,H)$ with resultants by the TES and the SpS. The $\mathrm{Sylv}(G,H)$ mostly gives us resultants of large extraneous factors if G and H are sparse. The TES and SpS, with no extraneous-factor removal, will give us resultants with much smaller extraneous factors ($\Rightarrow$ Theorem 2 in **3.3**), but they seldom give us $\widehat{S}_2$, the lowest order polynomial in $\langle\{G,H\}\rangle\cap\mathbb{K}[\boldsymbol{u}]$. In order to obtain the $\widehat{S}_2$, we must do as follows: suppose we obtained a resultant P_k by TES or SpS. Then, we compute $\mathrm{Elim}(E,P_k)$ or $\mathrm{Spol}(E,P_k)$ for each element E of TES or SpS. We show a wonderful theory of extraneous-factor removal for TES ($\Rightarrow$ Theorem 3 in **3.3**).

(*Important parts of the text, such as theorems, are written in English.*)

1 Introduction

最初に多変数多項式の**再帰表現** (recursive representation) と**単項式表現** (monomial representation) を定義し述語を定める。G と H は変数 $(\boldsymbol{x})=(x_1,\ldots,x_m)$ の数体 $\mathbb{K}$ 上の多項式とし，それらの x_1 に関する次数をそれぞれ d と e とする $(d\geq e)$。$(\boldsymbol{x}')=(x_2,..,x_m)$ とすれば，G と H は下記のように表せる。

$$G=g_d(\boldsymbol{x}')x_1^d+g_{d-1}(\boldsymbol{x}')x_1^{d-1}+\cdots+g_0(\boldsymbol{x}')x_1^0,\quad H=h_e(\boldsymbol{x}')x_1^e+h_{e-1}(\boldsymbol{x}')x_1^{e-1}+\cdots+h_0(\boldsymbol{x}')x_1^0. \tag{1}$$

ここで，係数多項式 $g_i(\boldsymbol{x}')$ や $h_j(\boldsymbol{x}')$ はさらに変数 $\boldsymbol{x}'$ に関して再帰的に表現する。これが再帰表現である。一方，単項式表現では多項式 G や H を単項式の和として表現する。ここで，単項式は数係数を除き一意的に順序づけられるとする。そのような順序は多々あるが，変数消去の観点からグレブナー基底計算を論じるため，本稿では**辞書式順序** (lexicographic order; LEX 順序と略記) のみを扱う [5, 6]。

$$\begin{aligned}&G=M_1+M_2+\cdots+M_k,\quad M_1\succ M_2\succ\cdots\succ M_k,\ \text{where}\\&\quad M_i=c_ix_1^{e_{i,1}}x_2^{e_{i,2}}\cdots x_m^{e_{i,m}},\quad c_i\in\mathbb{K},\ e_{i,l}\in\mathbb{N}\cup\{0\},\quad M_i\succ M_{j(>i)}\iff\\&\quad\text{either } [e_{i,1}>e_{j,1}] \text{ or } \exists l>1 \text{ s.t. } [e_{i,1}=e_{j,1},\cdots,e_{i,l-1}=e_{j,l-1},\ e_{i,l}>e_{j,l}].\end{aligned} \tag{2}$$

*1 〒 305-8571 茨城県つくば市天王台 1-1-1　E-mail: sasaki@math.tsukuba.ac.jp

上式 (1) と (2) において，$g_d(\boldsymbol{x}')x_1^d$ と M_1 をそれぞれ G の**主項**及び**主単項**と呼び，それぞれ $\mathrm{ltm}(G)$ 及び $\mathrm{lmn}(G)$ と表す。また，$g_d(\boldsymbol{x}')$ と c_1 を**主係数**と呼び，それぞれ $\mathrm{lcf}(G)$ 及び $\mathrm{lc}(G)$ と表す。G から主項と主単項を除いた残りの多項式をそれぞれ**残余項**および**残余単項**と呼び，$\mathrm{rest}(G)$ 及び $\mathrm{rst}(G)$ と表す。G の x^0-次項を**定数項**と呼び，$\mathrm{ctm}(G)$ と表す。

グレブナー基底を計算する際の基本演算は**S多項式**生成である；**M簡約**[1] はS多項式の特殊な場合なので，S多項式に含める。多項式 G と H を単項式表現したとき，$\mathrm{Spol}(G,H)$ は次式で定義される [6]。

$$\mathrm{Spol}(G,H) := [\mathrm{lmn}(H)/C]\cdot G - [\mathrm{lmn}(G)/C]\cdot H, \quad C := \gcd(\mathrm{lmn}(G), \mathrm{lmn}(H)). \tag{3}$$

数式に限らず例えば論理式の集合が与えられた場合，各論理式のみならず，それぞれの基本単位も含めて “項” と呼び，与集合を次々に変形して目的の集合に到達する体系的手法を “項書き換えシステム” と言う。項書き換え算法の中で際立っているのが Knuth-Bendix の “完備化手順 (completion procedure)” である。ここで，完備化された集合とはグレブナー基底のようなものである。この手順の基本演算は，項集合の任意の二つの項 T_1 と T_2 に対し，それらの先頭項 H_1 と H_2 とをキャンセルさせるに足る最低位の項 t_1 と t_2 をそれぞれ T_1 と T_2 に掛けて，新しい項 $T_3 := t_1\times T_1 - t_2\times T_2$ を生成し，T_3 が 0 でなければそれを項集合に付加することである。T_3 は正にS多項式に対応し，また，T_1 が T_2 で消去されることもある。T_3 は T_1 と T_2 の臨界対 (critical pair) と呼ばれる。すなわち，グレブナー基底計算は単項式表現された多項式集合における完備化操作であると見做せる。なお，一般の項書き換えシステムでは，完備化手順が停止性を持つことも結果が完備性を持つことも保証されない。詳しくは [7, 12] 等を参照されたい。

本章の頭で述べたように，多項式の表現として単項式表現と再帰表現という異なる二種があるのだから，再帰表現に対しても臨界対を定義すべきである。日本の研究者がグレブナー基底を知って 4 ～ 5 年後，岩波講座応用数学の一分冊『計算代数と計算幾何』の前半部分の執筆依頼があった。何処でどう使うかの思案が全くないまま，「とりあえず書き記しておこう」と書いたのが下記の $\mathrm{Elim}(G,H)$ である [13]。

$$\mathrm{Elim}(G,H) := [\mathrm{ltm}(H)/C]\cdot G - [\mathrm{ltm}(G)/C]\cdot H, \quad C := \gcd(\mathrm{ltm}(G), \mathrm{ltm}(H)). \tag{4}$$

上式 (3) と (4) を比較すれば，“lmn(∗)” と “ltm(∗)” が入れ替わることを除けば全く同じである。このことから，$\mathrm{Elim}(G,H)$ は $\mathrm{Spol}(G,H)$ と同様に根源的役割を果すのでは？，との期待が膨らむ。

まず変数消去の観点から，$\mathrm{Spol}(G,H)$ に基づく**グレブナー基底法**と終結式に基づく消去法 (これを**旧式終結式法**と呼ぶ) を比較する。本段落では，与えられた多項式系を $\mathcal{F} = \{F_1,\ldots,F_m,F_{m+1}\} \subset \mathbb{K}[\boldsymbol{x},\boldsymbol{u}]$, $(\boldsymbol{x}) = (x_1,\cdots,x_m)$, $(\boldsymbol{u}) = (u_1,\cdots,u_n)$ とする。そして，$x_1,\ldots,x_m$ をこの順に消去し $\boldsymbol{u}$ の多項式を得ることを目的とする。グレブナー基底法は、F_i と $F_{j(\neq i)}$ の先頭単項を消去し最低順位のS多項式を生成するのみならず、そのS多項式を他の多項式でM簡約し，生き残った多項式を $\mathcal{F}$ に付加し、あらゆる対に対してS多項式を生成し続ける。この “最も低順位の多項式” と “あらゆる対に対して” という二つの臨界性のため、$\mathcal{F}$ の (LEX-順序での) グレブナー基底 $\mathbf{GB}(\mathcal{F})$ の最低元がイデアル $\langle\mathcal{F}\rangle$ の最低元となる。その代償として，計算に多大な時間がかかる ($m+n$ に関して 2 重指数的 [8])。終結式法では、G を係数ベクトル $(g_d, g_{d-1},\ldots,g_0)$ に対応づけることで、消去結果を行列式で表現する。実際、$G,H \in \mathbb{K}[x,\boldsymbol{u}]$ に対しては、**擬剰余** $\mathrm{Prem}(G,H) \stackrel{\mathrm{def}}{=} \mathrm{remainder}(h_e^{d-e+1}G, H)$ は $\mathbb{K}[x,\boldsymbol{u}]$ に含まれ、$\deg_x(\mathrm{Prem}(G,H)) < e$ であり、G と $x^{d-e}H,\ldots,x^0H$ の係数ベクトルを行とする行列式で表すことができる。G と H が互いに素なとき、G と H から x を消去すれば $\boldsymbol{u}$ の多項式が計算できる。これが旧式終結式である [9, 10, 2, 3, 4]。旧式終結式を G と H の係数ベクトルで表すのが有名な Sylvester 行列式である。

以上より，旧式終結式法はグレブナー基底法とは全く異なる消去法だが，理論的にはまとまっていることがわかる。しかしながら，大きな問題点を含む：旧式終結式は大抵の場合，**余計因子** (extraneous factor) を

[1] Buchberger did not put the “M”. Since the word “reduction” is used in many different meanings, the author attach M to emphasize that the reduction is performed on each monomial.

含むのである。余計因子の存在は，20 世紀初頭に Macaulay や Dixon らが多変数多項式系の旧式終結式を研究した際に既に気付いていた。その後，1980 年代に Kapur と彼の協力者ら多くの研究者が余計因子除去に取り組んだが，失敗した。余計因子と Kapur らの研究については [11] を参照されたい。なお，Macaulay たちの理論も Kapur らの理論も，旧式終結式を行列式で表現する点は同じである。

さて，$\mathrm{Elim}(G,H)$ は再帰表現での主項消去に他ならないので，これを繰り返せば変数 $x_1,\ldots,x_m$ を順に消去できる。本稿では，この方法で計算できる $\mathbb{K}[\boldsymbol{u}]$ の多項式を**終結式**あるいは**新型終結式**と呼ぶ。二つの与多項式から始まる擬剰余計算の列を**ＰＲＳ** (Polynomial Remainder Sequence) というので，G と H から始まる主項消去演算の列を**ＴＥＳ** (Term Elimination Sequence) と命名した。

$G,H\in\mathbb{K}[x,\boldsymbol{u}]$ に対するＴＥＳの定義とその性質は次章に述べるが，簡単なものである。そして，ＴＥＳに基づく終結式計算とグレブナー基底計算 (ただし，終結式計算まで) との関係も明快に解明される。だが，それだけでは全く不十分である：ＴＥＳとグレブナー基底との関係をより深く調べるには，Eulid の互除法に関する拡張互除法のような概念が是非とも必要である。そのことを簡単な例で示そう。

Example 1 下記の二多項式系 $\mathcal{F}_2$ のイデアルの最低元 $\widehat{S}_2$ は実に興味深い性質を持つ

$$\mathcal{F}_2=\begin{cases} G=x^4\times(u^2+uv)+x^2\times(u^2-uv)+(u^2+uw),\\ H=x^4\times(uv+v^2)-x^2\times(uv+v^2)+(v^2-vw).\end{cases}\tag{5}$$

$\gcd(\mathrm{lcf}(G),\mathrm{lcf}(H))=u+v$, $\mathrm{cont}(G)=u$, $\mathrm{cont}(H)=v$ [2] に注意されたい。
Buchberger 算法を多項式系 $\mathcal{F}_2$ に適用して得られる多項式の中で，変数 x が消去された多項式は順に $P_6=(u-v)\,\widehat{S}_2$, $P_7=v\,\widehat{S}_2$, $P_8=w\,\widehat{S}_2$, $P_{11}=\widehat{S}_2$ である。ここで，$\widehat{S}_2$ はイデアル $\langle\mathcal{F}_2\rangle$ の最低元で，次式である：$\widehat{S}_2=3u^4v+3u^3v^2+4u^3vw-3u^2v^3+4u^2v^2w+4u^2vw^2+uv^4-4uv^3w+4uv^2w^2$. 参考までに，$P_6=A_6G+B_6H$ を満たす多項式 A_6,B_6 を提示する：$A_6=x^2\times(-u^3v-u^2v^2)+(2u^3v+u^2v^2+yu^3)$, $B_6=x^2\times(u^3v+y^2v^2)+(\,u^4+u^3v+2u^2v^2)$。$A_i,B_i$ は P_i を生成元 G と H で表現する “$P_i=A_iG+B_iH$” の係数なので，**生成元係数** (Coefficients of Generators, **CofGs** と略す) と命名する。CofGs は二多項式系のみならず多多項式系にも定義する[3]。次に A_{11} と B_{11} を提示する。P_{11} は終結式を越えて消去を行ったので，**次数条件** (degree conditions) $\deg_x(A_6)<\deg_x(H)$, $\deg_x(B_6)<\deg_x(G)$ を満たしていない。なお，Buchberger 算法における CofGs の算法については，文献 [1] の第 2 章 3 節を参照されたい。

$$\begin{cases} A_{11} &=& x^6\times(8u^2v-8v^3)\\ &+& x^4\times(-8u^2v+4uv^2-8uvw+12v^3-8v^2w)\\ &+& x^2\times(-2u^2v+2uv^2-12v^3+16v^2w)\\ &+& (3u^2v+2uv^2+2uvw+3v^3-10v^2w+8vw^2)\\ B_{11} &=& x^6\times(-8u^3+8uv^2)\\ &+& x^4\times(-8u^3+12u^2v+8u^2w-12uv^2+8uvw\\ &+& x^2\times(-6u^3+6u^2v+4uv^2)\\ &+& (\,u^3-6u^2v+6u^2w+uv^2-6uvw+8uw^2).\end{cases}$$

実は，本例題の二多項式系は，論文 [14] の研究の中で現れた系である。そこでは，“拡張ヘンゼル構成” という演算の結果式を，グレブナー基底の最低元とその CofGs を用いて最も簡潔な形で表現したかった。そこで，A_{11} と B_{11} が簡単にならないかと，試みに A_{11} を H で，B_{11} を G で割ってみたところ，いずれも剰余が多項式になった。参考までに，これら除算の剰余を提示する。

$$\begin{aligned}\widehat{A}_{11}:=\mathrm{remainder}(A_{11},H) &= -x^2\times(2u^2v+2uv^2)+3u^2v+2uv^2+2uvw-v^3+2v^2w,\\ \widehat{B}_{11}:=\mathrm{remainder}(B_{11},G) &= x^2\times(2u^3+2u^2v)+u^3-2u^2v-2u^2w+uv^2-2uvw.\end{aligned}$$

[2] $F=f_l(\boldsymbol{u})x^l+f_{l-1}(\boldsymbol{u})x^{l-1}+\cdots+f_0(\boldsymbol{u})$ のとき，$\mathrm{cont}(F)=\gcd(f_l,f_{l-1},\ldots,f_0)$ である。

[3] $G,H\in\mathbb{K}[x]$ の場合，(A_i,B_i) は Coefficients of Bezout's identity と呼ばれるが，Bezout's identity は Euclid の拡張互除法の公式そのものである。今の場合，生成元は多変数多項式でしかも 3 個以上でもよいので，CofGs の方がよい命名であろう。

$\mathrm{quotient}(A_{11},H)\cdot G+\mathrm{quotient}(B_{11},G)\cdot H=0$ なので，$\widehat{A}_{11}G+\widehat{B}_{11}H=\widehat{S}_2$ が得られる。筆者はこれには驚くとともに，このことは一般的に成立するに違いないと確信した。証明は第３章で与える。 //

ほとんどの読者は，特にブレブナー基底算法の信奉者は，多変数多項式イデアルの最低元は $\mathrm{Spol}(G,H)$ 演算を用いなければ計算できない，と思っているだろう。しかし，少なくとも二多項式系に対しては，上例に示した CofGs の性質を使えば，Ｓ多項式を一切計算することなく，イデアルの辞書式順序での最低元がＰＲＳとＧＣＤ演算で計算できる。なお，CofGs の性質自体は，ＴＥＳによって明快に解析されることを付記しておく。多多項式系に対しては，まだ証明したわけではないが，Ｓ多項式を使わなくてもイデアルの最低元を計算できると筆者は思っている。だが，筆者自身はその研究を遂行する気はない。

2 Definition of ＴＥＳ and Derivation of various formulas

本章では，$\deg_x(G)\geq\deg_x(H)$ を満たし２個以上の項を持つ，relatively prime $G,H\in\mathbb{K}[x,\boldsymbol{u}]$ から始まるＴＥＳ ($P_1{:=}G,\ P_2{:=}H,\ P_3{:=}\mathrm{Elim}(P_1,P_2),\ \cdots,\ P_{i+1}{:=}\mathrm{Elim}(P_{i-1},P_i),\ \cdots,\ P_k{:=}\mathrm{Elim}(P_{k-2},P_{k-1})$), $P_k\in\mathbb{K}[\boldsymbol{u}]$), を考える。各 $\mathrm{Elim}(P_{i-1},P_i)$ において，P_{i-1} と P_i をそれぞれ **operand**, **eliminator** と呼ぶ。前章では，$\mathrm{Spol}(G,H)$ との類似性を強調するため $\mathrm{Elim}(G,H)$ を (4) 式で定義したが，実際計算の観点からは x を表に出した方が解り易く，次のように書き改める；こうしても内容は不変である。

$$\left\{\begin{array}{c} P_{i+1}:=\mathrm{Elim}(P_{i-1},P_i)=[\mathrm{lcf}(P_i)/c_i]\cdot P_{i-1}-[\mathrm{lcf}(P_{i-1})/c_i]\cdot x^{\delta_i}P_i,\\ c_i=\gcd(\mathrm{lcf}(P_{i-1}),\mathrm{lcf}(P_i)),\quad \delta_i=\deg_x(P_{i-1})-\deg_x(P_i).\end{array}\right. \tag{6}$$

2.1 Generation rules of ＴＥＳ and basic properties of ＴＥＳ

初期基底を $\{P_1,P_2\}$，現基底を $\{P_{i-1},P_i\}$ とするとき，ＴＥＳの生成規則は次の三つである。

規則１ ： operand P_{i-1} は現基底の最大次数元である。
： eliminator P_i は現基底の残りの元である。
$\Longrightarrow P_{i+1}:=\mathrm{Elim}(P_{i-1},P_i)$ を生成する。
規則２ ： $\Longrightarrow P_{i-1}$ を現基底から削除する。
規則３ ： $\Longrightarrow P_i$ を新基底に付加する。

ＴＥＳの基本的性質は次の三つである。

性質Ａ ： $\deg(P_{i+1})<\deg(P_{i-1})\ \Longleftarrow\ d_j\stackrel{\mathrm{def}}{=}\deg(P_j)$；
$d_{i-1}=d_i,\ d_{i-1}>d_i$ の両場合でそうだから。
性質Ｂ ： operand は現基底の次数最大の元だが，
$d_{i-1}=d_i$ の場合，一意に定まらない。
$\Longrightarrow$ ＴＥＳは二つに**枝分かれ**する。
性質Ｃ ： 同じ多項式を複数回 eliminator に使うこともある。
($\deg_x(P_{i-1})\geq\deg_x(P_i)+2$ が必要)。
$\Longrightarrow$ ＴＥＳを **abnormal** と呼ぶ。

まず，枝分かれ (**branching**) の場合 (即ち，$\deg_x(P_{i-1})=\deg_x(P_i)$ の場合) の特徴を述べる。なお，枝分かれの実際の状況は分かり難いので，次節で具体例を与える。

特徴１ ： P_{i+1} は $\pm$ 符号を除き **operand 選択** に依らない。
$\Longleftarrow\ \mathrm{Elim}(P_{i-1},P_i)=-\mathrm{Elim}(P_i,P_{i-1})$ ゆえ。

特徴２　：　P_{i+2} では **operand 選択** の差が現れる(下記の二通り)。

$$P_{i+1}=\mathrm{Elim}(P_{i-1},P_i) \implies P_{i+2}=\mathrm{Elim}(P_i,P_{i+1}).$$
$$P_{i+1}=\mathrm{Elim}(P_i,P_{i-1}) \implies P_{i+2}=\mathrm{Elim}(P_{i-1},P_{i+1}).$$
$$\text{いずれの場合も } P_{i+3}=\mathrm{Elim}(P_{i+1},P_{i+2}).$$

特徴３　：　枝分かれを全て辿れば，**最低順位の終結式**が得られる。

上記の特徴１を見て，筆者は “ＴＥＳは±符号を除いて一意的だ” と早合点したが，ゆっくり考えて，“P_{i+2} の計算時点で分岐する” と気付いた。特徴３については第３章第一節で具体的に述べる。

次に，**abnormal** な場合 (同一要素が $r\,(>1)$ 回，eliminator として使用される) を詳しく述べる。簡単のため，ＴＥＳが先頭項から abnormal となる場合を扱い，ＴＥＳ中の abnormal な要素等は P'_j のように $'$ をつけて区別する $\implies P'_1=G,\, P'_{1+r}=H$。この場合，$(P'_1,\, P'_2,\, \cdots,\, P'_r,\, P'_{1+r})$ を abnormal な要素列とする；$P'_{1+r}=H$ ゆえ P'_{1+r} は Elim 演算で計算すべき要素ではなく，下記で知るように $\deg(P'_r)=\deg(P'_{1+r})$ となる可能性があり，その場合は (P'_r, P'_{1+r}) で枝分かれするので，P'_{1+r} を abnormal 列の最終要素とした。上記のように定めたＴＥＳの abnormal 要素の生成公式と性質は次である。

$$\begin{cases} P'_{1+j} \;:=\; [\mathrm{lcf}(H)/c'_j]\,P'_j - [\mathrm{lcf}(P'_j)/c'_j]x^{\delta'_j}H \quad (1\le j<r), \\ c'_j=\gcd(\mathrm{lcf}(P'_j),\mathrm{lcf}(H)), \quad \delta'_j=\deg_x(P'_j)-\deg_x(H)\ge 0. \end{cases} \tag{7}$$

a)　ＴＥＳが先頭から abnormal となる必要十分条件は
$\deg_x(\mathrm{Elim}(G, x^{\deg(G)-\deg(H)}H))\ge\deg_x(H)$ である。

b)　ＴＥＳの途中からでも abnormal になりえる。

c)　$\deg(G=P'_1)>\deg(P'_2)>\cdots>\deg(P'_r)\ge\deg(H)$ である。

d)　P'_{1+r} の続きは $P_3:=\mathrm{Elim}(P'_r,H)$ から始まるが，
$\deg(P'_r)=\deg(H)$ の場合は枝分かれする。

a) と **b**) は自明だろう。(7) 式より，P'_j の主項は $x^{\delta'_j}H$ で消去されるので，$\delta'_j>0$ なら $\deg(P'_{1+j})<\deg(P'_j)$ であり，$\delta'_j=0$ は $j=r$ の場合にのみ生じ得る $\Rightarrow$ **c**)。abnormal ＴＥＳの最終基底は $(P'_r,\, H=P'_{1+r})$ であるが，**d**) の P_3 は，枝分かれが生じるか否かに関わらず，normal なＴＥＳ要素と見做す。

2.2　An example of computing braching ＴＥＳ

Example 1 (continued)：　Branching を起こす $\mathrm{TES}_x(G,H)$ を具体的に計算してみよう。

$P_1:=G=x^4{\cdot}(u^2+uv)+x^2{\cdot}(u^2-uv)+(u^2+uw), \quad \mathrm{cont}(P_1)=u,\ \mathrm{cont}(P_2)=v.$

$P_2:=H=x^4{\cdot}(uv+v^2)-x^2{\cdot}(uv+v^2)+(v^2-vw), \quad \gcd(\mathrm{lcf}(P_1),\mathrm{lcf}(P_2))=u+v.$

$P_3:=[(uv+v^2)/(u{+}v)]{\times}P_1-[(u^2+uv)/(u{+}v)]{\times}P_2=2x^2u^2v+u^2v-uv^2+2uvw.$

ＴＥＳの先頭から branching が始まっている $\implies$ **二つの枝を追跡する！**

$$\gcd(\mathrm{lcf}(P_1),\mathrm{lcf}(P_3))=u, \qquad \gcd(\mathrm{lcf}(P_2),\mathrm{lcf}(P_3))=v.$$

$P_{41}:=[(2u^2v)/u]{\times}P_1-[(u^2+uv)/u]{\times}x^2P_3=x^2{\cdot}(u^3v-2u^2v^2-2u^2vw+uv^3-2uv^2w)+2u^3v+2u^2vw.$

$P_{42}:=[2u^2v/v]{\times}P_2-[(uv+v^2)/v]{\times}x^2P_3=x^2{\cdot}(-3u^3v-2u^2v^2-2u^2vw+uv^3-2uv^2w)+2u^2v^2-2u^2vw.$

二つの枝をさらに追跡する！

$$\gcd(\mathrm{lcf}(P_3),\mathrm{lcf}(P_{41}))=uv, \qquad \gcd(\mathrm{lcf}(P_3),\mathrm{lcf}(P_{42}))=uv.$$

$P_{51}:=[\mathrm{lcf}(P_{41})/uv]{\times}P_3-[(2u^2v)/uv]{\times}P_{41}=3u^4v+3u^3v^2+4u^3vw-3u^2v^3+(5\text{ terms})=\widehat{S}_2.$

$P_{52}:=[\mathrm{lcf}(P_{42})/uv]{\times}P_3-[(2u^2v)/uv]{\times}P_{42}=-3u^4v-3u^3v^2-4u^3vw+3u^2v^3-(5\text{ terms})=-\widehat{S}_2.$

ウワー，ビックリ仰天だ $\cdots$ 一気に $\widehat{S}_2$ が出てきちゃったよ！　//

2.3 Derivation of CofGs for each element of ＴＥＳ

第 1 章の **Ex.1** で，グレブナー基底計算中に現れる多項式の CofGs の重要性を述べた。重要性はＴＥＳに対しても言える (本稿ではそうでもないのだが…)。本節では，まず $A_iG+B_iH=P_i$ を満たす CofGs $(A_i,B_i)\in\mathbb{K}[x,\boldsymbol{u}]^2$ を，ＴＥＳが normal な場合と abnormal な場合に対して別々に導出する。

ＴＥＳが normal な場合 **:** $(A_1,B_1)=(1,0)$, $(A_2,B_2)=(0,1)$ は自明である。さらに，A_{i+1},B_{i+1} が

$$\begin{aligned} A_{i+1} &:= [\mathrm{lcf}(P_i)/c_i]\,A_{i-1}-[\mathrm{lcf}(P_{i-1})/c_i]\,x^{\delta_i}A_i,\\ B_{i+1} &:= [\mathrm{lcf}(P_i)/c_i]\,B_{i-1}-[\mathrm{lcf}(P_{i-1})/c_i]\,x^{\delta_i}B_i, \end{aligned} \tag{8}$$

なる逐次公式で計算できることは，i に関する帰納法で簡単に示せる。また，ＴＥＳの最終要素 $P_k\in\mathbb{K}[\boldsymbol{u}]$ に対しては，次式が成立する; $\deg(A_k)$ と $\deg(B_k)$ の差は $(A_2,B_2)=(0,1)$ に基づく。

$$\begin{aligned} \deg(A_k)&=\delta_3+\cdots+\delta_{k-1}=\deg(H)-\deg(P_{k-1}),\\ \deg(B_k)&=\delta_2+\cdots+\delta_{k-1}=\deg(G)-\deg(P_{k-1}). \end{aligned} \tag{9}$$

ＴＥＳの要素 P_i の次数は i に関して単調減少だが，A_i と B_i の次数は単調増加ゆえ，**2.1** 節の性質Ａより $\deg(A_{i+1})>\deg(A_{i-1})$, $\deg(B_{i+1})>\deg(B_{i-1})$ である。したがって，(8) 式より次式が得られる。

$$\mathrm{ltm}(A_{i+1})=-[\mathrm{lcf}(P_{i-1})/c_i]\,x^{\delta_i}\cdot\mathrm{ltm}(A_i),\quad \mathrm{ltm}(B_{i+1})=-[\mathrm{lcf}(P_{i-1})/c_i]\,x^{\delta_i}\cdot\mathrm{ltm}(B_i). \tag{10}$$

次にabnormal な場合の CofGs **:** 前節と同様，$P'_1{=}G$ かつ $P'_{1+r}{=}H$ (すなわち先頭の r 項が abnormal) とする。自明な $(A'_1,B'_1)=(1,0)$ から出発し，各要素 P'_i $(2\le i\le r)$ に対し，$A'_iG+B'_iH=P'_i$ を満たす $(A'_i,B'_i)\in\mathbb{K}[x,\boldsymbol{u}]^2$ を算式 (7) に基づき計算する。$i=2$ では，$P'_2=[\mathrm{lcf}(H)/c'_1]G-[\mathrm{lcf}(P'_1)/c'_1]x^{\delta'_1}H$ だが $\gcd(G,H)=1$ ゆえ，$(A'_2,B'_2)=(\,[\mathrm{lcf}(H)/c'_1],-[\mathrm{lcf}(P'_1)/c'_1]x^{\delta'_1}\,)$ と一意に決まる。$i=3$ では，$A'_3G+B'_3H=P'_3=[\mathrm{lcf}(H)/c'_2]P'_2-[\mathrm{lcf}(P'_2)/c'_2]x^{\delta'_2}H$ なので，右辺の P'_2 を前記の G と H で表すと，$A'_3=[\mathrm{lcf}(H)/c'_2][\mathrm{lcf}(H)/c'_1]$, $B'_3=-[\mathrm{lcf}(H)/c'_2][\mathrm{lcf}(P'_1)/c'_1]x^{\delta'_1}-[\mathrm{lcf}(P'_2)/c'_2]x^{\delta'_2}$ が得られる。A'_3 と A'_2 は 漸化式 $A'_3=[\mathrm{lcf}(H)/c'_2]\cdot A'_2$ を満たし，B'_3 と B'_2 は $B'_3=[\mathrm{lcf}(H)/c'_2]\cdot B'_2-[\mathrm{lcf}(P'_2)/c'_2]x^{\delta'_2}$ を満たす。念のために，$i=4$ の場合も計算したところ，$A'_4=[\mathrm{lcf}(H)/c'_3][\mathrm{lcf}(H)/c'_2][\mathrm{lcf}(H)/c'_1]=[\mathrm{lcf}(H)/c'_3]\times A'_3$, $B'_4=-[\mathrm{lcf}(H)/c'_3][\mathrm{lcf}(H)/c'_2][\mathrm{lcf}(P'_1)/c'_1]x^{\delta'_1}-[\mathrm{lcf}(H)/c'_3][\mathrm{lcf}(P'_2)/c'_2]x^{\delta'_2}-[\mathrm{lcf}(P'_3)/c'_3]x^{\delta'_3}$ が得られた。B'_4 と B'_3 は漸化式 $B'_4=[\mathrm{lcf}(H)/c'_3]\times B'_3-[\mathrm{lcf}(P'_3)/c'_3]x^{\delta'_3}$ を満たす。これらを一般化したのが次式である。

$$\begin{aligned} A'_{i+1}=[\mathrm{lcf}(H)/c'_i]\times A'_i,\quad B'_{i+1}&=[\mathrm{lcf}(H)/c'_i]\times B'_i-[\mathrm{lcf}(P'_i)/c'_i]x^{\delta'_i},\\ \deg_x(A'_{i+1})=0,\qquad\qquad \mathrm{ltm}(B'_{i+1})&=[\mathrm{lcf}(H)/c'_i]\times\mathrm{ltm}(B'_i). \end{aligned} \tag{11}$$

証明は簡単なので読者にお任せする。

3 Usage of ＴＥＳ for two-polynomial systems

従来，旧式終結式法とグレブナー基底法との間にはほとんど接点がなかった。前者は後者から全く相手にされなかったのである。前者の研究者は何とか後者との関わりを示したく，たとえば Wang は深い関係を発見したと主張している [18] が，筆者には深い関係とは思えない。だが，二多項式系 $\mathcal{F}_2=\{G,H\}$ に関しては，ＴＥＳと “主変数の次数を低下させる Spol の集合” との間には深い関係がある。本章では第一節で，その関係を定理の形で提示する。次いで第二節では，二多項式系の最低元を計算する算法を与える Thm.2 を証明する。実は，その証明として 2017 年論文 [16] に記したものは複雑かつ細部の説明が不明確であった。そこで，今年度 (2023 年) に簡単明瞭かつ完全な証明を行った。本稿では最新証明に加え，旧証明との対比

も行う。Buchberger 算法は，主変数が消去された (終結式に対応する) 多項式と他の多項式とのＳ多項式を次々に生成し，イデアルの最低元を生成する。第三節では，これと同様な方法をＴＥＳに対して試行する。その結果，正に “出来過ぎだ” と形容してもよいだろう定理を見出した。

まず，本章で重要な役割を果す定理をThm.0として提示する。証明には [15] と文献 [8] を参照されたい。

Theorem 0 *Let* $\mathrm{GB}(\mathcal{F}_2)$ *be the reduced Gröbner basis of* $\langle\mathcal{F}_2\rangle$ *w.r.t. the monomial order* $x \succ u_1, \ldots, u_n$ *(the* $\boldsymbol{u}$*-order may be any). Then, we have* $\mathrm{GB}(\mathcal{F}_2)\cap\mathbb{K}[\boldsymbol{u}] = \{\widehat{S}_2\}$. (Hence, any polynomial in $\langle\mathcal{F}_2\rangle\cap\mathbb{K}[\boldsymbol{u}]$ is a multiple of $\widehat{S}_2$.) □

3.1 Deep relationship between the ＴＥＳ method and Buchberger's method

まず，深い関係とはどんなものか，簡単な例を提示する。

Ex.2 Given $G := x^4\cdot(u+v) + x^2\cdot(u-2w) + (2v+w)$ and $H := x^4\cdot(u-w) + x^2\cdot(2u+v) + (v-2w)$, eliminate only the x^4-term of $\{G, H\}$ by both the Elim operation and Buchberger's method.

系 $\{G, H\}$ に対して $E_1 := \mathrm{Elim}(G, H) = (u-w)\times G - (u+v)\times H$ を実行すると x^4-項が消去されて，$E_1 = (u-w)[x^2\,(u-2w) + (2v+w)] - (u+v)[x^2\,(2u+v) + (v-2w)]$ を得る。

次に，x^4-項消去をＳ多項式生成で行うのだが，Buchberger 算法は可能な限りＳ多項式生成を行うので，制限されたＳ多項式だけを生成するように，$G = x^4u + x^4v + R_G$，$H = x^4u - x^4w + R_H$ と書き換える。すると，Spol 集合として，たとえば $\mathrm{Spol}(G, H) = G - H = x^4v + x^4w + R_G - R_H =: G_3$，$\Rightarrow$ $\mathrm{Spol}(G, G_3) = -x^4uw + x^4v^2 - (u-v)\,R_G + (u+w)\,R_H \xrightarrow{G_3\!\!\!\!\!\!\rightarrow} -(u-w)\,R_G + (u+v)\,R_H =: \widehat{E}_1$，$\mathrm{Spol}(H, G_3)\cdots\xrightarrow{G} -(u-w)\,R_G + (u+v)\,R_H = \widehat{E}_1$ を得る。見て分かるとおり，$E_1 = \widehat{E}_1$ である。 //

x^4-項を消去して得られる多くの多項式の中で，上記の E_1 が最低順序の多項式であることは，$\mathrm{Elim}(G, H)$ 演算が臨界対であることによる。$\mathrm{Elim}(G, H)$ は正に単刀直入，ＴＥＳの面目躍如である。

上記の例を一般化すれば次の定理が得られる: なお下記では，当然ながら G も H も複数項から成り，$F \in \mathbb{K}[x, \boldsymbol{u}]$ に対し，$F\rfloor_{e'}$ は F の項のうち x-次数が e' 以上の全ての項の和を表すとする。

Theorem 1 *Let* $\deg(G) = d \geq e = \deg(H)$. *Let* e' *be any integer s.t.* $e > e' > 0$ *and at least one of* $G\rfloor_{e'-1} - G\rfloor_{e'}$ *and* $H\rfloor_{e'-1} - H\rfloor_{e'}$ *is not zero. Let* $P_{e'}$ *and* $\widehat{P}_{e'}$ *be the lowest-order polynomials obtained by eliminating all the and only the terms of* $G\rfloor_{e'}$ *and* $H\rfloor_{e'}$, *as follows. The* $P_{e'}$ *is obtained by the TES method, by tracing all the branches encountered and finding the lowest-order polynomial. The* $\widehat{P}_{e'}$ *is obtained by Buchberger's method. So,* $\deg_x(P_{e'}) = \deg_x(\widehat{P}_{e'}) < e'$. *Then,* $\widehat{P}_{e'} = cP_{e'}$, *where* $c \in \mathbb{K}$.

Proof 指数 e' は G and/or H のどれか一つの項を定めているが，このことは定理には必要不可欠である。実際の計算においては，次数が e' 未満の項全体を別記号で置き換えるのが間違いがなく効率的である。

さて，各演算 $P_{i+1} := \mathrm{Elim}(P_{i-1}, P_i)$ は，P_{i-1} と P_i の主項どうしを消去して得られる多くの多項式の中で最低順位のものである。今の場合，多くの Elim 演算を繋いで $G\rfloor_{e'}$ 及び $H\rfloor_{e'}$ の項消去が行われる。当然，枝分かれが何度も起きるだろうが，全ての枝を辿り，それらの中で順序が最低の多項式を選び出し，それを $P_{e'}$ としている。したがって，$P_{e'}$ は定理が目的とする多項式である。

問題は Buchberger 法が $P_{e'}$ の定数倍の多項式を計算できるか，である。それには $P_{e'}$ に対する CofGs 列を利用する；この CofGs 列は初期系 $\{G, H\}$ から $P_{e'}$ に至る “最短経路” を示すから，最短経路に沿いつつ Buchberger 法を適用すればよい。しかも，$P_{e'}$ の計算は Elim 演算の列であるから，個々の Elim 演算が Buchberger 法に変換できれば十分である。当該の Elim 演算を $P_{i+1} := \phi P_{i-1} - \psi x^{\delta_i} P_i$ とする。ここで，$\phi = \mathrm{lcf}(P_i)/c_i$，$\psi = \mathrm{lcf}(P_{i-1})/c_i$ であるが，c_i は後で割るとして本段落では 1 とおく。ϕ と ψ は再帰

表現での $\boldsymbol{u}$ の多項式だが，これらを単項式表現に変換して $\widetilde{\phi}$ および $\widetilde{\psi}$ と表し，$\widetilde{\phi} = s_1 + s_2 + \cdots + s_\mu$, $\widetilde{\psi} = t_1 + t_2 + \cdots + t_\nu$，$s_1 \succ s_2 \succ \cdots \succ s_\mu$, $t_1 \succ t_2 \succ \cdots \succ t_\nu$ とする (s_μ and/or t_ν は定数も有り得る)。上記 Elim 演算は，その主係数だけに着目すると $\phi \times \mathrm{lcf}(P_{i-1}) - \psi \times \mathrm{lcf}(P_i) = (\phi\psi - \psi\phi) = 0$ なる恒等式である。この恒等式は単項式表現に変換しても当然成立する。さらに，$R_{i-1} := \mathrm{rest}(P_{i-1})$, $R_i := \mathrm{rest}(P_i)$ とおき，$d = \deg_x(P_{i-1})$ とすれば，上記 Elim 演算は下式のように表せる ($(\widetilde{\phi}, \widetilde{\psi})$ と (ϕ, ψ) は同値)。

$$[(s_1 + \cdots + s_\mu) \times (t_1 + \cdots + t_\nu) \cdot x^d + \phi R_{i-1}] \; - \; [(t_1 + \cdots + t_\nu) \times (s_1 + \cdots + s_\mu) \cdot x^d + \psi x^{\delta_i} R_i]. \qquad (12)$$

上式で x^d の係数を見ると，各添字対 (j_1, j_2) に対して $s_{j_1} t_{j_2} = t_{j_2} s_{j_1}$ ゆえ，左部の $s_{j_1} t_{j_2}$ と右部の $t_{j_2} s_{j_1}$ は正確に打ち消し合う。すなわち，(12) 式の x^d-項の係数部を単項式表現で素直に計算するだけで，x^d-項が消去される。以上より，S 多項式を計算するまでもなく，非常に簡単に定理が証明される。 □

Remark 1 上記定理で $e' = 1$ とすると新型の終結式が計算できる。だが，Thm.1 で計算される $\widehat{P}_1$ はイデアルの最低元 $\widehat{S}_2$ ではない。第 1 章の Ex.1 で言うならば，$\widehat{P}_1$ は多項式 P_6 に対応する。実際，$\widehat{P}_1$ も P_6 も，それらの CofGs は次数条件を満たす。$\widehat{S}_2$ は，$\widehat{P}_1$ と他の多項式との S 多項式 s を次々に計算して得られる。なお，本稿は “次々と S 多項式 s を計算しないで $\widehat{S}_2$ を計算してやる”，という野心的なものである。 //

3.2 Computing $\widehat{S}_2$ without constructing any Spolynomial

Theorem 2 (S and Inaba [16]) *Let $G, H \in \mathbb{K}[x, \boldsymbol{u}]$, with $\deg(G) \geq \deg(H) \geq 1$, be relatively prime, $P_k \in \mathbb{K}[\boldsymbol{u}]$ be the last element of $\mathrm{PRS}_x(G, H)$, and $A_k, B_k \in \mathbb{K}[x, \boldsymbol{u}]$ be the CofGs of P_k. Let $\widehat{S}_2$ be the lowest-order element of $\mathrm{GB}(\{G, H\})$, and $\widetilde{A}, \widetilde{B} \in \mathbb{K}[x, \boldsymbol{u}]$ be the CofGs of $\widehat{S}_2$. If $\widetilde{A}$ and $\widetilde{B}$ satisfy the degree conditions, $\deg(\widetilde{A}) < \deg(H)$ and $\deg(\widetilde{B}) < \deg(G)$, then we have $P_k / \gcd(\mathrm{cont}(A_k), \mathrm{cont}(B_k)) = c\,\widehat{S}_2$, where $c \in \mathbb{K}$. If $\widetilde{A}$ and $\widetilde{B}$ do not satisfy the degree conditions, we can convert them to $\mathrm{remainder}(\widetilde{A}, H)$ and $\mathrm{remainder}(\widetilde{B}, G)$, respectively.*

Proof 拡張互除法に関する有名な定理は，“次数条件を満たす A_k と B_k は P_k から一意的に定まる”，と主張する。今の場合，$\widetilde{A}$ と $\widetilde{B}$ が次数条件を満たすならば，Thm.0 から $P_k = C\widehat{S}_2$, $C \in \mathbb{K}[\boldsymbol{u}]$, ゆえ，$(P_k, A_k, B_k) = C \times (\widehat{S}_2, \widetilde{A}, \widetilde{B})$, となり，$C = c\,\gcd(\mathrm{cont}(A_k), \mathrm{cont}(B_k))$, $c \in \mathbb{K}$, と定まる。

次に，$\widetilde{A}$ と $\widetilde{B}$ が次数条件を満たさない場合を考える。P_k はイデアル $\langle \mathcal{F}_2 \rangle$ の要素ゆえ，Thm.0 によれば，$P_k = C\,\widehat{S}_2$ を満たす多項式 $C \in \mathbb{K}[\boldsymbol{u}]$ が存在する。C を使えば，定理の最終行が下記のように簡潔に証明できる。なお，次の段落では簡単のため $\mathrm{remainder}(A, D)$ を $\mathrm{rem}(A, D)$ と表す。

前提 $\widetilde{A}G + \widetilde{B}H = \widehat{S}_2$ と $C\widehat{S}_2 = P_k = A_kG + B_kH$ とから，$C \times (\widetilde{A}G + \widetilde{B}H) = C\,\widehat{S}_2 = A_kG + B_kH \implies (C\widetilde{A} - A_k)\,G + (C\widetilde{B} - B_k)\,H = 0$ を得る。$\gcd(G, H) = 1$ ゆえ，$C\widetilde{A} - A_k$ と $C\widetilde{B} - B_k$ はそれぞれ H と G の倍数 $\implies \mathrm{rem}(C\widetilde{A} - A_k, H) = 0$ かつ $\mathrm{rem}(C\widetilde{B} - B_k, G) = 0$ が成立する (ここで，C を remainder 演算内に残すのは，H と G による除算で C の一部が $\mathrm{lcf}(H)$ と $\mathrm{lcf}(G)$ に食われる可能性があるからである)。次数条件 $\deg(A_k) < \deg(H)$, $\deg(B_k) < \deg(G)$ より，$\mathrm{rem}(C\widetilde{A} - A_k, H) = \mathrm{rem}(C\widetilde{A}, H) - A_k = 0$ かつ $\mathrm{rem}(C\widetilde{B} - B_k, G) = \mathrm{rem}(C\widetilde{B}, G) - B_k = 0$ となり，さらに $\mathrm{rem}(C\widetilde{A}, H)\,G + \mathrm{rem}(C\widetilde{B}, G)\,H = A_kG + B_kH = P_k = C\,\widehat{S}_2$ を得るので，remainder 演算内の C を外に出すことができる。以上より，$\widehat{A} := \mathrm{rem}(\widetilde{A}, H)$, $\widehat{B} := \mathrm{rem}(\widetilde{B}, G)$ とおくと，$\widehat{A}G + \widehat{B}H = \widehat{S}_2$ を得る。 □

Remark 2 上記の証明は，論文 [16] の Theorem 2 の証明と同じに見えるが，同論文の Theorem 2 は本論の Thm.2 とは全く異なる。論文 [16] では，最も重要な命題は Lemma 1 と 2 である。Lemma 1 では，$\widetilde{A}$ と $\widetilde{B}$ の高次項で次数条件を満たさない部分の係数部は $\gamma := \gcd(\mathrm{lcf}(G), \mathrm{lcf}(H))$ の倍数であることを，G と H

の Elim 演算を利用して導いている。ついで Lemma 2 では，$(\widehat{A},\widehat{B}) := (\mathrm{rem}(\widetilde{A},H),\mathrm{rem}(\widetilde{B},G)) \in \mathbb{K}[x,\boldsymbol{u}]^2$ であることを導いている。 論文 [16] の Theorem 2 は，上記の証明の第一段落に相当する。 //

Thm.2 は第 1 章の Ex.1 に対処するもので，定理の証明では $C\widetilde{A}$ と $C\widetilde{B}$ を無条件に H と G で割っており，Ex.1 の計算をそのまま実行している。誰しも，上記の証明はずーっと以前に発見されたと思うに違いない。ところが然に非ず，証明は 2023 年 1 月に発見されたのである。以前の証明は，2017 年の論文 [16] に記されたもので，非常に複雑で読者に解りにくいし，$\widetilde{A},\widetilde{B}$ を直接扱わずＴＥＳを介するという点で筆者も不満であった。以前の証明がどんなものだったかを振り返ってみるのも読者に有用だろう。

まず，$\gamma \stackrel{\mathrm{def}}{=} \gcd(\mathrm{lcf}(G),\mathrm{lcf}(H))$ と定める。今の場合，次数条件を満たさない $\widetilde{A},\widetilde{B}$ が対象である。最初に考えたことは，$\widetilde{A}$ と $\widetilde{B}$ をそれぞれ H と G で割ると，剰余が共に $\mathbb{K}[x,\boldsymbol{u}]$ に入る条件を求めることだった。次数条件が成立しないので，$\deg(\widetilde{A}G) = \deg(\widetilde{B}H) \geq \deg(GH) \implies \mathrm{ltm}(\widetilde{A}G) + \mathrm{ltm}(\widetilde{B}H) = 0$ が成立。よって，$\gamma = 1$ ならば目的が達成される。なぜなら，$\gamma = 1 \Longrightarrow \mathrm{lcf}(G)\,|\,\mathrm{lcf}(\widetilde{B})$ と $\mathrm{lcf}(H)\,|\,\mathrm{lcf}(\widetilde{A})$ が成立する $\implies$ 多項式 $q_A := \mathrm{quotient}(\mathrm{ltm}(\widetilde{A}),\mathrm{ltm}(H))$ と $q_B := \mathrm{quotient}(\mathrm{ltm}(\widetilde{B}),\mathrm{ltm}(G))$ は $q_A + q_B = 0$ を満たす $\implies \widetilde{A} = q_A H + \widetilde{A}',\ \widetilde{B} = q_B G + \widetilde{B}'$ と表すと，$\widetilde{A}'$ と $\widetilde{B}'$ は多項式で $\widetilde{A}'G + \widetilde{B}'H = \widehat{S}_2$，かつ $\deg(\widetilde{A}') < \deg(\widetilde{A}),\ \deg(\widetilde{B}') < \deg(\widetilde{B})$ を満たす。この操作を繰り返せば，$\widehat{A}G + \widehat{B}H = \widehat{S}_2$ かつ次数条件を満たす多項式 $\widehat{A},\widehat{B}$ が計算できる。

次に，$\gamma \neq 1$ の場合を考えた。$d = \deg_x(G),\ e = \deg_x(H)$ とする。この場合でも，$\widetilde{A},\widetilde{B}$ の計算過程で，$\widetilde{A}$ の e 次以上と $\widetilde{B}$ の d 次以上の項の係数部が全て γ と互いに素になるならば，$\widetilde{A}$ と $\widetilde{B}$ の次数はそれぞれ H と G による除算で低減できる。しかし，$\widetilde{A}$ と $\widetilde{B}$ の具体的表現は未知が前提である。そこで，$\widetilde{A}$ と $\widetilde{B}$ の高次項の係数部に γ の因子がどのように入り込むかを，ＴＥＳと Gröbner 基底計算を対比することで考察した。前節の議論によれば，Gröbner 基底計算と $\mathrm{TES}_x(G,H)$ 計算とは深い関係がある。$\mathrm{TES}_x(G,H)$ の要素 P_i に対する CofGs を (A_i,B_i) とする。P_i の x-次数の減少につれて，A_i と B_i の x-次数は増加する。そして，γ の因子がどのように A_i と B_i の主係数に入り込むかは，非常に明快に解るのである。

そのことを簡単に見ておく。γ の定義式より，γ は P_1 と P_2 の主係数には含まれているが，i が増加するにつれて，γ の因子が P_{i-1} の主係数から何処かへ行く運命にある。そこで，γ の因子である $\hat{\gamma}$ が，P_{i-1} の主係数には含まれているが P_i の主係数には含まれていない，と仮定する。ＴＥＳの基本的演算である公式 (6) によれば，$c_i = \gcd(\mathrm{lcf}(P_{i-1}),\mathrm{lcf}(P_i))$ は $\hat{\gamma}$ を含まないので，$\mathrm{lcf}(P_{i-1})/\hat{\gamma}$ は $\hat{\gamma}$ を含むが，$\mathrm{lcf}(P_i)/\hat{\gamma}$ は $\hat{\gamma}$ を含まない。よって，公式 (10) によれば，$\hat{\gamma}$ は A_{i+1} と B_{i+1} の主係数に飛び移っていることがわかる。したがって，ＴＥＳの計算が終了した時点では，γ はすべて A_k と B_k の主係数に移っていることになる $\cdots$ ただ一つの例外を除いて。例外とは，G と H の定数項を除く全ての項の係数部が，γ の多項式因子をもつ場合である。よって，例外対策を考えれば一応，話は出来上がる。なお，上記はＴＥＳが normal な場合であるが，abnormal な場合にも同様な議論ができる。それでもなお，前記の筆者の不満は尤もだろう。

不満を抱えながらも，多項式の再帰表現に基づく，多・多項式系のグレブナー基底計算の高速化の研究に没頭され，証明の改良はごく最近まで放っておいた。グレブナー基底計算の高速化に関する一連の研究をサーベイ論文 [1] にまとめたあと，改めて Thm.2 の証明の改良に取り組んだ結果，拍子抜けするほど簡単に申し分ない証明が得られた；それが Thm.2 の直下に書いた証明である。

3.3 New theorem on the extraneous-factor removal for $\mathcal{F}_2$

In Buchberger's algorithm, the lowest-order polynomial $\widehat{S}_2$ of the Gröbner basis $\mathrm{GB}(\mathcal{F}_2)$ is computed as follows. Suppose a resultant $P_k(\boldsymbol{u})$ has been computed[4)], and let $\Gamma_2 := \{E_1,E_2,\ldots,E_l\} \subset \mathbb{K}[x,\boldsymbol{u}]$ be an intermediate basis when the P_k has just been computed. Then, the algorithm computes $\mathrm{Spol}(E_i,P_k)$

[4)] In actual computation, neither the user nor the system programmer recognizes when the $P_k(\boldsymbol{u})$ is computed.

for each element E_i of Γ_2, updating Γ_2. We will do a similar computation for the TES: for each element P_i of the TES, we eliminate x by P_k, with the Elim operation. 現在のところ二多項式系に限定されるが，これにより，一世紀以上も未解決だった “余計因子除去” が簡単明快に解決されるのである。

第 2 章に定義した Elim 演算では operand も eliminator も x を含み，Elim 演算により x-次数が下がっていく。しかしながら，その演算では上述の試みは実行できない。本節では，we allow polynomials in $\mathbb{K}[\boldsymbol{u}]$ as the arguments of the Elim operator. We note that, the formula in (6) gives us $\mathrm{Elim}(g,h)=0$ for $\forall g,h\in\mathbb{K}[\boldsymbol{u}]$. Hence, we add the following 性質D to Basic Properties of ＴＥＳ given in **2.1**.

性質Ｄ　：　For $\forall g,h\in\mathbb{K}[\boldsymbol{u}]$, we have $\mathrm{Elim}(g,h)=0$.

Let $\mathrm{TES}_x(G,H):=(P_1(=G),\,P_2(=H),\,P_3,\,\ldots,\,P_k)$ be “optimal ＴＥＳ”, in that its last element P_k is the lowest-order polynomial among those computable by applying the Elim operations to $\{G,H\}$.

Below, for each element P_{k-i} $(1\le i\le k-1)$ of the optimal $\mathrm{TES}_x(G,H)$, we eliminate x by P_k with the Elim operation, and denote the resulting polynomial in $\mathbb{K}[\boldsymbol{u}]$ by P_{k+i}. We express the GCD corresponding to c_i in (6) as $\theta_{i,j}:=\gcd(C_{i,j},P_k)$, where $C_{i,j}$ is the coefficient of $x^{e_{i,j}}$-term of P_{k-i}.
試みに P_{k-1} から P_{k+1} を計算してみよう。

P_{k-1} は x に関して二つの項から成るので $C_{1,1}(\boldsymbol{u})x^{e_{1,1}}+C_{1,0}(\boldsymbol{u})$ と表す。P_k を用いて P_{k-1} から主変数 x を消去することを考える。$\underline{\theta_{1,1}:=\gcd(C_{1,1},P_k)}$ とすれば，$P_{k+1}\overset{\mathrm{def}}{=}\mathrm{Elim}(P_{k-1},P_k)=[P_k/\theta_{1,1}]P_{k-1}-[C_{1,1}/\theta_{1,1}]x^{e_{1,1}}P_k=[P_k/\theta_{1,1}](C_{1,1}x^{e_{1,1}}+C_{1,0})-[C_{1,1}/\theta_{1,1}]x^{e_{1,1}}P_k=[P_k/\theta_{1,1}]C_{1,0}$ を得る。$C_{1,0}\in\mathbb{K}[\boldsymbol{u}]$ ゆえ，上記の性質Ｄにより消去は終了である。結果式を見ると P_k の一部 $(=\theta_{1,1})$ が除去されている。これは出来過ぎなので，P_{k-2} の消去も試みる。$P_{k-2}=C_{2,2}x^{e_{2,2}}+C_{2,1}x^{e_{2,1}}+C_{2,0}$ と表し，$\underline{\theta_{2,2}:=\gcd(C_{2,2},P_k)}$ とすれば，$P'_{k+2}\overset{\mathrm{def}}{=}\mathrm{Elim}(P_{k-2},P_k)=[P_k/\theta_{2,2}]\cdot(C_{2,1}x^{e_{2,1}}+C_{2,0})$ となる。P'_{k+2} は x を含むので，さらなる消去が必要である。$\underline{\theta_{2,1}:=\gcd(C_{2,1},P_k)}$ として $x^{e_{2,1}}$-項を消去すれば，$P_{k+2}\overset{\mathrm{def}}{=}\mathrm{Elim}(P'_{k+2},P_k)=[P_k/\theta_{2,2}]\times\big([P_k/\theta_{2,1}](C_{2,1}x^{e_{2,1}}+C_{2,0})-[C_{2,1}/\theta_{2,1}]x^{e_{2,1}}P_k\big)=[P_k/\theta_{2,2}][P_k/\theta_{2,1}]\,C_{2,0}$ が得られる。P_{k-2} に対する結果式も P_{k-1} に対する結果式と同様，出来過ぎと言うほかないほどよく出来ている。上記の P_k による主変数の消去計算は簡単に一般化できて，P_{k-i} $(0<i<k)$ に対して次なる P_{k+i} が得られる。

$$\left\{\begin{array}{l} P_{k-i}\text{ を }\ C_{i,i}(\boldsymbol{u})x^{e_{i,i}}+C_{i,i-1}(\boldsymbol{u})x^{e_{i,i-1}}+\cdots+C_{i,0}(\boldsymbol{u})x^0\ \text{ と表すならば,}\\ P_{k+i}=[P_k/\theta_{i,i}]\cdots[P_k/\theta_{i,1}]C_{i,0},\ \ \text{where }\ \theta_{i,j}=\gcd(P_k,C_{i,j})\quad (i\ge j\ge 1).\end{array}\right. \tag{13}$$

なお，上式において，$C_{i,j}=0$ の場合も当然あり得る。

筆者は上記の結果式を “出来過ぎ” と形容したが，何故なのか？ それは上記の主変数消去を詳しく検討すれば解る。これまで何度も言及してきたように，終結式 P_k はイデアル $\langle\mathcal{F}_2\rangle$ の最低元 $\widehat{S}_2$ の倍数で，我々の目的は $\underline{P_k}$ に含まれる余計因子の除去である。その観点から，例えば P_{k-1} の P_k による x の消去を観よう。今の場合，$\theta_{1,1}=\gcd(C_{1,1},P_k)$ が結果を決める。直感的に考えれば，誰しも $C_{1,1}$ から $\theta_{1,1}$ が除去されると思うだろう。だが実際に現れたのは $P_k/\theta_{1,1}$ だ。このことは，$\gcd(C_{1,1},P_k)\neq 1$ でありさえすれば，$\theta_{1,1}$ は P_k の余計因子 (の一部) であることを意味する。P_k から余計因子を除去したい者にとって，まるで “カモがネギを背負ってくる” ような話だ。しかも演算は超簡単だ。これが “出来過ぎ” でなくて何だろうか！

$\mathrm{TES}_x(G,H)$ の各要素 P_i $(1\le i\le k-1)$ を用いて P_k の余計因子除去を行う際の注意点をまとめた。Note that G and H are relatively prime, hence we will have $g\neq h$ and $\gcd(\gamma_0,gh)=1$, below.

Useful $\theta_{i,\star}$ **：** $\{\theta_{i,i},\theta_{i,i-1},\ldots,\theta_{i,1}\}$ contains at least one element $\neq 1$.

1) The extraneous factors due to $C_{i,i},C_{i,i-1},\ldots,C_{i,1}$ are often double-counted. The double-counting is avoided by computing non-zero LCM(Least Common Multiple) of $\theta_{i,i},\theta_{i,i-1},\ldots,\theta_{i,1}$.
2) $C_{i,j}$ の大きさ (含まれる単項式の個数) は通常 i の値が小さいほど大きく，一般に P_k が一番大きい。そこで，$P_{k-1}\Rightarrow P_{k-2}\Rightarrow\cdots$ の順にチェックしていくのが効率的である。

3) If extraneous factors are found in P_{k-i}, remove the factors found ($\Leftrightarrow$ update the P_k). Since $\theta_{i,j} = \gcd(P_k, C_{i,j}) = 1$ for the updated P_k, it is enough to check $P_{k-i-1} \Rightarrow P_{k-i-2} \Rightarrow \cdots$.

Useless $\theta_{i,\star}$ **:** all the elements of $\{\theta_{i,i}, \theta_{i,i-1}, \ldots, \theta_{i,1}\}$ are 1.

1) Once P_{k-i} is decided to be Useless, we need not check P_{k-i} any more.

factrbyGH : the factors of $\widehat{S}_2$ which are determind by G and H only.

1) Let $g := \mathrm{cont}(G)$, $h := \mathrm{cont}(H)$ then gh is a factor of $\widehat{S}_2$, where $g \neq h$. In this case, put $\widetilde{G} := G/g$, $\widetilde{H} := H/h$ and compute the lowest-order element of ideal $\langle\{\widetilde{G}, \widetilde{H}\}\rangle$.

2) $\gamma_0 := \gcd(\mathrm{ctm}(G), \mathrm{ctm}(H)) \neq 1$ is a factor of $\widehat{S}_2$; $\mathrm{ctm}(F)$ is the x^0-term of polynomial F. x を消去する際，低次項には multipliers が掛けられるが，定数項 $\mathrm{ctm}(G)$ と $\mathrm{ctm}(H)$ の因子が消えることはなく，消去結果は $\mathrm{ctm}(G)$ の倍数と $\mathrm{ctm}(H)$ の倍数の和である。なお，$\gcd(\gamma_0, gh) = 1$。

X) $\gamma := \gcd(\mathrm{lcf}(G), \mathrm{lcf}(H)) \neq 1$ の場合 **:** P_3 や P_4 などの高次項の係数部は γ または γ の因子を因子として持つ場合があるが，γ is irrelevant to the extraneous factor, because $\gcd(P_k, \gamma) = 1$.

Theorem 3 *First, separate the* **factrbyGH** *factors from the initial basis* $\{G, H\}$*, reserve them, and let* $\{G', H'\}$ *be the resulting basis. Next, compute* $\mathrm{TES}_x(G', H')$*, and for each element* P_{k-i} *of it, check if* $\theta_{i,\star}$ *is* **useful** *or* **useless***, in order* $P_{k-1} \Rightarrow P_{k-2} \Rightarrow \cdots \Rightarrow P_1$*. If* $\theta_{i,\star}$ *is* **useful** *then remove extraneous factors found from* P_{k-i} *(*$\Leftrightarrow$ *update* P_k*), according to the above* **Usefull** $\theta_{i,\star}1$*). This process stops in a finite number of steps. After checking all the* P_{k-i}*s, multiply the reserved* **factrbyGH** *factors to the* P_k *updated last. Then, the product is the* $\widehat{S}_2$*.*

Proof Theorem 0 assures us that we can find the lowest-order element of ideal $\langle\{G', H'\}\rangle$ as a factor of P_k. The formula in (13) tells us that if $\theta_{i,j} \neq 1$ then $\theta_{i,j}$ is an extraneous factor of P_k. Hence, the operation of extraneous-factor removal specified in the theorem removes only exraneous factors of the P_k. This process stops in a finite number of steps, because P_k contains only a finite number of factors.

The question is that "does the process remove *all* the extraneous factors ?". The answer is YES. The reason is that the Elim is the critical-pair operation, that gives us the lowest-order element attainable from the given system, and the operation is applied to the $\{G, H\}$ as widely and deeply as possible. Therefore, the process given in the theorem gives us the $\widehat{S}_2$. □

Note that the Theorem 2 utilizes the CofGs of P_k, while the Theorem 3 utilizes no CofGs.

(Elim 演算は予想外に強力だ。多・多項式系に適用したら，一体，どういうことになるだろう？)

謝　辞

この研究は日本学術振興会の科研費 (課題番号 18K03389) および部分的に数理解析研究所・国際共同研究センター (京都大学内) の助成を受けている。研究の遂行にあたり，CentOS 上で稼働する Lisp 処理系を提供して頂いた加古富志雄氏 (元・奈良女子大学教授)，筆者の研究環境の整備等に関して種々の問題を解決して頂いた稲葉大樹博士 (日本数学検定協会) および讃岐勝博士 (筑波大学医学医療系) に深く感謝します。

参　考　文　献

[1] T. Sasaki: A Bridge between Euclid and Buchberger (An Attempt to Enhance Gröbner Basis Algorithm by PRSs and GCDs). 28 pages, ACM Communications in Comp. Alg., 2023 (to appear).

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

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

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

[5] B. Buchberger: An algorithm for finding a basis for the residue class ring of a zero-dimensional polynomial ideal (in German), Ph.D Thesis. Univ. of Innsbruck. Math. Inst. (1965).

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

[7] B. Buchberger and R. Loos: Algebraic Simplification. *Computer Algebra (Computing Supplementum 4)*, Springer-Verlag, pp.11-43 (1982).

[8] D. Cox, J. Little, D. O'Shea: *Ideals, Varieties, and Algorithms–An Introduction to Computational Algebraic Geometry and Commutative Algebra*, Second Edition, Chap. 3 (Elimination Theory), §6, Springer-Verlag, 1997.

[9] G.E. Collins: Polynomial remainder sequences and determinants, Amer. Math. Mon. **73** (7), 708-712 (1966).

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

[11] D. Kapur: Algebraic elimination methods. Tutorial paper to ISSAC '95. Mail to kapur@cs.albany-edu.

[12] D.E. Knuth and P.B. Bendix: Simple Word Problem in Universal Algebras. *Proceedings of Conference on Comput. Problems in Abstract Algebra*, Oxford, 261-298 (1967).

[13] T. Sasaki, H. Imai, T. Asano and K. Sugihara: *Computational Algebra and Computational Geometry* (in Japanese). Chap. 5. Iwanami Lecture Series on Applied Mathematics, Vol. 5, Iwanami Book Publishing (Japan), (1993).

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

[15] T. Sasaki and D. Inaba: Various enhancements of extended Hensel constructions for sparse multivariate polynomials. *Proceedings of SYNASC 2016* (Symb. Numer. Algori. Sci. Comp.), IEEE Conf. Publ. Serv., 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 SYNASC 2017* (Symb. Numer. Algori. Sci. Comp.), IEEE Conf. Publ. Serv., 55-62 (2018).

[17] T. Sasaki: A theory and an algorithm for computing sparse multivariate polynomial remainder sequence. *Proceedings of CASC 2018* (Computer Algebra in Scientific Computing), Springer LNCS **11077**, 345-360 (2018).

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