

T E S (Term Elimination Sequence) について

佐々木 建昭 (筑波大学・名誉教授)

- 0) 多変数多項式系の変数消去に関する予備知識
- 1) 二種類の多項式表現と先頭(単)項の消去
- 2) 二種類の変数消去法：T E S法とG B法
- 3) T E Sに基づく生成元係数の算法と性質
- 4) T E SおよびG B法に基づく変数消去の関係
- 5) 多変数系でT E Sは利用できるだろうか？

多項式系の多変数消去に関する予備知識

- 関 孝和らの驚異的な偉業 (1674～1685)
- 欧州における終結式法と余計因子問題
Newton, Euler ～ Macaulay, Dixon
- G B計算法：完璧だが超遅いのが欠点
(単項式順序が辞書式の場合)
- 近年、画期的方法が日本で提案された
- その方法は三つの定理に基づくのだが、
T E Sは第一の定理に関わる

本論に先立ち、余計因子と第一の定理を実例で

PRS (= Polynomial Remainder Sequence)

$$G, H \in \mathbb{K}[x, \mathbf{u}], \quad (\mathbf{u}) = (u_1, \dots, u_n)$$

$\deg_x(G) \geq \deg_x(H)$, G と H は互いに素とする

$$\text{PRS}(G, H) = (P_1, P_2, P_3, \dots, P_k), \quad d_i := \deg_x(P_i)$$

$$P_1 = G, \quad P_2 = H, \quad P_k \in \mathbb{K}[\mathbf{u}] \neq 0 \quad (\leftarrow \text{変数消去})$$

$$P'_{i+1} := \text{Prem}(P_{i-1}, P_i) = (\alpha_i P_{i-1} - Q_i P_i)$$

$$d_{i+1} < d_i \quad (i \geq 3), \quad \alpha_i \in \mathbb{K}[\mathbf{u}], \quad Q_i \in \mathbb{K}[x, \mathbf{u}]$$

($\implies P'_{i+1}$ は $\mathbb{K}[x, \mathbf{u}]$ での剰余だ)

$$P_{i+1} := P'_{i+1} / \beta_i, \quad P_{i+1} \in \mathbb{K}[x, \mathbf{u}], \quad \beta_i \in \mathbb{K}[\mathbf{u}]$$

($\implies \beta_i$ は余計因子 (次頁で例示) の多くを除去)

PRS法を疎な二多項式系に適用すると...

$$\text{Ex.I} \quad \begin{cases} G = x^{10}y^3z^3 + x^5(3y^4 - 3z^4) - 9yz, \\ H = x^{10}y^3z^3 - x^5(2y^4 - 2z^4) - 4yz. \end{cases}$$

$\text{PRS}_x(G, H)$ の結果は

$$-9765625 y^{20} z^{20} (3y^4 - 2z^4)^5 (2y^4 - 3z^4)^5$$

イデアル $\langle \{G, H\} \rangle$ の最低元 \hat{S}_2 は

$$\begin{aligned} &yz \times (6y^8 - 13y^4z^4 + 6z^8) \\ &= yz (3y^4 - 2z^4) (2y^4 - 3z^4) \end{aligned}$$

- $\text{PRS}_x(G, H) / \hat{S}_2$ は余計因子 (extraneous factor)
- PRS を **sparsePRS** にすれば余計因子は大幅減少

\widehat{S}_2 は PRS と extndedPRS で計算可能？

$$\text{Ex.II} \begin{cases} G = x^4 \times (y^2 + yz) + x^2 \times (y^2 - yz) + (y^2 + yw), \\ H = x^4 \times (yz + z^2) - x^2 \times (yz + z^2) + (z^2 - zw). \end{cases}$$

Buchberger 算法を上記系に適用すると、

$$P_6 = (y - z) \widehat{S}_2, \dots, P_8 = w \widehat{S}_2, P_{11} = \widehat{S}_2$$

ここで、 \widehat{S}_2 は次の多項式である：

$$3y^4z + 3y^3z^2 + 4y^3zw - 3y^2z^3 + 4y^2z^2w + 4y^2zw^2$$

$P_i = A_iG + B_iH$ を満たす (A_i, B_i) を計算する：

たとえば、 A_6, B_6 は次の多項式となる

$$\begin{aligned} A_6 &= x^2 \times (-y^3z - y^2z^2) + (2y^3z + y^2z^2 + yz^3) \\ B_6 &= x^2 \times (y^3z + y^2z^2) + (y^4 + y^3z + 2y^2z^2) \end{aligned}$$

(A_{11}, B_{11}) を見ると、驚愕する事実が …

$$\begin{aligned} A_{11} &= x^6 \times (8y^2z - 8z^3) \\ &+ x^4 \times (-8y^2z + 4yz^2 - 8yzw + 12z^3 - 8z^2w) \\ &+ x^2 \times (-2y^2z + 2yz^2 - 12z^3 + 16z^2w) \\ &+ (3y^2z + 2yz^2 + 2yzw + 3z^3 - 10z^2w + 8zw^2) \\ B_{11} &= x^6 \times (-8y^3 + 8yz^2) \\ &+ x^4 \times (-8y^3 + 12y^2z + 8y^2w - 12yz^2 + 8yzw) \\ &+ x^2 \times (-6y^3 + 6y^2z + 4yz^2) \\ &+ (y^3 - 6y^2z + 6y^2w + yz^2 - 6yzw + 8yw^2) \end{aligned}$$

$$\widetilde{A} := \text{rem}(A_{11}, H), \quad \widetilde{B} := \text{rem}(B_{11}, H) \in \mathbb{Q}[x, y, z, w]$$

$\widetilde{A}G + \widetilde{B}H = \widehat{S}_2$ かつ次数条件 OK $\implies \widehat{S}_2$ が決まる

次数条件： $\deg(\widetilde{A}) < \deg(H), \deg(\widetilde{B}) < \deg(G)$

二多項式系 $\{G, H\}$ に対する主定理

定理 1 (S & Inaba, SYNASC 2017)

$G, H \in \mathbb{K}[x, \mathbf{u}]$ は互いに素で $\deg_x(G) \geq \deg_x(H)$ 。

$P_k \in \mathbb{K}[\mathbf{u}]$ は $\text{PRS}_x(G, H)$ の最終要素で, A_k, B_k は $A_k G + B_k H = P_k$ と次数条件を満たすとする。

\hat{S}_2 はイデアル $\langle \{G, H\} \rangle$ の最低元, その “CofGs” を \tilde{A}, \tilde{B} とする: $\tilde{A}G + \tilde{B}H = \hat{S}_2$ 。

\tilde{A} と \tilde{B} が次数条件を満たせば, 次式が成立する:

$$P_k / \gcd(\text{cont}(A_k), \text{cont}(B_k)) = c\hat{S}_2$$

満たさない場合, \tilde{A} と \tilde{B} を十分次数低減できる。

解説 と $\gamma = \gcd(\text{lcf}(G), \text{lcf}(H))$

- \tilde{A}, \tilde{B} が次数条件を満たせば, $(G \sim H \Leftrightarrow uG = vH \ (uv \neq 0))$
 $(A_k, B_k, P_k) \sim (\tilde{A}, \tilde{B}, \hat{S}_2)$ が成立 \Rightarrow 定理の前半
- しかし, 次数条件が満たされることは, ほとんどない。
- $\gamma = 1$ なら, $\tilde{A}G + \tilde{B}H = \hat{S}_2 \Rightarrow \text{ltm}(\tilde{A}G) + \text{ltm}(\tilde{B}H) = 0$
 $\Rightarrow \tilde{A} = QH + \tilde{A}', Q = \text{ltm}(\tilde{A})/\text{ltm}(H), \deg(\tilde{A}) > \deg(\tilde{A}')$
 これを繰り返せば, 次数条件を満足させられる。
- 問題は $\gamma \neq 1$ の場合である。この場合 (後に示すが),
 $\text{TrmElim}(P_{i-1}, P_i)$ を実行する度 $\text{lcf}(P_{i-1})$ に含まれる
 γ の因子 (の一部) が $\text{ltm}(A_{i+1})$ と $\text{ltm}(B_{i+1})$ に移る。

多項式表現：単項表現 と 再帰表現

$$(\mathbf{x}) = (x_1, x_2, \dots, x_m), \quad (\mathbf{x}') = (x_2, \dots, x_m)$$

$$(\mathbf{u}) = (u_1, \dots, u_n)$$

単項表現：多項式を単項式の和として表現する

$$F = M_1 + \dots + M_k, \quad M_1 \succ \dots \succ M_k$$

$$M_i = c_i x_1^{d_{i,1}} \dots x_m^{d_{i,m}} u_1^{e_{i,1}} \dots u_n^{e_{i,n}}$$

$$\underline{\text{lmn}(F)} = M_1, \quad \underline{\text{lc}(F)} = c_1$$

再帰表現：従変数部分を再帰的に係数に含める

$$F = f_d(\mathbf{u}') x_1^d + \dots + f_0(\mathbf{u}') x_1^0$$

各係数 f_i も下位変数で再帰的に

$$\underline{\text{ltm}(F)} = f_d x_1^d, \quad \underline{\text{lcf}(F)} = f_d$$

主単項消去 と 主項消去

単項消去：単項表現における先頭単項の消去

前記 F と $F' = M'_1 + \dots + M'_{k'}$ に対し

$$\text{Spol}(F, F') = (\text{lmn}(F')/C) F - (\text{lmn}(F)/C) F'$$

$$\text{where } C = \text{gcd}(\text{lmn}(F), \text{lmn}(F'))$$

主項消去：再帰表現における先頭項の消去

前記 F と $F' = f'_{d'} x_1^{d'} + \dots + f'_0$ に対し

$$\text{Elim}(F, F') = (\text{ltm}(F')/C) F - (\text{ltm}(F)/C) F'$$

$$\text{where } C = \text{gcd}(\text{ltm}(F), \text{ltm}(F'))$$

Knuth-Bendix の臨界対の観点では

Spol(G, H) : 単項表現での臨界対 (critical pair)

1965年, Buchberger が発見

⇒ 以後, Gröbner 基底論が大発展

Elim(G, H) : 再帰表現での臨界対 (critical pair)
(TrmElim の略) 1993年, T. Sasaki が指摘

近年になって注目を集め始めた

: PRS より根源的なことは明白

⇒ 二多項式系の TES を調べよう

TES に関する 記号一覧

(**Elim**(G, H) := $[lcf(H)/\gamma]G - [lcf(G)/\gamma]x^\delta H$)

G, H : $\in \mathbb{K}[x, \mathbf{u}]$, $\deg_x(G) \geq \deg_x(H)$, 互いに素

: called operand and eliminator

TES(G, H) : ($P_1 = G, P_2 = H, P_3, P_4, \dots, P_k \in \mathbb{K}[\mathbf{u}]$)

$P_{i+1} := \text{TrmElim}(P_{i-1}, P_i)$

$\gamma_i = \gcd(lcf_x(P_{i-1}), lcf_x(P_i))$

$\delta_i = \deg_x(P_{i-1}) - \deg_x(P_i)$

CofGs : Coefficients-of-Generators (\Leftarrow new name)

((1, 0), (0, 1), (A_3, B_3), (A_4, B_4), \dots , (A_k, B_k))

satisfying $A_i G + B_i H = P_i$ for $\forall i$

TES の基本的な生成規則

$$(P_{i+1} := \text{TrmElim}(P_{i-1}, P_i))$$

規則 1 : operand P_{i-1} は基底の最大次数元とする
: eliminator P_i は基底の第二次数元とする
 $\implies P_{i-1}$ と P_i から P_{i+1} を生成する

規則 2 : $\implies P_{i-1}$ を現基底から削除する

規則 3 : $\implies P_{i+1}$ を新基底に追加する

$\text{TES}_x(G, H)$ では, i によらず基底の元数は 2

TES の基本的性質

性質 A : $\deg(P_{i+1}) < \deg(P_{i-1})$ ($i \geq 2$)
 $\Leftarrow d_{i-1} = d_i, d_{i-1} > d_i$ 両場合で成立

性質 B : **operand** は現基底の次数最大の元だが,
複数個の可能性あり (同次数の場合)
 \implies TES は二つに **枝分かれ** する

性質 C : 同じ式を複数回 **eliminator** に使うことも
($\deg_x(P_{i-1}) \geq \deg_x(P_i) + 2$ が必要)
 \implies TES を **abnormal** と呼ぶ

枝分かれ (**branching**) の場合を詳しく

(すなわち, $\deg_x(P_{i-1}) = \deg_x(P_i)$ の場合)

P_{i+1} : \pm 因子を除き operand 選択 に 依らない
 $\Leftarrow \text{Elim}(P_{i-1}, P_i) = -\text{Elim}(P_i, P_{i-1})$ ゆえ

P_{i+2} : operand 選択 の 差が現れる

$$P_{i+1} = \text{Elim}(P_{i-1}, P_i) \Rightarrow P_{i+2} = \text{Elim}(P_i, P_{i+1})$$

$$P_{i+1} = \text{Elim}(P_i, P_{i-1}) \Rightarrow P_{i+2} = \text{Elim}(P_{i-1}, P_{i+1})$$

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

対処法 : 枝分かれを 全て辿れば最低順位終結式 を得る

Abnormal な場合を詳しく

($\text{TES}_x(G, H)$ が先頭で **abnormal** となる
必要十分条件は $G' = \text{Elim}(G, x^{\delta_2} H)$ が
条件 $\deg_x(G') \geq \deg_x(H)$ を満たすこと)

↓

- 1) : 上記条件が続く限り, eliminator は H
TES の生成公式は意外に簡単
しかも, 定理 1 の証明に無関係
(これらは後ほど具体的に示す)
- 2) : **枝分かれ** は起きても abnormal の最後

CofGs (**normal** T E S の場合)

$$(P_{i+1} := [\text{lcf}(P_i)/\gamma_i] P_{i-1} - [\text{lcf}(P_{i-1})/\gamma_i] x^{\delta_i} P_i)$$

↓

$$(A_1, A_2) = (1, 0), \quad (B_1, B_2) = (0, 1)$$

$$A_{i+1} := [\text{lcf}(A_i)/\gamma_i] A_{i-1} - [\text{lcf}(A_{i-1})/\gamma_i] x^{\delta_i} A_i$$

$$B_{i+1} := [\text{lcf}(B_i)/\gamma_i] B_{i-1} - [\text{lcf}(B_{i-1})/\gamma_i] x^{\delta_i} B_i$$

$$\deg(A_k) = \delta_3 + \cdots + \delta_{k-1} = \deg(H) - \deg(P_{k-1})$$

$$\deg(B_k) = \delta_2 + \cdots + \delta_{k-1} = \deg(G) - \deg(P_{k-1})$$

公式 III

$$\text{ltm}(A_{i+1}) = -[\text{lcf}(P_{i-1})/\gamma_i] x^{\delta_i} \text{ltm}(A_i)$$

$$\text{ltm}(B_{i+1}) = -[\text{lcf}(P_{i-1})/\gamma_i] x^{\delta_i} \text{ltm}(B_i)$$

CofGs (**abnormal** T E S の場合)

$$\left(\begin{array}{l} P'_{1+j} := [\text{lcf}(P_2)/\gamma'_j] P'_j - [\text{lcf}(P'_j)/\gamma'_j] x^{\delta'_j} P_2 \\ \gamma'_j = \gcd(\text{lcf}(P'_j), \text{lcf}(P_2)), \quad \delta'_j = \deg(P'_j) - \deg(P_2) \end{array} \right)$$

↓

$$(A'_1, B'_1) := (1, 0), \quad (j = 1, \dots, r) \text{ below}$$

$$A'_{1+j} = [\text{lcf}(P_2)/c'_j] A'_j = [\text{lcf}(P_2)/c'_j] \cdots [\text{lcf}(P_2)/c'_1]$$

$$\begin{aligned} B'_{1+j} &= [\text{lcf}(P_2)/c'_j] B'_j - [\text{lcf}(P'_j)/c'_j] x^{\delta'_j} \\ &= -[\text{lcf}(P_2)/c'_j] \cdots [\text{lcf}(P_2)/c'_1] x^{\delta'_1} \\ &\quad - \cdots - [\text{lcf}(P'_j)/c'_j] x^{\delta'_j} \end{aligned}$$

$$A'_{i+j} = \text{ltm}(A'_{i+j}), \quad \text{ltm}(B'_{1+j}) = -\text{ltm}(A'_{1+j}) x^{\delta'_1}$$

γ はどうなる？ (normal TES の場合)

(公式III (以下に再掲) が教えてくれる)

$$\left(\begin{array}{l} \text{ltm}(A_{i+1}) = -[\text{lcf}(P_{i-1})/\gamma_i] x^{\delta_i} \text{ltm}(A_i) \\ \text{ltm}(B_{i+1}) = -[\text{lcf}(P_{i-1})/\gamma_i] x^{\delta_i} \text{ltm}(B_i) \end{array} \right)$$

γ の因子 $\hat{\gamma}$ は, $\text{lcf}(P_{i-1})$ の因子だが, $\text{lcf}(P_i)$ の因子ではないとする。 $\gamma_i = \text{gcd}(\text{lcf}(P_{i-1}), \text{lcf}(P_i))$ であるから, $\hat{\gamma}$ は $[\text{lcf}(P_{i-1})/\gamma_i]$ の因子である。
公式IIIより, このことは $\text{lcf}(P_{i-1})$ の因子 $\hat{\gamma}$ が A_{i+1} と B_{i+1} の 主項に飛び移ることを意味する。

γ はどうなる？ (abnormal TES の場合)

(公式III と同種の公式は全く役に立たない)
(しかし, 全く別の観点から簡単明瞭に解る)

$$P'_{1+j} := [\text{lcf}(P_2)/\gamma'_j] P'_j - [\text{lcf}(P'_j)/\gamma'_j] x^{\delta'_j} P_2$$

$j = 1$: $P'_1 = G, P_2 = H$ ゆえ $\gamma'_1 = \gamma$ である

$j > 1$: 一般に $\text{lcf}(P'_j)$ は γ を因子には持たない
: しかし $[\text{lcf}(P_2)/\gamma'_j] \text{lcf}(P'_j)$ 全体は持つ
⇒ そこで, 足りない分を $\text{lcf}(P'_j)$ に掛ける

まとめ : $P'_1 \Rightarrow P'_2 \Rightarrow \dots \Rightarrow P'_r$ の過程中 $\text{lcf}(P'_j) = \gamma$

TES と GB 基底法 との関係 I

- (終結式法と GB 法の関係づけは長年の課題)
 (その課題が TES を使うと簡単に解決する)

G, H に対し, $d = \deg_x(G) \geq \deg_x(H) = e$, $\delta = d - e$,
 $E_1 := \text{TrmElim}(G, x^\delta H)$, \hat{E}_1 は $\text{lcm}(G)$ と $\text{lcm}(x^\delta H)$
 だけを Buchberger 算法で消去したものとする。叩し,
 x^d 項を消去した結果式は, 消去には使わないとする。
 すると, $\hat{E}_1 = cE_1$, $c \in \mathbb{K}$ が成立する。

(簡単に) E_1 が最小なのは TrmElim の定義より明白。
 $[\text{lcf}(H)/\gamma]$ と $[\text{lcf}(G)/\gamma]x^\delta$ の単項式表現より
 \hat{E}_1 が Spol と M簡約で具体的に表現できる。

上記の命題に対する簡単な例題

$$\begin{cases} G := x^4 \times (y+u) + x^2 \times (y-2w) + (2u+w), \\ H := \underline{x^4 \times (y-w)} + x^2 \times (2y+u) + (u-2w). \end{cases}$$

Buchberger 算法での \hat{E}_1 の計算例 :

(we put $R_G := \text{rest}(G)$ and $R_H := \text{rest}(H)$)

$$\begin{aligned} G &= \underline{2x^4y} + x^4u + R_G, & H &= \underline{2x^4y} - x^4w + R_H, \\ \text{Spol}(G, H) &= G - H = \underline{2x^4u} + x^4w + R_G - R_H \Rightarrow G_3, \\ \text{Spol}(G, G_3) &= -\underline{2x^4yw} + x^4u^2 - (y-u)R_G + (y+w)R_H \\ &\xrightarrow{H} \underline{2x^4u^2} - x^4w^2 - (y-u)R_G + (y+w)R_H \\ &\xrightarrow{G_3} -(y-w)R_G + (y+u)R_H \Rightarrow \hat{E}_1, \\ \text{Spol}(H, G_3) &= \dots \xrightarrow{G} -(y-w)R_G + (y+u)R_H = \hat{E}_1. \end{aligned}$$

続：TES と GB 基底法 との関係 II

本頁では、 $F]_{e'}$ は F の次数 e' 以上の項の和を意味する

$e \geq e' > 0$ なる任意の指数 e' に対し $G]_{e'-1} - G]_{e'}$ と $H]_{e'-1} - H]_{e'}$ の少くとも一方は 0 でないとする。 $E_{e'}$ および $\hat{E}_{e'}$ は $G]_{e'}$ と $H]_{e'}$ の全項をそれぞれ TES 法 および Buchberger 算法で消去した結果式とする。ただし、 $E_{e'}$ は全ての枝を辿って最小順序多項式に定め、消去の結果式は消去には使わない。すると、 $E_{e'} = c\hat{E}_{e'}$, $c \in \mathbb{K}$ が成立する。

$E_{e'} = c\hat{E}_{e'}$ の証明

- 上記をグレブナー基底論で証明するのは実は厄介
GB は、指定項消去後の結果式も消去に使うから。
- $E_{e'}$ の計算手順を利用すれば明快に証明できる：
 $E_{e'}$ の計算 $\Rightarrow E_{e'} = A_{e'}G + B_{e'}x^\delta H$ が定まり、
 $(A_{e'}, B_{e'})$ は定義より $E_{e'}$ に至る最短経路を示す。
- そこで、最短経路を辿って $\hat{E}_{e'}$ を計算すればよい
例えば、 $A_1 = \text{lmn}(A_1) + \text{rst}(A_1)$ 等と分割すれば、
 $\text{lmn}(A_1)G + \text{lmn}(B_1)H$ は $\text{Spol}(G, H)$ の倍数だ。

終結式の彼方 ... 何があるんだろう？

- 最初は興味本位：

$$G = g_d x^d + \cdots + g_0, \quad H = h_e x^e + \cdots + h_0$$

$\hat{\gamma} \notin \mathbb{K}$ に対し $\hat{\gamma} \mid P_{k-1}, A_k, B_k$ の場合あり

- T E S ($P_1 = G, P_2 = H, P_3, \dots, P_k \in \mathbb{K}[u]$)

$$\deg_x(A_k) < \deg_x(H), \quad \deg_x(B_k) < \deg_x(G)$$

- そこで, $P_{k+1} := \text{TrmElim}(P_{k-1}, P_k)$ を計算

$$\underline{\deg(A_{k+1}) = \deg(H)}, \quad \underline{\deg(B_{k+1}) = \deg(G)}$$

- ♠ そうか, **GB 基底計算同様**, 延々と続くんだ！

延々と続けると, **いいこと**があるかもな！

因みに Characteristic Set では

GB 基底法は **S 多項式生成** と **M 簡約** で与系 \mathcal{F} を変形していくが, **Char. Set 法** は, これら両演算の代わりに **擬除算 (Prem)** だけで \mathcal{F} を変形していく。算法としては両者は同じようだが, 結果は大きく異なる。

GB 法との違いは **イデアル所属問題** をみれば明白

\mathcal{F} の Char. Set を $\mathcal{C} = \{C_1, \dots, C_r\}$ とし,
 $\forall F \in \mathbb{K}[x, u]$ の \mathcal{C} による **擬除算簡約** を次式とする。

$$\text{lcf}(C_{i_1})^{e_1} \cdots \text{lcf}(C_{i_r})^{e_r} \times F = Q_1 C_{i_1} + \cdots + Q_r C_{i_r} + \tilde{F}$$

定理 $F \in \langle \mathcal{F} \rangle \implies \tilde{F} = 0$ ($\iff \tilde{F} = 0$ ではない)

文献

本講演は下記論文(投稿中)の最初の約 1/3 の纏めです
A Bridge between Euclid and Buchberger
(国際会議 SCSS2021 (held at RISC Linz) での招待講演)

残りの 2/3 は**多項式系**のグレブナー基底の各元の
小倍数を**S 多項式計算なし**で計算するという画期的
なものです。**奇想天外かつ簡単で強力**なアイデアの
てんこ盛りです。興味ある人は e-mail ください。
(なお、この研究での私の役割はほぼ終了しました)

謝辞

ご清聴ありがとうございました。

研究過程で、加古富士雄氏(前 奈良女子大学教授)、
稲葉 大樹氏(数学検定協会)、讃岐 勝氏(筑波大学)
の三氏に非常にお世話になりました。
深く感謝申し上げます。