階数制御を行う Matrix-F5 型のグレブナー基底計算法

Rank-Controlled Matrix-F5 Type Algorithm for Gröbner Basis

神戸大学 大学院 人間発達環境学研究科　　長坂 耕作 [*1]
Kosaku Nagasaka
Graduate School of Human Development and Environment, Kobe University

Abstract

In this talk, we briefly introduced our new polynomial representation used with a matrix-F5 type algorithm for computing a Gröbner basis. This approach allows us to control the rank range of specific rows of the Macaulay matrix, which is suitable for computing an approximate Gröbner basis for a set of polynomials whose coefficients may have a priori numerical errors.

1　はじめに

本講演では，行列を用いた Gröbner 基底の高速算法である F_4 アルゴリズム [Fau99] に基づいた，係数に誤差を含む多項式系の Gröbner 基底計算法として提案した構造化 Gröbner 基底計算アルゴリズム [Nag09, Nag11] の改善に資すると考えられる理論的な考察を行った。特に，厳密な（本稿では，誤差を含まない通常の問題をこのように表現する）Gröbner 基底の高速算法である F_5 アルゴリズム [Fau02] に対して，多項式環での解釈等を与えた野呂・横山 [野横 21] によるアルゴリズムを取り上げ，その構造化 Gröbner 基底への適用可能性を議論した長坂 [長 22] のアプローチに対する理論的裏付けが可能であることを示した。

注意 1 (厳密な計算への適用可能性)
本稿で議論している内容はすべて通常の *Gröbner* 基底計算を対象としているが，誤差を含む問題に適用するために厳密な問題では不要となる付加的な情報・計算を大量に求めている。そのため，F_4 や F_5 などのアルゴリズムを高速化するという観点からは，非常に遅くなる手続きを多数含むことに留意してほしい。◁

2　階数制御とは

本章では，タイトルに含まれる「階数制御」が何を意図するものであるかを説明しておく。以下では，広く知られていると思われる「部分終結式行列の階数」と「最大公約因子の次数」との関係を用いて階数制御の意図するところを説明した後に，Gröbner 基底計算における意図（「Macaulay 行列の階数」と「S 多項式が 0 に簡約されるか否か」）について説明する。

[*1] E-mail: nagasaka@main.h.kobe-u.ac.jp

2.1 多項式 GCD 計算での階数制御

$K[x]$ を体 K 上の多項式環とし，その多項式 $f(x), g(x) \in K[x]$ の最大公約因子（以後，GCD）について考える。ここでは簡単のため，これらの多項式の次数はともに n であり（つまり，$n = \deg(f) = \deg(g)$），かつ n は十分に大きいとする。$f(x)$ と $g(x)$ の r 次の部分終結式行列 $\mathrm{Syl}_r(f,g) \in K^{(2n-r)\times(2n-2r)}$ は次のように定義される。

$$\mathrm{Syl}_r(f,g) = \begin{pmatrix} C_{n-r-1}(f) & C_{n-r-1}(g) \end{pmatrix}^T$$

ここで $C_k(p)$ は，多項式 $p(x) \in K[x]$ の k 次の畳み込み行列であり，k 次の任意の多項式 $q(x)$ に対して $h(x) = p(x)q(x)$ とおけば，$C_k(p)\boldsymbol{q} = \boldsymbol{h}$ を満たす（$\boldsymbol{q}$ と $\boldsymbol{h}$ はそれぞれ $q(x)$ と $h(x)$ の密な係数ベクトルを表す）。このとき，部分終結式行列に関するよく知られている性質（$\mathrm{Syl}_r(f,g)$ が階数落ちする最大の整数を r とすれば，$f(x)$ と $g(x)$ の GCD の次数は $r+1$ である）から次のことを順次確定させられる。

- $\deg(\gcd(f,g)) = n$ の可能性（$f(x)$ と $g(x)$ の GCD の次数が n である可能性の判定）
  $n-1$ 次の部分終結式行列は，$f(x)$ と $g(x)$ の密な係数ベクトル（横ベクトル）をそれぞれ $\vec{f}$ と $\vec{g}$ とすれば次のような構造となっている。その階数は，仮定より多項式の次数が 1 以上なので，次のように $[1,2] \subset \mathbb{Z}$ の範囲（階数の変化の幅が高々1 である範囲）に含まれていることがわかる。

  $$1 \le \mathrm{rank} \left(\begin{array}{|l} \hline \bullet\vec{f} \\ \hline \bullet\vec{g} \\ \hline \end{array} \right) \le 2$$

  以下，この階数は 2 であったと仮定する。

- $\deg(\gcd(f,g)) = n-1$ の可能性（$f(x)$ と $g(x)$ の GCD の次数が $n-1$ である可能性の判定）
  同様に，$n-2$ 次の部分終結式行列は次のような構造となっており，その階数は，既に赤い部分の階数が 2 と判明していることから，次のように $[3,4] \subset \mathbb{Z}$ の範囲（階数の変化の幅が高々1 である範囲）に含まれることがわかる。

  $$3 \le \mathrm{rank} \left(\begin{array}{|l} \hline \bullet\vec{f} \\ \hline \quad \bullet\vec{f} \\ \hline \bullet\vec{g} \\ \hline \quad \bullet\vec{g} \\ \hline \end{array} \right) \le 4$$

  以下，この階数は 4 であったと仮定する。

- $\deg(\gcd(f,g)) = n-2$ の可能性（$f(x)$ と $g(x)$ の GCD の次数が $n-2$ である可能性の判定）
  同様に，$n-3$ 次の部分終結式行列は次のような構造となっており，その階数は，既に赤と青の部分の階数が 4 と判明していることから，次のように $[5,6] \subset \mathbb{Z}$ の範囲（階数の変化の幅が高々1 である範囲）に含まれることがわかる。

  $$5 \le \mathrm{rank} \left(\begin{array}{|l} \hline \bullet\vec{f} \\ \hline \quad \bullet\vec{f} \\ \hline \quad\quad \bullet\vec{f} \\ \hline \bullet\vec{g} \\ \hline \quad \bullet\vec{g} \\ \hline \quad\quad \bullet\vec{g} \\ \hline \end{array} \right) \le 6$$

  以下，この手続きを繰り返す限りにおいては，常に対象の部分終結式行列の階数を高々1 の変動の幅に抑え込むことが可能である。この何らかの性質を行列の階数で判定する際に「高々1 の変動の幅に階数を抑え込む」ことを本稿では階数制御と呼んでいる。

2.2 Gröbner 基底計算での階数制御

$R = K[\vec{x}] = [x_1, \ldots, x_d]$ を体 K 上の多項式環とし，R の元のうち冪積（power product）全体の集合を T とする。多項式 $f(\vec{x}) \in R$ の冪積 $t \in T$ の係数を $\mathrm{coef}_t(f)$ で表し，$f(\vec{x})$ の台（support）を $\mathrm{supp}(f) = \{\, t \in T \mid \mathrm{coef}_t(f) \neq 0 \,\}$ とする。有限集合 $F = \{f_1, \ldots, f_\ell\} \subset R$ に対して，その生成するイデアル $I = \langle F \rangle$ の Gröbner 基底を求めたいとする。このとき，本稿における Macaulay 行列を次のように定義する。

定義 1 (Macaulay 行列)
有限集合 $H = \{h_1, \ldots, h_\tau\} \subset R$ と T の項順序 $\prec$ に対して，H の台の和集合 $\{t_1, \ldots, t_\kappa\} = \bigcup_{h \in H} \mathrm{supp}(h) \subset T$ を項順序 $\prec$ で順序付けられたものとする（降順）。このとき，(i, j) 成分が $\mathrm{coef}_{t_j}(h_i)$ である τ 行 κ 列行列を H の ***Macaulay*** 行列と定義する。 ◁

なお，Macaulay 行列の掃き出しにより $I = \langle F \rangle$ の Gröbner 基底を計算する方法（[Laz83] など）では，定義内の H は $\{\, t \cdot f \mid f \in F,\, t \in T \,\}$ の部分集合となる。以下本稿においても，$\{\, t \cdot f \mid f \in F,\, t \in T \,\}$ の部分集合 H の Macaulay 行列を，単に Macaulay 行列と呼ぶ。

Gröbner 基底計算での階数制御とは，次の条件を満たす Macaulay 行列を構成することとする。

- S 多項式が 0 に単項簡約されるなら，Macaulay 行列は行階数が 1 だけ不足（row rank deficient by 1）
- S 多項式が 0 に単項簡約されないのなら，Macaulay 行列は行フルランク（row full rank）

このような行列を構成することは冒頭でも述べたが，通常の Gröbner 基底計算において必要性は薄い。特に，毎回の単項簡約の際に生成元のみから構成される Macaulay 行列を再構成することは，既存の掃き出し結果を再利用しないこととなり効率が悪い。しかしながら，係数に誤差を含む多項式系の Gröbner 基底計算においては，誤差の拡大を防ぐことやイデアルの次元に基づく係数の摂動を行うために，繰り返し異なる Macaulay 行列を構成することや，その行列の階数を制御することは重要となる。例えば，階数制御されていない冗長な行列を構成した場合，階数だけから（数値的には特異値などから）単項簡約結果が 0 であるか否かを判定することは難しい（実際，構造化 Gröbner 基底計算アルゴリズム [Nag11] では複雑な条件充足を求めている）。

上記の条件を満たす Macaulay 行列を構成することは，構造化 Gröbner 基底計算アルゴリズム [Nag11] で用いた F_4 アルゴリズム [Fau99] では難しい。前述の通り，既存の掃き出し結果を再利用すると生成元のみを用いた Macaulay 行列ではなくなってしまうことや，仮に掃き出し前の行列を再利用しても階数制御が困難となるからである（階数制御のためには，冗長な部分を削除したり別の生成元由来のものと交換したりする必要があるが，その正当性の保証を F_4 アルゴリズムはしていないため）。このため，長坂 [長 22] では F_5 アルゴリズム [Fau02] の一種である野呂・横山 [野横 21] によるアルゴリズムを用いることを提案していたが，理論的枠組みを示すに至っていなかった。本稿後半ではこのアプローチの正当性を説明する。

3 多項式環での signature based algorithm

本稿で必要となる範囲において，野呂・横山 [野横 21] によるアルゴリズムを簡単に紹介しておく。なお，このアルゴリズムにおいて用いられる基底候補の表現は通常の Buchberger アルゴリズムと同じく多項式環の元であるが，後述の加群の元を用いた表現を採用しているアルゴリズム [Sak20, Sak21] や，これらのトロピカル版と解釈可能なアルゴリズム [VY17, Vac15, VVY18] も必要に応じて参照されたい。

繰り返しとなるが，$R = K[\vec{x}] = [x_1, \ldots, x_d]$ を体 K 上の多項式環とし，R の元のうち冪積（power product）全体の集合を T とする。有限集合 $F = \{f_1, \ldots, f_\ell\} \subset R$ に対して，その生成するイデアル

アルゴリズム 1 signature based algorithm （野呂-横山 [野横 21]，抄）

入力: $F = \{f_1, \ldots, f_\ell\} \subset R$, compatible な R と R^ℓ の項順序 $\prec_R, \prec$
出力: $I = \langle F \rangle$ の $\mathfrak{S}$-Gröbner 基底

$G = F$, $S = \phi$, D: 擬正則ペアの集合（F の元のペアの部分集合）
while $D \neq \phi$ **do**
  $s = \min_\prec \{\tilde{\mathrm{sig}}(p) \mid p \in D\}$
  if $s'|s$ となる $s' \in S$ が存在しない **then**
    $P = \{m \cdot g \mid g \in G,\ m \in T,\ m \cdot \mathrm{sig}(g) = s\}$
    $m \cdot g \leftarrow \mathrm{argmin}_{m \cdot g \in P} \mathrm{lpp}(m \cdot g)$
    if $m \cdot g$ を主成分とする $p \in D$ が存在 **then**
      $r \leftarrow$ 擬正則ペア p の S 多項式の $\mathfrak{S}$-簡約の結果
      if $r = 0$ **then**
        $S \leftarrow S \cup \{s\}$
      else
        $G \leftarrow G \cup \{r\}$, $\mathrm{sig}(r) = s$, D の更新（r を含む擬正則ペアの追加）
      end if
    end if
  end if
  $D \leftarrow D \setminus \{p \in D \mid \tilde{\mathrm{sig}}(p) = s\}$
end while
return G

$I = \langle F \rangle$ の Gröbner 基底を求めたいとする。F に対して，R^ℓ を基本ベクトルの組 $\{\vec{e}_1, \ldots, \vec{e}_\ell\}$ を基底とする R-加群とし，R^ℓ から R への写像（加群の元を多項式に写す写像）を $\mathrm{poly} : R^\ell \to R$, $\vec{h} \mapsto \sum_{i=1}^{\ell} h_i f_i$ ($\vec{h} = (h_i) \in R^\ell$）で定める。$R^\ell$ の元のうち冪積全体の集合を M とする（$M = \bigcup_{i=1}^{\ell} T\vec{e}_i$）。$\prec_R$ を $T(R)$ の項順序とし，$\prec$ を $M(R^\ell)$ の加群項順序とする。ただし，$\prec_R$ と $\prec$ は compatible であるとする（即ち，$t, s \in T$ が $t \prec_R s$ を満たすならば，$t\vec{e}_i \prec s\vec{e}_i$ $(i = 1, \ldots, \ell)$ を満たす）。$f(\vec{x}) \in R$ と $\vec{h} \in R^\ell$ それぞれの非ゼロ係数をもつ冪積のうち，これらの順序（$\prec_R, \prec$）による最大順序のもの（先頭項）をそれぞれ $\mathrm{lpp}(f) \in T$ と $\mathrm{lpp}(\vec{h}) \in M$ で表す。以下の定義のもと，アルゴリズム 1 は $I = \langle F \rangle$ の $\mathfrak{S}$-Gröbner 基底を計算する。

定義 2 ((minimal) signature)
$f(\vec{x}) \in I \setminus \{0\}$ に対して，次式で定める $\mathrm{sig}(f)$ を $f(\vec{x})$ の ***signature*** と呼ぶ。

$$\mathrm{sig}(f) = \min_{\prec} \left\{ \mathrm{lpp}(\vec{h}) \,\middle|\, \vec{h} \in R^\ell, \mathrm{poly}(\vec{h}) = f \right\} \in M$$

◁

定義 3 ($\mathfrak{S}$-簡約と $\mathfrak{S}$-既約)
$f(\vec{x}) \in I$ の先頭項 $\mathrm{lpp}(f)$ を $g(\vec{x}) \in I$ で単項簡約する際，$\mathrm{sig}(f) \succ \mathrm{sig}(m \cdot g)$ $(m = \frac{\mathrm{lpp}(f)}{\mathrm{lpp}(g)})$ が成り立つとき **$\mathfrak{S}$-簡約**と呼ぶ（正確には $\mathfrak{S}$-*top*-簡約）。$f(\vec{x})$ を $\mathfrak{S}$-簡約する $g(\vec{x}) \in I$ が存在しないとき，**$\mathfrak{S}$-既約**という。◁

定義 4 ($\mathfrak{S}$-Gröbner 基底)
$G \subset I$ が，任意の $\mathfrak{S}$-既約な $h(\vec{x}) \in I$ に対し $g(\vec{x}) \in G$, $m \in T$ が存在して $\mathrm{lpp}(h) = m \cdot \mathrm{lpp}(g)$, $\mathrm{sig}(h) = m \cdot \mathrm{sig}(g)$ を満たすとき，G を I の ***$\mathfrak{S}$-Gröbner* 基底**と呼ぶ。◁

定義 5 (s 以下（未満）$\mathfrak{S}$-Gröbner 基底)
$s \in M$ に対し，$G \subset I = \langle F \rangle$ が，任意の $\mathfrak{S}$-既約で $\mathrm{sig}(h) \preceq s$（$\mathrm{sig}(h) \prec s$）を満たす $h(\vec{x}) \in I$ に対し $g(\vec{x}) \in G$, $m \in T$ が存在して $\mathrm{lpp}(h) = m \cdot \mathrm{lpp}(g)$, $\mathrm{sig}(h) = m \cdot \mathrm{sig}(g)$ を満たすとき，G を I の s **以下（未満）$\mathfrak{S}$-*Gröbner* 基底**と呼ぶ。 ◁

定義 6 (擬正則ペア)
$f(\vec{x}), g(\vec{x}) \in I$ の S 多項式 $c_f m_f \cdot f(\vec{x}) - c_g m_g \cdot g(\vec{x})$ $(c_f, c_g \in K,\ m_f, m_g \in T)$ が，$m_f \cdot \mathrm{sig}(f) \neq m_g \cdot \mathrm{sig}(g)$ を満たすとき，(f, g) を**擬正則ペア**と呼ぶ。このとき，$m_f \cdot \mathrm{sig}(f) \succ m_g \cdot \mathrm{sig}(g)$ ならば $m_f \cdot f(\vec{x})$ を，$m_f \cdot \mathrm{sig}(f) \prec m_g \cdot \mathrm{sig}(g)$ ならば $m_g \cdot g(\vec{x})$ を，擬正則ペアの**主成分**と呼ぶ。また，主成分に対応する $m_f \cdot \mathrm{sig}(f)$（または $m_g \cdot \mathrm{sig}(g)$）を擬正則ペアの ***guessed signature*** と呼び，$\tilde{\mathrm{sig}}(f, g)$ で表す。 ◁

4 Pivot 表現による signature based algorithm

本稿の目的は，アルゴリズム 1 の第 9 行目の分岐条件（$\mathfrak{S}$-簡約結果が 0 であるか否か）を，前述の階数制御された Macaulay 行列のみを用いて判定することである。このため，基底候補に含まれる多項式（初期の F に含まれる多項式だけでなく，その後に G に追加される多項式も含む）を，多項式環 R の元ではなく，はたまた R-加群 R^ℓ の元としてでもなく，下記で導入する Pivot 表現を用いて表現する。

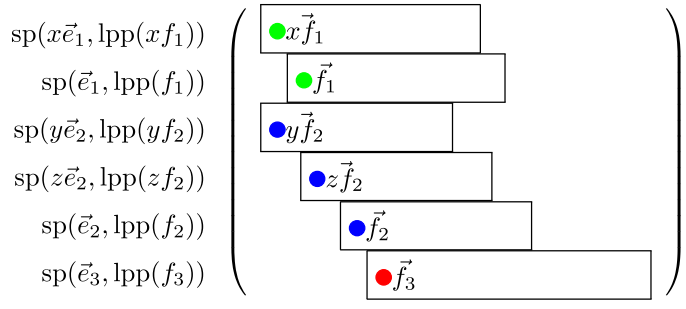
仮定 7 (lower finite な加群項順序)
Pivot 表現によるアルゴリズムでは，加群項順序 $\prec$ が *lower finite*（任意の元よりも順序が低い元は有限個）でなければならないため，以後，加群項順序 $\prec$ は *lower finite* であるとする。なお，*Schreyer* 順序 $\prec$ と全次数逆辞書式 $\prec_R$ の組は *lower finite* である。 ◁

4.1 Pivot 表現（多項式の部分空間表現）

行列の掃き出しを用いて Gröbner 基底を計算する方法（[Laz83, Fau99] など）では，掃き出し対象の行列の行ベクトルが，S 多項式を構成するペアの多項式や，S 多項式を単項簡約する簡約子（reductor）に対応する。繰り返しになるが本稿では，$\{ m \cdot f \mid f \in F,\ m \in T \}$ の部分集合 H の Macaulay 行列のみを Macaulay 行列と呼ぶ。逆説的な定義となるが，これら Macaulay 行列の個々の行ベクトルに対応する概念として，**single pivot** を導入する。

定義 8 (single pivot)
Macaulay 行列の行ベクトルに対応する多項式 $m \cdot f_i(\vec{x})$ の R-加群における表現 $m\vec{e}_i = \tilde{\mathrm{sig}}(m \cdot f_i)$ と，その行ベクトルの行主成分の列に対応する冪積 $t = \mathrm{lpp}(m \cdot f_i)$ のペアで表される $\mathrm{sp}(m\vec{e}_i, t) \in M \times T$ を ***single pivot*** と呼ぶ。また，このとき $m\vec{e}_i$ を *single pivot* の *(guessed) signature* と，t を先頭項と呼ぶ。 ◁

下記は，single pivot の概念図である。右側が Macaulay 行列を想定しており，左側に各行ベクトルに対応する single pivot を記載している。



注意 2
single pivot を $M \times T$ の元として表現することは冗長のように見える。実際には M の元は *signature* を，T の元は先頭項をそれぞれ表しており，*single pivot* ではどちらも同じ元に対応しているため冗長に見えるが，以後で導入する *reduced pivot* や *virtual pivot* では異なるため，この形式を用いている。 ◁

single pivot の有限集合 $\mathcal{S} \subset M \times T$ に対して，$\{\, \mathrm{poly}(m\vec{e}_i) \mid \mathrm{sp}(m\vec{e}_i, t) \in \mathcal{S} \,\}$ の Macaulay 行列を $\mathcal{M}(\mathcal{S})$ で，$\{\, m\vec{e}_i \mid \mathrm{sp}(m\vec{e}_i, t) \in \mathcal{S} \,\}$ の張る K 上の線形空間としての R^ℓ の部分空間を $\mathrm{span}(\mathcal{S}) \subset R^\ell$ で表す。この部分空間に含まれる元の多項式としての先頭項の集合として，$\mathcal{S}$ の先頭項集合 $\mathrm{lpps}(\mathcal{S})$ を定義する。即ち，$\mathrm{lpps}(\mathcal{S}) = \left\{ \mathrm{lpp}(\mathrm{poly}(\vec{h})) \,\middle|\, \vec{h} \in \mathrm{span}(\mathcal{S}) \right\}$ とする。$\mathcal{S}$ の各元 $\mathrm{sp}(m\vec{e}_i, t)$ がすべて異なる t を持てば，先頭項集合の要素数は $\mathcal{S}$ の要素数に一致する（$|\,\mathrm{lpps}(\mathcal{S})| = |\mathcal{S}|$）。$\mathcal{S}$ の台も同様に，部分空間に含まれる元の多項式としての台の和集合として $\mathrm{supp}(\mathcal{S})$ を定義する。即ち，$\mathrm{supp}(\mathcal{S}) = \bigcup_{\vec{h} \in \mathrm{span}(\mathcal{S})} \mathrm{supp}(\mathrm{poly}(\vec{h}))$ とする。

本稿の目的であるアルゴリズム 1 の第 9 行目の操作（擬正則ペアの S 多項式の $\mathfrak{G}$-簡約）を，階数制御された Macaulay 行列 $\mathcal{M}(\mathcal{S})$ で実現する場合，$G = F$ である限りにおいては，single pivot のみを用いて G を表現することが可能である。しかしながら，はじめて $\mathfrak{G}$-簡約結果が 0 とならなかった以後は G が変化し $G \neq F$ となるため，single pivot 以外の pivot 表現が必要となってくる。例えば，主成分を $f_1(\vec{x})$ とする擬正則ペア (f_1, f_2) の S 多項式の $\mathfrak{G}$-簡約において，簡単のため，簡約子が他に存在しなかったとする。図 1 は，この $\mathfrak{G}$-簡約結果が 0 にならなかった状況を表している。signature として $\mathrm{sig}(f_1)$（赤い丸印に対応）をもち，先頭項が $\mathrm{lpp}(f_2 - f_1)$（緑の丸印に対応）である多項式が G に追加されることになる。この様相を多項式環の元を直接用いて表現せず，single pivot のような表現を用いて表すため，以下の **reduced pivot** と **primary component link** を導入する。

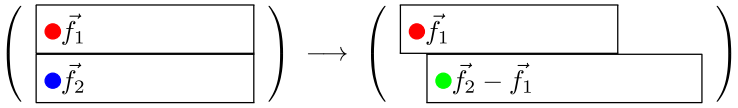


図 1: 擬正則ペアの S 多項式の掃き出しに関する様相（左: 掃き出し前，右: 掃き出し後）

定義 9 (reduced pivot)
Macaulay 行列 $\mathcal{M}(\mathcal{S})$ が階数制御されているような *single pivot* の有限集合 $\mathcal{S} \subset M \times T$ に対して，$U \subset \mathrm{lpps}(\mathcal{S})$ を $\mathcal{M}(\mathcal{S})$ の行階段形（*row echelon form*）に現れる既知の行主成分に対応する冪積集合とする。即ち，$|U| = |\,\mathrm{lpps}(\mathcal{S})|$ であるか $|U| = |\,\mathrm{lpps}(\mathcal{S})| - 1$ であるかを満たしている。$|U| = |\,\mathrm{lpps}(\mathcal{S})| - 1$ であるとき，$\mathcal{M}(\mathcal{S})$ の行階段形に現れる既知でない行主成分を含む行ベクトルを ***reduced pivot*** と呼び，$\mathrm{rp}(s, t) \in M \times T$ と表す。ここで，s は $\max_{\prec} \{\, s \mid \mathrm{sp}(s, t) \in \mathcal{S} \,\}$ であり，t は $\mathrm{lpps}(\mathcal{S}) \setminus U$ のただ一つの元である。 ◁

定義 10 (primary component link)
擬正則ペアの S 多項式の $\mathfrak{G}$-簡約に対応する階数制御された *Macaulay* 行列 $\mathcal{M}(\mathcal{S})$ により，*reduced pivot* として $\mathrm{rp}(s, t) \in M \times T$ が生じたとし，この擬正則ペアの主成分に対応する *single pivot* または *reduced pivot* を $p \in M \times T$ とする。このとき，$\mathrm{rlink}(p, \mathrm{rp}(s, t)) \in (M \times T)^2$ のことを ***primary component link*** と呼ぶ。また，この *primary component link* の p を *parent*，$\mathrm{rp}(s, t)$ を *child* と呼ぶ。 ◁

以上の定義により，図 1 においては，single pivot の集合 $\mathcal{S} = \{\mathrm{sp}(\vec{e}_1, \mathrm{lpp}(f_1)),\ \mathrm{sp}(\vec{e}_2, \mathrm{lpp}(f_2))\}$ から reduced pivot の集合 $\mathcal{R} = \{\mathrm{rp}(\vec{e}_1, \mathrm{lpp}(f_2 - f_1))\}$ が生成され，その関係性が primary component link の集合 $\mathcal{L} = \{\mathrm{rlink}(\mathrm{sp}(\vec{e}_1, \mathrm{lpp}(f_1)), \mathrm{rp}(\vec{e}_1, \mathrm{lpp}(f_2 - f_1)))\}$ として表現されることになる。色のついた丸印で表現するならば，$\mathcal{S} = \{$●, ●$\}$, $\mathcal{R} = \{$●$\}$, $\mathcal{L} = \{$●→●$\}$ となっている。この表現を用いてアルゴリズム 1 内の多項式を表現するため，次の **virtual pivot** を導入する。

定義 11 (virtual pivot)
single pivot の有限集合 $\mathcal{S}$，*reduced pivot* の有限集合 $\mathcal{R}$，*primary component link* の有限集合 $\mathcal{L}$ が次の条件を満たすとき，***virtual pivot*** と呼び $\mathrm{vp}(\mathcal{S},\mathcal{R},\mathcal{L})$ と表す。

1. $|\mathcal{S}| = |\,\mathrm{lpps}(\mathcal{S})|$ であり，$\mathrm{lpps}(\mathcal{S}) = \{\,t \mid \mathrm{sp}(s,t) \in \mathcal{S}\,\} \bigcup \{\,t \mid \mathrm{rp}(s,t) \in \mathcal{R}\,\}$
2. $|\mathcal{R}| = |\mathcal{L}|$ であり，$\forall c \in \mathcal{R},\ \exists p \in \mathcal{S} \bigcup \mathcal{R},\ \exists\,\mathrm{rlink}(p,c) \in \mathcal{L}$
3. $|\mathcal{S}| = 1$ かつ $\mathcal{R} = \mathcal{L} = \phi$ でなければ，$\exists\,\mathrm{rp}(s,t) \in \mathcal{R},\ t = \min_{\prec_R} \mathrm{lpps}(\mathcal{S})$

また，$\mathrm{sig}(\mathrm{vp}(\mathcal{S},\mathcal{R},\mathcal{L})) = \max_{\prec} \{\,s \mid \mathrm{sp}(s,t) \in \mathcal{S}\,\}$ とし，$\mathrm{lpp}(\mathrm{vp}(\mathcal{S},\mathcal{R},\mathcal{L})) = \min_{\prec_R} \mathrm{lpps}(\mathcal{S})$ と定義する。なお，条件 *1* または *3* が満たされていない場合は，***guessed virtual pivot*** と呼び $\tilde{\mathrm{vp}}(\mathcal{S},\mathcal{R},\mathcal{L})$ と表す。◁

条件 1 は，Macaulay 行列 $\mathcal{M}(\mathcal{S})$ が行フルランクであることと，$\mathcal{M}(\mathcal{S})$ の行階段形に現れる行主成分に対応する冪積がすべて $\mathcal{S} \bigcup \mathcal{R}$ に含まれていることを保証する。条件 2 は，$\mathcal{R}$ の元が擬正則ペアの S 多項式の $\mathfrak{S}$-簡約の結果に由来していることと，その情報を含むことを保証する。なお，primary component link において parent と child の signature は同一であるため，条件 2 は，signature 最大のものが $\mathcal{S}$ に含まれることを暗に含む。条件 3 の前半の条件は，single pivot そのものを表現していることに対応する。そうでない場合，$\mathfrak{S}$-簡約（$\mathfrak{S}$-top-簡約）に不要であることが自明な single pivot は $\mathcal{S}$ に含まれないことを意味する。結果として，$\mathrm{vp}(\mathcal{S},\mathcal{R},\mathcal{L})$ の表す多項式は，単元倍の不定性があって，$\vec{h} \in \mathrm{span}(\mathcal{S})$ かつ $\mathrm{lpp}(\mathrm{poly}(\vec{h})) = \min_{\prec_R} \mathrm{lpps}(\mathcal{S})$ を満たすものとなる。virtual pivot $p = \mathrm{vp}(\mathcal{S},\mathcal{R},\mathcal{L})$ に対して，p の表す多項式を $\mathrm{poly}(p)$ で表すこととする。

表記を簡単にするため，virtual pivot $p = \mathrm{vp}(\mathcal{S},\mathcal{R},\mathcal{L})$ と冪積 $m \in T$ に対して，これらの積 $m \cdot p$ を次のように定義する。single pivot と reduced pivot に対しては，$m \cdot \mathrm{sp}(s,t) = \mathrm{sp}(m \cdot s, m \cdot t)$ と $m \cdot \mathrm{rp}(s,t) = \mathrm{rp}(m \cdot s, m \cdot t)$ とする。そして，$m \cdot p = \mathrm{vp}(m\mathcal{S}, m\mathcal{R}, m\mathcal{L})$ とし，$m\mathcal{S} = \{\,\mathrm{sp}(m \cdot s, m \cdot t) \mid \mathrm{sp}(s,t) \in \mathcal{S}\,\}$, $m\mathcal{R} = \{\,\mathrm{rp}(m \cdot s, m \cdot t) \mid \mathrm{rp}(s,t) \in \mathcal{R}\,\}$, $m\mathcal{L} = \{\,\mathrm{rlink}(m \cdot p_1, m \cdot p_2) \mid \mathrm{rlink}(p_1,p_2) \in \mathcal{L}\,\}$ とする。なお，これらの演算は Macaulay 行列において，行ベクトルの各要素を左方向にシフトすることに対応している（同じ冪積 m に対して，各行ベクトルの各要素のシフト量は同じでないことに留意すること）。

4.2 $\mathfrak{S}$-簡約と Pivot 表現による階数制御

アルゴリズム 1 では，その第 9 行目の操作（擬正則ペアの S 多項式の $\mathfrak{S}$-簡約）を除き，signature (guessed signature) と 先頭項のみを用いた処理が行われている。このため，virtual pivot（Pivot 表現）でアルゴリズムを動作させるためには，$\mathfrak{S}$-簡約を virtual pivot に対応させる必要がある。以下では，アルゴリズム 1 における G は virtual pivot の集合であり，その初期値は $G = \{\,\mathrm{vp}(\{\mathrm{sp}(\vec{e}_i, \mathrm{lpp}(f_i))\}, \phi, \phi) \mid f_i \in F\,\}$ として定めたものとして扱う（実質的には，single pivot の集合である）。まず，virtual pivot による S 多項式について定義を行う。

定義 12 (virtual pivot による S 多項式)
$m_1 \cdot g_1$ を主成分とする擬正則ペア (g_1, g_2) の S 多項式（$\exists m_1, m_2 \in T,\ m_1 \cdot \mathrm{lpp}(g_1) = m_2 \cdot \mathrm{lpp}(g_2)$ とする）を，*guessed virtual pivot* を用いて $\tilde{\mathrm{vp}}(\mathcal{S},\mathcal{R},\mathcal{L})$ と表す。ここで，$g_1 = \mathrm{vp}(\mathcal{S}_1,\mathcal{R}_1,\mathcal{L}_1)$, $g_2 = \mathrm{vp}(\mathcal{S}_2,\mathcal{R}_2,\mathcal{L}_2)$ に対して，$\mathcal{S} = m_1\mathcal{S}_1 \bigcup m_2\mathcal{S}_2$, $\mathcal{R} = m_1\mathcal{R}_1 \bigcup m_2\mathcal{R}_2$, $\mathcal{L} = m_1\mathcal{L}_1 \bigcup m_2\mathcal{L}_2$ である。◁

実際の S 多項式に対応する R^ℓ の元が $\mathrm{span}(\mathcal{S}) = \mathrm{span}(m_1\mathcal{S}_1 \bigcup m_2\mathcal{S}_2)$ に含まれることは明らかであるが，このままでは Macaulay 行列 $\mathcal{M}(\mathcal{S})$ の階数制御を保証できず，かつ，$\mathfrak{S}$-簡約を行う G の簡約子に対応する行ベクトルも含まれないため不十分である。そこで，S 多項式の guessed virtual pivot をアルゴリズム 2 を用いて，$\mathfrak{S}$-簡約（階数制御された Macaulay 行列）に対応するよう更新する。

アルゴリズム 2 guessed virtual pivot による S 多項式の minimum signature representation

入力: 主成分を $m_1 \cdot g_1$ とする擬正則ペア (g_1, g_2), $s = m_1 \cdot \mathrm{sig}(g_1)$ 未満 $\mathfrak{S}$-Gröbner 基底 G
（主成分 $m_1 \cdot g_1$ でない方を $m_2 \cdot g_2$ とし，$g_1 = \mathrm{vp}(\mathcal{S}_1, \mathcal{R}_1, \mathcal{L}_1)$, $g_2 = \mathrm{vp}(\mathcal{S}_2, \mathcal{R}_2, \mathcal{L}_2)$ とする）

出力: 擬正則ペア (g_1, g_2) の minimum signature representation である guessed virtual pivot

1: $\tilde{\mathrm{vp}}(\mathcal{S}, \mathcal{R}, \mathcal{L}) \leftarrow \tilde{\mathrm{vp}}(m_1\mathcal{S}_1 \bigcup m_2\mathcal{S}_2,\ m_1\mathcal{R}_1 \bigcup m_2\mathcal{R}_2,\ m_1\mathcal{L}_1 \bigcup m_2\mathcal{L}_2)$, $L \leftarrow \mathrm{supp}(\mathcal{S})$
2: **while** $L \neq \phi$ **do**
3: $\quad t \leftarrow \min_{\prec_R} L$, $L \leftarrow L \setminus \{t\}$, $\mathcal{T} \leftarrow \left\{ p \in \mathcal{S} \bigcup \mathcal{R} \,\middle|\, \mathrm{lpp}(p) = t,\ \tilde{\mathrm{sig}}(p) \prec s,\ \nexists \mathrm{rlink}(p, c) \in \mathcal{L} \right\}$
4: $\quad$ **if** $\mathcal{T} = \phi$ **then**
5: $\quad\quad V \leftarrow \{\, m \cdot g \mid g \in G,\ m \in T,\ m \cdot \mathrm{sig}(g) \prec s,\ m \cdot \mathrm{lpp}(g) = t \,\}$
6: $\quad\quad$ **if** $V \neq \phi$ **then**
7: $\quad\quad\quad \mathrm{vp}(\mathcal{S}_r, \mathcal{R}_r, \mathcal{L}_r) \leftarrow \min_{\prec} V$, $L \leftarrow L \bigcup \mathrm{supp}(\mathcal{S}_r)$, $\mathcal{S} \leftarrow \mathcal{S} \bigcup \mathcal{S}_r$, $\mathcal{R} \leftarrow \mathcal{R} \bigcup \mathcal{R}_r$, $\mathcal{L} \leftarrow \mathcal{L} \bigcup \mathcal{L}_r$
8: $\quad\quad$ **end if**
9: $\quad$ **else**
10: $\quad\quad \tilde{p} = \mathrm{argmin}_{p \in \mathcal{T}} \tilde{\mathrm{sig}}(p)$, $\mathcal{T} \leftarrow \mathcal{T} \setminus \{\tilde{p}\}$
11: $\quad\quad$ **for** $p' \in \mathcal{T}$ **do**
12: $\quad\quad\quad \mathcal{S} \leftarrow \mathcal{S} \setminus \{p'\}$, $\mathcal{R} \leftarrow \mathcal{R} \setminus \{p'\}$, $\mathcal{L} \leftarrow \{\, \mathrm{rlink}(p, c) \in \mathcal{L} \mid c \neq p' \,\}$
13: $\quad\quad$ **end for**
14: $\quad\quad V \leftarrow \left\{\, m \cdot g \,\middle|\, g \in G,\ m \in T,\ m \cdot \mathrm{sig}(g) \prec \tilde{\mathrm{sig}}(\tilde{p}),\ m \cdot \mathrm{lpp}(g) = t \,\right\}$
15: $\quad\quad$ **if** $V \neq \phi$ **then**
16: $\quad\quad\quad \mathcal{S} \leftarrow \mathcal{S} \setminus \{\tilde{p}\}$, $\mathcal{R} \leftarrow \mathcal{R} \setminus \{\tilde{p}\}$, $\mathcal{L} \leftarrow \{\, \mathrm{rlink}(p, c) \in \mathcal{L} \mid c \neq \tilde{p} \,\}$
17: $\quad\quad\quad \mathrm{vp}(\mathcal{S}_r, \mathcal{R}_r, \mathcal{L}_r) \leftarrow \min_{\prec} V$, $L \leftarrow L \bigcup \mathrm{supp}(\mathcal{S}_r)$, $\mathcal{S} \leftarrow \mathcal{S} \bigcup \mathcal{S}_r$, $\mathcal{R} \leftarrow \mathcal{R} \bigcup \mathcal{R}_r$, $\mathcal{L} \leftarrow \mathcal{L} \bigcup \mathcal{L}_r$
18: $\quad\quad$ **end if**
19: $\quad$ **end if**
20: **end while**
21: **return** $\tilde{\mathrm{vp}}(\mathcal{S}, \mathcal{R}, \mathcal{L})$

定義 13 (minimum signature representation)
$m_1 \cdot g_1$ を主成分とする擬正則ペア (g_1, g_2) の S 多項式は，$\exists m_1, m_2 \in T,\ m_1 \cdot \mathrm{lpp}(g_1) = m_2 \cdot \mathrm{lpp}(g_2)$ を満たすとする。$\mathrm{poly}(g_1)$ と $\mathrm{poly}(g_2)$ の S 多項式を $r \in R$ とし，$\{\, \mathrm{poly}(g) \mid g \in G \,\}$ による $\mathfrak{S}$-簡約の結果を $\tilde{r} \in R$ とする。このとき，*guessed virtual pivot* $\tilde{\mathrm{vp}}(\mathcal{S}, \mathcal{R}, \mathcal{L})$ が次の条件を満たすとき，擬正則ペア (g_1, g_2) の ***minimum signature representation*** であるという。

1. $\exists \vec{h}, \vec{\tilde{h}} \in \mathrm{span}(\mathcal{S}),\ \mathrm{poly}(\vec{h}) = r,\ \mathrm{poly}(\vec{\tilde{h}}) = \tilde{r}$
2. $|\mathcal{S}| = |\{\, t \mid \mathrm{sp}(s, t) \in \mathcal{S} \,\} \bigcup \{\, t \mid \mathrm{rp}(s, t) \in \mathcal{R} \,\}| + 1$
3. $|\mathcal{R}| = |\mathcal{L}|$ であり，$\forall c \in \mathcal{R},\ \exists p \in \mathcal{S} \bigcup \mathcal{R},\ \exists \mathrm{rlink}(p, c) \in \mathcal{L}$
4. $\forall t \in \mathrm{supp}(\mathcal{S}) \bigcap \{\, m \cdot \mathrm{lpp}(g) \mid g \in G,\ m \in T,\ m \cdot \mathrm{sig}(g) \prec s \,\}, \exists p \in \mathcal{S} \bigcup \mathcal{R},\ \mathrm{lpp}(p) = t$
5. $\forall t \in \left\{ \mathrm{lpp}(p) \,\middle|\, p \in \mathcal{S} \bigcup \mathcal{R} \right\}, \left| \left\{ p \in \mathcal{S} \bigcup \mathcal{R} \,\middle|\, \mathrm{lpp}(p) = t \right\} \setminus \{\, p \mid \mathrm{rlink}(p, c) \in \mathcal{L} \,\} \right| = 1$

ここで，$g_1 = \mathrm{vp}(\mathcal{S}_1, \mathcal{R}_1, \mathcal{L}_1)$, $g_2 = \mathrm{vp}(\mathcal{S}_2, \mathcal{R}_2, \mathcal{L}_2)$ であり，$s = m_1 \cdot \mathrm{sig}(g_1)$ とする。 ◁

定理 14 (停止性)
アルゴリズム 2 は停止性をもつ。 ◁

証明 台集合（L）に含まれる冪積 t を消去する簡約子が新規に追加される際（第 7 行と第 17 行）は，加群項順序 $\prec$ 最小の簡約子が追加れる。仮に同じ冪積 t に対して，二度目のループがあったとしても，既に

最小の簡約子が追加されているため，第 5 行と第 14 行では $V = \phi$ となり，台集合（L）は増加しない。また，加群項順序 $\prec$ は lower finite であり，擬正則ペアの主成分の guessed signature よりも順序の低い先頭項をもつ簡約子も有限個である。よって，新たに追加される簡約子には限りがあるため，台集合（L）が増加し続けることはなく，アルゴリズム 2 は停止する。 ∎

定理 15 (正当性)
アルゴリズム 2 は擬正則ペア (g_1, g_2) の *minimum signature representation* を出力する。 ◁

証明 アルゴリズム 2 の出力 $\tilde{\mathrm{vp}}(\mathcal{S}, \mathcal{R}, \mathcal{L})$ が，定義 13 の 5 つの条件を満たすことの概略を示す（略証）。

1. $\exists \vec{h}, \vec{\tilde{h}} \in \mathrm{span}(\mathcal{S}),\ \mathrm{poly}(\vec{h}) = r,\ \mathrm{poly}(\vec{\tilde{h}}) = \tilde{r}$
$\mathcal{M}(\mathcal{S})$ の構成から S 多項式に対応する $\vec{h}$ が含まれることは明らかであるが，$\mathfrak{S}$-簡約後の既約な $\vec{\tilde{h}}$ が含まれることは，次のことから保証される。台集合 L の各元に対して，$\mathfrak{S}$-簡約可能な簡約子が存在する場合，第 7, 17 行目において行空間に追加されている。また，第 12, 16 行目では，冪積 t に対する簡約子を 1 つを除き削除しているが，s 未満 $\mathfrak{S}$-Gröbner 基底の性質から，冗長な簡約子を削除しても結果に影響は与えない。なお，reduced pivot を構成する簡約子の削除も，台集合 L に削除された簡約子の分も含めていることから，同理由により，行空間に影響は与えない。

2. $|\mathcal{S}| = |\{\, t \mid \mathrm{sp}(s,t) \in \mathcal{S} \,\} \bigcup \{\, t \mid \mathrm{rp}(s,t) \in \mathcal{R} \,\}| + 1$
第 1, 7, 17 行目の和集合の形成前には，それぞれが virtual pivot であることから，行空間の次元と single pivot の要素数は一致（$|\mathcal{S}| = |\{\, t \mid \mathrm{sp}(s,t) \in \mathcal{S} \,\} \bigcup \{\, t \mid \mathrm{rp}(s,t) \in \mathcal{R} \,\}|$ に準ずる）している。S 多項式を構成した直後（第 1 行目），少なくとも主成分に対応する冪積においては重複が発生しているため，差は「1 以上」ある。主成分に対応する部分以外で重複がなければ差は「1」となるが，それらの重複部分は第 12, 16 行目で削除が行われる（parent 要素は child 要素の冪積を表すことにも注意）。

3. $|\mathcal{R}| = |\mathcal{L}|$ **であり，** $\forall c \in \mathcal{R},\ \exists p \in \mathcal{S} \bigcup \mathcal{R},\ \exists\, \mathrm{rlink}(p,c) \in \mathcal{L}$
$\tilde{\mathrm{vp}}(\mathcal{S}, \mathcal{R}, \mathcal{L})$ が virtual pivot であれば，この条件は満たされるため，第 1 行目の冪積倍，第 1, 7, 17 行目の和集合の形成，第 12, 16 行目の部分集合の形成，の直後にも条件を満たしていることを示す必要がある。まず，冪積倍は $\mathcal{M}(\mathcal{S})$ における左シフトで順序関係も維持されるため，明らかに条件は満たしている。他の操作による変化は，s 未満 $\mathfrak{S}$-Gröbner 基底であることと，guessed signature の低い擬正則ペアから計算を行っていることから，$\mathrm{rlink}(p,c)$ となる c が重複することはない（一旦生成されれば，c に対応する簡約子が存在するため）。このことから，$\mathcal{R}$ と $\mathcal{L}$ の要素数は常に一致する。

4. $\forall t \in \mathrm{supp}(\mathcal{S}) \bigcap \{\, m \cdot \mathrm{lpp}(g) \mid g \in G,\ m \in T,\ m \cdot \mathrm{sig}(g) \prec s \,\},\ \exists p \in \mathcal{S} \bigcup \mathcal{R},\ \mathrm{lpp}(p) = t$
簡約子が追加されるたびに台集合 L を更新しており，行空間に含まれる冪積に対して簡約子が存在するならば，その簡約子は第 7, 17 行目において必ず追加されているため，この関係式は成立している。

5. $\forall t \in \left\{ \mathrm{lpp}(p) \,\middle|\, p \in \mathcal{S} \bigcup \mathcal{R} \right\},\ \left| \left\{ p \in \mathcal{S} \bigcup \mathcal{R} \,\middle|\, \mathrm{lpp}(p) = t \right\} \setminus \{\, p \mid \mathrm{rlink}(p,c) \in \mathcal{L} \,\} \right| = 1$
この関係式が成立しないならば，第 12, 16 行目で冗長な簡約子が削除されるため，成立している。

∎

注意 3 (lower finite の必要性)
アルゴリズム 2 において，台集合（L）の各冪積 t に対して，*signature* 最小となる簡約子を随時追加（または更新）している。実際には同じ t に対して簡約子の追加（または更新）が繰り返されることはないが，加群項順序が *lower finite* でない場合，台集合（L）が空集合になることを保証できない。通常のアルゴリズム 1 では，$\mathfrak{S}$-簡約（$\mathfrak{S}$-*top*-簡約）の手続きで用いる簡約子の先頭項は狭義減少列となるため，手続きは

有限停止性を有する。しかしながら，*virtual pivot* 表現における $\mathfrak{S}$-簡約では，$\mathrm{vp}(\mathcal{S}_r, \mathcal{R}_r, \mathcal{L}_r)$ が簡約子として追加される。このとき *virtual pivot* の性質から，$\mathcal{S}_r$ には t よりも多項式環における順序が高い先頭項をもつ *single pivot* が存在し得るため，台集合（L）に関して狭義減少列を構成できない。実際に，以下の系の *Schreyer* 順序と辞書式順序の組み合わせでは，アルゴリズム 2 は停止しない。

$$I = \langle xy^4 + yz^4 - 2x^2y - 3,\ y^4 + xy^2z + x^2 - 2xy + y^2 + z^2,\ -x^3y^2 + xyz^3 + y^4 + xy^2z - 2xy \rangle$$

なお，定理 15 の証明において，冪積による左シフト後に簡約子の交換が発生した場合にも同一の *reduced pivot* が生成されることの保証で，交換前の台集合に対する簡約子の充足性を必要としている。 ◁

4.3 計算例

次のイデアル $\langle f_1, f_2, f_3 \rangle \subset \mathbb{C}[x, y, z]$ を対象に，Schreyer 順序と全次数逆辞書式順序の組み合わせでの $\mathfrak{S}$-Gröbner 基底を，virtual pivot を用いて求める場合の計算例を示す。ただし，講演時の実装において，Schreyer 順序における基底添字の優先度を，大きな添字の基底ほど高い順序としていたことから，本報告でも本来の「小さな添字の基底ほど高い順序」ではなく，「大きな添字の基底ほど高い順序」とした計算結果であることに留意してほしい（つまり，f_1 と f_3 の添字が入れ替わっている結果となっている）。

$$\langle f_1 = -5x^2 + yz - x - 1,\ f_2 = 3xy + y^2 + 2x,\ f_3 = xz - 2z^2 + x - 3y \rangle$$

参考までに，実際の $\mathfrak{S}$-Gröbner 基底は次のとおりである。

$$\begin{aligned}
\{\ & xz - 2z^2 + x - 3y,\ 3xy + y^2 + 2x,\ 5x^2 - yz + x + 1,\ yz^2 - 20z^3 + 5y^2 - 29yz + 18z^2 + 27y - z - 1, \\
& y^2z + 120z^3 - 20y^2 + 174yz - 104z^2 - 156y + 6z + 6, \\
& 15y^3 + 3240z^3 - 559y^2 + 4680yz - 2808z^2 - 20x - 4185y + 162z + 180, \\
& 1560z^4 + 78768z^3 - 17140y^2 + 114129yz - 70866z^2 - 20x - 106386y + 4086z + 4026 \qquad \}
\end{aligned}$$

最初の擬正則ペアは $(y \cdot f_3,\ z \cdot f_2)$ となり，それぞれの先頭項に対応する部分に，f_1 は赤色，f_2 は青色，f_3 は緑色を用いて強調表示をすると，次のような $\mathcal{M}(\mathcal{S})$ が構成される（左側の行列）。各列の対応する冪積は左から $xyz, y^2z, yz^2, xy, y^2, xz, z^2, x, y$ となっている。この擬正則ペアの minimum signature representation である $\mathcal{M}(\mathcal{S})$ の掃き出しを行った結果，得られた新しい行主成分をもつ行ベクトルが右側のものである。

$$\begin{pmatrix}
0 & 0 & 0 & 0 & 0 & \textcircled{1} & -2 & 1 & -3 \\
\textcircled{1} & 0 & -2 & 1 & -3 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & \textcircled{3} & 1 & 0 & 0 & 2 & 0 \\
\textcircled{3} & 1 & 0 & 0 & 0 & 2 & 0 & 0 & 0
\end{pmatrix} \to \begin{pmatrix} 0 & \textcircled{1} & 6 & 0 & 10 & 0 & 4 & 0 & 6 \end{pmatrix}$$

結果として，紫色で先頭項を表している新たな多項式 f_4 に対応する virtual pivot として，

$$\mathrm{vp}\left(\{\mathrm{sp}(y\vec{e}_3, xyz),\ \mathrm{sp}(z\vec{e}_2, xyz)\},\ \{\mathrm{rp}(y\vec{e}_3, y^2z)\},\ \{\mathrm{sp}(y\vec{e}_3, xyz) \to \mathrm{rp}(y\vec{e}_3, y^2z)\}\right)$$

が得られたことになる。

次の擬正則ペアは $(x \cdot f_3,\ z \cdot f_1)$ となり，次のような $\mathcal{M}(\mathcal{S})$ が構成される（左側の行列）。各列の対応する冪積は左から $x^2z, xz^2, yz^2, z^3, x^2, xy, y^2, xz, yz, z^2, x, y, z, 1$ となっている。この擬正則ペアの minimum signature representation である $\mathcal{M}(\mathcal{S})$ の掃き出しを行った結果，得られた新しい行主成分をもつ行ベクト

ルが右側のものである。

$$\begin{pmatrix} 0 & 0\,0 & 0 & 0 & 0\,0 & \textcircled{1} & 0 & -2 & 1 & -3 & 0 & 0 \\ \textcircled{1} & -2\,0 & 0 & 1 & -3\,0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \textcircled{1}\,0 & -2 & 0 & 0\,0 & 1 & -3 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0\,0 & 0 & 0 & \textcircled{3}\,1 & 0 & 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0\,0 & 0 & \textcircled{-5} & 0\,0 & 0 & 1 & 0 & -1 & 0 & 0 & -1 \\ \textcircled{-5} & 0\,1 & 0 & 0 & 0\,0 & -1 & 0 & 0 & 0 & 0 & -1 & 0 \end{pmatrix} \to \begin{pmatrix} 0\,0\,\textcircled{1} & -20\,0\,0\,5\,0 & -29 & 18\,0 & 27 & -1 & -1 \end{pmatrix}$$

結果として，マゼンダで先頭項を表している新たな多項式 f_5 に対応する virtual pivot として，

$$\mathrm{vp}\left(\{\mathrm{sp}(x\vec{e}_3, x^2z), \mathrm{sp}(z\vec{e}_3, xz^2), \mathrm{sp}(z\vec{e}_1, x^2z)\},\ \{\mathrm{rp}(x\vec{e}_3, yz^2)\},\ \{\mathrm{sp}(x\vec{e}_3, x^2z) \to \mathrm{rp}(x\vec{e}_3, yz^2)\}\right)$$

が得られたことになる。

3 つ目の擬正則ペアは $(x \cdot f_2,\ y \cdot f_1)$ となり，次のような $\mathcal{M}(\mathcal{S})$ が構成される。各列の対応する冪積は左から $x^2y, xy^2, y^3, x^2z, xyz, y^2z, xz^2, yz^2, z^3, x^2, xy, y^2, xz, yz, z^2, x, y, z, 1$ となっている。この例では，同一の冪積に対応する行主成分をもつ行ベクトルが，擬正則ペアの主成分以外にも存在していることがわかる。掃き出し結果を再利用しないことから発生するもので，定理 15 の証明などが必要になる要因となっている。

$$\begin{pmatrix} 0 & 0\,0 & 0 & 0\,0 & 0 & 0 & 0 & 0 & 0 & 0 & \textcircled{1} & 0 & -2 & 1 & -3 & 0 & 0 \\ 0 & 0\,0 & \textcircled{1} & 0\,0 & -2 & 0 & 0 & 1 & -3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0\,0 & 0 & \textcircled{1}\,0 & 0 & -2 & 0 & 0 & 1 & -3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0\,0 & 0 & 0\,0 & \textcircled{1} & 0 & -2 & 0 & 0 & 0 & 1 & -3 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0\,0 & 0 & 0\,0 & 0 & 0 & 0 & 0 & 0 & \textcircled{3} & 1 & 0 & 0 & 0 & 2 & 0 & 0 \\ \textcircled{3} & 1\,0 & 0 & 0\,0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \textcircled{3}\,1 & 0 & 0\,0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0\,0 & 0 & \textcircled{3}\,1 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0\,0 & 0 & 0\,0 & 0 & 0 & 0 & \textcircled{-5} & 0 & 0 & 0 & 1 & 0 & -1 & 0 & 0 & -1 \\ \textcircled{-5} & 0\,0 & 0 & 0\,1 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0\,0 & \textcircled{-5} & 0\,0 & 0 & 1 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & -1 & 0 \end{pmatrix}$$

この擬正則ペアの minimum signature representation である $\mathcal{M}(\mathcal{S})$ の掃き出しを行った結果，得られた新しい行主成分をもつ行ベクトルが次のものであり，その下側の virtual pivot が茶色で先頭項を表している新たな多項式 f_6 に対応するものである。

$$\begin{pmatrix} 0 & 0 & \textcircled{1} & 0 & 0 & 0 & 0 & 0 & 216 & 0 & 0 & -\frac{559}{15} & 0 & 312 & -\frac{936}{5} & -\frac{4}{3} & -279 & \frac{54}{5} & 12 \end{pmatrix}$$

$$\mathrm{vp}\left(\{\mathrm{sp}(x\vec{e}_2, x^2y), \mathrm{sp}(y\vec{e}_2, xy^2), \mathrm{sp}(y\vec{e}_1, x^2y)\},\ \{\mathrm{rp}(x\vec{e}_2, y^3)\},\ \{\mathrm{sp}(x\vec{e}_2, x^2y) \to \mathrm{rp}(x\vec{e}_2, y^3)\}\right)$$

以後，計算は続いていくことになるが，冗長であることと紙面の関係もあり省略する。

5　まとめと今後の課題

本報告では，野呂・横山 [野横 21] によるアルゴリズムにおける多項式表現を変更し，入力多項式のみが現れる Macaulay 行列の階数制御を行うことで，$\mathfrak{S}$-Gröbner 基底を求めるアルゴリズムの提案を行った。このアルゴリズムでは，virtual pivot という表現により，擬正則ペアが必要か不要かを Macaulay 行列の階数が 1 変化する否かに帰着させた。これにより，入力多項式の係数を摂動させる必要のある近似 Gröbner 基底計算アルゴリズムなどの改善が見込まれる。しかしながら，現時点においては，lower finite な順序を用いる必要があり，辞書式順序での計算を実現できていないことが，今後の課題となっている。

5.1 近似 Gröbner 基底計算への応用

構造化 Gröbner 基底の近似計算アルゴリズム [Nag11] では，F_4 アルゴリズム [Fau99] に基づいていたため，誤差により次元の下がった（Macaulay 行列の階数が上がった）多項式系の係数摂動を最後に一括して行う必要があった。この必要性は，すべての S 多項式の計算を完了させるまでは，誤差を含む入力多項式のみに基づいて（なんとか）計算を進めることを求めており，計算可能な系の拡大に大きな課題が残った。

本報告での階数制御を実現した virtual pivot による signature based algorithm と，近似 GCD 向けに開発した SLRA Interpolation[Nag23, Nag25] を組み合わせることで，逐次的な係数摂動を可能とする構造化 Gröbner 基底の近似計算アルゴリズムが実現可能である。アルゴリズムの概略のみ述べる。まず，$\mathfrak{S}$-簡約の際は Macaulay 行列が階数制御されていることから，0 に簡約される否かの判定は安定的に可能である。以下の計算例では，階数制御により 1 つ以外の行主成分が確定している情報を活用した Householder 変換に基づく QR 分解と特異値分解に基づく SLRA を併用することで，0 簡約される可能性が高い場合は係数摂動を実施している。すべての係数摂動は連動し，計算済みの virtual pivot や 0 簡約の性質を変化させないことが必要であるため，その部分の実現に SLRA Interpolation で用いたブロック対角行列向け SLRA を入れ子構造で使用する（これを SNLRA と呼んでいる）。最終的にすべての擬正則ペアの計算が完了した段階で，virtual pivot から実際の多項式表現を得るため，確定している行主成分の情報に基づいて，最小二乗法を利用する。なお，すべての計算は Mathematica 上に実装して実験をしている。

例 1 (Example 3 [Nag11])
次の多項式系 ex_3 は，構造化 *Gröbner* 基底の論文 *[Nag11]* の *Example 3* で使われている。

$$ex_3 = \{0.002 + 1.01x^2 - 2.09y^2,\ 3.06xy + 4.03x^2y,\ 0.504x^2 + 1.504xy + 2.04x^2y - 1.02y^2\}$$

イデアル $\langle ex_3 \rangle$ の全次数辞書式順序（$x \succ y$）の構造化 *Gröbner* 基底として，次の集合が得られる。

$$\{1.58287\texttt{e-13} + 1.01198x^2 - 2.08901y^2,\ -7.57713\texttt{e-14}y + 0.365673xy + y^3\}$$

◁

例 2 (Example 1,2 [Nag11])
次の多項式系 ex_3 は，構造化 *Gröbner* 基底の論文 *[Nag11]* の *Example 1* と *Example 2* で使われている。

$$ex_{1,2} = \{x^3 + x^2y^2,\ x^2y^2 - y^3,\ 1.000001x^2 - x^2y + 0.999999y^2 + xy^2\}$$

イデアル $\langle ex_{1,2} \rangle$ の辞書式順序（$x \succ y$）の構造化 *Gröbner* 基底として，次の集合が得られる。

$$\begin{cases} -3.47964\texttt{e-18}y^2 - y^3 + 9.07052\texttt{e-14}y^4 + 8.99276\texttt{e-16}y^5 + y^6, \\ xy^2 - 3.21114\texttt{e-16}y^3 + y^4, \\ x^2 + 0.999999y^2 - 9.02731\texttt{e-14}y^3 - 0.999999y^4 - 0.999998y^5 \end{cases}$$

辞書式順序に対しては，本報告のアルゴリズムの有限停止性は無保証となるが，この計算例では停止し上記の結果を得ることが出来る。なお，元論文が辞書式順序のため，辞書式順序を用いた計算例とした。 ◁

謝　　辞

This work was supported by JSPS KAKENHI Grant Number 19K11827 and 24K14823.

参 考 文 献

[Fau99] Jean-Charles Faugére. A new efficient algorithm for computing Gröbner bases (F_4). *J. Pure Appl. Algebra*, 139(1-3):61–88, 1999. Effective methods in algebraic geometry (Saint-Malo, 1998).

[Fau02] Jean-Charles Faugère. A new efficient algorithm for computing Gröbner bases without reduction to zero (F_5). In *ISSAC 2002—Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation*, pages 75–83. ACM, New York, 2002.

[Laz83] D. Lazard. Gröbner bases, Gaussian elimination and resolution of systems of algebraic equations. In *Computer algebra (London, 1983)*, volume 162 of *Lecture Notes in Comput. Sci.*, pages 146–156. Springer, Berlin, 1983.

[Nag09] Kosaku Nagasaka. A study on Gröbner basis with inexact input. In *CASC 2009—Proceedings of the 11th International Workshop on Computer Algebra in Scientific Computing*, volume 5743 of *Lecture Notes in Comput. Sci.*, pages 247–258. Springer, Berlin, 2009.

[Nag11] Kosaku Nagasaka. Computing a structured Gröbner basis approximately. In *ISSAC 2011—Proceedings of the 36th International Symposium on Symbolic and Algebraic Computation*, pages 273–280. ACM, New York, 2011.

[Nag23] Kosaku Nagasaka. SLRA interpolation for approximate GCD of several multivariate polynomials. In *ISSAC 2023—Proceedings of the 48th International Symposium on Symbolic and Algebraic Computation*, pages 470–479. ACM, New York, 2023.

[Nag25] Kosaku Nagasaka. Approximate GCD of several multivariate sparse polynomials based on SLRA interpolation. *J. Symbolic Comput.*, 127:(in press), 2025.

[Sak20] Kosuke Sakata. Simple signature-based algorithms with correctness and termination. *Communications of JSSAC*, 4:33–49, 2020.

[Sak21] Kosuke Sakata. *Efficient signature-based algorithms for computing Gröbner bases*. Ph.D. Thesis. Graduate School of Environmental and Information Science, Yokohama National University, 2021.

[Vac15] Tristan Vaccon. Matrix-F5 algorithms and tropical Gröbner bases computation. In *ISSAC'15—Proceedings of the 2015 ACM International Symposium on Symbolic and Algebraic Computation*, pages 355–362. ACM, New York, 2015.

[VVY18] Tristan Vaccon, Thibaut Verron, and Kazuhiro Yokoyama. On affine tropical F5 algorithms. In *ISSAC'18—Proceedings of the 2018 ACM International Symposium on Symbolic and Algebraic Computation*, pages 383–390. ACM, New York, 2018.

[VY17] Tristan Vaccon and Kazuhiro Yokoyama. A tropical F5 algorithm. In *ISSAC'17—Proceedings of the 2017 ACM International Symposium on Symbolic and Algebraic Computation*, pages 429–436. ACM, New York, 2017.

[長 22] 長坂耕作. 近似 Gröbner 基底の逐次算法に向けて（再訪）. 京都大学数理解析研究所講究録, 2224:95–102, 2022.

[野横 21] 野呂正行 and 横山和弘. Risa/Asir における signature based algorithm の実装について. 京都大学数理解析研究所講究録, 2185:139–148, 2021.