冗長な線形制約を伴う近似 Gröbner 基底計算法

On Computing Approximate Gröbner Bases with Redundant Linear Constraints

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 a new approach to computing an approximate Gröbner basis with redundant linear constraints on the coefficients of given polynomials. This work aims to relax the assumptions of, and extend, our matrix-F5-type numerical algorithm to handle non-simple, non-orthogonal coefficient structures.

1　はじめに

本講演では，係数に誤差を含む多項式系の Gröbner 基底計算法に関して検討中の取り組みを報告した。以前に提案した近似 Gröbner 基底計算法 [Nag09, Nag11] を，signature based algorithm[Fau02, 野横 21, Nor24] に基づいて改善した Matrix-F5 型の Gröbner 基底計算法 [長 22, 長 25] による近似 Gröbner 基底計算法には，大きく 2 つの要改善点が存在する。本講演では，係数に含まれる誤差の構造に対して仮定されていた直交性などの条件を緩和する方法について紹介した。以下，前提となる Matrix-F5 型の Gröbner 基底計算法と，それに基づく近似 Gröbner 基底について簡単に述べたのち，条件緩和に関する取り組みを紹介する。

1.1　Matrix-F5 型の Gröbner 基底計算法

簡単に，Matrix-F5 型の Gröbner 基底計算法 [長 25] について述べる。体 K 上の多項式環 $R = K[\vec{x}] = K[x_1, \ldots, x_d]$ の元のうち冪積（power product）全体の集合を T，多項式 $f(\vec{x}) \in R$ の冪積 $t \in T$ の係数を $\mathrm{coef}_t(f)$，$f(\vec{x})$ の台（support）を $\mathrm{supp}(f) = \{\, t \in T \mid \mathrm{coef}_t(f) \neq 0 \,\}$ と表す。イデアルの生成系として有限集合 $F = \{f_1, \ldots, f_\ell\} \subset R$ が与えられ，その生成するイデアル $I = \langle F \rangle$ の Gröbner 基底を求めるものとする。Matrix-F5 型では，次のように定義される Macaulay 行列を用いる。

定義 1 (Macaulay 行列)
有限集合 $H = \{h_1, \ldots, h_\tau\} \subset R$ と T の項順序 $\prec_R$ 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 $\prec_R$ 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。 ◁

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

Matrix-F5 型アルゴリズムは，signature based algorithm[野横 21, Nor24] に基づいているため，その最小限の枠組みを導入する。イデアルの生成系 F に対して，R^ℓ を基本ベクトルの組 $\{\vec{e}_1,\dots,\vec{e}_\ell\}$ を基底とする R-加群，R^ℓ の元のうち冪積全体の集合を M とする（$M=\bigcup_{i=1}^{\ell} T\vec{e}_i$）。多項式環の項順序を $\prec_R$ とし，$\prec$ を $M(R^\ell)$ の加群項順序とする。ただし，$\prec_R$ と $\prec$ は以下に定義する compatible かつ lower finite であるとする（lower finite は，signature based algorithm には不要であるが，Matrix-F5 型計算法に必須の仮定）。

定義 2 (compatible)
任意の $t,s\in T$ に対して，$t\prec_R s$ ならば $t\vec{e}_i\prec s\vec{e}_i$ $(i=1,\dots,\ell)$ であるとき，$\prec_R$ と $\prec$ は ***compatible*** であるという。 ◁

定義 3 (lower finite)
加群項順序 $\prec$ に関して，任意の元よりも順序が低い元が有限個ならば，$\prec$ は ***lower finite*** であるという。◁

signature based algorithm 及び Matrix-F5 型計算法が求めるものは，実際には Gröbner 基底というよりも，以下で定義される $\mathfrak{S}$-Gröbner 基底である。以下では，$f(\vec{x})\in R$ と $\vec{h}\in R^\ell$ それぞれの非ゼロ係数をもつ冪積のうち，対応する順序（$\prec_R,\prec$）による最大順序のもの（先頭項）を $\mathrm{lpp}(f)\in T$ と $\mathrm{lpp}(\vec{h})\in M$ で表す。また，R^ℓ から R への写像を $\mathrm{poly}:R^\ell\to R,\ \vec{h}\mapsto\sum_{i=1}^{\ell}h_if_i$ （$\vec{h}=(h_i)\in R^\ell$）で定める。

定義 4 ((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 5 ($\mathfrak{S}$-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 6 ($\mathfrak{S}$-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。 ◁

実際に $\mathfrak{S}$-Gröbner 基底を signature based algorithm を用いて求めるには，以下の擬正則ペアという概念が必要となる。また，signature based algorithm に基づく，Matrix-F5 型アルゴリズムでは，擬正則ペアの $\mathfrak{S}$-簡約を直接計算するのではなく，対応する（階数制御された）Macaulay 行列を構成し，その階数により代替する。アルゴリズム 1 は，実際の Matrix-F5 型アルゴリズムとなるが，本稿では階数制御された Macaulay 行列の構成部分に関係する部分は省略する（[長 25] を参照のこと）。

定義 7 (擬正則ペア)
$f(\vec{x}),g(\vec{x})\in I$ の S 多項式 $c_fm_f\cdot f(\vec{x})-c_gm_g\cdot g(\vec{x})$ $(c_f,c_g\in K,\ m_f,m_g\in T)$ 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，$\mathrm{gsig}(f,g)$ で表す。 ◁

定義 8 (階数制御)
Macaulay 行列 $\mathcal{M}$ が次の条件を満たすならば，擬正則ペア (f,g) に関して**階数制御**されているという。

- (f,g) の S 多項式が 0 に $\mathfrak{S}$-簡約されるなら，$\mathcal{M}$ は行数よりもちょうど 1 だけ小さい行階数をもつ。
- (f,g) の S 多項式が 0 に $\mathfrak{S}$-簡約されないのなら，$\mathcal{M}$ は行数と同じ行階数をもつ。 ◁

アルゴリズム 1 Matrix-F5 型アルゴリズム（抄）

入力: $F = \{f_1, \ldots, f_\ell\} \subset R$, compatible かつ lower finite 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 = φ, D: 擬正則ペアの集合（F の元のペアの部分集合）
while D ≠ φ do
  s = min_≺{gsig(p) | p ∈ D}
  if s'|s となる s' ∈ S が存在しない then
    P = {m · g | g ∈ G, m ∈ T, m · sig(g) = s}
    m · g ← argmin_{m·g∈P} lpp(m · g)
    if m · g を主成分とする p ∈ D が存在 then
      M ← 擬正則ペア p に対応する階数制御された Macaulay 行列
      if M の行階数が行数に一致しない then
        S ← S ∪ {s}
      else
        r ← 擬正則ペア p の S 多項式の 𝔖-簡約の結果（M の行簡約結果から得られる）
        G ← G ∪ {r}, 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 ← D \ {p ∈ D | gsig(p) = s}
end while
return G
```

1.2 Matrix-F5 型の近似 Gröbner 基底計算法

現時点において，近似 Gröbner 基底という概念は固定化されておらず，大きく分けると 2 種類に分類されることが知られている [SK07]。本稿で取り扱う近似 Gröbner 基底は，与えられたイデアルの生成系 $F = \{f_1, \ldots, f_\ell\}$ の多項式の係数には誤差が含まれているという前提のもとで，その生成するイデアル $I = \langle F \rangle$ の Gröbner 基底を，誤差を考慮した上で求める問題である。F_4 アルゴリズムに基づき提案した構造化 Gröbner 基底 [Nag11] では，行空間の基底が Gröbner 基底を与える Macaulay 行列を構成し，係数の誤差により大きくなっているであろう階数を，小さな摂動で修正（階数を小さく）した結果の Gröbner 基底を求めることとしていた。しかしながら，摂動前（誤差をそのまま含む）の状態から構成した Macaulay 行列の性質が，摂動により変化しないことを保証する条件が厳しいという課題があった。Matrix-F5 型アルゴリズムに基づく近似 Gröbner 基底では，事後的に条件を満たす必要性を排除し，許容度の範囲内で結果（計算経路）が変わらないことを保証することとした。

定義 9 (構造化 𝔖-Gröbner 基底)
有限多項式集合 $F = \{f_1, \ldots, f_\ell\} \subset R$，係数ベクトルの結合から多項式への線形写像 $\mathcal{F} : K^n \to R^\ell$，初期ベクトル $\overrightarrow{c_{init}} \in K^n$ は， $F = \mathcal{F}(\overrightarrow{c_{init}})$ を満たすとする。このとき， $G \subset R$ が許容度 $\varepsilon \in \mathbb{R}_{\geq 0}$ でのイデアル $I = \langle F \rangle$ の**構造化 𝔖-*Gröbner* 基底**とは，$\overrightarrow{c_{perturb}} \in K^n$ が存在し次を満たすことをいう。

- G は $\langle \mathcal{F}(\overrightarrow{c_{perturb}}) \rangle$ の $\mathfrak{S}$-*Gröbner* 基底であり，$\| \overrightarrow{c_{perturb}} - \overrightarrow{c_{init}} \|_2 = \varepsilon$ を満たす。
- G の各先頭項および計算過程の *Macaulay* 行列の階数は，$\| \overrightarrow{c} - \overrightarrow{c_{init}} \|_2 \leq \varepsilon$ なる $\overrightarrow{c} \in K^n$ で極小。 ◁

実際に構造化 Gröbner 基底を計算する方法を簡潔に述べる。アルゴリズム 1 の階数制御された Macaulay 行列を常に与えられた生成系 F の多項式のみから構成（詳細は [長 25] を参照）することで，$\mathcal{F}$ を K^n から階数制御された Macaulay 行列への写像に拡張することができる。これにより，階数の最小化（階数制御などの諸条件から階数は最大でも 1 しか落ちない）と先頭項の最小化は，構造化低階数近似（SLRA, Structured Low-Rank Approximation）問題に帰着させられる。定義 9 の極小条件を満たすため，計算過程において現れる Macaulay 行列の最小化された階数は，以後の計算過程でも維持する必要があり，複数の SLRA を同時に解く必要がある。複数の SLRA を同時に解く方法としては，ブロック対角行列を用いた 1 つの SLRA に帰着する方法 [Nag25] などがある。

例 1 (近似 Gröbner 基底（構造化 $\mathfrak{S}$-Gröbner 基底）の計算例)
Faugère と *Liang[FL11]* に掲載されている次の生成系 F_ϵ を取り上げる。$\epsilon \in \mathbb{R}_{\geq 0}$ はパラメータである。

$$F_\epsilon = \left\{4x^2 + y^2 - 4,\ 4\epsilon xy + 15y^2 - 12\right\} \subset \mathbb{C}[x, y].$$

イデアル $\langle F_\epsilon \rangle$ の全次数逆辞書式順序（$x \succ_R y$）に関する *Gröbner* 基底は，$\epsilon \neq 0$ ならば，以下の $G_{\epsilon\neq 0}$ となり，$\epsilon = 0$ ならば，以下の $G_{\epsilon=0}$ となる。これらは誤差を含まない厳密な結果である。

$$G_{\epsilon\neq 0} = \left\{xy + \frac{15}{4\epsilon}y^2 - \frac{3}{\epsilon},\ x^2 + \frac{1}{4}y^2 - 1,\ y^3 + \frac{48\epsilon}{225 + 4\epsilon^2}x - \frac{180 + 16\epsilon^2}{225 + 4\epsilon^2}y\right\}$$
$$G_{\epsilon=0} = \left\{x^2 - \frac{4}{5},\ y^2 - \frac{4}{5}\right\}$$

Matrix-F5 型アルゴリズムに基づく方法で，イデアル $\langle F_{1.0\mathtt{e}\text{-}2}\rangle$ と $\langle F_{1.0\mathtt{e}\text{-}3}\rangle$ の近似 *Gröbner* 基底を *Schreyer* 加群順序で求めた結果が次の $G_{\varepsilon=1.0\mathtt{e}\text{-}2}$ と $G_{\varepsilon=1.0\mathtt{e}\text{-}3}$ である。

$$G_{\varepsilon=1.0\mathtt{e}\text{-}2} = \left\{4.0x^2 - 3.2,\ 15.0y^2 - 12.0\right\},\ \varepsilon = 4.0\mathtt{e}\text{-}3$$
$$G_{\varepsilon=1.0\mathtt{e}\text{-}3} = \left\{0.004xy + 15.0y^2 - 12.0,\ 4.0x^2 + y^2 - 4.0,\ 1.0y^3 + 0.00021333x - 0.8y\right\},\ \varepsilon \approx 1.0\mathtt{e}\text{-}13$$

従来の F_4 に基づく近似 *Gröbner* 基底アルゴリズム *[Nag11]* では，計算経路保証条件を満たすことができなかったが，参考までに出力は次のとおりである（当時の実装は簡約に未対応）。許容度を大きくしても，厳密な結果の $G_{\epsilon\neq 0}$ にはたどり着けない（*artificial discontinuity* と呼ばれるものに対応する）。

$$\{1.0xy + 3750.0y^2 - 3000.0,\ 1.0x^2 - 0.00012435xy - 0.21632y^2 - 0.62694,\ 1.0y^3 + 0.00021333x - 0.8y\}$$

変数順序を $y \succ_R x$ としても，*Matrix-F5* 型アルゴリズムに基づく方法では次の結果が得られる。

$$G_{\varepsilon=1.0\mathtt{e}\text{-}2} = \left\{1.0x^2 - 0.8,\ 15.0y^2 - 12.0\right\},\ \varepsilon \approx 4.0\mathtt{e}\text{-}3$$
$$G_{\varepsilon=1.0\mathtt{e}\text{-}3} = \left\{xy - 15000.0x^2 + 12000.0,\ 15.0y^2 + 60.0x^2 - 60.0,\ 1.0x^3 - 5.333\mathtt{e}\text{-}5y - 0.8x\right\},\ \varepsilon \approx 3.4\mathtt{e}\text{-}14$$

◁

2　冗長な線形制約への対応

Matrix-F5 型に基づく近似 Gröbner 基底計算法には，大きく 2 つの要改善点が存在する。1 つが，加群順序と項順序は compatible かつ lower-finite でなければならないという点である。compatible は signature based algorithm の要件であり，Matrix-F5 型として新たに追加されている lower-finite の条件を削除することが望まれるが，本稿では取り上げない。本稿での改善点は，もう 1 つの要改善である定義 9 で許されている摂動の形式が，

- $\mathcal{F} : K^n \to K[\vec{x}]^\ell$ （線形写像）かつ
- $\mathcal{F}^{-1}$ が存在し，$\mathcal{F}^{-1}$ は F の係数ベクトルの結合（つまり，成分 = 係数）

に限定されているものを，任意の affine 写像に緩和したいというものである。

例 2 (任意の affine 写像への緩和)
Matrix-F5 型に基づく近似 *Gröbner* 基底計算法が対応している写像（係数ベクトルとなる線形写像）は，

$$\mathcal{F} : \mathbb{R}^9 \ni (c_1, \ldots, c_9) \mapsto \{c_1x^2 + c_2y^2 + c_3,\ c_4x^2y + c_5xy,\ c_6x^2y + c_7x^2 + c_8xy + c_9y^2\} \in \mathbb{R}[x, y]^3$$

のような形式のものであるが，次のような一般の *affine* 写像に緩和したい。

$$\begin{aligned}\mathcal{F} : \mathbb{R}^6 \ni (c_1, \ldots, c_6) \mapsto \quad & \{c_1 + c_2x^2 + (c_3 - c_4)y^2,\ (c_1 + c_2 - 1.0135)x^3 + c_4xy + c_5x^2y, \\ & c_6x^2 + (0.5c_4 - c_1)xy + (c_4 - c_3 - 3.05)x^2y - c_2y^2\} \qquad \in \mathbb{R}[x, y]^3\end{aligned}$$

◁

2.1 現行手法が一般の affine 写像に直接は対応していない背景

入力の多項式の係数に誤差を含む場合を想定した代数的な問題において，最も研究が進んでいる近似 GCD の主流の定義では，許容度（摂動の大きさ）は係数ベクトルの摂動量とされる。定義 9 の写像は，近似 GCD の扱いをそのまま近似 Gröbner に持ち込んだものであり，扱いやすい大きな特徴をもっている。例えば，写像が次のような場合を考える。

$$\mathcal{F} : \mathbb{R}^9 \ni (c_1, \ldots, c_9) \mapsto \{c_1x^2 + c_2y^2 + c_3,\ c_4x^2y + c_5xy,\ c_6x^2y + c_7x^2 + c_8xy + c_9y^2\} \in \mathbb{R}[x, y]^3$$

このとき，2 つ目と 3 つ目の多項式の S 多項式に対応する階数制御された Macaulay 行列は，次のように直交した生成系をもつ部分空間に属する。

$$\begin{pmatrix} c_6 & c_7 & c_8 & c_9 & 0 \\ c_4 & 0 & c_5 & 0 & 0 \\ 0 & c_1 & 0 & c_2 & c_3 \end{pmatrix} \in \mathbb{R} \begin{pmatrix} 0&0&0&0&0 \\ 0&0&0&0&0 \\ 0&1&0&0&0 \end{pmatrix} + \mathbb{R} \begin{pmatrix} 0&0&0&0&0 \\ 0&0&0&0&0 \\ 0&0&0&1&0 \end{pmatrix} + \mathbb{R} \begin{pmatrix} 0&0&0&0&0 \\ 0&0&0&0&0 \\ 0&0&0&0&1 \end{pmatrix} + \mathbb{R} \begin{pmatrix} 0&0&0&0&0 \\ 1&0&0&0&0 \\ 0&0&0&0&0 \end{pmatrix}$$

$$+\mathbb{R} \begin{pmatrix} 0&0&0&0&0 \\ 0&0&1&0&0 \\ 0&0&0&0&0 \end{pmatrix} + \mathbb{R} \begin{pmatrix} 1&0&0&0&0 \\ 0&0&0&0&0 \\ 0&0&0&0&0 \end{pmatrix} + \mathbb{R} \begin{pmatrix} 0&1&0&0&0 \\ 0&0&0&0&0 \\ 0&0&0&0&0 \end{pmatrix} + \mathbb{R} \begin{pmatrix} 0&0&1&0&0 \\ 0&0&0&0&0 \\ 0&0&0&0&0 \end{pmatrix} + \mathbb{R} \begin{pmatrix} 0&0&0&1&0 \\ 0&0&0&0&0 \\ 0&0&0&0&0 \end{pmatrix}$$

実際の近似 Gröbner 基底の計算時には，階数制御された Macaulay 行列に関する SLRA を解く必要がある。SLRA 自体は以下の定義からも，必ずしも前述のシンプルな線形写像に限定されていないが，実際に SLRA の解を求めるアルゴリズムにおいては，構造を指定する affine 空間に対応する正規直交基底を用いるものが多い。このため，定義 9 の写像では係数ベクトルに対応する線形写像のみとしている。

定義 10 (構造化低階数近似（SLRA, Structured Low-Rank Approximation）)
$p \times q$ 行列の集合を $K^{p\times q}$，階数 r を持つ $p \times q$ 行列の集合を $K_r^{p\times q}$ とし，$\mathcal{S} \subset K^{p\times q}$ を $K^{p\times q}$ の *affine* 部分空間とする。このとき， $M \in \mathcal{S}$ と $r \in \mathbb{N}$ に対し，$\|M - M^*\|_F$ を小さくする $M^* \in \mathcal{S} \cap K_r^{p\times q}$ を求めよ。なお，$\|\cdot\|_F$ で *Frobenius* ノルムを表す。 ◁

2.2 一般の affine 写像への要件緩和

SLRA の解法において正規直交基底が求められることを脇に置き，本来どのような問題を解こうとしているのかを改めて確認する。$\mathcal{F}: K^n \to K[\vec{x}]^\ell$ の各 Macaulay 行列への自然な拡張を，各 Macaulay 行列 $\mathcal{M}_i \in K^{r_i \times c_i}$ $(i = 1, \ldots, s)$ に対して，

$$\mathcal{F}_i : K^n \to K^{r_i \times c_i} \ (i = 1, \ldots, s)$$

とすれば，各 Macaulay 行列 $\mathcal{M}_i$ は次のように表せる。これは $\mathcal{F}$ が一般の affine 写像であっても成立する。

$$\mathcal{F}_i(\vec{c}) = B_{i,0} + \sum_{j=1}^{n} c_j B_{i,j},\ \vec{c} = (c_j) \in K^n,\ B_{i,j} \in K^{r_i \times c_i}$$

定義 9 の求める極小化を行うために必要な計算は，次のような最適化問題となる。

$$\min_{\vec{c} \in K^n} \| \overrightarrow{c} - \overrightarrow{c_{init}} \|_2 \ \text{ s.t. } \operatorname{rank}(\mathcal{F}_i(\vec{c})) < r_i \ (i = 1, \ldots, s)$$

2.2.1 SLRA として解く場合（従来の方法）

affine 空間の生成系 $B_{i,j}$ が直交基底（従来の方法で対応済のケース）の場合，$B_{i,j}$ を正規化し正規直交基底に変形する。変形後の正規直交基底を $\tilde{B}_{i,j} = \mu_{i,j} B_{i,j}$ とおけば，$\mathcal{F}_i(\vec{c}) = B_{i,0} + \sum_{j=1}^{n} c_j \mu_{i,j}^{-1} \tilde{B}_{i,j}$ と表せる。このとき，SLRA の目的関数は $\sum_{i,j} (c_j \mu_{i,j}^{-1})^2$ となり，本来の目的関数 $\| \overrightarrow{c} - \overrightarrow{c_{init}} \|_2$ の結果とは異なるものの，$\mathcal{M}_i$ のパラメータ成分分布が均一なら概ね同一となることが期待される。

一方，生成系 $B_{i,j}$ が冗長（直交性を有しない，または従属）な場合，$B_{i,j}$ を基底かつ正規直交化する必要がある。この場合，生成系に含まれる行列の個数が変化し得るし，結果の正規直交基底は，$\tilde{B}_{i,j} = \sum \mu_{i,j,k} B_{i,k}$ のように表現されることから，最小化の目的関数が本来の目的関数からかなり変化する可能性が高い。

2.2.2 SLRA を STLS に書き換えて双線形制約付き二乗和最小化問題へ

近似 GCD も SLRA に帰着可能な問題であるが，Kaltofen らの近似 GCD アルゴリズム [KYZ06] では，SLRA を構造化行列最小二乗問題（STLS, Structured Total Least Squares）に書き換えて解いている。定義 9 に求められる SLRA では，階数制御された Macaulay 行列が対象となり，階数が最大でも 1 しか落ちないことから，次のように STLS として書き換え可能である。

$$\begin{aligned} \operatorname{rank}(\mathcal{F}_i(\vec{c})) < r_i \quad \Longleftrightarrow \quad & \exists \vec{x}_i,\ A_i(\vec{c})\vec{x}_i = \vec{b}_i(\vec{c}),\ \mathcal{M}_i = \left(A_i(\vec{c}) \,\middle|\, \vec{b}_i(\vec{c})\right) \\ & A_i(\vec{c}) = A_{i,0} + \textstyle\sum_{j=1}^{n} c_j A_{i,j},\ \vec{b}_i(\vec{c}) = \vec{b}_{i,0} + \sum_{j=1}^{n} c_j \vec{b}_{i,j} \end{aligned}$$

これらの STLS を同時に解く必要があるため，最終的には次のような双線形制約付き二乗和最小化問題に帰着される。ここで，m は各 $\vec{x}_i$ の要素数の総和を，$\cdot^T$ は行列の転置を表す。説明変数 $\vec{q}$ は，縦ベクトルの結合を $\operatorname{stack}(\vec{v}, \vec{u}) := (\vec{v}^T\ \vec{u}^T)^T$ で表すとして，$\vec{q} = \operatorname{stack}(\vec{c}, \vec{x})$, $\vec{x} = \operatorname{stack}(\vec{x}_1, \ldots, \vec{x}_s)$ となる。

$$\min_{\vec{q} \in K^{n+m}} \sum_{j=1}^{n} c_j^2 \ \text{ s.t. } \ A_i(\vec{c})\vec{x}_i = \vec{b}_i(\vec{c}) \ (i = 1, \ldots, s)$$

直接的な SLRA の場合と異なり，目的関数と制約式が分離されているため，次のように生成系をベクトル化してスタックした行列 Y の特異値分解 $U\Sigma V^T$ により，生成系を正規直交化できる。なお，$U_{i,j}$ は U から $B_{i,j}$ 相当を抜き出した逆像を表す。

$$\min \vec{c}^T \vec{c} = \min \vec{c'}^T T^T T \vec{c'} \ \text{ s.t. } \ A'_i(\vec{c'})\vec{x'}_i = \vec{b'}_i(\vec{c'}) \ (i = 1, \ldots, s)$$

$$B_{i,0}+\sum_{j=1}^{n} c'_j U_{i,j} = \left(A'_i(\vec{c'}) \,\middle|\, \vec{b'}_i(\vec{c'})\right),\ \vec{q'} = \mathrm{stack}(\vec{c'}, \vec{x'}),\ \vec{x'} = \mathrm{stack}(\vec{x'}_1, \ldots, \vec{x'}_s)$$

$$U\Sigma V^T = Y,\ U = (\vec{u}_1\ \cdots\ \vec{u}_{n'}),\ \vec{c'} = \Sigma V^T \vec{c},\ T = V\Sigma^{-1}$$

$$Y = (\vec{g}_1\ \cdots\ \vec{g}_n) \in \mathbb{R}^{(\sum_{i=1}^{s} r_i c_i)\times n},\ \vec{g}_j = \mathrm{stack}(\mathrm{vect}(B_{1,j}), \ldots, \mathrm{vect}(B_{n,j}))$$

2.3 一般の affine 写像の場合における解法の選択

解くべき問題は，双線形制約付き二乗和最小化問題であり，逐次二次計画法（SQP, Sequential Quadratic Programming）や信頼領域付き Gauss-Newton 法などで解ける [Ber16, FL02, NW06, Ste83]。特に，今回の問題では目的関数がベクトルの要素の二乗和となっていることから，Hessian が疎なスカラー行列 $2I$ となる。一方で，特異値分解などを用いて，生成系の正規直交化を行った場合は，目的関数が複雑化し Hessian は密な行列 T^TT となる。以下の数値実験では，SQP における Hessian は近似せず直接計算（双線形なので軽量）を行い，二次計画部分問題は零空間を用いて KKT 条件を解く方法を採用し，ステップサイズはラインサーチ（フィルタ）とし，制約条件の充足を優先するために Feasibility Restoration Phase も用いた。Gauss-Newton 法については，Hessian は近似式を用い，信頼領域などの閾値は相対的に設定し，Jacobian が特異な場合は打ち切り共役勾配法を用い，ステップの受け入れ基準はメリット関数を使用することとした。なお，これらの手法選択に理論的な背景はなく，比較的実装しやすく展開しやすい一般的な手法を選択し，Mathematica 12 に実装し実験を行った。

2.4 計算例と効果検証

まず，従来の方法でも求めることのできる冗長でない次の写像を取り上げる。

$$\mathcal{F} : \mathbb{R}^9 \ni (c_1, \ldots, c_9) \mapsto \{c_2x^2 + c_3y^2 + c_1,\ c_5x^2y + c_4xy,\ c_8x^2y + c_6x^2 + c_7xy + c_9y^2\} \in \mathbb{R}[x, y]^3$$

$$\overrightarrow{c_{init}} = (0.002, 1.01, -2.09, 3.06, 4.03, 0.504, 1.504, 2.04, -1.02)$$

Schreyer 加群順序と全次数辞書式順序の組合せで，構造化 $\mathfrak{S}$-Gröbner 基底を計算したところ，結果として求まる基底の構造は同じであったが，摂動は異なる結果となった（表 1）。

続いて，線形写像でなく冗長である次の affine 写像について取り上げる。

$$\begin{aligned}\mathcal{F} : \mathbb{R}^6 \ni (c_1, \ldots, c_6) \mapsto \quad & \{c_1 + c_2x^2 + (c_3 - c_4)y^2,\ (c_1 + c_2 - 1.0135)x^3 + c_4xy + c_5x^2y,\\ & c_6x^2 + (0.5c_4 - c_1)xy + (c_4 - c_3 - 3.05)x^2y - c_2y^2\} \qquad \in \mathbb{R}[x, y]^3\end{aligned}$$

$$\overrightarrow{c_{init}} = (0.002, 1.01, -2.09, 3.06, 4.03, 0.504)$$

表 1: 冗長でない写像の場合の摂動量

アルゴリズム	生成系を直接使用	生成系を正規直交化
Cazdow[Cad88]	0.0333222	0.0333222
NewtonSLRA[SS16]	0.0333223	0.0333223
GNTR	0.0333308	0.0334912
SQP	0.0333308	0.0334912

表 2: 線形写像でなく冗長である場合の摂動量

アルゴリズム	生成系を直接使用	生成系を正規直交化
Cazdow	–	0.0703648*
NewtonSLRA	–	0.070618*
GNTR	0.0568261	0.0749769
SQP	0.0568261	0.0749769

$\star$ は収束してないもの（1024 回）

Schreyer 加群順序と全次数辞書式順序の組合せで，構造化 $\mathfrak{S}$-Gröbner 基底を計算した。結果得られた摂動量は表 2 の通りである。計算結果を例示すると，摂動後の $\mathcal{F}(\overrightarrow{c_{pertub}})$ として，

$$\{1.0135x^2 - 5.07433y^2,\ 3.02247xy + 4.04867x^2y,\ 0.502735x^2 + 1.51124xy + 2.02433x^2y - 1.0135y^2\}$$

が得られ，構造化 $\mathfrak{S}$-Gröbner 基底 G は次のようなものであった。

$$G = \{1.0y^2,\ 1.0xy,\ 1.0135x^2\}$$

最後に，冗長ではないが線形写像でない次の affine 写像について取り上げる。

$$\begin{aligned}\mathcal{F} : \mathbb{R}^6 \ni (c_1, \ldots, c_6) \mapsto \quad & \{c_1 + c_2x^2 + c_3y^2,\ (c_1 - 0.002)x^3 + c_4xy + c_5x^2y,\\ & c_6x^2 + 0.5c_4xy - c_3x^2y - c_2y^2\} \qquad \in \mathbb{R}[x, y]^3\end{aligned}$$

$$\overrightarrow{c_{init}} = (0.002, 1.01, -2.09, 3.06, 4.03, 0.504)$$

Schreyer 加群順序と全次数辞書式順序の組合せで，構造化 $\mathfrak{S}$-Gröbner 基底を計算した。結果得られた摂動量は表 3 の通りである。計算結果を例示すると，摂動後の $\mathcal{F}(\overrightarrow{c_{pertub}})$ として，

$$\{0.002{+}1.01043x^2{-}2.03027y^2,\ 3.05905xy{+}4.06054x^2y,\ 0.502872x^2{+}1.52952xy{+}2.03027x^2y{-}1.01043y^2\}$$

が得られ，構造化 $\mathfrak{S}$-Gröbner 基底 G は次のようなものであった。

$$G = \{0.002 + 1.01043x^2 - 2.03027y^2,\ -0.000243994 - 0.00098509y + 0.374933xy + 1.0y^3\}$$

謝　　辞

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

表 3: 線形写像でなく冗長でない場合の摂動量

アルゴリズム	生成系を直接使用	生成系を正規直交化
Cazdow	0.0670971*	0.0670971*
NewtonSLRA	0.0670976	0.0670976
GNTR	0.0671063*	0.0671024*
SQP	0.0671063†	0.0671024†

$\star$ は未収束（1024 回または領域半径下限到達），$\dagger$ は精度不足

参 考 文 献

[Ber16] Dimitri P. Bertsekas. *Nonlinear programming*. Athena Scientific Optimization and Computation Series. Athena Scientific, Belmont, MA, third edition, 2016.

[Cad88] J.A. Cadzow. Signal enhancement-a composite property mapping algorithm. *IEEE Transactions on Acoustics, Speech, and Signal Processing*, 36(1):49–62, 1988.

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

[FL02] Roger Fletcher and Sven Leyffer. Nonlinear programming without a penalty function. *Math. Program.*, 91(2):239–269, 2002.

[FL11] Jean-Charles Faugère and Ye Liang. Pivoting in extended rings for computing approximate Gröbner bases. *Math. Comput. Sci.*, 5(2):179–194, 2011.

[KYZ06] Erich Kaltofen, Zhengfeng Yang, and Lihong Zhi. Approximate greatest common divisors of several polynomials with linearly constrained coefficients and singular polynomials. In *ISSAC 2006*, pages 169–176. ACM, New York, 2006.

[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.

[Nag25] Kosaku Nagasaka. Approximate GCD of several multivariate sparse polynomials based on SLRA interpolation. *J. Symbolic Comput.*, 127:102368, 2025.

[Nor24] Masayuki Noro. Signature-based algorithm under non-compatible term orders and its application to change of ordering. *J. Comput. Algebra*, 12:Paper No. 100027, 9, 2024.

[NW06] Jorge Nocedal and Stephen J. Wright. *Numerical optimization*. Springer Series in Operations Research and Financial Engineering. Springer, New York, second edition, 2006.

[SK07] Tateaki Sasaki and Fujio Kako. Computing floating-point Gröbner bases stably. In *Proceedings of the 2007 International Workshop on Symbolic-Numeric Computation*, SNC '07, page 180–189, New York, NY, USA, 2007. Association for Computing Machinery.

[SS16] Éric Schost and Pierre-Jean Spaenlehauer. A quadratically convergent algorithm for structured low-rank approximation. *Found. Comput. Math.*, 16(2):457–492, 2016.

[Ste83] Trond Steihaug. The conjugate gradient method and trust regions in large scale optimization. *SIAM J. Numer. Anal.*, 20(3):626–637, 1983.

[長 22] 長坂耕作. 近似 Gröbner 基底の逐次算法に向けて（再訪）. In 研究集会 *Computer Algebra – Theory and Applications*, volume 2224 of 京都大学数理解析研究所講究録, pages 95–102. 京都大学数理解析研究所, 2022.

[長 25] 長坂耕作. 階数制御を行う matrix-f5 型のグレブナー基底計算法. In 研究集会 *Computer Algebra – Foundations and Applications*, volume 2320 of 京都大学数理解析研究所講究録, pages 187–199. 京都大学数理解析研究所, 2025.

[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. In 研究集会 *Computer Algebra – Theory and Applications*, volume 2185 of 京都大学数理解析研究所講究録, pages 139–148. 京都大学数理解析研究所, 2021.