

# 二変数多項式の近似 GCD

## Approximate GCD of Bivariate Polynomials

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 introduce our newly developed approach for finding approximate GCD of bivariate polynomials, whose size of matrix appeared in the algorithm is much smaller than the well-known algorithms based on several matrix decompositions, and resulting size of perturbations is moderately small.

## 1 はじめに

本報告では、二変数多項式の近似 GCD アルゴリズムにおける課題を克服する新しいアプローチについて取り扱います。近似 GCD は、互いに素である多項式を摂動させて、自明でない GCD を持つ状態にさせるアルゴリズムで、何らかの誤差の影響で互いに素になってしまった多項式本来の性質を求めようとするものです。一般に、一変数多項式の近似 GCD のアルゴリズムには、広義の意味で行列分解に基づく方法（最適化を含む）と、誤差を含まない多項式向けの Euclid の互除法に基づく方法とがあります（例えば、Maple に含まれている QRGCD アルゴリズム [CWZ04] は QR 分解に基づくものです）。これらのアルゴリズムを二変数多項式や多変数多項式向けに拡張する場合、行列分解に基づく前者のアルゴリズムでは、取り扱う行列のサイズが変数の個数に関して指数関数的に増大します。一方で、互除法に基づく後者のアルゴリズムでは、Hensel 構成などの手法（モジュラー算法や補間法など）で、変数の復元をすることになり、結果として得られる摂動量（入力多項式と最終的に得られた近似 GCD を持つ多項式との距離）が急速に拡大することになります。本稿では、これら二者の課題を両者の中間となるアプローチにより解決しようとする試みについて報告を行います。まず、本稿で扱う近似 GCD は次の定義に基づきます。そのため、指定した次数  $d$  に対して、摂動量をなるべく小さくしつつ、計算時間を短くすることが課題となります。

**定義 1 (近似 GCD (指定次数に対する摂動量最小化問題))**

変数  $\vec{x} = \{x_1, \dots, x_\ell\}$  に関する実数係数多項式の集合  $F = \{f_1, \dots, f_n\} \subset \mathbb{R}[\vec{x}]$  と正整数  $d \in \mathbb{N}$  に対して、多項式  $\Delta_{f_1}(\vec{x}), h_1(\vec{x}), \dots, \Delta_{f_n}(\vec{x}), h_n(\vec{x}) \in \mathbb{R}[\vec{x}]$  が存在して、全次数  $d$  の多項式  $g(\vec{x}) \in \mathbb{R}[\vec{x}]$  が以下を満たすならば、 $g(\vec{x})$  を全次数  $d$  の  $F$  の近似 GCD と定義する ( $\text{tdeg}(\cdot)$  は全次数を表す)。

$$f_i(\vec{x}) + \Delta_{f_i}(\vec{x}) = h_i(\vec{x})g(\vec{x}), \text{tdeg}(\Delta_{f_i}) \leq \text{tdeg}(f_i) \quad (i = 1, \dots, n).$$

また、このとき以下の量（全ての係数を並べたベクトルの 2 ノルムの相対変化量）を摂動量と呼ぶ。

$$\|(\|\Delta_{f_1}\|_2, \dots, \|\Delta_{f_n}\|_2)\|_2 / \|(\|f_1\|_2, \dots, \|f_n\|_2)\|_2$$

<

---

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

## 1.1 二変数の近似 GCD における課題

誤差を考慮する必要のない通常の GCD アルゴリズムについて簡単に紹介します。一変数多項式の GCD はよく知られている Euclid の互除法で求めることができますが、一般に、二変数多項式または多変数多項式の場合に直接 Euclid の互除法を使うことは行われません。 $\mathbb{R}[x_1]$  における互除法を二変数以上の多項式に直接拡張した場合、 $\mathbb{R}(x_2, \dots, x_\ell)[x_1]$  における互除法となり、有理関数体上の計算が必要で、多くの場合、中間式膨張と呼ばれる現象（入力多項式と実際に求まる GCD に比べて、計算途中に現れる式が爆発的に大きくなること）が発生し、効率的ではないためです。このため、多くのアルゴリズムでは、一変数多項式の GCD を求める問題に帰着し、一変数多項式としての GCD から Hensel 構成や補間法などにより本来の GCD を構成します [Bro71, MY73, Zip79]。これらのアルゴリズムでは、与えられた多項式を摂動させる必要がありませんので、図 1 のように変数や係数の復元が容易に行うことができます。

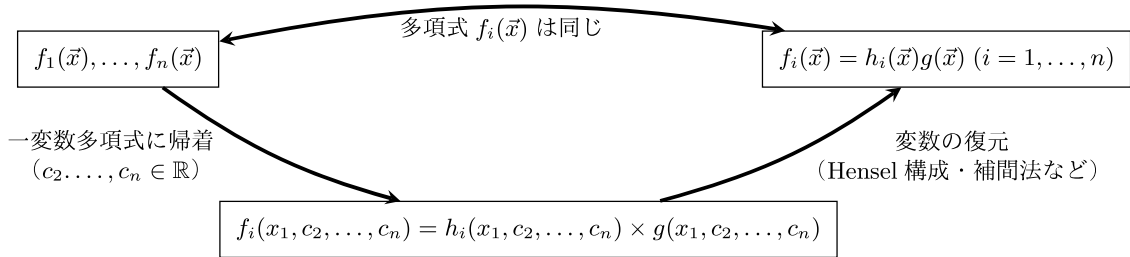


図 1: 一変数多項式に帰着して求めた GCD から本来の GCD を得る図式

一方、係数部分に誤差を含むであろう多項式を扱う近似 GCD の計算においては、一変数多項式に帰着して求めた近似 GCD から本来の近似 GCD を復元することが容易ではありません。1つの変数を除き、残りの変数に何らかの数値を代入（以後、この代入値をサンプル点と呼称）するなどして得られる一変数多項式は、摂動を行わなければ元の多項式に復元可能ですが、近似 GCD においては摂動が不可避となります。このとき、一変数多項式としての近似 GCD 計算における最小の摂動は、それぞれのサンプル点に依存するため、結果得られる近似 GCD から変数を復元したところで、本来の二変数あるいは多変数多項式の近似 GCD として、最適な摂動になりません。これを図示したものが、図 2 になります。

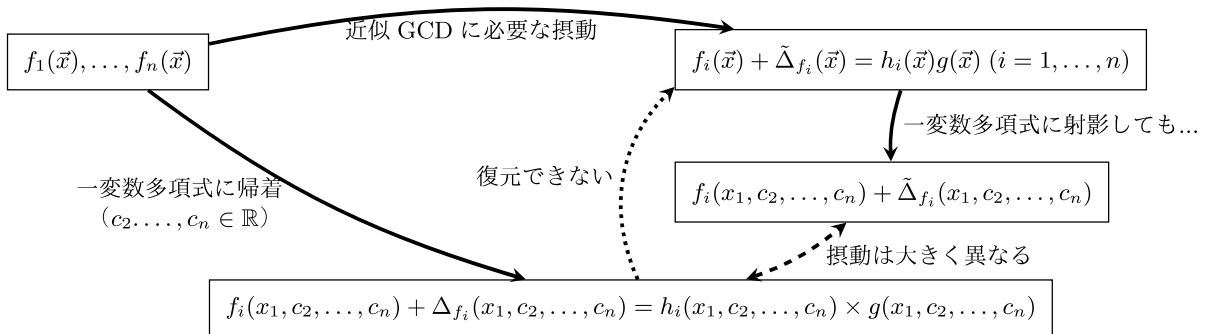


図 2: 一変数多項式に帰着して求めた近似 GCD と本来の近似 GCD は異なる

結果として、二変数あるいは多変数多項式の近似 GCD 計算においては、Hensel 構成や補間法などの通常の GCD 計算で主流の方法が採用しづらくなります。一方、QR 分解や特異値分解などの行列分解に基づく方法であれば、後述する一般化された Sylvester 行列などを用いることで、そのままの枠組みで一変数多項式向けのアルゴリズムを使うことができます。しかしながら、この方法においても課題があり、一般化さ

れた Sylvester 行列などのサイズは変数の個数に関して指数的に増大するため、計算量や精度の点で問題が残ります。今回紹介するアプローチでは、これら補間法と行列分解に基づく方法の良いところを組み合わせる試みを行っています。

## 2 SLRA による補間法

本稿で紹介するアルゴリズムは、一般化された Sylvester 行列, SLRA (構造化階数落ち行列近似) による近似 GCD, 特異値分解による近似 GCD, 補間法による旧来の GCD, FFT による近似 GCD[LYZ10], など参考にしており、これらのうち説明に必要な部分について、以下で簡単に導入していきます。

### 2.1 特異値分解による近似 GCD

今回のアプローチの基礎となる近似 GCD を特異値分解で求める方法 [GKM<sup>+</sup>04] を最初に説明します。この方法では、以下で定義される一般化された Sylvester 行列の階数落ちと、与えられた多項式の GCD との関係を用いて、近似 GCD を計算します。

**定義 2 (一般化された Sylvester 行列 (部分終結式行列))**

全次数がそれぞれ  $d_i = \text{tdeg}(f_i)$  の多項式  $f_1(\vec{x}), \dots, f_n(\vec{x}) \in \mathbb{R}[\vec{x}]$  と、正整数  $k \in \mathbb{N}$  に対して、次式の  $\text{Syl}_k(f_1, \dots, f_n)$  を、これら多項式の  $k$  次一般化された Sylvester 行列と呼ぶ ( $k-1$  次とする定義もある)。

$$\text{Syl}_k(f_1, \dots, f_n) = \begin{pmatrix} C_{d_1-k}(f_2) & C_{d_2-k}(f_1) & \mathbf{0} & \cdots & \mathbf{0} \\ C_{d_1-k}(f_3) & \mathbf{0} & C_{d_3-k}(f_1) & & \mathbf{0} \\ \vdots & \vdots & & \ddots & \vdots \\ C_{d_1-k}(f_n) & \mathbf{0} & \cdots & \mathbf{0} & C_{d_n-k}(f_1) \end{pmatrix}$$

ここで、 $C_k(p)$  は、全次数  $k$  の任意の多項式  $q(\vec{x})$  に対し、 $h(\vec{x}) = p(\vec{x})q(\vec{x})$  かつ  $C_k(p)\vec{q} = \vec{h}$  を満たす畳み込み行列を表す。これらは、項順序に依存しており、本稿では辞書式順序の昇順を基本とするが、特に限定はしない。なお、第 1 列群を右端に配置する定義もある [KYZ06]。◁

特異値分解により直接的に近似 GCD を求めるには、一般化された Sylvester 行列の次の性質を用います。

$$\text{tdeg}(\text{gcd}(f_1, \dots, f_n)) \geq k \iff \text{Syl}_k(f_1, \dots, f_n) \text{ is rank deficient.}$$

具体的には、 $\text{Syl}_k(f_1, \dots, f_n)$  の特異値分解により得られるゼロベクトルは、近似 GCD による  $f_1(\vec{x}), \dots, f_n(\vec{x})$  の余因子  $h_1(\vec{x}), \dots, h_n(\vec{x})$  の係数ベクトル候補となります。近似 GCD 自体は、これら余因子と与えられた多項式から立式される以下の最小二乗法により、その係数ベクトルを求めることができます (多項式  $p(\vec{x})$  の係数ベクトルを  $\vec{p}(\vec{x})$  で、行列やベクトルの転置を  $\cdot^T$  で表しています)。

$$\min_{\vec{g}(\vec{x})} \left\| \begin{pmatrix} C_d(h_1) \\ \vdots \\ C_d(h_n) \end{pmatrix} \vec{g}(\vec{x}) - \begin{pmatrix} \vec{f}_1(\vec{x})^T & \cdots & \vec{f}_n(\vec{x})^T \end{pmatrix}^T \right\|_2$$

この方法で求まる近似 GCD は余因子をゼロベクトルから直接求めている関係上、指定した次数に対して摂動の最小化を行っていないため、結果として得られる摂動量は大きくなります。このため、例えば、MVGCD アルゴリズム [ZD04] であれば、Gauss-Newton 法による最小化で、STLN ベースのアルゴリズム [KYZ06] であれば、ペナルティ法による最小化でもって、摂動量を小さくする仕組みになっています。

## 2.2 SLRA による近似 GCD

特異値分解による近似 GCD 計算では、対象となる多項式を摂動させるまえに、そのゼロベクトルを求めるため、結果として求まる近似 GCD の摂動量は大きくなってしまいます。STLN ベースのアルゴリズム [KYZ06] では、近似 GCD やその余因子を求める代わりに、一般化された Sylvester 行列の階数が落ちるように構造化された摂動を求めています。同じことを、STLN ではなく、SLRA (Structured Low Rank Approximation) で行うアルゴリズム [SS16] も提案されています。以下、簡単にその紹介を行います。

以下では、 $m \times n$  の実行列全体のベクトル空間を  $\mathcal{M}_{m,n}(\mathbb{R})$  と表し、 $\mathcal{M}_{m,n}(\mathbb{R})$  の内積を  $\langle M_1, M_2 \rangle := \text{trace}(M_1 M_2^T)$  とします (この内積で導かれるノルムは、Frobenius ノルム)。階数が  $r$  となる行列の集合を  $\mathcal{D}_r \subset \mathcal{M}_{m,n}(\mathbb{R})$  で、 $E \subset \mathcal{M}_{m,n}(\mathbb{R})$  を  $\mathcal{M}_{m,n}(\mathbb{R})$  の affine 部分空間、 $\{E_1, \dots, E_d\}$  をその基準ベクトル空間の正規直交基底とします。これらの記法のもと、SLRA は次のように定義されます。

### 定義 3 (SLRA: Structured Low Rank Approximation)

行列  $M \in E$  と正整数  $r$  に対し、 $\|M - M^*\|_F$  が小さくなるような行列  $M^* \in E \cap \mathcal{D}_r$  を求めよ。 ◁

例えば、 $f(x) = f_2x^2 + f_1x + f_0$  と  $g(x) = g_2x^2 + g_1x + g_0$  の 1 次の近似 GCD を求める場合、次の Sylvester 行列 (階数落ちに転置は影響を与えないので、この例では本稿で導入した一般化された Sylvester 行列を転置したものを採用しています) が SLRA における行列  $M$  となり、目標とする階数は  $r = 3$  となります。この SLRA を解き、階数が  $r$  となる  $M^*$  を求められれば、その摂動を係数の  $f_2, f_1, f_0, g_2, g_1, g_0$  に反映した多項式は、自明でない GCD を持つこととなります。その GCD が近似 GCD となります。

$$M = \begin{pmatrix} f_0 & f_1 & f_2 & 0 \\ 0 & f_0 & f_1 & f_2 \\ g_0 & g_1 & g_2 & 0 \\ 0 & g_0 & g_1 & g_2 \end{pmatrix}$$

この例では、 $E$  の基準ベクトル空間の正規直交基底は、係数の  $f_2, f_1, f_0, g_2, g_1, g_0$  にそれぞれ対応する行列から構成される次の直交基底を正規化したものになります (それぞれ  $1/\sqrt{2}$  倍となります)。SLRA の解法には、Lift-and-Project 法 [Cad88] や NewtonSLRA [SS16] などのアルゴリズムが知られています。

$$\left\{ \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \right\}$$

## 2.3 SLRA と補間法による近似 GCD

以上の準備のもと、一般化された Sylvester 行列をそのまま使用することに伴う行列サイズの指数関数的な増大を抑えるための、新しいアプローチの説明を行います。この方法では、離散 Fourier 変換 (高速 Fourier 変換) や数値的な Ben-Or/Tiwari アルゴリズム (補間法) [GLL09, GLL06] などで使用される「1 の原始  $p$  乗根」における評価を用いて補間を試みますが、直接的な補間ではなく、SLRA による近似 GCD の枠組みの中で間接的に補間を行います。以下、 $\ell = 2, n = 2$  (二変数多項式ペア) として説明を行います。

### 2.3.1 サンプル点と SLRA

与えられた多項式ペア  $f_1(x_1, x_2), f_2(x_1, x_2) \in \mathbb{R}[x_1, x_2]$  の次数  $k \in \mathbb{N}$  の近似 GCD を直接求めるのではなく、一変数多項式に射影した結果の多項式ペアの一変数多項式としての近似 GCD から補間することを考え

ます。そこで、 $\omega_1, \dots, \omega_p$  を 1 の原始  $p$  乗根の累乗とし、これらをサンプル点として、 $f_1(x_1, \omega_i), f_2(x_1, \omega_i)$  から二変数多項式  $f_1(x_1, x_2), f_2(x_1, x_2)$  を補間するのに十分な大きさを  $p$  が持っているとします (例えば、 $p > \text{tdeg}(f_1), \text{tdeg}(f_2)$  を満たす素数など)。このとき、 $f_1(x_1, x_2), f_2(x_1, x_2)$  が互いに素でなければ、次の行列  $M$  は階数落ちする必要があります。

$$M = \begin{pmatrix} \text{Syl}_k(f_1(x_1, \omega_1), f_2(x_1, \omega_1)) & & \mathbf{0} \\ & \ddots & \\ \mathbf{0} & & \text{Syl}_k(f_1(x_1, \omega_p), f_2(x_1, \omega_p)) \end{pmatrix}$$

しかしながら、この行列  $M$  が階数落ちするのは、 $f_1(x_1, x_2), f_2(x_1, x_2)$  が互いに素でないことの必要条件であって、十分条件ではありません。必要十分となるためには、対角部分である次の  $M_1, \dots, M_p$  のすべてが同時に階数落ちする必要があります。

$$M_1 = \text{Syl}_k(f_1(x_1, \omega_1), f_2(x_1, \omega_1)), \dots, M_p = \text{Syl}_k(f_1(x_1, \omega_p), f_2(x_1, \omega_p))$$

これらの性質を用いて近似 GCD を求めること考えます。 $f_1(x_1, x_2), f_2(x_1, x_2)$  は互いに素であると考えられることから、それぞれ摂動を行って、 $M_1, \dots, M_p$  のすべてが同時に階数落ちさせることになります。しかしながら、これらの  $M_1, \dots, M_p$  が独立して摂動してしまうと、同じ多項式のサンプル点における評価結果ではなくなるため、補間することが難しくなります。本稿では、評価結果が独立して摂動することを避けるため、SLRA の対象を全体行列  $M$  としつつ、 $M_1, \dots, M_p$  が階数落ちすることを条件に加えた上で、 $M$  としての SLRA を解くことを提案しています。

$M$  自体の特異値分解は行列サイズが大きく計算量の課題が残りますが、 $M$  はブロック対角行列であり、 $M_i$  それぞれの特異値分解から  $M$  全体の特異値分解を構成することが出来ますので、多くの行列分解に基づくアルゴリズムに比べて小さく抑えることができます。また、Lift-and-Project 法や NewtonSLRA などの Eckart-Young-Mirsky の定理 [GVL13, Mar19] に基づくアルゴリズムは、無理なく自然な形で SLRA の対象を全体行列  $M$  としつつ、 $M_1, \dots, M_p$  が階数落ちする条件を加えることが出来ます。なお、この方法では補間法に基づいてサンプル点は選択しますが、実際には補間を行わず、SLRA による摂動を求めることとなります。このとき、SLRA の対象となる affine 部分空間の基準ベクトル空間の基底は、SLRA を導入した際の Sylvester 行列の例と同じく、サンプル点を代入する前の各係数に対応する行列から構成されます (係数を含まない変数の積であるサポートにサンプル点を代入したものが、正規化前の行列の要素となります)。

### 2.3.2 複数の一変数多項式

複数の一変数多項式に対して近似 GCD を求める場合、一般化された Sylvester 行列を用いることも出来ますが、本稿では、二変数多項式ペアに帰着させる方法を採用します。次のように、 $F = \{f_1(x_1), \dots, f_n(x_1)\}$  に対して、 $m$  個と  $(n - m)$  個に多項式を分け、新たにスラック変数として  $x_2$  を導入して、二変数多項式  $\bar{f}_1(x_1, x_2)$  と  $\bar{f}_2(x_1, x_2)$  を構成します。

$$\bar{f}_1 = f_1(x_1) + x_2 f_2(x_1) + \dots + x_2^{m-1} f_m(x_1), \bar{f}_2 = f_{m+1}(x_1) + x_2 f_{m+2}(x_1) + \dots + x_2^{n-m-1} f_n(x_1)$$

このとき、 $m = 1$  であれば、元の多項式集合の GCD と、新たな多項式ペアの GCD は一致しますので、この変換で二変数多項式ペア向けの近似 GCD アルゴリズムで、複数の一変数多項式の近似 GCD も計算できることとなります。ただし、 $m = 1$  の場合、新しい多項式の全次数は大きくなりやすいため、必要十分条件とはならない  $m \neq 1$  を用いた近似 GCD 計算が期待されます。しかしながら、いくつかの例では、 $m \neq 1$  の場合に得られる摂動量は  $m = 1$  の場合に比べて大きくなる傾向があり、 $m \neq 1$  は推奨できないと考えられます。

### 3 数値実験

この章では、Mathematica 12.2 を用いて実施した数値実験の結果について報告します。

#### 3.1 二変数多項式ペア

Kaltofen らの STLN ベースのアルゴリズムの論文 [KYZ06] で実験に使われている Ex.5 (二変数実多項式) と Ex.8 (二変数実多項式) を用いて、計算結果の各摂動量の二乗和を表 1 にまとめました。なお、MVGCD は Zeng らによるアルゴリズム [ZD04], GKMYZ は特異値分解によるアルゴリズム [GKM+04], STLN は Kaltofen らのアルゴリズム [KYZ06] による結果を表していますが、これらの結果は Kaltofen らの論文 [KYZ06] からの引用値となります。ただし、比較のため、特異値分解によるアルゴリズムは本方法でも使用するため、今回の実験のために実装したものを使用した結果を「GKMYZ(自実装)」としてあります。今回提案の方法も含めて実装における設定は、最大反復回数制限を 16 回、反復における補正項の終了判定の閾値を  $1.49012e-8$ , 最小二乗法の精度を  $1.0e-2$  としています。

	tdeg : $f_1, f_2, g$	MVGCD	GKMYZ	GKMYZ(自実装)	STLN	本方法
Ex.5	6, 6, 3	2.26617	1.49524	1.44864	$4.80154e-1$	$4.82423e-1$
Ex.8	40, 40, 30	$1.39858e-3$	$4.83931e-4$	$4.83876e-4$	$4.39489e-4$	$4.47442e-4$

表 1: Ex.5 と Ex.8 の計算結果における両多項式の摂動の二乗和

本方法と採用する SLRA の解法との関係性を調べるため、全次数が 10 次と 9 次以下の二変数多項式のペア (GCD の全次数は 3 次) をランダムに 100 組生成して実験を行いました。それぞれの多項式ペアは、各単項式に関して 0.5 の確率で  $[-1, 1] \in \mathbb{R}$  の非ゼロ係数を生成し、最後に  $[-1.0e-3, +1.0e+3]$  を各非ゼロ係数に加える摂動を誤差として行っています。図 3 が結果となります。計算結果の各多項式の摂動 (2 ノルム) の二乗和の常用対数を図示したものです (直線は常用対数の平均)。なお、Cadzow は Lift-and-Project 法 [Cad88] で、NewtonSLRA は NewtonSLRA[SS16] による結果となります。

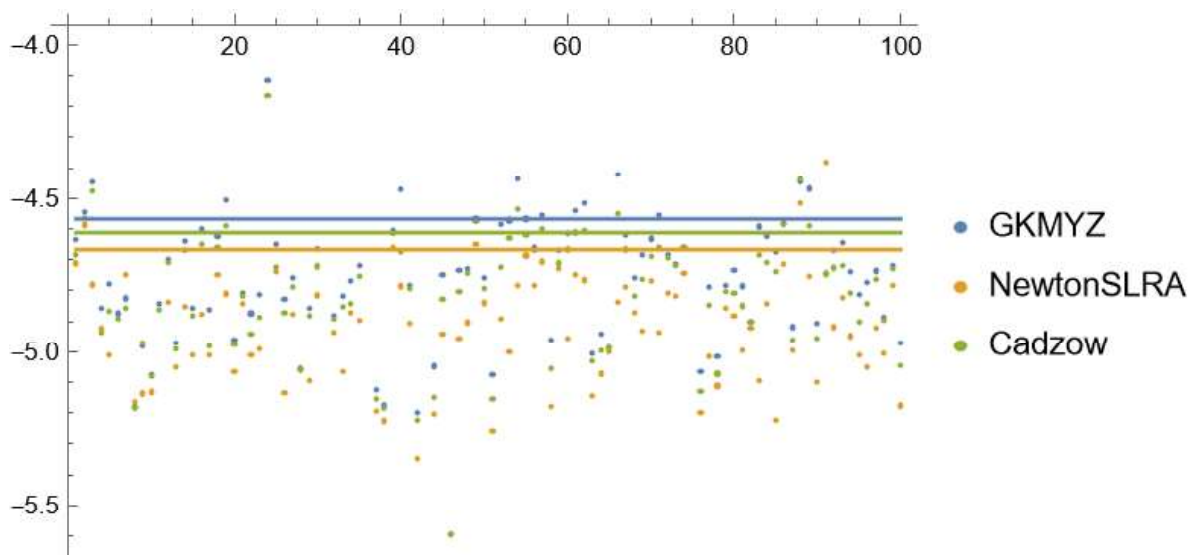


図 3: 二変数のランダム実験結果 (両多項式の摂動の二乗和の常用対数グラフ)

### 3.2 複数の一変数多項式

Saha と Khare の論文 [SK21] で取り上げられている次の多項式集合  $F = \{f_1, f_2, f_3\}$  の近似 GCD を、今回提案の方法（スラック変数による二変数多項式ペアへの帰着）で求めた結果を比較します。

$$f_1 = 5 - 6x + x^2, f_2 = 10.8 - 7.4x + x^2, f_3 = 15.6 - 8.2x + x^2$$

引用元の論文の方法（SLRA）では、二種類の Sylvester 行列の一般化で実験が行われています。本稿で紹介した一般化された Sylvester 行列と同じ方法での結果が 0.0390 となっており、異なる一般化での結果が 0.0373 となっています。今回提案の方法では、摂動させる前の段階で 0.0641 であり、SLRA のマジックパラメータを調整した場合で 0.0376、調整しない場合で 0.181 という結果でした。なお、ペアへの分け方も含めて調整有りの場合は最良で 0.0373 となっています。

本方法と採用する SLRA の解法との関係を調べるため、次数が 9 次以下の一変数多項式の集合（10 個の多項式から構成され、その GCD の次数は 3 次）をランダムに 100 組生成して実験を行いました。それぞれの多項式集合は、各単項式に関して 0.5 の確率で  $[-1, 1] \in \mathbb{R}$  の非ゼロ係数を生成し、最後に  $[-1.0e-3, +1.0e+3]$  を各非ゼロ係数に加える摂動を誤差として行っています。図 4 が結果となります。計算結果の各多項式の摂動（2 ノルム）の二乗和の常用対数を図示したものです。

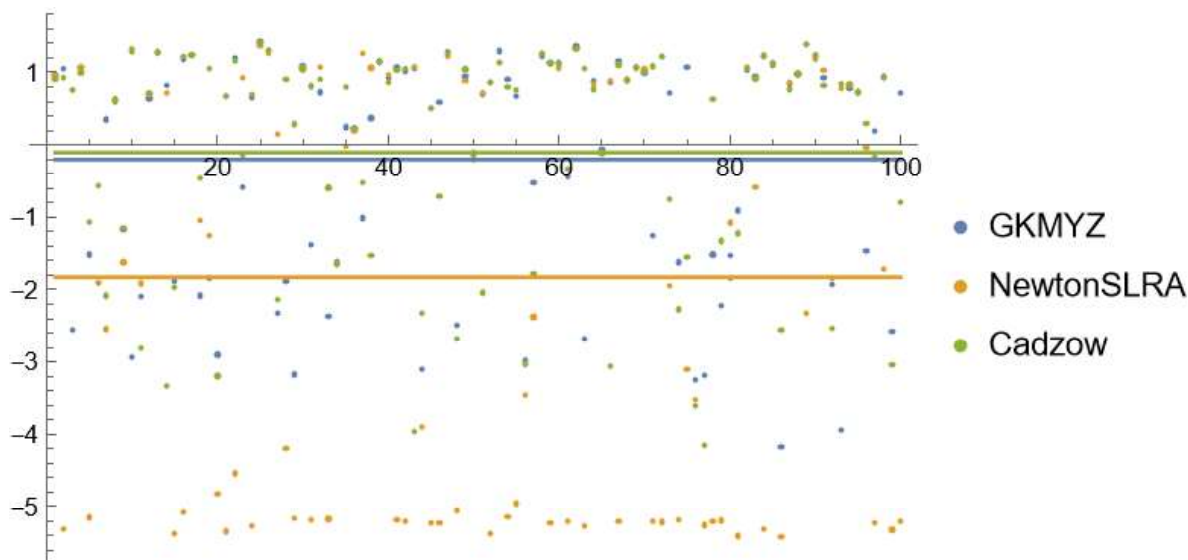


図 4: 一変数 10 多項式のランダム実験結果（各多項式の摂動の二乗和の常用対数グラフ）

また、次数が 13 次以下の一変数多項式の集合（6 個の多項式から構成され、その GCD の次数は 3 次）をランダムに 100 組生成して実験を行いました。それぞれの多項式集合は、各単項式に関して 0.5 の確率で  $[-1, 1] \in \mathbb{R}$  の非ゼロ係数を生成し、最後に  $[-1.0e-3, +1.0e+3]$  を各非ゼロ係数に加える摂動を誤差として行っています。図 5 が結果となります。計算結果の各多項式の摂動（2 ノルム）の二乗和の常用対数を図示したものです。

## 謝 辞

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

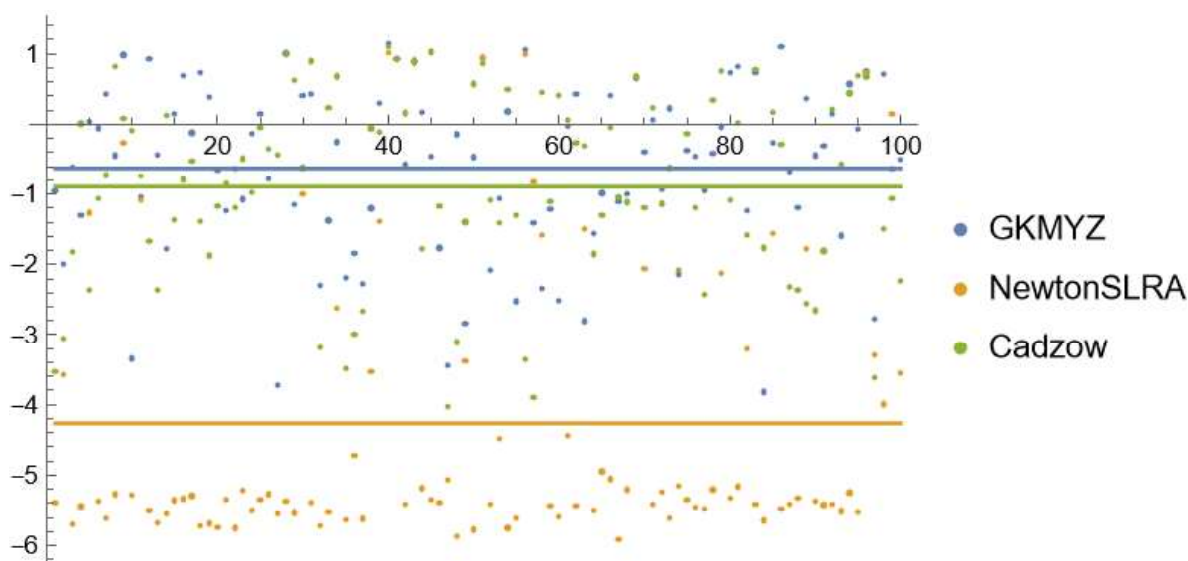


図 5: 一変数 6 多項式のランダム実験結果 (各多項式の摂動の二乗和の常用対数グラフ)

## 参 考 文 献

- [Bro71] W. S. Brown. On Euclid’s algorithm and the computation of polynomial greatest common divisors. *J. Assoc. Comput. Mach.*, 18:478–504, 1971.
- [Cad88] J.A. Cadzow. Signal enhancement—a composite property mapping algorithm. *IEEE Transactions on Acoustics, Speech, and Signal Processing*, 36(1):49–62, 1988.
- [CWZ04] Robert M. Corless, Stephen M. Watt, and Lihong Zhi.  $QR$  factoring to compute the GCD of univariate approximate polynomials. *IEEE Trans. Signal Process.*, 52(12):3394–3402, 2004.
- [GKM<sup>+</sup>04] Shuhong Gao, Erich Kaltofen, John May, Zhengfeng Yang, and Lihong Zhi. Approximate factorization of multivariate polynomials via differential equations. In *ISSAC 2004*, pages 167–174. ACM, New York, 2004.
- [GLL06] Mark Giesbrecht, George Labahn, and Wen-shin Lee. Symbolic-numeric sparse interpolation of multivariate polynomials. In *ISSAC 2006*, pages 116–123. ACM, New York, 2006.
- [GLL09] Mark Giesbrecht, George Labahn, and Wen-shin Lee. Symbolic-numeric sparse interpolation of multivariate polynomials. *J. Symbolic Comput.*, 44(8):943–959, 2009.
- [GVL13] Gene H. Golub and Charles F. Van Loan. *Matrix computations*. Johns Hopkins Studies in the Mathematical Sciences. Johns Hopkins University Press, Baltimore, MD, fourth edition, 2013.
- [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.
- [LYZ10] Zijia Li, Zhengfeng Yang, and Lihong Zhi. Blind image deconvolution via fast approximate GCD. In *ISSAC 2010—Proceedings of the 2010 International Symposium on Symbolic and Algebraic Computation*, pages 155–162. ACM, New York, 2010.



- [Mar19] Ivan Markovskiy. *Low-rank approximation*. Communications and Control Engineering Series. Springer, Cham, 2019. Algorithms, implementation, applications, Second edition.
- [MY73] Joel Moses and David Y. Y. Yun. The ez gcd algorithm. In *Proceedings of the ACM Annual Conference*, ACM '73, pages 159–166, New York, NY, USA, 1973. Association for Computing Machinery.
- [SK21] Tanay Saha and Swanand Khare. Structured low-rank approximation: optimization on matrix manifold approach. *Int. J. Appl. Comput. Math.*, 7(6):Paper No. 242, 31, 2021.
- [SS16] Éric Schost and Pierre-Jean Spaenlehauer. A quadratically convergent algorithm for structured low-rank approximation. *Found. Comput. Math.*, 16(2):457–492, 2016.
- [ZD04] Zhonggang Zeng and Barry H. Dayton. The approximate GCD of inexact polynomials. II. A multivariate algorithm. In *ISSAC 2004*, pages 320–327. ACM, New York, 2004.
- [Zip79] Richard Zippel. Probabilistic algorithms for sparse polynomials. In *Symbolic and algebraic computation (EUROSAM '79, Internat. Sympos., Marseille, 1979)*, volume 72 of *Lecture Notes in Comput. Sci.*, pages 216–226. Springer, Berlin-New York, 1979.