数理解析研究所講究録
第2019巻 2017年 39-52

摂動に強い疎な多変数多項式の補間について
A robust algorithm for sparse interpolation of multivariate polynomials

沼畑 大

Dai Numahata *

東京理科大学大学院 理学研究科

Graduate School of Science, Tokyo University of Science

Abstract

We propose a robust algorithm for sparse interpolation of multivariate black-box polynomials in floating-point arithmetic.

1 はじめに

多変数多項式のブラックボックス $f(x_1,\ldots,x_n)=\sum_{j=1}^{t} c_j x_1^{d_{j,1}}\cdots x_n^{d_{j,n}} \in \mathbb{C}[x_1,\ldots,x_n]$ $(c_j\neq 0)$ が与えられたとき，このブラックボックスをホワイトボックスにする (係数 c_j, 指数部 $d_{j,k}$ を求める) 問題を多変数多項式の補間とよぶ．特に項数が少ない (疎である) 場合を考えた多種多様な先行研究が存在し，大きく Zippel [10] による確率的なアルゴリズムの発展と Ben-Or, Tiwari [1] によるアルゴリズム (以下 BT とよぶ) の発展の 2 種類に分かれる．疎な多変数多項式の補間には GCD 計算，因数分解，信号処理など数多くの応用が存在する．本稿では BT を数値的誤差を含む場合に拡張した Giesbrecht, Labahn, Lee [5] の方法 (以下 GLL とよぶ) に着目し，著者が以前提案した GLL において必要となる，次数の上界を外したアルゴリズム [9] を紹介する．また今回新たにブラックボックスの出力に対する摂動に強い補間アルゴリズムを提案する．以下，第 2 章で関連する先行研究の紹介を行う．第 3 章では数値的誤差を含む演算の下での疎な多変数多項式の補間で次数の上界を要求しない手法を紹介する．第 4 章では摂動に強い疎な多変数多項式の補間手法を提案する．第 5 章では発表で述べることのできなかった上記手法の改良について述べる．第 6 章では従来の項数推定の手法を本稿の提案手法に適用する場合の注意点を述べる．最後に第 7 章で今回の研究結果をまとめ，今後の課題や応用について述べる．

2 先行研究

以下，本稿の提案手法を説明するのに必要な先行研究のアルゴリズムの概略を説明する．

*nd0451@gmail.com

2.1 BT

アルゴリズム 1 (Ben-Or, Tiwari [1] (1988))
以下のように記号を設定する.

- $\beta_j(x_1,\ldots,x_n) = x_1^{d_{j_1}}\ldots x_n^{d_{j_n}}$
- p_i: i 番目の素数
- $b_j = \beta_j(p_1,\ldots,p_n)$
- $\alpha_s = f(p_1^s,\ldots,p_n^s)$

Input: 項数 t のブラックボックス n 変数多項式

$$f(x_1,\ldots,x_n) = \sum_{j=1}^{t} c_j x_1^{d_{j_1}}\ldots x_n^{d_{j_n}} \ (d_{j_k}\text{は非負整数},\ c_j(\neq 0)\text{は複素数}) .$$

Output: $d_{j_k},\ c_j\ (1\le j\le t,\ 1\le k\le n)$.

(1) 以下の Hankel 方程式を解く.

$$\begin{pmatrix} \alpha_0 & \cdots & \alpha_{t-1} \\ \alpha_1 & \cdots & \alpha_t \\ \vdots & \ddots & \vdots \\ \alpha_{t-1} & \cdots & \alpha_{2t-2} \end{pmatrix} \begin{pmatrix} \lambda_0 \\ \lambda_1 \\ \vdots \\ \lambda_{t-1} \end{pmatrix} = - \begin{pmatrix} \alpha_t \\ \alpha_{t+1} \\ \vdots \\ \alpha_{2t-1} \end{pmatrix}$$

(2) 以下の z の方程式を解く (解は各 b_j と一致する) .

$$\Lambda(z) = \prod_{j=1}^{t}(z-b_j) = z^t + \lambda_{t-1}z^{t-1} + \cdots + \lambda_1 z + \lambda_0 = 0$$

(3) b_j から $d_{j_1},\ldots,d_{j_n}$ を復元する.

(4) 以下の Vandermonde 方程式を解く (解は f の係数 c_j と一致する) .

$$\begin{pmatrix} 1 & \cdots & 1 \\ b_1 & \cdots & b_t \\ \vdots & \ddots & \vdots \\ b_1^{t-1} & \cdots & b_t^{t-1} \end{pmatrix} \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_t \end{pmatrix} = \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{t-1} \end{pmatrix}$$

数値的誤差を含む演算で BT を用いるとき, 行列が悪条件となることが問題になるが, ブラックボックスへの入力を素数ではなく単位円上の点にすることで悪条件を回避できる (これが GLL のアイデアである) .

2.2 GLL

アルゴリズム 2 (Giesbrecht, Labahn, Lee [5] (2009))
以下のように記号を設定する.

- $\beta_j(x_1,\ldots,x_n) = x_1^{d_{j_1}} \ldots x_n^{d_{j_n}}$
- $m = D_1 \ldots D_n$
- $\omega = \exp(2\pi i/m)$
- $\omega_k = \exp(2\pi i/D_k) = \omega^{m/D_k}$
- $b_j = \beta_j(\omega_1,\ldots,\omega_n)$
- $\alpha_s = f(\omega_1^s,\ldots,\omega_n^s)$

Input: 出力に数値的誤差を含む項数 t のブラックボックス n 変数多項式

$$f(x_1,\ldots,x_n) = \sum_{j=1}^{t} c_j x_1^{d_{j_1}} \ldots x_n^{d_{j_n}} \quad (d_{j_k}\text{は非負整数},\ c_j(\neq 0)\text{は複素数}),$$

$D_1,\ldots,D_n$: $D_j > \deg(f_{x_j})$, $D_1,\ldots,D_n$は互いに異なる素数

($\deg(f_{x_j})$ は変数 x_jについての f の次数を表す).

Output: d_{j_k}, c_j $(1 \le j \le t,\ 1 \le k \le n)$

以降の手順は BT と同じだが，BT(3) は以下のようにする.

(3.1) $\omega^{d_j} = b_j$ から計算した d_j を丸めて整数にしたものを d_j と置き直す.

(3.2) 中国剰余定理

$$d_j \equiv d_{j_k} \cdot \frac{m}{D_k} \mod D_k, \qquad d_j = d_{j_1} \cdot \frac{m}{D_1} + \cdots + d_{j_n} \cdot \frac{m}{D_n}$$

から各 d_{j_k} を計算する.

単位円上の b_1, ..., b_t の距離が近いと行列が悪条件となるが，$\omega_k^{r_k}$ (r_k は $1 \le r_k < D_k$ を満たす適当な整数) を改めて ω_k とすることで悪条件を回避できる (これを randomized reconditioning とよぶ).

2.3 QD アルゴリズムによる手法

次数の上界を必要としないアルゴリズムとして，QD アルゴリズムを用いた方法が Cuyt, Lee [3] (2008) で提案されている．具体的には BT において (1), (2) の代わりに漸化式

$$\begin{aligned}
&e_0^{(s)} = 0, \qquad s = 1,2,\ldots \\
&q_1^{(s)} = \frac{\alpha_{s+1}}{\alpha_s}, \qquad s = 0,1,\ldots \\
&e_u^{(s)} = q_u^{(s+1)} - q_u^{(s)} + e_{u-1}^{(s+1)}, \qquad u = 1,2,\ldots, \qquad s = 0,1,\ldots \\
&q_{u+1}^{(s)} = \frac{e_u^{(s+1)}}{e_u^{(s)}} q_u^{(s+1)}, \qquad u = 1,2,\ldots, \qquad s = 0,1,\ldots
\end{aligned}$$

を用いて

$$\lim_{s\to\infty} q_j^{(s)} = b_j \qquad (\text{ただし } b_1 > b_2 > \cdots \text{とする})$$

として各 b_j を計算する方法である (以下，この方法を CLp とよぶ).

GLL (単位円周上の点の入力) においても (1), (2) の代わりに

$$\rho_0^{(s)}(z) = 1,$$
$$\rho_{j+1}^{(s)}(z) = z\rho_j^{(s+1)}(z) - q_{u+j+1}^{(s)}\rho_j^{(s)}, \qquad s \geq 0, \qquad j = 0, 1, \ldots, l-1,$$
$$\lim_{s\to\infty} \rho_j^{(s)} = \prod_{j=1}^{t}(z - b_j)$$

として各 b_j を計算できる (以下，この方法を CLru とよぶ) .

2.4 先行研究のまとめ

先行研究では入力を素数にすると演算が数値的誤差を含むときには一般に悪条件で，入力を単位円周上の点とすると悪条件を回避できるが次数の上界が必要という特徴がある．表 1 は各手法の特徴をまとめたものである．

表 1: 各手法の特徴

手法	入力	指数の計算	次数の上界	条件数
BT [1]	素数	Hankel 方程式	要求しない	大
GLL [5]	単位円周上の点	Hankel 方程式	要求する	小
CLp [3]	素数	QD アルゴリズム	要求しない	大
CLru [3]	単位円周上の点	QD アルゴリズム	要求する	小

3 次数の上界を要求しない数値的誤差を含む補間

3.1 問題設定

GLL および CLru は，入力を単位円周上の点にすることで悪条件を避けたものの，BT および CLp にはなかった変数 x_k に対する次数の上界 D_k を必要とする．そこで本稿では数値的誤差を含む演算の下で D_k を必要としないアルゴリズムを設計できるか考察する．

この問題を解くアプローチは以下の二つが考えられる．

- 素数入力の方法を改良する．
- 単位円周上の点入力の方法を改良する．

しかし，素数入力の方法は悪条件が解決されても素因数分解の問題がある．

例 1
与えられたブラックボックスを

$$f = x^{100}y + 123y^{23}z^{40} + 8x^{54}y^{98}z^{32}$$

として，QD アルゴリズムにより精度 10 桁で

$$b_1 = 2.401833330 \times 10^{85} (2^{54}3^{98}5^{32}\text{の近似値})$$

が計算できる (b_2, $b_3 < b_1$ は計算できない). ここで $b_1 = 2.401833330 \times 10^{85}$ に最も近い $2^i3^j5^k$ の (i,j,k) の計算が必要になるが変数の数に関して指数オーダーで計算時間がかかってしまう.

従って単位円周上の点入力の方法を改良するアプローチをとる. まず, D_k を適当に設定して GLL を用いるとどうなるか見ていく.

3.2 係数 c_j の計算

例 2

与えられたブラックボックスを $f = x_1^{100}x_2 + 123x_2^{50}x_3^{40} + 8x_1^{55}x_2^{98}x_3^{32}$, 次数の上界を $\tilde{D}_1 = 23$, $\tilde{D}_2 = 41$, $\tilde{D}_3 = 13$ (次数の真でない上界) として, GLL を用いると $x_1^8x_2 + 123x_2^9x_3 + 8x_1^9x_2^{16}x_3^6$ が得られる. この多項式の各指数は, 元の f の各項における x_k の指数をそれぞれ $\tilde{D}_k$ で割った余りである.

例 3

与えられたブラックボックスを $f = x_1^{100}x_2 + 123x_1^{77}x_2 + 8x_1^{55}x_2^{98}x_3^{32}$, 次数の上界を $\tilde{D}_1 = 23$, $\tilde{D}_2 = 41$, $\tilde{D}_3 = 13$ (次数の真でない上界) として, GLL を用いると, $x_1^{100}x_2$ と $x_1^{77}x_2$ の指数は $\tilde{D}_1, \tilde{D}_2$ による剰余を取ると同一となり連立方程式の係数行列が正則ではなくなる.

一般に次のことが言える.

定理 1

GLL または CLru にブラックボックスと正しいとは限らない次数の上界 $\tilde{D}_k$ を入力したときの出力を

$$g(x_1, \ldots, x_n) = \sum_{j=1}^{t} c_j x_1^{\tilde{d}_{j,1}} \ldots x_n^{\tilde{d}_{j,n}} \quad (\tilde{d}_{j,k}\text{は非負整数},\ c_j(\neq 0)\ \text{は複素数})$$

とする. ここで行列が正則になる $\tilde{D}_k$ を選択でき, さらに行列の悪条件性を回避できたとする. このとき, 真のブラックボックス f は

$$f(x_1, \ldots, x_n) = \sum_{j=1}^{t} c_j x_1^{\tilde{d}_{j,1}+u_{j,1}\tilde{D}_1} \ldots x_n^{\tilde{d}_{j\,n}+u_{j\,n}\tilde{D}_n} \quad (u_{j,k}(1 \le j \le t,\ 1 \le k \le n)\ \text{は非負整数}).$$

証明 $\omega_k = \exp(2\pi i/\tilde{D}_k)$ とすると

$$f(\omega_1^s, \ldots, \omega_n^s) = \sum_{j=1}^{t} c_j (\omega_1^s)^{\tilde{d}_{j,1}} \ldots (\omega_n^s)^{\tilde{d}_{j,n}} = g(\omega_1^s, \ldots, \omega_n^s)\ (s = 0, 1,\ \ldots)$$

より, 正しいとは限らない次数の上界 $\tilde{D}_k$ を入力したとき f から作られる Hankel 方程式は g から作られるものと同一である. またこの Hankel 方程式を導出できるブラックボックスは

$$\sum_{j=1}^{t} c_j x_1^{\tilde{d}_{j\,1}+u_{j\,1}\tilde{D}_1} \ldots x_n^{\tilde{d}_{j,n}+u_{j,n}\tilde{D}_n} \quad (u_{j,k}(1 \le j \le t,\ 1 \le k \le n)\ \text{は非負整数})$$

の形に限られる. ∎

定理 1 より, 次数の上界が正しくなくても係数を得ることができる.

3.3 指数 $d_{j,k}$ の計算

以下の命題 2 を用いて次数の上界の推定を行う.

命題 2
$f(x)=\sum_{j=0}^{d} a_j x^j \in \mathbb{C}[x]$ とすると

$$f(M)\approx a_d M^d \quad \left(M \gg \frac{\max_j |a_j|}{\min_{j,\ a_j\neq 0} |a_j|}\right), \qquad \log_\gamma \frac{|f(\gamma M)|}{|f(M)|}\approx d \quad (\gamma \gg 1).$$

f の係数がわかっていれば命題 2 を用いる際に適切な M を定めることができる.

命題 2 は 1 変数多項式に対する命題であるが, 多変数多項式においても適当な定数を代入して 1 変数にすれば適用できる. 簡単のため, 3 変数多項式 $f(x_1,x_2,x_3)$ の x_1 に対する次数の上界を求めることを考察する. 例えば x_2, x_3 に定数 1 を代入してできる 1 変数多項式 $f(x_1,1,1)$ に対して命題 2 を用いる方法が考えられるが, それでは項の打消しが起きる危険性があるので定数の選び方は工夫する必要がある.

例 4
与えられたブラックボックスを $f=x_1^{100}x_2-x_1^{100}x_3+x_3^{50}$, 次数の上界を $\tilde{D}_1=23$, $\tilde{D}_2=41$, $\tilde{D}_3=13$ (次数の真でない上界) として, GLL を用いると以下が得られる.

$$x_1^8x_2-x_1^8x_3+x_3^{11}$$

$f(x,1,1)=1$ に対して命題 1 を用いても項の打消しが発生するため x_1 における次数の上界の推定はできない.

- x_1 における次数の上界が知りたい場合, 各項の x_1 における次数が違うことが分かれば $f(x,1,1)$ として問題ない.
- x_1 における次数が同じ項が存在する可能性があるとき, $f(x,1,1)$ とするのではなく工夫する必要がある.

例 5
与えられたブラックボックスを f : 3 変数多項式, 次数の上界を $\tilde{D}_1=23$, $\tilde{D}_2=41$, $\tilde{D}_3=13$ (次数の真でない上界) として, GLL を用いて $x_1^8x_2-x_1^8x_3+x_3^{11}$ が得られたとする. $f(x,1,\omega_3^6)$ は, 定理 1 より $(1-e^{12\pi i/13})x^{8+23u}+e^{2\pi i/13}$ または $x^{8+23u_1}-e^{12\pi i/13}x^{8+23u_2}+e^{2\pi i/13}$ であるとわかる. x_1 の次数の上界が知りたい場合, $f(x,\omega_2^{e_2},\omega_3^{e_3})$ (e_k は $0\le e_k<\tilde{D}_k$ を満たす適当な整数) とすれば元の f と係数が同一となるため打ち消しが起きるか予測できるので, 適切な $f(x,\omega_2^{e_2},\omega_3^{e_3})$ に命題 2 を用いれば x_1 の次数の上界が得られる.

一般の多変数多項式の次数の上界の推定も同様に行える.

3.4 アルゴリズム

提案手法の流れは, まず適当な素数を次数の上界と思って GLL または CLru を実行し, 次に得られた出力から命題 2 を適切に用いて正しい次数の上界を求め, 最初に入力された素数が真の上界であるとわかれば得られた出力を正しい出力とし, そうでなければ正しい次数の上界を用いて GLL または CLru を再実行, となる.

アルゴリズム 3 (沼畑 [9] (2016))
Input: 出力に数値的誤差を含む項数 t のブラックボックス n 変数多項式

$$f(x_1,\dots,x_n)=\sum_{j=1}^{t} c_j x_1^{d_{j,1}}\dots x_n^{d_{j,n}}\ (d_{j,k}\text{は非負整数},\ c_j(\neq 0)\text{は複素数})$$

Output: $d_{j,k},\ c_j\ (1\le j\le t,\ 1\le k\le n)$

(1) 互いに異なる素数 $\tilde{D}_1,\dots,\tilde{D}_k$ を適当に設定し $\tilde{D}_1,\dots,\tilde{D}_k$ を上界として GLL または CLru を用いる．
出力の係数を c_j, 指数部を $\tilde{d}_{j,k}$ とする．

(2) 各 k に対して $e_l\ (0\le e_l<\tilde{D}_l)$ を $f_k(x)=f(\omega_1^{e_1},\dots,\omega_{k-1}^{e_{k-1}},x,\omega_{k+1}^{e_{k+1}},\dots,\omega_n^{e_n})$ で打消しが起こらない形になるようにとる．
f_k に命題 2 を用いて正しい D_k を得る．

(3) $\tilde{D}_k$ が適切な次数の上界であれば $c_j,\ \tilde{d}_{j,k}$ を結果とする．
そうでなければ正しい上界 D_k を用いて再度 GLL または CLru を実行して得られた出力を結果とする (BT(4) の Vandermonde 方程式を解く必要はない)

注意 1

- 方程式が悪条件 (または非正則) のときは randomized reconditioning と同時に $\tilde{D}_k$ を変化させる．
- 計算時間は元の手法に命題 2 を用いる時間と (3) にかかる時間を足したものになる．

応用によっては命題 2 を用いる際ブラックボックスに大きな値を入力する計算が困難である可能性がある．

3.5 数値実験

数値的な誤差を含んだ演算の下で次数の上界を要求しないという設定で，提案手法が既存の手法より優れていることを Mathematica 10.2 による数値実験で示す．ただし，OS は Windows 10 Home, CPU は Intel Core i7 2.60 GHz, メモリは 16.0 GB である．

ブラックボックスとして係数が -99 から 99 (0 を除く) の整数係数 3 変数多項式を用い，連立方程式の解法は NSolve, QD アルゴリズムは [3] の漸化式を用いる．各グラフの縦軸は計算時間 (秒)，横軸は多項式の項数を表す．提案手法は “modified” とラベル付けしている．

図 1 のグラフは数値的誤差を含む演算の下で既存手法 (BT と CLp) と提案手法 (modifiedGLL と modifiedCLru) の計算時間を比較している実験の結果だが，既存手法は方程式の悪条件性により出力が適切ではない．また modifiedCLru は漸化式による評価が計算時間と連動している．この結果から提案手法の優位性が示される．

図 2 のグラフは，提案手法 (modifiedGLL) と正確演算の下での既存手法 (BT) との計算時間を比較した実験の結果である．BT は方程式を Solve で解いている．この結果から，入力が正確でも欲しい出力が近似値でよい場合は提案手法の優位性が言える．

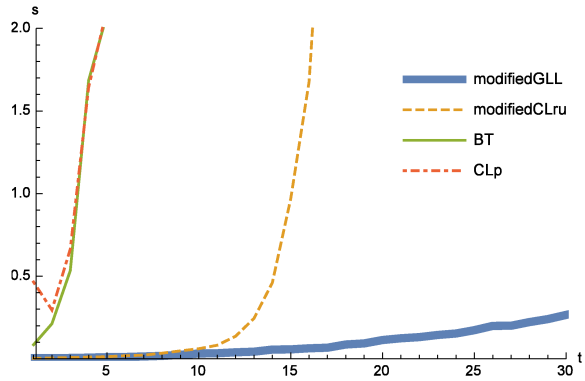

図 1: 実験結果 1

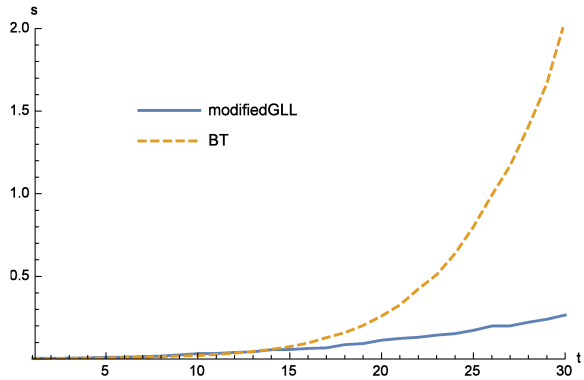

図 2: 実験結果 2

4　摂動に強い多変数多項式の補間

前章では次数の上界を要求しない補間手法を設計したが，次数の上界を正しく推定する意義は補間の計算が誤差や摂動に強くなる点にある．

例 6

与えられたブラックボックスを $f = x_1^{100}x_2 + 123x_2^{23}x_3^{40} + 8x_1^{54}x_2^{98}x_3^{32}$, 次数の上界を $D_1 = 101$, $D_2 = 103$, $D_3 = 107$ とし，$m = D_1 \ldots D_n$, $\omega = \exp(2\pi i/m)$ とする．GLL(2) において

$$b_1 = \omega^{1112907},\ b_2 = \omega^{873995},\ b_3 = \omega^{664681}$$

が計算できる．よって ω の指数部から中国剰余定理より

$$1112907 \to \{100, 1, 0\},\ 873995 \to \{54, 98, 32\},\ 664681 \to \{0, 23, 40\}$$

が計算できる．b_1, b_2, b_3 の指数部が 1 でもずれると結果は全く異なるものとなる（(b_3 の指数部)+1 $=$ $664682 \to \{59, 10, 98\}$）．従って Hankel 方程式の解 b_j は大体 π/m までの誤差を許容し，高すぎる次数の上界を取ると誤差・摂動に弱くなることがわかる．

逆に真でない上界を利用することで以下のように誤差・摂動に強くすることができるという予想ができる.

例 7
与えられたブラックボックスを $f = x_1^{100}x_2$ とする.

$$\text{次数の上界を } \tilde{D}_1 = 13, \quad \tilde{D}_2 = 19 \text{ とすると出力は } x_1^9 x_2$$
$$\text{次数の上界を } \tilde{D}_1 = 17, \quad \tilde{D}_2 = 19 \text{ とすると出力は } x_1^{15} x_2$$

したがって中国剰余定理から $x_1^{100}x_2$ が構成され, $D_1 = 101$, $D_2 = 19$ として計算した場合よりも誤差・摂動に強いと予想される.

またこの手法には以下の課題点がある.

例 8
与えられたブラックボックスを $f = x_1^{100}x_2 + x_1^5$ とする.

$$\text{次数の上界を } \tilde{D}_1 = 13, \quad \tilde{D}_2 = 19 \text{ とすると出力は } x_1^9 x_2 + x_1^5$$
$$\text{次数の上界を } \tilde{D}_1 = 17, \quad \tilde{D}_2 = 19 \text{ とすると出力は } x_1^{15} x_2 + x_1^5$$

このとき上の行で $x_1^9x_2$ となった項に対応する項が下の行では $x_1^{15}x_2$ なのか x_1^5 なのかわからないことが問題となる. 一般に係数が同じで項の区別がつかないと, 考えられる項の構成の仕方が一つではないので, 構成の仕方を 1 つ 1 つ試さないといけない.

提案手法をアルゴリズムとして書くと以下の様になる. ここでは簡単のため入力に次数の上界を要求しているが, 前章で述べた方法を用いることで次数の上界を要求しないアルゴリズムを設計できる. またブラックボックスの係数は区別できるとしているが係数が区別できない場合でも項の構成の組み合わせを総当たりで試すことで計算可能なアルゴリズムを設計できる.

アルゴリズム 4
Input: 出力に数値的誤差を含む項数 t のブラックボックス n 変数多項式

$$f(x_1, \ldots, x_n) = \sum_{j=1}^{t} c_j x_1^{d_{j1}} \ldots x_n^{d_{jn}} \ (d_{jk}\text{は非負整数}, \ c_j(\neq 0) \text{ は複素数}) \ ,$$
$$D_1, \ldots, D_n\text{: } D_j > \deg(f_{x_j}), \ D_1, \ldots, D_n\text{は互いに異なる素数}$$
$$(\deg(f_{x_j}) \text{ は変数 } x_j\text{についての } f \text{ の次数を表す}) \ .$$

Output: $d_{j,k}$, c_j $(1 \leq j \leq t, \ 1 \leq k \leq n)$

(1) 各 D_k に対して $D_k < \tilde{D}_{1,k} \ldots \tilde{D}_{l,k}$ を適当に設定し $\{\tilde{D}_{1,1}, \ldots, \tilde{D}_{1,n}\}, \ldots, \{\tilde{D}_{l,1}, \ldots, \tilde{D}_{l,n}\}$ をそれぞれ上界として l 回 GLL または CLru を用いる.

(2) 得られた各出力から係数が同じ指数を取り出して中国剰余定理から真の指数を計算して対応する係数と共に結果とする.

注意 2
- 方程式が悪条件 (または非正則) のときは randomized reconditioning と同時に対応する真でない上界を変化させる.

4.1 数値実験

上記の予想を数値実験により確かめる．ブラックボックス f の出力に実数値の摂動を加えた補間の計算を 100 回行い，正しい結果が返ってきた回数をカウントする．実験環境は第 3 章で述べたものと同様である．精度は 10 進 20 桁とし，表にある摂動の大きさは相対でなく絶対とする．

例 9

表 2 は $f = x_1^{100}x_2 + 123x_2^{23}x_3^{40} + 8x_1^{54}x_2^{98}x_3^{32}$ の実験結果である．真の上界は $B = \{101, 103, 107\}$, 真でない上界は $B_1 = \{13, 17, 19\}$, $B_2 = \{17, 19, 23\}$ としている．この結果から，真でない上界を用いたほうが摂動に強いことがわかる．

表 2: $f = x_1^{100}x_2 + 123x_2^{23}x_3^{40} + 8x_1^{54}x_2^{98}x_3^{32}$

摂動の大きさ	真の上界	真でない上界
$10^{-11} \sim 10^{-10}$	100	100
$10^{-10} \sim 10^{-9}$	97	100
$10^{-9} \sim 10^{-8}$	87	95
$10^{-8} \sim 10^{-7}$	84	95
$10^{-7} \sim 10^{-6}$	60	88
$10^{-6} \sim 10^{-5}$	28	91
$10^{-5} \sim 10^{-4}$	4	55
$10^{-4} \sim 10^{-3}$	0	18

例 10

表 3 は $f = x_1^{1000}x_2^{10} + 123x_2^{230}x_3^{400} + 8x_1^{540}x_2^{980}x_3^{320}$ の実験結果である．真の上界は $B = \{1009, 1013, 1019\}$, 真でない上界は $B_1 = \{13, 17, 19\}$, $B_2 = \{17, 19, 23\}$, $B_3 = \{19, 23, 29\}$ としている．真の上界を用いている計算は例 9 と比較すると，各次数の上界を 10 倍しているので摂動に対しては大体 10^3 倍弱くなっているといえる．真でない上界を用いている計算は例 9 と比較すると，計算回数が 2 回に分けていたものが 3 回になったのでその分計算の成功率が下がっている．

表 3: $f = x_1^{1000}x_2^{10} + 123x_2^{230}x_3^{400} + 8x_1^{540}x_2^{980}x_3^{320}$

摂動の大きさ	真の上界	真でない上界
$10^{-11} \sim 10^{-10}$	88	100
$10^{-10} \sim 10^{-9}$	66	100
$10^{-9} \sim 10^{-8}$	31	99
$10^{-8} \sim 10^{-7}$	6	95
$10^{-7} \sim 10^{-6}$	0	87
$10^{-6} \sim 10^{-5}$	0	72
$10^{-5} \sim 10^{-4}$	0	40
$10^{-4} \sim 10^{-3}$	0	13

4.2 オーバーサンプリング

誤差に強い補間を実現する既存の手法としてオーバーサンプリングがある．具体的には Hankel 方程式を

$$\begin{pmatrix} \alpha_0 & \cdots & \alpha_{t-1} \\ \alpha_1 & \cdots & \alpha_t \\ \vdots & \ddots & \vdots \\ \alpha_{2T-t-1} & \cdots & \alpha_{2T-2} \end{pmatrix} \begin{pmatrix} \lambda_0 \\ \lambda_1 \\ \vdots \\ \lambda_{t-1} \end{pmatrix} = - \begin{pmatrix} \alpha_t \\ \alpha_{t+1} \\ \vdots \\ \alpha_{2T-1} \end{pmatrix} \quad (T > t)$$

という矩形の係数行列にして，最小二乗法で解く方法である．今回の提案手法とオーバーサンプリングを数値実験で比較する．

真の上界は $B = \{1009, 1013, 1019\}$，真でない上界は $B_1 = \{13, 17, 19\}$，$B_2 = \{17, 19, 23\}$，$B_3 = \{19, 23, 29\}$, t を実際の項数として，P1: 真の上界，P2: 真でない上界，P3: オーバーサンプリング $(T = 2t)$ and 真の上界，P4: オーバーサンプリング $(T = 2t)$ and 真でない上界，P5: オーバーサンプリング $(T = 4t)$ and 真の上界 の 5 種類の問題を解く．すなわち P2 が提案手法，P4 が提案手法とオーバーサンプリングの組み合わせである．

例 11

表 4 は $f = x_1^{1000}x_2^{10} + 123x_2^{230}x_3^{400} + 8x_1^{540}x_2^{980}x_3^{320}$ の実験結果である．提案手法である P2 と P4 の優位性がわかる．

表 4: $f = x_1^{1000}x_2^{10} + 123x_2^{230}x_3^{400} + 8x_1^{540}x_2^{980}x_3^{320}$

摂動の大きさ	P1	P2	P3	P4	P5
$10^{-11} \sim 10^{-10}$	84	100	95	100	100
$10^{-10} \sim 10^{-9}$	67	99	91	100	97
$10^{-9} \sim 10^{-8}$	37	99	78	100	90
$10^{-8} \sim 10^{-7}$	4	95	37	100	61
$10^{-7} \sim 10^{-6}$	0	87	0	98	3
$10^{-6} \sim 10^{-5}$	0	69	0	95	0
$10^{-5} \sim 10^{-4}$	0	39	0	82	0
$10^{-4} \sim 10^{-3}$	0	8	0	47	0

例 12

表 5 は係数が $-1 \sim 1$ (すべて区別がつく)，項数が 20 の 3 変数多項式の実験結果である．提案手法の 1 つである P2 は既存手法の P3 より劣っている．しかし P4 はブラックボックスの評価回数が同一である P5 と比較して優位性が示されている．また P4 の合計 800 回の補間計算の所要時間は 292 秒，P5 の合計 800 回の補間計算の所要時間は 387 秒であることから，計算速度の面からも優位性が示される．

5 手法の改良

提案手法の改良として以下の方法が考えられる．

表 5: f : 3 変数，係数が $-1 \sim 1$，項数が 20

摂動の大きさ	P1	P2	P3	P4	P5
$10^{-11} \sim 10^{-10}$	0	2	14	69	37
$10^{-10} \sim 10^{-9}$	0	0	1	52	17
$10^{-9} \sim 10^{-8}$	0	0	1	34	2
$10^{-8} \sim 10^{-7}$	0	0	0	12	0
$10^{-7} \sim 10^{-6}$	0	0	0	4	0
$10^{-6} \sim 10^{-5}$	0	0	0	0	0
$10^{-5} \sim 10^{-4}$	0	0	0	0	0
$10^{-4} \sim 10^{-3}$	0	0	0	0	0

例 13

与えられたブラックボックスを $f = x^{99} + 8x^{88} + x^{66}$ とし，真でない次数の上界 $\tilde{D} = 13$ を入力として GLL を用いると，出力は $x^8 + 8x^{10} + x$ となる．命題 2 を用いて指数 99 を得たのち，$\tilde{D} = 13$ で割った余りからブラックボックスの先頭項は出力の x^8 に対応することから x^{99} であることがわかる．ここで $f - x^{99}$ に対して命題 2 を用いると指数 88 が得られる．以下同様の議論で，2 回目の連立方程式の計算を行うことなく次数の上界を要求しない補間が可能となる．また，次数の上界を真の上界より低いものでとった計算しかしていないことから，摂動に強い補間法にもなっている．その上前章で述べた係数を区別できない場合の課題も解消されている．

以上の方法は多変数多項式の場合においても以下の命題を用いることで 1 変数多項式にすることで適用できる．

命題 3 (Kronecker substitution の変形)

$f \in F[x_1, \ldots, x_n]$($F$ は体), $\deg f_{x_j} < D_j$とすると

$\hat{f} = f(x,\ x^{D_1},\ x^{D_1 D_2},\ \ldots,\ x^{D_1 \cdots D_{n-1}}) \in F[x]$ の項は f の項と *1* 対 *1* 対応する

従って例 13 の方法をアルゴリズムの形に書くと以下の様になる．

アルゴリズム 5

Input: 出力に数値的誤差を含む項数 t のブラックボックス n 変数多項式

$$f(x_1, \ldots, x_n) = \sum_{j=1}^{t} c_j x_1^{d_{j1}} \ldots x_n^{d_{jn}} \ (d_{jk}\text{は非負整数},\ c_j(\neq 0)\ \text{は複素数})$$

Output: $d_{j,k},\ c_j\ (1 \leq j \leq t,\ 1 \leq k \leq n)$

(1) 互いに異なる素数 $\tilde{D}_1, \ldots, \tilde{D}_k$ を適当に設定し $\tilde{D}_1, \ldots, \tilde{D}_k$ を上界として GLL または CLru を用いる．出力の係数を c_j, 指数部を $\tilde{d}_{j,k}$ とする．

(2) 各 k に対して $e_l\ (0 \leq e_l < \tilde{D}_l)$ を $f_k(x) = f(\omega_1^{e_1}, \ldots, \omega_{k-1}^{e_{k-1}}, x, \omega_{k+1}^{e_{k+1}}, \ldots, \omega_n^{e_n})$ で打消しが起こらない形になるようにとる．

f_k に命題 2 を用いて正しい D_k を得る．

(3) $\tilde{D}_k$ が適切な次数の上界であれば c_j, $\tilde{d}_{j,k}$ を結果とする.

そうでなければ命題 3 を用いて 1 変数多項式に変形して命題 2 から先頭項の指数を得て，命題 3 で多変数の表現に直した後各 $\tilde{D}_k$ の剰余から対応する係数を求める．ブラックボックスからこの先頭項を引いて同様の操作を行う．この操作を繰り返すことで得られた係数と指数の組を結果とする.

注意 3

- 方程式が悪条件 (または非正則) のときは randomized reconditioning と同時に $\tilde{D}_k$ を変化させる.
- 計算時間は元の手法に命題 2 を用いる時間と (3) にかかる時間を足したものになる.

応用によっては命題 3 を用いた多項式に命題 2 を用いる際大きな値をブラックボックスに代入する計算が困難である可能性がある.

6 項数の推定手法

これまで紹介した疎な多変数多項式の補間の手法ではブラックボックスの項数を入力に要求していた．しかし応用上項数が事前にわからない場合が想定される．項数の推定手法についての研究は [7] などがある．以下 [7] のアイデアについて簡単に解説する.

ブラックボックスの真の項数を t, 項数の入力を s としたときの Hankel 方程式の係数行列を H_s とすると，入力の項数 s を t より大きな値としたとき H_s が特異になる．このことから，入力の項数をしだいに増やして $\det H_s \neq 0$, $\det H_{s+1} = 0$ となる s を見つけることが出来る．この s は正確には $s = t$ を満たすとは限らないが，高確率で $s = t$ となる．このことを利用して確率的に項数を推定しているのが [7] であり，数値的誤差を含む場合では正確に $\det H_s = 0$ であるか判定ができないので悪条件性を基準とした手法 [8] や 0 に近い特異値を持つことを基準とした手法 [6] が提案されている.

本稿の提案手法でのブラックボックスの項数推定では，例 3 のように真でない次数の上界を入力したことにより連立方程式の係数行列が特異になる場合も考察しなければならない．ブラックボックスの項の指数の分布がランダムであると仮定すると，項数 t のブラックボックスの各項の指数を $\tilde{D}_1, \ldots, \tilde{D}_n$ で剰余を取ったとき重複する指数が出ない確率は $m = \tilde{D}_1 \ldots \tilde{D}_n$ としたとき

$$\frac{m(m-1)\cdots(m-t+1)}{m^t}$$

となる．従って本稿の提案手法においてはもともとの項数推定の成功確率と上式の確率を掛けたものが項数推定の成功確率となる.

7 おわりに

本稿では数値的誤差を含む設定の下で，多変数多項式の補間において次数の上界を外したアルゴリズムを紹介し，新たにブラックボックスの出力に対する摂動に強い補間アルゴリズムおよびこれらの手法の改良を提案した．また数値実験により既存手法と比較し提案手法の優位性を示した．これらの手法は応用により一長一短になると考えられる．今後の課題として，提案手法で項の打消しを回避できるかの十分な解析，方程式を解く際の手法選択 (Hankel 方程式，一般固有値問題，QD アルゴリズム)，他の設定 (例えば [2]) での疎な多変数多項式の補間における次数の上界を外したアルゴリズムの設計，より詳細なオーバーサンプリングと提案手法の比較，提案手法の近似 GCD や近似因数分解 [4] への応用などが挙げられる.

参 考 文 献

[1] M. Ben-Or and P. Tiwari. A deterministic algorithm for sparse multivariate polynomial interpolation. In *Proc. 20th Annual ACM Symp. Theory Comput.*, pages 301–309, New York, N.Y., 1988. ACM.

[2] M. T. Comer, E. L. Kaltofen, and C. Pernet. Sparse polynomial interpolation and Berlekamp/Massey algorithms that correct outlier errors in input values. In *Proc. 37th Internat. Symp. Symb. Alg. Comput.*, pages 138–145. ACM, 2012.

[3] A. Cuyt and W.-s. Lee. A new algorithm for sparse interpolation of multivariate polynomials. *Theoretical Computer Science*, 409 (2):180–185, 2008.

[4] S. Gao, E. Kaltofen, J. P. May, Z. Yang, and L. Zhi. Approximate factorization of multivariate polynomials via differential equations. In *Proc. 2004 Internat. Symp. Symbolic Algebraic Comput.*, ISSAC ' 04, pages 167—174.

[5] M. Giesbrecht, G. Labahn, and W.-s. Lee. Symbolic-numeric sparse interpolation of multivariate polynomials. *J. Symbolic Comput.*, 44:943–959, 2009.

[6] Z. Hao, E. L. Kaltofen, and L. Zhi. Numerical sparsity determination and early termination. In *Proc. 2016 ACM Internat. Symp. Symbolic Algebraic Comput.*, ISSAC'16, pages 247-254.

[7] E. Kaltofen and W.-s. Lee. Early termination in sparse interpolation algorithms. *J. Symbolic Comput.*, 36(3-4):365-400, 2003.

[8] E. L. Kaltofen, W.-s. Lee, and Z. Yang. Fast estimates of hankel matrix condition numbers and numeric sparse interpolation. In *Proc. 2011 Internat. Workshop Symb.-Numer. Comput.*, SNC'11, pages 130–136, New York, NY, USA, 2011. ACM.

[9] 沼畑大, 次数の上限を要求しない数値的誤差を含む疎な多変数多項式の補間, 数式処理, 掲載決定.

[10] R. Zippel. Probabilistic algorithms for sparse polynomials. In *Proc. EUROSAM '79. In: Lecture Notes in Comput. Sci., vol. 72.* Springer-Verlag, Heidelberg, Germany, pages 216–226.