

多変数 Hensel 構成における展開点の 特異点からの距離

長坂 耕作 (Kosaku Nagasaka) *

筑波大学大学院数学研究科

DOCTORAL PROGRAM OF MATHEMATICS, UNIV. OF TSUKUBA

1 はじめに

因数分解などの代数演算に使われる多変数多項式の Hensel 構成は，浮動小数を用いて計算した場合，丸め誤差や桁落ち誤差などにより破綻することがある．特に桁落ち誤差の影響は大きい．例えば，次の減算是大きな桁落ち誤差を生じる（有効数字が 9 術失われる）．

$$0.\underline{3674301083421}?? - 0.\underline{3674301082389}?? = \underline{1.032}????????? \times 10^{-10}, \quad (1)$$

ここで，下線部は有効数字である．よって，浮動小数を用いて多変数多項式の Hensel 構成を行う場合，桁落ち誤差が発生することを考慮する必要がある．

多変数多項式の Hensel 構成は幅広く使われているが，その誤差解析はあまり進んでいない．これまでの研究は次の 2 つ．佐々木と山口 [SY98] は，特異点近傍に展開点を取ると大きな桁落ち誤差が生じることを示した．その解析は Cauchy-Hadamard の定理に基づいており，因子が特異点において整数べき（交差）の場合に桁落ち誤差が生じることを示している．佐々木 [Sas00] は項消去の 4 つのメカニズムを明らかにしている．

しかしながら，実際の計算において桁落ち誤差を予測することは次のような観点から難しい．(1) 通常，特異点の位置は未知である．(2) 通常，因子が交差しているかは未知である．そこで，本論ではこれらの点を考慮しつつ桁落ち誤差の見積もりを議論する．2 章で多変数多項式の Hensel 構成を紹介し，展開点の特異点までの距離の見積もりについて 3 章で論ずる．桁落ち誤差の見積もりを 4 章で，数値実験例を 5 章で示し，6 章でまとめを行う．

本論では，次の記号を用いる．

- $F(x, u_1, \dots, u_\ell)$: $\mathbb{C}[x, u_1, \dots, u_\ell]$ の多変数多項式，Hensel 構成する与式;
 x, u_1, \dots, u_ℓ : 変数， x を主変数とする；
 u : u_1, \dots, u_ℓ の省略表記，(例， $F(x, u) = F(x, u_1, \dots, u_\ell)$)；

*nagasaka@math.tsukuba.ac.jp

- $\deg(P)$: 多項式 P の x に関する次数 , $n = \deg(F)$ とする;
 $\omega_1, \dots, \omega_n$: $F(x, 0)$ の根;
 S : u_1, \dots, u_ℓ によって生成される多項式イデアル , $\langle u_1, \dots, u_\ell \rangle$;
 $\text{Syl}(P_1, P_2)$: 多項式 P_1 と P_2 の Sylvester 行列;
 $\|P\|_p$: 多項式 $P = \sum_{i=0}^n c_i x^i$ の次式で定義されるノルム ,
 $\|P\|_p = (\sum_i |c_i|^p)^{1/p}$ ($p < \infty$), $\|P\|_\infty = \max_i |c_i|$;
 $\gcd(P_1, P_2)$: 多項式 P_1 と P_2 の最大公約因子 .

本論では , $F(x, u)$ を x に関してモニックで無平方 , 次式の F_i で $F_1(x, u) \neq 0$ を仮定する .

$$\begin{aligned} F(x, u) &= F_0(x, u) + F_1(x, u) + \cdots + F_{e-1}(x, u) + F_e(x, u), \\ e &= \deg_{u_1, \dots, u_\ell}(F), \quad \deg_{u_1, \dots, u_\ell}(F_i) = i \quad (i = 0, 1, \dots, e). \end{aligned} \tag{2}$$

Hensel 構成を行う展開点を原点とし , 原点で $F(x, u)$ が特異な場合は適当な変数変換を行うとする (特異の定義は次章で述べる) . また , 一般性を失わず $F(x, 0)$ は x に関してモニックで無平方であるとする . 更に , 本論においては , 次の制約 **R** を課す .

R: $F(x, u)$ は疎でなく , $\|F(x, u)\|_\infty \simeq 1$ かつ $\|F_1(x, u)\|_1 \gg \|F_j(x, u)\|_1$ ($j > 1$) を満たす .

桁落ち誤差の監視には , 加古と佐々木 [KS97] による有効浮動小数を用いる . *Mathematica* も似た仕組みを備えているが , 丸め誤差も同列に扱うため今回の目的に合致しない .

2 多変数多項式の Hensel 構成

この章では , 次のような初期因子 $G^{(0)}$ と $H^{(0)}$ に関し , Hensel 構成を簡単に紹介する .

$$G^{(0)} = \prod_{i \in N_G} (x - \omega_i), \quad H^{(0)} = \prod_{i \in N_H} (x - \omega_i), \quad m = \#N_G, \tag{3}$$

ここで , N_G と N_H は $N_G \cap N_H = \emptyset$ かつ $N_G \cup N_H = \{1, \dots, n\}$ を満たす . また , $\gcd(G^{(0)}, H^{(0)}) \neq 1$ のとき , $F(x, u)$ は原点で特異であるという . 展開点 (今回は原点) で特異な場合 , Hensel 構成を行うことは出来ない .

多変数多項式の Hensel 構成は , 次式の $G^{(k)}(x, u)$ と $H^{(k)}(x, u)$, $k = 1, 2, \dots$ を計算する .

$$\begin{aligned} F(x, u) &\equiv G^{(k)}(x, u)H^{(k)}(x, u) \pmod{S^{k+1}}, \\ G^{(0)} &\equiv G^{(k)}(x, u), \quad H^{(0)} \equiv H^{(k)}(x, u) \pmod{S}. \end{aligned} \tag{4}$$

実際の構成にあたっては , 事前に拡張 Euclid の互除法を用いて次式を満たす Moses-Yun の補間多項式 $A_i(x)$ と $B_i(x)$ ($i = 0, \dots, n-1$) を求めておく必要がある .

$$\begin{cases} A_i(x)H^{(0)}(x) + B_i(x)G^{(0)} = x^i & (i = 0, \dots, n-1), \\ \deg(A_i) < \deg(G^{(0)}), \quad \deg(B_i) \leq \deg(H^{(0)}). \end{cases} \tag{5}$$

$G^{(\kappa)}$ と $H^{(\kappa)}$ ($\kappa = 0, 1, \dots, k-1$) から $G^{(k)}$ と $H^{(k)}$ を構成する方法を述べる .

$$\text{Step 1} \quad \underline{D}^{(k)} \equiv G^{(k-1)}H^{(k-1)} \pmod{S^{k+1}}. \tag{6}$$

$$\text{Step 2} \quad D^{(k)} \equiv F - \underline{D}^{(k)} \equiv \sum_{i=0}^{n-1} d_i^{(k)} x^i \pmod{S^{k+1}}. \tag{7}$$

$$\text{Step 3} \quad G_k = \sum_{i=0}^{n-1} A_i d_i^{(k)}, \quad H_k = \sum_{i=0}^{n-1} B_i d_i^{(k)}. \tag{8}$$

$$\text{Step 4} \quad G^{(k)} = G^{(k-1)} + G_k, \quad H^{(k)} = H^{(k-1)} + H_k. \tag{9}$$

3 特異点からの距離

この章では、原点(展開点)から最も近い特異点までの距離について議論する。

定義 1

$F(x, u)$ の原点に最も近い特異点を v とし、原点から v までの距離を δ と定義する。つまり、 $F(x, v)$ は x に関して無平方でなく、少なくとも重根を持つ。

$\omega_1^*, \dots, \omega_n^*$ を $\sum_{i=1}^n |\omega_i - \omega_i^*|$ を最小にするような $F(x, v)$ の根とし、下記を定義する。

$$\Delta_G = G^{(0)} - G^{(0)*}, \quad \Delta_H = H^{(0)} - H^{(0)*}, \quad G^{(0)*} = \prod_{i \in N_G} (x - \omega_i^*), \quad H^{(0)*} = \prod_{i \in N_H} (x - \omega_i^*).$$

制約 Rにより、 $\delta \gg 1$ ということはほとんどの場合起こらない。更に言えば、[Sas00]によれば、彼らの制限の元、特異点が展開点から遠方にあるとき大きな桁落ち誤差は生じない。よって、本論では $\delta \simeq 1$ と $\delta \ll 1$ の場合のみ扱う。従って、

$$\begin{aligned} F(x, 0) - F(x, v) &= G^{(0)} H^{(0)} - G^{(0)*} H^{(0)*} \\ &= G^{(0)} H^{(0)} - (G^{(0)} - \Delta_G)(H^{(0)} - \Delta_H) \\ &= G^{(0)} \Delta_H + \Delta_G H^{(0)} - \Delta_G \Delta_H \\ &= F_1(x, v) + \dots + F_e(x, v). \end{aligned} \tag{10}$$

より、次式が成立する。

$$\|F_1(x, v)\|_1 \simeq \|G^{(0)}\|_1 \|\Delta_H\|_1 + \|H^{(0)}\|_1 \|\Delta_G\|_1 + \|\Delta_G\|_1 \|\Delta_H\|_1. \tag{11}$$

多項式 $G^{(0)*}$ と $H^{(0)*}$ は、元の初期因子 $G^{(0)}$ と $H^{(0)}$ が GCD を持つように係数を変化させたものだと考えられる。そこで、近似 GCD 問題に関する Beckermann と Labahn [BL98] の結果を引用しておく。

定義 2 ([BL98] ϵ -prime)

$\epsilon(G^{(0)}, H^{(0)})$ を次式で定義する。

$$\epsilon(G^{(0)}, H^{(0)}) := \inf \max\{\|G^{(0)} - G^*\|_1, \|H^{(0)} - H^*\|_1\}, \tag{12}$$

ここで G^* と H^* は共通根を持つ $\deg(G^*) \leq m$ かつ $\deg(H^*) \leq n - m$ を満たす多項式。

補題 3 ([BL98] Lemma 2.1)

$$\epsilon(G^{(0)}, H^{(0)}) \geq \frac{1}{\|\text{Syl}(G^{(0)}, H^{(0)})^{-1}\|_1}. \tag{13}$$

補題 4 ([BL98] Corollary 3.2)

$$\kappa := \max\{\|A_0 + x^m B_0\|_1, \|A_{n-1} + x^m B_{n-1}\|_1\}. \tag{14}$$

に対して、次式が成立する。

$$\kappa \leq \|\text{Syl}(G^{(0)}, H^{(0)})^{-1}\|_1 \leq \kappa + 2 \|B_{n-1} A_0 - A_{n-1} B_0\|_1 \max\{\|G^{(0)}\|_1, \|H^{(0)}\|_1\}. \tag{15}$$

$G^{(0)*}$ と $H^{(0)*}$ は、その定義より制約があり、 $G^{(0)}$ と $H^{(0)}$ の近似 GCD を持つ多項式には一般に一致しないため、次の不等式のみ成立する。

$$\epsilon(G^{(0)}, H^{(0)}) \leq \max\{\|G^{(0)} - G^{(0)*}\|_1, \|H^{(0)} - H^{(0)*}\|_1\} = \max\{\|\Delta_G\|_1, \|\Delta_H\|_1\}. \tag{16}$$

定理 5

以上の議論により， δ は次のように見積もられる．

$$\delta = (\kappa^{-1} \|G^{(0)}\|_1 + \kappa^{-1} \|H^{(0)}\|_1 + \kappa^{-2}) / \|F(x, u)\|_1. \quad (17)$$

この見積もりは，3変数以上のときは特異点の各変数の大きさがほぼ等しいことを仮定している．また，この見積もりに必要な κ は，Hensel 構成に必要な計算 (5) でほとんど求まっているので， δ の見積もりのために，Hensel 構成に不要な計算をする必要はない．

4 衍落ち誤差の見積もり

この章では，展開点からの特異点までの距離を用いて，Hensel 構成で生じる衍落ち誤差を事前に見積もることを考える．シンプルなモデルの導入により，簡便な判定法を目指す．

いま $P(x, u) = G(x, u)H(x, u)$ を G と H から計算しようとすると仮定する．もしも， $\|P(x, u)\|_\infty$ に比べて $\|G(x, u)\|_\infty \times \|H(x, u)\|_\infty$ が大きければ，衍落ちが生じる可能性がある．この章では，衍落ち誤差の発生を見積もるために， $\|G^{(k)}\|_\infty$ や $\|H^{(k)}\|_\infty$ などの大きさを見積もり，衍落ち誤差の発生について議論する．

まず [SY98] と同じように，分岐と交差を定義する．

定義 6 ([SY98] branching and crossing)

t を u_1, \dots, u_ℓ に関する全次数変数とし， $F(x, tu)$ を次式のように t に関して分数べきの範囲で因数分解される，原点に特異点を持つ多変数多項式とする．

$$F(x, tu) = G(x, tu)H(x, tu), \quad (18)$$

このとき， $G(x, tu)$ と $H(x, tu)$ が t に関して整数べき級数ならば，原点で交差していると言う．そうでない場合，分岐していると言う．

Cauchy-Hadamard の定理により， $k \gg 1$ に対して次式が成り立つ．

$$\text{分岐: } \frac{\|G^{(k+1)}\|_\infty}{\|G^{(k)}\|_\infty}, \frac{\|H^{(k+1)}\|_\infty}{\|H^{(k)}\|_\infty} = O(\delta^{-1}), \quad \text{交差: } \frac{\|G^{(k+1)}\|_\infty}{\|G^{(k)}\|_\infty}, \frac{\|H^{(k+1)}\|_\infty}{\|H^{(k)}\|_\infty} = O(\delta^0),$$

ここで， O は Landau のオーダー記号を表す． $k \geq 1$ に対しても同様のオーダー評価が可能と仮定すれば，分岐の場合，次式が成り立つ．

$$\|G_k\|_\infty \approx \|G_1\|_\infty + (k-1)\delta^{-1}, \quad \|H_k\|_\infty \approx \|H_1\|_\infty + (k-1)\delta^{-1}. \quad (19)$$

G_k と H_k の ∞ ノルムについて考える．

$$\|G_k\|_\infty = \left\| \sum_{i=0}^{n-1} A_i d_i^{(k)} \right\|_\infty \rightarrow \max_i \|A_i\|_\infty |d_i^{(k)}|. \quad (20)$$

$$\|H_k\|_\infty = \left\| \sum_{i=0}^{n-1} B_i d_i^{(k)} \right\|_\infty \rightarrow \max_i \|B_i\|_\infty |d_i^{(k)}|. \quad (21)$$

$|d_i^{(k)}|$ に関しては，(6) より $\|\underline{D}^{(k)}\|_\infty \leq \max_{i+j=k, i, j < k} \|G_i\|_\infty \|H_j\|_\infty = \|G_1\|_\infty + \|H_1\|_\infty + (k-2)\delta^{-1}$ が成り立っている．これらの大きさを比較すると，(19) と (20) (ないしは (21)) の間に大きな違いがあれば，

そこで桁落ち誤差が生じる可能性が高い。ここで注目すべき点は、 G_k (H_k に関しても同様) の計算において、 A_i と $D^{(k)}$ に含まれる絶対値最大の項が掛け合わされるとは限らないことである。そこで、次のような簡単なモデルを考える。

$$\max_i \|A_i\|_\infty |d_i^{(k)}| \approx \|A_{j_1}\|_\infty \|\underline{D}^{(k)}\|_\infty, \quad \max_i \|B_i\|_\infty |d_i^{(k)}| \approx \|B_{j_2}\|_\infty \|\underline{D}^{(k)}\|_\infty, \quad (22)$$

ここで、 j_1 と j_2 は次式を最大化する整数である。

$$\begin{aligned} A_G &= \max_{j_1} \|A_{j_1}\|_\infty |G_1(x, u)H_1(x, u)|, \\ B_H &= \max_{j_2} \|B_{j_2}\|_\infty |G_1(x, u)H_1(x, u)|. \end{aligned} \quad (23)$$

以上のモデルを用いて係数部の大きさを比較すると次の定理が導き出される。

定理 7

分岐の場合、 k 次までの構成で発生する桁落ち誤差の大きさは次式で見積もることが出来る。

$$\max\{A_G/(\|G_1(x, u)\|_\infty \times \delta), B_H/(\|G_1(x, u)\|_\infty \times \delta)\}^k. \quad (24)$$

注意 1

交差の場合、係数の大きさが一定と仮定すれば、(24)において $\delta = 1$ とした式で見積もることが可能であろう。また、上記モデルは G_1H_1 の係数間の大きさの関係が、 G_kH_k の関係に大体等しいことを暗黙に仮定しているが、実験によれば全く関係ない場合も少なからずある。

5 数値実験の結果

今回導出した見積もりの精度を倍精度の浮動小数を用いて調査した。まず、 x と u_1 の次数がそれぞれ n と e の二変数多項式を 100 個生成した。その係数は実区間 $[-1, 1]$ からランダムに決定した。そして k 次まで Hensel 構成を行った。図 1 と 2 は、その結果を図示したものである。“Actual δ^{-k} ” は、 $\|G^{(k)}\|_\infty$ と $\|H^{(k)}\|_\infty$ の平均を、“Estimation of δ^{-k} ” は、(17) による見積もりを表し，“reducible” と “irreducible” は、生成し実験に用いた多項式が可約か既約かを表している（ただし、初期因子として $F(x, 0)$ の根の全ての組み合わせを用いている）。図 3 と 4 も結果を図示したものであり、“Actual Errors” は、実際の計算において生じた桁落ち誤差の大きさを、“Estimation of Cancellation Errors” は、前章で議論した見積もり（(17) による δ ではなく、より正確な実測値を用いて計算したもの）を表している。全ての図は、常用対数グラフであり、目盛は数の桁数を表す。

図 1 では、 δ の見積もりが実際の係数の大きさに近いことがわかる。逆に図 2 では、 δ の見積もりは過大になりすぎている。この過大見積もりの原因是、与式の可約性により不等式 (16) の両辺の差が大きくなっているためと思われる。また、Hensel 因子 $G^{(k)}$ と $H^{(k)}$ が厳密に、ないしは近似的に F の多項式因子であれば、それらは交差しており係数の絶対値は大きくならないだろう。

図 3 では、今回実験に使用した既約多項式の場合、大きな桁落ち誤差を生じていないことがわかる。逆に図 4 では、ほぼ桁落ち誤差の大きさを見積もれている。図の中央から上辺に位置しているデータ群は、Hensel 因子が与式の既約因子の場合であり、桁落ち誤差は問題とならない。なぜなら、既約因子の場合 $D^{(k)} \simeq 0$ なる k が存在しており、有効桁が失われるのはその次数以上の計算においてであるからだ。

6まとめ

本論では、多変数多項式の Hensel 構成における桁落ち誤差について議論した。数値実験によれば、 δ の実測値を用いれば今回の見積もりが実際の計算に使用できそうなことがわかる。(24) による見積もりは、小

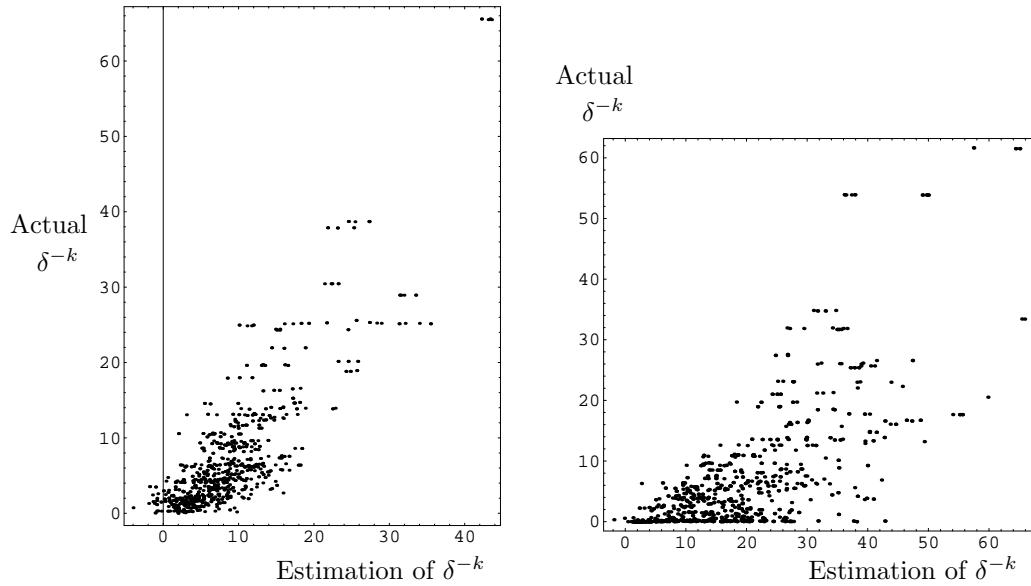


Fig. 1: irreducible, $n = 5$, $e = 5$ and $k = 24$. Fig. 2: reducible, $n = 5$, $e = 5$ and $k = 24$.

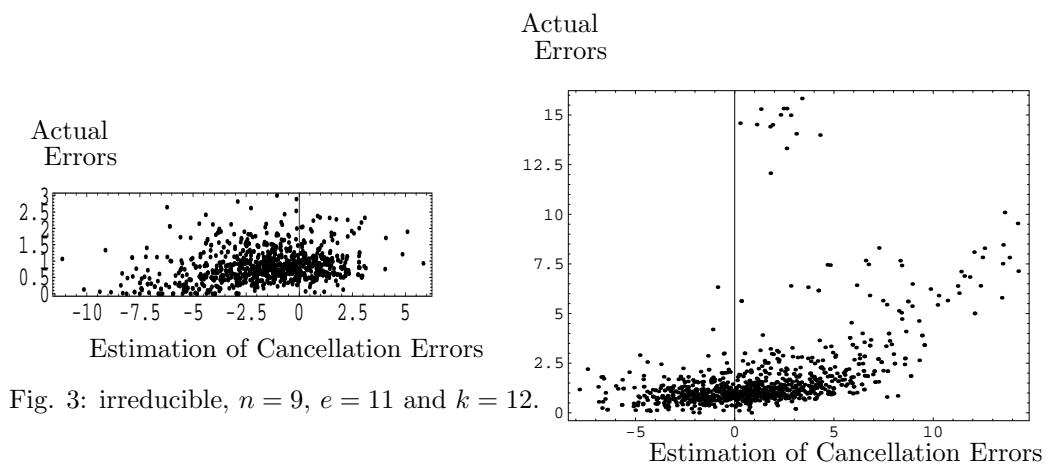


Fig. 3: irreducible, $n = 9$, $e = 11$ and $k = 12$.

Fig. 4: reducible, $n = 9$, $e = 11$ and $k = 12$.

さい桁落ち誤差は図 3 にあるように検出出来てないが、図 4 のような大きな桁落ち誤差の検出には成功している。大きな桁落ち誤差が見込まれる場合、失われる桁分だけ精度を増やして計算することが可能となる。

しかしながら、 δ の実測値を用いずに (17) による見積もりを使うと、可約多項式に対して過大な見積もりを行ってしまい、桁落ち誤差の見積もりは破綻する(そのため、図 4 では δ の実測値を用いている)。より効果的な δ の見積もりが桁落ち誤差の見積もりには必要であることがわかる。

参 考 文 献

- [BL98] B. Beckermann and G. Labahn. When are two numerical polynomials relatively prime? *J. Symb. Comput.* (1998) **267**, 677–689.
- [KS97] F. Kako and T. Sasaki. Proposal of “effective floating-point number” for approximate algebraic computation. *preprint*, 10 pages (1997).
- [Sas00] T. Sasaki. Mechanism of cancellation errors in multivariate Hensel construction with floating-point numbers. *preprint*.
- [SY98] T. Sasaki and S. Yamaguchi. An Analysis of Cancellation Error in Multivariate Hensel Construction with Floating-point Number Arithmetic. *Proc. ACM Internat. Symp. on Symbolic and Algebraic Computation* (1998), 1–8.