拡張Hensel構成の効率化 – 疎な多変数多項式の因数分解を念頭に –

Enhancing the Extended Hensel Construction – for factoring sparse multivariate polynomials –

佐々木 建昭 (Tateaki Sasaki)
sasaki@math.tsukuba.ac.jp
筑波大学 名誉教授
(Prof. emeritus, Univ. Tsukuba)

讃岐 勝 (Masaru Sanuki)
sanuki@md.tsukuba.ac.jp
筑波大学 医学医療系
(Faculty of Medicine, Univ. Tsukuba)

稲葉 大樹 (Daiju Inaba)
d.inaba@su-gaku.net
(公財) 日本数学検定協会
(Japan Assoc. Math. Certification)

Abstract

拡張 Hensel 構成とは、多変数多項式の GCD 計算や因数分解で絶大な威力を発揮する一般 Hensel 構成を、算法が破綻する場合にも成立するように拡張したものである。発表時 (2000 年) には、主係数特異な多変数多項式の因数分解では他の追随を許さなかった。近年、欧米で Zippel や Ben-Or/Tiwari の疎補間法に基づく因数分解法が開発され、拡張 Hensel 法の優位が脅かされている。そのため、筆者らは数年前から拡張 Hensel 法の効率化に取り組んできた。本稿ではそれらの成果の上に、多項式因数分解への応用に限定した一つの効率化法を呈示する。拡張 Hensel 因子は従変数に関して有理式となるのが特徴だが、従変数の一つを除き他を 2 倍に重み付けることにより、有理式の分母因子を小さくするとともに、計算全体が分割される可能性を持つ方法である。研究は緒についたばかりだが、本報告では簡単な例によりアイデアの有用性を示す。

1 今、疎な多変数多項式の因数分解の研究が熱い

本稿では x は主変数を、$u_1, \ldots, u_\ell$ $(\ell \geq 2)$ は従変数を、$\boldsymbol{u}$ は従変数全体を表す。多変数多項式 $F(x, \boldsymbol{u})$ に対し、$\deg(F)$, $\mathrm{lc}(F)$, $\mathrm{ctm}(F)$, $\mathrm{cont}(F)$ はそれぞれ、主変数 x に関する**次数**、**主係数**、**定数項** (x^0-項)、**係因数** (content) を表す。$T = c\,u_1^{e_1} \cdots u_\ell^{e_\ell}$, $c \in \mathbb{Q}$, に対し、$e_1 + \cdots + e_\ell$ を $\boldsymbol{u}$ に関する**全次数** (total degree) といい $\mathrm{tdeg}(T)$ と表す。$\mathrm{lc}(F)$ が $\boldsymbol{u}$ の原点 $\boldsymbol{0}$ で 0 になるとき、F は**主係数特異**であるという。F を x に関して G で割った剰余を $\mathrm{rem}(F, G)$ と表し、$\mathrm{rem}(F, G) = 0$ のとき G は F を割り切るといい、$G \,|\, F$ と表わす。$\mathrm{res}(F, G)$ は x に関する**終結式** (resultant) を表し、$\langle F, G \rangle$ は F と G から生成される**イデアル**を表す。

GCD(最大公約子) 計算と因数分解の算法は、一変数であれ多変数であれ、計算機数学では研究され尽くされたと思われるだろう。実際、蜜な多項式に対しては GCD では EZ-GCD 算法 [8] が、因数分解では一般 Hensel 構成 (Generalized Hensel Construction, **GHC** と略記) に基づく Wang-Rothchild 算法 [18, 19] が、見事な性能を発揮する。しかしながら、疎な多変数多項式に対しては今も世界中で熱い闘いが繰り広げられている。理由は、与式 $F(x, \boldsymbol{u})$ が主係数特異だと GHC が適用できず、GHC を適用するためには従変数 $\boldsymbol{u}$ の原点を移動する必要があるが、F が $\boldsymbol{u}$ に関して疎ならば、原点移動 $\boldsymbol{u} \to \boldsymbol{v} + \boldsymbol{s}$, $(\boldsymbol{s}) \in \mathbb{Z}^\ell$, により $F(x, \boldsymbol{v} + \boldsymbol{s})$ の項数が爆発的に増えることが多いからである。これは**非零代入問題**と呼ばれ、永らく多変数多項式の因数分解における最大の問題だった。

この問題を解決するために二つの方法が提案された。一方は Zippel による**疎補間 (sparse interpolation) 法**である [20, 21]。L は大きな自然数とし、S は $-L$ から L までの整数の集合とする。非零の多変数多項式 $f(\boldsymbol{u}) \in \mathbb{Q}[\boldsymbol{u}]$ に対し、ランダムに $\boldsymbol{r} \in S^\ell$ を選んで $f(\boldsymbol{u})$ に代入した場合、$f(\boldsymbol{r}) = 0$ となる確率は L が大ならば非常に小さい (Schwartz-Zippel の補題 [17])。そこで Zippel は、未知多項式 $F(x, \boldsymbol{u}) = f_n(\boldsymbol{u})x^n + \cdots + f_0(\boldsymbol{u})$ の $\boldsymbol{u}$ に $\boldsymbol{r}$ を代入

したとき $f_k(\boldsymbol{r}) = 0$ であるなら、$f_k(\boldsymbol{u})$ は元から 0 だったとみなして算法を作ることを提案した（算法は確率的にしか成立しない）。他方は GHC を素直に拡張した方法で、主係数特異な $F(x, \boldsymbol{u})$ を非零代入することなく Hensel 因子に分解できる。1993 年に日本で考案され、拡張 Hensel 構成 (Extended Hensel Construction, **EHC**) と命名された [14, 15]。当初目的は 1 変数代数関数 (2 変数多項式の根) の Puiseux 級数展開の多変数化であったが、著者らは 2000 年、初期因子を多項式に設定することで計算代数での幅広い応用を目指した [10]。EHC は著者の一人 (D.I) が実装し、疎な多変数多項式の因数分解に適用して有用性を明確に実証した [4]。2015 年には Sanuki と共に疎な多変数多項式の GCD 計算にも応用した [16]。

Zippel の方法は GCD 計算には有用だが、因数分解の観点からは EHC の方が数学的にも算法的にもスマートなことは明白である。GCD 計算に関しても、EHC 法は大した工夫をしないでも Maple の GCD コマンドと同程度の性能を発揮した。しかし、欧米も手をこまねいてはいなかった。Zippel の提案から約 10 年後、Ben-Or/Tiwari 算法が提案された [1]。この算法は、項数が N 以下の未知の ℓ 変数多項式 $f(\boldsymbol{u}) \in \mathbb{Z}[\boldsymbol{u}]$ に対し、ℓ 個の異なる素数 $p_1, p_2, \ldots, p_\ell$ を用意し、$2N$ 個の点 $(\boldsymbol{s}_i) = (p_1^i, p_2^i, \ldots, p_\ell^i)$, $(i = 0, 1, \ldots, 2N-1)$, での $f(\boldsymbol{u})$ の関数値 $f(\boldsymbol{s}_0), f(\boldsymbol{s}_1), \ldots, f(\boldsymbol{s}_{2N-1})$ から、Vandelmonde 行列式を用いて $f(\boldsymbol{u})$ を決定するものである。当初の算法は効率がよいものではなかったが、その後、各国の研究者により次々と効率化された。筆者らはこの事態にも悠然としていた：$F(x, \boldsymbol{u})$ の従変数に多数個の異なる点 $(\boldsymbol{s}_i)$ $(i \in \{1, \ldots, N\})$ を代入して $F(x, \boldsymbol{s}_i)$ を因数分解したとして、それらの因子群からどうやって多変数因子を補間するのか？、と思っていたのである。だが、最近、Monagan らが、$F(x, \boldsymbol{s}_i)$ の因数分解から、Diophantine 方程式を解いて従変数を一つづつ復元していく算法を提案した [6, 7]。そこでは、Zippel の疎補間法を用いて著しい効率化が達成されている [6, 7]。ここに至って筆者らも安穏としてはいられなくなった。筆者らは数年前から EHC 算法の効率化に取り組み、既にかなりの効率化を成し遂げた；従来の効率化については第 2 章で述べる。Monagan らは Hensel 構成の細部まで細かく効率化しているので、筆者らも多項式因数分解への応用に限定した効率化を行って対抗することにした。

2　拡張 Hensel 構成と昨年度までの効率化研究の概要

拡張 Hensel 構成で最も基本的な概念は **Newton 線**と **Newton 多項式**である。

定義 1 (Newton 線と Newton 多項式、正味 Newton 多項式; 次頁の図 1 参照)
$F(x, \boldsymbol{u})$ の各項に $F(x, t\boldsymbol{u})$ なる変換で従変数の全次数変数 t を導入する。$F(x, t\boldsymbol{u})$ の項を $cx^i t^j u_1^{j_1} \cdots u_\ell^{j_\ell}$ とする；ここで、$c \in \mathbb{Q}$, $j = j_1 + \cdots + j_\ell$ である。この項を (x 指数, t 指数)-面上の点 (i, j) にプロットする。プロットされた全ての点を囲む凸包を $\boldsymbol{\mathcal{N}}$ と表す。$\boldsymbol{\mathcal{N}}$ の全底辺を時計周りに $\mathcal{N}_1, \ldots, \mathcal{N}_\mu$ と表し、それぞれ **Newton 線**と呼ぶ。各 $i \in \{1, \ldots, \mu\}$ に対して、$\mathcal{N}_i$ 上にプロットされた全ての項の和を **Newton 多項式**と呼び、$\overline{F}_{\mathcal{N}_i}(x, \boldsymbol{u})$ と表す。$\mathcal{N}_i$ の左端の x 指数を d_i とすれば $\overline{F}_{\mathcal{N}_i}$ は x^{d_i} で割り切れる。$\overline{F}_{\mathcal{N}_i}/x^{d_i}$ を $F_{\mathcal{N}_i}(x, \boldsymbol{u})$ と表し**正味 Newton 多項式** *(net Newton polynomial)* と呼ぶ。 □

GHC では Newton 線は x 軸上に 1 本だけあり、x の最高次数項 (の一部) と最低次数項 (の一部) が共に x 軸上にプロットされている必要がある。また、Newton 多項式が互いに素な二つ以上の多項式に因数分解されることも必要である。よって、GHC は特殊な場合での Hensel 構成で、一般には EHC を扱うのが自然であることが解る。特に、疎な多変数多項式では、与式を自然に Hensel 構成しようとすれば EHC になるだろう。

拡張 Hensel 因子には **maximal 因子**及び **minimal 因子**と命名した 2 種類の因子がある。前者は、各 Newton 線 $\mathcal{N}_i$ 上で Newton 多項式 $\overline{F}_{\mathcal{N}_i}$ の互いに素な二つの因子 x^{d_i} と $F_{\mathcal{N}_i}$ を初期因子として構成される因子で、後者は各 Newton 線 $\mathcal{N}_i$ 上で正味 Newton 多項式 $F_{\mathcal{N}_i}$ の互いに素な多項式因子を初期因子として構成される因子である。次頁の図左は $\mathcal{N}_1, \mathcal{N}_2, \mathcal{N}_3$ 上の maximal 因子を、右は $\mathcal{N}_2$ 上の minimal 因子を概念的に図示したものである。

Hensel 構成はイデアルを法とする因数分解に他ならない。法は、Hensel により提案された構成では p^{k+1} (p は素数) で、GHC では $\langle u_1, \ldots, u_\ell \rangle^{k+1}$ である。EHC では、法は各 Newton 線毎に別々に定められるが、変数 x と $\boldsymbol{u}$ を重み付ける形で次のように定式化されている [10, 11]。

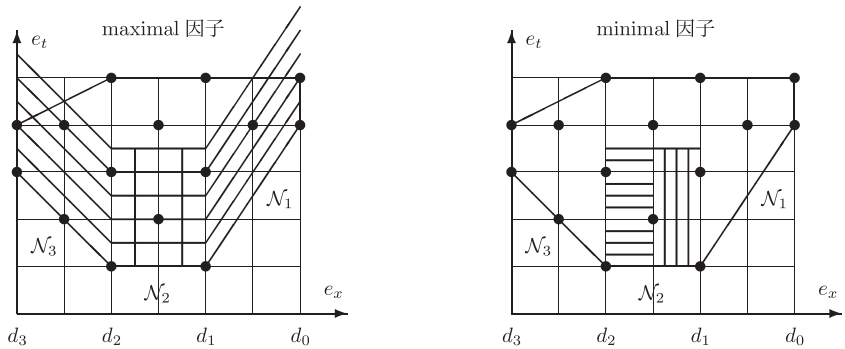


図 1: maximal 因子 と minimal 因子 の概念図

定義 2 (変数の重み付けと拡張 Hensel 構成の法 $\mathcal{I}_k$; 重み付け変数を W とする)
$\mathcal{N}_1$ の右端の座標点を (d_0, e_0)、$\mathcal{N}_i$ の左端の座標点を (d_i, e_i) とすれば、$\mathcal{N}_i$ の傾きは $\lambda_i = (e_{i-1}-e_i)/(d_{i-1}-d_i)$ である。$\hat{d}_i$ と $\hat{e}_i$ は $\hat{d}_i > 0, \hat{e}_i/\hat{d}_i = \lambda_i, \gcd(\hat{d}_i, \hat{e}_i) = 1$ を満たす整数とする。このとき、重み付きの多項式 $\mathcal{F}(x, \boldsymbol{u}, W)$, $\mathcal{F}_{\mathcal{N}_i}(x, \boldsymbol{u})$ および法となるイデアル $\mathcal{I}_k$ を次式で定義する。(次章以降では、簡単のため添字 i を略す)。

$$\left\{ \begin{array}{rcl} \mathcal{F}(x, \boldsymbol{u}, W) & \stackrel{\text{def}}{=} & W^{\hat{d}_i(\lambda_i d_i - e_i)} F(x/W^{\hat{e}_i}, W^{\hat{d}_i}\boldsymbol{u}), \\ \mathcal{F}_{\mathcal{N}_i}(x, \boldsymbol{u}) & \stackrel{\text{def}}{=} & W^{\hat{d}_i(\lambda_i d_i - e_i)} F_{\mathcal{N}_i}(x/W^{\hat{e}_i}, W^{\hat{d}_i}\boldsymbol{u}), \\ \mathcal{I}_k & \stackrel{\text{def}}{=} & \langle W^k \rangle, \quad k=1,2,3,\ldots. \end{array} \right. \tag{2.1}$$

上式中で $\mathcal{F}_{\mathcal{N}_i}(x, \boldsymbol{u})$ が W を含まないのは、$\overline{F}_{\mathcal{N}_i}$ の各項が e_x 軸上にプロットされるように重み付けをしたからである。したがって、$\mathcal{F}_{\mathcal{N}_i}$ の因子から決まる初期因子も重み 0 としてよい。そして、拡張 Hensel 構成は、maximal であれ minimal であれ、法であるイデアル $\mathcal{I}_k$ を $\mathcal{I}_1 \Rightarrow \mathcal{I}_2 \Rightarrow \mathcal{I}_3 \Rightarrow \cdots$ と上げて行われる (**リフティング**)。 □

拡張 Hensel 構成は、maximal であれ minimal であれ概略、次の算法で実行される。

Choose: $\left\{ \begin{array}{ll} \text{maximal}: & \overline{F}_{\mathcal{N}_i} = H_0 G_0,\ H_0 = x^{d_i}, G_0 = F_{\mathcal{N}_i}; \\ \text{minimal}: & F_{\mathcal{N}_i} = G_0 H_0, \quad \gcd(G_0, H_0) = 1; \end{array} \right.$
Initial: $\mathcal{F}(x, \boldsymbol{u}, W) \equiv \mathcal{G}^{(0)}\mathcal{H}^{(0)} = G_0 H_0 \pmod{W}$;
Lifting: **for** $k := 1, K$ **do**
calc: $W^k \delta F^{(k)} \equiv \mathcal{F} - \mathcal{G}^{(k-1)}\mathcal{H}^{(k-1)} \pmod{W^{k+1}}$;
solve: $\delta F^{(k)} = \delta H^{(k)} G_0 + \delta G^{(k)} H_0$ w.r.t. $\delta H^{(k)}, \delta G^{(k)}$;
reset: $\mathcal{G}^{(k)} = \mathcal{G}^{(k-1)} + W^k \delta G^{(k)}$, $\mathcal{H}^{(k)} = \mathcal{H}^{(k-1)} + W^k \delta H^{(k)}$;
endfor
end: **return** $(\mathcal{G}^{(K)}(x, \boldsymbol{u}, 1), \mathcal{H}^{(K)}(x, \boldsymbol{u}, 1))$.

Maximal 因子の EHC は、一方の因子が x^{d_i} で簡単なので 2000 年論文 [10] の算式で実行する。

従来、効率化は専ら minimal 因子に対し行われた。第 i 番目 $(1 \le i \le \mu)$ の Newton 線 $\mathcal{N}_i$ 上の EHC を考える。第 i 番目の正味 Newton 多項式を $F_{\mathcal{N}}(x, \boldsymbol{u})$ とし (添字 i は省く)、その互いに素な多項式因子を G_0 と H_0 とする。G_0, H_0 を初期因子とする EHC は、次式で定義される補間多項式 $A_l, B_l \in \mathbb{Q}(\boldsymbol{u})[x],\ 0 \le l < \deg(F_{\mathcal{N}})$, を用いて行われる。$A_l$ と B_l を Moses-Yun 多項式と呼び、**MY-多項式**と略記する。

$$A_l G_0 + B_l H_0 = x^l, \quad \deg(A_l) < \deg(H_0),\ \deg(B_l) < \deg(G_0). \tag{2.2}$$

MY-多項式を使えば、算法の **solve:**での $\delta H^{(k)}$ と $\delta G^{(k)}$ は、$\delta F^{(k)} = \delta f_{n-1}^{(k)} x^{n-1} + \cdots + \delta f_0^{(k)} x^0$ と表せば、$(\delta H^{(k)}, \delta G^{(k)}) = \sum_{l=0}^{n-1} (A_l, B_l)\, \delta f_l^{(k)}$ と非常に簡単に計算できる。($\delta f_n^{(k>0)}$ が 0 となるように、$G^{(0)}$ または $H^{(0)}$ の主係数を $\mathrm{lc}(F)$ で置き換える)。

A_0, B_0 は G_0 と H_0 から互除法で計算でき、$A_{l>0} = \mathrm{rem}(x^l A_0, H_0)$、$B_{l>0} = \mathrm{rem}(x^l B_0, G_0)$ と計算できる。$G_0, H_0 \in \mathbb{Q}[x, \boldsymbol{u}]$ ゆえ $A_l, B_l \in \mathbb{Q}(\boldsymbol{u})[x]$ となるから、$\mathcal{F}(x, \boldsymbol{u}, w) \equiv \mathcal{G}^{(k)}\mathcal{H}^{(k)} \pmod{W^{k+1}}$ を満たす $\mathcal{G}^{(k)}, \mathcal{H}^{(k)}$ は $\boldsymbol{u}$ の有理式を係数とする x の多項式である。$\mathcal{G}^{(k)}, \mathcal{H}^{(k)}$ の分母因子を如何に処理するかが効率化の鍵である。

上記の計算法 (=以前の計算法) では A_0 と B_0 の分母因子は終結式 $\mathrm{res}(G_0, H_0)$ である。G_0 と H_0 が x に関して疎な場合、終結式を Sylvester 行列式で計算してみれば、終結式には同じ因子が多重に現れることがすぐわかる。CASC2016 論文 [11] では、イデアル $\langle G_0, H_0\rangle$ の辞書式順序のグレブナー基底 $\Gamma(G_0, H_0)$ を用いて EHC を定式化した。そして、A_0 と B_0 の最小の分母因子は $\Gamma(G_0, H_0)$ の最低元であることを示した。

SYNASC2016 論文 [12] では $\Gamma(G_0, H_0) \cap \mathbb{Q}[\boldsymbol{u}] = \{\widehat{S}(\boldsymbol{u})\}$、すなわち A_0, B_0 の最小の分母因子の候補は定数倍を除き一意であることを証明し、$F_{N_i}(x, \boldsymbol{u})$ が 3 個以上の既約因子を持つ場合の分母因子の効率的計算法 (ある種の分割征服算法) や、maximal 因子の計算法の改善策、リフティング後の Hensel 因子の簡単化などを記述した。

グレブナー基底で定式化することで EHC は理論的に整理されたが、従変数が多い場合 ($\ell \geq 4$) にはグレブナー基底計算が非常に重くなる。ところで、上述した計算の本質は単に G_0 と H_0 から主変数 x を消去することである。変数消去の立場から Buchberger 算法と互除法の間隙を埋めていけば、互除法により $\Gamma(G_0, H_0)$ の最低元 $\widehat{S}(\boldsymbol{u})$ が計算できそうに思える。SYNASC2017 論文 [13] では、剰余列 ($P_1 := G_0,\ P_2 := H_0,\ \cdots,\ P_k \in \mathbb{Q}[\boldsymbol{u}]$) と余因子列 ($(1,0),\ (0,1),\ (U_3, V_3),\ \cdots,\ (U_k, V_k)$) を計算すれば、$\widehat{S}(\boldsymbol{u})$ が次式で得られることを証明した。

$$\widehat{S}(\boldsymbol{u}) = P_k(\boldsymbol{u}) / \gcd(\mathrm{cont}(U_k), \mathrm{cont}(V_k)). \tag{2.3}$$

なお、余因子 $U_i, V_i \in \mathbb{Q}[x, \boldsymbol{u}]$ $(i = 3, \ldots, k)$) は次式を満たす。

$$U_i G_0 + V_i H_0 = P_i, \quad \deg(U_i) < \deg(H_0) - \deg(P_i),\ \deg(V_i) < \deg(G_0) - \deg(P_i). \tag{2.4}$$

この算法とグレブナー基底法を従変数の個数 ℓ が 3, 4, 5, 6 の簡単な例で比較したところ、$\ell = 3$ ではグレブナー基底法が勝ったが、$\ell = 4$ では剰余列法が約 50 倍、$\ell = 5, 6$ では全く比較にならないほど剰余列法が高速だった。なお SYNASC2017 論文では、MY 多項式 $A_{i>0}, B_{i>0}$ の分母には $\gcd(\mathrm{lc}(G_0), \mathrm{lc}(H_0))$ も現れ得ることを示した。

上記算式 (2.3) は非常に有用だが初等的なので、外国人査読者の一人は “but it (算式 (2.3) に対する定理) was probably known already to experts in this area. In fact, it may be a consequence of the results of [18].” とまで書いた (論文評価は “borderline paper”)。これには筆者らも看過できず、“known already to experts” と言うなら上記定理を記述した論文を示せ、文献 [18] は余因子に全く言及してないのに [18] から (上記定理が) 簡単に導けるはずがない、と査読者に厳しく反論したところ、異論なく受理された。

ここまでくると疎多変数多項式の剰余列算法が気になる。主変数 x の次数に飛びのある剰余列も部分終結式理論に基づく Brown の算法 [2] で計算できるが、それは効率が悪い。疎多項式に対する**疎擬剰余**は Loos[5] が定義したが、彼は係数の共通因子の除去には従前の算法を使った。疎擬剰余列からの因子除去算法は筆者らが SYNASC2017 論文で呈示した (Hearn の**試し除算法** [3] を利用する) が、それでもなお、中間式膨張が残っていた。中間式膨張は CASC18 論文 [9] でようやく除去された。

3 因数分解に限定した EHC 算法の効率化

EHC 算法の効率化策は、主変数と従変数を固定した場合には、前章に概観した方策で重要なものは尽きるのではないかと思っている。しかし、EHC の使用目的を限定すれば非常に有効な方策はまだ幾つもある。本章では、使用目的を疎な多変数多項式の因数分解に限定して、一つの有効そうな効率化策を呈示する。

3.1 従変数の重み変換: 基本的命題と実際の重み変換

前章で見たように、主係数特異な多変数多項式を EHC 法で因数分解すると、計算途中で従変数に関する有理式が出現するのは不可避だが、有理式は最終結果では消えている。よって、従変数を変換して有理式の分母因子を出来る限り小さくすることを考える。

命題 1 多項式 $F(x,u_1,\ldots,u_\ell)$ に対する変換 $\mathcal{T}$ を $\mathcal{T}F=F(x,u_1^{w_1},\ldots,u_\ell^{w_\ell})$, $w_1,\ldots,w_\ell\in\mathbb{N}$, とすれば、$F$ における因数分解は $\mathcal{T}F$ においても成立する。なお、逆は成立するとは限らない (F の因数分解が既約でも $\mathcal{T}F$ のそれが既約分解とは限らない)。

証明 従変数の重み w_i は自然数なので、$F(x,\boldsymbol{u})$ の因数分解において同じ変換をすれば $\mathcal{T}F$ の因数分解が得られる。一方、$F(x,\boldsymbol{u})$ がたとえば因子 u_1-u_2 を含み $w_1=w_2=2$ ならば $\mathcal{T}F$ は因子 $(u_1+u_2)\times(u_1-u_2)$ を持つので、逆は成立しない。 □

従変数の変換は Newton 多項式の項数を減少させることが目的ゆえ、実際には従変数の一つ、それを u_i とする、を除き他の従変数のべきを 2 倍にする次の変換を用いる。

$$\mathcal{T}_{u_i}F=F(x,u_1^2,..,u_i,..,u_\ell^2)\qquad(1\le i\le\ell). \tag{3.1}$$

実際の算法では、$i=1,2,\ldots,\ell$ 全てに対して $\mathcal{T}_{u_i}$ を $F(x,\boldsymbol{u})$ に適用して Newton 多項式を求め、その中から条件に合う最適な $\mathcal{T}_{u_i}$ を選ぶ。

3.2 簡単な例による有効性の検討

以下、$\mathcal{T}_{u_i}F$ の Newton 多項式を $\widetilde{F}_{[u_i]\mathcal{N}_j}$ $(j=1,\ldots,\mu)$ と表す：Newton 線が μ 本あれば Newton 多項式も μ 個あるので、添字 j で区別する。下記の例はいずれも、例題の Newton 多項式が $\mathcal{T}_{u_i}$ でどのように変換されるかが簡単に解るように、例題の Newton 多項式がそのまま元の多項式となるように選んでいる。また、例題はいずれも Newton 線は 1 本だが Newton 多項式は 2 個の既約因子を持つ。

例 1 $F_{\mathrm{Ex1}}=\big(X^4(u+v)+X^2(u-2w)+(2v+w)\big)\times\big(X^4(u-v)+X^2(2u+v)+(v-2w)\big)$.

F_{Ex1} に $\mathcal{T}_u,\mathcal{T}_v,\mathcal{T}_w$ を適用すると、F_{Ex1} は下記の表のようにそれぞれ 2 個、1 個、3 個の Newton 多項式に分離する。Newton 多項式は高次多項式から順に記述する: 各行の多項式が Newton 多項式で、下線を付したのが正味 Newton 多項式である。

$$\begin{aligned}
\widetilde{F}_{[u]\mathcal{N}_{1,2}}:&\quad(X^4)\times(\underline{X^2+2})\times(\underline{X^2+1})\times(u^2),\\
&\quad(\underline{2X^2u+v^2-2w^2})\times(\underline{X^2u+2v^2+w^2}).\\
\widetilde{F}_{[v]\mathcal{N}_1}:&\quad(\underline{X^4-X^2-1})\times(\underline{X^4+2})\times(v^2).\\
\widetilde{F}_{[w]\mathcal{N}_{1,2,3}}:&\quad(X^6)\times(\underline{X^2u^2+X^2v^2-2w})\times(u^2-v^2),\\
&\quad(X^2)\times(\underline{X^4u^2-X^4v^2-2w})\times(w),\\
&\quad(\underline{2X^2-1})\times(w^2),
\end{aligned}$$

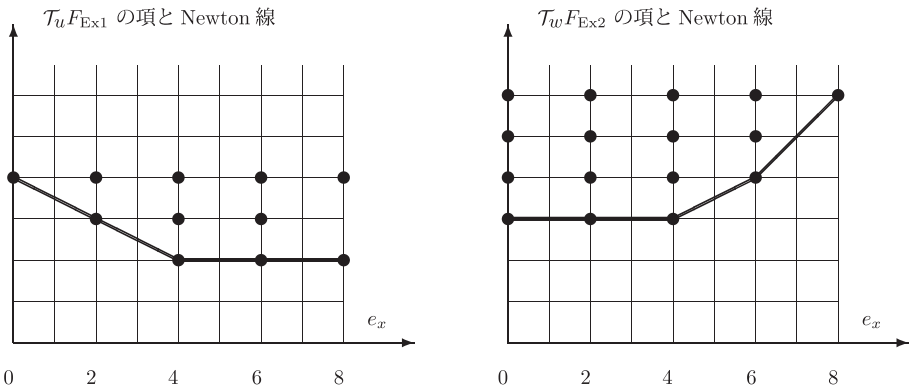
例 2 $F_{\mathrm{Ex2}}=\big(X^4(u+v)+X^2(u-2w)+(2v+w)\big)\times\big(X^4(u^2+uv)+X^2(u^2-2w^2)+(2v^2+w^2)\big)$.

F_{Ex2} に $\mathcal{T}_u,\mathcal{T}_v,\mathcal{T}_w$ を適用すると、F_{Ex2} は下記の表のようにそれぞれ 3 個、2 個、3 個の Newton 多項式に分離する。Newton 多項式は高次多項式から順に記述する: 各行の多項式が Newton 多項式で、下線を付したのが正味 Newton 多項式である。

$$\begin{aligned}
\widetilde{F}_{[u]\mathcal{N}_{1,2,3}}:&\quad(X^4)\times(\underline{X^2+1})^2\times(u^3),\qquad\text{(使用には不適)}\\
&\quad(X^2)\times(\underline{X^2u+2v^2+w^2})\times(u^2),\\
&\quad(\underline{X^2u^2+2v^4+w^4})\times(2v^2+w^2),\\
\widetilde{F}_{[v]\mathcal{N}_{1,2}}:&\quad(X^4v^2)\times(\underline{X^4u^2+2v}),\\
&\quad(\underline{X^4+2})\times(v^3),\\
\widetilde{F}_{[w]\mathcal{N}_{1,2,3}}:&\quad(X^6)\times(\underline{X^2u^4+X^2u^2v^2-2w^2})\times(u^2+v^2),\\
&\quad(X^4)\times(\underline{X^2u^2+X^2v^2-2w})\times(w^2),\\
&\quad(\underline{2X^2-1})^2\times(w^3).\qquad\text{(使用には不適)}
\end{aligned}$$

$\widetilde{F}_{[u]\mathcal{N}_1}$ と $\widetilde{F}_{[w]\mathcal{N}_3}$ の正味 Newton 多項式は重複因子を持つので、使用には適さない。 □

参考までに、$\mathcal{T}_u F_{\mathrm{Ex1}}$ と $\mathcal{T}_w F_{\mathrm{Ex2}}$ の各項 (●) と Newton 線 (折れ線) を図示する (それぞれ左図と右図)。



上記の例は簡単だが、変換 $\mathcal{T}_{u_i}$ がもたらす効果として次の特徴が見てとれる。

特徴 A 元の Newton 多項式の項のうち一部だけが変換後の Newton 多項式に現れる (上図参照)。よって、変換後の Newton 多項式全体の項数が減少する。

特徴 B 元の一つの Newton 多項式が大抵、複数個の Newton 多項式に分離する。結果として、変換後の一つの正味 Newton 多項式の項数が大幅に減少する。

特徴 C 新たに出現する Newton 多項式の大部分は maximal Hensel 因子に対応する。異なる Newton 多項式は異なる傾きの Newton 線に対応するから、当然である。

3.3 変換後の minimal 因子の EHC に現れる分母因子

上記の特徴 A と B によれば、従変数の重み変換により個々の正味 Newton 多項式の項数が減るので、minimal 因子の EHC に出現する分母因子は大幅に小さくなると期待できる。まず、変換前と変換後の正味 Newton 多項式の既約因子間の対応について述べる。

命題 2 与多項式 F の l 番目の正味 Newton 多項式 $F_{\mathcal{N}}$ (添字 l は省略) の既約因数分解を $F_{\mathcal{N}} = F_{\mathcal{N}_1} \cdots F_{\mathcal{N}_r}$ $(r \geq 2)$ とする。$\mathcal{T}_{u_i} F_{\mathcal{N}}$ の正味 Newton 多項式の既約因子全体の集合は $\mathcal{T}_{u_i} F_{\mathcal{N}_1}, \ldots, \mathcal{T}_{u_i} F_{\mathcal{N}_r}$ それぞれの正味 Newton 多項式の既約因子全体の集合に等しい。

証明 $F_{\mathcal{N}} = F_{\mathcal{N}_1} \cdots F_{\mathcal{N}_r}$ より $\mathcal{T}_{u_i} F_{\mathcal{N}} = (\mathcal{T}_{u_i} F_{\mathcal{N}_1}) \cdots (\mathcal{T}_{u_i} F_{\mathcal{N}_r})$ である。$\mathcal{T}_{u_i} F_{\mathcal{N}}$ の正味 Newton 多項式は一般に複数個あり、Newton 多角形 $\mathcal{N}$ の下辺部に乗る項全体から成る。$\mathcal{T}_{u_i} F_{\mathcal{N}_j}$ の正味 Newton 多項式も同様であるが、Newton 多角形の凸性から左辺の Newton 多角形の下辺部は右辺の個々の Newton 多角形の下辺部の積と一致し、命題が成立する。 □

系 $\mathcal{T}_{u_i} F_{\mathcal{N}_1}, \ldots, \mathcal{T}_{u_i} F_{\mathcal{N}_r}$ の正味 Newton 多項式がそれぞれ、$\mathcal{T}_{u_i} F_{\mathcal{N}}$ のどの正味 Newton 多項式に対応するかは、前者が全体として共通因子を持たない限り直ちにわかる。 □

命題 2 を 3.2 節に与えた例 1: F_{Ex1} で見てみよう。$\mathcal{T}_u F_{\mathrm{Ex1}}$ は二つの正味 Newton 多項式 $\widetilde{F}_{[u]\mathcal{N}_1} = (X^2{+}1){\times}(X^2{+}2)$ と $\widetilde{F}_{[u]\mathcal{N}_2} = (X^2u + 2v^2 + w^2){\times}(2X^2u + v^2 - 2w^2)$ を与える。一方、$F_{\mathrm{Ex1}} = F_1 F_2$, $F_1 = X^4\,(u{+}v) + X^2\,(u{-}2w) + (2v{+}w)$, $F_2 = X^4\,(u{-}v) + X^2\,(2u{+}v) + (v{-}2w)$ であり、$\mathcal{T}_u F_1$ は二つの正味 Newton 多項式 $X^2 + 1$ と $X^2u + 2v^2 + w^2$ を与え、$\mathcal{T}_u F_2$ は二つの正味 Newton 多項式 $X^2 + 2$ と $2X^2u + v^2 - 2w^2$ を与える。

つぎに、例題多項式 F_{Ex1} と F_{Ex2} を正味 Newton 多項式とする minimal EHC で出現する分母因子が、従変数の重み変換でどのようになるかを、例 1, 2 で別々にみよう。因みに、例 1, 2 ともに $F_{\mathrm{Ex}} = F_1F_2$ の形をしており、分母因子はイデアル $\langle F_1, F_2\rangle$ の消去順序 $x \succ u, v, w$ でのグレブナー基底の最低元 $\widehat{S}_i$ で、次の多項式である。

$$\begin{aligned}
(\text{for } F_{\mathrm{Ex1}})\ \widehat{S}_1 &= 3u^3v + 4u^3w + 15u^2v^2 + 31u^2vw + 13u^2w^2 + 5uv^3 - 2uv^2w \\
&- 12uvw^2 - 8uw^3 + 11v^4 - 7v^3w - 9v^2w^2 + 8vw^3, \\
(\text{for } F_{\mathrm{Ex2}})\ \widehat{S}_2 &= 4u^3v^2 + 8u^3vw + 3u^3w^2 - 4u^2v^3 - 4u^2v^2w - 7u^2vw^2 \\
&- 6u^2w^3 - 4uv^4 - 4uv^3w + 12uv^2w^2 - 10uvw^3 + 3uw^4 \\
&+ 4v^5 + 4v^3w^2 - 8v^2w^3 + 9vw^4.
\end{aligned}$$

例 1 の F_{Ex1} に従変数の重み変換をした場合の分母因子

3.2 節で与えた $\mathcal{T}_uF_{\mathrm{Ex1}}$, $\mathcal{T}_vF_{\mathrm{Ex1}}$, $\mathcal{T}_wF_{\mathrm{Ex1}}$ の各 Newton 多項式より次を得る。

$$\begin{aligned}
&\widetilde{F}_{[u]\mathcal{N}_1}, \widetilde{F}_{[v]\mathcal{N}_1} && \Rightarrow \text{ 分母因子は } 1 \\
&\widetilde{F}_{[w]\mathcal{N}_{1,2,3}} && \Rightarrow \text{ maximal EHC のみ (分母因子は } \underline{w \text{ or } 1}) \\
& && \quad (\text{maximal EHC の分母因子は } \mathrm{ctm}(G_0)) \\
&\widetilde{F}_{[u]\mathcal{N}_2} && \Rightarrow \text{ 下記イデアルより分母因子は } \underline{3v^2 + 4w^2} \\
& && \quad \langle 2X^2u + v^2 - 2w^2,\ X^2u + 2v^2 + w^2\rangle
\end{aligned}$$

例 2 の F_{Ex2} に従変数の重み変換をした場合の分母因子

3.2 節で与えた $\mathcal{T}_uF_{\mathrm{Ex2}}$, $\mathcal{T}_vF_{\mathrm{Ex2}}$, $\mathcal{T}_wF_{\mathrm{Ex2}}$ の各 Newton 多項式より次を得る。

$$\begin{aligned}
&\widetilde{F}_{[u]\mathcal{N}_{1,2,3}}, \widetilde{F}_{[w]\mathcal{N}_{1,2,3}} && \Rightarrow \text{ 平方因子が現れるため使用せず} \\
&\widetilde{F}_{[v]\mathcal{N}_{1,2}} && \Rightarrow \text{ maximal EHC のみ (分母因子は } \underline{v \text{ or } 1}) \\
& && \quad (\text{maximal EHC の分母因子は } \mathrm{ctm}(G_0))
\end{aligned}$$

これらの結果をみると、従変数の重み変換により、minimal 因子の EHC で出現する分母因子は期待以上に大きく減少することが解る。

4 まとめと今後の作業

従変数の重み変換は、実例でみる限り、下記の三つの効果をもたらす。

1. minimal EHC での分母因子を劇的に低サイズ化する。
2. 小サイズの maximal EHC を多く出現させる。
   これは、EHC 全体の分割計算に他ならず、計算効率化に資する。
   なお、maximal EHC の増加で因子組合わせが増えることはない (⇐ 命題 2 の系)。
3. $\ell-1$ 個の従変数の次数が 2 倍されたので、リフティング回数も 2 倍に増える (不利)。

主係数特異かつ疎な多変数多項式の EHC 法による因数分解で、従変数の重み変換が顕著な高速化をもたらすか否かは実際にプログラムを書いてテストする必要があり、現在、プログラミングに取り組んでいるところである。なお、上記第 2 点は目新しいことで、minimal EHC を実行する前の段階で、maximal 因子組合わせにより中間的な因数分解が得られる可能性を強く示唆する。従来は全く考えていなかったことで、maximal 因子の組合わせによる中間的因数分解算法の開発にも取り組んでいる。さらに、プログラミングの過程で、従来は大して重要視してなかった maximal EHC が、Newton 線が多い場合には大きな問題を引き起こすことに気付いた。一つの Newton 線上での maximal EHC は通常、一つの新しい分母因子をもたらすが、従来の算法ではその分母因子がその後の maximal 因子全体に伝播し、Newton 線が多い場合には巨大な有理式を扱うことになるのである。この問題は実は既に解決された：i 番目の Newton 線上で導入される分母因子は、i+1 番目の Newton 線上での maximal EHC にしか伝播しない算法を発見したのである。

謝辞 本研究は科研費 (課題番号 18K03389) の援助で遂行された。

参 考 文 献

[1] M. Ben-Or and P. Tiwari: A deterministic algorithm for sparse multivariate polynomial interpolation. In: *'88 Proceedings of twentieth annual ACM symp. on Theory of Computing*, ACM Press, 301-309 (1988).

[2] W.S. Brown: The subresultant PRS algorithm. ACM TOMS **4**, 237-249 (1978).

[3] A.C. Hearn: Non modular computation of polynomial GCD using trial division. In: *Proceedings EUROSAM'79* (Springer LNCS **72**), 227-239 (1979).

[4] D. Inaba: Factorization of multivariate polynomials by extended Hensel construction. ACM SIGSAM Bulletin, **39**(1), 2-14 (2005).

[5] R. Loos: Generalized Polynomial Remainder Sequence. In: *Computer Algebra (Computing Supplementum 4)*, 115–137, Springer-Verlag (1982).

[6] M. Monagan and B. Tuncer: Using sparse interpolation in Hensel lifting. In: *Computer Algebra in Scientific Computing* (Proceedings of CASC 2016), LNCS **9890**, 381–400. Springer (2016).

[7] M. Monagan and B. Tuncer: Factoring multivariate polynomials with many factors and huge coefficients. In: *Computer Algebra in Scientific Computing* (Proceeding of CASC 2018), LNCS **11077**, 319–334. Springer (2018).

[8] J. Moses and D.Y.Y. Yun: The EZGCD algorithm. In: *Proc. 1973 ACM National Conference*, ACM, 159-166 (1973).

[9] T. Sasaki: A theory and an algorithm for computing sparse multivariate polynomial remainder sequence. In: *Computer Algebra in Scientific Computing* (Proceedings of CASC 2018), Springer LNCS **11077**, 345-360, 2018.

[10] T. Sasaki and D. Inaba: Hensel construction of $F(x, u_1, \ldots, u_\ell)$, $\ell \geq 2$, at a singular point and its applications. ACM SIGSAM Bulletin, **34**(1), 9-17 (2000).

[11] T. Sasaki and D. Inaba: Enhancing the extended Hensel construction by using Gröbner bases. In: *Computer Algebra in Scientific Computing* (Proceedings of CASC2016), Springer LNCS **9890**, 457-472 (2016).

[12] T. Sasaki and D. Inaba: Various enhancements of extended Hensel construction for sparse multivariate polynomials. In: *SYNASC2016* (Symbolic and Numeric Algorithms for Scientific Computing), IEEE Computer Society, 83-96 (2017).

[13] T. Sasaki and D. Inaba: Simple relation between the lowest-order element of ideal $\langle G, H \rangle$ and the last element of polynomial remainder sequence. In: *SYNASC 2017* (Symbolic and Numeric Algorithms for Scientific Computing), Universitatea de Vest, IEEE Conference Publishing Services, 55-62 (2018).

[14] T. Sasaki and F. Kako: Solving multivariate algebraic equation by Hensel construction. Preprint of Univ. Tsukuba, March, 1993.

[15] T. Sasaki and F. Kako: Solving multivariate algebraic equation by Hensel construction. Japan J. Indust. Appl. Math., **16**(2), 257-285 (1999). (This is almost the same as [14]: the delay of publication is due to very slow reviewing process.)

[16] M. Sanuki, D. Inaba and T. Sasaki: Computation of GCD of Sparse Multivariate Polynomial by Extended Hensel Construction. In: *SYNASC 2015* (Symbolic and Numeric Algorithms for Scientific Computing), IEEE Computer Society, 34–41 (2016).

[17] J.T. Schwarz: Fast probabilistic algorithms for verification of polynomial identities. J. ACM **27**, 701-717 (1980).

[18] P.S. Wang and L. P. Rothschild: Factoring multivariate polynomials over the integers. Math. Comp. **29**, 935-950 (1975).

[19] P.S. Wang: An improved multivariate factoring algorithm. Math. Comp. **32**, 1215-1231 (1978).

[20] R. Zippel: Probabilistic algorithm for sparse polynomials. In: *Proceedings of EUROSAM'79*, Springer-Verlag LNCS **72**, 216-226 (1979).

[21] R. Zippel: Newton's iteration and the sparse Hensel lifting (extended abstract), In: *Proceedings of SYMSAC'81*, 68-72 (1981).