数理解析研究所講究録
第1955巻 2015年 48-61

疎な多変数多項式のGCDと因数分解の効率的算法

Efficient Algorithms for GCD and Factorization of Sparse Multivariate Polynomials

稲葉 大樹 (Daiju Inaba) *
(公財) 日本数学検定協会
(Japan Assoc. Math. Certification)

讃岐 勝 (Masaru Sanuki) †
筑波大学 医療医学系
(Univeristy of Tsukuba)

佐々木 建昭 (Tateaki Sasaki) ‡
筑波大学 名誉教授
(University of Tsukuba)

Abstract

多変数多項式のGCD計算と因数分解では一般Hensel構成を用いる方法が確立され普及しているが、疎な高次多項式では驚くほど計算が遅くなることが多々ある。この現象は非零代入と呼ばれる演算がひき起こす。非零代入は長らく未解決の難問だったが、2000年、Sasaki·Inabaが拡張Hensel構成を利用した算法を考案して、決定的に解決した。しかし、その算法には未完成の箇所があり、効率化の余地もある。また、算法は多変数多項式のGCD計算にも広げることができる。本稿では因数分解算法の未完成箇所を完成させ、効率化を図るとともに、GCD計算を実行するための理論を記述する。ただし、現在実装中で実験データはない。

1 はじめに

多変数多項式のGCDと因数分解は計算機代数の中でも最も初期から精力的に研究され、最も成功を収めた演算である。算法の基礎になるのは一般Hensel構成で、算法の簡潔さと高速性は見事である[13, 1, 2]。既に算法は完成されて、研究の余地などないと思われるだろう。しかし、疎な高次多項式を対象にすると話は一変する：既存の数式処理システムで疎な高次多項式を因数分解させると非常に時間がかかる。しかも、応用面で現れる高次多変数多項式の多くは疎であると言っても過言ではないだろう。

与えられた多変数多項式を$F(x, \boldsymbol{u})$, $\boldsymbol{u}$は従変数全体, とする。因数分解では、従変数に数値$\boldsymbol{s}$を代入した1変数多項式$F_0(x) \stackrel{\text{def}}{=} F(x, \boldsymbol{s})$を因数分解し、その互いに素な因子を

*d.inaba@su-gaku.net
†sanuki@md.tsukuba.ac.jp
‡sasaki@math.tsukuba.ac

初期因子として $(\boldsymbol{u}-\boldsymbol{s})$ を法とするHensel構成を行う。得られたHensel因子を掛け合わせて多項式因子を得るのだが、既約な分解を行うために $F_0(x)$ に次の二つの条件を課す：1) $\deg_x(F)=\deg(F_0)$、2) F_0 は無平方 ($F(x,\boldsymbol{u})$ は入力時に既に無平方)。因数分解では F の主係数は各分解因子に一意的に割り振られるが、各因子の主係数は因数分解で決まるもので、Hensel構成時には未知である。そこで、$F(x,\boldsymbol{u})$ の主係数を如何にHensel因子に割り振るかが問題になる：この割り振りが悪いと、Hensel因子の積が多項式にならない。これが**主係数問題**である。上記条件1) は主係数が定数項を含まない場合、従変数の原点を移動することを要求する。これが**非零代入問題**である。なぜこれが問題か？ 理由は、主係数が定数項を含まないような多項式は疎であることが多く、その場合、原点移動すれば項数が爆発的に増加するからである (次章で具体例を与える)。

非零代入問題自体は明快だがHensel構成の土台に関わるので解決が難しい。Wang[15]は、条件1) が満たされない場合、原点移動用の $\boldsymbol{s}$ を変数毎に異なる素数の組に選ぶことにより、F の主係数の各因子を多項式因子に割り振る方法を考案し、主係数問題を巧みに解決した。彼は非零代入問題にも挑戦したが[14]、大した成果は得ていない。非零代入問題には因子多項式を補間する解決策も考えられるが[3, 6]、実際にインプリメントして成功したとの報告は聞いたことがない。次段落で見るように、この問題は小手先の技法で解決できる代物ではなく、解決にはブレイクスルー的技法が必要である。

非零代入問題はSasaki·Kakoによる**拡張Hensel構成**[11, 12]で決定的に解決された。拡張Hensel構成とは、$F(x,\boldsymbol{u})$ の主係数が定数項を含まない場合でも従変数の原点移動を行うことなく多変数Hensel構成を行うものである。ただし、1993年執筆の最初の論文は多変数代数方程式の "根の (従変数の有理式に関する) 級数展開法" として定式化したもので、原点移動することなく因数分解を実行する方法は、初期因子を多変数多項式としてHensel構成する方法を定式化した、2000年のSasaki·Inabaの論文[10]に記述してある。なお、2変数の場合、拡張Hensel構成と全く同じ方法がKuo[7]により定式化されていた (論文を書いた当時は知らなかった)。次章でみるように、拡張Hensel構成では "Newton多項式" が決定的役割を果たすのだが、2変数の場合、Newton多項式は主変数と従変数に関する斉次な多項式であり、実質的に1変数多項式と同じである。そのため、2変数の拡張Hensel構成は一般Hensel構成とほとんど同じものとなる。2変数の拡張Hensel構成を利用した因数分解法については[4, 9]を見られたい。

Inaba[5]は、文献[10]で記述された因数分解法をインプリメントし、拡張Hensel構成に基づく算法が従来算法の遅さをほぼ解消することを実証した。その算法では主係数問題にWangの方法が使えず、Inabaは疎な多項式用の主係数割り振り法を新たに考案した。しかし、因数分解に限っても、算法にはまだ次の二つの欠陥がある。

欠陥a) Newton多項式が無平方でない場合の処理法が未開発である。

欠陥b) Hensel因子は従変数の有理式級数となるが、その組み合せ方が非効率である。さらに、GCDに関しては全く手付かずである。

本稿では、第2章で拡張Hensel構成を簡単に復習したあと、第3章でNewton多項式が無平方でない場合の処理方法を述べ、第4章で拡張Hensel級数をGCDと因数分解の観点から理論解析し、第5章で疎な多変数多項式のGCD算法を具体的に説明する。

2 拡張Hensel構成の簡単な復習

読者は多変数多項式に対する(一般)Hensel構成法を熟知しているとする。まず、拡張Hensel構成で最も重要な概念である**Newton多項式**を定義する。与式$F(x,\boldsymbol{u})$は体$\mathbb{K}$上の多項式だが、後々のため下記では$\mathbb{K}(\boldsymbol{u})[x]$の元とする。また、定義中、$\boldsymbol{u}$の多項式$f(\boldsymbol{u})$の位数$\mathrm{ord}(f)$とは、$f$の各項の全次数の中で最小のものである。

定義 1 (Newton線とNewton多項式、正味Newton多項式)
$F(x,\boldsymbol{u})$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。$F(x,t\boldsymbol{u})$の各項を$cx^it^ju_1^{j_1}\cdots u_\ell^{j_\ell}/D(t\boldsymbol{u})$とする；ここで、$c\in\mathbb{K}$, $j=j_1+\cdots+j_\ell$、$D(\boldsymbol{u})$は$\mathrm{ord}(D)=d<j$なる$\boldsymbol{u}$の多項式である。この項を(e_x,e_t)-面上の点$(i,j-d)$にプロットする。全プロット点を囲む凸包$\boldsymbol{\mathcal{N}}$を**Newton多角形**という。$\boldsymbol{\mathcal{N}}$の全底辺を時計周りに$\mathcal{N}_1,\ldots,\mathcal{N}_\rho$と表し、それぞれ**Newton線**と呼ぶ。各$i\in\{1,\ldots,\rho\}$に対し、$\mathcal{N}_i$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$x$座標を$n_i$とすれば$\overline{F}_{\mathcal{N}_i}$は$x^{n_i}$で割り切れる。$\overline{F}_{\mathcal{N}_i}/x^{n_i}$を$F_{\mathcal{N}_i}(x,\boldsymbol{u})$と表し**正味Newton多項式**と呼ぶ。 □

注釈 上定義では$F(x,\boldsymbol{u})\in\mathbb{K}(\boldsymbol{u})[x]$としたが、入力式は$\mathbb{K}[x,\boldsymbol{u}]$の要素であり、従変数の有理式がHensel因子に現れるのは初期因子以外の項だけである。したがって、拡張Hensel因子に対するNewton多項式も$\mathbb{K}[x,\boldsymbol{u}]$の要素である。

(一般)Hensel構成では、前章の条件2)を満足させるため、$F_0(x)$が無平方になるように展開点$\boldsymbol{s}$を選ぶ。しかし、拡張Hensel構成では基本的に原点移動は行わず、従変数$\boldsymbol{u}$の原点で展開する；特異点近傍での代数関数の振舞い等を見るには特異点上で展開するのがよいからである。したがって、一般に無平方ではない複数のNewton多項式を扱う。

拡張Hensel構成は、ρ個のNewton線上で$\mathcal{N}_1\Rightarrow\mathcal{N}_2\Rightarrow\cdots\Rightarrow\mathcal{N}_\rho$の順に実行される。定義1でNewton多項式を定義するために全次数変数tを導入したが、拡張Hensel構成では各Newton線の傾きに依存してxと従変数$\boldsymbol{u}$の重み付けを行う(それにより式表現と計算が簡潔になる)。その重み付けにも変数tを用いる。$\mathcal{N}_1$の右端の座標点を(n_0,ν_0)、$\mathcal{N}_i$の左端の座標点を(n_i,ν_i)とすれば、$\mathcal{N}_i$の傾きは$\lambda_i=(\nu_{i-1}-\nu_i)/(n_{i-1}-n_i)$である。$\hat{n}_i$と$\hat{\nu}_i$は$\hat{n}_i>0$, $\hat{\nu}_i/\hat{n}_i=\lambda_i$, $\gcd(\hat{n}_i,\hat{\nu}_i)=1$を満たす整数とする。このとき、重み付きの多項式$\mathcal{F}_i(x,\boldsymbol{u},t)$, $\overline{\mathcal{F}}_{\mathcal{N}_i}(x,\boldsymbol{u})$およびイデアル$\mathcal{I}_k$を次式で定義する(簡単のため添字$i$を略す)。

$$\begin{cases} \mathcal{F}(x,\boldsymbol{u},t) & \stackrel{\mathrm{def}}{=} & t^{\hat{n}(\lambda n-\nu)}F(x/t^{\hat{\nu}},t^{\hat{n}}\boldsymbol{u}), \\ \overline{\mathcal{F}}_{\mathcal{N}}(x,\boldsymbol{u}) & \stackrel{\mathrm{def}}{=} & t^{\hat{n}(\lambda n-\nu)}\overline{F}_{\mathcal{N}}(x/t^{\hat{\nu}},t^{\hat{n}}\boldsymbol{u}), \\ \mathcal{I}_k & \stackrel{\mathrm{def}}{=} & \langle t^k\rangle, \quad k=1,2,3,\ldots. \end{cases} \tag{2.1}$$

上記で、$\overline{\mathcal{F}}_{\mathcal{N}}(x,\boldsymbol{u})$が$t$を含まないのは誤植ではなく、そうなるように重み付けを行ったのである。さらに、$\mathcal{I}_k$もiによらない。

拡張Hensel構成では、Newton多項式$\overline{F}_{\mathcal{N}}(x,\boldsymbol{u})$を因数分解し、その因子を初期因子としてHensel構成を行う。多変数代数関数の解析では$\overline{F}_{\mathcal{N}}(x,\boldsymbol{u})$を$x$の1次因子の積に分解した(明示的に分解できるとは限らないので、一般には$\overline{F}_{\mathcal{N}}$の根を記号的に導入する必要

がある)。しかし、GCD と因数分解では $\mathbb{K}[x,\boldsymbol{u}]$ 内で因数分解する。通常、まず行うのが各 Newton 線に Hensel 因子 1 個が対応するように $F(x,\boldsymbol{u})$ を分解することである (よって $\rho=1$ の場合は不必要)。この分解を **Newton 線上の最大因子の分離**という。

$$F(x,t\boldsymbol{u}) \equiv F_1^{(k)}(x,t\boldsymbol{u})\cdots F_\rho^{(k)}(x,t\boldsymbol{u}) \pmod{t^{k+1}}, \quad \deg_x(F_i^{(k)}) = n_{i-1}-n_i\ (\forall u). \tag{2.2}$$

上記の分解は一度に行えないので、$\mathcal{N}_1 \Rightarrow \mathcal{N}_2 \Rightarrow \mathcal{N}_3 \Rightarrow \cdots$ と順に行う。しかし、方法は全く同じなので、添え字 i を省き、Newton 線 $\mathcal{N}$ 上で $\overline{F}_{\mathcal{N}}(x,\boldsymbol{u}) = x^m F_{\mathcal{N}}(x,\boldsymbol{u})$ であるとして、$\mathcal{N}$ 上の最大因子の分離を説明する。x^m と $F_{\mathcal{N}}(x,\boldsymbol{u})$ は互いに素なので、

$$\begin{cases} A_l(x,\boldsymbol{u})F_{\mathcal{N}}(x,\boldsymbol{u}) + B_l(x,\boldsymbol{u})x^m = x^l \quad (l=0,1,\ldots,\deg_x(\overline{F}_{\mathcal{N}})-1), \\ \deg_x(A_l) < m, \quad \deg_x(B_l) < \deg_x(F_{\mathcal{N}}), \end{cases} \tag{2.3}$$

を満たす組 (A_l,B_l) が拡張互除法で計算できる。A_l と B_l を用いれば、一般 Hensel 構成と全く同様に、次式を満たす k 次の Hensel 因子 $F_*^{(k)}(x,t\boldsymbol{u})$ と $\widetilde{F}^{(k)}(x,t\boldsymbol{u})$ が計算できる；具体的な計算公式は次項「Newton 線上での Hensel 因子の計算」で与える。

$$\begin{cases} F(x,t\boldsymbol{u}) \equiv F_*^{(k)}(x,t\boldsymbol{u})\widetilde{F}^{(k)}(x,t\boldsymbol{u}) \pmod{t^{k+1}}, \\ F_*^{(0)}(x,\boldsymbol{u}) = F_{\mathcal{N}}(x,\boldsymbol{u}), \quad \widetilde{F}^{(0)}(x,\boldsymbol{u}) = x^m. \end{cases} \tag{2.4}$$

$\mathcal{N}=\mathcal{N}_1$ の場合、$F_*^{(k)} = F_1^{(k)}$ かつ $\widetilde{F}^{(k)} \equiv F_2^{(k)}\cdots F_\rho^{(k)}$ となる。(2.3) では、$A_l, B_l \in \mathbb{K}(\boldsymbol{u})[x]$ であることに注意されたい。そのため、Hensel 因子も一般に $\mathbb{K}(\boldsymbol{u})[x]$ に属する。(A_l,B_l) は以下のように簡単に計算できるので、Newton 線上の最大因子は意外に簡潔になる。

命題 1 (最大因子分離での多項式 A_l,B_l； Sasaki·Inaba 2000)
(2.3) を満たす A_l,B_l は次式で与えられる：下記で、$F_{\mathrm{Inv}\langle x^m\rangle} \in \mathbb{K}(\boldsymbol{u})[x]$ は $\deg(F_{\mathrm{Inv}\langle x^m\rangle}) < m$ を満たし、x^m を法とする $F_{\mathcal{N}}$ の逆元として計算できる $\Rightarrow F_{\mathrm{Inv}\langle x^m\rangle}F_{\mathcal{N}} \equiv 1 \pmod{x^m}$。

$$\begin{cases} \text{for } l \geq m \ : \ A_l = 0, & B_l = x^{l-m}, \\ \text{for } l < m \ : \ A_l = F_{\mathrm{Inv}\langle x^{m-l}\rangle}x^l, & B_l = [1 - F_{\mathrm{Inv}\langle x^{m-l}\rangle}F_{\mathcal{N}}]/x^{m-l}. \end{cases} \tag{2.5}$$

各 Newton 線 $\mathcal{N}_i$ 上の最大 Hensel 因子 $F_i^{(k)}(x,\boldsymbol{u})$ を分離すると、次にはこの因子をさらに低次の Hensel 因子の積に分解する (以下、添字 i を省略する)。まず、$F_{\mathcal{N}}(x,\boldsymbol{u})$ を既約因子に因数分解する；次式で $\mathrm{cont}(F_{\mathcal{N}})$ は $F_{\mathcal{N}}$ の**係因数** (係数の GCD) を表す。

$$\begin{cases} F_{\mathcal{N}}(x,\boldsymbol{u}) = \mathrm{cont}(F_{\mathcal{N}})\, G_1^{(0)}(x,\boldsymbol{u})\cdots G_r^{(0)}(x,\boldsymbol{u}), \\ \gcd(G_{j_1}^{(0)}, G_{j_2}^{(0)}) = 1 \quad (\forall j_1 \neq j_2). \end{cases} \tag{2.6}$$

次に、$l=0,1,\ldots,n-1$ に対して、次式を満たす多項式 $A_1^{(l)},\cdots,A_r^{(l)}$ を計算する。

$$\begin{cases} A_1^{(l)}(x,\boldsymbol{u})\dfrac{F_{\mathcal{N}}(x,\boldsymbol{u})}{G_1^{(0)}(x,\boldsymbol{u})} + \cdots + A_r^{(l)}(x,\boldsymbol{u})\dfrac{F_{\mathcal{N}}(x,\boldsymbol{u})}{G_r^{(0)}(x,\boldsymbol{u})} = x^l, \\ \deg(A_i^{(l)}) < \deg(G_i^{(0)}) \quad (1 \leq \forall i \leq r). \end{cases} \tag{2.7}$$

次に、F の主係数、それを $\mathrm{lc}(F)$ と表す、の各因子を $\mathrm{lc}(F)=\mathrm{lc}(G_1^{(0)}\cdots G_r^{(0)})$ が成立するように $F, G_1^{(0)}, \ldots, G_r^{(0)}$ に分配する。具体的には、$\mathrm{lc}(F)$ の各因子の Newton 線上の項は $F_{\mathcal{N}}$ に入っているので、Newton 線上の項が $\mathrm{lc}(G_1^{(0)}), \ldots, \mathrm{lc}(G_r^{(0)})$ にどのように分配されているかを見て、各因子を割り振る。詳細は [5] を参照されたい。$\mathrm{cont}(F_{\mathcal{N}})$ は Hensel 構成した後で同様に分配する。そして、(2.1) により t-order を導入しイデアル $\mathcal{I}_k$ を定義する。この過程で、$F, G_1^{(0)}, \ldots, G_r^{(0)}$ をそれぞれ $\mathcal{F}, \mathcal{G}_1^{(0)}, \ldots, \mathcal{G}_r^{(0)}$ に変換する。

最後に、$\mathcal{G}_1^{(0)}, \ldots, \mathcal{G}_r^{(0)}$ を初期因子として、よく知られた次の計算式により、$\mathcal{G}_1^{(k)}, \ldots, \mathcal{G}_r^{(k)}$ を $k=0\to 1\to 2\to\cdots$ と逐次的に構成する (次式で $n=\deg_x(F(x,\boldsymbol{u}))$ である)。

$$\left\{\begin{array}{rcl} \delta\mathcal{F}^{(k)} & \equiv & \mathcal{F}(x,\boldsymbol{u},t)-\mathcal{G}_1^{(k-1)}(x,\boldsymbol{u},t)\cdots\mathcal{G}_r^{(k-1)}(x,\boldsymbol{u},t) \pmod{t^{k+1}} \\ & = & t^{k+\hat{n}(\nu-\lambda n)}\,[\delta f_{n-1}(\boldsymbol{u})x^{n-1}+\cdots+\delta f_0(\boldsymbol{u})], \\ \mathcal{G}_i^{(k)} & = & \mathcal{G}_i^{(k-1)}+t^{k+\gamma_i}\sum_{l=0}^{n-1}A_i^{(l)}(x,\boldsymbol{u})\delta f_l(\boldsymbol{u}) \quad (i=1,\ldots,r), \\ & & \text{where } \gamma_i \text{ is the } t\text{-order of } G_i^{(0)}(x/t^{\hat{\nu}}, t^{\hat{n}}\boldsymbol{u}). \end{array}\right. \tag{2.8}$$

ここで、$A_i^{(l)}\in\mathbb{K}(\boldsymbol{u})[x]$ は $\deg_x(A_i^{(l)})<\deg(G_i^{(0)})$ を満たし、計算法は以下に示す。

第 4 章で有理式を含む Hensel 因子の組み合わせ方を論じるが、その際に Hensel 因子に含まれる有理式の分母が重要になる。有理式の分母は $A_i^{(l)}$ と $B_i^{(l)}$ の分母因子に決定的に依存する。そこで、分母因子がどんなものか調べておこう。$A_i^{(0)}$ と $B_i^{(0)}$ は次式を満たす x の多項式として一意的に定まる (Euclid の拡張互除法で計算できる)。

$$A_i^{(0)}(x,\boldsymbol{u})\frac{F_{\mathcal{N}}(x,\boldsymbol{u})}{G_i^{(0)}(x,\boldsymbol{u})}+B_i^{(0)}(x,\boldsymbol{u})G_i^{(0)}(x,\boldsymbol{u})=1, \tag{2.9}$$

$A_i^{(l)}$ と $B_i^{(l)}$ $(l\geq 1)$ は、$A_i^{(0)}$ と $G_i^{(0)}$ から $\mathrm{rem}(x^lA_i^{(0)}, G_i^{(0)})$ で計算できる (rem は剰余演算である)。以上より、つぎの命題が得られる。

命題 2 (各 Newton 線上の因子分離での $A_i^{(l)}, B_i^{(l)}$; Sasaki · Inaba 2000)
$F(x,\boldsymbol{u})$ は $\mathbb{K}(\boldsymbol{u})[x]$ の要素で、$\deg_x(F)=n$ であり、その *Newton* 線は $\mathcal{N}$ 一本だけであるとする。F の *Newton* 多項式 $F_{\mathcal{N}}$ の $\mathbb{K}$ 上での互いに素な因数分解を $F_{\mathcal{N}}=G_1^{(0)}\cdots G_r^{(0)}$ とするとき *($r\geq 2$ とする)*、(2.7) を満たす $A_i^{(l)}(x,\boldsymbol{u})$ は次式で表される。

$$A_i^{(l)}(x,\boldsymbol{u})=\frac{N_i^{(l)}(x,\boldsymbol{u})}{\mathrm{lc}(G_i^{(0)})^l\,\mathrm{res}(G_i^{(0)}, F_{\mathcal{N}}/G_i^{(0)})}, \quad N_i^{(l)}\in\mathbb{K}[x,\boldsymbol{u}]. \tag{2.10}$$

ここで、分子と分母の共通因子の除去は行わないものとする。 □

なお、$r\geq 3$ のとき、$R_{j_1,j_2}(\boldsymbol{u})=\mathrm{res}_x(G_{j_1}^{(0)}, G_{j_2}^{(0)})$ $(\forall j_1\neq j_2)$ とおけば、次式が成立する。

$$\mathrm{res}(G_i^{(0)}, F_{\mathcal{N}}/G_i^{(0)})=\textstyle\prod_{j=1,\neq i}^{r}R_{i,j}(\boldsymbol{u}). \tag{2.11}$$

本章の最後に、Inaba[5] による実験結果の一部を再掲して、筆者らの方法が疎な多変数多項式の因数分解に如何に有効かを示そう。例題は下記の多項式 P_k を展開したもので、Inaba は $k = 10,\ 20,\ \ldots,\ 50$ に対して三つの方法で因数分解し、計算時間を比較した。三つの方法とは、一般 Hensel 構成を用いる古典的方法 (H)、Wang の主係数割り当てを行って効率化した方法 (W)、拡張 Hensel 構成を用いた方法 (E)、である。

$$\begin{aligned} P_k &= [\, x^2y^2z + x\,(y^k + z^k) + 3y + 3z - 3z^2 - 2y^{k/2}z^{k/2} \,] \\ &\times [\, x^3y^2z^2 + x\,(y^k + z^k) - 2y - 5z + 4y^2 + 3y^{k/2}z^{k/2} \,] \end{aligned}$$

k	T_H (sec)	T_W (sec)	T_E (sec)	T_H/T_E	T_W/T_E
10	0.0918	0.0240	0.0167	5.50	1.44
20	0.910	0.194	0.0319	28.5	6.08
30	5.66	0.823	0.0440	129.	18.7
40	21.6	2.61	0.0460	470.	56.7
50	63.6	6.23	0.0520	1220.	120.

- method H : 古典的方法 (一般 Hensel 構成)
- method W : Wang の方法 (主係数の振分け)
- method E : 我々の方法 (拡張 Hensel 構成)

拡張 Hensel 構成を用いる方法が従来法を如何に改善するか、目を見張る (非零代入がそれほど大きな数式爆発を引き起こしたということ)。因みに、P_k は k の値によらず項数が 39 だが、従来法では y, z とも原点移動する必要があり、$(y, z) = (1, 1)$ に移動すると P_{50} では項数が 9813 に爆発し、係数も最大 29 桁に成長する。拡張 Hensel 構成を用いる方法の計算時間はほぼ k に比例するが、これは P_k が y, z に関して全次数が $2k$ なので、k に比例して高く Hensel 因子を計算する必要があるからである。

3 Newton 多項式が無平方でない場合への対処法

第 1 章で、因数分解では「$F_0(x)$ が無平方である」との条件が必要であることを述べた。そのためには $F(x, \boldsymbol{u})$ の無平方性が必要だが、$F(x, \boldsymbol{u})$ の無平方性は事前に無平方分解を実行して保証する。しかし、$F_0(x)$ の無平方性は保証されないので、$F_0(x)$ が無平方になるまで $F(x, \boldsymbol{u})$ で従変数の原点移動を繰り返す (そのため、疎な多項式では項数が増える)。しかし、第 2 章で述べたように、拡張 Hensel 構成を用いる方法では原点移動を行わない。したがって、原点移動を行わずに Newton 多項式の重複因子を処理しなければならない。本章ではその問題解決を目指す。なお、多変数代数方程式の "特異点での級数展開" 法では、根の低次項を使って主変数 x の原点移動を行い問題を解決したが、本稿では Hensel 構成の初期因子は多項式なので、その方法は一般には使えない。

筆者らは、因数分解算法で使うことを念頭に五つの対処法を考えた。対処法 A) 従変数に重み付けを行う、対処法 B) 従変数をたとえば $z \to 1/z$ と変換する、対処法 C) 主変数を取り替える、対処法 D) 2 変数なら原点移動する (従来法)。以下では、Newton 線 $\mathcal{N}$ 上

の正味Newton多項式 $F_{\mathcal{N}}(x,\boldsymbol{u})$ が重複因子 $[Q(x,\boldsymbol{u})]^{\sigma}$, $\sigma \geq 2$, を含むとし、この重複因子を初期因子とするHensel因子 $G^{(k)}(x,\boldsymbol{u})$ が既に分離されたと仮定する。

対処法 A) 次の例を考えよう (下記で y の重みが w_y なら $y \to y^{w_y}$ と変換する)。

$$G(x,y,z) = (1-z^2)\,x^2 + (2y-2z^3)\,x + (y^2-z^4).$$

$G_{\mathcal{N}}(x,y,z) = (x+y)^2$ に注意。試みに $(w_y, w_z) = (2,1)$ としてみる (下記では $y \to y^2$ とすると紛らわしいので、$y \to u^2$ とする)。

$$\widetilde{G}(x,u,z) \stackrel{\text{def}}{=} G(x,u^2,z) = (1-z^2)\,x^2 + (2u^2-2z^3)\,x + (u^4-z^4).$$

$\widetilde{G}$ のNewton多項式は $\widetilde{G}_{\mathcal{N}} = x^2+2u^2x+u^4-z^4 = (x+u^2+z^2)\,(x+u^2-z^2)$ で、目出度く無平方となった。右辺の互いに素な多項式を初期因子とし、$G(x,y,z)$ の主係数 $1-z^2$ を因数分解し、その各因子 $1+z$, $1-z$ をInabaの方法で $\widetilde{G}_{\mathcal{N}}$ の2因子に分配し、拡張Hensel構成により $\widetilde{G}$ を因数分解すると、次なる分解が得られる。

$$\widetilde{G}(x,u,z) = [(1+z)x + u^2+z^2] \cdot [(1-z)x + u^2-z^2].$$

最後に、$u^2 \to y$ と戻せばよい。 □

対処法 B) 次の例を考えよう：$G(x,y,z) = (x+y+z^2)\,(x+y+yz)$.
x が主変数のとき：$G_{\mathcal{N}} = (x+y)^2$.
z が主変数のとき：$G_{\mathcal{N}_1} = yz+(x+y)$, $G_{\mathcal{N}_2} = (x+y)z^2 + (x+y)^2$.
目出度くNewton多項式が無平方になった。

対処法 C) 次の例を考えよう： $G(x,y,z) = x^2 + (2y+yz+z^2)\,x + (y+z^2)(y+yz)$.
従変数 z の高次項と低次項を入れ替える変換を G に行うと、

$$\widetilde{G}(x,y,z) = z^3 G(x,y,1/z) \Longrightarrow \widetilde{G}_{\mathcal{N}} = zx(z^2x+1)$$

となり、Newton多項式が目出度く無平方になった。

対処法 D) 本対処法は2変数限定である。上記の対処法のうち対処法A) が最も自由度が高いが、2変数多項式には全く無力である。そこで、2変数の場合には非零代入による数式爆発は大したことはないだろうとの希望的観測の下、本対処法を設けたのである。

筆者らは対処法A) を最も重視している。Newton多項式の無平方化に加え、GCD計算では“ラッキー”なNewton多項式を生成する必要がある。そのため自由度の高いNewton多項式生成法が欲しいのである。以下で対処法A) を簡単に分析する。

与式 $F(x,u_1,\ldots,u_\ell)$ では従変数 $u_1,\ldots,u_\ell$ の重みはすべて1である。与式に対する正味Newton多項式を $F_{\mathcal{N}}(x,u_1,\ldots,u_\ell)$ とする。F の従変数に重み付けを行った多項式とそのNewton多項式をそれぞれ $\widetilde{F}$, $\widetilde{F}_{\mathcal{N}}$ と表す。さらに、$\mathrm{ltm}(P)$ と $\mathrm{ctm}(P)$ は多項式 $P(x,\boldsymbol{u})$ の主変数 x に関する**主項 (最高次数項)** と**定数項**をそれぞれ表す。

従変数の重み付けでは、我々は従変数 u_i を選び (稀には u_i,u_j と 2 個選ぶこともあり、さらに多く選ぶ場合もある)、u_i の重みを 2 にする (重みを多くすると従変数の全次数が大きくなり、Hensel lifting を多数回実行することになるので不利である)。

$$F(x,..,u_i,..) \to F(x,..,v_i^2,..). \tag{3.1}$$

従変数 u_i の選び方には自由度があり、目的に応じて (厳格ではないが) 次のように選ぶ。

- **Newton 多項式を無平方化する場合**: u_i は $F_{\mathcal{N}}$ の従変数から自由に選ぶ。
- **Newton 多項式をラッキー化する場合**: u_i は $\mathrm{ltm}(F_{\mathcal{N}})$ または $\mathrm{ctm}(F_{\mathcal{N}})$ から選ぶ。
- **下記の *easyFactori* では**: $\mathrm{ltm}(F_{\mathcal{N}})$ または $\mathrm{ctm}(F_{\mathcal{N}})$ に含まれる全ての従変数。

Newton 多項式をラッキー化するのに u_i を $\mathrm{ltm}(F_{\mathcal{N}})$ または $\mathrm{ctm}(F_{\mathcal{N}})$ から選ぶのは、そうすることで元の Newton 線が右端または左端で上に折れ曲がる可能性が高くなり、5 章で述べる条件 b) が満足され易いからである。プロシジャ *easyFactori* は、Newton 多項式 $F_{\mathcal{N}}$ を引数とし、$F_{\mathcal{N}}$ が二つ以上の因子に分解されることが分っている場合に、この因数分解 (既約分解とは限らない) を安直に実行する。

Procedure *easyFactori*$(F_{\mathcal{N}}(x,\boldsymbol{u})) ==$
step-1: choose subvariables to be weighted;
step-2: **do** $\boldsymbol{u}$-weighting of $F_{\mathcal{N}}$: $F_{\mathcal{N}}(x,\boldsymbol{u}) \mapsto G(x,\boldsymbol{v})$,
such that $G(x,\boldsymbol{v})$ has $r \geq 2$ Newton lines;
let r net Newton polynomials
on the Newton lines be $G_1^{(0)},\ldots,G_r^{(0)}$;
step-3: **do** EHC of G with initial factors $G_1^{(0)},\ldots,G_r^{(0)}$
and try to get polynomial factors of $G(x,\boldsymbol{v})$;
step-4: **if** not gotten **then return** nil
else return polynomial factors in $\boldsymbol{u}$.

補題 1 $F_{\mathcal{N}}$ が 1 変数でない限り u_i を選ぶことができる。
証明 u_i を $\mathrm{ltm}(F_{\mathcal{N}})$ または $\mathrm{ctm}(F_{\mathcal{N}})$ から選ぶ場合だけを考えればよい。$F_{\mathcal{N}}$ は $(x/t^{\hat{\nu}}, t^{\hat{n}}\boldsymbol{u})$-斉次であるから、$\mathrm{ltm}(F_{\mathcal{N}})$ と $\mathrm{ctm}(F_{\mathcal{N}})$ がともに従変数を含まなければ $F_{\mathcal{N}}$ 全体が x だけの多項式となり、仮定に反する。 □

上記の、無平方化とラッキー化のための u_i の選択法は、非常に高い確率で $\widetilde{G}_{\mathcal{N}}$ を無平方にするだろう。というのも、多項式が重複因子を含むことは係数間に強い関係があることを意味するが、u_i を上記のように選ぶと u_i を含む項は $\widetilde{G}_{\mathcal{N}}$ では消えており、強い関係も失われているだろうからである。しかし、常に無平方化できるとは限らない。

次に、*easyFactori*$(F_{\mathcal{N}})$ について考えよう。この安直な因数分解法は、下記の補題 2 に記した二つの条件が成立する場合に限り有用である；下記で、$\mathrm{subvars}(F)$ は多項式 F に含まれるすべての従変数の集合を表す。

補題 2 F_N は次の条件 i) と ii) を満たすとする。条件 i) x の異なる指数が 3 個以上ある、条件 ii) $\mathrm{subvars}(\mathrm{ltm}(F_N)) \neq \mathrm{subvars}(F_N)$, $\mathrm{subvars}(\mathrm{ctm}(F_N)) \neq \mathrm{subvars}(F_N)$ の一方あるいは両方が成立する。このとき、条件 ii) を満たす $\mathrm{ltm}(F_N)$ あるいは $\mathrm{ctm}(F_N)$ に含まれる従変数を重み付けることにより、$\widetilde{F}_N$ は 2 個以上の Newton 線を持つようにできる。

証明 簡単のため $\mathrm{ltm}(F_N)$ が条件 ii) を満たすとし、$\mathrm{ltm}(F_N)$ の全ての項の重みが増えるように重み付ける。すると、F_N の主項はより高い位置にプロットされる。しかし、主項でない項の少なくとも一つは同じ位置にプロットされる。したがって、$\widetilde{F}_N$ の Newton 線は少なくとも 2 本の異なる傾きをもつ Newton 線を持つ。 □

4 Hensel 因子に対する基本的な命題と定理

$F(x, \boldsymbol{u})$, $\deg_x(F) = n$, で項 $f_i(\boldsymbol{u})x^i$ $(1 \leq i \leq n)$ を $f_i(\boldsymbol{u})x^{n-i}$ に移す変換を Rev とする。

$$\mathrm{Rev}(F(x, \boldsymbol{u})) = x^n F(1/x, \boldsymbol{u}). \tag{4.1}$$

まず初めに Hensel 因子 $G_i^{(\infty)}$ を分類しておく。

Class-1) $G_i^{(\infty)} \in \mathbb{K}[x, \boldsymbol{u}]$ (多項式因子)

Class-2) $G_i^{(\infty)} \in \mathbb{K}\{\boldsymbol{u}\}[x]$ (係数は $\boldsymbol{u}$ の形式的べき級数)

Class-3) $G_i^{(\infty)} \in \mathbb{K}\{(\boldsymbol{u})\}[x]$ (係数は $\boldsymbol{u}$ の有理式の形式的級数)
ただし、分子分母は可能なかぎり簡約する。

最終的に欲しいのは Class-1 の因子で、それは Class-2 や Class-3 の因子を掛けて得られる。どの因子を掛ければよいかは、Class-3 の因子に関してはかなり解っているが、Class-2 の因子に関しては解っていない。算法では如何に速く Class-1 の因子を得るかが重要である。

命題 3 ($F = GH$ に対する Newton 線に関する命題; Sasaki · Inaba 2000)
F, G, H は $\mathbb{K}[x, \boldsymbol{u}]$ の要素で、$F = GH$ を満たすとする。G の *Newton* 線を $\mathcal{N}'_1, \ldots, \mathcal{N}'_{\rho'}$, その傾きの集合を $\Lambda' = \{\lambda'_1, \ldots, \lambda'_{\rho'}\}$、$H$ の *Newton* 線を $\mathcal{N}''_1, \ldots, \mathcal{N}''_{\rho''}$, その傾きの集合を $\Lambda'' = \{\lambda''_1, \ldots, \lambda''_{\rho''}\}$ とする *(添え字は対応させる)*。このとき、F の *Newton* 線を $\mathcal{N}_1, \ldots, \mathcal{N}_\rho$ とすれば、その傾きの集合は $\Lambda = \Lambda' \cup \Lambda''$ である。$F_{\mathcal{N}_i}, G_{\mathcal{N}'_i}, H_{\mathcal{N}''_i}$ はそれぞれ F, G, H の $\mathcal{N}_i$ 上の *Newton* 多項式とする *($\mathcal{N}'_i, \mathcal{N}''_i$ が無い場合には対応する G と H の Newton 多項式は 1 とする)*。このとき、次式が成立する *("hleng" は "horizontal length" を表す)*。

$$\begin{cases} \mathrm{hleng}(\mathcal{N}_i) = \mathrm{hleng}(\mathcal{N}'_i) + \mathrm{hleng}(\mathcal{N}''_i), \\ F_{\mathcal{N}_i}(x, \boldsymbol{u}) = G_{\mathcal{N}'_i}(x, \boldsymbol{u}) \cdot H_{\mathcal{N}''_i}(x, \boldsymbol{u}). \end{cases} \tag{4.2}$$

同様に、F_1, F_2, D は $\mathbb{K}[x, \boldsymbol{u}]$ の要素で、$D = \gcd(F_1, F_2)$ とする。F_1, F_2, D の *Newton* 線 $\mathcal{N}_i$ 上の *Newton* 多項式をそれぞれ $F_{1\mathcal{N}_i}, F_{2\mathcal{N}_i}, D_{\mathcal{N}_i}$ とすれば、次式が成立する。

$$D_{\mathcal{N}_i}(x, \boldsymbol{u}) \mid \gcd(F_{1\mathcal{N}_i}(x, \boldsymbol{u}), F_{2\mathcal{N}_i}(x, \boldsymbol{u})). \tag{4.3}$$

証明 異なる傾きの線に乗る2項以上の多項式の積の項は厚みのある平行四辺形内に分布する。(4.2) はその対偶から得られる。(4.2) より、異なる傾きの Newton 線上の Newton 多項式は共通因子を持たないから、(4.3) を得る。 □

定理 1 (有理式係数の分母因子に関する定理)
定理1と同様、$F_{\mathcal{N}_i}$ の互いに素な因数分解を $G_{i,1}^{(0)}\cdots G_{i,r_i}^{(0)}$ とし、初期因子 $G_{i,j_1}^{(0)}$ と $G_{i,j_2}^{(0)}$ $(j_1 \neq j_2)$ の x に関する終結式を $R_{i;j_1,j_2} = \mathrm{res}_x(G_{i,j_1}^{(0)}, G_{i,j_2}^{(0)})$ とすれば，$G_{i,j}^{(0)}$ に対応する *Hensel* 因子 $G_{i,j}^{(k)}$ に現れる有理式の分母因子は下記の三つのみである。

$$\begin{cases} \mathrm{lc}(G_{i,j}^{(0)}) \text{ と } \mathrm{ctm}(G_{i,j}^{(0)}) \text{ のべき乗} \\ R_{i;j,j'} \ (j \neq j') \text{ の積のべき乗} \end{cases}$$

証明 この定理は単に命題1と命題2をまとめただけである。

定理 2 (同じ Newton 線上の Class-3 因子の組合せに関する定理)
Newton 線 $\mathcal{N}$ 上の最大 *Hensel* 因子を $F(x,\boldsymbol{u})$、その *Newton* 多項式を $F_{\mathcal{N}}$、その $\mathbb{K}$ 上での互いに素な因数分解を $F_{\mathcal{N}} = G_1^{(0)}\cdots G_r^{(0)}$ $(r \geq 2)$ とし、$G_i^{(0)}$ に対応する *Hensel* 因子を $G_i^{(k)}$ とする。$F(x,\boldsymbol{u})$ が *Class-3* でなく、*Hensel* 因子 $G_i^{(k)}$ の幾つかが *Class-3* のとき、*Hensel* 因子のどれかを掛けて有理式を含まない因子を得るには、分母が同じか共通因子を持つ *Hensel* 因子を掛ける必要がある。

証明 k に関する帰納法による。初期因子に有理式は現れないので $k=0$ では定理は正しい。$j=0,\ldots,k-1$ まで各 $G_i^{(j)}$ は有理式を含まないと仮定して、$j=k$ の場合を考える。算式 (2.8) より $\mathcal{G}_i^{(k)} = \mathcal{G}_i^{(k-1)} + \delta\mathcal{G}_i^{(k)}$ だが、まず、$\delta\mathcal{G}_i^{(k)}$ だけに分母因子 $\delta\widehat{G}_i^{(k)}/D_i$ が現れる場合を考える。$\mathcal{F} - \left(\prod_{j=1}^r \mathcal{G}_j^{(k)}\right) \pmod{t^{k+1}}$ に現れる有理式は $\left(\prod_{j\neq i}\mathcal{G}_j^{(0)}\right)\delta\widehat{G}_i^{(k)}/D_i$ だけだが、$G_i^{(0)}$ が原始的ゆえ D_i は $\left(\prod_{j\neq i}\mathcal{G}_j^{(0)}\right)$ とキャンセルせず、有理式が残る。このことは $\mathcal{F} \equiv \left(\prod_{j=1}^r \mathcal{G}_j^{(k)}\right) \pmod{t^{k+1}}$ に反するので、この場合は起こり得ない。

次に、$\delta\mathcal{G}_{i_1}^{(k)}$ と $\delta\mathcal{G}_{i_2}^{(k)}$ $(i_1 \neq i_2)$ だけにそれぞれ有理式 $\delta\widehat{G}_{i_1}^{(k)}/D_{i_1}$ と $\delta\widehat{G}_{i_2}^{(k)}/D_{i_2}$ が含まれる場合を考える。$\mathcal{F} - \mathcal{G}_1^{(k)}\cdots\mathcal{G}_r^{(k)} \pmod{t^{k+1}}$ に現れる有理式項は次式だけである：$\left(\prod_{j=1,\neq i_1,i_2}^r G_j^{(0)}\right)\cdot\left(G_{i_2}^{(0)}\delta\widehat{G}_{i_1}^{(k)}/D_{i_1} + G_{i_1}^{(0)}\delta\widehat{G}_{i_2}^{(k)}/D_{i_2}\right)$. この式も0でなければならない。しかし、分母項 D_{i_1}, D_{i_2} は対応する分子とはキャンセルしないので、$D_{i_1} = D_{i_2}$ あるいは $\gcd(D_{i_1}, D_{i_2}) \neq 1$ が必要である。

3個以上の Hensel 因子に有理式項が現れる場合も全く同様である。 □

拡張 Hensel 因子に限らず Hensel 因子全般には単元の不定性がある。$F(x,\boldsymbol{u})$ が与えられ初期因子とそれらの主係数が指定されれば、Hensel 因子は一意的に計算できるのだが、主係数を変更したり $\mathrm{Rev}(F(x,\boldsymbol{u}))$ を拡張 Hensel 構成したりすれば (このことは Newton 線で言えば $\mathcal{N}_\rho \Rightarrow \mathcal{N}_{\rho-1} \Rightarrow \cdots \Rightarrow \mathcal{N}_1$ の順で拡張 Hensel 構成することに対応する)、Hensel 因子も変わってくる。今の場合、単元は有理式を含み得るので注意を要する。たとえば、法が t^{k+1} で $R(\boldsymbol{u})$ が有理式の場合、$f = 1 + tR(\boldsymbol{u})$, $g = 1 - tR(\boldsymbol{u}) + t^2R^2(\boldsymbol{u}) + \cdots$ は

$fg \equiv 1 \pmod{t^{k+1}}$ を満たすので、f と g は t^{k+1} を法とする単元である。この不定性は、異なる傾きの Newton 線上の因子の組み合わせ方を複雑にする。

たとえば次の多項式を考えよう (これは次章で GCD 計算の例題に用いる)。

$$F(x,y,z) = [(x+y)(xz+1)+yz]\cdot[(x+z)(xy+1)-z^2]. \tag{4.4}$$

主変数を x、従変数を y,z とするとき、$F(x,y,z)$ は傾き $1,-1$ の 2 本の Newton 線 $\mathcal{N}_1,\mathcal{N}_2$ を持ち、正味 Newton 多項式はそれぞれ $F_{\mathcal{N}_1} = x^2yz+xy+xz+1$, $F_{\mathcal{N}_2} = x^2+xy+xz+yz$ となる。$\mathrm{ctm}(F_{\mathcal{N}_1}) = 1$ ゆえ、$\mathcal{N}_1,\mathcal{N}_2$ 上の最大 Hensel 因子は Class-2 となることが分かる：

$$\begin{aligned} F_1^{(5)} &= (x^2yz+xy+xz+1) - xy^2z^2 + xyz^3 - xy^3z^3 + xy^2z^4, \\ F_2^{(5)} &= (x^2) + xy + xz + xyz - xz^2 + yz + xy^2z^2 - xyz^3. \end{aligned} \tag{4.5}$$

$F(x,y,z)$ は二つの既約多項式の積だが、各既約多項式が二つの Hensel 因子に分裂して、上記の $F_1^{(5)}$ と $F_2^{(5)}$ に 1 個づつ入っている。したがって、既約多項式を得るには $F_1^{(5)}$ と $F_2^{(5)}$ をさらに 1 次の Hensel 因子に分解し、1 次因子の積を計算して多項式か否かをチェックする必要がある。具体的な因子は 5 章に示すが、従変数の全次数 3 まで計算したところ、$F_1^{(5)}$ の Hensel 因子は Class-2 で $F_2^{(5)}$ の Hensel 因子は Class-3 であった。すなわち、Class-2 と Class-3 の Hensel 因子の積で既約多項式を作り出す必要がある。こんな複雑な状況になったのは上述の Hensel 因子の不定性の所為であろう。実際、$\mathrm{Rev}(F)$ を拡張 Hensel 構成したところ、F の Hensel 因子とは異なる因子が得られた。傾きが異なる Newton 線上の Hensel 因子の組み合わせに関しては、まだまだ研究が必要である。現時点で確たることは言えないが、Newton 多項式は Hensel 因子の不定性には無関係なので、F と $\mathrm{Rev}(F)$ の終結式に関する情報は上記の因子組み合わせに有効であろう。

5 疎な多変数多項式の効率的 GCD 算法

与式 $F(x,\boldsymbol{u}), G(x,\boldsymbol{u})$ はともに原始的 (係数の GCD が 1) とし、$D(x,\boldsymbol{u}) = \gcd(F,G)$ とする。多変数多項式の GCD 計算法として、代表的で最も効率的と見なされているのは Moses・Yun による EZGCD 算法 [8] である (EZ は Extended Zassenhaus の略)。この方法は、まず適当な展開点 $\boldsymbol{s}$ において $D_0(x) = \gcd(F(x,\boldsymbol{s}), G(x,\boldsymbol{s}))$ を計算し、つぎに $D_0(x)$ と $H_0(x) = F(x,\boldsymbol{s})/D_0(x)$ を初期因子にして $F(x,\boldsymbol{u})$ を Hensel 構成する：

$$\begin{cases} F(x,\boldsymbol{u}) \equiv D^{(k)}(x,\boldsymbol{u})H^{(k)}(x,\boldsymbol{u}) \pmod{(\boldsymbol{u}-\boldsymbol{s})^{k+1}}, \\ D^{(0)}(x,\boldsymbol{u}) = D_0(x), \quad H^{(0)}(x,\boldsymbol{u}) = H_0(x). \end{cases} \tag{5.1}$$

Hensel 構成が可能なためには条件 a) $\gcd(D_0,H_0) = 1$ が必要で、$D^{(k)}(x,\boldsymbol{u})$ から $D(x,\boldsymbol{u})$ が計算できるためには条件 b) $\deg(D_0) = \deg_x(D)$ が必要である。$g = \gcd(\mathrm{lc}(F),\mathrm{lc}(G))$ は (算法を再帰的に適用して) 計算できるから、D_0 の主係数は $\mathrm{lc}(D^{(k)}) = g$ となるように調整する。問題は上記の 2 条件である。

条件 a) は常に成立するとは限らない。たとえば、 $F_0(x) \stackrel{\text{def}}{=} F(x, \boldsymbol{s}) = U(x)^2 V(x)$, $G_0(x) \stackrel{\text{def}}{=} G(x, \boldsymbol{s}) = U(x)V(x)^2$, $\gcd(U, V) = 1$, のときがそうである。幸いなことに、EZGCD 算法は $F_0(x)$ か $G_0(x)$ の一方が無平方なら適用でき、(次段落で説明するように) 無平方分解にも使える。EZGCD 算法により $F(x, \boldsymbol{u})$ と $G(x, \boldsymbol{u})$ が無平方化できるので、条件 a) は展開点 $\boldsymbol{s}$ をうまく選べば満足される。条件 b) は、EZGCD 算法に限らず、どのモジュラー算法でも必要な条件で、条件 b) が成立するとき D_0 は**ラッキー**であるという。条件 b) を満足させるためにも従変数の原点移動は必要である。

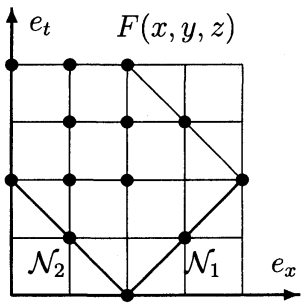
拡張 Hensel 構成を用いた GCD 計算法を考えよう。我々の方法でも上記条件 a) と b) は必要なので、まず上述した無平方分解を拡張 Hensel 構成に即して説明する。多変数多項式の無平方分解では $\gcd(P, dP/dx)$ なる形の GCD が次々に計算される。$P = Q_1 Q_2^2 \cdots Q_m^m$, $\gcd(Q_i, Q_j) = 1$ $(\forall i \neq j)$ に対して、$dP/dx = Q_0 Q_2 Q_3^2 \cdots Q_m^{m-1}$, $\gcd(Q_0, Q_i) = 1$ $(\forall i \geq 1)$ となる。そこで、$F = dP/dx$, $G = \gcd(P, dP/dx)$, $H = F/G$ とおくと、$H = Q_0$ となり、$\gcd(G, H) = 1$ となる。今の場合、与式は P と $F = dP/dx$ で、求めるものは $G = \gcd(P, dP/dx)$ である。そこで、$P(x, \boldsymbol{u})$ と $F(x, \boldsymbol{u})$ の Newton 多項式 $P_{\mathcal{N}}$ と $F_{\mathcal{N}}$ から $G_{\mathcal{N}} := \gcd(P_{\mathcal{N}}, F_{\mathcal{N}})$ を計算し、$G_{\mathcal{N}}$ と $H_{\mathcal{N}} := F_{\mathcal{N}}/G_{\mathcal{N}}$ を初期因子として $F(x, \boldsymbol{u})$ を拡張 Hensel 構成して $G(x, \boldsymbol{u})$ を求めればよい。

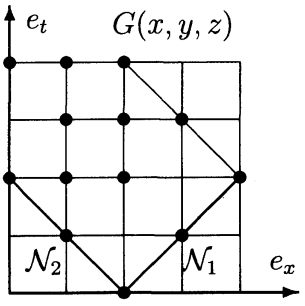
以上より、与多項式 $F(x, \boldsymbol{u})$ と $G(x, \boldsymbol{u})$ は無平方であるとしてよいが、非零代入を行わずに上記条件 a) と b) を満足させる必要がある。そのために筆者らは従変数の重み付けを利用する。さらに、従変数の重み付けは Newton 多項式の因子構造を安直に知ることにも使える。以下、GCD 計算の具体例を示しながらこれを説明する。

例 GCD 次の $F(x, y, z)$ と $G(x, y, z)$ の GCD を計算しよう (違いは最後の項だけ)。

$$\begin{aligned} F &= [(x+y)(xz+1) + yz] \cdot [(x+z)(xy+1) - z^2] \\ G &= [(x+y)(xz+1) + yz] \cdot [(x+z)(xy+1) - y^2] \end{aligned}$$

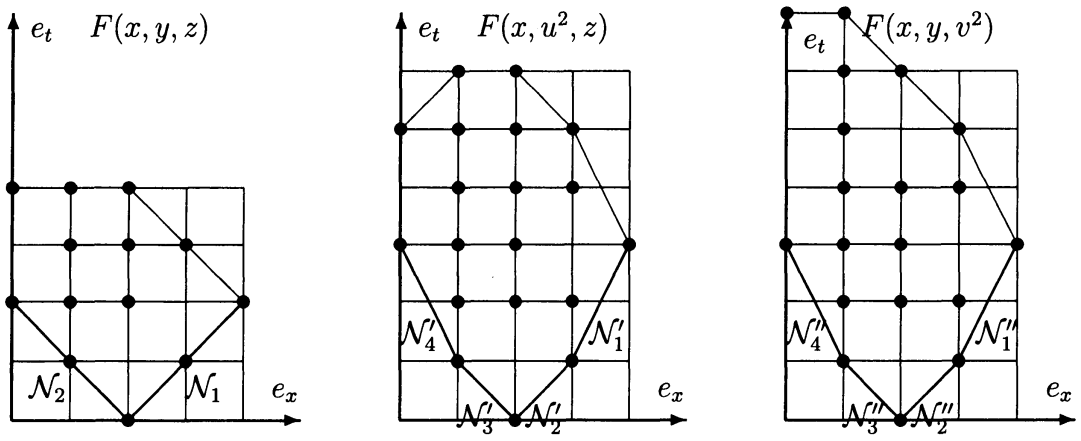
F と G は対応する Newton 線を 2 本づつ持ち (下図参照)、各線上の Newton 多項式は全く同じである：$F_{\mathcal{N}_1} = G_{\mathcal{N}_1} = x^2yz + xy + xz + 1$, $F_{\mathcal{N}_2} = G_{\mathcal{N}_2} = x^2 + xy + xz + yz$。





したがって命題 3 は使えず、各 $\mathcal{N}_1, \mathcal{N}_2$ 上での Hensel 因子を計算する必要があり、Newton 多項式 $F_{\mathcal{N}_1}$ と $F_{\mathcal{N}_1}$ を因数分解する必要がある。因数分解は計算が重いので、安直な方法で因子構造を知ることができないかと思うが、それは従変数の重み付けで可能である。

本例の $F(x,y,z)$ で従変数の重みを $F(x,u^2,z)$, $F(x,y,v^2)$ と変え、それぞれの多項式の各項を (e_x,e_t)-平面上にプロットすると下図となる。



上左図の Newton 線 $\mathcal{N}_1,\mathcal{N}_2$ が、中図と右図で傾きの異なる 2 本の Newton 線になることは、$\mathcal{N}_1,\mathcal{N}_2$ 上の Newton 多項式が異なる因子に分離 (すなわち因数分解) することを意味する。その因数分解には因数分解ルーチンを起動してもよいが、$\mathcal{N}_1$ 上と $\mathcal{N}_2$ 上の Newton 多項式に対してプロシジャ *easyFactori* を起動してもよい。

$$F_{\mathcal{N}_1}=(xy+1)(xz+1)=G_{\mathcal{N}_1},\qquad F_{\mathcal{N}_2}=(x+y)(x+z)=G_{\mathcal{N}_2}$$

これらの因子を $D_1:=xy+1$, $D_2=xz+1$, $D_3:=x+y$, $D_4=x+z$, とおくと、

$$\begin{aligned}\mathrm{res}(D_1,\mathrm{Rev}(D_3)) &= \mathrm{res}(D_2,\mathrm{Rev}(D_4)) = 0,\\ \mathrm{res}(D_1,\mathrm{Rev}(D_4)) &= \mathrm{res}(D_3,\mathrm{Rev}(D_2)) = y-z.\end{aligned}$$

Newton 多項式は前章に述べた "Hensel 因子の不定性" には無関係なので、終結式が同じなら (定理 2 が主張するように)Hensel 因子の積が Class-1 になる可能性が高い。そこで、"$\mathcal{N}_1$ 上の D_1 に対応する F の因子" と "$\mathcal{N}_2$ 上の D_4 に対応する F の因子" の積、"$\mathcal{N}_1$ 上の D_2 に対応する F の因子" と "$\mathcal{N}_2$ 上の D_3 に対応する F の因子" の積、が多項式になるかどうかを調べてみるのがよいだろう。

本例の最後に GCD 計算の実際を記述しよう。まず、$F(x,\boldsymbol{u})$ を $\mathcal{N}_1,\mathcal{N}_2$ 上の Hensel 因子 $F_1^{(k)},F_2^{(k)}$ に分解する ($k=5$ まで計算した結果は前章の (4.5) に与えた)。次に、初期因子 D_1 と D_2 で $F_1^{(5)}$ を、初期因子 D_3 と D_4 で $F_2^{(5)}$ を Hensel 構成する：

$$\begin{aligned}D_1^{(3)}&=xy+1+yz^2,\quad D_3^{(2)}=x+y+yz-(yz^3)/(y-z),\\ D_2^{(3)}&=xz+1-yz^2,\quad D_4^{(2)}=x+z-z^2+(yz^3)/(y-z).\end{aligned}$$

積 $D_1^{(3)}\times D_4^{(2)}$, $D_2^{(3)}\times D_3^{(2)}$ を全次数 2 で打ち切る (有理式部分は切り捨てられる)：

$$\begin{aligned}D_2^{(3)}D_3^{(2)} &\equiv (x+y)(zx+1)+yz,\\ D_1^{(3)}D_4^{(2)} &\equiv (x+z)(yx+1)-z^2.\end{aligned}$$

最後に、G を試し割りすることにより $\mathrm{GCD}=D_2^{(3)}D_3^{(2)}$ が得られる。 □

参 考 文 献

[1] K.O. Geddes, S.R. Czapor and G. Labahn: *Algorithms for computer algebra.* Kluwer Academic Publishers, 1992.

[2] J. von zur Gathen and J. Gerhard: *Modern Computer Algebra.* Cambridge Univ. Press, 1999.

[3] J. von zur Gathen and E. Kaltofen: Factoring sparse multivariate polynomials. J. Comp. System Sci. **31**, 265-287 (1985).

[4] S. Gao and A.G.B. Lauder: Hensel lifting and bivariate polynomial factorization over finite fields. Math. Comp. **71**,1663-1676 (2002).

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

[6] E. Kaltofen and B.M. Trager: Computing with polynomials given by black boxes for their evaluations: greatest common divisors, factorization, separation of numerators and denominators. J. Symb. Comput. **9**, 301-320 (1990).

[7] T.-C. Kuo: Generalized Newton-Puiseux theory and Hensel's lemma in $\mathbf{C}[[x, y]]$. *Canad. J. Math.*, **XLI**, 1101-1116 (1989).

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

[9] F.K. Abu Salem, S. Gao and A.G.B. Lauder, Factoring polynomials via polytopes: *Proceedings of ISSAC'04*, ACM, 4-11 (2004).

[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 F. Kako: Solving multivariate algebraic equation by Hensel construction. Preprint of Univ. Tsukuba, March, 1993.

[12] T. Sasaki and F. Kako: Solving multivariate algebraic equation by Hensel construction. *Japan J. Indust. Appl. Math.*, **16**(2), 257-285 (1999). (内容は [11] とほぼ同じである。出版の遅れはレフェリーからの返事が約3年に1度だったことによる)。

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

[14] P.S. Wang: Preserving sparseness in multivariate polynomial factorization. *Proceedings of 1977 MACSYMA Users Conference*, MIT, 55-61 (1977).

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