数理解析研究所講究録
第2019巻 2017年 3-17

疎な多変数多項式の拡張Hensel構成算法の再構築

Reconstruction of Algorithm for the Extened Hensel Construction of Sparse Multivariate Polynomials

佐々木 建昭 (Tateaki Sasaki) *
筑波大学 名誉教授
(UNIVERSITY OF TSUKUBA)

稲葉 大樹 (Daiju Inaba) †
(公財) 日本数学検定協会
(JAPAN ASSOC. MATH. CERTIFICATION)

Abstract

筆者らは昨年12月の数理研研究集会で、拡張Hensel構成をMoses-Yun補間式ではなく初期因子のGröbner基底を使うことで高速化する考えを発表した。その時点では単なるアイデアだったが、2段階で研究が進展し、従変数の個数が少ない場合には十分高速な算法が出来上がった。研究成果は進展に応じて2論文として、国際会議CASC2016とSYNASC2016で発表された。特に後者では、Gröbner基底の簡単かつ新しい定理を基に、"minimal因子"分離に対する分割征服算法が考案され、著しい高速化が達成された。また、"maximal因子"分離に対しては、主変数の次数の低いHensel因子から順に構成する算法とHensel因子の歪みを矯正する算法が考案された。前者は拡張Hensel構成の解析関数への適用を可能にするものである。

1 拡張Hensel構成の旧来算法の概略

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、$\deg(F)$, $\mathrm{lc}(F)$, $\mathrm{ctm}(F)$, $\mathrm{cont}(F)$は主変数xに関する**次数**、**主係数**、**定数項**(x^0-項)、**係因数**(content, xに関する係数の**最大公約子**(GCD))を、それぞれ表す。$T=c\,u_1^{e_1}\cdots u_\ell^{e_\ell}$, $c\in\mathbb{Q}$, に対し、$e_1+\cdots+e_\ell$を$\boldsymbol{u}$に関する**全次数**(total degree)と言い$\mathrm{tdeg}(T)$と表す。$\mathrm{res}(F,G)$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。GがFを割り切るとき$G|F$と表わす。

拡張Hensel構成(extended Hensel construction, EHCと略記)とは、多変数多項式の因数分解やGCD計算で絶大な威力を発揮する**一般Hensel構成**(generalized Hensel construction, GHCと略記)を、GHCが破綻する場合に自然に拡張したものである。その由来等については、昨年12月の数理研研究集会の講究録[7]を参照されたい。

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

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。

定義 1 (Newton 線と Newton 多項式、正味 Newton 多項式; 下記図 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。$F(x,t\boldsymbol{u})$ の各項を $cx^it^ju_1^{j_1}\cdots u_\ell^{j_\ell}$ とする；ここで、$c\in\mathbb{Q}$, $j=j_1+\cdots+j_\ell$ である。この項を (e_x,e_t)-面上の点 (i,j) にプロットする。全てのプロット点を囲む凸包を $\boldsymbol{\mathcal{N}}$ と表す。$\boldsymbol{\mathcal{N}}$ の全底辺を時計周りに $\mathcal{N}_1,\ldots,\mathcal{N}_\rho$ 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** *(net Newton polynomial)* と呼ぶ。 □

GHC では Newton 線は x 軸上に 1 本だけあり、かつ 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が必要である。すなわち、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る必要がある。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ろう。特に、疎な多変数多項式では、項がまばらにプロットされるはずなので、自然に Hensel 構成しようと思えば EHC になるだろう。因みに、GHC が適用できない場合には従変数の原点移動を行って適用可能な多項式に変換するのが常道だが、そうすると項数が爆発的に増大するなどの不都合が生じ、疎な多変数多項式の扱いが世界的な課題になっている。EHC は疎な多変数多項式に対する決定的な算法の一つであると自負している。

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^{n_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 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。下図左は 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。

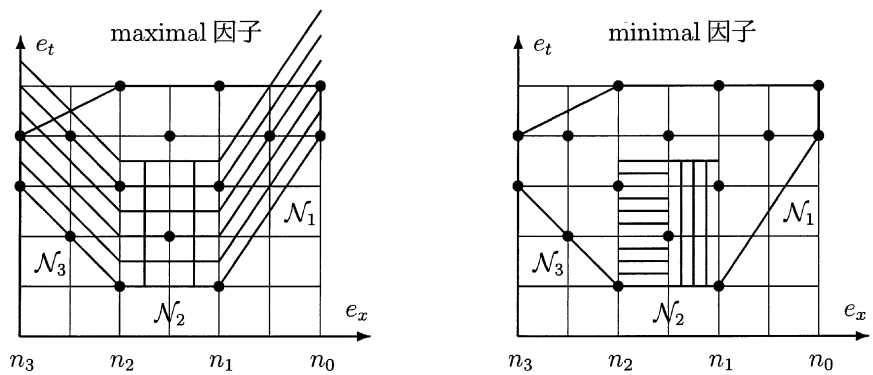


図 1: maximal 因子 と minimal 因子 の概念図

Hensel 構成とは、Hensel によるオリジナルな構成は p^{k+1} (p は素数) を法とする、GHC は $\langle u_1,\ldots,u_\ell\rangle^{k+1}$ を法とする因数分解である。拡張 Hensel 構成の場合は、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。

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 (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 $\mathcal{F}(x, \boldsymbol{u}, w)$, $\mathcal{F}_{\mathcal{N}_i}(x, \boldsymbol{u})$ 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)。

$$\left\{ \begin{array}{rcl} \mathcal{F}(x, \boldsymbol{u}, w) & \stackrel{\text{def}}{=} & w^{\hat{n}_i(\lambda_i n_i - \nu_i)} F(x/w^{\hat{\nu}_i}, w^{\hat{n}_i}\boldsymbol{u}), \\ \mathcal{F}_{\mathcal{N}_i}(x, \boldsymbol{u}) & \stackrel{\text{def}}{=} & w^{\hat{n}_i(\lambda_i n_i - \nu_i)} F_{\mathcal{N}_i}(x/w^{\hat{\nu}_i}, w^{\hat{n}_i}\boldsymbol{u}), \\ \mathcal{I}_k & \stackrel{\text{def}}{=} & \langle w^k \rangle, \quad k = 1, 2, 3, \ldots. \end{array} \right. \tag{1.1}$$

上式中で $\mathcal{F}_{\mathcal{N}_i}(x, \boldsymbol{u})$ が w を含まないのは、$\mathcal{F}_{\mathcal{N}_i}$ の各項が 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 (**Hensel 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;mximal の場合には、第 3 章で詳述するように $F(x, \boldsymbol{u})$ でなく $\mathrm{ctm}(G_0)F(x, \boldsymbol{u})$ を EHC する。

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

2 CASC2016 論文までの研究の復習

CASC'16 論文 [9] に記載された内容の約半分は昨年 12 月の数理研研究集会で話したし、また内容の多くは数理研講究録 [7] に記載した。しかし、Hensel 因子の簡単化については全く記載されていない。簡単化は CASC 論文のみならず SYNASC 論文でも決定的に重要なので、本稿では簡単化を中心に、CASC2016 論文までの研究を簡単に復習する。

CASC'16 論文では minimal な Hensel 因子の分離を扱った。第 l 番目 $(1 \le l \le \rho)$ の Newton 線 $\mathcal{N}_l$ 上の EHC を考える。第 l 番目の正味 Newton 多項式を $F_{\mathcal{N}}(x, \boldsymbol{u})$ とし、その因数分解を次式とする ; ここで、$r \ge 2$ であり、添字 l は簡単のため適宜省く。

$$F_{\mathcal{N}}(x, \boldsymbol{u}) = G_1(x, \boldsymbol{u}) \cdots G_r(x, \boldsymbol{u}), \quad \gcd(G_i, G_j) = 1 \ \ (\forall i \ne j). \tag{2.1}$$

$i = 1, \ldots, r$ に対し、G_i と $H_i = F_{\mathcal{N}}/G_i$ を初期因子として、$\mathcal{N}_l$ 上の maximal 因子 $F(x, \boldsymbol{u})$ を拡張 Hensel 構成すれば、G_i に対応する因子が minimal 因子となる。その際、Moses-Yun

補間式 [4] (MY 補間式と略記) を用いる旧来の方法は $F(x,\boldsymbol{u})$ が x に関して高次の場合には非常に効率が悪い。そこで、筆者らは前章最後の算法の **solve** 行の方程式

$$\left\{\begin{array}{l} \delta F^k(x,\boldsymbol{u}) = \delta H^{(k)}(x,\boldsymbol{u})G_i(x,\boldsymbol{u}) + \delta G^{(k)}(x,\boldsymbol{u})H_i(x,\boldsymbol{u}), \\ \quad \deg(\delta H^{(k)}) < \deg(H_i), \quad \deg(\delta G^{(k)}) < \deg(G_i), \end{array}\right. \tag{2.2}$$

の解 $\delta H^{(k)}, \delta G^{(k)} \in \mathbb{Q}(\boldsymbol{u})[x]$ を、イデアル $\langle G_i, H_i\rangle$ の Gröbner 基底とその各要素に対するシジジーを利用して計算することを提案した。ここで、$\delta G^{(k)}, \delta H^{(k)}$ はそれぞれ $G_i^{(k)}, H_i^{(k)}$ の k 次補正項である。Gröbner 基底に対する項順序 $\succ_1$ は、$x \succ_1 u_1, \ldots, u_\ell$ とする。G_i, H_i は係数が $u_1, \ldots, u_\ell$ に関して斉次多項式なので、$\boldsymbol{u}$ に関する順序は全次数式でも辞書式でもよい。また、補正項は多くの場合 $\boldsymbol{u}$ に関して有理式となるが、その分母は初期因子で決まるので、分母因子の逆元をシステム変数で置き換えることで有理式演算を多項式演算に変換し、高速化することも提案した。

補正項の計算は、$\delta F^{(k)} = \delta P^{(k)} + \delta R^{(k)}$, $\delta P^{(k)} \in \langle G_i, H_i\rangle$, $\delta R^{(k)} \notin \langle G_i, H_i\rangle$ と分離することから始めた。k 次補正項が分母因子を持つか否かは $\delta R^{(k)}$ が非零か否かで決まるので、この分離は当然であると思ったのである。$\langle G_i, H_i\rangle$ の Gröbner 基底を $\Gamma = \{\widehat{G}_1, \cdots, \widehat{G}_s\}$, $\widehat{G}_1 \succ \cdots \succ \widehat{G}_s$, とし、各要素 $\widehat{G}_j$ に対するシジジーを (a_j, b_j) とする：$\widehat{G}_j = a_j G_i + b_j G_i$ (シジジーの本来の定義は左辺が 0 なので、本稿では常に “要素 xx に対する” をつける)。$\delta F^{(k)}$ の上記分離は $\delta F^{(k)}$ を Γ で簡約することで実行でき (簡約できなかった部分が $\delta R^{(k)}$)、同時に $\delta P^{(k)} = p_1\widehat{G}_1 + \cdots + p_s\widehat{G}_s$ を満たす $p_1, \ldots, p_s \in \mathbb{Q}[x, \boldsymbol{u}]$ も計算できる。式右辺の各 $\widehat{G}_j$ を $a_j G_i + b_j G_i$ で置き換えれば、$\delta P^{(k)} = \delta C\, G_i + \delta D\, H_i$ を満たす $\delta C, \delta D \in \mathbb{Q}[x, \boldsymbol{u}]$ が得られる。あとは次数条件を満たすように次数を低減すれば、$\delta G^{(k)}, \delta H^{(k)}$ の多項式部分が計算できる。次数低減法については数理研講究録 [7] を参照されたい。

次に $\delta R^{(k)}$ だが、$\delta R^{(k)}$ は補正項の有理式部分を与えるので、分母因子を如何に定めるかが最大の課題である。$\delta R^{(k)}$ だけでは手がつかないが、$\gcd(G_i, H_i) = 1$ ゆえ $\widehat{G}_1 \in \mathbb{Q}[\boldsymbol{u}]$ なので、$\delta R^{(k)}\widehat{G}_1$ を扱うことにした。この多項式は $\langle G_i, H_i\rangle$ の要素なので、$\delta R^{(k)}\widehat{G}_1 = \delta S' G_i + \delta T' H_i$ を満たす $\delta S', \delta T' \in \mathbb{Q}[x, \boldsymbol{u}]$ が $\widehat{G}_1$ に対するシジジーより計算できる。したがって、$\delta S', \delta T'$ の x に関する次数が低減できさえすれば、$\delta R^{(k)} = \delta S\, G_i + \delta T H_i$ を満たす $\delta S, \delta T \in \mathbb{Q}(\boldsymbol{u})[x]$ を $\delta S = \delta S'/\widehat{G}_1$, $\delta T = \delta T'/\widehat{G}_1$ と計算できる。

実は、CASC 論文を書きつつ、$\langle G_i, H_i\rangle$ の Gröbner 基底 Γ に対し、$\Gamma \cap \mathbb{Q}[\boldsymbol{u}]$ が何個の要素を含むか、ずーっと気になっていた。もしも複数の要素を含み得るなら、分母因子を決める多項式として $\widehat{G}_1$ を選ぶ必然性はなく、別の要素を選択する場合も考察しなければならない。上記 $\delta S', \delta T'$ の次数低減も $\delta C, \delta D$ と同様に行えるとは限らず、CASC 論文では “強制次数低減法” を導入せざるを得なかった。この問題は SYNASC 論文でやっと解決された：Γ が簡約基底ならば Γ は $\mathbb{Q}[\boldsymbol{u}]$ の要素を 1 個しか含まないのである。

上述のように計算された minimal な Hensel 因子の簡単化を実例を用いて考察する。

例 1：Hensel 因子の簡単化の実例

$$\begin{aligned} F = \; & (y^2z)\,x^4 + (y^3z^2+yz^2+yz)\,x^3 + (y^4z+y^2z^3+2y^2z^2+y-z)\,x^2 \\ & + (y^3z^2+y^3z+y^2z+yz^3)\,x + (y^3-y^2z+yz-z^2) + 3xyz. \end{aligned}$$

F の Newton 多項式は $\overline{F_{\mathcal{N}}} = x^2 \times (x^2y^2z+xyz+y-z)$ なので、初期因子を $H_0 = x^2$, $G_0 = x^2y^2z+xyz+y-z$ とする。イデアル $\langle G_0, H_0\rangle$ の Gröbner 基底は

$$\{\underline{y^2-2yz+z^2},\ xz^2+y-z,\ xy-xz,\ x^2\}$$

なので、$y^2-2yz+z^2$ が分母因子となる。以下では、$\%D[1] = 1/(y^2-2yz+z^2)$ とする。2 次の補正項 $\delta G^{(2)}, \delta H^{(2)}$ と 3 次の残余項 $\delta F^{(3)}$ は下記となる ($\%W$ は重み変数)。

$$\begin{aligned}
\delta G^{(2)} &= \%W^2\,\%D[1]\,(3xy^4z^2 - 3xy^3z^3 \underline{- 3y^4z + 9y^3z^2 - 6y^2z^3}) \\
&\qquad + \%W^2\,\underline{(-3y^2z)} \qquad (\Leftarrow \Uparrow \text{ can be canceled out}) \\
\delta H^{(2)} &= \%W^2\,\%D[1]\,(-3xy^2z + 3xyz^2 \underline{+ 3y^2 - 6yz + 3z^2}) \\
&\qquad + \%W^2\,\underline{(3)} \qquad (\Leftarrow \Uparrow \text{ can be canceled out}) \\
\delta F^{(3)} &= \%W^3\text{-terms} + \%W^2\,\%D[1]\,\underline{(-3y^3 + 9y^2z - 9yz^2 + 3z^3)} \\
&\qquad + \%W^2\,\underline{(-3y + 3z)} \qquad (\Leftarrow \Uparrow \text{ can be canceled out})
\end{aligned}$$

$\delta G^{(2)}, \delta H^{(2)}, \delta F^{(3)}$ いずれにおいても、下線部が完全にキャンセルし、キャンセル後の数式が著しく簡単になる。 □

著者らは、上記の簡単化を実現すべく種々のアイデアを試した：数式処理では、例えば公式 $\sin^2(x)+\cos^2(x) = 1$ による三角関数の簡単化等、この種の簡単化は頻繁に出現し、著者らには多くの経験があった。そのため、複雑なプログラムも書いて試した。しかし、それらのいずれもが満足できる代物ではなかった。最終的に残った簡単化は次である。

拡張 Hensel 因子の簡単化：多項式も有理式も含め、全てを単一分母にまとめる。

実際、CASC 論文に載せた高次の計算例はそうなっている。

3 maximal な Hensel 因子に対する EHC 算法の改善

本章から SYNASC2016 で発表した研究になる。SYNASC'16 論文 [10] は研究途上と判定され、掲載が半分の 4 頁に制限されたので大幅に縮めて記載した。そこで本稿では SYNASC 論文に書き切れなかった部分を存分に書くことにする。

maximal な Hensel 因子は、Newton 線 $\mathcal{N}_i$ 上で Newton 多項式 $\overline{F_{\mathcal{N}_i}}(x, \boldsymbol{u})$ の互いに素な因子 x^{n_i} と $F_{\mathcal{N}_i}(x, \boldsymbol{u})$ を初期因子として $F(x, \boldsymbol{u})$ を EHC して構成するが、x^{n_i} に対応する Hensel 因子の Newton 多項式が $F_{\mathcal{N}_{i-1}}$ になる (後で証明する) ように、$H_0 := g_0(\boldsymbol{u})x^{n_i}$ と $G_0 := F_{\mathcal{N}_i}(x, \boldsymbol{u})$ を初期因子として $g_0(\boldsymbol{u})F(x, \boldsymbol{u})$ を EHC する；ここで、g_0 は G_0 の定数項である：$g_0 = \mathrm{ctm}(G_0)$。以下、本章では $n_i = m$、$G_0 = g_{n'}x^{n'} + \cdots + g_1x + g_0$ とおく。もちろん $g_0 \neq 0$ である。また、簡単のため添字 i を省略する。

minimal な因子の EHC では Gröbner 基底により計算の高速化を目指すが、maximal な因子の EHC では旧来の MY 補間式をそのまま利用する。初期因子の一方が g_0x^m の場合、下記の公式により MY 補間式が簡単に計算でき、後述するように公式は x に関して疎な

$F(x,\boldsymbol{u})$にも有用な形だからである。因みに、初期因子 $G_0(x,\boldsymbol{u})$ と $H_0=g_0x^m$ に対するMY補間式とは次式を満たす $A_l,B_l\in\mathbb{Q}[\boldsymbol{u}][x]$ のことである。

$$A_l(x,\boldsymbol{u})G_0(x,\boldsymbol{u})+B_l(x,\boldsymbol{u})(g_0x^m)=x^l,\quad l=0,1,\ldots,n. \tag{3.1}$$

A_l と B_l は、次数条件 $\deg(A_l)<m$, $\deg(B_l)\le n$ を課すとき一意的に定まり、次の公式で与えられることが文献 [5] に示されている。

$$\text{For } l\ge m:\ \begin{cases} A_l=0,\\ B_l=x^{l-m}/g_0. \end{cases} \tag{3.2}$$

$$\text{For } l<m:\ \begin{cases} A_l=G_{\mathrm{Inv}\langle x^{m-l}\rangle}x^l,\\ B_l=[1-G_{\mathrm{Inv}\langle x^{m-l}\rangle}G_0]/(g_0x^{m-l}). \end{cases} \tag{3.3}$$

上記で、$G_{\mathrm{Inv}\langle x^j\rangle}$ とは、x^j を法とする G_0 の逆元である：$G_{\mathrm{Inv}\langle x^j\rangle}G_0\ \equiv\ 1\ (\mathrm{mod}\ x^j)\ \Rightarrow \deg(G_{\mathrm{Inv}\langle x^j\rangle})<j$。$G_{\mathrm{Inv}\langle x^j\rangle}$ が示すように、$l<m$ に対する A_l,B_l は、$G_{\mathrm{Inv}\langle x^1\rangle}=1/g_0\ \Rightarrow G_{\mathrm{Inv}\langle x^2\rangle}\ \Rightarrow\cdots\Rightarrow G_{\mathrm{Inv}\langle x^m\rangle}$ と計算し、$(A_{m-1},B_{m-1})\ \Rightarrow\ (A_{m-1},B_{m-1})\ \Rightarrow\cdots\Rightarrow\ (A_0,B_0)$ と計算するとよい。このとき、$G_{\mathrm{Inv}\langle x^j\rangle}$ は G_0 を定数項から順に高次に辿って計算されるが、新たな非零項に出会うまでは $G_{\mathrm{Inv}\langle x^j\rangle}$ は不変であり、その間、A_{m-j}/x^{m-j} と x^jB_{m-j} も不変なので、これらは $F(x,\boldsymbol{u})$ の疎性を利用して効率的に計算できる。

MY補間式を用いるEHCは次のように簡単明快である。$\delta F^{(k)}=\delta f_n(\boldsymbol{u})x^n+\delta f_{n-1}(\boldsymbol{u})x^{n-1}+\cdots+\delta f_0(\boldsymbol{u})$ とすれば、$\delta G^{(k)},\delta H^{(k)}$ は次式で定まる。

$$\delta G^{(k)}(x,\boldsymbol{u})=\sum_{l=0}^{n}\delta f_l(\boldsymbol{u})\,B_l(x,\boldsymbol{u}),\quad \delta H^{(k)}(x,\boldsymbol{u})=\sum_{l=0}^{m-1}\delta f_l(\boldsymbol{u})\,A_l(x,\boldsymbol{u}). \tag{3.4}$$

命題1 k が十分大きいとき、$\mathrm{NewtonPolynom}(H^{(k)})=F_{\mathcal{N}_{i-1}}$ である。

証明 公式 (3.3) によると、$l<m$ のとき A_l は次のように表せる。

$$A_l(x,\boldsymbol{u})=a_{m-1}(\boldsymbol{u})x^{m-1}+\cdots+a_l(\boldsymbol{u})x^l,\quad a_l(\boldsymbol{u})=1/g_0. \tag{3.5}$$

$F_{\mathcal{N}_{i-1}}=g'_mx^m+g'_{m-1}x^{m-1}+\cdots$ とおけば、$g'_m=g_0$ である。$k=0$ では $H^{(0)}=H_0=g_0x^m$ ゆえ、命題は正しい。$\widetilde{F}=g_0F$ の $\mathcal{N}_{i-1}$ 上のNewton多項式は $g_0g'_mx^m+g_0g'_{m-1}x^{m-1}+\cdots+g_0g'_{n_{i-1}}x^{n_{i-1}}$ である。$\widetilde{F}=g_0F$ のEHCでは、リフティングを進める毎に、項 $g_0g'_{m-1}x^{m-1},\ldots,g_0g'_{n_{i-1}}x^{n_{i-1}}$ が順に現れ、(3.4) の $\delta H^{(k)}$ に対する算式により、それぞれ $A_{m-1},\ldots,A_{n_{i-1}}$ の x^{m-1}-,$\ldots$, $x^{n_{i-1}}$-項により処理される。公式 (3.5) によれば、これらの項は最低次の非零項で、係数が $1/g_0$ ゆえ g_0 がキャンセルされ、命題が証明される。 □

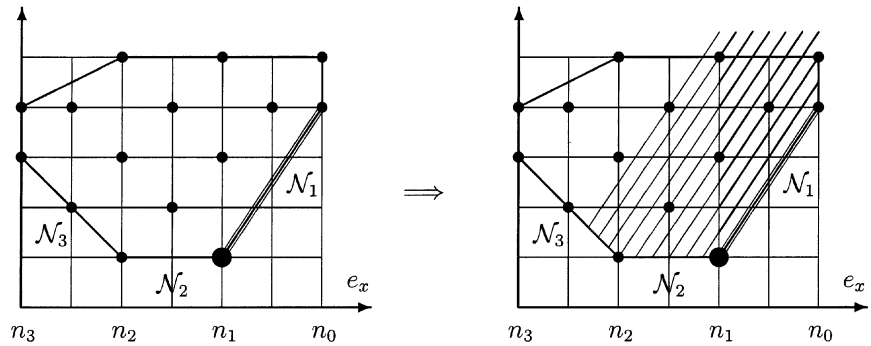
maximalな因子に対するEHCの改善策は次の三つである。

- **maxH-A** 従来のmaximalな因子分離は、$\overline{F}_{\mathcal{N}_1}$ を使い $\mathcal{N}_1$ 上の因子を分離 $\Rightarrow\overline{F}_{\mathcal{N}_2}$ を使い $\mathcal{N}_2$ 上の因子を分離 $\Rightarrow\cdots$ と行っていたが、改善算法では $\overline{F}_{\mathcal{N}_{\rho-1}}$ を使い $\mathcal{N}_\rho$ 上の因子を分離 $\Rightarrow\overline{F}_{\mathcal{N}_{\rho-2}}$ を使い $\mathcal{N}_{\rho-1}$ 上の因子を分離 $\Rightarrow\cdots$、と行う。

- **maxH-B** $\mathcal{N}_i$ 上での正味 Newton 多項式 $F_{\mathcal{N}_i}$ が非数値の係因数 c を持つ場合には、$F_{\mathcal{N}_i}$ の代りに $F_{\mathcal{N}_i}/c$ を使って EHC を行う。これによって、maximal な因子の分母は大部分が g_0/c のべき乗になる。
- **maxH-C** maximal な因子分離は公式 (3.2) の A_l, B_l を用いて行うため、A_l で計算される $H^{(k)}$ の最高次項は k によらず g_0x^m であり、$F(x, \boldsymbol{u})$ の x^m-項はすべて $G^{(k)}$ に組み込まれる。即ち、maximal な Hensel 因子は "歪んでいる (lopsided)"。歪みを矯正する簡単な方法を提案する。

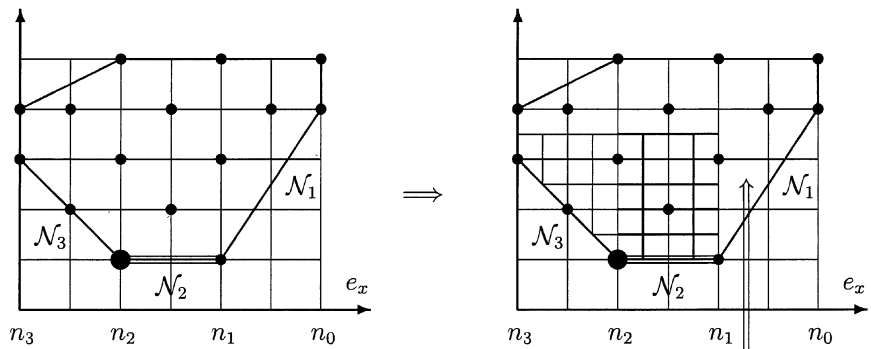
改善策 maxH-A について

旧来の方法の最初の EHC ($\mathcal{N}_1$ 上での maximal 因子分離) を図解したのが図 2.1 である。



Initial factors: x^{n_1}, $F_{\mathcal{N}_1}$ 図 2.1 Need EHC on **wide area**

新算法で最初の EHC($\mathcal{N}_{\rho-1}$ 上での maximal 因子分離) を図解したのが図 2.2 である。



Initial factors: x^{n_2}, $F_{\mathcal{N}_2}$ 図 2.2 white zone: Unchanged

図 2.1 と図 2.2 を比較すると、旧算法では広い領域をカバーするように Hensel 構成を実行しなければならないが、新算法では実質、隣り同士の二つの Newton 線上でだけ構成すればよい：下記に示すように右側の全ての Newton 線上では与式は不変だし、$\mathcal{N}_{\rho-1}$ 上での EHC が終了すれば $\mathcal{N}_\rho$ 上の maximal 因子は分離できることに注意。新算法は計算量

を (桁違いではないが) かなり減らすが、そのこと以上に重要な意味をもつことを第5章で指摘する。

maximal因子の分離に対する新算法を定式化しておく。$\delta F^{k)} = \delta f_n(\boldsymbol{u})x^n + \delta f_{n-1}(\boldsymbol{u})x^{n-1} + \cdots + \delta f_0 x^0$ とする。まず、$\delta F^{k)}$ を次式のように分離する。

$$\delta F^{(k)} = \delta F^{(k)}_{(<m)} + \delta F^{(k)}_{(\geq m)}, \quad \delta F^{(k)}_{(<m)} = \sum_{l=0}^{m-1} \delta f_l(\boldsymbol{u})\, x^l, \quad \delta F^{(k)}_{(\geq m)} = \sum_{l=m}^{n} \delta f_l(\boldsymbol{u})\, x^l. \tag{3.6}$$

MY補間式によるEHC算式 (3.4) によると、$\delta F^{(k)}_{(<m)}$ は (3.3) により $\delta G^{(k)}$ と $\delta H^{(k)}$ に寄与するが、$\delta F^{(k)}_{(\geq m)}$ の方は (3.2) により $\delta F^{(k)}_{(\geq m)}/x^m$ がそのまま $\delta G^{k)}$ に加えられる；(3.2),(3.3) の B_l に対する公式の分母因子 g_0 は $F(x,\boldsymbol{u})$ に掛けられた g_0 とキャンセルする。

命題2 新算法で $\mathcal{N}_{\rho-1}$ 上のmaximal因子分離をしても、$\mathcal{N}_{\rho-2}, \ldots, \mathcal{N}_1$ 上で与式 $F(x,\boldsymbol{u})$ は不変である。

証明 $\deg(G_{\mathrm{Inv}\langle x^{s^j}\rangle}) \leq j-1$ ゆえ、公式 (3.3) より $\deg(B_l) < \deg(G_0)$ である。よって、$\delta F^{(k)}_{(<m)}$ の $\delta G^{(k)}$ への寄与は x の次数が n' 未満に限られる。これを $F(x,\boldsymbol{u})$ 全体でみれば、次数が $m+n'$ 未満の項のみが変化する。 □

改善策 maxH-B について

まず、Newton多項式 $F_{\mathcal{N}}$ が非数値の係因数を持つことは、与式 $F(x,\boldsymbol{u})$ が因数分解可能な場合にはよくある事を指摘しておく。

MY補間式を定める式は $A_l F_{\mathcal{N}} + B_l(g_0 x^m) = x^l$ であるが、$\mathrm{cont}(F_{\mathcal{N}}) = c \neq 1$ ならば、$A'_l\,(F_{\mathcal{N}}/c) + B'_l\,(g_0 x^m) = x^l$ を満たすMY補間式 A'_l, B'_l を用いて、$(g_0/c)F$ をEHCすることを考える。$(g_0/c)F$ のNewton多項式は $(g_0 x^m/c)\times F_{\mathcal{N}} = (g_0 x^m)\times(F_{\mathcal{N}}/c)$ ゆえ、初期因子を $G_0 = F_{\mathcal{N}}/c,\ H_0 = g_0 x^m$ と選べる。公式 (3.3) と同様、$l < m$ に対する A'_l は G_0 の逆元として計算でき、(3.5) と同様、A'_l の非零最低次項は $(g_0/c)\,x^l$ である。したがって、この場合にも命題1が成立する。B'_l の方は、公式 (3.2),(3.3) と同様、分母に g_0 が現れる。$(g_0/c)F/g_0 = F/c$ ゆえ、c はキャンセルせずに分母に残る。

新算法では、A'_l, B'_l が A_l, B_l よりも幾分簡単になるので、高次までリフティングする際には計算量の大きな節約になるだろう。しかし、重要な意味を持つ分母因子が小さくなるのはそれ以上の価値を持つと言える。

改善策 maxH-C について

maximal因子は命題1と2のように巧みに構成できるし、将来、多くの局面で利用されることになると思われるので、因子の歪みはなんとしても矯正したい。

前記と同様、$\delta G^{(k)}, \delta H^{(k)}$ は k 次残余項 $\delta F^{(k)}$ による $G^{(k)}, H^{(k)}$ の k 次補正項とし、矯正後の k 次補正項をそれぞれ $\delta G^{(k)}_{\mathrm{cor}}, \delta H^{(k)}_{\mathrm{cor}}$ とする。補正項対はどちらも G_0 と $g_0 x^m$ を初期因子として $\delta F^{(k)}$ を補間するものであるから、次式を満たす。

$$(\delta H^{(k)}_{\mathrm{cor}} - \delta H^{(k)})\, G_0 + (\delta G^{(k)}_{\mathrm{cor}} - \delta G^{(k)})\, g_0 x^m = 0. \tag{3.7}$$

ここで、$\delta H^{(k)}_{\mathrm{cor}} \neq \delta H^{(k)}$ ならば $\deg(\delta H^{(k)}_{\mathrm{cor}}) = m > \deg(\delta H^{(k)})$ である。

次数条件 $\deg(\delta H^{(k)}_{\rm cor}) = m$ を満たす (3.7) の解は次の命題のように無数にある。

命題 3 次数条件 $\deg(\delta H^{(k)}_{\rm cor}) = m$ を満たす (3.7) の一般解は次式で与えられる。

$$(\delta G^{(k)}_{\rm cor}, \delta H^{(k)}_{\rm cor}) = (\delta G^{(k)}, \delta H^{(k)}) + c\times(-G_0,\ g_0 x^m), \quad c \in \mathbb{Q}[\boldsymbol{u}] \text{ は任意.} \tag{3.8}$$

証明 $\delta H^{(k)}_{\rm cor}$ を m 次と m 次未満の部分に分けて考えれば明白である。 □

歪みの矯正法は一意的ではなく、maximal 因子に要求される性質に依存する。実際上は、その性質を満たすように (3.8) の c を決めることになる。

本稿では、$\delta G^{(k)}_{\rm cor}$ が最も簡単になる (項数が少なくなる) ように、具体的に決めてみよう。(3.8) によれば、$\delta G^{(k)}_{\rm cor} = \delta G^{(k)} - cG_0$ なので、$\delta G^{(k)} - cG_0$ の項数が最も少なくなるように c を決め、つぎに $\delta H^{(k)}_{\rm cor} = \delta H^{(k)} + c\, g_0 x^m$ とすればよい。

例 2 : $H^{(k)}$ の歪み (lopsidedness) 矯正 $G = x^2(y+z) + xy + z,\ H = x^2 z + y^2 - z^2$ とし、$F = (G + xyz)\times(H + x^2 yz)$ を考える；敢えて因数分解可能な例を使うのは読者が計算を理解し易いからである。F は二つの Newton 多項式を持ち、その右側のものは $\overline{F}_{\mathcal{N}_1} = x^2 z \times G$ である。$g_0 = z$ なので、初期因子を $G_0 := G,\ H_0 := x^2 z^2$ として $g_0 F = zF$ を 2 次まで Hensel 構成すると次式が得られる。実は計算は 1 次までででよいのだが、矯正をしないと高次まで EHC が進むことを示すために 2 次まで計算した (W は重み変数)。

$$\begin{aligned}
\delta F^{(1)}_{(<m)} &= x(y^3 z - yz^3) + (y^2 z^2 - z^4), \quad \delta F^{(1)}_{(\geq m)}/x^2 = x^2(y^2 z^2 + yz^3) + \cdots, \\
\delta F^{(2)}_{(<m)} &= x(-y^4 z + y^2 z^3) + (-y^3 z^2 + yz^4), \\
\mathcal{G}^{(2)} &= W^2(xy^2 z) + W\left(x^2(y^2+yz) + x(y^2+yz) + yz\right) + \left(x^2(y+z) + xy + z\right), \\
\mathcal{H}^{(2)} &= W^2(-y^3 z + yz^3) + W\left(y^2 z - z^3\right) + x^2 z^2.
\end{aligned}$$

実際の構成では y, z に関する有理式が多く現れるが、第 2 章に述べた簡単化により上記のように簡潔になった。$\mathcal{G}^{(2)}$ を見ると W の 1 次項の係数が $y\,G_0 + xyz$ なので、上記手順に従い $y\,G_0$ を $\mathcal{G}^{(1)}$ から引き、$yg_0 x^2$ を $\mathcal{H}^{(1)}$ に加えると歪みの矯正ができる。

$$\begin{aligned}
\mathcal{G}^{(1)} &\Rightarrow \mathcal{G}^{(1)}_{\rm cor} = W(xyz) + \left(x^2(y+z) + xy + z\right), \\
\mathcal{H}^{(1)} &\Rightarrow \mathcal{H}^{(1)}_{\rm cor} = W\left(x^2 yz + (y^2 z - z^3)\right) + x^2 z^2.
\end{aligned}$$

$W^2 zF \equiv \mathcal{G}^{(2)}\mathcal{H}^{(2)} \pmod{W^3}$ だが、$\mathcal{G}^{(1)}_{\rm cor}, \mathcal{H}^{(1)}_{\rm cor}$ は $W^2 zF = \mathcal{G}^{(1)}_{\rm cor}\mathcal{H}^{(1)}_{\rm cor}$ を満たす。 □

4 minimal な Hensel 因子に対する算法の更なる改善

CASC 論文で旧来の算法を桁違いに高速にしたとは言え、Gröbner 基底を従来の算法のまま使っている限り、"大きな問題では計算量が非常に大きくなって使い物にならない" と言う批判が起きるに違いない。そこで、さらなる高速化に取り組んだ。

CASC 論文の最終段階で、Hensel 因子の簡単化と格闘しているとき、残余項を $\delta F^{(k)} = \delta P^{(k)} + \delta R^{(k)}$ と分離する必然性が無いことに気付くとともに、イデアル $\langle G_i, H_i\rangle$ の順序

$\succ_1$ での簡約 Gröbner 基底が $\mathbb{Q}[\boldsymbol{u}]$ 内に二つ以上要素を持つ例をなかなか作れないことに気付いた。そこで、この簡約 Gröbner 基底は $\mathbb{Q}[\boldsymbol{u}]$ 内に要素を一つしか持たないのだろうと推測し、その方向で研究を進めることにした。

本章では第2章と同様、第 l 番 Newton 線 $\mathcal{N}$ 上で、第 l 番 maximal 因子 (それを $F(x,\boldsymbol{u})$ とする) の minimal 因子への分離を扱うが、分離に必要な (Gröbner 基底に関係する) 数式の計算のみを扱う；Hensel リフティングは CASC 論文とほぼ同じ である。$F(x,\boldsymbol{u})$ の正味 Newton 多項式を $F_{\mathcal{N}}$ とし、$F_{\mathcal{N}}$ は次のように因数分解されるとする；$r \geq 2$ とする。

$$F_{\mathcal{N}} = G_1 \cdots G_r, \quad H_i = F_{\mathcal{N}}/G_i \ \ (\forall i), \quad \gcd(G_i, G_j) = 1 \ \ (\forall i \neq j). \tag{4.1}$$

4.1 $\langle G_i, G_j \rangle$ の Gröbner 基底に関する理論的解析

本章では項順序 $\succ_1$ を $x \succ_1 u_1, \ldots, u_\ell$ と定める。イデアル $\langle G_i, G_j \rangle$ の順序 $\succ_1$ に関する簡約 Gröbner 基底を $\Gamma_{i,j}$、$\mathcal{I}_{\boldsymbol{u}} = \langle G_i, G_j \rangle \cap \mathbb{Q}[\boldsymbol{u}]$、$\Gamma_{\boldsymbol{u}} = \Gamma_{i,j} \cap \mathbb{Q}[\boldsymbol{u}]$ とする。$\mathcal{I}_{\boldsymbol{u}}$ は (x が消去された) 消去イデアル、$\Gamma_{\boldsymbol{u}}$ は $\mathcal{I}_{\boldsymbol{u}}$ のグレブナー基底であり、$\Gamma_{\boldsymbol{u}} = \{\widehat{G}_1, \ldots, \widehat{G}_l, \ldots\}$, $\widehat{G}_1 \prec_1 \cdots \prec_1 \widehat{G}_l \prec_1 \cdots$ とする。また、$R(\boldsymbol{u}) = \mathrm{res}(G_i, G_j) \in \mathbb{Q}[\boldsymbol{u}]$ とする。$\gcd(G_i, G_j) = 1$ ゆえ $R \neq 0$ だが、さらに R は非数値多項式であると仮定する ($R \in \mathbb{C}$ の場合は扱う意味がない)。なお、以下では次の定理 A、B を使う。**定理** A ([2] を参照)：“$R(\boldsymbol{c}) = 0$ for some $\boldsymbol{c} \in \mathbb{C}^\ell \iff$ i) $\mathrm{lc}[G_i](\boldsymbol{c})\,\mathrm{lc}[G_j](\boldsymbol{c}) = 0$ or ii) $\{G_i(x,\boldsymbol{c}) = 0,\ G_j(x,\boldsymbol{c}) = 0\}$ has solution(s) w.r.t. x.” **定理 B** (イデアルと代数多様体に関する基本定理)：“連立方程式 $\{G_i = 0,\ G_j = 0\}$ の任意の解 (イデアルの零点) は $\langle G_i, G_j \rangle$ の全要素の共通零点である”。

注釈 1 $(x, \boldsymbol{c})$ が連立方程式の解のとき、$\boldsymbol{c}$ を $\boldsymbol{u}$ に関する部分解という。定理 A は連立方程式の解と部分解との関係を端的に表わす。定理 A 自体は一つの部分解に関するものだが、任意の部分解に対するものなので、部分解のみを零点とする多項式因子に対しても成立する。下記定理では解の多重度が重要だが、Gröbner 基底算法はイデアルを変えないので、$\widehat{G}_l$ の各零点は部分解の多重度を正しく反映している。なお、G_i と G_j が x に関して疎な場合には、終結式 R は一般に多重度の高い因子を持つ。 □

定理 1 簡約 Gröbner 基底 $\Gamma_{i,j}$ は $\Gamma_{i,j} \cap \mathbb{Q}[\boldsymbol{u}] = \{\widehat{G}_1(\boldsymbol{u})\}$ を満たす。

証明 $\widetilde{R}(\boldsymbol{u})$ は、上記連立方程式の $\boldsymbol{u}$ に関する (多重度を正しく保持した) 部分解の全体だけを零点とする多項式とする。$\widetilde{R}$ の存在と一意性は定理 A が保証する。$\widetilde{R} \in \mathcal{I}_{\boldsymbol{u}}$ ゆえ $\widetilde{R} \in \langle G_i, G_j \rangle$ なので、零点の個数に関する最小性より $\widetilde{R}$ は $\widehat{G}_1$ の定数倍である。さらに、定理 B より $\widetilde{R} \,|\, \widehat{G}_l$ $(\forall l)$ も成立する。一方、$\Gamma_{\boldsymbol{u}}$ は簡約基底ゆえ、$\widehat{G}_{l \geq 2}$ は $\widehat{G}_1$ で簡約され、$\Gamma_{\boldsymbol{u}} = \{\widehat{G}_1\}$ となる。 □

定理 2 $\widehat{G}_{i,j}, \widehat{G}_{i,k}, \widehat{G}_{i,jk}$ $(i \neq j,k)$ をイデアル $\langle G_i, G_j \rangle$, $\langle G_i, G_k \rangle$, $\langle G_i, G_j G_k \rangle$ の順序 $\succ_1$ に関する簡約 Gröbner 基底の最低順位の要素とすれば、$\widehat{G}_{i,jk}(\boldsymbol{u}) = \widehat{G}_{i,j}(\boldsymbol{u})\widehat{G}_{i,k}(\boldsymbol{u})$ である。(本定理と下記証明は $\gcd(G_j, G_k) \neq 1$ の場合でも成立する)。

証明 $G_j G_k$ 中の G_j の x を G_i で消去すれば $\widehat{G}_{i,j} G_k$ を得る。つぎに、$\widehat{G}_{i,j} G_k$ 中の G_k の x を G_i で消去すれば $\widehat{G}_{i,j}\widehat{G}_{i,k}$ を得る。即ち、$\widehat{G}_{i,j}\widehat{G}_{i,k} \in \langle G_i, G_j G_k \rangle$ である。部分解に関し

ては定理1より $\mathrm{zeros}(\widehat{G}_{i,jk}) = \mathrm{zeros}(\widehat{G}_{i,j}) \cup \mathrm{zeros}(\widehat{G}_{i,k})$ が成立する。一方、Gröbner 基底は零点の多重度を変えないから、上式より $\widehat{G}_{i,jk} = \widehat{G}_{i,j}\widehat{G}_{i,k}$ を得る。 □

さて、上記の Gröbner 基底 $\Gamma_{i,j}$ を計算するとき、最低順位要素 $\widehat{G}_{i,j}$ が計算される前に、主変数 x が消去された多項式 $\widehat{G}'_{i,j}$ が計算されることが多々ある。

定理3 $\widehat{G}'_{i,j}$ が上記の多項式であるとき、$\widehat{G}_{i,j}(\boldsymbol{u}) \mid \widehat{G}'_{i,j}(\boldsymbol{u})$ が成立する。

証明 $\Gamma_{i,j} = \{\widehat{G}_{i,j}(\boldsymbol{u})\}$ と $\widehat{G}'_{i,j}(\boldsymbol{u}) \in \mathcal{I}_{\boldsymbol{u}}$ から明白。 □

例3 下記 F_1, F_2, F_3 に対する順序 $\succ_1$ での三つの Gröbner 基底と最低順位要素。

$$\left\{ \begin{array}{l} F_1 = x^2\,(u+v) + x\,(u-v) + 2u + 3v, \\ F_2 = x^2u + 2xv + v, \quad F_3 = x^2v - 2xu + u. \end{array} \right\}$$

Gröbner 基底は下記となる:下線を付した要素のみが $\mathbb{Q}[u,v]$ に属する。

$$\begin{array}{ll} \text{Gröbner 基底}\,(F_1, F_2) & = \{\underline{G_{13}}, G_{10}, G_4, G_{12}, G_3, F_2\}, \\ \text{Gröbner 基底}\,(F_1, F_3) & = \{\underline{G_{12}}, G_9, G_3, G_{11}, F_3, F_1\}, \\ \text{Gröbner 基底}\,(F_1, F_2F_3) & = \{\underline{G_{21}}, G_{23}, G_{17}, G_{22}, G_{19}, \cdots\}. \end{array}$$

$$\begin{array}{l} \underline{G_{13}} = u^4 + 5/4u^3v + 1/2u^2v^2 + 23/4uv^3 + 15/4v^4, \\ \underline{G_{12}} = u^4 + 23/11u^3v + 5/11u^2v^2 + 1/11uv^3 + 9/11v^4, \\ \underline{G_{21}} = u^8 + 147/44u^7v + 157/44u^6v^2 + 82/11u^5v^3 + \cdots. \end{array}$$

上記の $\underline{G_{13}}, \underline{G_{12}}, \underline{G_{21}}$ は $\underline{G_{21}} = \underline{G_{13}G_{12}}$ を満たす。 □

例4 定理3に対する例：定理3と同じ F_1, F_2, F_3 を用いる。
Gröbner 基底 (F_1, F_2F_3) の計算中に次の多項式が生成された。

$$\underline{G_{15}} = u^9 + 191/44u^8v + 76/11u^7v^2 + 485/44u^6v^3 + \cdots.$$

$\underline{G_{15}}$ と $\underline{G_{21}}$ は $\underline{G_{15}} = (u+v)\,\underline{G_{21}}$ を満たす。 □

4.2 minimal な Hensel 因子に対する三つの改善策

minimal 因子の分離では、通常、各 $i \in \{1, \ldots, r\}$ に対し G_i と $H_i = F/G_i$ を初期因子として F を EHC する。したがってイデアル $\langle G_1, H_1\rangle, \ldots, \langle G_r, H_r\rangle$ を扱うことになる。以下では、$\langle G_i, H_i\rangle$ の順序 $\succ_1$ に関する Gröbner 基底を $\Gamma_{i,*/i}$、この基底の最低順位項を $\widehat{G}_{i,*/i}$、この要素に対するシジジーを $(a_{i,*/i},\ b_{i,*/i})$ と表わす：$\widehat{G}_{i,*/i} = a_{i,*/i}G_i + b_{i,*/i}H_i$。
minimal 因子の分離に対しては、筆者らはさらに次の三つの改善策を提案する。

- **minH-a** $\delta F^{(k)} = \delta P(k) + \delta R^{(k)}$ における $\delta P^{(k)}$ を 0 であるとみなす。そうすれば、Gröbner 基底全体を計算する必要はなく、最小順序要素 $\widehat{G}_{1,*/i}, \cdots, \widehat{G}_{r,*/i}$ とこれらに対するシジジーのみを計算すれば事足りる。

- **minH-b** この改善策は $r \geq 3$ の場合にのみ適用できる。たとえば $r = 3$ の場合、$\widehat{G}_{1,23}$ は定理2より $\widehat{G}_{1,2}\widehat{G}_{1,3}$ と計算できるし、シジジーも $(a_{1,j},\, b_{1,j})$ $(j = 2, 3)$ から簡単に計算できる。
- **minH-c** 各 $\Gamma_{i,*/i}$ の計算中、変数 x が消去されたら、その時点で Gröbner 基底計算をストップする。

minH-a について このアイデアは、$\delta R^{(k)} \neq 0$ のときは [9] でも既に採用されているが、第2章の後半で説明した簡単化が基礎になっている。その簡単のお陰で、たとえ $\delta R^{(k)} = 0$ でも $\delta G^{(k)}$ と $\delta H^{(k)}$ はきちんと計算されることが分かる。

minH-b について $r = 3$ の場合に、$\widehat{G}_{1,23}$ に対するシジジーを、$\widehat{G}_{1,2}$ と $\widehat{G}_{1,3}$ に対するシジジーから計算する公式を与える。$\widehat{G}_{1,23} = \widehat{G}_{1,2}\widehat{G}_{1,3}$ で、$\widehat{G}_{1,23} = a_{1,23}G_1 + b_{1,23}G_2G_3$ の左辺は $\widehat{G}_{1,2}\widehat{G}_{1,3}$ に等しい。そこで、$\widehat{G}_{1,j}$ $(i = 2, 3)$ に $a_{1,j}G_1 + b_{1,j}G_j$ を代入して纏めると、G_1 と G_2G_3 の係数として次式が得られる。

$$\begin{cases} a_{1,23} = a_{1,2}a_{1,3}G_1 + a_{1,3}b_{1,2}G_2 + a_{1,2}b_{1,3}G_3, \\ b_{1,23} = b_{1,2}b_{1,3}. \end{cases} \tag{4.2}$$

$r \geq 4$ の場合には $r = 3$ の場合の公式を再帰的に用いればよい。

いくつかの実験によると、上記の方法で計算したシジジーは、$\Gamma_{i,*/i}$ を計算する過程で計算されるシジジーに比べ、数式も係数もはるかに簡単な場合が多くあった。これは上記算法の大きな利点である。

minH-c について 定理3は、$\widehat{G}'_{i,j} = g\widehat{G}_{i,j}$, $g \in \mathbb{Q}[\boldsymbol{u}]$ を主張するが、これまでの経験では g は小さな多項式であった。しかも、$\delta R^{(k)} = \delta S\, G_i + \delta T\, H_i$ を満たす $\delta S, \delta T \in \mathbb{Q}(\boldsymbol{u})[x]$ と分母因子 D は、第2章に述べたよりも巧妙に次のように計算される。第2章と同様、$\delta R^{(k)}\, \widehat{G}_1 = \delta S' G_i + \delta T' H_i$ を満たす $\delta S', \delta T' \in \mathbb{Q}[x, \boldsymbol{u}]$ を計算したあと、

$$\begin{cases} c := \gcd(\mathrm{cont}(\widehat{G}_1), \mathrm{cont}(\delta S'), \mathrm{cont}(\delta T')), \\ D := \widehat{G}_1/c, \quad \delta S := (\delta S'/c)/D, \quad \delta T := (\delta T'/c)/D, \end{cases}$$

と計算される。したがって、上記因子 g は、c の計算を少し重くはするが、最後には全て除かれることになる。

4.3 算法のテストと結果に対するコメント

前節で述べた三つの改善策を数式処理システム GAL にインプリメントして、有効性を簡単な例でテストした。査読者からは、使用例が簡単で少数であることを強く批判され、低い評価しか得られなかったが、筆者らは実験結果には満足している。本章冒頭にも述べたが、下記で記述するのは minimal 因子の EHC 全体ではなく、$\widehat{G}_{i,*/i}$ とそのシジジー計算に関する算法のみのテストである。使用した計算機は Intel(R)-U2300 (1.20GHz) (Linux 3.4.100 上で稼働) である。

実験例 5 [$r=3$ の場合] G_1, G_2, G_3 を次の多項式とする。

$$G_1 = x^2(u+v) + x(u-v) + 2u + 3v,$$
$$G_2 = x^2u + 2xv + v, \quad G_3 = x^2v - 2xu + u.$$

筆者らは、イデアル $\langle G_i, G_jG_k\rangle$, $\{i,j,k\} = \{1,2,3\}$, に対し、下記の 4 通りの計算を行い、実行時間 (msec) を計測した。

- **Gb&Szs:** Gröbner 基底 $\Gamma_{1,23}, \Gamma_{2,31}, \Gamma_{3,12}$ とそれらの要素すべてに対するシジジーを CASC'16 論文 [9] の算法で計算する。改善策との比較の基準として用いる。
- **Gb_only:** シジジー計算を行わないことを除けば **Gb&Szs** と同じ。
  この計算はシジジー計算が重いかどうかを知るために行う。
- $\widehat{G}'_{i,*}$**&Sz:** 各イデアル $\langle G_i, G_jG_k\rangle$ の計算において、$\widehat{G}'_{i,*/i} \in \mathbb{Q}[\boldsymbol{u}]$ なる多項式が計算された時点で Gröbner 基底計算をストップする。
  この計算は改善策 **minH-c** の有効性を知るために行う。
- **NEW :** $\langle G_1, G_2\rangle$, $\langle G_1, G_3\rangle$, $\langle G_2, G_3\rangle$ に対して、$\widehat{G}'_{1,2}, \widehat{G}'_{1,3}, \widehat{G}'_{2,3} \in \mathbb{Q}[\boldsymbol{u}]$ とそれらに対するシジジーを計算する。次に、これらを用いて、算式 (4.2) により $(a_{i,*/i}, b_{i,*/i})$ $(i=1,2,3)$ を計算する。この計算は改善策 **minH-b** の有効性を知るために行う。

実験例 6 [$r=4$ の場合] G_1, G_2, G_3, G_4 を次の多項式とする。

$$G_1 = x^{10}u + x^5v + u - 2v, \quad G_2 = x^{10}u - 2x^5v + 2u + v,$$
$$G_3 = x^{10}v + 3x^5u - 2v + u, \quad G_4 = x^{10}v - x^5u - 2u + 3v.$$

イデアル $\langle G_i, G_jG_kG_l\rangle$, $(\{i,j,k,l\} = \{1,2,3,4\})$, を扱うことを除けば、計算は例 5 と全く同じである。

Table I: 実験例 5 と実験例 6 に対する計測時間 (msec)

Example 5	Gb&Szs	Gb_only	$\widehat{G}'_{i,*}$&Sz	NEW
all $\Gamma_{i,j}$s.				4.03
$\Gamma_{1,23}$	50.06	41.72	16.51	(0.51)
$\Gamma_{2,31}$	36.56	29.67	36.39	(0.31)
$\Gamma_{3,12}$	35.75	30.14	1.45	(0.38)

Example 6	Gb&Szs	Gb_only	$\widehat{G}'_{i,*}$&Sz	NEW
all $\Gamma_{i,j}$s				6.01
$\Gamma_{1,234}$	591.1	473.4	589.2	(1.53)
$\Gamma_{2,341}$	428.9	351.2	427.7	(1.47)
$\Gamma_{3,412}$	878.5	695.8	18.9	(1.60)
$\Gamma_{4,123}$	543.0	429.1	11.8	(1.51)

最右列の "(*.**)" はシジジーの計算時間を示す

Gb&Szs 列 と Gb_only 列 との数値を比較すると、我々のシジジー算法は十分効率的だと言えよう。Gb&Szs 列 と $\widehat{G}'_{i,*}$&Sz 列 との数値を比較すると、改善策 minH-c は時には有効だが、常に有効とは言えない。一方、r 個の minimal 因子全てを構成するには各列で全ての計算をしなければならないので、改善策 minH-b は常に非常に有効であると言えるが、これも改善策 minH-a があってのことである。

上記のテストはいずれも従変数の個数が 2 の場合である。我々は従変数の個数が 3 個と 4 個の場合もテストしてみたが、Gröbner 基底の計算は急激に遅くなった。本稿のように Gröbner 基底的算法を使用しようとするなら、従変数の個数が多い場合の最低順位要素を効率的に計算する算法の開発が不可欠である。

5 今後の研究に向けて

minimal 因子の分離に関して、筆者らは当初、改善策 minH-a と minH-c とを思い描いており、これらが大きな効率化を達成してくれると期待した。だが、これらは期待外れで、当初は予想しなかった minH-b が急浮上してきた。それは高速算法の王道とも言える分割征服算法で、$r \geq 3$ でのみ適用可能との制限はあるものの、評判に違わず著しい効率化を達成してくれる。定理 1,2,3 は今後、種々の局面で計算の効率化に利用されるだろう。

しかし、上記の成果だけでは “拡張 Hensel 構成の再構築” とは言わない。再構築と言うのは、maximal 因子の分離で質的に著しい進歩が達成されたからである；算法の効率化は大したことはない (旧来の算法が元々、効率的だった)。まず、改善策 maxH-A について。旧来の算法では最右端の Newton 多項式 $\overline{F}_{N_1}(x, \boldsymbol{u})$ が最も重要な役割を果たした。$\overline{F}_{N_1}$ を重要視したのは、代数関数では主係数が最も重要だとの考えがあったからである。だが、拡張 Hensel 構成を解析関数に適用する際には、最も重要視すべきは x の最低次項であり、高次項が少々変化しても、低次項に対する maxmal 因子が不変なような算法が望ましい。改善策 maxH-A は正にそれを実現するのである。また、maximal 因子の歪みを矯正する改善策 maxH-C も大きな進歩である。実際、たとえば多変数多項式の因数分解を EHC を用いて行うには、maximal 因子が因数分解に合致するように分解されることが望ましいからである。筆者らは既に、このような方向で次の研究に着手している。

謝辞 本研究は科研費 (課題番号 15K00005) の援助で遂行された。

参 考 文 献

[1] B. Buchberger: Gröbner bases: an algorithmic methods in polynomial ideal theory. in *Multidimensional Systems Theory*, Chap. 6. Reidel Publishing, 1985.

[2] D. Cox, J. Little, D. O'Shea: *Ideals, Varieties, and Algorithms – An Introduction to Computational Algebraic Geometry and Commutative Algebra*, Second Edition, Chap. 3, §6, Springer-Verlag, 1997.

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

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

[5] 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).

[6] T. Sasaki and D. Inaba: A study of Hensel series in general case. *Proceedings of SNC'11*, M. Moreno Maza ((Ed.), ACM Press, 34-43 (2011).

[7] T. Sasaki and D. Inaba: 拡張Hensel構成のグレブナー基底による効率化。数理研講究録??巻, 2016 (出版予定).

[8] M. Sanuki, D. Inaba and T. Sasaki: Computation of GCD of Sparse Multivariate Polynomial by Extended Hensel Construction. *Proceedings of SYNASC2015 (Symbolic and Numeric Algorithms for Scientific Computing)*, IEEE Computer Society, 34-41 (2016).

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

[10] T. Sasaki and D. Inaba: Various enhancements of extended Hensel construction for sparse multivariate polynomials. *Proceedings of SYNASC2016 (Symbolic and Numeric Algorithms for Scientific Computing)*, IEEE Computer Society, 2017 (to appear).

[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). (This is almost the same as [11]: the delay of publication is due to very slow reviewing process.)

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

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

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