多変数多項式に対する Newton polytope
Newton Polytope of Multivariate Polynomials on Singular Point

讃岐　勝
Masaru Sanuki *
筑波大学医学医療系臨床医学域
Department of Clinical Medicine, Faculty of Medicine, University of Tsukuba †

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

佐々木 建昭
Tateaki Sasaki
筑波大学名誉教授
Prof. emeritus/, University of Tsukuba §

Abstract

拡張 Hensel 構成の初期因子を定めるためには、与多項式の各項の (主変数の次数、従変数の全次数) を 2 次元平面にプロットし、それを包含する Newton Polytope の辺から初期因子を構成する。辺には与多項式の因子の情報が含まれるが、2 次元に射影したためにいくつかの情報が失われている。

本講演では、3 次元空間など次元の高い空間での Newton Polytope を考えることで拡張 Hensel 構成の効率化を考える。Newton Polytope の辺・面・頂点に存在する因子に関する性質について具体例を示しながら説明する。

Abstract

In strategies of exteneded Hensel construction (EHC), we need to plot pairs of degrees for eacf term of given polynomial, on 2-dimension plane (we consider the Newton polygon). However, in multivariate case (more than 3-variable), several information will be vanished as the factorization. In this paper, we consider the Newton polytope instead of the Newton polygon, we show several examples as the EHC with Newton polytope.

1　Hensel 構成のフレームワーク

$\mathbb{K}[x, u_1, \ldots, u_\ell] = \mathbb{K}[x, \boldsymbol{u}]$ を主変数 x，従変数 $(\boldsymbol{u}) = (u_1, \ldots, u_\ell)$ の数係数 $\mathbb{K}$ 上の多変数多項式環全体とし，本稿ではこの多項式環に含まれる多項式の (因数) 分解を考える．多変数多項式の分解を行うよく利用されるアルゴリズムの 1 つである Hensel 構成に関する研究は古くから行われており，因数分解や GCD 計算への利用や解析接続など幅広く利用がされている．この Hensel 構成はリフティング法に基づく因数分解

*本研究は筑波大学研究基盤支援プログラム（タイプ A）「数値数式融合計算による中規模構造化行列の高速 rank 計算法の開発」の助成を受けています

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

アルゴリズムであり，主変数とそれ以外と統括する変数の 2 つの変数がキーとなって動作する．複数の変数を統括する全次数変数 t を導入する．

- 一般 Hensel 構成（1.1 節を参照）
  $u_i \to tu_i$ $(i = 1, \ldots, \ell)$ なる変換を施す．
- 拡張 Hensel 構成 [8, 9]（2 章を参照）
  $x \to t^{\lambda}x$ かつ $u_i \to t^{-\lambda}u_i$ $(i = 1, \ldots, \ell)$ なる変換を施す．

本稿で考えるのは，$F(x, t, \boldsymbol{u}) \in \mathbb{K}[x, t, \boldsymbol{u}]$ の (因数) 分解である；

$$F(x, t, \boldsymbol{u}) = G_1(x, t, \boldsymbol{u}) \cdots G_m(x, t, u_1, \boldsymbol{u}).$$

$G_1, \ldots, G_m$ は多項式であったり，代数関数であったりと目的に依存するが，本稿ではある級数環に属していると仮定する (因数分解されていると考えてもらえればよい)．この (因数) 分解を達成するため，全次数変数 t に関するリフティングを行う．すなわち，

$$F(x, t, u_1, \boldsymbol{u}) \equiv G_1^{(k-1)}(x, t, \boldsymbol{u}) \cdots G_m^{(k-1)}(x, t, \boldsymbol{u}) \pmod{t^k} \tag{1}$$

なる分解が与えられているとき

$$F(x, t, \boldsymbol{u}) \equiv G_1^{(k)}(x, t, \boldsymbol{u}) \cdots G_m^{(k)}(x, t, \boldsymbol{u}) \pmod{t^{k+1}} \tag{2}$$

なるリフティングを行う．ここで，$G_i^{(k-1)}(x, t, \boldsymbol{u})$ は全次数変数 t に関する次数が $k-1$ の多項式であり，Hensel 構成では $G_i^{(k)}(x, t, \boldsymbol{u}) = G_i^{(k-1)}(x, t, \boldsymbol{u}) + \delta G_i^{(k)}(x, t, \boldsymbol{u})$ を満たす全次数変数 t に関する斉次多項式 $\delta G_i^{(k)}(x, t, \boldsymbol{u})$ $(i = 1, \ldots, m)$ を同時に，かつ，効率的に構成ができる．

本稿では，アルゴリズムを振り返り問題点を再認識することで，新たに算法を開発する．

1.1 よく知られる Hensel 構成（一般 Hensel 構成）

よく知られる Hensel 構成（以下，一般 Hensel 構成）は次の手順で行われる．与えられた多変数多項式 $F(x, t, u_1, \ldots, u_\ell)$ に対して展開点 $\boldsymbol{s} = (s_1, \ldots, s_\ell) \in \mathbb{K}^\ell$ をひとつ決め（本稿では $\boldsymbol{s} = \boldsymbol{0}$ とする．$\boldsymbol{s} \neq \boldsymbol{0}$ の場合には，$\boldsymbol{u} - \boldsymbol{s}$ と原点へ平行移動するため，結局は算法は常に原点で展開される），決めた展開点を代入した $F^{(0)}(x) = F(x, \boldsymbol{0})$ を因数分解する．

$$F^{(0)}(x) = G_1^{(0)}(x) \cdots G_m^{(0)}(x)$$

ここで，$G_i^{(0)}(x)$ と $G_j^{(0)}(x)$ は互いに素であることを満たす必要がある $(i \neq j)$．満たさなない場合，$\boldsymbol{s}$ を取り直して，互いに素になるまで選ぶ．

いま，式 (2) を満たす $G_1^{(k-1)}(x, t, \boldsymbol{u}), \ldots, G_m^{(k-1)}(x, t, \boldsymbol{u})$ が既知と仮定して，$G_1^{(k)}(x, t, \boldsymbol{u}), \ldots, G_m^{(k)}(x, t, \boldsymbol{u})$ を計算するため，次の多項式 (Moses-Yun の補間多項式)$W_i^{(j)}(x)$ $(i = 1, \ldots, m \ \& \ j = 0, \ldots, n = \deg(F))$ を計算する．

$$W_1^{(j)}(x)\frac{G_1^{(0)} \cdots G_m^{(0)}}{G_1^{(0)}} + \ldots + W_m^{(j)}(x)\frac{G_1^{(0)} \cdots G_m^{(0)}}{G_m^{(0)}} = x^j. \tag{3}$$

このとき，求めたい $G_1^{(k)}(x, t, \boldsymbol{u}), \ldots, G_m^{(k)}(x, t, \boldsymbol{u})$ は次の手順で計算すれば良い．

1. 差分 $\delta F^{(k)}(x,t,\boldsymbol{u}) = F(x,t,\boldsymbol{u}) - G_1^{(k-1)}(x,t,\boldsymbol{u})\cdots G_1^{(k-1)}(x,t,\boldsymbol{u}) \mod t^{k+1}$ を計算；

$$\delta F^{(k)}(x,t,\boldsymbol{u}) = \delta f_n^{(k)}(t,\boldsymbol{u})x^n + \ldots + \delta f_0^{(k)}(t,\boldsymbol{u})x^0. \tag{4}$$

2. $G_i^{(k)}(x,t,\boldsymbol{u})$ は次で構成される $(i = 1,\ldots,m)$.

$$G_i^{(k)}(x,t,\boldsymbol{u}) = \delta f_n^{(k)}(t,\boldsymbol{u})W_i^{(n)} + \ldots + \delta f_0^{(k)}(t,\boldsymbol{u})W_i^{(0)}. \tag{5}$$

1.2 多くの研究者が考える (一般)Hensel 構成の限界

前節からも明らかなように，$G_i^{(0)}(x)$ と $G_j^{(0)}(x)$ は互いに素でないとき算法は破綻する．この場合，展開点を動かせばよいが，$(u+v)^{10}$ から $\{(u-1)+(v-2)\}^{10}$ への変換をみてわかる通り，項数が 11 項から 66 項と爆発的に増える（非零代入問題）.

2 変数多項式の場合 (x と u_1)， Newton-Puisuex 法が平行移動しない分解法として知られているが変数が多くなると適応することは難しい.

Salem-Gao-Lauder らによる考察（2004）

Salem-Gao-Lauder らは，ISAC2004 において，Hensel 構成における初期因子の構成方法として Newton Polytope を利用について考察をしている [6].

定義 1 (Newton polytope)
$F(x,u_1,\ldots,u_\ell) = \sum_{\boldsymbol{\alpha}_i} f_{\boldsymbol{\alpha}} x^{\alpha_{i,0}} {u_1}^{\alpha_{i,1}} \cdots {u_\ell}^{\alpha_{i,\ell}} = \sum_{\boldsymbol{\alpha}_i} f_{\boldsymbol{\alpha}} x^{\alpha_{i,0}} \boldsymbol{u}^{\boldsymbol{\alpha}_i}$ の 0 でない係数をもつ単項式の次数のリスト $(\alpha_{i,0},\alpha_{i,1},\ldots,\alpha_{i,\ell}) \in \mathbb{Z}_{\geq 0}^{\ell+1}$ について $(\alpha_{i,0},\alpha_{i,1},\ldots,\alpha_{i,\ell}) \in \mathbb{Z}_{\geq 0}^{\ell+1}$ をプロットし，その凸包を *Newton Polytope* と呼ぶことにし，$New(F)$ で表す. ∎

このとき，多項式の積について次が成り立つ.

定理 2 (Ostrowski)
$F = GH$ のとき,

$$New(F) = New(G) + New(H)$$

ここで，和は *Minkowski* 和である. ∎

多項式の積で考えると，「積の最大・最小次数はそれぞれの最大・最小次数の和」で示しているが，凸包として考えると積もまた凸包になることを示している.

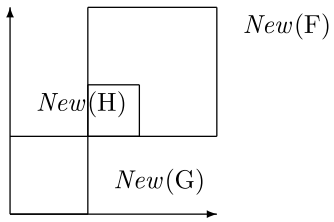

表 1: Minkowski 和：$New(F) = New(G) + New(H)$

この事実を利用して，Salem-Gao-Lauder らは Hensel 構成のステップが $G_i^{(0)}$ が多変数多項式の場合にも適応できることを述べている．ただし，次の制約はある.

1. 変数の個数は 2 つ (x と u_1)
2. 入力多項式はもニックに限る.

このような条件のもとでは，1 変数のときと同様の振る舞いをするため Hensel 構成の各ステップが動作する.

- Moses-Yun 補間式

$$W_1^{(j)}(x,u_1)G_1^{(0)} + W_2^{(j)}(x,u_1)G_2^{(0)} = x^j$$

  について，$W_1^{(j)} \in \mathbb{K}[x,u_1]$.

- $G_1^{(k)} = G_1^{(k-1)} + \delta G_1^{(k)}$ と $G_2^{(k)} = G_2^{(k-1)} + \delta G_2^{(k)}$ を計算
  1. $F - G_1^{(k-1)}G_2^{(k-1)} \equiv \delta F^{(k)}(x,u_1) \pmod{{u_1}^{k+1}}$

$$\delta F^{(k)}(x,u_1) \quad = \quad \delta G_2^{(k)}G_1^{(0)} + \delta G_1^{(k)}G_2^{(0)}$$

  2. $G_1^{(k)}, G_2^{(k)}$ は次で構成

$$(\delta G_1^{(k)}, \delta G_2^{(k)}) = (\sum_j W_2^{(j)}(x,u_1) \times \delta f_j^{(k)}(u_1), \sum_j W_1^{(j)}(x,u_1) \times \delta f_j^{(k)}(u_1)$$

制約を取り除くと，$W_{1,i} \in \mathbb{K}[x](u_1)$ となるため算法は破綻する.

2 拡張 Hensel 構成

非零代入問題および，Salem-Gao-Lauder らの問題を解決する方法として，拡張 Hensel 構成がある [8, 9]. 一般 Hensel 構成と拡張 Hensel の違いは初期因子 $G_1, \ldots G_m$ のとり方である.

定義 3 (Newton Poygon と Newton 線)
$H = \sum_i h_i {x^{e_x^{(i)}}} {u_1}^{e_{u_1}^{(i)}} \cdots {u_\ell}^{e_{u_\ell}^{(i)}}$ と表す時，各項 ${x^{e_x^{(i)}}} {u_1}^{e_{u_1}^{(i)}} \cdots {u_\ell}^{e_{u_\ell}^{(i)}}$ の指数部なる点 $(e_x^{(i)}, e_{u_1}^{(i)} + \cdots + e_{u_\ell}^{(i)})$ を平面上にプロットし，この点集合からなる凸包（*Newton Polygon*）を構成する．*Newton Polygon* の下包において，各辺 $\mathcal{L}_1, \ldots, \mathcal{L}_d$ を *Newton* 線と呼ぶ．任意に選んだ *Newton* 線 $\mathcal{L}_i$ 上の点に対応する多項式の和を $H^{(0)}$ とおき，この多項式を *Newton* 線 $\mathcal{L}_i$ に対する *Newton* 多項式 $N_{\mathcal{L}_i}$ と呼ぶ（通常，下包の最右点を含む *Newton* 線 $N_{\mathcal{L}}$ を選ぶ）. ∎

λ を Newton 線 $N_{\mathcal{L}}$ の傾きとする．このとき，分解する多項式を次のように変換する.

$$F_{New}(x,t,\boldsymbol{u}) = \frac{F(tx, t^{w_1}u_1, \ldots, t^{w_\ell}u_\ell)}{t^{n-\lambda d}}$$

この変換によって $F_{New}(x,t,\boldsymbol{u}) = F_{New}(x,T,\boldsymbol{u})$ は，2 つの変数 x と $T = t^\lambda$ で特徴づけられた多項式となる．$F_{New}(x, T = t^\lambda, \boldsymbol{u})$ において，$T = t^\lambda$ の次数は $0, 1, 2, \ldots$ と整数値である.

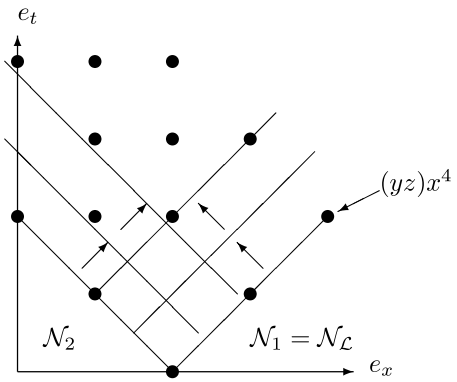

表 2: $[(x+y)(xz+1)+yz] \times [(x+z)(xy+1)-z^2]$

3 初期因子

初期因子 $G_1^{(0)}, \ldots, G_{m^{(0)}}$ は $F_{New}(x, T, \boldsymbol{u})$ の変数 T の次数が 0 である多項式 $F_{New}^{(0)}(x, T, \boldsymbol{u})$ を分解したものにする：

$$F_{New}(x, T, \boldsymbol{u}) = G_1^{(0)}(x, T, \boldsymbol{u}) \cdots G_m^{(0)}(x, T, \boldsymbol{u}).$$

変数 T によって特徴付けられているので，1.1 節で述べた手続きによって計算が可能になる．異なるのは，初期因子が 1 変数（一般 Hensel 構成）であるか多変数（拡張 Hensel 構成）であるかであり，変数 T を導入していることによって，[6] のように一般 Hensel 構成の枠に収まることなくアルゴリズムが実行できる．

4 Newton Polygon から Newton Polytope

4 章では Newton Polygon(Newton 線) を利用した方法を述べたが，2 次元平面上に項を射影させて 2 つの変数 x と T によって既存のフレームに帰着させた．

本章では，初期因子の作り方を一般化すべく 1.1 節で述べた Newton Polytope を利用した方法について検討する．

定義 4 (Newton polytope と Newton 面 (Newton face))
Newton polytope の下包において，各面 $\mathcal{F}_1, \ldots, \mathcal{F}_r$ を *Newton* 面と呼ぶ．任意に選んだ *Newton* 面 $\mathcal{F}_i$ 上の点に対応する多項式の和を $H^{(0)}$ とおき，この多項式を *Newton* 面 $\mathcal{F}_i$ に対する *Newton* 多項式と呼ぶ． ∎

4 次元以上の場合，視覚的に Newton Polytope が想像しづらいので本稿では 3 次元の場合 (x, u_1, u_2) の 1 例を紹介する．

例 1 (3 項の場合)
$F(x, u_1, u_2) = x^4u_1 + x^2u_2 - xu_1u_2$ を考える．この場合，*Newton Polytope* は平面になり，すべての項がこの中に含まれる．*Newton Polytope* と *Newton* 面が一致する場合，差分 $(F - F_{New})$ が取れないので *Hensel* 構成は破綻する．

上の例から，Newton Polytope の頂点は 4 点以上必要なことがわかる．

例 2
$F(x, u_1, u_2) = x^4u_1 + x^2u_2 - xu_1u_2 - u_1u_2^5$ を考える．*Newton Polytope* は *4* 頂点 $(4, 1, 0), (2, 0, 1), (1, 1, 1), (0, 1, 5)$ からなり，*Newton* 面は *4* つ取ることができる．

ここで，$F_{New}(x,u_1,u_2)=x^4u_1+x^2u_2-xu_1u_2$ に対応する *Newton* 面と選んだとする．これを統一的に扱うような変数を導入する変換は次のように選べば良い．

- *3* 頂点 $(4,1,0),(2,0,1),(1,1,1)$ を通る平面は $e_x+e_{u_1}+3e_{u_2}-5=0$ であり，法線ベクトルは $(1,1,3)$ である．

  ゆえに平面 $e_x+e_{u_1}+3e_{u_2}-5=0$ から法線ベクトル方向にリフティングをすれば良いことがわかる．必要なのは *3* 次元格子を含むようにリフティングすればよく，平面 $e_x+e_{u_1}+3e_{u_2}-5=0$ の定数部から $(1/5,1/5,5/5)=(1/3,1/3,1)$ 刻みにリフティングをすればよい．

以上の情報より，$F_{New}(x,u_1,u_2)=F(tx,tu_1,t^3u_2)/t^5=x^4u_1+x^2u_2+-xu_1u_2-t^{13}u_1u_2^5$ と変換できる．初期因子およびステップ幅が決定できたので，拡張 *Hensel* 構成が可能となる．

参 考 文 献

[1] P. Alvandi, M. Ataei, M. M. Maza, On the Extended Hensel Construction and its Application to the Computation of Limit Points, *Proc. of ISSAC2017*, ACM Press, 13–20(2017).

[2] L. Bernardin, On bivariate Hensel and its parallelization, *Proc. of ISSAC1998*, ACM Press, 96–100 (1998).

[3] L. Dong, S. Yao and W. Dingkang, A new algorithm for computing the extended Hensel construction of multivariate polynomials, preprint, 2014.
Be able to access from `http://www.mmrc.iss.ac.cn/ dwang/papers/E17426CM.pdf`

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

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

[6] F. Abu Salem, S. Gao, and A. G .B .Lauder: Factoring Polynomials via Polytopes, *Proc of ISSAC2004, ACM Press*, 4–11 (2004).

[7] 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).

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

[9] 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 [8]: the delay of publication is due to very slow reviewing process.)