パラメータを含む1変数多項式の因数分解について

factorization of parametric univariate polynomial over finite field

神戸大学大学院人間発達環境学研究科　　関伯実
NORIMITSU SEKI
GRADUATE SCHOOL OF HUMAN DEVELOPMENT AND ENVIRONMENT, KOBE UNIVERSITY

神戸大学大学院人間発達環境学研究科　　長坂耕作 *1
KOSAKU NAGASAKA
GRADUATE SCHOOL OF HUMAN DEVELOPMENT AND ENVIRONMENT, KOBE UNIVERSITY

Abstract

We proposed a new algorithm for factoring parametric univariate polynomial over finite field by extending the Niederreiter algorithm. Our algorithm computes many pairs of factorization and parametric constraint that are in a form similar to comprehensive Gröbner system.

1　はじめに

近年，パラメータを含む多項式の計算が様々な分野に応用されるようになり，それぞれのアルゴリズムの効率化などの研究が盛んに行われている。例えば，comprehensive Gröbner system (CGS) は，1992 年に Weispfenning によって提唱 [Wei92] され，2000 年代の Suzuki-Sato algorithm[SS06] を契機にする様々な研究により汎用的で効率的な計算が可能となっている。parametric GCD も CGS に前後して研究が進められ，長坂 [Nag17] や Kapur ら [KLM+18] などによって多変数多項式への一般化や効率的な計算ができるようになり，一部の数式処理ソフトに実装されるようになった。しかしながら，パラメータを含む多項式の計算のうち，因数分解には実際に計算が可能なアルゴリズムの先行研究が見られない。そこで本発表では，有限体上でのパラメータを含む 1 変数多項式の因数分解について考察した。なお，発表後での質疑応答においても話題となったが，パラメータを含む 1 変数多項式の整域上での因数分解はヒルベルトの第 10 問題に関連するため，パラメータを含まない因数分解とは異なり，本発表で扱った有限体上のアルゴリズムからただちに整域上の因数分解が可能となるわけではないことに留意して欲しい。

1.1　記法及び parametric factorization の定義

K を標数 p，位数 $q = p^t$ $(t \in \mathbb{N})$ の有限体，L を K の代数閉包とする。また，$\sim_K$ を K における同伴，$\sim_L$ を L における同伴の記号とする。$\vec{u} = u_1, \ldots, u_n$ をパラメータとし，$K[\vec{u}]$ を $\vec{u}$ を変数とする K 上の多項式環，$K[\vec{u}][x]$ を x を変数とする $K[\vec{u}]$ 上の多項式環とする。また，$L[x]$ も同様に x を変数とする L 上の多項式環とする。

*1 E-mail: nagasaka@main.h.kobe-u.ac.jp

$f_1, \ldots, f_r \in K[\vec{u}]$ により生成される $K[\vec{u}]$ のイデアルを $\langle f_1, \ldots, f_r \rangle$ で表し，イデアル $I \subset K[\vec{u}]$ のアフィン多様体を $V(I)$ で表す。つまり，$V(I) = \{(a_1, \ldots, a_n)^t \in L^n \mid \forall f \in I,\ f(a_1, \ldots, a_n) = 0\}$ である。パラメータ $\vec{u}$ の制約条件（L^n の部分集合）を，$(E, N) = V(E) \setminus V(N) \subset L^n$, $s_1, \ldots, s_r, t_1, \ldots, t_\ell \in K[\vec{u}]$, $E = \langle s_1, \ldots, s_r \rangle$, $N = \langle t_1, \ldots, t_\ell \rangle$ で表し，これを **parametric constraint** と呼ぶ。$\vec{a} \in L^n$ に対して，各 u_i へ a_i を代入する操作に対応する写像を $\sigma_{\vec{a}} : K[\vec{u}] \to L$ とし，特化準同型と呼ぶ。また，x に関する多項式としての各係数多項式に $\sigma_{\vec{a}}$ を適用することで，$\sigma_{\vec{a}} : K[\vec{u}][x] \to L[x]$ と自然に拡張しておく。

絶対因数分解ではない一般の因数分解では，与えられた係数体（ないしは係数環）により結果が異なるため，特化準同型を制限する必要がある。そこで，parametric constraint A に対して，その特化準同型による因数分解すべき多項式 f の像が元の有限体 K 上にのみ写されるようなパラメータのみを集めた集合を A_f と定義する。すなわち，$A_f = \{\vec{a} \in A \mid \sigma_{\vec{a}}(f) \in K[x]\}$ である。

定義 1 (parametric factorization)
$S \subset L^n$ に対し，$F = \{(A_1, F_1), \ldots, (A_\ell, F_\ell)\}$ とする。ただし，$A_i \subset S$ は *parametric constraint* であり，$F_i = \prod_{j=1}^{r_i} f_{ij}$, $f_{ij} \in K[\vec{u}][x]$ とする。このとき，以下の条件を満たすならば，F を多項式 $f \in K[\vec{u}][x]$ の S 上の ***parametric factorizaton*** と呼ぶ。

1. $S = \cup_{i=1}^{\ell} A_i$
2. $\forall \vec{a} \in A_i$, $\sigma_{\vec{a}}(f_{ij}) \in L[x]$ は，K 上既約な多項式に L 上同伴
3. $\forall \vec{a} \in (A_i)_f, \sigma_{\vec{a}}(f) \sim_L \prod_{j=1}^{r_i} \sigma_{\vec{a}}(f_{ij})$ ◀

1.2 有限体上の因数分解アルゴリズム

parametric factorization を求めるアルゴリズムは，パラメータを含まない有限体上の因数分解アルゴリズムをパラメータに対応できるように拡張する形で構成する。ベースとなるアルゴリズムは，パラメータの条件分岐の数が多くなることを避けるため，使われている性質や演算に注視し選択しなければならない。本発表では，次の 3 つのアルゴリズムについて検討し，Niederreiter アルゴリズムを選択した。

Cantor-Zassenhaus アルゴリズム [CZ81]
distinct degree factorization (DDF) と呼ばれる，多項式を次数が等しい既約因子からなる多項式の因子の積に分解するアルゴリズムと，equal degree factorization (EDF) と呼ばれる，DDF で得られた既約因子からなる多項式を既約因子に分解するアルゴリズムから構成される。計算量が小さく高速とされるが，確率的アルゴリズムであり，このアルゴリズムを直接拡張するのは簡単ではないと考え，今回は選択しなかった。

Berlekamp アルゴリズム [Ber67]
Petr-Berlekamp 行列という行列を構成し，その解空間の基底を求め，基底多項式と因数分解すべき多項式との GCD 計算を行うことで因子に分解していくアルゴリズムである。決定的アルゴリズムであり，Cantor-Zassenhaus アルゴリズムと同じくよく用いられている。しかしながら，行列の構成時に多項式剰余演算が必要なため，本発表ではパラメータに関する条件分岐がより増えてしまうことを懸念し，今回は選択しなかった。

Niederreiter アルゴリズム [Nie93]
Berlekamp アルゴリズムと同様に，Niederreiter 行列という行列を構成し，その解空間の基底を求め，GCD 計算を行うことで因子に分解していくアルゴリズムである。特徴として，Berlekamp アルゴリ

ズムと異なり，行列構成時に多項式剰余演算を必要としない。このため，係数にパラメータを含む多項式の分解に適すると考えられる。

本発表でパラメータを含む多項式に対応する形へと拡張する Niederreiter アルゴリズムは，大きく次の 3 ステップに分かれている。これらそれぞれのステップにおいて，パラメータへの対応が求められる。

1. 因数分解すべき多項式に基づき，その Niederreiter 行列 N の構成
2. $(N - E)$ の解空間の基底を求める（E は単位行列）
3. 基底多項式と因数分解すべき多項式との GCD 計算などで既約因子を導出

なお，Niederreiter アルゴリズムは因数分解すべき多項式の無平方性を必要としないが，第 3 ステップの GCD 計算に大きく影響を与えるため，本発表のアルゴリズムでは，事前に無平方分解を行うこととした。

2 parametric factorization のアルゴリズム

2.1 無平方分解と解空間のパラメータへの拡張

前述のように，本発表でベースとする Niederreiter アルゴリズムは，無平方分解，解空間の基底計算，GCD 計算，を必要とするため，パラメータを含む多項式の場合の無平方分解，解空間の基底計算，GCD 計算について定義しておく。なお，再度後述するが，解空間の基底計算と GCD 計算のパラメータを含む多項式への拡張は，先行研究が存在する。

定義 2 (parametric squarefree decomposition)
$S \subset L^n$ に対し，$F = \{(A_1, F_1), \ldots, (A_\ell, F_\ell)\}$ とする。ただし，$A_i \subset S$ は *parametric constraint* であり，$F_i = ((f_{i1}, 1), \ldots, (f_{ir_i}, r_i))$, $f_{ij} \in K[\vec{u}][x]$ とする。このとき，以下の条件を満たすならば，F を多項式 $f \in K[\vec{u}][x]$ の S 上の ***parametric squarefree decomposition*** と呼ぶ。

1. $S = \cup_{i=1}^{\ell} A_i$
2. $\forall \vec{a} \in (A_i)_f$, $\sigma_{\vec{a}}(f_{ij}) \in L[x]$ は，L 上で無平方かつ $\gcd(\sigma_{\vec{a}}(f_{ij}), \sigma_{\vec{a}}(f_{ik})) = 1$ $(j \neq k)$
3. $\forall \vec{a} \in (A_i)_f$, $\sigma_{\vec{a}}(f) \sim_L \prod_{j=1}^{r_i} \sigma_{\vec{a}}(f_{ij}^j)$ ◀

定義 3 (parametric solution space (cf. [Sit91]))
$S \subset L^n$ に対し，$Z = \{(A_1, Z_1), \ldots, (A_\ell, Z_\ell)\}$ とする。ただし，$A_i \subset S$ は *parametric constraint* であり，$Z_i = \left\{\vec{0}, \vec{z}_{i1}, \ldots, \vec{z}_{id_i}\right\}$, $\vec{z}_{ij} \in K[\vec{u}]^r$ とする。このとき，以下の条件を満たすならば，Z を同次線形方程式 $C\vec{x} = \vec{0}$, $C \in K[\vec{u}]^{r \times r}$ の S 上の ***parametric solution space*** と呼ぶ。

1. $S = \cup_{i=1}^{\ell} A_i$
2. $\forall \vec{a} \in A_i$ に対し，$\{\sigma_{\vec{a}}(\vec{z}_{i1}), \ldots, \sigma_{\vec{a}}(\vec{z}_{id_i})\}$ は，L 上の同次線形方程式 $\sigma_{\vec{a}}(C)\vec{x} = \vec{0}$ の解空間の基底 ◀

定義 4 (parametric GCD (cf. [KLM+18]))
$S \subset L^n$ に対し，$G = \{(A_1, g_1), \ldots, (A_\ell, g_\ell)\}$ とする。ただし，$A_i \subset S$ は *parametric constraint* であり，$g_i \in K[\vec{u}][x]$ とする。このとき，以下の条件を満たすならば，G を多項式 $F = \{f_1, \ldots, f_s\} \subset K[\vec{u}][x]$ の S 上の ***parametric GCD*** と呼ぶ。

1. $S = \cup_{i=1}^{\ell} A_i$
2. $\forall \vec{a} \in A_i$ に対し，$\sigma_{\vec{a}}(g_i)$ は $\{\sigma_{\vec{a}}(f_1), \ldots, \sigma_{\vec{a}}(f_s)\}$ の *GCD* ◀

2.2 アルゴリズムの概要

前述の通り，事前に無平方分解を行った上で，Niederreiter アルゴリズムを用いてパラメータを含む多項式の因数分解を行うため，全体のアルゴリズムは次の 4 つのステップから構成される。

1. 因数分解すべき多項式の parametric squarefree decomposition を求める
2. 無平方因子に対して，その Niederreiter 行列 N の構成
3. $(N - E)$ の parametric solution space を求める（E は単位行列）
4. 基底多項式と無平方因子との parametric GCD 計算などで既約因子を導出

以下では，これらについてそれぞれの計算について概要を述べていく。

parametric squarefree decomposition

有限体上の無平方分解を，パラメータを含む多項式に対応する形に拡張していくことで，parametric squarefree decomposition を計算するアルゴリズムを与える。本発表では，主に次の 3 つの計算を用いる Yun のアルゴリズム [Yun76] を拡張した。

- GCD 計算
- 多項式除算
- 多項式の p 乗根

これら 3 つの計算を，パラメータを含む多項式に対応する形に拡張しなければならない。このうち上の 2 つは [KLM+18] や [Mon02] などの先行研究の方法で計算可能である。他方，多項式の p 乗根に関しては特別な扱いが必要ではあるが，パラメータを含まない場合と同様に求めることができる（証明については割愛するが，parametric constraint として，A_i ではなく $(A_i)_f$ を用いる必要がある）。

Niederreiter 行列の構成

Niederreiter 行列の構成に必要な計算は，多項式を q 乗することと，それぞれの係数を取り出して行列の要素に格納するだけである。従って，パラメータを含む多項式であっても特に変更は必要としない。

parametric solution space

パラメータを含む行列を伴う線形方程式は，parametric system of linear equations (PSLE) と呼ばれ [Sit91]，同論文で計算方法が提案されている。本発表で定義した parametric solution space は，PSLE を同次線形方程式に限定して簡易化したものである。どちらにせよ，既知の方法で計算可能である。

parametric GCD

最後のステップでは，parametric GCD を繰り返し計算することで既約因子を求めるが，前述の通り，parametric GCD は既知の方法 [KLM+18] で計算可能である。

3 例

最後に計算例を紹介する。多項式 $f = x^4 + u_1x^3 + u_2x + u_1 \in \mathbb{F}_3[u_1, u_2][x]$ について因数分解を行う。

parametric squarefree decomposition

このステップで与えられた多項式は，次の形に無平方分解される。

$$\begin{array}{ll}\{ & \left(\left(\langle 0\rangle, \langle u_1u_2-u_1\rangle\right), \left\{x^4+u_1x^3+u_2x+u_1\right\}\right), \\ & \left(\left(\langle u_1\rangle, \langle u_2\rangle\right), \left\{(x+u_1)(x+u_2)^3\right\}\right), \\ & \left(\left(\langle u1, u2\rangle, \langle 1\rangle\right), \left\{x^4\right\}\right), \\ & \left(\left(\langle u_2+2\rangle, \langle u_1^2+2u_1\rangle\right), \left\{(x+u_1)(x+1)^3\right\}\right), \\ & \left(\left(\langle u_2+2, u_1+2\rangle, \langle 1\rangle\right), \left\{(x+1)^4\right\}\right) \qquad\qquad \}\end{array}$$

このうち，最初のペア $\left(\left(\langle 0\rangle, \langle u_1u_2-u_1\rangle\right), \left\{x^4+u_1x^3+u_2x+u_1\right\}\right)$ 以外は，既に 1 次因子の積に分解されており，以後のステップの計算は不要となる。そのため，以下では最初のペアについてのみ計算していく。

Niederreiter 行列の構成

parametric squarefree decomposition の最初のペアに含まれる無平方な多項式 $x^4+u_1x^3+u_2x+u_1$ に関して，その Niederreiter 行列を作成する。この多項式は 4 次なので以下の 4×4 行列となる。

$$N=\begin{pmatrix} u_2^2 & -u_1u_2 & u_1^2 & 0 \\ -u_2 & -u_1u_2-u_2 & -u_1^2 & u_2^2 \\ 1 & -u_1 & u_1^2 & -u_2 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

parametric solution space

Niederreiter 行列 N に対して，線形方程式 $(N-E)\vec{x}=0$ を解き，その parametric solution space を求めると，次の基底が得られる。

$$\left\{\begin{pmatrix} u_1^3u_2+u_1^3+u_1^2u_2+u_1^2-u_1u_2-u_2-1 \\ u_1u_2-u_2-1 \\ -u_1^2u_2 \\ 0 \end{pmatrix}, \begin{pmatrix} -u_1^2u_2^2+u_1^2u_2+u_2^2 \\ 0 \\ 0 \\ -u_1^2u_2 \end{pmatrix}\right\}$$

parametric GCD による既約因子の確定

得られた基底に基づく基底多項式と，元の多項式 $f(x)$（今回の例では，$x^4+u_1x^3+u_2x+u_1$）との GCD を複数回計算することで因子を取り出せる。この GCD 計算の結果により，パラメータの条件は分割（2 つの parametric constraint に分解）され，与式が既約のペアと，可約となるペアが得られる（可約となるペアの結果は $\left(\left(\langle u_2+1, u_1+1\rangle, \langle 1\rangle\right), \left\{(x^2+1)(x^2+u_1x+2)\right\}\right)$ である）。よって，与えられた $f(x)$ の parametric factorization は，次式となる。

$$\begin{array}{ll}\{ & \left(\left(\langle 0\rangle, \langle u_1u_2-u_1\rangle\right), \left\{x^4+u_1x^3+u_2x+u_1\right\}\right), \\ & \left(\left(\langle u_2+1, u_1+1\rangle, \langle 1\rangle\right), \left\{(x^2+1)(x^2+u_1x+2)\right\}\right), \\ & \left(\left(\langle u_1\rangle, \langle u_2\rangle\right), \left\{(x+u_1)(x+u_2)^3\right\}\right), \\ & \left(\left(\langle u1, u2\rangle, \langle 1\rangle\right), \left\{x^4\right\}\right), \\ & \left(\left(\langle u_2+2\rangle, \langle u_1^2+2u_1\rangle\right), \left\{(x+u_1)(x+1)^3\right\}\right), \\ & \left(\left(\langle u_2+2, u_1+2\rangle, \langle 1\rangle\right), \left\{(x+1)^4\right\}\right) \qquad\qquad \}\end{array}$$

参 考 文 献

[Ber67] E. R. Berlekamp. Factoring polynomials over finite fields. *Bell System Tech. J.*, 46:1853–1859, 1967.

[CZ81] David G. Cantor and Hans Zassenhaus. A new algorithm for factoring polynomials over finite fields. *Math. Comp.*, 36(154):587–592, 1981.

[GCL92] K. O. Geddes, S. R. Czapor, and G. Labahn. *Algorithms for computer algebra*. Kluwer Academic Publishers, Boston, MA, 1992.

[KLM+18] Deepak Kapur, Dong Lu, Michael Monagan, Yao Sun, and Dingkang Wang. An efficient algorithm for computing parametric multivariate polynomial GCD. In *ISSAC'18—Proceedings of the 2018 ACM International Symposium on Symbolic and Algebraic Computation*, pages 239–246. ACM, New York, 2018.

[Mon02] Antonio Montes. A new algorithm for discussing Gröbner bases with parameters. *J. Symbolic Comput.*, 33(2):183–208, 2002.

[Nag17] Kosaku Nagasaka. Parametric greatest common divisors using comprehensive Gröbner systems. In *ISSAC'17—Proceedings of the 2017 ACM International Symposium on Symbolic and Algebraic Computation*, pages 341–348. ACM, New York, 2017.

[Nie93] Harald Niederreiter. Factorization of polynomials and some linear-algebra problems over finite fields. volume 192, pages 301–328. 1993. Computational linear algebra in algebraic and related problems (Essen, 1992).

[Sit91] William Y. Sit. A theory for solving parametric linear systems. In *ISSAC 1991*, pages 112–121. ACM, New York, 1991.

[SS06] Akira Suzuki and Josuke Sato. A simple algorithm to compute comprehensive Gröbner bases using Gröbner bases. In *ISSAC 2006*, pages 326–331. ACM, New York, 2006.

[Wei92] Volker Weispfenning. Comprehensive Gröbner bases. *J. Symbolic Comput.*, 14(1):1–29, 1992.

[Yun76] David Y.Y. Yun. On square-free decomposition algorithms. In *Proceedings of the Third ACM Symposium on Symbolic and Algebraic Computation*, SYMSAC '76, page 26–35, New York, NY, USA, 1976. Association for Computing Machinery.