数式処理 *Bulletin of JSSAC(2023)*
Vol. 29, No. 2, pp. 3 - 30

奨励賞受賞論文

代数多様体のコホモロジー群へのフロベニウス作用を計算するアルゴリズム

工藤 桃成 *

福岡工業大学情報工学部情報通信工学科

(Received November 29, 2021 Revised December 4, 2022 Accepted February 15, 2023)

概　　要

We present an algorithm to compute the Frobenius action to cohomology groups of algebraic varieties over a field of positive characteristic. We also give an efficient algorithm specific to complete intersections. This paper is a resume of the following two papers: [29] and [30].

1 序

代数幾何学では**代数多様体**が主な研究対象であるが，特に正標数の体上の代数多様体においては**フロベニウス射**と呼ばれる射が定義でき，これは正標数の代数多様体の研究における重要な道具と考えられている．特に，代数多様体の**コホモロジー群**には，**絶対フロベニウス写像**と呼ばれる射が作用し，その作用を用いて代数多様体の性質が分類される．本稿では主に，一般の射影スキームに対し，そのコホモロジー群上のフロベニウス作用を計算する方法 [30] を紹介する．

本稿を通して，K を標数 $p > 2$ の体，$S := K[x_0, \ldots, x_r]$ を K 上の $r+1$ 変数多項式環，$\mathbb{P}^r_K := \mathrm{Proj}(S)$ を K 上の r 次元射影空間とする．文脈から K が明らかである場合には単に $\mathbb{P}^r$ とも書く．体 K 上の射影多様体 $X \subset \mathbb{P}^r$ に対して，$\mathcal{O}_X$ をその構造層，$H^q(X, \mathcal{O}_X)$ を X 上の q 次 $\mathcal{O}_X$ 係数コホモロジー群とする．このとき，各 q 次コホモロジー群 $H^q(X, \mathcal{O}_X)$ は有限次元 K 線形空間であり，**絶対フロベニウス写像** $F : X \to X$ が $H^q(X, \mathcal{O}_X)$ に p 線形に作用する．コホモロジー群の次数 q を固定したとき，この作用は F^* などと書かれる．また，$g = \dim_K H^q(X, \mathcal{O}_X)$ とするとき，$H^q(X, \mathcal{O}_X)$ の適当な基底 $\mathcal{B} = \{\mathbf{b}_1, \ldots, \mathbf{b}_g\}$ に対し $(F^*(\mathbf{b}_1), \ldots, F^*(\mathbf{b}_g)) = (\mathbf{b}_1, \ldots, \mathbf{b}_g) \cdot H$ を満たす K 上の g 次正方行列 H を，本稿では基底 $\mathcal{B}$ に関して p 線形写像 F^* を表現する行列，あるいは単に F^* の表現行列と呼ぶ．

フロベニウス作用 F^* を表現する行列の計算は，X の性質を分類する上で非常に重要である．最も重要な例の一つとして，有限体上定義される射影多様体の有理点勘定や，曲線に対するヤコ

*m-kudo@fit.ac.jp

ビ多様体の位数計算が挙げられる．具体的には，a を正整数，X を位数 p^a の有限体 $\mathbb{F}_{p^a}$ 上定義される射影多様体とするとき，特性多項式 $\det(I_{g_i} - T \cdot H_i H_i^{(p)} \cdots H_i^{(p^{a-1})})$ は素体 $\mathbb{F}_p$ 上の多項式であり，ゼータ関数 $Z_{X/\mathbb{F}_{p^a}}(T)$ に関する Katz [25, Theorem 3.1] の合同式

$$Z_{X/\mathbb{F}_{p^a}}(T) := \exp\left(\sum_{k=1}^{\infty} \frac{\#X(\mathbb{F}_{p^a})}{k} T^k\right) \equiv \prod_{i=0}^{\dim(X)} \det(I_{g_i} - T \cdot H_i H_i^{(p)} \cdots H_i^{(p^{a-1})})^{(-1)^{i+1}} \pmod{p}$$

が成立する．ここで $g_i := \dim_{\mathbb{F}_{p^a}} H^i(X, \mathcal{O}_X)$ であり，I_{g_i} は g_i 次単位行列，H_i は $H^i(X, \mathcal{O}_X)$ 上のフロベニウス作用を表現する行列，$H_i^{(p^k)}$ は H_i の各成分を p^k 乗した行列である．一方 Weil 予想によって $Z_{X/\mathbb{F}_{p^a}}(T)$ は有理数係数多項式の商として書けるが [12]，特に $\dim(X) = 1$ のとき，L 多項式 $L_{X/\mathbb{F}_{p^a}}(T) = \prod_{i=1}^{2g_1}(1 - \alpha_i T)$（$\alpha_i$ は $|\alpha_i| = p^{a/2}$ を満たす複素数）を用いて $Z_{X/\mathbb{F}_{p^a}}(T) = \frac{L_{X/\mathbb{F}_{p^a}}(T)}{(1-T)(1-p^a T)}$ と表され，さらに $\det(I_{g_1} - T \cdot H_1 H_1^{(p)} \cdots H_1^{(p^{a-1})}) \equiv L_{X/\mathbb{F}_{p^a}}(T) \bmod p$ が成立する [37]．従って

$$\#X(\mathbb{F}_{p^a}) - (p^a + 1) = -\sum_{1 \le i \le 2g_1} \alpha_i \equiv -\mathrm{trace}\left(H_1 H_1^{(p)} \cdots H_1^{(p^{a-1})}\right) \pmod{p}$$

が得られ，H_1 から $\#X(\mathbb{F}_{p^a}) - (p^a + 1) \bmod p$ の値が求まる．特に $a = 1$ かつ $p > 4{g_1}^2$ のときは $\mathrm{trace}(H_1)$ の代表元 $t_p \in [0, \ldots, p-1]$ に対し $\#X(\mathbb{F}_p) = p + 1 - t_p$ と計算できる．また，曲線 X のヤコビ多様体 $\mathrm{Jac}(X)$ に対し $\#(\mathrm{Jac(X)}(\mathbb{F}_{p^a})) = L_{X/\mathbb{F}_{p^a}}(1)$ が成立し，この事実に基づいたヤコビ多様体の位数計算アルゴリズムがこれまでに多く提案されている（e.g., [19]，[40] など）．

フロベニウス作用 F^* の他の応用例として，曲線に対する a-number や p-rank などの不変量は，$q = 1$ に対する F^* の表現行列を計算することで求められる（一般に $q = \dim(X)$ に対する F^* の表現行列を X の **Hasse-Witt 行列**と呼ぶ [24]，[37]，[39]，[26]）．特に，a-number が種数に等しい（i.e., $H^1(X, \mathcal{O}_X)$ の F^* による像が 0 である）曲線は**超特別曲線**と呼ばれ，代数曲線・アーベル多様体のモジュライ空間の構造を調べる上で中心的な役割を果たす（cf. [16]，[32]，[31]）．

本稿では，標数 p の値と射影多様体 X の定義多項式が与えられたときに，$H^q(X, \mathcal{O}_X)$ のある基底に関して F^* を表現する行列を symbolic に計算する方法について考察する．先行研究では主に，X が特定の曲線である場合に適用可能な方法・アルゴリズムが提案されている．具体的には，楕円曲線 [22, Chapter IV]，超楕円曲線 [4, 23, 27, 37, 39, 47]，フェルマー曲線 [20]，低種数の非超楕円曲線 [2, 9, 32, 31] などが挙げられる．しかし，一般の代数曲線，さらには一般次元の射影多様体については，コホモロジー群の計算困難性などからフロベニウス作用の計算アルゴリズムは与えられていなかった（詳細は [30, Section 1] を参照）．本稿では，X が一般の射影スキームで，有限個の斉次多項式 $f_1, \ldots, f_m \in S$ によって $X = V(f_1, \ldots, f_m) \subset \mathbb{P}^r$ と書ける場合に適用可能なアルゴリズム [30] の概略を述べる（3 節）．また，アルゴリズム [30] の構成において鍵となる，連接層のコホモロジー群の基底を明示的に計算する方法 [29] についても紹介する（2 節）．

なお本稿では，[29]，[30] の内容を和文にまとめただけでなく，新規に以下を加えた．

- [29] では実験結果は示されていたものの，計算の具体例が与えられていないため，本稿 2.3 節に新たに挙げている．その際，提案アルゴリズムの通りに計算する方法と，ホモロジー代数を使って理論的に計算する方法（注意 8）の二種類を解説している．前者では極小でない自由分解を用いたのに対して，後者では極小自由分解を用いている．

- [30] では X が特殊な完全交叉の場合に計算が簡略化されることを示していたが，本稿では一般の完全交叉に対する主張を記述し（命題 13），その系として [30] で扱った上記の特殊な場合を述べている（系 14，注意 15）．加えて新たに，別の特殊な場合として，退化完全交叉に対する公式を導出し（命題 16），適用できるパラメータの例を挙げている（例 21）．
- [30] にはない計算例として，種数 $4, 5$ 非超楕円曲線，Calabi-Yau 多様体を扱っている（例 19，例 20）．また，例 17 は [30] でも扱ったが，[30] では極小自由分解を用いて F^* を計算したのに対し，本稿では極小でない自由分解を用いる場合の計算を詳細に解説している．
- その他，計算を効率的に行うための補足（注意 12）や，計算結果の理論的解釈（注意 18）を記述している．

記法の注意として，特に断らない限り有限階数自由加群（特に有限次元線形空間）の元は行ベクトルで表す．

2　射影スキームのコホモロジー群

本節では，射影スキームのコホモロジー群の概念，および，その計算方法を復習する．射影スキームのコホモロジー群（より一般に射影空間上の連接層係数コホモロジー群）の計算方法には二種類（2.2 節の (A) と (B)）があるが，本稿 3 節で紹介するコホモロジー群上のフロベニウス作用を計算する方法 [30] では (A) の方法が用いられているので，本節では (A) の方法を概説する．

2.1　Čech コホモロジーの概念

一般に，体 K 上の射影スキーム X 上の構造層 $\mathcal{O}_X$ に関するコホモロジー群 $H^q(X, \mathcal{O}_X)$ は $\mathcal{O}_X$ の**脆弱分解 (flabby resolution)** を用いて定義されるが，計算の観点では **Čech コホモロジー**の概念が非常に有用である．ここではまず，一般の位相空間とその上の層に対する Čech コホモロジーの定義を復習する．

$\mathcal{F}$ を位相空間 X 上のアーベル群の層とする．$\mathcal{U} = \{U_i\}_{i \in I}$ を X の開被覆とし，簡単のため $I \subset \mathbb{Z}$ とする．各整数 $q \geq 0$ および $(i_0, \ldots, i_q) \in I^{q+1}$ に対して $U_{i_0,\ldots,i_q} := U_{i_0} \cap U_{i_1} \cap \cdots \cap U_{i_q}$ と書く．さらに，直積群

$$C^q(\mathcal{U}, \mathcal{F}) := \prod_{(i_0,\ldots,i_q) \in I^{q+1} \text{ with } i_0 < \cdots < i_q} \mathcal{F}(U_{i_0,\ldots,i_q})$$

を **Čech q-コチェイン**という．

q **次境界作用素** $d^{(q)} : C^q(\mathcal{U}, \mathcal{F}) \longrightarrow C^{q+1}(\mathcal{U}, \mathcal{F})$ を，$f = (f_{i_0,\ldots,i_q})_{i_0,\ldots,i_q} \in C^q(\mathcal{U}, \mathcal{F})$ に対して

$$(d^{(q)} f)_{i_0,\ldots,i_{q+1}} := \sum_{j=0}^{q+1} (-1)^j f_{i_0,\ldots,\widehat{i_j},\ldots,i_{q+1}}$$

と定義する．ここで $\widehat{i_j}$ は i_j を省くという意味の記号であり，右辺の各 $f_{i_0,\ldots,\widehat{i_j},\ldots,i_{q+1}}$ は制限写像 $\mathcal{F}(U_{i_0,\ldots,\widehat{i_j},\ldots,i_{q+1}}) \longrightarrow \mathcal{F}(U_{i_0,\ldots,i_{q+1}})$ による像である．また，$(d^{(q)} f)_{i_0,\ldots,i_{q+1}}$ は $d^{(q)} f$ の $i_0, \ldots, i_{q+1}$ 成分，すなわち $(d^{(q)} f)_{i_0,\ldots,i_{q+1}} \in \mathcal{F}(U_{i_0,\ldots,i_{q+1}})$ である．

このとき，$d^{(q+1)} \circ d^{(q)} = 0$ が成り立つことが確認でき，従って次の群準同型列

$$0 \longrightarrow C^0(\mathcal{U}, \mathcal{F}) \xrightarrow{d^{(0)}} C^1(\mathcal{U}, \mathcal{F}) \xrightarrow{d^{(1)}} C^2(\mathcal{U}, \mathcal{F}) \xrightarrow{d^{(2)}} C^3(\mathcal{U}, \mathcal{F}) \xrightarrow{d^{(3)}} \cdots$$

は複体である．いま，層 $\mathcal{F}$ の**開被覆 $\mathcal{U}$ に関する q 次 Čech コホモロジー群**を次で定義する：

$$\check{H}^q(\mathcal{U},\mathcal{F}) := \mathrm{Ker}\left(d^{(q)}\right)/\mathrm{Im}\left(d^{(q-1)}\right).$$

ただし $d^{(-1)} = 0$ と約束する．群 $\check{H}^q(\mathcal{U},\mathcal{F})$ は一般には開被覆 $\mathcal{U}$ のとり方に依存する．そこで，X の開被覆 $\mathcal{U}$ の全体に細分による順序を入れ，$\check{H}^q(\mathcal{U},\mathcal{F})$ の帰納極限をとることによって，層 $\mathcal{F}$ の q **次 Čech コホモロジー群** $\check{H}^q(X,\mathcal{F})$ が定義される．

$\mathcal{F}$ が分離スキーム X 上の準連接層で $\mathcal{U}$ がアファイン開被覆である場合には $\mathcal{U}$ の選び方に依らない．すなわち，分離スキーム X の任意のアファイン開被覆 $\mathcal{U}$ に対して次の同型が存在する：

$$\check{H}^q(\mathcal{U},\mathcal{F}) \cong \check{H}^q(X,\mathcal{F}) \cong H^q(X,\mathcal{F}).$$

特に X が r 次元射影空間 $X = \mathbb{P}^r = \mathrm{Proj}(S)$ の場合，開被覆 $\mathcal{U}$ を標準的なアファイン開被覆 $\{U_j := D_+(x_j) : 0 \le j \le r\}$ にとることで，$H^q(\mathbb{P}^r, \mathcal{O}_{\mathbb{P}^r}(m))$ の K 線形空間としての基底を明示的に書くことができる．ここで $S = K[x] = K[x_0,\ldots,x_r]$ であり，$\mathcal{O}_{\mathbb{P}^r}(m)$ は $\mathcal{O}_{\mathbb{P}^r}$ の m-th Serre twist である．また，

$$D_+(x_j) = \{\mathfrak{p} \in \mathbb{P}^r : x_j \notin \mathfrak{p}\} \cong \mathrm{Spec}\left(K\left[\frac{x_0}{x_j},\ldots,\frac{x_{j-1}}{x_j},\frac{x_{j+1}}{x_j},\ldots,\frac{x_r}{x_j}\right]\right)$$

であることに注意する．

以下では，コホモロジー群 $H^q(\mathbb{P}^r, \mathcal{O}_{\mathbb{P}^r}(m))$ の構造に関する幾つかの基本性質を復習する．多項式環 S における d 次斉次多項式の全体を S_d と書く．整数 $m \in \mathbb{Z}$ に対して，次数付き環 $S(m)$（S の m-twist と呼ばれる）を $S(m)_t = S_{m+t}$（$t \in \mathbb{Z}$）により定義し，$S(m)_{x_0\cdots x_r}$ で $S(m)$ の $x_0\cdots x_r$ のべきによる局所化を表す．また，$\alpha = (\alpha_0,\ldots,\alpha_r) \in \mathbb{Z}^{r+1}$ に対して，総次数 $|\alpha| := \sum_{i=0}^r \alpha_i$ の有理単項式 $x_0^{\alpha_0}\cdots x_r^{\alpha_r}$ を x^α と表す．局所化 $S(m)_{x_0\cdots x_r}$ の d 次斉次部分を $(S(m)_{x_0\cdots x_r})_d$ と書く．特に 0 次斉次部分 $(S(m)_{x_0\cdots x_r})_0$ は次の集合で張られる K 線形空間となる：

$$\left\{ax^\alpha : a \in K, \text{ and } \alpha \in \mathbb{Z}^{r+1} \text{ with } |\alpha| = m\right\}.$$

また，$(S(m)_{x_0\cdots x_r})_0$ の K 線形部分空間 L_m を次で定義する：

$$L_m := \left\langle x^\alpha : \alpha \in \mathbb{Z}^{r+1} \text{ with } \alpha_i \ge 0 \text{ for some } 0 \le i \le r \text{ and } |\alpha| = m\right\rangle_K.$$

定理 1 ([22, Theorem 5.1])
記号は上の通りとする．このとき，次が成り立つ：

(1) 次の K 線形空間の同型がある：

$$H^0(\mathbb{P}^r, \mathcal{O}_{\mathbb{P}^r}(m)) \cong \begin{cases} S_m & \text{if } m \ge 0, \\ 0 & \text{if } m < 0. \end{cases}$$

従って，各 $m \ge 0$ に対して次の集合

$$\left\{x^\alpha : \alpha \in (\mathbb{Z}_{\ge 0})^{r+1} \text{ with } |\alpha| = m\right\}$$

は $H^0(\mathbb{P}^r, \mathcal{O}_{\mathbb{P}^r}(m))$ の K 線形空間としての基底を与える．

(2) 任意の $q \notin \{0, r\}$ と $m \in \mathbb{Z}$ に対して，$H^q(\mathbb{P}^r, \mathcal{O}_{\mathbb{P}^r}(m)) = 0$ が成り立つ．

(3) 次の K 線形空間の同型がある：

$$H^r(\mathbb{P}^r, \mathcal{O}_{\mathbb{P}^r}(m)) \quad \cong \quad (S(m)_{x_0 \cdots x_r})_0 \,/\, L_m. \tag{1}$$

従って，各 $m < 0$ に対して次の集合

$$\left\{ x^\alpha : \alpha \in (\mathbb{Z}_{<0})^{r+1} \text{ with } |\alpha| = m \right\}$$

は同型 (1) のもとで $H^r(\mathbb{P}^r, \mathcal{O}_{\mathbb{P}^r}(m))$ の K 線形空間としての基底を与える．

系 2 ([22, Theorem 5.1])
次が成り立つ：

$$\dim_K H^0(\mathbb{P}^r, \mathcal{O}_{\mathbb{P}^r}(m)) = \begin{cases} {}_{m+r}\mathrm{C}_r & \text{if } m \geq 0, \\ 0 & \text{if } m < 0. \end{cases}$$

$$\dim_K H^r(\mathbb{P}^r, \mathcal{O}_{\mathbb{P}^r}(m)) = \begin{cases} {}_{-m-1}\mathrm{C}_r & \text{if } m \leq -r-1, \\ 0 & \text{if } m > -r-1. \end{cases}$$

より一般に，次が成り立つ：

定理 3 ([42])
Noether 環 A 上の任意の射影スキーム X およびその上の連接層 $\mathcal{F}$ に対して，$H^q(X, \mathcal{F})$ は有限生成 A 加群である．また，$\mathcal{F}$ に依存するある整数 m_0 が存在して，各 $q > 0$ および各 $m \geq m_0$ に対し $H^q(X, \mathcal{F}(m)) = 0$ が成り立つ．

2.2 連接層係数コホモロジー群の計算方法

$X \subset \mathbb{P}^r$ を体 K 上の射影スキーム，$\mathcal{M}$ を X 上の連接層とする．前節の定理 3 より，コホモロジー群 $H^q(X, \mathcal{M})$ は有限次元 K 線形空間である．本小節では，$H^q(X, \mathcal{M})$ の K 線形空間としての次元および基底を計算する方法について概説する．以下簡単のため，$h^q(X, \mathcal{M}) := \dim_K H^q(X, \mathcal{M})$ と書くことにする．

計算方法を概説する前に，入力データである X および $\mathcal{M}$ をどのように「具体的に」与えるかを考察する．まず，この問題は射影空間 $\mathbb{P}^r$ 上の連接層を係数にもつコホモロジー群の計算に帰着できる．実際，$\iota : X \hookrightarrow \mathbb{P}^r$ を埋め込み，$\iota_* \mathcal{M}$ を ι による $\mathcal{M}$ の順像層とするとき，K 線形空間の同型

$$H^q(X, \mathcal{M}) \cong H^q(\mathbb{P}^r, \iota_* \mathcal{M}) \tag{2}$$

が各 $q \in \mathbb{Z}$ に対し成立する．順像層 $i_* \mathcal{M}$ が $\mathbb{P}^r$ 上の連接層であることと，同型 (2) によって，$X = \mathbb{P}^r$ の場合を考えればよい．次に，連接層 $\mathcal{M}$ をどのように与えるか，であるが，次の事実を用いて代替となる入力を与える：有限生成次数付き $S = K[x_0, \ldots, x_r]$ 加群 M が存在して，$\mathcal{M}$ は M から誘導された $\mathbb{P}^r$ 上の加群層 $M^\sim$ に同型である．さらに，ある正整数 t_0，整数 $d_1^{(0)}, \ldots, d_{t_0}^{(0)}$，

および，$\bigoplus_{j=1}^{t_0} S\left(-d_j^{(0)}\right)$ の有限生成斉次部分加群 N が存在して，次数付き S 加群の同型

$$\left(\bigoplus_{j=1}^{t_0} S\left(-d_j^{(0)}\right)\right)\Big/ N \cong M$$

が成立する．従って M は，正整数 t_0，整数 $d_1^{(0)},\ldots,d_{t_0}^{(0)}$, 次数付き S 加群 $\bigoplus_{j=1}^{t_0} S\left(-d_j^{(0)}\right)$ の有限個の斉次元から決定される．

さて一般に，有限生成次数付き S 加群 M が与えられたときに，$\mathbb{P}^r$ 上の連接層 $\mathcal{M} := M^{\sim}$ を係数にもつコホモロジー群 $H^q(\mathbb{P}^r,\mathcal{M})$ を計算する方法は次の二種類に集約される：

(A) 多項式環上の加群の自由分解計算に基づく方法 [14, 29, 38, 45],
(B) 外積代数上の加群の自由分解計算に基づく方法 [11, 15].

両者の特徴や計算コストの比較については，[29, Section 4] を参照されたい．(A), (B) ともにコホモロジー群 $H^q(\mathbb{P}^r,\mathcal{M})$ の次元を計算することが可能であるが，本稿の主課題であるコホモロジー群上のフロベニウス作用を計算する上では，射影スキーム X に対し $H^q(X,\mathcal{O}_X)$ の基底を明示的に計算する必要がある．[29] において著者は，(A) の計算方法を，$H^q(\mathbb{P}^r,\mathcal{M})$（$1 \le q \le r$）の基底が明示的に計算できる形でアルゴリズムとして記述し，計算機への実装方法を与えた．以下では，[29] において記述されたアルゴリズムの概略を述べる．

有限生成次数付き S 加群 M の次数付き自由分解を

$$\mathbf{F}_\bullet : 0 \longrightarrow \mathbf{F}_s \xrightarrow{\varphi_s} \cdots \xrightarrow{\varphi_2} \mathbf{F}_1 \xrightarrow{\varphi_1} \mathbf{F}_0 \longrightarrow 0 \tag{3}$$

とする．すなわち $\mathbf{F}$ は次数付き自由 S 加群の複体であって複体 $0 \to M \to 0$ と擬同型なものである．各 $\mathbf{F}_i$ は $\mathbf{F}_i = \bigoplus_{j=1}^{t_i} S(-d_j^{(i)})$（$t_i$ および $d_j^{(i)}$ は整数）の形をしており，また，φ_i は次数 0 の次数付き準同型である．以下，φ_i の標準基底に関する表現行列を $A_i := \left(g_{k,\ell}^{(i)}\right)_{k,\ell}$ とする．ここで A_i は S 上の $t_{i-1} \times t_i$ 行列であり，各成分 $g_{k,\ell}^{(i)}$ は S における次数 $d_\ell^{(i)} - d_k^{(i-1)}$ の斉次多項式である．分解 (3) は，次の連接層の完全列を誘導する：

$$\mathcal{F}_\bullet : 0 \longrightarrow \mathcal{F}_s \xrightarrow{\varphi_s^{\sim}} \cdots \xrightarrow{\varphi_2^{\sim}} \mathcal{F}_1 \xrightarrow{\varphi_1^{\sim}} \mathcal{F}_0 \longrightarrow 0.$$

ここで各 $0 \le i \le s$ に対し $\mathcal{F}_i := \mathbf{F}_i^{\sim} = \bigoplus_{j=1}^{t_i} \mathcal{O}_{\mathbb{P}^r}(-d_j^{(i)})$ であり，$\varphi_i^{\sim}$ は φ_i から誘導された層の射を表す．準同型 $H^r(\varphi_i^{\sim}) : H^r(\mathbb{P}^r,\mathcal{F}_i) \longrightarrow H^r(\mathbb{P}^r,\mathcal{F}_{i-1})$ の列で定義される複体を $H^r(\mathcal{F}_\bullet)$ と書く．このとき，次が成り立つ（[38, Chapter 6] と同様の手法で証明できる）：

定理 4 ([29, Theorem 5])
記号は上の通りとするとき，次が成り立つ：

$$h^0(\mathbb{P}^r,\mathcal{M}) = h^0(\mathbb{P}^r,\mathcal{F}_0) - h^r(\mathbb{P}^r,\mathcal{F}_{r+1}) + h^r(\mathbb{P}^r,\mathcal{F}_r) - \mathrm{rank}H^0\left(\varphi_1^{\sim}\right) - \mathrm{rank}H^r\left(\varphi_r^{\sim}\right).$$

さらに，$1 \le q \le r$ に対し，次の K 線形空間の同型が存在する：

$$H^q\left(\mathbb{P}^r,\mathcal{M}\right) \cong \mathrm{H}_{r-q}(H^r(\mathcal{F}_\bullet)).$$

ここで $\mathrm{H}_i(H^r(\mathcal{F}_\bullet)) := \mathrm{Ker}\left(H^r(\mathcal{F}_i)\right)/\mathrm{Im}\left(H^r(\mathcal{F}_{i+1})\right)$ である．

次のアルゴリズム 5 は，$1 \leq q \leq r-1$ および M が与えられたときに，定理 4 の同型のもとで，$H^q(\mathbb{P}^r, \mathcal{M})$ の基底を計算するアルゴリズムである：

アルゴリズム 5 ([29, Subsection 3.2.1])

Step A. 次数付き自由分解 (3) を計算する．すなわち，

$$t_i,\ d_j^{(i)},\ \text{and}\ \left(g_{k,\ell}^{(i)}\right)_{k,\ell}\ \text{for}\ 0 \leq i \leq s. \tag{4}$$

を求める．計算には，多項式環 S 上の自由加群における Gröbner 基底計算を用いる．

Step B. 前のステップで得られた元 (4) に対し，以下を実行する：

(B-1) 各 $r-q-1 \leq i \leq r-q+1$ に対し，定理 1 により次のコホモロジー群の基底を計算する：

$$H^r(\mathbb{P}^r, \mathcal{F}_i) \cong \bigoplus_{j=1}^{t_i} H^r(\mathbb{P}^r, O_{\mathbb{P}^r}(-d_j^{(i)})). \tag{5}$$

具体的には，同型 (5) の右辺の基底は次で与えられる：

$$\mathcal{V}_i := \left\{ x^{\alpha_j}\mathbf{e}_j : 1 \leq j \leq t_i,\ \alpha_j \in (\mathbb{Z}_{<0})^{r+1},\ |\alpha_j| = -d_j^{(i)} \right\}.$$

ここで $\mathbf{e}_j$ は $\bigoplus_{j=1}^{t_i} H^r(\mathbb{P}^r, O_{\mathbb{P}^r}(-d_j^{(i)}))$ におけるベクトルで，j 番目の成分が 1，それ以外が全て 0 であるようなものを表す．以下，$g_0 := h^r(\mathbb{P}^r, \mathcal{F}_{r-q})$ とおき，$\mathcal{V}_{r-q}$ の元を適当に順序付けて $\mathcal{V}_{r-q} = \{\mathbf{v}_1, \ldots, \mathbf{v}_{g_0}\}$ とする．

(B-2) $i = r-q+1,\ r-q$ に対して，K 線形写像 $H^r(\varphi_i^{\sim})$ の基底 $\mathcal{V}_i$，$\mathcal{V}_{i-1}$ に関する表現行列を計算する．ここで各 $H^r(\varphi_i^{\sim}) : H^r(\mathbb{P}^r, \mathcal{F}_i) \longrightarrow H^r(\mathbb{P}^r, \mathcal{F}_{i-1})$ は Step A で計算された $A_i := \left(g_{k,\ell}^{(i)}\right)_{k,\ell}$ を用いて $\mathbf{v} \mapsto \mathbf{v}\,{}^tA_i$ で与えられるので，その表現行列は計算可能である．

(B-3) $H^r(\varphi_{r-q+1}^{\sim})$ および $H^r(\varphi_{r-q}^{\sim})$ の表現行列から，$\mathrm{Im}\left(H^r(\varphi_{r-q+1}^{\sim})\right)$ と $\mathrm{Ker}\left(H^r(\varphi_{r-q}^{\sim})\right)$ の基底を計算する．ただし $\mathrm{Im}\left(H^r(\varphi_{r-q+1}^{\sim})\right)$ の基底は $\mathcal{A} := \left\{\mathbf{a}_i := \sum_{k=1}^{g_0} a_{i,k}\mathbf{v}_k : 1 \leq i \leq g_2\right\}$（$a_{i,k} \in K$）の形で計算し，また，$\mathrm{Ker}\left(H^r(\varphi_{r-q}^{\sim})\right)$ の基底は $\mathcal{A}$ を拡張した形で求める．ここで $g_2 := \dim_K \mathrm{Im}\left(H^r(\varphi_{r-q+1}^{\sim})\right)$ とおいた．

(B-4) 商線形空間 $\mathrm{Ker}\left(H^r(\varphi_{r-q}^{\sim})\right)/\mathrm{Im}\left(H^r(\varphi_{r-q+1}^{\sim})\right)$ の基底 $\mathcal{B} := \left\{\mathbf{b}_i := \sum_{k=1}^{g_0} b_{i,k}\mathbf{v}_k : 1 \leq i \leq g\right\}$（$b_{i,k} \in K$）を求め，出力する．ここで $g := h^r(\mathbb{P}^r, \mathcal{M})$ とおいた．

アルゴリズム 5 の計算量は次の定理 6 に示す通りである：

定理 6 ([29, Corollary 17])

r を固定したときに，次数付き自由分解 (3) は既に計算されたと仮定し，

$$\begin{aligned} t^{(\max)} &:= \max\{t_i : r-q-1 \leq i \leq r-q+1\} \\ d^{(\max)} &:= \max\{d_j^{(i)} : r-q-1 \leq i \leq r-q+1 \text{ and } 1 \leq j \leq t_i\} \\ D &:= \max\{\dim_K H^r(\mathbb{P}^r, \mathcal{F}_i) : r-q-1 \leq i \leq r-q+1\} \end{aligned} \tag{6}$$

とおく．このとき，$t^{(\max)}d^{(\max)} = O(D)$ なら，アルゴリズム 5 の Step B の計算量は $O(D^4)$ である．

注意 7

(1) アルゴリズム 5 において，Step A で次数付き自由分解 (3) として極小なものをとれば，Step B の計算がより無駄のないものになると考えられる．ただし 3.2 節で後述のアルゴリズム 11 では，極小でないもの（Schreyer 分解 [43], [44]）をとることで後の計算がしやすいと期待される（注意 12）．

(2) 定理 6 において，アルゴリズム 5 の計算量評価に Step A の自由分解計算を考慮していないのは次の理由による：自由分解の正確な計算量は現時点で知られておらず，わかっているのは加群の Gröbner 基底の計算量による上からの評価のみであり，これは最悪で指数時間である．このため，[29] および [30] では，自由分解は計算されたものとして，得られた自由分解の型を用いて計算量を評価している．詳細は [29, Remark 8, Subsection 3.5] および [30, Remark 1.1, Subsections 2.4 and 3.4] を参照とする．

(3) 定理 6 における計算量は $O(D^4)$ であるが，原著 [29] では $O(D^4 + \alpha^2 D^2)$ であった．ここで α は自由分解の表現行列に現れる斉次多項式の項数の最大値である．しかし [29] の評価は後に [30, Proposition 3.6] の証明内で $O(D^4)$ に改善されている．そのため，上記の定理 6 では修正後の $O(D^4)$ を採用した．

2.3 計算例

計算例として，種数 2 の曲線

$$y^2 + (-x^3 - x - 1)y = -2x^5 - 3x^2 + 2x - 2$$

を考える．これは $\mathbb{Q}$ 上の曲線として，レベル 23 の古典モジュラー曲線である（cf. [5]）．以下ではこの曲線を p で reduction したものを考える．この曲線の射影モデル $C \subset \mathbb{P}^4$ の定義方程式を計算すると以下のようになる：

$$\begin{aligned} f_1 &:= y^2 + (-x_3 - x_1 - x_0)y + 2x_3x_2 + 3x_1^2 - 2x_1x_0 + 2x_0^2, \\ f_2 &:= x_1^2 - x_0x_2, \quad f_3 := x_2^2 - x_3x_1, \quad f_4 := x_3x_0 - x_2x_1. \end{aligned}$$

超楕円曲線の射影モデルを定義する方程式の計算方法については [18, Chapter 10] を参考にした．$K = \overline{\mathbb{F}_p}$（$\mathbb{F}_p$ の代数閉包），$S = K[x_0, x_1, x_2, x_3, y]$，$I := \langle f_1, f_2, f_3, f_4 \rangle_S$，$M := S/I$ とおく．以下では計算がしやすい $p = 5$ の場合に，アルゴリズム 5 によって $H^1(C, \mathcal{O}_C) \cong H^1(\mathbb{P}^4, M^\sim)$ の基底を計算する．記号の簡略化のため，$H^r(\mathbb{P}^r, \mathcal{O}_{\mathbb{P}^r}(m))$ の形のコホモロジー群を $H^r(\mathcal{O}_{\mathbb{P}^r}(m))$ と書く．

Step A. まず $M := S/I$ の次数付き自由分解 (3) を計算する．$q = 1$ の場合を考えているので，後の計算で必要となるのは $\mathbf{F}_4 \to \mathbf{F}_3 \to \mathbf{F}_2$ の部分のみであり，これを具体的に書くと次のようになる：

$$S(-6) \xrightarrow{\varphi_4} S(-6) \oplus S(-5)^2 \oplus S(-4) \xrightarrow{\varphi_3} S(-4)^4 \oplus S(-3)^2. \tag{7}$$

ここで φ_4，φ_3 の標準基底に関する表現行列をそれぞれ A_4，A_3 と表す．例えば A_4 は次の形である：

$$A_4 = {}^t\begin{pmatrix} 1 & x_2 & 4x_1 & x_0^2 + 2x_0y + 2x_3y + 3y^2 \end{pmatrix}.$$

Step B. 列 (7) から誘導される 4 次コホモロジー群の間の K 線形写像

$$H^4(\mathcal{O}_{\mathbb{P}^4}(-6)) \xrightarrow{H^4(\varphi_4^{\sim})} H^4(\mathcal{O}_{\mathbb{P}^4}(-6)) \oplus H^4(\mathcal{O}_{\mathbb{P}^4}(-5))^{\oplus 2} \oplus H^4(\mathcal{O}_{\mathbb{P}^4}(-4)) \tag{8}$$

を考える．ここで $S(-4)^4 \oplus S(-3)^2$ に対応するコホモロジー群 $H^4(\mathcal{O}_{\mathbb{P}^4}(-4))^{\oplus 4} \oplus H^4(\mathcal{O}_{\mathbb{P}^4}(-3))^{\oplus 2}$ は零であるので，$H^4(\varphi_3^{\sim})$ は零写像であることに注意する．

(B-1) K 線形写像 (8) の定義域と値域の基底を求める．定義域 $H^4(\mathcal{O}_{\mathbb{P}^4}(-6))$ については，

$$\mathbf{u}_1 = \frac{1}{x_0^2x_1x_2x_3y},\ \mathbf{u}_2 = \frac{1}{x_0x_1^2x_2x_3y},\ \mathbf{u}_3 = \frac{1}{x_0x_1x_2^2x_3y},\ \mathbf{u}_4 = \frac{1}{x_0x_1x_2x_3^2y},\ \mathbf{u}_5 = \frac{1}{x_0x_1x_2x_3y^2}$$

とおくと，$\mathcal{U} = \{\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3, \mathbf{u}_4, \mathbf{u}_5\}$ が基底となる．一方で，K 線形写像 (8) の値域 $H^4(\mathcal{O}_{\mathbb{P}^4}(-6)) \oplus H^4(\mathcal{O}_{\mathbb{P}^4}(-5))^{\oplus 2} \oplus H^4(\mathcal{O}_{\mathbb{P}^4}(-4))$ については，

$$\mathbf{v}_1 = \begin{pmatrix} \frac{1}{x_0^2x_1x_2x_3y}, & 0, & 0, & 0 \end{pmatrix}, \qquad \mathbf{v}_2 = \begin{pmatrix} \frac{1}{x_0x_1^2x_2x_3y}, & 0, & 0, & 0 \end{pmatrix},$$

$$\mathbf{v}_3 = \begin{pmatrix} \frac{1}{x_0x_1x_2^2x_3y}, & 0, & 0, & 0 \end{pmatrix}, \qquad \mathbf{v}_4 = \begin{pmatrix} \frac{1}{x_0x_1x_2x_3^2y}, & 0, & 0, & 0 \end{pmatrix},$$

$$\mathbf{v}_5 = \begin{pmatrix} \frac{1}{x_0x_1x_2x_3y^2}, & 0, & 0, & 0 \end{pmatrix}, \qquad \mathbf{v}_6 = \begin{pmatrix} 0, & \frac{1}{x_0x_1x_2x_3y}, & 0, & 0 \end{pmatrix},$$

$$\mathbf{v}_7 = \begin{pmatrix} 0, & 0, & \frac{1}{x_0x_1x_2x_3y}, & 0 \end{pmatrix}$$

とおくと，$\mathcal{V} = \{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3, \mathbf{v}_4, \mathbf{v}_5, \mathbf{v}_6, \mathbf{v}_7\}$ が基底となる．

(B-2) φ_4 の表現行列 A_4 と基底 $\mathcal{U}, \mathcal{V}$ から，これらの基底に関する $H^4(\varphi_4^{\sim})$ の表現行列を求める．例えば，$\mathbf{u}_1$ の像は，

$$\begin{aligned} \mathbf{u}_1 \cdot {}^tA_4 &= \begin{pmatrix} \frac{1}{x_0^2x_1x_2x_3y}, & \frac{1}{x_0^2x_1x_3y}, & \frac{4}{x_0^2x_2x_3y}, & \frac{x_0^2+2x_0y+2x_3y+3y^2}{x_0^2x_1x_2x_3y} \end{pmatrix} \\ &= \begin{pmatrix} \frac{1}{x_0^2x_1x_2x_3y}, & 0, & 0, & 0 \end{pmatrix} = \mathbf{v}_1 \end{aligned}$$

と計算され，結果として

$$\begin{pmatrix} H^4(\varphi_4^{\sim})(\mathbf{u}_1) \\ H^4(\varphi_4^{\sim})(\mathbf{u}_2) \\ H^4(\varphi_4^{\sim})(\mathbf{u}_3) \\ H^4(\varphi_4^{\sim})(\mathbf{u}_4) \\ H^4(\varphi_4^{\sim})(\mathbf{u}_5) \end{pmatrix} = \begin{pmatrix} \mathbf{u}_1 \cdot {}^tA_4 \\ \mathbf{u}_2 \cdot {}^tA_4 \\ \mathbf{u}_3 \cdot {}^tA_4 \\ \mathbf{u}_4 \cdot {}^tA_4 \\ \mathbf{u}_5 \cdot {}^tA_4 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 4 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} \mathbf{v}_1 \\ \mathbf{v}_2 \\ \mathbf{v}_3 \\ \mathbf{v}_4 \\ \mathbf{v}_5 \\ \mathbf{v}_6 \\ \mathbf{v}_7 \end{pmatrix}$$

を得る．なお，今回の場合 $H^4(\varphi_3^{\sim})$ は零写像であるので，その表現行列は零行列であるものとみなす．

(B-3) $H^4(\varphi_4^{\sim})$ および $H^4(\varphi_3^{\sim})$ の表現行列から，$\mathrm{Im}\left(H^4(\varphi_4^{\sim})\right)$ と $\mathrm{Ker}\left(H^4(\varphi_3^{\sim})\right)$ の基底を計算する．$\mathrm{Im}\left(H^4(\varphi_4^{\sim})\right)$ については，(B-2) で求めた $H^4(\varphi_4^{\sim})$ の表現行列が既に行簡約形

であることに注意して，

$$\begin{pmatrix} \mathbf{a}_1 \\ \mathbf{a}_2 \\ \mathbf{a}_3 \\ \mathbf{a}_4 \\ \mathbf{a}_5 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 4 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} \mathbf{v}_1 \\ \mathbf{v}_2 \\ \mathbf{v}_3 \\ \mathbf{v}_4 \\ \mathbf{v}_5 \\ \mathbf{v}_6 \\ \mathbf{v}_7 \end{pmatrix}$$

とおくと，$\mathcal{A} = \{\mathbf{a}_1, \ldots, \mathbf{a}_5\}$ が基底となる．$\mathrm{Ker}\left(H^4(\varphi_3^{\sim})\right)$ については，$H^4(\varphi_3^{\sim})$ は零写像であるため (B-1) で求めた $\mathcal{V}$ が既に基底であるが，$\mathcal{A}$ を拡張することで，

$$\begin{pmatrix} \mathbf{a}_1 \\ \mathbf{a}_2 \\ \mathbf{a}_3 \\ \mathbf{a}_4 \\ \mathbf{a}_5 \\ \mathbf{a}_6 \\ \mathbf{a}_7 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 4 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} \mathbf{v}_1 \\ \mathbf{v}_2 \\ \mathbf{v}_3 \\ \mathbf{v}_4 \\ \mathbf{v}_5 \\ \mathbf{v}_6 \\ \mathbf{v}_7 \end{pmatrix} \tag{9}$$

とおくと，$\mathcal{A}' = \{\mathbf{a}_1, \ldots, \mathbf{a}_7\}$ が基底となる．

(B-4) 商線形空間 $\mathrm{Ker}\left(H^4(\varphi_3^{\sim})\right)/\mathrm{Im}\left(H^4(\varphi_4^{\sim})\right)$ の基底 $\mathcal{B}$ は $\mathcal{A}'$ から $\mathcal{A}$ を除いたものとして得られ，よって出力される $H^1(C, \mathcal{O}_C)$ の基底は

$$\mathcal{B} = \{\mathbf{a}_6, \mathbf{a}_7\} = \{\mathbf{v}_6, \mathbf{v}_7\} = \left\{\left(\ 0,\quad \frac{1}{x_0x_1x_2x_3y},\quad 0,\quad 0\ \right), \left(\ 0,\quad 0,\quad \frac{1}{x_0x_1x_2x_3y}, 0\ \right)\right\} \tag{10}$$

となる（これは種数の計算式 $h^1(C, \mathcal{O}_C) = g(C)$ とも整合性がとれている）．

注意 8

ホモロジー代数を使えば，M の（極小）次数付き分解を，次のようにして計算機を用いず理論的に求めることができる．なお，この方法は査読者の一人に教わったものである．

まず，y のない式 f_2, f_3, f_4 に着目すると，これらの定める $\mathbb{P}^3 = \mathrm{Proj}(K[x_0, x_1, x_2, x_3])$ 内の零点集合は捩れ三次曲線に他ならず，特に $\langle f_2, f_3, f_4\rangle_{K[x_0,x_1,x_2,x_3]}$ は素イデアルであることに注意する．また，Buchberger の判定法を手計算で実行することで，$\{f_2, f_3, f_4\}$ は $x_0 > x_1 > x_2 > x_3$ なる次数付き逆辞書式順序に関して Gröbner 基底であることもわかる．

次に，f_1 が $S/\langle f_2, f_3, f_4\rangle_S$ における正則元（非零因子）であることに注意する．実際，$h = h_d y^d + \cdots + h_1 y + h_0 \in S$（$h_i \in K[x_0, x_1, x_2, x_3]$）に対して $hf_1 \in \langle f_2, f_3, f_4\rangle_S$ なら，hf_1 に $y = 0$ を代入することで $h_0 \cdot f_1|_{y=0} \in \langle f_2, f_3, f_4\rangle_{K[x_0,x_1,x_2,x_3]}$ が得られる。ここで $x_0 > x_1 > x_2 > x_3$ なる次数付き逆辞書式順序に関する $f_1|_{y=0}$ の先頭項 $2x_0^2$ は $\langle f_2, f_3, f_4\rangle_{K[x_0,x_1,x_2,x_3]}$ の先頭項イデアルに属さないため，$f_1|_{y=0} \notin \langle f_2, f_3, f_4\rangle_{K[x_0,x_1,x_2,x_3]}$ である．また，$\langle f_2, f_3, f_4\rangle_{K[x_0,x_1,x_2,x_3]}$ は素イデアルであるので $h_0 \in \langle f_2, f_3, f_4\rangle_{K[x_0,x_1,x_2,x_3]} \subset \langle f_2, f_3, f_4\rangle_S$ となる．よって，$h' = h_d y^{d-1} + \cdots + h_2 y + h_1$ に

対して $h'f_1 \in \langle f_2, f_3, f_4\rangle_S$ となるため，h_0 のときと同様に $h_1 \in \langle f_2, f_3, f_4\rangle_S$ を得る．これを繰り返せば最終的に $h \in \langle f_2, f_3, f_4\rangle_S$ となる．

さて，y のない式 f_2, f_3, f_4 は $\mathbb{P}^3 = \mathrm{Proj}(K[x_0, x_1, x_2, x_3])$ 内の捩れ三次曲線を定めるので，よく知られているように（cf. [13, Example 3.5]），Hilbert-Burch 型の（極小）次数付き自由分解

$$\mathbf{G}_\bullet : 0 \longrightarrow S(-3)^2 \xrightarrow{\delta_2=\begin{pmatrix} x_3 & x_1 & x_2 \\ x_2 & x_0 & x_1 \end{pmatrix}} S(-2)^3 \xrightarrow{\delta_1=\begin{pmatrix} f_2 \\ f_3 \\ f_4 \end{pmatrix}} S \longrightarrow 0$$

をもつ．$\mathbf{G}_\bullet$ に右から S 上 $S(-2)$ をテンソルすることで得られる複体を $\mathbf{G}'_\bullet$ とし，また，各成分の f_1 倍写像 $\times f_1 : \mathbf{G}'_\bullet \to \mathbf{G}_\bullet$ の写像錐（mapping cone）として得られる複体を $\mathbf{C}_\bullet$ とし，$\mathbf{G}'[-1]_\bullet$ を $\mathbf{G}'[-1]_i = \mathbf{G}'_{i-1}$ で定義される複体とすると，縦の系列が全て完全となるような次の可換図式を得る：

$$\begin{array}{ccccccccccc}
 & & & & 0 & & 0 & & 0 & & \\
 & & & & \downarrow & & \downarrow & & \downarrow & & \\
\mathbf{G}_\bullet : & & 0 & \longrightarrow & S(-3)^2 & \xrightarrow{\delta_2} & S(-2)^3 & \xrightarrow{\delta_1} & S & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\
\mathbf{C}_\bullet : 0 & \longrightarrow & S(-5)^2 & \xrightarrow{\eta_3} & S(-4)^3 \oplus S(-3)^2 & \xrightarrow{\eta_2} & S(-2) \oplus S(-2)^3 & \xrightarrow{\eta_1} & S & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\
\mathbf{G}'[-1]_\bullet : 0 & \longrightarrow & S(-5)^2 & \xrightarrow{\delta_2(-2)} & S(-4)^3 & \xrightarrow{\delta_1(-2)} & S(-2) & \longrightarrow & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & & & \\
 & & 0 & & 0 & & 0 & & & &
\end{array}$$

ここで η_3，η_2，η_1 の表現行列はそれぞれ

$$\begin{pmatrix} -x_3 & -x_1 & -x_2 & -f_1 & 0 \\ -x_2 & -x_0 & -x_1 & 0 & -f_1 \end{pmatrix}, \quad \begin{pmatrix} -f_2 & -f_1 & 0 & 0 \\ -f_3 & 0 & -f_1 & 0 \\ -f_4 & 0 & 0 & -f_1 \\ 0 & x_3 & x_1 & x_2 \\ 0 & x_2 & x_0 & x_1 \end{pmatrix}, \quad \begin{pmatrix} -f_1 \\ f_2 \\ f_3 \\ f_4 \end{pmatrix}$$

である．また，縦の $\mathbf{G}_\bullet \to \mathbf{C}_\bullet$ と $\mathbf{C}_\bullet \to \mathbf{G}'[-1]_\bullet$ はそれぞれ自然な埋め込みと射影により定義される準同型である．蛇の補題によってコホモロジー群の長完全列

$$\mathrm{H}_i(\mathbf{C}_\bullet) \longrightarrow \mathrm{H}_i(\mathbf{G}'[-1]_\bullet) \longrightarrow \mathrm{H}_{i-1}(\mathbf{G}_\bullet) \longrightarrow \mathrm{H}_{i-1}(\mathbf{C}_\bullet)$$

が誘導され，各連結準同型 $\mathrm{H}_i(\mathbf{G}'[-1]_\bullet) \to \mathrm{H}_{i-1}(\mathbf{G}_\bullet)$ は $\times f_1$ から誘導されたものに一致する．ここで $\mathrm{H}_i(\mathbf{G}_\bullet) = 0$（$i \geq 1$）および $\mathrm{H}_i(\mathbf{G}[-1]'_\bullet) = 0$（$i \geq 2$）より，任意の $i \geq 2$ に対し $\mathrm{H}_i(\mathbf{C}_\bullet) = 0$

が成り立つ．また，$i = 1$ においても短完全列

$$\mathrm{H}_1(\mathbf{G}_\bullet) = 0 \longrightarrow \mathrm{H}_1(\mathbf{C}_\bullet) \longrightarrow \mathrm{H}_1(\mathbf{G}'[-1]_\bullet) \xrightarrow{\times f_1} \mathrm{H}_0(\mathbf{G}_\bullet) \longrightarrow \mathrm{H}_0(\mathbf{C}_\bullet) = S/\langle f_1, f_2, f_3, f_4\rangle_S$$

があり，$\mathrm{H}_0(\mathbf{G}_\bullet) = S/\langle f_2, f_3, f_4\rangle_S$ および $\mathrm{H}_1(\mathbf{G}'[-1]_\bullet) = S(-2)/\langle f_2, f_3, f_4\rangle$ となるが，f_1 が $S/\langle f_2, f_2, f_4\rangle_S$ 正則元であることから $\mathrm{H}_1(\mathbf{G}'[-1]_\bullet) \to \mathrm{H}_0(\mathbf{G}_\bullet)$ は単射である．従って $\mathrm{H}_1(\mathbf{C}_\bullet) = 0$ であり，複体 $\mathbf{C}_\bullet$ は $S/\langle f_1, f_2, f_3, f_4\rangle_S$ の次数付き自由分解を与える．表現行列 η_i の成分に定数が現れないことから，この分解は極小である．いま，$H^4(\mathbb{P}^4, \mathcal{O}_{\mathbb{P}^4}(-4)^{\oplus 3} \oplus \mathcal{O}_{\mathbb{P}^4}(-3)^{\oplus 2}) = 0$ より $H^4(\eta_3^{\sim})$ は零射であり，ゆえに

$$H^1(C, \mathcal{O}_C) \cong \mathrm{Ker}\left(H^4(\eta_3^{\sim})\right) = H^4(\mathbb{P}^4, \mathcal{O}_{\mathbb{P}^4}(-5))^{\oplus 2} = \left\langle \left(\frac{1}{x_0x_1x_2x_3y}, 0 \right), \left(0, \frac{1}{x_0x_1x_2x_3y} \right) \right\rangle_K$$

となる．これは上記 **(B-4)** の結果 $h^1(C, \mathcal{O}_C) = \#\mathcal{B} = 2$ と整合的である．

3　コホモロジー群上のフロベニウス作用

本節ではまず，射影スキーム上の絶対フロベニウス写像の定義と，そのコホモロジー群への作用の概念を復習する．次に，射影スキームのコホモロジー群へのフロベニウス作用の計算アルゴリズム [30] を概説する．最後に，2.3 節で扱った例を含む幾つかの例に対し，コホモロジー群へのフロベニウス作用の表現行列を計算する．本節を通して，K を標数 $p > 2$ の体とする．

3.1　絶対フロベニウス写像とそのコホモロジー群への作用

$f_1, \ldots, f_m \in S = K[x_0, \ldots, x_r]$ を斉次多項式，$X = V(f_1, \ldots, f_m) \subset \mathbb{P}^r$ を K 上の射影スキームとするとき，X 上の**絶対フロベニウス写像 (absolute Frobenius map)** $F : (X, \mathcal{O}_X) \to (X, \mathcal{O}_X)$ とは，位相空間 X 上では恒等写像であって，構造層 $\mathcal{O}_X$ 上では p 乗写像であるようなスキームの射のことである．$\mathcal{O}_X$ を省略して単に $F : X \to X$ とも書く．絶対フロベニウス写像 F は各 q 次コホモロジー群 $H^q(X, \mathcal{O}_X)$ に作用する．次数 q を固定したときに，この作用を

$$F^* : H^q(X, \mathcal{O}_X) \longrightarrow H^q(X, \mathcal{O}_X)$$

と書く．F^* は p 線形である，すなわち，任意の $a_1, a_2 \in K$ および $f_1, f_2 \in H^q(X, \mathcal{O}_X)$ に対し $F^*(a_1f_1 + a_2f_2) = a_1^p F^*(f_1) + a_2^p F^*(f_2)$ を満たす．また，q を固定したとき，$H^q(X, \mathcal{O}_X)$ の適当な基底 $\mathcal{B} = \{\mathbf{b}_1, \ldots, \mathbf{b}_g\}$ に対し $(F^*(\mathbf{b}_1), \ldots, F^*(\mathbf{b}_g)) = (\mathbf{b}_1, \ldots, \mathbf{b}_g) \cdot H$ を満たす K 上の g 次正方行列 H を，基底 $\mathcal{B}$ に関して p 線形写像 F^* を表現する行列，あるいは単に F^* の表現行列と呼ぶ．ここで $g = \dim_K H^q(X, \mathcal{O}_X)$ とおいた．

1 節で述べたように，F^* の表現行列を計算することで X の性質を分類することが可能となり，例えば X が曲線の場合に a-number や p-rank などの不変量が計算ができる．本稿の主課題は，標数 p，X の定義多項式 $f_1, \ldots, f_m$，および，コホモロジー群の次数 q が与えられたときに，作用 F^* を $H^q(X, \mathcal{O}_X)$ の適当な基底のもとで行列表示するアルゴリズムを与えることである．ここではまず，最も基本的な例として，X が楕円曲線である場合を考える：

例 9 ([22, Chapter IV])
$E = V(f) \subset \mathbb{P}^2$ を $S = K[x, y, z]$ の三次形式 f で定義される楕円曲線とし，$F : E \to E$ を絶対フロベニウス写像とする．[22, Chapter IV] における $F^* : H^1(E, \mathcal{O}_E) \to H^1(E, \mathcal{O}_E)$ の計算のアイデアは，可約な射影スキーム $E_p := V(f^p)$ を考え，F を二つの写像 $E \longrightarrow E_p \longrightarrow E$ に分解し，対応するコホモロジー群の間の写像 $H^1(E, \mathcal{O}_E) \to H^1(E_p, \mathcal{O}_{E_p})$ および $H^1(E_p, \mathcal{O}_{E_p}) \to H^1(E, \mathcal{O}_E)$ の合成として F^* を計算することである．具体的には，以下のようにして実現される：まず，座標環 $S/\langle f \rangle$，$S/\langle f^p \rangle$ の自由分解 $\mathbf{F}_\bullet$ と $\mathbf{F}_\bullet^{(p)}$ を “つなぎ合わせる” ことで，次のような可換図式が自然に得られる：

$$\begin{array}{ccccccccc}
\mathbf{F}_\bullet : & 0 & \longrightarrow & S(-3) & \xrightarrow{\varphi_1} & S & \xrightarrow{\varphi_0} & S/\langle f \rangle & \longrightarrow & 0 \\
 & & & \downarrow & & \downarrow & & \downarrow & & \\
\mathbf{F}_\bullet^{(p)} : & 0 & \longrightarrow & S(-3p) & \xrightarrow{\varphi_1^{(p)}} & S & \xrightarrow{\varphi_0^{(p)}} & S/\langle f^p \rangle & \longrightarrow & 0 \\
 & & & \downarrow{\scriptstyle \times f^{p-1}} & & \downarrow{\scriptstyle \mathrm{id}_S} & & \downarrow & & \\
\mathbf{F}_\bullet : & 0 & \longrightarrow & S(-3) & \xrightarrow{\varphi_1} & S & \xrightarrow{\varphi_0} & S/\langle f \rangle & \longrightarrow & 0.
\end{array}$$

ここで $\mathbf{F}_\bullet$ から $\mathbf{F}_\bullet^{(p)}$ への各写像は p 乗作用であり，id_S は S 上の恒等写像，$S/\langle f^p \rangle \to S/\langle f \rangle$ は $h + \langle f^p \rangle \mapsto h + \langle f \rangle$ で定義される準同型である．特に $S/\langle f \rangle \to S/\langle f^p \rangle$ と $S/\langle f^p \rangle \to S/\langle f \rangle$ はそれぞれ $E_p \to E$ と $E \to E_p$ の構造射（座標環の間の準同型）に対応する．これにより，次の層の可換図式が誘導される：

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathcal{O}_{\mathbb{P}^2}(-3) & \xrightarrow{\tilde{\varphi_1}} & \mathcal{O}_{\mathbb{P}^2} & \xrightarrow{\tilde{\varphi_0}} & \mathcal{O}_E & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathcal{O}_{\mathbb{P}^2}(-3p) & \xrightarrow{(\varphi_1^{(p)})\tilde{}} & \mathcal{O}_{\mathbb{P}^2} & \xrightarrow{(\varphi_0^{(p)})\tilde{}} & \mathcal{O}_{E_p} & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \times f^{p-1}} & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathcal{O}_{\mathbb{P}^2}(-3) & \xrightarrow{\tilde{\varphi_1}} & \mathcal{O}_{\mathbb{P}^2} & \xrightarrow{\tilde{\varphi_0}} & \mathcal{O}_E & \longrightarrow & 0.
\end{array}$$

従って，定理 4 の証明（cf. [29, Theorem 5]）と同様に，次のコホモロジー群の可換図式を得る：

$$\begin{array}{ccc}
H^2(\mathbb{P}^2, \mathcal{O}_{\mathbb{P}^2}(-3)) \cong \mathrm{Ker}(H^2(\tilde{\varphi_1})) & \xleftarrow{\cong} & H^1(E, \mathcal{O}_E) \\
\downarrow{\scriptstyle F_1^*} & & \downarrow \\
H^2(\mathbb{P}^2, \mathcal{O}_{\mathbb{P}^2}(-3p)) \cong \mathrm{Ker}(H^2((\varphi_1^{(p)})\tilde{})) & \xleftarrow{\cong} & H^1(E_p, \mathcal{O}_{E_p}) \\
\downarrow{\scriptstyle \times f^{p-1}} & & \downarrow \\
H^2(\mathbb{P}^2, \mathcal{O}_{\mathbb{P}^2}(-3)) \cong \mathrm{Ker}(H^2(\tilde{\varphi_1})) & \xleftarrow{\cong} & H^1(E, \mathcal{O}_E).
\end{array}$$

ここで F_1 は $\mathbb{P}^2$ 上の絶対フロベニウス写像である．定理 1 (3) により，$H^1(E, \mathcal{O}_E) \cong H^2(\mathbb{P}^2, \mathcal{O}_{\mathbb{P}^2}(-3))$ の基底として $\{(xyz)^{-1}\}$ がとれる．また，その F^* による像は $f^{p-1} \cdot (xyz)^{-p}$ である．ここで $f^{p-1} \cdot$

$(xyz)^{-p}$ に現れる有理単項式は，$H^2(\mathbb{P}^2, \mathcal{O}_{\mathbb{P}^2}(-3))$ において $(xyz)^{-1}$ を除き 0 とみなせるので，F^* は f^{p-1} における $(xyz)^{p-1}$ の係数のみによって決まることがわかる．

例 9 の方法は，[32] や [9] において二つの多項式で定義される曲線の場合に拡張された．次の小節（3.2 節）で述べるアルゴリズムは，これらの方法を任意個数の多項式で定義される射影スキームへ一般化したものである．

3.2 アルゴリズムの概略

記号は前小節の通りとし，I を X の定義イデアル，すなわち，$f_1, \ldots, f_m$ で生成される S のイデアル $\langle f_1, \ldots, f_m \rangle_S$ とする．本節ではまず，[30] の主結果を定理 10 にまとめた後，アルゴリズムの概略（下の Steps A, B）を述べる．その後，X が完全交叉の場合におけるアルゴリズムの簡略化（命題 13）を説明する．

定理 10 ([30, Algorithm (I)])
射影空間 $\mathbb{P}^r$ の次元 r を固定する．このとき，体 K の標数 p，斉次多項式 $f_1, \ldots, f_m \in S$，整数 $1 \leq q \leq r-1$ を入力として，フロベニウス作用 $F^* : H^q(X, \mathcal{O}_X) \longrightarrow H^q(X, \mathcal{O}_X)$ の表現行列 H を出力するアルゴリズム（下の Steps A, B）が存在する．また，$t^{(\max)} d^{(\max)} = O(D)$ なら，Step B の時間計算量（K 上の演算量）は $\tilde{O}\left(D^4 + D^3 p^r\right)$ で上から bound できる．ここで D は式 (6) で定まる値である．

定理 10 のアルゴリズムの構成において鍵となるアイデアは，フロベニウス作用 F^* を p 線形写像 $H^q(X, \mathcal{O}_X) \longrightarrow H^q(X_p, \mathcal{O}_{X_p})$ と K 線形写像 $H^q(X_p, \mathcal{O}_{X_p}) \longrightarrow H^q(X, \mathcal{O}_X)$ に分解することである（これは例 9 の方法の一般化にあたる）．ここで X_p は S のイデアル $I_p := \langle f_1^p, \ldots, f_m^p \rangle_S$ により定義される（可約な）射影スキームである．この分解により，F^* の表現行列 H は次のアルゴリズム 11 に示す二つのステップにより計算可能となる（個々の計算ステップの詳細は [30, Section 3] を参照されたい）：

アルゴリズム 11 ([30, Algorithm (I)])

Step A. 次数付き S 加群 S/I（resp. S/I_p）の次数付き自由分解 $\mathbf{F}_\bullet$（resp. $\mathbf{F}_\bullet^{(p)}$），および，複体間の射 $\psi_\bullet : \mathbf{F}_\bullet^{(p)} \to \mathbf{F}_\bullet$ を $\psi_0 := \mathrm{id} : \mathbf{F}_0^{(p)} \to \mathbf{F}_0$ を持ち上げることで計算する（$\psi_\bullet$ の計算方法については [30, Subsection 3.2] を参照）：

$$\begin{array}{ccccccccccc}
0 & \longrightarrow & \mathbf{F}_\ell^{(p)} & \xrightarrow{\varphi_\ell^{(p)}} & \cdots & \xrightarrow{\varphi_2^{(p)}} & \mathbf{F}_1^{(p)} & \xrightarrow{\varphi_1^{(p)}} & \mathbf{F}_0^{(p)} = S & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \psi_\ell} & & & & \downarrow{\scriptstyle \psi_1} & & \downarrow{\scriptstyle \psi_0} & & \\
0 & \longrightarrow & \mathbf{F}_\ell & \xrightarrow{\varphi_\ell} & \cdots & \xrightarrow{\varphi_2} & \mathbf{F}_1 & \xrightarrow{\varphi_1} & \mathbf{F}_0 = S & \longrightarrow & 0.
\end{array}$$

Step B. Step A で計算された $\mathbf{F}_\bullet$，$\mathbf{F}_\bullet^{(p)}$ および $\psi_\bullet$ から，$H^q(X, \mathcal{O}_X)$ の K 線形空間としての基底 $\mathcal{B}$ および $F^* : H^q(X, \mathcal{O}_X) \longrightarrow H^q(X, \mathcal{O}_X)$ の $\mathcal{B}$ に関する表現行列 H を計算する：

(B-1) アルゴリズム 5 により，$\mathbf{F}_\bullet$ から基底 $\mathcal{B}$ を計算する．

(B-2) 基底 $\mathcal{B}$ の p 線形写像 $H^q(X, \mathcal{O}_X) \longrightarrow H^q(X_p, \mathcal{O}_{X_p})$ による像 $\mathcal{B}^{(p)}$ を計算する．

(B-3) 次数 0 の S 加群準同型 ψ_{r-q} の表現行列を用いることで，集合 $\mathcal{B}^{(p)}$ の K 線形写像 $H^q(X_p, \mathcal{O}_{X_p}) \longrightarrow H^q(X, \mathcal{O}_X)$ による像 C を計算し，C と $\mathcal{B}$ から行列 H を計算する．

アルゴリズム 11 の実装実験結果については [30, Section 4] に記述している．実装は Magma [3] を用いて行った．

注意 12

Step A における各持ち上げ ψ_i の計算では，各 $1 \leq k \leq t_i$ に対し

$$\left\{\left(\psi_{i-1} \circ \varphi_i^{(p)}\right)(\mathbf{e}_k^{(p)})\right\} \cup \left\{-\varphi_i(\mathbf{e}_j) : 1 \leq j \leq t_i\right\} \subset \mathbf{F}_{i-1}$$

の syzygy 加群の Gröbner 基底を計算する（[30, Subsection 3.2] の **Sub-algorithm** `LIFT` を参照）．ここで $\mathbf{e}_j$ と $\mathbf{e}_k^{(p)}$ はそれぞれ $\mathbf{F}_i$ と $\mathbf{F}_i^{(p)}$ の標準基底ベクトルである．ただし，Step A の次数付き自由分解 $\mathbf{F}_\bullet$ として Schreyer 分解 [43], [44] をとれば，各 φ_i の表現行列（の行ベクトルがなす集合 $\{\varphi_i(\mathbf{e}_j) : 1 \leq j \leq t_i\}$）として $\mathrm{Im}(\varphi_i)$ の Gröbner 基底が既に求まっているので，Gröbner 基底による割り算で $\left(\psi_{i-1} \circ \varphi_i^{(p)}\right)(\mathbf{e}_k^{(p)}) = \sum_{j=1}^{t_i} h_{j,k}\varphi_i(\mathbf{e}_j)$ を満たす $h_{j,k} \in S$ を計算すれば，持ち上げ ψ_i を構成できる．従って新たに Gröbner 基底を計算する必要はない．

3.3 完全交叉に対する計算の簡略化

本小節では，$X = V(f_1, \ldots, f_m) \subset \mathbb{P}^r$ が**完全交叉 (complete intersection)**，すなわち $(f_1, \ldots, f_m)$ が正則列である場合に有効な計算の簡略化を与える．ここで列 $(f_1, \ldots, f_m)$ が正則であるとは，任意の $1 \leq i \leq m$ に対し，f_i が $S/\langle f_1, \ldots, f_{i-1}\rangle_S$ において非零因子であるときをいう．

命題 13 (cf. [30, Proposition 4.1])

斉次多項式列 $(f_1, \ldots, f_m)$ は正則，よって射影スキーム $X = V(f_1, \ldots, f_m) \subset \mathbb{P}^r = \mathrm{Proj}(S)$ は完全交叉であるとする．f_j を並べ替えて $\deg(f_1) \leq \cdots \leq \deg(f_m)$ と仮定してよく，さらに，$d_{1\cdots m} := \sum_{j=1}^m \deg(f_j)$，各 $1 \leq j \leq m$ に対し $d_{1\cdots\hat{j}\cdots m} := \sum_{1\leq k\leq m,\ k\neq j} \deg(f_k)$ とおく．また，

$$\Lambda \quad := \quad \left\{\beta = (\beta_0, \ldots, \beta_r) \in (\mathbb{Z}_{>0})^{r+1} : \sum_{k=0}^{r} \beta_k = d_{1\cdots m}\right\}$$

とする．このとき，次が成り立つ：

(1) $q := \dim(X) = r - m$ に対し，同型

$$H^q(X, \mathcal{O}_X) \cong \mathrm{Ker}(H^r(\varphi_m^{\sim}))$$

が成り立つ．ここで

$$H^r(\varphi_m^{\sim}) : H^r\left(\mathbb{P}^r, \mathcal{O}_{\mathbb{P}^r}(-d_{1\cdots m})\right) \to \bigoplus_{j=1}^{m} H^r\left(\mathbb{P}^r, \mathcal{O}_{\mathbb{P}^r}\left(-d_{1\cdots\hat{j}\cdots m}\right)\right) \tag{11}$$

は，$H^r\left(\mathbb{P}^r, \mathcal{O}_{\mathbb{P}^r}(-d_{1\cdots m})\right)$ の基底 $\mathcal{B} := \left\{x^{-\beta} : \beta \in \Lambda\right\}$ の元 $x^{-\beta}$ を

$$\sum_{j=1}^{m} (-1)^{j-1} f_j x^{-\beta} \mathbf{e}_j = \left(\frac{f_1}{x^\beta}, -\frac{f_2}{x^\beta}, \frac{f_3}{x^\beta}, \ldots, \frac{(-1)^{m-1} f_m}{x^\beta}\right)$$

に移す K 線形写像である．

(2) $\mathrm{Ker}(H^r(\varphi_m^{\sim}))$ の元 $\sum_{\beta\in\Lambda} c_\beta x^{-\beta}$（$c_\beta \in K$）の F^* による像は $(f_1\cdots f_m)^{p-1}\sum_{\beta\in\Lambda} c_\beta^p x^{-\beta p}$ で与えられる．

命題 13 の特別な場合として次が成立する：

系 14 ([30, Proposition 4.1])
命題 13 の状況で，さらに $\sum_{j=2}^m \deg(f_j) \le r$ を満たすとする．$\alpha = (\alpha_0,\ldots,\alpha_r) \in \mathbb{Z}^{r+1}$ に対し，多項式 $(f_1\cdots f_m)^{p-1}$ における $x^\alpha := x_0^{\alpha_0}\cdots x_r^{\alpha_r}$ の係数を c_α と表す．このとき，次が成り立つ：

(1) $H^q(X,\mathcal{O}_X) \cong \mathrm{Ker}(H^r(\varphi_m^{\sim})) = H^r(\mathbb{P}^r,\mathcal{O}_{\mathbb{P}^r}(-d_{1\cdots m}))$ であり，よってこの同型のもと $\mathcal{B}$ は $H^q(X,\mathcal{O}_X)$ の基底とみなせる．
(2) 集合 Λ の元を適当に順序付けて $\Lambda = \left\{\beta^{(1)},\ldots,\beta^{(g)}\right\}$ とする．ここで $g := \dim_K H^q(X,\mathcal{O}_X)$ である．基底 $\mathcal{B} = \left\{x^{-\beta^{(1)}},\ldots,x^{-\beta^{(g)}}\right\}$ に関する $F^* : H^q(X,\mathcal{O}_X) \longrightarrow H^q(X,\mathcal{O}_X)$ の表現行列 H の (i,j) 成分は $c_{p\cdot\beta^{(j)}-\beta^{(i)}}$ である（$1 \le i,j \le g$）．従って，H の計算量は $(f_1\cdots f_m)^{p-1}$ の計算コストで上から bound できる．

さらに特別な場合として，$\sum_{j=1}^m \deg(f_j) = r+1$ のとき，$H^q(X,\mathcal{O}_X) \cong H^r(\mathbb{P}^r,\mathcal{O}_{\mathbb{P}^r}(-r-1)) \cong K$ の基底として $\{\frac{1}{x_0\cdots x_r}\}$ がとれる．このとき，F^* は $\frac{a}{x_0\cdots x_r} \mapsto \frac{a^p c_{(p-1,\ldots,p-1)}}{x_0\cdots x_r}$ で与えられる（$a \in K$）．

注意 15
$\mathbb{P}^r$ 内の非特異完全交叉 X が系 14 後半の条件 $\sum_{j=1}^m \deg(f_j) = r+1$ を満たすとき，X は $\mathbb{P}^r$ 内で余次元 m の **Calabi-Yau 多様体**である．ここで次元 d の非特異射影多様体 Y が Calabi-Yau 多様体であるとは，(1) 全ての $0 < i < d$ に対し $H^i(Y,\mathcal{O}_Y) = 0$，かつ，(2)$K_Y := \bigwedge^d \Omega^1_Y \simeq \mathcal{O}_Y$ となるときをいい，この場合 Serre 双対性によって $H^0(Y,\mathcal{O}_Y) \cong H^d(Y,\mathcal{O}_Y) \cong K$ となる．なお，一次元 Calabi-Yau 多様体は楕円曲線のことであり，二次元 Calabi-Yau 多様体は **K3 曲面**のことである．

系 14 後半の条件 $\sum_{j=1}^m \deg(f_j) = r+1$ を満たす X は上記 (1)，(2) を満たす．実際，座標環の極小自由分解は Koszul 複体で与えられ，定理 1 および定理 4 より $0 < i < \dim(X)$ に対し $H^i(X,\mathcal{O}_X) = 0$ が従う．また，$\sum_{j=1}^r \deg(f_j) = r+1$ の仮定および完全交叉に対する一般論から $K_X \cong \mathcal{O}_X(\sum_{j=1}^r \deg(f_j) - r - 1) = \mathcal{O}_X$ となる．

系 14 とは異なる特別な場合として，完全交叉 X が退化しているとき（入力となる多項式に一次式が含まれるとき）も，$\mathrm{Ker}(\varphi_m^{\sim})$ の基底や F^* の表現行列を明示的に記述できることがある．[9, Section 4] では，$\mathbb{P}^3$ 内の超平面と四次超曲面の完全交叉，すなわち $(r,m) = (3,2)$，$(d_1,d_2) = (1,4)$ の場合に，F^* の表現行列を計算する公式が示されている（[9, Proposition 6]）．次の命題 16 は，この結果の一般化にあたる（証明は [9, Proposition 6] と同様である）：

命題 16
命題 13 の状況で，さらに $d_{1\cdots m} = \sum_{j=1}^m \deg(f_j) = r+2$ を満たすとし，$\ell := \max\{j : \deg(f_j) = 1\}$ とする．このとき，次が成り立つ：

(1) $\beta_k := (1,\dots,1,2,1,\dots,1) \in \mathbb{Z}^{r+1}$（第 k 成分のみ 2）とおくと，K 線形写像 (11) の定義域は

$$\begin{aligned} H^r\left(\mathbb{P}^r, \mathcal{O}_{\mathbb{P}^r}(-d_{1\cdots m})\right) &= H^r(\mathbb{P}^r, \mathcal{O}_{\mathbb{P}^r}(-r-2)) \\ &= \left\langle v_k := x^{-\beta_k} = \frac{1}{x_0\cdots x_{k-1}x_k^2x_{k+1}\cdots x_r} : 0 \le k \le r \right\rangle_K, \end{aligned}$$

値域は

$$\bigoplus_{j=1}^{m} H^r\left(\mathbb{P}^r, \mathcal{O}_{\mathbb{P}^r}\left(-d_{1\cdots\hat{j}\cdots m}\right)\right) = H^r(\mathbb{P}^r, \mathcal{O}_{\mathbb{P}^r}(-r-1))^{\oplus\ell} = \left\langle w_j := \frac{1}{x_0x_1\cdots x_r}\mathbf{e}_j : 1 \le i \le \ell \right\rangle_K$$

を満たし，よってそれぞれの基底として $\mathcal{V} := \{v_k : 0 \le k \le r\}$ と $\mathcal{W} := \{w_j : 1 \le j \le \ell\}$ がとれる．また，各一次式 f_j（$1 \le j \le \ell$）を $a_{j,k} \in K$ を用いて $f_j = \sum_{k=0}^r a_{j,k}x_k$ と書くと，

$$\mathrm{Ker}(H^r(\varphi_m^{\sim})) = \left\{ \sum_{k=0}^r c_kv_k : c_k \in K,\ \sum_{k=0}^r a_{j,k}c_k = 0\ (1 \le \forall j \le \ell) \right\} \cong \bigcap_{j=1}^{\ell} \mathrm{syz}_K(a_{j,0},\dots,a_{j,r})$$

が成り立つ．

(2) $\ell = 1$ のとき，$f := f_1 = \sum_{k=0}^r a_kx_k$（$a_k \in K$）と表し，$a_t \ne 0$ なる $t \in \{0,\dots,r\}$ を一つ選び固定する．このとき，$\mathrm{Ker}(H^r(\varphi_m^{\sim}))$ の基底として $\mathcal{U}^{(t)} := \{u_j^{(t)} := a_tv_j - a_jv_t : 0 \le j \le r,\ j \ne t\}$ がとれて，$h^{r-m}(X, \mathcal{O}_X) = r$ となる．さらに，この基底に関する F^* の表現行列は

$$H = \left(a_t^{p-1}c_{p\beta_i-\beta_j} - a_j^pa_t^{-1}c_{p\beta_i-\beta_t}\right)_{0\le i,j\le r, i\ne t, j\ne t}$$

で与えられる．

証明

(1) 定義域に関する主張は明らかである．値域については，任意の $j \ge \ell+1$ に対し $\sum_{k\ne j} d_k \le r$ であるから $H^r(\mathbb{P}^r, \mathcal{O}_{\mathbb{P}^r}(-d_{1\cdots\hat{j}\cdots m})) = 0$ となり，よって主張が従う．後半の主張を示す．$H^r\left(\mathbb{P}^r, \mathcal{O}_{\mathbb{P}^r}(-d_{1\cdots m})\right)$ の任意の元は $v = \sum_{k=0}^r c_kv_k$（$c_k \in K$）の形に書けて，

$$H^r(\varphi_m^{\sim})(v) = \sum_{j=1}^{\ell}(-1)^{j-1}f_jv \cdot \mathbf{e}_j = \sum_{j=1}^{\ell}(-1)^{j-1}\left(\sum_{k=0}^r c_kf_jv_k\right)\cdot \mathbf{e}_j$$

を満たす．各 $1 \le j \le \ell$ に対し，$H^r(\mathbb{P}^r, \mathcal{O}_{\mathbb{P}^r}(-r-1))$ において $f_jv_k = \frac{a_{j,k}}{x_0\cdots x_r}$ であるから，

$$H^r(\varphi_m^{\sim})(v) = \sum_{j=1}^{\ell}(-1)^{j-1}\left(\sum_{k=0}^r c_ka_{j,k}\right)\cdot w_j$$

が成り立つ．従って，任意の $1 \le j \le \ell$ に対して $\sum_{k=0}^r c_ka_{j,k} = 0$ が成り立つことと，$v \in \mathrm{Ker}(H^r(\varphi_m^{\sim}))$ は同値である．

(2) (1) の結果から $\mathcal{U}^{(t)} \subset \mathrm{Ker}(H^r(\varphi_m^{\sim}))$ が従う．一次独立性を示すために，$b_i \in K$ に対し

$$\sum_{0\le i\le r,\ i\ne t} b_iu_i^{(t)} = \sum_{0\le i\le r,\ i\ne t} b_i(a_tv_i - a_iv_t) = 0$$

と仮定する．ここで，

$$\sum_{0\le i\le r,\ i\neq t} b_i(a_t v_i - a_i v_t) = \left(a_t \sum_{0\le i\le r,\ i\neq t} b_i v_i\right) - \left(\sum_{0\le i\le r,\ i\neq t} a_i b_i\right) v_t \tag{12}$$

である．よって，$\mathcal{V}$ の一次独立性と $a_t \neq 0$ から，$i \neq t$ なる任意の $0 \le i \le r$ に対し $b_i = 0$ が従い，ゆえに $\mathcal{U}^{(t)}$ は K 上一次独立である．次に $\mathcal{U}^{(t)}$ が $\mathrm{Ker}(H^r(\varphi_m^{\sim}))$ を K 上生成することを示す．(1) で示したことから $\mathrm{Ker}(H^r(\varphi_m^{\sim}))$ の任意の元 $\sum_{k=0}^r c_k v_k$（$a_k \in K$）は $\sum_{k=0}^r a_k c_k = 0$ を満たし，よって $c_t = -a_t^{-1} \sum_{0\le k\le r,\ k\neq t} a_k c_k$ である．ゆえに

$$\begin{aligned}
\sum_{k=0}^{r} c_k v_k &= \left(-a_t^{-1} \sum_{0\le k\le r,\ k\neq t} a_k c_k\right) v_t + \sum_{0\le k\le r,\ k\neq t} c_k v_k \\
&= \sum_{0\le k\le r,\ k\neq t} c_k a_t^{-1} a_t v_k - \sum_{0\le k\le r,\ k\neq t} c_k a_t^{-1} a_k v_t \\
&= \sum_{0\le k\le r,\ k\neq t} c_k a_t^{-1} (a_t v_k - a_k v_t)
\end{aligned}$$

であり，従って $\mathcal{U}^{(t)}$ は $\mathrm{Ker}(H^r(\varphi_m^{\sim}))$ を K 上生成する．

基底 $\mathcal{U}^{(t)}$ に関する F^* の表現行列を求めるために，$b_{i,j} \in K$ を用いて

$$(f_1 \cdots f_m)^{p-1} F_1^*(u_j^{(t)}) = \sum_{0\le i\le r,\ i\neq t} b_{i,j} u_i^{(t)} = \sum_{0\le i\le r,\ i\neq t} b_{i,j}(a_t v_i - a_i v_t) \tag{13}$$

とおく．ここで F_1^* は $\mathbb{P}^r$ 上の絶対フロベニウス写像から誘導される $H^r(\mathbb{P}^r, \mathcal{O}_{\mathbb{P}^r}(-d_{1\cdots m}))$ から $H^r(\mathbb{P}^r, \mathcal{O}_{\mathbb{P}^r}(-d_{1\cdots m}p))$ への写像である．等式 (13) の左辺を計算すると，

$$\begin{aligned}
(f_1 \cdots f_m)^{p-1} F_1^*(u_j^{(t)}) &= a_t^p (f_1 \cdots f_m)^{p-1} F_1^*(v_j) - a_j^p (f_1 \cdots f_m)^{p-1} F_1^*(v_t) \\
&= a_t^p \sum_{\alpha} \frac{c_\alpha x^\alpha}{x_0^p \cdots x_j^{2p} \cdots x_r^{2p}} - a_j^p \sum_{\alpha} \frac{c_\alpha x^\alpha}{x_0^p \cdots x_t^{2p} \cdots x_r^{2p}} \\
&= a_t^p \sum_{i=0}^{r} c_{p\beta_j - \beta_i} v_i - a_j^p \sum_{i=0}^{r} c_{p\beta_t - \beta_i} v_i \\
&= \sum_{i=0}^{r} (a_t^p c_{p\beta_j - \beta_i} - a_j^p c_{p\beta_t - \beta_i}) v_i
\end{aligned} \tag{14}$$

が得られ，右辺は式 (12) と同様に

$$\sum_{0\le i\le r,\ i\neq t} b_{i,j}(a_t v_i - a_i v_t) = \left(a_t \sum_{0\le i\le r,\ i\neq t} b_{i,j} v_i\right) - \left(\sum_{0\le i\le r,\ i\neq t} a_i b_{i,j}\right) v_t \tag{15}$$

が得られる．式 (14) と (15) における $i \neq t$ なる各 v_i の係数を比較して，

$$b_{i,j} = a_t^{-1}(a_t^p c_{p\beta_j - \beta_i} - a_j^p c_{p\beta_i - \beta_t}), \tag{16}$$

であり，これは v_t の係数を比較して得られる等式

$$(a_t^p c_{p\beta_j - \beta_t} - a_j^p c_{p\beta_t - \beta_t}) + \sum_{0\le i\le r,\ i\neq t} a_i b_{i,j} = 0 \tag{17}$$

に矛盾しない．実際，式 (16) に対する (17) の左辺は

$$a_t^{-1}\sum_{i=0}^{r}(a_t^p c_{p\beta_j-\beta_i}-a_j^p c_{p\beta_i-\beta_t})a_i \tag{18}$$

であり，$F^*(u_j^{(t)})=(f_1\cdots f_m)^{p-1}F_1^*(u_j^{(t)})\in \mathrm{Ker}(H^r(\tilde{\varphi_m}))$ と式 (14) より (18) は 0 となる．

∎

3.4 計算例

本節では例を用いてアルゴリズム 11 を説明した後，入力多項式のなす列が正則である場合に有効な系 14 と命題 16 の適用例を述べる．

例 17 (入力多項式のなす列が正則でない場合)

2.3 節で扱った $\mathbb{F}_p$ 上の種数 2 の曲線 $y^2+(-x^3-x-1)y=-2x^5-3x^2+2x-2$ について，$p=5$ の場合にフロベニウス作用 $F^*: H^1(C,\mathcal{O}_C)\longrightarrow H^1(C,\mathcal{O}_C)$ の表現行列をアルゴリズム 11 によって計算する．以下，記号は 2.3 節と同一とする．

Step A. $I_p:=\langle f_1^p,f_2^p,f_3^p,f_4^p\rangle_S$ とおき，S/I (resp. S/I_p) の自由分解 $\mathbf{F}_\bullet$（resp. $\mathbf{F}_\bullet^{(p)}$），および複体間の射 $\psi_\bullet:\mathbf{F}_\bullet^{(p)}\to\mathbf{F}_\bullet$ を計算する．$q=1$ の場合を考えているので，後の計算で必要となるのは $\mathbf{F}_4\to\mathbf{F}_3\to\mathbf{F}_2$ と $\mathbf{F}_4^{(p)}\to\mathbf{F}_3^{(p)}\to\mathbf{F}_2^{(p)}$ の部分のみであり，これを具体的に書くと次のようになる：

$$\begin{array}{ccccc}
S(-6) & \xrightarrow{\varphi_4} & S(-6)\oplus S(-5)^2\oplus S(-4) & \xrightarrow{\varphi_3} & S(-4)^4\oplus S(-3)^2\\
\downarrow & & \downarrow & & \downarrow\\
S(-6p) & \xrightarrow{\varphi_4^{(p)}} & S(-6p)\oplus S(-5p)^2\oplus S(-4p) & \xrightarrow{\varphi_3^{(p)}} & S(-4p)^4\oplus S(-3p)^2\\
\downarrow{\scriptstyle\psi_4} & & \downarrow{\scriptstyle\psi_3} & & \downarrow{\scriptstyle\psi_2}\\
S(-6) & \xrightarrow{\varphi_4} & S(-6)\oplus S(-5)^2\oplus S(-4) & \xrightarrow{\varphi_3} & S(-4)^4\oplus S(-3)^2.
\end{array}$$

上と下の写像列が $\mathbf{F}_\bullet$ に，真ん中の写像列が $\mathbf{F}_\bullet^{(p)}$ にそれぞれ対応する．また，$\mathbf{F}_\bullet$ から $\mathbf{F}_\bullet^{(p)}$ への各写像は p 乗作用である．ψ_3 の標準基底に関する表現行列を C_3 と表す．

Step B. 前のステップで求めた $\mathbf{F}_\bullet$，$\mathbf{F}_\bullet^{(p)}$，および $\psi_\bullet$ から，次のような 4 次コホモロジー群の可換図式が得られる：

$$\begin{array}{ccc}
H^4(\mathcal{O}_{\mathbb{P}^4}(-6)) & \xrightarrow{H^4(\tilde{\varphi_4})} & H^4(\mathcal{O}_{\mathbb{P}^4}(-6))\oplus H^4(\mathcal{O}_{\mathbb{P}^4}(-5))^{\oplus 2}\oplus H^4(\mathcal{O}_{\mathbb{P}^4}(-4))\\
\downarrow & & \downarrow\\
H^4(\mathcal{O}_{\mathbb{P}^4}(-6p)) & \xrightarrow{H^4((\tilde{\varphi_4^{(p)}})^{\sim})} & H^4(\mathcal{O}_{\mathbb{P}^4}(-6p))\oplus H^4(\mathcal{O}_{\mathbb{P}^4}(-5p))^{\oplus 2}\oplus H^4(\mathcal{O}_{\mathbb{P}^4}(-4p))\\
\downarrow{\scriptstyle H^4(\tilde{\psi_4})} & & \downarrow{\scriptstyle H^4(\tilde{\psi_3})}\\
H^4(\mathcal{O}_{\mathbb{P}^4}(-6)) & \xrightarrow{H^4(\tilde{\varphi_4})} & H^4(\mathcal{O}_{\mathbb{P}^4}(-6))\oplus H^4(\mathcal{O}_{\mathbb{P}^4}(-5))^{\oplus 2}\oplus H^4(\mathcal{O}_{\mathbb{P}^4}(-4)).
\end{array}$$

さらに，次の可換図式が誘導される：

$$\begin{array}{ccc}
\mathrm{Ker}(H^4(\tilde{\varphi_3}))/\mathrm{Im}(H^4(\tilde{\varphi_4})) & \xleftarrow{\cong} & H^1(C,\mathcal{O}_C) \\
\downarrow & & \downarrow \\
\mathrm{Ker}(H^4((\varphi_3^{(p)})\tilde{\ }))/\mathrm{Im}(H^4((\varphi_4^{(p)})\tilde{\ })) & \xleftarrow{\cong} & H^1(C_p,\mathcal{O}_{C_p}) \\
\downarrow{\scriptstyle H^4(\tilde{\psi_3})} & & \downarrow \\
\mathrm{Ker}(H^4(\tilde{\varphi_3}))/\mathrm{Im}(H^4(\tilde{\varphi_4})) & \xleftarrow{\cong} & H^1(C,\mathcal{O}_C).
\end{array}$$

上から真ん中への二つの写像はともに p 乗作用である．また，2.3 節で見たように

$$\mathrm{Ker}(H^4(\tilde{\varphi_3})) = H^4(\mathcal{O}_{\mathbb{P}^4}(-6)) \oplus H^4(\mathcal{O}_{\mathbb{P}^4}(-5))^{\oplus 2} \oplus H^4(\mathcal{O}_{\mathbb{P}^4}(-4))$$

であり，この空間の基底は $\mathcal{V} = \{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3, \mathbf{v}_4, \mathbf{v}_5, \mathbf{v}_6, \mathbf{v}_7\}$ であった（2.3 節 **Step (B-1)** 参照）．

(B-1) アルゴリズム 5 により，商線形空間 $\mathrm{Ker}\left(H^4(\tilde{\varphi_3})\right)/\mathrm{Im}\left(H^4(\tilde{\varphi_4})\right)$ の基底 $\mathcal{B}$ を計算する．$\mathcal{B}$ は式 (10) で与えられ，これは $\mathrm{Ker}\left(H^4(\tilde{\varphi_3})\right)$ の基底 $\mathcal{A}' = \{\mathbf{a}_1, \ldots, \mathbf{a}_7\}$ から $\mathrm{Im}\left(H^4(\tilde{\varphi_4})\right)$ の基底 $\mathcal{A} = \{\mathbf{a}_1, \ldots, \mathbf{a}_5\}$ を除いたものとして得られたことに注意する（$\mathcal{A}$，$\mathcal{A}'$ については 2.3 節 **Step (B-3)** 参照）．$\mathbf{b}_1 := \mathbf{a}_6 = \left(\ 0,\quad \frac{1}{x_0x_1x_2x_3y},\quad 0,\quad 0\ \right)$，$\mathbf{b}_2 := \mathbf{a}_7 = \left(\ 0,\quad 0,\quad \frac{1}{x_0x_1x_2x_3y}, 0\ \right)$ とおく．

(B-2) $\mathcal{B}$ の $H^1(C,\mathcal{O}_C) \longrightarrow H^1(C_p,\mathcal{O}_{C_p})$ による像 $\mathcal{B}^{(p)}$ は

$$\mathcal{B}^{(p)} = \left\{\left(\ 0,\quad \frac{1}{x_0^p x_1^p x_2^p x_3^p y^p},\quad 0,\quad 0\ \right), \left(\ 0,\quad 0,\quad \frac{1}{x_0^p x_1^p x_2^p x_3^p y^p}, 0\ \right)\right\}$$

である．$\mathbf{b}_1^{(p)} := \left(\ 0,\quad \frac{1}{x_0^p x_1^p x_2^p x_3^p y^p},\quad 0,\quad 0\ \right)$，$\mathbf{b}_2^{(p)} := \left(\ 0,\quad 0,\quad \frac{1}{x_0^p x_1^p x_2^p x_3^p y^p}, 0\ \right)$ とおく．

(B-3) ψ_3 の表現行列 C_3 から，$\mathcal{B}^{(p)}$ の元の $H^4(\tilde{\psi_3})$ による像を計算し，$\mathcal{B}$ の元の一次結合として表す．$H^4(\tilde{\psi_3})(\mathbf{b}_i^{(p)}) = \mathbf{b}_i^{(p)} \cdot {}^tC_3$ であり，これを計算すると

$$\begin{pmatrix} H^4(\tilde{\psi_3})(\mathbf{b}_1^{(p)}) \\ H^4(\tilde{\psi_3})(\mathbf{b}_2^{(p)}) \end{pmatrix} = \begin{pmatrix} \mathbf{b}_1^{(p)} \cdot {}^tC_3 \\ \mathbf{b}_2^{(p)} \cdot {}^tC_3 \end{pmatrix} = \begin{pmatrix} 2 & 2 & 0 & 1 & 3 & 0 & 1 \\ 3 & 3 & 2 & 4 & 2 & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} \mathbf{v}_1 \\ \mathbf{v}_2 \\ \mathbf{v}_3 \\ \mathbf{v}_4 \\ \mathbf{v}_5 \\ \mathbf{v}_6 \\ \mathbf{v}_7 \end{pmatrix}$$

となる．$H^4(\tilde{\psi_3})(\mathbf{b}_i^{(p)})$ は $\mathbf{v}_1, \ldots, \mathbf{v}_7$ の線形結合として表されているが，$\mathbf{b}_1$，$\mathbf{b}_2$ の線形

結合として表すには次のようにすればよい：まず，$H^4(\psi_3^{\sim})(\mathbf{b}_i^{(p)}) \in \mathrm{Ker}(H^4(\varphi_3^{\sim}))$ より

$$\begin{pmatrix} 2 & 2 & 0 & 1 & 3 & 0 & 1 \\ 3 & 3 & 2 & 4 & 2 & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} \mathbf{v}_1 \\ \mathbf{v}_2 \\ \mathbf{v}_3 \\ \mathbf{v}_4 \\ \mathbf{v}_5 \\ \mathbf{v}_6 \\ \mathbf{v}_7 \end{pmatrix} = Z \cdot \begin{pmatrix} \mathbf{a}_1 \\ \mathbf{a}_2 \\ \mathbf{a}_3 \\ \mathbf{a}_4 \\ \mathbf{a}_5 \\ \mathbf{a}_6 \\ \mathbf{a}_7 \end{pmatrix} \tag{19}$$

を満たす $\mathbb{F}_5$ 上の 2×7 行列 Z が一意的に存在する．実際，式 (9) を式 (19) に代入して得られる線形方程式

$$\begin{pmatrix} 2 & 2 & 0 & 1 & 3 & 0 & 1 \\ 3 & 3 & 2 & 4 & 2 & 0 & 0 \end{pmatrix} = Z \cdot \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 4 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

を解くことで

$$Z = \begin{pmatrix} 2 & 2 & 0 & 1 & 3 & 0 & 3 \\ 3 & 3 & 2 & 4 & 2 & 3 & 3 \end{pmatrix}$$

と求まる．$\mathcal{A} = \{\mathbf{a}_1, \ldots, \mathbf{a}_5\} \subset \mathrm{Im}\left(H^4(\varphi_4^{\sim})\right)$ に注意すると，

$$\begin{pmatrix} H^4(\psi_3^{\sim})(\mathbf{b}_1^{(p)}) \\ H^4(\psi_3^{\sim})(\mathbf{b}_2^{(p)}) \end{pmatrix} = Z \cdot \begin{pmatrix} \mathbf{a}_1 \\ \mathbf{a}_2 \\ \mathbf{a}_3 \\ \mathbf{a}_4 \\ \mathbf{a}_5 \\ \mathbf{a}_6 \\ \mathbf{a}_7 \end{pmatrix} = \begin{pmatrix} 0 & 3 \\ 3 & 3 \end{pmatrix} \cdot \begin{pmatrix} \mathbf{a}_6 \\ \mathbf{a}_7 \end{pmatrix} = \begin{pmatrix} 0 & 3 \\ 3 & 3 \end{pmatrix} \cdot \begin{pmatrix} \mathbf{b}_1 \\ \mathbf{b}_2 \end{pmatrix}$$

が得られ，出力される表現行列は $H = \begin{pmatrix} 0 & 3 \\ 3 & 3 \end{pmatrix}$ となる．

注意 18

1. 一般に $q = \dim(X)$ に対する $F^* : H^q(X, \mathcal{O}_X) \longrightarrow H^q(X, \mathcal{O}_X)$ の表現行列は，X の **Hasse-Witt 行列**と呼ばれる（cf. [24]，[37]，[39]，[26, p. 125]，[46]）．F^* が全単射であるとき，X は **弱通常（weakly ordinary）**と呼ばれる（cf. [41]）．特に X が種数 g の曲線で，弱通常よ

りさらに強い条件として，$(F^*)^g$ が全単射のときは**通常（ordinary）**曲線（同値なことであるが，厳密には X のヤコビ多様体がアーベル多様体として通常であるものと定義される）と呼ばれる．一方，Hasse-Witt 行列の階数が 0 となる曲線は**超特別（superspecial）**と呼ばれ，有限体上では種数に対して多くの有理点をもちうること（cf. [16]）や，種数 1, 2 の場合に同種写像暗号への応用（[8] など）が知られている．

2. 例 17 において，計算結果から C の Hasse-Witt 行列は可逆であり，従って曲線 C は $p = 5$ において弱通常である．この例では計算がしやすいように $p = 5$ としたが，[30, Subsection 5.2] において $3 \leq p \leq 17$ なる各 p に対する計算結果も得ており，その各 p でもやはり H は可逆，従って C は弱通常である（一般の p に対しての弱通常性を理論的に示せるのかもしれない）．

次に，アルゴリズム 11 の入力となる斉次多項式のなす列 $(f_1, \ldots, f_m) \in S^m$ が正則である場合に，系 14 や命題 16 を適用して計算する例を幾つか挙げる．

例 19 (系 14 が適用できる例 1：種数 4 の非超楕円曲線)
種数 4 の非超楕円曲線は $\mathbb{P}^3 = \mathrm{Proj}(\overline{K}[x, y, z, w])$ に埋め込まれ，この埋め込みのもとで二次曲面と三次曲面の完全交叉に同型となることが知られている．すなわち，C を代数閉包 $\overline{K}$ 上の種数 4 の非超楕円曲線とすると，ある既約二次形式 $Q \in \overline{K}[x, y, z, w]$ と既約三次形式 $P \in \overline{K}[x, y, z, w]$ が存在して，C は $V(Q, P)$ に $\overline{K}$ 上同型である．ここで $\deg(P) = 3$ は射影空間 $\mathbb{P}^3$ の次元以下であるので，系 14 が適用できて，次の (1)，(2) が成り立つ：

(1) $H^1(C, \mathcal{O}_C) \cong H^3(\mathbb{P}^3, \mathcal{O}_{\mathbb{P}^3}(-5))$ は $\mathcal{B} = \left\{ \frac{1}{x^2yzw}, \frac{1}{xy^2zw}, \frac{1}{xyz^2w}, \frac{1}{xyzw^2} \right\}$ を基底にもつ．

(2) $\Lambda = \{(2, 1, 1, 1), (1, 2, 1, 1), (1, 1, 2, 1), (1, 1, 1, 2)\}$ であり，基底 $\mathcal{B}$ に関する F^* の表現行列は

$$\begin{pmatrix} c_{2p-2,p-1,p-1,p-1} & c_{p-2,2p-1,p-1,p-1} & c_{p-2,p-1,2p-1,p-1} & c_{p-2,p-1,p-1,2p-1} \\ c_{2p-1,p-2,p-1,p-1} & c_{p-1,2p-2,p-1,p-1} & c_{p-1,p-2,2p-1,p-1} & c_{p-1,p-2,p-1,2p-1} \\ c_{2p-1,p-1,p-2,p-1} & c_{p-1,2p-1,p-2,p-1} & c_{p-1,p-1,2p-2,p-1} & c_{p-1,p-1,p-2,2p-1} \\ c_{2p-1,p-1,p-1,p-2} & c_{p-1,2p-1,p-1,p-2} & c_{p-1,p-1,2p-1,p-2} & c_{p-1,p-1,p-1,2p-2} \end{pmatrix} \tag{20}$$

となる．

[2, Example 8] において $p = 3$ での具体例が計算されており，さらに [32] において任意 $p \geq 5$ で適用可能な公式 (20) が示された．

より具体的な例として，$Q = 2yw + z^2$，$P = x^3 + xw^2 + y^3$ とし，$\mathbb{P}^3 = \mathrm{Proj}(\overline{\mathbb{F}_p}[x, y, z, w])$ 内の完全交叉 $C_p = V(Q, P)$ を考える．ヤコビ判定法によって $p \geq 5$ のとき C_p は非特異であることが確認でき，従って種数 4 の非超楕円曲線であることに注意する．また，C_p は $p = 11$ のときに超特別，すなわち $F^* = 0$ となることが知られている [33]．ここでは一般の p に対する C_p の Hasse-Witt 行列を計算する．

まず，$QP = 2x^3yw + x^3z^2 + 2xyw^3 + xz^2w^2 + 2y^4w + y^3z^2$ であるから

$$(QP)^{p-1} = \sum_{a+b+c+d+e+f=p-1} 2^{a+c+e} \cdot \begin{pmatrix} p-1 \\ a, b, c, d, e, f \end{pmatrix} x^{3a+3b+c+d} y^{a+c+4e+3f} z^{2b+2d+2f} w^{a+3c+2d+e}$$

が成立する．従って，$(i,j,k,\ell) \in (\mathbb{Z}_{\geq 0})^4$ に対し，$(QP)^{p-1}$ における $x^i y^j z^k w^\ell$ の係数 $c_{i,j,k,\ell}$ は，a,b,c,d,e,f に関する $\mathbb{Z}$ 上の方程式系

$$\begin{cases} a+b+c+d+e+f = p-1, \\ 3a+3b+c+d = i, \\ a+c+4e+3f = j, \\ 2b+2d+2f = k, \\ a+3c+2d+e = \ell \end{cases} \tag{21}$$

が $0 \leq a,b,c,d,e,f \leq p-1$ の条件下で解をもたないとき必ず 0 となる．方程式系 (21) の拡大係数行列を行基本変形することで

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & p-1 \\ 3 & 3 & 1 & 1 & 0 & 0 & i \\ 1 & 0 & 1 & 0 & 4 & 3 & j \\ 0 & 2 & 0 & 2 & 0 & 2 & k \\ 1 & 0 & 3 & 2 & 1 & 0 & \ell \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & p-1 \\ 0 & 1 & 0 & 1 & -3 & -2 & p-1-j \\ 0 & 0 & 2 & 2 & -3 & -3 & \ell - j \\ 0 & 0 & 0 & 0 & 6 & 6 & j-(i+\ell-3(p-1)) \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

となる．これより，方程式系 (21) が解をもつとき，

$$\begin{cases} k \equiv 0 \bmod 2, \\ j-(i+\ell-3(p-1)) \equiv 0 \bmod 6, \\ 2(\ell-j)+j-(i+\ell-3(p-1)) \equiv 0 \bmod 4 \end{cases} \tag{22}$$

を満たす必要がある．式 (20) に現れる各 $c_{i,j,k,\ell}$ のインデックス (i,j,k,ℓ) に対し，12 を法とした p の各値を (22) に代入することで次が得られる：

- $p \equiv 1 \bmod 12$ のとき，方程式系 (22) を満たす (i,j,k,ℓ) は $(2p-2,p-1,p-1,p-1)$, $(p-1,2p-2,p-1,p-1)$, $(p-1,p-1,2p-2,p-1)$, $(p-1,p-1,p-1,2p-2)$ のみであり，よって H は対角行列となる．
- $p \equiv 5 \bmod 12$ のとき，方程式系 (22) を満たす (i,j,k,ℓ) は $(p-1,2p-2,p-1,p-1)$ のみであり，よって H の $(2,2)$ 成分以外の成分は全て 0 である．
- $p \equiv 7 \bmod 12$ のとき，方程式系 (22) を満たす (i,j,k,ℓ) は $(p-2,p-1,p-1,2p-1)$, $(p-1,p-1,2p-2,p-1)$, $(2p-1,p-1,p-1,p-2)$ のみであり，よって H の $(1,4),(3,3),(4,1)$ 成分以外の成分は全て 0 である．
- $p \equiv 11 \bmod 12$ のとき，方程式系 (22) を満たす (i,j,k,ℓ) は存在しない．よって H は零行列であり，ゆえに C_p は超特別となる．

例 20 (系 14 が適用できる例 2：種数 5 の非超楕円曲線，Calabi-Yau 多様体)
種数 5 の非超楕円曲線 C は $\mathbb{P}^4$ に埋め込まれ，この埋め込みのもとで三つの二次曲面の完全交叉に同型となることが知られている．すなわち，ある既約二次形式 $Q_1,Q_2,Q_3 \in \overline{K}[x,y,z,v,w]$ が存在して，C は $V(Q_1,Q_2,Q_3)$ に $\overline{K}$ 上同型である．$\deg(Q_2)+\deg(Q_3)=4$ は射影空間 $\mathbb{P}^4$ の次元以下であるので，系 14 が適用できて，次の (1)，(2) が成り立つ：

(1) $H^1(C,\mathcal{O}_C) \cong H^4(\mathbb{P}^4,\mathcal{O}_{\mathbb{P}^4}(-6))$ は $\mathcal{B} = \left\{\frac{1}{x^2yzvw}, \frac{1}{xy^2zvw}, \frac{1}{xyz^2vw}, \frac{1}{xyzv^2w}, \frac{1}{xyzvw^2}\right\}$ を基底にもつ.

(2) $\Lambda = \{(2,1,1,1,1),(1,2,1,1,1),(1,1,2,1,1),(1,1,1,2,1),(1,1,1,1,2)\}$ であり, 基底 $\mathcal{B}$ に関する F^* の表現行列は $(c_{p\beta^{(j)}-\beta^{(i)}})_{1\le i,j\le 5}$ となる. ここで, $c_{i,j,k,\ell,m}$ は $(Q_1Q_2Q_3)^{p-1}$ の $x^iy^jz^kv^\ell w^m$ の係数で, $\beta^{(1)} = (2,1,1,1,1)$, $\beta^{(2)} = (1,2,1,1,1)$, $\beta^{(3)} = (1,1,2,1,1)$, $\beta^{(4)} = (1,1,1,2,1)$, $\beta^{(5)} = (1,1,1,1,2)$ とおいた.

数値例として, [30, Example 5.1] においてレベル 67 の古典モジュラー曲線を扱っている.

また, 高次元の場合に適用できる例として, K3 曲面を含む Calabi-Yau 多様体（cf. 注意 15）の中には射影空間内の完全交叉で実現できるものもあり, そのような場合は系 14 後半の特別な場合にあたる. 例えば $\mathbb{P}^5$ 内の二次曲面 3 つ, あるいは三次曲面 2 つの非特異な完全交叉は, それぞれ K3 曲面, Calabi-Yau 3-fold であり, これらは系 14 後半の条件 $\sum_{j=1}^m \deg(f_j) = r+1$ を満たす. 従って系 14 により $d = \dim(X)$ に対し $F^* : H^d(X,\mathcal{O}_X) \longrightarrow H^d(X,\mathcal{O}_X)$ を計算できる. 実際, [1, Propostion 6.1] において, $\mathbb{P}^5$ 内のある三次曲面 2 つの完全交叉として定義される $\overline{\mathbb{F}_3}$ 上の Calabi-Yau 3-fold に対し, F^* の計算に系 14 が用いられている（原著 [30] の対応する命題 [30, Proposition 4.1] が引用されている）.

例 21 (命題 16 を適用できる場合と例)
X の次元を d とし, $d_j = \deg(f_j)$ とする. 命題 16 (2) を適用できるのは, $\sum_{j=1}^{r-d} d_j = r+2$ および $\ell = 1$ を満たすときであり, この条件を満たす $(d_1,\dots,d_{r-d})$ が存在するのは $\frac{r-3}{2} \le d \le r-2$（あるいは同値な条件である $d+2 \le r \le 2d+3$）が成り立つとき, かつそのときに限る. 例えば, $d = 1$, すなわち X が曲線の場合は $r = 3,4,5$ である. 初等的な組み合わせの計算によって, それぞれの r に対する $(d_1,\dots,d_{r-1})$ は以下の通りとわかる：

- $(1,4)$；$\mathbb{P}^3$ 内の種数 3 の曲線.
- $(1,2,3)$；$\mathbb{P}^4$ 内の種数 4 の曲線.
- $(1,2,2,2)$；$\mathbb{P}^5$ 内の種数 5 の曲線.

命題 16 の前の段落でも述べたが, 最初のケースである $\mathbb{P}^3$ 内の $(1,4)$ 型の完全交叉として定義される種数 3 曲線については, [9, Section 4] において F^* の表現行列を計算する公式（命題 16 の特別な場合）が示されており, その公式は与えられた p-rank の値をもつ曲線や Prym 多様体の構成に応用されている.

4 今後の課題

最後に今後の課題を述べる. 記号は前節と同様に, K を標数 $p > 2$ の体, $X \subset \mathbb{P}^r$ を K 上の射影スキームで斉次多項式 $f_1,\dots,f_m \in K[x_0,\dots,x_r]$ によって定義されるものとし, 以下 $F^* : H^q(X,\mathcal{O}_X) \longrightarrow H^q(X,\mathcal{O}_X)$ を絶対フロベニウスの作用とする.

1. **提案手法（アルゴリズム 11, 特に自由分解計算）のより精密な計算量評価：**
   定理 10 におけるアルゴリズム 11 の計算量評価では, Step A が考慮されていない. 特に, X の座標環 $K[x_0,\dots,x_r]/\langle f_1,\dots,f_m\rangle$ の自由分解 $\mathbf{F}_\bullet$ の計算量については, 注意 7 (2) と同様

の理由である．多項式環上の加群の自由分解を計算する基本的な方法は [10]，[28, Section 4.8]，[21, Section 2.5] などに記されており，その改良がこれまで多く提案され（e.g., [43], [44], [6], [35], [17], [34]），実験による計算時間の振る舞いについては報告がなされているが，入力パラメータを用いた明示的な計算量の評価式は得られていない．一方で，本研究で計算の対象としているコホモロジー群は（幾何的）同型に関する不変量であるため，その計算量もやはり X や $\mathbf{F}_\bullet$ がもつ不変量を漸近パラメータとして評価されるべきである．従ってまず，そのような不変量を用いて自由分解の計算量を評価することが必要であり，それによって提案手法についても精密な計算量評価を与えることができると考えられる．

2. **完全交叉に対する計算の高速化：**
   X が完全交叉で $q = \dim(X)$ のとき，$h := f_1 \cdots f_m$ とおくと，フロベニウス作用 F^* は h^{p-1} を用いて記述できる（命題 13）．特に系 14 の状況では，F^* の表現行列 H は h^{p-1} における g^2 個の係数で与えられる．従って H の計算量は $K[x_0, \ldots, x_r]$ における積とべき乗のコストで上から bound できるが，実際には h^{p-1} の全ての係数を求める必要はなく一部の係数を求めればよいので，そのための効率的な計算アルゴリズムの開発が今後の課題となる．先行研究においても，アファイン平面曲線モデル $y^2 = f(x)$（$f(x)$ は K 上の $2g+1$ または $2g+2$ 次一変数多項式）で与えられる超楕円曲線については，F^* の表現行列（厳密には双対概念にあたる Cartier-Manin 行列 [7]，[36]）は $f^{(p-1)/2}$ の g^2 個の係数で決定されることがわかっており（cf. [39]，[47]），[27]，[23] などにおいて高速なアルゴリズムが提案されている．これらのアルゴリズムは非斉次一変数多項式 f の累乗 f^n と f^{n-1} の係数間の線形漸化式に基づいている [4]．従って h のような斉次多変数多項式の場合にも，類似の線形漸化式を構成できれば，h^{p-1} の g^2 個の係数の計算を効率化できる可能性があると考えられる．

謝　辞

この度，奨励賞という非常に名誉ある賞を授与いただいた事に対して，日本数式処理学会の関係者の方々に心より御礼申し上げます．本大会を通して参加者の皆様より，本研究の進展に大きく繋がるコメントを数多く賜りました．重ねて深く感謝申し上げます．また，貴重なお時間を割き本論文を精査いただき，大変有益なコメントをくださいました査読者の方々に深く御礼申し上げます．特に，査読者のお一方からは，注意 8 に述べたホモロジー代数を用いた極小自由分解の計算方法などを教えていただきました．本研究は科学研究費補助金（18H05836）・基金（19K21026，20K14301）の助成を受けて行われました．

参 考 文 献

[1] Addington, N., Bragg, D. and Petrov, A: *Hodge numbers are not derived invariants in positive characteristic*, Math. Ann., 2022.

[2] Baker, M.: *Cartier points on curves*, International Mathematics Research Notices, **2000**, Issue 7, pp. 353–370, 2000.

[3] Bosma, W., Cannon, J. and Playoust, C.: *The Magma algebra system. I. The user language*, J. Symb. Comput., **24**, pp. 235–265, 1997.

[4] Bostan, A., Gaudry, P. and Schost, É.: *Linear recurrences with polynomial coefficients and computation of the Cartier-Manin operator on hyperelliptic curves*, In: Mullen G. L., Poli A. and Stichtenoth, H. (eds), Finite Fields and Applications. Fq 2003, Lecture Notes in Computer Science, **2948**, pp. 40–58, Springer, Berlin, Heidelberg.

[5] Bruin, P. and Najman, F.: *Hyperelliptic modular curves $X_0(n)$ and isogenies of elliptic curves of quadratic fields*, LMS J. Comput. Math., **18** (1), pp. 578–602, 2015.

[6] Capani, A., De Dominicis, G., Niesi, G. and Robbiano, L.: *Computing minimal finite free resolutions*, Journal of Pure and Applied Algebra, **117**-**118**, pp. 105–117, 1997.

[7] Cartier, P.: *Questions de rationalite des diviseurs en geometrie algebrique*, Bull. Soc. Math. France, **86** (1958), pp. 177–251.

[8] Castryck, W., Decru, T. and Smith, B.: *Hash functions from superspecial genus-2 curves using Richelot isogenies*, Journal of Mathematical Cryptology, **14**, no. 1, 2020, pp. 268–292.

[9] Celik, T. O., Elias, Y., Gunes, B., Newton, R., Ozman, E., Pries, R. and Thomas, L.: *Non-Ordinary curves with a Prym variety of low p-rank*, In: Bouw I., Ozman E., Johnson-Leung J. and Newton R. (eds), Women in Numbers Europe II. Association for Women in Mathematics Series, **11**, pp. 117–158, Springer, Cham, 2018.

[10] Cox, D., Little, J. and O'shea, D.: *Using Algebraic Geometry*, GTM **185**, Springer-Verlag, New York – Berlin, 1998.

[11] Decker, W. and Eisenbud, D.: *Sheaf Algorithm Using the Exterior Algebra*, In: Eisenbud, D., Grayson, D. R., Stillman, M. and Sturmfels, B. (eds.), *Computations in Algebraic Geometry with Macaulay2*, pp. 215–249, Springer-Verlag, 2002.

[12] Dwork, B.: *On the rationality of the zeta function of an algebraic variety*, American Journal of Mathematics, **82**, No. 3, pp. 631-〓 648, 1960.

[13] Eisenbud, D.: *The Geometry of Syzygies - A Second Course in Algebraic Geometry and Commutative Algebra* -, GTM **229**, Springer, 2005.

[14] Eisenbud, D.: Chapter 8: Computing cohomology, pp. 219–226, In: Vasconcelos, W.: *Computational Methods in Commutative Algebra and Algebraic Geometry*, Algorithms and Computation in Mathematics, **2**, Springer, 1998.

[15] Eisenbud, D., Fløystad, G. and Schreyer F.-O.: *Sheaf Cohomology and Free Resolutions over Exterior Algebras*, Trans. Amer. Math. Soc., **355**, no. 11, pp. 4397–4426, 2003.

[16] Ekedahl, T.: *On supersingular curves and abelian varieties.* Math. Scand., **60** (1987), pp. 151–178.

[17] Erocal, B., Motsak, O., Schreyer, F.-O. and Steenpass, A.: *Refined Algorithms to Compute Syzygies*, J. Symb. Comput., **74** (2016), pp. 308–327.

[18] Galbraith, S. D.: *Mathematics in Public Key Cryptography*, Cambridge University Press,

2012.

[19] Gaudry, P. and Schost, É.: *Genus 2 point counting over prime fields*, J. Symb. Comput., **47** (4), pp. 368–400, 2012.

[20] González, J.: *Hasse-Witt matrices for the Fermat curves of prime degree*, Tohoku Math. J., **49** (1997), no. 2, pp. 149–163. MR 1447179 (98b:11064)

[21] Greuel, G.-M. and Pfister, G.: *A Singular Introduction to Commutative Algebra*, Second edition, Springer (2007).

[22] Hartshorne, R.: *Algebraic Geometry*, GTM **52**, Springer-Verlag, 1977.

[23] Harvey, D. and Sutherland, A. V.: *Computing Hasse-Witt matrices of hyperelliptic curves in average polynomial time*, LMS J. of Computation and Mathematics, **17**, pp. 257–273, 2014.

[24] Hasse, H. and Witt, E.: *Zyklische unverzweigte Erweiterungskörper vom Primzahlgrade p über einem algebraischen Funktionenkörper der Charakteristik p*, Monatsh. für Math. u. Phys., **43** (1936), pp. 477–493.

[25] Katz, N.: *Une formule de congruence pour la fonction ζ*, In: Groupes de Monodromie en Géométrie Algébrique. Lecture Notes in Mathematics, **340**. Springer, Berlin, Heidelberg, 1973.

[26] Koblitz, N.: *p-adic variation of the zeta-function over families of varieties defined over finite fields*, Compositio Mathematica, **31** (1975) no. 2, pp. 119-218.

[27] Komoto, H., Kozaki, S. and Matsuo, K.: *Improvements in the computation of the Hasse-Witt matrix*, JSIAM Letters, **2**, pp. 17–20, 2010.

[28] Kreuzer, M. and Robbiano, L.: *Computational Commutative Algebra 2*, Springer–Verlag Berlin Heidelberg, 2005.

[29] Kudo, M.: *Analysis of an algorithm to compute the cohomology groups of coherent sheaves and its applications*, Japan J. Indust. Appl. Math., **34** (1), pp. 1–40, 2017.

[30] Kudo, M.: *Computing representation matrices for the action of Frobenius on cohomology groups*, J. Symb. Comput., **109**, pp. 441–464, 2022.

[31] Kudo, M. and Harashita, S.: *Computational approach to enumerate non-hyperelliptic superspecial curves of genus 4*, Tokyo Journal of Mathematics, **43**, Number 1, pp. 259–278, 2020.

[32] Kudo, M. and Harashita, S.: *Superspecial curves of genus* 4 *in small characteristic*, Finite Fields and Their Applications, **45**, pp. 131–169, 2017.

[33] Kudo, M., Harashita, S. and Senda, H.: *Automorphism groups of superspecial curves of genus 4 over* $\mathbb{F}_{11}$, Journal of Pure and Applied Algebra, **224**, Issue 9, 19 pages, 2020.

[34] La Scala, R.: *Computing minimal free resolutions of right modules over noncommutative algebras*, Journal of Algebra, **478**, pp. 458–483, 2017.

[35] La Scala, R. and Stillman, M.: *Strategies for Computing Minimal Free Resolutions*, J. Symb. Comput., **26** (4) (1998), pp. 409–431.

[36] Manin, J. I.: *On the theory of Abelian varieties over fields of finite characteristic*, Izo. Akad. Auk SSSR Sev. Mat. **26** (1962), pp.frm-e81–292 (Russian.)

[37] Manin, J. I.: *The Hasse-Witt matrix of an algebraic curve*, AMS Translations, Series 2 **45** (1965), pp. 245–264, (originally published in Izv. Akad. Nauk SSSR Ser. Mat., **25** (1961), pp. 153–172). MR 0124324 (23 #A1638)

[38] 丸山正樹: グレブナー基底とその応用, 共立出版, 2002.

[39] Miller, L.: *The Hasse-Witt-matrix of special projective varieties*, Pasific Journal of Mathematics, **43** (1972), No. 2, pp. 443-〓 455

[40] Novoselov, S., A.: *Counting points on hyperelliptic curves of type* $y^2 = x^{2g+1} + ax^{g+1} + bx$, Finite Fields and Their Applications, **68**, 101757, 2020.

[41] Patakfalvi, Z. and Zdanowicz, M.: *Ordinary varieties with trivial canonical bundle are not uniruled*, Math. Ann., **380**, pp. 1767-〓 1799 (2021).

[42] Serre, J.-P.: *Faisceaux algébriques cohérents*, Annals of Math., **61**, pp. 197–278, 1955.

[43] Schreyer, F.-O.: *Die Berechnung von Syzygien mit dem verallgemeinerten Weierstrasschen Divisionssatz*, Diplomarbeit, Hamburg, 1980.

[44] Schreyer, F.-O.: *A Standard Basis Approach to Syzygies of Canonical Curves*, J. Reine Angew. Math., **421**, pp. 83–123, 1991.

[45] Smith, G. G.: *Computing Global Extension Module*, J. Symb. Comput., **29**, pp. 729–746, 2000.

[46] Toki, K.: *On Hasse-Witt matrices of Fermat varieties*, Hiroshima Math. J., **18** (1988), pp. 95–111.

[47] Yui, N.: *On the Jacobian varieties of hyperelliptic curves over fields of characterisctic* $p > 2$, Journal of algebra, **52**, pp. 378–410, 1978.