Study on Computational Algebraic Geometry : Computing the Frobenius on sheaf cohomology and its applications

工藤, 桃成

https://doi.org/10.15017/1866254

出版情報：九州大学, 2017, 博士（機能数理学）, 課程博士
バージョン：
権利関係：

Study on Computational Algebraic Geometry: Computing the Frobenius on sheaf cohomology and its applications

Momonari Kudo

A disssertation submitted to
Kyushu University
for the degree of
Doctor of Philosophy (Mathematics)
July, 2017
Supervisor: Associate Professor Masaya Yasuda

Contents

Chapter 1

Introduction

Computational Algebraic Geometry (*CAG* for short) is a branch of mathematics that studies computational approaches in algebraic geometry. Specifically CAG aims to develop algorithms for computing mathematical objects such as the locus of the zeros of multivariate systems, singularities of algebraic varieties and the cohomology groups of coherent sheaves. As developed mathematical softwares, these computational methods have become more useful and helpful to study algebraic varieties; using these methods over computer algebra systems enables us to obtain many new results.

To know the structure of an algebraic variety, it is important to investigate its invariants. The *cohomology groups* of coherent sheaves play central roles, and they define many kinds of invariants such as genus, Kodaira dimension, Hilbert function and Hasse-Witt matrix. Therefore, algorithms for computing the cohomology groups shall help us to determine such invariants.

Chapter 2 gives a brief review of theory of the cohomology groups of coherent sheaves. Let K be a field, and $S = K[x_0, \ldots, x_n]$ the polynomial ring of $n+1$ variables over K. For a graded K-vector space V, let V_d denote its subspace of degree d. We denote by $\mathbf{P}^n = \mathrm{Proj}(S)$ the projective n-space over K, and by $\mathcal{O}_{\mathbf{P}^n}$ its structure sheaf. For a sheaf $\mathcal{H}$ on $\mathbf{P}^n$, let $H^j(\mathbf{P}^n, \mathcal{H})$ denote its j-th cohomology group. Serre [51] first proved *theoretically* that the cohomolgy groups can be computed. Specifically he showed the *local duality*, that is, for any coherent sheaf $\mathcal{F}$ on $\mathbf{P}^n$, we have the isomorphism

$$H^j(\mathbf{P}^n, \mathcal{F}(m)) \cong \left(\mathrm{Ext}^{n-j}(\mathcal{F}, \mathcal{O}_{\mathbf{P}^n})^\vee\right)_{-n-1-m} \tag{1.0.1}$$

of K-vector spaces for arbitrary j and m, where $\mathcal{F}(m)$ denotes the m-th Serre twist of $\mathcal{F}$, say $\mathcal{F}(m) = \mathcal{F} \otimes_{\mathcal{O}_{\mathbf{P}^n}} \mathcal{O}_{\mathbf{P}^n}(m)$, and $(\cdot)^\vee$ denotes the K-vector space dual functor. In particular, for a finitely generated graded S-module $M = \bigoplus_{d\in\mathbb{Z}} M_d$ with $\mathcal{F} = M^\sim$, the isomorphism (1.0.1) derives the isomorphism

$$\left(\mathrm{Ext}^{n-j}(\mathcal{F}, \mathcal{O}_{\mathbf{P}^n})^\vee\right)_{-n-1-m} \cong \left(\mathrm{Ext}^{n-j}(M, S)^\vee\right)_{-n-1-m} \tag{1.0.2}$$

of K-vector spaces, where $M^\sim$ is the sheaf associated to the S-module M. In the literature of CAG, Eisenbud [19], Smith [53] and Maruyama [49, Chapter 6] proposed methods for computing the cohomology groups based on Serre's local duality. Their methods compute the dimensions of the right hand side of (1.0.2) by computing a free resolution for the finitely generated graded module M over the polynomial ring. On the other hand, Eisenbud-Fløystad-Schreyer [21] gave a method based on the Bernstein-Gel'fand-Gel'fand correspondence [4]. Specifically, Eisenbud-Fløystad-Schreyer's method computes the *Tate resolution* of $\mathcal{F}$, which is a doubly infinite complex of graded free

modules over an exterior algebra. Since the dimensions of $H^j(\mathbf{P}^n, \mathcal{F}(m))$ appear as values in the Betti diagram of the Tate resolution of $\mathcal{F}$, one can obtain the dimensions by computing the Tate resolution.

In Chapter 3, we review these two main strategies for computing the cohomology groups, and compare the two methods over Magma [6], [9], a computer algebra system. This chapter includes the result [41] by the author on analyzing the first method [19], [53], [49, Chapter 6]. The first method is called the *polynomial ring-based method* (or the *local cohomology based-method*). Specifically, in Maruyama's polynomial ring-based method [49, Chapter 6], computing a free resolution for M of the form

$$0 \longrightarrow P_{n+1} \longrightarrow \cdots \longrightarrow P_1 \longrightarrow P_0 \longrightarrow M \longrightarrow 0,$$

one has the exact sequence

$$0 \longrightarrow \mathcal{G}_{n+1} \xrightarrow{\Phi_{n+1}} \cdots \xrightarrow{\Phi_2} \mathcal{G}_1 \xrightarrow{\Phi_1} \mathcal{G}_0 \xrightarrow{\Phi_0} \mathcal{F} \longrightarrow 0$$

of coherent sheaves, where each P_i is a free S-module, and where each $\mathcal{G}_i$ is a locally free sheaf of the form $\mathcal{G}_i = \bigoplus_{j=1}^{t_i} \mathcal{O}_{\mathbf{P}^n}(m_j^{(i)})$ for some integers t_i and $m_j^{(i)}$. Maruyama [49, Chapter 6] showed that computing $H^0(\mathbf{P}^n, \mathcal{G}_i)$, $H^n(\mathbf{P}^n, \mathcal{G}_i)$, $H^0(\Phi_i)$ and $H^n(\Phi_i)$ enables one to compute $\dim_K H^j(\mathbf{P}^n, \mathcal{F}(m))$. In this thesis, we focus on Maruyama's method, and write down his method as a concrete algorithm. The second method [21] is called the *exterior algebra-based method*. In the exterior algebra-based method, we first construct the following doubly infinite complex of free modules over $E = \bigwedge V$:

$$\cdots \longrightarrow \mathrm{Hom}_K(E, M_d) \longrightarrow \mathrm{Hom}_K(E, M_{d+1}) \longrightarrow \cdots,$$

where V is a K-vector space of dimension $n+1$. As Eisenbud-Fløystad-Schreyer showed in [21], the truncated complex $\mathbf{R}(M)_{\geq d}$ is acyclic if and only if d is greater than or equal to the Castelnuovo-Mumford regularity $\mathrm{reg}(M)$ of M. Taking a free resolution of the kernel of $\mathrm{Hom}_K(E, M_{r+1}) \longrightarrow \mathrm{Hom}_K(E, M_{r+2})$ for $r = \mathrm{reg}(M)$, one gets a doubly infinite exact sequence of free E-modules, say

$$\mathbf{T}(M): \qquad \cdots \longrightarrow T_r \longrightarrow T_{r+1} = \mathrm{Hom}_K(E, M_{r+1}) \longrightarrow \mathrm{Hom}_K(E, M_{r+2}) = T_{r+2} \longrightarrow \cdots$$

where each T_i is a free E-module. We call $\mathbf{T}(M)$ the *Tate resolution* of M. Eisenbud-Fløystad-Schreyer proved in [21] that $\dim_K H^j(\mathbf{P}^n, \mathcal{F}(m))$ are included in the Betti diagram of $\mathbf{T}(M)$, and thus one can obtain the values of the dimensions by computing a free resolution of the E-module $\mathrm{Ker}\,(\mathrm{Hom}_K(E, M_{r+1}) \longrightarrow \mathrm{Hom}_K(E, M_{r+2}))$. From a viewpoint of efficient computation, we observe that the cost of the exterior algebra-based method might be cheaper than the polynomial ring-based one since the computation of free resolutions over E is more efficient than that over S. However, the exterior algebra-based method might require large memory usage, since Tate resolutions can become big structures because of their doubly infiniteness. We demonstrate this observation by computing several examples over Magma. In our experiments, we used our implementation of the polynomial ring-based method, whereas the exterior algebra-method is adopted in Magma's built-in function[1].

[1]The exterior algebra-method computes free resolutions via the Gröbner basis computation, which might be costly for large n. To conduct experiments for large n, it requires to efficiently compute Gröbner bases. We use Magma, since it is well-known to have efficient implementations of the F_4 algorithm [23], which is the most efficient algorithm for computing Gröbner bases.

For investigating the structure of algebraic varieties, it is helpful to compute *other* objects, such as Hasse-Witt invariants, and differential maps of cohomology groups, derived from their cohomology groups. For such objects, the polynomial ring-based method is very useful since it computes explicit representations such as concrete bases of the cohomology groups. In particular, in algebraic geometry over a field with positive characteristic, the Frobenius map on an algebraic variety plays an important role to clarify the structure of the variety. Specifically computing the *Frobenius action* on the cohomology groups helps us to determine the number of rational points of the algebraic variety.

In Chapter 4, given a projective variety $X = V(f_1, \ldots, f_t) \subset \mathbf{P}^n$ over a perfect field with characteristic p, we shall give two algorithms for computing the Frobenius on $H^j(X, \mathcal{O}_X)$ based on the polynomial ring-based method for computing the cohomology groups. While several existing algorithms work for specific varieties, our first algorithm works for *arbitrary* projective varieties. Specifically for homogeneous polynomials $f_1, \ldots, f_t \in S$ defining X, our algorithm computes the representation matrix for the Frobenius on $H^j(X, \mathcal{O}_X)$ for $1 \leq j \leq n$. Our second algorithm works when X is a complete intersection, i.e., $(f_1, \ldots, f_t)$ is an S-regular sequence. In this case, we can compute the representation matrix from certain coefficients in $(f_1 \cdots f_t)^{p-1}$. Applying this computational method for complete intersections, we have results on the (non-)existence of certain special curves over a field with characteristic p in Chapter 5.

In Chapter 5, we shall study *superspecial curves*, where a superspecial curve is defined as a (non-singular) projective variety of dimension 1 whose Jacobian is isomorphic to a product of supersingular elliptic curves over the algebraic closure. Specifically we investigate the (non-)existence of superspecial curves of genus 4 in characteristic $3 \leq p \leq 11$. Based on our algorithms given in Chapter 4, we also present algorithms to enumerate (nonhyperelliptic) superspecial curves of genus 4. Using these enumeration algorithms, one gets explicit defining equations of superspecial curves of genus 4. In this chapter, we enumerate superspecial curves of genus 4 over $\mathbb{F}_5$, $\mathbb{F}_{25}$, $\mathbb{F}_7$, $\mathbb{F}_{49}$ and $\mathbb{F}_{11}$. In particular, we shall prove the non-existence of superspecial curves in characteristic $p = 7$, which also implies that there does not exist any maximal curve over finite fields $\mathbb{F}_q$ with $q = p^s$. Here a curve is said to be maximal (resp. minimal) if it attains the Hasse-Weil upper (resp. lower) bound of the number of $\mathbb{F}_q$-rational points. Our enumeration algorithms shall be useful to study maximal and minimal curves over finite fields. This chapter involves the results in [43], [44] and [45], which are joint works with Shushi Harashita.

Chapter 6 concludes our works, and states our future work.

Acknowledgments

My deepest thanks go to my supervisor Masaya Yasuda for helpful comments, discussion, suggestions and editorial comments on this thesis.

I also thank Kazuhiro Yokoyama, Shushi Harashita, Eiichi Sato, Takeshi Shimoyama and Yuichiro Taguchi for helpful comments on this study.

I am very grateful to Shun'ichi Yokoyama for helpful comments on this thesis. He taught me many about computational mathematics. Thanks to his guidance to computational mathematics, I started to learn this area in earnest when I was a first degree-student of PhD course at Kyushu University.

Thanks go to Wolfram Decker and Gerhard Pfister for their help during my stay at the Singular group of the University of Kaiserslautern from July 2016 to August 2016.

Thanks go to Allan Steel, John Cannon and Steve Donnelly for their help and comments on this study during my stay at the Magma group of University of Sydney from February 2016 to March 2016.

This thesis is dedicated to the late Masaki Maruyama. I learned many about Gröbner bases and their applications to algebraic geometry from his Japanese book [49]. I am honored to write a paper [41] on analyzing a computational method written in a chapter of his book.

I thank my family and all my friends for their support and patience with me.

Chapter 2

Preliminaries

In this chapter, we introduce basic notions and tools that are used in main chapters (Chapters 3 – 5) of this thesis. Specifically, the first section of this chapter gives a review on basic facts in abstract algebra such as modules, exterior algebras, and their properties. In the second and the third sections, we shall study fundamental properties of the cohomology groups of coherent sheaves on a projective space. In particular, we focus on *resolutions* of coherent sheaves (or finitely generated graded modules). The fourth and fifth sections describe Frobenius morphisms on schemes and the Frobenius functor for the category of modules.

2.1 Basic facts in abstract algebra

Let K be a field and V a K-vector space of dimension $n+1$. Let $W = V^*$ denote its dual space. Throughout this chapter, we denote by $S := \mathrm{Sym}(W)$ the symmetric algebra of W. Note that S is isomorphic to the polynomial ring in $n+1$ variables over K, and thus we identify S with $K[x_0, \ldots, x_n]$. Let $\mathbf{P}^n = \mathrm{Proj}(S)$ be the projective n-space over K. For a scheme $X \subset \mathbf{P}^n$, let $\mathcal{O}_X$ denote its structure sheaf. For an $\mathcal{O}_X$-module sheaf $\mathcal{F}$ on X, let $H^q(X, \mathcal{F})$ denote the q-th cohomology group of $\mathcal{F}$, where q is an integer. The ℓ-th Serre twist $\mathcal{F} \otimes_{\mathcal{O}_X} \mathcal{O}_X(\ell)$ is denoted by $\mathcal{F}(\ell)$. For a graded module M and an integer ℓ, we denote by $M(\ell)$ its ℓ-twist given by $M(\ell)_t = M_{\ell+t}$.

We give the definitions of the Tor and Ext functors of homological algebra. First, we define the Tor functors to be derived functors of the tensor product functor. Let R be a commutative ring with unity. Let A and B be R-modules. For a projective resolution

$$\cdots \longrightarrow P_2 \longrightarrow P_1 \longrightarrow P_0 \longrightarrow A \longrightarrow 0,$$

we have a chain complex

$$\cdots \longrightarrow P_2 \otimes_R B \longrightarrow P_1 \otimes_R B \longrightarrow P_0 \otimes_R B \longrightarrow 0$$

tensoring with B over R. Note that the tensor product functor $(\cdot)_R \otimes B$ is right exact. We define the j-th *torsion module*, denoted by $\mathrm{Tor}_j^R(A, B)$, to be the j-th homology group of the chain complex $P_\bullet \otimes_R B$, i.e.,

$$\mathrm{Tor}_j^R(A, B) := \mathrm{Ker}(P_j \otimes_R B \to P_{j-1} \otimes_R B)/\mathrm{Im}(P_{j+1} \otimes_R B \to P_j \otimes_R B).$$

The R-module $\mathrm{Tor}_j^R(A,B)$ does not depend on a choice of a projective resolution of A. Next, we define the Ext functors to be derived functors of Hom functors. Let

$$0 \longrightarrow B \longrightarrow Q_0 \longrightarrow Q_1 \longrightarrow Q_2 \longrightarrow \cdots$$

be an injective resolution of B. Taking the left-exact functor $\mathrm{Hom}_R(A,\cdot)$, we have the following cochain complex:

$$0 \longrightarrow \mathrm{Hom}_R(A,Q_0) \longrightarrow \mathrm{Hom}_R(A,Q_1) \longrightarrow \mathrm{Hom}_R(A,Q_2) \longrightarrow \cdots .$$

We define the j-th *extension module*, denoted by $\mathrm{Ext}_j^R(A,B)$, to be the j-th cohomology group of the cochain complex $\mathrm{Hom}_R(A,Q_\bullet)$, i.e.,

$$\mathrm{Ext}_j^R(A,B) := \mathrm{Ker}(\mathrm{Hom}_R(A,Q_j) \longrightarrow \mathrm{Hom}_R(A,Q_{j+1}))/\mathrm{Im}(\mathrm{Hom}_R(A,Q_{j-1}) \longrightarrow \mathrm{Hom}_R(A,Q_j)).$$

The R-module $\mathrm{Ext}_j^R(A,B)$ does not depend on a choice of an injective resolution of B. We have another definition of Ext. Let

$$\cdots \longrightarrow R_2 \longrightarrow R_1 \longrightarrow R_0 \longrightarrow A \longrightarrow 0$$

be a projective resolution of A. Taking the contravariant left-exact functor $\mathrm{Hom}_R(\cdot,B)$, we have the following cochain complex:

$$0 \longrightarrow \mathrm{Hom}_R(R_0,B) \longrightarrow \mathrm{Hom}_R(R_1,B) \longrightarrow \mathrm{Hom}_R(R_2,B) \longrightarrow \cdots .$$

We define $\mathrm{Ext}_R^j(A,B)$ to be the j-th cohomology group of the cochain complex $\mathrm{Hom}_R(R_\bullet,B)$, i.e.,

$$\mathrm{Ext}_R^j(A,B) := \mathrm{Ker}(\mathrm{Hom}_R(A,Q_j) \longrightarrow \mathrm{Hom}_R(A,Q_{j+1}))/\mathrm{Im}(\mathrm{Hom}_R(A,Q_{j-1}) \longrightarrow \mathrm{Hom}_R(A,Q_j)).$$

The R-module $\mathrm{Ext}_R^j(A,B)$ does not depend on a choice of a projective resolution of A. It is known that the above two extension modules are isomorphic to each other, i.e.,

$$\mathrm{Ext}_j^R(A,B) \cong \mathrm{Ext}_R^j(A,B)$$

as R-modules.

Definition 2.1.1 (Linear free resolutions) Let M be an S-module. A *linear free resolution* of M is a free resolution of the form

$$\cdots \longrightarrow \bigoplus_{j=1}^{\beta_i} S(-n-i) \longrightarrow \cdots \longrightarrow \bigoplus_{j=1}^{\beta_1} S(-n-1) \longrightarrow \bigoplus_{j=1}^{\beta_0} S(-n) \longrightarrow M \longrightarrow 0$$

where $S(\ell)$ denotes the ℓ-twist of the graded ring S given by $S(\ell)_t = S_{\ell+t}$. Note that the representation matrix for each homomorphism in the resolution is a matrix of linear forms. In other words, the i-th syzygy of the linear free resolution of M is generated in degree $n+i$ for each i.

Definition 2.1.2 (Castelnuovo-Mumford regularity) Let $M = \bigoplus_i M_i$ be a finitely generated graded S-module. The *Castelnuovo-Mumford regularity* of M, denoted by $\mathrm{reg}(M)$, is the smallest integer r such that the truncation $M_{\geq r} = \bigoplus_{i \geq r} M_i$ is generated by M_r and such that M_r has a linear free resolution.

We next define *tensor algebras*, *exterior algebras* and *symmetric algebras*.

Definition 2.1.3 (Tensor algebras) Let R be a ring, and M an R-module. The *tensor algebra*, denoted by $T(M)$, is

$$T(M) := \bigoplus_{i\geq 0} M^{\otimes i} = R \oplus M \oplus (M \otimes_R M) \oplus (M \otimes_R M \otimes_R M) \oplus \cdots .$$

Definition 2.1.4 (Exterior algebras) Let R be a ring, and M an R-module. Let $J(M)$ be the two-side ideal generated by the subset $\{x\otimes x : x \in M\}$ of $T(M)$. We have that $\bigwedge M := T(M)/J(M)$ is a graded R-algebra, and that the canonical homomorphism $T(M) \to \bigwedge M$ is a homomorphism of graded R-algebras. For each element $x_1\otimes\cdots\otimes x_k \in T(M)$, we denote by $x_1\wedge\cdots\wedge x_k$ its image in $\bigwedge M$. The graded R-algebra $\bigwedge M$ is called the *exterior algebra* of M. For each d, the degree d homogeneous part of $\bigwedge M$ is $\bigwedge^d M := T(M)_d/J_d(M)$, where $T(M)_d = M^{\otimes d}$ and $J_d(M) = T(M)_d \cap J(M)$.

The multiplication in the exterior algebra $\bigwedge M$ is *alternating* (and thus *antisymmetric*) on elements in M, i.e., $x\wedge x = 0$ for all $x \in M$. Since $(x+y)\wedge(x+y) = (x\wedge x)+(x\wedge y)+(y\wedge x)+(y\wedge y) = (x \wedge y) + (y \wedge x)$, we have $x \wedge y = -y \wedge x$ for all $x, y \in M$.

We show that $\operatorname{rank}_R(\bigwedge M) = 2^t$ if M is free with finite rank t. We denote by $\bigwedge^k M$ the k-th *exterior power*, that is, the R-submodule generated by

$$\{x_1 \wedge \cdots \wedge x_k : x_i \in M\} \subset \bigwedge M.$$

For a basis $\{m_1, \ldots, m_t\}$ of the R-module M, the set

$$\{m_{i_1} \wedge \cdots \wedge m_{i_k} : 0 \leq i_1 < \cdots < i_k \leq t\}$$

is a basis of the K-submodule $\bigwedge^k M$, whose rank equals the binomial coefficient $\binom{t}{k}$. For example, $\{m_1 \wedge \cdots \wedge m_t\}$ is a basis of $\bigwedge^t M$, and thus $\operatorname{rank}_R\left(\bigwedge^t M\right) = 1$. We also have that $\bigwedge^k M = 0$ for $k > t$. Hence

$$\bigwedge M = \bigoplus_{k=0}^{t} \left(\bigwedge^k M\right),$$

and thus $\dim_R(\bigwedge M) = \sum_{k=0}^{t} \binom{t}{k} = 2^t$.

Definition 2.1.5 (Symmetric algebras) Let R be a ring, and M an R-module. Let $I(M)$ be the two-side ideal generated by the subset $\{x \otimes y - y \otimes x : x \in M\}$ of $T(M)$. We have that $\operatorname{Sym}(M) := T(M)/I(M)$ is a graded R-algebra, and that the canonical homomorphism $T(M) \to \operatorname{Sym}(M)$ is a homomorphism of graded R-algebras. The graded R-algebra $\operatorname{Sym}(M)$ is called the *symmetric algebra* of M. For each d, the degree d homogeneous part of $\operatorname{Sym}(M)$ is $\operatorname{Sym}^d(M) := T(M)_d/I_d(M)$, where $T(M)_d = M^{\otimes d}$ and $I_d(M) = T(M)_d \cap I(M)$.

It is known that the symmetric algebra of a free module over a ring is isomorphic to a polynomial ring over the ring.

Proposition 2.1.6 *Let R be a ring, and M a free R-module of rank $n+1$. Let $\{m_0, \ldots, m_n\}$ be an arbitrary basis of M. Then the following is an isomorphism of graded R-algebras:*

$$R[x_0, \ldots, x_n] \to \operatorname{Sym}(M) \ ; \ x_i \mapsto m_i.$$

2.2 Coherent shaves and their cohomology groups

We use the same notation as in the previous section. For a scheme X, a sheaf of $\mathcal{O}_X$-modules $\mathcal{F}$ is said to be *coherent*, or called a *coherent sheaf* if

(1) There exists an affine open covering $\{U_i := \mathrm{Spec}(A_i)\}_i$ for X such that $\mathcal{F}|_{U_i} \cong M_i$ for some A_i-module M_i.

(2) Each M_i is a finitely generated A_i-module.

An important fact is that coherent sheaves are corresponding to finitely generated graded modules: For a coherent sheaf $\mathcal{F}$ on $\mathbf{P}^n = \mathrm{Proj}(S)$, there exists a finitely generated graded S-module M such that $\mathcal{F} = M^{\sim}$, where $M^{\sim}$ denotes the sheaf associated to the S-module M.

For a sheaf of $\mathcal{O}_X$-modules $\mathcal{F}$, its q-th *cohomology groups* are formally defined as follows. First there exists a flabby resolution of $\mathcal{F}$:

$$0 \longrightarrow \mathcal{F} \longrightarrow \mathcal{G}_0 \longrightarrow \mathcal{G}_1 \longrightarrow \mathcal{G}_2 \longrightarrow \mathcal{G}_3 \longrightarrow \cdots .$$

Since the above resolution is exact, we have the following complex of S-modules:

$$0 \longrightarrow \Gamma(X, \mathcal{G}_0) \xrightarrow{\delta^{(0)}} \Gamma(X, \mathcal{G}_1) \xrightarrow{\delta^{(1)}} \Gamma(X, \mathcal{G}_2) \xrightarrow{\delta^{(2)}} \Gamma(X, \mathcal{G}_3) \xrightarrow{\delta^{(3)}} \cdots ,$$

where $\Gamma(X, \mathcal{H})$ denotes the global section for a sheaf $\mathcal{H}$ on the scheme X, and where $\delta^{(q)}$ denotes the q-th differential map for each $q \geq 0$. We here define the q-th cohomology groups of the sheaf $\mathcal{F}$ to be the q-th cohomology groups of the above complex, say

$$H^q(X, \mathcal{F}) := \mathrm{Ker}\left(\delta^{(q)}\right) / \mathrm{Im}\left(\delta^{(q-1)}\right)$$

for $q \geq 0$. The cohomology group does not depend on one's choice of a flabby resolution of $\mathcal{F}$, and hence the above definition is well-defined. Note that the 0-th cohomology group $H^0(X, \mathcal{F})$ is isomorphic to the global section $\Gamma(X, \mathcal{F})$.

In a view of computational points, the notion of *Čech cohomology* gives a useful tool for computing the cohomology groups $H^q(X, \mathcal{F})$. Let $\mathcal{U} = \{U_i\}_{i \in I}$ be an open covering for X. To simplify the notation, we set $U_{i_0,\ldots,i_q} := U_{i_0} \cap U_{i_1} \cap \cdots \cap U_{i_q}$ for each $(i_0, \ldots, i_q) \in I^{q+1}$. For $q \geq 0$, the *Čech q-cochain* is defined by

$$C^q(\mathcal{U}, \mathcal{F}) := \prod_{(i_0,\ldots,i_q) \in I^{q+1} \text{ with } i_0 < \cdots < i_q} \mathcal{F}(U_{i_1,\ldots,i_q}),$$

where $\mathcal{F}(U_{i_0,\ldots,i_q}) = \Gamma(U_{i_0,\ldots,i_q}, \mathcal{F}|_{U_{i_0,\ldots,i_q}})$. We define the q-th differential map $d^{(q)}$ by

$$d^{(q)} \ : \ C^q(\mathcal{U}, \mathcal{F}) \longrightarrow C^{q+1}(\mathcal{U}, \mathcal{F}) \ ; \ (f_{i_0,\ldots,i_q})_{i_0,\ldots,i_q} \mapsto ((d^{(q)} f)_{i_0,\ldots,i_{q+1}})_{i_0,\ldots,i_{q+1}},$$

where

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

One can verify that $d^{(q+1)} \circ d^{(q)} = 0$, and thus the sequence

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

is a complex. With this complex, the q-th Čech cohomology group is defined as follows:

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

Note that the group $H^q(\mathcal{U},\mathcal{F})$ depends on one's choice of the covering $\mathcal{U}$ in general. However, for any separable scheme X with an affine open covering $\mathcal{U}$, the group does not depend on such a choice. In other words, we have

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

for any affine open covering $\mathcal{U}$ for X.

For the n-projective space $X = \mathbf{P}^n = \mathrm{Proj}(S)$ and a line bundle $\mathcal{F} = \mathcal{O}_X(m)$, taking $\mathcal{U}$ to be the Zariski open covering, we can compute $H^q(\mathbf{P}^n, \mathcal{O}_{\mathbf{P}^n}(m))$. In the following, we collect some basic facts on the cohomology groups $H^q(\mathbf{P}^n, \mathcal{O}_{\mathbf{P}^n}(m))$. We grade S by taking S_d to be the set of homogeneous polynomials of degree d. For an integer $m \in \mathbb{Z}$, let $S(m)$ denote the m-twist of S defined by $S(m)_t = S_{m+t}$. Let $S(m)_{x_0\cdots x_n}$ denote the localization of $S(m)$ by the powers of $x_0\cdots x_n$ For an integer ℓ, we denote by $(S(m)_{x_0\cdots x_n})_\ell$ the homogeneous part of degree ℓ of the localization $S(m)_{x_0\cdots x_n}$. In particular, the homogeneous part $(S(m)_{x_0\cdots x_n})_0$ of degree 0 is the vector space over K spanned by the set

$$\left\{ a x_0^{\ell_0}\cdots x_n^{\ell_n} : a \in K, \text{ and } (\ell_0,\ldots,\ell_n) \in \mathbb{Z}^{n+1} \text{ with } \sum_{i=0}^{n} \ell_i = m \right\}.$$

We define L_m to be the subspace

$$\left\langle x_0^{\ell_0}\cdots x_n^{\ell_n} : (\ell_0,\ldots,\ell_n) \in \mathbb{Z}^{n+1} \text{ with } \ell_i \geq 0 \text{ for some } i \text{ and } \sum_{i=0}^{n} \ell_i = m \right\rangle_K$$

of the vector space $(S(m)_{x_0\cdots x_n})_0$.

Theorem 2.2.1 ([33], Theorem 5.1) *With notation as above, we have the following:*

(1) *We have the following isomorphisms of vector spaces over K:*

$$H^0\left(\mathbf{P}^n, \mathcal{O}_{\mathbf{P}^n}(m)\right) \cong \begin{cases} S_m & \text{if } m \geq 0, \\ 0 & \text{if } m < 0. \end{cases}$$

In particular, for each $m \geq 0$, the set

$$\left\{ x_0^{\ell_0}\cdots x_n^{\ell_n} : (\ell_0,\ldots,\ell_n) \in (\mathbb{Z}_{\geq 0})^{n+1} \text{ with } \sum_{i=0}^{n} \ell_i = m \right\}$$

is a basis for the K-vector space $H^0\left(\mathbf{P}^n, \mathcal{O}_{\mathbf{P}^n}(m)\right)$.

(2) *For $0 < q < n$ and arbitrary m, we have $H^q\left(\mathbf{P}^n, \mathcal{O}_{\mathbf{P}^n}(m)\right) = 0$.*

(3) *One has the isomorphism*

$$H^n\left(\mathbf{P}^n, \mathcal{O}_{\mathbf{P}^n}(m)\right) \quad \cong \quad (S(m)_{x_0\cdots x_n})_0 \ / \ L_m \tag{2.2.1}$$

of vector spaces over K. Thus for each $m < 0$, the set

$$\left\{ x_0^{\ell_0} \cdots x_n^{\ell_n} : (\ell_0, \ldots, \ell_n) \in (\mathbb{Z}_{<0})^{n+1} \text{ with } \sum_{i=0}^{n} \ell_i = m \right\}$$

gives rise to a basis for $H^n(\mathbf{P}^n, \mathcal{O}_{\mathbf{P}^n}(m))$ via the above isomorphism (2.2.1).

Corollary 2.2.2 ([33], Theorem 5.1) *One has the following:*

$$\begin{aligned} \dim_K H^0(\mathbf{P}^n, \mathcal{O}_{\mathbf{P}^n}(m)) &= \begin{cases} \binom{m+n}{n} & \text{if } m \geq 0, \\ 0 & \text{if } m < 0. \end{cases} \\ \dim_K H^n(\mathbf{P}^n, \mathcal{O}_{\mathbf{P}^n}(m)) &= \begin{cases} \binom{-m-1}{n} & \text{if } m \leq -n-1, \\ 0 & \text{if } m > -n-1. \end{cases} \end{aligned}$$

For $q \notin \{0, n\}$ and $m \in \mathbb{Z}$, one has $H^q(\mathbf{P}^n, \mathcal{O}_{\mathbf{P}^n}(m)) = 0$.

The problem we shall consider is: Given a finitely generated graded S-module M representing a coherent sheaf $\mathcal{F}$ on $\mathbf{P}^n$, present an algorithm for computing $H^q(\mathbf{P}^n, \mathcal{F}) = H^q(\mathbf{P}^n, M^{\sim})$. As we will see in Chapter 3, computing *resolutions* helps us to compute the cohomology groups. Specifically we have two kinds of resolutions. One is called a *projective resolution* or a *locally free resolution*, and the other is called a *Tate resolution*. We shall study these in the next section.

2.3 Resolutions of coherent sheaves for their cohomology groups

In this section, we give a review on known properties of resolutions of coherent sheaves. The notation is same as in the previous section.

2.3.1 Projective resolutions of coherent sheaves

This subsection reviews some properties on *projective resolutions* (or *locally free resolutions*) of coherent sheaves on the projective n-space $\mathbf{P}^n$. Specifically we shall introduce a result (Theorem 2.3.1) by Maruyama [49, Chapter 6]. As we will see in Section 3.1, this result provides a method for computing the cohomology groups of coherent sheaves on $\mathbf{P}^n$.

As in the previous section, we denote by $\mathbf{P}^n = \mathrm{Proj}(S)$ the projective n-space with $S = K[x_0, \ldots, x_n] \cong \mathrm{Sym}(W)$, and $\mathcal{O}_{\mathbf{P}^n}$ the structure sheaf on $\mathbf{P}^n$. Let $\mathcal{F}$ be a coherent sheaf on $\mathbf{P}^n$. It is straightforward that there exists an exact sequence of the following form:

$$0 \to \bigoplus_{j=1}^{t_{n+1}} \mathcal{O}_{\mathbf{P}^n}\left(m_j^{(n+1)}\right) \to \cdots \to \bigoplus_{j=1}^{t_0} \mathcal{O}_{\mathbf{P}^n}\left(m_j^{(0)}\right) \to \mathcal{F} \to 0. \tag{2.3.1}$$

We interpret $\bigoplus_{j=1}^{t_i} \mathcal{O}_{\mathbf{P}^n}\left(m_j^{(i)}\right)$ as 0 if $t_i = 0$. We set $\mathcal{G}_i := \bigoplus_{j=1}^{t_i} \mathcal{O}_{\mathbf{P}^n}\left(m_j^{(i)}\right)$ and denote by Φ_i the morphism $\mathcal{G}_i \to \mathcal{G}_{i-1}$ for each i. The exact sequence (2.3.1) is called a *projective resolution*, or a *locally free resolution* of the coherent sheaf $\mathcal{F}$.

For a sheaf $\mathcal{H}$ on a topological space, its cohomology groups are, in general, defined by its (canonical) flabby resolution, and the groups can be computed by the flabby resolution (see e.g., [33, Chapter 3]). We have also seen this in Section 2.2. However, one has a *projective* resolution

(2.3.1) for the coherent sheaf $\mathcal{F}$ on $\mathbf{P}^n$, and thus the cohomology groups are computed by the projective resolution without computing any flabby resolution. In this case, the following result enables to compute the cohomology groups.

Theorem 2.3.1 ([49], Chapter 6) *With notation as above, there exist the following isomorphisms of vector spaces over K:*

(1) $H^q(\mathbf{P}^n, \mathcal{F}) \cong \mathrm{Ker}\left(H^n(\Phi_{n-q})\right) / \mathrm{Im}\left(H^n(\Phi_{n-q+1})\right)$ for $1 \leq q \leq n-1$,

(2) $H^n(\mathbf{P}^n, \mathcal{F}) \cong \mathrm{Coker}\left(H^n(\Phi_1)\right)$,

where $H^n(\Phi_i)$ denotes the morphism $H^n(\mathbf{P}^n, \mathcal{G}_i) \longrightarrow H^n(\mathbf{P}^n, \mathcal{G}_{i-1})$ induced by Φ_i for $1 \leq i \leq n+1$.

Proof. See the proof of [41, Theorem 5] for a complete proof (cf. only a sketch of a proof is given in [49, Chapter 6]). □

Theorem 2.3.1 derives the following explicit formulae of the dimensions of the cohomology groups.

Corollary 2.3.2 *We use the same notation as in* Theorem 2.3.1. *We have*

$$\dim_K H^q(\mathbf{P}^n, \mathcal{F}) = \dim_K H^n(\mathbf{P}^n, \mathcal{G}_{n-q}) - \mathrm{rank} H^n(\Phi_{n-q}) - \mathrm{rank} H^n(\Phi_{n-q+1})$$

for $1 \leq q \leq n-1$, and

$$\dim_K H^n(\mathbf{P}^n, \mathcal{F}) = \dim_K H^n(\mathcal{G}_0) - \mathrm{rank} H^n(\Phi_1).$$

Theorem 2.3.1 provides a method for computing $H^q(\mathbf{P}^n, \mathcal{F})$: Once one gets a projective resolution of the form (2.3.1), one can compute a basis and the dimension of $H^q(\mathbf{P}^n, \mathcal{F})$ via the isomorphisms in Theorem 2.3.1. We shall see this in Section 3.1.

2.3.2 Tate resolutions of coherent sheaves

This section gives a review on *Tate resolutions* of coherent sheaves, which exploit a method for computing the cohomology groups of coherent sheaves via Gröbner bases theory over exterior algebras [1]. A key theorem (Theorem 2.3.11) in this section was proved in 2003 by Eisenbud-Fløystad-Schreyer, see [21] for the original paper. See also [14] for detailed description of Tate resolutions.

Let V be a finite-dimensional vector space over K of dimension $n+1$, and $W := V^*$ its dual space. Let $S = \mathrm{Sym}(W)$ be the symmetric algebra on W. Let $\{e_0, \ldots, e_n\}$ and $\{y_0, \ldots, y_n\}$ be dual bases of V and W respectively. Recall from Proposition 2.1.6 that S is isomorphic to $K[x_0, \ldots, x_n]$, the polynomial ring of $n+1$ variables over K. We identify x_i with y_i for each $0 \leq i \leq n$. Let $E = \bigwedge V$ be the exterior algebra on the K-vector space V. We grade S (resp. E) by taking elements of W (resp. V) to have degree 1 (resp. -1). In particular, we have $\deg(x_i) = 1$ and $\deg(e_i) = -1$ for $0 \leq i \leq n$.

Given a graded S-module $M = \bigoplus_{d \in \mathbb{Z}} M_d$, we define $\mathbf{R}(M)$ to be the following complex of E-modules:

$$\mathbf{R}(M): \qquad \cdots \xrightarrow{\phi_{d-1}} \mathrm{Hom}_K(E, M_d) \xrightarrow{\phi_d} \mathrm{Hom}_K(E, M_{d+1}) \xrightarrow{\phi_{d+1}} \cdots,$$

where each $\mathrm{Hom}_K(E, M_d)$ is an E-module via the scaler multiplication $(e, \alpha) \mapsto (e' \mapsto \alpha(e' \wedge e))$ for $e, e' \in E$ and $\alpha \in \mathrm{Hom}_K(E, M_d)$. Here each ϕ_d is a map sending $\alpha \in \mathrm{Hom}_K(E, M_d)$ to the K-linear map

$$E \longrightarrow M_{d+1} \ ; \ e \mapsto \sum_{i=0}^{n} x_i \alpha(e_i \wedge e).$$

Note that $x_i \in W \subset S = \mathrm{Sym}(W)$ and $\alpha(e_i \wedge e) \in M_d$ with $e_i \wedge e \in E$. For simplicity of the notation, we denote by $\omega_E := \mathrm{Hom}_K(E, K)$ the K-vector space dual of E.

An important fact for constructing Tate resolutions is that we have $\mathrm{Hom}_K(E, M_d) \cong M_d \otimes_K \omega_E \cong \omega_E^{m_d}(-d) \cong E^{m_d}(-n-1-d)$ as graded E-modules, where we set $m_d := \dim_K M_d$.

Proposition 2.3.3 ([17], Proposition 7.19) *With notation as above, the graded E-module $\omega_E = \mathrm{Hom}_K(E, K)$ is generated by $\mathrm{Hom}_K\left(\bigwedge^{n+1} V, K\right) = \bigwedge^{n+1} W$. Moreover, we have*

$$\omega_E = \mathrm{Hom}_K(E, K) \cong E \otimes_K \bigwedge^{n+1} W \cong E(-n-1)$$

as graded E-modules.

Proof. Put $I := \{(i_0, \ldots, i_k) : 0 \leq k \leq n+1,\ 0 \leq i_0 < \cdots < i_k \leq n+1\} \cup \{(n+2)\}$. For each $\underline{i} = (i_0, \ldots, i_k) \in I$ with $\underline{i} \neq (n+2)$, we denote by $e_{\underline{i}}$ the monomial $e_{i_0} \wedge \cdots \wedge e_{i_k}$. Put $e_{(n+2)} := 1_E$. For each $\underline{i} \in I$, we denote by $\alpha_{\underline{i}}$ the K-linear map

$$E \to K \ ; \ e = \sum_{\underline{j} \in I} a_{\underline{j}} e_{\underline{j}} \mapsto a_{\underline{i}},$$

where $a_{\underline{j}} \in K$ with $\underline{j} \in I$. It is straightforward that $\{\alpha_{\underline{i}} : \underline{i} \in I\}$ is a basis for the K-vector dual space $\omega_E = \mathrm{Hom}_K(E, K)$. Since $\alpha_{(0,\ldots,n)}$ is a generator of the E-submodule (and K-vector subspace) $\mathrm{Hom}_K\left(\bigwedge^{n+1} V, K\right)$, it suffices to show that $\alpha_{(0,\ldots,n)}$ generates ω_E. Each element $\alpha \in \omega_E$ is written as $\alpha = \sum_{\underline{i} \in I} a_{\underline{i}} \alpha_{\underline{i}}$ for some elements $a_{\underline{i}} \in K$ with $\underline{i} \in I$. Let $e \in E$ be an arbitrary nonzero element. As showed in the proof of [17, Proposition 7.19], for each nonzero element $e' \in E$, there exists $e'' \in E$ such that $e' \wedge e'' = e_{(0,\ldots,n)}$. By this fact, there exists $e' \in E$ such that $e \wedge e' = e_{(0,\ldots,n)}$. Putting $c_{\underline{i}} := \alpha_{\underline{i}}(e)$, we have that

$$\begin{aligned} \alpha(e) = \sum_{\underline{i} \in I} a_{\underline{i}} c_{\underline{i}} &= \sum_{\underline{i} \in I} a_{\underline{i}} c_{\underline{i}} \alpha_{(0,\ldots,n)}(e_{(0,\ldots,n)}) \\ &= \sum_{\underline{i} \in I} a_{\underline{i}} c_{\underline{i}} \alpha_{(0,\ldots,n)}(e \wedge e') \\ &= \sum_{\underline{i} \in I} a_{\underline{i}} c_{\underline{i}} (e' \cdot \alpha_{(0,\ldots,n)})(e), \end{aligned}$$

for each $e \in E$ with $e \neq 0$, and thus

$$\alpha = \sum_{\underline{i} \in I} (a_{\underline{i}} c_{\underline{i}} e') \cdot \alpha_{(0,\ldots,n)}.$$

This shows $\omega_E = \langle \alpha_{(0,\ldots,n)} \rangle_E$, and hence ω_E is a rank 1 free E-module.

Now we have the canonical surjection $E \otimes_K \bigwedge^{n+1} W \to \omega_E \ ; \ (e, \alpha) \mapsto e \cdot \alpha$. Note that this surjection is also a K-linear map. Since both the K-vector spaces $E \otimes_K \bigwedge^{n+1} W$ and ω_E have the same dimension, this surjection is bijective, and hence is an isomorphism of E-modules. Therefore we have

$$\omega_E \cong E \otimes_K \bigwedge^{n+1} W \cong E(-n-1)$$

as graded E-modules. □

Based on Proposition 2.3.3 and its proof, we have the following corollaries.

Corollary 2.3.4 *With notation as above, we have*

$$E(-n-1-d)^{m_d} \cong \omega_E^{m_d}(-d)$$

as graded E-modules via the map

$$e \cdot \mathbf{e}_j \mapsto \left(e \cdot \alpha_{(0,\dots,n)}\right) \cdot \mathbf{e}_j^\vee,$$

which we denote by λ_d. Here $\mathbf{e}_j$ denotes the vector of $E(-n-1-d)^{m_d}$ with 1_E in the j-th coordinate and 0's elsewhere, and $\mathbf{e}_j^\vee$ denotes the dual basis element in $\omega_E^{m_d}(-d)$ corresponding to $\mathbf{e}_j$. In particular, this map sends the basis element $1_E \cdot \mathbf{e}_j$ of the E-module $\omega_E^{m_d}(-d)$ to $\alpha_{(0,\dots,n)} \cdot \mathbf{e}_j^\vee$.

Corollary 2.3.5 *With notation as above, we have*

$$\omega_E^{m_d}(-d) \cong M_d \otimes_K \omega_E$$

as graded E-modules via the map

$$\left(e \cdot \alpha_{(0,\dots,n)}\right) \cdot \mathbf{e}_j^\vee \mapsto y_j \otimes \left(e \cdot \alpha_{(0,\dots,n)}\right),$$

which we denote by μ_d. In particular, this map sends the basis element $\alpha_{(0,\dots,n)} \cdot \mathbf{e}_j^\vee$ of the E-module $\omega_E^{m_d}(-d)$ to $y_j \otimes \alpha_{(0,\dots,n)}$, where $\{y_1, \dots, y_{m_d}\}$ is a basis for the K-vector space M_d.

Corollary 2.3.6 *With notation as above, we have*

$$M_d \otimes_K \omega_E \cong \mathrm{Hom}_K(E, M_d)$$

as graded E-modules via the map

$$m \otimes \psi \mapsto (e \mapsto \psi(e) \cdot m),$$

which we denote by τ_d. In particular, this map sends the basis element $y_j \otimes \alpha_{(0,\dots,n)}$ of the E-module $M_d \otimes_K \omega_E$ to $(e \mapsto \alpha_{(0,\dots,n)}(e) \cdot y_j)$, where $\{y_1, \dots, y_{m_d}\}$ is a basis for the K-vector space M_d.

Proof. It is straightforward that the map is a homomorphism of graded E-modules. It suffices to show that the map is bijective.

First we show that the map is injective. For this, assume that the K-linear map $e \mapsto \psi(e)m$ is the zero map, i.e., $\psi(e)m = 0$ for all $e \in E$, for $m \in M_d$ and $\psi \in \omega_E$. It follows from $\psi(e) \in K$ that $\psi(e) = 0$ for all $e \in E$, or $m = 0$. Thus we have $m \otimes \psi = 0$.

The surjectivity follows from Proposition 2.3.3. □

Corollary 2.3.7 *With notation as above, we have*

$$E(-n-1-d)^{m_d} \cong \omega_E^{m_d}(-d) \cong M_d \otimes_K \mathrm{Hom}_K(E,K) = M_d \otimes_K \omega_E \cong \mathrm{Hom}_K(E, M_d)$$

as graded E-modules.

We define the following homomorphism of E-modules:

$$\phi'_d : M_d \otimes_K \omega_E \longrightarrow M_{d+1} \otimes_K \omega_E \ ; \ m \otimes \alpha \mapsto \sum_{j=0}^{n} (x_j \cdot m) \otimes (e_j \cdot \alpha).$$

With this homomorphism and ϕ_d, we can construct E-homomorphisms $E(-n-1-d)^{m_d} \longrightarrow E(-n-1-d-1)^{m_{d+1}}$ and $\omega_E^{m_d}(-d) \longrightarrow \omega_E^{m_{d+1}}(-d-1)$ such that the following diagram commutes:

$$\begin{array}{ccccccc}
E(-n-1-d)^{m_d} & \xrightarrow{\lambda_d} & \omega_E^{m_d}(-d) & \xrightarrow{\mu_d} & M_d \otimes_K \omega_E & \xrightarrow{\tau_d} & \mathrm{Hom}_K(E, M_d) \\
\downarrow & & \downarrow & & \downarrow{\scriptstyle \phi'_d} & & \downarrow{\scriptstyle \phi_d} \\
E(-n-1-d-1)^{m_{d+1}} & \xrightarrow{\lambda_{d+1}} & \omega_E^{m_{d+1}}(-d-1) & \xrightarrow{\mu_{d+1}} & M_{d+1} \otimes_K \omega_E & \xrightarrow{\tau_{d+1}} & \mathrm{Hom}_K(E, M_{d+1})
\end{array}$$

Theorem 2.3.8 ([21], Corollary 2.4, or [14], Theorem 2.1) *Let M be a finitely generated graded S-module, and r its Castelnuovo-Mumford regularity. Then the complex $\mathbf{R}(M)$ is exact at $\mathrm{Hom}_K(E, M_i)$ for all $i \geq d$ if and only if $d > r$.*

Let r be the Castelnuovo-Mumford regularity of M. For an arbitrary $d > r$, it follows from Theorem 2.3.8 that the truncation of $\mathbf{R}(M)$

$$\mathbf{R}(M)_{\geq d} : \qquad F^{(d)} \xrightarrow{\phi_d} F^{(d+1)} \xrightarrow{\phi_{d+1}} \cdots$$

is exact, where we set $F^{(i)} := \mathrm{Hom}_K(E, M_i) \cong E^{m_i}(-n-1-i)$ (as graded E-modules) with $m_i = \dim_K M_i$.

Definition 2.3.9 (Tate resolutions of modules) With notation as above, let

$$\cdots \longrightarrow \bigoplus_{j=1}^{t_{r-1}} E(-d_j^{(r-1)}) \xrightarrow{\psi_{r-1}} \bigoplus_{j=1}^{t_r} E(-d_j^{(r)}) \xrightarrow{\psi_r} P_{r+1}$$

be a minimal projective resolution of the E-module $P_{r+1} := \mathrm{Ker}(\phi_{r+1})$. The *Tate resolution* of M is an E-free complex $\mathbf{T}(M)$ with vanishing homology (possibly infinite in both directions), given by

$$\cdots \longrightarrow \bigoplus_{j=1}^{t_{r-1}} E(-d_j^{(r-1)}) \xrightarrow{\psi_{r-1}} \bigoplus_{j=1}^{t_r} E(-d_j^{(r)}) \xrightarrow{\psi_r} F^{(r+1)} \xrightarrow{\phi_{r+1}} F^{(r+2)} \xrightarrow{\phi_{r+2}} F^{(r+3)} \longrightarrow \cdots,$$

where $r := \mathrm{reg}(M)$ denotes the Castelnuovo-Mumford regularity of M. Note that the representation matrix for each ϕ_i consists of linear forms in E.

Definition 2.3.10 (Tate resolutions of coherent sheaves) With notation as above, let $\mathcal{F} = M^{\sim}$ be a coherent sheaf on the projective n-space $\mathbf{P}^n = \mathrm{Proj}(S)$, where M is a finitely generated graded S-module. The Tate resolution of the coherent sheaf $\mathcal{F}$ is defined by $\mathbf{T}(\mathcal{F}) := \mathbf{T}(M)$, which depends only on the sheaf associated to M.

Theorem 2.3.11 ([21], Theorem 4.1, or [14], Theorem 3.1) *With notation as above, the term of* $\mathbf{T}(M)$ *with cohomological degree* i *is given by*

$$\bigoplus_{j=0}^{n} H^j(\mathbf{P}^n, \mathcal{F}(i-j)) \otimes_K \omega_E,$$

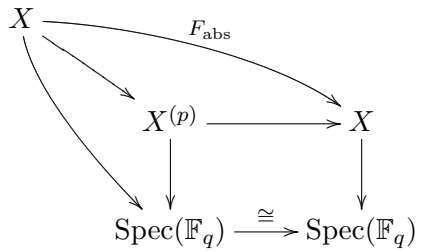
where we regard $H^j(\mathbf{P}^n, \mathcal{F}(i-j))$ *as a linear space concentrated in degree* $i-j$.

2.4 Frobenius morphisms on schemes

In this section, we define the absolute and the relative Frobenius on schemes over a field with characteristic $p > 0$. We denote by $\mathbb{F}_q$ the finite field of q elements, where $q = p^s$ for some $s \geq 1$.

Definition 2.4.1 (Absolute Frobenius) Let X be a scheme over $\mathbb{F}_q$ with its structure morphism $X \to \mathrm{Spec}(\mathbb{F}_q)$. The *absolute Frobenius* on X is a morphism $F_{\mathrm{abs}} : X \to X$ with the identity map on X and $a \mapsto a^p$ on sections.

Definition 2.4.2 (Relative Frobenius) Let X be a scheme over $\mathbb{F}_q$ with its structure morphism $X \to \mathrm{Spec}(\mathbb{F}_q)$. We define $X^{(p)}$ as the fiber product, and the *relative Frobenius* on X as the induced morphism $F_X : X \to X^{(p)}$ in the following commutative diagram:



2.5 Frobenius functor for the category of modules

In this section, we review properties of the Frobenius functor for the category of modules, see e.g., [50] for more details. Let R be a commutative ring of characteristic $p > 0$. Let M be an R-module, and f the Frobenius endomorphism on R. We denote by ${}^fM$ the left R-module structure defined on M by restriction of scalars via f, that is, for $r \in R$ and $m \in M$, we define $r \cdot m := r^p m$.

The Frobenius functor is defined to be a functor from the category of R-modules to itself, and it is defined by the extension of scalers $F_R(M) := M \otimes_R {}^fR$. Lemma 2.5.1 enumerates some fundamental properties of the Frobenius functor $F_R(\cdot)$.

Lemma 2.5.1 *Let* R *be a ring with positive characteristic* p, f *the Frobenius endomorphism on* R, *and* $F_R(\cdot)$ *the Frobenius functor from the category of* R*-modules to itself.*

(1) $F_R(\cdot)$ *is right exact.*

(2) $F_R(R) = R \otimes_R {}^fR \simeq {}^fR \simeq R$ *as* R*-modules via* $a \otimes b \mapsto a \cdot b = a^p b$. *For free modules, one has* $F_R(R^t) = (\bigoplus_{i=1}^t R) \otimes_R {}^fR \simeq ({}^fR)^t \simeq R^t$ *via* $(a_1, \ldots, a_t) \otimes b \mapsto (a_1 \cdot b, \ldots, a_t \cdot b) = (a_1^p b, \ldots, a_t^p b)$.

(3) *For any ideal $J \subset R$, we have $F_R(R/J) = (R/J) \otimes_R {}^fR \simeq R/J_p$, where J_p denotes the ideal generated by the p-th powers of elements of J.*

(4) *Let $\varphi : R^t \to R^s$ be a homomorphism of R-modules, and $(r_{i,j})_{i,j}$ a $t \times s$ matrix which represents φ via standard bases. Then $F_R(\varphi) : R^t \to R^s$ is given by the matrix with entries equal to the p-th powers of the entries of the matrix $(r_{i,j})_{i,j}$.*

Proof. (1) Since tensor product is right exact, the claim holds. (2) Straightforward. (3) The claim follows from $F_R(R/J) = (R/J) \otimes_R {}^fR \simeq R/(J \cdot {}^fR)$. In this case $J \cdot {}^fR := \langle a^p x : a \in J,\ x \in {}^fR \rangle_R = J_p$. (4) Let $\mathbf{e}_i$ be an element of the standard basis of R^t. By (2), we identify $\mathbf{e}_i$ with $\mathbf{e}_i \otimes 1$, and it follows that $F_R(\varphi)(\mathbf{e}_i) = (\varphi \otimes \mathrm{id}_{{}^fR})(\mathbf{e}_i \otimes 1) = (\sum_{j=1}^s r_{i,j}\mathbf{e}_j) \otimes 1 = \sum_{j=1}^s (r_{i,j}\mathbf{e}_j \otimes 1) = \sum_{j=1}^s (r_{i,j} \cdot 1)\mathbf{e}_j = \sum_{j=1}^s r_{i,j}^p \mathbf{e}_j$. □

Theorem 2.5.2 (Kunz's Theorem, [46], Theorems 2.1 and 3.3) *Let R be a local ring of characteristic p. Then R is a regular ring if and only if f^n is flat for all $n > 0$, where f denotes the Frobenius endomorphism on R.*

Since regularity and flatness can be each checked locally, we have the following corollary.

Corollary 2.5.3 *Let R be a ring with positive characteristic p. Then R is a regular ring if and only if f^n is flat for all $n > 0$, where f denotes the Frobenius endomorphism on R.*

Lemma 2.5.4 *Let L be a field with positive characteristic $p > 0$, and $R := L[y_1, \ldots, y_n]$ the polynomial ring with n indeterminates over L. Let $f_1, \ldots, f_t \in R$ be homogeneous polynomials with $d_j^{(1)} = \deg(f_j)$ for $1 \le j \le t$, and $J \subset R$ the ideal generated by $f_1, \ldots, f_t$. Suppose that R/J has the following graded free resolution:*

$$0 \to \bigoplus_{j=1}^{t_n} R\left(-d_j^{(n)}\right) \overset{\varphi_n}{\to} \cdots \overset{\varphi_2}{\to} \bigoplus_{j=1}^{t_1} R\left(-d_j^{(1)}\right) \overset{\varphi_1}{\to} R \overset{\varphi_0}{\to} R/J \to 0. \tag{2.5.1}$$

We denote by $\left(g_{k,\ell}^{(i)}\right)_{k,\ell}$ the representation matrix for φ_i. Then there exists a graded free resolution for R/J_p of the form

$$0 \to \bigoplus_{j=1}^{t_n} R\left(-d_j^{(n)}p\right) \overset{\varphi_n^{(p)}}{\to} \cdots \overset{\varphi_2^{(p)}}{\to} \bigoplus_{j=1}^{t_1} R\left(-d_j^{(1)}p\right) \overset{\varphi_1^{(p)}}{\to} R \overset{\varphi_0^{(p)}}{\to} R/J_p \to 0, \tag{2.5.2}$$

where $J_p := \langle f_1^p, \ldots, f_t^p \rangle_R$, and $\varphi_i^{(p)}$ is given by the matrix with entries equal to the p-th powers of the entries of the matrix for φ_i for each $0 \le i \le n$.

Proof. By Lemma 2.5.1 and Corollary 2.5.3 together with the fact that R is a regular ring of dimension n, the sequence

$$0 \to \bigoplus_{j=1}^{t_n} R\left(-d_j^{(n)}p\right) \overset{\varphi_n^{(p)}}{\to} \cdots \overset{\varphi_2^{(p)}}{\to} \bigoplus_{j=1}^{t_1} R\left(-d_j^{(1)}p\right) \overset{\varphi_1^{(p)}}{\to} R \overset{\varphi_0^{(p)}}{\to} R/J_p \to 0 \tag{2.5.3}$$

is exact. It is straightforward that the sequence (2.5.3) gives a graded free resolution for R/J_p. □

Chapter 3

Computing sheaf cohomology

This chapter reviews methods for computing the cohomology groups of coherent sheaves on a projective space. A number of invariants for classifying algebraic varieties are computed from their cohomology groups, and thus computing the cohomology groups plays an important role for investigating the structures of algebraic varieties.

In the literature, there are two main strategies for computing the cohomology groups: (1) Polynomial ring-based method, and (2) Exterior algebra-based method. Table 3.1 summarizes main references to algorithms based on (1) and (2), and analyses of the algorithms. The method (1) was introduced by Eisenbud in [19], and by Maruyama in his Japanese book [49]. The method (1) requires to compute Gröbner bases over a polynomial ring. The method (2) was proposed by Eisenbud-Fløystad-Schreyer [21], and it requires to compute Gröbner bases over an exterior algebra. The method (2) is expected to be more efficient than (1), since the cost of the Gröbner basis computation over an exterior algebra can be cheaper than that over a polynomial ring in general.

While both the two methods are useful in theory, they have not been analyzed yet from a viewpoint of the *actual* computation. Specifically, the complexity of both the methods have not been determined for any asymptotic parameter. This is because both the methods require the Gröbner basis computation, whose complexity is known to be exponential in general.

In this chapter, we shall compare the methods from a viewpoint of computer algebra. Specifically, we first write down the methods as concrete algorithms, and estimate the complexity of the first method for certain asymptotic parameters. Furthermore, experiments by our implementation shall clarify merits, efficiency and memory usage and possible applications of the methods. This chapter includes some computational results given in the paper [41].

Table 3.1: Main references to algorithms for computing the cohomology groups of coherent sheaves, or their analyses. There are two major strategies, one of which is based on free resolutions over polynomial rings, and the other is based on those over exterior algebras.

Polynomial ring-based	Exterior algebra-based
Eisenbud [19], Smith [53]	Eisenbud-Fløystad-Schreyer [21]
Maruyama [49, Chapter 6]	Decker-Eisenbud [14]
Decker-Lossen [15, Appendix A]	Eisenbud [18, Chapter 7]
Kudo [41]	Decker-Lossen [15, Appendix A]

3.1 Polynomial ring-based method

Let K be a field. We denote by $S = K[x_0, \ldots, x_n]$ the polynomial ring of $n+1$ variables. Let $\mathbf{P}^n = \mathrm{Proj}(S)$ be the projective n-space, and $\mathcal{F}$ a coherent sheaf on $\mathbf{P}^n$. Let $M = \bigoplus_{d \geq 0} M_d$ be a finitely generated graded S-module representing $\mathcal{F}$. We denote by $\mathcal{F}(m)$ the m-th Serre twist of $\mathcal{F}$.

We shall introduce the polynomial ring-based method [19], [49, Chapter 6], [53], [41] for computing the cohomology groups $H^q(\mathbf{P}^n, \mathcal{F}(m))$. Specifically we focus on the method by Maruyama [49]. For simplicity, we here consider to compute only the dimensions $\dim_K H^q(\mathbf{P}^n, \mathcal{F}(m))$ (but in fact we can compute bases of $H^q(\mathbf{P}^n, \mathcal{F}(m))$ by Theorem 2.3.1). The module M is presented as follows: Since M is a finitely generated graded module over S, one has

$$M \cong \left(\bigoplus_{j=1}^{t} S(-d_j) \right) / \langle \mathbf{u}_1, \ldots, \mathbf{u}_{t_0} \rangle_S, \tag{3.1.1}$$

for some integers t, t_0, d_j and homogeneous elements $\mathbf{u}_j \in \bigoplus_{j=1}^{t} S(-d_j)$ with $1 \leq j \leq t_0$. We take the integers q, t, d_j for $1 \leq j \leq t$ and the homogeneous elements $\mathbf{u}_1, \ldots, \mathbf{u}_{t_0}$ in $\bigoplus_{j=1}^{t} S(-d_j)$ as inputs.

Algorithm 3.1.1 outputs $\dim_K H^q(\mathbf{P}^n, \mathcal{F}(m))$. For the correctness and a pseudocode of Algorithm 3.1.1, see [41, Section 3].

Algorithm 3.1.1 Let $\mathbf{u}_1, \ldots, \mathbf{u}_{t_0}$ be homogeneous elements in the S-module $\bigoplus_{j=1}^{t} S(-d_j)$, and M the finitely generated graded S-module given in (3.1.1) with $\mathcal{F} := M^{\sim}$. Given q, t, d_j for $1 \leq j \leq t$ and $\mathbf{u}_1, \ldots, \mathbf{u}_{t_0}$, we proceed with the following steps:

Step 1. Compute a graded free resolution of M. For the free resolution computation, see e.g., [13, Chapter 6].

$$0 \to \bigoplus_{j=1}^{t_{n+1}} S\left(-d_j^{(n+1)}\right) \stackrel{\varphi_{n+1}}{\to} \cdots \stackrel{\varphi_1}{\to} \bigoplus_{j=1}^{t_0} S\left(-d_j^{(0)}\right) \stackrel{\varphi_0}{\to} M \to 0. \tag{3.1.2}$$

Specifically we compute all the elements

$$t_i,\ d_j^{(i)},\ \text{and}\ \left(g_{k,\ell}^{(i)}\right)_{k,\ell}\ \text{for}\ 1 \leq i \leq n+1, \tag{3.1.3}$$

where $\left(g_{k,\ell}^{(i)}\right)_{k,\ell}$ is the representation matrix for the homomorphism φ_i for each i. The above exact sequence (3.1.2) induces an exact sequence of coherent sheaves on $\mathbf{P}^n$. The induced sequence is of the form

$$0 \to \bigoplus_{j=1}^{t_{n+1}} \mathcal{O}_{\mathbf{P}^n}\left(m - d_j^{(n+1)}\right) \stackrel{\varphi_{n+1}(m)^{\sim}}{\to} \cdots \stackrel{\varphi_1(n)^{\sim}}{\to} \bigoplus_{j=1}^{t_0} \mathcal{O}_{\mathbf{P}^n}\left(m - d_j^{(0)}\right) \stackrel{\varphi_0(m)^{\sim}}{\to} \mathcal{F}(m) \to 0, \tag{3.1.4}$$

where each $\varphi_i(m)$ denotes the m-th twisted morphism of φ_i. We set

$$\mathcal{G}_i := \bigoplus_{j=1}^{t_i} \mathcal{O}_{\mathbf{P}^n}\left(m - d_j^{(i)}\right)\ \text{and}\ \Phi_i := \varphi_i(m)^{\sim}\ \text{for}\ 0 \leq i \leq n+1. \tag{3.1.5}$$

Step 2. If $q < n$ (resp. $q = n$), generate bases of $H^n(\mathbf{P}^n, \mathcal{G}_i)$ for $n-q-1 \leq i \leq n-q+1$ (resp. $n-q \leq i \leq n-q+1$) by Theorem 2.2.1 (3). If $q = 0$, additionally generate bases of $H^0(\mathbf{P}^n, \mathcal{G}_0)$ and $H^0(\mathbf{P}^n, \mathcal{G}_1)$ by Theorem 2.2.1 (1).

Step 3. If $1 \leq q \leq n-1$ (resp. $q = 0$), compute the representation matrices for $H^n(\Phi_{n-q+1})$ and $H^n(\Phi_{n-q})$ (resp. $H^0(\Phi_1)$ and $H^n(\Phi_{r-q})$) via the bases obtained in Step 2 and compute their ranks. If $q = n$, compute the representation matrix for $H^n(\Phi_{n-q+1})$ and its rank. Finally output $\dim_K H^q(\mathbf{P}^n, \mathcal{F}(m))$ by the formulae given in Corollary 2.3.1.

Step 3 computes the representation matrices for $H^n(\Phi_i)$ or $H^0(\Phi_i)$ for some i. In the following, we give a concrete description of how to compute the representation matrices, by which the algorithm shall be implemented more exactly.

Computing $H^n(\Phi_i)$: Let $t > 0$ and $t' > 0$, and let m_k and m'_ℓ be integers for $1 \leq k \leq t$ and $1 \leq \ell \leq t'$. Let $A = (g_{k,\ell})_{k,\ell}$ be a $(t \times t')$ matrix over S such that each (k,ℓ)-entry $g_{k,\ell}$ is homogeneous of degree $m_k - m'_\ell$. Then A defines the following graded homomorphism φ of degree zero:

$$\varphi \ : \ \bigoplus_{j=1}^{t} S(m_j) \longrightarrow \bigoplus_{j=1}^{t'} S(m'_j) \ ; \ \mathbf{u} \mapsto \mathbf{u} \cdot A. \tag{3.1.6}$$

Clearly φ induces a morphism $\varphi^\sim$ of coherent sheaves on $\mathbf{P}^n$

$$\varphi^\sim \ : \ \bigoplus_{j=1}^{t} \mathcal{O}_{\mathbf{P}^n}(m_j) \longrightarrow \bigoplus_{j=1}^{t'} \mathcal{O}_{\mathbf{P}^n}(m'_j) \tag{3.1.7}$$

and the following K-linear map of the cohomlogy groups:

$$H^n(\Phi) \ : \ H^n(\mathbf{P}^n, \mathcal{G}) \longrightarrow H^n(\mathbf{P}^n, \mathcal{G}') \ ; \ w \mapsto w \cdot A, \tag{3.1.8}$$

where we set

$$\Phi := \varphi^\sim, \quad \mathcal{G} := \bigoplus_{j=1}^{t} \mathcal{O}_{\mathbf{P}^n}(m_j) \text{ and } \mathcal{G}' := \bigoplus_{j=1}^{t'} \mathcal{O}_{\mathbf{P}^n}(m'_j). \tag{3.1.9}$$

For an element $v \in H^n(\mathbf{P}^n, \mathcal{O}_{\mathbf{P}^n}(m_i))$, we denote by $\eta_i(v)$ the vector with v in the i-th coordinate and 0's elsewhere in $H^n(\mathbf{P}^n, \mathcal{G})$. Namely, we define the map η_i to be the following embedding:

$$\eta_i : H^n(\mathbf{P}^n, \mathcal{O}_{\mathbf{P}^n}(m_i)) \hookrightarrow H^n(\mathbf{P}^n, \mathcal{G}) \ ; \ v \mapsto (0, \ldots, 0, v, 0, \ldots, 0). \tag{3.1.10}$$

It follows from Theorem 2.2.1 (3) that the n-th cohomology group

$$H^n(\mathbf{P}^n, \mathcal{G}) = H^n\left(\mathbf{P}^n, \bigoplus_{j=1}^{t} \mathcal{O}_{\mathbf{P}^n}(m_j)\right) \cong \bigoplus_{j=1}^{t} H^n(\mathbf{P}^n, \mathcal{O}_{\mathbf{P}^n}(m_j))$$

is a finite-dimensional K-vector space with the basis

$$\mathcal{V} := \left\{ \eta_j\left(x_0^{\ell_0} \cdots x_n^{\ell_n}\right) : 1 \leq j \leq t, \text{ and } (\ell_0, \ldots, \ell_n) \in (\mathbb{Z}_{<0})^{n+1} \text{ with } \sum_{i=0}^{n} \ell_i = m_j \right\}. \tag{3.1.11}$$

Similarly the set

$$\mathcal{V}' := \left\{ \eta_j \left(x_0^{\ell_0} \cdots x_n^{\ell_n} \right) : 1 \leq j \leq t', \text{ and } (\ell_0, \ldots, \ell_n) \in (\mathbb{Z}_{<0})^{n+1} \text{ with } \sum_{i=0}^{n} \ell_i = m'_j \right\} \quad (3.1.12)$$

gives rise to a basis for $H^n(\mathbf{P}^n, \mathcal{G}')$. Given t, t', m_k, m'_ℓ with $1 \leq k \leq t$ and $1 \leq \ell \leq t'$ and $A = (g_{k,\ell})_{k,\ell}$, the following procedures compute the representation matrix for $H^n(\Phi)$ via the bases (3.1.11) and (3.1.12):

Step 3-1. Compute the image of $\mathcal{V}$ by $H^n(\Phi)$. Each $v \in \mathcal{V}$ is of the form $v = \eta_j \left(x_0^{\ell_0} \cdots x_n^{\ell_n} \right)$ for some $1 \leq j \leq t$ and $(\ell_0, \ldots, \ell_n) \in (\mathbb{Z}_{<0})^{n+1}$ with $\sum_{i=0}^{n+1} \ell_i = m_j$. Then we have

$$\begin{aligned} (H^n(\Phi))(v) &= \sum_{k=1}^{t'} g_{j,k} \eta_k (x_0^{\ell_0} \cdots x_n^{\ell_n}) \\ &= \sum_{k=1}^{t'} \sum_{(k_0,\ldots,k_n) \in \Lambda(g_{j,k})} c_{k_0,\ldots,k_n}(g_{j,k}) x_0^{k_0} \cdots x_n^{k_n} \eta_k (x_0^{\ell_0} \cdots x_n^{\ell_n}) \\ &= \sum_{k=1}^{t'} \sum_{(k_0,\ldots,k_n) \in \Lambda(g_{j,k})} c_{k_0,\ldots,k_n}(g_{j,k}) \eta_k (x_0^{\ell_0+k_0} \cdots x_n^{\ell_n+k_n}), \end{aligned} \quad (3.1.13)$$

where $c_{k_0,\ldots,k_n}(g)$ denotes the coefficient of $x_0^{k_0} \cdots x_n^{k_n}$ in g for each polynomial $g \in S$, and where $\Lambda(g) := \{(k_0, \ldots, k_n) \in (\mathbb{Z}_{\geq 0})^{n+1} : c_{k_0,\ldots,k_n}(g) \neq 0\}$. It follows from Theorem 2.2.1 (3) that $\eta_k(x_0^{\ell_0+k_0} \cdots x_n^{\ell_n+k_n})$ is regarded as $\mathbf{0}$ if $\ell_i + k_i \geq 0$ for some i.

Step 3-2. Comparing the representation (3.1.13) with the basis $\mathcal{V}'$ of $H^n(\mathbf{P}^n, \mathcal{G}')$, we compute the representation matrix for $H^n(\Phi)$.

Computing $H^0(\Phi_i)$: This can be done in a way similar to $H^n(\Phi_i)$ given in the previous paragraph.

Correspondence between Maruyama's and Eisenbud's results. In this paragraph, we use some fundamental facts of homomorphisms of graded modules (see e.g., [24, Section 1], [47, Chapter 1] or [54, Chapter 2]). For a finitely generated graded S-module $N = \bigoplus_{d \in \mathbb{Z}} N_d$, we denote by

$$\mathrm{Hom}_S(N, S)_i := \{\varphi : N \to S : \varphi \text{ is a homomorphism with } \varphi(N_d) \subset S_{d+i} \text{ for each } d \in \mathbb{Z}\}$$

for each $i \in \mathbb{Z}$. We also denote by N^* the graded S-module dual defined by

$$N^* := \bigoplus_{i \in \mathbb{Z}} \mathrm{Hom}_S(N, S)_i = \bigoplus_{i \in \mathbb{Z}} \mathrm{Hom}_S(N(-i), S)_0,$$

whereas denote by $N^\vee$ the graded K-vector space dual $\mathrm{Hom}_K(N, K)$. For example,

$$S(\ell)^* = \bigoplus_{i \in \mathbb{Z}} \mathrm{Hom}_S(S(\ell), S)_i = \bigoplus_{i \in \mathbb{Z}} \mathrm{Hom}_S(S(\ell - i), S)_0 \cong \bigoplus_{i \in \mathbb{Z}} (S^*)_{-\ell+i} = S^*(-\ell).$$

In particular, we have $(S(\ell)^*)_i = (S^*)_{i-\ell}$ for each $i \in \mathbb{Z}$. We use the same notation as in Algorithm 3.1.1. While Maruyama [49] showed

$$H^q(\mathbf{P}^n, \mathcal{F}(m)) \cong \mathrm{Ker}(H^q(\Phi_{n-q}))/\mathrm{Im}(H^q(\Phi_{n-q+1})),$$

Eisenbud [19] proved that $\dim_K H^q(\mathbf{P}^n, \mathcal{F}(m))$ is computable based on the local duality

$$H^q(\mathbf{P}^n, \mathcal{F}(m)) \cong \left(\mathrm{Ext}_S^{n-q}(M, S)^\vee\right)_{-n-1-m}$$

by Serre [51]. In the following, we confirm by a direct computation that these two vector spaces are isomorphic to each other, i.e.,

$$\mathrm{Ker}(H^q(\Phi_{n-q}))/\mathrm{Im}(H^q(\Phi_{n-q+1})) \cong \left(\mathrm{Ext}_S^{n-q}(M, S)^\vee\right)_{-n-1-m}.$$

For this, it suffices to show

$$H^q(\mathbf{P}^n, \mathcal{F}(m))^\vee \cong \left(\mathrm{Ext}_S^{n-q}(M, S)\right)_{-n-1-m} \tag{3.1.14}$$

as K-vector spaces.

First we claim the K-isomorphism

$$H^q(\mathbf{P}^n, \mathcal{F}(m))^\vee \cong \mathrm{Ker}(H^n(\Phi_{n-q})^\vee)/\mathrm{Im}(H^n(\Phi_{n-q-1})^\vee). \tag{3.1.15}$$

Indeed, it follows from the right-exactness of the vector space dual functor $(\cdot)^\vee$ that

$$0 \longrightarrow H^n(\mathbf{P}^n, \mathcal{F}(m))^\vee \xrightarrow{H^n(\Phi_0)^\vee} H^n(\mathbf{P}^n, \mathcal{G}_0)^\vee \xrightarrow{H^n(\Phi_1)^\vee} H^n(\mathbf{P}^n, \mathcal{G}_1)^\vee$$

is exact. In a way similar to the proof of Theorem 2.3.1, we have (3.1.15).

Second we prove that there exists a commutative diagram of K-vector spaces

$$\begin{array}{ccc} H^n(\mathbf{P}^n, \mathcal{G}_{i-1})^\vee & \xrightarrow{H^n(\Phi_i)^\vee} & H^n(\mathbf{P}^n, \mathcal{G}_i)^\vee \\ \downarrow & & \downarrow \\ \bigoplus_{j=1}^{t_{i-1}} (S^*)_{-n-1-m+d_j^{(i-1)}} & \longrightarrow & \bigoplus_{j=1}^{t_i} (S^*)_{-n-1-m+d_j^{(i)}} \end{array}$$

and that $H^n(\mathbf{P}^n, \mathcal{G}_i)^\vee$ is K-isomorphic to $\bigoplus_{j=1}^{t_i} (S^*)_{-n-1-m+d_j^{(i)}}$ via this commutative diagram. We denote by $K[x_0^{-1}, \ldots, x_n^{-1}]$ the $\mathbb{Z}$-graded ring with x_i^{-1} in degree -1. We have the following *pairing*:

$$S \times \frac{1}{x_0 \cdots x_n} K[x_0^{-1}, \ldots, x_n^{-1}] \to K,$$

which is defined by

$$(f, g) \mapsto \left(\text{the coefficient of } \frac{1}{x_0 \cdots x_n} \text{ in } fg\right).$$

With this pairing, we have the isomorphisms

$$\left(\left(\frac{1}{x_0 \cdots x_n} K[x_0^{-1}, \ldots, x_n^{-1}]\right)_m\right)^\vee \cong \mathrm{Hom}_K(S_{-n-1-m}, K) = (S_{-n-1-m})^\vee \cong (S^*)_{-n-1-m}$$

as K-vector spaces for each m. One can also check that

$$((S(m)_{x_0\cdots x_n})_0 / L_m)^\vee \cong \left(\left(\frac{1}{x_0\cdots x_n}K[x_0^{-1},\ldots,x_n^{-1}]\right)_m\right)^\vee \cong (S^*)_{-n-1-m}$$

as K-vector spaces, where $(S(m)_{x_0\cdots x_n})_0$ and L_m are defined as in Theorem 2.2.1. Hence we have

$$H^n(\mathbf{P}^n,\mathcal{G}_i)^\vee \cong \bigoplus_{j=1}^{t_i} H^n(\mathbf{P}^n,\mathcal{O}_{\mathbf{P}^n}(m-d_j^{(i)}))^\vee \cong \bigoplus_{j=1}^{t_i}(S^*)_{-n-1-m+d_j^{(i)}}$$

for each $0 \leq i \leq n+1$.

Finally we show

$$\mathrm{Ker}(H^q(\Phi_{n-q})^\vee)/\mathrm{Im}(H^q(\Phi_{n-q-1})^\vee) \cong \left(\mathrm{Ext}_S^{n-q}(M,S)\right)_{-n-1-m}.$$

Let

$$0 \longrightarrow P_{n+1} \longrightarrow \cdots \longrightarrow P_1 \longrightarrow P_0 \longrightarrow M \longrightarrow 0$$

be the projective resolution of M given in (3.1.2), where we set $P_i := \bigoplus_{j=1}^{t_i} S(-d_j^{(i)})$. It follows from the isomorphisms

$$P_i(m)^* = \left(\bigoplus_{j=1}^{t_i} S(m-d_j^{(i)})\right)^* \cong \left(\bigoplus_{j=1}^{t_i} S(m-d_j^{(i)})^*\right) \cong \left(\bigoplus_{j=1}^{t_i} S^*(-m+d_j^{(i)})\right)$$

that we have

$$(P_i^*)_{-n-1-m} \cong (P_i^*(-m))_{-n-1} \cong (P_i(m)^*)_{-n-1} \cong \bigoplus_{j=1}^{t_i}(S^*)_{-n-1-m+d_j^{(i)}} \cong H^n(\mathbf{P}^n,\mathcal{G}_i)^\vee.$$

We also have

$$\begin{aligned}
& \mathrm{Ext}_{n-q}^S(M,S) \\
= \;& \mathrm{Ker}(\mathrm{Hom}_S(P_{n-q},S) \longrightarrow \mathrm{Hom}_S(P_{n-q+1},S))/\mathrm{Im}(\mathrm{Hom}_S(P_{n-q-1},S) \longrightarrow \mathrm{Hom}_S(P_{n-q},S)) \\
\cong \;& \mathrm{Ker}(P_{n-q}^* \to P_{n-q+1}^*)/\mathrm{Im}(P_{n-q-1}^* \to P_{n-q}^*),
\end{aligned}$$

and hence

$$\begin{aligned}
& \left(\mathrm{Ext}_{n-q}^S(M,S)\right)_{-n-1-m} \\
\cong \;& \mathrm{Ker}((P_{n-q}^*)_{-n-1-m} \to (P_{n-q+1}^*)_{-n-1-m})/\mathrm{Im}((P_{n-q-1}^*)_{-n-1-m} \to (P_{n-q}^*)_{-n-1-m}) \\
\cong \;& \mathrm{Ker}(H^n(\mathbf{P}^n,\mathcal{G}_{n-q})^\vee \longrightarrow H^n(\mathbf{P}^n,\mathcal{G}_{n-q+1})^\vee)/\mathrm{Im}(H^n(\mathbf{P}^n,\mathcal{G}_{n-q-1})^\vee \longrightarrow H^n(\mathbf{P}^n,\mathcal{G}_{n-q})^\vee) \\
\cong \;& \mathrm{Ker}(H^n(\Phi_{n-q})^\vee)/\mathrm{Im}(H^n(\Phi_{n-q-1})^\vee).
\end{aligned}$$

Remark 3.1.2 Since both Maruyama's method and Eisenbud's one are based on the free resolution computation over a polynomial ring, they are included in a class of the polynomial ring based method. Both compute the dimensions of the cohomology groups, but Maruyama's one computes explicit bases of the cohomology groups. As we will see in Chapter 4, computing these bases is compatible to computing the homomorphisms on the cohomology groups induced by morphisms of coherent sheaves. Hence Maruyama's method is useful to compute some other mathematical invariants such as Hasse-Witt matrices, which represent the Frobenius on the cohomology groups.

Remark 3.1.3 Macaulay2 (resp. Singular) already has the function `HH` (resp. `sheafCoh`), which computes $\dim_K H^q(\mathbf{P}^n, \mathcal{F}(m))$ based on Eisenbud's method [19]. The author implemented Algorithm 3.1.1, which is based on Maruyama's method [49], over Magma.

3.2 Exterior algebra-based method

Let K be a field. Let V be a finite-dimensional vector space over K of dimension $n+1$, and $W := V^*$ its dual space. We denote by $E = \bigwedge V$ and $S = \mathrm{Sym}(W)$ the exterior algebra on V and the symmetric algebra on W respectively. Let $\{e_0, \ldots, e_n\}$ and $\{x_0, \ldots, x_n\}$ be dual bases of V and W respectively. Recall from Proposition 2.1.6 that the symmetric algebra S is isomorphic to the polynomial ring with $n+1$ indeterminates over K. As in Section 2.3.2 of Chapter 2, the algebra S (resp. E) is graded by taking elements of W (resp. V) to have degree 1 (resp. -1).

Let $\mathcal{F}$ be a coherent sheaf on $\mathbf{P}^n = \mathrm{Proj}(S)$, and $M = \bigoplus_{d \geq 0} M_d$ a finitely generated graded module over S representing $\mathcal{F}$. Based on Theorem 2.3.11, we shall introduce the exterior algebra-based method [14], [21] for computing the dimensions of the cohomology groups $H^q(\mathbf{P}^n, \mathcal{F}(m))$, where we denote by $\mathcal{F}(m)$ the m-th Serre twist of $\mathcal{F}$. As in Section 3.1, the module M is assumed to be of the following form:

$$M \cong \left(\bigoplus_{j=1}^{t} S(-d_j) \right) / \langle \mathbf{u}_1, \ldots, \mathbf{u}_{t_0} \rangle_S \tag{3.2.1}$$

for some integers t, t_0, d_j and homogeneous elements $\mathbf{u}_i \in \bigoplus_{j=1}^{t} S(-d_j)$ with $1 \leq i \leq t_0$. We take the integers q, t, d_j for $1 \leq j \leq t$ and $\mathbf{u}_1, \ldots, \mathbf{u}_{t_0}$ as inputs.

Algorithm 3.2.1 computes $\dim_K H^q(\mathbf{P}^n, \mathcal{F}(m))$. The correctness of Algorithm 3.2.1 follows from Theorem 2.3.11 by Eisenbud-Fløystad-Schreyer [21].

Algorithm 3.2.1 Let $\mathbf{u}_1, \ldots, \mathbf{u}_{t_0}$ be homogeneous elements in the S-module $\bigoplus_{j=1}^{t} S(-d_j)$, and M the finitely generated graded S-module given in (3.2.1) with $\mathcal{F} := M^{\sim}$. Given q, t, d_j for $1 \leq j \leq t$ and $\mathbf{u}_1, \ldots, \mathbf{u}_{t_0}$, we proceed with the following steps:

Step 1. For each d, choose a basis $\{y_1, \ldots, y_{m_d}\}$ for the K-vector space M_d, where we set $m_d := \dim_K M_d$. The basis $\{y_1, \ldots, y_{m_d}\}$ can be computed via Gröbner basis algorithms over S, see Appendix for the case of a coordinate ring S/I. Let r be the Castelnuovo-Mumford regularity of M (see Definition 2.1.2 for the definition). For computational methods of the regularity, see e.g., [2] and [3], or Remark 3.2.2 below.

Step 2. Put $T^{(d)} := M_d \otimes_K \omega_E$ for $d > r := \mathrm{reg}(M)$. As seen in Section 2.3.2 in Chapter 2, we have $\mathrm{Hom}_K(E, M_d) \cong M_d \otimes_K \omega_E \cong \omega_E^{m_d}(-d) \cong E(-n-1-d)^{m_d}$ as graded E-modules for each d. Construct an injective resolution of the graded E-module $T^{(r+1)}$.

$$\mathbf{R}(M)_{\geq r+1} : \qquad T^{(r+1)} \xrightarrow{\phi'_{r+1}} T^{(r+2)} \xrightarrow{\phi'_{r+2}} \cdots,$$

where each ϕ'_d is defined as follows:

$$\phi'_d : M_d \otimes_K \omega_E \longrightarrow M_{d+1} \otimes_K \omega_E \ ; \ m \otimes \alpha \mapsto \sum_{j=0}^{n} (x_j \cdot m) \otimes (e_j \cdot \alpha).$$

Note that $\mathbf{R}(M)_{\geq r+1}$ is a linear exact complex of free E-modules.

Step 3. Compute a free resolution of $\mathrm{Ker}(\phi'_{r+1})$, say

$$\cdots \longrightarrow \bigoplus_{j=1}^{t_{r-1}} E(-d_j^{(r-1)}) \xrightarrow{\psi_{r-1}} \bigoplus_{j=1}^{t_r} E(-d_j^{(r)}) \xrightarrow{\psi_r} \mathrm{Ker}(\phi'_{r+1}) \subset T^{(r+1)}.$$

By adjoining $\mathbf{R}(M)_{\geq r+1}$, we have the following Tate resolution:

$$\cdots \longrightarrow T^{(r-2)} \xrightarrow{\psi_{r-2}} T^{(r-1)} \xrightarrow{\psi_{r-1}} T^{(r)} \xrightarrow{\psi_r} T^{(r+1)} \xrightarrow{\psi_{r+1}} T^{(r+2)} \longrightarrow \cdots,$$

where we set $T^{(i)} := \bigoplus_{j=1}^{t_i} E(-d_j^{(i)})$ for $i \leq r$ and $\psi_j := \phi'_j$ for $j \geq r+1$. We also write $T^{(i)} = \bigoplus_{j\in\mathbb{Z}} E(-j)^{\gamma_{i,j}}$ (in particular we have $\gamma_{i+1,n+1+i} = m_i = \dim_K M_i = \dim_K H^0(\mathbf{P}^n, \mathcal{F}(i))$). Finally return $\gamma_{q+\ell+1,n+1+\ell}$.

Remark 3.2.2 Since the regularity of a finitely generated S-module M is upper-bounded, one can compute the Tate resolution using the bound (but this is generally impractical due to a gap between $\mathrm{reg}(M)$ and the upper bound): For simplicity, consider the case of $M = S/I$ for some homogeneous ideal I generated in degree $\leq d$. In this case, we have $\mathrm{reg}(M) \leq (2d)^{2^{n-1}}$. For $r_0 := (2d)^{2^{n-1}} + 1$, the complex $\mathbf{R}(M)_{r_0}$ is exact, and thus one can compute the Tate resolution from $\mathbf{R}(M)_{r_0}$. For upper bounds of $\mathrm{reg}(M)$, see e.g., [10] and [11].

Remark 3.2.3 Algorithm 3.2.1 has been implemented in Magma, Macaulay2 and Singular. Specifically these computer algebra systems have the following built-in function, which adopt the exterior algebra-based method for computing $\dim_K H^q(\mathbf{P}^n, \mathcal{F}(m))$:

Magma: `CohomologyDimension`,

Macaulay2: `cohomologyTable`,

Singular: `sheafCohBGG` and `sheafCohBGG2`.

3.3 Comparison of two methods

This section introduces an experimental[1] comparison in [41] of the two algorithms (Algorithms 3.1.1 and 3.2.1) for computing the cohomology groups of coherent sheaves. In [41, Section 4.3], the author compared them over Magma by using our implementation of the polynomial ring-based method (Algorithm 3.1.1) and Magma's function "`CohomologyDimension`" which adopts Eisenbud-Fløystad-Schreyer's exterior algebra-based method (Algorithm 3.2.1). Table 3.2 shows the same experimental results as in [41, Section 4.3, Table 3]. For the setting of each case, see [41, Section 4.1] for details. We compare the two algorithms from a viewpoint of time performance and memory usage, and discuss merits of each of the two algorithms.

Time Performance: From our experiments, we observe that performance of Algorithm 3.1.1 mainly depends on the size of D, whereas that of Algorithm 3.2.1 depends on the size of n. Therefore, Algorithm 3.1.1 is more efficient for large n when D is fixed, but Algorithm 3.2.1 is more efficient for large D. For instance, we expect that Algorithm 3.1.1 is more efficient for $r \geq 7$ and $D \leq 3000$, but Algorithm 3.2.1 is more efficient for $r \leq 7$ and $D \geq 3000$.

[1] We used a computer with 2.60GHz CPU (Intel Core i5), 16GB memory and Mac OS X 64bit, and did experiments over Magma V2.21-7 [6].

Memory Usage: Algorithm 3.2.1 constructs Tate resolutions by computing free resolutions over exterior algebras. Specifically if n, $r = \mathrm{reg}(M)$ and m_{r+1} are large enough, the exterior algebra-based method constructs big size algebraic structures such as the vector space E with dimension 2^{n+1}, and the free E-modules $E^{m_i}(-i)$ with rank m_i and with dimension $\dim_K E^{m_i}(-i) = 2^{n+1}m_i$. Thus it might require large memory usage. For instance, the memory usage by Magma's one for $n = 7$ is 15GB, respectively (cf. the memory usage by ours (polynomial ring-based method) is 108MB). Magma's function is much slower than ours for $n = 7$, and we infer that this is due to the large memory usage in Magma's function.

Merits of each method: (Polynomial ring-based) Once one gets a free resolution, one can obtain an explicit basis by Theorem 2.3.1. Those explicit representations shall derive fruitful applications for further computation of mathematical objects such as Hasse-Witt matrices, which represent the Frobenius on the cohomology groups. In fact we will give an algorithm for computing the Frobenius on the cohomologry groups in Chapter 4.

(Exterior algebra-based) If one wants to compute only the dimensions without bases, we recommend to use the exterior-algebra method. Specifically once one gets bases for the K-vector spaces M_d for $d > \mathrm{reg}(M)$, one might efficiently compute the dimensions of cohomology groups with higher degree compared to the polynomial ring-based method. This is because the free resolution computation over an exterior algebra is relatively efficient than that over a polynomial ring. Moreover, one can also obtain the values of the dimensions of $H^i(\mathbf{P}^n, M^{\sim}(m))$ at the same time from the Betti table of the Tate resolution of M, see Theorem 2.3.11.

Table 3.2: Experimental results for comparing the polynomial ring-based method (Algorithms 3.1.1) and the exterior algebra-based method (Algorithm 3.2.1). The parameter n and m denotes the dimension of $\mathbf{P}^n$ and the number of twists, respectively. The parameter D is the asymptotic parameter for the complexity of Algorithm 3.1.1, and it depends on the value of m in our experiments. The notation "time" means the average of time for performing our implemetation or Magma's built-in function.

Case	Parameters			Method			
				Polynomial ring-based method by Maruyama [49] (Our implementation of Algorithm 3.1.1)			Exterior algebra-based method (Magma's function)
	n	m	D	Step 1 (Free resolution)	Steps 2–3	(total) time	time
1	3	0	10	0.000s	0.001s	0.001s	0.038s
	3	−2	35	0.000s	0.012s	0.012s	0.036s
	3	−4	84	0.001s	0.021s	0.022s	0.047s
	3	−6	165	0.000s	0.080s	0.080s	0.066s
	3	−8	286	0.000s	0.215s	0.215s	0.104s
Total memory usage				32MB			32MB
2	3	0	35	0.001s	0.005s	0.006s	0.221s
	3	−2	84	0.000s	0.021s	0.021s	0.241s
	3	−4	165	0.000s	0.051s	0.051s	0.284s
	3	−6	286	0.000s	0.152s	0.152s	0.367s
	3	−8	455	0.001s	0.414s	0.415s	0.559s
Total memory usage				32MB			32MB
3	3	0	56	0.030s	0.010s	0.040s	0.227s
	3	−2	120	0.029s	0.054s	0.083s	0.162s
	3	−4	252	0.029s	0.194s	0.223s	0.214s
	3	−6	495	0.028s	0.654s	0.683s	0.261s
	3	−8	858	0.030s	1.876s	1.906s	0.326s
Total memory usage				64MB			32MB
4	5	0	21	0.082s	0.011s	0.093s	61.802s
	5	−1	56	0.070s	0.020s	0.090s	88.210s
	5	−2	126	0.076s	0.068s	0.144s	108.970s
	5	−3	252	0.069s	0.207s	0.275s	120.690s
	5	−4	504	0.066s	0.678s	0.744s	142.230s
Total memory usage				32MB			808MB
5	7	0	36	0.006s	0.090s	0.096s	960.480s
	7	−1	120	0.003s	0.180s	0.183s	971.120s
	7	−2	330	0.005s	0.400s	0.405s	972.850s
	7	−3	792	0.007s	1.273s	1.280s	974.590s
	7	−4	1716	0.005s	5.576s	5.581s	978.270s
Total memory usage				108MB			15GB

Chapter 4

The Frobenius on cohomology groups

This chapter is based on the papers [41, Section 5], [42] and [43, Appendix B]. In this chapter, we give algorithms for computing the Frobenius action to the cohomology groups of algebraic varieties over a perfect field with characteristic $p > 0$. Specifically our algorithms compute the representation matrices for the Frobenius actions, which are p-linear maps on the cohomology groups induced by the absolute Frobenius on algebraic varieties.

Throughout this chapter, let K denote a perfect field with characteristic $p > 0$. We denote by $S = K[x_0, \ldots, x_n]$ the polynomial ring in $n+1$ variables over K, and denote by $\mathbf{P}^n = \mathrm{Proj}(S)$ the projective n-space. For homogeneous polynomials $f_1, \ldots, f_t$, we denote by $V(f_1, \ldots, f_t)$ the locus of the zeros in $\mathbf{P}^n$ of the system of $f_1, \ldots, f_t$. Put $X := V(f_1, \ldots, f_t)$. Let $F := F_{\mathrm{abs}}$ denote the absolute Frobenius on X. Let $X^{(p)}$ be the scheme given in Definition 2.4.2, and let $F_X : X \to X^{(p)}$ denote the relative Frobenius. The absolute (resp. relative) Frobenius induces the map $F^{*,q} : H^q(X, \mathcal{O}_X) \longrightarrow H^q(X, \mathcal{O}_X)$ (resp. $(F_X)^{*,q} : H^q(X^{(p)}, \mathcal{O}_{X^{(p)}}) \longrightarrow H^q(X, \mathcal{O}_X)$). This chapter aims to present algorithms for computing $F^{*,q}$. Specifically for given $p > 0$, $f_1, \ldots, f_t$ and $1 \leq q \leq n$, our algorithms output the representation matrix for the p-linear map $F^{*,q} : H^q(X, \mathcal{O}_X) \longrightarrow H^q(X, \mathcal{O}_X)$ via a suitable basis.

4.1 Related works for curves

Since algebraic varieties defined over the perfect field K with $\mathrm{char}(K) = p$ can be characterized by investigating $F^{*,q}$, computing the Frobenius action $F^{*,q}$ is important in algebraic geometry over fields with positive characteristic. For example, a non-singular curve is *superspecial* if and only if the Frobenius on the 1st cohomology group is zero, and thus computing $F^{*,1}$ allows us to determine its superspecialty.

In case of curves, i.e., one-dimensional algebraic varieties, there are many previous works for computing $F^{*,1}$, see e.g., [7], [28], [34], [40], [48] and [57]. We here briefly review results on computation methods only for elliptic curves and hyperelliptic curves.

First, for the case of elliptic curves, there is a well-known and standard method for computing $F^{*,1}$. Let E be an elliptic curve in $\mathbf{P}^2$ defined by a cubic form $f \in K[x, y, z]$, and F the absolute Frobenius on E. The 1st cohomology group $H^1(E, \mathcal{O}_E)$ has a basis $\{x^{-1}y^{-1}z^{-1}\}$, and thus the Frobenius action $F^{*,1} : H^1(E, \mathcal{O}_E) \longrightarrow H^1(E, \mathcal{O}_E)$ sends the basis element to $f^{p-1} \cdot (x^{-1}y^{-1}z^{-1})^p$. One can determine whether $F^{*,1} = 0$ or not by computing the values of coefficients in f^{p-1}, see [33, Chapter IV] for details.

For the case of hyperelliptic curves, in [48] or in the proof of [57, Proposition 2.1], we have an explicit method to get the representation matrix for $F^{*,1}$ when a hyperelliptic curve is given as an affine model $y^2 = f(x)$. Specifically this method computes the action on $H^0(X, \Omega^1_X)$ derived from $F^{*,1}$ on $H^1(X, \mathcal{O}_X)$, where Ω^1_X denotes the sheaf of Kähler differentials on X. In this case, $F^{*,1}$ is determined by computing the values of coefficients in $f^{(p-1)/2}$, where p is an odd prime. Based on this method, several algorithms and their improvements for hyperelliptic curves have been proposed, see e.g., [7], [34], and [40].

4.2 Our results: General-case algorithms

While several algorithms for specific cases have been published as above, no general-purpose explicit algorithm, which works for *arbitrary* algebraic varieties (of dimension ≥ 1) with defining equations, has been proposed and precisely analyzed yet. (cf. In [41, Section 5], a basic framework is proposed, but neither written as a concrete algorithm nor precisely analyzed.) This is because representing elements of $H^q(X, \mathcal{O}_X)$ depends on one's specific choice of an open covering for X. In this chapter, we give two algorithms for computing $F^{*,q}$ with $1 \leq q \leq n$ based on theory of computational algebraic geometry such as Gröbner bases. One of them aims to compute $F^{*,q}$ for arbitrary varieties, and the other is an algorithm for complete intersections.

Theorem 4.2.1 *With notation as above, we fix n the dimension of $\mathbf{P}^n$. Given $1 \leq q \leq n$, characteristic p and an algebraic variety $X \subset \mathbf{P}^n = \mathrm{Proj}(K[x_0, \ldots, x_n])$ with defining homogeneous polynomials $f_1, \ldots, f_t \in S = K[x_0, \ldots, x_n]$, there exists an algorithm* (Algorithm (I)) *for computing the representation matrix for $F^{*,q} : H^q(X, \mathcal{O}_X) \longrightarrow H^q(X, \mathcal{O}_X)$ such that it terminates in*

$$O(D^4 + \alpha^2 D^2 \log(p)) \tag{4.2.1}$$

arithmetic operations over K, under some assumptions. Here D is a certain invariant for X, and α depends on lifting morphisms between free resolutions for $S/\langle f_1, \ldots f_t\rangle$ and $S/\langle f_1^p, \ldots, f_t^p\rangle$.

For constructing Algorithm (I) in Section 4.4 below, we shall reduce computing $F^{*,q}$ on X into that on the projective space $\mathbf{P}^n$. Then we shall compute an explicit basis of the cohomology group via the local cohomology-based method ([19], [41] and [53]). Algorithm (I) is roughly divided into the following two steps: (*Step A*) Compute (graded minimal) free resolutions and lifting morphisms. (*Step B*) Compute the image of each basis element by $F^{*,q}$. For computing free resolutions, we shall apply Kunz's theorem [46] in our algorithm, which reduces total time for the computation, and allows us a reasonable assumption to analyze its complexity.

For complete intersections, one can simplify Algorithm (I). As stated in the following theorem, the simplified algorithm (Algorithm (II) in Section 4.5.3 below) has a more precise evaluation on the complexity:

Theorem 4.2.2 *With notation as above, we fix n the dimension of $\mathbf{P}^n$. Let $S = K[x_0, \ldots, x_n]$, and $X = V(f_1, \ldots, f_t)$ a complete intersection in $\mathbf{P}^n$ with an S-regular sequence $(f_1, \ldots, f_t) \in S^t$. Assume $d_{j_1 \ldots j_{t-1}} := \sum_{k=1}^{t-1} \deg(f_{j_k}) \leq n$ for all $1 \leq j_1 < \cdots < j_{t-1} \leq t$ and $\gcd(f_i, f_j) = 1$ in S for $i \neq j$. Given the characteristic p and $(f_1, \ldots, f_t)$, there exists an algorithm* (Algorithm (II)) *for computing the representation matrix for $F^{*,q} : H^q(X, \mathcal{O}_X) \longrightarrow H^q(X, \mathcal{O}_X)$ with $q = \dim(X) = n - t$ such that it terminates in*

$$O(tM(p-1)) \tag{4.2.2}$$

arithmetic operations over S, where $M(m)$ denotes the cost for computing the m-th power in S.

Since the strategy for Algorithm (Ⅱ) is theoretically the same as that for Algorithm (I), Algorithm (I I) can be viewed as a specific case of Algorithm (I). By contrast, Algorithm (Ⅱ) has a computationally simplified and clarified structure, which makes the computation more efficient: In practice Algorithm (Ⅱ) computes neither a free resolution nor a lifting homomorphism. Specifically, for a given complete intersection $X = V(f_1, \ldots, f_t)$ defined by an S-regular sequence $(f_1, \ldots, f_t) \in S^t$ with certain conditions, we show that the representation matrix for $F^{*,q} : H^q(X, \mathcal{O}_X) \longrightarrow H^q(X, \mathcal{O}_X)$ is completely determined by coefficients in $(f_1 \ldots f_t)^{p-1}$, where $q = \dim(X) = n-t$. We prove this fact by constructing *Koszul complex of graded free modules* and certain special lifting homomorphisms. Thanks to this fact, one also obtains a more precise evaluation on the complexity. We also note that this simplified method is viewed as a generalization of a standard method to compute $F^{*,q}$ for an elliptic curve in $\mathbf{P}^2$ (or a hypersurface in $\mathbf{P}^n$) with $q = \dim(X) = n - 1$.

We demonstrate the correctness of our algorithms by computing some examples, one of which is $X_0(23)$, the (classical) modular curve of level 23. Our computational results for $X_0(23)$ coincide with theoretical results computed by Yui's method [57]. We also examine efficiency of Algorithm (I). As stated in Theorem 4.2.1, under some assumptions, Algorithm (I) is proved to be performed in polynomial time with respect to D, α and p. In particular, Algorithm (I) terminates in $O(\alpha^2 \log(p))$ when D is fixed. For $X_0(23)$ with $D = 7$, we confirm, with our implementation over Magma [6], [9], that Algorithm (I) performs in the estimated upper bound (4.2.1).

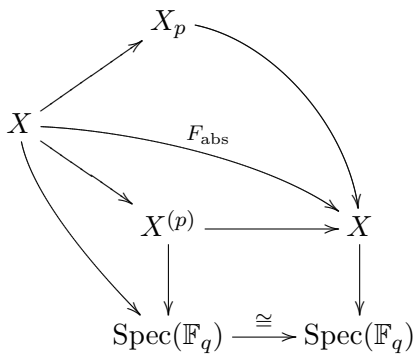
With our algorithms and computational examples, one can compute representation matrices for the Frobenius action algorithmically for more general objects, which shall provide further theoretical/computational results. (For instance, the author and Harashita already obtained theoretically new results on superspecial curves of genus 4 by applying our algorithm for complete intersections, see [43] and [44].)

4.3 Our strategy

Given a concrete X and its open affine covering, one can *theoretically* compute $H^q(X, \mathcal{O}_X)$ by Čech cohomology. However, the representation of elements of $H^q(X, \mathcal{O}_X)$ depends on one's choice of an open covering $\mathcal{U} = \{U_i\}_{i \in I}$ for X. Furthermore, we need to represent the image of each basis element by the Frobenius $F^{*,q}$ as a linear combination of the same basis.

In our strategy to compute *algorithmically* such a representation, we shall construct two morphisms, the composition of which coincides with $F = F_{\mathrm{abs}}$. With these two morphisms and their composition, computing $F^{*,q}$ is reduced into that over the projective space $\mathbf{P}^n$.

First we consider the following commutative diagram of morphisms:



where we put $X_p := V(f_1^p, \ldots, f_t^p)$, and where $X \to X_p$ and $X_p \to X$ are certain morphisms defined below. Instead of the composition of $X \to X^{(p)}$ and $X^{(p)} \to X$, we use that of $X \to X_p$ and $X_p \to X$.

Put $I := \langle f_1, \ldots, f_t \rangle_S$ and $I_p := \langle f_1^p, \ldots, f_t^p \rangle_S$, and let $\mathcal{I} := I^\sim$ and $\mathcal{I}_p := (I_p)^\sim$ denote the ideal sheaves associated to I and I_p respectively. Let $\psi : S/I_p \to S/I$ be the homomorphism defined by $h + I_p \mapsto h + I$, and let $\psi^\sim : \mathcal{O}_{X_p} \to \mathcal{O}_X$ denote the induced morphism of sheaves. We denote by F_1 the absolute Frobenius morphism on $\mathbf{P}^n$. Here, we can reduce the computation of $F^{*,q}$ over X into that over the projective space $\mathbf{P}^n$ by the following commutative diagram:

$$\begin{array}{ccccc}
 & & H^q(X, \mathcal{O}_X) & \xrightarrow{\cong} & H^{q+1}(\mathbf{P}^n, \mathcal{I}) \\
 & & \downarrow{\scriptstyle (F_1|_{X_p})^{*,q}} & & \downarrow{\scriptstyle F_1^{*,q+1}} \\
H^q(X^{(p)}, \mathcal{O}_{X^{(p)}}) & \overset{F^{*,q}}{\searrow\nearrow} & H^q(X_p, \mathcal{O}_{X_p}) & \xrightarrow{\cong} & H^{q+1}(\mathbf{P}^n, \mathcal{I}_p) \\
 & & \downarrow{\scriptstyle H^q(\psi^\sim)} & & \downarrow \\
 & & H^q(X, \mathcal{O}_X) & \xrightarrow{\cong} & H^{q+1}(\mathbf{P}^n, \mathcal{I})
\end{array}$$

where the homomorphism $H^{q+1}(\mathbf{P}^n, \mathcal{I}_p) \longrightarrow H^{q+1}(\mathbf{P}^n, \mathcal{I})$ is induced from the inclusion $I_p \to I$.

Next we give a method for computing $H^{q+1}(\mathbf{P}^n, \mathcal{I}) \longrightarrow H^{q+1}(\mathbf{P}^n, \mathcal{I})$ in the above diagram. For the finitely generated graded S-module S/I, we have a (minimal) free resolution of the form

$$0 \longrightarrow \bigoplus_{j=1}^{t_{n+1}} S\left(-d_j^{(n+1)}\right) \xrightarrow{\varphi_{n+1}} \cdots \xrightarrow{\varphi_2} \bigoplus_{j=1}^{t_1} S\left(-d_j^{(1)}\right) \xrightarrow{\varphi_1} S \xrightarrow{\varphi_0} S/I \longrightarrow 0.$$

We denote by $g_{k,\ell}^{(i)}$ the (k,ℓ)-entries of the representation matrix for φ_i. Recall from Section 2.5 that we can take the graded free resolution for S/I_p as the following form:

$$0 \longrightarrow \bigoplus_{j=1}^{t_{n+1}} S\left(-d_j^{(n+1)} p\right) \xrightarrow{\varphi_{n+1}^{(p)}} \cdots \xrightarrow{\varphi_2^{(p)}} \bigoplus_{j=1}^{t_1} S\left(-d_j^{(1)} p\right) \xrightarrow{\varphi_1^{(p)}} S \xrightarrow{\varphi_0^{(p)}} S/I_p \longrightarrow 0,$$

where the matrix for each $\varphi_i^{(p)}$ is the matrix with entries equal to the p-th powers of the entries of the matrix for φ_i. For the above free resolutions of S/I_p and S/I, there exists a morphism of complexes:

$$\begin{array}{ccccccccccccc}
0 & \longrightarrow & \bigoplus_{j=1}^{t_{n+1}} S\left(-d_j^{(n+1)} p\right) & \xrightarrow{\varphi_{n+1}^{(p)}} & \cdots & \xrightarrow{\varphi_2^{(p)}} & \bigoplus_{j=1}^{t_1} S\left(-d_j^{(1)} p\right) & \xrightarrow{\varphi_1^{(p)}} & S & \xrightarrow{\varphi_0^{(p)}} & S/I_p & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \psi_{n+1}} & & & & \downarrow{\scriptstyle \psi_1} & & \downarrow{\scriptstyle \psi_0} & & \downarrow{\scriptstyle \psi} & & \\
0 & \longrightarrow & \bigoplus_{j=1}^{t_{n+1}} S\left(-d_j^{(n+1)}\right) & \xrightarrow{\varphi_{n+1}} & \cdots & \xrightarrow{\varphi_2} & \bigoplus_{j=1}^{t_1} S\left(-d_j^{(1)}\right) & \xrightarrow{\varphi_1} & S & \xrightarrow{\varphi_0} & S/I & \longrightarrow & 0
\end{array}$$

For a computation method of each morphism ψ_i, see e.g., [17, Chapter 15]. We denote by C_i be the representation matrix for ψ_i. Let $\Psi := \psi^\sim$ denote the sheaf morphism $\mathcal{O}_{\mathbf{P}^n}/\mathcal{I}_p \to \mathcal{O}_{\mathbf{P}^n}/\mathcal{I}$ induced by ψ. We set $\Psi_i := \psi_i^\sim$,

$$\begin{aligned}
\mathcal{G}_i &:= \bigoplus_{j=1}^{t_i} \mathcal{O}_{\mathbf{P}^n}\left(-d_j^{(i)}\right), \quad \Phi_i := \varphi_i^\sim \text{ and} \\
\mathcal{G}_i^{(p)} &:= \bigoplus_{j=1}^{t_i} \mathcal{O}_{\mathbf{P}^n}\left(-d_j^{(i)} p\right), \quad \Phi_i^{(p)} := \left(\varphi_i^{(p)}\right)^\sim
\end{aligned}$$

for $0 \leq i \leq n+1$, where $\varphi_i^{\sim}$, $(\varphi_i^{(p)})^{\sim}$ and $\psi_i^{\sim}$ denote the sheaf morphisms $\mathcal{G}_i \to \mathcal{G}_{i-1}$, $\mathcal{G}_i^{(p)} \to \mathcal{G}_{i-1}^{(p)}$ and $\mathcal{G}_i^{(p)} \to \mathcal{G}_i$ induced by φ_i, $\varphi_i^{(p)}$ and ψ_i, respectively. The above commutative diagram of graded S-modules induces the following commutative diagram of the cohomology groups:

$$\begin{array}{ccccccccccc}
0 & \longrightarrow & H^n(\mathbf{P}^n, \mathcal{G}_{n+1}^{(p)}) & \xrightarrow{H^n(\Phi_{n+1}^{(p)})} & \cdots & \xrightarrow{H^n(\Phi_1^{(p)})} & H^n(\mathbf{P}^n, \mathcal{G}_0^{(p)}) & \xrightarrow{H^n(\Phi_0^{(p)})} & H^n(\mathbf{P}^n, \mathcal{O}_{\mathbf{P}^n}/\mathcal{I}_p) & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle H^n(\Psi_{n+1})} & & & & \downarrow{\scriptstyle H^n(\Psi_0)} & & \downarrow{\scriptstyle H^n(\Psi)} & & \\
0 & \longrightarrow & H^n(\mathbf{P}^n, \mathcal{G}_{n+1}) & \xrightarrow{H^n(\Phi_{n+1})} & \cdots & \xrightarrow{H^n(\Phi_1)} & H^n(\mathbf{P}^n, \mathcal{G}_0) & \xrightarrow{H^n(\Phi_0)} & H^n(\mathbf{P}^n, \mathcal{O}_{\mathbf{P}^n}/\mathcal{I}) & \longrightarrow & 0
\end{array}$$

It follows from the right-exactness of the functor $H^n(\cdot)$ that each horizontal sequence is a complex.

Lemma 4.3.1 ([41], Section 5) *With notation as above, the following diagram commutes:*

$$\begin{array}{ccccc}
H^q(X, \mathcal{O}_X) & \xrightarrow{\cong} & H^{q+1}(\mathbf{P}^n, \mathcal{I}) & \xrightarrow{\cong} & \mathrm{Ker}\left(H^n(\Phi_{n-q})\right)/\mathrm{Im}\left(H^n(\Phi_{n-q+1})\right) \\
\downarrow{\scriptstyle (F_1|_{X_p})^{*,q}} & & \downarrow{\scriptstyle F_1^{*,q+1}} & & \downarrow{\scriptstyle \text{power } p} \\
H^q(X_p, \mathcal{O}_{X_p}) & \xrightarrow{\cong} & H^{q+1}(\mathbf{P}^n, \mathcal{I}_p) & \xrightarrow{\cong} & \mathrm{Ker}\left(H^n(\Phi_{n-q}^{(p)})\right)/\mathrm{Im}\left(H^n(\Phi_{n-q+1}^{(p)})\right) \\
\downarrow{\scriptstyle H^q(\psi^{\sim})} & & \downarrow & & \downarrow{\scriptstyle H^n(\Psi_{n-q})} \\
H^q(X, \mathcal{O}_X) & \xrightarrow{\cong} & H^{q+1}(\mathbf{P}^n, \mathcal{I}) & \xrightarrow{\cong} & \mathrm{Ker}\left(H^n(\Phi_{n-q})\right)/\mathrm{Im}\left(H^n(\Phi_{n-q+1})\right)
\end{array}$$

(with $F^{*,q}$ the composite down the left side)

Here the representation matrix for $F^{*,q}$ is computed as follows.

(1) Compute a basis $\mathcal{B} = \{\mathbf{b}_1, \ldots, \mathbf{b}_g\}$ of $H^q(X, \mathcal{O}_X) \cong \mathrm{Ker}\left(H^n(\Phi_{n-q})\right)/\mathrm{Im}\left(H^n(\Phi_{n-q+1})\right)$ with $g := \dim_K H^q(X, \mathcal{O}_X)$. Here we recall from Section 3.1 that the basis $\mathcal{B}$ is given as follows: $H^n(\mathbf{P}^n, \mathcal{G}_{n-q})$ has a K-basis of the form

$$\{\mathbf{v}_1, \ldots, \mathbf{v}_{g'}\} = \{x_0^{\ell_0} \cdots x_n^{\ell_n} \mathbf{e}_j : 1 \leq j \leq t_{n-q},\ (\ell_0, \ldots, \ell_n) \in (\mathbb{Z}_{<0})^{n+1},\ \ell_0 + \cdots + \ell_n = -d_j^{(n-q)}\}.$$

where we set $g' := \dim_K H^n(\mathbf{P}^n, \mathcal{G}_{n-q})$, and where each $\mathbf{e}_j$ denotes the vector with 1 in the j-th coordinate and 0's elsewhere. We have

$$\begin{bmatrix} \mathbf{b}_1 \\ \vdots \\ \mathbf{b}_g \end{bmatrix} = B \cdot \begin{bmatrix} \mathbf{v}_1 \\ \vdots \\ \mathbf{v}_{g'} \end{bmatrix}$$

for some $g \times g'$ matrix B over K. One can compute the matrix B by Algorithm 3.1.1 together with Theorem 2.3.1 (for an algorithm to compute B, see [41, Section 3]).

(2) Compute the vector, each entry of which is the p-th power of each entry of $\mathbf{b}_i$ for $1 \leq i \leq g$. We denote by $\mathbf{b}_i^{(p)}$ the vector for $1 \leq i \leq g$.

(3) Compute $\mathbf{b}_i^{(p)} \cdot {}^t C_{n-q}$ for $1 \leq i \leq g$, and the representation matrix for $F^{*,q}$ via the basis $\mathcal{B}$.

Remark 4.3.2 (1) If the sequence $(f_1, \ldots, f_t)$ is S-regular, i.e., $X = V(f_1, \ldots, f_t)$ is a complete intersection, then one can compute lifting maps between free S-modules in free resolutions for S/I and S/I_p via the *Koszul complex*. Moreover in such a case with $q = \dim(X)$, the representation matrix for $F^{*,q}$ is determined by certain coefficients in $(f_1 \cdots f_t)^{p-1}$. We will see that in Section 4.5 (see also [43, Appendix B]).

(2) As seen in Section 2.5, we obtain a free resolution for S/I_p from a free resolution for S/I with p-th power multiplications.

4.4 Proof of Theorem 4.2.1: Algorithm and complexity analysis

We use the same notation as in the previous section. In this section, we prove Theorem 4.2.1 stated in Section 4.2. Specifically we shall give a concrete algorithm for computing representation matrices for $F^{*,q} : H^q(X, \mathcal{O}_X) \longrightarrow H^q(X, \mathcal{O}_X)$, prove its correctness, and investigate its complexity.

4.4.1 Concrete algorithm

In the following, we give our main algorithm (Algorithm (I) below). First we fix n, the dimension of the projective space $\mathbf{P}^n = \mathrm{Proj}(S)$ with $S = K[x_0, \ldots, x_n]$. The inputs are a tuple of homogeneous polynomials $(f_1, \ldots, f_t) \in S^t$ with $X := V(f_1, \ldots, f_t) \subset \mathbf{P}^n$, the characteristic p, and an integer $1 \leq q \leq n-1$. The output is the representation matrix for the Frobenius $F^{*,q} : H^q(X, \mathcal{O}_X) \longrightarrow H^q(X, \mathcal{O}_X)$.

Algorithm (I) Given a tuple of homogeneous polynomials $(f_1, \ldots, f_t) \in S^t$, a rational prime p and an integer $1 \leq q \leq n-1$, we here present an algorithm for computing the representation matrix for the action of Frobenius to $H^q(X, \mathcal{O}_X)$, where $X = V(f_1, \ldots, f_t)$. Our algorithm is divided into the following two steps (Steps A and B), and Step A (resp. Step B) has two (resp. three) sub-procedures (A-1)–(A-2) (resp. (B-1)–(B-3)):

Step A. Compute free resolutions for S/I and S/I_p, and lifting morphisms. This step has the following two sub-procedures:

(A-1) Given a tuple of homogeneous polynomials $(f_1, \ldots, f_t) \in S^t$ and a rational prime p, we compute (minimal) free resolutions for S/I and S/I_p. Recall from Lemma 2.5.4 that we can compute a free resolution of S/I_p by p-th power multiplications from the resolution of S/I. Specifically, we compute all the elements

$$t_i,\ d_j^{(i)},\ \left(g_{k,\ell}^{(i)}\right)_{k,\ell},\ \text{and}\ \left(\left(g_{k,\ell}^{(i)}\right)^p\right)_{k,\ell}\ \text{for}\ 1 \leq i \leq n+1 \tag{4.4.1}$$

in Lemma 2.5.4. These elements are determined from the resolution for S/I.

(A-2) For the elements of (4.4.1), compute homomorphisms ψ_i for $1 \leq i \leq n+1$ such that the following diagram commutes:

$$\begin{array}{ccccccccccccc}
0 & \longrightarrow & \bigoplus_{j=1}^{t_{n+1}} S\left(-d_j^{(n+1)}p\right) & \xrightarrow{\varphi_{n+1}^{(p)}} & \cdots & \xrightarrow{\varphi_2^{(p)}} & \bigoplus_{j=1}^{t_1} S\left(-d_j^{(1)}p\right) & \xrightarrow{\varphi_1^{(p)}} & S & \xrightarrow{\varphi_0^{(p)}} & S/I_p & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \psi_{n+1}} & & & & \downarrow{\scriptstyle \psi_1} & & \downarrow{\scriptstyle \psi_0} & & \downarrow{\scriptstyle \psi} & & \\
0 & \longrightarrow & \bigoplus_{j=1}^{t_{n+1}} S\left(-d_j^{(n+1)}\right) & \xrightarrow{\varphi_{n+1}} & \cdots & \xrightarrow{\varphi_2} & \bigoplus_{j=1}^{t_1} S\left(-d_j^{(1)}\right) & \xrightarrow{\varphi_1} & S & \xrightarrow{\varphi_0} & S/I & \longrightarrow & 0
\end{array}$$

where ψ_0 is the identity map on S, and where ψ is given by $h+I_p \mapsto h+I$. Specifically, we compute the representation matrices for ψ_i via standard bases for $1 \leq i \leq n+1$, say

$$C_i = \left(h_{k,\ell}^{(i)}\right)_{k,\ell} \text{ for } 1 \leq i \leq n+1. \tag{4.4.2}$$

Each homomorphism ψ_i is called a *lifting homomorphism*. A method for computing lifting homomorphisms is given in e.g., [17, Chapter 15], which is based on division algorithms on free S-modules.

Step B. For the elements of (4.4.1) and (4.4.2), we next compute the representation matrix for the Frobenius $F^{*,q} : H^q(X, \mathcal{O}_X) \longrightarrow H^q(X, \mathcal{O}_X)$. This step has the following three subprocedures:

(B-1) Compute a basis of $H^q(X, \mathcal{O}_X)$ based on Algorithm 3.1.1 together with Theorem 2.3.1 (for a concrete algorithm to compute the basis, see [41, Section 3]). For this, we use the elements of (4.4.1).

(B-2) From the basis $\mathcal{B} = \{\mathbf{b}_1, \ldots, \mathbf{b}_g\}$ of $H^q(X, \mathcal{O}_X)$, compute the image of the basis by $F_1^{*,q}$, where F_1 denotes the absolute Frobenius on $\mathbf{P}^n$. More concretely, we compute the p-th power of each entry of $\mathbf{b}_i$ for $1 \leq i \leq g$.

(B-3) From the image $\mathbf{b}_i^{(p)} := F_1^{*,q}(\mathbf{b}_i)$, the representation matrix C_{n-q} for the lifting homomorphism ψ_{n-q} and the basis $\mathcal{B}$, we compute the representation matrix for $F^{*,q}$. More concretely, we compute $F^{*,q}(\mathbf{b}_i) = H^n(\psi_{n-q}^{\sim})(F_1^{*,q}(\mathbf{b}_i)) = H^n(\psi_{n-q}^{\sim})(\mathbf{b}_i^{(p)}) = \mathbf{b}_i^{(p)} \cdot {}^tC_{n-q}$, and the representation matrix for $F^{*,q} : H^q(X, \mathcal{O}_X) \longrightarrow H^q(X, \mathcal{O}_X)$ via the basis $\mathcal{B}$. Finally, output the representation matrix.

We here prove the correctness of Algorithm (I).

Proposition 4.4.1 Algorithm (I) *outputs the representation matrix for* $F^{*,q}$.

Proof. It is straightforward from the construction of Algorithm (I) that the output is the representation matrix for the composition map of

$$\mathrm{Ker}(H^n(\Phi_{n-q}))/\mathrm{Im}(H^n(\Phi_{n-q+1})) \xrightarrow{\text{power } p} \mathrm{Ker}(H^n(\Phi_{n-q}^{(p)}))/\mathrm{Im}(H^n(\Phi_{n-q+1}^{(p)}))$$

and

$$\mathrm{Ker}(H^n(\Phi_{n-q}^{(p)}))/\mathrm{Im}(H^n(\Phi_{n-q+1}^{(p)})) \xrightarrow{H^n(\psi_{n-q}^{\sim})} \mathrm{Ker}(H^n(\Phi_{n-q}))/\mathrm{Im}(H^n(\Phi_{n-q+1})).$$

By Lemma 4.3.1, the rank of this composition coincides with that of $F^{*,q}$. □

Remark 4.4.2 In the case of $q = n$, one has

$$H^n(X, \mathcal{O}_X) \cong \mathrm{Coker}(H^n(\Phi_1)) \tag{4.4.3}$$

and thus one can compute $F^{*,n}$ in a way similar to the cases of $1 \leq q \leq n-1$.

In theory of Gröbner bases over a polynomial ring, the computation in Step A is well-known. For details on the computation in Step A, see e.g. [13, Chapter 6], [15, Sections 4.1 and 4.2], and [17, Chapter 15]. For Step (B-1), [41] gives a concrete description. Let us omit to describe in this thesis Steps A and (B-1).

In the following paragraph, we write down the computation of Steps (B-2) and (B-3) in algorithmic format, which shall give a useful information to implement the algorithm over mathematical softwares.

A pseudocode for Steps (B-2) and (B-3) Recall from Step (B-1) of Algorithm (I) together with Algorithm 3.1.1 and Theorem 2.3.1 that we have a basis $\{\mathbf{b}_1, \ldots, \mathbf{b}_g\}$ for $H^q(X, \mathcal{O}_X)$ with $g = \dim_K H^q(X, \mathcal{O}_X)$ as follows: The basis of $H^n(\mathbf{P}^n, \mathcal{G}_{n-q})$ computed in our algorithm is

$$\{\mathbf{v}_1, \ldots, \mathbf{v}_{g'}\} = \{x_0^{\ell_0} \cdots x_n^{\ell_n} \mathbf{e}_j : 1 \leq j \leq t_{n-q},\ (\ell_0, \ldots, \ell_n) \in (\mathbb{Z}_{<0})^{n+1},\ \ell_0 + \cdots + \ell_n = -d_j^{(n-q)}\},$$

where $g' := \dim_K H^n(\mathbf{P}^n, \mathcal{G}_{n-q})$. One has a K-basis of $\mathrm{Ker}\,(H^n(\Phi_{n-q}))\,/\mathrm{Im}\,(H^n(\Phi_{n-q+1}))$ as

$$\begin{bmatrix} \mathbf{b}_1 \\ \vdots \\ \mathbf{b}_g \end{bmatrix} = B \cdot \begin{bmatrix} \mathbf{v}_1 \\ \vdots \\ \mathbf{v}_{g'} \end{bmatrix}$$

for some $g \times g'$ matrix $B = (b_{i,j})_{i,j}$ over K (for an algorithm to compute B, see [41, Section 3]). We denote by C_{n-q} the representation matrix for ψ_{n-q} computed in Step (A-2), say

$$(\psi_{n-q}(\mathbf{e}_1), \ldots, \psi_{n-q}(\mathbf{e}_{t_{n-q}})) = (\mathbf{e}_1, \ldots, \mathbf{e}_{t_{n-q}}) \cdot C_{n-q}.$$

With these B, $\{\mathbf{v}_1, \ldots, \mathbf{v}_{g'}\}$ and $C_{n-q} = (h_{i,j})_{i,j}$ as inputs, we here write down a pseudocode (Algorithm 4.4.1.1) for Steps (B-2)-(B-3).

Proposition 4.4.3 Algorithm 4.4.1.1 *outputs the representation matrix for* $F^{*,q}$.

Proof. We first claim

$$\begin{bmatrix} F_1^{*,q}(\mathbf{b}_1) \\ \vdots \\ F_1^{*,q}(\mathbf{b}_g) \end{bmatrix} = B^{(p)} \cdot \begin{bmatrix} \mathbf{v}_1^{(p)} \\ \vdots \\ \mathbf{v}_{g'}^{(p)} \end{bmatrix}.$$

Indeed, we have

$$\begin{aligned} F_1^{*,q}(\mathbf{b}_i) &= F_1^{*,q}\left(\sum_{j=1}^{g'} b_{i,j}\mathbf{v}_j\right) = F_1^{*,q}\left(\sum_{j=1}^{g'} b_{i,j} x_0^{\ell_0(j)} \cdots x_n^{\ell_n(j)} \mathbf{e}_{k(j)}\right) \\ &= \sum_{j=1}^{g'} (b_{i,j})^p x_0^{\ell_0(j)p} \cdots x_n^{\ell_n(j)p} \mathbf{e}_{k(j)} = \sum_{j=1}^{g'} (b_{i,j})^p \mathbf{v}_j^{(p)}, \end{aligned}$$

where we write $\mathbf{v}_j = x_0^{\ell_0(j)} \cdots x_n^{\ell_n(j)} \mathbf{e}_{k(j)}$ for some $\ell_0(j), \ldots, \ell_n(j) \in \mathbb{Z}_{<0}$ and $k(j) \geq 1$.

Algorithm 4.4.1.1 `MatrixOfFrobenius`$(p, B, [\mathbf{v}_i]_{i=1}^{g'}, C_{n-q})$

Input: characteristic p, a matrix $B = (b_{i,j})_{i,j}$, a basis $[\mathbf{v}_i]_{i=1}^{g'}$, and a matrix C_{n-q}
Output: the representation matrix for $F^{*,q}$

1: Compute the p-th power of each entry of B
2: $B^{(p)} \leftarrow (b_{i,j}^p)_{i,j}$
3: **for** $j = 1$ **to** g' **do**
4: Write $\mathbf{v}_j = x_0^{\ell_0(j)} \cdots x_n^{\ell_n(j)} \mathbf{e}_{k(j)}$ for some $\ell_0(j), \ldots, \ell_n(j) \in \mathbb{Z}_{<0}$ and $k(j) \geq 1$
5: $\mathbf{v}_j^{(p)} \leftarrow x_0^{\ell_0(j)p} \cdots x_n^{\ell_n(j)p} \mathbf{e}_{k(j)}$
6: **end for**
7: Compute

$$B^{(p)} \cdot \begin{bmatrix} \mathbf{v}_1^{(p)} \\ \vdots \\ \mathbf{v}_{g'}^{(p)} \end{bmatrix} \cdot {}^t C_{n-q}$$

8: Write

$$B^{(p)} \cdot \begin{bmatrix} \mathbf{v}_1^{(p)} \\ \vdots \\ \mathbf{v}_{g'}^{(p)} \end{bmatrix} \cdot {}^t C_{n-q} = B' \cdot \begin{bmatrix} \mathbf{v}_1 \\ \vdots \\ \mathbf{v}_{g'} \end{bmatrix}$$

for some $g \times g'$ matrix B' over K
9: Solve the linear system $YB = B'$
10: **return** ${}^t Y$

Moreover we have

$$\begin{aligned} \left(\sum_{j=1}^{g'} (b_{i,j})^p \mathbf{v}_j^{(p)} \right) \cdot {}^t C_{n-q} &= \left(F_1^{*,q}(\mathbf{b}_i) \right) \cdot {}^t C_{n-q} = \left(H^n(\Psi_{n-q}) \circ F_1^{*,q} \right) (\mathbf{b}_i) \\ &= (F^{*,q})(\mathbf{b}_i) \in \mathrm{Ker}\left(H^n(\Phi_{n-q}) \right) / \mathrm{Im}\left(H^n(\Phi_{n-q+1}) \right). \end{aligned}$$

Since $\mathrm{Ker}\left(H^n(\Phi_{n-q}) \right) \subset H^n(\mathbf{P}^n, \mathcal{G}_{n-q})$, there exist matrices B' and Y over K such that

$$B^{(p)} \cdot \begin{bmatrix} \mathbf{v}_1^{(p)} \\ \vdots \\ \mathbf{v}_{g'}^{(p)} \end{bmatrix} \cdot {}^t C_{n-q} = B' \cdot \begin{bmatrix} \mathbf{v}_1 \\ \vdots \\ \mathbf{v}_{g'} \end{bmatrix} = YB \cdot \begin{bmatrix} \mathbf{v}_1 \\ \vdots \\ \mathbf{v}_{g'} \end{bmatrix}.$$

The matrix ${}^t Y$ gives the representation matrix for $F^{*,q}$ via the basis $\{\mathbf{b}_1, \ldots, \mathbf{b}_g\}$. □

Remark 4.4.4 Similarly to Algorithm 3.1.1, Step A computes free resolutions for a module over a polynomial ring. In addition, this step computes a homomorphism of free complexes. Several algorithms for computing free resolutions and homomorphisms of free complexes (over a polynomial ring) have been presented, but they are done in exponential time. However, objects such as the cohomology groups and their related invariants are determined by mathematical invariants of input structures. From this viewpoint, in the next subsection (Section 4.4.2), we analyze the complexity by setting certain mathematical invariants, which are determined from the form of free resolutions and a homomorphisms of free complexes as asymptotic parameters.

4.4.2 Complexity analysis

In this subsection, we analyze the complexity of Algorithm (I) in Section 4.4.1. Recall from Section 4.4.1 that the inputs of Algorithm (I) are an integer $1 \leq q \leq n-1$, a rational prime p, and a tuple of homogeneous polynomials $(f_1, \dots f_t) \in S^t$. As mentioned in Remark 4.4.4, the computation of Step A is generally done in exponential time for the degrees and the number of the monomials of f_i's. For fixed n and q, the output is determined by p and the elements of (4.4.1) and (4.4.2), which are computed in Step A. From this, we determine the complexity over S of Algorithm (I) with respect to the following parameters: p, $t^{(\max)} := \max\{t_i : n-q-1 \leq i \leq n-q+1\}$, $d^{(\max)} := \max\{d^{(i,\max)} : n-q-1 \leq i \leq n-q+1\}$, where $d^{(i,\max)} := \max\{d_j^{(i)} : 1 \leq j \leq t_i\}$.

Proposition 4.4.5 *With notation as above,* Step B *of* Algorithm (I) *in* Section 4.4.1 (*not counting the generation of a basis for the K-vector space $H^n(\mathbf{P}^n, \mathcal{G}_i)$ with $n-q-1 \leq i \leq n-q+1$) performs in*

$$O\left(\left(t^{(\max)}(d^{(\max)})^n\right)^4 + \left((t^{(\max)})(d^{(\max)})^n\right)^2 \log(p)\right) \tag{4.4.4}$$

arithmetic over $S = K[x_0, \dots, x_n]$.

Proof. We determine the complexity for each of Steps (B-1) – (B-3) of Algorithm (I) in Section 4.4.1.

First consider Step (B-1). In this step, we compute the basis of $H^q(X, \mathcal{O}_X)$. From [41, Proposition 3.5.1], this computation terminates in

$$O\left(\left(t^{(\max)}(d^{(\max)})^n\right)^4\right) \tag{4.4.5}$$

arithmetic over S. Recall from Algorithm (I) in Section 4.4.1 that this step computes a basis $\mathcal{B}$ of $H^q(X, \mathcal{O}_X) \cong \mathrm{Ker}\left(H^n(\Phi_{n-q})\right) / \mathrm{Im}\left(H^n(\Phi_{n-q+1})\right)$ with a basis $\mathcal{V} = \{\mathbf{v}_1, \dots, \mathbf{v}_{g'}\}$ of $H^n(\mathbf{P}^n, \mathcal{G}_{n-q})$ and a $g \times g'$ matrix $(b_{i,j})_{i,j}$ such that

$$\mathbf{b}_i = \sum_{j=1}^{g'} b_{i,j}\mathbf{v}_j. \tag{4.4.6}$$

Next we consider (B-2). This step computes the image of $\mathcal{B}$ by $F_1^{*,q}$. For this, for each $\mathbf{b}_i \in \mathcal{B}$, one computes the p-th power of its each entry. Recall from the proof of Proposition 4.4.3 that one has

$$\mathbf{b}_i^{(p)} := F_1^{*,q}(\mathbf{b}_i) = F_1^*\left(\sum_{j=1}^{g'} b_{i,j}\mathbf{v}_j\right) = \sum_{j=1}^{g'} (b_{i,j})^p \mathbf{v}_j^{(p)},$$

where $\mathbf{v}_j^{(p)}$ denotes the vector with entries equal to the p-th powers of the entries of $\mathbf{v}_j$. Assume here that one computes exponentiation in $O(\log(e))$ arithmetic operations, where e is the exponent. By $g' = O(t^{(\max)}(d^{(\max)})^n)$, computing $\mathbf{b}_i^{(p)}$ is estimated to be done in

$$O\left(t^{(\max)}(d^{(\max)})^n \log(p)\right).$$

Since $g = \dim_K H^q(X, \mathcal{O}_X) = O(t^{(\max)}(d^{(\max)})^n)$, this computation performs in

$$O\left(\left(t^{(\max)}(d^{(\max)})^n\right)^2 \log(p)\right) \tag{4.4.7}$$

arithmetic over K.

We determine the complexity for Step (B-3), which computes the representation matrix for F^*. In this part, one first computes the image of $\mathcal{B}^{(p)} := F_1^{*,q}(\mathcal{B})$ by the map $H^q(\Psi_{n-q})$. Recall that we have $g = \#\mathcal{B}^{(p)} = O(t^{(\max)}(d^{(\max)})^n)$. Since C_i is a $(t_i \times t_i)$ matrix over S, the computation terminates in

$$O\left((t^{(\max)})^3(d^{(\max)})^n\right) \tag{4.4.8}$$

arithmetic over S. For each $1 \leq i \leq g$, one computes $y_{i,1}, \ldots y_{i,g} \in K$ such that

$$\mathbf{b}_i^{(p)} \cdot {}^tC_{n-q} = \sum_{j=1}^{g} y_{i,j}\mathbf{b}_j. \tag{4.4.9}$$

To find $y_{i,1}, \ldots y_{i,g} \in K$, one solves a linear system over K. Specifically one first represents $\mathbf{b}_i^{(p)} \cdot C_{n-q}$ as

$$\mathbf{b}_i^{(p)} \cdot {}^tC_{n-q} = \sum_{j=1}^{g'} b'_{i,j}\mathbf{v}_j \tag{4.4.10}$$

for each i, where $\mathcal{V} = \{\mathbf{v}_1, \ldots \mathbf{v}_{g'}\}$ is a basis of $H^n(\mathbf{P}^n, \mathcal{G}_{n-q})$. Then we solve the system

$$(y_{i,1}, \ldots, y_{i,g}) \begin{pmatrix} b_{1,1} & \cdots & b_{1,g'} \\ \vdots & & \vdots \\ b_{g,1} & \cdots & b_{g,g'} \end{pmatrix} = (b'_{i,1}, \ldots b'_{i,g'}) \tag{4.4.11}$$

for each $1 \leq i \leq g$. The size of the coefficient matrix $(b_{i,j})_{i,j}$ is $g' = O(t^{(\max)}(d^{(\max)})^n)$. Thus the computation terminates in

$$O\left((t^{(\max)})^4(d^{(\max)})^{4n}\right) \tag{4.4.12}$$

arithmetic over $K \subset S$. Hence the complexity in this step is estimated as

$$O\left(\left(t^{(\max)}(d^{(\max)})^n\right)^4\right) \tag{4.4.13}$$

arithmetic over $K \subset S$.

Considering (4.4.5)-(4.4.13), we have the complexity stated in Proposition 4.4.5. □

By Proposition 4.4.5 together with [41, Corollary 3.5.2], one can also determine the complexity of Step B of Algorithm (I) in Section 4.4.1 over the ground field K.

Corollary 4.4.6 *We use the same notation as in* Proposition 4.4.5. *We denote by* α *the maximum of the number of the terms of the components in* C_{n-q} *and* A_i *for* $n-q \leq i \leq n-q+1$. *The complexity of* Step B *of* Algorithm (I) *over* K *is bounded by*

$$O\left(\left(t^{(\max)}(d^{(\max)})^n\right)^4 + \alpha^2\left(t^{(\max)}(d^{(\max)})^n\right)^2 \log(p)\right). \tag{4.4.14}$$

where we do not count the generation of bases for $H^n(\mathbf{P}^n, \mathcal{G}_i)$ *with* $n-q-1 \leq i \leq n-q+1$.

The value

$$D := \max\{\dim_K H^n(\mathbf{P}^n, \mathcal{G}_i) : n-q-1 \leq i \leq n-q+1\} \tag{4.4.15}$$

is also appropriate as an asymptotic parameter for the complexity of Step B in Algorithm (I). We describe in the following the reason why D is a suitable asymptotic parameter. Recall that one has

$$\dim_K H^n(\mathbf{P}^n, \mathcal{G}_i) = \sum_{j=1}^{t_i} \binom{d_j^{(i)}}{n} \text{ for } n-q-1 \leq i \leq n-q+1, \tag{4.4.16}$$

and therefore $\dim_K H^n(\mathbf{P}^n, \mathcal{G}_i)$ is bounded by $t^{(\max)}(d^{(\max)})^n$. Here the values t_i and $d_j^{(i)}$ are uniquely determined from the inputs $(f_1, \ldots, f_t)$ and p, since the form of the minimal resolution of S/I with $I = \langle f_1, \ldots, f_t\rangle_S$ is uniquely determined (up to isomorphism of minimal resolutions). Thus each value (4.4.16) is also uniquely determined by S/I. From this, we can take D as an asymptotic parameter for estimating the complexity of Step B of Algorithm (I). In a way similar to Corollary 4.4.6, the arithmetic complexity of Step B of Algorithm (I) with respect to D is determined as follows.

Corollary 4.4.7 *We use the same notation as in* Proposition 4.4.5 *and* Corollary 4.4.6. *We fix* n *and set* $D := \max\{\dim_K H^n(\mathbf{P}^n, \mathcal{G}_i)\ ;\ n-q-1 \leq i \leq n-q+1\}$ *as in* (4.4.15). *Then the arithmetic complexity of* Step B *of* Algorithm (I) *in* Section 4.4.1 *over* K *is*

$$O(D^4 + \alpha^2 D^2 \log(p)), \tag{4.4.17}$$

where α *is same as in* Corollary 4.4.6.

In addition, we can give the binary complexity of Step B of Algorithm (I) for $K = \mathbb{F}_p$, where p is a rational prime.

Corollary 4.4.8 *The notation is same as in* Proposition 4.4.5, Corollary 4.4.6 *and* Corollary 4.4.7. *Let* p *be a rational prime and put* $K = \mathbb{F}_p$. *We fix* n, *and assume that the computation in* $\mathbb{F}_p$ *is done in* $O((\log(p))^3)$ *bit operations. Then the binary complexity of* Step B *of* Algorithm (I) *in* Section 4.4.1 *is*

$$O(D^4(\log(p))^3 + \alpha^2 D^2(\log(p))^4), \tag{4.4.18}$$

where α *is same as in* Corollary 4.4.6.

4.4.3 Comparison with conventional computations for affine hypersurfaces

This section gives a brief comparison between Algorithm (I) in Section 4.4.1 and conventional computations for affine hypersurfaces, specifically hyperelliptic curves in $\mathbf{P}^2$. In this case, the input variety of our algorithm is given as a *projective* model defined by homogeneous polynomials in $S = K[x_0, \ldots, x_n]$ for some n whereas that of the conventional algorithms in [7], [34], [40], [48] and [57] is given as an *affine* model of the form $y^2 - g(x) = 0$ defined by *one* polynomial $y^2 - g(x) \in K[x, y]$ not necessary to be homogeneous. For a comparison, we here assume that the input variety of our algorithm is given as the locus of the zeros of one homogeneous polynomial $f \in K[X, Y, Z]$, and that its de-homogenization is of the form $y^2 - g(x)$ for some $g \in K[x, y]$. Let $X = V(f)$ be the hypersurface in $\mathbf{P}^2 = \mathrm{Proj}(K[X, Y, Z])$ defined by $f = 0$. It is straightforward that the output of our algorithm with an input f coincides with that of the conventional algorithms with an input $y^2 - g(x)$. Thus one can choose one of the conventional algorithms with the input $y^2 - g(x)$ to compute the Frobenius on $H^1(X, \mathcal{O}_X)$. In this sense, our algorithm is viewed as a generalization of the conventional computations. Moreover we interpret that the complexity of our algorithm is equivalent to that of the algorithms in [7], [34], [40], [48] and [57] for inputs as above.

4.5 Proof of Theorem 4.2.2: Algorithm for complete intersections

As in the previous section, let K be a perfect field with $\mathrm{char}(K) = p > 0$, and $S = K[x_0, \ldots, x_n]$ the polynomial ring in $n + 1$ variables. Let $f_1, \ldots, f_t$ be homogeneous polynomials in S, and put $X := V(f_1, \ldots, f_t) \subset \mathbf{P}^n = \mathrm{Proj}(S)$.

In this section, we give a specific method for computing the representation matrix for the Frobenius $F^{*,q}$ with $q = \dim(X)$ when X is a *complete intersection*, i.e., the sequence $(f_1, \ldots, f_t) \in S^t$ is *S-regular*. For this, we first prove that the representation matrix for $F^{*,q}$ for a suitable basis is given by certain coefficients in $(f_1 \cdots f_t)^{p-1}$. In particular when $q = \dim(X) = 1$, this representation matrix is called the *Hasse-Witt matrix* of the curve X, which determines the *superspecialty* of X.

First we collect some basic properties on regular sequences of modules.

4.5.1 Regular sequences of modules

Definition 4.5.1 Let R be a commutative ring with unity. Let M be an R-module. An ordered t-tuple $(y_1, \ldots, y_t) \in R^t$ is called an *M-regular sequence* (or simply called *M-regular*) if

(1) $M/(y_1, \ldots, y_t)M \neq 0$, and

(2) For each $1 \leq i \leq t$, the element y_i is a *nonzerodivisor* in the quotient module $M/(y_1, \ldots, y_{i-1})M$, that is, there is no element $y \in M/(y_1, \ldots, y_{i-1})M$ with $y \neq 0$ such that $y_i \cdot y = 0$.

Lemma 4.5.2 *Let R be a local commutative ring with unity, and M an R-module. If $\langle y_1, \ldots, y_t \rangle_R \subset R$ is a proper ideal containing an M-regular sequence of length t, then $(y_1, \ldots, y_t)$ is an M-regular sequence.*

Lemma 4.5.3 *Let R be a commutative ring with unity, and M an R-module. If $(y_1, \ldots, y_t) \in R^t$ is M-regular, then $(y_1^m, \ldots, y_t^m)$ is M-regular for any $m > 0$.*

Proof. We show the statement by the induction on t. First consider the case of $t = 1$. Let y_1 be an element in R such that y_1 is a nonzerodivisor in M with $M \neq y_1 M$. Clearly we have $M \neq y_1^m M$. We show that y_1^m is a nonzerodivisor. For this, assume $y_1^m y = 0$ in M for some $y \in M$. Since y_1 is a nonzerodivisor, we have that $y_1^{m-1} y$ is equal to $0 \in M$, and recursively we have $y = 0$.

Next consider the case of $t > 1$. Since $(y_1^m, \ldots, y_t^m)M \subset (y_1, \ldots, y_t)M$, we have $(y_1^m, \ldots, y_t^m)M \neq M$. Here we claim that it suffices to prove that y_t is a nonzerodivisor in $M/(y_1^m, \ldots, y_{t-1}^m)M$. Indeed, if y_t is a nonzerodivisor in $M/(y_1^m, \ldots, y_{t-1}^m)M$ and if $y_t^m y = 0$ in $M/(y_1^m, \ldots, y_{t-1}^m)M$ for some $y \in M$, then $y_t^{m-1} y = 0$ in $M/(y_1^m, \ldots, y_{t-1}^m)M$, and recursively $y = 0$ in $M/(y_1^m, \ldots, y_{t-1}^m)M$. In addition, we may assume that R is local and its maximal ideal contains y_i for all $1 \leq i \leq t$. Indeed, let P be a prime ideal of R with $\mathrm{Ann}(M) := \{r \in R : ry = 0 \text{ for all } y \in M\} \subset P$. We consider the localization

$$\big(M/(y_1^m, \ldots, y_{t-1}^m)M\big)_P \simeq M_P/(y_1^m, \ldots, y_{t-1}^m)M_P \quad (\text{as } R_P\text{-modules})$$

at P. Note that if y_t is a nonzerodivisor in $M_P/(y_1^m, \ldots, y_{t-1}^m)M_P$, then y_t is a nonzerodivisor in $M/(y_1^m, \ldots, y_{t-1}^m)M$. If there exists $1 \leq i \leq t$ such that $y_i \notin P$, then the either $M_P = (y_1^m, \ldots, y_{t-1}^m)M_P$ or $y_t \in (R_P)^\times$, and thus the result holds. From this, we may assume that R is a local ring and that its maximal ideal contains y_i for all $1 \leq i \leq t$. The condition that $(y_1, \ldots, y_t)$ is M-regular implies that $(y_1, \ldots, y_{t-1}, y_t^m)$ is M-regular. By applying Lemma 4.5.2, it is concluded that $(y_t^m, y_1, \ldots, y_{t-1})$ is an M-regular sequence. Consequently, by repeating the argument, $(y_1^m, \ldots, y_t^m)$ is an M-regular sequence. □

We next define the Koszul complex of *graded* free S-modules.

Definition 4.5.4 (Koszul complex of graded free modules) For a tuple of homogeneous polynomials $(f_1, \ldots, f_t) \in (S \smallsetminus \{0\})^t$ and an index i, we define the following graded free S-module of rank $\binom{t}{i}$:

$$K_i(f_1, \ldots, f_t)_{\mathrm{grd}} := \bigoplus_{1 \leq j_1 < \cdots < j_i \leq t} S(-d_{j_1 \ldots j_i}) \mathbf{e}_{j_1 \ldots j_i},$$

where we set $d_{j_1 \ldots j_i} := \sum_{k=1}^{i} \deg(f_{j_k})$. We define the graded homomorphism $\varphi_i : K_i(f_1, \ldots, f_t)_{\mathrm{grd}} \longrightarrow K_{i-1}(f_1, \ldots, f_t)_{\mathrm{grd}}$ of degree zero by putting

$$\varphi_i(\mathbf{e}_{j_1 \ldots j_i}) := \sum_{k=1}^{i} (-1)^{k-1} f_{j_k} \mathbf{e}_{j_1 \ldots \hat{j_k} \ldots j_i}.$$

The sequence $K(f_1, \ldots, f_t)_{\mathrm{grd}} := (K_i(f_1, \ldots, f_t)_{\mathrm{grd}}, \varphi_i)_i$ is a chain complex of graded free S-modules. We call this complex the *graded Koszul complex defined by* $(f_1, \ldots, f_t)$. It is straightforward that $K(f_1, \ldots, f_t)_{\mathrm{grd}}$ is exact if $(f_1, \ldots, f_t)$ is S-regular.

Lemma 4.5.5 *With notation as above, let $(f_1, \ldots, f_t) \in S^t$ be an S-regular sequence with $\gcd(f_i, f_j) = 1$ for $i \neq j$. To simplify the notation, we put*

$$M_i := K_i(f_1, \ldots, f_t)_{\mathrm{grd}}, \quad \text{and } I := \langle f_1, \ldots, f_t \rangle_S,$$
$$M_i^{(m)} := K_i(f_1^m, \ldots, f_t^m)_{\mathrm{grd}}, \quad \text{and } I_m := \langle f_1^m, \ldots, f_t^m \rangle_S.$$

We denote by $\varphi_i^{(m)}$ the i-th differential of the complex $M_\bullet^{(m)} = K(f_1^m, \ldots, f_t^m)_{\mathrm{grd}}$. We also define a graded homomorphism $\psi_i : K_i(f_1^m, \ldots, f_t^m)_{\mathrm{grd}} \longrightarrow K_i(f_1, \ldots, f_t)_{\mathrm{grd}}$ of degree zero as follows:

$$\psi_i(\mathbf{e}_{j_1 \ldots j_i}) := (f_{j_1} \cdots f_{j_i})^{m-1} \mathbf{e}_{j_1 \ldots j_i}.$$

Then the following diagram of homomorphisms of graded S-modules commutes, and each horizontal sequence is exact:

$$\begin{array}{ccccccccccccc}
0 & \xrightarrow{\varphi_{t+1}^{(m)}} & M_t^{(m)} & \xrightarrow{\varphi_t^{(m)}} & \cdots & \xrightarrow{\varphi_2^{(m)}} & M_1^{(m)} & \xrightarrow{\varphi_1^{(m)}} & M_0^{(m)} = S & \xrightarrow{\varphi_0^{(m)}} & M_{-1}^{(m)} := S/I_m & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \psi_t} & & & & \downarrow{\scriptstyle \psi_1} & & \downarrow{\scriptstyle \psi_0} & & \downarrow{\scriptstyle \psi} & & \\
0 & \xrightarrow{\varphi_{t+1}^{(1)}} & M_t & \xrightarrow{\varphi_t^{(1)}} & \cdots & \xrightarrow{\varphi_2^{(1)}} & M_1 & \xrightarrow{\varphi_1^{(1)}} & M_0 = S & \xrightarrow{\varphi_0^{(1)}} & M_{-1} := S/I & \longrightarrow & 0
\end{array}$$

where ψ_0 is the identity map on S, and ψ is the homomorphism defined by $h + I_m \mapsto h + I$.

Proof. By our assumption together with Lemma 4.5.3, the sequence $(f_1^m, \ldots, f_t^m)$ is S-regular, and hence the complex $K(f_1^m, \ldots, f_t^m)_{\mathrm{grd}} = (M_i^{(m)}, \varphi_i^{(m)})_i$ is exact. We show that the diagram commutes. For a basis element $\mathbf{e}_{j_1 \ldots j_{i+1}} \in M_{i+1}^{(m)}$, we have

$$\begin{aligned}
\left(\psi_i \circ \varphi_{i+1}^{(m)}\right)(\mathbf{e}_{j_1 \ldots j_{i+1}}) &= \psi_i \left(\sum_{k=1}^{i+1} (-1)^{k-1} f_{j_k}^m \mathbf{e}_{j_1 \ldots \hat{j_k} \ldots j_{i+1}} \right) \\
&= \sum_{k=1}^{i+1} (-1)^{k-1} f_{j_k}^m \psi_i(\mathbf{e}_{j_1 \ldots \hat{j_k} \ldots j_{i+1}}) \\
&= \sum_{k=1}^{i+1} (-1)^{k-1} f_{j_k}^m (f_{j_1} \cdots f_{j_{k-1}} f_{j_{k+1}} \cdots f_{j_{i+1}})^{m-1} \mathbf{e}_{j_1 \ldots \hat{j_k} \ldots j_{i+1}} \\
&= (f_{j_1} \cdots f_{j_{i+1}})^{m-1} \sum_{k=1}^{i+1} (-1)^{k-1} f_{j_k} \mathbf{e}_{j_1 \ldots \hat{j_k} \ldots j_{i+1}},
\end{aligned}$$

and

$$\begin{aligned}
\left(\varphi_{i+1}^{(1)} \circ \psi_{i+1}\right)(\mathbf{e}_{j_1 \ldots j_{i+1}}) &= \varphi_{i+1}^{(1)} \left((f_{j_1} \cdots f_{j_{i+1}})^{m-1} \mathbf{e}_{j_1 \ldots j_{i+1}} \right) \\
&= (f_{j_1} \cdots f_{j_{i+1}})^{m-1} \varphi_{i+1}^{(1)} \left(\mathbf{e}_{j_1 \ldots j_{i+1}} \right) \\
&= (f_{j_1} \cdots f_{j_{i+1}})^{m-1} \sum_{k=1}^{i+1} (-1)^{k-1} f_{j_k} \mathbf{e}_{j_1 \ldots \hat{j_k} \ldots j_{i+1}}.
\end{aligned}$$

Hence we have $\psi_i \circ \varphi_{i+1}^{(m)} = \varphi_{i+1}^{(1)} \circ \psi_{i+1}$. □

4.5.2 The Frobenius action for complete intersections

We present a specific method for computing the Frobenius $F^{*,q} : H^q(X, \mathcal{O}_X) \longrightarrow H^q(X, \mathcal{O}_X)$ with $q = \dim(X)$ when X is a complete intersection.

Proposition 4.5.6 *Let K be a perfect field with $\mathrm{char}(K) = p > 0$. Let $f_1, \ldots, f_t$ be homogeneous polynomials with $d_{j_1 \ldots j_{t-1}} \leq n$ for all $1 \leq j_1 < \cdots < j_{t-1} \leq t$ such that $\gcd(f_i, f_j) = 1$ in $S := K[x_0, \ldots, x_n]$ for $i \neq j$. Suppose that the sequence $(f_1, \ldots, f_t)$ is S-regular. Let $X = V(f_1, \ldots, f_t)$*

be the variety defined by the equations $f_1 = 0, \ldots, f_t = 0$ *in* $\mathbf{P}^n = \mathrm{Proj}(S)$*, and* $q := \dim(X) = n - t$*. Write* $(f_1 \cdots f_t)^{p-1} = \sum c_{i_0,\ldots,i_n} x_0^{i_0} \cdots x_n^{i_n}$ *and*

$$\{(k_0, \ldots, k_n) \in (\mathbb{Z}_{<0})^{n+1} : \sum_{i=0}^{n} k_i = -\sum_{j=1}^{t} \deg(f_j)\} = \{(k_0^{(1)}, \ldots, k_n^{(1)}), \ldots, (k_0^{(g)}, \ldots, k_n^{(g)})\},$$

where we set $g = \dim_K H^q(X, \mathcal{O}_X)$*. Then the representation matrix for the Frobenius* $F^{*,q}$ *is given by*

$$\begin{bmatrix} c_{-k_0^{(1)}p+k_0^{(1)},\ldots,-k_n^{(1)}p+k_n^{(1)}} & \cdots & c_{-k_0^{(g)}p+k_0^{(1)},\ldots,-k_n^{(g)}p+k_n^{(1)}} \\ \vdots & & \vdots \\ c_{-k_0^{(1)}p+k_0^{(g)},\ldots,-k_n^{(1)}p+k_n^{(g)}} & \cdots & c_{-k_0^{(g)}p+k_0^{(g)},\ldots,-k_n^{(g)}p+k_n^{(g)}} \end{bmatrix}.$$

Proof. We use the same notation as in Lemma 4.5.5, and take $m = p$. Put $\varphi_i := \varphi_i^{(1)}$ and

$$\Phi_i := \varphi_i^{\sim}, \quad \Phi_i^{(p)} := \left(\varphi_i^{(p)}\right)^{\sim}, \quad \Psi := \psi^{\sim}, \quad \text{and} \quad \Psi_i := \psi_i^{\sim}. \tag{4.5.1}$$

By Lemma 4.5.5, the following diagram commutes:

$$\begin{array}{ccccccc}
H^q(X, \mathcal{O}_X) & \xrightarrow{\cong} & H^{q+1}(\mathbf{P}^n, \widetilde{I}) & \xrightarrow{\cong} & \mathrm{Ker}\,(H^n(\Phi_{n-q})) & \xrightarrow{\cong} & H^n(\mathbf{P}^n, \mathcal{O}_{\mathbf{P}^n}(-\sum_{j=1}^t d_j)) \\
\downarrow{\scriptstyle (F_1|_{X^p})^{*,q}} & & \downarrow{\scriptstyle F_1^{*,q+1}} & & \downarrow{\scriptstyle \text{power } p} & & \downarrow{\scriptstyle \text{power } p} \\
H^q(X_p, \mathcal{O}_{X_p}) & \xrightarrow{\cong} & H^{q+1}(\mathbf{P}^n, \widetilde{I_p}) & \xrightarrow{\cong} & \mathrm{Ker}\left(H^n(\Phi_{n-q}^{(p)})\right) & \longrightarrow & H^n(\mathbf{P}^n, \mathcal{O}_{\mathbf{P}^n}(-\sum_{j=1}^t d_j p)) \\
\downarrow{\scriptstyle H^q(\Psi)} & & \downarrow{\scriptstyle H^{q+1}(\Psi_0)} & & \downarrow{\scriptstyle H^n(\Psi_{n-q})} & & \downarrow{\scriptstyle (f_1\cdots f_t)^{p-1}} \\
H^q(X, \mathcal{O}_X) & \xrightarrow{\cong} & H^{q+1}(\mathbf{P}^n, \widetilde{I}) & \xrightarrow{\cong} & \mathrm{Ker}\,(H^n(\Phi_{n-q})) & \xrightarrow{\cong} & H^n(\mathbf{P}^n, \mathcal{O}_{\mathbf{P}^n}(-\sum_{j=1}^t d_j))
\end{array}$$

(the curved arrow on the left is $F^{*,q}$)

where F_1 (resp. F) is the Frobenius morphism on $\mathbf{P}^n$ (resp. X) and $X_p := V(f_1^p, \ldots, f_t^p)$. The K-vector space $H^n(\mathbf{P}^n, \mathcal{O}_{\mathbf{P}^n}(-\sum_{j=1}^t d_j))$ has a basis $\{x_0^{k_0} \cdots x_n^{k_n} : (k_0, \ldots, k_n) \in (\mathbb{Z}_{<0})^{n+1},\ \sum_{i=0}^n k_i = -\sum_{j=1}^t \deg(f_j)\}$. For each $(k_0^{(i)}, \ldots, k_n^{(i)})$, we have

$$\begin{aligned}
(f_1 \cdots f_t)^{p-1} \cdot \left(x_0^{k_0^{(i)}} \cdots x_n^{k_n^{(i)}}\right)^p &= (f_1 \cdots f_t)^{p-1} \cdot x_0^{k_0^{(i)}p} \cdots x_n^{k_n^{(i)}p} \\
&= \sum c_{i_0,\ldots,i_n} x_0^{i_0+k_0^{(i)}p} \cdots x_n^{i_n+k_n^{(i)}p} \\
&= \sum_{j=1}^{g} c_{-k_0^{(i)}p+k_0^{(j)},\ldots,-k_n^{(i)}p+k_n^{(j)}} x_0^{k_0^{(j)}} \cdots x_n^{k_n^{(j)}}.
\end{aligned}$$

Hence our claim holds. □

4.5.3 Algorithm and complexity

Proposition 4.5.6 gives a simplification of Algorithm (I) in Section 4.4.1 if the input $(f_1, \ldots, f_t)$ is S-regular and if $q = \dim(X) = n - t$: To compute $F^{*,q}$, we not necessarily compute any free resolution, but only $(f_1 \cdots f_t)^{p-1}$. Moreover this method is viewed as a generalization of a standard method to compute $F^{*,1}$ for elliptic curves, see Section 4.1 or [33, Chapter IV]. Here we write down an algorithm for complete intersections:

Algorithm (II) (algorithm for complete intersections) Let $f_1, \ldots, f_t$ be homogeneous polynomials in $S = K[x_0, \ldots, x_n]$ with $d_{j_1 \ldots j_{t-1}} := \sum_{k=1}^{t-1} \deg(f_{j_k}) \leq n$ for all $1 \leq j_1 < \cdots < j_{t-1} \leq t$ such that $\gcd(f_i, f_j) = 1$ in $S := K[x_0, \ldots, x_n]$ for $i \neq j$. Given $f_1, \ldots, f_t$ such that $(f_1, \ldots, f_t)$ is S-regular, a rational prime p and an integer $q = n - t = \dim(X)$, we give an algorithm to compute the representation matrix for the action of Frobenius to $H^q(X, \mathcal{O}_X)$, where $X = V(f_1, \ldots, f_t)$. Write $(f_1 \cdots f_t)^{p-1} = \sum c_{i_0,\ldots,i_n} x_0^{i_0} \cdots x_n^{i_n}$ and

$$\{(k_0, \ldots, k_n) \in (\mathbb{Z}_{<0})^{n+1} : \sum_{i=0}^{n} k_i = -\sum_{j=1}^{t} \deg(f_j)\} = \{(k_0^{(1)}, \ldots, k_n^{(1)}), \ldots, (k_0^{(g)}, \ldots, k_n^{(g)})\},$$

where we set $g = \dim_K H^q(X, \mathcal{O}_X)$.

(1) Compute the coefficients $c_{-k_0^{(i)}p+k_0^{(j)},\ldots,-k_n^{(i)}p+k_n^{(j)}}$ for $1 \leq i, j \leq g$ in $(f_1 \cdots f_t)^{p-1}$.

(2) Output

$$\begin{bmatrix} c_{-k_0^{(1)}p+k_0^{(1)},\ldots,-k_n^{(1)}p+k_n^{(1)}} & \cdots & c_{-k_0^{(g)}p+k_0^{(1)},\ldots,-k_n^{(g)}p+k_n^{(1)}} \\ \vdots & & \vdots \\ c_{-k_0^{(1)}p+k_0^{(g)},\ldots,-k_n^{(1)}p+k_n^{(g)}} & \cdots & c_{-k_0^{(g)}p+k_0^{(g)},\ldots,-k_n^{(g)}p+k_n^{(g)}} \end{bmatrix}.$$

Complexity The complexity heavily depends on one's choice of algorithms for computing the multiplication and the power computation over the multivariate polynomial ring $K[x_0, \ldots, x_n]$; for a fixed n, the complexity can be bounded in polynomial time with respect to $\max_{1 \leq j \leq t}(\deg(f_j))$ and p, see e.g., [37, Theorem 3.1].

4.6 Examples and experimental results

This section shows computational examples and experimental results obtained by our implementation over Magma [6], [9].

4.6.1 Examples

Example 4.6.1 Let K be a perfect field with $\mathrm{char}(K) = p > 2$. Put

$$\begin{aligned} f &:= 5vz - 2wx - 3wy + wz, \\ g &:= 10v^2 + 5wv - 5w^2 + 4x^2 - 12xy + 2xy - 2y^2 - 35yz - 12z^2, \\ h &:= 15v^2 - 5wv + 5w^2 + 8x^2 - 12xy - 14xz - 11y^2 - 3yz + 15z^2, \end{aligned}$$

and $C := V(f, g, h) \subset \mathbf{P}^4 := \mathrm{Proj}(K[x, y, z, v, w])$. The curve C is the (classical) modular curve of level 67, say $C = X_0(67)$. For defining equations for modular curves, see e.g., [26]. In the following, we compute the representation matrix for the Frobenius action to $H^1(C, \mathcal{O}_C)$ for the case of $p = 3$. In this case, we have the following commutative diagram:

$$\begin{array}{ccccccccccccc} 0 & \xrightarrow{\varphi_4^{(p)}} & S(-6p) & \xrightarrow{\varphi_3^{(p)}} & \bigoplus_{j=1}^{3} S(-4p) & \xrightarrow{\varphi_2^{(p)}} & \bigoplus_{j=1}^{3} S(-2p) & \xrightarrow{\varphi_1^{(p)}} & S & \xrightarrow{\varphi_0^{(p)}} & S/I_p & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \psi_3} & & \downarrow{\scriptstyle \psi_2} & & \downarrow{\scriptstyle \psi_1} & & \downarrow{\scriptstyle \psi_0} & & \downarrow{\scriptstyle \psi} & & \\ 0 & \xrightarrow{\varphi_4} & S(-6) & \xrightarrow{\varphi_3} & \bigoplus_{j=1}^{3} S(-4) & \xrightarrow{\varphi_2} & \bigoplus_{j=1}^{3} S(-2) & \xrightarrow{\varphi_1} & S & \xrightarrow{\varphi_0} & S/I & \longrightarrow & 0 \end{array}$$

For the presentation matrices for the above homomorphisms, see the text files on the web page of the author [59]. The 1st cohomology group $H^1(C, \mathcal{O}_C) \cong H^4(\mathbf{P}^4, \mathcal{O}_{\mathbf{P}^4}(-6))$ has a basis

$$\left\{ \frac{1}{x^2yzvw}, \frac{1}{xy^2zvw}, \frac{1}{xyz^2vw}, \frac{1}{xyzv^2w}, \frac{1}{xyzvw^2} \right\},$$

which implies that C has genus 5. From the output of our program, the representation matrix for $F^{*,1}$ is

$$\begin{bmatrix} 1 & 1 & 0 & 0 & 0 \\ 2 & 0 & 2 & 0 & 0 \\ 0 & 2 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix},$$

and its rank is equal to 3. The Eigen polynomial is $a^5 + a^4 + a^3$, where a is an indeterminate.

Example 4.6.2 Let K be a perfect field with $\mathrm{char}(K) = p > 0$. Put

$$\begin{aligned} f_1 &:= Y^2 + (-X_3 - X_1 - X_0)Y + 2X_3X_2 + 3X_1^2 - 2X_1X_0 + 2X_0^2, \\ f_2 &:= X_1^2 - X_0X_2, \quad f_3 := X_2^2 - X_1X_3, \quad f_4 := X_3X_0 - X_2X_1, \end{aligned}$$

and $C := V(f_1, f_2, f_3, f_4) \subset \mathbf{P}^4 := \mathrm{Proj}(K[X_0, X_1, X_2, X_3, Y])$. The curve C is a normalization of the modular curve $X_0(23)$, which is a hyperelliptic curve of genus 2 given as an affine model in [8]. For a method of the normalization of hyperelliptic curves, see [27, Chapter 10]. In what follows, we compute the representation matrix for the Frobenius action to $H^1(C, \mathcal{O}_C)$ for the case of $p = 5$. By a way similar to Example 4.6.1, we can compute a basis of $H^1(C, \mathcal{O}_C)$. (For more information of the computation, see the text files on the web page of the author [59].) The output basis is

$$\left\{ \begin{bmatrix} 0 & \frac{1}{X_0X_1X_2X_3Y} & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & \frac{1}{X_0X_1X_2X_3Y} & 0 \end{bmatrix} \right\},$$

which implies that C has genus 2. From the output of our program, the representation matrix for $F^{*,1}$ is

$$\begin{bmatrix} 0 & 3 \\ 3 & 3 \end{bmatrix},$$

and it has full-rank. The Eigen polynomial is $a^2 + 2a + 1$, where a is an indeterminate.

4.6.2 Experimental results

To confirm practical time performance of our algorithm, we compute the representation matrix for the Frobenius action $F^{*,1}$ to the 1st cohomology group of $X_0(23)$ for $3 \leq p \leq 17$. Table 4.1 shows our experimental results for $X_0(23)$ of Example 4.6.2. We use the same notation as in Section 4.4.

Observation

Time performance: Recall from Corollary 4.4.8 that the binary complexity of Step B of Algorithm (I) is estimated as

$$O(D^4(\log(p))^3 + \alpha^2 D^2(\log(p))^4). \tag{4.6.1}$$

Table 4.1: Experimental results for examining time performance on our algorithm for $X_0(23)$

p	α	D	Rank of $F^{*,1}$	Eigen polynomial	Time for Step A	Time for Step B
3	221	7	2	a^2+1	0.040	0.010
5	2975	7	2	a^2+2a+1	0.315	0.015
7	13720	7	2	a^2+5a+3	1.680	0.052
11	104891	7	2	a^2+6a+4	11.044	0.360
13	215664	7	2	a^2+7a+9	24.186	0.761
17	676146	7	2	$a^2+11a+4$	84.482	2.664

In the cases of our experiments, $D = 7$ is fixed. We here examine that time performance is better than the estimated upper bound $O(\alpha^2(\log(p))^4)$. For $(p_1, \alpha_1) = (11, 104891)$ and $(p_2, \alpha_2) = (17, 676146)$, we calculate the ratio $\alpha_2^2(\log(p_2))^4/\alpha_1^2(\log(p_1))^4$. One gets this value ≈ 131.33. From experimental results in Table 1, the ratio of time for Step B is ≈ 7.40, which is smaller than 131.33. We can say the same for the other cases, e.g., $(p_3, \alpha_3) = (7, 13720)$ and $(p_4, \alpha_4) = (13, 215664)$. From this, we observe that time performance of Step B is better than $O(\alpha^2(\log(p))^4)$ for this computational example.

Correctness: In [8], an affine model of $X_0(23)$ is given as

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

ans its genus is 2. Using Yui's method [57], one can calculate the rank and the Eigen polynomial of $F^{*,1}$, which coincide with those in Table 4.1.

Value of α: For large p, we see that α takes an extremely large value. However, rather than p, the value α depends on lifting morphisms computed in Step (A-2). This means that a computational method adopted in Step (A-2) deeply affects total time performance and memory usage. Thus, if one computes lifting morphisms such that α is small, Algorithm (I) may perform more efficiently, and save memory usage.

Chapter 5

Application to finding superspecial curves

This chapter is based on the papers [43], [44] and [45]. Let p be a rational prime, and K a perfect field with characteristic p. In this chapter, we shall apply an algorithm in Chapter 4 to enumerating superspecial curves of genus 4. A curve C of genus 4 over K is said to be *superspecial* if its Jacobian $J(C)$ is isomorphic to a product of supersingular elliptic curves E^g over the algebraic closure $\overline{K}$. Here is a classical problem: Given (g, K), does there exist a superspecial curve of genus g over K? In particular, given $q = p^s$ with $s \geq 1$, does there exist a superspecial curve of genus g over the finite field $\mathbb{F}_q$? If $g \leq 3$, some theoretical approaches to finding superspecial curves are available, which are based on Torelli's theorem. However if $g \geq 4$, any theory stating such a thing for arbitrary large p (or q) has not been found. Hence the case of $g = 4$ is a next target. Based on our algorithm in Chapter 4 for computing the Frobenius on cohomology groups, we shall give algorithms for enumerating superspecial curves of genus $g = 4$, and execute them in small characteristic. Specifically we completely determine the isomorphism classes of superspceial curves over $K = \mathbb{F}_5$, $\mathbb{F}_{25}$, $\mathbb{F}_7$, $\mathbb{F}_{49}$ and $\mathbb{F}_{11}$, where we consider only the nonhyperelliptic case for $K = \mathbb{F}_{11}$.

5.1 Definition and properties of superspecial curves

By a curve, we mean a non-singular projective variety of dimension 1. Let C be a curve of genus g over K. The curve C is said to be *superspecial* if $J(C) \cong E^g$ over $\overline{K}$ for some supersingular elliptic curve E, where $J(C)$ denotes the Jacobian variety of C. An important fact is that any superspecial curve over $\mathbb{F}_q$ has at lease one $\mathbb{F}_q$-rational point:

Lemma 5.1.1 ([44], Lemma 3.1.1) *Let C be a curve over $\mathbb{F}_q$ with p-rank 0. Then we have $\#C(\mathbb{F}_q) \equiv 1 \bmod p$, where $\#C(\mathbb{F}_q)$ denotes the set of $\mathbb{F}_q$-rational points. Since a superspecial curve over $\mathbb{F}_q$ has p-rank 0, it has at least one $\mathbb{F}_q$-rational point.*

Another important property is that any maximal or minimal curve over $\mathbb{F}_{p^2}$ is superspecial. Conversely any superspecial curve over an algebraically closed field descends to a maximal or minimal curve over $\mathbb{F}_{p^2}$, see the proof of [22, Theorem 1.1]. In particular, for small p, any superspecial curve descends to a maximal curve over $\mathbb{F}_{p^2}$:

Lemma 5.1.2 *Let k be an algebraically closed field with characteristic p, and C a superspecial curve of genus g over k. Assume that $g > \frac{p^2+1}{2p}$. Then there exists a maximal curve X of genus g over $\mathbb{F}_{p^2}$ such that $X_k := X \times_{\mathrm{Spec}(\mathbb{F}_{p^2})} \mathrm{Spec}(k) \cong C$.*

Proof. Using the proof of [22, Theorem 1,1], the curve C descends to a curve X over $\mathbb{F}_{p^2}$ with $\#X(\mathbb{F}_{p^2}) = 1 \pm 2gp + p^2$, where $\#X(K)$ denotes the set of K-rational points of the curve X. It follows from our assumption that $1 - 2gp + p^2 < 0$. Thus we have $\#X(\mathbb{F}_{p^2}) = 1 + 2gp + p^2$, which means that X is a maximal curve over $\mathbb{F}_{p^2}$. □

If $g \geq 2$, the number of K-isomorphism classes of superspcial curves over general finite fields $\mathbb{F}_{p^a}$ depends only on the parity of a:

Proposition 5.1.3 ([44], Proposition 2.3.1) *Let $\mathrm{SSp}_g(K)$ denote the set of K-isomorphism classes of superspecial curves of genus g over K. Suppose $g \geq 2$. Then there exists a bijection between $\mathrm{SSp}_g(\mathbb{F}_{p^a})$ and $\mathrm{SSp}_g(\mathbb{F}_{p^b})$ if $a \equiv b \pmod 2$.*

Proposition 5.1.3 is an analogue of the result by Xue, Yang and Yu in the case of abelian varieties, see [56, Theorem 1.3].

5.2 Previous results

In the literature, there are many works on the enumeration of superspecial curves, see Table 5.1 for a summary. Specifically Ekedahl proved in [22, Theorem 1.1] that the existence of a non-hyperelliptic superspecial curves of genus g in characteristic p implies that $2g \leq p^2 - p$. He also showed in [22, Theorem 1.1] that if there exists a hyperelliptic superspecial curve of genus g in characteristic p with $(g, p) \neq (1, 2)$, then one has that $2g \leq p - 1$. If $g \leq 3$, some theoretical approaches to finding superspecial curves are available, which are based on Torelli's theorem. In particular, it is known that there exists a maximal curve of genus g over $\mathbb{F}_{p^{2e}}$ if $g = 2$ and $p^{2e} \neq 4, 9$ (cf. Serre [52, Théorème 3]) and if $g = 3$, $p \geq 3$ and e is odd (cf. Ibukiyama [38, Theorem 1]). However, if $g \geq 4$, any theory stating such a thing for arbitrary large p has not been found. Hence the case of $g = 4$ is a next target; By Ekedahl's result [22, Theorem 1.1], there does not exist any superspecial curve of genus 4 for $p = 3$. In the case of $p = 5$, Fuhrmann-Garcia-Torres [25] found a maximal curve C_0 over $K = \mathbb{F}_{25}$, and proved that it gives a unique isomorphism class over the algebraic closure $\overline{K}$. For $p \leq 7$, all isomorphism classes of superspecial curves of genus 4 over $\mathbb{F}_{p^2}$ were computationally determined in [43]. In particular, the result of [43] enumerated all the maximal curves over $K = \mathbb{F}_{25}$, which are included in the unique isomorphism class of C_0 over $\overline{K}$. Moreover, nonhyperelliptic superspecial curves of genus 4 over prime fields $\mathbb{F}_p$ for $p = 5$ and 11 were enumerated in [44] and [45].

5.3 Our results: Enumeration in genus 4

This section introduces our results given in [43], [44] and [45] for enumerating superspecial curves of genus 4. Specifically we determine the isomorphism classes of superspceial curves for $K = \mathbb{F}_5$, $\mathbb{F}_{25}$, $\mathbb{F}_7$, $\mathbb{F}_{49}$ and $\mathbb{F}_{11}$. For $K = \mathbb{F}_{11}$, we consider only the nonhyperelliptic case.

Table 5.1: Main references to enumerations of K-isomorphism classes of superspecial curves of genus g over $\mathbb{F}_q$ for $g \leq 4$ (replace "curves" by "elliptic curves" if $g = 1$). There are two cases $q = p^{2e-1}$ or p^{2e} for each g, where e is a natural number. Our results are Theorems 5.3.1 – 5.3.5 stated in the next section (Section 5.3).

g \ q	$p \leq 3$	5^{2e-1}	5^{2e}	7^{2e-1} 7^{2e}	11^{2e-1}	11^{2e}	$p \geq 13$
1	($K = \overline{\mathbb{F}_q}$): Deuring [16], ($K = \mathbb{F}_q$): Xue-Yang-Yu [56, Prop. 4.4]						
2	($K = \overline{\mathbb{F}_q}$): Hashimoto-Ibukiyama [36] for p^{2e}, Ibukiyama-Katsura [39] for p^{2e-1}						
3	($K = \overline{\mathbb{F}_q}$): Hashimoto [35] for p^{2e}, Existence for p^{2e-1}: Ibukiyama [38]						
4	Non-Existence by Ekedahl [22]	**Thm. 5.3.4** [44] or [45]	($K = \overline{\mathbb{F}_q}$): [25] **Thm. 5.3.1** [43]	**Thm. 5.3.2** [43]	**Thm. 5.3.5** [44] or [45]	Existence (e.g. [31])	No general result

5.3.1 Main theorems

Here we state our main theorems on enumerating superspecial curves.

Theorem 5.3.1 ([43], Theorem A and Corollary 6.2.3) *Any superspecial curve of genus* 4 *over* $\mathbb{F}_{25}$ *is* $\mathbb{F}_{25}$*-isomorphic to the complete intersection defined by*

$$Q = 2yw + z^2, \text{ and } P = x^3 + a_1y^3 + a_2w^3 + a_3zw^2$$

in the projective 3*-space* $\mathbf{P}^3$*, where* $a_1, a_2 \in \mathbb{F}_{25}^{\times}$ *and* $a_3 \in \mathbb{F}_{25}$*. Moreover there are precisely* 21 *superspecial curves of genus* 4 *over* $\mathbb{F}_{25}$ *up to isomorphism over* $\mathbb{F}_{25}$*. (Note that there exists precisely the* 1 *superspecial curve of genus* 4 *over* $\mathbb{F}_{25}$ *up to isomorphism over the algebraic closure, cf.* Corollary 5.3.14 *in* Section 5.3.5.)

By Theorem 5.3.1, we can give another proof of the uniqueness of maximal curves over $\mathbb{F}_{25}$. The original and theoretical proof is given in [25].

Theorem 5.3.2 ([43], Theorem B) *There is no superspecial curve of genus* 4 *in characteristic* 7*.*

Theorem 5.3.2 gives a negative answer to the genus 4 case of the problem proposed in 1987 by Ekedahl, see p. 173 of [22]. This also implies the non-existence of maximal curve of genus 4 over $\mathbb{F}_{49}$, which updated the table at `manypoints.org`[1]. Using Theorem 5.3.2, we can determine the value of $N_{49}(4)$, where $N_q(g)$ denotes the maximal number of $\mathbb{F}_q$-rational points of curves of genus g over the finite field $\mathbb{F}_q$. The author learned much about this from E. W. Howe.

Corollary 5.3.3 ([43], Corollary 5.1.3) *We have* $N_{49}(4) = 102$*.*

Theorem 5.3.4 ([44], Theorem A, or [45], Main Theorem) *There exist precisely* 7 *superspecial curves of genus* 4 *over* $\mathbb{F}_5$ *up to isomorphism over* $\mathbb{F}_5$*. The seven isomorphism classes are given*

[1] After the paper [32] by van der Geer and van der Vlugt was published, the site `manypoints.org` updates the upper and lower bounds of $N_q(g)$, the maximal number of rational points of curves of genus g over $\mathbb{F}_q$.

by $C_i = V(Q, P_i)$ *with* $Q = 2yw + z^2$ *and*

$$\begin{aligned} P_1 &= x^3 + y^3 + w^3, \\ P_2 &= x^3 + 2y^3 + w^3, \\ P_3 &= x^3 + y^3 + w^3 + zw^2, \\ P_4 &= x^3 + y^3 + 2w^3 + zw^2, \\ P_5 &= x^3 + y^3 + 3w^3 + zw^2, \\ P_6 &= x^3 + y^3 + 4w^3 + zw^2, \\ P_7 &= x^3 + y^2z + zw^2. \end{aligned}$$

(*Note that there exists precisely the* 1 *superspecial curve of genus* 4 *over* $\mathbb{F}_5$ *up to isomorphism over the algebraic closure, cf.* Corollary 5.3.14 *in* Section 5.3.5.)

Theorem 5.3.5 ([44], Theorem B, or [45], Main Theorem) *There exist precisely* 30 *nonhyperelliptic superspecial curves of genus* 4 *over* $\mathbb{F}_{11}$ *up to isomorphism over* $\mathbb{F}_{11}$. *The thirty isomorphism classes are given by* (N1) $C_i = V(Q, P_i^{(\mathrm{N1})})$ *with* $Q = 2xw + 2yz$ *for* $1 \leq i \leq 8$ *as in* Proposition 5.3.27, (N2) $C_i = V(Q, P_i^{(\mathrm{N2})})$ *with* $Q = 2xw + y^2 - \epsilon z^2$ *for* $1 \leq i \leq 5$ *as in* Proposition 5.3.28, *and* (Dege) $C_i = V(Q, P_i^{(\mathrm{Dege})})$ *with* $Q = 2yw + z^2$ *for* $1 \leq i \leq 17$ *as in* Proposition 5.3.29. (*Note that there exist precisely* 9 *nonhyperelliptic superspecial curves of genus* 4 *over* $\mathbb{F}_{11}$ *up to isomorphism over the algebraic closure, cf.* Corollary 5.3.16 *in* Section 5.3.5.)

5.3.2 Our enumeration algorithms

In this subsection, we shall present algorithms for enumerating nonhyperlliptic superspceial curves of genus 4. As a canonical curve, any nonhyperelliptic curve of genus 4 over K is defined in $\mathbf{P}^3 = \mathrm{Proj}(\overline{K}[x, y, z, w])$ to be the zero-locus of an irreducible quadratic form Q and an irreducible quadratic form P in x, y, z and w (cf. [33, Chapter IV, Example 5.2.2]). As we proved in [43, Section 2.1], we can take all coefficients in Q and P as elements of the field K.

First we state a criterion for superspceialty of nonhyperelliptic curves of genus 4. As a special case of Proposition 4.5.6, we have the following criterion.

Corollary 5.3.6 ([43], Corollary 3.1.6) *Let* $C = V(Q, P)$ *be the curve of genus* 4 *defined by a quadratic form* Q *and a cubic form* P *of* $K[x, y, z, w]$ *in* $\mathbf{P}^3$. *Then the curve* C *is superspecial if and only if the coefficients of* $x^{pi-i'}y^{pj-j'}z^{pk-k'}w^{p\ell-\ell'}$ *in* $(PQ)^{p-1}$ *equal to* 0 *for all positive integers* i, j, k, ℓ, i', j', k' *and* ℓ' *with* $i + j + k + \ell = i' + j' + k' + \ell' = 5$.

As we will see in Section 5.3.5, we have the fact that Q is assumed to be one of three quadratic forms. Based on this fact together with Corollary 5.3.6, we have a strategy for enumerating nonyperelliptic superspecial curves of genus 4 over K:

Given Q, enumerate P such that all the coefficients of the 16 monomials in Corollary 5.3.6 are zero and such that $V(Q, P)$ is non-singular.

For this, we regard all the 16 coefficients as multivariate algebraic equations on coefficients in P, and seek all roots of the system of the algebraic equations such that $V(Q, P)$ is non-singular.

Let Q be an irreducible quadratic form in $K[x, y, z, w]$ and let $\{x^{k_i}y^{\ell_i}z^{m_i}w^{n_i} : 1 \leq i \leq t\}$ be a set of monomials of degree 3. Given Q and $\{x^{k_i}y^{\ell_i}z^{m_i}w^{n_i} : 1 \leq i \leq t\}$, we here present two algorithms

for enumerating cubic forms of the form $P = \sum_{i=1}^{t} a_i x^{k_i} y^{\ell_i} z^{m_i} w^{n_i}$ such that $C = V(Q, P)$ is superspecial. The first one is proposed in [43]. The second one is presented in [44] and [45] as a modified version of the first algorithm.

First Enumeration Algorithm (**Main Algorithm in** [**43**])

Input: The characteristic p of $K = \mathbb{F}_q$, a quadratic form $Q \in K[x, y, z, w]$, and a set of monomials of degree three $\{x^{k_i} y^{\ell_i} z^{m_i} w^{n_i} : 1 \leq i \leq t\}$.

Output: A list of cubic forms of the form $P = \sum_{i=1}^{t} a_i x^{k_i} y^{\ell_i} z^{m_i} w^{n_i}$.

(1) Regard some unknown coefficients in P as indeterminates. For simplicity, we here regard the first s coefficients $a_1, \ldots, a_s$ as indeterminates. The remaining part $(a_{s+1}, \ldots, a_t)$ runs through $\mathbb{F}_q^{\oplus(t-s)}$.

(2) For each $(a_{s+1}, \ldots, a_t) \in \mathbb{F}_q^{\oplus(t-s)}$, proceed with the following four steps:

  (a) Compute $h := (PQ)^{p-1}$ over $\mathbb{F}_q[a_1, \ldots, a_s][x, y, z, w]$, which is a polynomial ring whose ground ring is also a polynomial ring.

  (b) Let $\mathcal{S}$ denote the set of the coefficients of the 16 monomials in $h = (PQ)^{p-1}$, given in Corollary 5.3.6. Note that we have $\mathcal{S} \subset \mathbb{F}_q[a_1, \ldots, a_s]$.

  (c) Using Gröbner basis algorithms, solve the system of multivariate equations $f(a_1, \ldots, a_s) = 0$ for all $f \in \mathcal{S}$ over $\mathbb{F}_q$.

  (d) For each root of the above system, substitute it into unknown coefficients in P, and test whether $C = V(Q, P)$ is non-singular or not. If C is non-singular, store the cubic form P. For testing non-singularity, we use a known Gröbner basis method, see [43, Section 3.2], or [44, Section 2.2].

Return the list of stored cubic forms P.

Second Enumeration Algorithm (**Modified version of Main Algorithm in** [**43**])

Input: The characteristic p of $K = \mathbb{F}_q$, a quadratic form $Q \in K[x, y, z, w]$, and a set of monomials of degree three $\{x^{k_i} y^{\ell_i} z^{m_i} w^{n_i} : 1 \leq i \leq t\}$.

Output: A list of cubic forms of the form $P = \sum_{i=1}^{t} a_i x^{k_i} y^{\ell_i} z^{m_i} w^{n_i}$.

(0) Regard some unknown coefficients in P as indeterminates. For simplicity, we here regard the first s_1 coefficients $a_1, \ldots, a_{s_1}$ as indeterminates. The remaining part $(a_{s_1+1}, \ldots, a_t)$ runs through $\mathbb{F}_q^{\oplus(t-s_1)}$.

For each $(a_{s_1+1}, \ldots, a_t) \in \mathbb{F}_q^{\oplus(t-s_1)}$, proceed with the following three steps:

(1) Compute $h := (PQ)^{p-1}$ over $\mathbb{F}_q[a_1, \ldots, a_{s_1}][x, y, z, w]$, which is a polynomial ring whose ground ring is also a polynomial ring.

(2) Regard some unknown coefficients among $a_1, \ldots, a_{s_1}$ as indeterminates. For simplicity, we here regard the first s_2 coefficients $a_1, \ldots, a_{s_2}$ with $s_2 \leq s_1$ as indeterminates. The remaining part $(a_{s_2+1}, \ldots, a_{s_1})$ runs through $\mathbb{F}_q^{\oplus(s_1-s_2)}$.

(3) For each $(a_{s_2+1}, \ldots, a_{s_1}) \in \mathbb{F}_q^{\oplus(s_1-s_2)}$, proceed with the following three steps:

3a. Let $\mathcal{S}$ denote the set of the coefficients of the 16 monomials in $h = (PQ)^{p-1}$, given in Corollary 5.3.6. Note that we have $\mathcal{S} \subset \mathbb{F}_q[a_1, \ldots, a_{s_2}]$.

3b. Using Gröbner basis algorithms, solve the system of multivariate equations $f(a_1, \ldots, a_{s_2}) = 0$ for all $f \in \mathcal{S}$ over $\mathbb{F}_q$.

3c. For each root of the above system, substitute it into unknown coefficients in P, and test whether $C = V(Q, P)$ is non-singular or not. If C is non-singular, store the cubic form P. For testing non-singularity, we use a known Gröbner basis method, see [43, Section 3.2], or [44, Section 2.2].

Return the list of stored cubic forms P.

Remark 5.3.7 For Steps 2–3b in Second Enumeration Algorithm, we apply Bettale et al.'s method [5], called *hybrid approach*, to solving multivariate systems over $\mathbb{F}_q$. Their idea is to mix the brute-force and Gröbner basis techniques for efficiency, but there is a trade-off between them. Note that an optimal choice of coefficients to be regarded as indeterminants is not unique, and deeply depends on the situation. In our case, such a choice is heuristically decided from experimental computations for each situation (Propositions 5.3.17 – 5.3.29 in Section 5.3.6).

Our modification and its effects: We briefly describe our modification of the previous algorithm (Main Algorithm in [43]), and its effects on total time for our enumeration. In the following, we denote by

t_{mlt}: average time for computing the multiple $(PQ)^{p-1}$, and

t_{GBslv}: average time for solving multivariate systems.

In the previous version, we use the *same* number of indeterminates in computing $(PQ)^{p-1}$ and solving multivariate systems. In other words, we consider the case of $s := s_1 = s_2$ only and skip Step 2. In this case, the number of total iterations is q^{t-s}, and hence required time is roughly estimated as $q^{t-s}(t_{mlt} + t_{GBslv})$, where we suppose that non-singularity testing is negligible. From outputs obtained by the previous algorithm in our experiments, we observe in our enumeration that the computation of $(PQ)^{p-1}$ might be dominant for large p if each multivariate system is quite efficiently solved. This depends on the value of p, rather than that of $s = s_1$. From this, we consider to use *different* number of indeterminates in computing $(PQ)^{p-1}$ and solving multivariate systems. In other words, we consider the cases of $s_1 \neq s_2$. In such a case, required time is roughly estimated as $q^{t-s_1}\,(t_{mlt} + q^{s_1-s_2}t_{GBslv})$. Hence, if p (or q) is large enough and if t_{GBslv} is negligible compared to t_{mlt}, we expect

$$q^{t-s_1}\left(t_{mlt} + q^{s_1-s_2}t_{GBslv}\right) \ll q^{t-s} \cdot (t_{mlt} + t_{GBslv}).$$

For example, if $q = 11$, $t = 10$, $s_1 = 9$, $s_2 = s = 5$, $t_{mlt} = 10$ (seconds) and $t_{GBslv} = 0.05$ (seconds), we estimate $q^{t-s}(t_{mlt} + t_{GBslv}) \approx 1618562$, whereas $q^{t-s_1}\,(t_{mlt} + q^{s_1-s_2}t_{GBslv}) \approx 8162$, which is about 198 times faster than using the previous version. We heuristically decided s_1 and s_2 from experimental computations for each case (Propositions 5.3.25 – 5.3.29 in Section 5.3.6).

5.3.3 Reduction of cubic forms

Enumeration Algorithms in the previous subsection requires to solve multivariate systems. In general, the number of indeterminates deeply affects the efficiency of solving multivariate systems. Hence it is important for the efficiency of our enumeration that we reduce the number. In this subsection, we give a reduction of cubic forms P by elements of the orthogonal similitude group $\tilde{\mathrm{O}}_\varphi(K)$ associated to the symmetric matrix φ of Q, which reduces the number as much as possible.

By the classification theory of quadratic forms, Q is isomorphic to either of (N1) $2xw + 2yz$, (N2) $2xw + y^2 - \epsilon z^2$ for $\epsilon \in \mathbb{F}_q^\times \smallsetminus (\mathbb{F}_q^\times)^2$ and (Dege) $2yw + z^2$ (cf. [43, Remark 2.1.1]). Hence we may assume that Q is one of them. We denote by φ the symmetric matrix associated to Q. Let $\mathrm{O}_\varphi(K)$ and $\tilde{\mathrm{O}}_\varphi(K)$ be the orthogonal group $\{g \in \mathrm{GL}_4(K) \mid {}^t g\varphi g = \varphi\}$ and the orthogonal similitude group $\{g \in \mathrm{GL}_4(K) \mid {}^t g\varphi g = \mu\varphi \text{ with } \mu \in K^\times\}$ respectively. We call $\mu = \mu(g)$ the similitude of g since μ is determined by g.

The orthogonal groups in the non-degenerate case

The symmetric matrix φ of Q in each case of (N1) and (N2) is respectively

$$\text{(N1):}\quad \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}, \qquad \text{(N2):}\quad \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -\epsilon & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix},$$

where $\epsilon \in K^\times \smallsetminus (K^\times)^2$. Recall the Bruhat decomposition of the orthogonal (similitude) group

$$\mathrm{O}_\varphi(K) = \mathrm{BWU} \quad \text{and} \quad \tilde{\mathrm{O}}_\varphi(K) = \tilde{\mathrm{B}}\mathrm{WU}$$

with $\mathrm{B} = \mathrm{ATU}$ and $\tilde{\mathrm{B}} = \mathrm{A}\tilde{\mathrm{T}}\mathrm{U}$, where A, T, $\tilde{\mathrm{T}}$, W and U in each case are given as follows.
(N1) We set $\mathrm{T} = \{\mathrm{diag}(a, b, b^{-1}, a^{-1}) \mid a, b \in K^\times\}$ and $\tilde{\mathrm{T}} = \{\mathrm{diag}(a, b, cb^{-1}, ca^{-1}) \mid a, b, c \in K^\times\}$,

$$\mathrm{U} = \left\{ \begin{pmatrix} 1 & a & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & -a \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & b & 0 \\ 0 & 1 & 0 & -b \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} : a, b \in K \right\}, \quad \mathrm{A} = \left\{ 1_4, \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \right\}$$

and $\mathrm{W} := \{1_4, s_1, s_2, s_1 s_2\}$ with

$$s_1 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \quad s_2 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}.$$

(N2) We set $\mathrm{A} := \{1_4, \mathrm{diag}(1,1,-1,1)\}$,

$$\mathrm{U} = \left\{ \begin{pmatrix} 1 & a & 0 & -a^2/2 \\ 0 & 1 & 0 & -a \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & b & b^2/(2\epsilon) \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & b/\epsilon \\ 0 & 0 & 0 & 1 \end{pmatrix} : a, b \in K \right\},$$

$$\mathrm{W} := \left\{ 1_4, \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} \right\}, \quad \tilde{\mathrm{C}} = \left\{ R(a,b) := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & a & \epsilon b & 0 \\ 0 & b & a & 0 \\ 0 & 0 & 0 & a^2 - \epsilon b^2 \end{pmatrix} : \begin{array}{c} a, b \in K, \\ a^2 - \epsilon b^2 \neq 0 \end{array} \right\}.$$

Put $\mathrm{C} = \{R(a,b) \in \tilde{\mathrm{C}} : a^2 - \epsilon b^2 = 1\}$ and $\mathrm{T} = \mathrm{HC}$ and $\tilde{\mathrm{T}} = \mathrm{H}\tilde{\mathrm{C}}$, where $\mathrm{H} = \{\mathrm{diag}(a,1,1,a^{-1}) : a \in K^\times\}$. Considering the reduction of cubic forms for (N2), we shall use the following lemma:

Lemma 5.3.8 ([43], Lemma 4.1.1) *Let V be the vector space consisting of cubics in y, z over K. Consider the natural representation of $\tilde{\mathrm{C}}$ on V.*

(1) *The representation V is the direct sum of two subrepresentations $V_1 := \langle y(y^2 - \epsilon z^2), z(y^2 - \epsilon z^2)\rangle$ and $V_2 := \langle y(y^2 + 3\epsilon z^2), z(3y^2 + \epsilon z^2)\rangle$.*

(2) *V_1 consists of four $\tilde{\mathrm{C}}$-orbits in V_1. They are the orbits of $\delta y(y^2 - \epsilon z^2)$ with $\delta \in \{0\} \cup K^\times/(K^\times)^3$ respectively.*

The orthogonal groups in the degenerate case

The symmetric matrix φ for the degenerate case is

$$\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}.$$

(Dege) As shown in [43, Lemma 4.2.1], we have the Bruhat decomposition

$$\mathrm{O}_\varphi(K) = (\mathrm{B} \sqcup \mathrm{B}s\mathrm{U})\mathrm{V} \quad \text{and} \quad \tilde{\mathrm{O}}_\varphi(K) = (\tilde{\mathrm{B}} \sqcup \tilde{\mathrm{B}}s\mathrm{U})\mathrm{V}$$

with $\mathrm{B} := \mathrm{ATU}$ and $\tilde{\mathrm{B}} := \mathrm{A}\tilde{\mathrm{T}}\mathrm{U}$, where $\mathrm{A} := \{1_4, \mathrm{diag}(1,1,-1,1)\}$,

$$\mathrm{T} := \left\{ T(a) := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & a & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & a^{-1} \end{pmatrix} : a \in K^\times \right\}, \quad \mathrm{U} := \left\{ U(a) := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & a & a^2(2\epsilon)^{-1} \\ 0 & 0 & 1 & a\epsilon^{-1} \\ 0 & 0 & 0 & 1 \end{pmatrix} : a \in K \right\},$$

$$s := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \quad \mathrm{V} = \left\{ \begin{pmatrix} a & b & c & d \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} : a \in K^\times \text{ and } b, c, d \in K \right\}$$

and $\tilde{\mathrm{T}} := \{\mathrm{diag}(1, b, b, b) : b \in K^\times\}\mathrm{T}$.

Reduction of cubic forms in the case of (N1)

Let K be a field with $\mathrm{char}(K) = p \neq 2$. Consider the case of $Q = 2xw + 2yz$. Let P be an irreducible cubic form in x, y, z, w over K. Assume that $C = V(Q, P)$ has a K-rational point. We use the same notation as in Section 5.3.3 (N1).

1. Considering $\bmod Q$, it suffices to consider only P which has no term containing xw.

$$\begin{aligned} P &= a_1x^3 + (a_2y + a_3z)x^2 + (a_4y^2 + a_5yz + a_6z^2)x \\ &\quad + a_7y^3 + a_8y^2z + a_9yz^2 + a_{10}z^3 \\ &\quad + (a_{11}y^2 + a_{12}yz + a_{13}z^2)w + (a_{14}y + a_{15}z)w^2 + a_{16}w^3. \end{aligned} \tag{5.3.1}$$

2. By the assumption $C(K) \neq \emptyset$ and considering the action of W, there is a rational point with non-zero w-coordinate. Let $(-bc, b, c, 1)$ be such a K-rational point on C, which provides us an element of $\mathrm{O}_\varphi(K)$

$$\begin{pmatrix} -bc & -b & -c & 1 \\ b & 0 & 1 & 0 \\ c & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

   Let P' be the cubic obtained by transforming P by this element. One can check that the x^3-coefficient of P' is $P(-bc, b, c, 1) = 0$. Thus we may assume that the x^3-coefficient a_1 of P is zero.

3. Now we have the following two cases:

   - If $a_2 \neq 0$ or $a_3 \neq 0$, then considering $y \leftrightarrow z$, we may assume $a_2 \neq 0$. Then the transformation of an element of U eliminates the xy^2-term and the xyz-term from P.
   - The case of $a_2 = a_3 = 0$. In this case C is singular at $(1, 0, 0, 0)$. Hence it suffices to consider only the case where $a_2 \neq 0$ or $a_3 \neq 0$.

4. The composition of a certain element $(x \mapsto cx, w \mapsto w/c,\ y \mapsto dy, z \mapsto z/d)$ of T and a constant-multiplication to the whole P transforms P into a cubic where the x^2y-coefficient is 1 and the x^2z-coefficient is 0 or a representative of an element of $K^\times/(K^\times)^2$ and the xz^2-coefficient is in $\{0, 1\}$.

Lemma 5.3.9 ([44], Lemma 3.4.1) *An element of* $\tilde{\mathrm{O}}_\varphi(K)$ *transforms* P *into*

$$\begin{aligned}&(y+b_1z)x^2+b_2xz^2\\&+a_1y^3+a_2y^2z+a_3yz^2+a_4z^3\\&+(a_5y^2+a_6yz+a_7z^2)w+(a_8y+a_9z)w^2+a_{10}w^3,\end{aligned}$$

for $a_1,\dots,a_{10}\in K$ *and for* $b_1\in\{0\}\cup K^\times/(K^\times)^2$ *and* $b_2\in\{0,1\}$.

We also have the following lemma on the reduction of cubic forms in the case of (N1).

Lemma 5.3.10 ([43], Lemma 4.3.1) *An element of* $\tilde{\mathrm{O}}_\varphi(K)$ *transforms* P *into*

(i)

$$\begin{aligned}&(a_1y+a_2z)x^2+a_3yzx+y^3+a_4z^3+b_1y^2z+a_5yz^2\\&+(a_6y^2+a_7yz+b_2z^2)w+(a_8y+a_9z)w^2+a_{10}w^3\end{aligned}$$

for $a_i\in K$ *with* $a_1\neq 0$, $a_2\neq 0$ *and for* $b_1\in\{0\}\cup K^\times/(K^\times)^2$ *and* $b_2\in\{0,1\}$, *or*

(ii)

$$\begin{aligned}&(a_1y+a_2z)x^2+a_3yzx+b_1y^2z+b_2yz^2\\&+(a_4y^2+a_5yz+b_3z^2)w+(a_6y+a_7z)w^2+a_8w^3\end{aligned}$$

for $a_i\in K$ *with* $a_1\neq 0$, $a_2\neq 0$ *and for* $b_1\in\{0,1\}$, $b_2\in\{0\}\cup K^\times/(K^\times)^2$ *and* $b_3\in\{0,1\}$.

Reduction of cubic forms in the case of (N2)

Let K be a field with $\mathrm{char}(K)=p\neq 2,3$. Recall that the quadratic form in (N2) case is $Q=2xw+y^2-\epsilon z^2$, where $\epsilon\notin(K^\times)^2$. Consider an irreducible cubic form P in $K[x,y,z,w]$. Assume that $C=V(Q,P)$ has a K-rational point. We use the same notation as in Section 5.3.3 (N2).

1. Considering $\bmod Q$, it suffices to consider only P which has no term containing xw.

2. By the assumption, we have a K-rational point (r,s,t,u) on C. If both of r and u were zero, then $Q(r,s,t,u)=0$ implies $s=t=0$. Hence $r\neq 0$ or $u\neq 0$. Considering the action of W, we may assume $u\neq 0$. Let $(-(b^2-\epsilon c^2)/2,b,c,1)$ be such a rational point on C, which provides us an element of $\mathrm{O}_\varphi(K)$

$$\begin{pmatrix}-(b^2-\epsilon c^2)/2 & -b & \epsilon c & 1\\ b & 1 & 0 & 0\\ c & 0 & 1 & 0\\ 1 & 0 & 0 & 0\end{pmatrix}.$$

Let P' be the cubic obtained by transforming P by this element. The x^3-coefficient of P' is $P(-(b^2-\epsilon c^2)/2,b,c,1)=0$. Thus we may assume that P has $a_1=0$.

3. Now we have the following two cases:

   - If $a_2 \neq 0$ or $a_3 \neq 0$, an element of U transforms P into a cubic of which x-coefficient is a constant-multiplication of $(y^2 - \epsilon z^2)$, where we used $p \neq 3$.
   - If $a_2 = a_3 = 0$, then C is singular at $(1, 0, 0, 0)$. Hence it suffices to consider only the case where $a_2 \neq 0$ or $a_3 \neq 0$.

4. The composition of an element of $\tilde{\mathrm{C}}$ and a constant-multiplication to the whole P transforms P into a cubic whose terms only in y, z is of the form

$$\alpha y(y^2 - \epsilon z^2) + \beta y(y^2 + 3\epsilon z^2) + \gamma z(3y^2 + \epsilon z^2)$$

   for $\alpha \in \{0, 1\}$ and some $\beta, \gamma \in K$. Here we use Lemma 5.3.8.

5. There is an element $(x \mapsto cx, w \mapsto w/c)$ of H such that it transforms P into a cubic whose z^2w-term is 0 or 1.

Thus we obtain the unconditional version of [43, Lemma 4.4.1]:

Lemma 5.3.11 *An element of* $\tilde{\mathrm{O}}_\varphi(K)$ *transforms* P *into the following form*

$$\begin{aligned}&(a_1y + a_2z)x^2 + a_3(y^2 - \epsilon z^2)x + b_1y(y^2 - \epsilon z^2) + a_4y(y^2 + 3\epsilon z^2) + a_5z(3y^2 + \epsilon z^2)\\ &+(a_6y^2 + a_7yz + b_2z^2)w + (a_8y + a_9z)w^2 + a_{10}w^3\end{aligned}$$

for some $a_i \in K$ *with* $(a_1, a_2) \neq (0, 0)$ *and for* $b_1, b_2 \in \{0, 1\}$.

Degenerate case

We assume that $p \neq 2, 3$. The case of $q > 5$ has been treated in [43, Section 4.5]. Here we study the case of $q = 5$. Assume $K = \mathbb{F}_5$ before the next lemma.

1. An element $(x \mapsto x + ay + bz + cw)$ of V transforms P into a cubic without terms of x^2y, x^2z, x^2w. We may assume that the coefficients of x^2y, x^2z, x^2w of P are zero.

2. Considering $\bmod Q$, we may assume that there is no term containing yw in P, since $yw \equiv -2^{-1}z^2 \bmod Q$.

3. (I) If there exists an element of $\mathrm{O}_\varphi(\mathbb{F}_5)$ stabilizing x which transforms P into P' with non-zero term of y^3, an element of U transforms P' into one without term of y^2z, and the same reduction as steps 4, 5 in [43, Section 4.5] works. The final reduced form is as in Lemma 5.3.12 (1) below, which is of the same form as in the case of $q > 5$.

   (II) Otherwise P has to be of the form

$$a_0x^3 + (a_1y^2 + a_2z^2 + a_3w^2 + a_4yz + a_5zw)x + a_6(y^2z + zw^2). \tag{5.3.2}$$

   Indeed, we may consider only P whose y^3-term and w^3-term are zero, considering the action of s (the transposition of y and w). The general form of P is

$$a_0x^3 + (a_1y^2 + a_2z^2 + a_3w^2 + a_4yz + a_5zw)x + a_6y^2z + a_7yz^2 + a_8z^3 + a_9z^2w + a_{10}zw^2.$$

The element of $s\,\mathrm{U}\,s$ given by $z \mapsto z - cy$, $w \mapsto w + cz - 2^{-1}c^2y$ for $c \in \mathbb{F}_5$ transforms P into a cubic form, whose y^3-coefficient is

$$(a_{10} - a_6)c + a_7c^2 - a_8c^3 + 2a_9c^4.$$

This is zero for every $c \in \mathbb{F}_5$ if and only if $a_6 = a_{10}$ and $a_7 = a_8 = a_9 = 0$. As P is irreducible, we have $a_6 \neq 0$.

Remaining steps in case (II):

4. Composing some element $(y \mapsto cy, w \mapsto w/c)$ of T and some constant-multiplication to the whole P, we transform P into a cubic where a_6 in (5.3.2) is 1 and a_5 is 0 or $a_0^{1/3}$. Here we used $(\mathbb{F}_5^\times)^3 = \mathbb{F}_5^\times$.

5. The transformation $x \mapsto d \cdot x$ for a certain $d \in K^\times$ sends P to a cubic whose coefficient of x^3 is 1. Then the coefficient of xzw becomes 0 or 1 in case (II).

Summarizing this reduction for $q = 5$ and that for $q > 5$ obtained in [43, Lemma 4.5.1], we have the following lemma:

Lemma 5.3.12 *An element of $\tilde{\mathrm{O}}_\varphi(K)$ transforms P into the following form* (1) *if $\#K > 5$, and into either of the following forms* (1) *and* (2) *if $\#K = 5$.*

(1)
$$\begin{aligned} &a_0x^3 + (a_1y^2 + a_2z^2 + a_3w^2 + a_4yz + a_5zw)x \\ &+a_6y^3 + a_7z^3 + a_8w^3 + a_9yz^2 + b_1z^2w + b_2zw^2, \end{aligned}$$

for some $a_i \in K$ with $a_0, a_6 \in K^\times$ and for $b_1, b_2 \in \{0, 1\}$, where the leading coefficient of $R := a_1y^2 + a_2z^2 + a_3w^2 + a_4yz + a_5zw$ is 1 or $R = 0$;

(2)
$$x^3 + (a_1y^2 + a_2z^2 + a_3w^2 + a_4yz + b_1zw)x + y^2z + zw^2$$

for $a_i \in K = \mathbb{F}_5$ and $b_1 \in \{0, 1\}$.

5.3.4 Isomorphism testing

This subsection gives a computational method for determining whether two nonhyperelliptic curves of genus 4 over a perfect field K are isomorphic or not. Let $K = \mathbb{F}_q$ denote the finite field with q elements. Let Q an irreducible quadratic form in $K[x, y, z, w]$, and φ the symmetric matrix associated to Q. Let $C_1 = V(Q, P_1)$ and $C_2 = V(Q, P_2)$ be two nonhyperelliptic curves of genus 4 over K with irreducible cubic forms P_1 and P_2 in $K[x, y, z, w]$. The two curves C_1 and C_2 are isomorphic over K if and only if there exists $g \in \tilde{\mathrm{O}}_\varphi(K)$ such that

$$g \cdot P_1 \equiv \lambda P_2 \bmod Q \tag{5.3.3}$$

for some $\lambda \in K^\times$. With this fact and the Bruhat decomposition of $\tilde{\mathrm{O}}_\varphi(K)$, we present an algorithm for testing whether two curves of genus 4 are isomorphic over K or not. Let us describe an algorithm only for (N1) in this thesis, since algorithms for the cases (N2) and (Dege) can be constructed in ways similar to (N1), see Remark 5.3.13.

Now we consider the case (N1), that is, $Q = 2xw + 2yz$ with

$$\varphi = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

As in Section 5.3.3, put

$$\mathrm{T} := \{\mathrm{diag}(a, b, b^{-1}, a^{-1}) : a, b \in K^\times\}, \quad \tilde{\mathrm{T}} := \{\mathrm{diag}(a, b, cb^{-1}, ca^{-1}) : a, b, c \in K^\times\},$$

$$U_1(a) := \begin{pmatrix} 1 & a & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & -a \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad U_2(b) := \begin{pmatrix} 1 & 0 & b & 0 \\ 0 & 1 & 0 & -b \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad \mathrm{U} := \{U_1(a)U_2(b) : a, b \in K\},$$

$$\mathrm{A} := \left\{ 1_4, \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \right\}, \quad s_1 := \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \quad s_2 := \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}.$$

Put $\mathrm{W} := \{1_4, s_1, s_2, s_1 s_2\}$, $\mathrm{B} := \mathrm{ATU}$ and $\tilde{\mathrm{B}} := \mathrm{A}\tilde{\mathrm{T}}\mathrm{U}$. Recall from Section 5.3.3 that the Bruhat decomposition for (N1) is given by

$$\mathrm{O}_\varphi(K) = \mathrm{BWU} \quad \text{and} \quad \tilde{\mathrm{O}}_\varphi(K) = \tilde{\mathrm{B}}\mathrm{WU}.$$

Given irreducible cubic forms P_1 and P_2 in $K[x, y, z, w]$, we give an algorithm for testing whether $V(Q, P_1)$ and $V(Q, P_2)$ are isomorphic over K or not. The correctness of this algorithm is straightforward from its construction.

Isomorphism Testing Algorithm for (N1) With notation as above,

Input: A power of primes q, an integer $q' \in \{0, q\}$, and two cubic forms P_1 and P_2 in $\mathbb{F}_q[x, y, z, w]$.

Output: "Isomorphic" or "Not isomorphic".

(0) Let $K = \mathbb{F}_q$ if $q' = q$, and $K = \overline{\mathbb{F}_q}$ if $q' = 0$.

(1) Let $t_1, \ldots, t_7$ and λ be indeterminates.

(2) For each $M_\mathrm{A} \in \mathrm{A}$ and $M_\mathrm{W} \in \mathrm{W}$, proceed with the following four steps:

2a. Put $M_{\tilde{\mathrm{T}}} := \mathrm{diag}(t_1, t_2, t_3 t_2^{-1}, t_3 t_1^{-1}) \in \tilde{\mathrm{T}}$, and compute

$$g := M_\mathrm{A} \cdot M_{\tilde{\mathrm{T}}} \cdot U_1(t_4) \cdot U_2(t_5) \cdot M_\mathrm{W} \cdot U_1(t_6) \cdot U_2(t_7).$$

2b. Construct a multivariate system from the equation (5.3.3) together with

$$t_i^{q'-1} = 1 \text{ for } 1 \le i \le 3, \quad t_j^{q'} = t_j \text{ for } 4 \le j \le 7, \text{ and } \quad \lambda^{q'-1} = 1.$$

Let $\mathcal{S} \subset K[t_1, t_2, t_3, t_4, t_5, t_6, t_7, \lambda]$ be the set of defining polynomials for the system.

2c. Compute the reduced Gröbner basis G for the ideal $\langle \mathcal{S} \rangle$.

2d. If $\#G \neq 1$, output "Isomorphic".

If the systems have no solution over K, i.e., $\#G = 1$ for all $M_{\mathrm{A}} \in \mathrm{A}$ and $M_{\mathrm{W}} \in \mathrm{W}$, then output "Not isomorphic". In this case, $V(Q, P_1)$ and $V(Q, P_2)$ are not isomorphic over K.

Remark 5.3.13 Based on the Bruhat decompositions given in Section 5.3.3, we can also construct an algorithm for each of (N2) and (Dege) as a variant of Isomorphism Testing Algorithm for (N1).

5.3.5 Proofs of main theorems

Proof of Theorem 5.3.1. Let C be a curve of genus 4 over $K = \mathbb{F}_{25}$. As we mentioned in Section 5.2, there is no superspecial hyperelliptic curve in characteristic 5. Hence we may assume that C is nonhyperelliptic, and is written as $C = V(Q, P)$ for an irreducible quadratic form Q and an irreducible cubic form P in $\mathbb{F}_{25}[x, y, z, w]$. We may also assume that Q is either of (N1) $2xw + 2yz$ and (N2) $2xw + y^2 - \epsilon z^2$, or (Dege) $2yw + z^2$, where ϵ is an element of $\mathbb{F}_{25}^{\times} \smallsetminus (\mathbb{F}_{25}^{\times})^2$.

First we show that there does not exist a superspecial curve $C = V(Q, P)$ if Q is non-degenerate. By Lemma 5.1.1, if such a superspecial curve exists, then it has at least one $\mathbb{F}_{25}$-rational point. Thus we may assume that $\#C(\mathbb{F}_{25}) \neq 0$. By Lemmas 5.3.10 and 5.3.11, we may also assume that P is of the following form:

(N1) (i)

$$\begin{aligned} P &= (a_1 y + a_2 z)x^2 + a_3 yzx + y^3 + a_4 z^3 + b_1 y^2 z + a_5 yz^2 \\ &\quad + (a_6 y^2 + a_7 yz + b_2 z^2)w + (a_8 y + a_9 z)w^2 + a_{10} w^3, \end{aligned}$$

where $a_i \in K$ with $a_1 \neq 0$, $a_2 \neq 0$, $b_1 \in \{0\} \cup K^{\times}/(K^{\times})^2$ and $b_2 \in \{0, 1\}$.

(N1) (ii)

$$\begin{aligned} P &= (a_1 y + a_2 z)x^2 + a_3 yzx + b_1 y^2 z + b_2 yz^2 \\ &\quad + (a_4 y^2 + a_5 yz + b_3 z^2)w + (a_6 y + a_7 z)w^2 + a_8 w^3, \end{aligned}$$

where $a_i \in K$ with $a_1 \neq 0$, $a_2 \neq 0$, $b_1 \in \{0, 1\}$, $b_2 \in \{0\} \cup K^{\times}/(K^{\times})^2$ and $b_3 \in \{0, 1\}$.

(N2)

$$\begin{aligned} P &= (a_1 y + a_2 z)x^2 + a_3(y^2 - \epsilon z^2)x + b_1 y(y^2 - \epsilon z^2) + a_4 y(y^2 + 3\epsilon z^2) + a_5 z(3y^2 + \epsilon z^2) \\ &\quad + (a_6 y^2 + a_7 yz + b_2 z^2)w + (a_8 y + a_9 z)w^2 + a_{10} w^3, \end{aligned}$$

where $a_i \in K$ with $(a_1, a_2) \neq (0, 0)$ and $b_1, b_2 \in \{0, 1\}$.

It follows from Propositions 5.3.17 – 5.3.19 in Section 5.3.6 that for each of the above cases (N1) (i), (ii) and (N2), there does not exist any cubic form P of the form stated in the case such that $V(Q, P)$ is a superspecial curve.

Next we consider the degenerate case (Dege): $Q = 2yw + z^2$.

(Dege) By Lemma 5.3.12, we may assume that P is of the form

$$\begin{aligned} P &= a_0x^3 + a_1xy^2 + a_2xz^2 + a_3xw^2 + a_4xyz + a_5xzw \\ &\quad + a_6y^3 + a_7z^3 + a_8w^3 + a_9yz^2 + b_1z^2w + b_2zw^2, \end{aligned}$$

where $a_i \in K$ with $a_0, a_6 \in K^\times$, $b_1, b_2 \in \{0, 1\}$. It follows from Proposition 5.3.20 in Section 5.3.6 that $V(Q, P)$ is superspecial if and only if $a_0, a_6, a_8 \in \mathbb{F}_{25}^\times$, $b_2 \in \{0, 1\}$, $a_i = 0$ for $i = 1, \ldots, 5, 7, 9$ and $b_1 = 0$. □

Using Theorem 5.3.1, we give a computational proof of the uniqueness of superspecial curve of genus 4 over the algebraic closure $\overline{K}$, see [25] for the original and theoretical proof.

Corollary 5.3.14 ([43], Corollary 5.1.1) *All superspecial curves of genus* 4 *in characteristic* 5 *are isomorphic to each other over an algebraically closed field.*

Proof. It suffices to prove that the superspecial curves listed in Theorem 5.3.1 are all isomorphic over $\overline{K}$. By the transformation $(x \mapsto x, y \mapsto \lambda\mu y, z \mapsto \mu z, w \mapsto \frac{\mu}{\lambda} w)$, one has the following cubic equation

$$x^3 + a_1\lambda^3\mu^3y^3 + a_2\frac{\mu^3}{\lambda^3}w^3 + a_3\frac{\mu^3}{\lambda^2}zw^2 = 0.$$

Since there exists $(\lambda, \mu) \in (\overline{K})^{\oplus 2}$ such that $a_1\lambda^3\mu^3 = 1$ and $a_2\frac{\mu^3}{\lambda^3} = 1$, we may consider only the following form:

$$C_\alpha : \quad x^3 + y^3 + w^3 + \alpha zw^2 = 0.$$

By a computation with Gröbner bases, we have that there exists an element of BsU over $\overline{K}$ transforming C_0 to C_α, where we regard some entries of matrices in BsU as indeterminates (cf. Remark 5.3.15). □

Remark 5.3.15 One can verify the claim of the last sentence in the proof of Corollary 5.3.14 from our computation programs over Magma [6], [9] and Maple [58]. The programs with outputs are available at the web page of the first author [59].

Proof of Theorem 5.3.2. Similarly to the proof of Theorem 5.3.2, the theorem follows from Propositions 5.3.21 – 5.3.24 in Section 5.3.6. □

Proof of Theorem 5.3.4. Let C be a curve of genus 4. In a way similar to the proof of Theorem 5.3.1, we may assume that C is nonhyperelliptic, and is written as $C = V(Q, P)$ for an irreducible quadratic form Q and an irreducible cubic form P in $\mathbb{F}_5[x, y, z, w]$. We may also assume that Q is either of (N1) $2xw + 2yz$, (N2) $2xw + y^2 - \epsilon z^2$, or (Dege) $2yw + z^2$, where ϵ is an element in $\mathbb{F}_5^\times \setminus (\mathbb{F}_5^\times)^2$. Moreover it suffices to consider the case (Dege), say $Q = 2yw + z^2$. By Lemma 5.3.12, we may assume that the P is of the following form:

(1)

$$\begin{aligned} &a_0x^3 + (a_1y^2 + a_2z^2 + a_3w^2 + a_4yz + a_5zw)x \\ &+ a_6y^3 + a_7z^3 + a_8w^3 + a_9yz^2 + b_1z^2w + b_2zw^2 \end{aligned}$$

where $a_i \in K = \mathbb{F}_5$ with $a_0, a_6 \in K^\times = \mathbb{F}_5^\times$ and $b_1, b_2 \in \{0, 1\}$, or

(2)
$$x^3 + (a_1y^2 + a_2z^2 + a_3w^2 + a_4yz + b_1zw)x + y^2z + zw^2$$
where $a_i \in K = \mathbb{F}_5$ and $b_1 \in \{0, 1\}$.

By Proposition 5.3.25 in Section 5.3.6, we have that the $\mathbb{F}_5$-isomorphism classes of superspecial curves of genus 4 over $\mathbb{F}_5$ are given by $C = V(Q, P_i)$ for $1 \le i \le 7$. □

Proof of Theorem 5.3.5. Let C be a nonhyperelliptic curve of genus 4 over $\mathbb{F}_{11}$. The curve C is written as $C = V(Q, P)$ for an irreducible quadratic form Q and an irreducible cubic form P in $\mathbb{F}_{11}[x, y, z, w]$, where Q is either of (N1) $2xw + 2yz$, (N2) $2xw + y^2 - \epsilon z^2$ and (Dege) $Q = 2yw + z^2$. Here ϵ is an element in $\mathbb{F}_{11}^\times \smallsetminus (\mathbb{F}_{11}^\times)^2$. Let $\zeta := \zeta^{(11)}$ be a generator of the cyclic group $\mathbb{F}_{11}^\times$. We first consider the non-degenerate cases (N1) and (N2).

(N1): By Lemma 5.3.9, we may assume that P is of the following form:
$$\begin{aligned} P =&(y + b_1z)x^2 + b_2xz^2 \\ &+ a_1y^3 + a_2y^2z + a_3yz^2 + a_4z^3 \\ &+ (a_5y^2 + a_6yz + a_7z^2)w + (a_8y + a_9z)w^2 + a_{10}w^3, \end{aligned}$$
where $a_1, \dots, a_{10} \in \mathbb{F}_{11}$, $b_1 \in \{0, 1, \zeta\}$ and $b_2 \in \{0, 1\}$. It follows from Proposition 5.3.27 in Section 5.3.6 that $V(Q, P)$ is superspecial, up to isomorphism over $\mathbb{F}_{11}$, if and only if P is one of $P_i^{(\mathrm{N1})}$ for $1 \le i \le 8$.

(N2): By Lemma 5.3.11, we may assume that P is of the following form:
$$\begin{aligned} P =&(a_1y + a_2z)x^2 + a_3(y^2 - \epsilon z^2)x + b_1y(y^2 - \epsilon z^2) + a_4y(y^2 + 3\epsilon z^2) + a_5z(3y^2 + \epsilon z^2) \\ &+ (a_6y^2 + a_7yz + b_2z^2)w + (a_8y + a_9z)w^2 + a_{10}w^3, \end{aligned}$$
where $a_i \in \mathbb{F}_{11}$ with $(a_1, a_2) \ne (0, 0)$ and $b_1, b_2 \in \{0, 1\}$. It follows from Proposition 5.3.28 in Section 5.3.6 that $V(Q, P)$ is superspecial, up to isomorphism over $\mathbb{F}_{11}$, if and only if P is one of $P_i^{(\mathrm{N2})}$ for $1 \le i \le 5$.

Next let us consider the degenerate case (Dege): $Q = 2yw + z^2$.

(Dege): By Lemma 5.3.12, we may assume that P is of the following form:
$$\begin{aligned} P =&a_0x^3 + (a_1y^2 + a_2z^2 + a_3w^2 + a_4yz + a_5zw)x \\ &+ a_6y^3 + a_7z^3 + a_8w^3 + a_9yz^2 + b_1z^2w + b_2zw^2, \end{aligned}$$
where $a_i \in \mathbb{F}_{11}$ with $a_0, a_6 \in \mathbb{F}_{11}^\times$ and $b_1, b_2 \in \{0, 1\}$. It follows from Proposition 5.3.29 in Section 5.3.6 that $V(Q, P)$ is superspecial, up to isomorphism over $\mathbb{F}_{11}$, if and only if P is one of $P_i^{(\mathrm{Dege})}$ for $1 \le i \le 17$.

Summarizing the above descriptions, we have the theorem. □

Corollary 5.3.16 *Any nonhyperelliptic superspecial curve of genus* 4 *over* $\mathbb{F}_{11}$ *is isomorphic over* $\overline{\mathbb{F}_{11}}$ *to one of the curves* $V(Q^{(\mathrm{N1})}, P_i^{(\mathrm{alc})})$ *for* $1 \leq i \leq 3$, *or* $V(Q^{(\mathrm{Dege})}, P_j^{(\mathrm{alc})})$ *for* $4 \leq j \leq 9$, *where* $Q^{(\mathrm{N1})} := 2xw + 2yz$, $Q^{(\mathrm{Dege})} := 2yw + z^2$ *and*

$$\begin{aligned}
P_1^{(\mathrm{alc})} &:= x^2y + x^2z + 2y^2z + 5y^2w + 9yz^2 + yzw + 4z^3 + 3z^2w + 10zw^2 + w^3,\\
P_2^{(\mathrm{alc})} &:= x^2y + x^2z + y^3 + y^2z + 7yz^2 + 4yw^2 + 2z^3 + 9zw^2,\\
P_3^{(\mathrm{alc})} &:= x^2y + x^2z + y^3 + 8y^2z + 3yz^2 + 10yw^2 + 10z^3 + 10zw^2,\\
P_4^{(\mathrm{alc})} &:= x^3 + y^3 + w^3,\\
P_5^{(\mathrm{alc})} &:= x^3 + y^3 + z^3 + 5w^3,\\
P_6^{(\mathrm{alc})} &:= x^3 + xw^2 + y^3,\\
P_7^{(\mathrm{alc})} &:= x^3 + xzw + y^3 + 7z^3 + w^3,\\
P_8^{(\mathrm{alc})} &:= x^3 + xyz + xw^2 + y^3 + 5z^3 + 4w^3,\\
P_9^{(\mathrm{alc})} &:= x^3 + xyz + 6xw^2 + y^3 + 8z^3 + 8w^3.
\end{aligned}$$

Proof. The result follows from the proof of Theorem 5.3.5 together with Propositions 5.3.27 – 5.3.29 and 5.3.31. □

5.3.6 Computational parts of our proofs

In this subsection, we give computational results, which help proving our main theorems (Theorems 5.3.1 – 5.3.5) and Corollaries 5.3.14 and 5.3.16. Our computational results are obtained by executing algorithms given in Sections 5.3.2 and 5.3.4. We implemented and executed the computations over Magma [6], [9] in its 64-bit student version. Specifically our computations for Propositions 5.3.17 – 5.3.24 were conducted on a computer with Magma V2.22-3, Windows 10 OS at 2.60 GHz CPU (Intel Core i5) and 8 GB memory. Our computations for Propositions 5.3.25 – 5.3.29 and Corollary 5.3.31 were conducted on a computer with Windows 10 home OS at 3.40 GHz CPU (Intel Core i7) and 20 GB memory. The source codes and the log files are available at [59] and [60]. For the details of our computational setting, including timing data, see also [43, Section 5.4] and [44, Section 4.5].

Case of (N1) (i) for $q = 25$

Proposition 5.3.17 *Consider the quadratic form* $Q = 2xw + 2yz \in \mathbb{F}_{25}[x, y, z, w]$ *and*

$$\begin{aligned}
P &= (a_1y + a_2z)x^2 + a_3yzx + y^3 + a_4z^3 + b_1y^2z + a_5yz^2\\
&\quad +(a_6y^2 + a_7yz + b_2z^2)w + (a_8y + a_9z)w^2 + a_{10}w^3,
\end{aligned}$$

where $a_i \in \mathbb{F}_{25}$ *with* $a_1, a_2 \in \mathbb{F}_{25}^{\times}$, $b_1 \in \{0, 1, \epsilon\}$ *and* $b_2 \in \{0, 1\}$, *and where* ϵ *is an element of* $\mathbb{F}_{25}^{\times} \smallsetminus (\mathbb{F}_{25}^{\times})^2$. *Then there does not exist* $(b_1, b_2, a_1, \ldots, a_{10})$ *such that* $V(Q, P)$ *is superspecial.*

Proof. For the inputs $K = \mathbb{F}_{25}$ with $p = 5$, $Q = 2xw + 2yz \in \mathbb{F}_{25}[x, y, z, w]$ and

$$\{yx^2, zx^2, yzx, y^3, z^3, y^2z, yz^2, y^2w, yzw, z^2w, yw^2, zw^2, w^3\},$$

we execute First Enumeration Algorithm in Section 5.3.2. For our choice of coefficients to be regarded as indeterminates in solving multivariate systems, we state it below. Specifically we proceed with the following. We set $\mathcal{P} := \emptyset$. Put

$$\begin{aligned}\{p_1, \ldots, p_t\} &= \{yx^2, zx^2, yzx, z^3, yz^2, y^2w, yzw, yw^2, zw^2, w^3\},\\ \{q_1, \ldots, q_u\} &= \{y^2z, z^2w\}.\end{aligned}$$

with $t = 10$, $u = 2$.

(1) Put $s := 8$, and $(i_1, \ldots, i_8) := (3, 4, 5, 6, 7, 8, 9, 10)$ (we regard the 8 coefficients a_3, a_4, a_5, a_6, a_7, a_8, a_9 and a_{10} as indeterminates). For solving systems of multivariate equations over $\mathbb{F}_{25}[a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}]$ in the next step, we adopt the graded reverse lexicographical (grevlex) order with

$$a_{10} \prec a_9 \prec a_4 \prec a_8 \prec a_7 \prec a_5 \prec a_6 \prec a_3.$$

For $\mathbb{F}_{25}[x, y, z, w]$, we adopt the grevlex order with $w \prec z \prec y \prec x$.

(2) For each $b_1 \in \{0, 1, \epsilon\}$, $b_2 \in \{0, 1\}$ and $(a_1, a_2) \in \mathbb{F}_{25}^{\times} \times \mathbb{F}_{25}^{\times}$, we conduct the following procedures:

(a) Compute $h := (PQ)^{p-1}$ over $\mathbb{F}_{25}[a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}][x, y, z, w]$, where a_3, a_4, a_5, a_6, a_7, a_8, a_9 and a_{10} are indeterminates.

(b) Let $\mathcal{S}$ be the set of the coefficients of $\mathcal{M}$ in h, where $\mathcal{M}$ consists of the 16 monomials in Corollary 5.3.6. Note that $\mathcal{S} \subset \mathbb{F}_{25}[a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}]$.

(c) Solve the system of multivariate equations $f(a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}) = 0$ for all $f \in \mathcal{S}$ over $\mathbb{F}_{25}$ with known algorithms via the Gröbner basis computation.

(d) For each root $(a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10})$ of the system, substitute it into unknown coefficients in P, and decide whether $C = V(Q, P)$ is non-singular or not. If C is non-singular, then replace $\mathcal{P}$ by $\mathcal{P} \cup \{P\}$.

The outputs of our computation show $\mathcal{P} = \emptyset$, and hence there does not exist $(b_1, b_2, a_1, \ldots, a_{10})$ such that $V(Q, P)$ is superspecial. □

Case of (N1) (ii) for $q = 25$

Proposition 5.3.18 *Consider the quadratic form $Q = 2xw + 2yz \in \mathbb{F}_{25}[x, y, z, w]$ and*

$$\begin{aligned}P &= (a_1y + a_2z)x^2 + a_3yzx + b_1y^2z + b_2yz^2\\ &\quad +(a_4y^2 + a_5yz + b_3z^2)w + (a_6y + a_7z)w^2 + a_8w^3,\end{aligned}$$

where $a_i \in \mathbb{F}_{25}$ with $a_1, a_2 \in \mathbb{F}_{25}^{\times}$, $b_1 \in \{0, 1\}$, $b_2 \in \{0, 1, \epsilon\}$ and $b_3 \in \{0, 1\}$, and where ϵ is an element of $\mathbb{F}_{25}^{\times} \setminus (\mathbb{F}_{25}^{\times})^2$. Then there does not exist $(b_1, b_2, b_3, a_1, \ldots, a_8)$ such that $V(Q, P)$ is superspecial.

Proof. For the inputs $K = \mathbb{F}_{25}$ with $p = 5$, $Q = 2xw + 2yz \in \mathbb{F}_{25}[x, y, z, w]$ and

$$\{yx^2, zx^2, yzx, y^2z, yz^2, y^2w, yzw, z^2w, yw^2, zw^2, w^3\},$$

we execute First Enumeration Algorithm in Section 5.3.2. For our choice of coefficients to be regarded as indeterminates in solving multivariate systems, we state it below. Specifically we proceed with the following. We set $\mathcal{P} := \emptyset$. Put

$$\begin{aligned}\{p_1, \ldots, p_t\} &= \{yx^2, zx^2, yzx, y^2w, yzw, yw^2, zw^2, w^3\},\\ \{q_1, \ldots, q_u\} &= \{y^2z, yz^2, z^2w\}.\end{aligned}$$

with $t = 8$, $u = 3$.

(1) Put $s := 6$, and $(i_1, \ldots, i_6) := (3, 4, 5, 6, 7, 8)$ (we regard the 6 coefficients a_3, a_4, a_5, a_6, a_7 and a_8 as indeterminates). For solving systems of multivariate equations over $\mathbb{F}_{25}[a_3, a_4, a_5, a_6, a_7, a_8]$ in the next step, we adopt the grevlex order with

$$a_8 \prec a_7 \prec a_6 \prec a_5 \prec a_4 \prec a_3.$$

For $\mathbb{F}_{25}[x, y, z, w]$, we adopt the grevlex order with $w \prec z \prec y \prec x$.

(2) For each $b_1 \in \{0, 1\}$, $b_2 \in \{0, 1, -\epsilon\}$, $b_3 \in \{0, 1\}$ and $(a_1, a_2) \in \mathbb{F}_{25}^{\times} \times \mathbb{F}_{25}^{\times}$, as in Case of (N1) (i) for $q = 25$, we enumerate $(a_3, a_4, a_5, a_6, a_7, a_8)$ such that $C = V(Q, P)$ is superspecial.

The outputs of our computation show that the resulting list $\mathcal{P}$ is empty, and hence there does not exist $(b_1, b_2, b_3, a_1, \ldots, a_8)$ such that $V(Q, P)$ is superspecial. □

Case of (N2) for $q = 25$

Proposition 5.3.19 *Consider the quadratic form $Q = 2xw + y^2 - \epsilon z^2 \in \mathbb{F}_{25}[x, y, z, w]$ and*

$$\begin{aligned}P &= (a_1y + a_2z)x^2 + a_3(y^2 - \epsilon z^2)x + b_1y(y^2 - \epsilon z^2) + a_4y(y^2 + 3\epsilon z^2) + a_5z(3y^2 + \epsilon z^2)\\ &\quad +(a_6y^2 + a_7yz + b_2z^2)w + (a_8y + a_9z)w^2 + a_{10}w^3,\end{aligned}$$

where ϵ is an element of $\mathbb{F}_{25}^{\times} \smallsetminus (\mathbb{F}_{25}^{\times})^2$, and where $a_i \in \mathbb{F}_{25}$ with $(a_1, a_2) \neq (0, 0)$ and $b_1, b_2 \in \{0, 1\}$. Then there does not exist $(b_1, b_2, a_1, \ldots, a_{10})$ such that $V(Q, P)$ is superspecial.

Proof. For the inputs $K = \mathbb{F}_{25}$ with $p = 5$, $Q = 2xw + y^2 - \epsilon z^2 \in \mathbb{F}_{25}[x, y, z, w]$ and

$$\{yx^2, zx^2, (y^2 - \epsilon z^2)x, y(y^2 - \epsilon z^2), y(y^2 + 3\epsilon z^2), z(3y^2 + \epsilon z^2), y^2w, yzw, z^2w, yw^2, zw^2, w^3\},$$

we execute First Enumeration Algorithm in Section 5.3.2. For our choice of coefficients to be regarded as indeterminates in solving multivariate systems, we state it below. Specifically we proceed with the following. We set $\mathcal{P} := \emptyset$. Put

$$\begin{aligned}\{p_1, \ldots, p_t\} &= \{yx^2, zx^2, (y^2 - \epsilon z^2)x, y(y^2 + 3\epsilon z^2), z(3y^2 + \epsilon z^2), y^2w, yzw, yw^2, zw^2, w^3\},\\ \{q_1, \ldots, q_u\} &= \{y(y^2 - \epsilon z^2), z^2w\}.\end{aligned}$$

with $t = 10$, $u = 2$.

(1) Put $s := 8$, and $(i_1, \ldots, i_8) := (3, 4, 5, 6, 7, 8, 9, 10)$ (we regard the 8 coefficients a_3, a_4, a_5, a_6, a_7, a_8, a_9 and a_{10} as indeterminates). For solving systems of multivariate equations over $\mathbb{F}_{25}[a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}]$ in the next step, we adopt the grevlex order with

$$a_{10} \prec a_9 \prec a_8 \prec a_7 \prec a_6 \prec a_5 \prec a_4 \prec a_3.$$

For $\mathbb{F}_{25}[x, y, z, w]$, we adopt the grevlex order with $w \prec z \prec y \prec x$.

(2) For each $b_1, b_2 \in \{0,1\}$ and $(a_1, a_2) \in (\mathbb{F}_{25} \times \mathbb{F}_{25}) \setminus \{(0,0)\}$, as in Case of (N1) (i) for $q = 25$, we enumerate $(a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10})$ such that $C = V(Q, P)$ is superspecial.

The outputs of our computation show that the resulting list $\mathcal{P}$ is empty, and hence there does not exist $(b_1, b_2, b_3, a_1, \ldots, a_{10})$ such that $V(Q, P)$ is superspecial. □

Case of (Dege) for $q = 25$

Proposition 5.3.20 *Consider the degenerate quadratic form $Q = 2yw + z^2 \in \mathbb{F}_{25}[x, y, z, w]$ and*

$$\begin{aligned} P &= a_0x^3 + (a_1y^2 + a_2z^2 + a_3w^2 + a_4yz + a_5zw)x \\ &\quad + a_6y^3 + a_7z^3 + a_8w^3 + a_9yz^2 + b_1z^2w + b_2zw^2, \end{aligned}$$

where $a_i \in \mathbb{F}_{25}$ with $a_0, a_6 \neq 0$ and $b_1, b_2 \in \{0,1\}$. Then $V(Q, P)$ is superspecial if and only if $a_0, a_6, a_8 \in \mathbb{F}_{25}^{\times}$, $b_2 \in \{0,1\}$, $a_i = 0$ for $i = 1, \ldots, 5, 7, 9$ and $b_1 = 0$.

Moreover the number of the $\mathbb{F}_{25}$-isomorphism classes in the set of curves defined by Q and the enumerated P is 21.

Proof. For the inputs $K = \mathbb{F}_{25}$ with $p = 5$, $Q = 2yw + z^2 \in \mathbb{F}_{25}[x, y, z, w]$ and

$$\{x^3, y^2x, z^2x, w^2x, yzx, zwx, y^3, z^3, w^3, yz^2, z^2w, zw^2\},$$

we execute First Enumeration Algorithm in Section 5.3.2. For our choice of coefficients to be regarded as indeterminates in solving multivariate systems, we state it below. Specifically we proceed with the following. We set $\mathcal{P} := \emptyset$. Put

$$\begin{aligned} \{p_1, \ldots, p_t\} &= \{x^3, xy^2, xz^2, xw^2, xyz, xzw, y^3, z^3, w^3, yz^2\}, \\ \{q_1, \ldots, q_u\} &= \{z^2w, zw^2\}. \end{aligned}$$

with $t = 10$, $u = 2$.

(1) Put $s := 7$, and $(i_1, \ldots, i_7) := (2, 3, 4, 5, 7, 8, 9)$ (we regard the 7 coefficients a_2, a_3, a_4, a_5, a_7, a_8 and a_9 as indeterminates). For solving systems of multivariate equations over $\mathbb{F}_{25}[a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9]$ in the next step, we adopt the grevlex order with

$$a_8 \prec a_7 \prec a_9 \prec a_3 \prec a_5 \prec a_2 \prec a_4.$$

For $\mathbb{F}_{25}[x, y, z, w]$, we adopt the grevlex order with $w \prec z \prec y \prec x$.

(2) For each $b_1, b_2 \in \{0,1\}$ and $(a_0, a_1, a_6) \in \mathbb{F}_{25}^{\times} \times \mathbb{F}_{25} \times \mathbb{F}_{25}^{\times}$, as in Case of (N1) (i) for $q = 25$, we enumerate $(a_2, a_3, a_4, a_5, a_7, a_8, a_9)$ such that $C = V(Q, P)$ is superspecial.

The outputs of our computation show that the resulting list $\mathcal{P}$ is

$$\mathcal{P} = \{\alpha x^3 + \beta y^3 + \gamma w^3 + \delta zw^2 : \alpha, \beta, \gamma \in \mathbb{F}_{25}^{\times} \text{ and } \delta \in \{0,1\}\}.$$

Thus $V(Q, P)$ is superspecial if and only if $a_0, a_6, a_8 \in \mathbb{F}_{25}^{\times}$, $b_2 \in \{0,1\}$, $a_i = 0$ for $i = 1, \ldots, 5, 7, 9$ and $b_1 = 0$.

We next compute a subset $\mathcal{P}' \subset \mathcal{P}$ such that $V(Q, P_1')$ and $V(Q, P_2')$ are not isomorphic over $\mathbb{F}_{25}$ for all P_1' and P_2' in $\mathcal{P}'$ with $P_1' \neq P_2'$. Using a variant of Isomorphism Testing Algorithm for (N1) in Section 5.3.4 for each pair of cubics in $\mathcal{P}$, we obtain a required subset $\mathcal{P}' \subset \mathcal{P}$. Note that we need not test all pair of elements of $\mathcal{P}$ by pruning.

The outputs of our computation show that the resulting list $\mathcal{P}'$ consists of 21 cubic forms. Hence the number of the $\mathbb{F}_{25}$-isomorphism classes in the set of curves defined by Q and the enumerated P is 21. □

Case of (N1) (i) for $q = 49$

Proposition 5.3.21 *Consider the quadratic form $Q = 2xw + 2yz \in \mathbb{F}_{49}[x, y, z, w]$ and*

$$\begin{aligned} P &= (a_1y + a_2z)x^2 + a_3yzx + y^3 + a_4z^3 + b_1y^2z + a_5yz^2 \\ &\quad +(a_6y^2 + a_7yz + b_2z^2)w + (a_8y + a_9z)w^2 + a_{10}w^3, \end{aligned}$$

where $a_i \in \mathbb{F}_{49}$ with $a_1, a_2 \neq 0$, $b_1 \in \{0, 1, \epsilon\}$ and $b_2 \in \{0, 1\}$, and where ϵ is an element of $\mathbb{F}_{49}^{\times} \smallsetminus (\mathbb{F}_{49}^{\times})^2$. Then there does not exist $(b_1, b_2, a_1, \ldots, a_{10})$ such that $V(Q, P)$ is superspecial.

Proof. For the inputs $K = \mathbb{F}_{49}$ with $p = 7$, $Q = 2xw + 2yz \in \mathbb{F}_{49}[x, y, z, w]$ and

$$\{yx^2, zx^2, yzx, y^3, z^3, y^2z, yz^2, y^2w, yzw, z^2w, yw^2, zw^2, w^3\},$$

we execute First Enumeration Algorithm in Section 5.3.2. For our choice of coefficients to be regarded as indeterminates in solving multivariate systems, we state it below. Specifically we proceed with the following. We set $\mathcal{P} := \emptyset$. Put

$$\begin{aligned} \{p_1, \ldots, p_t\} &= \{yx^2, zx^2, yzx, z^3, yz^2, y^2w, yzw, yw^2, zw^2, w^3\}, \\ \{q_1, \ldots, q_u\} &= \{y^2z, z^2w\}. \end{aligned}$$

with $t = 10$, $u = 2$.

(1) Put $s := 7$, and $(i_1, \ldots, i_7) := (4, 5, 6, 7, 8, 9, 10)$ (we regard the 7 coefficients a_4, a_5, a_6, a_7, a_8, a_9 and a_{10} as indeterminates). For solving systems of multivariate equations over $\mathbb{F}_{49}[a_4, a_5, a_6, a_7, a_8, a_9, a_{10}]$ in the next step, we adopt the grevlex order with

$$a_{10} \prec a_9 \prec a_4 \prec a_8 \prec a_7 \prec a_5 \prec a_6.$$

For $\mathbb{F}_{49}[x, y, z, w]$, we adopt the grevlex order with $w \prec z \prec y \prec x$.

(2) For each $b_1 \in \{0, 1, \epsilon\}$, $b_2 \in \{0, 1\}$ and $(a_1, a_2, a_3) \in \mathbb{F}_{49}^{\times} \times \mathbb{F}_{49}^{\times} \times \mathbb{F}_{49}$, as in Case of (N1) (i) for $q = 25$, we enumerate $(a_4, a_5, a_6, a_7, a_8, a_9, a_{10})$ such that $C = V(Q, P)$ is superspecial.

The outputs of our computation show that the resulting list $\mathcal{P}$ is empty, and hence there does not exist $(b_1, b_2, a_1, \ldots, a_{10})$ such that $V(Q, P)$ is superspecial. □

Case of (N1) (ii) for $q = 49$

Proposition 5.3.22 *Consider the quadratic form $Q = 2xw + 2yz \in \mathbb{F}_{49}[x, y, z, w]$ and*

$$\begin{aligned} P &= (a_1y + a_2z)x^2 + a_3yzx + b_1y^2z + b_2yz^2 \\ &\quad +(a_4y^2 + a_5yz + b_3z^2)w + (a_6y + a_7z)w^2 + a_8w^3, \end{aligned}$$

where $a_i \in \mathbb{F}_{49}$ with $a_1, a_2 \neq 0$, $b_1 \in \{0, 1\}$, $b_2 \in \{0, 1, \epsilon\}$ and $b_3 \in \{0, 1\}$, and where ϵ is an element of $\mathbb{F}_{49}^{\times} \smallsetminus (\mathbb{F}_{49}^{\times})^2$. Then there does not exist $(b_1, b_2, b_3, a_1, \ldots, a_8)$ such that $V(Q, P)$ is superspecial.

Proof. For the inputs $K = \mathbb{F}_{49}$ with $p = 7$, $Q = 2xw + 2yz \in \mathbb{F}_{49}[x, y, z, w]$ and

$$\{yx^2, zx^2, yzx, y^2z, yz^2, y^2w, yzw, z^2w, yw^2, zw^2, w^3\},$$

we execute First Enumeration Algorithm in Section 5.3.2. For our choice of coefficients to be regarded as indeterminates in solving multivariate systems, we state it below. Specifically we proceed with the following. We set $\mathcal{P} := \emptyset$. Put

$$\begin{aligned} \{p_1, \ldots, p_t\} &= \{yx^2, zx^2, yzx, y^2w, yzw, yw^2, zw^2, w^3\}, \\ \{q_1, \ldots, q_u\} &= \{y^2z, yz^2, z^2w\}. \end{aligned}$$

with $t = 8$, $u = 3$.

(1) Put $s := 6$, and $(i_1, \ldots, i_6) := (3, 4, 5, 6, 7, 8)$ (we regard the 6 coefficients a_3, a_4, a_5, a_6, a_7 and a_8 as indeterminates). For solving systems of multivariate equations over $\mathbb{F}_{49}[a_3, a_4, a_5, a_6, a_7, a_8]$ in the next step, we adopt the grevlex order with

$$a_8 \prec a_7 \prec a_6 \prec a_5 \prec a_4 \prec a_3.$$

For $\mathbb{F}_{49}[x, y, z, w]$, we adopt the grevlex order with $w \prec z \prec y \prec x$.

(2) For each $b_1 \in \{0, 1\}$, $b_2 \in \{0, 1, -\epsilon\}$, $b_3 \in \{0, 1\}$ and $(a_1, a_2) \in \mathbb{F}_{49}^{\times} \times \mathbb{F}_{49}^{\times}$, as in Case of (N1) (i) for $q = 25$, we enumerate $(a_3, a_4, a_5, a_6, a_7, a_8)$ such that $C = V(Q, P)$ is superspecial.

The outputs of our computation show that the resulting list $\mathcal{P}$ is empty, and hence there does not exist $(b_1, b_2, b_3, a_1, \ldots, a_8)$ such that $V(Q, P)$ is superspecial. □

Case of (N2) for $q = 49$

Proposition 5.3.23 *Consider the quadratic form $Q = 2xw + y^2 - \epsilon z^2 \in \mathbb{F}_{49}[x, y, z, w]$ and*

$$\begin{aligned} P &= (a_1y + a_2z)x^2 + a_3(y^2 - \epsilon z^2)x + b_1y(y^2 - \epsilon z^2) + a_4y(y^2 + 3\epsilon z^2) + a_5z(3y^2 + \epsilon z^2) \\ &\quad + (a_6y^2 + a_7yz + b_2z^2)w + (a_8y + a_9z)w^2 + a_{10}w^3, \end{aligned}$$

where ϵ is an element of $\mathbb{F}_{49}^{\times} \setminus (\mathbb{F}_{49}^{\times})^2$, and where $a_i \in \mathbb{F}_{49}$ with $(a_1, a_2) \neq (0, 0)$ and $b_1, b_2 \in \{0, 1\}$. Then there does not exist $(b_1, b_2, a_1, \ldots, a_{10})$ such that $V(Q, P)$ is superspecial.

Proof. For the inputs $K = \mathbb{F}_{49}$ with $p = 7$, $Q = 2xw + y^2 - \epsilon z^2 \in \mathbb{F}_{49}[x, y, z, w]$ and

$$\{yx^2, zx^2, (y^2 - \epsilon z^2)x, y(y^2 - \epsilon z^2), y(y^2 + 3\epsilon z^2), z(3y^2 + \epsilon z^2), y^2w, yzw, z^2w, yw^2, zw^2, w^3\},$$

we execute First Enumeration Algorithm in Section 5.3.2. For our choice of coefficients to be regarded as indeterminates in solving multivariate systems, we state it below. Specifically we proceed with the following. We set $\mathcal{P} := \emptyset$. Put

$$\begin{aligned} \{p_1, \ldots, p_t\} &= \{yx^2, zx^2, (y^2 - \epsilon z^2)x, y(y^2 + 3\epsilon z^2), z(3y^2 + \epsilon z^2), y^2w, yzw, yw^2, zw^2, w^3\}, \\ \{q_1, \ldots, q_u\} &= \{y(y^2 - \epsilon z^2), z^2w\}. \end{aligned}$$

with $t = 10$, $u = 2$.

(1) Put $s := 7$, and $(i_1, \ldots, i_7) := (4, 5, 6, 7, 8, 9, 10)$ (we regard the 7 coefficients a_4, a_5, a_6, a_7, a_8, a_9 and a_{10} as indeterminates). For solving systems of multivariate equations over $\mathbb{F}_{49}[a_4, a_5, a_6, a_7, a_8, a_9, a_{10}]$ in the next step, we adopt the grevlex order with

$$a_{10} \prec a_9 \prec a_8 \prec a_7 \prec a_6 \prec a_5 \prec a_4.$$

For $\mathbb{F}_{49}[x, y, z, w]$, we adopt the grevlex order with $w \prec z \prec y \prec x$.

(2) For each $b_1, b_2 \in \{0, 1\}$ and $(a_1, a_2) \in \{(c_1, c_2, c_3) \in \mathbb{F}_{49} \times \mathbb{F}_{49} \times \mathbb{F}_{49} : (c_1, c_2) \neq (0, 0)\}$, as in Case of (N1) (i) for $q = 25$, we enumerate $(a_4, a_5, a_6, a_7, a_8, a_9, a_{10})$ such that $C = V(Q, P)$ is superspecial.

The outputs of our computation show that the resulting list $\mathcal{P}$ is empty, and hence there does not exist $(b_1, b_2, b_3, a_1, \ldots, a_{10})$ such that $V(Q, P)$ is superspecial. □

Case of (Dege) for $q = 49$

Proposition 5.3.24 *Consider the degenerate quadratic form $Q = 2yw + z^2 \in \mathbb{F}_{49}[x, y, z, w]$ and*

$$\begin{aligned} P &= a_0x^3 + a_1xy^2 + a_2xz^2 + a_3xw^2 + a_4xyz + a_5xzw \\ &\quad + a_6y^3 + a_7z^3 + a_8w^3 + a_9yz^2 + b_1z^2w + b_2zw^2, \end{aligned}$$

where $a_i \in \mathbb{F}_{49}$ with $a_0, a_6 \neq 0$ and $b_1, b_2 \in \{0, 1\}$. Then there does not exist $(b_1, b_2, a_0, \ldots, a_9)$ such that $V(Q, P)$ is superspecial.

Proof. For the inputs $K = \mathbb{F}_{49}$ with $p = 7$, $Q = 2yw + z^2 \in \mathbb{F}_{49}[x, y, z, w]$ and

$$\{x^3, y^2x, z^2x, w^2x, yzx, zwx, y^3, z^3, w^3, yz^2, z^2w, zw^2\},$$

we execute First Enumeration Algorithm in Section 5.3.2. For our choice of coefficients to be regarded as indeterminates in solving multivariate systems, we state it below. Specifically we proceed with the following. We set $\mathcal{P} := \emptyset$. Put

$$\begin{aligned} \{p_1, \ldots, p_t\} &= \{x^3, xy^2, xz^2, xw^2, xyz, xzw, y^3, z^3, w^3, yz^2\}, \\ \{q_1, \ldots, q_u\} &= \{z^2w, zw^2\}. \end{aligned}$$

with $t = 10$, $u = 2$.

(1) Put $s := 7$, and $(i_1, \ldots, i_7) := (2, 3, 4, 5, 7, 8, 9)$ (we regard the 7 coefficients a_2, a_3, a_4, a_5, a_7, a_8 and a_9 as indeterminates). For solving systems of multivariate equations over $\mathbb{F}_{49}[a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9]$ in the next step, we adopt the grevlex order with

$$a_8 \prec a_7 \prec a_9 \prec a_3 \prec a_5 \prec a_2 \prec a_4.$$

For $\mathbb{F}_{49}[x, y, z, w]$, we adopt the grevlex order with $w \prec z \prec y \prec x$.

(2) For each $b_1, b_2 \in \{0, 1\}$ and $(a_0, a_1, a_6) \in \mathbb{F}_{49}^{\times} \times \mathbb{F}_{49} \times \mathbb{F}_{49}^{\times}$, as in Case of (N1) (i) for $q = 25$, we enumerate $(a_2, a_3, a_4, a_5, a_7, a_8, a_9)$ such that $C = V(Q, P)$ is superspecial.

The outputs of our computation show that the resulting list $\mathcal{P}$ is empty, and hence there does not exist $(b_1, b_2, a_0, \ldots, a_{10})$ such that $V(Q, P)$ is superspecial. □

Case of (Dege) for $q = 5$

Proposition 5.3.25 *Consider the quadratic form $Q = 2yw + z^2 \in \mathbb{F}_5[x, y, z, w]$ and cubic forms $P \in \mathbb{F}_5[x, y, z, w]$ of the form*

(i)

$$\begin{aligned} P =& a_0x^3 + (a_1y^2 + a_2z^2 + a_3w^2 + a_4yz + a_5zw)x \\ &+ a_6y^3 + a_7z^3 + a_8w^3 + a_9yz^2 + b_1z^2w + b_2zw^2, \end{aligned} \tag{5.3.4}$$

for $a_0, a_6 \in \mathbb{F}_5^\times$ and $b_1, b_2 \in \{0, 1\}$, or

(ii)

$$P = x^3 + (a_1y^2 + a_2z^2 + a_3w^2 + a_4yz + b_1zw)x + y^2z + zw^2 \tag{5.3.5}$$

for $a_i \in K = \mathbb{F}_5$ and $b_1 \in \{0, 1\}$.

Then a cubic form P of the form (5.3.4) *or* (5.3.5) *such that $V(Q, P)$ is superspecial is one of*

$$\begin{aligned} P_1 &= x^3 + y^3 + w^3, \\ P_2 &= x^3 + y^3 + 2w^3, \\ P_3 &= x^3 + y^3 + w^3 + zw^2, \\ P_4 &= x^3 + y^3 + 2w^3 + zw^2, \\ P_5 &= x^3 + y^3 + 3w^3 + zw^2, \\ P_6 &= x^3 + y^3 + 4w^3 + zw^2, \\ P_7 &= x^3 + y^2z + zw^2 \end{aligned}$$

up to isomorphism over $\mathbb{F}_5$.

Proof. (i) For the inputs $K = \mathbb{F}_5$ with $p = 5$, $Q = 2yw + z^2 \in \mathbb{F}_5[x, y, z, w]$ and

$$\{x^3, y^2x, z^2x, w^2x, yzx, zwx, y^3, z^3, w^3, yz^2, z^2w, zw^2\},$$

we execute First Enumeration Algorithm in Section 5.3.2. For our choice of coefficients to be regarded as indeterminates in solving multivariate systems, we state it below. Specifically we proceed with the following. Put $t = 10$, $u = 2$ and

$$\begin{aligned} \{p_1, \ldots, p_t\} &= \{x^3, xy^2, xz^2, xw^2, xyz, xzw, y^3, z^3, w^3, yz^2\}, \\ \{q_1, \ldots, q_u\} &= \{z^2w, zw^2\}. \end{aligned}$$

(1) Put $s := 8$ and $(i_1, \ldots, i_8) := (1, 2, 3, 4, 5, 7, 8, 9)$ (we regard the 8 coefficients a_1, a_2, a_3, a_4, a_5, a_7, a_8 and a_9 as indeterminates). For solving systems of multivariate equations over $\mathbb{F}_5[a_1, a_2, a_3, a_4, a_5, a_7, a_8, a_9]$ in the next step, we adopt the grevlex order with

$$a_8 \prec a_7 \prec a_9 \prec a_3 \prec a_5 \prec a_2 \prec a_4 \prec a_1.$$

For $\mathbb{F}_5[x, y, z, w]$, we adopt the grevlex order with $w \prec z \prec y \prec x$.

(2) For each $(b_1, b_2) \in \{0, 1\}^{\oplus 2}$ and $a_0, a_6 \in \mathbb{F}_5^\times$, as in Case of (N1) (i) for $q = 25$, we enumerate $(a_1, a_2, a_3, a_4, a_5, a_7, a_8, a_9)$ such that $V(Q, P)$ is superspecial.

(ii) For the inputs $K = \mathbb{F}_5$ with $p = 5$, $Q = 2yw + z^2 \in \mathbb{F}_5[x, y, z, w]$ and

$$\{x^3, y^2x, z^2x, w^2x, yzx, zwx, y^2z, zw^2\},$$

we execute First Enumeration Algorithm in Section 5.3.2. For our choice of coefficients to be regarded as indeterminates in solving multivariate systems, we state it below. Specifically we proceed with the following. Put $t = 4$, $u = 1$ and

$$\begin{aligned}\{p_1, \ldots, p_t\} &= \{y^2x, z^2x, w^2x, yzx\},\\ \{q_1, \ldots, q_u\} &= \{zwx\}.\end{aligned}$$

(1) Put $s := 4$ and $(i_1, \ldots, i_4) := (1, 2, 3, 4)$ (we regard the 4 coefficients a_1, a_2, a_3 and a_4 as indeterminates). For solving systems of multivariate equations over $\mathbb{F}_5[a_1, a_2, a_3, a_4]$ in the next step, we adopt the grevlex order with $a_3 \prec a_2 \prec a_4 \prec a_1$. For $\mathbb{F}_5[x, y, z, w]$, we adopt the grevlex order with $w \prec z \prec y \prec x$.

(2) For each $b_1 \in \{0, 1\}$, as in Case of (N1) (i) for $q = 25$, we enumerate (a_1, a_2, a_3, a_4) such that $V(Q, P)$ is superspecial.

Let $\mathcal{P}$ denote the list of cubics P such that $V(Q, P)$ was determined to be superspecial in the above procedures (i) and (ii). We next compute a subset $\mathcal{P}' \subset \mathcal{P}$ such that $V(Q, P_1')$ and $V(Q, P_2')$ are not isomorphic over $\mathbb{F}_5$ for all P_1' and P_2' in $\mathcal{P}'$ with $P_1' \neq P_2'$. Using a variant of Isomorphism Testing Algorithm for (N1) in Section 5.3.4 for each pair of cubics in $\mathcal{P}$, we obtain a required subset $\mathcal{P}' \subset \mathcal{P}$. Note that we need not test all pair of elements of $\mathcal{P}$ by pruning.

The outputs of our computation show that the resulting list $\mathcal{P}'$ consists of cubic forms P_i for $1 \leq i \leq 7$. Hence a cubic form P of the form (5.3.4) or (5.3.5) such that $V(Q, P)$ is superspecial is one of P_i for $1 \leq i \leq 7$, up to isomorphism over $\mathbb{F}_5$. □

Remark 5.3.26 The efficiency of First Enumeration Algorithm in Section 5.3.2 deeply depends on the choice of s, coefficients to be regarded as indeterminates, and the term order. We experimentally estimated optimal ones for each case to compute.

Case of (N1) for $q = 11$

Proposition 5.3.27 *Consider the quadratic form $Q = 2xw + 2yz \in \mathbb{F}_{11}[x, y, z, w]$ and cubic forms $P \in \mathbb{F}_{11}[x, y, z, w]$ of the form*

$$\begin{aligned}P =&(y + b_1z)x^2 + b_2xz^2\\ &+ a_1y^3 + a_2y^2z + a_3yz^2 + a_4z^3\\ &+ (a_5y^2 + a_6yz + a_7z^2)w + (a_8y + a_9z)w^2 + a_{10}w^3,\end{aligned} \tag{5.3.6}$$

where $a_1, \ldots, a_{10} \in \mathbb{F}_{11}$, $b_1 \in \{0, 1, \zeta^{(11)}\}$ *and* $b_2 \in \{0, 1\}$. *Here* $\zeta^{(11)}$ *is a primitive element of* $\mathbb{F}_{11}$. *Then a cubic form* P *of the form* (5.3.6) *such that* $V(Q, P)$ *is superspecial is one of*

$$\begin{aligned}
P_1^{(\mathrm{N1})} &= x^2y + x^2z + 2y^2z + 5y^2w + 9yz^2 + yzw + 4z^3 + 3z^2w + 10zw^2 + w^3,\\
P_2^{(\mathrm{N1})} &= x^2y + x^2z + y^3 + y^2z + 7yz^2 + 4yw^2 + 2z^3 + 9zw^2,\\
P_3^{(\mathrm{N1})} &= x^2y + x^2z + y^3 + 8y^2z + 3yz^2 + 10yw^2 + 10z^3 + 10zw^2,\\
P_4^{(\mathrm{N1})} &= x^2y + x^2z + y^3 + 9y^2z + 2y^2w + 3yz^2 + 3yzw + 4yw^2 + 10z^3 + 2z^2w + 6zw^2,\\
P_5^{(\mathrm{N1})} &= x^2y + x^2z + xz^2 + 10y^2w + 9yz^2 + 9yw^2 + 8z^3 + 8z^2w + 8zw^2 + 3w^3,\\
P_6^{(\mathrm{N1})} &= x^2y + x^2z + xz^2 + 9y^2z + 5y^2w + yzw + 8yw^2 + 3z^3 + 9z^2w + 2zw^2 + 5w^3,\\
P_7^{(\mathrm{N1})} &= x^2y + x^2z + xz^2 + 4y^3 + 2y^2z + 10y^2w + 3yz^2 + 8yzw + 8yw^2 + 8z^3 + 7z^2w + 7zw^2 + 4w^3,\\
P_8^{(\mathrm{N1})} &= x^2y + x^2z + xz^2 + 9y^3 + 6y^2z + 5y^2w + 8yz^2 + 5yzw + 2yw^2 + z^3 + 2z^2w + 7zw^2 + w^3
\end{aligned}$$

up to isomorphism over $\mathbb{F}_{11}$.

Proof. For the inputs $K = \mathbb{F}_{11}$ with $p = 11$, $2xw + 2yz \in \mathbb{F}_{11}[x, y, z, w]$ and

$$\{yx^2, zx^2, xz^2, y^3, y^2z, yz^2, z^3, y^2w, yzw, z^2w, yw^2, zw^2, w^3\},$$

we execute Second Enumeration Algorithm in Section 5.3.2. For our choice of coefficients to be regarded as indeterminates in solving multivariate systems, we state it below. Specifically we proceed with the following. Put $t = 10$, $u = 2$ and

$$\begin{aligned}
\{p_1, \ldots, p_t\} &= \{y^3, y^2z, yz^2, z^3, y^2w, yzw, z^2w, yw^2, zw^2, w^3\},\\
\{q_1, \ldots, q_u\} &= \{x^2z, xz^2\}.
\end{aligned}$$

We divide our computation into the following three cases (this is our technical strategy to avoid the out of memory errors).

(i) Case of $b_1 \neq 0$**.** (0) Put $s_1 := 8$, and $(k_1, \ldots, k_{s_1}) := (3, \ldots, 10)$ (we regard the 8 coefficients a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10} as indeterminates).

For each $b_1 \in \{1, \zeta^{(11)}\}$, $b_2 \in \{0, 1\}$, and $(a_1, a_2) \in \mathbb{F}_{11} \times \mathbb{F}_{11}$, we conduct the following three steps:

(1) Compute $h := (PQ)^{p-1}$ over $\mathbb{F}_{11}[a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}][x, y, z, w]$, where a_4, a_5, a_6, a_8, a_9 and a_{10} are indeterminates.

(2) Put $s_2 := 6$, and $(i_1, \ldots, i_{s_2}) := (4, 5, 6, 8, 9, 10)$ (regard the 6 coefficients a_4, a_5, a_6, a_8, a_9 and a_{10} as indeterminates). For solving multivariate systems over $\mathbb{F}_{11}[a_4, a_5, a_6, a_8, a_9, a_{10}]$ in the next step, we adopt the grevlex order with $a_{10} \prec a_9 \prec a_4 \prec a_8 \prec a_6 \prec a_5$. For $\mathbb{F}_{11}[x, y, z, w]$, we adopt the grevlex order with $w \prec z \prec y \prec x$.

(3) For each $(a_3, a_7) \in \mathbb{F}_{11} \times \mathbb{F}_{11}$, we proceed the following three steps:

(a) Let $\mathcal{S}$ denote the set of the coefficients of certain 16 monomials in $h = (PQ)^p$, where the 16 monomials are given in Corollary 5.3.6 and where $\mathcal{S} \subset \mathbb{F}_{11}[a_4, a_5, a_6, a_8, a_9, a_{10}]$.

(b) Using Gröbner basis algorithms, solve the system of multivariate polynomial equations $f(a_4, a_5, a_6, a_8, a_9, a_{10}) = 0$ for all $f \in \mathcal{S}$ over $\mathbb{F}_{11}$.

(c) For each root $(a_4, a_5, a_6, a_8, a_9, a_{10})$ of the system, substitute it into unknown coefficients in P, and decide whether $C = V(Q, P)$ is non-singular or not.

(ii) Case of $b_1 = 0$ and $a_4 \neq 0$. (0) Put $s_1 := 9$, and $(k_1, \ldots, k_{s_1}) := (2, \ldots, 10)$ (we regard the 9 coefficients a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9 and a_{10} as indeterminates).

For each $b_2 \in \{0, 1\}$ and $a_1 \in \mathbb{F}_{11}$, we conduct the following three steps:

(1) Compute $h := (PQ)^{p-1}$ over $\mathbb{F}_{11}[a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}]$, where a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9 and a_{10} are indeterminates.

(2) Put $s_2 := 5$, and $(i_1, \ldots, i_{s_2}) := (5, 6, 8, 9, 10)$ (we regard the 5 coefficients a_5, a_6, a_8, a_9 and a_{10} as indeterminates). For solving multivariate systems over $\mathbb{F}_{11}[a_5, a_6, a_8, a_9, a_{10}]$ in the next step, we adopt the grevlex order with $a_{10} \prec a_9 \prec a_8 \prec a_6 \prec a_5$. For $\mathbb{F}_{11}[x, y, z, w]$, we adopt the grevlex order with $w \prec z \prec y \prec x$.

(3) We conduct a procedure similar to Step 3 in Case of $b_1 \neq 0$. Specifically for each $(a_2, a_3, a_4, a_7) \in \mathbb{F}_{11} \times \mathbb{F}_{11} \times \mathbb{F}_{11}^{\times} \times \mathbb{F}_{11}$, enumerate $(a_5, a_6, a_8, a_9, a_{10})$ such that $C = V(Q, P)$ is superspecial.

(iii) Case of $b_1 = 0$ and $a_4 = 0$. (0) Put $s_1 := 8$, and $(k_1, \ldots, k_{s_1}) := (2, 3, 5, 6, \ldots, 10)$ (we regard the 8 coefficients a_2, a_3, a_5, a_6, a_7, a_8, a_9 and a_{10} as indeterminates).

For each $b_2 \in \{0, 1\}$ and $a_1 \in \mathbb{F}_{11}$, we conduct the following three steps:

(1) Compute $h := (PQ)^{p-1}$ over $\mathbb{F}_{11}[a_2, a_3, a_5, a_6, \ldots, a_{10}][x, y, z, w]$, where a_2, a_3, a_5, a_6, a_7, a_8, a_9 and a_{10} are indeterminates.

(2) Put $s_2 := 4$, and $(i_1, \ldots, i_{s_2}) := (6, 8, 9, 10)$ (we regard the 4 coefficients a_6, a_8, a_9 and a_{10} as indeterminates). For solving multivariate systems over $\mathbb{F}_{11}[a_6, a_8, a_9, a_{10}]$ in the next step, we adopt the grevlex order with $a_{10} \prec a_9 \prec a_8 \prec a_6$. For $\mathbb{F}_{11}[x, y, z, w]$, we adopt the grevlex order with $w \prec z \prec y \prec x$.

(3) We conduct a procedure similar to Step 3 in Case of $b_1 \neq 0$. Specifically for each $(a_2, a_3, a_5, a_7) \in \mathbb{F}_{11} \times \mathbb{F}_{11} \times \mathbb{F}_{11} \times \mathbb{F}_{11}$, enumerate (a_6, a_8, a_9, a_{10}) such that $C = V(Q, P)$ is superspecial.

Let $\mathcal{P}$ be the list of cubics P such that $V(Q, P)$ was determined to be superspecial in the above procedures (i), (ii) and (iii). We next compute a subset $\mathcal{P}' \subset \mathcal{P}$ such that $V(Q, P_1)$ and $V(Q, P_2)$ are not isomorphic over $\mathbb{F}_{11}$ for all P_1 and P_2 in $\mathcal{P}'$ with $P_1 \neq P_2$. Using Isomorphism Testing Algorithm for (N1) in Section 5.3.4 for each pair of cubics in $\mathcal{P}$, we obtain a required subset $\mathcal{P}' \subset \mathcal{P}$. Note that we need not test all pair of elements of $\mathcal{P}$ by pruning.

The outputs of our computation show that the resulting list $\mathcal{P}'$ consists of cubic forms $P_i^{(\mathrm{N1})}$ for $1 \leq i \leq 8$. Hence a cubic form P of the form (5.3.6) such that $V(Q, P)$ is superspecial is one of $P_i^{(\mathrm{N1})}$ for $1 \leq i \leq 8$, up to isomorphism over $\mathbb{F}_{11}$. □

Case of (N2) for $q = 11$

Proposition 5.3.28 *Consider the quadratic form $Q = 2xw + y^2 - \epsilon z^2 \in \mathbb{F}_{11}[x, y, z, w]$ with $\epsilon \in \mathbb{F}_{11}^{\times} \setminus (\mathbb{F}_{11}^{\times})^2$ and cubic forms of the form*

$$\begin{aligned} P =& (a_1 y + a_2 z)x^2 + a_3(y^2 - \epsilon z^2)x + b_1 y(y^2 - \epsilon z^2) + a_4 y(y^2 + 3\epsilon z^2) + a_5 z(3y^2 + \epsilon z^2) \\ &+ (a_6 y^2 + a_7 yz + b_2 z^2)w + (a_8 y + a_9 z)w^2 + a_{10} w^3, \end{aligned} \tag{5.3.7}$$

where $a_i \in \mathbb{F}_{11}$ *with* $(a_1, a_2) \in (\mathbb{F}_{11} \times \mathbb{F}_{11}) \setminus \{(0,0)\}$ *and* $(b_1, b_2) \in \{0,1\}^{\oplus 2}$. *Then a cubic form* P *of the form* (5.3.7) *such that* $V(Q,P)$ *is superspecial is one of*

$$\begin{aligned}
P_1^{(\mathrm{N2})} &= x^2y + x^2z + xy^2 + 9xz^2 + 6y^3 + y^2z + 5y^2w + 3yz^2 + 9yw^2 + 8z^3 + z^2w + 9zw^2 + 6w^3,\\
P_2^{(\mathrm{N2})} &= x^2z + 5y^3 + 4zw^2,\\
P_3^{(\mathrm{N2})} &= x^2y + x^2z + 9y^3 + 8y^2z + 2yz^2 + 4yw^2 + 9z^3 + 4zw^2,\\
P_4^{(\mathrm{N2})} &= 8x^2y + 2x^2z + y^3 + 8y^2z + 6y^2w + 9yz^2 + 2yzw + 5yw^2 + 9z^3 + z^2w + 4zw^2 + w^3,\\
P_5^{(\mathrm{N2})} &= 6x^2y + 4x^2z + 6xy^2 + 10xz^2 + 10y^3 + 4y^2z + 3y^2w + 8yz^2 + 6yzw + 9yw^2 + 10z^3\\
&\quad + z^2w + zw^2 + 9w^3,
\end{aligned}$$

up to isomorphism over $\mathbb{F}_{11}$.

Proof. For the inputs $K = \mathbb{F}_{11}$ with $p = 11$, $2xw + y^2 - \epsilon z^2 \in \mathbb{F}_{11}[x,y,z,w]$ and

$$\{yx^2, zx^2, (y^2 - \epsilon z^2)x, y(y^2 - \epsilon z^2), y(y^2 + 3\epsilon z^2), z(3y^2 + \epsilon z^2), y^2w, yzw, z^2w, yw^2, zw^2, w^3\}$$

we execute Second Enumeration Algorithm in Section 5.3.2. For our choice of coefficients to be regarded as indeterminates in solving multivariate systems, we state it below. Specifically we proceed with the following. Put $t = 10$, $u = 2$ and

$$\begin{aligned}
\{p_1, \ldots, p_t\} &= \{yx^2, zx^2, (y^2 - \epsilon z^2)x, y(y^2 + 3\epsilon z^2), z(3y^2 + \epsilon z^2), y^2w, yzw, yw^2, zw^2, w^3\},\\
\{q_1, \ldots, q_u\} &= \{y(y^2 - \epsilon z^2), z^2w\}.
\end{aligned}$$

(0) We set $s_1 := 9$, and $(k_1, \ldots, k_{s_1}) := (1, 2, 4, \ldots, 10)$ (we regard the 9 coefficients a_1, a_2, a_4, a_5, a_6, a_7, a_8, a_9 and a_{10} as indeterminates).

For each $(b_1, b_2) \in \{0,1\}^{\oplus 2}$ and $a_3 \in \mathbb{F}_{11}$, we conduct the following three steps:

(1) Compute $h := (PQ)^{p-1}$ over $\mathbb{F}_{11}[a_1, a_2, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}]$, where a_1, a_2, a_4, a_5, a_6, a_7, a_8, a_9 and a_{10} are indeterminates.

(2) Put $s_2 := 5$, and $(i_1, \ldots, i_{s_2}) := (6, 7, 8, 9, 10)$ (we regard the 5 coefficients a_6, a_7, a_8, a_9 and a_{10} as indeterminates). For solving multivariate systems over $\mathbb{F}_{11}[a_6, a_7, a_8, a_9, a_{10}]$ in the next step, we adopt the grevlex order with $a_{10} \prec a_9 \prec a_8 \prec a_7 \prec a_6$. For $\mathbb{F}_{11}[x,y,z,w]$, we adopt the grevlex order with $w \prec z \prec y \prec x$.

(3) We conduct a procedure similar to Case of $b_1 \neq 0$ in the proof of Proposition 5.3.27. Specifically for each $(a_1, a_2, a_4, a_5) \in (\mathbb{F}_{11} \times \mathbb{F}_{11} \setminus \{(0,0)\}) \times \mathbb{F}_{11} \times \mathbb{F}_{11}$, enumerate $(a_6, a_7, a_8, a_9, a_{10})$ such that $C = V(Q,P)$ is superspecial.

Let $\mathcal{P}$ be the list of cubics P such that $V(Q,P)$ was determined to be superspecial in the above procedures. We next compute a subset $\mathcal{P}' \subset \mathcal{P}$ such that $V(Q,P_1)$ and $V(Q,P_2)$ are not isomorphic over $\mathbb{F}_{11}$ for all P_1 and P_2 in $\mathcal{P}'$ with $P_1 \neq P_2$. Using a variant of Isomorphism Testing Algorithm for (N1) in Section 5.3.4 for each pair of cubics in $\mathcal{P}$, we obtain a required subset $\mathcal{P}' \subset \mathcal{P}$. Note that we need not test all pair of elements of $\mathcal{P}$ by pruning.

The outputs of our computation show that the resulting $\mathcal{P}'$ consists of cubic forms $P_i^{(\mathrm{N2})}$ for $1 \leq i \leq 5$. Hence a cubic form P of the form (5.3.7) such that $V(Q,P)$ is superspecial is one of $P_i^{(\mathrm{N2})}$ for $1 \leq i \leq 5$, up to isomorphism over $\mathbb{F}_{11}$. □

Case of (Dege) for $q = 11$

Proposition 5.3.29 *Consider the quadratic form $Q = 2yw + z^2 \in \mathbb{F}_{11}[x, y, z, w]$ and cubic forms $P \in \mathbb{F}_{11}[x, y, z, w]$ of the form*

$$\begin{aligned} P =& a_0x^3 + (a_1y^2 + a_2z^2 + a_3w^2 + a_4yz + a_5zw)x \\ &+ a_6y^3 + a_7z^3 + a_8w^3 + a_9yz^2 + b_1z^2w + b_2zw^2, \end{aligned} \tag{5.3.8}$$

where $a_i \in \mathbb{F}_{11}$ with $a_0, a_6 \in \mathbb{F}_{11}^{\times}$ and $(b_1, b_2) \in \{0, 1\}^{\oplus 2}$. Then a cubic form P of the form (5.3.8) *such that $V(Q, P)$ is superspecial is one of*

$$\begin{aligned}
P_1^{(\mathrm{Dege})} &= w^3 + x^3 + y^3, \\
P_2^{(\mathrm{Dege})} &= 2w^3 + x^3 + y^3, \\
P_3^{(\mathrm{Dege})} &= 5w^3 + x^3 + y^3 + z^3, \\
P_4^{(\mathrm{Dege})} &= w^2x + x^3 + y^3, \\
P_5^{(\mathrm{Dege})} &= 2w^2x + x^3 + y^3, \\
P_6^{(\mathrm{Dege})} &= w^3 + wxz + x^3 + y^3 + 7z^3, \\
P_7^{(\mathrm{Dege})} &= 4w^3 + w^2x + x^3 + xyz + y^3 + 5z^3, \\
P_8^{(\mathrm{Dege})} &= 8w^3 + 6w^2x + x^3 + xyz + y^3 + 8z^3, \\
P_9^{(\mathrm{Dege})} &= 4w^3 + w^2z + x^3 + 5y^3 + 2yz^2 + z^3, \\
P_{10}^{(\mathrm{Dege})} &= 2w^3 + wz^2 + x^3 + y^3 + 8yz^2, \\
P_{11}^{(\mathrm{Dege})} &= 3w^3 + wz^2 + x^3 + 2y^3 + 2yz^2 + 4z^3, \\
P_{12}^{(\mathrm{Dege})} &= 10w^3 + wz^2 + x^3 + 2y^3 + 4yz^2, \\
P_{13}^{(\mathrm{Dege})} &= 7w^3 + w^2z + wz^2 + x^3 + 2y^3 + 4yz^2 + z^3, \\
P_{14}^{(\mathrm{Dege})} &= 7w^3 + 2w^2x + w^2z + 8wxz + wz^2 + x^3 + xy^2 + 7xyz + 8xz^2 + 2y^3 + 4yz^2 + z^3, \\
P_{15}^{(\mathrm{Dege})} &= 10w^3 + w^2z + wz^2 + x^3 + 5y^3 + 3yz^2 + 5z^3, \\
P_{16}^{(\mathrm{Dege})} &= 6w^3 + w^2z + wz^2 + x^3 + 6y^3 + 2yz^2 + 6z^3, \\
P_{17}^{(\mathrm{Dege})} &= w^2z + wz^2 + x^3 + 10y^3 + 6yz^2 + 7z^3,
\end{aligned}$$

up to isomorphism over $\mathbb{F}_{11}$.

Proof. For the inputs $K = \mathbb{F}_{11}$ with $p = 11$, $2yw + z^2 \in \mathbb{F}_{11}[x, y, z, w]$ and

$$\{x^3, y^2x, z^2x, w^2x, yzx, zwx, y^3, z^3, w^3, yz^2, z^2w, zw^2\},$$

we execute Second Enumeration Algorithm in Section 5.3.2. For our choice of coefficients to be regarded as indeterminates in solving multivariate systems, we state it below. Specifically we proceed with the following. Put $t = 10$, $u = 2$ and

$$\begin{aligned}
\{p_1, \ldots, p_t\} &= \{x^3, xy^2, xz^2, xw^2, xyz, xzw, y^3, z^3, w^3, yz^2\}, \\
\{q_1, \ldots, q_u\} &= \{z^2w, zw^2\}.
\end{aligned}$$

(0) We set $s_1 := 9$, and $(k_1, \ldots, k_{s_1}) := (1, \ldots, 9)$ (we regard the 9 coefficients a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8 and a_9 as indeterminates).

For each $(b_1, b_2) \in \{0,1\}^{\oplus 2}$ and $a_0 \in \mathbb{F}_{11}^{\times}$, we proceed with the following three steps:

(1) Compute $h := (PQ)^{p-1}$ over $\mathbb{F}_{11}[a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9]$, where a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8 and a_9 are indeterminates.

(2) Put $s_2 := 6$, and $(i_1, \ldots, i_{s_2}) := (2, 3, 5, 7, 8, 9)$ (we regard the 6 coefficients a_2, a_3, a_5, a_7, a_8 and a_9 as indeterminates). For solving multivariate systems over $\mathbb{F}_{11}[a_2, a_3, a_5, a_7, a_8, a_9]$, we adopt the grevlex order with $a_8 \prec a_7 \prec a_9 \prec a_3 \prec a_5 \prec a_2$. For $\mathbb{F}_{11}[x, y, z, w]$, we adopt the grevlex order with $w \prec z \prec y \prec x$.

(3) We conduct a procedure similar to Case of $b_1 \neq 0$ in the proof of Proposition 5.3.27. Specifically for each $(a_1, a_4, a_6) \in \mathbb{F}_{11} \times \mathbb{F}_{11} \times \mathbb{F}_{11}^{\times}$, enumerate $(a_2, a_3, a_5, a_7, a_8, a_9)$ such that $C = V(Q, P)$ is superspecial.

Let $\mathcal{P}$ be the list of cubics P such that $V(Q, P)$ was determined to be superspecial in the above procedures. We next compute a subset $\mathcal{P}' \subset \mathcal{P}$ such that $V(Q, P_1)$ and $V(Q, P_2)$ are not isomorphic over $\mathbb{F}_{11}$ for all P_1 and P_2 in $\mathcal{P}'$ with $P_1 \neq P_2$. Using a variant of Isomorphism Testing Algorithm for (N1) in Section 5.3.4 for each pair of cubics in $\mathcal{P}$, we obtain a required subset $\mathcal{P}' \subset \mathcal{P}$. Note that we need not test all pair of elements of $\mathcal{P}$ by pruning.

The outputs of our computation show that the resulting $\mathcal{P}'$ consists of cubic forms $P_i^{(\mathrm{Dege})}$ for $1 \leq i \leq 17$. Hence a cubic form P of the form (5.3.8) such that $V(Q, P)$ is superspecial is one of $P_i^{(\mathrm{Dege})}$ for $1 \leq i \leq 17$, up to isomorphism over $\mathbb{F}_{11}$. □

Remark 5.3.30 The efficiency of Second Enumeration Algorithm in Section 5.3.2 deeply depends on the choice of s_1, s_2, coefficients to be regarded as indeterminates, and the term order. We experimentally estimated optimal ones for each case to compute.

Computational parts for our proof of Corollary 5.3.14

Proposition 5.3.31 *Consider the quadratic forms* $Q^{(\mathrm{N1})} = 2xw + 2yz$, $Q^{(\mathrm{N2})} = 2xw + y^2 - \epsilon z^2$ *with* $\epsilon \in \mathbb{F}_{11}^{\times} \smallsetminus (\mathbb{F}_{11}^{\times})^2$, $Q^{(\mathrm{Dege})} = 2yw + z^2$ *and the cubic forms*

$$\begin{aligned}
P_1^{(\mathrm{alc})} &:= x^2y + x^2z + 2y^2z + 5y^2w + 9yz^2 + yzw + 4z^3 + 3z^2w + 10zw^2 + w^3,\\
P_2^{(\mathrm{alc})} &:= x^2y + x^2z + y^3 + y^2z + 7yz^2 + 4yw^2 + 2z^3 + 9zw^2,\\
P_3^{(\mathrm{alc})} &:= x^2y + x^2z + y^3 + 8y^2z + 3yz^2 + 10yw^2 + 10z^3 + 10zw^2,\\
P_4^{(\mathrm{alc})} &:= x^3 + y^3 + w^3,\\
P_5^{(\mathrm{alc})} &:= x^3 + y^3 + z^3 + 5w^3,\\
P_6^{(\mathrm{alc})} &:= x^3 + xw^2 + y^3,\\
P_7^{(\mathrm{alc})} &:= x^3 + xzw + y^3 + 7z^3 + w^3,\\
P_8^{(\mathrm{alc})} &:= x^3 + xyz + xw^2 + y^3 + 5z^3 + 4w^3,\\
P_9^{(\mathrm{alc})} &:= x^3 + xyz + 6xw^2 + y^3 + 8z^3 + 8w^3
\end{aligned}$$

in $\mathbb{F}_{11}[x, y, z, w]$. *Let* $P_i^{(\mathrm{N1})}$, $P_j^{(\mathrm{N2})}$ *and* $P_k^{(\mathrm{Dege})}$ *be as in* Propositions 5.3.27 – 5.3.29.

(1) *Each of* $V(P_i^{(\mathrm{N1})}, Q^{(\mathrm{N1})})$ *and* $V(P_j^{(\mathrm{N2})}, Q^{(\mathrm{N2})})$ *with* $1 \leq i \leq 8$ *and* $1 \leq j \leq 5$ *is isomorphic to* $V(P_k^{(\mathrm{alc})}, Q^{(\mathrm{N1})})$ *over* $\overline{\mathbb{F}_{11}}$ *for some* $1 \leq k \leq 3$*, and vice versa. Moreover,* $V(P_i^{(\mathrm{alc})}, Q^{(\mathrm{N1})})$ *is not isomorphic to* $V(P_j^{(\mathrm{alc})}, Q^{(\mathrm{N1})})$ *over* $\overline{\mathbb{F}_{11}}$ *for each* $1 \leq i < j \leq 3$*.*

(2) *Each* $V(P_i^{(\mathrm{Dege})}, Q^{(\mathrm{Dege})})$ *with* $1 \leq i \leq 17$ *is isomorphic to* $V(P_j^{(\mathrm{alc})}, Q^{(\mathrm{Dege})})$ *over* $\overline{\mathbb{F}_{11}}$ *for some* $4 \leq j \leq 9$*, and vice versa. Moreover,* $V(P_i^{(\mathrm{alc})}, Q^{(\mathrm{Dege})})$ *is not isomorphic to* $V(P_j^{(\mathrm{alc})}, Q^{(\mathrm{Dege})})$ *over* $\overline{\mathbb{F}_{11}}$ *for each* $4 \leq i < j \leq 9$*.*

Proof. We prove (1). Take $\epsilon = 2 \in \mathbb{F}_{11}$. We first transform $V(P_i^{(\mathrm{N2})}, Q^{(\mathrm{N2})})$ into $V(P, Q^{(\mathrm{N1})})$ for some cubic form P by the actions of elements in $\mathrm{GL}_4(\overline{\mathbb{F}_{11}})$. Put

$$M_Q := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1/2 & 1 & 0 \\ 0 & 1/2\sqrt{\epsilon} & -1/\sqrt{\epsilon} & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

and $P_{8+i}^{(\mathrm{N1})} := M_Q \cdot P_i^{(\mathrm{N2})} \pmod{Q^{(\mathrm{N1})}}$, where "(mod $Q^{(\mathrm{N1})}$)" means here replacing xw in $M_Q \cdot P_i^{(\mathrm{N2})}$ by $-2^{-1}(Q^{(\mathrm{N1})} - 2xw)$ via $xw \equiv -2^{-1}(Q^{(\mathrm{N1})} - 2xw) \bmod Q^{(\mathrm{N1})}$. Note that each $V(P_i^{(\mathrm{N2})}, Q^{(\mathrm{N2})})$ is isomorphic to $V(P_{8+i}^{(\mathrm{N1})}, Q^{(\mathrm{N1})})$ over $\overline{\mathbb{F}_{11}}$.

For $\mathcal{P} := (P_1^{(\mathrm{N1})}, \ldots, P_8^{(\mathrm{N1})}, P_9^{(\mathrm{N1})}, \ldots, P_{13}^{(\mathrm{N1})})$, we compute a subset $\mathcal{P}' \subset \mathcal{P}$ such that $V(Q, P_1)$ and $V(Q, P_2)$ are not isomorphic over $\overline{\mathbb{F}_{11}}$ for all P_1 and P_2 in $\mathcal{P}'$ with $P_1 \neq P_2$. Using a variant of Isomorphism Testing Algorithm for (N1) in Section 5.3.4 for each pair of cubics in $\mathcal{P}$, we obtain a required subset $\mathcal{P}' \subset \mathcal{P}$. Note that we need not test all pair of elements of $\mathcal{P}$ by pruning.

The outputs of our computations show that each $V(P_i^{(\mathrm{N1})}, Q^{(\mathrm{N1})})$ is isomorphic to $V(P_j^{(\mathrm{alc})}, Q^{(\mathrm{N1})})$ over $\overline{\mathbb{F}_{11}}$ for some $1 \leq j \leq 3$, and vice versa. The outputs also show that $V(P_i^{(\mathrm{alc})}, Q^{(\mathrm{N1})})$ is not isomorphic to $V(P_j^{(\mathrm{alc})}, Q^{(\mathrm{N1})})$ over $\overline{\mathbb{F}_{11}}$ for each $1 \leq i < j \leq 3$.

(2) is proved by a computation similar to (1). □

Chapter 6

Concluding remarks

In this thesis, we first reviewed two major methods for computing sheaf cohomology. One is based on the free resolution computation over a polynomial ring, whereas the other is based on that over an exterior algebra. We wrote down these two methods as concrete algorithms, and compared them over Magma, from a viewpoint of computer algebra. By our comparison together with concrete algorithms and our implementation over a computer algebra system, merits, efficiency, memory usage and possible applications of both the methods were clarified.

In main chapters (Chapters 4 and 5), we presented the following new algorithms based on the polynomial ring-based method: (1) Algorithms for computing the Frobenius on the cohomology groups of projective varieties. (2) Algorithms for enumerating (nonhyperelliptic) superspecial curves of genus 4. Different from previous works, the algorithms (1) involve a general-purpose algorithm, which works for arbitrary varieties of any dimension. The algorithms (2) are based on the algorithms (1). By executing the algorithms (2) over Magma, we determined the isomorphism classes of (nonhyperelliptic) superspecial curves of genus 4 over $\mathbb{F}_q$ for $q = 5, 25, 7, 49$ and 11.

Our future works are the following: (a) Develop an algorithm for computing the Frobenius on the cohomology groups based on the exterior algebra computation (cf. our algorithms given in this thesis are based on the polynomial ring computation). (b) Analyze the efficiency of the enumeration algorithms in this thesis, and improve them. (c) Investigate the (non-)existence of superspecial curves for lager p and for higher genus. Specifically the case of genus 5 is a next target.

Appendix: Computing homogeneous parts of a coordinate ring

Let $S = K[x_0, \ldots, x_n]$ denote the polynomial ring of $n+1$ variables over a field K, and let S_d denote the set of homogeneous polynomials in S of degree d for each $d \geq 0$. Let $\mathrm{Mon}(S)$ denote the set of monomials in S, and let $\mathrm{Mon}(S)_d$ denote the set of monomials of degree d. Let $I \subset S$ be a homogeneous ideal, and put $I_d := I \cap S_d$. The quotient ring S/I has a graded K-vector space structure by $(S/I)_d = S_d/I_d$. In this appendix, we review a method for computing a basis of the K-vector space $(S/I)_d$.

First we claim that it suffices to compute a basis of I_d. Indeed, once a basis $\{f_1, \ldots, f_s\}$ of I_d is computed, a basis of the quotient space S_d/I_d is computed from $\{f_1, \ldots, f_s\}$ and the basis

$$\left\{ x_0^{i_0} \cdots x_n^{i_n} : (i_0, \ldots, i_n) \in \mathbb{Z}_{\geq 0} \text{ with } \sum_{k=0}^{n} i_k = d \right\}$$

of S_d.

Here we construct a basis of I_d. Let $\succ$ be a term order on $x_0, \ldots, x_n$. There exist finite elements $f_1, \ldots, f_s \in I_d$ such that

$$\{\mathrm{LM}_{\succ}(f) : f \in I_d = I \cap S_d\} = \{\mathrm{LM}_{\succ}(f_i) : 1 \leq i \leq s\}$$

since

$$\{\mathrm{LM}_{\succ}(f) : f \in I_d = I \cap S_d\} \subset \mathrm{Mon}(S)_d$$

is finite. We may assume $\mathrm{LM}_{\succ}(f_1) \succ \cdots \succ \mathrm{LM}_{\succ}(f_s)$. One can verify that the set $\{f_1, \ldots, f_s\}$ is a basis of the K-vector space I_d, see e.g., [12, Section 9.3, Proposition 9] for a proof.

We can compute the above $f_1, \ldots, f_s$ as follows. Let G be a Gröbner basis for I with respect to a term order $\succ$. For each $f \in S$, we denote by $f^{(d)}$ its homogeneous part of degree d. Here we have

$$\{\mathrm{LM}_{\succ}(mg) : g \in G \text{ and } m \in \mathrm{Mon}(S) \text{ with } \deg(\mathrm{LM}_{\succ}(mg)) = d\} = \{\mathrm{LM}_{\succ}(f) : f \in I_d\}.$$

Thus putting

$$F_G := \{mg : g \in G \text{ and } m \in \mathrm{Mon}(S) \text{ with } \deg(\mathrm{LM}_{\succ}(mg)) = d\},$$

we have

$$\{\mathrm{LM}_{\succ}(h^{(d)}) : h \in F_G\} = \{\mathrm{LM}_{\succ}(f) : f \in I_d\}.$$

Consequently $\{h^{(d)} : h \in F_G\} \subset I_d$ is a basis of I_d.

Bibliography

[1] Aramova, A., Herzog, J. and Hibi, T.: *Gotzmann Theorems for Exterior Algebras and Combinatorics*, J. of Algebra, **191**, pp. 174–211, 1997.

[2] Bermejo, I. and Gimenez, P.: *Computing the Castelnuovo-Munford regularity of some subschemes of $\mathbb{P}^n_K$ using quotients of monomial ideals*, Journal of Pure and Applied Algebra, **164**, pp. 23–33, 2001.

[3] Bermejo, I. and Gimenez, P.: *Saturation and Castelnuovo-Munford regularity*, Journal of Algebra, **303**, pp. 592–617, 2006.

[4] Bernšteĭn, I. N., Gel'fand, I. M. and Gel'fand, S. I.: *Algebraic vector bundles on $\mathbf{P}^n$ and problems of linear algebra*, Functional Anal. Appl. **12**, pp. 212–214, 1978.

[5] Bettale, L., Faugère, J.-C. and Perret, L.: *Hybrid approach for solving multivariate systems over finite fields*, J. Math. Crypt., **3**, pp. 177–197, 2009.

[6] Bosma, W., Cannon, J. and Playoust, C.: *The Magma algebra system. I. The user language*, Journal of Symbolic Computation **24**, pp. 235–265, 1997.

[7] Bostan, A., Gaudry, P. and Schost, É.: *Linear recurrences with polynomial coefficients and computation of the Cartier-Manin operator on hyperelliptic curves*, LNCS **2948**, pp. 40–58, Springer-Verlag, 2004.

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

[9] Cannon, J., et al.: *Magma A Computer Algebra System*, School of Mathematics and Statistics, University of Sydney, 2016. `http://magma.maths.usyd.edu.au/magma/`

[10] Caviglia, G. and Sbarra, S.: *Characteristic-free bounds for the Castelnuovo-Mumford regularity*, Compositio Mathematica, vol. **141**, pp. 1365–1373, 2005.

[11] Chardin, M., Fall, A. L. and Nagel, U.: *Bounds for the Castelnuovo-Mumford regularity of modules*, Mathematische Zeitschrift, Vol. **258**, Issue 1, pp. 69–80, 2008.

[12] Cox, D., Little, J. and O'shea, D.: *Ideals, Varieties, and Algorithms*, Springer-Verlag, New York, 1992.

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

[14] Decker, W. and Eisenbud, D.: Sheaf Algorithm Using the Exterior Algebra, pp. 215–249, In: [20], 2002.

[15] Decker, W. and Lossen, C.: *Computing in Algebraic Geometry, A Quick Start using SINGULAR*, ACM **16**, Springer, 2000.

[16] Deuring, M.: Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. Abh. Math. Sem. Univ. Hamburg, **14**, no. 1, pp. 197–272, 1941.

[17] Eisenbud, D.: *Commutative Algebra: With a View Toward Algebraic Geometry*, GTM **150**, Springer, 1995.

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

[19] Eisenbud, D.: Chapter 8: Computing cohomology, pp. 219–226, In: [55], 1998.

[20] Eisenbud, D., Grayson, D. R., Stillman, M. and Sturmfels, B. eds.: *Computations in Algebraic Geometry with Macaulay2*, Springer-Verlag, 2002.

[21] 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.

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

[23] Faugère, J.-C.: *A new efficient algorithm for computing Gröbner bases (F4)*, Journal of Pure and Applied Algebra, **139**, pp. 61–88, 1999.

[24] Fossum, R. and Foxby, H.-S.: *The Category of Graded Modules*, Mathematica Scandinavica, **35**, no. 2, pp. 288–300, 1975.

[25] Fuhrmann R., Garcia, A. and Torres, F.: *On maximal curves*, Journal of number theory, **67**, pp. 29–51, 1997.

[26] Galbraith, S. D.: *Equations for modular curves*, Doctoral Thesis, Oxford University, 1996.

[27] Galbraith, S. D.: *Mathematics in Public Key Cryptography*, Cambridge University Press, 2012.

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

[29] Grayson, Daniel R. and Stillman, Michael E.: *Macaulay2, a software system for research in algebraic geometry*, available at `http://www.math.uiuc.edu/Macaulay2/`

[30] Greuel, G.-M., Pfister, G. and Schönemann, H.: *SINGULAR 3.0. A Computer Algebra System for Polynomial Computations, Centre for Computer Algebra*, University of Kaiserslautern, 2005, `http://www.singular.uni-kl.de`

[31] van der Geer, et al.: *Tables of Curves with Many Points*, 2009, `http://www.manypoints.org`, Retrieved at 5th April, 2017.

[32] van der Geer, G. and van der Vlugt, M.: *Tables of curves with many points*, Math. Comp. **69**, no. 230, pp. 797–810, 2000.

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

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

[35] Hashimoto K.: *Class numbers of positive definite ternary quaternion Hermitian forms.* Proc. Japan Acad. Ser. A Math. Sci., **59**, no. 10, pp. 490–493, 1983.

[36] Hashimoto, K. and Ibukiyama, T.: *On class numbers of positive definite binary quaternion Hermitian forms. II*, J. Fac. Sci. Univ. Tokyo Sect. IA Math., **28** (1981), no. 3, pp. 695–699, 1982.

[37] Horowitz, E.: *The Efficient Calculation of Powers of Polynomials*, Journal of Computer and System Science, **7**, pp. 469–480, 1973.

[38] Ibukiyama, T.: *On rational points of curves of genus* 3 *over finite fields*, Tohoku Math. J. **45**, pp. 311-329, 1993.

[39] Ibukiyama, T. and Katsura, T.: *On the field of definition of superspecial polarized abelian varieties and type numbers*, Compositio Math. **91**, no. 1, pp. 37–46, 1994.

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

[41] Kudo, M.: *Analysis of an algorithm to compute the cohomology groups of coherent sheaves and its applications*, Japan Journal of Industrial and Applied Mathematics, Vol. **31**, No. 1, pp. 1–40, 2017.

[42] Kudo, M.: *Computing representation matrices for the action of Frobenius to cohomology groups*, arXiv: 1704.08110 [math.AG], 2017.

[43] Kudo, M. and Harashita, S.: *Superspecial curves of genus 4 in small characteristic*, Finite Fields and Their Applications, **45**, pp. 131–169, 2017 (preprint version: arXiv: 1607.01114 [math.AG]).

[44] Kudo, M. and Harashita, S.: *Enumerating superspecial curves of genus 4 over prime fields*, arXiv: 1702.05313 [math.AG], 2017.

[45] Kudo , M. and Harashita, S.: *Enumerating Superspecial Curves of Genus 4 over Prime Fields*, In: Proceedings of The Tenth International Workshop on Coding and Cryptography 2017 (WCC2017), September 18-22, 2017, Saint-Petersburg, Russia, to appear.

[46] Kunz, E.: *Characterization of regular local rings of characteristic p*, American Journal of Mathematics, **41**, pp. 772–784, 1969.

[47] Madapusi, K.: *Commutative Algebra*, Harvard University, 2007, available at `http://math.uchicago.edu/~keerthi/files/CA.pdf`

[48] 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) 153–172). MR 0124324 (23 #A1638).

[49] Maruyama, M.: [Gröbner Bases and the Application] (in Japanese), Kyoritsu Publisher, 2002.

[50] Miler, C.: *The Frobenius endomorphism and homological dimensions*, arXiv, math. AC: 0301208v3, 2003.

[51] Serre, J.-P.: *Faisceaux algébriques cohérents*, Ann. of Math. (2), **61**, pp. 197–278, 1995.

[52] Serre, J.-P.: *Nombre des points des courbes algebrique sur* $\mathbb{F}_q$, Sém. Théor. Nombres Bordeaux (2) 1982/83, 22, 1983.

[53] Smith, G. G.: *Computing Global Extension Module*, Journal of Symbolic Computation, **29**, pp. 729–746, 2000.

[54] Tignol, J.-P. and Wadsworth, A. R.: *Value Functions on Simple Algebras, and Associated Graded Rings*, Springer Monographs in Mathematics, Springer International Publishing, 2015.

[55] Vasconcelos, W.: *Computational Methods in Commutative Algebra and Algebraic Geometry*, Algorithms and Computation in Mathematics, **2**, Springer, 1998.

[56] Xue, J., Yang, T.-C. and Yu, C.-F.: *On superspecial abelian surfaces over finite fields*, Doc. Math., **21**, pp. 1607–1643, 2016.

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

[58] Maple User Manual: Toronto: Maplesoft, a division of Waterloo Maple Inc., 2016., available on the web page
`http://www.maplesoft.com/products/maple/`

[59] Computation programs and log files for the paper "Computing representation matrices for the action of Frobenius to cohomology groups", available on the web page
`http://www2.math.kyushu-u.ac.jp/~m-kudo/comp_Frobenius.html`

[60] Computation programs and log files for the paper "Superspecial curves of genus 4 in small characteristic", available on the web page
`http://www2.math.kyushu-u.ac.jp/~m-kudo/kudo-harashita-comp.html`

List of papers

Journal

1. Momonari Kudo, *Analysis of an algorithm to compute the cohomology groups of coherent sheaves and its applications*, Japan Journal of Industrial and Applied Mathematics, Vol. **31**, No. 1, pp. 1–40, 2017.
2. Momonari Kudo and Shushi Harashita, *Superspecial curves of genus* 4 *in small characteristic*, Finite Fields and Their Applications, **45**, pp. 131–169, 2017.

Refereed International Conference Papers

1. Momonari Kudo, Junpei Yamaguchi, Yang Guo and Masaya Yasuda, *Practical Analysis of Key Recovery Attack against Search-LWE Problem*, In: Proceedings of The 11th International Workshop on Security (IWSEC), September 12-14, 2016, Tokyo, Japan, Lecture Notes in Computer Science, **9836**, pp. 164–181, 2016.
2. Jintai Ding, Momonari Kudo, Shinya Okumura, Tsuyoshi Takagi and Chengdong Tao, *Cryptanalysis of a public key cryptosystem based on Diophantine equations via weighted LLL reduction* (short paper), In: Proceedings of The 11th International Workshop on Security (IWSEC), September 12-14, 2016, Tokyo, Japan, Lecture Notes in Computer Science, **9836**, pp. 305–315, 2016.
3. Momonari Kudo and Shushi Harashita, *Enumerating Superspecial Curves of Genus 4 over Prime Fields*, In: Proceedings of The Tenth International Workshop on Coding and Cryptography 2017 (WCC2017), September 18-22, 2017, Saint-Petersburg, Russia.
4. Yuki Yokota, Momonari Kudo and Masaya Yasuda, *Practical Limit of Index Calculus Algorithms for ECDLP over Prime Fields*, In: Proceedings of The Tenth International Workshop on Coding and Cryptography 2017 (WCC2017), September 18-22, 2017, Saint-Petersburg, Russia.

Preprints

1. Momonari Kudo, *Computing representation matrices for the action of Frobenius to cohomology groups*, arXiv: 1704.08110 [math.AG], 2017, submitted.
2. Momonari Kudo, *Attacks against search Poly-LWE*, IACR Cryptology ePrint Archive, 2016/1153, 2016.