Master's thesis

Counting the numbers of points of curves in a family

Author:
Casper Putz

Supervisor:
Prof. Dr. Carel Faber

Second reader:
Prof. Dr. Frits Beukers

Utrecht University

8th July 2017

Abstract

The zeta function of an algebraic variety X over a finite field k is an exponential sum involving the number of points on the variety over all finite extensions of k. One would like find explicit expressions for zeta functions in an efficient way. We discuss a method for computing zeta functions of smooth projective hypersurfaces called the deformation method. The deformation method involves embedding the hypersurface X in a family of hypersurfaces, containing a hypersurface X_0 for which we know the action of Frobenius on rigid cohomology. We use that we can easily compute the action of Frobenius on diagonal hypersurfaces. The action of Frobenius satisfies a p-adic differential equation. Using a Lefschetz formula and the theory of p-adic differential equations, we can compute the zeta function of the hypersurface we started with.

In this thesis, we formulate the deformation method for families in many variables. We investigate if we can use the deformation method for the universal curve of genus 3. There turns out to be an explicit condition for when the deformation method fails, and we try to understand this condition. The condition is very unnatural in the sense that it depends on the choice of coordinates.

Acknowledgements

Firstly I would like to thank my supervisor Prof. Dr. Carel Faber for providing me with an interesting subject and guiding me during the process. I learned a lot during our biweekly meetings, and although we encountered many obstacles, he always came with new ideas for solutions.

I would also like to thank Prof. Dr. Frits Beukers for taking the time to be my second reader.

Furthermore, I would like to thank Prof. Dr. Gunther Cornelissen for providing me feedback during the go/no go presentation, and reading my early drafts halfway through the project.

I would like to thank my fellow students in the master's thesis seminar. Their enthousiasm and positive feedback made our weekly presentations not only useful, but also very enjoyable.

Lastly, I would like to thank my friends and family for their support during this project.

Contents

Chapter 1

Introduction

The first three paragraphs of this chapter are based on [PT14, section 1].

One problem in algebraic geometry is counting the number of points on a variety over some finite field, and its finite extensions. One way to capture this data is to write down a generating function called the *zeta function* $Z(X,T)$ of a variety X. As we will see in section 2.1, there exists a naive way of determining $Z(X,T)$. However, this method is not very efficient, thus one would like to have better algorithms to determine the zeta function.

The method we will look at uses p-adic cohomology. In [Ked01], Kedlaya introduces a method to compute the zeta function of a hyperelliptic curve in odd characteristic using Monsky-Washnitzer cohomology (which is a p-adic cohomology theory). For this, Kedlaya computes the action of the Frobenius endomorphism on cohomology, and uses a Lefschetz formula. This idea will be central in this thesis. In [AKR10], this method is generalised for smooth projective hypersurfaces.

Lauder ([Lau04a, Lau04b]) showed that in terms of time complexity there is an even better way of computing zeta functions of smooth projective hypersurfaces. Instead of directly computing the action of Frobenius on the cohomology group of a smooth projective hypersurface X, one first embeds X into a family of smooth projective hypersurfaces which contains a diagonal fibre (see section 1.1 for the definition and more details). It turns out that computing the action of Frobenius on the diagonal hypersurface is easier, and the action of Frobenius satisfies some p-adic differential equation. Hence, solving the differential equation gives us the action of Frobenius on the p-adic cohomology of X. This is called the deformation method. Lauder's method uses Dwork cohomology. Gerkmann reformulated Lauder's method for rigid cohomology, which is somewhat easier to work with [Ger07]. Gerkmann also made improvements to precision bounds and the algorithm in general.

The original motivation of the deformation method was improving the time complexity for computing the zeta function of a single smooth projective hypersurface. However, the method also gives us a way of computing the zeta function of every fibre in a family $\mathcal{X}/\mathcal{S}$ that contains a diagonal fibre[1]. This brings us to the question whether this method could be used to effectively count all points in some family of hypersurfaces. One example of this is counting the number of points on a universal curve (for example the universal curve of genus g). Many moduli spaces can be stratified in a natural way. In many cases, one can determine normal forms for the objects belonging to a given stratum. In the case of a moduli space of curves, this is a family of smooth projective curves such that each curve in a given stratum is represented by at least one fibre. However, some fibres may be isomorphic and we need to account for that. Counting all points on the universal curve then boils down to counting all points on the normal form and compensating for the points that we counted multiple times.

Our main reference for the deformation method is [PT14], which gives a description of the method for 1-parameter families of smooth projective hypersurfaces. In this thesis we generalize the deformation method to families in multiple parameters. Then we look into whether this method can be applied to compute the zeta function of a universal curve. For computations, we use a very fast implementation of the 1-parameter version of the deformation method for smooth projective hypersurfaces by Sebastian Pancratz [Pan14]. His method has been implemented for families in many parameters using both Mathematica [Put17a] and Sage [Put17b] by the author.

We start in Chapter 2 by introducing our main object of study: the zeta function of an algebraic variety. We give some theorems which we will use to compute zeta functions. We then give an overview of the deformation method, which will motivate the rest of the chapters.

After this, we discuss algebraic de Rham cohomology and rigid cohomology in Chapter 3. We also introduce the Gauss-Manin connection on the algebraic de Rham cohomology. The last two sections go into computation of the Gauss-Manin connection.

The essential part of the deformation method is a collection of differential equations which we derive in Chapter 4. In the first part of the chapter we derive the differential equations, and in the second part we solve the differential equations.

In Chapter 5, the last parts of the deformation method are presented. This involves computing the action of Frobenius on the rigid cohomology of a diagonal fibre, and recovering the zeta function from approximations of the action of Frobenius.

[1] Except for all s in some subvariety of $\mathcal{S}$ of codimension 1.

As these last computations are not dependend on the dimension of the family, and the 1-dimensional case is already discussed in [PT14], we do not give any proofs. This completes our description of the deformation method.

In Chapter 6 we give examples of the deformation method for a 1-dimensional family and a 2-dimensional family of quartic curves.

Finally, in Chapter 7 we discuss the main question of this thesis: Can we use the deformation method to efficiently compute the zeta function of the universal curve of genus 3? We do so by first going into the case of curves of degree 2 and 3. After this, we discuss quartic curves (which are our main objects of study as "almost all genus 3 curves are quartic curves").

1.1 Setup and notation

In this thesis we use the following setup and notation. Let p be a prime and q a power of p. Let $\mathbb{Q}_p$ denote the field of p-adic integers, and $\mathbb{Q}_q$ denote the unique unramified extension of $\mathbb{Q}_p$ with residue field $\mathbb{F}_q$. Let $\mathbb{Z}_p$ and $\mathbb{Z}_q$ be the rings of integers of $\mathbb{Q}_p$ and $\mathbb{Q}_q$, respectively.

Given is a family of smooth projective hypersurfaces in $\mathbb{P}^n$ over $\mathbb{F}_q$, $f\colon X \to S$, where S is a Zariski open subset of $\mathbb{P}^s_{\mathbb{F}_q}$ and $n, s \in \mathbb{N}$. We take a smooth lift $\mathcal{X}/\mathcal{S}$ of X/S defined over $\mathbb{Z}_q$. Let $\mathcal{U}/\mathcal{S}$ be the complement of $\mathcal{X}/\mathcal{S}$ in $\mathbb{P}^n_{\mathcal{S}}$. Then the special fibres of $\mathcal{X}$, $\mathcal{U}$ and $\mathcal{S}$ are $X = \mathcal{X} \otimes \mathbb{F}_q$, $U = \mathcal{U} \otimes \mathbb{F}_q$ and $S = \mathcal{S} \otimes \mathbb{F}_q$, respectively. The generic fibres are denoted by $\mathfrak{X} = \mathcal{X} \otimes \mathbb{Q}_q$, $\mathfrak{U} = \mathcal{U} \otimes \mathbb{Q}_q$ and $\mathfrak{S} = \mathcal{S} \otimes \mathbb{Q}_q$.

Suppose that the family $\mathcal{X}/\mathcal{S} \subset \mathbb{P}^n_{\mathcal{S}}$ of smooth hypersurfaces is given by a polynomial $P \in \mathbb{Z}_q[t_1, \ldots, t_s][x_0, \ldots, x_n]$, homogeneous of degree d in $x_0, \ldots, x_n$. We assume that $\mathcal{X}/\mathcal{S}$ contains a smooth *diagonal fibre*, i.e. for some $\tau_0 \in \mathcal{S}$ the fibre $\mathcal{X}_{\tau_0}$ is defined by a polynomial equation of the form

$$a_0 x_0^d + a_1 x_1^d + \cdots + a_n x_n^d = 0,$$

with $a_0, \ldots, a_n \in \mathbb{Z}_q^\times$. By applying a projective transformation, we may assume that $0 \in \mathcal{S}$ and that $\mathcal{X}_0$ is a smooth diagonal fibre.

We will also assume that $\mathcal{X}/\mathcal{S}$ admits a *relative normal crossing compactification* (for the definition, see [Tui10, Definition 3.3.1]). This is needed for the algebraic de Rham cohomology and rigid cohomology of X/S to "behave well".

Chapter 2

Zeta functions

In this chapter we introduce the zeta function of an algebraic variety and some properties of zeta functions which we will use to compute them. We also give a brief description of the deformation method.

2.1 Introduction to zeta functions

Suppose we want to count the number of points on an algebraic variety $X/\mathbb{F}_q$ over every finite extension of $\mathbb{F}_q$. We can capture this data using the following generating function.

Definition 2.1. Let X be an algebraic variety over $\mathbb{F}_q$. Then we define the *zeta function* of X to be the formal power series

$$Z(X,T) = \exp\left(\sum_{i=1}^{\infty} |X(\mathbb{F}_{q^i})| \frac{T^i}{i}\right). \tag{2.1}$$

Theorem 2.2 (Weil conjectures[1])**.** *Let X be a smooth projective variety over $\mathbb{F}_q$ of dimension m. Then*

$$Z(X,T) = \frac{p_1 p_3 \cdots p_{2m-1}}{p_0 p_2 \cdots p_{2m}},$$

with $p_i = \prod_j (1 - \alpha_{i,j} T) \in \mathbb{Z}[T]$ for all $0 \leq i \leq 2n$. Furthermore, the map $t \mapsto q^m/t$ sends the $\alpha_{i,j}$ bijectively to the $\alpha_{2m-i,k}$ preserving multiplicities, and $|\alpha_{i,j}| = q^{i/2}$ for all embeddings $\overline{\mathbb{Q}} \to \mathbb{C}$.

[1] The statements of the theorem were originally conjectured by Weil. Although they are often still refered to as the "Weil conjectures", the conjectures were proven by Dwork, Artin, Grothendieck and Deligne in the 1960s and 1970s.

The rationality of $Z(X,T)$ means that we can find it by only computing a finite amount of data. There exist bounds on the degrees of the numerator and of the denominator of $Z(X,T)$ [Bom78]. This gives us a simple algorithm to determine $Z(X,T)$ by naively computing finitely many of the coefficients $|X(\mathbb{F}_{q^i})|$.

The running time of this algorithm is polynomial in q, which means that it is exponential in its number of digits $\log q$. The following method gives us a better time complexity. For a smooth proper algebraic variety, we can compute the zeta function using the Lefschetz formula.

Theorem 2.3 (Lefschetz formula [PT14, Theorem 2.3])**.** *Let X be a smooth proper algebraic variety over $\mathbb{F}_q$ of dimension m. Then*

$$Z(X,T) = \prod_{i=0}^{2m} \det(1 - TF_q \mid \mathcal{H}^i_{\mathrm{rig}}(X))^{(-1)^{i+1}}, \tag{2.2}$$

where F_q is the q-Frobenius endomorphism on $\mathcal{H}^i_{\mathrm{rig}}(X)$ and $\mathcal{H}^i_{\mathrm{rig}}(X)$ is the i-th rigid cohomology sheaf on X, which will be introduced in Section 3.2.

If X is a smooth projective hypersurface, then we can directly compute almost all terms of (2.2). The following theorem is formulated for the case we are interested in, which is a family of smooth projective hypersurfaces.

Theorem 2.4. *Suppose that X/S is a family of smooth projective hypersurfaces in $\mathbb{P}^n_{\mathbb{F}_q}$ and $\mathbb{F}_\mathfrak{q}/\mathbb{F}_q$ is a finite field extension. For all $\tau \in S(\mathbb{F}_\mathfrak{q})$ we have*

$$Z(X_\tau, T) = \frac{\chi(T)^{(-1)^n}}{(1-T)(1-\mathfrak{q}T)\cdot \ldots \cdot (1-\mathfrak{q}^{n-1}T)},$$

with $\chi(T) = \det(1 - T\mathfrak{q}^{-1}F_\mathfrak{q} \mid \mathcal{H}^n_{\mathrm{rig}}(U_\tau))$.

Proof. See [Ger07, Theorem 3.1]. ■

Using a Lefschetz formula, Kedlaya ([Ked01]) gave an algorithm for computing the zeta function of a hyperelliptic curve of genus g over $\mathbb{F}_{p^k}$. For fixed p, this algorithm runs in time complexity $O(g^{4+\epsilon}k^{3+\epsilon})$ (where ϵ is arbitrarily small), which is much better than the naive approach since it is polynomial in $k = \log_p(q)$.

2.2 The deformation method

We now briefly describe the deformation method. We will use the results that we prove in chapters 3, 4 and 5.

Let $\mathfrak{q} = p^a$ with $q \mid \mathfrak{q}$ and let $\tau \in S(\mathbb{F}_\mathfrak{q})$. We want to compute the zeta function of the fibre X_τ of X/S. Using Theorem 2.4 we can do this by computing the action of $\mathfrak{q}^{-1}F_\mathfrak{q}$ on the rigid cohomology space $\mathcal{H}^n_{\mathrm{rig}}(U_\tau)$ where U_τ is the fibre at τ of U/S. In Section 3 we will introduce the algebraic de Rham cohomology spaces $\mathcal{H}^i_{\mathrm{dR}}(\mathfrak{X}/\mathfrak{S})$, and using Theorem 3.8 we can relate $\mathcal{H}^n_{\mathrm{rig}}(U/S)$ to $\mathcal{H}^n_{\mathrm{dR}}(\mathfrak{U}/\mathfrak{S})$. It will be more convenient for us to work with de Rham cohomology instead of rigid cohomology. The algebraic de Rham cohomology space also has an action of Frobenius and the isomorphism from Theorem 3.8 preserves the action of Frobenius. Hence, we shifted the problem to computing the action of $\mathfrak{q}^{-1}F_\mathfrak{q}$ on $\mathcal{H}^n_{\mathrm{dR}}(\mathfrak{U}_{\hat{\tau}})$ (where $\hat{\tau}$ is a lift of τ).

In Section 3.1, we show that $\mathcal{H}^n_{\mathrm{dR}}(\mathfrak{U}/\mathfrak{S})$ is equipped with a structure called a connection ∇, which is similar to a derivative, and this connection induces a connection on $\mathcal{H}^n_{\mathrm{rig}}(U/S)$. The actions of ∇ and $p^{-1}F_p$ are given by matrices $M^{(k)}$ with $k = 1, \ldots, s$ and A_p, respectively. One can show that the connection commutes with the action of Frobenius and using this we derive p-adic differential equations

$$\frac{dA_p}{dt_k} + M^{(k)}A_p = pt_k^{p-1}A_p\big(M^{(k)}\big)^F,$$

for $k = 1, \ldots, s$, where F is the p-power Frobenius on $\mathbb{Q}_q$ and sends $t_i \mapsto t_i^p$ (Section 4.1). The trick of the deformation method is to compute $M^{(k)}$ for all $\hat{\tau} \in \mathcal{S}(\mathbb{Z}_\mathfrak{q})$ (so in terms of $t_1, \ldots, t_s$), and compute A_p for one single fibre. It turns out that it is convenient to choose a diagonal fibre as this single fibre for which we need to compute the action of Frobenius. If we then solve these differential equations for A_p, we find A_p for all $\hat{\tau} \in \mathcal{S}(\mathbb{Z}_\mathfrak{q})$. Write $A_{p,\tau}$ for the action of $p^{-1}F_p$ on $\mathcal{H}^n_{\mathrm{rig}}(U_\tau)$. We can then derive the action of $\mathfrak{q}^{-1}F_\mathfrak{q}$ on $\mathcal{H}^n_{\mathrm{rig}}(U_\tau)$ (Section 5.2), which we denote by $A_{\mathfrak{q},\tau}$, via the formula

$$A_{\mathfrak{q},\tau} = A_{p,\tau}A_{p,\tau}^{\sigma} \cdots A_{p,\tau}^{\sigma^{a-1}}.$$

Here $\sigma\colon \mathbb{Q}_q \to \mathbb{Q}_q$ is the p-Frobenius map. We can then compute $Z(X_\tau, T)$ using Theorem 2.4 and Theorem 5.10.

Chapter 3

Cohomology theories

In this chapter, we first briefly discuss the algebraic de Rham cohomology and the construction of the Gauss-Manin connection. After this, we introduce rigid cohomology and give a comparison theorem. Lastly, we look at computations in the de Rham cohomology and specifically at computing the Gauss-Manin connection.

3.1 Algebraic de Rham cohomology and the Gauss-Manin connection

Let $f\colon \mathfrak{X} \to \mathfrak{S}$ be a smooth family of algebraic varieties over k. Let $\Omega^1_{\mathfrak{X}/\mathfrak{S}}$ be the sheaf of relative 1-forms of $\mathfrak{X}$ over $\mathfrak{S}$. We have a map $d_{\mathfrak{X}/\mathfrak{S}}\colon \mathcal{O}_{\mathfrak{X}} \to \Omega^1_{\mathfrak{X}/\mathfrak{S}}$, which is an $\mathfrak{S}$-derivation of $\mathcal{O}_{\mathfrak{X}}$ in $\Omega^1_{\mathfrak{X}/\mathfrak{S}}$ and which is universal in the sense that any S-derivation of $\mathcal{O}_{\mathfrak{X}}$ in an $\mathcal{O}_{\mathfrak{X}}$-module M factors through $\Omega^1_{\mathfrak{X}/\mathfrak{S}}$ [Ill96, §1, 1.2]. For all $i \in \mathbb{Z}$ we define

$$\Omega^i_{\mathfrak{X}/\mathfrak{S}} = \begin{cases} \bigwedge^i \Omega^1_{\mathfrak{X}/\mathfrak{S}} & \text{if } i \geq 1; \\ \mathcal{O}_{\mathfrak{X}} & \text{if } i = 0; \\ 0 & \text{if } i < 0. \end{cases}$$

Then $d_{\mathfrak{X}/\mathfrak{S}}$ induces a family of maps that turns $\Omega^\bullet_{\mathfrak{X}/\mathfrak{S}}$ into a complex.

Proposition 3.1. *For all $i \geq 0$ there exist maps $d_i\colon \Omega^i_{\mathfrak{X}/\mathfrak{S}} \to \Omega^{i+1}_{\mathfrak{X}/\mathfrak{S}}$ such that:*

(i) d_i is an $f^{-1}(\mathcal{O}_{\mathfrak{S}})$-linear map with $d_i(ab) = d_i(a) \wedge b + (-1)^j a \wedge d_i(b)$ for all $i \geq 0$, $j \geq 0$ and $a \in \Omega^j_{\mathfrak{X}/\mathfrak{S}}$;

(ii) $d_{i+1} \circ d_i = 0$ for all $i \geq 0$;

(iii) $d_0(a) = d_{\mathfrak{X}/\mathfrak{S}}(a)$ for all $a \in \mathcal{O}_{\mathfrak{X}}$.

Proof. See [Ill96, §1, 1.7]. ■

Hence, we get a complex

$$0 \xrightarrow{d_0} \mathcal{O}_{\mathfrak{X}} \xrightarrow{d_1} \Omega^1_{\mathfrak{X}/\mathfrak{S}} \xrightarrow{d_2} \Omega^2_{\mathfrak{X}/\mathfrak{S}} \xrightarrow{d_3} \dots,$$

which we denote by $\Omega^\bullet_{\mathfrak{X}/\mathfrak{S}}$. The algebraic de Rham cohomology is constructed using this complex.

Definition 3.2. We define the *relative de Rham cohomology sheaf* as $\mathcal{H}^\bullet_{\mathrm{dR}}(X/S) = \mathcal{R}^i f_*(\Omega^\bullet_{X/S})$ where $\mathcal{R}^i f_*$ is the i-th hyperderived functor of f_*.

Lemma 3.3. *If $\mathfrak{X}/\mathfrak{S}$ admits a relative normal crossing compactification, then $\mathcal{H}^i_{\mathrm{dR}}(\mathfrak{X}/\mathfrak{S})$ is locally free for all i.*

Proof. This is [Tui10, Theorem 3.4.2]. ■

This lemma has a nice corollary.

Corollary 3.4. *If $\mathfrak{X}/\mathfrak{S}$ admits a relative normal crossing compactification, then $\mathcal{H}^i_{\mathrm{dR}}(\mathfrak{X}/\mathfrak{S})$ is a vector bundle on $\mathfrak{S}$ for all i.*

Now that we have vector bundles, we define connections on vector bundles.

Definition 3.5. Let $\mathfrak{E}$ be a vector bundle on $\mathfrak{S}$. A *connection* on $\mathfrak{E}$ is a map of vector bundles $\nabla\colon \mathfrak{E} \to \mathfrak{E} \otimes_{\mathcal{O}_{\mathfrak{S}}} \Omega^1_{\mathfrak{S}/k}$ which satisfies the Leibniz rule, i.e.

$$\nabla(\omega e) = \omega\nabla(e) + e \otimes d\omega,$$

for all local sections ω of $\mathcal{O}_{\mathfrak{S}}$ and e of $\mathfrak{E}$.

We will construct a connection on the vector bundle $\mathcal{H}^j_{\mathrm{dR}}(\mathfrak{X}/\mathfrak{S})$ for $j \geq 0$ called the Gauss-Manin connection. We can define a filtration $F^i = F^i(\Omega^\bullet_{\mathfrak{X}}) = \mathrm{im}(\Omega^{\bullet-i}_{\mathfrak{X}/k} \otimes_{\mathcal{O}_{\mathfrak{X}}} f^*\Omega^i_{\mathfrak{S}/k} \xrightarrow{g_i} \Omega^\bullet_{\mathfrak{X}/k})$, where the map g_i is given by $\wedge^{\bullet-i}\mathrm{id}_{\Omega_{\mathfrak{X}/k}} \otimes \wedge^i (f^*\Omega_{\mathfrak{S}/k} \to \Omega_{\mathfrak{X}/k})$. This filtration gives rise to a spectral sequence $(E^{p,q}_r, d^{p,q}_r)$ on $\mathfrak{S}$ as is described in [GH78, §3.5, p. 439]. If we use that $\Omega^i_{\mathfrak{X}/k}$ and $\Omega^i_{\mathfrak{S}/k}$ are locally free, that f is smooth, and that the differentials in the complex $\Omega^\bullet_{\mathfrak{X}/k} \otimes_{\mathcal{O}_{\mathfrak{X}}} f^*\Omega^i_{\mathfrak{S}/k}$ are $f^{-1}(\mathcal{O}_{\mathfrak{S}})$-linear, a computation in [KO68, §2, p. 202] gives us

$$E^{i,j}_1 = \mathcal{H}^j_{\mathrm{dR}}(\mathfrak{X}/\mathfrak{S}) \otimes_{\mathcal{O}_{\mathfrak{S}}} \Omega^i_{\mathfrak{S}/k}.$$

We have maps $d^{0,j}_1\colon E^{0,j}_1 \to E^{1,j}_1$ from the spectral sequence. Using the previous calculation we can define the Gauss-Manin connection.

Definition 3.6. The *Gauss-Manin connection* $\nabla\colon \mathcal{H}^j_{\mathrm{dR}}(\mathfrak{X}/\mathfrak{S}) \to \mathcal{H}^j_{\mathrm{dR}}(\mathfrak{X}/\mathfrak{S}) \otimes_{\mathcal{O}_{\mathfrak{S}}} \Omega^1_{\mathfrak{S}/k}$ is defined as the map $d_1^{0,j}$ for all $j \geq 0$.

Another calculation in [KO68, §2, p. 203] gives us that ∇ is indeed a connection.

3.2 Rigid cohomology

In this section we give the basic properties of rigid cohomology. We do not give any details or proofs as our goal is only to relate it to the algebraic de Rham cohomology, and use the Lefschetz formula.

One can define the *rigid analytic spaces* $]\overline{X}[$ and $]\overline{S}[$. We can think about a rigid analytic space as the analogue of a complex analytic space over a non-Archimedean field. The analogue of the structure sheaf and the sheaf of differentials of S are the *overconvergent structure sheaf* $\mathcal{O}_S^\dagger$ and the *overconvergent sheaf of differentials* ${\Omega^1_S}^\dagger$. As the analogue of the relative algebraic de Rham cohomology, we have the *relative rigid cohomology sheaf* of a family X/S denoted by $\mathcal{H}^1_{\mathrm{rig}}(X/S)$, which is a sheaf on the rigid analytic space $]\overline{S}[$. We now give some of the properties of rigid cohomology.

Proposition 3.7. *Let $i \geq 0$. Then $\mathcal{H}^i_{\mathrm{rig}}(U/S)$ satisfies the following properties.*

(i) *The space $\mathcal{H}^i_{\mathrm{rig}}(X/S)$ is a so called overconvergent F-isocrystal. This means that $\mathcal{H}^i_{\mathrm{rig}}(X/S)$ is eqquiped with a connection (which comes from the Gauss-Manin connection ∇) and a Frobenius isomorphism*

$$\mathcal{F}\colon F^*\mathcal{H}^i_{\mathrm{rig}}(X/S) \to \mathcal{H}^i_{\mathrm{rig}}(X/S).$$

Furthermore, ∇ and $\mathcal{F}$ commute [Tui10, Definition 3.4.8 and Theorem 3.4.10].

(ii) *The connection $\nabla\colon \mathcal{H}^i_{\mathrm{rig}}(U/S) \to \mathcal{H}^i_{\mathrm{rig}}(U/S) \otimes {\Omega^1_S}^\dagger$ is a linear action so there exist matrices $M^{(k)} \in M_{b\times b}(\mathbb{Q}_q(t_1, \ldots, t_s))$ for $k = 1, \ldots, s$ such that*

$$\nabla(m_j) = \sum_{k=1}^{s}\sum_{i=1}^{b} M^{(k)}_{ij} m_i \otimes dt_k, \tag{3.1}$$

for all $j = 1, \ldots, b$ where $\{m_1, \ldots, m_b\}$ forms a basis of global sections of $H^0(]\overline{S}[, \mathcal{H}^i_{\mathrm{rig}}(U/S))$.

(iv) *The sheaf $\mathcal{H}^i_{\mathrm{rig}}(U/S)$ is a locally free sheaf of $\mathbb{Q}_q\langle t_1, \ldots, t_s, 1/r\rangle^\dagger$-modules. Here $\mathbb{Q}_q\langle t_1, \ldots, t_s, 1/r\rangle^\dagger$ is a ring of overconvergent functions [Tui10, Definition 3.2.3] and $r \in \mathbb{Z}_q[t_1, \ldots, t_s]$ is the common denominator of the matrices $M^{(k)}$ of ∇.*

(iii) *The action of Frobenius on* $\mathcal{H}^i_{\mathrm{rig}}(U/S)$ *is defined as follows. Let* F_p *denote the* p*-th power Frobenius endomorphism* $\mathbb{F}_p \to \mathbb{F}_p$*. We can lift this to* $\sigma\colon \mathbb{Q}_q \to \mathbb{Q}_q$*. Let* $F\colon \mathbb{Q}_q\langle t_1, \ldots, t_s, 1/r\rangle^\dagger \to \mathbb{Q}_q\langle t_1, \ldots, t_s, 1/r\rangle^\dagger$ *be given by* σ *on* $\mathbb{Q}_q$ *and* $F(t_i) = t_i^p$ *for* $i = 1, \ldots, s$*. Then* F *induces an action* $\mathcal{F}\colon \mathcal{H}^i_{\mathrm{rig}}(U/S) \to \mathcal{H}^i_{\mathrm{rig}}(U/S)$*.*

Proof. See [Tui10, Section 3.4.2]. ■

The last property that we will use is that we can relate the rigid cohomology of the special fibre to the de Rham cohomology of the generic fibre.

Theorem 3.8. *Suppose that* $\mathcal{X}/\mathcal{S}$ *admits a relative normal crossing compactification. Then there is a canonical isomorphism*

$$\mathcal{H}^i_{\mathrm{dR}}(\mathfrak{X}/\mathfrak{S}) \otimes \mathcal{O}^\dagger_S \to \mathcal{H}^i_{\mathrm{rig}}(X/S),$$

of locally free sheaves of $\mathcal{O}^\dagger_S$*-modules with connection, for all* $i \geq 0$*.*

Proof. See [Tui10, Theorem 3.4.12]. ■

As we will see later, we need to compute the action of ∇ on $\mathcal{H}^n_{\mathrm{rig}}(U/S)$. By the previous theorem, we can instead compute the action of ∇ on $\mathcal{H}^n_{\mathrm{dR}}(\mathfrak{U}/\mathfrak{S})$. In the next section, we find a basis of $\mathcal{H}^n_{\mathrm{dR}}(\mathfrak{U}/\mathfrak{S})$ so that we can do explicit computations.

3.3 Computations of the de Rham cohomology

The following proposition gives an explicit description of the algebraic de Rham cohomology of the complement of a smooth projective hypersurface.

Proposition 3.9. *Let* Ω *denote the* n*-form on* $\mathfrak{U}/\mathfrak{S}$ *defined by*

$$\Omega = \sum_{i=0}^{n} (-1)^i x_i dx_0 \wedge \cdots \wedge \widehat{dx_i} \wedge \cdots \wedge dx_n.$$

Let C *be the space of closed* n*-forms* $Q\Omega/P^k$ *with* $k \in \mathbb{N}$ *and* $Q \in H^0(\mathfrak{S}, \mathcal{O}_{\mathfrak{S}})[x_0, \ldots, x_n]$ *homogeneous of degree* $kd-(n+1)$*. Let* E *be the subspace of exact* n*-forms generated by*

$$\frac{(\partial_i R)\Omega}{P^k} - k\frac{R(\partial_i P)\Omega}{P^{k+1}}, \tag{3.2}$$

with $0 \leq i \leq n$*,* $k \in \mathbb{N}$ *and* $R \in H^0(\mathfrak{S}, \mathcal{O}_{\mathfrak{S}})[x_0, \ldots, x_n]$ *homogeneous of degree* $(k-1)d-n$*. Here* ∂_i *denotes the partial derivative operator with respect to* x_i*. Then* $\mathcal{H}^n_{\mathrm{dR}}(\mathfrak{U}/\mathfrak{S}) \cong C/E$

Proof. See [PT14, Proposition 3.1]. ∎

We want to find an explicit basis for $\mathcal{H}^n_{\mathrm{dR}}(\mathfrak{U}/\mathfrak{S})$. Instead of working with $\mathfrak{U}/\mathfrak{S}$, we work over the generic fibre

$$\mathfrak{U}_{\mathbb{Q}_q(t_1,\dots,t_s)} = \mathfrak{U}/\mathfrak{S} \times_{\mathfrak{S}} \mathbb{Q}_q(t_1,\dots,t_s).$$

This gives the advantage that $\mathcal{H}^n_{\mathrm{dR}}\big(\mathfrak{U}_{\mathbb{Q}_q(t_1,\dots,t_s)}\big)$ is a $\mathbb{Q}_q(t_1,\dots,t_s)$-vector space, so we can apply linear algebra. Our approach is to reduce the poles of monomial elements of $\mathcal{H}^n_{\mathrm{dR}}(\mathcal{U}/\mathcal{S})$ using (3.2). We then show that our reduced set forms a basis of $\mathcal{H}^n_{\mathrm{dR}}(\mathcal{U}/\mathcal{S})$.

First we define the following sets of monomials:

Definition 3.10. Let $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$. For $k \in \mathbb{N}$, we define

$$\begin{aligned} F_k &= \big\{x^u \mid u \in \mathbb{N}_0^{n+1} \text{ and } |u| = kd - (n+1)\big\}; \\ B_k &= \{x^u \in F_k \mid u_i < d-1 \text{ for all } 0 \le i \le n\}; \\ R_k &= F_k - B_k, \end{aligned}$$

with $x^u = x_0^{u_0} \cdot \ldots \cdot x_n^{u_n}$ and $|u| = \sum_{i=0}^n u_i$ for $u = (u_0,\dots,u_n) \in \mathbb{N}_0^{n+1}$. Furthermore, for $k \in \mathbb{N}$ we define

$$\mathcal{B}_k = \{Q\Omega/P^k \mid Q \in B_k\}.$$

Write $B = B_1 \cup \cdots \cup B_n$ and $\mathcal{B} = \mathcal{B}_1 \cup \cdots \cup \mathcal{B}_n$.

We will show that if $\mathcal{X}/\mathcal{S}$ contains a diagonal fibre, then $\mathcal{B}$ forms a basis of $\mathcal{H}^n_{\mathrm{dR}}\big(\mathfrak{U}_{\mathbb{Q}_q(t_1,\dots,t_s)}\big)$. For this, we construct an algorithm for reducing an n-form $Q\Omega/P^k$ with $Q \in F_k$ to an element of the $\mathbb{Q}_q(t_1,\dots,t_s)$-span of $\mathcal{B}$ in cohomology.

Definition 3.11. For $k \in \mathbb{N}$, let

$$C_k^{(0)} = \big\{x^u \mid u \in \mathbb{N}_0^{n+1} \text{ and } |u| = (k-1)d - n\big\}.$$

For $1 \le j \le n$ we define inductively

$$C_k^{(j)} = \Big\{x^u \in C_k^{(j-1)} \;\Big|\; x_{j-1}^{d-1} \nmid x^u\Big\}.$$

We then define C_k as the disjoint union $C_k^{(0)} \sqcup \cdots \sqcup C_k^{(n)}$. We will denote an element of C_k by (j,g) where $0 \le j \le n$ and $g \in C_k^{(j)}$.

Lemma 3.12. *For all $k \in \mathbb{N}$, the sets R_k and C_k have the same cardinality.*

Proof. See [PT14, Lemma 3.4]. ∎

Definition 3.13. For $k \in \mathbb{N}$, let V_k and W_k be the $\mathbb{Q}_q(t_1, \ldots, t_s)$-vector space of polynomials with bases F_k and R_k, respectively. Furthermore, for $0 \leq j \leq n$, let $U_k^{(j)}$ be the $\mathbb{Q}_q(t_1, \ldots, t_s)$-vector space with basis $C_k^{(j)}$ and define $U_k = U_k^{(0)} \times \cdots \times U_k^{(n)}$ (so C_k is a basis of U_k). Let $\pi \colon V_k \to W_k$ be the projection which sends every element of B_k to 0 and sends an element of R_k to itself. We define a map $\phi_k \colon U_k \to W_k$ by

$$\phi_k(Q_0, \ldots, Q_n) = \pi(Q_0 \partial_0 P + \cdots + Q_n \partial_n P).$$

For $k \in \mathbb{N}$ we also define the square matrix Δ_k with row and column index sets R_k and C_k as follows: for $f \in R_k$ and $(j, g) \in C_k$ we define the corresponding entry of Δ_k to be

$$(\Delta_k)_{f,(j,g)} = \begin{cases} \text{the coefficient of } f/g \text{ in } \partial_j P & \text{if } g \mid f; \\ 0 & \text{otherwise.} \end{cases} \tag{3.3}$$

Note that f and g are monomials, and if $g \mid f$, then

$$\deg(f/g) = \deg(f) - \deg(g) = (kd - (n+1)) - ((k-1)d - n) = d - 1 = \deg(\partial_j P),$$

so it makes sense to talk about the coefficient of f/g in $\partial_j P$.

The matrix Δ_k corresponds to the linear map ϕ_k. Namely, for $(j, g) \in C_k$, we have $\phi_k(0, \ldots, 0, g, 0, \ldots, 0) = g \partial_j P$ (where we put g in the j-th position) and so the element on position $(f, (j, g))$ of the matrix of ϕ_k is as in (3.3).

Theorem 3.14 ([PT14, Theorem 3.6])**.** *Suppose that $\mathcal{X}/\mathcal{S}$ contains a diagonal fibre, then ϕ_k is an isomorphism of $\mathbb{Q}_q(t_1, \ldots, t_s)$-vector spaces for all $k \in \mathbb{N}$.*

Proof. We already know that $\dim U_k = \dim W_k$ by Lemma 3.12. We need to show that $\det(\Delta_k) \neq 0$ (since Δ_k is the matrix representing ϕ_k). We do this by showing that $\det(\Delta_k)$ does not vanish on the diagonal fibre $\mathcal{X}_0$ of $\mathcal{X}/\mathcal{S}$, which shows that Δ_k cannot be identically zero.

Let $(j, g) \in C_k$. Then we have $g x_j^{d-1} \in R_k$ and since $\partial_j P(x_0, \ldots, x_n)|_{t=0} = \partial_j (a_0 x_0^d + \cdots + a_n x_n^d) = d a_j x_j^{d-1}$, the entry of $\det(\Delta_k)|_{t=0}$ at row $g x_j^{d-1}$ and column (j, g) is $d a_j \neq 0$. If there is another non-zero element in the row $g x_j^{d-1}$, then it is in column $(i, h) \in C_k$ for some i and $h \mid g x_j^{d-1}$ and $g x_j^{d-1}/h = x_i^{d-1}$ so $g x_j^{d-1} = h x_i^{d-1}$. This means that $x_j^{d-1} \mid h$ and $x_i^{d-1} \mid g$. If $i < j$ then the first gives a contradiction and if $j < i$ then the second gives a contradiction, by the definition of C_k. Hence, we get $i = j$ and this gives $g = h$. Hence, the only non-zero element in row $g x_j^{d-1}$ is in column (j, g). Hence, every column and row contains precisely one non-zero element. Therefore, $\det(\Delta_k)_{t=0} \neq 0$, which completes the proof. ∎

Using the previous theorem, we can describe an algorithm to reduce n-forms in cohomology to n-forms in the span of $\mathcal{B}$.

Let $Q \in \mathbb{Q}_q(t_1, \dots, t_s)[x_0, \dots, x_n]$ be homogeneous of degree $kd - (n+1)$ for some $k \in \mathbb{N}$. If we apply π to Q, we get an element of W_k. Theorem 3.14 yields $(Q_0, \dots, Q_n) = \phi_k^{-1}(\pi(Q)) \in U_k$. Hence, applying ϕ_k gives

$$\pi(Q_0\partial_0 P + \dots + Q_n\partial_n P) = \pi(Q).$$

This means that $Q = Q_0\partial_0 P + \dots + Q_n\partial_n P + \gamma_k$ with γ_k in the $\mathbb{Q}_q(t_1, \dots, t_s)$-span of B_k. Consider the element $Q\Omega/P^k$ of $\mathcal{H}^n_{\mathrm{dR}}(\mathfrak{U}_{\mathbb{Q}_q(t_1,\dots,t_s)})$. Using the previous computation and the relations of Proposition 3.9 we can write

$$\begin{aligned} \frac{Q\Omega}{P^k} &= \frac{(Q_0\partial_0 P + \dots + Q_n\partial_n P)\Omega}{P^k} + \frac{\gamma_k\Omega}{P^k} \\ &\equiv \frac{(\partial_0 Q_0 + \dots + \partial_n Q_n)\Omega}{(k-1)P^{k-1}} + \frac{\gamma_k\Omega}{P^k}, \end{aligned}$$

where $\equiv$ means equality in $\mathcal{H}^n_{\mathrm{dR}}(\mathfrak{U}_{\mathbb{Q}_q(t_1,\dots,t_s)})$. Suppose that $\partial_0 Q_0 + \dots + \partial_n Q_n \neq 0$. Note that $\deg(\partial_0 Q_0 + \dots + \partial_n Q_n) = (k-1)d - (n+1)$ since the Q_i that are non-zero must be homogeneous of degree $(k-1)d - n$ (and one of the $\partial_i Q_i$ is non-zero). Hence, we can repeat the reduction step for $\partial_0 Q_0 + \dots + \partial_n Q_n$. If we repeat this we can write

$$\frac{Q\Omega}{P^k} \equiv \frac{\gamma_k\Omega}{P^k} + \dots + \frac{\gamma_2\Omega}{P^2} + \frac{Q'\Omega}{P^1},$$

with $Q' \in V_k$. Note that $B_1 = F_1$ since $d - (n+1) < d - 1$. This means that Q' is in the $\mathbb{Q}_q(t_1, \dots, t_s)$-span of B_1 and therefore we can take $\gamma_1 = Q'$. Furthermore, if $k > n$, then $B_k = \emptyset$ and so $\gamma_k = 0$. Hence, we can write

$$\frac{Q\Omega}{P^k} \equiv \frac{\gamma_n\Omega}{P^n} + \dots + \frac{\gamma_1\Omega}{P^1},$$

with γ_i in the $\mathbb{Q}_q(t_1, \dots, t_s)$-span of B_i for $1 \leq i \leq n$.

Algorithm 3.15. The method above describes an algorithm to write an element $Q\Omega/P^k \in \mathcal{H}^n_{\mathrm{dR}}(\mathfrak{U}_{\mathbb{Q}_q(t_1,\dots,t_s)})$ as a $\mathbb{Q}_q(t_1, \dots, t_s)$-linear combination of elements of $\mathcal{B}$.

Theorem 3.16. *Suppose that $\mathcal{X}/\mathcal{S}$ contains a diagonal fibre. Then $\mathcal{B}$ is a basis of the $\mathbb{Q}_q(t_1, \dots, t_s)$-vector space $\mathcal{H}^n_{\mathrm{dR}}(\mathfrak{U}_{\mathbb{Q}_q(t_1,\dots,t_s)})$.*

Proof. Using Algorithm 3.15 we see that $\mathcal{B}$ spans $\mathcal{H}^n_{\mathrm{dR}}(\mathfrak{U}_{\mathbb{Q}_q(t_1,\dots,t_s)})$. Here we use that ϕ_k is invertible by Theorem 3.14. By [PT14, Proposition 3.7] and [PT14, Proposition 3.8], the cardinality of $\mathcal{B}$ is equal to the dimension of $\mathcal{H}^n_{\mathrm{dR}}(\mathfrak{U}_{\mathbb{Q}_q(t_1,\dots,t_s)})$ as a $\mathbb{Q}_q(t_1, \dots, t_s)$-vector space. Hence, $\mathcal{B}$ forms a basis of $\mathcal{H}^n_{\mathrm{dR}}(\mathfrak{U}_{\mathbb{Q}_q(t_1,\dots,t_s)})$. ■

Definition 3.17. We define the polynomial $R' \in \mathbb{Z}_q[t_1, \ldots, t_s]$ by

$$R' = \prod_{k=2}^{n} \det(\Delta_k).$$

Furthermore, we define $R = R' \cdot \det(\Delta_{n+1})$.

Corollary 3.18. *If $\mathcal{S}$ does not intersect the zero-locus of R' in $\mathbb{P}^1_{\mathbb{Z}_q}$, then $\mathcal{B}$ is a basis for $\mathcal{H}^n_{\mathrm{dR}}(\mathfrak{U}/\mathfrak{S})$.*

Proof. By [Gri69, (4.11)], $\mathcal{H}^n_{\mathrm{dR}}(\mathfrak{U}/\mathfrak{S})$ is given by all n-forms with poles of order at most n (higher poles can always be reduced in cohomology). By applying Algorithm 3.15, we see that $\mathcal{B}$ spans $\mathcal{H}^n_{\mathrm{dR}}(\mathfrak{U}/\mathfrak{S})$ since we may use the algorithm for $k = 2, \ldots, n$ as $\det(\Delta_k)$ does not vanish on $\mathfrak{S}$ by assumption. The fact that $\mathcal{B}$ is linearly independent over $H^0(\mathfrak{S}, \mathcal{O}_{\mathfrak{S}})$ follows from the fact that it is linearly independent over $\mathbb{Q}_q(t_1, \ldots, t_s)$. ■

3.4 Computing the Gauss-Manin connection

We want to find the matrix of the Gauss-Manin connection ∇ on $\mathcal{H}^n_{\mathrm{dR}}(\mathfrak{U}/\mathfrak{S})$. Since we have an explicit basis of $\mathcal{H}^n_{\mathrm{dR}}(\mathfrak{U}/\mathfrak{S})$, we can describe its action on the basis elements. Let $x^u\Omega/P^k \in \mathcal{B}$. Note that $\mathfrak{U}/\mathfrak{S}$ is affine, and therefore we can use [PT14, Remark 2.7]. This tells us that

$$\nabla\left(\frac{x^u\Omega}{P^k}\right) = d\left(\frac{x^u\Omega}{P^k}\right),$$

where d is the absolute differential on $\Omega^n_{\mathfrak{X}}$. Since Ω is an n-form, and there do not exist $(n+1)$-forms on $\mathfrak{X}$, all terms where we differentiate with respect to x_i vanish and we get

$$\nabla\left(\frac{x^u\Omega}{P^k}\right) = \sum_{k=1}^{s} \frac{d}{dt_k}\left(\frac{x^u\Omega}{P^k}\right) \otimes dt_k = \sum_{k=1}^{s} \frac{-kx^u(dP/dt_k)\Omega}{P^{k+1}} \otimes dt_k.$$

Hence, using Algorithm 3.15 we obtain

$$\nabla\left(\frac{x^u\Omega}{P^k}\right) \equiv \sum_{k=1}^{s}\left(\frac{\gamma_n^{(k)}}{P^n} + \cdots + \frac{\gamma_1^{(k)}}{P^1}\right)\Omega \otimes dt_k.$$

where $\gamma_i^{(k)}$ is an element of the $\mathbb{Q}_q(t_1, \ldots, t_s)$-span of B_i for all $1 \leq k \leq s$ and $1 \leq i \leq n$ and where $\equiv$ means equality in $\mathcal{H}^n_{\mathrm{dR}}(\mathfrak{U}/\mathfrak{S}) \otimes \Omega^1_{\mathfrak{S}}$. Hence, we have computed the matrices of ∇ on $\mathcal{H}^n_{\mathrm{dR}}(\mathfrak{U}/\mathfrak{S})$.

Remark 3.19. In the previous computation, we used Algorithm 3.15, which is valid if ϕ_k is invertible for all k that we apply it for. Note that $\deg_x(-kx^u(dP/dt_k)) = kd-(n+1)+d = (k+1)d-(n+1)$. Since $k \leq n$, we need to apply the algorithm for $k = 2, \ldots, n+1$. Hence, if we assume that $\mathcal{S}$ does not vanish on the zero-locus of $R = R' \cdot \det(\Delta_{n+1})$ in $\mathbb{P}^1_{\mathbb{Z}_q}$ (which means that $\det(\Delta_2), \ldots, \det(\Delta_{n+1})$ do not vanish), we may apply the algorithm.

Remark 3.20. There also is another criterion for applying the deformation method. We can write $M^{(k)} = H^{(k)}/r^{(k)}$ with $r^{(k)} \in \mathbb{Z}_q[t_1, \ldots, t_s]$, $H^{(k)} \in M_{b\times b}(\mathbb{Q}_q[t_1, \ldots, t_s])$ and $b = |\mathcal{B}|$. Let $\hat{\tau} \in \mathcal{S}(\mathbb{Z}_q)$. If $r^{(k)}(\hat{\tau}) \neq 0$, then specializing $M^{(k)}$ at $t = \hat{\tau}$ gives us the action of ∇ on the fibre $\mathcal{X}_{\hat{\tau}}$. Hence, if $r^{(k)}$ does not vanish at $t = \hat{\tau}$ for $k = 1, \ldots, s$, we may apply the deformation method. By [PT14, Proposition 3.13], we have that $r^{(k)} \mid R$ for all $k = 1, \ldots, s$. Hence, it is less restrictive to assume that $r^{(k)}$ does not vanish on $\mathcal{S}$ for $k = 1, \ldots, s$, than to assume that R does not vanish on $\mathcal{S}$.

In practice, we want to know if the deformation method will work before we compute $M^{(k)}$ for $k = 1, \ldots, s$. Therefore, we will work with the criterion in Remark 3.19 and we investigate the vanishing of R in Chapter 7.

Algorithm 3.21. The above computation, together with Remark 3.19 (or Remark 3.20) gives an algorithm to compute ∇ on $\mathcal{H}^n_{\mathrm{dR}}(\mathfrak{U}/\mathfrak{S})$ and so all matrices $M^{(k)}$.

Remark 3.22. Suppose that P has coefficients in $\mathbb{Z} \hookrightarrow \mathbb{Z}_q$. Then we can compute ∇ over $\mathbb{Q}$, so we get matrices $M^{(k)} \in M_{b\times b}(\mathbb{Q}(t_1, \ldots, t_s))$. In practice, this will be our approach to the deformation method. Namely, we either have to determine the $M^{(k)}$ over $\mathbb{Q}$, or over $\mathbb{Q}_q$ with some finite p-adic precision N_M. This p-adic precision depends on a constant K, which can be determined from $M^{(k)}$ over $\mathbb{Q}$ [PT14, Theorem 5.8]. Hence, we need to determine the $M^{(k)}$ over $\mathbb{Q}$ in both cases. Therefore, we first determine M over $\mathbb{Q}$, then determine K, and then consider M as an element of $M_{b\times b}(\mathbb{Q}_q(t_1, \ldots, t_s))$.

Chapter 4

The differential equation

In this chapter, we first derive differential equations involving the Gauss-Manin connection and the action of Frobenius on $\mathcal{H}^n_{\mathrm{dR}}(\mathfrak{U}/\mathfrak{S})$. We then show how to solve these differential equations so we can compute the action of Frobenius.

Recall the following definitions:

- By $F_p\colon \mathbb{F}_p \to \mathbb{F}_p$ or $F_p\colon \mathbb{F}_q \to \mathbb{F}_q$ we denote the p-Frobenius map.
- The map $\sigma\colon \mathbb{Q}_q \to \mathbb{Q}_q$ is a lift of F_p.
- The maps $F\colon \mathbb{Q}_q\langle t_1,\dots,t_s,1/r\rangle^\dagger \to \mathbb{Q}_q\langle t_1,\dots,t_s,1/r\rangle^\dagger$ and $F\colon \mathbb{Q}_q(t_1,\dots,t_s) \to \mathbb{Q}_q(t_1,\dots,t_s)$ are the natural maps equal to σ on $\mathbb{Q}_q$ and which satisfy $F(t_i) = t_i^p$ for $i = 1,\dots,s$.

4.1 Finding the differential equations

Write $M = H^0(\mathfrak{S}, \mathcal{H}^n_{\mathrm{dR}}(\mathfrak{U}/\mathfrak{S}))$ and let $\{m_1,\dots,m_b\}$ be a basis of M (where $b = |\mathcal{B}|$). Note that $dt_1,\dots,dt_s$ forms a basis of $\Omega^1_{\mathfrak{S}}$. Since $\nabla\colon M \to M \otimes \Omega^1_{\mathfrak{S}}$ is a linear map, we can describe its action by describing how it acts on the basis elements, i.e.

$$\nabla(m_j) = \sum_{k=1}^{s}\sum_{i=1}^{b} M^{(k)}_{ij} m_i \otimes dt_k, \tag{4.1}$$

with $M^{(k)} \in M_{b\times b}(\mathbb{Q}_q(t_1,\dots,t_s))$ for $k = 1,\dots,s$. We define $r \in \mathbb{Z}_q[t_1,\dots,t_s]$ to be a common denominator of all $M^{(k)}$ for $k = 1,\dots,s$.

We define $\mathcal{M} = H^0(]\overline{S}[, \mathcal{H}^n_{\mathrm{rig}}(U/S))$, which is a free $\mathbb{Q}_q\langle t_1,\dots,t_s,1/r\rangle^\dagger$-module of rank b with basis $\{m_1,\dots,m_b\}$ (where the m_i correspond to m_i in the basis of M). We also have the Gauss-Manin connection $\nabla\colon \mathcal{M} \to \mathcal{M} \otimes {\Omega^1_S}^\dagger$ on $\mathcal{M}$ (Proposition 3.7).

We have the isomorphism $\mathcal{F}\colon F^*\mathcal{M} \to \mathcal{M}$ induced by F . Note that if we view $\mathcal{F}$ as a map $\mathcal{M} \to \mathcal{M}$ then $\mathcal{F}$ is an F-semilinear map. This means that $\mathcal{F}$ is additive and $\mathcal{F}(\lambda x) = F(\lambda)\mathcal{F}(x)$ for all $x \in \mathcal{M}$ and $\lambda \in \mathbb{Q}_q$. We are interested in the action of $p^{-1}\mathcal{F}$. We can describe $p^{-1}\mathcal{F}\colon F^*\mathcal{M} \to \mathcal{M}$ by its action on the basis elements, so

$$p^{-1}\mathcal{F}(m_j) = \sum_{i=1}^{b} (A_p)_{ij} m_i. \tag{4.2}$$

We can compute the matrices $M^{(k)} \in M_{b\times b}(\mathbb{Q}_q(t_1, \dots, t_s))$ for $k = 1, \dots, s$ and we want to compute the matrix $A_p \in M_{b\times b}(\mathbb{Q}_q\langle t_1, \dots, t_s, 1/r\rangle^\dagger)$. For this, we derive differential equations involving $M^{(k)}$ and A_p.

Theorem 4.1. *For $k = 1, \dots, s$, the matrices $M^{(k)}$ and A_p satisfy the differential equation*

$$\frac{dA_p}{dt_k} + M^{(k)} A_p = p t_k^{p-1} A_p \big(M^{(k)}\big)^F.$$

Proof. By Proposition 3.7(i) we have that $\mathcal{H}^n_{\mathrm{rig}}(U/S)$ is an overconvergent F-isocrystal so the action of Frobenius commutes with the connection on $\mathcal{H}^n_{\mathrm{rig}}(U/S)$. The isomorphism $p^{-1}\mathcal{F}$ also commutes with the connection ∇ (where we use that the Tate twist of $\mathcal{M}$ is also an overconvergent F-isocrystal [Tui10, Definition 2.4.9]), so we have a commutative diagram

$$\begin{array}{ccc}
\mathcal{M} & \xrightarrow{\ \nabla\ } & \mathcal{M} \otimes {\Omega^1_S}^\dagger \\
\Big\downarrow{\scriptstyle p^{-1}\mathcal{F}} & & \Big\downarrow{\scriptstyle p^{-1}\mathcal{F}\otimes dF} \\
\mathcal{M} & \xrightarrow{\ \nabla\ } & \mathcal{M} \otimes {\Omega^1_S}^\dagger
\end{array}$$

Using (4.1) and (4.2) we can derive the differential equations. Let m_j be a basis element of $\mathcal{M}$. Using the fact that $p^{-1}\mathcal{F}\colon \mathcal{M} \to \mathcal{M}$ is F-semilinear we can write

$$\begin{aligned}
(p^{-1}\mathcal{F} \otimes dF)(\nabla(m_j)) &= (p^{-1}\mathcal{F} \otimes dF)\left(\sum_{k=1}^{s}\sum_{i=1}^{b} M_{ij}^{(k)} m_i \otimes dt_k\right) \\
&= \sum_{k=1}^{s}\sum_{i=1}^{b} F\Big(M_{ij}^{(k)}\Big) p^{-1}\mathcal{F}(m_i) \otimes dF(t_k) \\
&= \sum_{k=1}^{s} \Big(p t_k^{p-1} A_p \big(M^{(k)}\big)^F\Big)(m_j) \otimes dt_k.
\end{aligned} \tag{4.3}$$

Here we used that $dF(t_k) = d(t_k^p) = p t_k^{p-1} dt_k$. Using the linearity of ∇ we can write

$$\nabla(p^{-1}\mathcal{F}(m_j)) = \nabla\left(\sum_{i=1}^{b} (A_p)_{ij} m_i\right) = \sum_{i=1}^{b} \nabla((A_p)_{ij} m_i).$$

Since $(A_p)_{ij} \in \mathbb{Q}_q\langle t_1,\dots,t_s,1/r\rangle^\dagger$ is a local section of $\mathcal{O}_{\mathfrak{S}}$, we can apply the Leibniz rule for ∇ to obtain

$$\begin{aligned}
\nabla(p^{-1}\mathcal{F}(m_j)) &= \sum_{i=1}^{b}((A_p)_{ij}\nabla(m_i) + m_i \otimes d(A_p)_{ij}) \\
&= \sum_{i=1}^{b}(A_p)_{ij}\sum_{k=1}^{s}\sum_{l=1}^{b} M_{\ell i}^{(k)} m_\ell \otimes dt_k + \sum_{i=1}^{b}\sum_{k=1}^{s} m_i \otimes \frac{d(A_p)_{ij}}{dt_k}dt_k \\
&= \sum_{k=1}^{s}(M^{(k)}A_p)(m_j) + \sum_{k=1}^{s}\left(\frac{dA_p}{dt_k}\right)(m_j)\otimes dt_k \\
&= \sum_{k=1}^{s}\left(\frac{dA_p}{dt_k} + M^{(k)}A_p\right)(m_j)\otimes dt_k. \qquad (4.4)
\end{aligned}$$

If we compare (4.3) and (4.4) and use that $dt_1,\dots,dt_s$ are linearly independent, we obtain

$$\frac{dA_p}{dt_k} + M^{(k)}A_p = pt_k^{p-1}A_p\big(M^{(k)}\big)^F,$$

for all $k = 1,\dots,s$. ■

4.2 Solving the differential equations

In order to solve the differential equations from Theorem 4.1, we show that we can reduce to simpler differential equations.

Proposition 4.2. *Let $M \in M_{b\times b}(\mathbb{Q}_q(t_1,\dots,t_s))$ and let $C \in M_{b\times b}\Big(\mathbb{Q}_q\langle t_1,\dots,t_s,1/r\rangle^\dagger\Big)$ be a solution of the differential equation*

$$\left(\frac{d}{dt_k} + M\right)C = 0, \qquad C(0) = I. \qquad (4.5)$$

Then $A_p = CA_0\big(C^F\big)^{-1}$ is a solution of the differential equation

$$\left(\frac{d}{dt_k} + M\right)A_p = pt_k^{p-1}A_pM^F, \qquad A_p(0) = A_0. \qquad (4.6)$$

Proof. We first show two identities: for any invertible matrix C we have

$$\frac{dC^{-1}}{dt_k} = -C^{-1}\frac{dC}{dt_k}C^{-1} \qquad \text{and} \qquad \frac{dC^F}{dt_k} = pt_k^{p-1}\left(\frac{dC}{dt_k}\right)^F.$$

For the first identity, note that $CC^{-1} = I$ and $\frac{dI}{dt_k} = 0$. Applying the product rule gives

$$C\frac{dC^{-1}}{dt_k} + \frac{dC}{dt_k}C^{-1} = \frac{dI}{dt_k} = 0,$$

which gives the first identity after multiplying by C^{-1} on the left. For the second identity, write $t = (t_1, \dots, t_s)$ and note that the chain rule yields

$$\frac{dC^F(t)}{dt_k} = \frac{dC^\sigma(F(t))}{dt_k} = \sum_{i=1}^{s} \frac{dC^\sigma}{dt_i}(F(t)) \cdot \frac{d(t_i^p)}{dt_k},$$

where we interpret σ as a map $\mathbb{Q}_q\langle t_1, \dots, t_s, 1/r\rangle^\dagger \to \mathbb{Q}_q\langle t_1, \dots, t_s, 1/r\rangle^\dagger$ by acting as σ on $\mathbb{Q}_q$ and $\sigma(t_i) = t_i$ for all $i = 1, \dots, s$. Since $\frac{d(t_i^p)}{dt_k} = 0$ for $i \neq k$, we find that

$$\frac{dC^F(t)}{dt_k} = pt_k^{p-1}\frac{dC^\sigma}{dt_k}(F(t)) = pt_k^{p-1}\left(\frac{dC}{dt_k}\right)^\sigma(F(t)) = pt_k^{p-1}\left(\frac{dC}{dt_k}\right)^F.$$

Here we used that applying σ commutes with taking derivatives.

Let C be a solution of (4.5) and let $A_p = CA_0\big(C^{F_p}\big)^{-1}$. Using the product rule and the two identities we find

$$\begin{aligned}
\frac{dA_p}{dt_k} + MA_p &= \frac{d\Big(CA_0\big(C^{F_p}\big)^{-1}\Big)}{dt_k} + MCA_0\big(C^{F_p}\big) \\
&= \frac{dC}{dt_k}A_0\big(C^{F_p}\big)^{-1} + C\frac{dA_0}{dt_k}\big(C^{F_p}\big)^{-1} + CA_0\frac{d\big(C^{F_p}\big)^{-1}}{dt_k} + MCA_0\big(C^{F_p}\big) \\
&= \frac{dC}{dt_k}A_0\big(C^{F_p}\big)^{-1} - CA_0\big(C^{F_p}\big)^{-1}pt_k^{p-1}\left(\frac{dC}{dt_k}\right)^{F_p}\big(C^{F_p}\big)^{-1} + MCA_0\big(C^{F_p}\big).
\end{aligned}$$

Here we used that $\frac{dA_0}{dt_k} = 0$ since A_0 is a constant matrix. By assumption we have $MC = -\frac{dC}{dt_k}$ so this gives

$$\begin{aligned}
\frac{dA_p}{dt_k} + MA_p &= -CA_0\big(C^{F_p}\big)^{-1}pt_k^{p-1}\left(\frac{dC}{dt_k}\right)^{F_p}\big(C^{F_p}\big)^{-1} \\
&= -pt_k^{p-1}A_p\left(\frac{dC}{dt_k}C^{-1}\right)^{F_p} \\
&= pt_k^{p-1}A_pM^{F_p}.
\end{aligned}$$

Lastly, we have $A_p(0) = C(0)A_0\big(C^{F_p}\big)^{-1}(0) = A_0$ since $C(0) = I$. ■

We see that instead of solving (4.6) we can solve the easier differential equation (4.5). We now describe how we can solve the system of differential equations

$$\left(\frac{d}{dt_k} + M^{(k)}\right)C = 0 \text{ for } k = 1, \dots, s, \qquad C(0) = I.$$

Recall that $r \in \mathbb{Z}_q[t_1, \dots, t_s]$ is a common denominator for the matrices $M^{(k)}$ with $k = 1, \dots, s$. We can write $M^{(k)} = G^{(k)}/r$ with $G^{(k)} \in M_{b\times b}(\mathbb{Q}_q[t_1, \dots, t_s])$.

Write $G^{(k)} = \sum_{j\in I_k} G_j^{(k)} t^j$ and $r = \sum_{j\in J} r_j t^j$ where $I_k, J \subset \mathbb{Z}_{\geq 0}^s$ are finite sets. We need to solve

$$r\frac{dC}{dt_k} + G^{(k)}C = 0 \text{ for } k = 1, \ldots, s, \qquad C(0) = I. \tag{4.7}$$

Write C as a possibly infinite power series $C = \sum_{i\in\mathbb{Z}_{\geq 0}^s} C_i t^i$. From $C(0) = I$ we get $C_0 = I$. Let $i = (i_1, \ldots, i_s) \in \mathbb{Z}_{\geq 0}^s$. Applying the k-th equation of (4.7) and looking at the coefficient of t^i we find

$$\sum_{j\in J} r_j(i_k - j_k + 1)C_{i+e_k-j} + \sum_{j\in I_k} G_j^{(k)} C_{i-j} = 0,$$

where e_k is the k-th standard basis vector of $\mathbb{Z}^s$ and $C_j = 0$ for $j \in \mathbb{Z}^s \setminus \mathbb{Z}_{\geq 0}^s$. We have assumed that $P|_{t=0}$ defines a smooth hypersurface. Therefore, $R(0) \in \mathbb{Z}_q^\times$ and since $r \mid R$ we get $r(0) \in \mathbb{Z}_q^\times$. This implies that $r_0 = r(0) \neq 0$. We obtain a recursion

$$\begin{aligned} C_0 &= I; \\ C_{i+e_k} &= \frac{-1}{r_0(i_k+1)}\left(\sum_{\substack{j\in J\\ j\neq 0}} (i_k - j_k + 1) r_j C_{i+e_k-j} + \sum_{j\in I_k} G_j^{(k)} C_{i-j}\right), \end{aligned}$$

for $k = 1, \ldots, s$ and $i \in \mathbb{Z}_{\geq 0}^s$. Using this recursion we can compute C_i for all $i \in \mathbb{Z}_{\geq 0}^s$. Note that the answer should not depend on the ordering of $\mathbb{Z}_{\geq 0}^s$, as the elements of our matrices are rational functions. Therefore the order of differentiation does not matter.

We extend the p-adic valuation to matrices and power series.

Definition 4.3. If A is a matrix with entries A_{ij} that have a p-adic valuation, then $\mathrm{ord}_p(A) = \min_{i,j} \mathrm{ord}_p(A_{ij})$. If f is a power series with coefficients a_i that have a p-adic valuation, then $\mathrm{ord}_p(f) = \min_i \mathrm{ord}_p(a_i)$.

Suppose we want to find C to p-adic precision N_C and t-adic precision K. We can write down an approximate recursion

$$\begin{aligned} \tilde{C}_0 &= I; \\ \tilde{C}_{i+e_k} &= \frac{-1}{r_0(i_k+1)}\left(\sum_{\substack{j\in J\\ j\neq 0}} (i_k - j_k + 1) r_j \tilde{C}_{i+e_k-j} + \sum_{j\in I_k} G_j^{(k)} \tilde{C}_{i-j}\right) + E_{i+e_k}, \end{aligned} \tag{4.8}$$

where the E_j are error terms satisfying $\mathrm{ord}_p(E_j) \geq N_C'$ for all $j \in \{0, \ldots, K-1\}^s$.

Definition 4.4 ([PT14, Definition 3.18])**.** Define

$$\delta = \mathrm{ord}_p((n-1)!) + \sum_{i=1}^{n-1} \lfloor \log_p(i) \rfloor .$$

Definition 4.5. For a matrix A of the form $A = \sum_{i \in \mathbb{Z}_{\geq 0}^s} A_i t^i$ we write $\overline{A} = \sum_{i \in \{0,\ldots,K-1\}^s} A_i t^i$.

The following proposition gives a value of N_C' in terms of N_C and K such that $\mathrm{ord}_p(\overline{\tilde{C} - C}) \geq N_C$.

Proposition 4.6. *Let $K, N_C \in \mathbb{N}$, and let*

$$N_C' = N_C + (2(2\delta + (n-1)) + 1)\lceil \log_p(K-1) \rceil .$$

Then $\mathrm{ord}_p(\tilde{C}_i - C_i) \geq N_C$ *for all* $i \in \{0, \ldots, K-1\}^s$.

Before we give the proof, we first need the following two lemmas.

Lemma 4.7. *For all $i \geq 0$ we have*

$$\mathrm{ord}_p(C_i) \geq \big(\mathrm{ord}_p(A_p) + \mathrm{ord}_p\big(A_p^{-1}\big)\big)\lceil \log_p(i) \rceil .$$

Proof. The proof is a generalization of the proof of [Ked10, Lemma 18.3.2] to the case of multiple variables. For $i \geq 0$, write $I_i = \{0, \ldots, i\}^s$. Let $i \geq 0$. We have $C = A_p C^{F_p} A_0^{-1}$ by Proposition 4.2. This gives

$$\begin{aligned} \min_{j \in I_i} \mathrm{ord}_p(C_j) &= \min_{j \in I_i} \mathrm{ord}_p\Big(\big(A_p C^{F_p} A_0^{-1}\big)_j\Big) \\ &= \mathrm{ord}_p\big(A_0^{-1}\big) + \min_{j \in I_i} \mathrm{ord}_p\Big(\big(A_p C^{F_p}\big)_j\Big) \\ &\geq \mathrm{ord}_p\big(A_0^{-1}\big) + \min_{j \in I_i} \mathrm{ord}_p\Big(\big(A_p\big)_j\Big) + \min_{j \in I_i} \mathrm{ord}_p\Big(\big(C^{F_p}\big)_j\Big). \end{aligned}$$

Note that $\big(C^{F_p}\big)_j = C_{j/p}$ if $p \mid j$ and $\big(C^{F_p}\big)_j = 0$ otherwise. Furthermore, we have $\min_{j \in I_i} \mathrm{ord}_p\Big(\big(A_p\big)_j\Big) \geq \mathrm{ord}_p(A_p)$ and $\mathrm{ord}_p\big(A_0^{-1}\big) = \mathrm{ord}_p\Big(\big(A_p^{-1}\big)_0\Big) \geq \mathrm{ord}_p\big(A_p^{-1}\big)$. We obtain

$$\min_{j \in I_i} \mathrm{ord}_p(C_j) \geq \mathrm{ord}_p(A_p) + \mathrm{ord}_p\big(A_p^{-1}\big) + \min_{j \in I_{\lfloor i/p \rfloor}} \mathrm{ord}_p(C_j). \tag{4.9}$$

Applying inequality (4.9) $\lceil \log_p(i) \rceil$ times yields

$$\mathrm{ord}_p(C_i) \geq \min_{j \in I_i} \mathrm{ord}_p(C_j) \geq \big(\mathrm{ord}_p(A_p) + \mathrm{ord}_p\big(A_p^{-1}\big)\big)\lceil \log_p(i) \rceil + \mathrm{ord}_p(C_0).$$

Using $C_0 = I$, we get the desired statement. ∎

Lemma 4.8. *We have*

$$\mathrm{ord}_p(A_p) \geq -\delta \qquad \textit{and} \qquad \mathrm{ord}_p\big(A_p^{-1}\big) \geq -\delta - (n-1).$$

Proof. See [PT14, Theorem 3.17, Corollary 3.19]. The proofs are the same as we specialise A_p and A_p^{-1} to some $\tau \in S(\overline{\mathbb{F}_q})$, and so the proof does not depend on the dimension of S. ■

Proof of Proposition 4.6. We modify the proof of [PT14, Proposition 5.5] to the case of multiple variables. Write $E = \sum_{i \in \mathbb{Z}_{\geq 0}^s} E_i t^i$. Note that $\tilde{C}$ satisfies the differential equations

$$\frac{d\tilde{C}}{dt_k} + M^{(k)}\tilde{C} = E \text{ for } k = 1, \dots, s, \qquad \tilde{C}(0) = I.$$

Using the fact that $\frac{dC^{-1}}{dt_k} = -C^{-1}\frac{dC}{dt}C^{-1}$, we obtain

$$\begin{aligned}
\frac{d\Big(C^{-1}\tilde{C}\Big)}{dt_k} &= C^{-1}\frac{d\tilde{C}}{dt} + \frac{dC^{-1}}{dt}\tilde{C} \\
&= C^{-1}\bigg(E - M^{(k)} - \frac{dC}{dt_k}C^{-1}\tilde{C}\bigg) \\
&= C^{-1}\Big(E - M^{(k)} + M^{(k)}CC^{-1}\tilde{C}\Big) \\
&= C^{-1}E.
\end{aligned}$$

Hence, $C^{-1}\tilde{C}$ satisfies the differential equations

$$\frac{d(C^{-1}\tilde{C})}{dt_k} = C^{-1}E \text{ for } k = 1, \dots, s, \qquad (C^{-1}\tilde{C})(0) = I.$$

For $t = (t_0, \dots, t_s) \in \mathbb{Q}_q^s$, we define a path $\gamma_t \colon [0,1] \to \mathbb{Q}_q^s$ by $\gamma_t(\lambda) = \lambda t$. Note that we have

$$\frac{d(C^{-1}\tilde{C}\gamma_t)}{d\lambda}(\lambda) = \sum_{k=1}^{s} \frac{d(C^{-1}\tilde{C})}{dt_k}(\gamma_t(\lambda)) \cdot \frac{d(\lambda t_k)}{d\lambda} = \sum_{k=1}^{s}(C^{-1}E\gamma_t)(\lambda) \cdot t_k.$$

Hence, for fixed t we have

$$\tilde{C}(t) - C(t) = C(t)(C^{-1}\tilde{C} - I)(t) = C(t)\left(\int_0^1 \sum_{k=1}^{s}(C^{-1}E\gamma_t)(\lambda) \cdot t_k \, d\lambda\right). \tag{4.10}$$

We can write

$$\begin{aligned}
\int_0^1 \sum_{k=1}^{s}(C^{-1}E\gamma_t)(\lambda)t_k \, d\lambda &= \sum_{k=1}^{s}\int_0^1 (C^{-1}E)(\gamma_t(\lambda))t_k \, d\lambda \\
&= \sum_{k=1}^{s}\int_0^{t_k} (C^{-1}E)(\gamma_t(\mu/t_k))d\mu.
\end{aligned}$$

Here we used substitutions $\mu = t_k\lambda$ in the second step. Note that it could happen that $t_k = 0$, so we cannot divide by t_k. In this case, the k-th integral in the sum is 0, and we do not have to consider it. We will work out the case where $t_k \neq 0$ for all $k = 1, \ldots, s$.

Similarly to [PT14, Theorem 5.1], we apply Lemma 4.7 and Lemma 4.8 to conclude $\operatorname{ord}_p(C_i) \geq -(2\delta + (n-1))\lceil \log_p(i) \rceil$ for all $i \geq 0$. Applying this for $i = 1, \ldots, K-1$ gives us $\operatorname{ord}_p(\overline{C}), \operatorname{ord}_p(\overline{C^{-1}}) \geq -(2\delta + (n-1))\lceil \log_p(K-1) \rceil$. From this, we obtain

$$\operatorname{ord}_p\left(\overline{\int_0^{t_k} (C^{-1}E)(\gamma_t(\mu/t_k))d\mu} \right) \geq N_C + (2\delta + (n-1))\lceil \log_p(K-1) \rceil,$$

using $\operatorname{ord}_p(E_i) \geq N'_C$. From (4.10) we conclude that $\operatorname{ord}_p(\overline{\tilde{C} - C}) \geq N_C$. ■

Suppose that we want to compute A_p to p-adic precision N_{A_p} and t_i-adic precisions K. In the following theorem we give sufficient precisions for all other steps in the algorithm.

Theorem 4.9. *Let $N_{A_p}, K \in \mathbb{N}$. We define*

$$\begin{aligned}
N_{A_0} &= N_{A_p} \;+ (2\delta + (n-1))\big(\lceil \log_p(K-1) \rceil + \lceil \log_p(\lceil K/p \rceil - 1) \rceil\big); \\
N_C &= N_{A_p} \;+ (2\delta + (n-1))\lceil \log_p(\lceil K/p \rceil - 1) \rceil + \delta; \\
N_{C^{-1}} &= N_{A_p} \;+ (2\delta + (n-1))\lceil \log_p(K-1) \rceil + \delta; \\
N'_C &= N_C \;+ (2(2\delta + (n-1)) + 1)\lceil \log_p(K-1) \rceil; \\
N'_{C^{-1}} &= N_{C^{-1}} + (2(2\delta + (n-1)) + 1)\lceil \log_p(\lceil K/p \rceil - 1) \rceil.
\end{aligned}$$

We can compute A_p with p-adic precision N_{A_p} and t_i-adic precisions K by computing A_0, C and C^{-1} to p-adic precisions N_{A_0}, N_C and $N_{C^{-1}}$, and to t_i-adic precisions K, K and $\lceil K/p \rceil$, respectively. Furthermore, the computation of $\tilde{C}$ and $\tilde{C}^{-1}$ using (4.8) *has to be done with p-adic precisions N'_C and $N_{C^{-1}}$, respectively.*

Proof. It is clear that we have to compute C and A_0 with t_i-adic precisions K, and we have to compute $\sigma(C^{-1})$ with t_i-adic precisions K, so C^{-1} with t_i-adic precisions $\lceil K/p \rceil$.

By Lemma 4.8 we have $\operatorname{ord}_p(\overline{A_0}) \geq -\delta$ and by Lemma 4.7 we have $\operatorname{ord}_p(\overline{C}) \geq (2\delta + (n-1))\lceil \log_p(K-1) \rceil$ and $\operatorname{ord}_p(\overline{\sigma(C^{-1})}) \geq (2\delta + (n-1))\lceil \log_p(\lceil K/p \rceil - 1) \rceil$. We apply [PT14, Proposition 2.19] to $\overline{A_p} = \overline{CA_0\sigma(C^{-1})}$. We have

$$\begin{aligned}
\operatorname{ord}_p(\overline{C - \tilde{C}}) \geq N_C &= N_{A_p} + (2\delta + (n-1))\lceil \log_p(\lceil K/p \rceil - 1) \rceil + \delta \\
&= N_{A_p} - \big(-(2\delta + (n-1))\lceil \log_p(\lceil K/p \rceil - 1) \rceil\big) - (-\delta).
\end{aligned}$$

Similarly, the choices of N_{A_0} and $N_{C^{-1}}$ meet the conditions of [PT14, Proposition 2.19]. Hence, we get

$$\mathrm{ord}_p(\overline{A_p - \tilde{A}_p}) = \mathrm{ord}_p(\overline{CA_0\sigma C^{-1} - \tilde{C}\tilde{A}_0\sigma(\tilde{C}^{-1})}) \geq N_{A_p},$$

so N_C, N_{A_0} and $N_{C^{-1}}$ are sufficiently large. Proposition 4.6 gives us the correct precisions N'_C and $N'_{C^{-1}}$. ■

Remark 4.10. In [PT14], the integer N_M is defined, which is the sufficient p-adic precision of M (or $M^{(1)}, \ldots, M^{(s)}$ in our case). However, in order to determine K, we need to compute $M^{(1)}, \ldots, M^{(s)}$ over $\mathbb{Q}$. Therefore, we already know the exact value of the $M^{(k)}$ and there is no need to define N_M.

Algorithm 4.11. Using Algorithm 3.21 we can compute $M^{(k)}$ for $k = 1, \ldots, s$ and so r and $G^{(k)}$ for $k = 1, \ldots, s$. Using the recursion (4.8) and the p-adic and t_i-adic precisions from Theorem 4.9 we can compute A_p to p-adic precision N_{A_p}.

Chapter 5

The deformation method

In this chapter we will describe the deformation method, and discuss some remaining problems. First, we give a formula for the action of Frobenius on a diagonal hypersurface. Then we give the final steps of the deformation method after we have solved the differential equation.

5.1 Frobenius on diagonal hypersurfaces

Since computing the action of Frobenius on the diagonal fibre for a family in multiple parameters is the same as doing it in the 1-parameter case, we will cite results from [PT14, Section 4], without giving details or proofs.

Suppose that the diagonal fibre X_0 of X/S is given by

$$P_0 = a_0 x_0^d + a_1 x_1^d + \cdots + a_n x_n^d = 0$$

with $a_0, \ldots, a_n \in \mathbb{Z}_q^\times$. We define the following two integers:

Definition 5.1. For $l \in \mathbb{Q}$ and $r \in \mathbb{Z}_{\geq 0}$, we define the *rising factorial* $(l)_r$ by

$$(l)_r = \prod_{i=0}^{r-1} (l+i).$$

Definition 5.2. Let $u \in B$. We define $k(u) \in \mathbb{N}$ to be the integer such that

$$k(u)d - (n+1) = \sum_{i=0}^{n} u_i.$$

We can write down a direct formula for the action of $p^{-1}F_p$ on $\mathcal{H}^n_{\mathrm{rig}}(U_0)$.

Theorem 5.3 ([PT14, Theorem 4.3]). *Let $u \in \mathbb{N}_0^{n+1}$ and let $\omega_1 \in \mathcal{B}$ be the unique element corresponding to u. Let $v \in \mathbb{N}_0^{n+1}$ be the unique tuple satisfying $p(u_i+1) \equiv v_i + 1 \pmod{d}$ for all $0 \leq i \leq n$ and let $\omega_2 \in \mathcal{B}$ be the unique element corresponding to v. Then*

$$p^{-1}F_p(\omega_1) = (-1)^{k(v)}\frac{(k(v)-1)!}{(k(u)-1)!}p^{n-k(u)}\alpha_{u,v}^{-1} \cdot \omega_2,$$

with

$$\alpha_{u,v} = \prod_{i=0}^{n} a_i^{(p(u_i+1)-(v_i+1))/d}\left(\sum_{m,r}\binom{\frac{u_i+1}{d}}{r}\sum_{j=0}^{r}\frac{(pa_i^{p-1})^{r-j}}{(m-pj)!j!}\right),$$

where we sum the i-th factor of the product over all integers $m, r \geq 0$ that satisfy $p(u_i+1)-(v_i+1) = d(m-pr)$.

The only problem with the above theorem is that we need to evaluate an infinite sum. However, we only need finite p-adic precision and it turns out we therefore only need to compute a finite number of terms.

Proposition 5.4 ([PT14, Proposition 4.10]). *Define*

$$\mathcal{M} = \left\lceil \frac{p^2}{p-1}(N + \log_p(N+3)+4)\right\rceil - 1, \qquad \mathcal{R} = \lfloor \mathcal{M}/p \rfloor.$$

In order to compute $\alpha_{u,v}$ to p-adic precision N, it suffices to restrict the sums in Theorem 5.3 to pairs $m, r \geq 0$ such that $m \leq \mathcal{M}$ or equivalently $r \leq \mathcal{R}$.

Proposition 5.5 ([PT14, Corollary 4.8]). *In order to compute A_0 to p-adic precision N_{A_0}, it is sufficient to compute the $\alpha_{u,v}$ to p-adic precision*

$$N_{A_0} + (n-1) + \mathrm{ord}_p((n-1)!) + 2\delta.$$

We now can compute A_0 with p-adic precision N_{A_0}.

Algorithm 5.6. Using Theorem 5.3, Proposition 5.4 and Proposition 5.5 we can compute the action of Frobenius on the diagonal fibre A_0 with p-adic precision N_{A_0}.

5.2 Computing the zeta function

In this section, we evaluate the solution of the differential equations at a fibre, and use this to compute the zeta function of a fibre in our family.

Let $A_{p,\tau}$ denote the action of $p^{-1}F_p$ on $\mathcal{H}^n_{\mathrm{rig}}U_\tau$ for $\tau \in S(\mathbb{F}_q)$. We want to compute $A_{p,\tau}$ up to p-adic precision N_{A_p}. For this we want to find a power r^m of r such that $r^m A_p$ has no poles if we reduce all coefficients modulo $p^{N_{A_p}}$. In the case that $s = 1$, we can in practice take m to be about pN_{A_p} using [PT14, Remark 6.2], and we can take $K = m(\deg(r) + 1)$ by [PT14, Theorem 6.6]. By experiments with the author's Mathematica implementation of the deformation method [Put17a], we conjecture that we can take the same m and K in the higher dimensional case.

Conjecture 5.7. *Let $N_{A_p} \in \mathbb{N}$. There exists a $m \in \mathbb{N}$ such that $S = r^m \in \mathbb{Z}_q[t_1, \ldots, t_s]$ satisfies $SA_p \equiv \tilde{A}_p \pmod{p^{N_{A_p}}}$ with $\tilde{A}_p \in M_{b\times b}(\mathbb{Q}_q[t_1, \ldots, t_s])$ such that all elements of $\tilde{A}_p$ have degree $< K = m(\deg(r) + 1)$ in t_i for $i = 1, \ldots, s$.*

In practice, we can take m as in [PT14, Remark 6.2].

Remark 5.8. We would want to generalise [PT14, Theorem 6.4] (and [PT14, Theorem 6.1]) in order to show Conjecture 5.7. In the proof of [PT14, Theorem 6.4], orders of poles at points in a residue disk are considered. Here a residue disk of a point $z \in S(\overline{\mathbb{F}_q})$ is defined as all points on $\mathcal{S}(\overline{\mathbb{Q}_q})$ that reduce modulo p to z.

If we want to generalise this theorem, we probably need to consider orders along hypersurfaces in $\mathbb{P}^s$ or $(\mathbb{P}^1)^s$ instead of orders in points. It is also not clear what the right notion of a residue disk is when $s > 1$ and we want to consider hypersurfaces instead of points.

Let us suppose that we can find such S and K as in the previous conjecture. We can compute the matrix A_p to p-adic precision N_{A_p} and t_i-adic precisions K. Let $\tau \in S(\mathbb{F}_q)$ and let $\hat{\tau} \in \mathcal{S}(\mathbb{Z}_q)$ be a Teichmüller lift of τ computed to p-adic precision $N_{A_p} + \delta$. Then we compute

$$A_{p,\tau} = S(\hat{\tau})^{-1}(SA_p \pmod{t^K})|_{t=\hat{\tau}} \pmod{p^{N_{A_p}}}.$$

Here we write $SA_p \pmod{t^K}$ for SA_p modulo t_i^K for all $i = 1, \ldots, s$. We have $\mathrm{ord}_p(s(\hat{\tau})) = 0$ (by the definition of r), $\mathrm{ord}_p(\hat{\tau}) \geq 0$ and $\mathrm{ord}_p(A_p) \geq -\delta$ by Lemma 4.8. By [PT14, Proposition 2.19] and using that $\hat{\tau}$ has p-adic precision $N_{A_p} + \delta$, we find that $A_{p,\tau}$ is computed to p-adic precision N_{A_p}.

Algorithm 5.9. The discussion above gives us a method of computing $A_{p,\tau}$ to p-adic precision N_{A_p}.

Now that we have specialised our matrix to τ, our situation does not differ from the case where $s = 1$. Hence, we can use all theory in [PT14, Section 6.2].

We can compute the action of $p^{-1}F_p$ on $\mathcal{H}^n_{\mathrm{rig}}(U_\tau)$, and we want to know the action of $\mathfrak{q}^{-1}F_\mathfrak{q}$ on $\mathcal{H}^n_{\mathrm{rig}}(U_\tau)$. Recall that $a = \log_p \mathfrak{q}$. Since $A_{p,\tau}$ is σ-semilinear and $F_\mathfrak{q} = F_p^a$ we have

$$A^{(a)}_{p,\tau} = A_{p,\tau}A^{\sigma}_{p,\tau} \ldots A^{\sigma^{a-1}}_{p,\tau}. \tag{5.1}$$

is the matrix of the action of $\mathfrak{q}^{-1}F_{\mathfrak{q}}$ on $\mathcal{H}^n_{\mathrm{rig}}(U_\tau)$. Namely, write $A = A_{p,\tau}$ and let $x \in \mathcal{H}^n_{\mathrm{rig}}(U_\tau)$. Then

$$\begin{aligned} A^{(2)}(x) = A(A(x)) = A\left(\sum_{i=1}^{b}\sum_{j=1}^{b} A_{ij}x_j\mathbf{e}_i\right) &= \sum_{i=1}^{b}\sum_{j=1}^{b}\sum_{k=1}^{b}\sigma(A_{ij})A_{ki}x_j\mathbf{e}_k \\ &= \sum_{k=1}^{b}\sum_{j=1}^{b}(A\cdot A^{\sigma})_{kj}x_j\mathbf{e}_k = (A\cdot A^{\sigma})(x). \end{aligned}$$

By induction on a, we obtain formula (5.1).

We want to find

$$\chi(T) = \det\left(1 - TA^{(a)}_{p,\tau}\right),$$

from Theorem 2.4. Since $\chi(T) \in \mathbb{Z}[T]$, we can compute it exactly by only computing $A_{p,\tau}$ up to finite precision.

Theorem 5.10 ([PT14, Theorem 6.12])**.** *Write $\chi(T) = 1 + \sum_{i=1}^{b}\chi_i T^i$. In order to recover the polynomial $\chi(T) \in \mathbb{Z}[T]$, it suffices to compute χ_i to p-adic precision*

$$N_{\chi_i} = \left\lfloor \log_p(2(b/i)p^{\mathfrak{q}^{i(n-1)/2}})\right\rfloor + 1,$$

for $i = 1, \ldots, b$.

Theorem 5.11 ([PT14, Theorem 6.14])**.** *We can take*

$$N_{A_p} = \max_{1\le i\le b}\{N_{\chi_i}\} + \delta.$$

The proof of Theorem 5.10 tells us how we can compute the exact value of χ_i from the approximation $\tilde{\chi}_i$. First of all, we can write (essentially by the Weil conjectures)

$$\chi(T) = \prod_{i=1}^{b}(1 - \alpha_i T),$$

with $\alpha_i \in \mathbb{C}$ and $|\alpha_i| = \mathfrak{q}^{(n-1)/2}$ for $1 \le i \le b$. We denote $s_j = \sum_{i=1}^{b}\alpha_i^j$ for $1 \le j \le b$. Then we have

$$|s_j| \le b\mathfrak{q}^{j(n-1)/2}, \tag{5.2}$$

for $1 \le j \le b$. By the Newton-Girard identities we have

$$s_j + j\chi_j = -\sum_{i=1}^{j-1} s_{j-i}\chi_i, \tag{5.3}$$

for $1 \leq j \leq b$. It turns out that given $\chi_1, \ldots, \chi_{j-1} \in \mathbb{Z}$, and χ_j up to p-adic precision N_{χ_j}, the expressions (5.2) and (5.3) determine $\chi_j \in \mathbb{Z}$ uniquely. In chapter 6 we show how we can use this in practice. This completes the deformation method.

5.3 Summary of the deformation method

The deformation method can be summarised as follows:

1. We compute the action of ∇ on $\mathcal{H}^n_{\mathrm{dR}}(\mathfrak{U}/\mathfrak{S})$ using Algorithm 3.21, which is also its action on $\mathcal{H}^n_{\mathrm{rig}}(U/S)$.

2. We solve the differential equations from Theorem 4.1 up to sufficient p-adic and t_i-adic precisions using Algorithm 4.11.

3. We compute the action of Frobenius on the diagonal fibre at 0. This is done using Theorem 5.3.

4. We evaluate our solution at a Teichmüller lift $\hat{\tau} \in \mathcal{S}(\mathbb{Z}_{\mathfrak{q}})$ of τ. This gives the action of $p^{-1}F_p$ on $\mathcal{H}^n_{\mathrm{rig}}(U_\tau)$, the matrix of which we denote by $A_{p,\tau}$.

5. We compute $A^{(a)}_{p,\tau} = A_{p,\tau}A^{\sigma}_{p,\tau} \ldots A^{\sigma^{a-1}}_{p,\tau}$, which gives the action of $\mathfrak{q}^{-1}F_{\mathfrak{q}}$ on $\mathcal{H}^n_{\mathrm{rig}}(U_\tau)$.

6. We compute $\chi(T) = \det(1 - TA^{(a)}_{p,\tau})$ and

$$Z(X_\tau, T) = \frac{\chi(T)^{(-1)^n}}{(1-T)(1-\mathfrak{q}T)\cdots(1-\mathfrak{q}^{n-1}T)},$$

   using Theorem 5.10.

Chapter 6

Examples

In this chapter we show how to apply the deformation method using two examples. We first show the deformation method for a 1-dimensional family of curves, and then discuss it for a 2-dimensional family of curves.

6.1 A 1-dimensional family

Suppose we are interested in the zeta function of the smooth quartic $Q = x^3y + y^3z + z^3x = 0$ in $\mathbb{P}^2_{\mathbb{F}_5}$. Let $\mathcal{X}/\mathcal{S}$ be the family of smooth quartics in $\mathbb{P}^2_{\mathbb{Z}_5}$ given by the polynomial $(1-t)(x^4+y^4+z^4) + t(x^3y+y^3z+z^3x)$ in $\mathbb{Z}_5[t][x,y,z]$ (so we take a lift and embed $\{Q=0\}$ in a family containing a diagonal fibre). We are interested in the zeta function of the fibre at $t=1$.

In Remark 3.19 we noted that if R does not vanish on $\mathcal{S}$, then we can compute the Gauss-Manin connection using our reduction algorithm. In particular, this means that $\det(\Delta_3)$ does not vanish. However, we can show that $\det(\Delta_3)$ vanishes at $t=1$: We have $x^9 \in R_3$. Note that x^6 is the only monomial of degree 6 that divides x^9. Hence, the only non-zero entry of δ_3 in the row indexed by x^9 can be in the columns $(j, x^6) \in C_3$. Since $x^{d-1} = x^3 \mid x^6$, we have $(0, x^6) \in C_3$ but $(1, x^6), (2, x^6) \notin C_3$. Since $\partial_0 P = (1-t)4x^3 + t(3x^2y + z^3)$ does not contain the term x^3 for $t=1$, we see that the row x^9 contains only zeroes, so $\det(\Delta_3)|_{t=1} = 0$.

Remark 6.1. Suppose we have some smooth quartic given by $Q \in \mathbb{Z}_q[x,y,z]$, and $\mathcal{X}/\mathcal{S}$ is defined by $(1-t)(x^4+y^4+z^4) + tQ = 0$. Then we saw that $\det(\Delta_3)$ always vanishes for $t=1$ if $\partial_0 Q$ does not contain the term x^3, so if Q does not contain the term x^4. However, it turns out that we can use the deformation method for many of these curves, since r (the denominator of the matrix of ∇) does not vanish. Hence, R not vanishing on $\mathcal{S}$ is too strong of a criterion for applying the deformation method.

Also, note that this problem cannot be solved by choosing a different diagonal fibre (so considering the family $(1-t)(ax^4+by^4+cz^4)+tQ$ for some $a,b,c \in \mathbb{Z}_q^\times$).

In practice, we ideally do want R to be non-vanishing, because this criterion is easier to verify than the non-vanishing of r. In order to determine R we only have to determine Δ_2 and Δ_3, but in order to determine r, we have to compute the Gauss-Manin connection M for the generic fibre.

One way to solve this problem is to apply the action of PGL(3) on Q. For example, we can apply the transformation

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

This transformation maps $\gamma(x) = x+z$, $\gamma(y) = y$ and $\gamma(z) = x$. If we apply γ to Q, then R does not vanish for $P' = (1-t)(x^4+y^4+z^4)+t(\gamma Q)$. The curve given by $\gamma Q = 0$ is isomorphic to $X_1 : Q = 0$ over $\mathbb{F}_5$ because γ is invertible over $\mathbb{F}_5$. This means that they have the same zeta function. Hence, we could work with P' instead. However, as we pointed out earlier, the criterion of Remark 3.19 is a sufficient but not necessary condition for using the deformation method. It turns out that $\det(\Delta_2)$ does not vanish for all $t \in \mathbb{F}_5^\times$, and $\mathcal{B}$ forms a basis of $\mathcal{H}^n_{\mathrm{dR}}(\mathfrak{U}/\mathfrak{S})$. Furthermore, we can compute ∇ on the generic fibre, and its matrix has denominator $r \in \mathbb{Z}_q[t]$ with $\deg(r) = 24$. We have $r(1) \not\equiv 0 \pmod 5$, so we can also apply the deformation method to P.

First we compute the Gauss-Manin connection M over $\mathbb{Q}$ using Algorithm 3.21. It has denominator $r \in \mathbb{Z}[t]$ with $\deg(r) = 24$. We compute some of the necessary constants. We have $\delta = \mathrm{ord}_5(2!) = 0$, $N_{\chi_1} = N_{\chi_2} = N_{\chi_3} = N_{\chi_4} = 3$, $N_{\chi_5} = N_{\chi_6} = 4$ so $N_{A_p} = 4$ and by Conjecture 5.7 we can take $K = 550$. We get $N_{A_0} = 11$ and using Algorithm 5.6 we can compute that the matrix of Frobenius at $t = 0$ is given by

$$A_0 = \mathrm{diag}(\alpha, \alpha, \alpha, \beta, \beta, \beta).$$

Here α and β are computed up to 5-adic precision $A_0 = 11$ and they are given by $\alpha = 3\cdot 5 + 4\cdot 5^2 + 2\cdot 5^3 + 5^4 + O(5^5)$ and $\beta = 2 + 2\cdot 5 + 2\cdot 5^3 + 3\cdot 5^4 + O(5^5)$ up to 5-adic precision 5.

We solve the differential equation to 5-adic precision N_{A_p} and t-adic precision K. Using Conjecture 5.7 we can choose $S = r^{\lceil 1.1\cdot pN_{A_p}\rceil}$ and compute $S(1)^{-1}(sA_p \pmod{t^K})|_{t=1} \pmod{p^{N_{A_p}}}$ gives us that the action of Frobenius on $\mathcal{H}^n_{\mathrm{rig}}(U_1)$ is given by

$$A_{p,1} = \begin{pmatrix} 0 & 0 & 0 & 0 & \gamma & 0 \\ 0 & 0 & 0 & \gamma & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \gamma \\ \delta & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \delta & 0 & 0 & 0 \\ 0 & \delta & 0 & 0 & 0 & 0 \end{pmatrix},$$

with $\gamma = 2 + 3 \cdot 5^2 + O(5^4)$ and $\delta = 2 \cdot 5 + 2 \cdot 5^2 + 4 \cdot 5^3 + O(5^4)$. Note that we have computed $A_{p,1}$ only to 5-adic precision $N_{A_p} = 4$. We compute $\chi(T) = \det(1 - T\Phi_1) = 1 - \gamma^3\delta^3T^6 \pmod{5^4}$. Write

$$\chi(T) = 1 + \sum_{i=1}^{6} \chi_i T^i = \prod_{i=1}^{6}(1 - \alpha_i T),$$

with $\chi_i \in \mathbb{Z}$ and $\alpha_i \in \mathbb{C}$. We also define $s_j = \sum_{i=1}^{6} \alpha_i^j$ for $j = 1, \ldots, 6$. Using (5.2) and (5.3) we know that we have $\chi_i = s_i = 0$ for $i = 1, \ldots, 5$. For example, we have $s_1 = -\chi_1$, $\chi_1 \equiv 0 \pmod{5^{N_{\chi_1}}}$ and $|s_1| \leq 6 \cdot 5^{1/2} < 5^{N_{\chi_1}} = 5^3$ so $s_1 = 0$. Similarly we have $s_2 = s_3 = s_4 = s_5 = 0$. Using (5.3) we find

$$s_6 + 6\chi_6 = 0.$$

We have $\chi_6 = -\gamma^3\delta^3 = -(77 + \mathcal{O}(5^4))^3(560 + \mathcal{O}(5^4))^3 = 125 + \mathcal{O}(5^4)$. Now (5.2) gives us

$$|-6\chi_6| = |s_6| \leq 6 \cdot 5^3 = 750,$$

so $|\chi_6| \leq 125$. Using the fact that $\chi_6 \equiv 125 \pmod{5^4}$, this gives us that $\chi_6 = 125$. Hence, $\chi(T) = 1 + 125T^6$. By Theorem 2.4 we get

$$Z(X_1, T) = \frac{1 - 125T^6}{(1 - T)(1 - 5T)}.$$

6.2 A 2-dimensional family

Consider the 2-parameter family of smooth quartics $\mathcal{X}/\mathcal{S}$ over $\mathbb{Z}_5$ given by $P = x^4 + y^4 + z^4 + tx^2y^2 + sxyz^2 = 0$.

We first compute the matrices $M^{(1)}$ and $M^{(2)}$ over $\mathbb{Q}$ using Algorithm 3.21. They have common denominator $r = 16(-2 + 9s^2 - t)(2 + 9s^2 - t)(-2 + t)(2 + t)$. In particular, $\deg_{s,t}(r) = 6$. We have $\delta = 0$, $N_{\chi_1} = N_{\chi_2} = N_{\chi_3} = N_{\chi_4} = 3$, $N_{\chi_5} = N_{\chi_6} = 4$ and so $N_{A_p} = 4$ and by Conjecture 5.7 we get $K = 154$. This gives us $N_{A_0} = 11$ by Theorem 4.9. Since the diagonal fibre is $x^4 + y^4 + z^4 = 0$ (the same as in Example 1), the action of Frobenius at $t = 0$ is given by

$$A_0 = \mathrm{diag}(\alpha, \alpha, \alpha, \beta, \beta, \beta),$$

where α and β are the same as in the first example.

Again we can solve the differential equation to p-adic precision N_{A_p} and s-adic precision and t-adic precision K. We can take $S = r^{\lceil 1.1 \cdot pN_{A_p} \rceil}$ and compute $B = SA_p \pmod{t^k} \pmod{s^k}$. We will show that we can compute the zeta function for different fibres in our 2-dimensional family.

Suppose $\tau = (s_0, t_0) = (1, 0)$. We evaluate $A_{p,\tau}$ using Algorithm 5.9:

$$A_{p,\tau} = s(1,0)^{-1}B|_{(s,t)=(1,0)} \pmod{p^{N_{A_p}}} = \begin{pmatrix} 465 & 0 & 0 & 0 & 0 & 162 \\ 0 & 215 & 0 & 595 & 0 & 0 \\ 0 & 0 & 215 & 0 & 595 & 0 \\ 0 & 110 & 0 & 412 & 0 & 0 \\ 0 & 0 & 110 & 0 & 412 & 0 \\ 195 & 0 & 0 & 0 & 0 & 158 \end{pmatrix}.$$

We define $\chi_1, \ldots, \chi_6$ and $s_1, \ldots, s_6$ in the same way as in the first example. We evaluate $\det(1 - TA_{p,\tau})$ and find that

$$\chi_1 = 123 + O(5^3); \quad \chi_2 = 11 + O(5^3); \quad \chi_3 = 613 + O(5^3);$$
$$\chi_4 = 55 + O(5^3); \quad \chi_5 = 575 + O(5^4); \quad \chi_6 = 125 + O(5^4).$$

We will use (5.2) and (5.3) multiple times to compute the exact values of $\chi_1, \ldots, \chi_6$. We have $s_1 + \chi_1 = 0$. This gives

$$|-\chi_1| = |s_1| \leq 6\sqrt{5}.$$

Since $\chi_1 \equiv -2 \pmod{125}$ we get $\chi_1 = -2$ and $s_1 = 2$. We have $s_2 + 2\chi_2 = -s_1\chi_1 = 4$. Hence, we have

$$|-2\chi_1 + 4| = |s_2| \leq 30.$$

Since $\chi_2 \equiv 11 \pmod{125}$ this gives that $\chi_2 = 11$ and $s_2 = 4 - 22 = -18$. We have $s_3 + 3\chi_3 = -s_1\chi_2 - s_2\chi_1 = -58$. So then

$$|-3\chi_3 - 58| = |s_3| \leq 30\sqrt{5} < 68.$$

Since $\chi_3 \equiv -12 \pmod{125}$ we see that $\chi_3 = -12$ and $s_3 = -22$. The steps for χ_4, χ_5 and χ_6 are similar. We find that $\chi_4 = 55$, $\chi_5 = -50$ and $\chi_6 = 125$. Hence, we get

$$Z(X_{(1,0)}, T) = \frac{1 - 2T + 11T^2 - 12T^3 + 55T^4 - 50T^5 + 125T^6}{(1-T)(1-5T)},$$

by Theorem 2.4.

We can also do the exact same for other fibres in our family, as long as $r(s_0, t_0) \not\equiv 0 \pmod 5$. For example, we can compute that

$$Z(X_{(0,1)}, T) = \frac{1 - 6T + 15T^2 - 28T^3 + 75T^4 - 150T^5 + 125T^6}{(1-T)(1-5T)},$$

and

$$Z(X_{(1,-1)}, T) = \frac{1 - 6T + 27T^2 - 68T^3 + 135T^4 - 150T^5 + 125T^6}{(1-T)(1-5T)}.$$

Chapter 7

Application to curves of genus 3

In this chapter the main question we want to answer is on how to compute the zeta function of the universal curve of genus 3 over a finite field. Our approach will be to use the deformation method, and preferably to exploit the fact that we can compute the zeta function of multple fibres “at once”.

As is stated in Remark 3.19, in order to apply the deformation method to a fibre of a family, we need the polynomial R not to vanish at this fibre. Unfortunately, this condition turns out to be dependent on the choice of coordinates. In this chapter we investigate whether we can choose coordinates such that R does not vanish. Curves of genus 3 are either hyperelliptic or quartic curves. We are interested in the latter. Before looking at quartic curves, we first look at conics and cubic curves. However, we first need some theory about discriminants.

7.1 Discriminants

Let k be a field and let $f \in k[x]$ be a polynomial. A discriminant $\Delta(f)$ of f has the property that it is zero if and only if f has a double root in some field extension of k. Note that this is equivalent with saying that f has a common root to $\frac{\partial f}{\partial x}$.

One can also define the discriminant of a multivariate polynomial. For this we will look at the more general notion of a *resultant*.

Proposition 7.1 ([Kal]). *Let k be a field and let $x_1, \ldots, x_n$ denote formal variables. Fix degrees $d_1, \ldots, d_n \in \mathbb{N}$. Consider the homogeneous polynomials*

$$F_i = \sum_{\substack{\alpha \in \mathbb{N}^n \\ |\alpha| = d_i}} u_{i,\alpha} x^\alpha,$$

for $1 \leq i \leq n$, where the $u_{i,\alpha}$ are formal variables and x^α denotes $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$. Then there exists a polynomial $\mathrm{Res}(F_1, \ldots, F_n) \in \mathbb{Z}[\{u_{i,\alpha}\}]$, which is called the resultant of $F_1, \ldots, F_n$, such that

(i) *If we specialize all $u_{i,\alpha}$ to values in k, then the polynomials $F_1, \ldots, F_n$ have a non-trivial common zero in some field extension of k if and only if*

$$\mathrm{Res}(F_1, \ldots, F_n) = 0;$$

(ii) *The resultant $\mathrm{Res}(F_1, \ldots, F_n)$ is irreducible over k;*

(iii) *The resultant $\mathrm{Res}(F_1, \ldots, F_n)$ is a polynomial in the $u_{i,\alpha}$ of degree $d_1 \cdots d_n/d_i$ if we fix some $1 \leq i \leq n$;*

(iv) *We have $\mathrm{Res}(x_1^{d_1}, \ldots, x_n^{d_n}) = 1$.*

One construction of such a resultant is due to Macaulay [Mac].

Remark 7.2. We have defined the resultant of n homogeneous polynomials in n variables only when the coefficients of these polynomials are formal variables (in which case the resultant is a polynomial in the coefficients). However, we will say that the resultant of n polynomials $F_1, \ldots, F_n \in k[x_1, \ldots, x_n]$ of degrees $d_1, \ldots, d_n$ is the resultant of n general polynomials of degree $d_1, \ldots, d_n$, specialised to the values of the coefficients of $F_1, \ldots, F_n$. We will also denote it by $\mathrm{Res}(F_1, \ldots, F_n) \in k$.

Definition 7.3. Let $f \in k[x_1, \ldots, x_n]$ be a homogeneous polynomial. We define the *discriminant* of f to be

$$\mathrm{disc}(f) = \mathrm{Res}\left(\frac{\partial f}{\partial x_1}, \ldots, \frac{\partial f}{\partial x_n}\right).$$

We know from Proposition 7.1 that $\mathrm{disc}(f) = 0$ if and only if $\frac{\partial f}{\partial x_1}, \ldots, \frac{\partial f}{\partial x_n}$ have a non-trivial common zero in some field extension of k. By Euler's homogeneous function theorem, this implies that f also vanishes at this point. Hence, this point is a singular point of $V(f)$. We conclude that $\mathrm{disc}(f) = 0$ if and only if $V(f) \subset \mathbb{P}_k^{n-1}$ is singular.

Proposition 7.4. *Let $f \in k[x_1, \ldots, x_n]$ be a homogeneous polynomial and let $\gamma \in \mathrm{PGL}_n(k)$ be a projective transformation. Then we have*

$$\mathrm{disc}(f) = 0 \quad \Longleftrightarrow \quad \mathrm{disc}(\gamma f) = 0.$$

Here we write γf for $f(\gamma(x_1, \ldots, x_n))$.

Proof. We know that if $\operatorname{disc}(f) = 0$, then partial derivatives of f have a non-trivial common zero by Proposition 7.1. Let $y = (y_1, \ldots, y_n)$ be such a non-trivial common zero, then $\gamma^{-1}(y)$ is a non-trivial common zero of γf. Hence, $\operatorname{disc}(\gamma f) = 0$. We use the same reasoning where we substitute γf for f and γ^{-1} for γ, to get the other implication. ■

7.2 Conics in $\mathbb{P}^2$

We want to understand the deformation method for quartic curves. We want to understand when r (or R) vanishes on S. As this is hard for curves of degree 4, we first look at the case of degree 2 curves, in following section.

Let $q = p^a$ is a prime power with $p \neq 2$ and let Z be a smooth conic in $\mathbb{P}^2_{\mathbb{F}_q}$ given by

$$Q = a_1x^2 + a_2xy + a_3xz + a_4y^2 + a_5yz + a_6z^2 = 0,$$

with $a_1, \ldots, a_6 \in \mathbb{F}_q$. We embed Z in a family X/S with $S \subset \mathbb{P}^1_{\mathbb{F}_q}$ given by the zero set of the polynomial

$$P = (1-t)(x^2 + y^2 + z^2) + tQ.$$

Here we take $S \subset \mathbb{P}^1_{\mathbb{F}_q}$ to be all points with a smooth fibre (here we mean smooth over the algebraic closure of $\mathbb{F}_q$).

We want to inspect for which values of $a_1, \ldots, a_6$, the polynomial

$$R = \det(\Delta_2) \cdot \det(\Delta_3)$$

vanishes. We can compute

$$\Delta_2 = \begin{pmatrix} 2(1-t) + 2a_1t & a_2t & a_3t \\ a_2t & 2(1-t) + 2a_4t & a_5t \\ a_3t & a_5t & 2(1-t) + 2a_6t \end{pmatrix}.$$

Furthermore, we have

$$\det(\Delta_3) = -8(1 - t + a_1t)^3(4(a_1t + a_4t - t + 1)(1-t) + 4a_1a_4t^2 - a_2^2t^2)^2 \cdot \det(\Delta_2).$$

Hence, if $\det(\Delta_3)$ does not vanish, then R does not vanish. We know that $\det(\Delta_2) = 2^3 \cdot \operatorname{disc}(P)$ and so $\det(\Delta_2)$ vanishes for $t = 1$ if and only if X_1 is singular. Since $X_1 = Z$ is smooth, we know that $\det(\Delta_2)$ does not vanish at $t = 1$.

We want that $a_2^2 - 4a_1a_4 \neq 0$. Note that this is the discriminant of $Q(x, y, 0)$ so we want that $Q(x, y, 0)$ does not have a double root. This means that the line $z = 0$ is not tangent to Z. By the Plücker formulas, the dual curve Z^* is a smooth conic, and therefore it has $q + 1$ $\mathbb{F}_q$-points. Hence, there is always a line in $\mathbb{P}^2_{\mathbb{F}_q}$ not tangent to Z. By a projective transformation, we may move the line $z = 0$ to a line not tangent to Z. We replace Z by this isomorphic conic, which has the same zeta function.

Lastly, we need that $a_1 \neq 0$, which says that Z does not contain the point $(1 : 0 : 0)$. If this is the case then we are finished. Suppose that Z does contain the point $(1 : 0 : 0)$. Then it is one of the intersection points of Z with the line $z = 0$. We then apply a projective transformation which moves $(1 : 0 : 0)$ to a different point on the line $z = 0$, and leaves the other point of intersection fixed. Now Z does not contain $(1 : 0 : 0)$ and $z = 0$ still is not tangent to Z.

Hence, after applying a projective transformation to Z, we know that R does not vanish at $t = 1$ and so we may apply our algorithm to the fibre at $t = 1$.

7.3 Cubic curves in $\mathbb{P}^2$

As we now understand the case of degree 2 curve, we will investigate the case of degree 3 curves.

A general smooth cubic curve in $\mathbb{P}^2_{\mathbb{F}_q}$ (where $q = p^a$ and $p \neq 2, 3$) is given by

$$Q = a_1x^3+a_2x^2y+a_3x^2z+a_4xy^2+a_5xyz+a_6xz^2+a_7y^3+a_8y^2z+a_9yz^2+a_{10}z^3 = 0,$$

for some specialisations of $a_1, \ldots, a_{10}$. Again we can embed Z in a family X/S via

$$P = (1 - t)(x^3 + y^3 + z^3) + tQ = 0.$$

The polynomial $\det(\Delta_2)$ is irreducible, has 441 terms and has degree 9 in $a_1, \ldots, a_{10}$. It is clear that it is hard to give a geometric criterion for the vanishing of $\det(\Delta_2)$. However, we know that $\mathcal{M}_{1,1}$ has dimension 1 and therefore we can set a lot of the a_i to 0. We first look at a special family and then try to work out the general case using Weierstrass forms.

A special family

Suppose that $p \neq 2, 3$. We consider the family X/S of cubic curves over $\mathbb{F}_q$ given by

$$P = x^3 + y^3 + z^3 + t(xy^2 + yz^2) = 0.$$

Here $S \subset \mathbb{P}^1$ is the subset of all t_0 such that X_{t_0} is smooth. First of all, the discriminant of P is equal to

$$(27 + 4t^3)(729 + 324t^3 + 16t^6),$$

up to a constant factor. We can compute

$$R = 3^{16}(27 + 4t^3)^5(729 + 324t^3 + 16t^6).$$

Hence, we have that $\mathrm{rad}(R) \mid \mathrm{disc}(P)$ and so $R|_{t=t_0} = 0$ implies that $\mathrm{disc}(P)|_{t=t_0} = 0$, which implies that X_{t_0} is singular. Hence, R does not vanish on S.

We now want to show that X/S has dimension 1 in $\mathcal{M}_{1,1}$. The j-invarians of X_0 and X_1 over $\mathbb{Q}$ are $j(X_0) = 0$ and $j(X_1) = 110592/33139 = 2^{12} \cdot 3^3 \cdot 31^{-1} \cdot 1069^{-1}$. Hence, if $p \neq 2, 3, 31, 1069$ we know that X_0 and X_1 are not isomorphic over $\overline{\mathbb{F}_q}$ (if $p = 31$ or $p = 1069$, then X_1 is singular and if $p = 2$ or $p = 3$, then $X_1 \cong X_0$). Since X/S has degree 1 in t, we know that X/S must be a 1-dimensional subscheme of $\mathcal{M}_{1,1}$. Since $\mathcal{M}_{1,1}$ has dimension 1, we get that the image of X/S in $\mathcal{M}_{1,1}$ is open and dense.

If $p = 31$ or $p = 1069$, we consider X_0 and X_2 instead and get the same result since $j(X_2) = 2^{21} \cdot 3^3 \cdot 5^{-1} \cdot 11^{-1} \cdot 59^{-1} \cdot 79^{-1}$ does not contain factors 31 and 1069.

The general case

The previous method gave us the zeta function of all cubic curves, except for a finite number of isomorphism classes. However, we did not know which curves we were missing. We now give a method which works for all isomorphism classes, except for the cubic curves with j-invariant 1728.

We know that if $\mathrm{char}(\mathbb{F}_q) \neq 2, 3$, every cubic curve in $\mathbb{P}^2_{\mathbb{F}_q}$ with an $\mathbb{F}_q$-point is isomorphic to a curve in short Weierstrass form:

$$P = y^2z - x^3 - axz^2 - bz^3 = 0,$$

with $a, b \in \mathbb{F}_q$. We would like to apply the deformation method to this family, so first compute the action of Frobenius on some fibre, and then solve the differential equations. However, it turns out that $R = 0$ for all $a, b \in \mathbb{F}_q$, and so we cannot apply the deformation method. To see that $\det(\Delta_2) = 0$, note that $R_2 = F_2 \setminus \{xyz\}$, $(1, x) \in C_2$ and $x \cdot \partial_1 P = 2xyz \in \langle \{xyz\} \rangle_{\mathbb{Q}_q}$, so $(0, x, 0) \in \ker(\phi_2)$ (in fact, $\ker(\phi_2) = \langle (0, x, 0) \rangle_{\mathbb{Q}_q}$).

We will perfom an invertible projective transformation to $V(P)$. Consider the projective transformation

$$\gamma = \begin{pmatrix} 0 & 0 & -1 \\ \frac{1}{2} & -\frac{1}{2} & 0 \\ 3 & 3 & 0 \end{pmatrix},$$

so $\gamma\colon x \mapsto -z$, $\gamma\colon y \mapsto \frac{x}{2} - \frac{y}{2}$ and $\gamma\colon z \mapsto 3x + 3y$. We have $\det(\gamma) = -3 \neq 0$ since $\mathrm{char}(\mathbb{F}_q) \neq 3$. Then $V(P)$ is send to

$$\left(\frac{3}{4} - 27b\right)(x^3 + y^3) + \left(-\frac{3}{4} - 81b\right)(x^2y + xy^2) + 9az(x+y)^2 + z^3 = 0. \quad (7.1)$$

We will denote this equation by $\gamma P = 0$. We can compute for γP that

$$\det(\Delta_2) = -2 \cdot 3^{12} \cdot (16a^3 - b + 108b^2),$$

and

$$\det(\Delta_3) = 2^{-5} \cdot 3^{43} \cdot b^2(36b-1)^6(108b-1)(4a^3 + 27b^2).$$

We know that $\mathrm{disc}(P) = 4a^3 + 27b^2$, and $\mathrm{disc}(P) = 0$ if and only if $\mathrm{disc}(\gamma P) = 0$ by Proposition 7.4. Hence, if $4a^3 + 27b^2 = 0$ then the fibre is singular. Also, we have that $(a, b) = (0, -1/108)$ is a diagonal fibre of $\gamma P = 0$. Hence, we may apply the deformation method to all non-singular fibres for which $b \neq 0$, $b \neq 1/36$, $b \neq 1/108$ and $16a^3 - b + 108b^2 \neq 0$.

We will show that every element of the moduli space $\mathcal{M}_{1,1}$ has a representative in short Weierstrass form with $b \neq 0, 1/36, 1/108$ and $16a^3 - b + 108b^2 \neq 0$, except when its j-invariant is 1728. Suppose that $b \neq 0$. If $b = 1/36$ or $b = 1/108$ then applying the transformation

$$x' = 4x; \quad y' = 8y; \quad z' = z,$$

sends a to $a/16$ and b to $b/64$, so if $b = 1/36$ or $b = 1/108$, then this is not the case after applying the transformation. Since the transformation is invertible, the resulting elliptic curve is isomorphic to the original, and it is in short Weierstrass form. If $16a^3 - b + 108b^2 = 0$, we apply the more general transformation

$$x' = u^2x; \quad y' = u^3y; \quad z' = z, \quad (7.2)$$

with $u \in \mathbb{F}_q^\times$. This sends a to a/u^4 and b to b/u^6. We want that $\left(\frac{a}{u^4}\right)^3 - \frac{b}{u^6} + 108\left(\frac{b}{u^6}\right)^2 = \frac{a^3 - bu^6 + 108b^2}{u^{12}} \neq 0$ so that $a^3 - bu^6 + 108b^2 \neq 0$. Since $a^3 - b + 108b^2 = 0$ we have

$$a^3 - bu^6 + 108b^2 = a^3 - bu^6 + 108b^2 - (a^3 - b + 108b^2) = (1 - u^6)b.$$

We assumed that $b \neq 0$ so we need $u^6 \neq 1$. If $q = 7$ then $u^6 = 1$ for all $u \in \mathbb{F}_q^\times$. If $q \neq 7$ (and $2, 3 \nmid q$ by assumption) then $u^6 \neq 1$ has a solution in $\mathbb{F}_q^\times$, and we are finished. If $q = 7$ then one can check that $a^3 - b + 108b^2 = 0$ has no solutions in $(\mathbb{F}_q)^2$.

If $b = 0$, then the corresponding elliptic curve has j-invariant 1728, and the equation is invariant under transformations of the form (7.2). Hence, every element of $\mathcal{M}_{1,1}$ with j-invariant not equal to 1728 has a representant in short Weierstrass form with $b \neq 0$, $b \neq 1/36$, $b \neq 1/108$ and $16a^3 - b + 108b^2 \neq 0$. After bringing this representant in the form (7.1) we can apply the deformation method.

7.4 Quartic curves in $\mathbb{P}^2$

In this section, we want to investigate the vanishing of R for families of quartic curves. If we can understand R in this case, we may be able to apply the deformation method to the stratum of smooth quartic curves in $\mathcal{M}_3$.

A smooth quartic curve Z in $\mathbb{P}^2_{\mathbb{F}_q}$ (where $q = p^a$ and $p \neq 2, 3$) is given by

$$Q = a_1x^4 + a_2x^3y + a_3x^3z + a_4x^2y^2 + a_5x^2yz + a_6x^2z^2 + a_7xy^3 + a_8xy^2z + a_9xyz^2 + a_{10}xz^3 + a_{11}y^4 + a_{12}y^3z + a_{13}y^2z^2 + a_{14}yz^3 + a_{15}z^4,$$

for some specialisations of $a_1, \ldots, a_{15}$. We embed Z in a family X/S via

$$P = (1-t)(x^4 + y^4 + z^4) + tQ = 0.$$

Again, $\det(\Delta_2)$ and $\det(\Delta_3)$ are very large expressions which we cannot work with directly. We first do some smaller examples. We then discuss the possibilities for applying the deformation method to the universal quartic curve.

Special families

We first compute R for some special families. We do this to get a better understanding of R. What makes these families special is that they appear in the classification of quartic curves with a non-trivial automorphism group (a complete list can be find in [Ver83, Theorem 5.5]). We picked four families which have a dimension ≥ 2 in the moduli space $\mathcal{M}_3$, from the list in [Ver83, Theorem 5.5].

- Consider the family over $\mathbb{F}_q$ given by

  $$Q = x^4 + y^4 + z^4 + ax^2y^2 + bx^2z^2 + cy^2z^2 = 0.$$

  This family has dimension 3 in the moduli space $\mathcal{M}_3$ over $\mathbb{C}$ ([Ver83, Theorem 5.5]). Therefore, it has dimension 3 over $\mathbb{Q}$ and it also has dimension 3 over $\mathbb{F}_q$ for all but finitely many primes p (where $q = p^a$). We can compute

  $$R = 2^{102}(a-2)^9(a+2)^9(b-2)^4(b+2)^4(c-2)^3(c+2)^4(a^2+b^2+c^2-abc-4).$$

  It turns out that $\mathrm{rad}(R) \mid \mathrm{disc}(Q)$ and so R vanishes only on the singular locus of $Q = 0$. This is the ideal situation.

- Consider the family over $\mathbb{F}_q$ given by

$$Q = x^4 + y^4 + z^4 + ax^2y^2 + bxyz^2 = 0.$$

This family has dimension 2 in the moduli space $\mathcal{M}_3$ over $\mathbb{C}$ ([Ver83, Theorem 5.5]) and therefore over $\mathbb{F}_q$ for almost all p (where $q = p^a$). We have that

$$R = 2^{98}(a-2)^9(a+2)^9(4a-b^2-8)^2(4a-b^2+8)^2.$$

Again we have that $\operatorname{rad}(R) \mid \operatorname{disc}(Q)$ so R vanishes only on the singular locus of $Q = 0$.

- Consider the family over $\mathbb{F}_q$ given by

$$Q = z^3y + x(x-y)(x-ay)(x-by) = 0.$$

This family has dimension 2 in moduli space $\mathcal{M}_3$ over $\mathbb{C}$ ([Ver83, Theorem 5.5]) and therefore over $\mathbb{F}_q$ for almost all p (where $q = p^a$). In this case we have $R = 0$. This is because $\det(\Delta_2) = 0$. Let A_d denote the set of monomials in x, y and z of degree d. Recall the definitions of C_k, F_k and R_k (Definition 3.10 and Definition 3.11). We have

$$C_2 = A_2 \sqcup A_2 \sqcup A_2 \qquad \text{and} \qquad R_2 = F_2 \setminus \{x^2y^2z, x^2yz^2, xy^2z^2\}.$$

We have $x^2\frac{\partial Q}{\partial z} = 3x^2yz^2$ and $xy\frac{\partial Q}{\partial z} = 3xy^2z^2$. Since $3x^2yz^2$ and $3xy^2z^2$ lie in the $\mathbb{Q}_q$-span of $F_2 \setminus R_2$ we get that $(0,0,x^2)$ and $(0,0,xy)$ are non-trivial elements of $\ker(\phi_2)$. It turns out that $\ker(\phi_2) = \langle (0,0,x^2), (0,0,xy)\rangle$. However, it is not clear what the geometric interpretation is of the vanishing of R.

- Consider the family over $\mathbb{F}_q$ given by

$$Q = x^3y + y^3z + x^2y^2 + axyz^2 + bz^4.$$

This family has dimension 2 in the moduli space $\mathcal{M}_3$ over $\mathbb{C}$ ([Ver83, Theorem 5.5]) and therefore over $\mathbb{F}_q$ for almost all p (where $q = p^a$). We have

$$\det(\Delta_2) = 2^8 \cdot 3^3 \cdot b(a^2 + 12b)^3.$$

We have $b \mid \operatorname{disc}(Q)$ but $a^2 + 12b \nmid \operatorname{disc}(Q)$. If $b = \frac{-a^2}{12}$ then we have

$$\begin{aligned}\ker(\phi_2) = \Big\langle &\left(\frac{axz}{6} - \frac{y^2}{2}, \frac{ayz}{6} - \frac{x^2}{2}, xy\right),\\ &\left(-\frac{x^2}{3} - yz, \frac{az^2}{3} + \frac{xy}{3}, xz\right),\\ &\left(\frac{az^2}{3} + \frac{xy}{3}, -\frac{y^2}{3} - xz, xy\right)\Big\rangle.\end{aligned}$$

The images of these vectors under $(Q_0, Q_1, Q_2) \mapsto Q_0\partial_0 Q + Q_1\partial_1 Q + Q_2\partial_2 Q$ are $(\frac{8}{3}a - 3)x^2y^2z$, $(\frac{8}{3}a - 3)x^2yz^2$ and $(\frac{8}{3}a - 3)xy^2z^2$, respectively.

We see that often R contains factors of the discriminant, which is fine as the discriminant vanishes if and only if the fibre is singular. However, R can also contains factors which do depend on the choice of coordinates, and we cannot find a geometric interpretation for these terms.

One possible solution to this problem is making a change of coordinates. Since R does depend on the choice of coordinates, it is possible that we can transform our family such that R does not vanish on a particular fibre. We will work out such an example in the next section.

Another family

We now consider another family of quartic curves.

Consider the case where $a_3 = a_5 = a_6 = a_7 = a_8 = a_9 = a_{10} = a_{12} = a_{13} = a_{14} = 0$, so Q is given by

$$Q = a_1x^4 + 4a_2x^3y + 6a_4x^2y^2 + 4a_7xy^3 + a_{11}y^4 + a_{15}z^4.$$

We consider this example to show the computations involved with the vanishing of R. By itself, this family is not very interesting as it has dimension 1 in $\mathcal{M}_3$ (while the base space has dimension 5). We may assume that $a_{15} \neq 0$ as otherwise the fibre is singular. Hence, we may take $a_{15} = 1$ and we get $z^4 = f_4(x, y)$ where f_4 is homogeneous in x and y of degree 4. The polynomial f_4 is determined by 4 distinct points in $\mathbb{P}^1$ (if two of them are equal then the fibre is singular), and by a projective transformation we may take the first three points to be 0, 1 and ∞. Hence, our family has dimension at most 1. The family also has dimension at least 1, as the fibres $z^4 + x^4 + y^4 = 0$ and $z^4 + x^4 + xy^3 + y^4 = 0$ are not isomorphic. We can see this by comparing the number of flex points of the two fibres, which are 12 and 24 respectively.

We can compute

$$\begin{aligned}
\det(\Delta_2) &= f_1 \cdot f_2 \cdot f_3;\\
f_1 &= 2^{28} \cdot a_{15}^6 \cdot \operatorname{disc}(Q(x, y, 0));\\
f_2 &= a_{11} - a_2a_7;\\
f_3 &= a_{11}^2 + 9a_{11}a_2^2a_4 - 9a_{11}a_4^2 - 2a_{11}a_2a_7 - 8a_2^2a_7^2 + 9a_4a_7^2.
\end{aligned}$$

First note that $a_{15} \neq 0$ because otherwise Z would be singular. It turns out that $2^{40} \cdot a_{15}^9 \cdot \operatorname{disc}(Q(x,y,0)) = \operatorname{disc}(Q(x,y,z))$. Hence, $\operatorname{disc}(Q(x,y,0)) = 0$ if and only if $\operatorname{disc}(Q(x,y,z)) = 0$ if and only if Z is singular. Hence, $f_1 \neq 0$.

Suppose that $\det(\Delta_2) = 0$ so $f_2 = 0$ or $f_3 = 0$. We may apply an affine transformation of the form $\gamma_e \colon x \mapsto x + ey$ with $e \in \mathbb{F}_q$. The polynomial f_1 is invariant under γ_e. After applying the transformation, we obtain

$$\begin{aligned}
\det(\Delta_2) &= f_1 \cdot g_2 \cdot g_3;\\
g_2 &= (a_{11} - a_2a_7) + (-3a_2a_4 + 3a_7)e + (-3a_2^2 + 3a_4)e^2;\\
g_3 &= (a_{11}^2 + 9a_{11}a_2^2a_4 - 9a_{11}a_4^2 - 2a_{11}a_2a_7 - 8a_2^2a_7^2 + 9a_4a_7^2)\\
&\quad + (18a_{11}a_2^3 - 24a_{11}a_2a_4 + 6a_{11}a_7 - 12a_2^2a_4a_7 + 18a_4^2a_7 - 6a_2a_7^2)e\\
&\quad + (3a_{11}a2^2 - 3a_{11}a_4 - 18a_2^2a_4^2 + 27a_4^3 + 24a_2^3a_7 - 42a_2a_4a_7 + 9a_7^2)e^2.
\end{aligned}$$

Suppose that for every $e \in \mathbb{F}_q$ we have $\det(\Delta_2) = 0$ after applying γ_e. Then for all $e \in \mathbb{F}_q$, either $g_2 = 0$ or $g_3 = 0$. However, the equations $g_2 = 0$ and $g_3 = 0$ both have at most 2 solutions for e, unless one of them is identically zero. If g_2 and g_3 are both not identically 0, then since $|\mathbb{F}_q| > 4$ (we assumed $p \neq 2, 3$) there must be an $e \in \mathbb{F}_q$ such that $g_2(e) \neq 0$ and $g_3(e) \neq 0$. Hence, g_2 or g_3 is identically zero. We will show that this leads to a contradiction, by making case distinctions.

Suppose that g_2 is identically zero, so $a_{11} = a_2a_7$, $a_7 = a_2a_4$ and $a_4 = a_2^2$. Then it follows that $a_7 = a_2^3$ and $a_{11} = a_2^4$ so that $Q = (x + a_2y)^4 + a_{15}z^4$. In this case $(-a_2 : 1 : 0)$ is a singular point of Z, which gives a contradiction.

Suppose that g_3 is identically zero. Write $g_3 = f_3 + ge + he^2$. We make a case distinction for whether $3a_2^3 - 4a_2a_4 + a_7$ is zero.

(1) Suppose that $3a_2^3 - 4a_2a_4 + a_7 \neq 0$. Since $g = 0$ we have

$$a_{11} = \frac{2a_2^2a_4a_7 - 3a_4^2a_7 + a_2a_7^2}{3a_2^3 - 4a_2a_4 + a_7}. \tag{7.3}$$

Substituting this expression for a_{11} in f_3 gives

$$f_3 = \frac{9(2a_2^3 - 3a_2a_4 + a_7)(-3a_2^2a_4^2 + 4a_4^3 + 4a_2^3a_7 - 6a_2a_4a_7 + a_7^2)}{3a_2^3 - 4a_2a_4 + a_7} = 0.$$

We make two case distinctions.

(i) Suppose that $2a_2^3 - 3a_2a_4 + a_7 = 0$ so $a_7 = a_2(3a_4 - 2a_2^2)$. Substituting a_7 in (7.3) gives $a_{11} = (3a_4 - 2a_2^2)^2$. Hence, we can write

$$Q = (x^2 + 2a_2xy + (3a_4 - 2a_2^2)y^2)^2 + a_{15}z^4.$$

This means that $(-a_2 \pm \sqrt{3}\sqrt{a_2^2 - a_4} : 1 : 0)$ is a singular point of Z over $\overline{\mathbb{F}_q}$, so we get a contradiction.

(ii) Suppose that $-3a_2^2a_4^2 + 4a_4^3 + 4a_2^3a_7 - 6a_2a_4a_7 + a_7^2 = 0$. Using (7.3), we can compute that

$$\begin{aligned} &Q(a_7 - a_2a_4, 2(a_2^2 - a_4), 0) \\ =&\frac{(-3a2^2a4^2 + 4a4^3 + 4a2^3a7 - 6a2a4a7 + a7^2) \cdot F}{3a_2^3 - 4a_2a_4 + a_7}, \end{aligned}$$

with $F \in \mathbb{Z}[a_2, a_4, a_7]$. Hence, $Q(a_7 - a_2a_4, 2(a_2^2 - a_4), 0) = 0$. Similarly, $\frac{\partial Q}{\partial x}(a_7 - a_2a_4, 2(a_2^2 - a_4), 0)$ and $\frac{\partial Q}{\partial y}(a_7 - a_2a_4, 2(a_2^2 - a_4), 0)$ are divisible by $-3a_2^2a_4^2 + 4a_4^3 + 4a_2^3a_7 - 6a_2a_4a_7 + a_7^2$, and $\frac{\partial Q}{\partial z}(a_7 - a_2a_4, 2(a_2^2 - a_4), 0) = 0$. Hence, the point $(a_7 - a_2a_4 : 2(a_2^2 - a_4) : 0)$ of Z is a singular, if it is well-defined.

If it is not defined, then $a_4 = a_2^2$ and $a_7 = a_2a_4 = a_2^3$. However, then $3a_2^3 - 4a_2a_4 + a_7 = 0$ which gives a contradiction.

(2) Suppose that $3a_2^3 - 4a_2a_4 + a_7 = 0$. Then $a_7 = a_2(4a_4 - 3a_2^2)$ and substituting in g gives

$$g = -18a_2(3a_2^2 - 4a_4)(a_2^2 - a_4)^2 = 0.$$

We make three case distinctions.

(i) Suppose that $a_2 = 0$. This means that $a_7 = 0$. Evaluating f_3 and h gives

$$\begin{aligned} f_3 &= a_{11}(a_{11} - 9a_4^2) = 0; \\ h &= -3a_4(a_{11} - 9a_4^2) = 0. \end{aligned}$$

We can make two case distinctions.

(a) Suppose that $a_{11} - 9a_4^2 = 0$. Then because $a_2 = a_7 = 0$, we can write $Q = (x + 3a_4y)^2 + a_{15}z^4$ so $(-3a_4 : 1 : 0)$ is a singular point of Z.

(b) Suppose that $a_4 = a_{11} = 0$. Then $Q = x^4 + a_{15}z^4$ which has a singular point $(0 : 1 : 0)$.

(ii) Suppose that $3a_2^2 - 4a_4 = 0$. Then $3a_2^3 - 4a_2a_4 + a_7 = 0$ gives us that $a_7 = 0$. Evaluating f_3 and h gives

$$\begin{aligned} f_3 &= \frac{1}{16}a_{11}(16a_{11} + 27a_2^4) = 0; \\ h &= \frac{3}{64}a_2^2(16a_{11} + 27a_2^4) = 0. \end{aligned}$$

Again, we make two case distinctions.

(a) Suppose that $16a_{11} + 27a_2^4 = 0$. Then we can write $Q = \frac{1}{16}(2x - a_2y)(2x + 3a_2y)^3 + a_{15}z^4$ and so $(-3a_2 : 2 : 0)$ is a singular point of Z.

(b) Suppose that $a_2 = a_{11} = 0$. Then also $a_4 = 0$ since $3a_2^2 = 4a_4$ and so $Q = x^4 + a_{15}z^4$ which has a singular point $(0 : 1 : 0)$.

(iii) Suppose that $a_2^2 - a_4 = 0$. Then $3a_2^3 - 4a_2a_4 + a_7 = 0$ gives $a_7 = a_2^3$. Then $f_3 = (a_{11} - a_2^4)^2 = 0$ so $a_{11} = a_2^4$. We can write $Q = (x + a_2y)^4 + a_{15}z^4$ so $(-a_2 : 1 : 0)$ is a singular point of Z.

We conclude that, as g_2 or g_3 is identically zero, Z must be singular. This gives a contradiction. Hence, there exists an $e \in \mathbb{F}_q$ such that $\det(\Delta_2)$ does not vanish after applying the transformation $\gamma_e \mapsto x + ey$ to Z.

It turns out that $\det(\Delta_3) = -2^{-22} \cdot f_1^5 \cdot f_2 \cdot f_3$. Therefore, $\det(\Delta_2) \neq 0$ implies $\det(\Delta_3) \neq 0$ so we can get R to be non-zero by applying a projective transformation.

Normal form for the stratum of quartics

The moduli space of genus 3 curve $\mathcal{M}_3$ has dimension 6 over $\mathbb{C}$. The stratum of quartic curves is also 6-dimensional, so any normal form has dimension at least 6. We know that the a smooth quartic curve has at most 28 bitangents ([Ver83, Theorem 2.2]), i.e. lines that are tangent in two points on the curve. Together with the fact that the general smooth quartic curve has no hyperflexes ([Ver83, pg. 81]), we conclude that the general smooth quartic curve has 28 bitangents.

As there are 15 monomials in x, y and z of degree 4, the space of smooth quartic curves has dimension 14. We may demand that a general smooth quartic goes through the 4 points $(1 : 0 : 0)$, $(0 : 1 : 0)$, $(0 : 0 : 1)$ and $(1 : 1 : 1)$, by acting with PGL(3). This gives 4 restrictions on our curve. We may also demand that one bitangent goes through $(0 : 0 : 1)$ and $(1 : 1 : 1)$, and another goes through $(1 : 0 : 0)$ and $(0 : 1 : 0)$. Hence, we assume that $x = y$ and $z = 0$ are bitangents of the general smooth quartic curve. This also gives 4 restrictions, since we add one tangent condition in every one of the 4 points. This makes for a total of 8 restrictions. Since these are generic conditions, the space $\mathcal{B}$ of curves with these conditions has dimension $14 - 8 = 6$. Since the stratum of smooth quartic curves has dimension 6, this means that $\mathcal{B}$ is dense in the stratum of smooth quartic curves.

We can explicitely compute what the element of $\mathcal{B}$ are. A general smooth quartic curve C is given by

$$\begin{aligned} 0 = a_1x^4 + a_2x^3y + a_3x^3z + a_4x^2y^2 + a_5x^2yz + a_6x^2z^2 + a_7xy^3 + a_8xy^2z \\ + a_9xyz^2 + a_{10}xz^3 + a_{11}y^4 + a_{12}y^3z + a_{13}y^2z^2 + a_{14}yz^3 + a_{15}z^4, \end{aligned}$$

with $a_i \in \mathbb{F}_q$ for $1 \le i \le 15$. The conditions that $(1:0:0)$, $(0:1:0)$, $(0:0:1)$ and $(1:1:1)$ lie on C give that

$$a_1 = 0; \quad a_{11} = 0; \quad a_{15} = 0; \quad \sum_{i=1}^{15} a_i = 0.$$

The condition that $z = 0$ is a tangent of C in $(1:0:0)$ and $(0:1:0)$ yields

$$a_2 = 0; \quad a_7 = 0.$$

Lastly, the condition that $x = y$ is a tangent of C in $(0:0:1)$ and $(1:1:1)$ gives

$$a_4 = a_{10}; \quad 4a_1 + 3a_2 + 3a_3 + 2a_4 + 2a_5 + 2a_6 + a_7 + a_8 + a_9 + a_{10} = 0.$$

Eliminating variables using these conditions gives that $\mathcal{C}$ is the space of smooth quartic curves of the form

$$\begin{aligned} 0 = {} & a_3x^3z + a_4(x^2y^2 + xz^3) + a_5x^2yz + a_6x^2z^2 + a_8xy^2z + a_{12}y^3z + a_{13}y^2z^2 \\ & + (-3a_3 - 3a_4 - 2a_5 - 2a_6 - a_8)xyz^2 + (2a_3 + a_4 + a_5 + a_6 - a_{12} - a_{13})yz^3, \end{aligned}$$

with $a_3, a_4, a_5, a_6, a_8, a_{12}, a_{13} \in \mathbb{F}_q$. Unfortunately, any curve in this space does not contain a term x^4 in its equation. Hence, $R = 0$ for every fibre, so we cannot use the deformation method. We can possibly fix this by performing a change of coordinates.

Since we want $\det(\Delta_3)$ to be non-zero, we need the equations of our curves to contain a term x^4. This means that the curve may not go through the point $(1:0:0)$. By applying a change of coordinates, for example $z \mapsto x + z$, we may move the point $(1:0:0)$ to another point of $\mathbb{P}^2$ such that $(0:1:0)$, $(0:0:1)$ and $(1:1:1)$ do not get send to $(1:0:0)$. However, it turns out to be computationally very hard to compute $\det(\Delta_3)$ as Δ_3 is a 55×55-matrix with too many non-zero elements. Even if we could compute $\det(\Delta_3)$, then it would be a too large of an expression. We compute:

$$\det(\Delta_2) = 256a_3a_4a_{12}^2 f,$$

where f is an irreducible polynomial of degee 14 in a_3, a_4, a_5, a_6, a_8, a_{12} and a_{13}, consisting of 17593 terms.

Conclusion

In the previous sections we saw that the vanishing of R is not very well-understood for quartic curves. For families with more than 1 parameter, the polynomial R may contain too many terms to allow for practical use. For our original problem involving curves of genus 3 we would need to consider normal forms with at least 7 parameters. Using our current knowledge, it is seems undoable to control R for these normal forms.

In addition, the deformation method becomes very slow when the number of parameters grows. Namely, when solving the differential equation, one has to calculate K^s terms. As this expression is exponential in s, the algorithm becomes slow very quickly as s gets larger.

We conclude that in practice, it would be very hard to use the deformation method on normal forms for the stratum of quartic curves. However, if one can find normal forms on which R behaves well (or we know its behaviour well), and q is small, then it may be possible to apply the deformation method.

Bibliography

[AKR10] T. Abbott, K. Kedlaya, and D. Roe. Bounding Picard numbers of surfaces using p-adic cohomology. *Arithmetics, geometry, and coding theory*, 21:125–159, 2010.

[Bom78] E. Bombieri. On Exponential Sums in Finite Fields, II. *Inventiones mathematicae*, 47:29–39, 1978.

[Ger07] R. Gerkmann. Relative Rigid Cohomology and Deformation of Hypersurfaces. *International Mathematics Research Papers*, (1), 2007.

[GH78] P. Griffiths and J. Harris. *Principles of Algebraic Geometry*. 1978.

[Gri69] P. Griffiths. On the Periods of Certain Rational Integrals: I. *Annals of Mathematics, Second Series*, 90(3):460–495, November 1969.

[Ill96] L. Illusie. *Frobenius and Hodge Degeneration, Introduction to Hodge Theory*, volume 8. American Mathematical Society, Société Mathématique de France, 1996. no. 3, 96-145.

[Kal] K. Kalorkoti. On Macaulay's Form of the Resultant. `http://homepages.inf.ed.ac.uk/kk/Reports/Macaulay.pdf`.

[Ked01] K. Kedlaya. Counting Points on Hyperelliptic Curves using Monsky-Washnitzer Cohomology. *Journal of the Ramanujan Mathematical Society*, 16(4):323–338, 2001.

[Ked10] K. Kedlaya. *p-adic Differential Equations*. Cambridge University Press, 2010.

[KO68] N.M. Katz and T. Oda. On the differentiation of De Rham cohomology classes with respect to parameters. *Kyoto Journal of Mathematics*, 8(2):199–213, 1968.

[Lau04a] A.G.B. Lauder. Counting solutions to equations in many variables over finite fields. *Foundations of Computational Mathematics*, 4(3):221–267, 2004.

[Lau04b] A.G.B. Lauder. Deformation theory and the computation of zeta functions. *Proc. London Math. Soc.*, 3:565–602, 2004.

[Mac] F.S. Macaulay. Some Formulæ in Elimination. *Proc. London Math. Soc.*, S1-35(1).

[Pan14] S. Pancratz. An implementation of the deformation method for 1-parameter families of smooth projective hypersurfaces. `https://github.com/SPancratz/deformation`, 2014.

[PT14] S. Pancratz and J. Tuitman. Improvements to the deformation method for counting points on smooth projective hypersurfaces. 2014.

[Put17a] C. Putz. An implementation of the deformation method for families of hypersurfaces in 2-parameter families in Mathematica. `https://github.com/CPutz/Deformation-Mathematica-`, 2017.

[Put17b] C. Putz. An implementation of the deformation method for families of hypersurfaces in s-parameter families in Sage. `https://github.com/CPutz/Deformation-Sage-`, 2017.

[Tui10] J. Tuitman. *Counting points in families of nondegenerate curves.* PhD thesis, 2010. https://perswww.kuleuven.be/ u0055310/thesis.pdf.

[Ver83] A.M. Vermeulen. *Weierstrass points of weight two on curves of genus three.* PhD thesis, Universiteit van Amsterdam, 1983.