Computing the Zeta Function of Two Classes of Singular Curves

by

Robert Burko

A thesis submitted in conformity with the requirements
for the degree of Doctor of Philosophy
Graduate Department of Mathematics
University of Toronto

Contents

1 Introduction **1**

1.0.1 Point Counting and the Zeta Function 1

1.0.2 Weil Cohomology 3

1.1 Algorithmic Approaches 4

1.1.1 ℓ-Adic Methods 4

1.1.2 p-Adic Methods 5

1.1.3 Deformation and Fibration Methods 6

1.1.4 Approaches to Singular Varieties 7

1.2 This Thesis 8

1.3 Applications and Future Work 8

1.3.1 Cryptography 9

1.3.2 Support for Dimca's Conjecture 10

1.3.3 Potential Generalizations and Improvements 11

2 Cohomology Theories **13**

2.1 Preliminaries 13

2.1.1 p-Adic numbers and Witt vectors 13

2.1.2 Useful Properties of Étale Maps 14

2.2 Algebraic de Rham Cohomology 15

2.2.1 Kähler Differentials 15

2.2.2 de Rham Cohomology for Schemes 15

2.2.3 de Rham Cohomology with Logarithmic Singularities 16

2.3 p-Adic Cohomology Theories 20

2.3.1 Monsky-Washnitzer Cohomology 20

2.3.2 Rigid Cohomology and Crystalline Cohomology 21

2.3.3 Comparisons Theorems Between p-Adic and de Rham Cohomology 22

2.4 Exact Sequences 23

3 Superelliptic Curves **25**
3.1 Basic Properties . . . 25
3.1.1 The Genus . . . 26
3.1.2 The Zeta Function . . . 30
3.1.3 The Vector Space $\mathrm{H}^1_{\mathrm{MW}}(C'_K/K)^-$ . . . 31
3.1.4 Some Useful Order-preserving Functions . . . 34
3.2 Computing a Basis for Cohomology . . . 38
3.2.1 The Reduction Process . . . 39
3.2.2 Two Lemmas . . . 43
3.3 The Matrix of Frobenius . . . 51
3.4 Working Within a Crystalline Basis . . . 52
3.5 p-Adic Precision Analysis . . . 59

4 Nodal Curves in $\mathbb{P}^2$ **62**
4.1 Cohomology of the Affine Complement of a Hypersurface in $\mathbb{P}^n$ . . . 62
4.2 Basic Properties of Nodal Curves . . . 68
4.2.1 Computing a Lift . . . 68
4.2.2 The Zeta Function of a Nodal Curve . . . 74
4.3 A Crystalline Lattice of the Affine Complement . . . 77
4.4 The Matrix of Frobenius . . . 85
4.5 p-Adic Precision Analysis . . . 88

5 Algorithms and Complexity Estimates **90**
5.1 Superelliptic Curve . . . 90
5.1.1 Algorithm . . . 90
5.1.2 Complexity Analysis . . . 92
5.2 Nodal Plane Curve . . . 92
5.2.1 Algorithm . . . 92
5.2.2 Complexity Analysis . . . 93

6 Experiments **95**
6.1 Examples of Superelliptic Curves . . . 95
6.2 Examples of Nodal Plane Curves . . . 97

Chapter 1

Introduction

1.0.1 Point Counting and the Zeta Function

Let p be a prime, let $\mathbb{F}_p$ be a finite field with p elements, and let X be an algebraic variety defined over $\mathbb{F}_p$. For instance, X might be the simultaneous solution of the system of polynomial equations

$$\begin{cases} f_1(x_1, ..., x_n) \equiv 0 \mod p \\ f_2(x_1, ..., x_n) \equiv 0 \mod p \\ \vdots \\ f_m(x_1, ..., x_n) \equiv 0 \mod p \end{cases}$$

where the variables $x_1, ..., x_n$ lie in $\overline{\mathbb{F}}_p$. If we restrict the variables to take values in a finite extension of $\mathbb{F}_p$, then there are only a finite set of possibilities for each variable, and so this system has a finite number of solutions. An interesting question in number theory, dating back at least of far as Gauss' *Disquisitiones Arithmeticae* [1], asks for the number of solutions to such systems.

An almost equivalent but slightly more involved question is to calculate what is known as the zeta function of X. In general, we let X be an algebraic variety defined over a finite field with $q = p^a$ elements, and let $\#X(\mathbb{F}_{q^k})$ denote the number of solutions its defining equation has over the finite field $\mathbb{F}_{q^k}$, the so-called "$\mathbb{F}_{q^k}$-rational points" of X. One defines the *zeta function*, a formal power series associated to X, by

$$Z(X, T) = \exp\left(\sum_{k=1}^{\infty} \#X(\mathbb{F}_{q^k}) \frac{T^k}{k}\right) \in \mathbb{Q}[[T]].$$

The zeta function has many interesting properties. For instance, from Galois theory one can determine that the coefficients of its expanded power series are integers. More

astonishingly, in 1960 it was proven by Dwork that the zeta function is rational, that is, a quotient of two polynomials with integer coefficients [2]. Dwork's proof is analytic in nature − he shows that the zeta function is meromorphic, both as a function on the complex plane and on the completion of the algebraic closure of the field of rational p-adic numbers. The following theorem was conjectured by Weil in 1948 and proven by him in the case of curves, but not proven in full generality until 1974 by Deligne [3].

Theorem 1.0.1. *Let X by a smooth projective variety of dimension n defined over $\mathbb{F}_q$. Then*

1. *$Z(X,T)$ is a rational function of T, and can be written*

$$Z(X,T) = \frac{P_1(T)P_3(T)\cdots P_{2n-1}(T)}{P_0(T)P_1(T)\cdots P_{2n}(T)}$$

with $P_i(T) \in 1 + T\mathbb{Z}[T]$. Moreover, the polynomials $P_i(T)$ satisfy the following properties:

i) $P_0(T) = 1 - T$ and $P_{2n}(T) = 1 - q^nT$.

ii) The map $x \to q^n/x$ sends the roots of $P_i(T)$ to the roots of $P_{2n-i}(T)$, preserving multiplicities.

iii) If one writes

$$P_i(T) = \prod_j (1 - \alpha_{ij}T)$$

then α_{ij} is an algebraic integer with complex absolute value $q^{i/2}$.

2. *Let $E = \sum_i (-1)^i \deg(P_i)$. There is a functional equation*

$$Z\left(X, \frac{1}{q^nT}\right) = \pm q^{nE/2}t^E Z(X,T).$$

3. *If R is the integer ring of a number field, $\mathfrak{p}$ is a prime ideal in R lying over p, and X is the reduction modulo $\mathfrak{p}$ of a smooth scheme Y over R, then $\deg(P_i)$ is the i-th Betti number of $Y \times_R \mathbb{C}$ as a topological space*

Note that the condition for this theorem is that X is smooth and projective, whereas Dwork's proof of the rationality of the zeta function is valid for any variety defined over $\mathbb{F}_q$.

1.0.2 Weil Cohomology

The proof of Theorem (1.0.1) requires finding a "good" cohomology theory for X, known as a Weil cohomology. Such a theory is not unique for X and can be defined in the following way.

Definition 1.0.2. Let $k = \mathbb{F}_q$ be a finite field of characteristic p, and let K be a field of characteristic 0. A *Weil cohomology* is a contravariant functor from smooth proper varieties X over k to graded algebras $H^\bullet(X)$, where each $H^i(X)$ is a finite dimensional K-vector space satisfying the following properties:

1. If $n = \dim(X)$, then $H^i(X) = 0$ for $i \notin \{0, 1, ..., 2n\}$.

2. (Lefschetz fixed point theorem) There are "Frobenius maps" $F_i : H^i(X) \to H^i(X)$, $i \in \{0, ..., 2n\}$ such that

$$\#X(\mathbb{F}_{q^k}) = \sum_{i=0}^{2n} (-1)^i \mathrm{Tr}(F_i^k | H^i(X))$$

3. (Poincaré duality) The vector space $H^{2n}(X)$ is one-dimensional, and the map

$$H^i(X) \times H^{2n-i}(X)(n) \to H^{2n}(X)(n)$$

   is a perfect pairing for $i \in \{0, 1, ..., 2n\}$, and equivariant under the Frobenius maps (here $H^i(X)(n)$ denotes the vector space $H^i(X)$ with F_i replaced by $q^{-n}F_i$).

In actuality, Weil cohomologies possess more structure than this, including a cycle class map, Künneth formula, and a Lefschetz hyperplane theorem, as well as Frobenius compatibility maps, but for the purposes of this thesis we are interested in the above properties.

When X is not smooth or proper, it is possible that $X \to H^i(X)$ is still a well-defined functor, and satisfies some of the above properties. For instance, the rigid cohomology groups $\mathrm{H}^i_{\mathrm{rig}}(X)$ are defined for any $\mathbb{F}_q$-scheme X, and are finite dimensional and satisfy the Lefschetz fixed point theorem when X is smooth and affine. If X is a singular, projective hypersurface, then Poincaré duality still holds for $0 \leq i \leq \dim(X) - \dim(Y)$, where Y is the singular locus of X. From the following lemma, to ensure rationality of the zeta function it is sufficient to have finite dimensionality of each $H^i(X)$ combined with the Lefschetz fixed point formula.

Lemma 1.0.3. *Let V be a finite dimensional vector space over a field K, and let I denote the identity on V. Then for any endomorphism F of V, there is an identity in the power series ring $K[[T]]$*

$$\exp\left(\sum_{k=1}^{\infty} Tr(F|V)\frac{T^k}{k}\right) = \det(I - TF|V)^{-1}.$$

Proof. A simple calculation, see for instance [4, Appx C, Lemma 4.1]. □

It follows immediately that if one defines $P_i(T) = \det(I - TF_i|H^i(X))$, then the zeta function of X can be written

$$\begin{aligned} Z(X,T) &= \exp\left(\sum_{k=1}^{\infty}\sum_{i=0}^{2n}(-1)^i \mathrm{Tr}(F_i^k|H^i(X))\frac{T^k}{k}\right) \\ &= \prod_{i=0}^{2n}\left(\exp\left(\sum_{k=1}^{\infty}\mathrm{Tr}(F_i^k|H^i(X))\frac{T^k}{k}\right)\right)^{(-1)^i} \\ &= \prod_{i=0}^{2n} P_i(T)^{(-1)^{i+1}}. \end{aligned}$$

1.1 Algorithmic Approaches

For a variety X defined over $\mathbb{F}_q$, the problem of computing the sequence $\{\#X(\mathbb{F}_{q^k})\}_{k=1}^{\infty}$ is considered to be a hard problem. The brute force approach of inserting values into the defining equation of X has running time polynomial in q (i.e. exponential in $\log q$) whereas modern approaches (albeit usually only studied for curves and abelian varieties) are expected to run in a number of operations polynomial in $\log q$. Methods for computation of zeta functions of algebraic varieties are commonly placed under two main headings, ℓ-adic and p-adic approaches. In this section we will give short summaries of the various algorithms, as well as work that has been done to broaden their scope.

1.1.1 ℓ-Adic Methods

The first polynomial-time algorithm was developed by Schoof [5] and is used to count points on an elliptic curve $E/\mathbb{F}_q$ given by a Weierstrass model $y^2 = x^3 + Ax + B$. Schoof computes the trace of the Frobenius endomorphism $t = q - \#E(\mathbb{F}_q) + 1$ modulo various primes ℓ different from the characteristic of $\mathbb{F}_q$, by computing the action of Frobenius on the ℓ-torsion points of the curve. He then uses the Hasse-Weil bound $|t| \leq 2\sqrt{q}$ along with the Chinese remainder theorem to calculate t. This algorithm, after improvements

by Atkins, Elkies and Couveignes, has running time $O((\log q)^4)$.

In 1990, an attempt to extend Schoof's algorithm to more general curves and abelian varieties was made by Pila in [6] and improved by Adelman and Huang [7]. Using a similar approach to that of Pila, a randomized algorithm was developed by Huang and Ierardi [8] in which one computes the number of points on a plane curve of degree d which has only ordinary multiple points in time $(\log q)^{d^{O(1)}}$. Practical methods for these "Schoof-like" algorithms have not been implemented nearly as much as in the case of elliptic curves. However, some success in the case of genus 2 curves has been achieved [9].

1.1.2 p-Adic Methods

In 2000, Satoh demonstrated algorithmically [10] that for an elliptic curve $E/\mathbb{F}_q$, one could explicitly construct a unique elliptic curve $\tilde{E}/K$ called the "canonical lift", defined over a p-adic field K, and satisfying $\mathrm{End}(E) \cong \mathrm{End}(\tilde{E})$. One could thereby compute the trace of Frobenius on E directly as the trace of some corresponding endomorphism on $\tilde{E}$. If $q = p^a$ and if we consider p to be fixed, then the running time of his algorithm is $O(a^{2+\varepsilon})$. This is much faster than corresponding ℓ-adic methods. However a significant drawback is that Satoh's algorithm runs exponentially in $\log p$, so one is forced to use curves over fields with small characteristic.

One of the great advantages of Satoh's algorithm is that it does not depend on the group structure of the curve. Rather one only needs to consider its defining equation. Thus it spawned a number of new techniques for computing zeta functions of more general algebraic varieties. What was required was a sufficiently strong cohomology theory for varieties over $\mathbb{F}_q$ that could somehow be represented using the defining equation. One theory that is especially relevant to this thesis originates from the work of Monsky and Washnitzer [11].

In a paper [12] which appeared in 2001, Kedlaya showed in odd characteristic how to explicitly construct the Monsky-Washnitzer cohomology groups of a curve C', obtained by removing points from a hyperelliptic curve $C/\mathbb{F}_q$ given by a nonsingular affine planar equation $y^2 = f(x)$. One lifts the coordinate ring of C' to the integer ring of a p-adic field and "weakly completes" it with respect to the p-adic norm (obtaining what is called a "dagger algebra"). This defines an object with two fibres, one of which is isomorphic to

C' (the special fibre), and the other defined over a field of characteristic 0 and possessing analytic properties (the generic fibre). One can then compute the trace of Frobenius from the cohomology of the generic fibre.

Kedlaya's algorithm has running time $O(g^{4+\varepsilon}a^{3+\varepsilon})$ where g is the genus of the curve, assuming that the characteristic of the base field is fixed. There has been effort made to show Kedlaya's algorithm can be implemented effectively for curves over finite field of large characteristic (see [13] and [14]). The algorithm has also been adapted extensively to include more general settings. The algorithm was extended to the characteristic 2 case by Denef and Vercauteren [15], to superelliptic curves by Gaudry and Gürel [16], to $C_{a,b}$ curves by Denef and Vercauteren [17], and to smooth projective hypersurfaces by Abbott, Kedlaya, and Roe [18].

1.1.3 Deformation and Fibration Methods

Other p-adic methods for computing zeta functions derive from p-adic analysis, based on the cohomology and deformation theory of Dwork. In 2004, Lauder [19] [20] proposed a method for computing zeta functions of projective hypersurfaces of arbitrary dimension by embedding the surface into a family of hypersurfaces containing a diagonal element[1]. On such a family Dwork associates a differential equation whose solution parameterizes the matrices of Frobenius for each fibre. One first computes the Frobenius matrix for Dwork cohomology on the diagonal fibre (a relatively simple task), solves the differential equation locally around this specific value, and then evaluates the solution at the intended fibre. This method was later recast by Gerkmann in a framework more akin to algebraic geometry, first for the case of families of elliptic curves [21] and later for families of smooth projective hypersurfaces [22] using Berthelot's "rigid cohomology" [23] [24]. This is a Weil cohomology theory that has the added advantage of being defined for arbitrary varieties (not necessarily smooth or proper), as well as comparison maps to de Rham cohomology from which it inherits the differential equation of Dwork's theory.

Yet another novel algorithm for computing zeta functions was proposed by Lauder [25] using a "fibration method". That is, instead of deforming X to a diagonal hypersurface, one views some affine open subset of X as a parameterized family $X \to S$ of lower dimensional subvarieties. The relative cohomology of this family is a vector bundle on a

[1] A hypersurface of the form $X_0^d + \cdots + X_n^d = 0$.

subset of the projective line, and one computes the cohomology of X as the cokernel of a natural integrable connection associated to this vector bundle. The Frobenius matrix can then be recovered through the commutativity between the connection and Frobenius maps. This method was later improved and implemented by Lauder [26] for the special case of a fibration into hyperelliptic curves, and for more general cases by Walker [27].

1.1.4 Approaches to Singular Varieties

Though methods for computing zeta functions on smooth varieties have been studied extensively, it appears that only a small amount of consideration has been given to varieties which possess singularities, or even smooth varieties which admit known singular models in affine space. This could be for any number of possible reasons: the lack of comparison isomorphisms between de Rham and rigid cohomology, the fact that the Weil conjectures do not hold for singular varieties, that families which possess singular fibres can be completed in various ways, or that they are thought to be less secure from a cryptographic standpoint. In general, computing the zeta function of a singular variety is considered a much harder problem. However the author feels that this study is undervalued and has great potential for the future.

In 2008, Kloosterman [28] published an article reviewing the various p-adic methods for computing zeta functions of hypersurfaces, and identifying the obstructions to extending these methods to hypersurfaces which possess singularities. He proposed a modified algorithm which attempts to compute the discrepancy between de Rham and rigid cohomology by searching for and discarding eigenvalues of Frobenius which contradict a weak form of the Riemann Hypothesis[2]. It is clear that this tactic is difficult to implement in practice, and only can be prescribed for special situations.

The fundamental obstruction that Kloosterman points out is that for the affine complement of a singular projective hypersurface, the spectral sequence associated to the pole order filtration of the de Rham complex used to compute cohomology does not degenerate at E_2. He argues that

> "One could try to adjust [Kedlaya's] algorithm by taking an equisingular lift, and try to identify the extra relations needed to obtain [the cohomology group] as a quotient of [the de Rham complex]. Unfortunately, such a lift

[2]Contrary to its name, this is in fact a theorem for varieties over finite fields.

> might not exist and, except for a few cases, it is not clear at all which relations one needs to add."

This thesis in part resolves certain cases where these obstructions are manageable, giving some evidence that one could eventually apply these types of algorithms to more general environments.

1.2 This Thesis

Modern methods have yet to provide effective algorithms for counting points on singular varieties. This thesis is comprised of two algorithms for computing the zeta function in specific cases. Chapter 2 reviews the cohomology theories that will be necessary, along with relevant comparison isomorphisms and useful exact sequences. The material in this chapter is not new, however Theorem (2.2.16) is a reformulation of part of Deligne's work [29] and can be viewed as a generalization of a proposition of Abbott, Kedlaya, and Roe [18, Proposition 2.2.8]. Chapter 3 covers the technical details of a polynomial-time algorithm which computes the zeta function of a superelliptic curve over a finite field whose equation $y^r = f(x)$ in affine space has singularities[3] along $y = 0$. This is an extension of the work of Kedlaya [12] as well as Gaudry and Gürel [16]. The main contribution of this chapter is the modified cohomological reduction method when $\gcd(f, f') \neq 1$ and the p-adic precision-loss estimates from Lemmas (3.2.3) and (3.2.4). Chapter 4 then deals with the case of computing the zeta function of a nodal curve in $\mathbb{P}^2$. The notable parts of this chapter are the construction of a finite equisingular lift of a curve with a small number of singularities (Proposition (4.2.5)), as well as finding a suitable integer k to meet the requirements of Proposition (4.3.2). In Chapter 5, the algorithms are assembled in a step-by-step manner, and estimates on the complexity of each are given. The final chapter displays several results of a simple-minded implementation of both algorithms in MAGMA programming language.

1.3 Applications and Future Work

The algorithms described in this thesis are woven from deep theories that arise from algebraic geometry and p-adic analysis, however the applications admit themselves to various Diophantine questions. For instance, if one desired to know how often a cube could be written as the square of the product of two adjacent numbers modulo a prime, then one

[3] Equivalently, $f(x)$ is not squarefree.

could rephrase the question as a point-counting problem on the singular superelliptic curve $y^3 = x^2(x-1)^2$ over $\mathbb{F}_p$. These algorithms are likely to have industrial applications as well.

1.3.1 Cryptography

Since the late 1980's, mathematicians and computer scientists have prolifically used algebraic varieties in encryption systems, with the majority of attention given to elliptic curves. This was made possible since elliptic curves over finite fields possess a natural group structure[4]. The encryption is devised in the following way: Alice and Bob wish to share a secret key. They choose an elliptic curve with a point P. Alice chooses a secret number m, computes mP, and sends the result to Bob. Bob chooses a secret number n, computes nP, and sends the result to Alice. Now Alice computes $mnP = m(nP)$ and Bob computes $mnP = n(mP)$, and this is the secret that they share. We assume that no one can determine the secret key mnP without knowledge of either m or n, even if they have intercepted all the communication between Alice and Bob (this is known as the Diffie-Hellman problem).

Elliptic curve cryptography (ECC) was shown to give similar security as RSA[5] but used smaller key sizes. In order to ensure the security of an ECC system, one needs to know that the number of rational points on the curve is divisible by a large prime, and it was this necessity that provided the initial motivation for fast point-counting algorithms. The natural question was then to ask whether other geometric objects could be useful in cryptography. A curve C in general does not have a group structure on its points, however one can consider the associated "Jacobian" variety $J(C)$ which does have the structure of an abelian group. Systems based on the Jacobians of hyperelliptic curves, superelliptic curves, and $C_{a,b}$ curves have been proposed and are widely studied, and they seem to share many of the advantages of ECC. In the vast majority of such systems, the affine planar representation of the curve has no singularities, which not only limits the number of possible choices for curves, but perhaps also misses some potential benefits.

There have been several attempts to create a secure cryptographic system using singular curves. In 1995 Koyama [30] proposed an RSA-type cryptosystem based on a nodal cubic curve of the form $y^2 + axy \equiv x^3 \mod n$, where n is the product of two large primes

[4]One can add two points P and Q together to get a new point $P+Q$ on the curve, or multiply P by an integer n to get a new point nP.

[5]A standard cryptographic protocol relying on the difficult of factoring large integers.

p and q, and showed that the decryption speed could be performed twice as fast as RSA. One uses what is known as the "generalized Jacobian", which in Koyama's case is a group comprised of the points on the curve minus the point at the origin. Generalized Jacobians of singular curves are quasi-projective group schemes, with some quotient isomorphic to the Jacobian of the normalization of the curve. Algorithms for representing elements and performing group operations on generalized Jacobians have been developed (see for instance [31] or [32]), giving hope for the idea of using singular curves for cryptographic purposes, however it is argued that generalized Jacobians are no more secure than standard Jacobians, and in some cases less secure due the presence of pairing-based attacks [33].

An alternative application, suggested in 2004 by Kohel [34], uses the idea of embedding a finite field problem into the generalized Jacobian group of a singular hyperelliptic curve[6] over a smaller base field that is amenable to the index calculus attack, which is subexponential in time. An interesting project for the future would be to see if one could extend this method to the singular curves studied in this thesis. The algorithms for computing zeta functions would then be essential for selecting a curve with an appropriate generalized Jacobian.

1.3.2 Support for Dimca's Conjecture

In a beautiful paper by Griffiths [35], the following statement is shown:

> If a closed i-form ω in complex projective space with pole order k along a smooth hypersurface V has the property that for some differential φ, $\omega + d\varphi$ has pole order $k-1$ along V, then there exists a differential ψ with pole order $k-1$ along V such that $\omega + d\psi$ also has pole order $k-1$ along V.

The same is not true if V is singular, in fact it is always false. Dimca proves [36] that one can make the same assertion for singular curves with ψ having pole order $k+1+i$. In the case that V is a normal crossings divisor in $\mathbb{P}^n$, Proposition (4.3.2) proves that for k large enough[7] one can take ψ with pole order $k+1$, or pole order k when $i = n$. Dimca's general conjecture is that one will be able to find ψ with pole order at most $k+n$ along V (see Conjecture (4.1.3)). The reduction algorithm of Chapter 4 could easily be adapted to more general singular hypersurfaces to provide evidence for this conjecture.

[6] Kohel considers curves of the form $y^2 = xf(x)^2$ where f is a squarefree polynomial.

[7] For nodal curves we see this is $k \geq 2$, for higher dimensional normal crossings divisors one would suspect the requirement to be $k \geq n$.

1.3.3 Potential Generalizations and Improvements

The methods used in this thesis should be immediately extendable to more general situations. For instance, one would expect that an algorithm similar to the one described in Chapter 3 should be extendable to $C_{a,b}$ curves with singular planar equations. For the algorithm of Chapter 4, one could try to extend this method to the case of curves in $\mathbb{P}^2$ with ordinary multiple points. Since every irreducible projective plane curve is birational to a curve with ordinary multiple points [37, Appx. A], one would then have an algorithm to compute the zeta function of a wide selection of curves. With additional effort, an extension of the algorithm to certain classes of higher dimensional singular varieties should be feasible, particularly in the case of normal crossings divisors.

For projective curves with worse singularities the situation may be more dire since an equisingular lift may not exist, however it seems highly likely that the zeta function may be recovered through different types of lifting. For instance, Kloosterman [28] considers the case where one can define a sequence of lifts to smooth varieties X_k where the singular locus is lifted mod p^k. Lauder [38] considers projective singular hypersurfaces that can be embedded into a family of smooth varieties and lifted to the integer ring of a number field. He then performs a base change of the parameterizing curve $t \mapsto t^e$ so that the family extends to "semistable degeneration", and shows that one can uniquely define a computable "limiting Frobenius structure" for the new family. It seems, at least experimentally, that Frobenius action on the cohomology of the semistable fibre can be computed from the limiting Frobenius structure. Unfortunately it is unclear for now what the relationship is to the zeta function of the original hypersurface. However, the theory behind limiting Frobenius structures suggests another possible application. If one could reverse the process, and use the Frobenius action on the degenerate fibre to compute the limiting Frobenius structure, there would immediately exist a deformation algorithm to compute the zeta function of a smooth variety from a singular one. This has the potential of leading to faster algorithms, since one expects at least heuristically that the cohomology of the singular fibre will have lower dimension.

Lastly, it should be mentioned that the author feels that the algorithm in Chapter 4 is not yet optimal. In particular, as opposed to the explicit reduction method of Chapter 3, the algorithm of Chapter 4 requires finding solutions to seemingly random systems of linear equations in a vector space of dimension roughly d^2, where d is the degree of the curve. This is the limiting step of that algorithm (see Step 4 of the complexity analysis) and might be possible to avoid using local data at the singular points of the curve in

conjunction with the Poincaré residue map (see Theorem (2.2.16)).

Chapter 2

Cohomology Theories

In this section we give an overview of the cohomology theories that will be used in this thesis, relevant theorems, as well as the comparison maps between them.

2.1 Preliminaries

2.1.1 p-Adic numbers and Witt vectors

Let p be a prime, a a positive integer, put $q = p^a$, and let k be the finite field with q elements.

Proposition 2.1.1. *There is a unique local domain $W(k)$ having characteristic 0, maximal ideal (p), complete with respect to its p-adic topology, and such that $W(k)/pW(k) \cong k$.*

Proof. See [39, Section 8.10]. □

Definition 2.1.2. The ring $W(k)$, which we will henceforth denote by $\mathscr{V}$, is called the *ring of Witt vectors of k.*

One can construct $\mathscr{V}$ explicitly: Let $\overline{\theta} \in k$ be a primitive element with minimal polynomial $\overline{P}(x)$. Let $P(x) \in \mathbb{Z}[x]$ be the monic polynomial with coefficients in $\{0, 1, ..., p\}$ such that its reduction modulo p is $\overline{P}$. Then $P(x)$ is irreducible, by irreducibility of $\overline{P}$. Fix an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$, and let $\theta \in \overline{\mathbb{Q}}$ be an algebraic integer with minimal polynomial $P(x)$. Then the ring $\mathbb{Z}_p[\theta]$ is then a local domain, complete with respect to its maximal ideal (p), and with residue field

$$\frac{\mathbb{Z}_p[\theta]}{p\mathbb{Z}_p[\theta]} \cong \mathbb{F}_p[\overline{\theta}] \cong k.$$

Therefore $\mathbb{Z}_p[\theta] = \mathscr{V}$.

Definition 2.1.3. Let $\mathbb{Z}_{(p)}$ denote the subring of $\mathbb{Q}$ consisting of elements whose denominators are not divisible by p. Then we will call $\mathbb{Z}_{(p)}[\theta] \subset \mathscr{V}$ the *ring of Witt vectors of finite length*, and denote it $\mathscr{V}_{\text{fin}}$.

Definition 2.1.4. Let K denote the quotient field of $\mathscr{V}$. The *p-adic valuation on* K, denoted $\text{ord}_p : K \to \mathbb{Z}$, is the function which sends $b \in K$ to $\max\{i \in \mathbb{Z} : b \in p^i\mathscr{V}\}$. Define the *p-adic absolute value*, denoted $|\cdot|_p$, to be the absolute value on K given by $|b|_p = p^{-\text{ord}_p(b)}$.

Remark 2.1.5. In the the case that $a = 1$, one has $\mathscr{V} = \mathbb{Z}_p$ and $K = \mathbb{Q}_p$. For $a > 1$, K is the unique unramified extension of $\mathbb{Q}_p$ of degree a.

Definition 2.1.6. The p-power Frobenius on k, which sends x to x^p, induces an endomorphism on $\mathscr{V}$ which extends to an automorphism on K. Either of these maps will be called the *p-power Frobenius map*, denoted by σ. If V is a K-vector space, and ϕ is an additive map on V, we will say that ϕ is *σ-linear* if $\phi(cv) = \sigma(c)\phi(v)$ for all $c \in K, v \in V$.

Remark 2.1.7. Note that σ^a is the identity on K, so if ϕ is a σ-linear map on a K-vector space V, then ϕ^a is linear. If V is finite dimensional, and M is the matrix of ϕ with respect to some basis $\mathcal{B}$, then the matrix for ϕ^a is $MM^\sigma \cdots M^{\sigma^{a-1}}$, where M^{σ^i} is the matrix with entries equal to the entries of M acted upon by σ^i.

2.1.2 Useful Properties of Étale Maps

We will use this section to recall a few results about étale morphisms. These will later allow us to collect information near singularities of particular curves by performing an étale base change.

Proposition 2.1.8. *Suppose S is a locally Noetherian scheme, and $f : X \to S$ be an étale morphism of schemes over an algebraically closed field. Fix a point $x \in X$. Then the map between formal completions of the local rings $\widehat{\mathcal{O}}_{S,f(x)} \to \widehat{\mathcal{O}}_{X,x}$ is an isomorphism.*

Proof. See [40, Proposition 3.26]. □

Definition 2.1.9. Let $\mathcal{I}$ be coherent sheaf of ideals on a locally Noetherian scheme X, defining a closed subscheme Y. The X-scheme $\text{Proj}(\oplus_{n\geq 0}\mathcal{I}^n) \to X$ is called the blowing-up of X along Y, and is denoted $\widetilde{X}_Y$.

Proposition 2.1.10. *Let X and Z be locally Noetherian schemes, and let Y be a closed subscheme of X. Let $g : Z \to X$ be a flat morphism of schemes. Then there is a canonical isomorphism*

$$\widetilde{Z}_{g^{-1}(Y)} \xrightarrow{\sim} \widetilde{X}_Y \times_X Z$$

Proof. See [40, Proposition 1.12 (c)]. □

2.2 Algebraic de Rham Cohomology

Algebraic de Rham Cohomology, introduced by Grothendieck, is the algebraic analogue of de Rham theory on smooth manifolds. Given a morphism $X \to S$ of objects in a category $\mathfrak{C}$, define the i-th (algebraic) relative de Rham cohomology group $\mathrm{H}^i_{\mathrm{dR}}(X/S)$.

2.2.1 Kähler Differentials

Let A be a commutative ring with identity, let B be an A-algebra, and let M be a B-module.

Definition 2.2.1. An *A-derivation of B into M* is an A-linear map $d : B \to M$ which satisfies $da = 0$ for all $a \in A$, as well as the Leibniz rule: for $b_1, bb_2 \in B$, $d(bb') = bdb' + b'db$.

Definition 2.2.2. A *module of relative differential forms* of B over A is a B-module $\Omega^1_{B/A}$ equipped with an A-derivation $d : B \to \Omega^1_{B/A}$, satisfying the following universal property: For any B-module M, and for any A-derivation $d' : B \to M$, there exists a unique B-module homomorphism $f : \Omega^1_{B/A} \to M$ such that $d' = f \circ d$.

The universal property ensures that $\Omega^1_{B/A}$ is unique. One way to prove existence of $\Omega^1_{B/A}$ is to give an explicit construction: One takes the free B-module generated by the symbols $\{db : b \in B\}$ and quotients by the submodule generated by $d(bb') - bdb' - b'db$ and $d(b + b') - db - db'$ for $b, b' \in B$, and da for $a \in A$. Define the *module of relative differential i-forms* to be i-th exterior power of the B-module $\Omega^1_{B/A}$

$$\Omega^i_{B/A} := \wedge^i \Omega^1_{B/A}$$

with induced maps $d_i : \Omega^i_{B/A} \to \Omega^{i+1}_{B/A}$ satisfying $d_{i+1} \circ d_i = 0$.

Definition 2.2.3. The complex $(\Omega^\bullet_{B/A}, d)$ is called the *de Rham complex of B over A*, and an element $\omega \in \Omega^i_{B/A}$ is called a relative i-form. We call ω *closed* if $d_i(\omega) = 0$ and *exact* if $\omega = d_{i-1}\nu$ for some $\nu \in \Omega^{i-1}_{B/A}$.

2.2.2 de Rham Cohomology for Schemes

Definition 2.2.4. Given affine schemes $X = \mathrm{Spec}(B)$ and $Y = \mathrm{Spec}(A)$, and a morphism $X \to Y$, we define the *(algebraic) relative de Rham cohomology of X over Y*, denoted

$\mathrm{H}^i_{\mathrm{dR}}(X/Y)$, to be the cohomology of the complex $(\Omega^\bullet_{B/A}, d)$.

To be more precise, we define $\mathrm{H}^i_{\mathrm{dR}}(X/Y)$ to be the closed i-forms modulo exact i-forms

$$\mathrm{H}^i_{\mathrm{dR}}(X/Y) := \frac{\ker\{d_i : \Omega^i_{B/A} \to \Omega^{i+1}_{B/A}\}}{\mathrm{im}\{d_{i-1} : \Omega^{i-1}_{B/A} \to \Omega^i_{B/A}\}}.$$

This definition can be generalized to arbitrary schemes.

Proposition 2.2.5. *Let $f : X \to Y$ be a morphism of schemes. Then there exists a unique quasi-coherent sheaf $\Omega^1_{X/Y}$ on X such that for any affine open subset V of Y, any affine open subset U of $f^{-1}(V)$, and any $x \in U$, we have*

$$\Omega^1_{X/Y}\big|_U \cong \Omega^1_{\mathcal{O}_X(U)/\mathcal{O}_Y(V)} \qquad (\Omega^1_{X/Y})_x \cong \Omega^1_{\mathcal{O}_{X,x}/\mathcal{O}_{Y,f(x)}}$$

Proof. see [40, Proposition 6.1.17]. □

Definition 2.2.6. The sheaf $\Omega^1_{X/Y}$ is called the *sheaf of relative differential 1-forms of X over Y*. The sheaf $\Omega^i_{X/Y} := \wedge^i_{\mathcal{O}_X}\Omega^1_{X/Y}$ is called the *sheaf of relative differential i-forms of X over Y*. Exterior differentiation then induces maps $d_i : \Omega^i_{X/Y} \to \Omega^{i+1}_{X/Y}$. If $Y = \mathrm{Spec(A)}$ is affine, we also denote these sheaves $\Omega^i_{X/A}$.

Definition 2.2.7. Let $f : X \to Y$ be a morphism of schemes. We define the *(algebraic) relative de Rham cohomology of X over Y*, denoted $\mathrm{H}^i_{\mathrm{dR}}(X/Y)$, to be the global sections of the sheaf $\mathbf{R}^i f_*\Omega^\bullet_{X/Y}$ on Y.

Remark 2.2.8. If Y is affine, and X is quasi-compact and separated, then $\mathbf{R}^i f_*\Omega^\bullet_{X/Y}(Y) = \mathrm{H}^i(X, \Omega^\bullet_{X/Y}) := \mathbf{R}^i\Gamma\Omega^\bullet_{X/Y}$, where Γ is the global sections functor [40, Proposition 2.28]. In this case, $\Omega^i_{X/Y}(U)$ is acyclic for any open affine subset U of X, and $\mathrm{H}^i(X, \Omega^\bullet_{X/Y})$ may be computed as $\mathbb{H}^i(X, \Omega^\bullet_{X/Y})$, i.e. the hypercohomology of $\Omega^\bullet_{X/Y}$. In particular, if X is affine, we arrive at the previous definition.

Remark 2.2.9. It can be shown (e.g. [40, Proposition 6.2.2]) that if $f : X \to Y$ is smooth, then $\Omega^i_{X/Y}$ is a locally free $\mathcal{O}_X$-module.

2.2.3 de Rham Cohomology with Logarithmic Singularities

Here we will review the constructions involving differentials with logarithmic poles along a subscheme. First we require several preliminary definitions.

Definition 2.2.10. Let $f : X \to S$ be a morphism of finite type. Then f is *smooth of relative dimension n* if it is smooth, and all of its non-empty fibres are equidimensional of dimension n. We say f is *étale* if it is smooth of relative dimension 0.

Definition 2.2.11. A *smooth pair* (resp. a *smooth proper pair*) of relative dimension n over a scheme S, is a pair of S-schemes (X, Z) in which $f : X \to S$ is smooth (resp. smooth proper) of relative dimension n, and Z is a relative reduced normal crossings divisor on X. That is, étale-locally on X, one can find an S-isomorphism of X with a Zariski open subset of $\mathbb{A}^n_S$ under which Z is carried to an open subset of a union of coordinate hyperplanes.

Remark 2.2.12. In the definition of a smooth pair (X, Z) we include the possibility of Z being empty.

Definition 2.2.13. Let (X, Z) be a smooth pair of relative dimension n over a scheme S, such that $U := X \setminus Z$ is affine with inclusion map $\iota : U \to X$. We define the *sheaf of relative differential 1-forms on X with logarithmic singularities along Z*, denoted $\Omega^1_{(X,Z)/S}$, to be the sub-$\mathcal{O}_X$-module of $\iota_*\Omega^1_{U/S}$ defined on affine étale open sets V in the following way: If $t_1, ..., t_n$ are local coordinates for V on $\mathbb{A}^1_S$, and $Z|_V$ is defined by an equation $t_1 \cdots t_r = 0$, then $\Gamma(V, \Omega^1_{(X,Z)/S})$ is defined to be the free $\Gamma(V, \mathcal{O}_X)$-module generated by the elements $dt_1/t_1, ..., dt_r/t_r, dt_{r+1}, ..., dt_n$.

Setting $\Omega^i_{(X,Z)/S} = \wedge^i_{\mathcal{O}_X}\Omega^1_{(X,Z)/S}$, the exterior differentiation operator inherited from $\iota_*\Omega^i_{U/S}$ induces maps

$$d_i : \Omega^i_{(X,Z)/S} \to \Omega^{i+1}_{(X,Z)/S}.$$

The resulting complex is called the *de Rham complex of* (X, Z) *over* S. We define the *i-th algebraic de Rham cohomology group* of (X, Z) over S, denoted $\mathrm{H}^i_{\mathrm{dR}}((X, Z)/S)$, to be the global sections of $\mathbf{R}^i f_*\Omega^\bullet_{(X,Z)/S}$.

Remark 2.2.14. As in the remark of the previous section, if S is affine then $\mathrm{H}^i_{\mathrm{dR}}((X, Z)/S)$ can be computed as $\mathbb{H}^i(X, \Omega^\bullet_{(X,Z)/S})$, the hypercohomology of the de Rham complex of (X, Z).

Definition 2.2.15. Using the notation from the previous definition, denote by $W_k(\Omega^i_{(X,Z)/S})$ the submodule of $\Omega^i_{(X,Z)/S}$ generated on affine étale open sets V by differentials of the form

$$\frac{dt_{j(1)}}{t_{j(1)}} \wedge \cdots \wedge \frac{dt_{j(l)}}{t_{j(l)}} \wedge dt_{j(l+1)} \wedge \cdots \wedge dt_{j(i)}, \quad l \leq k.$$

Then $W_k(\Omega^\bullet_{(X,Z)/S})$ is a subcomplex of $\Omega^\bullet_{(X,Z)/S}$. Let

$$\mathrm{Gr}^W_k(\Omega^\bullet_{(X,Z)/S}) = W_k(\Omega^\bullet_{(X,Z)/S})/W_{k-1}(\Omega^\bullet_{(X,Z)/S})$$

denote the associated graded complex.

We will make use of the following construction of Deligne from [29, section 3.I], adapted from the language of complex analytic geometry to our present environment. Let (X, Z) be a smooth pair over a scheme S of relative dimension n. Then around each point $P \in X$, there is an étale neighbourhood $i : U \to X$, and an open immersion $j : U \to \mathbb{A}^n_S$, such that $i^{-1}(Z)$ is a union $H_1 \cup \cdots \cup H_r$ where each H_i is the intersection of a distinct hyperplane in $\mathbb{A}^n_S$ with U. For a subset $J \subset \{1, ..., r\}$, let $H_J = \bigcap_{i \in J} H_i$, and define $Z^k_U = \bigcup_{|J|=k} H_J$ and $\widetilde{Z}^k_U = \bigsqcup_{|J|=k} H_J$, where the union is taken over all subsets of $\{1, ..., r\}$ of length k. These glue together to form S-schemes Z^k and $\widetilde{Z}^k$. Put $Z^0 = \widetilde{Z}^0 = X$. By construction, $\widetilde{Z}^k$ is a smooth scheme, $Z^1 = Z$, and for $k > 1$, Z^k is the singular locus of Z^{k-1}. Additionally, the projection $\bigsqcup_{|J|=k} H_J \to \bigcup_{|J|=k} H_J$ gives a map $\widetilde{Z}^k \to Z^k$ which is in fact the normalization of Z^k. Let $i_k : \widetilde{Z}^k \to X$ denote the compositions of the normalization with the inclusion map.

We now define a sheaf of $\mathbb{Z}$-modules ε^k on the small étale site of $\widetilde{Z}^k$ as follows. Let $\varepsilon^k(H_J) = \bigwedge^k(\bigoplus_{i \in J} \mathbb{Z}_{H_i})$, where $\mathbb{Z}_{H_i}$ denotes a copy of the integers corresponding to H_i. These glue together to form a locally free sheaf of rank 1. For a sheaf $\mathcal{F}$ on $\widetilde{Z}^k$, let $\mathcal{F}(\varepsilon^k)$ denote the tensor product $\mathcal{F} \times_{\mathbb{Z}} \varepsilon^k$.

Theorem 2.2.16 (Poincaré Residue Theorem)**.** *Suppose (X, Z) is a smooth pair of relative dimension n over S. Then for each $1 \leq k \leq n$ there is an isomorphism of $\mathcal{O}_X$-modules*

$$Res : Gr^W_k(\Omega^\bullet_{(X,Z)/S}) \to \iota_{k*}\Omega^\bullet_{\widetilde{Z}^k}(\varepsilon^k)[-k].$$

Proof. Étale-locally on X, Z is given in some Zariski-open set $U \subset \mathbb{A}^n_S$ as a union of hyperplanes $H_1, ..., H_r$. Localizing further, we may assume that $U = \mathrm{Spec}(R)$ and $S = \mathrm{Spec}(A)$ are affine, and the hyperplanes are defined by local coordinates $t_1, ..., t_r \in R$. Then by definition

$$\iota_{k*}\Omega^\bullet_{\widetilde{Z}^k}(\varepsilon^k)(U) = \bigoplus_{|J|=k} \Omega^\bullet_{R_J/A} \otimes \varepsilon^k(H_J)$$

where $R_J = R/(t_{j_1}, ..., t_{j_k})$ for $J = \{j_1, ..., j_k\} \subset \{1, .., r\}$. We can define a surjective map

$$W_k(\Omega^\bullet_{(X,Z)/S})(U) \to \iota_{k*}\Omega^\bullet_{Z^k}(\varepsilon)(U)$$

by first defining it on sections $\omega = \alpha \wedge \dfrac{dt_{j_1}}{t_{j_1}} \wedge \cdots \wedge \dfrac{dt_{j_k}}{t_{j_k}}$ to be

$$\omega \mapsto (\alpha \mod t_{j_1}, ..., t_{j_k}) \otimes (1_{H_{j_1}} \wedge \cdots \wedge 1_{H_{j_k}})$$

and extending linearly over A. We define Res to be the above map modulo its kernel, which is equal to $W_{k-1}(\Omega^\bullet_{(X,Z)/S})(U)$, thus defining an isomorphism on the graded complex. To see that Res is well-defined globally, it is enough to see that it is independent of the choice the local parameters defining Z. This is immediate from the following observations:

1. If σ is a permutation of J, then

$$\omega = \alpha \wedge \frac{dt_{j_1}}{t_{j_1}} \wedge \cdots \wedge \frac{dt_{j_k}}{t_{j_k}} = \operatorname{sgn}(\sigma)\alpha \wedge \frac{dt_{\sigma(j_1)}}{t_{\sigma(j_1)}} \wedge \cdots \wedge \frac{dt_{\sigma(j_k)}}{t_{\sigma(j_k)}},$$

   so the map

$$\begin{aligned} \omega &\mapsto (\operatorname{sgn}(\sigma)\alpha \mod t_{j_1}, ..., t_{j_k}) \otimes (1_{H_{\sigma(j_1)}} \wedge \cdots \wedge 1_{H_{\sigma(j_k)}}) \\ &= (\alpha \mod t_{j_1}, ..., t_{j_k}) \otimes (1_{H_{j_1}} \wedge \cdots \wedge 1_{H_{j_k}}) \end{aligned}$$

   is the same as the one defined previously.

2. If $u \in R^*$ is a unit and $\alpha \in W_{k-1}(\Omega^\bullet_{(X,Z)/S})(U)$, then

$$\alpha \wedge \frac{d(ut_{j_i})}{ut_{j_i}} - \alpha \wedge \frac{dt_{j_i}}{t_{j_i}} = \alpha \wedge \frac{du}{u} \in W_{k-1}(\Omega^\bullet_{(X,Z)/S})(U),$$

   so choosing a new parameter for H_{j_i} gives an equivalent element in the graded complex.

□

Remark 2.2.17. It is clear that ε^k is isomorphic to the constant sheaf on $\widetilde{Z}^k$ for $k = 1$. The same is true for $k = n$, since $\widetilde{Z}^n$ is a disjoint union of schemes isomorphic to S, on which ε^n is constant. Therefore for $n = 2$ we can ignore ε^k entirely, however it is worth noting that the map

$$\operatorname{Res} : \operatorname{Gr}_2^W(\Omega^\bullet_{(X,Z)/S}) \to i_{2*}\Omega^\bullet_{\widetilde{Z}^2}[-2]$$

is noncanonical, i.e. it depends on a choice of sign at each crossing.

Definition 2.2.18. Let (X, Z) be a smooth pair over a scheme S, let $\mathcal{F}$ be a sheaf of $\mathcal{O}_X$-modules, and let m be a nonnegative integer. Let $\mathcal{O}_X(mZ)$ denote the invertible sheaf on X corresponding to the divisor mZ. Define the *m-th twist of $\mathcal{F}$ along Z* to be $\mathcal{F}(mZ) := \mathcal{F} \otimes_{\mathcal{O}_X} \mathcal{O}_X(mZ)$.

Remark 2.2.19. On affine étale open sets V of X, where $V|_Z$ is defined by $t_1 \cdots t_r = 0$, $\Omega^i_{(X,Z)/S}$ is the sub-$\mathcal{O}_X$-module of $\Omega^i_{X/S}(Z)$ generated freely by $dt_1/t_1, ..., dt_r/t_r, dt_{r+1}, ..., dt_n$ and $\Omega^i_{X/S}$ is the submodule generated by $dt_1, ..., dt_n$. Thus for any integer m there are natural inclusions of $\mathcal{O}_X$-modules

$$\Omega^i_{X/S}(mZ) \subset \Omega^i_{(X,Z)/S}(mZ) \subset \Omega^i_{X/S}((m+1)Z) \subset \iota_*\Omega^i_{U/S},$$

and $\iota_*\Omega^i_{U/S}$ is equal to the direct limit of either $\Omega^i_{X/S}(mZ)$ or $\Omega^i_{(X,Z)/S}(mZ)$ as m increases. On affine subsets $V \subset X$, we can write

$$\Gamma(V, \Omega^i_{(X,Z)/S}) = \{s \in \Gamma(V, \Omega^i_{X/S}(Z)) : d_i s \in \Gamma(V, \Omega^{i+1}_{X/S}(Z))\}.$$

We have the following useful fact about the homology sheaves of differential forms and their twists.

Theorem 2.2.20. *Let (X, Z) be a smooth pair over a scheme S. For each nonnegative integer m, the natural map of complexes of sheaves*

$$\Omega^\bullet_{(X,Z)/S} \to \Omega^\bullet_{(X,Z)/S}(mZ)$$

induces maps on the homology sheaves whose kernels and cokernels are killed by $lcm(1, ..., m)$.

Proof. For the assertion about the cokernel, see [18, Theorem 2.2.5]. For the assertion about the kernel, see [41, Proposition 3] □

2.3 p-Adic Cohomology Theories

If a variety is defined over a field of characteristic $p > 0$, then de Rham cohomology is not a suitable cohomology theory, for it does not offer finite dimensionality in even the simplest of cases. For instance, the $\mathrm{H}^1_{\mathrm{dR}}(\mathrm{Spec}(\mathbb{F}_p[x]))$ contains the linearly independent set $\{x^{p^i-1}dx\}_{i=1}^\infty$. It is therefore necessary to develop cohomology theories over a field of characteristic 0.

2.3.1 Monsky-Washnitzer Cohomology

Definition 2.3.1. For a $\mathscr{V}$-algebra A, we will denote by $\hat{A}$ its completion with respect to the ideal pA, that is, the universal object of the inverse system $\cdots \to A/p^2A \to A/pA$.

Remark 2.3.2. If A is finitely generated by elements $\{x_1, ..., x_n\}$, then an element of $\hat{A}$ can be written as power series in multi-index notation

$$\sum c_\alpha x^\alpha$$

with $c_\alpha \in \mathscr{V}$ satisfying $|c_\alpha|_p \to 0$ as $|\alpha| \to \infty$. Here $\alpha = a_1, .., a_n$ is a multi-index of nonnegative integers, $x^\alpha = x_1^{a_1} \cdots x_n^{a_n}$, and $|\alpha| = a_1 + \cdots + a_n$.

Definition 2.3.3. Let A be a finitely generated $\mathscr{V}$-algebra, and let $\{x_1, ..., x_n\}$ be a set of generators. We define the *dagger algebra of* A, denoted $A^\dagger$, to be the subalgebra of $\hat{A}$ consisting of the *overconvergent power series*. That is, $A^\dagger$ consists of elements representable as

$$\sum c_\alpha x^\alpha$$

with $c_\alpha \in \mathscr{V}$, such that there exist real numbers C, r with $C > 0$, $0 < r < 1$, satisfying $|c_\alpha|_p \leq Cr^{|\alpha|}$ for all α.

Definition 2.3.4. Let X be a smooth affine variety over k with coordinate ring $\overline{A}$. By a theorem of Elkik [42], there exists a $\mathscr{V}$-algebra A such that $A/pA \cong \overline{A}$ and $\mathcal{X} = \mathrm{Spec}(A)$ is a smooth affine $\mathscr{V}$-scheme. The i-th cohomology group of the complex $\Omega^\bullet_{A^\dagger/\mathscr{V}}$ is denoted $\mathrm{H}^i_{\mathrm{MW}}(X/\mathscr{V})$. We define the *$i$-th Monsky-Washnitzer cohomology group of* X, denoted $\mathrm{H}^i_{\mathrm{MW}}(X/K)$, to be $\mathrm{H}^i_{\mathrm{MW}}(X/\mathscr{V}) \otimes_{\mathscr{V}} K$.

Remark 2.3.5. Monsky and Washnitzer prove [11, Theorem 5.6] that the map sending X to $\mathrm{H}^i_{\mathrm{MW}}(X/K)$ is a contravariant functor. In particular, it is independent of the choices that were made (namely, the choice of the $\mathscr{V}$-algebra A and its generators). Additionally, σ can be extended to a σ-linear map on $A^\dagger$, which induces a σ-linear map F on $\mathrm{H}^i_{\mathrm{MW}}(X/K)$.

2.3.2 Rigid Cohomology and Crystalline Cohomology

We now discuss the notions and relevant theorems of rigid cohomology and crystalline cohomology. We do not give the technical background, as it is lengthy and unnecessary for putting the theory to practical use. The explicit constructions may be found in a work of Shiho [43] for crystalline cohomology, and Berthelot [23] for rigid cohomology.

Definition 2.3.6. Let (X, Z) be a smooth proper pair over k. One can define a $\mathscr{V}$-module $\mathrm{H}^i_{\mathrm{crys}}((X, Z)/\mathscr{V})$, contravariantly functorial in the pair (X, Z), called the *i-th crystalline cohomology group* of (X, Z). Moreover, the Frobenius on k induces a σ-linear map on $\mathrm{H}^i_{\mathrm{crys}}((X, Z)/\mathscr{V})$. If Z is empty, we will write the crystalline cohomology as $\mathrm{H}^i_{\mathrm{crys}}(X/\mathscr{V})$.

Definition 2.3.7. Let X be a smooth k-scheme. One can define a finite-dimensional K-vector space $\mathrm{H}^i_{\mathrm{rig}}(X/K)$, contravariantly functorial in X, called the *i-th rigid cohomology group* of X, with a σ-linear map induced by the Frobenius on k.

From Berthelot [24, Propositions 1.9 and 1.10], we have the following comparison isomorphisms, connecting rigid, crystalline, and Monsky-Washnitzer cohomology groups.

Proposition 2.3.8. *Let X be a smooth, proper k-scheme. There is a functorial, Frobenius-equivariant isomorphism*

$$H^i_{rig}(X/K) \cong H^i_{crys}(X/\mathscr{V}) \otimes_{\mathscr{V}} K$$

Proposition 2.3.9. *Let X be a smooth, affine k-scheme. There is a functorial, Frobenius-equivariant isomorphism*

$$H^i_{rig}(X/K) \cong H^i_{MW}(X/K)$$

The following is a result of Shiho [43, Theorem 2.4.4]

Theorem 2.3.10. *Let (X, Z) be a smooth pair over k, and set $U = X \setminus Z$. There is a functorial, Frobenius-equivariant isomorphism*

$$H^i_{crys}((X, Z)/\mathscr{V}) \otimes_{\mathscr{V}} K \cong H^i_{rig}(U/K)$$

2.3.3 Comparisons Theorems Between p-Adic and de Rham Cohomology

Fundamental to all p-adic point counting algorithms is the ability to compute a p-adic cohomology group as the de Rham cohomology of some scheme. Additionally, the following comparison isomorphisms can be used to give effective p-adic bounds for the algorithms.

Theorem 2.3.11. *[44, Cor 2.6] Let $(\mathcal{X}, \mathcal{Z})$ be a smooth proper pair over $\mathscr{V}$. Put $\mathcal{U} = \mathcal{X} \setminus \mathcal{Z}$, and let U and $\mathcal{U}_K$ denote the special and generic fibres of $\mathcal{U}$. Then there is an isomorphism*

$$H^i_{rig}(U/K) \cong H^i_{dR}(\mathcal{U}_K/K)$$

In particular, when $\mathcal{Z}$ is empty the theorem reduces to an isomorphism

$$\mathrm{H}^i_{\mathrm{rig}}(X/K) \cong \mathrm{H}^i_{\mathrm{dR}}(\mathcal{X}_K/K).$$

Proposition 2.3.12. *Let $(\mathcal{X}, \mathcal{Z})$ be a smooth proper pair over $\mathscr{V}$. Let X and Z be the special fibres of $\mathcal{X}$ and $\mathcal{Z}$, respectively. Then there is an isomorphism*

$$H^i_{crys}((X,Z)/\mathscr{V}) \cong H^i_{dR}((\mathcal{X},\mathcal{Z})/\mathscr{V})$$

Proof. See [45, Theorem 6.4]. □

2.4 Exact Sequences

Of particular use to us will be several be exact sequences which have analogues in each cohomology theory. We begin with an algebraic version of the Gysin sequence from the theory of complex manifolds.

Theorem 2.4.1. *Let X be a smooth variety over a field of characteristic 0, and let Z be a smooth closed subvariety of pure codimension r. Then there is a long exact sequence*

$$\cdots \to H^i_{dR}(X) \to H^i_{dR}(X \setminus Z) \xrightarrow{\delta} H^{i+1-2r}_{dR}(Z) \to H^{i+1}_{dR}(X) \to \cdots$$

The map δ we will refer to as the Poincaré residue map.

Proof. Combine Theorem 3.3 and Proposition 3.4 from [46]. □

As in most cohomology theories, there is a notion of cohomology with compact support for both de Rham and rigid cohomology, denoted $\mathrm{H}^i_{\mathrm{dR},c}(X)$ and $\mathrm{H}^i_{\mathrm{rig},c}(X)$, respectively, which are isomorphic to cohomology without compact support for X proper. One has the following excision sequences for these objects, which carries the added benefit of allowing us to forgo smoothness assumptions.

Proposition 2.4.2. *Let X be variety over a field of characteristic 0, let Z be closed subvariety, and let U denote the complement. Then there is a long exact sequence*

$$\cdots \to H^i_{dR,c}(U) \to H^i_{dR,c}(X) \to H^i_{dR,c}(Z) \to H^{i+1}_{dR,c}(U) \to \cdots$$

Proof. See [47, Proposition 1.11] □

Proposition 2.4.3. *Let X be a separated k-scheme of finite type, let Z be closed subscheme, and let U denote the complement. Then there exists a Frobenius-equivariant long exact sequence*

$$\cdots \to H^i_{rig,c}(U/K) \to H^i_{rig,c}(X/K) \to H^i_{rig,c}(Z/K) \to H^{i+1}_{rig,c}(U/K) \to \cdots$$

Proof. See [48, 3.1 (iii)]. □

For a space M that has an action of Frobenius, given an integer l, we denote by $M(l)$ the space M with the action of Frobenius multiplied by q^{-l}. For X a smooth k-scheme of dimension n, Poincaré duality in rigid cohomology gives a Frobenius-equivariant K-pairing

$$\mathrm{H}^i_{\mathrm{rig,c}}(X) \times \mathrm{H}^{2n-i}_{\mathrm{rig}}(X)(n) \to K \tag{2.1}$$

which leads to the following proposition (for details of these constructions see [49]).

Proposition 2.4.4. *Let (X, Z) be a smooth pair over k with Z also smooth. Put $U = X \setminus Z$. Then there exists a Frobenius-equivariant long exact sequence*

$$\cdots \to H^i_{rig}(X/K) \to H^i_{rig}(U/K) \to H^{i-1}_{rig}(Z/K)(-1) \to H^{i+1}_{rig}(X/K) \to \cdots$$

Proof. See [18, Proposition 2.4.1 b] □

Chapter 3

Superelliptic Curves

3.1 Basic Properties

Definition 3.1.1. We define a *superelliptic curve* $C \to S$ of genus g to be a smooth projective morphism of schemes such that the fibre over each closed point $\eta \to S$ is connected, has dimension 1, genus g, and is birationally equivalent to an affine plane curve C^0 given by an equation

$$y^r = x^d + a_{d-1}x^{d-1} + \cdots + a_0 = \prod_{i=1}^{n}(x - \alpha_i)^{e_i} \in k(\eta)[x]$$

where r is a fixed prime and d is a positive integer such that $(r, d) = 1$. We require the singular points of the planar equation to be rational over $k(\eta)$ ($\alpha_i \in k(\eta)$ if $e_i > 1$) and if $\mathrm{char}(k(\eta)) = p > 0$, we require $(p, r) = 1$ and $(p, e_i) = 1$ for each i.

A superelliptic curve C over a field F comes equipped with an automorphism ρ of order r induced by the map $(x, y) \longmapsto (x, \zeta y)$, where ζ is a primitive r-th root of unity. Letting $C/\langle\rho\rangle$ be the quotient variety, there is an isomorphism

$$C/\langle\rho\rangle \to \mathbb{P}^1_F$$

given by $[(x, y)] \mapsto x$ on C^0.

Suppose C is a superelliptic curve over a field F, birationally equivalent to an affine plane curve C^0 defined by the equation

$$y^r = f(x) = \prod_{i=1}^{n}(x - \alpha_i)^{e_i}.$$

For simplicity assume that $\alpha_i \in F$ for all i, and write the division of e_i by r with remainder as $e_i = \delta_i r + \lambda_i$. Let D^0 be the curve defined by the equation

$$y^r = \prod_{i=1}^{n} (x - \alpha_i)^{\lambda_i}.$$

For a point $(a, b) \in D^0$ one has

$$\begin{aligned} \left(b \prod_{i=1}^{n} (a - \alpha_i)^{\delta_i} \right)^r &= b^r \prod_{i=1}^{n} (a - \alpha_i)^{r\delta_i} \\ &= \left(\prod_{i=1}^{n} (a - \alpha_i)^{\lambda_i} \right) \left(\prod_{i=1}^{n} (a - \alpha_i)^{r\delta_i} \right) \\ &= \prod_{i=1}^{n} (a - \alpha_i)^{e_i} \end{aligned}$$

so we can define a morphism $\varphi : D^0 \to C^0$ as the map which sends (a, b) to $(a, b \prod_{i=1}^{n} (a - \alpha_i)^{\delta_i})$. This gives a birational equivalence between C^0 and D^0 over F. We will therefore assume from now on that $1 \leq e_i \leq r - 1$ for all i.

3.1.1 The Genus

Let $p > 0$ be a prime, $p \neq 2$. Fix a positive integer a, and put $q = p^a$ and $k = \mathbb{F}_q$. Let $\mathscr{V}$ denote the ring of Witt vectors over k, $\mathscr{V}_{\text{fin}}$ the Witt vectors of finite length, and K the fraction field of $\mathscr{V}$.

Suppose $\widetilde{C}_k$ is a superelliptic curve over k with associated planar curve C_k^0 defined by an equation

$$y^r = \overline{f}(x) = \prod_{i=1}^{n} (x - \overline{\alpha}_i)^{e_i}.$$

Suppose that the singular points of C_k^0 are ordered $(\overline{\alpha}_1, 0), ..., (\overline{\alpha}_m, 0)$ for some $m \leq n$. Then by definition $\alpha_i \in k$ for $1 \leq i \leq m$. Let $\overline{\tau}(x) = \prod_{i=m+1}^{n} (x - \overline{\alpha}_i) \in k[x]$. Let $\alpha_1, ..., \alpha_m$ be lifts of the elements $\overline{\alpha}_1, ..., \overline{\alpha}_m$ to $\mathscr{V}_{\text{fin}}[x]$, and let $\tau(x) \in \mathscr{V}_{\text{fin}}[x]$ be a polynomial obtained by lifting the coefficients of $\overline{\tau}(x)$ to $\mathscr{V}_{\text{fin}}[x]$. We then define

$$f(x) = \tau(x) \prod_{i=1}^{m} (x - \alpha_i)^{e_i}.$$

The equation $y^r = f(x)$ defines a $\mathscr{V}$-scheme C^0 with special fibre isomorphic to C^0_k. Let C denote the closure of C^0 in $\mathbb{P}^2_{\mathscr{V}}$, and let C_K and C_k denote the generic and special fibres of C, respectively. Put $C' = C^0 \setminus \{y = 0\}$ and let C'_K and C'_k denote the generic and special fibres of C'.

Proposition 3.1.2. *There exists a smooth $\mathscr{V}$-scheme $\widetilde{C}$ over C, isomorphic to C' outside a finite number of points, and admitting a unique point lying above each singular point of C. If P_∞ is the closed point in $\widetilde{C}$ lying above ∞, then $ord_{P_\infty}(x) = -r$ and $ord_{P_\infty}(y) = -d$. If P_i is the closed point lying above $(\alpha_i, 0)$, then $ord_{P_i}(x - \alpha_i) = r$ and $ord_{P_i}(y) = e_i$.*

Proof. To prove the proposition we compute a sequence of blowups of the closed singular points of C restricted to affine neighbourhoods. Fix an algebraic closure $\overline{K}$ of K, and let $\overline{\mathscr{V}}$ denote its ring of integers. Then $\overline{\mathscr{V}}$ is flat over $\mathscr{V}$. Suppose $\widetilde{C} \to C$ is a blowup of C along a closed subvariety Z. To check that $\widetilde{C}$ is smooth, from [40, Ch. 4, Definition 3.35] it suffices to check smoothness at the closed points of $\widetilde{C} \times \mathrm{Spec}(\overline{\mathscr{V}})$, which by Proposition (2.1.10) is isomorphic to the blowup of $C \times \mathrm{Spec}(\overline{\mathscr{V}})$ along Z. Therefore we can assume $K = \overline{K}$ and $\mathscr{V} = \overline{\mathscr{V}}$.

Suppose $r < d$. Then C has equation $Y^r Z^{d-r} = Z^d f(\frac{X}{Z})$ in projective coordinates, which is the union of C^0 with an additional singular point at infinity $\infty = [0 : 1 : 0]$. Restricting to $Y \neq 0$ and letting (S, T) be projective coordinates for $\mathbb{P}^1_{\mathscr{V}}$, the blowup at the closed point of ∞ gives equations for the total transform of the curve in $\mathbb{A}^2_{\mathscr{V}} \times \mathbb{P}^1_{\mathscr{V}}$ as

$$\begin{aligned} z^{d-r} &= z^d f(\frac{x}{z}) \\ Tx &= Sz \end{aligned}$$

where $z := Z/Y$ and $x := X/Y$. Note that any point above ∞ occurs at $x = z = 0$. Let U_1 and U_2 be the affine spaces corresponding to $T \neq 0$ and $S \neq 0$ respectively. We choose $s := S/T$ to be an affine coordinate on U_1, and $t := T/S$ to be an affine coordinate on U_2. The local equation for the total transform of C on U_1 is $z^{d-r} = z^d f(s)$ so the coordinates of the strict transform satisfy the equation $z^r f(s) = 1$. Thus there is no point lying above ∞ on U_1, and the strict transform of the curve is contained entirely in U_2.

The total transform of C in U_2 is defined in affine coordinates by $t^{d-r}x^{d-r} = x^d t^d f(\frac{1}{t}) = x^d f_{-1}(t)$ where we have set $f_{-1}(t) = t^d f(1/t)$. Note that $f_{-1}(0) = 1 \neq 0$. The strict transform W satisfies the equation $t^{d-r} = x^r f_{-1}(t)$, which contains a single point lying above

∞, at $x = t = 0$. Let $\mathcal{O}_W$ denote the coordinate ring of W, and define

$$B = \frac{\mathcal{O}_W[u, \frac{1}{u}]}{(u^r - f_{-1}(t))}.$$

Let $g : \mathrm{Spec}(B) \to W$ denote the induced morphism of schemes. Since $(p, r) = 1$, we find that $\frac{d}{du}(u^r - f_{-1}(t)) = ru^{r-1}$ is a unit, so g is étale. Letting $v = ux$, we can rewrite the ring B

$$B = \frac{\mathcal{O}_W[u, \frac{1}{u}]}{(u^r - f_{-1}(t))} = \frac{\mathscr{V}[t, v, u, \frac{1}{u}]}{(t^{d-r} - v^r, u^r - f_{-1}(t))}.$$

Since $f_{-1}(0) \neq 0$, the set $g^{-1}((0, 0))$ consists of r distinct closed points, corresponding to the roots of $u^r - f_{-1}(0)$. Let $V \subset \mathrm{Spec}(B)$ be an open affine set containing exactly one of these points, which we will denote by Q_∞. The map

$$\begin{array}{rccc} \varphi : B & \longrightarrow & \dfrac{\mathscr{V}[w, u, \frac{1}{u}]}{(u^r - f_{-1}(w^r))} =: \widetilde{B} \\ t & \mapsto & w^r \\ v & \mapsto & w^{d-r} \end{array}$$

induces a morphism $\varphi^* : \mathrm{Spec}(\widetilde{B}) \to \mathrm{Spec}(B)$ which is the composition of a sequence of blowups at the closed point of $\mathrm{Spec}(B)$ where $t = v = 0$. Additionally, it resolves the singularity at Q_∞, admits a single closed point $\widetilde{Q}_\infty$ lying above Q_∞ with uniformizing parameter w, and is an isomorphism outside of the support of the divisor w. Let $\widetilde{V}$ denote the preimage of V under φ^*, and $\widetilde{W}$ denote the corresponding series of blowups of W at Q_∞, by (2.1.10) there is a commutative diagram

$$\begin{array}{ccc} \widetilde{V} \cong \widetilde{W} \times_W V & \longrightarrow & V \\ \downarrow & & \downarrow \\ \widetilde{W} & \longrightarrow & W \end{array}$$

Since there is only one point in $\widetilde{V}$ lying above Q_∞, there must be a unique point $P_\infty \in \widetilde{W}$ lying above Q_∞. Moreover, since g is étale, by Proposition (2.1.8) there is an isomorphism on the completed local rings

$$\hat{\mathcal{O}}_{\widetilde{W}, P_\infty} \cong \hat{\mathcal{O}}_{\widetilde{V}, \widetilde{Q}_\infty}.$$

which preserves the order of vanishing of an element in the coordinate ring. We have the following calculations

$$\begin{aligned}
\mathrm{ord}_{P_\infty}(Y/Z) &= -\mathrm{ord}_{P_\infty}(z) = -\mathrm{ord}_{P_\infty}(tx) = -\mathrm{ord}_{\widetilde{Q}_\infty}(tv/u) = -\mathrm{ord}_{\widetilde{Q}_\infty}(w^d/u)) = -d \\
\mathrm{ord}_{P_\infty}(X/Z) &= \mathrm{ord}_{P_\infty}(x) - \mathrm{ord}_{P_\infty}(z) \\
&= \mathrm{ord}_{\widetilde{Q}_\infty}(v/u) - d = \mathrm{ord}_{\widetilde{Q}_\infty}(w^{d-r}/u)) - d = d - r - d = -r.
\end{aligned}$$

We now turn our attention to points of the form $P_i := [\alpha_i : 0 : 1]$, $1 \leq i \leq n$. Around P_i, C satisfies the affine equation $y^r = f(x)$. Shifting coordinates so that $P_i = (0,0)$, we can write this equation as $y^r = x^{e_i} f_i(x)$, for some polynomial $f_i(x)$ with $f_i(0) \neq 0$. Since $(r, e_i) = 1$, the same argument as above implies that we introduce a change of coordinates $u^r = f_i(x)$, $v = \dfrac{y}{u}$ so that there is an étale neighbourhood of P_i given by the equation $v^r = x^{e_i}$. The resolution of singularities given by $v \mapsto w^{e_i}$, $x \mapsto w^r$ shows that there is a unique point $\widetilde{P}_i \in \widetilde{C}$ lying above $(0,0)$. Additionally we have

$$\begin{aligned}
\mathrm{ord}_{\widetilde{P}_i}(y) &= \mathrm{ord}_{\widetilde{P}_i}(uw^{e_i}) = e_i \\
\mathrm{ord}_{\widetilde{P}_i}(x - \alpha_i) &= \mathrm{ord}_{\widetilde{P}_i}(w^r) = r.
\end{aligned}$$

The case where $d < r$ is proved similarly. □

Proposition 3.1.3. *The scheme $\widetilde{C}$ is a superelliptic curve over $\mathscr{V}$ with genus $g = \dfrac{(r-1)(n-1)}{2}$.*

Remark 3.1.4. Note that in the case $r = 2$ we would have a hyperelliptic curve, and the proposition states that its genus is $\dfrac{n-1}{2}$. The fact that this is an integer is ensured by the condition $(d, 2) = 1$, and the fact that d and n have the same parity.

Proof. It is enough to check the genus on the special fibre $\widetilde{C}_k$. The map

$$C'_k \to \mathbb{P}^1_k \setminus \{\infty, [\alpha_i : 1]\}$$

sending (x, y) to $[x : 1]$ gives an r-fold cover of the projective line minus $n + 1$ points. We can then compute

$$\begin{aligned}
\chi(\widetilde{C}_k) &= \chi(\phi^{-1}(C'_k)) + n + 1 \\
&= r\chi(\mathbb{P}^1_k - \{n+1 \text{ points}\}) + n + 1 \\
&= r(2 - n - 1) + n + 1 \\
&= 2 - (r-1)(n-1).
\end{aligned}$$

If g is the genus of $\widetilde{C}_k$, from the Hurwitz genus formula we get $2-2g = 2-(r-1)(n-1)$, which gives $g = \dfrac{(r-1)(n-1)}{2}$.

□

3.1.2 The Zeta Function

Let C be a superelliptic curve over $\mathscr{V}$ of genus g, birationally equivalent to the plane curve defined by an equation $y^r = f(x) = \prod_{i=1}^{n}(x-\alpha_i)^{e_i}$ where f has degree d. Let C' denote the plane curve minus the points along $y = 0$. By the Weil conjectures for rigid cohomology, the zeta function of the special fibre C_k can be written

$$Z(C_k, T) = \frac{\det(1 - TF|\mathrm{H}^1_{\mathrm{rig,c}}(C_k))}{(1-T)(1-qT)}$$

where F is the map induced by Frobenius on cohomology with compact support. Since C_k is smooth, Poincaré duality (Equation (2.1)) gives a canonical non-degenerate pairing

$$\mathrm{H}^1_{\mathrm{rig,c}}(C_k) \times \mathrm{H}^1_{\mathrm{rig}}(C_k)(1) \to K$$

where $\mathrm{H}^1_{\mathrm{rig}}(C_k)(1)$ is a K-vector space where the Frobenius action is multiplied by q^{-1}. It follows that

$$\det(1 - TF|\mathrm{H}^1_{\mathrm{rig,c}}(C_k/K)) \;=\; \det(1 - qTF^{-1}|\mathrm{H}^1_{\mathrm{rig}}(C_k/K))$$

If V is a K-vector space with an automorphism induced by $\rho : C \to C$, we denote by V^l the subspace $\{w \in V | \rho w = \zeta^{-l} w\}$ and by V^- the direct sum $V^1 \oplus \cdots \oplus V^{r-1}$. The following two propositions allow us to view $\mathrm{H}^1_{\mathrm{dR}}(C/\mathscr{V})$ as a Frobenius-equivariant lattice of $\mathrm{H}^1_{\mathrm{rig}}(C'_k/K)$

Proposition 3.1.5. *There is an injective, Frobenius equivariant map*

$$H^1_{rig}(C_k/K) \to H^1_{rig}(C'_k/K)$$

whose image is equal to $H^1_{rig}(C'_k/K)^-$.

Proof. Let $Z_k = C_k \setminus C'_k$. By Proposition (2.4.4) there is a Frobenius-equivariant exact sequence containing

$$0 \to \mathrm{H}^1_{\mathrm{rig}}(C_k/K) \to \mathrm{H}^1_{\mathrm{rig}}(C'_k/K) \to \mathrm{H}^0_{\mathrm{rig}}(Z_k/K)(-1) \to \cdots \tag{3.1}$$

from which injectivity follows.

Since ρ commutes with the Frobenius and acts as the identity on Z_k, we have $\mathrm{H}^0_{\mathrm{rig}}(Z_k/K)^l = 0$ for $l \neq 0$. Therefore $\mathrm{H}^1_{\mathrm{rig}}(C_k/K)^l \to \mathrm{H}^1_{\mathrm{dR}}(C'_k/K)^l$ is an isomorphism for $0 < l < r$.

Since formation of cohomology commutes with ρ we also have

$$\mathrm{H}^1_{\mathrm{rig}}(C_k/K)^0 \cong \mathrm{H}^1_{\mathrm{rig}}(C_k/K)/\langle\rho\rangle \cong \mathrm{H}^1_{\mathrm{rig}}(\mathbb{P}^1_k/K) = 0$$

which completes the proof. □

Proposition 3.1.6. *The module $H^1_{dR}(C/\mathscr{V})$ is a Frobenius-equivariant $\mathscr{V}$-lattice in $H^1_{rig}(C'_k/K)$ with no subspace which is fixed under ρ.*

Proof. From Propositions (2.3.8) and (2.3.12), it follows that there is a Frobenius-equivariant isomorphism

$$\mathrm{H}^1_{\mathrm{dR}}(C/\mathscr{V}) \otimes_{\mathscr{V}} K \cong \mathrm{H}^1_{\mathrm{rig}}(C_k/K).$$

The result follows from Proposition (3.1.5) and [50, Proposition 3.2]. □

3.1.3 The Vector Space $\mathbf{H}^1_{\mathbf{MW}}(C'_K/K)^-$

Using the notation of the previous sections, C'_k has coordinate ring

$$\overline{\mathcal{A}} = \frac{k[x, y, \frac{1}{y}]}{(y^r - \overline{f}(x))}$$

and C' has coordinate ring

$$\mathcal{A} = \frac{\mathscr{V}[x, y, \frac{1}{y}]}{(y^r - f(x))}.$$

An element of the p-adic completion of $\mathcal{A}$, denoted $\hat{\mathcal{A}}$, can be represented

$$z = \sum_{\substack{0 \leq i < d \\ -\infty < j < \infty}} a_{ij} x^i y^j$$

such that $a_{ij} \in \mathscr{V}$ and $|a_{ij}|_p \to 0$ as $|j| \to \infty$.

The dagger ring $\mathcal{A}^\dagger$ is the subring of $\hat{\mathcal{A}}$ consisting of elements represented in the above form, such that there exists a number $0 < c < 1$ with $|a_{ij}|_p < c^{|j|}$. One can then define

the Monsky-Washnitzer cohomology groups $H^i_{MW}(\overline{\mathcal{A}}/K)$ as the cohomology of the de Rham complex over $\mathcal{A}^\dagger_K := \mathcal{A}^\dagger \otimes_{\mathscr{V}} K$.

We can construct this space explicitly. Let $\Omega^\bullet_{\mathcal{A}^\dagger_K}$ be the de Rham complex of $\mathcal{A}^\dagger_K$. The K-space $H^i_{MW}(\overline{\mathcal{A}}/K)$ is then the i-th cohomology group of the chain complex

$$0 \longrightarrow \mathcal{A}^\dagger_K \xrightarrow{d} \Omega^1_{\mathcal{A}^\dagger_K} \longrightarrow 0.$$

The relation $y^r = f(x)$ in $\mathcal{A}^\dagger$ leads to the relation $ry^{r-1}dy = f'(x)dx$ in $\Omega^1_{\mathcal{A}^\dagger_K}$. Writing this as $dy = \dfrac{f'(x)dx}{ry^{r-1}}$, it follows that any element in $\Omega^1_{\mathcal{A}^\dagger_K}$ can be written as a sum

$$\sum_{\substack{0\le i<d \\ -\infty<j<\infty}} a_{ij}x^i y^j dx.$$

We can decompose $\mathcal{A}^\dagger_K$ as

$$\mathcal{A}^\dagger_K = \bigoplus_{l=0}^{r-1} \mathcal{A}^\dagger_l$$

where $\mathcal{A}^\dagger_l$ only includes the terms $a_{ij}x^iy^j$ with $j = -l \pmod r$. This leads to a similar decomposition

$$\Omega^1_{\mathcal{A}^\dagger_K} = \bigoplus_{l=0}^{r-1} \Omega_l. \tag{3.2}$$

Since

$$d(x^iy^j) = ix^{i-1}y^j dx + jy^{j-1}x^i dy = ix^{i-1}y^j dx + \frac{j}{r}f'(x)x^iy^{j-r}dx,$$

therefore the operator d commutes with the decomposition (3.2), and we have a decomposition of cohomology groups

$$H^i_{MW}(\overline{\mathcal{A}}/K) = \bigoplus_{l=0}^{r-1} H^i_{MW}(\overline{\mathcal{A}}/K)^l.$$

To view this in another way, the above is the decomposition into invariant subspaces under the group action of $\mathbb{Z}/r\mathbb{Z}$ on $H^i_{MW}(\overline{\mathcal{A}}/K)$ induced by the automorphishm ρ. Each component corresponds to an eigenspace of ρ with eigenvalue ζ^{-l}, where $\zeta \in \overline{K}$ is an $r-$th root of unity.

Note that since $\mathcal{A}^\dagger_0 = K[x, \dfrac{1}{f}]^\dagger$ is the dagger ring of the coordinate ring of

$$\mathbb{A}^1_K - \{\text{zeroes of } f\},$$

the cohomology of the $l = 0$ part is the cohomology of projective space missing n points. In particular, $H^0_{MW}(\overline{\mathcal{A}}/K)^0 = K$ and $H^1_{MW}(\overline{\mathcal{A}}/K)^0$ is a vector space of dimension n.

We will now focus our attention on the case where $0 < l < r$. Let $S_k = \{i : e_i \geq k\}$. We will assume the set $\{\alpha_i\}$ is ordered so that $S_2 = \{1, 2, ..., m\}$. Define the polynomial $h(x) \in \mathscr{V}[x]$ to be the greatest common divisor of $f(x)$ and $f'(x)$. Then

$$\begin{aligned} h(x) &= \prod_{i=1}^{n} (x - \alpha_i)^{e_i - 1} \\ &= \prod_{k=2}^{e} T_k(x) \end{aligned}$$

where we have defined $T_k(x) = \prod_{i \in S_k} (x - \alpha_i)$ and $e = \max\{e_i\}$.

Remark 3.1.7. In the sections that follow we will regularly use the notation $K[x]_{<d}$ to denote the K-vector space of polynomials with degree strictly less than d.

Define polynomials $u(x) = \dfrac{f(x)}{h(x)} = T_1(x)$ and $v(x) = \dfrac{f'(x)}{h(x)}$. For $i \geq 0$, we can use division with remainder to find polynomials $a_i(x), b_i(x)$ such that

$$x^i v(x) = a_i(x)u(x) + b_i(x)$$

with $\deg(b_i(x)) < n$. Note that $a_0 = 0, b_0 = v(x)$, and the leading term of $a_i(x)$ is $d \cdot x^{i-1}$ for $i \geq 1$. Thus for any positive k, $\{a_i(x)\}_{i=1}^k$ is a basis for $K[x]_{<k}$, the K-module of polynomials of degree less than k. Define

$$\begin{aligned} a_{i,j}(x) &= \frac{j}{r} a_i(x) + i x^{i-1} \\ b_{i,j}(x) &= \frac{j}{r} b_i(x). \end{aligned}$$

Then the leading term of $a_{i,j}(x)$ is $\left(\dfrac{jd + ri}{r}\right) x^{i-1}$ which is nonzero as $(d, r) = 1$ and $d \nmid i$. Therefore $\{a_{i,j}(x)\}_{i=1}^k$ is also a basis for $K[x]_{<k}$ for all integers j.

Consider now the K-vector space homomorphism

$$\hat{v} : K[x] \to \frac{K[x]}{(u(x))}$$

defined by multiplication by $v(x)$. Since $u(x)$ and $v(x)$ have no common roots, $v(x)$ is not a zero divisor in $K[x]/(u(x))$. It follows that a polynomial is in the kernel of $\hat{v}$ if and only if it is divisible by $u(x)$. Therefore $\hat{v}$ induces a K-automorphism of $K[x]/(u(x)) \cong K[x]_{<n}$. Since the image of x^i is $b_i(x)$, it follows that $\{b_i(x)\}_{i=0}^{n-1}$ is a K-basis for $K[x]_{<n}$.

Using this notation, we can write

$$\begin{aligned} d(x^i y^j) &= i x^{i-1} y^j dx + \frac{j}{r} f'(x) x^i y^{j-r} dx \\ &= i x^{i-1} y^j dx + \frac{j}{r} a_i(x) y^j dx + \frac{j}{r} b_i(x) h(x) y^{j-r} dx \\ &= a_{i,j}(x) y^j dx + b_{i,j}(x) h(x) y^{j-r} dx. \end{aligned} \tag{3.3}$$

3.1.4 Some Useful Order-preserving Functions

Definition 3.1.8. Given totally ordered sets $\mathbb{T}_1, ..., \mathbb{T}_k$, define a total order on $\bigoplus_{i=1}^k \mathbb{T}_i$ called the *lexographical order* as follows: For elements $(t_1, ..., t_k), (s_1, ..., s_k) \in \bigoplus_{i=1}^k \mathbb{T}_i$, $(t_1, ..., t_k) < (s_1, ..., s_k)$ if and only if the first coordinates t_i, s_i which are different, from the left, satisfy $t_i < s_i$.

Given the coordinate ring $\mathcal{A}$ from the the previous section and any integer t, we can define a bijective map

$$\mathfrak{u}_\infty^t : \mathbb{Z} \times \{0, 1, ..., d-1\} \to (-dt + r\mathbb{Z})$$

by

$$\begin{aligned} \mathfrak{u}_\infty^t((k, s)) &= -\mathrm{ord}_{P_\infty}(x^s y^{-t+kr}) \\ &= rs + d(-t + kr) \\ &= -dt + r(s + kd) \end{aligned}$$

which is order preserving, where $\mathbb{Z} \times \{0, 1, ..., d-1\}$ is given the lexographical order and

$-dt + r\mathbb{Z}$ is given the natural order inherited from $\mathbb{Z}$. Suppose $A \in \mathcal{A}$ is given by

$$A = \sum_{j \in \mathbb{Z}} \sum_{s=0}^{d-1} \lambda_{s,j} x^s y^j.$$

Let $(j_0, s_0) = \max\{(j, s) : \lambda_{s,j} \neq 0\}$. Define a function $\mathfrak{o}_\infty : \mathcal{A} \to \mathbb{Z}$ by

$$\mathfrak{o}_\infty(A) = -\mathrm{ord}_{P_\infty}(x^{s_0} y^{j_0}).$$

Proposition 3.1.9. *Suppose $A \in \mathcal{A}_l$, given by a sum*

$$A = \sum_{k \in \mathbb{Z}} \sum_{s=0}^{d-1} \lambda_{s,l+kr} x^s y^{-l+kr}.$$

with j_0, s_0 defined as above. Then the expansion of A in the completed local ring at P_∞ has the same leading term as the expansion of $\lambda_{s_0,j_0} x^{s_0} y^{j_0}$. In particular, $\mathfrak{o}_\infty(A) = -ord_{P_\infty}(A)$.

Proof. It suffices to show that $\mathrm{ord}_{P_\infty}(A - \lambda_{s_0,j_0} x^{s_0} y^{j_0}) > \mathrm{ord}_{P_\infty}(\lambda_{s_0,j_0} x^{s_0} y^{j_0})$. Set $k_0 = (j_0 + l)/r$. Every term of $A - \lambda_{s_0,j_0} x^{s_0} y^{j_0}$ is of the form $\lambda_{s,-l+rk} x^s y^{-l+rk}$ with $(k, s) < (k_0, s_0)$. It follows that $\mathfrak{u}^l_\infty((k, s)) < \mathfrak{u}^l_\infty((k_0, s_0))$, which gives

$$\begin{aligned} \mathrm{ord}(\lambda_{s,-l+rk} x^s y^{-l+rk}) &= -\mathfrak{u}^l_\infty((k, s)) \\ &> -\mathfrak{u}^l_\infty((k_0, s_0)) \\ &= \mathrm{ord}_{P_\infty}(\lambda_{s_0,j_0} x^{s_0} y^{j_0}). \end{aligned}$$

The result follows since $\mathrm{ord}_{P_\infty}(A - \lambda_{s_0,j_0} x^{s_0} y^{j_0})$ is bounded by the minimum order of its terms. □

Similarly, for $i = 1, ..., n$, and any integer t, define

$$\mathfrak{u}^t_i : \mathbb{Z} \times \{0, 1, ..., e_i - 1\} \to (-e_i t + r\mathbb{Z})$$

by

$$\begin{aligned} \mathfrak{u}^t_i((k, s)) &= \mathrm{ord}_{P_i}((x - \alpha_i)^s y^{-t+rk}) \\ &= sr + e_i(-t + rk) \\ &= -e_i t + (s + e_i k) r \end{aligned}$$

for $k \in \mathbb{Z}$. Then clearly $\mathfrak{u}_i^t$ is order preserving.

For a polynomial $Q(x) \in K[x]$ of degree less than d, we can write the following partial fraction decomposition

$$\frac{Q(x)}{f(x)} = \sum_{i=1}^{n} \sum_{s=0}^{e_i-1} \frac{Q_{i,s}}{(x-\alpha_i)^{e_i-s}}.$$

for unique constants $Q_{i,s} \in \overline{K}$. Multiplying through by $f(x)$ and defining $f_i(x) = f(x)/(x-\alpha_i)^{e_i}$ we get

$$Q(x) = \sum_{i=1}^{n} \sum_{s=0}^{e_i-1} Q_{i,s}(x-\alpha_i)^s f_i(x). \tag{3.4}$$

Note that if $x - \alpha_i$ divides $Q(x)$ with multiplicity $t \leq e_i$, then the decomposition yields $Q_{i,s} = 0$ for $s = 0, 1, ..., t-1$.

Suppose $A \in \mathcal{A}$. Passing to an extension of K if necessary, by Equation (3.4) we can find constants $A_{i,s,k}$ such that

$$A = \sum_{i=1}^{n} \sum_{j \in \mathbb{Z}} \sum_{s=0}^{e_i} A_{i,s,j}(x-\alpha_i)^s f_i(x) y^j$$

Define $j_0 := \min\{j : A_{i,s,j} \neq 0 \text{ for some } i, s\}$, choose i_0 such that $A_{i_0,s,j_0} \neq 0$ for some s, and put $s_0 = \min\{s : A_{i_0,s,j_0} \neq 0\}$. Define

$$\mathfrak{o}_{i_0}(A) = \mathrm{ord}_{P_{i_0}}((x-\alpha_{i_0})^{s_0} y^{j_0}).$$

Remark 3.1.10. For any $A \in \mathcal{A}$, it is not necessarily true that $\mathfrak{o}_i(A)$ is defined for all i, but if $A \neq 0$ there exists some i such that it is defined.

Proposition 3.1.11. *Fix l, $0 < l < r$. Suppose $A \in \mathcal{A}_l$ is given by a sum*

$$A = \sum_{i=1}^{n} \sum_{k \geq k_0} \sum_{s=0}^{e_i-1} A_{i,s,-l+rk}(x-\alpha_i)^s f_i(x) y^{-l+rk},$$

where j_0, s_0, i_0 are as defined above, and $k_0 = \dfrac{j_0+l}{r}$. Choose positive integers a, b that satisfy $ar - be_{i_0} = 1$, so that $z := (x-\alpha_{i_0})^a y^{-b}$ is a uniformizing parameter at P_{i_0}. Then the terms of order less than $e_{i_0}(r+j_0)$ in the expansions of A and $\sum_{s=s_0}^{e_{i_0}-1} A_{i_0,s,j_0} f_{i_0}(x)^{bs+aj_0+1} z^{sr+j_0 e_{i_0}}$ as series in z in the completed local ring at P_{i_0} are equal. Moreover, $\mathfrak{o}_{i_0}(A) = ord_{P_{i_0}}(A)$.

Proof. To prove $\mathfrak{o}_{i_0}(A) = \mathrm{ord}_{P_{i_0}}(A)$, it is sufficient to prove the inequality

$$\mathrm{ord}_{P_{i_0}}(A - A_{i_0,s_0,j_0}(x-\alpha_{i_0})^{s_0} f_{i_0}(x) y^{j_0}) > \mathrm{ord}_{P_{i_0}}(A_{i_0,s_0,j_0}(x-\alpha_{i_0})^{s_0} f_{i_0}(x) y^{j_0}), \qquad (3.5)$$

from which it follows

$$\begin{aligned} \mathrm{ord}_{P_{i_0}}(A) &= \mathrm{ord}_{P_{i_0}}(A_{i_0,s_0,j_0}(x-\alpha_{i_0})^{s_0} f_{i_0}(x) y^{j_0}) \\ &= \mathrm{ord}_{P_{i_0}}(A_{i_0,s_0,j_0}(x-\alpha_{i_0})^{s_0} y^{j_0}) \\ &= \mathfrak{o}_i(A). \end{aligned}$$

By the minimality conditions used to define the pair (j_0, s_0), it follows that each term in $A - A_{i_0,s_0,j_0}(x-\alpha_{i_0})^{s_0} f_{i_0}(x) y^{j_0}$ has either the form $A_{i_0,s,-l+rk}(x-\alpha_{i_0})^s f_{i_0}(x) y^{-l+rk}$ for $(k,s) > (k_0,s_0)$, or the form $A_{i_1,s,j}(x-\alpha_{i_1})^s f_{i_1}(x) y^j$ for $i_1 \neq i_0$, $j \geq j_0$. For the first type, one can write

$$\begin{aligned} \mathrm{ord}_{P_{i_0}}(A_{i_0,s,-l+rk}(x-\alpha_{i_0})^s f_{i_0}(x) y^{-l+rk}) &\geq \mathrm{ord}_{P_{i_0}}((x-\alpha_{i_0})^s y^{-l+rk}) \\ &= \mathfrak{u}_{i_0}^l((k,s)) \\ &> \mathfrak{u}_{i_0}^l((k_0,s_0)) \\ &= \mathrm{ord}_{P_{i_0}}(A_{i_0,s_0,j_0}(x-\alpha_{i_0})^{s_0} f_{i_0}(x) y^{-l+rk_0}) \end{aligned}$$

where the second inequality comes from the fact that $\mathfrak{o}_{i_0}^l$ is order preserving. For the second type, we can compute

$$\begin{aligned} \mathrm{ord}_{P_{i_0}}(A_{i_1,s,j}(x-\alpha_{i_1})^s f_{i_1}(x) y^j) &= \mathrm{ord}_{P_{i_0}}(A_{i_1,s,j} f_{i_1}(x) y^j) \\ &\geq re_{i_0} + je_{i_0} \\ &\geq (r+j_0)e_{i_0} \\ &> rs_0 + j_0 e_{i_0} \\ &= \mathrm{ord}_{P_{i_0}}(A_{i_0,s_0,j_0}(x-\alpha_{i_0})^{s_0} f_{i_0}(x) y^{-l+rk_0}) \end{aligned}$$

which proves Equation (3.5).

For the main part of the proposition, we follow a similar process. It is clear that each term of

$$A - \sum_{s=s_0}^{e_{i_0}-1} A_{i_0,s,j_0}(x-\alpha_{i_0})^s f_{i_0}(x) y^{j_0}.$$

either has the form $A_{i_0,s,l+rk}(x-\alpha_{i_0})^s f_{i_0}(x) y^{-l+rk}$ where $k > k_0$, or the form $A_{i_1,s,j}(x -$

$\alpha_{i_1})^s f_{i_1}(x)y^j$ where $i_1 \neq i_0$, $j \geq j_0$. We have already seen that the second type has order greater or equal to $e_{i_0}(r+j_0)$ at P_{i_0}. For the first type, we calculate

$$\begin{aligned}\mathrm{ord}_{P_{i_0}}(A_{i_0,s,-l+rk}(x-\alpha_{i_0})^s f_{i_0}(x)y^{-l+rk}) &\geq \mathrm{ord}_{P_{i_0}}(y^{-l+rk}) \\ &= \mathfrak{u}_i^l((k,0)) \\ &= \mathfrak{u}_i^l((k_0+1,0)) \\ &= e_{i_0}(r+j_0).\end{aligned}$$

It follows that

$$\mathrm{ord}_{P_{i_0}}\left(A - \sum_{s=s_0}^{e_{i_0}-1} A_{i_0,s,j_0}(x-\alpha_{i_0})^s f_{i_0}(x)y^{j_0}\right) \geq e_{i_0}(r+j_0) \tag{3.6}$$

which show that the expansions for A and $\sum_{s=s_0}^{e_{i_0}-1} A_{i_0,s,j_0}(x-\alpha_{i_0})^s f_{i_0}(x)y^{j_0}$ in z are equal up to $z^{e_{i_0}(r+j_0)-1}$.

The computations

$$\begin{aligned}\frac{x-\alpha_{i_0}}{z^r} &= (x-\alpha_{i_0})^{1-ar}y^{br} = (x-\alpha_{i_0})^{-be_{i_0}}y^{br} = f_{i_0}(x)^b \\ \frac{y}{z^{e_{i_0}}} &= y^{1+be_{i_0}}(x-\alpha_{i_0})^{-ae_{i_0}} = y^{ar}(x-\alpha_{i_0})^{-ae_{i_0}} = f_{i_0}(x)^a\end{aligned} \tag{3.7}$$

give

$$(x-\alpha_{i_0})^{s_0} f_{i_0}(x)y^{j_0} = f_{i_0}(x)^{bs_0+aj_0+1}z^{rs_0+e_{i_0}j_0},$$

yielding the desired result □

3.2 Computing a Basis for Cohomology

Proposition 3.2.1. *For $0 < l < r$ the classes $[x^i h(x)dx/y^l]$, $0 \leq i \leq n-2$ form a basis for $H^1_{MW}(\overline{\mathcal{A}}/K)^l$.*

The proof of this proposition will be accomplished in several steps. First we will show that these classes generate the de Rham cohomology by giving a reduction algorithm for differentials with finite degree in y. Next, we will calculate a bound for the p-adic precision loss incurred by the algorithm, proving that the classes generate the dagger cohomology. Finally we will prove linear independence.

Using the relations $y^r = f(x)$ and $ry^{r-1}dy = f'(x)dx$, each element in Ω_l^1 can be written in the form

$$\frac{1}{y^l} \sum_{-\infty<k<\infty} \frac{A_k(x)dx}{y^{rk}}$$

where $A_k(x) \in K[x]$ has degree less than d.

3.2.1 The Reduction Process

We will begin by giving a "reduction of poles" procedure on differentials of the form $A(x)y^j dx$ with $\deg(A(x)) < d$, and $j = -l + rk$ with k an integer and $0 \leq l \leq r-1$. To ensure that all reduction steps are performed with coefficients in $\mathscr{V}$, we will assume that $\alpha_i \in K$ for all i such that $e_i > 1$.

To reduce differentials of the form $A(x)y^j dx$, $j > 0$, $\deg(A) < d$, one may write $A(x)$ as a linear combination of the $a_{i,j}(x)$'s, $1 \leq i \leq d$, and use Equation (3.3) to obtain $A(x)y^j dx$ as an exact differential plus a differential of the form $B(x)y^{j-r}dx$. Repeating this process we can write

$$A(x)y^j dx = \widetilde{A}(x)\frac{dx}{y^l} + d\nu$$

for some $0 \leq l < r$, and $\deg(\widetilde{A}) < d$.

To reduce differentials of the form $A(x)\dfrac{dx}{y^j}$, $j > 0$, we can similarly use Equation (3.3), but we must first reduce to the form $B(x)h(x)\dfrac{dx}{y^j}$. One begins with some preliminary computations.

For $i \in S_2$, recall we set $f_i(x) = f(x)(x-\alpha_i)^{-e_i}$. By a straightforward calculation, $f'(x)(x-\alpha_i)^{-e_i+1} = f_i'(x)(x-\alpha_i) + e_i f_i(x)$.

For $0 \leq t \leq e_i - 2$, we have

$$\begin{aligned}
d\left(\frac{f(x)}{(x-\alpha_i)^{e_i-t-1}y^j}\right) &= \left(\frac{f(x)}{(x-\alpha_i)^{e_i-t-1}}\right)'\frac{dx}{y^j} - j\left(\frac{f(x)}{(x-\alpha_i)^{e_i-t-1}}\right)\frac{dy}{y^{j+1}} \\
&= \left(\frac{f'(x)}{(x-\alpha_i)^{e_i-t-1}} - \frac{(e_i-t-1)f(x)}{(x-\alpha_i)^{e_i-t}}\right)\frac{dx}{y^j} - \frac{j}{r}\frac{f(x)(ry^{r-1}dy)}{(x-\alpha_i)^{e_i-t-1}y^{j+r}} \\
&= \left(\frac{f'(x)}{(x-\alpha_i)^{e_i-t-1}} - \frac{(e_i-t-1)f(x)}{(x-\alpha_i)^{e_i-t}}\right)\frac{dx}{y^j} - \frac{j}{r}\frac{f'(x)dx}{(x-\alpha_i)^{e_i-t-1}y^j} \\
&= \left((1-\frac{j}{r})\frac{f'(x)}{(x-\alpha_i)^{e_i-t-1}} - \frac{(e_i-t-1)f(x)}{(x-\alpha_i)^{e_i-t}}\right)\frac{dx}{y^j} \\
&= \Bigg((1-\frac{j}{r})(x-\alpha_i)^t(e_if_i(x)+(x-\alpha_i)f_i'(x)) \\
&\quad -(e_i-t-1)(x-\alpha_i)^tf_i(x)\Bigg)\frac{dx}{y^j} \\
&= \left((t+1-\frac{je_i}{r})(x-\alpha_i)^tf_i(x) + (1-\frac{j}{r})(x-\alpha_i)^{t+1}f_i'(x)\right)\frac{dx}{y^j}
\end{aligned}$$

Thus

$$(x-\alpha_i)^tf_i(x)\frac{dx}{y^j} \equiv c_{i,j,t}(x-\alpha_i)^{t+1}f_i'(x)\frac{dx}{y^j} \tag{3.8}$$

where $c_{i,j,t} = \dfrac{(j-r)}{(r(t+1)-je_i)}$.

Remark 3.2.2. This expression makes sense as the denominator of $c_{i,j,t}$ is nonzero: If $l \neq 0$, then $r(t+1) - je_i \equiv -le_i \pmod{r}$ which is nonzero. If $l = 0$ then $j = rk$ with $k > 0$, so $r(t+1) - je_i = r(t+1-ke_i) < 0$ since $t+1 < e_i$.

Note that for all i, $h(x) = T_2(x)\cdots T_e(x)$ divides $(x-\alpha_i)^{e_i-1}f_i'(x)$, and in general for $1 \leq te_i - 1$ we can write

$$(x-\alpha_i)^tf_i'(x) = T_2(x)T_3(x)\cdots T_{t+1}(x)R_{i,t}(x)$$

for some polynomial $R_{i,t}(x)$.

Let $f^{[1]}(x) := f(x)/T_2(x)$. Using a partial fraction decomposition and the fact that $\deg(A) < d$, we can find constants $A_{i,1}$ and a polynomial $Q^{[1]}(x)$ of degree less than $d-m$ such that

$$\frac{A(x)}{f(x)} = \frac{Q^{[1]}(x)}{f^{[1]}(x)} + \sum_{i=1}^{m}\frac{A_{i,1}}{(x-\alpha_i)^{e_i}}.$$

Multiplying both side of the equation by $f(x)$, one sees that

$$A(x) = Q^{[1]}(x)T_2(x) + \sum_{i=1}^{m} A_{i,1} f_i(x).$$

By Equation (3.8), we therefore have

$$\begin{aligned} A(x)\frac{dx}{y^j} &\equiv Q^{[1]}(x)T_2(x)\frac{dx}{y^j} + \sum_{i=1}^{m} c_{i,j,0}A_{i,1}(x-\alpha_i)f_i'(x)\frac{dx}{y^j} \\ &= T_2(x)\left(Q^{[1]}(x) + \sum_{i=1}^{m} c_{i,j,0}A_{i,1}R_{i,1}(x)\right)\frac{dx}{y^j} \\ &= T_2(x)A^{[1]}(x)\frac{dx}{y^j} \end{aligned}$$

where we have set $A^{[1]}(x) := Q^{[1]}(x) + \sum_{i=1}^{m} c_{i,j,0}A_{i,1}R_{i,1}(x)$. Letting $f^{[2]}(x) := f^{[1]}(x)/T_3(x)$, we begin the same process again by finding a polynomial $Q^{[2]}$ and constants $A_{i,2}$ for $i \in S_3$ such that

$$\frac{A^{[1]}(x)}{f^{[1]}(x)} = \frac{Q^{[2]}(x)}{f^{[2]}(x)} + \sum_{i\in S_3} \frac{A_{i,2}}{(x-\alpha_i)^{e_i-1}}.$$

Multiplying both sides by $f(x)$, one can then write

$$T_2(x)A^{[1]}(x) = T_2(x)T_3(x)Q^{[2]}(x) + \sum_{i\in S_3} A_{i,2}(x-\alpha_i)f_i(x),$$

so that

$$\begin{aligned} T_2(x)A^{[1]}(x)\frac{dx}{y^j} &\equiv T_2(x)T_3(x)Q^{[2]}(x)\frac{dx}{y^j} + \sum_{i\in S_3} c_{i,j,1}A_{i,2}(x-\alpha_i)^2 f_i'(x)\frac{dx}{y^j} \\ &= T_2(x)T_3(x)\left(Q^{[2]}(x) + \sum_{i\in S_3} c_{i,j,1}A_{i,2}R_{i,2}(x)\right)\frac{dx}{y^j} \\ &= T_2(x)T_3(x)A^{[2]}(x)\frac{dx}{y^j} \end{aligned}$$

where we set $A^{[2]}(x) = Q^{[2]}(x) + \sum_{i\in S_3} c_{i,j,1}A_{i,2}R_{i,2}(x)$.

Continuing in this manner, given $A^{[k]}(x)$, in the following manner we can define a polynomial $A^{[k+1]}$ satisfying

$$T_2(x)\cdots T_{k+1}A^{[k]}(x)\frac{dx}{y^j} \equiv T_2(x)\cdots T_{k+2}A^{[k+1]}(x)\frac{dx}{y^j}. \tag{3.9}$$

Define $f^{[k+1]}(x) = f^{[k]}(x)/T_{k+2}(x)$ and for each $i \in S_{k+2}$ find constants $A_{i,k+1}$ and a polynomial $Q^{[k+1]}(x)$ such that

$$\frac{A^{[k]}(x)}{f^{[k]}(x)} = \frac{Q^{[k+1]}(x)}{f^{[k+1]}(x)} + \sum_{i \in S_{k+2}} \frac{A_{i,k+1}}{(x-\alpha_i)^{(e_i-k)}}. \tag{3.10}$$

The values $A_{i,k+1}$ and the polynomial $Q^{[k+1]}(x)$ can be computed using

$$\begin{aligned} A_{i,k+1} &= \frac{A^{[k]}(x)(x-\alpha_i)^{e_i-k}}{f^{[k]}(x)}\Big|_{x=\alpha_i} \\ T_{k+2}(x)Q^{[k+1]}(x) &= A^{[k]}(x) - \sum_{i \in S_{k+2}} A_{i,k+1}\frac{f^{[k]}(x)}{(x-\alpha_i)^{e_i-k}}. \end{aligned} \tag{3.11}$$

After multiplication of Equation (3.10) by $f(x)$ one has

$$\begin{aligned} T_2(x)\cdots T_{k+1}(x)A^{[k]}(x)\frac{dx}{y^j} &= T_2(x)\cdots T_{k+2}(x)Q^{[k+1]}(x)\frac{dx}{y^j} + \sum_{i \in S_{k+2}} A_{i,k+1}(x-\alpha_i)^{k-1}f_i(x)\frac{dx}{y^j} \\ &\equiv T_2(x)\cdots T_{k+2}(x)Q^{[k+1]}(x)\frac{dx}{y^j} + \sum_{i \in S_{k+2}} c_{i,j,k}A_{i,k+1}(x-\alpha_i)^k f_i'(x)\frac{dx}{y^j} \\ &= T_2(x)\cdots T_{k+2}(x)\left(Q^{[k+1]}(x) + \sum_{i \in S_{k+2}} c_{i,j,k}A_{i,k+1}R_{i,k+1}(x)\right)\frac{dx}{y^j} \end{aligned}$$

and we then define $A^{[k+1]}(x) = Q^{[k+1]}(x) + \sum_{i \in S_{k+2}} c_{i,j,k}A_{i,k+1}R_{i,k+1}(x)$. Thus we can eventually compute a polynomial $B(x)$ of degree less than n such that

$$A(x)\frac{dx}{y^j} \equiv h(x)B(x)\frac{dx}{y^j}. \tag{3.12}$$

To reduce the differential $h(x)B(x)\frac{dx}{y^j}$, write $B(x)$ as a linear combination $B(x) = \sum_{i=0}^{n-1} B_i b_{i,r-j}(x)$ so that

$$\begin{aligned} h(x)B(x)\frac{dx}{y^j} &= \sum_{i=0}^{n-1} B_i b_{i,r-j}(x)h(x)\frac{dx}{y^j} \\ &= d\left(\sum_{i=0}^{n-1} B_i \frac{x^i}{y^{j-r}}\right) - \sum_{i=0}^{n-1} B_i a_{i,r-j}(x)\frac{dx}{y^{j-r}}. \end{aligned}$$

Repeating this process we can write any form $\omega = A(x)\frac{dx}{y^j}$ with $j > 0$ as an exact

differential plus a linear combination of the elements $\{\frac{x^i h(x)dx}{y^l}\}_{i=0}^{n-1}$. By subtracting an appropriate multiple of

$$d(y^{r-l}) = (r-l)y^{r-1-l}dy = \left(\frac{r-l}{r}\right)\frac{f'(x)dx}{y^l} = \left(\frac{r-l}{r}\right)\frac{v(x)h(x)dx}{y^l}$$

we can then reduce to a linear combination of the elements $\{\frac{x^i h(x)dx}{y^l}\}_{i=0}^{n-2}$.

In order to reduce differentials to a linear combination of elements $\{\frac{x^i dx}{y^l}\}_{i=0}^{n-2}$, we can use the relation

$$\begin{aligned} dy &= \frac{f'(x)}{ry^{r-1}}dx \\ &= \frac{v(x)}{ru(x)}ydx \end{aligned}$$

and obtain

$$\begin{aligned} d\left(\frac{x^i u(x)}{y^l}\right) &= (ix^{i-1}u(x) + x^i u'(x))\frac{dx}{y^l} - lx^i u(x)\frac{dy}{y^{l+1}} \\ &= \left(ix^{i-1}u(x) + x^i u'(x) - \frac{l}{r}x^i v(x)\right)\frac{dx}{y^l}. \end{aligned}$$

This equation is valid for $i \geq 0$ and has leading term $(i+n-dl/r)x^{i+n-1}\frac{dx}{y^l} \neq 0$. Therefore, appropriate multiples can be subtracted from $A(x)\frac{dx}{y^l}$ to obtain a linear combination of the elements $\{\frac{x^i dx}{y^l}\}_{i=0}^{n-2}$.

We have now shown that both sets $\{[x^i dx/y^l]\}_{i=0}^{n-2}$ and $\{[x^i h(x)dx/y^l]\}_{i=0}^{n-2}$ span the ζ^{-l}-eigenspace of $\mathrm{H}^1_{\mathrm{dR}}(C'_K/K)$. The fact that $\mathrm{H}^1_{\mathrm{dR}}(C'_K/K) \cong \mathrm{H}^1_{\mathrm{MW}}(C'_k/K)$ follows either from the comparison isomorphism (2.3.11), or from the lemmas below, which are an adapted version of [12, Lemma 1 and Lemma 2].

3.2.2 Two Lemmas

Lemma 3.2.3. *Suppose $\omega = A(x)\frac{dx}{y^j} \in \Omega_l$, where $A(x)$ is a polynomial of degree less than d with coefficients in $\mathscr{V}$. Set $e = max\{e_i\}$ and $N = p^{\lfloor \log_p |ej-r| \rfloor}$.*

i) For $j > r$, then there exist $\nu \in \mathcal{A}_l$, $\widetilde{A}(x) \in K[x]_{<n-1}$ such that

$$\omega = \widetilde{A}(x)\frac{dx}{y^l} + d\nu \tag{3.13}$$

and $N\widetilde{A}(x)$ has coefficients in $\mathscr{V}$.

ii) For $j > 0$, there exist $\nu \in \mathcal{A}_l$, $\widetilde{A}(x) \in K[x]_{<n-1}$ such that

$$\omega = \widetilde{A}(x)h(x)\frac{dx}{y^l} + d\nu \tag{3.14}$$

and $N\widetilde{A}(x)$ has coefficients in $\mathscr{V}$.

Proof. *i)* Write $j = kr + l$. By inspection of the reduction algorithm we see that without the conditions of integrality such a ν exists, and that we can write

$$\nu = \frac{R_0(x)u(x)}{y^j} + \sum_{t=1}^{k} \frac{R_t(x)}{y^{j-tr}}$$

for polynomials R_t such that $\deg(R_0) < d - n$, $\deg(R_k) < n$, and $\deg(R_t) < d$ for $1 \leq t \leq k-1$.

We consider the partial fraction decomposition in the same way as Equation (3.4)

$$R_0(x)u(x) = \sum_{i=1}^{n}\sum_{s=0}^{e_i-1} R_{0,i,s}(x-\alpha_i)^s f_i(x).$$

For each i, the linear term $x - \alpha_i$ divides $u(x)$ with multiplicity 1, and we therefore have $R_{0,i,0} = 0$. We can then write

$$\begin{aligned} R_0(x)u(x) &= \sum_{i=1}^{n}\sum_{s=1}^{e_i-1} R_{0,i,s}(x-\alpha_i)^s f_i(x) \\ &= \sum_{i\in S_2}\sum_{s=1}^{e_i-1} R_{0,i,s}(x-\alpha_i)^s f_i(x) \end{aligned} \tag{3.15}$$

Let P_i denote the closed point in C which lies over the point $(\alpha_i, 0)$ in affine space. Then P_i is $\mathbb{F}_{q^e}$-rational for some positive integer e. Set $\mathscr{V}' = W(\mathbb{F}_{q^e})$ and let K' denote its field of fractions. From Proposition (3.1.2) we have $\mathrm{ord}_{P_i}(x-\alpha_i) = r$ and $\mathrm{ord}_{P_i}(y) = e_i$. Since $(e_i, r) = 1$, we can find integers a_i and b_i such that $a_i r - b_i e_i = 1$, and therefore

$z_{(i)} := (x-\alpha_i)^{a_i}/y^{b_i}$ is a uniformizing parameter at P_i. By [51, Chapter VIII.5 Theorem 2], the completion of the local ring of $C/\mathscr{V}'$ at P_i is $\mathscr{V}'[[z_{(i)}]]$.

By Proposition (3.1.11), there exists some i such that for the leading terms up to $z_{(i)}^{e_i(r-j)}$ the local series expansion for ν at P_i is equal to the expansion of

$$\sum_{s=1}^{e_i-1} R_{0,i,s} f_i(x)^{b_i s - a_i j + 1} z_{(i)}^{rs-e_i j}.$$

Since $f_i(x)$ is invertible in the local ring at P_i, one can write the expansions

$$f_i(x)^{b_i s - a_i j + 1} = \sum_{t=0}^{\infty} a_{s,t} z_{(i)}^t \tag{3.16}$$

where $a_{s,t} \in \mathscr{V}'$ and $a_{s,0}$ is a unit. We can therefore write the expansion for ν at P_i as

$$\nu = \sum_{s=1}^{e_i-1} \sum_{t=0}^{\infty} R_{0,i,s} a_{s,t} z_{(i)}^{rs-e_i j+t} + O(z_{(i)}^{(r-j)e_i})$$

and the differential $d\nu$ as

$$d\nu = \sum_{s=1}^{e_i-1} \sum_{t=0}^{\infty} (rs - e_i j + t) R_{0,i,s} a_{s,t} z_{(i)}^{rs-e_i j+t-1} dz_{(i)} + O(z_{(i)}^{(r-j)e_i-1}). \tag{3.17}$$

Since

$$\mathrm{ord}_{z_{(i)}} \left(\frac{\widetilde{A}(x)dx}{y^l} \right) \geq r - 1 - le_i \geq r - 1 - (j-r)e_i,$$

the expansion in Equation (3.17) is equal to local expansion of the right side of (3.13). In the left side of (3.13), the coefficients of the expansion of $A(x)\dfrac{dx}{y^j}$ in the completed local ring at P_i are elements of $\mathscr{V}'$.

In particular we get the following system

$$\begin{aligned}
(r-e_ij)R_{0,i,1}a_{1,0} &\in \mathscr{V}' && (3.18)\\
(2r-e_ij)(R_{0,i,1}a_{1,r}+R_{0,i,2}a_{2,0}) &\in \mathscr{V}' && (3.19)\\
(3r-e_ij)(R_{0,i,1}a_{1,2r}+R_{0,i,2}a_{2,r}+R_{0,i,3}a_{3,0}) &\in \mathscr{V}'\\
&\vdots\\
((e_i-1)r-e_ij)(R_{0,i,1}a_{1,(e_i-2)r}+R_{0,i,2}a_{2,(e_i-3)r}+\ldots+R_{0,i,e_i-1}a_{e_i-1,0}) &\in \mathscr{V}'
\end{aligned}$$

Recalling that $e=\max\{e_i\}$, $N=p^{\lfloor \log_p(ej-r)\rfloor}$, and using the fact that $a_{s,0}$ is a unit for all s, by Equation (3.18) we have $NR_{0,i,1}\in\mathscr{V}$. From Equation (3.19) it then follows that $NR_{0,i,2}\in\mathscr{V}$ and continuing in this way we get $NR_{0,i,s}\in\mathscr{V}$ for $1\leq s\leq e_i-1$. We then move the term

$$d\left(\sum_{s=1}^{e_i-1}R_{0,i,s}(x-\alpha_i)^s f_i(x)y^{-j}\right)$$

to the left-hand side of Equation (3.13) and repeat for other values of $i\in S_2$. Eventually we get that the polynomial $NR_0(x)$ has coefficients in $\mathscr{V}$.

We repeat this process, considering next the equation

$$\omega - d\left(\frac{R_0(x)u(x)}{y^j}\right)=\widetilde{A}(x)\frac{dx}{y^l}+d\left(\frac{R_1(x)}{y^{j-r}}+\sum_{t=2}^{k}\frac{R_t(x)}{y^{j-tr}}\right) \tag{3.20}$$

and the decomposition

$$R_1(x)=\sum_{i=1}^{n}\sum_{s=0}^{e_i-1}R_{1,i,s}(x-\alpha_i)^s f_i(x).$$

Applying Proposition (3.1.11) again, locally at P_i we get

$$\frac{R_1(x)}{y^{j-r}}+\sum_{t=2}^{k}\frac{R_t(x)}{y^{j-tr}}=\sum_{s=0}^{e_i-1}R_{1,i,s}f_i(x)^{b_is-a_i(j-r)+1}z_{(i)}^{rs-e_i(j-r)}+O(z_{(i)}^{-(j-2r)e_i})$$

We follow the same process and for each degree less than $-(j-2r)e_i$ multiply the coefficients of the above expansion by the appropriate power of p so that the corresponding coefficients on both sides of Equation (3.20) are in $\mathscr{V}'$. We then find that $NR_{1,i,s}\in\mathscr{V}'$ for all i,s and thus $R_1(x)\in\mathscr{V}[x]$. Continuing in this way, we see that $NR_t(x)$ has integer coefficients for $t<k$.

For the final step we compute the expansion at P_i of the right side of the equation

$$\omega - d\left(\frac{R_0(x)u(x)}{y^j} + \sum_{t=1}^{k-1} \frac{R_t(x)}{y^{j-tr}}\right) = \widetilde{A}(x)\frac{dx}{y^l} + d\left(\frac{R_k(x)}{y^l}\right). \tag{3.21}$$

Using a partial fraction decomposition of $\dfrac{R_k(x)}{u(x)}$ we can write

$$R_k(x) = \sum_{i=1}^{n} R_{k,i}\left(\frac{u(x)}{x-\alpha_i}\right)$$

so locally at P_i we have

$$\frac{R_k(x)}{y^l} = R_{k,i}\lambda_i z_{(i)}^{-e_i l} + O(z_{(i)}^{-e_i l+1})$$

where

$$\lambda_i = \frac{f(x)^{a_i}u(x)}{x-\alpha_i}\Big|_{x=\alpha_i} = \prod_{i'\neq i}(\alpha_i - \alpha_{i'})^{e_{i'}a_i+1}.$$

This gives

$$d\left(\frac{R_k(x)}{y^l}\right) = -e_i l R_{k,i}\lambda_i z_{(i)}^{-e_i l-1}dz_{(i)} + O(z_{(i)}^{-e_i l})$$

which is equal to the expansion of the expression on the left side of (3.21) since

$$\mathrm{ord}_{P_i}\left(\frac{\widetilde{A}dx}{y^l}\right) \geq \mathrm{ord}_{P_i}(d(x-\alpha_i)) + \mathrm{ord}_{P_i}(y^{-l}) = r - 1 - e_i l > -e_i l.$$

Therefore $NR_{k,i} \in \mathscr{V}'$ for all i, which shows that $NR_k(x) \in \mathscr{V}'[x]$ and completes the proof of the first part of the proposition.

The proof of the second part follows the exact same procedure as in the first, with an added reduction step which gives

$$\nu = \frac{R_0(x)u(x)}{y^j} + \sum_{t=1}^{k} \frac{R_t(x)}{y^{j-tr}} + \frac{R_{k+1}(x)u(x)}{y^l}$$

where R_{k+1} is a polynomial of degree less than $d-n$.

One can write a local expansion at P_i

$$\begin{aligned}\frac{R_{k+1}(x)u(x)}{y^l} &= \sum_{s=1}^{e_i-1} R_{k+1,i,s} f_i(x)^{b_i s - a_i l + 1} z_{(i)}^{rs-e_i l} + O(z_{(i)}^{(r-l)e_i}) \\ &= \sum_{s=1}^{e_i-1}\sum_{t=0}^{\infty} R_{k+1,i,s} a_{s,t} z_{(i)}^{rs-e_i l+t} + O(z_{(i)}^{(r-l)e_i}). \end{aligned} \tag{3.22}$$

such that $a_{s,0}$ is a unit for all s. Since

$$\mathrm{ord}_{P_i}\left(\frac{\widetilde{A}(x)h(x)dx}{y^l}\right) \geq r(e_i-1)+r-1-e_i l = (r-l)e_i - 1,$$

the coefficients of the expansion (3.22) can be compared to the coefficients in the local expansion of

$$\omega - d\left(\frac{R_0(x)u(x)}{y^j} + \sum_{t=1}^{k}\frac{R_t(x)}{y^{j-tr}}\right),$$

which gives $NR_{k+1}(x) \in \mathscr{V}'$ by the procedure from the proof of part one. □

Lemma 3.2.4. *Let $\omega = A(x)y^j dx \in \Omega_l$, where $0 < l < r, j > 0$, and $A(x)$ is a polynomial with coefficients in $\mathscr{V}$ of degree $d' < d$. Set $N = p^{\lfloor \log_p(r(d'+1)+jd)\rfloor}$.*

i) There exists $\nu \in \mathcal{A}_l$, $\widetilde{A}(x) \in K[x]_{<n-1}$ such that

$$\omega = \widetilde{A}(x)\frac{dx}{y^l} + d\nu \tag{3.23}$$

and $N\widetilde{A}(x)$ has coefficients in $\mathscr{V}$.

ii) There exists $\nu \in \mathcal{A}_l$, $\widetilde{A}(x) \in K[x]_{<n-1}$ such that

$$\omega = \widetilde{A}(x)h(x)\frac{dx}{y^l} + d\nu \tag{3.24}$$

and $N\widetilde{A}(x)$ has coefficients in $\mathscr{V}$.

Proof. i) Writing $j = rk - l$, the reduction algorithm gives us Equation (3.23) where

$$\nu = \sum_{t=0}^{d'+1} R_{k,t}x^t y^j + \sum_{s=1}^{k-1}\sum_{t=0}^{d-1} R_{s,t}x^t y^{-l+sr} + \sum_{t=0}^{d-n-1} R_{0,t}x^t u(x) y^{-l}.$$

with $R_{s,t} \in \mathscr{V}$. Consider the completion of the local ring at the closed point at infinity $P_\infty \in \widetilde{C}$. We have $\mathrm{ord}_{P_\infty}(x) = -r$ and $\mathrm{ord}_{P_\infty}(y) = -d$, so we can choose a local parameter

$z = x^a y^{-b}$ where a and b are integers such that $bd - ar = 1$. Recall from section (3.1.4) that the map

$$\mathfrak{u}_\infty^l : \mathbb{Z} \times \{0, ..., d-1\} \to -ld + r\mathbb{Z} \tag{3.25}$$

$$(s,t) \mapsto -\mathrm{ord}_{P_\infty}(x^t y^{-l+sr}), \tag{3.26}$$

computed as $\mathfrak{u}_\infty^l((s,t)) = rt + d(-l+rs) = (t+sd)r - ld$, is order preserving. The term which has the largest pole at P_∞ is thus $R_{k,d'+1}x^{d'+1}y^j$, and we can then write the local expansions

$$\begin{aligned} \nu &= \sum_{i=-\mathfrak{u}_\infty^l((k,d'+1))}^{\infty} a_i z^i \\ d\nu &= \sum_{i=-\mathfrak{u}_\infty^l((k,d'+1))-1}^{\infty} (i+1)a_{i+1}z^i dz \end{aligned}$$

with $a_{-\mathfrak{u}_\infty^l((k,d'+1))} = R_{k,d'+1}$. Since the degree of $\widetilde{A}$ is less than $n-1$, the lowest possible order of the expansion of $\widetilde{A}(x)\dfrac{dx}{y^l}$ at P_∞ is

$$-r - 1 - \mathfrak{u}_\infty^l((0,n-2)) = -1 - \mathfrak{u}_\infty^l((0,n-1))$$

thus the coefficients of z^i in the expansions of $d\nu$ and ω are equal for

$$i < -1 - \mathfrak{u}_\infty^l((0,n-1)). \tag{3.27}$$

Since the expansion for ω is in $\mathscr{V}[[z]]dz$, we have $(i+1)a_{i+1} \in \mathscr{V}$ for all i satisfying Equation (3.27). Letting $N = p^{\lfloor \log_p(r(d'+1)+jd) \rfloor}$, it follows that $Na_i \in \mathscr{V}$ if $-i > \mathfrak{u}_\infty^l((0,n-1))$. In particular, since $(k,d'+1) > (0,n-1)$, therefore $\mathfrak{u}_\infty^l((k,d'+1)) > \mathfrak{u}_\infty^l((0,n-1))$ and it follows that $NR_{k,d'+1} \in \mathscr{V}$.

We repeat this process using the equation

$$\omega - d(R_{d'+1,k}x^{d'+1}y^j) = \widetilde{A}(x)\frac{dx}{y^l} + d(\nu - R_{d'+1,k}x^{d'+1}y^j)$$

and performing the same computation with the next highest term $R_{s',t'}x^{t'}y^{-l+rs'}$ of ν with respect to the lexographical ordering. For any such (s',t') we have $(s',t') > (0,n-1)$, from which it follows that $NR_{s',t'} \in \mathscr{V}$. Repeating this gives the result for part (i).

To prove the part (ii), we follow the same argument as part (i) with

$$\nu = \sum_{t=0}^{d'+1} R_{k,t} x^t y^j + \sum_{s=1}^{k-1} \sum_{t=0}^{d-1} R_{s,t} x^t y^{-l+rs}.$$

and using the fact that the order of $\widetilde{A}(x)h(x)\dfrac{dx}{y^l}$ at P_∞ is at least $-r-1-\mathfrak{u}^l_\infty((0,d-2)) = -1-\mathfrak{u}^l_\infty((0,d-1))$. Since the pairs (s',t') appearing in ν have only $s'>0$, we immediately have $(s',t') > (0,d-1)$, and the result follows by the method used in part (i). □

To complete the proof of Proposition (3.2.1), it suffices to show linear independence of the cohomology classes $[x^i dx/y^l]$.

Proposition 3.2.5. *For l, $0<l<r$, the cohomology classes $\{[x^i dx/y^l]\}$, $0 \le i \le n-2$, form a linearly independent set in the K-vector space $H^1_{MW}(\overline{\mathcal{A}}/K)^l$.*

Proof. We begin with the finite case. Let $\omega = \sum_{i=0}^{n-2} c_i x^i y^{-l} dx$ for some $c_i \in K$, and suppose there exist constants $\lambda_{i,k} \in K$ and integers $k_1 \le k_2$ such that

$$\omega = d\nu = \sum_{k=k_1}^{k_2} \sum_{i=0}^{d-1} d(\lambda_{i,k} x^i y^{kr-l})$$

Again consider the order function $\mathfrak{u}^l_\infty$ from Section (3.1.4). By Proposition (3.1.9), we have

$$\begin{aligned} \mathrm{ord}_{P_\infty}(\omega) &\ge \mathrm{ord}_{P_\infty}(x^{n-2}y^{-l}) + \mathrm{ord}_{P_\infty}(dx) \\ &= -r(n-2) + dl - r - 1 \\ &= -r(n-1) + dl - 1 \\ &= -\mathfrak{u}^l_\infty((0,n-1)) - 1 \end{aligned}$$

We also have

$$\begin{aligned} \mathrm{ord}_{P_\infty}(\nu) &= -\mathfrak{o}_\infty(\nu) \\ &= -\max\{\mathfrak{u}^l_\infty((k,i)) : \lambda_{i,k} \neq 0\}, \end{aligned}$$

so the order of $d\nu = \omega$ at P_∞ is one less than the above expression. Combining these two relations it follows that

$$\max\{\mathfrak{u}^l_\infty((k,i)) : \lambda_{i,k} \neq 0\} \le \mathfrak{u}^l_\infty((0,n-1))$$

i.e. $\lambda_{i,k} = 0$ for $(k,i) \geq (0,n)$. Therefore $k_2 \leq 0$, and $\lambda_{i,0} = 0$ for $i \geq n$.

Write

$$\nu = \sum_{j=k_1}^{0} \sum_{i=0}^{d-1} \lambda_{i,k} x^i y^{kr-l} = \sum_{i=1}^{n} \sum_{k=k_1}^{0} \sum_{s=0}^{e_i-1} a_{i,s,k} (x-\alpha_i)^s f_i(x) y^{-l+rk}$$

for constants $a_{i,s,k} \in \overline{K}$. Let $(k_0, s_0) = \min\{(k,s) : a_{i,s,k} \neq 0 \text{ for some } i\}$. By Proposition (3.1.11) we have, for some i,

$$\mathrm{ord}_{P_i}(\nu) \;\; = \;\; \mathfrak{u}_i^l((k_0, s_0)).$$

We also have

$$\mathrm{ord}_{P_i}(d\nu) = \mathrm{ord}_{P_i}(\omega) \geq -e_i l + r - 1 = \mathfrak{u}_i^l((0,1)) - 1.$$

It then follows that $(k_0, s_0) \geq (0,1)$, which implies $a_{i,s,k} = 0$ for all $(k,s) < (0,1)$. Hence, one can write

$$\begin{aligned} \nu &= \sum_{i \in S_2} \sum_{s=1}^{e_i-1} a_{i,s,0} (x-\alpha_i)^s f_i(x) y^{-l} \\ &= \frac{A(x)u(x)}{y^l} \end{aligned}$$

for some polynomial $A(x)$ with $\deg(A(x)u(x)) < d$. But $\deg(u(x)) = n$, and from the initial calculation we have that $A(x)u(x) = \sum_{i=0}^{n-1} \lambda_{i,0} x^i$. It follows that $A(x) = 0$, so $d\nu = 0$. □

An immediate consequence is that the sets

$$\{\frac{x^i dx}{y^l}\}_{\substack{0 \leq i \leq n-2 \\ 0 < l < r}} \text{ and } \{\frac{x^i h(x) dx}{y^l}\}_{\substack{0 \leq i \leq n-2 \\ 0 < l < r}}$$

form K-bases for $\mathrm{H}^1_{\mathrm{MW}}(\mathcal{A}/K)^-$, a vector space of dimension $(n-1)(r-1)$.

3.3 The Matrix of Frobenius

Following Gaudry and Gürel [16], we can compute a representative for the action of the semi-linear p-power Frobenius automorphism

$$F : H^1_{MW}(\overline{\mathcal{A}}/K) \to H^1_{MW}(\overline{\mathcal{A}}/K)$$

on our selected basis from the previous section. Let $\sigma : \mathscr{V} \to \mathscr{V}$ denote the Witt vector Frobenius automorphism. We can extend it to polynomials by taking $x^\sigma = x^p$, and to differentials by taking $(dx)^\sigma = px^{p-1}dx$. Setting $\Delta(x) = \frac{1}{p}(f(x)^\sigma - f(x)^p)$ we can now extend σ to $\mathcal{A}^\dagger$ by taking

$$\left(\frac{1}{y^l}\right)^\sigma = y^{-lp}\left(1 + \frac{p\Delta}{y^{rp}}\right)^{-l/r} = \sum_{k=0}^{\infty}\binom{-l/r}{k}\frac{p^k\Delta^k}{y^{pl+prk}}$$

where

$$\binom{-l/r}{k} = \frac{(-l/r)(-l/r-1)\cdots(-l/r-k+1)}{k!} \in \mathbb{Z}_p$$

since $(r,p) = 1$. Finally we have

$$\left(\frac{x^i h(x)dx}{y^l}\right)^\sigma = \sum_{k=0}^{\infty}\binom{-l/r}{k}\frac{p^{k+1}x^{pi+p-1}h(x)^\sigma\Delta^k}{y^{pl+prk}}dx. \tag{3.28}$$

For each i and l such that $0 \le i \le n-2$ and $0 < l < r$, the reduction algorithm is applied to a truncation of the above sum, which yields a $(r-1)(n-1) \times (r-1)(n-1)$ matrix M, an approximation of F with respect to the chosen basis. By semilinearity, the matrix for the q-power Frobenius F^a is calculated as $M^{\sigma^{a-1}}M^{\sigma^{a-2}}M\cdots M$.

Remark 3.3.1. The p-power Frobenius σ on a curve C over k is a morphism $C \to C^\sigma$, where the defining polynomial of C^σ is the polynomial for C with its coefficients replaced by their images under σ. One is therefore tempted to only consider a basis for cohomology whose coefficients are fixed by σ. This is unnecessary, since the end result will be the same: Suppose A is the matrix of Frobenius with respect to a basis α whose coefficients are stable under σ. Let B be the Frobenius matrix with respect to some other basis β, and suppose Q changes coordinates from α to β. Then $B = (Q^{-1})^\sigma AQ$, so that

$$\begin{aligned} B^{\sigma^{a-1}}B^{\sigma^{a-2}}\cdots B &= \left((Q^{-1})^{\sigma^a}A^{\sigma^{a-1}}Q^{\sigma^{a-1}}\right)\left((Q^{-1})^{\sigma^{a-1}}A^{\sigma^{a-2}}Q^{\sigma^{a-2}}\right)\cdots(Q^{-1})^\sigma AQ \\ &= Q^{-1}A^{\sigma^{a-1}}A^{\sigma^{a-2}}\cdots AQ. \end{aligned}$$

3.4 Working Within a Crystalline Basis

One technical difficulty with the computations involved in the previous section is that in the general the basis $\{x^i dx/y^l\}$ is not a $\mathscr{V}$-stable lattice of the Frobenius operator, i.e. the matrix M computed above may have p-power denominators. The goal of this section is to find a lower bound for s such that $p^s M$ has entries in $\mathscr{V}$.

Let C be a superelliptic curve over $\mathscr{V}$ of genus g, birationally equivalent to the plane curve defined by the equation $y^r = f(x) = \prod_{i=1}^{n}(x-\alpha_i)^{e_i}$, where f has degree d. As usual we will let C' denote the affine curve minus all points along $y = 0$, and use subscripts k and K to denote special and generic fibres, respectively. By [50, Thm 2.6 and Proposition 3.2], the $\mathscr{V}$-module $\mathrm{H}^1_{\mathrm{dR}}(C/\mathscr{V})$ is a Frobenius-stable lattice in $\mathrm{H}^1_{\mathrm{dR}}(C_K/K)$.

We compare a basis for $\mathrm{H}^1_{\mathrm{dR}}(C/\mathscr{V})$ with our chosen basis. The content of the next few pages is largely based on a proposition by Edixhoven [52, Proposition 5.3.1], the details of which can be found in a paper by van den Bogaart [50].

Let $\mathscr{D}$ denote the relative effective Cartier divisor of degree 1 on C corresponding to the section above infinity and let s be an integer greater than 1. Consider the $\mathscr{V}$-linear map of sheaves on C

$$\mathcal{O}_C((s-1)\mathscr{D}) \xrightarrow{d_s} \Omega^1_{C/\mathscr{V}}(s\mathscr{D})$$

which is just the restriction of the derivation $\mathscr{K}(C) \to \Omega^1_{\mathscr{K}(C)/K}$, where $\mathscr{K}(C)$ denotes the function field of C. Let $\overline{d}_s$ denote the map d_s composed with the projection

$$\Omega^1_{C/\mathscr{V}}(s\mathscr{D}) \to \frac{\Omega^1_{C/\mathscr{V}}(s\mathscr{D})}{\Omega^1_{C/\mathscr{V}}(\mathscr{D})},$$

and denote the cokernel of $\overline{d}_s$ by Υ_s. By construction we have an exact sequence of sheaves of $\mathcal{O}_C$-modules

$$\mathcal{O}_C((s-1)\mathscr{D}) \xrightarrow{\overline{d}_s} \frac{\Omega^1_{C/\mathscr{V}}(s\mathscr{D})}{\Omega^1_{C/\mathscr{V}}(\mathscr{D})} \to \Upsilon_s \to 0. \tag{3.29}$$

Note that the support of $\Omega^1_{C/\mathscr{V}}(s\mathscr{D})/\Omega^1_{C/\mathscr{V}}(\mathscr{D})$ and Υ_s is contained $\mathrm{Supp}\mathscr{D}$. Let P denote the special point of $\mathrm{Supp}\mathscr{D}$. By abuse of notation we will denote by Υ_s both the sheaf as well as its stalk at P.

In some neighbourhood of the support of $\mathscr{D}$, $\mathcal{O}_C(-\mathscr{D})$ is generated over $\mathcal{O}_C$ by an element t. From Bourbaki [51, Chapter VIII.5, Theorem 2], the completion of $\mathcal{O}_{C,P}$ with respect to its local ring is $\mathscr{V}[[t]]$. Therefore the map $\overline{d}_s$ has the local form

$$t^{-(s-1)}\mathscr{V}[[t]] \to \frac{t^{-s}\mathscr{V}[[t]]dt}{t^{-1}\mathscr{V}[[t]]dt} \cong \bigoplus_{i=-s}^{-2} \mathscr{V}\ t^i dt.$$

Since localization and completion are exact, from Equation (3.29) we obtain an exact sequence

$$t^{-(s-1)}\mathscr{V}[[t]] \to \bigoplus_{i=-s}^{-2} \mathscr{V}\ t^i dt \to \widehat{\Upsilon}_s \to 0 \tag{3.30}$$

where $\widehat{\Upsilon}_s$ denotes the completion of Υ_s with respect to its local ring. Therefore $\widehat{\Upsilon}_s$ is finitely generated over $\mathscr{V}$ by elements of Υ_s, so $\widehat{\Upsilon}_s = \Upsilon_s$. The first map in Equation (3.30) is the usual exterior derivative (modulo the ideal (dt/t)), so we can write

$$\begin{aligned} \Upsilon_s &= \bigoplus_{i=-s}^{-2} (\mathscr{V}/(i+1)\mathscr{V})\ t^i dt \\ &= \bigoplus_{\substack{-s<i<0 \\ p|i}} (\mathscr{V}/p^{v_p(i)}\mathscr{V})\ t^{i-1} dt. \end{aligned} \tag{3.31}$$

Let φ_s denote the map

$$\Gamma(C, \Omega^1_{C/\mathscr{V}}(s\mathscr{D})) \to \Upsilon_s.$$

The above discussion shows that $p^{\lfloor \log_p(s-1) \rfloor}\Upsilon_s = 0$, so $\ker \varphi_s$ contains $p^{\lfloor \log_p(s-1) \rfloor}\Gamma(C, \Omega^1_{C/\mathscr{V}}(s\mathscr{D}))$.

It turns out that one can relate $\ker \varphi_s$ to a crystalline basis.

Lemma 3.4.1. *For $s \geq 2g$, there is an isomorphism*

$$\ker \varphi_s / (im\ d_s \cap \ker \varphi_s) \xrightarrow{\sim} H^1_{dR}(C/\mathscr{V}) \tag{3.32}$$

which is equivariant for maps induced by automorphisms of C that map $\mathscr{D}$ to itself.

Proof. See [50, Lemma 3.10] □

Theorem 3.4.2. *Let $s \geq 2g$. There is a surjective map*

$$(\ker \varphi_s)^- \to H^1_{dR}(C/\mathscr{V})$$

Proof. Suppose $v \in \mathrm{H}^1_{\mathrm{dR}}(C/\mathscr{V})$. By Lemma (3.4.1), v lifts to an element $\widetilde{v} \in \ker \varphi_s$. Let ζ be a primitive r-th root of unity. Differentiating the identity $x^r - 1 = \prod_{i=0}^{r-1}(x - \zeta^i)$ and multiplying by x gives

$$rx^r = \sum_{l=0}^{r-1} \prod_{\substack{i=0 \\ i \neq l}}^{r-1} (x - \zeta^i)x.$$

Thus we can write

$$r\widetilde{v} = r\rho^r \cdot \widetilde{v} = \sum_{l=0}^{r-1} \prod_{\substack{i=0 \\ i\neq l}}^{r-1} (\rho - \zeta^i)\rho \cdot \widetilde{v} = (1 + \rho + \cdots + \rho^{r-1}) \cdot \widetilde{v} + \sum_{l=1}^{r-1} \prod_{\substack{i=0 \\ i\neq l}}^{r-1} (\rho - \zeta^i)\rho \cdot \widetilde{v}. \quad (3.33)$$

Now $(1 + \rho + \cdots + \rho^{r-1}) \cdot \widetilde{v} \in (\ker \varphi_s)^0$, so by Proposition (3.1.6) the image of this term in $\mathrm{H}^1_{\mathrm{dR}}(C/\mathscr{V})$ is zero. Therefore $(r - (1 + \rho + \cdots + \rho^{r-1})) \cdot \widetilde{v}$ is mapped to rv.

Each term $\prod_{\substack{i=0 \\ i\neq l}}^{r-1} (\rho - \zeta^i)\rho \cdot \widetilde{v}$ in (3.33) is killed by by $\rho - \zeta^l$, and thus belongs to $(\ker \varphi_s)^l$. Therefore $(r - (1 + \rho + \cdots + \rho^{r-1})) \cdot \widetilde{v} \in (\ker \varphi_s)^-$, which proves that $(\ker \varphi_s)^-$ maps surjectively to $r\mathrm{H}^1_{\mathrm{dR}}(C/\mathscr{V})$. The result follows as r is a unit in $\mathscr{V}$. □

Corollary 3.4.3. *For $s \geq 2g$, the images of $(\ker \varphi_s)^-$ and $H^1_{dR}(C/\mathscr{V})$ in $H^1_{dR}(C'_K/K)$ are equal.*

Proposition 3.4.4. *Fix an integer l with $0 < l < r$, let $s = (d-1)(r-1)$ and as usual let $h(x) = (f(x), f'(x))$. Then*

i) The $\mathscr{V}$-module $\Gamma(C, \Omega^1_{C/\mathscr{V}}(s\mathscr{D}))^l$ contains the $\mathscr{V}$-span of the set

$$\left\{ \frac{x^i h(x) dx}{y^l} \right\}_{i=0}^{n-2},$$

and

ii) the image of the restriction map

$$\Gamma(C, \Omega^1_{C/\mathscr{V}}(s\mathscr{D}))^l \to \Gamma(C', \Omega^1_{C/\mathscr{V}})^l$$

is contained in the $\mathscr{V}$-span of the set

$$\left\{ \frac{x^i dx}{y^l} \right\}_{i=0}^{m_l}$$

where $m_l = \lfloor \frac{d(l+r-1)}{r} - 2 \rfloor$.

Proof. (i) We consider when an element $\omega = \dfrac{x^i h(x) dx}{y^l} \in \Gamma(C', \Omega^1_{C/\mathscr{V}})^l$ can be extended to all of C, with a pole of order at most s along $\mathrm{Supp}\mathscr{D}$.

Let P_i denote the generic point in C lying above $(\alpha_i, 0)$ and let P_∞ denote the generic point above infinity. Recall from Proposition (3.1.2) that we have $\mathrm{ord}_{P_i}(y) =$

$e_i, \mathrm{ord}_{P_\infty}(y) = -d, \mathrm{ord}_{P_i}(x-\alpha_i) = r$, and $\mathrm{ord}_{P_\infty}(x) = -r$. An element $\omega = \dfrac{x^j h(x)dx}{y^l}$ can be extended to $\Omega^1_{C/\mathscr{V}}(s\mathscr{D})$ if $\mathrm{ord}_{P_i}\omega \geq 0$ for each i, and $\mathrm{ord}_{P_\infty}\omega \geq -s$.

For $0 \leq j \leq n-2$ we have

$$\begin{aligned}
\mathrm{ord}_{P_\infty}(\omega) &= (j+d-n)\cdot \mathrm{ord}_{P_\infty}(x) + \mathrm{ord}_{P_\infty}(dx) - l\mathrm{ord}_{P_\infty}(y) \\
&= -r(j+d-n) - r - 1 + ld \\
&\geq -r(n-2+d-n) - r - 1 + d \\
&= -r(d-2) - r + (d-1) \\
&= -(r-1)(d-1) = -s
\end{aligned}$$

and

$$\begin{aligned}
\mathrm{ord}_{P_i}(\omega) &= \mathrm{ord}_{P_i}(x^j) + \mathrm{ord}_{P_i}(h(x)) + \mathrm{ord}_{P_i}(dx) - l\cdot \mathrm{ord}_{P_i}(y) \\
&\geq \mathrm{ord}_{P_i}(h(x)) + r - 1 - le_i \\
&= (e_i - 1)r + r - 1 - le_i \\
&= e_i(r-l) - 1 \geq 0
\end{aligned}$$

which proves part (i). For part (ii), note that an element of $\Gamma(C', \Omega^1_{C/\mathscr{V}})$ can be written

$$\omega = \sum_{L_1 \leq j \leq L_2} A_j(x) y^j dx$$

where $A_j(x) \in \mathscr{V}[x]$ has degree less than $d-1$. An order calculation gives

$$\mathrm{ord}_{P_i}(\omega) \leq \mathrm{ord}_{P_i}(A_{L_1}(x)y^{L_1}dx) = \mathrm{ord}_{P_i}(A_j(x))r + L_1 e_i + r - 1.$$

Since $\sum_{i=1}^n e_i = d$ and $\sum_{i=1}^n \mathrm{ord}_{P_i}(A_{L_1}(x)) < d$, there must be some i such that $e_i > \mathrm{ord}_{P_i}(A_j(x))$. In order for ω to extend to this P_i we must have

$$\begin{aligned}
0 &\leq \mathrm{ord}_{P_i}(\omega) \\
&\leq (e_i - 1)r + L_1 e_i + r - 1 \\
&= e_i r + L_1 e_i - 1,
\end{aligned}$$

which gives

$$L_1 \geq \frac{1 - e_i r}{e_i} > -r.$$

Now if ω extends to $\Gamma(C, \Omega^1_{C/\mathscr{V}}(s\mathscr{D}))$ we must also have $-s \leq \mathrm{ord}_{P_\infty}\omega$, so that

$$-(d-1)(r-1) \leq -L_2 d - \deg(A_{L_2}(x))r - r - 1.$$

In particular $L_2 < r$. For l, $0 < l < r$, let ω_l denote the term in ω whose y-exponent is equal to $-l \bmod r$. Then we have

$$\begin{aligned} \omega_{r-l} &= \frac{A_{-l}(x)dx}{y^l} + A_{r-l}(x)y^{r-l}dx \\ &= \frac{B_l(x)dx}{y^l} \end{aligned}$$

For some polynomial $B_l(x) \in \mathscr{V}[x]$ whose degree satisfies

$$-(d-1)(r-1) \leq ld - \deg(B_l(x))r - r - 1,$$

that is,

$$\deg(B_l(x)) \leq \frac{(d-1)(r-1) + ld - r - 1}{r} = \frac{d(r+l-1)}{r} - 2.$$

□

Corollary 3.4.5. *For fixed l, $0 < l < r$, let V_l denote the $\mathscr{V}$-span of of the differentials $\{\frac{x^i h(x)dx}{y^l}\}_{0 \leq i \leq n-2}$ in $H^1_{dR}(C'_K/K)^l$ and let W_l denote the image of $H^1_{dR}(C/\mathscr{V})^l$ in $H^1_{dR}(C'_K/K)^l$. Set $e = \max\{e_i\}$, $N = \lfloor \log_p((d-1)(r-1)-1) \rfloor$, and put*

$$N_l = \begin{cases} \lfloor \log_p |el - r| \rfloor, & \frac{d(l-1)}{r} < 2 \\ N, & \frac{d(l-1)}{r} \geq 2 \end{cases}.$$

Then

$$p^{N_l} W_l \subset V_l \subset p^{-N} W_l.$$

Proof. By Equation (3.31) and Proposition (3.4.4)(i), the differentials

$$p^N \frac{x^i h(x)dx}{y^l}$$

belong to $(\ker \varphi)^l$. Therefore, by Corollary (3.4.3), $V_l \subset p^{-\lfloor \log_p((d-1)(r-1)-1) \rfloor} W_l$. By Proposition (3.4.4)$(ii)$, $(\ker \varphi)^l$ is contained in the $\mathscr{V}$-span of $\frac{x^i dx}{y^l}$, for $0 \leq i \leq \lfloor \frac{d(l+r-1)}{r} - 2 \rfloor$. If $A(x)$ is a polynomial of degree less than $\lfloor \frac{d(l+r-1)}{r} - 2 \rfloor$ with coefficients in $\mathscr{V}$, then

using division with remainder we can write

$$\frac{A(x)dx}{y^l} = \frac{B_1(x)dx}{y^l} + B_2(x)y^{r-l}dx$$

with $B_1(x), B_2(x) \in \mathscr{V}[x]$ where $B_1(x)$ is a polynomial of degree less than d. If $\frac{d(l-1)}{r} - 2 \geq 0$, then $B_2(x)$ is a polynomial with degree less than or equal to $\frac{d(l-1)}{r} - 2$. Otherwise $B_2(x) = 0$.

By Lemma (3.2.3) (ii) and Lemma (3.2.4) (ii), and using the computation

$$r\left(\frac{d(l-1)}{r} - 2 + 1\right) + (r-l)d = (d-1)(r-1) - 1,$$

it follows that there exist exact differentials $d\nu_1, d\nu_2$, and polynomials $\widetilde{B}_1(x), \widetilde{B}_2(x) \in \mathscr{V}[x]$ of degree less than $n-1$ such that $p^{\lfloor \log_p((d-1)(r-1)-1)\rfloor}\frac{B_2(x)dx}{y^l} = \frac{\widetilde{B}_2(x)h(x)dx}{y^l} + d\nu_1$ and $p^{\lfloor \log_p |el-r|\rfloor}\frac{B_1(x)dx}{y^l} = \frac{\widetilde{B}_1(x)h(x)dx}{y^l} + d\nu_2$. Since $e \leq d$ and $l \leq r-1$, it follows that $|el-r| \leq (d-1)(r-1)-1$, hence the image of $p^N\frac{A(x)dx}{y^l}$ lies in V_l. □

Let M_p, M_q denote the $(r-1)(n-1) \times (r-1)(n-1)$ matrices of the p-power and q-power Frobenius maps, respectively,

$$F_p, F_q : \mathrm{H}^1_{MW}(C'_k/K)^- \to \mathrm{H}^1_{MW}(C'_k/K)^-$$

with respect to the basis $\left\{\frac{x^i h(x)dx}{y^l}\right\}, 0 \leq i \leq n-2, 0 < l < r$.

Let $M_{p,l}$ denote the $(n-1) \times (n-1)$ submatrix of M_p defined by restricting the domain of F_p to $\mathrm{H}^1_{MW}(C'_k/K)^l$.

Theorem 3.4.6. *Let N and N_l be as defined in Corollary (3.4.5). Fix $0 < l < r$, and let l_p be the unique integer such that $0 < l_p < r$ and $l_p \equiv lp \pmod r$. Then*

i) the matrix $p^{N+N_{l_p}}M_{p,l}$ has entries in $\mathscr{V}$

ii) the matrix $p^{2N}M_p$ has entries in $\mathscr{V}$

iii) if $\widetilde{M}$ is an approximation of the matrix M_p, correct to precision $p^{N'}$ for some integer $N' \geq 4N$, then the matrix $\widetilde{M}^{\sigma^{a-1}}\widetilde{M}^{\sigma^{a-2}}\cdots\widetilde{M}$ is an approximation of M_q, correct to precision $p^{N'-4N}$.

Proof. For each l', $0 < l' < r$, let $\mathcal{B}_{l'}$ denote the set $\left\{\frac{x^i h(x)dx}{y^{l'}}\right\}_{i=0}^{n-2}$, and put $\mathcal{B} = \mathcal{B}_1 \cup \cdots \cup \mathcal{B}_{r-1}$. Additionally, let $H_{l'}$ denote a $\mathscr{V}$-bases for $\mathrm{H}^1_{dR}(C/\mathscr{V})^{l'}$ and put $H = H_1 \cup \cdots H_{r-1}$. By Proposition (3.1.6), $\mathrm{H}^1_{dR}(C/\mathscr{V})$ can be viewed as a Frobenius equivariant $\mathscr{V}$-lattice in $\mathrm{H}^1_{MW}(C'_k/K)$, so let $Q_{l'}$ denote the change of basis matrix from $H_{l'}$ to $\mathcal{B}_{l'}$ and let Q denote the change of basis matrix from H to $\mathcal{B}$. Then $M_{p,l} = Q_{l_p} A_l Q_l^{-1}$ and $M_p = QAQ^{-1}$ for certain matrices A_l, A with entries in $\mathscr{V}$. By Corollary (3.4.5), Q_{l_p} has entries in $p^{-N_{l_p}}\mathscr{V}$, and the matrices Q_l^{-1} and Q^{-1} have entries in $p^{-N}\mathscr{V}$, so part (i) follows immediately. Using the fact that $|el - r| \leq (d-1)(r-1) - 1$, so that $N_l \leq N$ for each l, we have that Q has entries in $p^{-N}\mathscr{V}$, and part (ii) follows.

The matrix $\widetilde{A} = Q^{-1}\widetilde{M}Q$ is an approximation of A, with

$$\widetilde{A} \equiv A \mod p^{N'-2N}.$$

The entries of $\widetilde{A}$ are therefore in $\mathscr{V}$, and thus

$$Q\widetilde{A}^{\sigma^{a-1}}\widetilde{A}^{\sigma^{a-2}}\cdots\widetilde{A}^{\sigma}Q^{-1} \equiv QA^{\sigma^{a-1}}A^{\sigma^{a-2}}\cdots AQ^{-1} \mod p^{N'-4N}.$$

The right side of this equation is the matrix of the q-power Frobenius with respect to the basis $\mathcal{B}$. We can assume H and $\mathcal{B}$ are chosen such that the matrix Q has entries in $\mathbb{Q}_p$. Therefore one can write

$$\begin{aligned}\widetilde{M}^{\sigma^{a-1}}\cdots\widetilde{M} &= (Q\widetilde{A}^{\sigma^{a-1}}Q^{-1})(Q\widetilde{A}^{\sigma^{a-2}}Q^{-1})\cdots(Q\widetilde{A}Q^{-1}) \\ &= Q\widetilde{A}^{\sigma^{a-1}}\widetilde{A}^{\sigma^{a-2}}\cdots\widetilde{A}Q^{-1},\end{aligned}$$

from which part (iii) follows. □

3.5 p-Adic Precision Analysis

By the Weil conjectures [4, Appx C], the numerator of the zeta function of C_k can be written

$$P(T) = \prod_{i=1}^{2g}(1 - \mu_i T) = \sum_{i=0}^{2g} a_i T^i \in \mathbb{Z}[T]$$

where $|\mu_i| = q^{1/2}$ for all i and g is the genus of C_k. Furthermore, we can order the μ_i's such that $\mu_{g+i} = q/\mu_i$ for $i = 1, .., g$.

Let $\mathfrak{I}_k$ denote the subsets of $\{1, ..., 2g\}$ of length k. For $I = (j_1, ..., j_k) \in \mathfrak{I}_k$, write $\mu_I = \mu_{j_1} \cdots \mu_{j_k}$. Then for each $1 \leq i \leq 2g$, we can write

$$\begin{aligned} a_i &= (-1)^i \sum_{I \in \mathfrak{I}_i} \mu_I \\ &= (-1)^i \sum_{I \in \mathfrak{I}_i} \frac{q^g}{\mu_{\{1,...,2g\} \setminus I}} \\ &= (-1)^i q^g \sum_{I \in \mathfrak{I}_{2g-i}} \frac{1}{\mu_I} \\ &= (-1)^i q^g \sum_{I \in \mathfrak{I}_{2g-i}} \frac{1}{q^{2g-i}} \mu_I \\ &= q^{i-g} a_{2g-i}. \end{aligned} \tag{3.34}$$

Therefore the polynomial $P(T)$ can be obtained by computing each a_i for $1 \leq i \leq g$. For each a_i, we have

$$|a_i| \leq \binom{2g}{i} q^{i/2} \leq \binom{2g}{g} q^{i/2},$$

which gives $|a_i| \leq \binom{2g}{g} q^{g/2}$ for $1 \leq i \leq g$.

We also have that

$$P(T) = \det(1 - qTF^{-1} | \mathrm{H}^1_{\mathrm{dR}}(C_k/K))$$

so if we define $Q(T) := T^{2g} P(1/T)$, then $Q(T)$ is the characteristic polynomial of qF^{-1}, whose eigenvalues are therefore the μ_i's. It follows that the set $\{q/\mu_i\} = \{\mu_i\}$ are the eigenvalues of F, so that $Q(T)$ is in fact the characteristic polynomial of F.

Each a_i is therefore a polynomial with integer coefficients over the entries of the q-power Frobenius matrix, thus our calculations for the matrix of F should be correct with p-adic precision at least p^{N_1}, where $N_1 := \lceil \log_p \left(2\binom{2g}{g} q^{g/2} \right) \rceil$. In order to ensure that no p-adic denominators arise in our calculation, we can appeal to Theorem (3.4.6), which gives that the denominators of the p-power Frobenius with respect to the basis $\{\frac{x^i h(x) dx}{y^l}\}$ are cleared upon multiplication by p^{N_2}, where $N_2 := 2\lfloor \log_p((d-1)(r-1)-1) \rfloor$. To ensure the correct precision of the q-power Frobenius, by the same theorem, we must increase the precision by p^{2N_2}. Therefore we must compute the matrix of $p^{N_2}F$ with accuracy up

to $p^{N_1+3N_2}$.

By Equation (3.28), the k-th term in the expansion of $F(p^{N_2}\frac{x^i h(x)dx}{y^l})$ is divisible by p^{k+N_2}, and by Lemma (3.2.3) the coefficients of its reduction are divisible by $p^{k+N_2-\lfloor \log_p(ep(l+r(k-1))-r)\rfloor}$ where $e = \max\{e_i\}$. Therefore it is sufficient to calculate the first N_3 terms with

$$N_3 + N_2 - \lfloor \log_p(ep(l + r(N_3 - 1)) - r)\rfloor \geq N_1 + 3N_2$$

and all calculations should be performed in $\mathscr{V}/p^{N_3+N_2}\mathscr{V}$. If we express Equation (3.28) as y^{-pl} multiplied by a polynomial in $\tau := y^{-r}$, we then are only required to compute this polynomial modulo τ^{pN_3}.

Chapter 4

Nodal Curves in $\mathbb{P}^2$

We now present an algorithm for computing the zeta function of a nodal plane curve in two dimensional projective space, by working on its affine complement. We begin with a discussion of hypersurfaces embedded in n-dimensional projective space.

4.1 Cohomology of the Affine Complement of a Hypersurface in $\mathbb{P}^n$

In this section the field K can denote any field of characteristic 0. We suppose $V \subset \mathbb{P}^n_K$ is a hypersurface defined by a homogeneous polynomial $f \in K[X_0, ..., X_n]$ of degree d, and set $U = \mathbb{P}^n_K \setminus V$. Then U is a smooth, affine variety, with coordinate ring

$$A = \{\frac{g}{f^s} : s \geq 0, g \in K[X_0, ..., X_n] \text{ is homogeneous of degree } ds\}.$$

Since U is affine of dimension n, its de Rham cohomology $\mathrm{H}^i_{\mathrm{dR}}(U)$ vanishes for $i > n$, and can be calculated as the cohomology of the de Rham complex

$$0 \to A \xrightarrow{d} \Omega^1_A \xrightarrow{d} \cdots \Omega^n_A \to 0.$$

The elements of Ω^k_A can be represented by a rational differential form on $\mathbb{A}^{n+1}_K$ with poles along V, that is,

$$\omega = \frac{1}{f(X)^s} \sum A_J(X) dX_J,$$

where we have used the shorthand notation $X = (X_0, X_1, ..., X_n)$, $J = (j_1, ..., j_k)$, $dX_J = dX_{j_1} \wedge \cdots dX_{j_k}$ and the sum runs over k-tuples $0 \leq j_1 < \cdots < j_k \leq n$. By the definition of the exterior derivative d, if one sets the degree of dX_i to be 1, then d preserves degrees,

so the $A_J(X)$'s can be taken to be homogeneous polynomials with $\deg A_J = ds - k$. To give a criterium that is sufficient to know when ω comes from Ω_A^k, it is convenient to define the Euler contraction operator Δ.

Definition 4.1.1. Let Δ denote the map on rational forms over $\mathbb{A}_K^{n+1}$, sending k-forms to rational $(k-1)$-forms, and satisfying the following properties:

$$\text{i)} \quad \Delta\left(\frac{1}{B(X)}\sum A_J(X)dX_J\right) = \frac{1}{B(X)}\sum A_J(X)\Delta(dX_J)$$

$$\text{ii)} \quad \Delta(dX_J) = \sum_{i=1}^{k}(-1)^{i-1}X_{j_i}dX_{j_1}\wedge\cdots\wedge\widehat{dX_{j_i}}\wedge\cdots dX_{j_k}$$

One can then show [35, Proposition 2.2] that ω comes from Ω_A^k if and only if $\Delta(\omega) = 0$. Additionally, Δ is exact [35, Lemma 2.8], from which it then follows that any element $\omega \in \Omega_A^k$ can be written

$$\begin{aligned}\omega &= \frac{1}{f(X)^s}\sum A_J(X)\Delta(dX_J)\\ &= \frac{1}{f(X)^s}\sum A_J(X)\sum_{i=1}^{k+1}(-1)^{i-1}X_{j_i}dX_{j_1}\wedge\cdots\wedge\widehat{dX_{j_i}}\wedge\cdots dX_{j_k}\end{aligned}$$

where the first sum runs over subsets J of size $k+1$, and $A_J(X)$ is a homogeneous polynomial of degree $sd-k-1$. In particular, all elements of Ω_A^n have the form

$$\omega = \frac{G}{f^s}\Omega$$

where G is a homogeneous polynomial of degree $sd-n-1$, and

$$\Omega = \sum_{i=0}^{n}(-1)^i X_i dX_0\wedge\cdots\wedge\widehat{dX_i}\wedge\cdots\wedge dX_n.$$

To calculate exact differentials in Ω_A^n, consider the subvariety $U' \subset U$ obtained by removing points along the hyperplane $X_0 = 0$. Then the coordinate ring of U' can be written in affine coordinates $x_i := X_i/X_0, i = 1,...,n$. Using the notation $x = (x_1,...,x_n)$ and $f(1,x) = f(1,x_1,...,x_n)$, one can write an element $\omega \in \Omega_{U'}^{n-1}$ as

$$\omega = \frac{1}{f(1,x)^s}\sum_{i=1}^{n}A_i(x)dx_1\wedge\cdots\wedge\widehat{dx_i}\wedge\cdots\wedge dx_n$$

for arbitrary polynomials $A_i(x)$, so that

$$\begin{aligned} d\omega &= \sum_{i=1}^{n} \frac{\partial}{\partial x_i}\left(\frac{A_i(x)}{f(1,x)^s}\right) dx_i \wedge dx_1 \wedge \cdots \wedge \widehat{dx_i} \wedge \cdots \wedge dx_n \\ &= \sum_{i=1}^{n} (-1)^{i-1} \frac{\partial}{\partial x_i}\left(\frac{A_i(x)}{f(1,x)^s}\right) dx_1 \wedge \cdots \wedge dx_n. \end{aligned}$$

By direct computation one has

$$\begin{aligned} dx_1 \wedge \cdots \wedge dx_n &= \frac{1}{X_0^{2n}}(X_0 dX_1 - X_1 dX_0) \wedge \cdots \wedge (X_0 dX_n - X_n dX_0) \\ &= \frac{1}{X_0^n} dX_1 \wedge \cdots \wedge dX_n \\ &\quad - \frac{1}{X_0^{n+1}} \sum_{i=1}^{n} X_i dX_1 \wedge \cdots \wedge dX_{i-1} \wedge dX_0 \wedge dX_{i+1} \wedge \cdots \wedge dX_n \\ &= \frac{1}{X_0^{n+1}} \Omega \end{aligned}$$

so that

$$\begin{aligned} d\omega &= \sum_{i=1}^{n} (-1)^{i-1} \frac{\partial}{\partial x_i}\left(\frac{A_i(x)}{f(1,x)^s}\right) \frac{1}{X_0^{n+1}} \Omega \\ &= \sum_{i=1}^{n} (-1)^{i-1} X_0 \frac{\partial}{\partial X_i}\left(\frac{A_i(X_1/X_0, ..., X_n/X_0)}{f(1, X_1/X_0, ..., X_n/X_0)^s}\right) \frac{1}{X_0^{n+1}} \Omega \\ &= \sum_{i=1}^{n} (-1)^{i-1} \frac{\partial}{\partial X_i}\left(\frac{X_0^{sd-n} A_i(X_1/X_0, ..., X_n/X_0)}{f(X)^s}\right) \Omega \end{aligned}$$

Since $A_i(x)$ can be chosen arbitrarily, it follows that exact differentials in Ω_A^n are combinations of elements of the form $\frac{\partial}{\partial X_i}(G/f^s)\Omega$ for G a homogeneous polynomial of degree $sd-n$, and thus the n-th de Rham cohomology group of of U can be written

$$\frac{\Omega_A^n}{d\Omega_A^{n-1}} = \frac{\mathrm{Span}_K\left\{\frac{G}{f^s}\Omega : \ G \text{ is homogeneous of degree } sd-n-1, s \geq 1\right\}}{\mathrm{Span}_K\left\{\frac{\partial(G/f^s)}{\partial X_i}\Omega : 0 \leq i \leq n, s \geq 1, \ G \text{ is homogeneous of degree } sd-n\right\}}.$$

The following theorem of Dimca gives two important pieces of information regarding representatives for cohomology classes in the complement of a hypersurface.

Theorem 4.1.2. *Let S be the singular locus of V. Then*

(i) any cohomology class in $H^n_{dR}(U)$ can be represented by a meromorphic differential form of the type

$$\omega = \frac{G(X)}{f(X)^n}\Omega$$

for some polynomial $G(X)$;

(ii) for $i < n - \dim S$, any exact form $\omega = \frac{1}{f(X)^s}\sum_{|J|=i} A_J(X)dX_J \in \Omega^i_A$ can be written

$$\omega = d\left(\frac{1}{f(X)^{s-1}}\sum_{|J|=i-1} B_J(X)dX_J\right)$$

for some polynomials $B_J(X)$;

(iii) there is a positive constant $k = k(V)$ such that any exact form $\omega = \frac{1}{f(X)^s}\sum_{|J|=i} A_J(X)dX_J$ can be written

$$\omega = d\left(\frac{1}{f(X)^{s+(i+1)k}}\sum_{|J|=i-1} B_J(X)dX_J\right)$$

for some polynomials $B_J(X)$.

Proof. See [36], Theorem B, as well as the paragraph following Theorem A. □

Dimca also offers the following conjecture that the constant $k(V)$ depends only on the dimension of the ambient space.

Conjecture 4.1.3. *Any exact form $\omega = \frac{1}{f(X)^s}\sum_{|J|=i} A_J(X)dX_J$ can be written*

$$\omega = d\left(\frac{1}{f(X)^{s+n}}\sum_{|J|=i-1} B_J(X)dX_J\right)$$

for some polynomials $B_J(X)$.

Assuming the validity of the conjecture, we obtain an algorithm to compute a basis for $\mathrm{H}^n_{\mathrm{dR}}(U)$ and a "reduction of poles" procedure. We simply need to compute a basis for the quotient of certain finitely generated K-vector spaces. Namely, set

$$\begin{aligned} Z_s &:= \mathrm{Span}_K\left\{\frac{G}{f^s} : G \text{ is homogeneous of degree } sd-n-1\right\} \\ B_s &:= \mathrm{Span}_K\left\{\frac{\partial(G/f^s)}{\partial W} : W \in \{X,Y,Z\}, G \text{ is homogeneous of degree } sd-n\right\}. \end{aligned}$$

Then by 4.1.2, we have for $s \geq n$,

$$\mathrm{H}^n_{\mathrm{dR}}(U) \cong \frac{Z_s}{Z_s \cap B_{s+n}}.$$

This procedure for computing cohomology is not so explicit, however. In the nonsingular case, one use Gröebner basis techniques from the partial derivatives of f to write any differential as the sum of an exact differential and a differential with lower pole order. In the singular case this does not work, since for any fixed pole order there will necessarily be exact differentials which cannot be written as a polynomial combination of the partial derivatives of f.

Though the constant $k(V)$ seems difficult to find for a general variety, in the case of a reduced curve embedded in $\mathbb{P}^2_K$ one can take $k(V) = 1$ [36, Example 3]. In addition, from the following proposition we see that if the curve is irreducible, then the only "interesting" de Rham cohomology group of the complement is $\mathrm{H}^2_{\mathrm{dR}}(U)$.

Proposition 4.1.4. *Suppose C is a reduced curve in $\mathbb{P}^2_K$ of degree d with isolated singularities. Let Σ denote the singular points of C, $U = \mathbb{P}^2_K \setminus C$, and let $m = \#\Sigma$. Then $H^0_{dR}(U) = K$, and $H^1_{dR}(U)$ has dimension $r - 1$ over K, where r is the number of irreducible components of C. If Σ consists of ordinary multiple points with multiplicities $k_1, ..., k_m$, then $H^2_{dR}(U)$ has dimension $(d-1)(d-2)+r-1-\sum_{i=1}^m (k_i-1)^2$. In particular, if C is an irreducible nodal curve, then $\dim_K H^2_{dR}(U) = (d-1)(d-2) - m$.*

Proof. Since cohomological dimension is preserved by flat base extension, we may assume that K is algebraically closed. Let $\mathbb{P}^* = \mathbb{P}^2_K \setminus \Sigma$ and $C^* = C \setminus \Sigma$. The Gysin sequence (Theorem (2.4.1)) for the pair $(\mathbb{P}^*, C^*)$ gives a long exact sequence

$$\cdots \to \mathrm{H}^k_{\mathrm{dR}}(\mathbb{P}^*) \to \mathrm{H}^k_{\mathrm{dR}}(U) \to \mathrm{H}^{k-1}_{\mathrm{dR}}(C^*) \to \mathrm{H}^{k+1}_{\mathrm{dR}}(\mathbb{P}^*) \to \cdots \tag{4.1}$$

which immediately shows there is an isomorphism $\mathrm{H}^0_{\mathrm{dR}}(\mathbb{P}^*) \cong \mathrm{H}^0_{\mathrm{dR}}(U)$. By affineness of U, $\mathrm{H}^3_{\mathrm{dR}}(U) = 0$, and using the fact that $\mathrm{H}^k_{\mathrm{dR}}(\mathbb{P}^*) \to \mathrm{H}^k_{\mathrm{dR}}(U)$ is trivial for $k = 1$ or 2 (see [53, Ch. 6, Ex. 3.9 (ii)]) gives us short exact sequences

$$0 \to \mathrm{H}^1_{\mathrm{dR}}(U) \to \mathrm{H}^0_{\mathrm{dR}}(C^*) \to \mathrm{H}^2_{\mathrm{dR}}(\mathbb{P}^*) \to 0$$
$$0 \to \mathrm{H}^2_{\mathrm{dR}}(U) \to \mathrm{H}^1_{\mathrm{dR}}(C^*) \to \mathrm{H}^3_{\mathrm{dR}}(\mathbb{P}^*) \to 0.$$

The Gysin sequence for the pair $(\mathbb{P}^2_K, \Sigma)$ gives an exact sequence

$$\cdots \to \mathrm{H}^k_{\mathrm{dR}}(\mathbb{P}^2_K) \to \mathrm{H}^k_{\mathrm{dR}}(\mathbb{P}^*) \to \mathrm{H}^{k-3}_{\mathrm{dR}}(\Sigma) \to \mathrm{H}^{k+1}_{\mathrm{dR}}(\mathbb{P}^2_K) \to \cdots \tag{4.2}$$

which shows that $\mathrm{H}^k_{\mathrm{dR}}(\mathbb{P}^*) \cong \mathrm{H}^k_{\mathrm{dR}}(\mathbb{P}^2_K)$ for $0 \leq k \leq 2$. Additionally, using the fact that $\mathrm{H}^3_{\mathrm{dR}}(\mathbb{P}^2_K) = \mathrm{H}^4_{\mathrm{dR}}(\mathbb{P}^*) = 0$, we obtain a short exact sequence

$$0 \to \mathrm{H}^3_{\mathrm{dR}}(\mathbb{P}^*) \to \mathrm{H}^0_{\mathrm{dR}}(\Sigma) \to \mathrm{H}^4_{\mathrm{dR}}(\mathbb{P}^2_K) \to 0.$$

Assembling this information, have

$$\begin{aligned}
\dim_K \mathrm{H}^0_{\mathrm{dR}}(U) &= \dim_K \mathrm{H}^0_{\mathrm{dR}}(\mathbb{P}^2_K) = 1, \\
\dim_K \mathrm{H}^1_{\mathrm{dR}}(U) &= \dim \mathrm{H}^0_{\mathrm{dR}}(C^*) - 1, \\
\dim_K \mathrm{H}^2_{\mathrm{dR}}(U) &= \dim \mathrm{H}^1_{\mathrm{dR}}(C^*) - \dim \mathrm{H}^3_{\mathrm{dR}}(\mathbb{P}^*) \\
&= \dim \mathrm{H}^1_{\mathrm{dR}}(C^*) - \dim \mathrm{H}^0_{\mathrm{dR}}(\Sigma) + \dim \mathrm{H}^4_{\mathrm{dR}}(\mathbb{P}^2_K) \\
&= \dim \mathrm{H}^1_{\mathrm{dR}}(C^*) - m + 1.
\end{aligned}$$

Therefore the dimension of $\mathrm{H}^1_{\mathrm{dR}}(U)$ is equal to one less than the number of connected components of $C \setminus \Sigma$, which is one less than the number of irreducible components of C. It remains to calculate the dimension of $\mathrm{H}^1_{\mathrm{dR}}(C^*)$. Denote by $\widetilde{C} \to C$ the nonsingular model of C. If $P \in \Sigma$ is ordinary with multiplicity k, then there are k points in $\widetilde{C}$ lying above Σ. Recalling that the genus g of $\widetilde{C}$ is $\dfrac{(d-1)(d-2)}{2} - \sum \dfrac{k_i(k_i-1)}{2}$, we have

$$\begin{aligned}
\dim_K \mathrm{H}^0_{\mathrm{dR}}(C^*) - \dim_K \mathrm{H}^1_{\mathrm{dR}}(C^*) &= \chi(C^*) \\
&= \chi(\widetilde{C} \setminus \{\sum_{i=1}^m k_i \text{ points}\}) \\
&= 2 - 2g - \sum_{i=1}^m k_i \\
&= 2 - (d-1)(d-2) + \sum_{i=1}^m k_i(k_i - 2).
\end{aligned}$$

Since $\dim_K \mathrm{H}^0_{\mathrm{dR}}(C^*) = r$, therefore $\dim \mathrm{H}^1_{\mathrm{dR}}(C^*) = (d-1)(d-2) + r - 2 - \sum_{i=1}^m k_i(k_i-2)$, so finally we obtain

$$\dim_K \mathrm{H}^2_{\mathrm{dR}}(U) = (d-1)(d-2) + r - 2 - \sum_{i=1}^m k_i(k_i-2) - (m-1)$$

which gives the result. □

4.2 Basic Properties of Nodal Curves

We now restrict our attention to the study of nodal curves in $\mathbb{P}^2$. Let C_k be a reduced, irreducible, plane curve over the field $k = \mathbb{F}_q$ whose singular points over the algebraic closure $\overline{k}$ are nodes. That is, the singularities of C_k are of multiplicity 2 and have distinct tangent directions. Suppose C_k is defined by an irreducible homogeneous polynomial $\overline{f} \in k[X, Y, Z]$ of degree d. If Σ_k is the singular locus of C_k and $m = \#\Sigma_k$, then we know (e.g. [37, 8.3, Proposition 5]) that the genus of the nonsingular model of C_k (i.e. the geometric genus of C_k) is

$$g = \frac{(d-1)(d-2)}{2} - m.$$

Computing the zeta function of C_k is clearly equivalent to computing the zeta function of its complement U_k in $\mathbb{P}^2_k$. Since U_k is smooth and affine, its zeta function $Z(U_k; T)$ can be recovered from the induced action of Frobenius on $\mathrm{H}^i_{\mathrm{MW}}(U_k/K)$.

4.2.1 Computing a Lift

Suppose $f \in \mathscr{V}[X, Y, Z]$ is a homogeneous polynomial with reduction modulo p equal to $\overline{f}$. Then f defines a scheme $C \to \mathrm{Spec}(V)$ whose fibre over the special point of $\mathrm{Spec}(V)$ can be identified with C_k. Let C_K denote the fibre over the generic point of $\mathscr{V}$.

For a point $P \in C_K$, there exist elements $X_0, Y_0, Z_0 \in \mathscr{V}$ such that P can be represented as the triple (X_0, Y_0, Z_0), and at least one of X_0, Y_0, Z_0 is a unit. One can define a map

$$\begin{aligned} \rho_C : \ C_K &\to C_k \\ P &\mapsto \overline{P} = (\overline{X}_0, \overline{Y}_0, \overline{Z}_0) \end{aligned}$$

sending P to the point $(X_0 \mod p, Y_0 \mod p, Z_0 \mod p)$.

Proposition 4.2.1. *If $\overline{P} \in C_k$ is non-singular, then $\rho_C^{-1}(\overline{P})$ contains only non-singular points. If $\overline{P}$ is a node, then $\rho_C^{-1}(\overline{P})$ contains at most one node.*

Proof. Without loss of generality we can assume $\overline{Z}_0 = 1$. Define $\overline{f}_0(X, Y) := \overline{f}(X, Y, 1)$ and $f_0(X, Y) := f(X, Y, 1)$. Suppose that $\overline{P}$ is non-singular and $Q \in \rho_C^{-1}(\overline{P})$. On the

affine subscheme of $\mathbb{P}^2_K$ defined by $Z = 1$, let $J(Q)$ denote the Jacobian matrix evaluated Q, that is

$$J(Q) = \left[\frac{df_0}{dX}(Q), \frac{df_0}{dY}(Q)\right].$$

This matrix, modulo p, is equal to $[\frac{d\overline{f}_0}{dX}(\overline{P}), \frac{d\overline{f}_0}{dY}(\overline{P})]$ which has rank 1 since $\overline{P}$ is non-singular. Therefore $J(Q)$ has rank 1, so Q is non-singular in C_K.

Suppose now that $\overline{P}$ is a node and $Q = (X_0, Y_0, 1) \in \rho_C^{-1}(\overline{P})$ is singular. After a change of variables, we can assume $\overline{P} = (0, 0, 1)$, and $f_0 = XY + h$, where each term of $h \in \mathscr{V}[X, Y]$ either has degree greater than 2 or is divisible by p. The Hessian matrix of f_0 at Q is

$$\begin{bmatrix} \frac{d^2h}{dX^2}(Q) & 1 + \frac{d^2h}{dXdY}(Q) \\ 1 + \frac{d^2h}{dXdY}(Q) & \frac{d^2h}{dY^2}(Q) \end{bmatrix} = \begin{bmatrix} a_1 & 1 + a_2 \\ 1 + a_3 & a_4 \end{bmatrix}$$

where $a_i \in p\mathscr{V}$ for each i. Therefore the determinant of the Hessian is in $1 + p\mathscr{V}$, and therefore a unit, hence Q is a node. By a version of Hensel's lemma [54, Chapter III.4.5, Corollary 2], it follows that there exists a unique pair $Q' = (X_0', Y_0') \in \mathscr{V}^2$ such that $Q' \equiv (0, 0) \mod p$, and $\frac{df_0}{dX}(Q') = \frac{df_0}{dY}(Q') = 0$. Since the pair (X_0, Y_0) satisfy the same properties, we must have that $X_0 = X_0'$ and $Y_0 = Y_0'$. Therefore Q is unique. □

Corollary 4.2.2. *C_K is a K-curve whose singularities consist of at most m nodes corresponding to a subset of nodes in C_k.*

Definition 4.2.3. Suppose $\overline{f} \in k[X, Y, Z]$ is a homogeneous polynomial of degree d, defining a nodal curve $C_k \subset \mathbb{P}^2_k$. Suppose $f \in \mathscr{V}[X, Y, Z]$ is a homogeneous polynomial of degree d whose coefficients module $p\mathscr{V}$ are equal to the coefficients of $\overline{f}$. Let C denote the corresponding $\mathscr{V}$-scheme, and C_K the fibre over the generic point of $\mathrm{Spec}(\mathscr{V})$. We will say f is an *equisingular lift* of $\overline{f}$ if for each node $\overline{P} \in C_k$ there a unique node $P \in \rho_C(\overline{P})$. We will call f a *finite equisingular lift* if f is an equisingular lift of $\overline{f}$, and additionally the coefficients of f are in $\mathscr{V}_{\mathrm{fin}}$.

Proposition 4.2.4. *Let $\overline{f} \in k[X, Y, Z]$ be a homogeneous irreducible polynomial defining a nodal curve C_k. Then there exists an equisingular lift of $\overline{f}$.*

Proof. Suppose $P_1, ..., P_m$ are the nodes of C_k. From the paragraph after Proposition 1.5 of a paper by Deligne and Mumford [55], it is shown that there exists a scheme $\mathscr{C}$, proper and flat over $\mathrm{Spec}(\mathscr{V}[[t_1, ..., t_m]])$, such that $\mathscr{C} \times \mathrm{Spec}(k) \cong C_k$, and in the completed local

rings one has

$$\widehat{\mathcal{O}}_{P_i,\mathscr{C}} \cong \frac{\mathscr{V}[[x,y,t_1,...,t_m]]}{(xy-t_i)}.$$

An equisingular lift of $\overline{f}$ is the defining polynomial of the fibre of $\mathscr{C}$ at $t_1 = t_2 = \cdots = t_m = 0$. □

We can compute an equisingular lift of a polynomial $\overline{f}$ up to precision p^N as follows. Let $\mathcal{M}_d$ be the set of monomials in X, Y, Z of degree d. For each monomial $M \in \mathcal{M}_d$ define a parameter c_M, and put $F = \sum_{M\in\mathcal{M}_d} c_M M$. Let f be any lift of $\overline{f}$ to $\mathscr{V}[X,Y,Z]$, and let $P_1,...,P_m$ be lifts of the nodal points of $\overline{f}$. One can then consider the system of equations in the variables $\{c_M\}_{M\in\mathcal{M}_d}$ and with coefficients in the ring $\mathscr{V}/p^{N-1}\mathscr{V}$, defined by

$$\begin{aligned} \frac{\partial F}{\partial X}(P_i) &= \frac{1}{p}\frac{\partial f}{\partial X}(P_i) \\ \frac{\partial F}{\partial Y}(P_i) &= \frac{1}{p}\frac{\partial f}{\partial Y}(P_i) \\ \frac{\partial F}{\partial Z}(P_i) &= \frac{1}{p}\frac{\partial f}{\partial Z}(P_i) \end{aligned} \tag{4.3}$$

where one interprets c/p to mean an element $b \in \mathscr{V}/p^{N-1}\mathscr{V}$ such that $pb = c$. Any solution of this system yields an approximation $\widetilde{f} := f - pF$ of an equisingular lift of $\overline{f}$.

In general, a finite equisingular lift will not exist, however, one can construct such a lift explicitly provided that the number of singularities of $\overline{f}$ is sufficiently small.

Proposition 4.2.5. *For $p \neq 2$, suppose $\overline{f} \in k[X,Y,Z]$ is homogeneous of degree d with $(p,d) = 1$, defining a reduced curve C_k with m nodes, rational over k, and possessing no other singularities. If $m \leq \dfrac{d+1}{2}$, then there exists a finite equisingular lift of $\overline{f}$.*

Proof. We will prove the proposition by constructing an equisingular lift of $\overline{f}$ explicitly. Let f be any lift of $\overline{f}$ to a homogeneous polynomial of degree d with coefficients in $\mathscr{V}_{\text{fin}}$. Let $\overline{P}_i = (\overline{X}_i, \overline{Y}_i, \overline{Z}_i) \in \mathbb{P}^2_k, i = 1,...,m$ denote the distinct singular points of the curve C_k, and for each i, lift $\overline{P}_i$ to a $\mathscr{V}_{\text{fin}}$-triple $P_i = (X_i, Y_i, Z_i)$. Since the partial derivatives

of f vanish modulo p at each P_i, we can define elements $a_i, b_i, c_i, \in \mathscr{V}_{\text{fin}}$ by

$$\begin{aligned} a_i &= \frac{1}{p}\frac{df}{dX}(X_i, Y_i, Z_i) \\ b_i &= \frac{1}{p}\frac{df}{dY}(X_i, Y_i, Z_i) \\ c_i &= \frac{1}{p}\frac{df}{dZ}(X_i, Y_i, Z_i) \end{aligned}$$

Suppose $F \in \mathscr{V}_{\text{fin}}[X, Y, Z]$ is homogeneous of degree d, and satisfies $\frac{dF}{dX}(X_i, Y_i, Z_i) = a_i, \frac{dF}{dY}(X_i, Y_i, Z_i) = b_i, \frac{dF}{dZ}(X_i, Y_i, Z_i) = c_i$ for all i. Then the polynomial $f - pF$ is a lift of $\overline{f}$, whose partial derivatives are zero at each P_i. By Corollary (4.2.2), $f - pF$ is a rational equisingular lift of $\overline{f}$. The method is to construct the polynomial F using a Lagrange interpolation-type approach.

To find a suitable polynomial F, it suffices to construct, for each point P_i, homogeneous polynomials $F_{i,X}, F_{i,Y}$, and $F_{i,Z}$ of degree d with coefficients in $\mathscr{V}_{\text{fin}}$, satisfying the following conditions:

1. $\frac{\partial F_{i,X}}{\partial X}(P_i) = \frac{\partial F_{i,Y}}{\partial Y}(P_i) = \frac{\partial F_{i,Z}}{\partial Z}(P_i) = 1$
2. $\frac{\partial F_{i,W}}{\partial W}(P_j) = 0$ for all other choices $W \in \{X, Y, Z\}$, $j \in \{1, ..., m\}$.

Assuming this is possible, one could write

$$F := \sum_{i=1}^{m} a_i F_{i,X} + b_i F_{i,Y} + c_i F_{i,Z}$$

satisfying the conditions for F. Therefore the task is to construct suitable polynomials $F_{i,X}, F_{i,Y}, F_{i,Z}$. Without loss of generality we can assume $i = 1$ and $P_1 = (X_1, Y_1, 1)$. We first will show that one can reduce to the case $P_1 = (0, 0, 1)$. Consider the linear transformation of the projective plane

$$\begin{aligned} X &\mapsto X - X_0 Z \\ Y &\mapsto Y - Y_0 Z \\ Z &\mapsto Z, \end{aligned}$$

under which the points $P_1, ..., P_m$ get mapped to some points $Q_1, ..., Q_m$, with $Q_1 = (0, 0, 1)$. Assuming that one could construct polynomials $G_{1,X}, G_{1,Y}, G_{1,Z}$ satisfying the

above properties for $Q_1, ..., Q_m$, it follows that for any elements $a, b, c \in \mathscr{V}$, the polynomial $G_{a,b,c}(X, Y, Z) := aG_{1,X} + bG_{1,Y} + cG_{1,Z}$ satisfies $\partial G_{a,b,c}/\partial X(Q_1) = a$, $\partial G_{a,b,c}/\partial Y(Q_1) = b$, $\partial G_{a,b,c}/\partial Z(Q_1) = c$, and $\partial G_{a,b,c}/\partial W(Q_j) = 0$ for all $W \in \{X, Y, Z\}$ and $j \neq i$. Now define

$$F_{a,b,c}(X, Y, Z) := G_{a,b,c}(X + X_0 Z, Y + Y_0 Z, Z)$$

and note that for $j = 1, ..., m$ we have

$$\begin{aligned}
\frac{\partial F_{a,b,c}}{\partial X}(P_j) &= \frac{\partial G_{a,b,c}}{\partial X}(Q_j) \\
\frac{\partial F_{a,b,c}}{\partial Y}(P_j) &= \frac{\partial G_{a,b,c}}{\partial Y}(Q_j) \\
\frac{\partial F_{a,b,c}}{\partial Z}(P_j) &= X_0 \frac{\partial G_{a,b,c}}{\partial X}(Q_j) + Y_0 \frac{\partial G_{a,b,c}}{\partial Y}(Q_j) + \frac{\partial G_{a,b,c}}{\partial Z}(Q_j).
\end{aligned}$$

The partial derivatives of $F_{a,b,c}$ at P_j therefore vanish for all $j \neq 1$, and one also has

$$\begin{bmatrix} \partial F_{a,b,c}/\partial X(P_1) \\ \partial F_{a,b,c}/\partial Y(P_1) \\ \partial F_{a,b,c}/\partial Z(P_1) \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ X_0 & Y_0 & 1 \end{bmatrix} \begin{bmatrix} a \\ b \\ c \end{bmatrix}.$$

Since the 3×3 matrix above is invertible, there exist choices for a, b, c such that $F_{a,b,c}$ satisfies the criteria for each of $F_{1,X}, F_{1,Y}$, and $F_{1,Z}$ at the points $P_1, ..., P_m$.

It remains to show that, under the conditions of the proposition, it is possible to construct $F_{1,X}, F_{1,Y}$, and $F_{1,Z}$ when $P_1 = (0, 0, 1)$, so for the remainder of the proof we will fix $P_1 = (0, 0, 1)$.

Claim For each $j \neq 1$, there exists a homogeneous polynomial $G_j \in \mathscr{V}_{\text{fin}}[X, Y, Z]$ of degree 2, with $G_j(P_1) = 1$, and $\dfrac{dG_j}{dX}(P_j) = \dfrac{dG_j}{dY}(P_j) = \dfrac{dG_j}{dZ}(P_j) = G_j(P_j) = 0$.

Proof of Claim. Write $G_j = Z^2 + aX^2 + bY^2 + cZX + dZY + eXY$. Since G_j is homogeneous, the vanishing of its partial derivatives at P_j will immediately give $G_j(P_j) = 0$, so we may ignore this condition. The conditions of the claim give a systems of equations over $\mathscr{V}_{\text{fin}}$

$$\begin{bmatrix} 2X_j & 0 & Z_j & 0 & Y_j \\ 0 & 2Y_j & 0 & Z_j & X_j \\ 0 & 0 & X_j & Y_j & 0 \end{bmatrix} \begin{bmatrix} a \\ b \\ c \\ d \\ e \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ -2Z_j \end{bmatrix}$$

If either X_j or Y_j is a unit modulo p, then the matrix on the left has rank 3 modulo p (since $p \neq 2$), so there exists a solution in $\mathscr{V}_{\text{fin}}$. Otherwise, $P_j \equiv P_1 \mod p$, which is impossible since $\overline{P}_j$ and $\overline{P}_1$ are distinct points, proving the claim.

With G_j given from the claim for each $j \neq 1$, define a homogeneous polynomial of degree $d-1$

$$G = Z^{d-2m+1} \prod_{j=2}^{m} G_j.$$

Then the polynomial

$$F_{1,Z} := \frac{1}{d}\left(Z - \frac{\partial G}{\partial X}(P_1)X - \frac{\partial G}{\partial Y}(P_1)Y\right)G = \frac{1}{d}Z^d + ...$$

satisfies the required conditions, since clearly its partial derivatives vanish at P_j for each $j \neq 1$, and

$$\begin{aligned}
\frac{\partial F_{1,Z}}{\partial Z}(P_1) &= 1 \\
\frac{\partial F_{1,Z}}{\partial X}(P_1) &= \frac{1}{d}\left(-\frac{\partial G}{\partial X}(P_1)G(P_1) + \frac{\partial G}{\partial X}(P_1)\right) = 0 \\
\frac{\partial F_{1,Z}}{\partial Y}(P_1) &= \frac{1}{d}\left(-\frac{\partial G}{\partial Y}(P_1)G(P_1) + \frac{\partial G}{\partial Y}(P_1)\right) = 0.
\end{aligned}$$

Defining $F_{1,X}$ and $F_{1,Y}$ to be XG and YG, respectively, it is immediate that these polynomials also satisfy the required criteria. □

If f is an equisingular lift of $\overline{f}$, then f defines a relative reduced normal crossings divisor $C \subset \mathbb{P}^2_{\mathscr{V}}$. Let U denote the complement of C in $\mathbb{P}^2_{\mathscr{V}}$, so that the special fibre of U can be identified with U_k. Then from Theorem (2.3.11), there is an isomorphism

$$\mathrm{H}^i_{\text{rig}}(U_k) \cong \mathrm{H}^i_{\text{dR}}(U_K)$$

which is natural in the sense that the de Rham cohomology inherits a Frobenius automorphism.

4.2.2 The Zeta Function of a Nodal Curve

To calculate the zeta function of a k-curve C_k in $\mathbb{P}^2_k$, it suffices to calculate the zeta function of its affine complement U_k, since

$$Z(U_k/k;T)Z(C_k/k;T) = Z(\mathbb{P}^2_k;T) = \frac{1}{(1-T)(1-qT)(1-q^2T)}.$$

Let $\overline{A}$ denote the coordinate ring of U_k, and let $N_a(\overline{A})$ denote the number of $\mathbb{F}_{q^a}$-homomorphisms $\overline{A} \to \mathbb{F}_{q^a}$. Then $\#U_k/\mathbb{F}_{q^a}$, the number of $\mathbb{F}_{q^a}$-rational points on U_k is equal to $N_a(\overline{A})$. The Lefschetz trace formula reads [56, Theorem 4.1]

$$\begin{aligned} N_a(\overline{A}) &= \sum_{i=0}^{2}(-1)^i \mathrm{Tr}(q^{2a}F_*^{-a}|\mathrm{H}^i_{\mathrm{MW}}(\overline{A}/K)) \\ &= q^{2a} - \mathrm{Tr}(q^{2a}F_*^{-a}|\mathrm{H}^1_{\mathrm{MW}}(\overline{A}/K)) + \mathrm{Tr}(q^{2a}F_*^{-a}|\mathrm{H}^2_{\mathrm{MW}}(\overline{A}/K)). \end{aligned}$$

We therefore have

$$\begin{aligned} Z(U_k/k;T) &= \exp\left(\sum_{l=1}^{\infty} \#U_k/\mathbb{F}_{q^l}\frac{T^l}{l}\right) \\ &= \exp\left(\sum_{a=1}^{\infty}(q^{2a} - \mathrm{Tr}(q^{2a}F_*^{-a}|\mathrm{H}^1_{\mathrm{MW}}(\overline{A}/K)) + \mathrm{Tr}(q^{2a}F_*^{-a}|\mathrm{H}^2_{\mathrm{MW}}(\overline{A}/K)))\frac{T^a}{a}\right). \end{aligned}$$

By Lemma (1.0.3) we can write

$$\exp\left(\sum_{a=1}^{\infty}\mathrm{Tr}(q^{2a}F_*^{-a}|\mathrm{H}^i_{\mathrm{MW}}(\overline{A}/K))\frac{T^a}{a}\right) = \det(1 - q^{2a}F_*^{-1}T|\mathrm{H}^i_{\mathrm{MW}}(\overline{A}/K))^{-1}$$

and obtain

$$Z(U_k/k;T) = \frac{P_1(T)}{(1-q^2T)P_2(T)}$$

where $P_i(T) := \det(1 - q^2F_*^{-1}T|\mathrm{H}^i_{\mathrm{MW}}(\overline{A}/K))$.

Suppose now that C_k is a reduced, irreducible, nodal curve of degree d with m singularities. We then have by Proposition (4.1.4) that $P_1 = 1$ and therefore we can write

$$Z(C_k/k;T) = \frac{P(T)}{(1-T)(1-qT)}$$

where $P(T) = \det(1 - q^2F_*^{-1}T|\mathrm{H}^2_{\mathrm{MW}}(\overline{A}/K)) \in 1 + \mathbb{Z}[T]$ is a polynomial of degree $(d -$

$1)(d-2)-m$.

Now the normalization $\widetilde{C}_k$ is a smooth, projective curve over k of genus $g = \frac{(d-1)(d-2)}{2} - m$, and its zeta function has the form

$$Z(C_k/k;t) = \frac{\widetilde{P}(t)}{(1-t)(1-qt)}$$

where $\widetilde{P}(T) \in \mathbb{Z}[T]$ is a polynomial of the form $c_0 + c_1T + c_2T^2 + \cdots + c_{2g}T^{2g}$ whose roots $\alpha_1, ..., \alpha_{2g}$ satisfy $\alpha_j\alpha_{g+j} = 1/q$ for $j = 1, ..., g$, each α_j has complex absolute value $q^{-1/2}$, and $c_{2g-i} = q^{g-i}c_i$ (see Section (3.5)).

Proposition 4.2.6. *$P(T) = \widetilde{P}(T)h(T)$ where $h(T) \in \mathbb{Z}[T]$ is a polynomial of degree m of the form*

$$h(t) = \prod_{i=1}^{k}(1 + \lambda_i T^{r_i})$$

where $r_1, ..., r_k$ are positive integers and $\lambda_i \in \{1, -1\}$.

Proof. Suppose $C_k/\overline{\mathbb{F}}_q$ has a node at a point Q, and r is the smallest integer such that Q is defined over $\mathbb{F}_{q^r}$. Then Q has r conjugates lying in $C_k/\mathbb{F}_{q^r}$ by applying the q-power Frobenius map to the coordinates of Q. Suppose C_k has no other singularities. There is a Zariski-open set around Q such that C satisfies a polynomial equation $Ax^2 + Bxy + Cy^2 + g(x, y)$ with coefficients in $\mathbb{F}_{q^r}$, and where Q corresponds to the point $(0, 0)$. Let $\delta \in \overline{F}_q$ be a square root of $B^2 - 4AC$.

case 1. $\delta \in \mathbb{F}_{q^r}$

In this case, the tangent directions at Q (and all its conjugates) are defined over $\mathbb{F}_{q^r}$, and each conjugate blows up to two points in $\widetilde{C_k}/\mathbb{F}_{q^r}$. We then have

$$\#\widetilde{C_k}/\mathbb{F}_{q^s} = \begin{cases} \#C_k/\mathbb{F}_{q^s} + r, & r \mid s \\ \#C_k/\mathbb{F}_{q^s}, & r \nmid s \end{cases}$$

Hence,

$$\begin{aligned} \frac{Z(\widetilde{C_k}/k;T)}{Z(C_k/k;t)} &= \exp\left(r\sum_{k=1}^{\infty}\frac{T^{rk}}{rk}\right) \\ &= \frac{1}{1-T^r} \end{aligned}$$

case 2. $\delta \notin \mathbb{F}_{q^r}$

In this case there is no point lying above any of the conjugates in $\widetilde{C}_k/\mathbb{F}_{q^r}$. Since δ satisfies a quadratic equation over $\mathbb{F}_{q^r}$, it follows that $\delta \in \mathbb{F}_{q^{2r}}$, and we have

$$\#\widetilde{C_k}/\mathbb{F}_{q^s} = \begin{cases} \#C_k/\mathbb{F}_{q^s} + r, & 2r \mid s \\ \#C_k/\mathbb{F}_{q^s} - r, & r \mid s, 2r \nmid s \\ \#C_k/\mathbb{F}_{q^s}, & r \nmid s \end{cases}$$

It then follows that

$$\begin{aligned} \frac{Z(\widetilde{C_k}/k;T)}{Z(C_k/k;T)} &= \exp\left(r\sum_{k=1}^{\infty}(-1)^k\frac{T^{rk}}{rk}\right) \\ &= \frac{1}{1+T^r} \end{aligned}$$

The case of other nodes defined over other extensions of $\mathbb{F}_q$ follows immediately. □

In light of the proof of Proposition (4.2.6), finding the polynomial $h(T)$ is computationally easy. Then, in order to calculate $\tilde{P}(T)$, one needs only to calculate the first $g+1$ coefficients of $P(T)h(T)$ via the following algorithm. Put

$$\begin{aligned} P(T) &= 1 + a_1T + \cdots + a_{2g+m}T^{2g+m} \\ h(T) &= 1 + b_1T + \cdots + b_mT^m. \end{aligned}$$

If we define $b_i = 0$ for $i > m$, then the coefficients $c_1, ..., c_g$ of $\tilde{P}(T) = 1+c_1T+\cdots+c_{2g}T^{2g}$ can be computed from the linear system

$$\begin{aligned} c_1 &= a_1 - b_1 \\ c_2 &= a_2 - c_1b_1 - b_2 \\ &\vdots \\ c_g &= a_g - c_{g-1}b_1 - c_{g-1}b_2 - \cdots - b_k. \end{aligned}$$

One can then calculate the other coefficients of $\tilde{P}(T)$ through the equality $c_{2g-i} = q^{g-i}c_i$ from the functional equation for $\tilde{C}_k$.

4.3 A Crystalline Lattice of the Affine Complement

Suppose that C is a relative reduced normal crossings divisor on $\mathbb{P}^2_{\mathscr{V}}$. That is, étale-locally on $\mathbb{P}^2_{\mathscr{V}}$, C can be identified with an open subset of the coordinate axes. Then the fibres C_K and C_k are nodal curves lying in the projective plane. Let $\Sigma \subset C$ denote the set of singular $\mathscr{V}$-valued points of C, and let $m = \#\Sigma$. Let $\rho : \widetilde{C} \to C$ be the normalization of C, so that $\widetilde{C}$ is a smooth $\mathscr{V}$-curve with two points lying above each point in Σ. We will also define $U = \mathbb{P}^2_{\mathscr{V}} \setminus C$. Let $i : C \to \mathbb{P}^2_{\mathscr{V}}$, $i_2 : \Sigma \to \mathbb{P}^2_{\mathscr{V}}$ and $j : U \to \mathbb{P}^2_{\mathscr{V}}$ denote the inclusion maps, and put $i_1 = i \circ \rho$.

Associated to the pairs $(\mathbb{P}^2_{\mathscr{V}}, C)$ and $(\mathbb{P}^2_K, C_K)$ are the log-de-Rham complexes $\Omega^\bullet_{(\mathbb{P}^2_{\mathscr{V}}, C)}$ and $\Omega^\bullet_{(\mathbb{P}^2_K, C_K)}$ with a natural isomorphism of hypercohomology

$$\mathrm{H}^i_{\mathrm{dR}}((\mathbb{P}^2_{\mathscr{V}}, C)/\mathscr{V}) \otimes_{\mathscr{V}} K \cong \mathrm{H}^i_{\mathrm{dR}}((\mathbb{P}^2_K, C_K)/K)$$

induced by the map $\Omega^\bullet_{(\mathbb{P}^2_{\mathscr{V}}, C)} \otimes_{\mathscr{V}} K \to \Omega^\bullet_{(\mathbb{P}^2_K, C_K)}$.

From [18, Corollary 2.2.6] the inclusion $\Omega^\bullet_{(\mathbb{P}^2_K, C_K)} \to j_* \Omega^\bullet_{U_K}$ induces an isomorphism of K-vector spaces

$$\mathrm{H}^i_{\mathrm{dR}}((\mathbb{P}^2_K, C_K)/K) \to \mathrm{H}^i_{\mathrm{dR}}(U_K),$$

therefore we can view $\mathrm{H}^i_{\mathrm{dR}}((\mathbb{P}^2_{\mathscr{V}}, C)/\mathscr{V})$ as a $\mathscr{V}$-lattice inside $\mathrm{H}^i_{\mathrm{dR}}(U_K)$.

From Theorem (2.3.11), $\mathrm{H}^i_{\mathrm{dR}}(U_K)$ inherits a Frobenius automorphism. From Proposition (2.3.12) combined with Theorem (2.3.10) it follows that $\mathrm{H}^i_{\mathrm{dR}}((\mathbb{P}^2_{\mathscr{V}}, C)/\mathscr{V})$ is a Frobenius-equivariant lattice.

We now let (X, Z) be any smooth pair. For a positive integer k, define $\Omega^\bullet_{(X,Z)}(kZ) = \Omega^\bullet_{(X,Z)} \otimes_{\mathcal{O}_X} \mathcal{O}_X(kZ)$, where $\mathcal{O}_X(kZ)$ is the sheaf on X of meromorphic functions with poles of order k along Z. Our goal now is to use Proposition (4.3.2) to compute $\mathrm{H}^i_{\mathrm{dR}}((\mathbb{P}^2_{\mathscr{V}}, C)/\mathscr{V})$ using differential forms in $\Omega^\bullet_{(\mathbb{P}^2, C)}(kC)$. To aid in the proof of Proposition (4.3.2) we introduce a convenient lemma.

Lemma 4.3.1. *Let R be a ring, n a nonnegative integer, and let M be an R-module. Let $M =: M^n \supset M^{n-1} \supset \cdots M^0 \supset M^{-1} = \{0\}$ be a decreasing filtration of sub-R-modules, and for $0 \leq i \leq n$ let $M^{(i)} := M^i/M^{i-1}$ be the i-th part of the graded module. Suppose $a_i \in R$ is a element such that $a_i M^{(i)} = 0$. Then $a_0 a_1 \cdots a_n M = 0$.*

Proof. Let x be an element of M, and let $\overline{x}$ be its image in $M^{(n)}$. Then $a_n \overline{x} = 0$,

so $a_n x \in M^{n-1}$. Similarly, $a_{n-1}a_n x \in M^{n-2}$, and continuing in this manner one has $a_0 a_1 \cdots a_n x = 0$. □

Proposition 4.3.2. *Let (X, Z) be a smooth pair of relative dimension n over an affine scheme $S = Spec(R)$, where R is a ring with characteristic 0. Suppose $j \leq n$ is a positive integer, and let k be a positive integer such that the sheaves $\Omega^i_{(X,Z)}(kZ)$ are acyclic for all $0 \leq i \leq j$. Then*

i) if $j = n$, there is a map

$$H^n_{dR}((X, Z)/S) \to \frac{\Gamma(X, \Omega^n_{(X,Z)/S}(kZ))}{d(\Gamma(X, \Omega^{n-1}_{(X,Z)/S}(kZ)))}$$

whose kernel is killed upon multiplication by $lcm(1, ..., k)^{2n-1}$ and whose cokernel is killed upon multiplication by $lcm(1, ..., k)^{2n}$.

ii) if $j < n$, there is a map

$$H^j_{dR}((X, Z)/S) \to \frac{\ker(d : \Gamma(X, \Omega^j_{(X,Z)/S}(kZ)) \to \Gamma(X, \Omega^{j+1}_{(X,Z)/S}(kZ)))}{d\Gamma(X, \Omega^{j-1}_{(X,Z)/S}(kZ))}$$

whose kernel is killed upon multiplication by $lcm(1, ..., k)^{2j-1}$ and whose cokernel is killed upon multiplication by $lcm(1, ..., k)^{2j+1}$.

Proof. From Remark (2.2.14), since S is affine one can compute $\mathrm{H}^n_{\mathrm{dR}}((X, Z)/S)$ as the hypercohomology $\mathbb{H}^n(X, \Omega^\bullet_{(X,Z)/S})$ of the complex of sheaves of $\mathcal{O}_X$-modules $\Omega^\bullet_{(X,Z)/S}$. Define a complex of sheaves $Q^\bullet$ such that the sequence

$$0 \to \Omega^\bullet_{(X,Z)/S} \to \Omega^\bullet_{(X,Z)/S}(kZ) \to Q^\bullet \to 0 \tag{4.4}$$

is exact. This induces a long exact sequence of homology sheaves

$$\begin{aligned} \cdots \quad &\to \quad \mathcal{H}^i(\Omega^\bullet_{(X,Z)/S}) \xrightarrow{\phi_i} \mathcal{H}^i(\Omega^\bullet_{(X,Z)/S}(kZ)) \to \mathcal{H}^i(Q^\bullet) \\ &\to \quad \mathcal{H}^{i+1}(\Omega^\bullet_{(X,Z)/S}) \xrightarrow{\phi_{i+1}} \mathcal{H}^{i+1}(\Omega^\bullet_{(X,Z)/S}(kZ)) \to \cdots \end{aligned}$$

from which we obtain the short exact sequence

$$0 \to \mathrm{cok}\phi_i \to \mathcal{H}^i(Q^\bullet) \to \ker \phi_{i+1} \to 0.$$

By Theorem (2.2.20), the sheaves $\mathrm{cok}\phi_i$ and $\ker \phi_{i+1}$ are killed by $\mathrm{lcm}(1, ..., k)$. Note that since $\Omega^{n+1}_{(X,Z)/S} = 0$ we therefore have $\ker \phi_{n+1} = 0$. Étale-locally on X one can write

$\mathcal{O}_{X/S} = R[x_1, ..., x_n]$, and $\mathcal{O}_{X/S}(kZ) \subset R[x_1, ..., x_n, 1/x_1, ..., 1/x_n]$, so that for a section $s \in \mathcal{O}_{X/S}(kZ)$, $ds = 0$ implies $s \in R$ since R has characteristic 0. It follows that the map $\phi_0 : \mathcal{H}^0(\Omega^\bullet_{(X,Z)/S}) \to \mathcal{H}^0(\Omega^\bullet_{(X,Z)/S}(kZ))$ is locally equal to the identity $R \to R$, and therefore $\text{cok}\phi_0 = 0$. From the short exact sequence above, $\text{cok}\phi_i$ and $\ker \phi_{i+1}$ together form a graded filtration of $\mathcal{H}^i(Q^\bullet)$, and it follows from Lemma (4.3.1) that $\mathcal{H}^i(Q^\bullet)$ is killed by $\text{lcm}(1, ..., k)^2$ for $1 \leq i \leq n-1$, and by $\text{lcm}(1, ..., k)$ for $i = 0$ or n.

From [57, Remark 2.1.6 (i)], there exists a spectral sequence from sheaf homology converging to hypercohomology with

$$E_2^{a,b} = H^a(X, \mathcal{H}^b(Q^\bullet)) \Rightarrow \mathbb{H}^{a+b}(Q^\bullet).$$

We then have that $E_2^{a,b}$, and consequently $E_\infty^{a,b}$, is killed by $\text{lcm}(1, ..., k)$ if b is equal to 0 or n, and by $\text{lcm}(1, ..., k)^2$ for any other b. For $a + b = j$, the modules $E_\infty^{a,b}$ are graded pieces of a filtration of the j-th hypercohomology group. Using Lemma (4.3.1) and taking into account cases where b is 0 or n, we have that $\mathbb{H}^n(Q^\bullet)$ is killed by $\text{lcm}(1, ..., k)^{2(n-1)+2} = \text{lcm}(1, ..., k)^{2n}$, and $\mathbb{H}^i(Q^\bullet)$ is killed by $\text{lcm}(1, ..., k)^{2i+1}$ for $0 \leq i < n$.

From Equation (4.4) one obtains a long exact sequence of hypercohomology

$$\cdots \to \mathbb{H}^{i-1}(Q^\bullet) \to \mathbb{H}^i(\Omega^\bullet_{(X,Z)/S}) \xrightarrow{\psi_i} \mathbb{H}^i(\Omega^\bullet_{(X,Z)/S}(kZ)) \to \mathbb{H}^i(Q^\bullet) \to \cdots$$

It follows that $\text{cok}\ \psi_i$ is a submodule of $\mathbb{H}^i(Q^\bullet)$ and $\mathbb{H}^{i-1}(Q^\bullet)$ maps surjectively onto $\ker \psi_i$. Putting everything together we have $\ker \psi_0 = 0$, $\ker \psi_i$ is killed by $\text{lcm}(1, ..., k)^{2i-1}$ for $1 \leq i \leq n$, $\text{cok}\ \psi_i$ is killed by $\text{lcm}(1, ..., k)^{2i+1}$ for $0 \leq j < n$, and $\text{cok}\ \psi_n$ is killed by $\text{lcm}(1, ..., k)^{2n}$.

One now can compute the hypercohomology of $\Omega^\bullet_{(X,Z)/S}(kZ)$ from an different spectral sequence (see [57, Remark 2.1.6 (ii)]) in which

$$E_1^{a,b} = H^b(X, \Omega^a_{(X,Z)/S}(kZ)) \Rightarrow \mathbb{H}^{a+b}(\Omega^\bullet_{(X,Z)/S}(kZ)).$$

By assumption $\Omega^a_{(X,Z)/S}(kZ)$ is acyclic for all $a \leq j$, so the terms $E_1^{a,b}$ for $a + b \leq j$ are all zero except for when $b = 0$. It follows that

$$E_r^{a-r,b+r-1} \to E_r^{a,b} \to E_r^{a+r,b-r+1}$$

are all zero maps for $r \geq 2$ and $a + b \leq j$, therefore the terms below the j-th diagonal of the spectral sequence degenerate at E_2. Since there is only one nonzero term in each diagonal, it computes the entire hypercohomology group (rather than a graded part of it). We then have

$$\begin{aligned}\mathbb{H}^j(\Omega^\bullet_{(X,Z)/S}(kZ)) &= E_2^{j,0} = \frac{\ker(E_1^{j,0} \to E_1^{j+1,0})}{\mathrm{im}(E_1^{j-1,0} \to E_1^{j,0})} \\ &= \frac{\ker(d : \Gamma(X, \Omega^j_{(X,Z)/S}) \to \Gamma(X, \Omega^{j+1}_{(X,Z)/S}))}{d\Gamma(X, \Omega^{j-1}_{(X,Z)/S})}.\end{aligned}$$

This proves the cases where $j < n$. For $j = n$, we have $E_1^{n+1,0} = 0$, so $\ker(E_1^{n,0} \to E_1^{n+1,0}) = E_1^{n,0} = \Gamma(X, \Omega^n_{(X,Z)/S})$ which completes the proof. □

By Serre vanishing, there exists some integer k satisfying the condition of Proposition (4.3.2). The next several pages will be devoted to finding such an integer.

Let e and k be integers with $k \geq 0$. For a sheaf of $\mathcal{O}_{\mathbb{P}^2}$-modules $\mathcal{F}$, we denote the Serre twist of $\mathcal{F}$ by $\mathcal{F}(e) := \mathcal{F} \otimes_{\mathcal{O}_{\mathbb{P}^2}} \mathcal{O}_{\mathbb{P}^2}(e)$. We will also set $\Omega^k_{\widetilde{C}}(e) = \Omega^k_{\widetilde{C}} \otimes_{\mathcal{O}_{\widetilde{C}}} i_1^*(\mathcal{O}_{\mathbb{P}^2}(e))$ and $\Omega^k_{\widetilde{C}}(0) = \Omega^k_{\widetilde{C}}$. We have the following two useful lemmas.

Lemma 4.3.3.

i) If $e \geq -2$ and $i > 0$, then $H^i(\mathbb{P}^2_{\mathscr{V}}, \mathcal{O}_{\mathbb{P}^2_{\mathscr{V}}}(e)) = 0$.

ii) If $i, e, k > 0$, then $H^i(\mathbb{P}^2_{\mathscr{V}}, \Omega^k_{\mathbb{P}^2_{\mathscr{V}}}(e)) = 0$. If $i, e, k \geq 0$, then $H^i(\mathbb{P}^2_{\mathscr{V}}, \Omega^k_{\mathbb{P}^2_{\mathscr{V}}}(e))$ is a free $\mathscr{V}$-module.

Proof. The cases where $i > 0$ are a standard calculation, see for instance [4, Theorem III.5.1] for part (i) and [18, Proposition 3.1.2] for part (ii). Let $\mathcal{F} = \Omega^k_{\mathbb{P}^2_{\mathscr{V}}}(e)$, $k = 0, 1$ or 2. Then $\mathrm{H}^i(\mathbb{P}^2_{\mathscr{V}}, \mathcal{F})$ is a finitely generated module over the local ring $\mathscr{V}$, so to show it is a free module is equivalent to showing it is flat over $\mathscr{V}$. One can use Grothendieck's criterion for cohomological flatness (EGA III.7.8.4) which gives that $\mathrm{H}^i(\mathbb{P}^2_{\mathscr{V}}, \mathcal{F})$ is flat if and only if the dimension of $\mathrm{H}^i(\mathbb{P}^2_s, \mathcal{F}_s)$ is independent of $s \in \mathrm{Spec}(V)$. By (EGA III.7.9.4), the Euler characteristic of $\mathcal{F}_s$ is independent of s. For $e > 0$, all cohomology groups vanish except for the zeroth, so the Euler characteristic is simply $\dim \mathrm{H}^0(\mathbb{P}^2_s, \mathcal{F}_s)$, which proves $\mathrm{H}^0(\mathbb{P}^2_s, \mathcal{F}_s)$ is flat. For $e = 0$, from [18, Proposition 3.1.2] we get that $\mathrm{H}^0(\mathbb{P}^2_{\mathscr{V}}, \mathcal{F})$ is free of rank 1 if $k = 0$ and vanishes for $k > 0$. □

Lemma 4.3.4.

i) If $i > 0$ and $e > d-3$, then $H^i(\widetilde{C}, \mathcal{O}_{\widetilde{C}}(e)) = 0$. For all $i \geq 0$, if $e > d-3$ or $e = 0$ then $H^i(\widetilde{C}, \mathcal{O}_{\widetilde{C}}(e))$ is free.

ii) If $i, e > 0$, then $H^i(\widetilde{C}, \Omega^1_{\widetilde{C}}(e)) = 0$. If $i, e \geq 0$, then $H^i(\widetilde{C}, \Omega^1_{\widetilde{C}}(e))$ is free.

Proof. Since $\widetilde{C}$ is one dimensional, we only need to treat the cases $i = 0$ and $i = 1$. By the projection formulas, [4, II, Exercise 5.1 and III, Exercise 8.2], $\mathrm{H}^1(\widetilde{C}, \mathcal{O}_{\widetilde{C}}(e)) \cong \mathrm{H}^1(\mathbb{P}^2_{\mathscr{V}}, i_{1*}(\mathcal{O}_{\widetilde{C}}(e))) \cong \mathrm{H}^1(\mathbb{P}^2_{\mathscr{V}}, (i_{1*}\mathcal{O}_{\widetilde{C}})(e))$. The map $i^\sharp : \mathcal{O}_C \to \rho_*\mathcal{O}_{\widetilde{C}}$ is injective with cokernel supported on Σ which we will denote M_Σ. Thus there is an exact sequence of sheaves

$$0 \to i_*\mathcal{O}_C(e) \to i_{1*}\mathcal{O}_{\widetilde{C}}(e) \to M_\Sigma \to 0$$

which gives rise to a long exact sequence in cohomology, part of which includes

$$\mathrm{H}^1(\mathbb{P}^2_{\mathscr{V}}, i_*\mathcal{O}_C(e)) \to \mathrm{H}^1(\mathbb{P}^2_{\mathscr{V}}, i_{1*}\mathcal{O}_{\widetilde{C}}(e)) \to \mathrm{H}^1(\mathbb{P}^2_{\mathscr{V}}, M_\Sigma) = 0.$$

Therefore, $\mathrm{H}^1(\mathbb{P}^2_{\mathscr{V}}, i_*\mathcal{O}_C(e)) = 0$ is enough to ensure that $\mathrm{H}^1(\widetilde{C}, \mathcal{O}_{\widetilde{C}}(e))$ vanishes as well. Using the fact that $\mathcal{I}_C = \mathcal{O}_{\mathbb{P}^2_{\mathscr{V}}}(-C) \cong \mathcal{O}_{\mathbb{P}^2_{\mathscr{V}}}(-d)$ we have an exact sequence

$$0 \to \mathcal{O}_{\mathbb{P}^2_{\mathscr{V}}}(e-d) \to \mathcal{O}_{\mathbb{P}^2_{\mathscr{V}}}(e) \to i_*\mathcal{O}_C(e) \to 0.$$

From the induced long exact sequence in cohomology, it follows that $\mathrm{H}^1(\mathbb{P}^2_{\mathscr{V}}, i_*\mathcal{O}_C(e)) = 0$ if $\mathrm{H}^1(\mathbb{P}^2_{\mathscr{V}}, \mathcal{O}_{\mathbb{P}^2_{\mathscr{V}}}(e)) = \mathrm{H}^2(\mathbb{P}^2_{\mathscr{V}}, \mathcal{O}_{\mathbb{P}^2_{\mathscr{V}}}(e-d)) = 0$, which is satisfied for $e \geq d-2$ by Lemma (4.3.3). This proves the first statement of part (i).

Regarding the first statement of part (ii), Serre duality gives an isomorphism

$$\begin{aligned} \mathrm{H}^1(\widetilde{C}, \Omega^1_{\widetilde{C}}(e)) &\cong \mathrm{H}^0(\widetilde{C}, \Omega^1_{\widetilde{C}}(e)^{-1} \otimes \Omega^1_{\widetilde{C}})^* \\ &= \mathrm{H}^0(\widetilde{C}, i_1^*\mathcal{O}_{\mathbb{P}^2}(-e))^* \end{aligned}$$

which vanishes if $e > 0$ since $i_1^*\mathcal{O}_{\mathbb{P}^2}(1))$ is an ample invertible sheaf.

Let $\mathcal{F} = \mathcal{O}_{\widetilde{C}}(e)$ or $\Omega^1_{\widetilde{C}}(e)$. Just as in the proof of Lemma (4.3.3), $\mathrm{H}^i(\widetilde{C}, \mathcal{F})$ is a free $\mathscr{V}$-module if $\dim \mathrm{H}^i(\widetilde{C}_s, \mathcal{F}_s)$ is a constant function of $s \in \mathrm{Spec}(\mathscr{V})$. As before, the Euler characteristic of $\mathcal{F}_s$ is independent of s, and equal to $\dim \mathrm{H}^0(\widetilde{C}_s, \mathcal{F}_s)$ for $e \geq d-2$ if $\mathcal{F} = \mathcal{O}_{\widetilde{C}}(e)$ and for $e > 0$ if $\mathcal{F} = \Omega^k_{\widetilde{C}}(e)$. Therefore $\mathrm{H}^0(\widetilde{C}, \mathcal{F})$ is free in these cases by Grothendieck's criterion.

It remains to show that $\mathrm{H}^i(\widetilde{C}, \mathcal{O}_{\widetilde{C}})$ and $\mathrm{H}^i(\widetilde{C}, \Omega^1_{\widetilde{C}})$ are free. This result follows again

from Grothendieck's criterion, that the Euler characteristic $\dim H^0(\widetilde{C}_s, \mathcal{F}_s) - \dim H^1(\widetilde{C}_s, \mathcal{F}_s)$ for these sheaves is independent of $s \in \mathrm{Spec}(\mathscr{V})$, and the fact that $\dim H^0(\widetilde{C}_s, \mathcal{O}_{\widetilde{C}_s}) = 1$ and $\dim H^0(\widetilde{C}_s, \Omega^1_{\widetilde{C}_s}) = g = \dfrac{(d-1)(d-2)}{2} - m$. □

Theorem 4.3.5.

i) If $i > 0$ and $e > \max\{0, d-3\}$, then $H^i(\mathbb{P}^2_{\mathscr{V}}, \Omega^1_{(\mathbb{P}^2_{\mathscr{V}}, C)}(e)) = 0$. If $e > \max\{0, d-3\}$ or $e = 0$ then $H^0(\mathbb{P}^2_{\mathscr{V}}, \Omega^1_{(\mathbb{P}^2_{\mathscr{V}}, C)}(e))$ is a free $\mathscr{V}$-module.

ii) If $i, e > 0$, then $H^i(\mathbb{P}^2_{\mathscr{V}}, \Omega^2_{(\mathbb{P}^2_{\mathscr{V}}, C)}(e)) = 0$. If $e \geq 0$, then $H^0(\mathbb{P}^2_{\mathscr{V}}, \Omega^2_{(\mathbb{P}^2_{\mathscr{V}}, C)}(e))$ is free.

Proof. Let $\mathscr{W} = W_1(\Omega^\bullet_{(\mathbb{P}^2_{\mathscr{V}}, C)})$. By remark (2.2.17), there exist short exact sequences of $\mathbb{P}^2_{\mathscr{V}}$-modules

$$0 \to \Omega^\bullet_{\mathbb{P}^2_{\mathscr{V}}} \to \mathscr{W}^\bullet \to i_{1*}\Omega^{\bullet-1}_{\widetilde{C}} \to 0 \tag{4.5}$$

$$0 \to \mathscr{W}^\bullet \to \Omega^\bullet_{(\mathbb{P}^2_{\mathscr{V}}, C)} \to i_{2*}\Omega^{\bullet-2}_{\Sigma} \to 0. \tag{4.6}$$

For an integer e, we can tensor both sequences with $\mathcal{O}_{\mathbb{P}^2_{\mathscr{V}}}(e)$ and take the corresponding long exact sequence in cohomology, obtaining two sequences

$$\cdots \to \mathrm{H}^i(\mathbb{P}^2, \mathscr{W}^k(e)) \to \mathrm{H}^i(\mathbb{P}^2, \Omega^k_{(\mathbb{P}^2, C)}(e)) \to \mathrm{H}^i(\mathbb{P}^2, i_{2*}\Omega^{k-2}_{\Sigma}(e)) \to \cdots \tag{4.7}$$

$$\cdots \to \mathrm{H}^i(\mathbb{P}^2, \Omega^k_{\mathbb{P}^2}(e)) \to \mathrm{H}^i(\mathbb{P}^2, \mathscr{W}^k(e)) \to \mathrm{H}^i(\mathbb{P}^2, i_{1*}\Omega^{k-1}_{\widetilde{C}}(e)) \to \cdots \tag{4.8}$$

The sheaf $i_{2*}\Omega^{k-2}_{\Sigma}(e)$ is supported only on Σ, therefore it is acyclic and its zeroth cohomology group is free. Considering sequence (4.7), we have that $\mathrm{H}^2(\mathbb{P}^2, \Omega^k_{(\mathbb{P}^2, C)}(e))$ is isomorphic to $\mathrm{H}^2(\mathbb{P}^2, \mathscr{W}^k(e))$, and $\mathrm{H}^1(\mathbb{P}^2, \Omega^k_{(\mathbb{P}^2, C)}(e))$ is isomorphic to a quotient of $\mathrm{H}^1(\mathbb{P}^2, \mathscr{W}^k(e))$.

Suppose $i, e > 0$. From Lemma (4.3.3) we have $\mathrm{H}^i(\mathbb{P}^2, \Omega^k_{\mathbb{P}^2}(e)) = 0$, which implies $\mathrm{H}^i(\mathbb{P}^2, \mathscr{W}^k(e)) \cong \mathrm{H}^i(\mathbb{P}^2, i_{1*}\Omega^{k-1}_{\widetilde{C}}(e)) \cong H^i(\widetilde{C}, \Omega^{k-1}_{\widetilde{C}}(e))$ from the exact sequence (4.8) and the projection formula [4, Ch. III, Ex. 8.2]. By Lemma (4.3.4), this is zero if $k = 2$, and also for $k = 1$ provided $e > d - 3$.

It remains to verify the freeness conditions hold for $i = 0$. For the cases involving $e \neq 0$, it follows as in previous proofs using Grothendieck's criterion for cohomological flatness, and the fact that the Euler characteristic is equal to the dimension of the zeroth cohomology group, which is the same for both fibres over $\mathrm{Spec}(\mathscr{V})$. For $e = 0$, sequence (4.8) begins

$$0 \to \mathrm{H}^0(\mathbb{P}^2, \Omega^k_{\mathbb{P}^2}) \to \mathrm{H}^0(\mathbb{P}^2, \mathscr{W}^k) \to \mathrm{H}^0(\widetilde{C}, \Omega^{k-1}_{\widetilde{C}}) \to \cdots$$

By Lemma (4.3.3) and Lemma (4.3.4), $\mathrm{H}^0(\mathbb{P}^2, \Omega^k_{\mathbb{P}^2})$ and $\mathrm{H}^0(\widetilde{C}, \Omega^{k-1}_{\widetilde{C}})$ are free $\mathscr{V}$-modules, which proves that $\mathrm{H}^0(\mathbb{P}^2, \mathscr{W}^k)$ is free. For if $x \in \mathrm{H}^0(\mathbb{P}^2, \mathscr{W}^k)$ is a torsion element, then its image in $\mathrm{H}^0(\widetilde{C}, \Omega^{k-1}_{\widetilde{C}})$ is zero. By exactness, x lives in the free submodule $\mathrm{H}^0(\mathbb{P}^2, \Omega^k_{\mathbb{P}^2})$, so $x = 0$. By exactness of the sequence

$$0 \to \mathrm{H}^0(\mathbb{P}^2, \mathscr{W}^k) \to \mathrm{H}^0(\mathbb{P}^2, \Omega^k_{(\mathbb{P}^2, C)}) \to \mathrm{H}^0(\Sigma, \Omega^{k-2}_{\Sigma}(e)) \to \cdots$$

the same reasoning shows that $\mathrm{H}^0(\mathbb{P}^2, \Omega^k_{(\mathbb{P}^2, C)})$ is free. The last statement of the theorem follows from the fact that $\mathcal{O}_{\mathbb{P}^2}(k_0 C) \cong \mathcal{O}_{\mathbb{P}^2}(k_0 d)$. □

Corollary 4.3.6. *For the pair $(\mathbb{P}^2_{\mathscr{V}}, C)$, the conditions of Proposition (4.3.2) are satisfied when $k \geq 1$.*

Proof. This is immediate from the acyclicity results of Lemma (4.3.3) part (i) and Theorem (4.3.5) parts (i) and (ii), and the fact that $\mathcal{O}_{\mathbb{P}^2_{\mathscr{V}}}(C) = \mathcal{O}_{\mathbb{P}^2_{\mathscr{V}}}(d)$. □

Proposition 4.3.7. *Let H denote the image of $H^2_{dR}((\mathbb{P}^2, C)/\mathscr{V})$ in $H^2_{dR}(U_K/K)$, and let V_s denote the $\mathscr{V}$-span in $H^2_{dR}(U_K/K)$ of elements of the form $\dfrac{M}{f^s}\Omega$ where M is a monomial of degree $sd-3$. Then $H = V_2$, and for $s > 2$,*

$$p^{4\lfloor \log_p(s-1) \rfloor} V_s \subset H \subset V_s$$

Proof. By definition, the complex $\Omega^{\bullet}_{(\mathbb{P}^2_{\mathscr{V}}, C)}$ is the subcomplex of $j_*\Omega^{\bullet}_U$ consisting of elements ω of pole order 1 along C such that $d\omega$ also has pole order 1 along C. More precisely, $\Omega^k_{(\mathbb{P}^2_{\mathscr{V}}, C)}$ is the subsheaf of $\Omega^k_{\mathbb{P}^2_{\mathscr{V}}}(C)$ consisting of differentials ω such that $d\omega \in \Omega^{k+1}_{\mathbb{P}^2_{\mathscr{V}}}(2C)$ lies in the image of the natural inclusion

$$\Omega^{k+1}_{\mathbb{P}^2_{\mathscr{V}}}(C) \to \Omega^{k+1}_{\mathbb{P}^2_{\mathscr{V}}}(2C).$$

Since $d\omega = 0$ for any $\omega \in \Omega^2_{\mathbb{P}^2_{\mathscr{V}}}(C)$, we therefore have $\Omega^2_{(\mathbb{P}^2_{\mathscr{V}}, C)} = \Omega^2_{\mathbb{P}^2_{\mathscr{V}}}(C)$, and similarly $\Omega^2_{(\mathbb{P}^2_{\mathscr{V}}, C)}(sC) = \Omega^2_{\mathbb{P}^2_{\mathscr{V}}}((s+1)C)$.

For $s \geq 2$, by Corollary (4.3.6) there is a map

$$\mathrm{H}^2_{\mathrm{dR}}((\mathbb{P}^2_{\mathscr{V}}, C)/\mathscr{V}) \to \frac{\Gamma(\mathbb{P}^2_{\mathscr{V}}, \Omega^2_{\mathbb{P}^2_{\mathscr{V}}}(sC))}{d(\Gamma(\mathbb{P}^2_{\mathscr{V}}, \Omega^1_{(\mathbb{P}^2_{\mathscr{V}}, C)}((s-1)C)))} \tag{4.9}$$

whose kernel and cokernel are killed by $\mathrm{lcm}(1, ..., s-1)^4 = up^{4\lfloor \log_p(s-1) \rfloor}$ for some unit $u \in \mathscr{V}$. For $s = 2$ this map is therefore an isomorphism, so it follows immediately that $H = V_2 \subset V_s$, and that the $\mathscr{V}$-module V_s/H is killed by $p^{4\lfloor \log_p(s-1) \rfloor}$, giving the result. □

For any integer $s \geq 1$ denote the sub-$\mathscr{V}$-module of $\Gamma(\mathbb{P}^2_{\mathscr{V}}, \Omega^2_{\mathbb{P}^2_{\mathscr{V}}}((s+1)C))$ consisting exact differentials derived from pole order s by B_s, that is,

$$B_s := d\left(\Gamma(\mathbb{P}^2_{\mathscr{V}}, \Omega^1_{\mathbb{P}^2_{\mathscr{V}}}(sC))\right) = \text{span}_{\mathscr{V}}\{\frac{d(g/f^s)}{dw}\Omega : w \in \{X,Y,Z\},\ g \in \mathscr{V}[X,Y,Z]_{sd-2}\}.$$

The following is a version of the previous proposition which lends itself better to computations.

Proposition 4.3.8. *Let $\mathcal{B} \subset \Gamma(\mathbb{P}^2_{\mathscr{V}}, \Omega^2_{\mathbb{P}^2_{\mathscr{V}}}(2C))$ be a set of differentials such that the image of $\mathcal{B}$ in $H^2_{dR}(U_K/K)$ is a $\mathscr{V}$-basis for H. Let $s \geq 2$ be an integer, and let r be an integer such that $p^r H^2_{dR}((\mathbb{P}^2_{\mathscr{V}}, C)/\mathscr{V})$ is free.*

Then for any $\omega \in \Gamma(\mathbb{P}^2_{\mathscr{V}}, \Omega^2_{\mathbb{P}^2_{\mathscr{V}}}(sC))$, there exists some $\tilde{\omega} \in span_{\mathscr{V}}(\mathcal{B})$ and $d\nu \in B_s + p^{-r}B_2$ such that

$$p^{4\lfloor \log_p(s-1)\rfloor}\omega = \tilde{\omega} + d\nu.$$

Proof. From Corollary (4.3.6) there is a map

$$\frac{\Gamma(\mathbb{P}^2_{\mathscr{V}}, \Omega^2_{\mathbb{P}^2_{\mathscr{V}}}(2C))}{d(\Gamma(\mathbb{P}^2_{\mathscr{V}}, \Omega^1_{(\mathbb{P}^2_{\mathscr{V}},C)}(C)))} \longrightarrow \frac{\Gamma(\mathbb{P}^2_{\mathscr{V}}, \Omega^2_{\mathbb{P}^2}(sC))}{d(\Gamma(\mathbb{P}^2_{\mathscr{V}}, \Omega^1_{(\mathbb{P}^2_{\mathscr{V}},C)}((s-1)C)))}$$

whose cokernel is killed by $p^{4\lfloor \log_p(s-1)\rfloor}$. From the fact that $d(\Gamma(\mathbb{P}^2_{\mathscr{V}}, \Omega^1_{(\mathbb{P}^2_{\mathscr{V}},C)}((s-1)C))) \subset B_s$, one can write

$$p^{4\lfloor \log_p(s-1)\rfloor}\omega = \omega' + d\nu'$$

for some $\omega' \in \Gamma(\mathbb{P}^2_{\mathscr{V}}, \Omega^2_{\mathbb{P}^2_{\mathscr{V}}}(2C))$ and $d\nu' \in B_s$. The kernel of the map

$$\frac{\Gamma(\mathbb{P}^2_{\mathscr{V}}, \Omega^2_{\mathbb{P}^2_{\mathscr{V}}}(2C))}{d(\Gamma(\mathbb{P}^2_{\mathscr{V}}, \Omega^1_{(\mathbb{P}^2_{\mathscr{V}},C)}(C)))} \xrightarrow{\text{id}\otimes 1_K} H$$

is the submodule of torsion elements, therefore one can write

$$p^r\omega' = p^r\widetilde{\omega} + d\nu''$$

with $\widetilde{\omega} \in \text{span}_{\mathscr{V}}(\mathcal{B})$ and $d\nu'' \in d\Gamma(\mathbb{P}^2_{\mathscr{V}}, \Omega^1_{(\mathbb{P}^2_{\mathscr{V}},C)}(C)) \subset B_2$. □

If $(d,p) = 1$, then elements of $d\Gamma(\mathbb{P}^2, \Omega^1_{(\mathbb{P}^2,C)}((s-1)C)) = d\Gamma(\mathbb{P}^2, \Omega^1_{\mathbb{P}^2}(sC)) \cap \Gamma(\mathbb{P}^2, \Omega^2_{\mathbb{P}^2}(sC))$ have a convenient interpretation in terms of syzygies of Jacobian ideal $(\partial f/\partial X, \partial f/\partial Y, \partial f/\partial Z)$,

that is, nontrivial homogeneous polynomial triplets (C_1, C_2, C_3) such that

$$C_1\frac{\partial f}{\partial X} + C_1\frac{\partial f}{\partial X} + C_2\frac{\partial f}{\partial Y} + C_3\frac{\partial f}{\partial Z} = 0.$$

For a polynomial $P \in \mathscr{V}[X, Y, Z]$, we will denote its partial derivatives with respect to X, Y, and Z by P_X, P_Y, and P_Z. Any element $\omega \in d\Gamma(\mathbb{P}^2, \Omega^1_{\mathbb{P}^2}(sC))$ can be represented by homogeneous polynomials A_1, A_2, and A_3 of degree $sd-2$ by the formula

$$\begin{aligned}\omega &= ((A_1/f^s)_X + (A_2/f^s)_Y + (A_3/f^s)_Z)\,\Omega \\ &= \left(\frac{A_{1X} + A_{2Y} + A_{3Z}}{f^s} - s\frac{A_1 f_X + A_2 f_Y + A_3 f_Z}{f^{s+1}}\right)\Omega.\end{aligned}$$

Therefore ω belongs to $\Gamma(\mathbb{P}^2, \Omega^2_{\mathbb{P}^2}(sC))$ if and only if $A_1 f_X + A_2 f_Y + A_3 f_Z = fB$ for some homogeneous polynomial B of degree $sd-3$ (or $B = 0$). Supposing this is the case, by writing $f = \frac{1}{d}(Xf_X + Yf_Y + Zf_Z)$, one sees there is a syzygy $(C_1, C_2, C_3) = (A_1 - XB/d, A_2 - YB/d, A_3 - ZB/d)$ of degree $sd-2$ in the partial derivatives of f such that $\omega = ((C_1/f^s)_X + (C_2/f^s)_Y + (C_3/f^s)_Z)\Omega$.

Conversely, given a triple of homogeneous polynomials (C_1, C_2, C_3) of degree $sd-2$ satisfying $C_1 f_X + C_2 f_Y + C_3 f_Z = 0$, one can define a differential $\omega \in d\Gamma(\mathbb{P}^2, \Omega^1_{(\mathbb{P}^2, C)}((s-1)C))$ by

$$\begin{aligned}\omega &:= ((C_1/f^s)_X + (C_2/f^s)_Y + (C_3/f^s)_Z)\Omega \\ &= \left(\frac{C_{1X} + C_{2Y} + C_{3Z}}{f^s}\right)\Omega.\end{aligned}$$

This gives a one-to-one correspondence between syzygies of the Jacobian ideal of degree $sd-2$ over K and elements of $d\Gamma(\mathbb{P}^2, \Omega^1_{(\mathbb{P}^2, C)}((s-1)C))$. One can in general filter the complex $j_*\Omega^\bullet_U$ by pole order along C, and show that, after a slight modification, the filtered complex is isomorphic to the de Rham-Koszul complex of f, whose associated spectral sequence can be identified with the Koszul complex of the elements (f_X, f_Y, f_Z) (see, for example, [58]).

4.4 The Matrix of Frobenius

Let C_k be a nodal curve with m singular points in $\mathbb{P}^2_k$. Suppose C_k has coordinate ring $\overline{A}$ and is defined by an equation $\overline{f} = 0$ where $\overline{f}$ is a polynomial of degree d. Let f denote an equisingular lift of $\overline{f}$ with coefficients in the ring $\mathscr{V}$, and let C denote the corresponding

$\mathscr{V}$-scheme. Letting $U = \mathbb{P}^2_{\mathscr{V}} \setminus C$, the coordinate ring of U is given by

$$A = \{\frac{g}{f^s} : s \geq 0, g \in \mathscr{V}[X,Y,Z] \text{ is homogeneous of degree ds}\}$$

Let $A^\dagger$ denote its dagger ring, and let $A^\dagger_K := A^\dagger \otimes_{\mathscr{V}} K$. A left inverse of the q-power Frobenius can be defined on $\Omega^\bullet_{A^\dagger_K}$, following [28].

Define the K-linear operator ψ on $K[X,Y,Z]$

$$\psi(X^{a_1}Y^{a_2}Z^{a_3}) = \begin{cases} X^{\frac{a_1}{q}}Y^{\frac{a_2}{q}}Z^{\frac{a_3}{q}}, & \text{if } a_i \equiv 0 \pmod q \text{ for all } i \\ 0, & \text{otherwise} \end{cases}$$

Set $\Delta := \dfrac{f(X^q,Y^q,Z^q) - f^q}{p}$. For a positive integer $s > 0$, let r, l be the unique integers with $l > 0$, $0 \leq r \leq q-1$, such that $s + r = ql$. We then extend ψ to $A^\dagger_K$ by the formula

$$\begin{aligned}
\psi(\frac{g}{f^s}) &= \psi(\frac{g}{f^{ql-r}}) \\
&= \psi(gf^r(f^{\sigma_q} - p\Delta)^{-l}) \\
&= \psi\left(gf^r \sum_{k=0}^{\infty} \frac{-l(-l-1)\cdots(-l-k+1)}{k!}(-p\Delta)^k f(X^q,Y^q,Z^q)^{-l-k}\right) \\
&= \psi\left(gf^r \sum_{k=0}^{\infty} \binom{l+k-1}{k} p^k \Delta^k f(X^q,Y^q,Z^q)^{-l-k}\right) \\
&= \sum_{k=0}^{\infty} \binom{l+k-1}{k} p^k \frac{\psi(gf^r\Delta^k)}{f^{k+l}}
\end{aligned}$$

The operator ψ extends naturally to differentials by setting $\psi(\dfrac{dw}{w}) = \dfrac{1}{q}\dfrac{dw}{w}$ for $w \in \{X,Y,Z\}$. In particular, for an element $g \in A^\dagger_K$,

$$\psi(g\Omega) = \psi(gXYZ)\psi\left(\frac{\Omega}{XYZ}\right) = \psi(gXYZ)\frac{1}{q^2}\frac{\Omega}{XYZ},$$

which is well-defined in the de Rham complex since XYZ divides $\psi(AXYZ)$. By definition, ψ is a left inverse of the q-power Frobenius map, and since the Frobenius induces an automorphism F_* on the cohomology groups $\mathrm{H}^i_{\mathrm{MW}}(\overline{A}/K)$, it must be that ψ induces ${F_*}^{-1}$. The matrix of $q^2{F_*}^{-1}$ can then computed as follows.

Let $\mathcal{B} = \{\beta_i\}$ denote a basis as in Proposition (4.3.8), and write $\beta_i = \frac{b_i}{f^2}\Omega$ with $b_i \in \mathscr{V}[X,Y,Z]_{2d-3}$. For each β_i we can write

$$\begin{aligned} q^2\psi(\beta_i) &= q^2\psi(\frac{b_iXYZ}{f^2})\psi(\frac{\Omega}{XYZ}) \\ &= q^2\psi(\frac{f^{q-2}b_iXYZ}{f^q})\frac{\Omega}{q^2XYZ} \\ &= \sum_{k=0}^{\infty} p^k \frac{\psi(f^{q-2}b_iXYZ\Delta^k)}{XYZf^{k+1}}\Omega \\ &= \sum_{k=0}^{\infty} p^k\beta_{i,k} \end{aligned} \tag{4.10}$$

where we have set $\beta_{i,k} = \frac{\psi(f^{q-2}b_iXYZ\Delta^k)}{XYZf^{k+1}}\Omega$.

For the purpose of computational efficiency, it is convenient to define an operator ψ_p, a left inverse of the p-power Frobenius on $A_K^\dagger$, rather than the q-power Frobenius. As above, one defines ψ_p first on $K[X,Y,Z]$ to be the semi-linear map that sends $X^{a_1}Y^{a_2}Z^{a_3}$ to $X^{a_1/p}Y^{a_2/p}Z^{a_3/p}$ if a_1, a_2 and a_3 are divisible by p and is zero otherwise, and satisfies $\psi_p(ab) = \sigma_p^{-1}(a)\psi_p(b)$ for $a \in K, b \in K[X,Y,Z]$, and where $\sigma : K \to K$ denotes the p-power Frobenius. Analogous to the above definitions, we then extend ψ_p to $A_K^\dagger$, and then to differentials, replacing q by p where appropriate. One can then compute $\psi(\beta_i)$ as $\psi_p^a(\beta_i)$, which avoids having to work with polynomials whose degree is a multiple of q.

For each $\beta_{i,k}$, one performs a reduction of poles to write it as a linear combination of elements of $\mathcal{B}$ plus an exact differential. More precisely, let W_k denote the $\mathscr{V}$-subspace of $\Gamma(\mathbb{P}^2, \Omega^2_{\mathbb{P}}((k+2)C))$ spanned by the β_i's via the inclusion

$$\begin{aligned} \Gamma(\mathbb{P}^2, \Omega^2_{\mathbb{P}^2}(2C)) &\to \Gamma(\mathbb{P}^2, \Omega^2_{\mathbb{P}^2}((k+2)C)) \\ \frac{b_i}{f^2}\Omega &\mapsto \frac{b_if^k}{f^{k+2}}\Omega \end{aligned}$$

By Proposition (4.3.8), if $k - 4\lfloor \log_p k \rfloor \geq 0$ we have

$$p^k\beta_{i,k} = p^{k-4\lfloor \log_p k \rfloor}\tilde{\beta}_{i,k} + d\nu$$

for some $\tilde{\beta}_{i,k} \in W_k$ and $d\nu \in p^{k-r-4\lfloor \log_p k \rfloor}B_{k+1}$. We then have the following proposition.

Proposition 4.4.1. *If $p \geq 5$, then for each i, $q^2\psi(\beta_i)$ is cohomologically equivalent to a $\mathscr{V}$-linear combination $\sum a_{i,j}\beta_j$. Moreover, let $N \geq 1$ be an integer, and N' be the smallest integer such that $k - 4\lfloor \log_p k \rfloor \geq N$ for all $k \geq N'$. Then if the sum of the first N' terms of $q^2\psi(\beta_i)$ in the expansion (4.10) is equivalent to a $\mathscr{V}$-linear combination $\sum \tilde{a}_{i,j}\beta_j$, then*

$$\tilde{a}_{i,j} \equiv a_{i,j} \mod p^N.$$

Proof. The first assertion follows immediately from the previous paragraph, and the fact that $n - 4\lfloor \log_p n \rfloor \geq 0$ for all $n \geq 1$ when $p \geq 5$. The second follows from the fact that for $k \geq N'$, the $k+1$-th term $p^k\beta_{i,k}$ reduces to $p^{k-4\lfloor \log_p k \rfloor}\tilde{\beta} \equiv 0 \mod p^N$. □

To calculate the reduction of $p^k\beta_{i,k}$ one can use linear algebra. For instance, one may compute a basis $\{\gamma_i\}$ for the vector space B_{k+1}, and view $\beta_{i,k}$ as an element of $W_k + B_{k+1}$ with basis $\mathcal{B}' = \{\beta_i\} \cup \{\gamma_i\}$. One then computes $p^{k-4\lfloor \log_p k \rfloor}\tilde{\beta}_{i,k}$ as the first $(d-1)(d-2) - m$ coordinates with respect to $\mathcal{B}'$.

4.5 p-Adic Precision Analysis

The numerator of the zeta function of $\widetilde{C}_k$ is a polynomial

$$\widetilde{P}(T) = \prod_{i=1}^{2g}(1 - \mu_i T) = \sum_{i=0}^{2g} c_i T^i \in \mathbb{Z}[T]$$

where $g = \dfrac{(d-1)(d-2)}{2} - m$, and $|\mu_i| = q^{1/2}$. As before we have $c_{2g-i} = q^{g-i}c_i$, and

$$|c_i| \leq \binom{2g}{i} q^{i/2} \leq \binom{2g}{g} q^{i/2},$$

If $P(t)$ is the numerator of the zeta function of C_k, by Proposition (4.2.6), we have $P(t) = \widetilde{P}(t)h(t)$, where $h(t) = b_0 + b_1 t + \cdots + b_m t^m \in \mathbb{Z}[t]$ is symmetric or antisymmetric, of degree m, and has roots with complex absolute value 1. In particular $|b_i| \leq \binom{m}{i}$.

To compute $P(t)$ from Section (4.2.2) it suffices to compute its first $g+1$ coefficients. Writing

$$P(t) = a_0 + a_1 t + \cdots a_{2g+m} t^{2g+m},$$

we have, for $k \leq g$,

$$\begin{aligned}
|a_k| &= \Big|\sum_{i+j=k} \tilde{a}_i b_j\Big| \\
&\leq \sum_{j=0}^{m} \binom{m}{j} |c_{k-j}| \\
&\leq \sum_{j=0}^{m} \binom{m}{j}\binom{2g}{g} q^{(k-j)/2} \\
&\leq \binom{2g}{g} q^{g/2} \sum_{j=0}^{m} \binom{m}{j} q^{-j/2} \\
&= \binom{2g}{g} q^{g/2} (q^{-1/2}+1)^m \\
&= \binom{2g}{g} q^{(g-m)/2} (q^{1/2}+1)^m
\end{aligned}$$

so the polynomial $\widetilde{P}(t)$ can be calculated in $\mathbb{Z}/p^{N_1}\mathbb{Z}$, where

$$N_1 = \lceil \log_p \left(2\binom{2g}{g} q^{(g-m)/2}(q^{1/2}+1)^m \right) \rceil.$$

Let $\mathcal{B} = \{\frac{b_i}{f^2}\Omega\}$ denote a basis for $\mathrm{H}^2_{\mathrm{dR}}(U_K/K))$ as in Proposition (4.4.1), and let M denote the matrix of $q^2 F_*^{-1}$ with respect to $\mathcal{B}$. Then by the statement of the proposition, M has entries in $\mathscr{V}$, and can be calculated with p-adic precision $p^{N-4\lfloor \log_p N \rfloor}$ by reducing the first N terms in the series expansions for each $q^2\psi(\beta_i)$. Therefore, choosing N_2 such that

$$N_2 - 4\lfloor \log_p N_2 \rfloor \geq N_1,$$

one may compute a matrix $\tilde{M}$ satisfying

$$\tilde{M} \equiv M \mod p^{N_1},$$

by reducing the first N_2 terms in the expansion of each basis element, and performing all operations in $\mathbb{Z}/p^{N_2}\mathbb{Z}$. One then derives the numerator of the zeta function from the lowest $g+1$ coefficients of the polynomial $\det(\tilde{M}T - I)$.

Chapter 5

Algorithms and Complexity Estimates

In this chapter we outline both algorithms, and give asymptotic bounds for the complexity of each, with respect to both the genus g of the curve and the index $a = [k : \mathbb{F}_p]$. In both algorithms we assume that p is fixed and that for two objects of bit size N, multiplication can be performed in time $O(N^{1+\varepsilon})$. Both algorithms also make use of the p power Frobenius operator σ_p on $\mathscr{V}$, which can be computed as follows. Write $\mathscr{V} = \mathbb{Z}_p[\theta]$, and let $P(x)$ be the minimal polynomial of θ. Then $\sigma(\theta)$ is a root of $P(x)$, and can be calculated up to the required precision by Newton interpolation

$$X \leftarrow X - P'(X)/P(X)$$

initialized at θ^p (see [12]). After this value has been stored, the action of σ_p can be calculated for any element using $O(a)$ ring operations.

5.1 Superelliptic Curve

5.1.1 Algorithm

For p an odd prime, set $q = p^a$, $k = \mathbb{F}_q$, and $\mathscr{V} = W(k)$. Let $\overline{f}(x) \in k[x]$ be a polynomial of degree d that has n distinct roots, m of which are k-rational multiple roots, such that the multiplicity of any root is not divisible by p. Denote by e the greatest multiplicity of any root of $\overline{f}$. Let $r > e$ be a prime different from p, and set $g = (n-1)(r-1)/2$. The following algorithm outlines the procedure for computing the zeta function of the k-curve defined by the equation $y^r = \overline{f}(x)$.

Step 1. Using the procedure of section (3.1.1), lift $\overline{f}$ to a polynomial $f \in \mathscr{V}_{\text{fin}}[x]$ such that $y^r = f(x)$ defines a superelliptic curve over $\mathscr{V}$.

Step 2. Letting e denote the greatest multiplicity of any linear factor of f, compute integers $N_1 = \lceil \log_p(2\binom{2g}{g} q^{g/2}) \rceil$, $N_2 = 2\lfloor \log_p((d-1)(r-1)-1) \rfloor$, and N_3 the smallest integer such that $N_3 - \lfloor \log_p(ep(l + r(N_3 - 1)) - r) \rfloor \geq N_1 + 2N_2$.

Step 3. Performing computations in $\mathscr{V}/p^{N_3+N_2}\mathscr{V}$, compute the first N_3 terms of $p^{N_2} F\left(\dfrac{x^i h(x)}{y^l}\right)$ for $0 < l < r$, $0 \leq i \leq n-2$. One effective way to do this, following [16] is to set $\tau = 1/y^r$, $\Delta = \dfrac{1}{p}(f(x)^\sigma - f(x)^p)$, and $S = 1 + p\Delta\tau^p$, so that

$$F\left(\frac{x^i h(x)}{y^l}\right) = \tau^{(pl \text{ div } r)} p x^{pi+p-1} h(x)^\sigma S^{-l/r} \frac{dx}{y^{p_l}}.$$

One can use Newton's method to quickly compute $X = S^{-1/r}$ as a root of the function $F(X) = 1 - \frac{1}{SX^r}$: set $X_0 = 1$ for the initial value, and let

$$X_{i+1} = X_i - F(X_i)/F'(X_i) = \frac{1}{r}((r+1)X_i - SX_i^{r+1}).$$

After each iteration one should use the relation $f = \tau^{-1}$ to rewrite the resulting expression so that the degree in x is less than d, and reduce modulo τ^{pN_3}.

Step 4. For $i \in S_2, k = 0, 1, ..., e_i - 2$, precompute the polynomials $f^{[k]}(x)/(x-\alpha_i)^{e_i-k}$ and $R_{i,k+1}(x)$. For $i, k = 0, ..., d-n-1$ compute the polynomials $b_i(x), a_{i+1}(x)$ from section (3.1.3) and constants $\lambda_{i,k}$ such that $\sum_{i=0}^{d-n-1} \lambda_{i,k} b_i(x) = x^k$. Use the stored data and the processes of section (3.2) to reduce the degree in τ of the polynomials found in Step 3, until one can write it as a linear combination of differentials $\dfrac{x^i h(x)}{y^l}$. Let M' denote the resulting matrix, and let $M = \dfrac{1}{p^{N_2}} M'$ (with entries viewed in $\dfrac{1}{p^{N_2}}\mathscr{V}_{\text{fin}}$ up to precision $p^{N_1+2N_2}$.

Step 5. Compute the norm matrix $|M| = M^{\sigma^{a-1}} M^{\sigma^{a-2}} \cdots M$, and $\det(|M| - T)$. Compute integers in $[-\frac{1}{2}p^{N_1}, \frac{1}{2}p^{N_1}]$ congruent to the integers of the resulting polynomial modulo p^{N_1}.

5.1.2 Complexity Analysis

Assume p is fixed. Assume also that multiplication of two objects of bit size N can be performed in time $O(N^{1+\varepsilon})$. Let $R = \mathscr{V}/p^{N_3+N_2}\mathscr{V}$. Then any element of R can be stored using $a(N_3 + N_2) = O(a^{2+\varepsilon}g^{1+\varepsilon})$ bits. Note that $N_3 = O(a^{1+\varepsilon}g^{1+\varepsilon})$, and $d \leq nr = O(g)$.

Step 1 and 2 can clearly be performed in $O(1)$ time and space. For Step 3, one can compute S in $O(a)$ ring operations. The expression we need to represent $S^{-j/r}$ is a polynomial over R of degree less than d in x and of degree less than pN_3 in τ, and thus requires $O(dpN_3a^{2+\varepsilon}g^{1+\varepsilon}) = O(a^{3+\varepsilon}g^{3+\varepsilon})$ bits of storage. Only $O(1)$ operations are required to compute $S^{-1/r}$, therefore the computation of $S^{-j/r}$ for $j = 1, ..., r-1$ is $O(ra^{3+\varepsilon}g^{3+\varepsilon})$ in runtime and space.

The precomputations for Step 4 can be done in comparable time to the rest of the step, and requires storing $O(d-n)$ polynomials of degree less than d over R, as well as another $(d-n)^2$ elements of R for a total of $O(d(d-n)a^{2+\varepsilon}g^{1+\varepsilon})$ bits. One uses the reduction process of section (3.2) for each of the $2g$ polynomials found in the previous step. For $j = pN_3, pN_3 - 1, ..., 1$, we repeat the following process on the polynomial associated with τ^j, which is of degree less than d over the ring R. From Equation (3.11), one computes $A^{[k+1]}(x)$ from $A^{[k]}(x)$ using $O(|S_{k+2}|d)$ ring operations to find the values $A_{i,k+1}$ for $i \in S_{k+2}$ as well finding the quotient $Q^{[k+1]}(x)$ using polynomial long division. Repeating this for $k = 0, ..., e-2$ gives a total of $O((d-n)d)$ ring operations until one obtains a polynomial $B(x)$ of degree less than $d-n$. Using the $\lambda_{i,k}$'s, another $O((d-n)^2)$ ring operations are required to compute $B(x)$ as linear combination of the polynomials $b_{i,r-j}(x), i = 0, ..., d-n-1$. In total, this step is $O(a^{3+\varepsilon}g^{5+\varepsilon})$ in complexity.

The final step in computing the norm matrix $|M|$ and its characteristic polynomial adds a time cost of $O(a^{3+\varepsilon}g^{4+\varepsilon})$ (see the resource analysis of Kedlaya [12]). Overall, the complexity of this algorithm is $O(a^{3+\varepsilon}g^{5+\varepsilon})$.

5.2 Nodal Plane Curve

5.2.1 Algorithm

The following is an algorithm to compute the zeta function of a projective, irreducible, planar k-curve $\overline{C}$ of degree d that has m nodes over $\overline{k} = \mathbb{F}_q$ and no other singularities. Suppose that $\overline{C}$ is defined in $\mathbb{P}^2_k$ by an equation $\overline{f} = 0$, let $g = \frac{(d-1)(d-2)}{2} - m$ be the genus, and let U_k denote its complement.

Step 1. Let $N_1 = \lceil \log_p 2\binom{2g}{g} q^{(g-m)/2}(q^{1/2}+1)^m \rceil$, and let N_2 be the smallest integer such that $k - 4\lfloor \log_p k \rfloor \geq N_1$ for all $k \geq N_2$. Lift $\overline{f}$ to a homogeneous polynomial

$f \in \mathscr{V}_{\text{fin}}[X, Y, Z]$ of degree d, such that $f \equiv \widetilde{f} \bmod p^{N_2}$, where $\widetilde{f}$ is an equisingular lift of $\overline{f}$ defining a $\mathscr{V}$-scheme C. Note that if $m \leq \dfrac{d+1}{2}$, we can take $f = \widetilde{f}$.

Step 2. Calculate a basis $\mathcal{B} = \{\beta_i\}_{i=1}^{g}$ for the image of $\mathrm{H}^2_{\text{crys}}((\mathbb{P}^2_k, \overline{C})/\mathscr{V})$ in $\mathrm{H}^2_{\text{MW}}(U_k/K)$ by taking the $\mathscr{V}$-span of differentials of the form $A\Omega/f^2$ modulo the subgroup generated by differentials of the form $\partial(B/f^2)/\partial W\Omega$. Here A and B represent monomial of degrees $2d-3$ and $2d-2$, respectively, and W is X, Y, or Z.

Step 3. Performing calculations in $\mathbb{Z}/p^{N_2}\mathbb{Z}$, evaluate the first N_2 terms of $q^2\psi(\beta_i)$ from (4.10).

Step 4. Using exact differentials with pole order one degree greater, reduce the terms found in Step 3 to a linear combination of the β_i's and write these as the i-th rows of a matrix M.

Step 5. Compute $\det(I - TM)$ modulo p^{N_1}, and calculate the numerator of the zeta function from the first $g+1$ coefficients.

5.2.2 Complexity Analysis

We will assume that the parameters p and m are fixed, and that multiplication of two objects of bit size N can be performed in time $O(N^{1+\varepsilon})$. In the process of Gaussian elimination for a matrix of dimension M by N, a column with a leading 1 and zeros beneath is formed using $O(NM)$ field operations. Therefore, since its rank is less or equal to $L = \min(M, N)$, the number of field operations required to reduce the matrix to row echelon form is $O(NML)$.

Our algorithm is implemented using matrices over the ring $R = \mathscr{V}/p^{N_2}\mathscr{V}$. For an element $b \in R$, we allow b/p to mean any element such that when multiplied by p is equal to b. Similarly, one can perform the row operation of dividing by p when all entries of the row are divisible by p.

Elements of the ring R can be stored using $aN_2 = O(a^{2+\varepsilon}g^{1+\varepsilon})$ bits. As in the algorithm for superelliptic curves, the p-power Frobenius σ can be calculated in R with $O(a)$ operations by precomputation of $\sigma(\theta)$. Similarly, one can precompute $\sigma^{-1}(\theta)$ by Newton interpolation initialized at $\theta^{p^{a-1}}$, and from then on compute the action of σ^{-1} on R in $O(a)$ ring operations.

The space of homogeneous polynomials of degree D in variables X, Y, Z has dimension $\binom{D+2}{2} = (D+1)(D+2)/2$. From Equation (4.3), Step 1 therefore requires finding a particular solution to a linear system of $3m$ equations in $(d+1)(d+2)/2$ variables. This

can be accomplished by row reducing a matrix of dimension $3m$ by $(d+1)(d+2)/2+1$ to echelon form and solving the system, which requires $O(m^2d^2) = O(g)$ ring operations. This step is therefore $O(a^{2+\varepsilon}g^{2+\varepsilon})$ in time and $O(a^{2+\varepsilon}g^{2+\varepsilon})$ in space.

For Step 2, one generates the $\binom{2d-1}{2}$-dimensional vector space of all differentials with pole order two as a subspace of the $\binom{3d-1}{2}$-dimensional vector space of differentials with pole order three. Then take β_i's to be representatives of this space modulo exact differentials, which is a subspace generated by $3\binom{2d}{2}$ elements. One may perform this step by row reducing a $\binom{3d-1}{2}$ by $\binom{2d-1}{2} + 3\binom{2d}{2}$ matrix, which uses $O(d^6) = O(g^3)$ operations in R and thus requires time $O(a^{2+\varepsilon}g^{4+\varepsilon})$.

For Step 3, one must first calculate the numerator of each $\beta_{i,k}$ from (4.10) for $k = 0, ..., N_2 - 1$, $i = 1, .., 2g + m$. One computes $q^2\psi(\beta_i) = (p^2\psi_p)^a(\beta_i)$ by iteration, in each step evaluating all the terms up to pole order N_2. The numerator of a differential with pole order k is a homogeneous polynomial of degree at most $N_2d - 3$ over the ring, therefore the storage requirement for each $q^2\psi(\beta_i)$ is $O(aN_2^3d^2) = O(a^{4+\varepsilon}g^{4+\varepsilon})$. In the first iteration, one evaluates the first N_2 terms of $p^2\psi_p(\beta_i)$. In each subsequent iteration, one evaluates $N_2 - k$ terms of the expansion of ψ_p on a differential with pole order k, for $k = 1, ..., N_2$. This requires applying ψ_p to $(N_2 - 1)(N_2 - 2)/2$ polynomials of degree at most N_2dp (a space of size $O(N_2^2d^2)$ over the ring). Each polynomial in the argument of ψ_p can be computed in $O(1)$ operations, and since ψ_p is a composition of selecting coordinates and applying σ^{-1}, this requires $O(aN_2^4d^2)$ ring operations. Adding the polynomials of corresponding degree together requires $O(N_2^2)$ operations on a space of size $O(N_2^2d^2)$ over the ring. In total, this step is $O(a^{4+\varepsilon}g^{5+\varepsilon})$ in space and $O(a^{7+\varepsilon}g^{7+\varepsilon})$ in time. We can speed this up by roughly a factor of a at a cost of $O(a^{3+\varepsilon}g^{2+\varepsilon})$ storage by precomputing the values of σ_p^k at the coefficients of f for $k = 1, ..., a - 1$ and storing these in a file.

In Step 4, the elements stored in Step 3 are then embedded into the space of differentials with pole order N_2, which has dimension $\binom{N_2d-1}{2}$. The space of exact differentials which sits inside here is generated by $3\binom{N_2d}{2}$ elements. One then must solve a matrix system of size $\binom{N_2d-1}{2}$ by $\binom{(N_2-1)d-1}{2} + 3\binom{N_2d}{2}$, which requires $O(N_2^6d^6)$ ring operations. This limiting step is $O(a^{7+\varepsilon}g^{10+\varepsilon})$ in time and $O(a^{5+\varepsilon}g^{8+\varepsilon})$ in space.

The final step in computing the characteristic polynomial requires $O(g^3)$ ring operations for a time cost of $O(a^{2+\varepsilon}g^{4+\varepsilon})$.

Chapter 6

Experiments

In this section we give the results of several experiments conducted using somewhat coarse implementations of each algorithm. The programming language used is MAGMA V2.19-7 and the machine used is the Sphere computer at the University of Toronto. This has a SunFire X4200 quad-core processor with 16 GB of RAM. In general the memory usage for these particular implementations is quite high due to their being somewhat crudely written, as well as the fact that they rely on certain intrinsic functions of the programming language for solving large systems of equations which trade time for memory consumption.

6.1 Examples of Superelliptic Curves

We begin with an example of a genus 5 curve defined over $\mathbb{F}_{5^{10}}$ by the equation

$$y^3 = x^2(x^5 + x^4 + x + t)$$

where t generates $\mathbb{F}_{5^{10}}$ over $\mathbb{F}_5$ and has minimal polynomial $z^{10}+3z^5+3z^4+2z^3+4z^2+z+2$. In this case we set $N_1 = 29$, $N_2 = 2$, and $N_3 = 37$. The highest working precision we will need is 5^{39}, and the zeta function should be calculated modulo 5^{29}. After 3 minutes and 18 seconds, and using 80MB of space, the algorithm revealed the first six coefficients of the numerator of the zeta function of the normalized curve to be $1-1253T+10171416T^2+10359663716T^3+177276031807004T^4-15438514067989687 5T^5$, and one can then compute the size of its Jacobian as $N = 888064554752583506264372336514315 09$.

As a second example, we compute the zeta function of a genus 8 curve over $\mathbb{F}_{3^{20}}$ with

planar equation

$$y^5 = x^4(x-1)^4(x-t)^4(x-t^2)^4$$

where $\mathbb{F}_{3^{20}}$ generated over $\mathbb{F}_3$ by t with minimal polynomial $z^{20}+2z^{13}+z^{11}+z^{10}+z^9+z^8+2z^5+2z^4+2z^3+z+2$. Here $N_1 = 67$, $N_2 = 6$ and $N_3 = 86$. The program outputted $1 - 222102T + 26390120031T^2 - 2538440313760890T^3 + 216995406474678950790T^4 - 15512966168826218109491232T^5 + 960365390614818936440153417604T^6$ giving a total of

$$N = 1797010425151142564400620717847005400323356502183342964163$$

points on the Jacobian. The running time was 22 minutes and the memory usage for this example was approximately 1 GB.

Consider now a curve defined over $\mathbb{F}_7$ with affine equation given by $y^3 = x^2(x^4-x-1)$. This does not define a superelliptic curve by Definition (3.1.1), since $(d, r) = 3$. We apply the same algorithm with $N_1 = 5$, $N_2 = 2$, $N_3 = 12$, and compute with precision 7^{11} the reduction of the first 12 terms of the Frobenius multiplied by 7^2. At the final step we divide by 49, and take the result modulo 7^5. The processing time was 1.82 seconds with 33 MB of memory usage, and the program outputted the polynomial

$$(1-T)^2(1+T+7T^2)(1+2T-3T^2+14T^3+49T^4).$$

This result can be interpreted as follows. The normal model is a curve C of genus 3, with three points at infinity which are permuted by the automorphism $\rho : (x, y) \mapsto (x, \zeta y)$, where ζ is a primitive cube root of unity. If we let Σ denote the points at infinity, then the Gysin sequence (Proposition (2.4.4)) gives

$$0 \to \mathrm{H}^1_{\mathrm{rig}}(C/K) \to \mathrm{H}^1_{\mathrm{rig}}(C'/K)^- \to \mathrm{H}^0_{\mathrm{rig}}(\Sigma/K)^- \to \cdots$$

where C' denotes the affine curve minus the points along $y = 0$. In this case (cf. Proposition (3.1.5)) $\mathrm{H}^0_{\mathrm{rig}}(\Sigma/K) = K[w]/(w^3-1)$ is non-trivial, with ρ given as the K-linear map $\rho(w) = \zeta w$. This decomposes into eigenspaces $K \oplus Kw \oplus Kw^2$, with the Frobenius acting trivially on each, and $\mathrm{H}^0_{\mathrm{rig}}(\Sigma/K)^- = K\dot{w} \oplus K\dot{w}^2$. We conclude that $(1-T)^2$ is the characteristic polynomial of the Frobenius acting on $\mathrm{H}^0_{\mathrm{rig}}(\Sigma/K)^-$, and that the zeta function of $\widetilde{C}$ is

$$\frac{(1+T+7T^2)(1+2T-3T^2+14T^3+49T^4)}{(1-T)(1-7T)}.$$

6.2 Examples of Nodal Plane Curves

It should be mentioned that the author suspects from two observations that the algorithm for nodal curves could be improved. Firstly, the precision bound $k - 4\lfloor k \rfloor \geq N$ in Proposition (4.4.1) in practice seems more than necessary in ensuring correct precision of the result, and for the implementations below we instead use $k - 2\lfloor k \rfloor \geq N$. This in fact is not an arbitrary choice, since it is claimed [41] that this bound is sufficient, however this author hesitated on one detail of the proof. One also suspects (as in the case with superelliptic curves) that there could exist a more explicit reduction method for differentials. Nevertheless, we demonstrate that this algorithm correctly computes the zeta function of two interesting cases of nodal curves.

For the first example we use is a random genus 5 quintic defined over $\mathbb{F}_{11}$ with a single node at $(0, 0, 1)$ and defining polynomial

$$\begin{aligned}&-2X^5 + 2X^4Y + 2X^3Y^2 + X^3YZ - 5X^3Z^2 - 5X^2Y^3 - 2X^2Y^2Z + X^2YZ^2\\&+2X^2Z^3 + 5XY^4 + 5XY^3Z - 5XY^2Z^2 - Y^5 - Y^4Z - 5Y^3Z^2 - 4Y^2Z^3.\end{aligned}$$

The nodal point is at (0,0,1) and the discriminant of the quadratic terms on the affine plane $Z = 1$ is $32 \equiv -1 \mod 11$ which is not a square in $\mathbb{F}_{11}$. We conclude that the numerator of the zeta function of the nodal curve is the degree 10 polynomial coming from the normalization, multiplied by the linear factor $1 + T$. For this curve we can take $N_1 = N_2 = 6$, so that calculation are performed on the first 6 terms of the Frobenius expansion with maximal precision 11^6, and the final matrix of Frobenius is calculated also with precision 11^6. The program outputted the polynomial

$$(1+T)(1-T-4T^2+3T^3+66T^4-104T^5+726T^6+363T^7-5324T^8-14641T^9+161051T^{10})$$

which is the correct numerator of the zeta function. The running time for this example was 44 seconds and the memory usage was 321 MB.

For a second example we apply the algorithm to a curve considered by Lauder [38]. It is the genus 4 sextic with 6 nodes over $\mathbb{F}_7$ defined by the equation

$$\begin{aligned}&X^6 - X^5Y - 2X^5Z + 2X^4Y^2 + 7/2X^4Z^2 + X^3Y^3 - 4X^3Y^2X - 3X^3Z^3\\&+1/2X^2Y^4 + 5X^2Y^2Z^2 - X^2YZ^3 + 7/2X^2Z^4 - 2XY^4Z - 4XY^2Z^3\\&-2XZ^5 + Y^6 + 3/2Y^4Z^2 + Y^3Z^3 + 3/2Y^2Z^4 + Z^6 = 0.\end{aligned}$$

The precision requirements from Chapter 5 are $N_1 = 6$, $N_2 = 8$, and therefore we are supposed to calculate the first 8 terms of the Frobenius series with maximal precision 7^8 and final precision 7^6. We can perhaps do slightly better by investigating the factor of the zeta function coming from the singular points on this curve. Two of the singularities, s_1 and s_2, occur at $Z = Y = 1$, and X satisfies $X^2 + 5X + 2 = 0$. Since the discriminant of this polynomial is $25 - 8 \equiv 3 \mod 7$ is not a square in $\mathbb{F}_7$ we must pass to $\mathbb{F}_{7^2}$ to find roots. Letting t generate $\mathbb{F}_{7^2}$ over $\mathbb{F}_7$ with minimal polynomial $x^2 - x + 3 = 0$ so that we may designate $s_1 = [t^2 : 1 : 1]$ and $s_2 = [t^{14} : 1 : 1]$. Then locally around s_1, the polynomial has the form

$$t^{27}X^2 + t^{13}XY + t^3Y^2 + \text{higher order terms}$$

and the discriminant of the quadratic terms is

$$\delta = t^{26} - 4t^{30} = 5$$

which is a square in $\mathbb{F}_{7^2}$. Therefore we can deduce that $1 - T^2$ is a factor of the zeta function of the curve. We can perform a similar computation to find that the remaining four singular points are conjugates defined over $\mathbb{F}_{7^4}$, with the discriminant of the local quadratic term not equal to a square in $\mathbb{F}_{7^4}$. We deduce from this the factor $1 + T^4$, and conclude that the zeta function of the curve has the form $(1 - T^2 + T^4 - T^6)Q(T)$, where $Q(T) \in \mathbb{Z}[T]$ is a polynomial of degree 8 whose roots have absolute value $7^{-1/2}$. As in Section (3.5), the i-th degree coefficient of $Q(T)$ is bounded by $\binom{8}{i}7^{i/2}$, and it follows that the largest coefficient of $(1 - T^2 + T^4 - T^6)Q(T)$ for degree less than or equal to four is at most 3627. Hence the polynomial can be calculated with precision 7^{N_1} where $N_1 = \lceil \log_7(2 \cdot 3627) \rceil = 5$, and one can then take $N_2 = 5$.

Using these precision bounds, after 53 seconds and 400 MB of memory the program outputted the polynomial

$$(1 - T^2 + T^4 - T^6)(1 + 2T + 11T^2 + 40T^3 + 72T^4 + 280T^5 + 539T^6 + 686T^7 + 2401T^8)$$

which is the numerator of the zeta function of the curve.

For a third example we consider a random genus 5 curve over $\mathbb{F}_{7^2}$ defined by the

polynomial

$$\begin{aligned} & t^{26}X^5 - X^4Y + t^2 7X^4Z + t^{11}X^3Y^2 - 3X^3YZ + t^{18}X^3Z^2 \\ + \;& t^{10}X^2Y^3 + t^{36}X^2Y^2Z + t^{25}X^2YZ^2 + t^{39}X^2Z^3 + t^{35}XY^4 + t^{33}XY^3Z \\ + \;& t^5XY^2Z^2 + t^{26}XYZ^3 + t^{42}Y^5 + t^{36}Y^4Z + t^{31}Y^3Z^2 + t^{45}Y^2Z^3 \end{aligned}$$

where the minimal polynomial for t over $\mathbb{F}_7$ is $x^2 - x + 3$. The only singular point is at $[0, 0, 1]$, and the discriminant of the quadratic terms at $Z = 1$ is

$$\delta = t^{52} - 4t^{39+45} = t^{28}$$

which is a square in $\mathbb{F}_{7^2}$, and hence $h(T) = 1 - T$. The parameters of the algorithm require the first 11 terms of the Frobenius expansion to be computed with working precision 7^{11} and final precision 7^9. The program outputted the numerator of the zeta function of the curve as

$$\begin{aligned} & (1 - T)(1 + 13T + 151T^2 + 1179T^3 + 8021T^4 + 59805T^5 \\ & +393029T^6 + 2830779T^7 + 17764999T^8 + 74942413T^9 + 282475249T^{10}). \end{aligned}$$

For this example the program ran for 170 minutes and consumed approximately 8 GB of memory.

Bibliography

[1] C. F. Gauss, *Disquisitiones Arithmeticae*. 1801.

[2] B. Dwork, "On the rationality of the zeta function of an algebraic variety," *American Journal of Mathematics*, vol. 82, no. 3, pp. 631 –648, 1960.

[3] P. Deligne, "La conjecture de Weil. I," *Publications Mathématiques de l'Institut des Hautes Études Scientifiques*, vol. 43, no. 1, pp. 273–307, 1974.

[4] R. Hartshorne, *Algebraic Geometry*. New York: Springer-Verlag, 1977.

[5] R. Schoof, "Elliptic Curves Over Finite Fields and the Computation of Square Roots mod p," *Mathematics of Computation*, vol. 44, no. 170, pp. 483–494, 1985.

[6] J. Pila, "Frobenius Maps of Abelian Varieties and Finding Roots of Unity in Finite Fields," *Mathematics of Computation*, vol. 55, no. 192, pp. 745–763, 1990.

[7] L. M. Adelman and M.-D. Huang, "Counting Points on Curves and Abelian Varieties over Finite Fields," *J. of Symbolic Computation*, vol. 32, pp. 171–189, 2001.

[8] M.-D. Huang and D. Ierardi, "Counting Points on Curves over Finite Fields," *J. of Symbolic Computation*, vol. 25, pp. 1–21, 1998.

[9] P. Gaudry and R. Harley, "Counting Points on Hyperelliptic Curves over Finite Fields," in *Algorithmic Number Theory*, ser. Lecture Notes in Computer Science, vol. 1838, Springer Berlin Heidelberg, 2000, pp. 313–332.

[10] T. Satoh, "The canonical lift of an ordinary elliptic curve over a finite field and its point counting," *J. of Ramanujan Math. Soc.*, vol. 15, no. 4, pp. 247–270, 2000.

[11] P. Monsky and G. Washnitzer, "Formal Cohomology I," *Annals of Math.*, vol. 88, pp. 181–217, 1968.

[12] K. S. Kedlaya, "Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology," *Journal of Ramanunan Mathematical Society*, vol. 16, pp. 323–338, 2001.

[13] P. Gaudry and N. Gürel, "Counting points in medium characteristic using Kedlaya's algorithm.," *Experimental Mathematics*, vol. 12, no. 4, pp. 395–402, 2003.

[14] D. Harvey, "Kedlayas algorithm in larger characteristic," 2007. arXiv: `math/0610973`.

[15] J. Denef and F. Vercauteren, "An Extension of Kedlaya's Algorithm to Hyperelliptic Curves in Characteristic 2," *Journal of Cryptology*, vol. 19, no. 1, pp. 1–25, 2006.

[16] P. Gaudry and N. Gürel, "An Extension of Kedlayas Point-Counting Algorithm to Superelliptic Curves," in *Advances in Cryptology ASIACRYPT 2001*, ser. Lecture Notes in Computer Science, C. Boyd, Ed., vol. 2248, Springer Berlin Heidelberg, 2001, pp. 480–494.

[17] J. Denef and F. Vercauteren, "Counting points on $C_{a,b}$ curves using MonskyWashnitzer cohomology," *Finite Fields and Their Applications*, vol. 12, no. 1, pp. 78 –102, 2006.

[18] T. G. Abbott, K. S. Kedlaya, and D. Roe, "Bounding picard numbers of surfaces using p-adic cohomology," *Séminaires et Congrés*, vol. 21, pp. 125–159, 2009.

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

[20] ——, "Counting solutions to equations in many variables over finite fields," *Foundations of Computational Mathematics*, vol. 4, no. 3, pp. 221–267, 2004.

[21] R. Gerkmann, "Relative rigid cohomology and point counting on families of elliptic curves," *J. Ramanujan Math. Soc.*, vol. 23, no. 1, pp. 1–31, 2008.

[22] ——, "Relative Rigid Cohomology and Deformation of Hypersurfaces," *International Mathematics Research Papers*, 2007.

[23] P. Berthelot, "Cohomologie rigide et cohomologie rigide à supports propres, Première partie," *Prépublication, Université de Rennes*, 1996.

[24] ——, "Finitude et pureté cohomologique en cohomologie rigide," *Invent. Math.*, vol. 128, pp. 329–377, 1997.

[25] A. G. B. Lauder, "A recursive method for computing the zeta functions of varieties," *LMS J. Comput. Math.*, vol. 9, pp. 222–269, 2006.

[26] ——, "Ranks of elliptic curves over function fields," *LMS J. Comput. Math.*, vol. 11, pp. 172–212, 2008.

[27] G. M. Walker, "Computing zeta functions of varieties via fibration," 2009.

[28] R. Kloosterman, "Point counting on singular hypersurfaces," in *Algorithmic Number Theory, 8th International Symposium, ANTS-VIII Proceedings*, A. van der Pooten and A. Stein, Eds., vol. 5011, Banff, Canada: Springer Verlag, 2008, pp. 327–341.

[29] P. Deligne, "Théorie de Hodge: II," *Publications Mathématiques de l'IHÉS*, vol. 40, pp. 5–57, 1971.

[30] K. Koyama, "Fast RSA-type schemes based on singular cubic curves $y^2 + axy \equiv x^3 \mod n$," in *Eurocrypt '95*, ser. Lec. Notes. in Comp. Sci. 1995, pp. 329–340.

[31] S. Arita, S. Miura, and T. Sekiguchi, "An addition algorithm on the Jacobian varieties of curves," *J. Ramanujan Math. Soc.*, vol. 19, no. 4, pp. 235–251, 2004.

[32] I. Déchène, "Arithmetic of Generalized Jacobians," in *Algorithmic Number Theory*, ser. Lecture Notes in Computer Science, vol. 4076, Springer Berlin Heidelberg, 2006, pp. 421–435.

[33] S. D. Galbraith and B. A. Smith, "Discrete logarithms in generalized Jacobians," 2006. arXiv: `math/0610073`.

[34] D. R. Kohel, "Constructive and destructive facets of torus-based cryptography," *preprint*, 2004.

[35] P. A. Griffiths, "On the periods of certain rational integrals: I," *Annals of Mathematics*, vol. 90, pp. 496–541, 1969.

[36] A. Dimca, "On the de Rham cohomology of a hypersurface complement," *American Journal of Mathematics*, vol. 113, no. 4, pp. 763–771, Aug., 1991.

[37] W. Fulton, *Algebraic Curves: An Introduction to Algebraic Geometry*, 2008 Edition, ser. Math. Lec. Note Series. W. A. Benjamin Inc, 1969.

[38] A. G. B. Lauder, "Degenerations and limit Frobenius structures in rigid cohomology," *London Math. Soc. J. Comp. Math.*, 2011.

[39] N. Jacobson, *Basic Algebra: II*, ser. Basic Algebra. W.H. Freeman & Company, 1989.

[40] Q. Liu, *Algebraic Geometry and Arithmetic Curves*. Oxford University Press, 2002.

[41] G. M. Walker, *Explicit crystalline lattices in rigid cohomology*, 2011. arXiv: `1110.4049`.

[42] R. Elkik, "Solutions d'équations à coefficients dans un anneau hensélien," *Ann. Sci. École Norm. Sup.*, vol. 6, pp. 553–603, 1973-74.

[43] A. Shiho, "Crystalline fundamental groups. II. Log convergent cohomology and rigid cohomology," *J. Math. Sci. Univ. Tokyo*, vol. 9, pp. 1–163, 2002.

[44] F. Baldassarri and B. Chiarellotto, "Algebraic versus rigid cohomology with logarithmic coefficients," in *Barsotti Symposium in Algebraic Geometry (Abano Terme,1991)*, Perspect. Math. 15, Academic Press, 1994, pp. 11–50.

[45] K. Kato, "Logarithmic structures of Fontaine-Illusie," in *Algebraic analysis, geometry, and number theory (Baltimore, MD, 1988)*, John Hopkins Univ. Press, 1989, pp. 191–224.

[46] R. Hartshorne, "On the de Rham cohomology of algebraic varieties," *Publications mathématiques de l'I.H.É.S.*, vol. 45, pp. 5–99, 1975.

[47] F. Baldassarri, M. Cailotto, and L. Fiorot, "Poincaré duality for algebraic de Rham cohomology," *manuscripta mathematica*, vol. 114, no. 1, pp. 61–116, 2004.

[48] P. Berthelot, "Géométrie rigide et cohomologie des variétés algébriques de caractéristique p," *Mém. de la Soc. Math. de France*, 2nd ser., vol. 23, pp. 7–32, 1986.

[49] N. Tsuzuki, "On the Gysin isomorphism of rigid cohomology," *Hiroshima Math. J.*, vol. 29, pp. 479–527, 1999.

[50] T. van den Bogaart, *About the choice of basis in Kedlaya's algorithm*, 2008. arXiv: `0809.1243`.

[51] N. Bourbaki, *Éléments de mathématique: Algèbre commutative*, VIII and IX. Springer, 2006.

[52] B. Edixhoven, "Point counting after Kedlaya," Notes from the EIDMA-Stieltjes graduate course in Leiden, 2003. [Online]. Available: `www.math.leidenuniv.nl/~edix/talks/2003_09_22-kedlaya-counting.pdf`.

[53] A. Dimca, *Singularities and Topology of Hypersurfaces*, ser. Universitext (1979). Springer-Verlag, 1992.

[54] N. Bourbaki, *Commutative Algebra*, ser. Elements of Mathematics I-VII. Paris: Hermann, 1972.

[55] P. Deligne and D. Mumford, "The irreducibility of the space of curves of a given genus," *Publ. Math., Inst. Hautes Étud. Sci.*, vol. 36, pp. 75–109, 1969.

[56] M. van der Put, "The cohomology of Monsky and Washnitzer, introductions aux cohomologies p-adiques," *Mém. Soc. Math. France*, vol. 23, pp. 33–59, 1986.

[57] A. Dimca, *Sheaves in Topology*. Berlin: Springer, 2004.

[58] A. Dimca and G. Sticlaru, "Koszul complexes and pole order filtrations," 2011. arXiv: 1108.3976.