

# Improvements to the deformation method for counting points on smooth projective hypersurfaces

Sebastian Pancratz, Jan Tuitman

September 11, 2014

## Abstract

We present various improvements to the deformation method for computing the zeta function of smooth projective hypersurfaces over finite fields using  $p$ -adic cohomology. This includes new bounds for the  $p$ -adic and  $t$ -adic precisions required to obtain provably correct results and gains in the efficiency of the individual steps of the method. The algorithm that we thus obtain has lower time and space complexities than existing methods. Moreover, our implementation is more practical and can be applied more generally, which we illustrate with examples of generic quintic curves and quartic surfaces.

## Contents

<b>1</b>	<b>Introduction</b>	<b>2</b>
<b>2</b>	<b>Theoretical background</b>	<b>3</b>
<b>3</b>	<b>Computing the connection matrix</b>	<b>8</b>
<b>4</b>	<b>Frobenius on diagonal hypersurfaces</b>	<b>15</b>
4.1	A formula for $\Phi_0$ . . . . .	15
4.2	Some estimates . . . . .	18
<b>5</b>	<b>Solving the differential equation</b>	<b>20</b>
<b>6</b>	<b>The zeta function of a fibre</b>	<b>24</b>
6.1	Evaluating $\Phi$ at a point . . . . .	24
6.2	Computing the zeta function . . . . .	28
<b>7</b>	<b>Complexity</b>	<b>31</b>
<b>8</b>	<b>Examples</b>	<b>36</b>
8.1	Quintic curve . . . . .	36
8.2	Quartic surface . . . . .	37
8.3	Generic quintic curve . . . . .	38
8.4	Generic quartic surface . . . . .	39
8.5	Larger primes . . . . .	40

# 1 Introduction

Let  $\mathbf{F}_q$  denote a finite field with  $q$  elements, where  $q$  is a power of the prime number  $p$ , and let  $X$  denote an algebraic variety over  $\mathbf{F}_q$ .

**Definition 1.1.** The zeta function of  $X$  is the formal power series

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

As we will see in the next section,  $Z(X, T)$  is a rational function, i.e. it is contained in  $\mathbf{Q}(T)$ , and hence can be given by a finite amount of data. Therefore, it is natural to ask whether it can be computed effectively and, in fact, it is not hard to provide an algorithm as follows. Using well known bounds by Bombieri [3] for the degrees of the numerator and denominator of  $Z(X, T)$ , one can reduce the computation of  $Z(X, T)$  to that of a finite number of the  $|X(\mathbf{F}_{q^i})|$ , which can be determined by naive counting.

A more interesting problem is whether, and if so how,  $Z(X, T)$  can be computed efficiently, where ‘efficiently’ can mean with low time complexity or just fast in practice. When  $X$  is a (hyper-)elliptic curve, this problem is important in cryptographic applications and has been the subject of much attention, resulting in very efficient algorithms. For example, when  $X$  is an elliptic curve, Schoof’s algorithm [27], which uses  $\ell$ -adic étale cohomology, has runtime polynomial in  $\log(q)$ , and is also very fast in practice using improvements due to Atkins and Elkies.

For more general algebraic varieties  $X$ , the only available option is usually to compute the rigid cohomology spaces of  $X$ , with their natural action of the Frobenius map, and then use a Lefschetz formula to deduce the zeta function. This method was introduced by Kedlaya in the case of hyperelliptic curves in odd characteristic [15]. The same idea has been shown to work in much greater generality, for example for smooth projective hypersurfaces [1].

Lauder [21, 22] showed that instead of computing the action of the Frobenius map on the rigid cohomology spaces of a smooth projective hypersurface  $X$  directly, it is better, at least in terms of time complexity, to embed  $X$  in a family of smooth projective hypersurfaces containing a diagonal hypersurface. Following his deformation method, one first computes the action of the Frobenius map on the rigid cohomology of the diagonal hypersurface, and then solves a  $p$ -adic differential equation to obtain the Frobenius map on the rigid cohomology of the original hypersurface.

To be more precise, in [21, 22] Lauder did not directly work with rigid cohomology but with Dwork cohomology. While the two cohomology theories are equivalent, various comparison and finiteness results are more easily stated and proved in the context of rigid cohomology. In [10] Gerkmann reformulated Lauder’s deformation method in terms of rigid cohomology. Moreover, he improved various precision bounds, making the algorithm more practical, which he demonstrated with many examples. Kedlaya introduced new ideas and results to further lower the precision bounds for the deformation method in [18].

The aim of this paper is to continue where Lauder, Gerkmann and Kedlaya left off. We make improvements to almost every step of the algorithm. This results in an algorithm with both lower time and space complexity than Lauder’s original algorithm, but perhaps more importantly, which is a lot more efficient in practice. The first author has written a (publicly available) implementation of our algorithm using the library FLINT [12]. This implementation lowers the runtimes of the examples in [10] by factors of 50 to 5,000. Moreover, it can be used to compute the zeta function in many cases where this was not possible before, e.g. for generic quartic surfaces.

We now briefly describe the contents of the remaining sections, necessarily relying on some terminology that is introduced only in Section 2. The reader who is not familiar with this terminology might prefer to start reading there.

In Section 2, we recall the main theoretical results that underpin the remaining sections of the paper. We limit ourselves to the bare minimum as there are already good references available for the relevant theory, see e.g. [18]. We also introduce the required terminology and notation. We conclude the section with an overview of the different steps of the deformation method, which are then treated individually in the next four sections.

In Section 3, we explain how to compute the Gauss–Manin connection on the cohomology of a family of smooth projective hypersurfaces. We define an explicit monomial basis for the cohomology that we will use throughout the paper. Our most important result in this section is Theorem 3.6, which allows us to compute very efficiently in the cohomology. We formalise the computation of the Gauss–Manin connection matrix in Algorithm 3.3. We also prove some lower bounds for the valuation of the matrix of Frobenius and its inverse that are essential for controlling the  $p$ -adic precision loss in the algorithm.

In Section 4, we show how to compute the Frobenius matrix of a diagonal hypersurface over a prime field. Our method is essentially based on a computation of Dwork, but by rewriting and slightly generalising his formulas we obtain Algorithm 4.1, which is a significant improvement to the corresponding algorithms of Lauder and Gerkmann, both in terms of time complexity and in practice.

In Section 5, we explain how to solve the differential equation for the Frobenius matrix. We use the same method as Lauder but incorporate improved convergence bounds for  $p$ -adic differential equations by Kedlaya. We collect the precision bounds that follow from our analysis in Theorem 5.8 and formalise the computation of the power series expansion of the Frobenius matrix in Algorithm 5.1.

In Section 6, we describe how to evaluate the Frobenius matrix at some fibre and compute its zeta function. We combine various bounds from different sources to lower the required  $p$ -adic and  $t$ -adic precisions. This finally results in Algorithm 6.1, which combines all of our previous algorithms, and is the main result of the paper.

In Section 7, we analyse the time and space complexity of our algorithm and compare these to Lauder’s work [21]. In Section 8, we compute various numerical examples, and compare our runtimes to those provided by Gerkmann [10].

Both authors were supported by the European Research Council (grant 204083) and additionally the second author was supported by FWO - Vlaanderen. We would like to thank Alan Lauder for all his help and in particular for his comments and suggestions on earlier versions of this paper. Finally, we thank the anonymous referees for their comments and suggestions.

## 2 Theoretical background

We start by recalling the main result about the zeta function of algebraic varieties over finite fields.

**Theorem 2.1** (Weil conjectures). *If  $X/\mathbf{F}_q$  is a smooth projective variety of dimension  $m$ , then*

$$Z(X, T) = \frac{p_1 p_3 \cdots p_{2m-1}}{p_0 p_2 p_4 \cdots p_{2m}},$$

where for all  $i$ :

- (i)  $p_i = \prod_j (1 - \alpha_{i,j} T) \in \mathbf{Z}[T]$ ,
- (ii) the transformation  $t \rightarrow q^m/t$  maps the  $\alpha_{i,j}$  bijectively to the  $\alpha_{2m-i,k}$ , preserving multiplicities,
- (iii)  $|\alpha_{i,j}| = q^{i/2}$  for all  $j$ , and every embedding  $\bar{\mathbf{Q}} \hookrightarrow \mathbf{C}$ .

*Proof.* The proof of this theorem was completed by Deligne in [5].  $\square$

We let  $\mathbf{Q}_q$  denote the unique unramified extension of  $\mathbf{Q}_p$  with residue field  $\mathbf{F}_q$  and  $\mathbf{Z}_q$  its ring of integers. We denote the  $p$ -adic valuation on  $\mathbf{Q}_q$  by  $\text{ord}_p(-)$ .

**Definition 2.2.** Let  $H_{\text{rig}}^i(X)$  denote the rigid cohomology spaces of  $X$ . These are finite dimensional vector spaces over  $\mathbf{Q}_q$  that are contravariantly functorial in  $X$ , and they are equipped with an action of the  $p$ -th and  $q$ -th power Frobenius map on  $X$  that we denote by  $F_p$  and  $F_q$ , respectively. For the construction and basic properties of these spaces we refer to [2].

The relation between the zeta function and the rigid cohomology spaces is given by the so called Lefschetz formula.

**Theorem 2.3** (Lefschetz formula). If  $X$  is a smooth proper algebraic variety over  $\mathbf{F}_q$  of dimension  $m$ , then

$$Z(X, T) = \prod_{i=0}^{2m} \det(1 - T F_q | H_{\text{rig}}^i(X))^{(-1)^{i+1}}.$$

*Proof.* See for example [9, Theorem 6.3].  $\square$

Let  $\pi: \mathfrak{X} \rightarrow \mathfrak{S}$  be a smooth family of algebraic varieties defined over  $\mathbf{Q}_q$ .

**Definition 2.4.** Let  $H_{\text{dR}}^i(\mathfrak{X}/\mathfrak{S})$  denote the  $i$ -th relative algebraic de Rham cohomology sheaf on  $\mathfrak{S}$ . If  $\mathfrak{X}/\mathfrak{S}$  admits a relative normal crossing compactification, then the  $H_{\text{dR}}^i(\mathfrak{X}/\mathfrak{S})$  are vector bundles.

The  $H_{\text{dR}}^i(\mathfrak{X}/\mathfrak{S})$  come equipped with an integrable connection, which is called the Gauss–Manin connection. Let us first recall the notion of a connection on a vector bundle.

**Definition 2.5.** Let  $\mathfrak{E}$  be a vector bundle on  $\mathfrak{S}$ . A connection on  $\mathfrak{E}$  is a map of vector bundles  $\nabla: \mathfrak{E} \rightarrow \Omega_{\mathfrak{S}}^1 \otimes \mathfrak{E}$  which satisfies the Leibniz rule

$$\nabla(fe) = f\nabla(e) + df \otimes e$$

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

The Gauss–Manin connection on  $H_{\text{dR}}^i(\mathfrak{X}/\mathfrak{S})$  can be defined as follows.

**Definition 2.6.** The de Rham complex  $\Omega_{\mathfrak{X}}^{\bullet}$  can be equipped with the decreasing filtration

$$F^i = \text{im}(\Omega_{\mathfrak{X}}^{\bullet-i} \otimes \pi^* \Omega_{\mathfrak{S}}^i \rightarrow \Omega_{\mathfrak{X}}^{\bullet}).$$

The spectral sequence associated to this filtration has as its first sheet

$$E_1^{p,q} = \Omega_{\mathfrak{S}}^p \otimes H_{\text{dR}}^q(\mathfrak{X}/\mathfrak{S}).$$

The Gauss–Manin connection  $\nabla: H^i(\mathfrak{X}/\mathfrak{S}) \rightarrow \Omega_{\mathfrak{S}}^1 \otimes H^i(\mathfrak{X}/\mathfrak{S})$  is now defined as the differential  $d_1: E_1^{0,i} \rightarrow E_1^{1,i}$  in this spectral sequence.

**Remark 2.7.** We can give a more explicit description of  $\nabla$  when  $\mathfrak{X}/\mathfrak{S}$  is affine. If we lift a relative  $i$ -cocycle  $\omega \in \Omega_{\mathfrak{X}/\mathfrak{S}}^i$  to an absolute  $i$ -form  $\omega' \in \Omega_{\mathfrak{X}}^i$  and apply the absolute differential  $d$ , we get an element of  $\Omega_{\mathfrak{S}}^1 \wedge \Omega_{\mathfrak{X}/\mathfrak{S}}^i$ . Projecting onto  $\Omega_{\mathfrak{S}}^1 \otimes H_{\text{dR}}^i(\mathfrak{X}/\mathfrak{S})$ , we obtain  $\nabla(\omega)$ .

**Definition 2.8.** We write  $\sigma$  for the standard  $p$ -th power Frobenius lift on  $\mathbf{P}_{\mathbf{Q}_q}^1$ , i.e. the semilinear map that lifts the  $p$ -th power Frobenius map on  $\mathbf{P}_{\mathbf{F}_q}^1$  and satisfies  $\sigma(t) = t^p$ .

Now suppose that  $\mathfrak{E}$  is a vector bundle with connection on some Zariski open subset  $\mathfrak{S}$  of  $\mathbf{P}_{\mathbf{Q}_q}^1$  with complement  $\mathfrak{Z}$ . Let  $V$  denote the rigid analytic subspace of  $\mathbf{P}_{\mathbf{Q}_q}^1$  which is the complement of the union of the open disks of radius 1 around the points of  $\mathfrak{Z}$ .

**Definition 2.9.** A Frobenius structure on  $\mathfrak{E}$  is an isomorphism of vector bundles with connection  $F: \sigma^* \mathfrak{E} \rightarrow \mathfrak{E}$  defined on some strict neighbourhood of  $V$ .

**Theorem 2.10.** Let  $\mathcal{S}$  be a Zariski open subset of  $\mathbf{P}_{\mathbf{Z}_q}^1$  and suppose that  $\mathcal{X}/\mathcal{S}$  is a smooth family of algebraic varieties that admits a relative normal crossing compactification. Denote the generic fibres of  $\mathcal{S}, \mathcal{X}$  by  $\mathfrak{S} = \mathcal{S} \otimes \mathbf{Q}_q, \mathfrak{X} = \mathcal{X} \otimes \mathbf{Q}_q$  and the special fibres by  $S = \mathcal{S} \otimes \mathbf{F}_q, X = \mathcal{X} \otimes \mathbf{F}_q$ , respectively. The vector bundle  $H_{\text{dR}}^i(\mathfrak{X}/\mathfrak{S})$  with the Gauss–Manin connection  $\nabla$  admits a Frobenius structure  $F$  with the following property. For any finite field extension  $\mathbf{F}_q/\mathbf{F}_q$  and all  $\tau \in S(\mathbf{F}_q)$ ,

$$(H_{\text{rig}}^i(X_\tau), F_p) \cong (H_{\text{dR}}^i(\mathfrak{X}/\mathfrak{S}), F)_{\hat{\tau}}$$

as  $\mathbf{Q}_q$ -vector spaces with a  $\sigma$ -semilinear endomorphism, where  $\hat{\tau} \in \mathcal{S}(\mathbf{Z}_q)$  denotes the Teichmüller lift of  $\tau$ . We will therefore denote this Frobenius structure on  $H_{\text{dR}}^i(\mathfrak{X}/\mathfrak{S})$  by  $F_p$  as well.

*Proof.* This result is well known, see for example [18, Theorem 6.1.3]. Although it is usually attributed to Berthelot, a complete reference seems to be missing from the literature.  $\square$

**Definition 2.11.** Let  $H_{\text{rig}}^i(X/S)$  denote the vector bundle  $H_{\text{dR}}^i(\mathfrak{X}/\mathfrak{S})$  with its Frobenius structure  $F_p$  from Theorem 2.10.

**Remark 2.12.** One can show that  $H_{\text{rig}}^i(X/S)$  is again functorial in  $X/S$  and so does not depend on the lift  $\mathcal{X}/\mathcal{S}$ . Moreover, one can still define  $H_{\text{rig}}^i(X/S)$  when  $X/S$  cannot be lifted to characteristic zero, see [2]. However, for our purposes the above definition will be sufficient.

In this paper we restrict our attention to one-parameter families of smooth projective hypersurfaces. So we let  $P \in \mathbf{Z}_q[t][x_0, \dots, x_n]$  denote a homogeneous polynomial of degree  $d$  and let  $\mathcal{S} \subset \mathbf{P}_{\mathbf{Z}_q}^1$  be a Zariski open subset such that  $P$  defines a family  $\mathcal{X}/\mathcal{S}$  of smooth hypersurfaces contained in  $\mathbf{P}_{\mathcal{S}}^n$ . We let  $\mathcal{U}/\mathcal{S}$  denote the complement of  $\mathcal{X}/\mathcal{S}$  in  $\mathbf{P}_{\mathcal{S}}^n$ , and write  $\mathfrak{X} = \mathcal{X} \otimes \mathbf{Q}_q, \mathfrak{U} = \mathcal{U} \otimes \mathbf{Q}_q, \mathfrak{S} = \mathcal{S} \otimes \mathbf{Q}_q$  for the generic fibres, and  $X = \mathcal{X} \otimes \mathbf{F}_q, U = \mathcal{U} \otimes \mathbf{F}_q, S = \mathcal{S} \otimes \mathbf{F}_q$  for the special fibres of  $\mathcal{X}, \mathcal{U}, \mathcal{S}$ , respectively. Moreover, we let  $\mathbf{F}_q/\mathbf{F}_q$  denote a finite field extension and denote  $a = \log_p(\mathfrak{q})$ .

**Theorem 2.13.** For all  $\tau \in S(\mathbf{F}_q)$ , we have

$$Z(X_\tau, T) = \frac{\chi(T)^{(-1)^n}}{(1-T)(1-\mathfrak{q}T) \cdots (1-\mathfrak{q}^{n-1}T)}, \quad (2.1)$$

where  $\chi(T) = \det(1 - T\mathfrak{q}^{-1}\mathbf{F}_q | H_{\text{rig}}^n(U_\tau)) \in \mathbf{Z}[T]$  denotes the reverse characteristic polynomial of the action of  $\mathfrak{q}^{-1}\mathbf{F}_q$  on  $H_{\text{rig}}^n(U_\tau)$ . Moreover, the polynomial  $\chi(T)$  has degree

$$\frac{1}{d}((d-1)^{n+1} + (-1)^{n+1}(d-1)). \quad (2.2)$$

*Proof.* This theorem is well known, see for example [1]. Since we need some intermediate results from the proof later on, we will give a brief sketch here. First, by Theorem 2.3, we have

$$Z(X_\tau, T) = \prod_{i=0}^{2(n-1)} \det(1 - T\mathbf{F}_q | H_{\text{rig}}^i(X_\tau))^{(-1)^{i+1}}.$$

Then, by the Lefschetz hyperplane theorem and Poincaré duality, we see that  $H_{\text{rig}}^i(X_\tau) \cong H_{\text{rig}}^i(\mathbf{P}_{\mathbf{F}_q}^n)$  for all  $i \neq (n-1)$ . Next, one shows by a computation that

$$H_{\text{rig}}^i(\mathbf{P}_{\mathbf{F}_q}^n) \cong \begin{cases} \mathbf{Q}_q(i) & \text{if } i \text{ even,} \\ 0 & \text{if } i \text{ odd,} \end{cases} \quad (2.3)$$

where  $(i)$  denotes the  $i$ -th Tate twist, for which  $\mathbf{F}_p$  is multiplied by  $p^{-i}$ . It remains to determine  $H_{\text{rig}}^{n-1}(X_\tau)$ . One uses the excision short exact sequence

$$0 \longrightarrow H_{\text{rig}}^n(U_\tau) \longrightarrow H_{\text{rig}}^{n-1}(X_\tau)(-1) \longrightarrow H_{\text{rig}}^{n+1}(\mathbf{P}_{\mathbf{F}_q}^n) \longrightarrow 0 \quad (2.4)$$

to relate  $H_{\text{rig}}^{n-1}(X_\tau)$  to  $H_{\text{rig}}^n(U_\tau)$  and complete the proof of (2.1). We will show in Proposition 3.8 that the dimension of  $H_{\text{rig}}^{n-1}(U_\tau)$  is given by (2.2).  $\square$

Let  $[e_1, \dots, e_b]$  be some basis of sections of  $H_{\text{dR}}^n(\mathcal{U}/\mathcal{S})$ , and let  $M \in M_{b \times b}(\mathbf{Q}_q(t))$  denote the matrix of the Gauss–Manin connection  $\nabla$  with respect to this basis, i.e.

$$\nabla(e_j) = \sum_{i=1}^b M_{i,j} e_i.$$

Let  $r \in \mathbf{Z}_q[t]$  with  $\text{ord}_p(r) = 0$  be a denominator for  $M$ , i.e. such that we can write  $M = G/r$  with  $G \in M_{b \times b}(\mathbf{Q}_q[t])$ , and let  $\Phi$  denote the matrix of  $p^{-1}F_p$  with respect to the basis  $[e_1, \dots, e_b]$ , i.e.

$$p^{-1}F_p(e_j) = \sum_{i=1}^b \Phi_{i,j} e_i.$$

**Definition 2.14.** We define the ring of overconvergent functions

$$\mathbf{Q}_q\langle t, 1/r \rangle^\dagger = \left\{ \sum_{i,j=0}^{\infty} a_{i,j} \frac{t^i}{r^j} : a_{i,j} \in \mathbf{Q}_q, \exists c > 0 \text{ s.t. } \lim_{i+j \rightarrow \infty} (\text{ord}_p(a_{i,j}) - c(i+j)) \geq 0 \right\},$$

as the  $p$ -adically meromorphic functions on  $\mathbf{P}_{\mathbf{Q}_q}^1$  that are analytic outside of the open disks of radius  $\rho$  around the zeros of  $r$  and the point at infinity for some  $\rho < 1$ .

**Definition 2.15.** We extend the  $p$ -adic valuation to  $\mathbf{Q}_q\langle t, 1/r \rangle^\dagger$  in the standard way, i.e.  $\text{ord}_p(f)$  is defined as the maximum, over all ways of writing the element  $f$  as  $\sum_{i,j=0}^{\infty} a_{i,j} t^i / r^j$ , of the minimum, over  $i, j \geq 0$ , of  $\text{ord}_p(a_{i,j})$ . Note that the norm on  $\mathbf{Q}_q\langle t, 1/r \rangle^\dagger$  corresponding to this valuation is the Gauss norm. We also extend  $\text{ord}_p(-)$  to polynomials and matrices over  $\mathbf{Q}_q\langle t, 1/r \rangle^\dagger$ , by taking the minimum over the coefficients and entries, respectively.

**Assumption 2.16.** From now on we will always assume that  $0 \in \mathcal{S}$ . Note that if this is not the case, then it can be achieved by applying a translation.

**Theorem 2.17.** The matrix  $\Phi$  is an element of  $M_{b \times b}(\mathbf{Q}_q\langle t, 1/r \rangle^\dagger)$  and satisfies the differential equation

$$\left( \frac{d}{dt} + M \right) \Phi = p t^{p-1} \Phi \sigma(M), \quad \Phi(0) = \Phi_0,$$

where  $\Phi_0$  is the matrix of  $p^{-1}F_p$  on  $H_{\text{rig}}^n(U_0)$  with respect to the basis  $[e_0, \dots, e_b]$ .

*Proof.* That the differential equation is satisfied is an immediate consequence of the fact that  $F_p$  is a horizontal map of vector bundles with connection, and that  $\Phi(0) = \Phi_0$  is also clear from Theorem 2.10. Note that by a residue disk on  $\mathcal{S}$  we mean all points on  $\mathcal{S}(\bar{\mathbf{Q}}_q)$  that reduce modulo  $p$  to a given point of  $S(\bar{\mathbf{F}}_q)$ . If  $M$  does not have any poles in a given residue disk, then  $\Phi$  cannot have any poles in that residue disk either, by Theorem 6.1 below. Hence the entries of  $\Phi$  are contained in  $\mathbf{Q}_q\langle t, 1/r \rangle^\dagger$ .  $\square$

The deformation method can now be sketched as follows:

- Step 1.* Compute the matrix  $M$  of the Gauss–Manin connection  $\nabla$ .
- Step 2.* Compute the matrix  $\Phi_0$  of the action of  $p^{-1}F_p$  on  $H_{\text{rig}}^n(U_0)$ . If the family is chosen such that  $X_0$  is a diagonal hypersurface over a prime field, this can be done as explained in Chapter 4.
- Step 3.* Solve the differential equation from Theorem 2.17 for  $\Phi$ .
- Step 4.* Substitute the Teichmüller lift  $\hat{\tau}$  of an element  $\tau \in S(\mathbf{F}_q)$  into  $\Phi$  to obtain the matrix  $\Phi_\tau$  of the action of  $p^{-1}F_p$  on  $H_{\text{rig}}^n(U_\tau)$ . Compute the matrix  $\Phi_\tau^{(a)}$  of the action of  $\mathfrak{q}^{-1}F_{\mathfrak{q}}$  on  $H_{\text{rig}}^n(U_\tau)$ , which is also equal to  $(p^{-1}F_p)^a$ . Use Theorem 2.13 to compute the zeta function  $Z(X_\tau, T)$  of the fibre  $X_\tau$ .

Note that we can only carry out these computations to finite  $p$ -adic precision. Therefore, we need to recall some bounds on the loss of  $p$ -adic precision when multiplying  $p$ -adic numbers and matrices.

**Proposition 2.18.** Let  $v_1, \dots, v_\ell \in \mathbf{Z}$  and  $x_1, \dots, x_\ell \in \mathbf{Q}_q$ ,  $\ell \geq 2$ , be such that  $\text{ord}_p(x_i) \geq v_i$  for all  $i$ . Suppose that  $N \in \mathbf{Z}$  satisfies  $N \geq \sum_{j=1}^{\ell} v_j$ . Let  $\tilde{x}_1, \dots, \tilde{x}_\ell$  denote  $p$ -adic approximations to  $x_1, \dots, x_\ell$  such that

$$\text{ord}_p(x_i - \tilde{x}_i) \geq N - \sum_{j \neq i} v_j$$

for all  $i$ . Then

$$\text{ord}_p(x_1 \cdots x_\ell - \tilde{x}_1 \cdots \tilde{x}_\ell) \geq N.$$

*Proof.* For all  $i$ ,

$$\begin{aligned} \text{ord}_p(\tilde{x}_i) &\geq \min\{\text{ord}_p(x_i - \tilde{x}_i), \text{ord}_p(x_i)\} \\ &\geq \min\left\{N - \sum_{j \neq i} v_j, \text{ord}_p(x_i)\right\} \geq v_i. \end{aligned}$$

Therefore, we also have that

$$\text{ord}_p((x_i - \tilde{x}_i)(\tilde{x}_1 \cdots \tilde{x}_{i-1} x_{i+1} \cdots x_\ell)) \geq N,$$

for all  $i$ . The result now follows by adding these  $\ell$  inequalities.  $\square$

**Proposition 2.19.** Let  $v_1, \dots, v_\ell \in \mathbf{Z}$  and  $A_1, \dots, A_\ell \in M_{b \times b}(\mathbf{Q}_q)$ ,  $\ell \geq 2$ , be such that  $\text{ord}_p(A_i) \geq v_i$  for all  $i$ . Suppose that  $N \in \mathbf{Z}$  satisfies  $N \geq \sum_{j=1}^{\ell} v_j$ . Let  $\tilde{A}_1, \dots, \tilde{A}_\ell$  denote  $p$ -adic approximations to  $A_1, \dots, A_\ell$  such that

$$\text{ord}_p(A_i - \tilde{A}_i) \geq N - \sum_{j \neq i} v_j$$

for all  $i$ . Then

$$\text{ord}_p(A_1 \cdots A_\ell - \tilde{A}_1 \cdots \tilde{A}_\ell) \geq N. \quad (2.5)$$

*Proof.* We can follow the proof of Proposition 2.18, observing that for matrices  $A, B \in M_{b \times b}(\mathbf{Q}_q)$ , we still have that  $\text{ord}_p(A + B) \geq \min\{\text{ord}_p(A), \text{ord}_p(B)\}$  and  $\text{ord}_p(AB) \geq \text{ord}_p(A) + \text{ord}_p(B)$ .  $\square$

### 3 Computing the connection matrix

In this section we compute the action of the Gauss–Manin connection  $\nabla$  on the algebraic de Rham cohomology  $H_{\text{dR}}^n(\mathfrak{U}/\mathfrak{S})$  of the generic fiber  $\mathfrak{U}/\mathfrak{S} = \mathcal{U}/\mathcal{S} \otimes \mathbf{Q}_q$  of the complement  $\mathcal{U}/\mathcal{S}$  of a family of smooth hypersurfaces  $\mathcal{X}/\mathcal{S}$  contained in  $\mathbf{P}_{\mathfrak{S}}^n$  over some Zariski open subset  $\mathcal{S} \subset \mathbf{P}_{\mathfrak{Z}_q}^1$ . Let  $\mathcal{X}/\mathcal{S}$  be defined by a homogeneous polynomial  $P \in \mathbf{Z}_q[t][x_0, \dots, x_n]$  of degree  $d$ . First we recall how to compute in  $H_{\text{dR}}^n(\mathfrak{U}/\mathfrak{S})$  following the method of Griffiths and Dwork.

**Proposition 3.1.** Let  $\Omega$  denote the  $n$ -form on  $\mathfrak{U}/\mathfrak{S}$  defined by

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

The algebraic de Rham cohomology space  $H_{\text{dR}}^n(\mathfrak{U}/\mathfrak{S})$  is isomorphic to the quotient of the space of closed  $n$ -forms  $Q\Omega/P^k$  with  $k \in \mathbf{N}$  and  $Q \in H^0(\mathfrak{S}, \mathcal{O}_{\mathfrak{S}})[x_0, x_1, \dots, x_n]$  homogeneous of degree  $kd - (n+1)$ , by the subspace of exact  $n$ -forms generated by

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

for all  $0 \leq i \leq n$  with  $k \in \mathbf{N}$  and  $Q \in H^0(\mathfrak{S}, \mathcal{O}_{\mathfrak{S}})[x_0, x_1, \dots, x_n]$  homogeneous of degree  $kd - n$ , where  $\partial_i$  denotes the partial derivative operator with respect to  $x_i$ .

*Proof.* The proof is straightforward, for details see [11, §4].  $\square$

The cohomology space  $H_{\text{dR}}^n(\mathfrak{U}/\mathfrak{S})$  is equipped with an increasing filtration by the pole order, for which  $\text{Fil}^k H_{\text{dR}}^n(\mathfrak{U}/\mathfrak{S})$  consists of all elements that can be represented by  $n$ -forms  $Q\Omega/P^k$  with  $Q \in H^0(\mathfrak{S}, \mathcal{O}_{\mathfrak{S}})[x_0, x_1, \dots, x_n]$  homogeneous of degree  $kd - (n+1)$ . It follows from a theorem of Macaulay [11, (4.11)] that  $\text{Fil}^n H_{\text{dR}}^n(\mathfrak{U}/\mathfrak{S}) = H_{\text{dR}}^n(\mathfrak{U}/\mathfrak{S})$ . Actually, the reverse filtration  $H_i = \text{Fil}^{n-i} H_{\text{dR}}^n(\mathfrak{U}/\mathfrak{S})$  corresponds to the restriction of the Hodge filtration on  $H_{\text{dR}}^{n-1}(\mathfrak{X}/\mathfrak{S})$  to  $H_{\text{dR}}^n(\mathfrak{U}/\mathfrak{S})$  by [11, (8.6.)].

As we prefer to perform linear algebra operations over a field, we will actually work with the de Rham cohomology vector space  $H_{\text{dR}}^n(\mathfrak{U}_{\mathbf{Q}_q(t)})$  of the generic fibre

$$\mathfrak{U}_{\mathbf{Q}_q(t)} = \mathfrak{U}/\mathfrak{S} \times_{\mathfrak{S}} \text{Spec } \mathbf{Q}_q(t).$$

We now define an explicit basis of a simple form for  $H_{\text{dR}}^n(\mathfrak{U}_{\mathbf{Q}_q(t)})$  for the families that we are interested in.

**Definition 3.2.** For  $k \in \mathbf{N}$ , we define the following sets of monomials:

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

where  $x^u = x_0^{u_0} \cdots x_n^{u_n}$  and  $|u| = \sum_{i=0}^n u_i$ . We also define

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

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

We will show below that if the family  $\mathcal{X}/\mathcal{S}$  contains a diagonal fibre, then the set  $\mathcal{B}$  forms a basis for  $H_{\text{dR}}^n(\mathfrak{U}_{\mathbf{Q}_q(t)})$ .

**Definition 3.3.** For  $k \in \mathbf{N}$ , let  $C_k^{(0)}$  be the set of monomials of total degree  $(k-1)d - n$  and then inductively, for  $1 \leq j \leq n$ , define  $C_k^{(j)}$  to be the set of monomials in  $C_k^{(j-1)}$  except for those divisible by  $x_{j-1}^{d-1}$ . Moreover, we define the multi-set  $C_k$  as the disjoint union of  $C_k^{(0)}, \dots, C_k^{(n)}$ . We shall write an element of this multi-set as  $(j, g)$ , when referring to a monomial  $g$  in  $C_k^{(j)}$ .



**Lemma 3.4.** For all  $k \in \mathbf{N}$ , the multi-sets  $R_k$  and  $C_k$  have the same cardinality.

*Proof.* We construct a bijection  $R_k \rightarrow C_k$ , representing the monomials by their exponent tuples. Let  $u = (u_0, \dots, u_n)$  be an element of  $R_k$ . If  $u_0 \geq d-1$ , we define the image as  $(u_0-d-1, u_1, \dots, u_n) \in C_k^{(0)}$ . More generally, if  $u_0 < d-1, \dots, u_{j-1} < d-1$  and  $u_j \geq d-1$ , we define the image as  $(u_0, \dots, u_{j-1}, u_j-(d-1), u_{j+1}, \dots, u_n) \in C_k^{(j)}$ . It is easy to verify that this map is indeed a bijection.  $\square$

**Definition 3.5.** We define a square matrix  $\Delta_k$  with row and column index sets  $R_k$  and  $C_k$  as follows. Given  $f \in R_k$  and  $(j, g) \in C_k$ , we set the corresponding entry in  $\Delta_k$  to be the coefficient of the monomial  $f/g$  in  $\partial_j P$  if  $g$  divides  $f$  and 0 otherwise.

**Theorem 3.6.** Suppose that the family  $\mathcal{X}/\mathcal{S}$  of smooth projective hypersurfaces given by the polynomial  $P$  in  $\mathbf{Z}_q[t][x_0, \dots, x_n]$  contains a diagonal fibre. For  $k \in \mathbf{N}$  and  $0 \leq j \leq n$ , let  $U_k^{(j)}$  be the  $\mathbf{Q}_q(t)$ -vector space of polynomials with basis  $C_k^{(j)}$ , and let  $U_k$  denote the cartesian product  $U_k = U_k^{(0)} \times \dots \times U_k^{(n)}$ . Moreover, let  $V_k$  and  $W_k$  be the  $\mathbf{Q}_q(t)$ -vector spaces of polynomials with bases  $F_k$  and  $R_k$ , respectively, and let  $\pi: V_k \rightarrow W_k$  denote the linear map that sends the elements of  $B_k$  to zero and the elements of  $R_k$  to themselves. Then the map

$$\phi_k: U_k \rightarrow W_k, \quad (Q_0, \dots, Q_n) \mapsto \pi(Q_0 \partial_0 P + \dots + Q_n \partial_n P) \quad (3.1)$$

is an isomorphism of  $\mathbf{Q}_q(t)$ -vector spaces.

*Proof.* Recall that  $R_k$  and  $C_k$  have the same cardinality by Lemma 3.4. If  $R_k$  and  $C_k$  are empty, then  $U_k$  and  $W_k$  are the zero vector spaces, and the theorem holds trivially. So suppose that  $R_k$  and  $C_k$  are nonempty. It is immediate that  $\Delta_k$  is the matrix representing  $\phi_k$  with respect to the bases  $C_k$  and  $R_k$  of  $U_k$  and  $W_k$ , respectively.

The assumption that the family  $\mathcal{X}/\mathcal{S}$  contains a diagonal hypersurface means that for some  $t_0 \in \mathcal{S}(\mathbf{Z}_q)$ , the fibre  $\mathcal{X}_{t_0}$  is defined by a polynomial of the form

$$P_{t_0}(x_0, \dots, x_n) = a_0 x_0^d + \dots + a_n x_n^d$$

with  $a_0, \dots, a_n \in \mathbf{Z}_q^\times$ .

We now show that the determinant of  $\Delta_k$  is nonzero. Since evaluation of the matrix at  $t = t_0$  commutes with computing the determinant, it suffices to show that the determinant of  $(\Delta_k)|_{t=t_0}$  is nonzero. Since, for  $0 \leq j \leq n$ , we have  $\partial_j P_{t_0}(x_0, \dots, x_n) = da_j x_j^{d-1}$ , there is precisely one nonzero entry in each column and each row of  $\Delta_k$ . Namely, in column  $(j, g) \in C_k$  and row  $gx_j^{d-1} \in R_k$  there is the nonzero entry  $da_j$ . Note that this also implies that  $(\Delta_k)|_{t=t_0} \in \mathbf{Z}_q^\times$ .  $\square$

We can use Theorem 3.6 to give a routine DECOMPOSE, formalised in Algorithm 3.1, which given  $Q \in \mathbf{Q}_q(t)[x_0, \dots, x_n]$  homogeneous of degree  $kd - (n+1)$  returns an expression

$$Q = Q_0 \partial_0 P + \dots + Q_n \partial_n P + \gamma_k$$

with  $Q_0, \dots, Q_n \in \mathbf{Q}_q(t)[x_0, \dots, x_n]$  homogeneous of degree  $kd - n$  and  $\gamma_k$  in the  $\mathbf{Q}_q(t)$ -span of  $B_k$ . We can in turn use DECOMPOSE to furnish another routine REDUCE, formalised in Algorithm 3.2, which given a closed  $n$ -form  $Q\Omega/P^k$  with  $Q \in \mathbf{Q}_q(t)[x_0, \dots, x_n]$  homogeneous of degree  $kd - (n+1)$  returns an expression

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

with  $\gamma_i$  in the  $\mathbf{Q}_q(t)$ -span of  $B_i$  for  $1 \leq i \leq n$  and where  $\equiv$  denotes equality in cohomology.

---

**Algorithm 3.1** Obtain coordinates in the Jacobian ideal modulo basis elements

---

**Input:**  $P$  in  $\mathbf{Z}_q[t][x_0, \dots, x_n]$  homogeneous of degree  $d$ , defining a family  $\mathcal{X}/\mathcal{S}$  of smooth projective hypersurfaces that contains a diagonal fibre,  $Q \in \mathbf{Q}_q(t)[x_0, \dots, x_n]$  homogeneous of degree  $kd - (n + 1)$ .

**Output:**  $Q_0, \dots, Q_n \in \mathbf{Q}_q(t)[x_0, \dots, x_n]$  homogeneous of degree  $k(d - 1) - n$ , and  $\gamma_k$  in the  $\mathbf{Q}_q(t)$ -span of  $B_k$ , such that  $Q = Q_0 \partial P_0 + \dots + Q_n \partial_n P + \gamma_k$ .

**procedure** DECOMPOSE( $P, Q$ )

1. Let  $w$  be the vector of length  $|R_k|$  such that the entry corresponding to  $x^u \in R_k$  is the coefficient of  $x^u$  in  $Q$ .
  2. Solve for the unique vector  $v$  of length  $|C_k|$  satisfying  $\Delta_k v = w$ . We write  $v$  as  $(v^{(0)}, \dots, v^{(n)})$ , where  $v^{(j)}$  is a vector of length  $|C_k^{(j)}|$  for  $0 \leq j \leq n$ , and let  $v_g^{(j)}$  be the entry in  $v^{(j)}$  corresponding to  $g \in C_k^{(j)}$ .
  3. For  $0 \leq j \leq n$ , compute  $Q_j \leftarrow \sum_{g \in C_k^{(j)}} v_g^{(j)} g$ .
  4. Set  $\gamma_k \leftarrow Q - (Q_0 \partial P_0 + \dots + Q_n \partial_n P)$ .
  5. **return**  $Q_0, \dots, Q_n, \gamma_k$
- 

---

**Algorithm 3.2** Reduce  $Q\Omega/P^k$  in  $H_{\text{dR}}^n(\mathcal{Y}_{\mathbf{Q}_q(t)})$

---

**Input:**  $P$  in  $\mathbf{Z}_q[t][x_0, \dots, x_n]$  homogeneous of degree  $d$ , defining a family  $\mathcal{X}/\mathcal{S}$  of smooth projective hypersurfaces that contains a diagonal fibre,  $Q \in \mathbf{Q}_q(t)[x_0, \dots, x_n]$  homogeneous of degree  $kd - (n + 1)$ .

**Output:**  $\gamma_i$  in the  $\mathbf{Q}_q(t)$ -span of  $B_i$  for  $1 \leq i \leq n$ , with  $Q\Omega/P^k \equiv \gamma_1 \Omega/P^1 + \dots + \gamma_n \Omega/P^n$ .

**procedure** REDUCE( $P, Q$ )

**while**  $k \geq n + 1$  **do**

$Q_0, \dots, Q_n, 0 \leftarrow \text{DECOMPOSE}(Q)$

$k \leftarrow k - 1$

$Q \leftarrow k^{-1} \sum_{i=0}^n \partial_i Q_i$

**while**  $Q \notin \mathbf{Q}_q(t)$ -span of  $B_k$  **do**

$Q_0, \dots, Q_n, \gamma_k \leftarrow \text{DECOMPOSE}(Q)$

$k \leftarrow k - 1$

$Q \leftarrow k^{-1} \sum_{i=0}^n \partial_i Q_i$

**if**  $Q \neq 0$  **then**

$\gamma_k \leftarrow Q$

$k \leftarrow k - 1$

$\gamma_1, \dots, \gamma_k \leftarrow 0$

**return**  $\gamma_1, \dots, \gamma_n$

---

We now establish that the set  $\mathcal{B}$  indeed forms a basis for  $H_{\text{dR}}^n(\mathfrak{U}_{\mathbf{Q}_q(t)})$ , as announced before. We start with an auxiliary result describing the cardinality of the set  $\mathcal{B}$ .

**Proposition 3.7.** The set  $\mathcal{B}$  has cardinality

$$\frac{1}{d} \left( (d-1)^{n+1} + (-1)^{n+1}(d-1) \right).$$

*Proof.* First note that if we denote

$$V = \left\{ (u_0, \dots, u_n) \in (\mathbf{Z}/d\mathbf{Z})^{n+1} : \sum_{j=0}^n u_j = -(n+1) \right\},$$

$$W_j = \left\{ (u_0, \dots, u_n) \in (\mathbf{Z}/d\mathbf{Z})^{n+1} : u_j = -1 \right\},$$

then  $\mathcal{B}$  is in one-to-one correspondence with the set  $V - (W_0 \cup \dots \cup W_n)$ . Now by the inclusion-exclusion principle,

$$\begin{aligned} |V \cap (W_0 \cup \dots \cup W_n)| &= \sum_{j=0}^n |V \cap W_j| - \sum_{0 \leq j < k \leq n} |V \cap W_j \cap W_k| \\ &\quad + \dots + (-1)^n |V \cap W_0 \cap \dots \cap W_n| \\ &= \binom{n+1}{1} d^{n-1} - \binom{n+1}{2} d^{n-2} + \dots + (-1)^{n-1} \binom{n+1}{n} + (-1)^n \\ &= \frac{1}{d} (d^{n+1} + (-1)^{n+1} - (d-1)^{n+1}) + (-1)^n, \end{aligned}$$

so that

$$\begin{aligned} |V - (W_0 \cup \dots \cup W_n)| &= |V| - |V \cap (W_0 \cup \dots \cup W_n)| \\ &= d^n - \frac{1}{d} (d^{n+1} + (-1)^{n+1} - (d-1)^{n+1} + d(-1)^n) \\ &= \frac{1}{d} \left( (d-1)^{n+1} + (-1)^{n+1}(d-1) \right), \end{aligned}$$

and the proof is complete.  $\square$

**Proposition 3.8.** The rank of  $H_{\text{dR}}^n(\mathfrak{U}/\mathfrak{S})$  is

$$\frac{1}{d} \left( (d-1)^{n+1} + (-1)^{n+1}(d-1) \right).$$

*Proof.* Let  $\mathfrak{U}_m/\mathfrak{S}$  denote the complement of a family  $\mathfrak{X}_m/\mathfrak{S}$  of smooth projective hypersurfaces of degree  $d$  in  $\mathbf{P}_{\mathfrak{S}}^m$  and let  $b(d, m)$  denote the rank of  $H_{\text{dR}}^m(\mathfrak{U}_m/\mathfrak{S})$ . It is known that  $b(d, m)$  only depends on  $d, m$ . Moreover, taking  $x = y = z$  in [6, Corollaire 2.4 (i)], we find that

$$\sum_{m=1}^{\infty} b(d, m) x^{m-1} = \frac{(d-1)}{(1+x)(1-(d-1)x)} = \frac{1}{xd} \left( \frac{d-1}{1-(d-1)x} - \frac{d-1}{1+x} \right)$$

as formal power series. From this the result follows easily.  $\square$

**Theorem 3.9.** Suppose that the family of smooth projective hypersurfaces  $\mathcal{X}/\mathcal{S}$  contains a diagonal fibre. Then the set  $\mathcal{B}$  from Definition 3.2 is a basis for the  $\mathbf{Q}_q(t)$ -vector space  $H_{\text{dR}}^n(\mathfrak{U}_{\mathbf{Q}_q(t)})$ .

*Proof.* We already know that  $H_{\text{dR}}^n(\mathfrak{U}_{\mathbf{Q}_q(t)})$  is spanned by the classes of the  $n$ -forms  $Q\Omega/P^k$  with  $Q \in \mathbf{Q}_q(t)[x_0, \dots, x_n]$  homogeneous of degree  $kd - (n+1)$  for  $k \in \mathbf{N}$ . Applying Algorithm 3.2, we obtain an expression for the class of  $Q\Omega/P^k$  as a  $\mathbf{Q}_q(t)$ -linear combination of elements in  $\mathcal{B}$ . This shows that  $\mathcal{B}$  spans the vector space  $H_{\text{dR}}^n(\mathfrak{U}_{\mathbf{Q}_q(t)})$ . However, by the two propositions above, the dimension of  $H_{\text{dR}}^n(\mathfrak{U}_{\mathbf{Q}_q(t)})$  is equal to the cardinality of  $\mathcal{B}$ , so that  $\mathcal{B}$  is linearly independent as well.  $\square$

**Remark 3.10.** Let  $H_i$  denote the restriction of the Hodge filtration on  $H_{\text{dR}}^{n-1}(\mathfrak{X}/\mathfrak{S})$  to  $H_{\text{dR}}^n(\mathfrak{U}/\mathfrak{S})$  and write

$$h^{i, n-1-i} = \text{rank}(H_i/H_{i+1})$$

for the corresponding Hodge numbers. Recall that  $H_i = \text{Fil}^{n-i} H_{\text{dR}}^n(\mathfrak{U}/\mathfrak{S})$  for the filtration by the pole order defined above. Applying the loop in Algorithm 3.2 just once, to lower the pole order from  $k$  to  $k-1$ , we see that  $\mathcal{B}_k$  spans

$$\text{Fil}^k H_{\text{dR}}^n(\mathfrak{U}_{\mathbf{Q}_q(t)}) / \text{Fil}^{k-1} H_{\text{dR}}^n(\mathfrak{U}_{\mathbf{Q}_q(t)})$$

for all  $1 \leq k \leq n$ . Hence it follows that  $|B_k| \geq h^{n-k, k-1}$ , but since

$$\sum_{k=1}^n |B_k| = \dim H_{\text{dR}}^n(\mathfrak{U}_{\mathbf{Q}_q(t)}) = \sum_{k=1}^n h^{n-k, k-1},$$

this implies that  $|B_k| = h^{n-k, k-1}$  for all  $1 \leq k \leq n$ . So the Hodge numbers can be read off from the basis  $\mathcal{B}$ .

We now describe the action of the Gauss–Manin connection  $\nabla$  on  $H_{\text{dR}}^n(\mathfrak{U}_{\mathbf{Q}_q(t)})$ . Suppose that we are given a basis element  $x^u \Omega / P^k \in \mathcal{B}_k$ . Following the description in Section 2, we compute

$$\nabla \left( \frac{x^u \Omega}{P^k} \right) \equiv dt \otimes \frac{-kx^u (\partial P / \partial t) \Omega}{P^{k+1}}, \quad (3.2)$$

where  $\equiv$  denotes equality in  $\Omega_{\mathbf{Q}_q(t)} \otimes H_{\text{dR}}^n(\mathfrak{U}_{\mathbf{Q}_q(t)})$ . We apply Algorithm 3.2 in order to write

$$dt \otimes \frac{-kx^u (\partial P / \partial t) \Omega}{P^{k+1}} \equiv dt \otimes \left( \frac{\gamma_1}{P} + \dots + \frac{\gamma_n}{P^n} \right) \Omega, \quad (3.3)$$

where  $\gamma_i$  is an element in the  $\mathbf{Q}_q(t)$ -span of  $B_i$  for  $1 \leq i \leq n$ .

**Remark 3.11.** For the matrix  $M$  of  $\nabla$  to be correct to  $p$ -adic precision  $N_M$ , we have to carry out this computation to a somewhat higher working precision  $N'_M$  due to the precision loss in Algorithm 3.2. For all  $k \in \mathbf{N}$ , by definition  $\text{ord}_p(\Delta_k) \geq 0$ , and from the proof of Theorem 3.6 we know that  $\text{ord}_p(\det(\Delta_k)) = 0$ . Therefore, there is no precision loss in Algorithm 3.1, and the only precision loss in Algorithm 3.2 comes from dividing by  $k-1$  for  $k = 2, \dots, n+1$ . Hence it is sufficient to take

$$N'_M = N_M + \text{ord}_p(n!).$$

This is formalised in Algorithm 3.3.

**Definition 3.12.** We define the polynomial  $R \in \mathbf{Z}_q[t]$  by

$$R = \prod_{k=2}^{n+1} \det(\Delta_k).$$

**Proposition 3.13.** The matrix  $M$  of  $\nabla$  with respect to  $\mathcal{B}$  is of the form  $H/R$ , with  $H \in M_{b \times b}(\mathbf{Q}_q[t])$ .

---

**Algorithm 3.3** Compute the Gauss–Manin connection matrix

---

**Input:**  $P$  in  $\mathbf{Z}_q[t][x_0, \dots, x_n]$  homogeneous of degree  $d$ , defining a family  $\mathfrak{X}/\mathfrak{S}$  of smooth projective hypersurfaces that contains a diagonal fibre,  $p$ -adic precision  $N_M$ .

**Output:** The matrix  $M$  of  $\nabla$  with respect to  $\mathcal{B}$  to  $p$ -adic precision  $N_M$ .

**procedure** GMCONNECTION( $P, N_M$ )

$N'_M \leftarrow N_M + \text{ord}_p(n!)$

Execute the following steps with  $p$ -adic working precision  $N'_M$ :

**for**  $g \in B$  **do**

$k \leftarrow (\deg(g) + (n + 1))/d$

$Q \leftarrow -kg(\partial P/\partial t)$

$\gamma_1, \dots, \gamma_n \leftarrow \text{REDUCE}(P, Q)$

**for**  $f \in B$  **do**

$l \leftarrow (\deg(f) + (n + 1))/d$

$M_{f,g} \leftarrow$  coefficient of  $f$  in  $\gamma_l$

**return**  $M$

---

*Proof.* The only time in Algorithm 3.3 that nonconstant denominators are introduced is when the subroutine REDUCE calls its subroutine DECOMPOSE and a linear system  $\Delta_k v = w$  is solved. Since this happens only for  $k = 2, \dots, n + 1$  and at most once for each such  $k$ , the result is clear.  $\square$

**Remark 3.14.** Recall that  $\mathcal{B}$  is a basis for  $H_{\text{dR}}^n(\mathcal{U}_{\mathbf{Q}_q(t)})$  but not necessarily for  $H_{\text{dR}}^n(\mathcal{U}/\mathfrak{S})$ . However, if the zero locus of  $R$  in  $\mathbf{P}_{\mathbf{Z}_q}^1$  does not intersect  $\mathcal{S}$ , then  $\mathcal{B}$  is a basis for  $H_{\text{dR}}^n(\mathcal{U}/\mathfrak{S})$ . That it spans the cohomology can be seen by applying Algorithm 3.2, and that it is linearly independent follows because it is so over  $\mathbf{Q}_q(t)$ . Therefore, it will be convenient to choose  $\mathcal{S}$  smaller, so that this condition is satisfied.

**Assumption 3.15.** From now on we assume that the zero locus of  $R$  in  $\mathbf{P}_{\mathbf{Z}_q}^1$  does not intersect  $\mathcal{S}$ . In particular, this implies that  $\mathcal{B}$  is a basis for  $H_{\text{dR}}^n(\mathcal{U}/\mathfrak{S})$ .

**Remark 3.16.** Note that in Algorithm 3.3, we solve  $O(|\mathcal{B}|)$  linear systems given by the matrices  $\Delta_k$  for  $k = 2, \dots, n + 1$ . In practice, it is important to take advantage of this, e.g. by computing the decomposition  $\Delta_k = LUP$ , where  $L$  is lower triangular,  $U$  is upper triangular, and  $P$  is a permutation matrix, which is guaranteed to exist for any square matrix. Since, moreover, the matrices  $\Delta_k$  contain many zeros, methods from sparse linear algebra can be used to compute such a decomposition. Then, every call to DECOMPOSE reduces to solving a lower and an upper diagonal linear system.

In the rest of this section we will freely use the definitions and notation from Section 2. We let all of our matrices be defined with respect to the basis  $\mathcal{B}$ . We have seen that there exists a Frobenius structure  $F_p$  on  $H_{\text{dR}}^n(\mathcal{U}/\mathfrak{S})$  and let  $\Phi \in M_{b \times b}(\mathbf{Q}_q\langle t, 1/r \rangle^\dagger)$  denote the matrix of the action of  $p^{-1}F_p$ , where  $r$  is the denominator of the connection matrix  $M$ . Recall that  $\mathbf{F}_q/\mathbf{F}_q$  denotes a finite field extension.

We need a priori lower bounds on the  $p$ -adic valuations of the matrices  $\Phi$  and  $\Phi^{-1}$  to bound the loss of  $p$ -adic precision in our computations. We will now recall how such bounds can be obtained following [1].

**Theorem 3.17.** For any finite field extension  $\mathbf{F}_q/\mathbf{F}_q$  and all  $\tau \in S(\mathbf{F}_q)$ , there exists a matrix  $W_\tau \in M_{b \times b}(\mathbf{Q}_q)$  such that

$$\text{ord}_p(W_\tau) \geq - \sum_{i=1}^{n-1} \lfloor \log_p(i) \rfloor, \quad \text{ord}_p(W_\tau \Phi_\tau \sigma(W_\tau^{-1})) \geq 0,$$

$$\text{ord}_p(W_\tau^{-1}) \geq -\text{ord}_p((n-1)!), \quad \text{ord}_p(W_\tau \Phi_\tau^{-1} \sigma(W_\tau^{-1})) \geq -(n-1).$$

*Proof.* Let  $\Lambda_{\tau, \text{crys}}$  be the image of the integral logarithmic de Rham cohomology space  $H_{\text{dR}}^n(\mathbf{P}_{\mathbf{Z}_q}^n, \mathcal{X}_\tau)$  in the rigid cohomology space  $H_{\text{rig}}^n(U_\tau)$ . It is known that  $\Lambda_{\tau, \text{crys}} \otimes \mathbf{Q}_q \cong H_{\text{rig}}^n(U_\tau)$ , so that  $\Lambda_{\tau, \text{crys}}$  is a lattice in  $H_{\text{rig}}^n(U_\tau)$ . Let  $\Lambda_{\tau, \text{mon}}$  be the  $\mathbf{Z}_q$ -module in  $H_{\text{rig}}^n(U_\tau)$  generated by the classes of  $x^u \Omega / P^n$  with  $u \in \mathbf{N}_0^{n+1}$  such that  $\sum_{i=0}^n u_i = nd - (n+1)$ . Since these classes generate  $H_{\text{rig}}^n(U_\tau)$ , we have that  $\Lambda_{\tau, \text{mon}}$  is a lattice in  $H_{\text{rig}}^n(U_\tau)$  as well. We know that

$$\Lambda_{\tau, \text{crys}} \subset \Lambda_{\tau, \text{mon}} \subset p^{-\sum_{i=1}^{n-1} \lfloor \log_p(i) \rfloor} \Lambda_{\tau, \text{crys}}.$$

The inclusion on the left is [1, Lemma 3.4.3], and the one on the right is [1, Proposition 3.4.6].

Let  $\Lambda_{\tau, \mathcal{B}}$  be the  $\mathbf{Z}_q$ -module in  $H_{\text{rig}}^n(U_\tau)$  generated by the basis  $\mathcal{B}$ . Since  $\mathcal{B}$  spans  $H_{\text{rig}}^n(U_\tau)$ , we have that  $\Lambda_{\tau, \mathcal{B}}$  is also a lattice in  $H_{\text{rig}}^n(U_\tau)$ . Now we know that

$$(n-1)! \Lambda_{\tau, \text{mon}} \subset \Lambda_{\tau, \mathcal{B}} \subset \Lambda_{\tau, \text{mon}}.$$

The inclusion on the left follows by explicitly reducing the generators of  $\Lambda_{\tau, \text{mon}}$  to the basis  $\mathcal{B}$  with Algorithm 3.2 using that  $R(\hat{\tau}) \in \mathbf{Z}_q^\times$ , and the inclusion on the right is clear.

Combining these inclusions of lattices, we find that

$$(n-1)! \Lambda_{\tau, \text{crys}} \subset \Lambda_{\tau, \mathcal{B}} \subset p^{-\sum_{i=1}^{n-1} \lfloor \log_p(i) \rfloor} \Lambda_{\tau, \text{crys}}. \quad (3.4)$$

Now let  $[d_1, \dots, d_b]$  be a  $\mathbf{Z}_q$ -basis for  $\Lambda_{\tau, \text{crys}}$  and let  $W_\tau \in M_{b \times b}(\mathbf{Q}_q)$  be the matrix in which the  $i$ -th column consists of the coordinates of  $d_i$  with respect to the basis  $\mathcal{B}$ . From the inclusions (3.4) it is clear that

$$\begin{aligned} \text{ord}_p(W_\tau) &\geq -\sum_{i=1}^{n-1} \lfloor \log_p(i) \rfloor, \\ \text{ord}_p(W_\tau^{-1}) &\geq -\text{ord}_p((n-1)!). \end{aligned}$$

Note that  $W_\tau \Phi_\tau \sigma(W_\tau^{-1})$  is the matrix of  $p^{-1} F_p$  on  $H_{\text{rig}}^n(U_\tau)$  with respect to the basis  $[d_1, \dots, d_b]$ . Now  $\Lambda_{\tau, \text{crys}}$  is contained in the crystalline cohomology space  $H_{\text{crys}}^{n-1}(X_\tau)$ , which maps to itself under  $F_p$ . So by the short exact sequence (2.4), the lattice  $\Lambda_{\tau, \text{crys}}$  maps to itself under  $p^{-1} F_p$ , and

$$\text{ord}_p(W_\tau \Phi_\tau \sigma(W_\tau^{-1})) \geq 0.$$

Similarly, note that  $W_\tau \Phi_\tau^{-1} \sigma(W_\tau^{-1})$  is the matrix of  $p F_p^{-1}$  on  $H_{\text{rig}}^n(U_\tau)$  with respect to the basis  $[d_1, \dots, d_b]$ . By Poincaré duality, the map  $p^{n-1} F_p^{-1}$  maps the crystalline cohomology space  $H_{\text{crys}}^{n-1}(X_\tau)$  to itself. So by the short exact sequence (2.4), the lattice  $\Lambda_{\tau, \text{crys}}$  maps to itself under  $p^{n-1} F_p^{-1}$ , and

$$\text{ord}_p(W_\tau \Phi_\tau^{-1} \sigma(W_\tau^{-1})) \geq -(n-1). \quad \square$$

**Definition 3.18.** Define the nonnegative integer

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

**Corollary 3.19.** We have

$$\begin{aligned} \text{ord}_p(\Phi) &\geq -\delta, \\ \text{ord}_p(\Phi^{-1}) &\geq -\delta - (n-1). \end{aligned}$$

*Proof.* For every  $\tau \in \mathcal{S}(\bar{\mathbf{F}}_q)$ , we can apply Theorem 3.17 to obtain

$$\begin{aligned} \text{ord}_p(\Phi_\tau) &\geq \text{ord}_p(W_\tau^{-1}) + \text{ord}_p(W_\tau \Phi_\tau \sigma(W_\tau^{-1})) + \text{ord}_p(\sigma(W_\tau)) \\ &\geq -\delta, \end{aligned}$$

and also

$$\begin{aligned} \text{ord}_p(\Phi_\tau^{-1}) &\geq \text{ord}_p(W_\tau^{-1}) + \text{ord}_p(W_\tau \Phi_\tau^{-1} \sigma(W_\tau^{-1})) + \text{ord}_p(\sigma(W_\tau)) \\ &\geq -\delta - (n-1). \end{aligned}$$

As these inequalities hold for infinitely many  $\tau \in S(\bar{\mathbf{F}}_q)$  we obtain the required bounds.  $\square$

## 4 Frobenius on diagonal hypersurfaces

### 4.1 A formula for $\Phi_0$

We consider a single smooth projective diagonal hypersurface  $\mathcal{X}_0$  over  $\mathbf{Z}_p$  defined by a polynomial  $P_0 \in \mathbf{Z}_p[x_0, \dots, x_n]$  of the form

$$P_0(x_0, x_1, \dots, x_n) = a_0 x_0^d + a_1 x_1^d + \dots + a_n x_n^d,$$

where  $a_0, a_1, \dots, a_n \in \mathbf{Z}_p^\times$  and  $p \nmid d$ . Let  $\mathfrak{X}_0 = \mathcal{X}_0 \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$  denote the generic fibre of  $\mathcal{X}_0$  and let  $\mathcal{U}_0$  and  $\mathfrak{U}_0$  be the complements of  $\mathcal{X}_0$  and  $\mathfrak{X}_0$ , respectively. We fix our choice of basis  $\mathcal{B}$  for  $H_{\text{dR}}^n(\mathfrak{U}_0)$  as in Definition 3.2. Our goal is to compute the matrix  $\Phi_0$  representing the action of  $p^{-1}F_p$  on  $H_{\text{rig}}^n(U_0) \cong H_{\text{dR}}^n(\mathfrak{U}_0)$ , with respect to the basis  $\mathcal{B}$ , to  $p$ -adic precision  $N_{\Phi_0}$ . It will turn out that this matrix has only one nonzero element in every row and column.

Let  $u = (u_0, \dots, u_n)$  and  $v = (v_0, \dots, v_n)$  be tuples of integers such that  $x^u, x^v \in B$  and  $p(u_i + 1) \equiv v_i + 1 \pmod{d}$ , for all  $i$ . Furthermore, let  $k(u) \in \mathbf{N}$  denote the positive integer such that

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

Finally, for all  $l \in \mathbf{Q}$  and integers  $r \geq 0$ , let the rising factorial  $\prod_{j=0}^{r-1} (l+j)$  be denoted by  $(l)_r$ .

**Definition 4.1.** Let  $u, v \in \mathbf{Z}^{n+1}$  be such that we have  $x^u, x^v \in B$  and  $p(u_i + 1) \equiv v_i + 1 \pmod{d}$  for all  $i$ . We define

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

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

The following lemma will be useful in what follows.

**Lemma 4.2.** Let  $x^u, x^v \in B$ ,  $0 \leq i \leq n$  and  $m, r \geq 0$  integers, such that

$$p(u_i + 1) - (v_i + 1) = d(m - pr).$$

Then we have  $r = \lfloor m/p \rfloor$ .

*Proof.* Since  $0 \leq u_i, v_i \leq d-2$ , we obtain

$$p - (d-1) \leq p(u_i + 1) - (v_i + 1) \leq p(d-1) - 1,$$

and from this the result follows, also using that  $m - pr \in \mathbf{Z}$ .  $\square$

The entries of  $\Phi_0$  can be expressed in terms of the  $\alpha_{u,v}$  in the following way.

**Theorem 4.3.** Let  $\omega_1$  denote an element of  $\mathcal{B}$  corresponding to a tuple  $u \in \mathbf{Z}^{n+1}$  and let  $\omega_2$  denote the unique element of  $\mathcal{B}$  corresponding to a tuple  $v \in \mathbf{Z}^{n+1}$  such that  $p(u_i + 1) \equiv v_i + 1 \pmod{d}$  for all  $i$ . Then

$$p^{-1} \mathbb{F}_p(\omega_1) = (-1)^{k(v)} \frac{(k(v) - 1)!}{(k(u) - 1)!} p^{n-k(u)} \alpha_{u,v}^{-1} \cdot \omega_2. \quad (4.1)$$

*Proof.* We start with some definitions. First, let  $\mathbf{Q}_p(\pi)$  denote the totally ramified extension of  $\mathbf{Q}_p$  with  $\pi^{p-1} = -p$  and extend the  $p$ -adic valuation such that  $\text{ord}_p(\pi) = (p-1)^{-1}$ . For  $0 \leq i \leq n$ , define sets

$$W^{(i)} = \{(w_0, \dots, w_n) \in \mathbf{N}_0^{n+1} : w_j \geq 1 \text{ for all } j \neq i \text{ and } |w| \equiv 0 \pmod{d}\},$$

with  $|w| = \sum_{i=0}^n w_i$ . Note that  $|w| = k(w-1)$ , where  $w-1$  denotes the tuple  $(w_0-1, \dots, w_n-1)$ . Furthermore, still for  $0 \leq i \leq n$ , define  $\mathbf{Q}_p(\pi)$ -vector spaces

$$\mathcal{L}^{(i)} = \left\{ \sum_{w \in W^{(i)}} b_w x^w : b_w \in \mathbf{Q}_p(\pi), \exists c > 0 \text{ s.t. } \lim_{|w| \rightarrow \infty} (\text{ord}_p(b_w) - c \cdot |w|) \geq 0 \right\}$$

and let  $\mathcal{L} = \bigcap_{i=0}^n \mathcal{L}^{(i)}$  be the intersection of the  $\mathcal{L}^{(i)}$ . Moreover, let  $D_i: \mathcal{L}^{(i)} \rightarrow \mathcal{L}$  denote the differential operator  $D_i = x_i \partial_i + \pi x_i \partial_i(P_0)$ . Finally, let  $\psi_p, \alpha: \mathcal{L} \rightarrow \mathcal{L}$  be the  $\mathbf{Q}_p(\pi)$ -linear maps defined by:

$$\begin{aligned} \psi_p(x^w) &= \begin{cases} x^{w/p} & \text{if } p \mid w_i \text{ for all } 0 \leq i \leq n \\ 0 & \text{otherwise} \end{cases} \\ \alpha(x^w) &= \psi_p \left( \exp \left( \pi (P_0(x_0, \dots, x_n) - P_0(x_0^p, \dots, x_n^p)) \right) \cdot x^w \right) \end{aligned}$$

and let  $\mathcal{R}: \mathcal{L} \rightarrow H_{\text{rig}}^n(U_0) \otimes \mathbf{Q}_p(\pi)$  denote the  $\mathbf{Q}_p(\pi)$ -linear map defined by

$$\mathcal{R}(x^w) = \frac{(|w| - 1)! x^{w-1} \Omega}{(-\pi)^{|w|-1} P_0^{|w|}},$$

where  $\Omega$  is defined as in Proposition 3.1.

Then by [14, Theorem 2.15], the diagram

$$\begin{array}{ccc} \mathcal{L} / \sum_{i=0}^n D_i \mathcal{L}^{(i)} & \xrightarrow{p^{-n} \alpha} & \mathcal{L} / \sum_{i=0}^n D_i \mathcal{L}^{(i)} \\ \downarrow \mathcal{R} & & \downarrow \mathcal{R} \\ H_{\text{rig}}^n(U_0) \otimes \mathbf{Q}_p(\pi) & \xrightarrow{(p^{-1} \mathbb{F}_p)^{-1}} & H_{\text{rig}}^n(U_0) \otimes \mathbf{Q}_p(\pi) \end{array}$$

commutes and by [14, Corollary 1.15] the vertical maps are isomorphisms. This implies that (4.1) is equivalent to

$$\alpha(x^{v+1}) \equiv \pi^{pk(u)-k(v)} \alpha_{u,v} \cdot x^{u+1} \pmod{\sum_{i=0}^n D_i \mathcal{L}^{(i)}},$$

which we will now prove.

Note that so far we have not used that  $P_0$  is diagonal. Since  $P_0(x_0, x_1, \dots, x_n)$  is equal to  $a_0 x_0^d + a_1 x_1^d + \dots + a_n x_n^d$ , we have

$$\exp \left( \pi (P_0(x_0, \dots, x_n) - P_0(x_0^p, \dots, x_n^p)) \right) = \prod_{i=0}^n \exp \left( \pi a_i (x_i^d - x_i^{dp}) \right)$$



and also

$$D_i = x_i \partial_i + (\pi a_i d) x_i^d.$$

For  $0 \leq i \leq n$ , we denote

$$\mathbf{Q}_p(\pi) \langle x_i \rangle^\dagger = \left\{ \sum_{j=0}^{\infty} b_j x_i^j : b_j \in \mathbf{Q}_p(\pi), \exists c > 0 \text{ s.t. } \lim_{j \rightarrow \infty} (\text{ord}_p(b_j) - c \cdot j) \geq 0 \right\}$$

and we define  $\mathbf{Q}_p(\pi)$ -linear maps  $\psi_p, D_i$  on  $\mathbf{Q}_p(\pi) \langle x_i \rangle^\dagger$  by the same formulas as before. Then

$$\begin{aligned} \psi_p \left( \exp(\pi a_i (x_i^d - x_i^{pd})) x_i^{v_i+1} \right) &= \sum_{\substack{m \geq 0 \text{ s.t.} \\ p \mid dm + v_i + 1}} \left( \sum_{j=0}^{\lfloor m/p \rfloor} \frac{(-1)^j (\pi a_i)^{m-(p-1)j}}{j!(m-pj)!} \right) x_i^{(dm+v_i+1)/p} \\ &= \sum_{m,r} \left( \sum_{j=0}^r \frac{(-1)^j (\pi a_i)^{m-(p-1)j}}{j!(m-pj)!} \right) x_i^{u_i+1+dr}, \end{aligned}$$

where the outer sum on the last line is over all integers  $m, r \geq 0$  that satisfy  $p(u_i+1) - (v_i+1) = d(m-pr)$  and we have used Lemma 4.2. It is clear that

$$x_i^{u_i+1+dr} \equiv \left( \frac{u_i+1}{d} \right)_r (-\pi a_i)^{-r} x_i^{u_i+1} \pmod{D_i \mathbf{Q}_p(\pi) \langle x_i \rangle^\dagger}.$$

Hence, it follows that

$$\begin{aligned} \psi_p \left( \exp(\pi a_i (x_i^d - x_i^{pd})) x_i^{v_i+1} \right) &\equiv \\ (\pi a_i)^{(p(u_i+1)-(v_i+1))/d} \left( \sum_{m,r} \left( \frac{u_i+1}{d} \right)_r \sum_{j=0}^r \frac{(pa_i^{p-1})^{r-j}}{(m-pj)!j!} \right) x_i^{u_i+1} &\pmod{D_i \mathbf{Q}_p(\pi) \langle x_i \rangle^\dagger}, \end{aligned}$$

where the sum is still over all integers  $m, r \geq 0$  that satisfy  $p(u_i+1) - (v_i+1) = d(m-pr)$ . For  $G_i \in \mathbf{Q}_p(\pi) \langle x_i \rangle^\dagger$  with  $0 \leq i \leq n$ , we have

$$\psi_p \left( \prod_{j=0}^n G_j \right) = \prod_{j=0}^n \psi_p(G_j), \quad D_i \left( \prod_{j=0}^n G_j \right) = D_i(G_i) \cdot \prod_{j \neq i} G_j.$$

Therefore, we can take the product of the congruences above to conclude that

$$\alpha(x^{v+1}) \equiv \pi^{pk(u)-k(v)} \alpha_{u,v} \cdot x^{u+1} \pmod{\sum_{i=0}^n D_i \mathbf{Q}_p(\pi) \langle x_i \rangle^\dagger}.$$

Since  $\mathcal{L} \cap \sum_{i=0}^n D_i \mathbf{Q}_p(\pi) \langle x_i \rangle^\dagger = \sum_{i=0}^n D_i \mathcal{L}^{(i)}$ , we can replace  $\sum_{i=0}^n D_i \mathbf{Q}_p(\pi) \langle x_i \rangle^\dagger$  by  $\sum_{i=0}^n D_i \mathcal{L}^{(i)}$  in this expression, completing the proof.  $\square$

**Remark 4.4.** The computation in the proof of Theorem 4.3 essentially goes back to Dwork [8, §4]. Following Dwork's work, Lauder obtained a formula similar to ours [22, Proposition 10], that was used both by him [22] and Gerkmann [10] in their algorithms.

However, our approach is different in two ways. Firstly, our formula for  $\alpha_{u,v}$  is defined over  $\mathbf{Q}_p$  instead of  $\mathbf{Q}_p(\pi)$ . By eliminating the  $\pi$ 's, we are able to improve the complexity of the computation of  $\Phi_0$ , and even of the whole deformation algorithm, by a factor  $p$ , as we will see in Section 7. Secondly, Lauder's formula is only valid when the  $a_i$  are Teichmüller lifts, i.e.  $a_i^{p-1} = 1$ . From a theoretical point of view, of course one can always choose the  $a_i$  to be Teichmüller lifts, but in computations this is unnecessarily restrictive.

## 4.2 Some estimates

There are two remaining problems for computing the matrix  $\Phi_0$ . Firstly, to compute  $\Phi_0$  to  $p$ -adic precision  $N_{\Phi_0}$  using Theorem 4.3, we have to compute the elements  $\alpha_{u,v}$  to a somewhat higher precision  $N'_{\Phi_0}$  because of loss of precision in the computation. In Corollary 4.8 we will obtain a bound for  $N'_{\Phi_0}$ . Secondly, the sums over  $m, r$  in Definition 4.1 consist of infinitely many terms. In Proposition 4.10 we will derive a finite expression for  $\alpha_{u,v}$  to precision  $N'_{\Phi_0}$ . We start with some estimates that will be needed in the proofs.

**Proposition 4.5.** For all integers  $j, d, r \geq 1$  with  $p \nmid d$ ,

$$\text{ord}_p\left(\frac{j}{d}\right)_r \geq \text{ord}_p(r!) \geq \frac{r}{p-1} - \lfloor \log_p(r) + 1 \rfloor.$$

*Proof.* Let  $s_p(r)$  denote the sum of digits in the  $p$ -adic expansion of  $r$  and observe that  $s_p(r) \leq (p-1) \lfloor \log_p(r) + 1 \rfloor$ . Then

$$\text{ord}_p\left(\frac{j}{d}\right)_r \geq \text{ord}_p(r!) = \frac{r - s_p(r)}{p-1} \geq \frac{r}{p-1} - \lfloor \log_p(r) + 1 \rfloor. \quad \square$$

**Proposition 4.6.** For all integers  $m \geq 0$  and  $0 \leq i \leq n$ ,

$$\text{ord}_p\left(\sum_{j=0}^{\lfloor m/p \rfloor} \frac{(pa_i^{p-1})^{\lfloor m/p \rfloor - j}}{(m-pj)!j!}\right) \geq \frac{p-1}{p^2}m + \left\lfloor \frac{m}{p} \right\rfloor - \frac{m}{p-1}.$$

*Proof.* Let  $\mathbf{Q}_p(\pi)$  denote the totally ramified extension of  $\mathbf{Q}_p$  with  $\pi^{p-1} = -p$  and extend the  $p$ -adic valuation such that  $\text{ord}_p(\pi) = (p-1)^{-1}$ . Expanding

$$\exp(\pi a_i(x - x^p)) = \sum_{m=0}^{\infty} \lambda_m x^m,$$

one checks easily that, for all  $m \geq 0$ ,

$$\begin{aligned} \lambda_m &= \sum_{j=0}^{\lfloor m/p \rfloor} \frac{(-1)^j (\pi a_i)^{m-(p-1)j}}{(m-pj)!j!} \\ &= (-1)^{\lfloor m/p \rfloor} (\pi a_i)^{m-(p-1)\lfloor m/p \rfloor} \left( \sum_{j=0}^{\lfloor m/p \rfloor} \frac{(pa_i^{p-1})^{\lfloor m/p \rfloor - j}}{(m-pj)!j!} \right). \end{aligned}$$

Therefore, it suffices to show that  $\text{ord}_p(\lambda_m) \geq m(p-1)/p^2$ . This is well-known in the case  $a_i = 1$ , but the proof from [7, Lemma 4.1] remains valid when  $a_i \in \mathbf{Z}_p^\times$ .  $\square$

**Theorem 4.7.** Let  $\alpha_{u,v}$  be defined as in Definition 4.1. Then

$$0 \leq \text{ord}_p(\alpha_{u,v}) \leq \text{ord}_p\left(\frac{(k(v)-1)!}{(k(u)-1)!}\right) + (n - k(u)) + \delta,$$

where  $\delta$  is defined as in Definition 3.18.

*Proof.* First, we prove the left-hand inequality. By Lemma 4.2, Proposition 4.5 and Proposition 4.6, it suffices to show that

$$\frac{p-1}{p^2}m + \left\lfloor \frac{m}{p} \right\rfloor - \frac{m}{p-1} + \text{ord}_p\left(\left\lfloor \frac{m}{p} \right\rfloor!\right) > -1, \quad (4.2)$$

for all integers  $m \geq p$ . From Proposition 4.5 and the fact that  $m \geq p \lfloor m/p \rfloor$ , it follows that

$$\frac{p-1}{p^2}m + \left\lfloor \frac{m}{p} \right\rfloor - \frac{m}{p-1} + \text{ord}_p \left( \left\lfloor \frac{m}{p} \right\rfloor! \right) \geq \frac{p-1}{p} \left\lfloor \frac{m}{p} \right\rfloor - \left\lfloor \log_p \left( \left\lfloor \frac{m}{p} \right\rfloor \right) + 1 \right\rfloor.$$

One checks easily that the right-hand side is greater than  $-1$ , unless we have  $p = 2$  and  $m = 4, 5$ . However, in these cases (4.2) still holds, as can be seen by direct substitution.

Next, we prove the right-hand inequality. Recall from Corollary 3.19 that the valuations of the entries of the matrix  $\Phi_0$  are bounded below by  $-\delta$ . Thus by Theorem 4.3, we have

$$-\delta \leq \text{ord}_p \left( \frac{(k(v)-1)!}{(k(u)-1)!} \right) + (n - k(u)) - \text{ord}_p(\alpha_{u,v}),$$

from which the result follows.  $\square$

Using Theorem 4.7, we can now bound the  $p$ -adic precision  $N'_{\Phi_0}$  to which we have to compute the  $\alpha_{u,v}$ .

**Corollary 4.8.** In order to compute the matrix  $\Phi_0$  to  $p$ -adic precision  $N_{\Phi_0}$ , it is sufficient to compute the  $\alpha_{u,v}$  to  $p$ -adic precision

$$N'_{\Phi_0} = N_{\Phi_0} + (n-1) + \text{ord}_p((n-1)!) + 2\delta,$$

where  $\delta$  is defined as in Definition 3.18.

*Proof.* Note that the loss of precision in inverting  $\alpha_{u,v}$  is at most  $2 \text{ord}_p(\alpha_{u,v})$ . Therefore, it follows from Theorem 4.3 and Theorem 4.7 that it is sufficient to compute  $\alpha_{u,v}$  to precision

$$N_{\Phi_0} + \text{ord}_p \left( \frac{(k(v)-1)!}{(k(u)-1)!} \right) + (n - k(u)) + 2\delta \leq N_{\Phi_0} + (n-1) + \text{ord}_p((n-1)!) + 2\delta,$$

where we have used that  $1 \leq k(u), k(v) \leq n$ .  $\square$

To derive a finite expression for  $\alpha_{u,v}$  to precision  $N'_{\Phi_0}$ , we start with the following elementary lemma.

**Lemma 4.9.** Given integers  $\alpha, \beta \geq 2$  and defining  $x = \beta + \log_\alpha(\beta) + 1$ , for all real numbers  $y \geq x$ , we have

$$y - \log_\alpha(y) \geq \beta.$$

*Proof.* We first note that the function  $y \mapsto y - \log_\alpha(y)$  is increasing for  $y \geq 2$  because it has derivative  $1 - \log_\alpha(e)/y > 0$ . Thus, it suffices to verify the result for  $x$ . Indeed, as  $\beta \geq 2$  we have that  $\log_\alpha(\beta) + 1 \leq \beta$ , hence  $\beta + \log_\alpha(\beta) + 1 \leq 2\beta \leq \alpha\beta$ , which upon taking logarithms and rearranging yields the result.  $\square$

**Proposition 4.10.** In order to compute  $\alpha_{u,v}$  to  $p$ -adic precision  $N'_{\Phi_0}$ , it suffices to restrict the sums in Theorem 4.1 to pairs  $m, r \geq 0$  such that  $m \leq \mathcal{M}$ , or equivalently  $r \leq \mathcal{R}$ , where

$$\mathcal{M} = \left\lfloor \frac{p^2}{p-1} (N'_{\Phi_0} + \log_p(N'_{\Phi_0} + 3) + 4) \right\rfloor - 1, \quad \mathcal{R} = \lfloor \mathcal{M}/p \rfloor.$$

*Proof.* By Proposition 4.5 and Proposition 4.6, we have

$$\begin{aligned} \text{ord}_p \left( \left( \frac{u_i + 1}{d} \right)_r \sum_{j=0}^r \frac{(pd_i^{p-1})^{r-j}}{(m-pj)!j!} \right) &\geq \frac{p-1}{p^2}m + \left\lfloor \frac{m}{p} \right\rfloor - \frac{m}{p-1} + \frac{r}{p-1} - \lfloor \log_p(r) + 1 \rfloor \\ &\geq \frac{p-1}{p^2}m - \log_p(m) - 1. \end{aligned}$$

Therefore, it is sufficient to restrict the sums in Definition 4.1 to  $m, r \geq 0$  for which

$$\frac{p-1}{p^2}m - \log_p(m) - 1 < N'_{\Phi_0}.$$

We can now apply Lemma 4.9 with  $y = m(p-1)/p^2$ ,  $\alpha = p$  and  $\beta = N'_{\Phi_0} + 3$  to obtain the result.  $\square$

Finally, we formalise the procedure for computing the entries of  $\Phi_0$  to  $p$ -adic precision  $N_{\Phi_0}$  in Algorithm 4.1.

---

**Algorithm 4.1** Compute the matrix  $\Phi_0$ .

---

**Input:**  $P_0 = a_0x_0^d + \dots + a_nx_n^d$  with  $a_0, \dots, a_n \in \mathbf{Z}_p^\times$ ,  $p$ -adic precision  $N_{\Phi_0} \geq 0$ .

**Output:** The matrix  $\Phi_0$  for the action of  $p^{-1}F_p$  on  $H_{\text{rig}}^n(U_0)$  with respect to basis  $\mathcal{B}$  to  $p$ -adic precision  $N_{\Phi_0}$ .

**procedure** DIAGFROB( $P_0, N_{\Phi_0}$ )

1. Determine  $N'_{\Phi_0}$  from Corollary 4.8.
2. Let  $\Phi_0 \in M_{b \times b}(\mathbf{Q}_p)$  be the zero matrix.

**for**  $x^u \in B$  **do**

1. Determine the unique  $x^v \in B$  such that  $v_i = p(u_i + 1) - 1 \pmod d$ .
2. Compute  $\alpha_{u,v}$  to  $p$ -adic precision  $N'_{\Phi_0}$  using Proposition 4.10.
3. Set  $(\Phi_0)_{u,v} \leftarrow (-1)^{k(v)} \binom{(k(v)-1)!}{(k(u)-1)!} p^{n-k(u)} \alpha_{u,v}^{-1} \pmod{p^{N_{\Phi_0}}}$ .

3. **return**  $\Phi_0$
- 

**Assumption 4.11.** From now on we assume that our family of hypersurfaces  $\mathcal{X}/\mathcal{S}$  is defined by a polynomial  $P \in \mathbf{Z}_q[t][x_0, \dots, x_n]$  for which  $P(0) \in \mathbf{Z}_q[x_0, \dots, x_n]$  is of the form  $P_0 = a_0x_0^d + \dots + a_nx_n^d$  with  $a_0, \dots, a_n \in \mathbf{Z}_p^\times$ , so that we can apply Algorithm 4.1.

**Remark 4.12.** Note that Assumption 4.11 also implies that  $\mathcal{S}$  can be chosen to satisfy Assumption 2.16 and Assumption 3.15, since  $P_0$  defines a smooth hypersurface and we have that  $R(0) \in \mathbf{Z}_p^\times$ .

## 5 Solving the differential equation

In this section we explain how to solve the  $p$ -adic differential equation for the horizontal sections of the Gauss–Manin connection  $\nabla$ , in order to obtain a local expansion of the matrix for the action of  $p^{-1}F_p$  on  $H_{\text{rig}}^n(U/S)$ .

All our matrices will be defined with respect to the basis  $\mathcal{B}$ . Recall that  $M \in M_{b \times b}(\mathbf{Q}_q(t))$  denotes the matrix for the Gauss–Manin connection  $\nabla$  on  $H_{\text{dR}}^n(\mathcal{U}/\mathcal{S})$  and  $\Phi \in M_{b \times b}(\mathbf{Q}_q\langle t, 1/r \rangle^\dagger)$  the matrix for the  $\sigma$ -semilinear action of  $p^{-1}F_p$  on  $H_{\text{rig}}^n(U/S)$ , where  $\sigma$  is defined as in Definition 2.8.

As we saw in Section 2, these matrices satisfy the differential equation

$$\left( \frac{d}{dt} + M \right) \Phi = pt^{p-1} \Phi \sigma(M), \quad \Phi(0) = \Phi_0, \quad (5.1)$$

where  $\Phi_0 \in M_{b \times b}(\mathbf{Q}_p)$  is the matrix for the action of  $p^{-1}F_p$  on  $H_{\text{rig}}^n(U_0)$ . Our goal is the computation of the power series expansion of  $\Phi$  at  $t = 0$  to  $t$ -adic precision  $K$  and  $p$ -adic precision  $N_\Phi$ , i.e. as an element of  $M_{b \times b}(\mathbf{Q}_q[[t]])$  modulo  $t^K$  and  $p^{N_\Phi}$ .

We first observe that if  $C \in M_{b \times b}(\mathbf{Q}_q[[t]])$  denotes the unique solution to the differential equation

$$\left(\frac{d}{dt} + M\right)C = 0, \quad C(0) = I, \quad (5.2)$$

where  $I$  denotes the identity matrix, then the matrix  $\Phi = C\Phi_0\sigma(C)^{-1}$  satisfies Equation (5.1). So it is sufficient to solve Equation (5.2). We now give a bound on the rate of convergence of  $C = \sum_{i=0}^{\infty} C_i t^i$  that follows from recent work of Kedlaya [17]. We let  $\delta$  be defined as in Definition 3.18.

**Theorem 5.1.** For all  $i \geq 1$ , we have

$$\text{ord}_p(C_i) \geq -(2\delta + (n-1)) \lceil \log_p(i) \rceil.$$

*Proof.* It follows from [17, Theorem 18.3.3] that

$$\text{ord}_p(C_i) \geq (\text{ord}_p(\Phi) + \text{ord}_p(\Phi^{-1})) \lceil \log_p(i) \rceil,$$

but from Corollary 3.19 we already know that  $\text{ord}_p(\Phi) \geq -\delta$  and  $\text{ord}_p(\Phi^{-1}) \geq -\delta - (n-1)$ .  $\square$

**Remark 5.2.** In [17, Remark 18.3.4] Kedlaya also includes the bound

$$\text{ord}_p(C_i) \geq (b-1) \text{ord}_p(M) + (\text{ord}_p(\Phi) + \text{ord}_p(\Phi^{-1})) \lceil \log_p(i) \rceil,$$

which can sometimes be used to improve Theorem 5.1 slightly, for example when  $\text{ord}_p(M)$  is nonnegative.

**Remark 5.3.** The bound from Theorem 5.1 also applies to the inverse matrix  $C^{-1}$ , as this matrix satisfies the dual differential equation

$$\left(\frac{d}{dt} - M^t\right)(C^{-1})^t = 0, \quad C^{-1}(0) = I, \quad (5.3)$$

that carries a Frobenius structure given by the matrix  $(\Phi^{-1})^t$ .

We only know the matrix  $M$  to some finite  $p$ -adic precision  $N_M$ , and we need to compute  $C$  to some finite  $t$ -adic and  $p$ -adic precisions  $K, N_C$ , respectively. The following result gives an expression for  $N_M$  in terms of  $K, N_C$ . For a matrix  $A = \sum_{i=0}^{\infty} A_i t^i$  we write  $\bar{A} = \sum_{i=0}^{K-1} A_i t^i$  in what follows.

**Proposition 5.4.** Let  $K, N_C \in \mathbf{N}$  and define

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

Let  $\tilde{M} \in M_{b \times b}(\mathbf{Q}_q(t))$  be an approximation of  $M$  to  $p$ -adic precision  $N_M$ , i.e. such that  $\text{ord}_p(\tilde{M} - M) \geq N_M$ , and suppose that  $\tilde{C} = \sum_{i=0}^{\infty} \tilde{C}_i t^i$  satisfies the differential equation

$$\left(\frac{d}{dt} + \tilde{M}\right)\tilde{C} = 0, \quad \tilde{C}(0) = I.$$

Then  $\text{ord}_p(\tilde{C}_i - C_i) \geq N_C$  for all  $i < K$ .

*Proof.* From the expressions

$$C(t) = \exp\left(-\int_0^t M(s)ds\right), \quad \tilde{C}(t) = \exp\left(-\int_0^t \tilde{M}(s)ds\right),$$

it follows that

$$\tilde{C}(t) - C(t) = C(t) \left( \exp\left(\int_0^t (\tilde{M}(s) - M(s)) ds\right) - I \right). \quad (5.4)$$

Since  $\text{ord}_p(\tilde{M} - M) \geq N_M$ , we obtain

$$\text{ord}_p \left( \frac{1}{i!} \left( \int_0^t (\tilde{M}(s) - M(s)) ds \right)^i \right) \geq N_C + (2\delta + n - 1) \lceil \log_p(K - 1) \rceil$$

for all  $1 \leq i \leq K - 1$ , where we have used that  $\text{ord}_p(i!) \leq i/(p - 1) \leq 1$ . Moreover, from Theorem 5.1, we already know that

$$\text{ord}_p(\overline{C}) \geq -(2\delta + n - 1) \lceil \log_p(K - 1) \rceil.$$

From these two inequalities and Equation (5.4), we deduce  $\text{ord}_p(\overline{\tilde{C} - C}) \geq N_C$ .  $\square$

Now we explain how to compute the solution  $C$  to Equation (5.2) to  $p$ -adic precision  $N_C$  and  $t$ -adic precision  $K$ , assuming that the connection matrix  $M$  has been computed to  $p$ -adic precision  $N_M$  as defined in Proposition 5.4. We can write  $M = G/r$ , with  $G = \sum_{i=0}^{\deg(G)} G_i t^i \in M_{b \times b}(\mathbf{Q}_q[t])$  and  $r = \sum_{i=0}^{\deg(r)} r_i t^i \in \mathbf{Z}_q[t]$  a divisor of the polynomial  $R$  defined in Definition 3.12. Note that the degree of  $r$  might be smaller than the degree of  $R$ , which will speed up our computations. By Assumption 4.11, we have  $r(0) \neq 0 \pmod{p}$ , so in particular  $r(0) \neq 0$ .

We can obtain a power series solution  $C = \sum_{i=0}^{\infty} C_i t^i$  to the equation

$$r \frac{dC}{dt} + GC = 0, \quad C(0) = I,$$

which is clearly equivalent to Equation (5.2), using the following recursion:

$$\begin{aligned} C_0 &= I, \\ C_{i+1} &= \frac{-1}{r_0(i+1)} \left( \sum_{j=\max\{0, i-\deg(G)\}}^i G_{i-j} C_j + \sum_{j=\max\{0, i-\deg(r)\}+1}^i r_{i-j+1} (j C_j) \right). \end{aligned} \quad (5.5)$$

Again we will only carry out this computation to some finite  $p$ -adic working precision  $N'_C$ , and if we want  $C$  to be correct to  $p$ -adic precision  $N_C$ , then the precision  $N'_C$  has to be somewhat higher because of error propagation. An expression for  $N'_C$ , in terms of  $N_C$  and the desired  $t$ -adic precision  $K$ , was given by Lauder [23, Theorem 5.1], but his result can be significantly improved using Theorem 5.1, as we will now show.

Let  $\tilde{C} = \sum_{i=0}^{\infty} \tilde{C}_i t^i$  denote an approximation to  $C$  obtained using the approximate recursion:

$$\begin{aligned} \tilde{C}_0 &= I, \\ \tilde{C}_{i+1} &= \frac{-1}{r_0(i+1)} \left( \sum_{j=\max\{0, i-\deg(G)\}}^i G_{i-j} \tilde{C}_j + \sum_{j=\max\{0, i-\deg(r)\}+1}^i r_{i-j+1} (j \tilde{C}_j) \right) + E_{i+1}, \end{aligned}$$

where  $\text{ord}_p(E_i) \geq N'_C$  for all  $i \geq 1$ , so that the matrices  $\tilde{C}_i$  are computed with  $p$ -adic working precision  $N'_C$ .

**Proposition 5.5.** Let  $K, N_C \in \mathbf{N}$ , and suppose that

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

Then  $\text{ord}_p(\tilde{C}_i - C_i) \geq N_C$  for all  $i < K$ .

*Proof.* The matrix  $\tilde{C}$  satisfies the differential equation

$$\frac{d\tilde{C}}{dt} + M\tilde{C} = E, \quad \tilde{C}(0) = I,$$

where we have denoted  $E = \sum_{i=1}^{\infty} E_i t^i$ . One also checks that the matrix  $C^{-1}\tilde{C}$  satisfies the differential equation

$$\frac{d(C^{-1}\tilde{C})}{dt} = C^{-1}E, \quad (C^{-1}\tilde{C})(0) = I,$$

from which it follows that

$$\tilde{C}(t) - C(t) = C(C^{-1}\tilde{C} - I) = C(t) \left( \int_0^t C^{-1}(s)E(s)ds \right). \quad (5.6)$$

We know from Theorem 5.1 and Remark 5.3 that

$$\text{ord}_p(\overline{C}), \text{ord}_p(\overline{C^{-1}}) \geq -(2\delta + n - 1) \lceil \log_p(K-1) \rceil, \quad (5.7)$$

and we hence obtain

$$\text{ord}_p \left( \overline{\int_0^t C^{-1}(s)E(s)ds} \right) \geq N_C + ((2\delta + (n-1))) \lceil \log_p(K-1) \rceil.$$

From the bounds (5.7) and Equation (5.6), we deduce that  $\text{ord}_p(\overline{\tilde{C} - C}) \geq N_C$ .  $\square$

**Remark 5.6.** A result similar to Proposition 5.5 with a larger constant in front of the logarithm was obtained by Lauder in [23, Theorem 5.1]. We have not been able to find something similar to Proposition 5.4 in Lauder's work.

**Remark 5.7.** In order to determine the power series expansion of the matrix  $\Phi$ , we also need to compute the matrix  $\sigma(C)^{-1}$ . We could compute the matrix  $C^{-1}$  using matrix inversion over the ring  $\mathbf{Q}_q[[t]]$ . However, solving (5.3) turns out to be more efficient.

We finally give all the precisions necessary for computing the power series expansion of  $\Phi$  at  $t = 0$  to  $t$ -adic precision  $K$  and  $p$ -adic precision  $N_\Phi$ .

**Theorem 5.8.** Let  $K, N_\Phi \in \mathbf{N}$  and define:

$$\begin{aligned} N_{\Phi_0} &= N_\Phi + (2\delta + (n-1)) (\lceil \log_p(K-1) \rceil + \lceil \log_p(\lceil K/p \rceil - 1) \rceil), \\ N_C &= N_\Phi + (2\delta + (n-1)) \lceil \log_p(\lceil K/p \rceil - 1) \rceil + \delta, \\ N_{C^{-1}} &= N_\Phi + (2\delta + (n-1)) \lceil \log_p(K-1) \rceil + \delta, \\ N_M &= N_\Phi + (2(2\delta + (n-1)) + 1) \lceil \log_p(K-1) \rceil + 1, \\ N'_C &= N_\Phi + (2(2\delta + (n-1)) + 1) \lceil \log_p(K-1) \rceil, \\ N'_{C^{-1}} &= N_\Phi + (2(2\delta + (n-1)) + 1) \lceil \log_p(\lceil K/p \rceil - 1) \rceil. \end{aligned}$$

In order to compute the power series expansion of the matrix  $\Phi$  at  $t = 0$  with  $t$ -adic precision  $K$  and  $p$ -adic precision  $N_\Phi$ , it is sufficient to compute the matrix  $\Phi_0$  to  $p$ -adic precision  $N_{\Phi_0}$ , the matrix  $C$  to  $t$ -adic precision  $K$  and  $p$ -adic precision  $N_C$ , the matrix  $C^{-1}$  to  $t$ -adic precision  $\lceil K/p \rceil$  and  $p$ -adic precision  $N_{C^{-1}}$ , and the matrix  $M$  to  $p$ -adic precision  $N_M$ .

Therefore, while solving Equation (5.2) for  $C$  and Equation (5.3) for  $C^{-1}$ , using a recursion like in Equation (5.5), it is sufficient to use  $p$ -adic working precisions  $N'_C$  and  $N'_{C^{-1}}$ , respectively.

*Proof.* Recall that  $\Phi = C\Phi_0\sigma(C)^{-1}$ . The sufficient  $t$ -adic precisions are clear. We can apply Proposition 2.19, using Theorem 5.1 for both  $C$  and  $C^{-1}$  and the fact that  $\text{ord}_p(\Phi_0) \geq -\delta$  from Corollary 3.19, to obtain the sufficient  $p$ -adic precisions for the matrices  $\Phi_0$ ,  $C$  and  $C^{-1}$ . The sufficient precision for the matrix  $M$  follows from Proposition 5.4, and the sufficient working precisions  $N'_C$  and  $N'_{C^{-1}}$  follow from Proposition 5.5.  $\square$

Now we have all the ingredients to compute the power series expansion of  $\Phi$  at  $t = 0$  to any given  $p$ -adic and  $t$ -adic precisions, as formalised in Algorithm 5.1.

---

**Algorithm 5.1** Compute the power series expansion of  $\Phi$  at  $t = 0$ .

---

**Input:**  $P \in \mathbf{Z}_q[t][x_0, \dots, x_n]$  satisfying Assumption 4.11,  $t$ -adic precision  $K$ ,  $p$ -adic precision  $N_\Phi$ .

**Output:** The power series expansion of  $\Phi$  at  $t = 0$  to  $t$ -adic precision  $K$  and  $p$ -adic precision  $N_\Phi$ .

**procedure** FROBSERIEEXPANSION( $N_\Phi, K$ )

1. Determine  $N_M, N_{\Phi_0}, N_C, N_{C^{-1}}, N'_C$ , and  $N'_{C^{-1}}$  from Theorem 5.8.
  2.  $M \leftarrow \text{GMCONNECTION}(P, N_M)$
  3.  $\Phi_0 \leftarrow \text{DIAGFROB}(P_0, N_{\Phi_0})$
  4. Solve Equation (5.2) for  $C$  to  $t$ -adic precision  $K$  and  $p$ -adic precision  $N_C$ :  
 $C_0 \leftarrow I$   
**for**  $i = 0$  **to**  $K - 2$  **do**  
 $C_{i+1} \leftarrow \frac{-1}{r_0(i+1)} \left( \sum_j G_{i-j} C_j + \sum_j r_{i-j+1} (j C_j) \right) \bmod p^{N'_C}$   
 $C \leftarrow \sum_{i=0}^{K-1} C_i t^i \bmod p^{N_C}$
  5. Solve Equation (5.3) for  $C^{-1}$  to  $t$ -adic precision  $\lceil K/p \rceil$  and  $p$ -adic precision  $N_{C^{-1}}$ :  
 $(C^{-1})_0 \leftarrow I$   
**for**  $i = 0$  **to**  $\lceil K/p \rceil - 2$  **do**  
 $(C^{-1})_{i+1} \leftarrow \frac{-1}{r_0(i+1)} \left( \sum_j -G_{i-j}^t (C^{-1})_j + \sum_j r_{i-j+1} (j (C^{-1})_j) \right) \bmod p^{N'_{C^{-1}}}$   
 $C^{-1} \leftarrow \sum_{i=0}^{\lceil K/p \rceil - 1} (C^{-1})_i t^i \bmod p^{N_{C^{-1}}}$
  6.  $\Phi \leftarrow C\Phi_0\sigma(C^{-1})$
  7. **return**  $\Phi$
- 

## 6 The zeta function of a fibre

### 6.1 Evaluating $\Phi$ at a point

In the previous section we described how to compute the power series expansion at  $t = 0$  of the matrix  $\Phi$  for the action of  $p^{-1}F_p$  on  $H_{\text{rig}}^n(U/S)$ . We now want to evaluate  $\Phi$  at the Teichmüller lift  $\hat{\tau}$  of some nonzero  $\tau \in S(\mathbf{F}_q)$ , where  $\mathbf{F}_q/\mathbf{F}_q$  is a finite field extension, but the power series expansion of  $\Phi$  at  $t = 0$  usually only converges on the open unit disc  $|t| < 1$  and hence cannot be evaluated at  $\hat{\tau}$ .

However, since  $\Phi$  is a matrix of overconvergent functions, i.e.

$$\Phi \in M_{b \times b} \left( \mathbf{Q}_q \langle t, 1/r \rangle^\dagger \right),$$

it can be approximated to any given  $p$ -adic precision  $N$  by a matrix of rational functions, which can then be evaluated at  $\hat{\tau}$ . To convert the power series expansion for  $\Phi$  to such an approximation by rational functions, we need a bound on the pole order of these rational functions at their poles, as a function of  $N$ .



The bounds used by Lauder [21, §8.1] and Gerkmann [10, §6] were not very sharp, and this significantly impacted their algorithms. Recently, under some small additional assumptions, Kedlaya and the second author [19, Theorem 2.1] obtained a sharper bound that we state below in a simplified form. For  $z \in \mathbf{P}^1(\bar{\mathbf{Q}}_q)$ , we denote the valuation on  $\mathbf{Q}_q(t)$  corresponding to  $z$  by  $\text{ord}_z(-)$ , and we extend  $\text{ord}_z(-)$  to polynomials and matrices over  $\mathbf{Q}_q(t)$  by taking the minimum over the coefficients and entries, respectively. We recall that  $M$  denotes the matrix of the Gauss–Manin connection  $\nabla$  with respect to the basis  $\mathcal{B}$  from Definition 3.2 and let  $\delta$  be defined as in Definition 3.18.

**Theorem 6.1.** Let  $D \subset \mathbf{P}^1(\bar{\mathbf{Q}}_q)$  be a residue disk and  $z \in D$  a point such that  $M$  has at most a simple pole at  $z$  and no other poles contained in  $D$ . Suppose that the exponents  $\lambda_1, \dots, \lambda_b$  of  $M$  at  $z$ , which are defined as the eigenvalues of the matrix  $(t - z)M|_{t=z}$  and known to be rational numbers, are contained in  $\mathbf{Z}_p \cap \mathbf{Q}$ . For  $i \in \mathbf{N}$ , let

$$f(i) = \max \left\{ - (2\delta + (n - 1)) \lceil \log_p(i) \rceil, (b - 1) \text{ord}_p(M) - (2\delta + (n - 1)) \lceil \log_p(i) \rceil \right\},$$

and define

$$c = \begin{cases} 0 & \text{if } \text{ord}_p(M) \geq 0, \\ \min\{0, i + f(i) : i \in \mathbf{N}\} & \text{if } \text{ord}_p(M) < 0. \end{cases}$$

For  $N \in \mathbf{N}$ , let

$$g(N) = \max\{i \in \mathbf{N} : i + f(i) - \delta + c < N\},$$

and define

$$\alpha_1 = \lfloor -p \min_i \{\lambda_i\} + \max_i \{\lambda_i\} \rfloor,$$

$$\alpha_2 = \begin{cases} 0 & \text{if } M \text{ does not have a pole at } z, \\ 0 & \text{if } z \in \{0, \infty\}, \\ g(N) & \text{otherwise.} \end{cases}$$

Then the matrix  $\Phi$  is congruent modulo  $p^N$  to a matrix  $\tilde{\Phi} \in M_{b \times b}(\mathbf{Q}_q(t))$  for which

$$\text{ord}_z(\tilde{\Phi}) \geq -(\alpha_1 + p\alpha_2)$$

and  $\tilde{\Phi}$  has no other poles contained in  $D$ .

*Proof.* Since the matrix  $\Phi$  defines a Frobenius structure on the vector bundle  $H_{\text{rig}}^n(U/S)$  with connection  $\nabla$ , we can apply [19, Theorem 2.1]. We have replaced  $\text{ord}_p(\Phi)$  and  $\text{ord}_p(\Phi) + \text{ord}_p(\Phi^{-1})$  by their respective lower bounds  $-\delta$  and  $-2\delta + (n - 1)$ , since we might not know them exactly a priori.  $\square$

**Remark 6.2.** In practice, the constants  $-(2\delta + (n - 1))$ ,  $c$ ,  $\alpha_1$ , and  $-\delta$  are very small in absolute value, so that  $g(N)$  is about  $N$  and the lower bound for the order of  $\Phi$  modulo  $p^N$  at the point  $z$  is roughly  $-pN$ .

**Remark 6.3.** The condition that  $M$  has a simple pole at  $z$  is not a serious restriction. By [24, Theorem 2.1], one can always find a matrix  $W \in GL_b(\mathbf{Q}_q[t, 1/(t - z)])$  such that the connection matrix has a simple pole at  $z$  with respect to the basis  $[w_1, \dots, w_b]$  defined by  $w_j = \sum_{i=1}^b W_{ij} e_i$  for all  $1 \leq j \leq b$ , where  $\mathcal{B} = [e_1, \dots, e_b]$  denotes our basis from Definition 3.2. Now by [19, Corollary 2.6], the matrix  $\Phi$  is congruent modulo  $p^{N + \text{ord}_p(W) + \text{ord}_p(W^{-1})}$  to a matrix  $\tilde{\Phi} \in M_{b \times b}(\mathbf{Q}_q(t))$  for which

$$\text{ord}_z(\tilde{\Phi}) \geq -(\alpha_1 + p\alpha_2) + \text{ord}_z(W) + p \text{ord}_z(W^{-1})$$

and  $\tilde{\Phi}$  has no other poles contained in  $D$ . Here,  $\alpha_1$  and  $\alpha_2$  are defined as in Theorem 6.1, but with  $\delta$  replaced by

$$\delta' = \delta - (\text{ord}_p(W) + \text{ord}_p(W^{-1})),$$

since for the matrix  $\Phi'$  of  $p^{-1}F_p$  with respect to the basis  $[w_1, \dots, w_b]$ , in general we only have that  $\text{ord}_p(\Phi') \geq -\delta'$ .

When one of the other conditions in Theorem 6.1 is not satisfied, we can use the alternative bound below. Recall that our family of smooth projective hypersurfaces  $\mathcal{X}/\mathcal{S}$  is defined by the homogeneous polynomial  $P \in \mathbf{Z}_q[t][x_0, \dots, x_n]$ .

**Theorem 6.4.** Define the matrices  $\Delta_k$  over  $\mathbf{Q}_q(t)$  as in Definition 3.5. Let  $D \subset \mathbf{P}^1(\bar{\mathbf{Q}}_q)$  be a residue disk and for any point  $z \in D$  put

$$\begin{aligned} \mu_z &= \sum_{k=2}^n \text{ord}_z(\Delta_k^{-1}), \\ \nu_z &= \text{ord}_z(\Delta_{n+1}^{-1}). \end{aligned}$$

For  $N \in \mathbf{N}$ , define

$$h(N) = \max \{i \in \mathbf{N} : i + (n-1) + \text{ord}_p((n-1)!) - n \lfloor \log_p(p(n+i)-1) \rfloor < N\},$$

and put

$$\beta_z = \begin{cases} -\mu_z - (p(n+h(N)) - n)\nu_z & \text{if } z \neq \infty, \\ -\mu_z - (p(n+h(N)) - n)\nu_z + ph(N) \deg_t(P) & \text{if } z = \infty. \end{cases}$$

Then  $\Phi$  is congruent modulo  $p^N$  to a matrix  $\tilde{\Phi} \in M_{b \times b}(\mathbf{Q}_q(t))$  for which

$$\text{ord}_z(\tilde{\Phi}) \geq -\beta_z,$$

for all points  $z \in D$ .

*Proof.* First we extend  $\sigma$  to the ring of overconvergent functions:

$$\begin{aligned} A^\dagger &= \left\{ \sum_{i_0, \dots, i_{n+3}=0}^{\infty} a_{i_0, \dots, i_{n+3}} \frac{x_0^{i_0} \dots x_n^{i_n} t^{i_{n+1}}}{r^{i_{n+2}} P^{i_{n+3}}} : a_{i_0, \dots, i_{n+3}} \in \mathbf{Q}_q, \right. \\ &\quad \left. \exists c > 0 \text{ s.t. } \lim_{i_0 + \dots + i_{n+3} \rightarrow \infty} (\text{ord}_p(a_{i_0, \dots, i_{n+3}}) - c(i_0 + \dots + i_{n+3})) \geq 0 \right\}, \end{aligned}$$

by putting  $\sigma(x_i) = x_i^p$  for  $0 \leq i \leq n$ . Note that

$$\sigma\left(\frac{1}{P}\right) = P^{-p} \left(1 - \frac{P^p - \sigma(P)}{P^p}\right)^{-1}$$

is an element of  $A^\dagger$  since

$$\text{ord}_p(P^p - \sigma(P)) \geq 1.$$

We use the notation and terminology from Section 3. It is known that the de Rham cohomology of  $A^\dagger/\mathbf{Q}_q\langle t, 1/r \rangle^\dagger$  is isomorphic to the rigid cohomology of  $U/S$ , and that the action of  $F_p$  on the rigid cohomology of  $U/S$  is induced by  $\sigma$ . Recall that our basis vectors for  $H_{\text{rig}}(U/S)$  are of the form  $x^u \Omega/P^\ell$  with  $x^u \in B_\ell$  and  $\ell \leq n$ . We observe that

$$p^{-1}F_p\left(\frac{x^u \Omega}{P^\ell}\right) \equiv \sum_{i=0}^{\infty} \eta_i p^{n-1+i} \left(\frac{P^p - \sigma(P)}{p}\right)^i (x_0 \dots x_n)^{p-1} \left(\frac{x^{pu} \Omega}{P^{p(\ell+i)}}\right)$$

in  $H_{\text{rig}}^n(U/S)$ , where  $\eta_i \in \mathbf{N}$  is defined by the equality  $(1-y)^{-\ell} = \sum_{i=0}^{\infty} \eta_i y^i$ . Using Algorithm 3.2, we can write

$$\eta_i p^{n-1+i} \left( \frac{P^p - \sigma(P)}{p} \right)^i (x_0 \cdots x_n)^{p-1} \left( \frac{x^{pu} \Omega}{P^{p(\ell+i)}} \right) \equiv \frac{\gamma_{i,1} \Omega}{P^1} + \cdots + \frac{\gamma_{i,n} \Omega}{P^n}, \quad (6.1)$$

where  $\gamma_{i,j}$  is contained in the  $L$ -span of  $B_j$  for all  $i \geq 0$  and  $0 \leq j \leq n$ .

Actually, we can slightly modify Algorithm 3.1, so that we only have to solve systems of the form  $\Delta_{n+1} v = w$  as long as the pole order is at least  $n+1$ . Indeed, we may assume, without loss of generality, that  $Q = x^v$  is a monomial, and can find some other monomial  $x^w$  such that  $x^{v-w}$  is of degree  $(n+1)d - (n+1)$ . Now we apply Algorithm 3.1 to  $x^{v-w}$ , noting that  $B_{n+1} = \emptyset$ , and multiply the output by  $x^w$  to obtain the decomposition of  $x^v$ .

Note that the left-hand side of Equation (6.1) does not have a pole at  $z \neq \infty$ , and has order at least  $-ip \deg_t(P)$  at  $z = \infty$ . When applying Algorithm 3.2 to this expression, as long as the pole order is at least  $n+1$ , the order at  $z$  drops by at most  $\nu_z$  in every reduction step, and it drops by at most  $\mu_z$  in the remaining reduction steps. This implies that

$$\text{ord}_z(\gamma_{i,j}) \geq \begin{cases} \mu_z + (p(n+i) - n)\nu_z & \text{if } z \neq \infty, \\ \mu_z + (p(n+i) - n)\nu_z - pi \deg_t(P) & \text{if } z = \infty. \end{cases} \quad (6.2)$$

For every  $\tau \in S(\bar{\mathbf{F}}_q)$ , we define lattices  $\Lambda_{\tau, \text{cryst}}$ ,  $\Lambda_{\tau, \mathcal{B}}$  in  $H_{\text{rig}}^n(U_{\tau})$  as in the proof of Theorem 3.17. It follows from [1, Proposition 3.4.6], Equation (6.1), and the inclusion  $(n-1)! \Lambda_{\tau, \text{cryst}} \subset \Lambda_{\tau, \mathcal{B}}$  that

$$\frac{\gamma_{i,1} \Omega}{P^1} + \cdots + \frac{\gamma_{i,n} \Omega}{P^n} \subset p^{i+(n-1) - \text{ord}_p((n-1)! - n \lfloor \log_p(p(n+i)-1) \rfloor)} \Lambda_{\tau, \mathcal{B}},$$

which implies that

$$\text{ord}_p(\gamma_{i,j}) \geq i + (n-1) - \text{ord}_p((n-1)! - n \lfloor \log_p(p(n+i)-1) \rfloor).$$

The entries of  $\Phi$  are coefficients of sums of the form  $\sum_{i=0}^{\infty} \gamma_{i,j}$ . Now modulo  $p^N$ , we can restrict this sum to terms for which  $\text{ord}_p(\gamma_{i,j}) < N$ , and we can compute the order at  $z$  of these terms using (6.2). This completes the proof.  $\square$

**Remark 6.5.** A result similar to, but weaker than, Theorem 6.4 was obtained by Gerkmann in [10, Section 6].

**Theorem 6.6.** Let  $N_{\Phi} \in \mathbf{N}$ . We can explicitly find  $s \in \mathbf{Z}_q[t]$  and  $K \in \mathbf{N}$ , where  $s$  divides some power of the polynomial  $R$  from Definition 3.12, such that  $s\Phi$  is congruent modulo  $p^{N_{\Phi}}$  to a matrix of polynomials of degree less than  $K$ .

*Proof.* On every residue disk  $D \subset \mathbf{P}^1(\bar{\mathbf{Q}}_q)$ , we can apply either Theorem 6.1 (when it applies) or Theorem 6.4 in order to find numbers  $\theta_z \in \mathbf{N}_0$  such that  $\Phi$  is congruent modulo  $p^N$  to a matrix  $\tilde{\Phi} \in M_{b \times b}(\mathbf{Q}_q(t))$  for which  $\text{ord}_z(\tilde{\Phi}) \geq -\theta_z$  for all  $z \in D$ . By Theorem 6.4, we can take  $\theta_z = 0$  for  $z \neq \infty$  if  $R(z) \neq 0$ , so that  $\theta_z$  vanishes for all but finitely many  $z \in \mathbf{P}^1(\bar{\mathbf{Q}}_q)$ . Moreover, by Theorem 6.1, we can also take  $\theta_z = 0$  whenever the matrix  $M$  does not have a pole in the residue disk at  $z$ . Finally, we may assume that  $\theta_z = \theta_{z'}$  if  $z, z'$  are conjugates over  $\mathbf{Q}_q$ . We now define

$$s = \prod_{z \neq \infty, \text{ord}_p(z) \geq 0} (t-z)^{\theta_z} \prod_{z \neq \infty, \text{ord}_p(z) < 0} \left( \frac{t}{z} - 1 \right)^{\theta_z}, \quad K = \left( \sum_z \theta_z \right) + 1,$$

which satisfy all the required conditions.  $\square$

We compute the matrix  $\Phi$  to  $t$ -adic precision  $K$  and  $p$ -adic precision  $N_\Phi$  using Algorithm 5.1. For any  $\tau \in S(\bar{\mathbf{F}}_q)$ , we can now compute

$$\Phi_\tau = s(\hat{\tau})^{-1} (s\Phi \bmod t^K) |_{t=\hat{\tau}} \bmod p^{N_\Phi}.$$

Since  $\text{ord}_p(s(\hat{\tau})) = 0$ ,  $\text{ord}_p(\hat{\tau}) \geq 0$  and  $\text{ord}_p(\Phi) \geq -\delta$ , by Proposition 2.19 the matrix  $\Phi_\tau$  will also be correct to precision  $N_\Phi$  provided that  $\hat{\tau}$  is computed to  $p$ -adic precision  $N_\Phi + \delta$ .

## 6.2 Computing the zeta function

Now we want to compute the zeta function of the fibre  $X_\tau$  of our family  $X/S$  lying over some  $\tau \in S(\mathbf{F}_q)$ , where  $\mathbf{F}_q/\mathbf{F}_q$  is a finite field extension. Recall from Theorem 2.13 that the zeta function of  $X_\tau$  is of the form

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

where  $\chi(T) = \det(1 - Tq^{-1}F_q | H_{\text{rig}}^n(U_\tau)) \in \mathbf{Z}[T]$  denotes the reverse characteristic polynomial of the action of  $q^{-1}F_q$  on  $H_{\text{rig}}^n(U_\tau)$ .

We start by computing the matrix of the action of  $q^{-1}F_q$  on  $H_{\text{rig}}^n(U_\tau)$ . Let us still denote  $a = \log_p(q)$ . Recall that  $\Phi_\tau$  is the matrix of the action of  $p^{-1}F_p$  on  $H_{\text{rig}}^n(U_\tau)$  with respect to the basis  $\mathcal{B}$ . As this action is  $\sigma$ -semilinear, we have that

$$\Phi_\tau^{(a)} = \Phi_\tau \sigma(\Phi_\tau) \cdots \sigma^{a-1}(\Phi_\tau)$$

is the matrix of the action of  $q^{-1}F_q$  on  $H_{\text{rig}}^n(U_\tau)$ .

We now analyse the loss of  $p$ -adic precision when computing the reverse characteristic polynomial  $\chi(T) = 1 + \sum_{i=1}^b \chi_i T^i = \det(1 - T\Phi_\tau^{(a)})$ .

**Theorem 6.7.** Let  $N_\Phi \in \mathbf{N}$  be such that  $N_\Phi \geq \delta$ , where  $\delta$  is defined as in Definition 3.18. Moreover, suppose that  $\tilde{\Phi}_\tau$  is an approximation to  $\Phi_\tau$  satisfying  $\text{ord}_p(\Phi_\tau - \tilde{\Phi}_\tau) \geq N_\Phi$ . Let us denote

$$\tilde{\chi}(T) = 1 + \sum_{i=1}^b \tilde{\chi}_i T^i = \det(1 - T\tilde{\Phi}_\tau^{(a)}).$$

Then for all  $1 \leq i \leq b$ , we have

$$\text{ord}_p(\chi_i - \tilde{\chi}_i) \geq N_\Phi - \delta.$$

*Proof.* Recall from Theorem 3.17 that there exists a matrix  $W_\tau \in M_{b \times b}(\mathbf{Q}_q)$  satisfying  $\text{ord}_p(W_\tau) + \text{ord}_p(W_\tau^{-1}) \geq -\delta$  such that for  $\Phi'_\tau = W_\tau \Phi_\tau \sigma(W)^{-1}$  we have  $\text{ord}_p(\Phi'_\tau) \geq 0$ .

Defining the matrix  $\tilde{\Phi}'_\tau = W_\tau \tilde{\Phi}_\tau \sigma(W)^{-1}$ , we find that  $\text{ord}_p(\Phi'_\tau - \tilde{\Phi}'_\tau) \geq N - \delta$  and in particular  $\text{ord}_p(\tilde{\Phi}'_\tau) \geq 0$ . Thus, we obtain

$$\text{ord}_p \left( \det(1 - T(\Phi'_\tau)^{(a)}) - \det(1 - T(\tilde{\Phi}'_\tau)^{(a)}) \right) \geq N - \delta.$$

Note that  $(\Phi'_\tau)^{(a)} = W_\tau \Phi_\tau^{(a)} W_\tau^{-1}$  and  $(\tilde{\Phi}'_\tau)^{(a)} = W_\tau \tilde{\Phi}_\tau^{(a)} W_\tau^{-1}$ , so that

$$\chi(T) = \det(1 - T(\Phi'_\tau)^{(a)}), \quad \tilde{\chi}(T) = \det(1 - T(\tilde{\Phi}'_\tau)^{(a)}).$$

This completes the proof.  $\square$

**Remark 6.8.** If we know  $\Phi_\tau$  to  $p$ -adic precision  $N_\Phi$ , then  $\chi(T)$  is determined to precision  $N_\Phi - \delta$ . However, we cannot compute  $\chi(T)$  as in the proof of Theorem 6.7, since we do not know the matrix  $W_\tau$  explicitly. When computing with respect to our basis  $\mathcal{B}$ , there will be loss of  $p$ -adic precision. The loss of precision in computing  $\Phi_\tau^{(a)}$  from  $\Phi_\tau$  is at most  $(a-1)\delta$ , and the loss of precision in computing  $\chi(T)$  from  $\Phi_\tau^{(a)}$  is at most  $(b-1)\delta$ , by Proposition 2.18 and Corollary 3.19. Therefore, for  $\chi(T)$  to be correct to  $p$ -adic precision  $N_\Phi - \delta$ , it is sufficient to compute  $\chi(T)$  from  $\Phi_\tau$  using  $p$ -adic working precision

$$(N_\Phi - \delta) + ((a-1) + (b-1))\delta = N_\Phi + (a+b-3)\delta.$$

When  $p \geq n$ , one can improve Theorem 6.7 by taking into account the Hodge numbers  $h^{i,n-1-i}$  of  $H_{\text{dR}}^n(\mathfrak{U}/\mathfrak{S})$ . Recall from Remark 3.10 that  $h^{i,n-1-i} = |B_i|$ .

**Definition 6.9.** Define  $\Gamma: [0, b] \rightarrow \mathbf{R}$  to be the function whose graph is the convex polygon in the plane whose left-most point is the origin and which has slope  $i$  over the interval of the horizontal axis

$$[h^{0,n-1} + \dots + h^{i-1,n-i}, h^{0,n-1} + \dots + h^{i,n-i-1}].$$

Note that  $\Gamma(b) = b(n-1)/2$  since  $h^{i,n-1-i} = h^{n-1-i,i}$  for all  $0 \leq i \leq n-1$ .

**Theorem 6.10.** We continue with the notation of Theorem 6.7. Let  $N_\Phi \in \mathbf{N}$  and suppose that  $p \geq n$ . If  $\tilde{\Phi}_\tau$  is an approximation to  $\Phi_\tau$  such that  $\text{ord}_p(\Phi_\tau - \tilde{\Phi}_\tau) \geq N_\Phi$  then, for all  $1 \leq i \leq b$ , we have

$$\text{ord}_p(\chi_i - \tilde{\chi}_i) \geq N_\Phi + a\Gamma(i-1).$$

*Proof.* Note that in this case  $\delta = 0$  and hence that  $\text{ord}_p(\Phi_\tau) \geq 0$ . By a result of Mazur [26, p. 665–666], the map  $p^{-1}\mathbb{F}_p$  sends  $(H_i)_{\tilde{\tau}} \cap \Lambda_{\tau, \text{crys}}$  into  $p^i \Lambda_{\tau, \text{crys}}$ , where  $\Lambda_{\tau, \text{crys}}$  is defined as in the proof of Theorem 3.17 and  $H_i$  as in Remark 3.10. This implies that the so called Hodge polygon of the  $F$ -crystal  $(\Lambda_{\tau, \text{crys}}, p^{-1}\mathbb{F}_p)$  lies above the graph of  $\Gamma$ . From this it follows that the Hodge polygon of the  $F$ -crystal  $(\Lambda_{\tau, \text{crys}}, \mathfrak{q}^{-1}\mathbb{F}_\mathfrak{q})$  lies above the graph of  $a\Gamma$ . Hence we can find an invertible matrix  $W_\tau \in M_{b \times b}(\mathbf{Z}_\mathfrak{q})$  such that for all  $1 \leq i \leq b$ , the sum of the valuations of any  $i$  different columns of  $W_\tau \Phi_\tau^{(a)} W_\tau^{-1}$  is at least  $a\Gamma(i)$ . Note that

$$\text{ord}_p(W_\tau \Phi_\tau^{(a)} W_\tau^{-1} - W_\tau \tilde{\Phi}_\tau^{(a)} W_\tau^{-1}) \geq N_\Phi.$$

The coefficients  $\chi_i$  and  $\tilde{\chi}_i$  are alternating sums of products of  $i$  elements from different columns of  $W_\tau \Phi_\tau^{(a)} W_\tau^{-1}$  and  $W_\tau \tilde{\Phi}_\tau^{(a)} W_\tau^{-1}$ , respectively. Therefore, the required bound follows from Theorem 2.18.  $\square$

**Remark 6.11.** For  $a = 1$ , Theorem 6.10 was obtained by Lauder in [23, Proposition 9.4] and the general idea of using the Hodge filtration to lower  $p$ -adic precision bounds had already been suggested before in [1, Remark 1.6.4]. However, we have not been able to find Theorem 6.10 in the literature for  $a \neq 1$ .

Now we determine the  $p$ -adic precision  $N_{\chi_i}$  to which we need to compute  $\chi_i$  in order to recover the integer polynomial  $\chi(T)$  exactly.

**Theorem 6.12.** In order to recover the integer polynomial  $\chi(T)$  exactly, it suffices to compute  $\chi_i$  to  $p$ -adic precision

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

*Proof.* By Theorem 2.1 and the short exact sequence (2.4), we have

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

where the  $\alpha_i$  are algebraic integers of absolute value  $\mathfrak{q}^{(n-1)/2}$  that are permuted under the map  $\alpha \mapsto \mathfrak{q}^{n-1}/\alpha$ . If we denote  $s_j = \sum_{i=1}^b \alpha_i^j$ , then clearly

$$|s_j| \leq b\mathfrak{q}^{j(n-1)/2}.$$

for all  $1 \leq j \leq b$ . Moreover, if we write  $\chi(T) = 1 + \sum_{i=1}^b \chi_i T^i$ , then by the Newton–Girard identities we have

$$s_j + j\chi_j = - \sum_{i=1}^{j-1} s_{j-i}\chi_i. \quad (6.3)$$

This means that if we are given  $\chi_1, \dots, \chi_{j-1}$ , then we can limit  $\chi_j$  to an explicit disk in the complex plane of radius  $(b/j)\mathfrak{q}^{j(n-1)/2}$ . Therefore, if we know each  $\chi_i$  to  $p$ -adic precision  $N_{\chi_i}$  satisfying

$$p^{N_{\chi_i}} > \frac{2b}{i}\mathfrak{q}^{i(n-1)/2},$$

we can determine  $\chi(T)$  exactly using the recursion (6.3).  $\square$

**Remark 6.13.** This bound was first obtained by Kedlaya in [16], although it does not appear there in exactly this form.

**Theorem 6.14.** Let  $N_{\chi_i}$  be defined as in Theorem 6.12. In order to compute  $\chi(T)$  exactly, it is sufficient to compute  $\Phi_\tau$  with  $p$ -adic precision

$$N_\Phi = \max_{1 \leq i \leq b} \{N_{\chi_i}\} + \delta.$$

If moreover  $p \geq n$ , then this can be improved to

$$N_\Phi = \max_{1 \leq i \leq b} \{N_{\chi_i} - a\Gamma(i-1)\}.$$

*Proof.* This follows easily by combining Theorem 6.12 with Theorem 6.7 and Theorem 6.10, respectively.  $\square$

**Remark 6.15.** If the sign  $\epsilon = \pm 1$  is known for which  $\det(\Phi_\tau^{(a)}) = \epsilon\mathfrak{q}^{b(n-1)/2}$ , then this can be improved further. Since  $\prod_{i=1}^b \alpha_i = \epsilon\mathfrak{q}^{b(n-1)/2}$ , and the  $\alpha_i$  are permuted under the map  $\alpha \mapsto \mathfrak{q}^{n-1}/\alpha$ , we have

$$\chi_{b-i} = \epsilon(-1)^b \mathfrak{q}^{(n-1)(b/2-i)} \chi_b.$$

So  $\chi(T)$  is uniquely determined already by  $\chi_1, \dots, \chi_{\lfloor b/2 \rfloor}$ , and it is sufficient to take the maxima in Theorem 6.14 running only over  $1 \leq i \leq \lfloor b/2 \rfloor$ .

It is well known that  $\epsilon = 1$  when  $n$  is even, but when  $n$  is odd  $\epsilon$  is usually not known. In practice it is then often still possible to use a smaller precision by computing  $\epsilon$  first. Let  $j$  be the smallest positive integer such that  $\chi_{\lfloor b/2 \rfloor - j} \neq 0$ . To recover  $\chi_0, \dots, \chi_{\lfloor b/2 \rfloor + j}$ , it is sufficient to take the maxima in Theorem 6.14 running only over  $1 \leq i \leq \lfloor b/2 \rfloor + j$ . This allows us to determine  $\epsilon$  from the two coefficients  $\chi_{\lfloor b/2 \rfloor - j}$  and  $\chi_{\lfloor b/2 \rfloor + j}$ .

We now formalise the complete algorithm for computing  $Z(X_\tau, T)$  in Algorithm 6.1.

**Remark 6.16.** The output of Algorithm 6.1 only depends on  $X_\tau$ . In particular, we can also take a polynomial  $\bar{P} \in \mathbf{F}_q[t][x_0, \dots, x_n]$  as input and at the start of the algorithm take  $P$  to be an arbitrary lift of  $\bar{P}$ . For the complexity analysis in the next section, we thus take the input size to be the size of  $\bar{P}$ . However, from a practical point of view, it is convenient to keep the lift  $P$  as the input, since:

- (i) the matrices  $M, \Phi_0, C, \Phi, \Phi_\tau$  do depend on  $P$ ,
- (ii) Assumption 4.11 needs to hold for  $P$ ,
- (iii) the runtime and memory usage of the algorithm depend on  $P$ .

---

**Algorithm 6.1** Compute  $Z(X_\tau, T)$ .

---

**Input:**  $P \in \mathbf{Z}_q[t][x_0, \dots, x_n]$  homogeneous of degree  $d$  satisfying Assumption 4.11 and  $\tau \in S(\mathbf{F}_q)$ .

**Output:** The zeta function  $Z(X_\tau, T)$  of the fibre  $X_\tau$  lying over  $\tau$ .

**procedure** ZETAFUNCTION( $P, \tau$ )

1. Determine  $N_\Phi$  from Theorem 6.14.
  2.  $N'_\Phi \leftarrow N_\Phi + (a + b - 3)\delta$
  3. Determine  $K \in \mathbf{N}$  and  $s \in \mathbf{Z}_q[t]$  from Theorem 6.6.
  4. Compute  $\Phi \leftarrow \text{FROBSERIESEXPANSION}(N_\Phi, K)$ .
  5. Determine  $\hat{\tau} \in \mathcal{S}(\mathbf{Z}_q)$  to  $p$ -adic precision  $N_\Phi + \delta$ .
  6. Compute  $\Phi_\tau \leftarrow s(\hat{\tau})^{-1}(a\Phi \bmod t^K)|_{t=\hat{\tau}}$  to  $p$ -adic precision  $N_\Phi$ , using  $p$ -adic working precision  $N_\Phi + \delta$ .
  7. Compute  $\chi(T) \leftarrow \det(1 - T(\Phi_\tau \sigma(\Phi_\tau) \cdots \sigma^{a-1}(\Phi_\tau)))$  to  $p$ -adic precision  $N_\Phi - \delta$ , using  $p$ -adic working precision  $N'_\Phi$ .
  8. Round  $\chi(T)$  to  $\mathbf{Z}[T]$  using the recursion (6.3).
  9. Set  $Z(X_\tau, T) \leftarrow (\chi(T)^{(-1)^n}) / ((1 - T)(1 - qT) \cdots (1 - q^{n-1}T))$ .
  10. **return**  $Z(X_\tau, T)$
- 

## 7 Complexity

In this section we determine the complexity of Algorithm 6.1. We denote  $a' = \log_p(q)$ , noting that  $a'$  divides  $a$ , and let  $d_t$  denote the degree of  $P$  in the variable  $t$ .

We use the  $\tilde{O}(-)$  notation that ignores logarithmic factors, i.e.  $\tilde{O}(f)$  denotes the class of functions that lie in  $O(f \log^k(f))$  for some  $k \in \mathbf{N}$ .

Let us first revisit some results concerning the complexity of the, sometimes basic, constituent operations. We recall that two  $k$ -bit integers can be multiplied in  $\tilde{O}(k)$  bit operations, and that two degree- $k$  polynomials can be multiplied in  $\tilde{O}(k)$  ring operations. We let  $\omega$  denote an exponent for matrix multiplication, so that two  $k \times k$  matrices can be multiplied in  $O(k^\omega)$  ring operations. An invertible  $k \times k$  matrix can then be inverted in  $O(k^\omega)$  ring operations as well. Moreover, it is known [28] that one can take  $\omega \leq 2.3729$ . Finally, we point out that the characteristic polynomial of a matrix can be computed in  $O(b^\omega \log(b))$  field operations using an algorithm of Keller-Gehrig [20].

Next we consider specific  $p$ -adic operations, referring the reader to Hubrechts [13] for further details. First, images of elements of  $\mathbf{Q}_q$  under  $\sigma^i$ , for  $0 < i < a$ , can be computed to  $p$ -adic precision  $N$  in time  $\tilde{O}(a \log^2(p) + aN \log(p))$ . Second, the Teichmüller lift of an element of  $\mathbf{F}_q$  can be computed to precision  $N$  in time  $\tilde{O}(aN \log^2(p))$ .

We start by estimating the degrees of the numerator and denominator of the connection matrix  $M$ .

**Proposition 7.1.** The degrees of  $H$ ,  $R$  from Proposition 3.13, and  $G$ ,  $r$  from Section 5 are all  $O(n(de)^n d_t) \subset \tilde{O}((de)^n d_t)$ .

*Proof.* Note that  $\Delta_k$  in Definition 3.12 is a square matrix of degree  $d_t$ , with

$$\binom{kd - 1}{n} \leq \left( \frac{e(kd - 1)}{n} \right)^n < (de)^n$$

columns, where  $e$  denotes the base for the natural logarithm. The result follows easily from this. Note that the degrees of the numerators and denominators of all intermediate results in Algorithm 3.3 are also  $\tilde{O}((de)^n d_t)$ .  $\square$

Next we estimate the precisions that we require.

**Proposition 7.2.** All  $p$ -adic precisions that we use lie in  $\tilde{O}(ad^n \log(d_t))$  and  $\deg(s), K$  are both  $\tilde{O}(apd^n(de)^n d_t)$ .

*Proof.* Note that  $b \in O(d^n)$  and  $\delta \in O(n)$ . In Theorem 6.14, we have

$$\max_{1 \leq i \leq b} \{N_{\chi_i}\} \in O(amb + \log(b)) \subset \tilde{O}(ad^n), \quad N_{\Phi} \in \tilde{O}(ad^n).$$

The precisions  $N'_{\Phi}$  and  $N_{\Phi} \pm \delta$  in Algorithm 6.1 are then  $\tilde{O}(ad^n)$  as well. It follows from Theorem 6.4 that in Theorem 6.6 we can take

$$\deg s \leq \deg\left(\prod_{k=2}^n \det(\Delta_k)\right) + (p(n + h(N_{\Phi})) - n) \deg(\det(\Delta_{n+1})),$$

$$K \leq \deg(s) + 1 + \deg\left(\prod_{k=2}^n \Delta_k^{-1}\right) + (p(n + h(N_{\Phi})) - n) \deg(\Delta_{n+1}^{-1}) + ph(N_{\Phi})d_t.$$

Consequently, we obtain

$$\deg(s), K \in \tilde{O}(apd^n(de)^n d_t).$$

The  $p$ -adic precisions  $N_{\Phi_0}, N_C, N_M, N_{C-1}, N'_C,$  and  $N'_{C-1}$  in Theorem 5.8 are in  $\tilde{O}(ad^n \log(d_t))$ , noting that the logarithms that appear there are to base  $p$ . Finally, the remaining  $p$ -adic precisions  $N'_M$  and  $N'_{\Phi}$  are also  $\tilde{O}(ad^n \log(d_t))$  by Remark 3.11 and Corollary 4.8, respectively.  $\square$

We now analyse the computation of the connection matrix  $M$ .

**Proposition 7.3.** The computation of the connection matrix  $M$  using Algorithm 3.3 requires

$$\begin{aligned} \text{time: } & \tilde{O}(aa' \log(p)(d^{n(\omega+2)} e^{n(\omega+1)} + d^{5n} e^{3n})d_t), \\ \text{space: } & \tilde{O}(aa' \log(p)d^{4n} e^{3n} d_t). \end{aligned}$$

*Proof.* We first need to construct and invert the matrices  $\Delta_k$ . This is dominated by the inversion, which requires  $O((de)^{n\omega})$  operations in the ring  $\mathbf{Q}_q[t]$  to  $p$ -adic precision  $\tilde{O}(ad^n \log(d_t))$ . As there are  $O(n)$  of these matrices, this takes time

$$\tilde{O}((de)^{n\omega}(a' \log(p))(ad^n \log(d_t))((de)^n d_t)) = \tilde{O}(aa' \log(p)d^{n(\omega+2)} e^{n(\omega+1)} d_t).$$

Then we multiply each of the monomials in our basis with  $-k(\partial P/\partial t)$  for some  $1 \leq k \leq n$  and reduce the product to the basis by repeatedly using Algorithm 3.1. For each of these monomials this takes time

$$\tilde{O}((de)^{2n}(a' \log(p))(ad^n \log(d_t))((de)^n d_t)) = \tilde{O}(aa' \log(p)d^{4n} e^{3n} d_t),$$

because of the quadratic complexity of the matrix-vector product. There are  $b \in O(d^n)$  monomials in our basis and hence this takes time  $\tilde{O}(aa' \log(p)d^{5n} e^{3n} d_t)$ .

During this computation we have to store  $O(n)$  matrices and vectors of size

$$\tilde{O}((de)^{2n}(a' \log(p))(ad^n \log(d_t))((de)^n d_t)),$$

which completes the proof.  $\square$

Next we consider the computation of the matrix  $\Phi_0$ .

**Proposition 7.4.** The computation of the matrix  $\Phi_0$  with Algorithm 4.1 requires

$$\begin{aligned} \text{time: } & \tilde{O}(a^3 p d^{4n} \log^3(d_t)), \\ \text{space: } & \tilde{O}(a \log(p) d^{2n} \log(d_t)). \end{aligned}$$



*Proof.* In Proposition 4.10, we have  $\mathcal{R} \in \tilde{O}(N'_{\Phi_0})$ . In Definition 4.1, the sums

$$\left(\frac{u_i + 1}{d}\right)_r \sum_{j=0}^r \frac{(pa_i^{p-1})^{r-j}}{(m-pj)!j!}$$

consist of  $O(\mathcal{R})$  terms. Note that each term can be computed from the previous one in  $O(p)$  operations in  $\mathbf{Z}_p$ . For each  $r$ , the sum can therefore be computed in time  $O(p\mathcal{R}N'_{\Phi_0})$ . We have to consider  $O(\mathcal{R})$  values of  $r$ , so each  $\alpha_{u,v}$  can be computed in time

$$\tilde{O}(np\mathcal{R}^2N'_{\Phi_0}) \subset \tilde{O}(a^3pd^{3n}\log^3(d_t)).$$

We need to compute  $b \in O(d^n)$  of these  $\alpha_{u,v}$ , so the computation of  $\Phi_0$  takes time  $\tilde{O}(a^3pd^{4n}\log^3(d_t))$ .

The required space is dominated by the size of the output, which is

$$\tilde{O}(b\log(p)N'_{\Phi_0}) \subset \tilde{O}(a\log(p)d^{2n}\log(d_t)). \quad \square$$

**Remark 7.5.** Note that the time complexity in Proposition 7.4 is quasilinear in  $p$ , while in the work of Lauder [21] it is quasiquadratic. The main reason for this is that Lauder computed in the totally ramified extension  $\mathbf{Q}_p(\pi)$  with  $\pi^{p-1} = -p$ , where a single multiplication already takes time quasilinear in  $p$ . It will turn out that this crucial improvement also decreases the overall time complexity of the deformation method from being quasiquadratic to quasilinear in  $p$ .

We should mention that there is a small downside to our approach. The time complexity in Proposition 7.4 is quasicubic in  $a$ , while by using fast exponentials over  $\mathbf{Q}_p(\pi)[[z]]$ , this can be decreased to being quasiquadratic in  $a$ , which again has an effect on the entire deformation method. We address this in the following proposition.

**Proposition 7.6.** Alternatively, the matrix  $\Phi_0$  can be computed in

$$\begin{aligned} \text{time: } & \tilde{O}(a^2pd^{2n}(p+d^n)\log^2(d_t)), \\ \text{space: } & \tilde{O}(a^2p^2d^{2n}\log^2(d_t)). \end{aligned}$$

*Proof.* In Proposition 4.10, we have  $\mathcal{M} \in \tilde{O}(pN'_{\Phi_0})$ . Let  $\mathbf{Q}_p(\pi)$  denote the totally ramified extension of  $\mathbf{Q}_p$  with  $\pi^{p-1} = -p$ . Recall from the proof of Proposition 4.6 that in Definition 4.1, up to a factor  $(-1)^r(\pi a_i)^{m-(p-1)r}$ , the sum

$$\sum_{j=0}^r \frac{(pa_i^{p-1})^{r-j}}{(m-pj)!j!}$$

is equal to the coefficient  $\lambda_m$  of  $x^m$  in the power series expansion of  $\exp(\pi a_i(x-x^p))$ . However, the power series expansion of  $\exp(\pi a_i(x-x^p))$  modulo  $x^{\mathcal{M}+1}$  can be computed in  $\tilde{O}(\mathcal{M})$  operations in  $\mathbf{Q}_p(\pi)$  following Brent [4]. Since a single operation in  $\mathbf{Q}_p(\pi)$  takes time  $\tilde{O}(pN'_{\Phi_0})$ , precomputing these power series expansions for all  $0 \leq i \leq n$  takes time

$$\tilde{O}(np^2(N'_{\Phi_0})^2) \subset \tilde{O}(a^2p^2d^{2n}\log^2(d_t)).$$

Each  $\alpha_{u,v}$  can now be computed as in Proposition 7.4 in time

$$\tilde{O}(p(N'_{\Phi_0})^2) \subset \tilde{O}(a^2pd^{2n}\log^2(d_t)),$$

so computing all  $b \in O(d^n)$  of these  $\alpha_{u,v}$  takes time  $\tilde{O}(a^2p^2d^{3n}\log^2(d_t))$ . Hence  $\Phi_0$  can be computed in time  $\tilde{O}(a^2pd^{2n}(p+d^n)\log^2(d_t))$ .

The space requirement is dominated by that of the power series expansions of  $\exp(\pi a_i(x-x^p))$  modulo  $x^{\mathcal{M}+1}$  for  $0 \leq i \leq n$  and is therefore given by

$$\tilde{O}(n\mathcal{M}pN'_{\Phi_0}) \subset \tilde{O}(a^2p^2d^{2n}\log^2(d_t)). \quad \square$$

We now consider the computation of the power series expansion of the matrix  $\Phi$ .

**Proposition 7.7.** Assume that the matrices  $M = G/r$  and  $\Phi_0$  have been computed already. The subsequent computation of the power series expansion of the matrix  $\Phi$  in Algorithm 5.1 then requires

$$\begin{aligned} \text{time: } & \tilde{O}(a^2 a' p d^{n(\omega+4)} e^{2n} d_t^2), \\ \text{space: } & \tilde{O}(a^2 a' p d^{5n} e^n d_t). \end{aligned}$$

*Proof.* The computation of the power series expansion of  $\Phi$  comprises three steps, namely the computation of the matrices  $C$ ,  $\sigma(C)^{-1}$  and the matrix product  $C\Phi_0\sigma(C)^{-1}$ .

As each of the  $K$  steps in the computation of  $C$  is dominated by the computation of  $\tilde{O}((de)^n d_t)$  matrix products, the matrix  $C$  can be computed in time

$$\tilde{O}(K((de)^n d_t) b^\omega (a' \log(p))(ad^n \log(d_t))) \subset \tilde{O}(a^2 a' p d^{n(\omega+4)} e^{2n} d_t^2).$$

Similarly, the matrix  $C^{-1}$  can be computed in time

$$\tilde{O}((K/p)((de)^n d_t) b^\omega (a' \log(p))(ad^n \log(d_t))) \subset \tilde{O}(a^2 a' \log(p) d^{n(\omega+4)} e^{2n} d_t^2).$$

Moreover, applying  $\sigma$  to the matrix  $C^{-1}$  takes time

$$\tilde{O}((K/p)b^2 (a' \log^2(p) + a'(ad^n \log(d_t)) \log(p))) \subset \tilde{O}(a^2 a' \log^2(p) d^{5n} e^n d_t).$$

Finally, the matrix product  $C\Phi_0\sigma(C)^{-1}$  can be computed in time

$$\tilde{O}(b^\omega K(a' \log(p))(ad^n \log(d_t))) \subset \tilde{O}(a^2 a' p d^{n(\omega+3)} e^n d_t).$$

The result on the time complexity now follows.

The space requirement is dominated by the matrix  $C$ , which has size

$$\tilde{O}(b^2 K(a' \log(p))(ad^n \log(d_t))) \subset \tilde{O}(a^2 a' p d^{5n} e^n d_t). \quad \square$$

We now move on to the computation of the matrix  $\Phi_\tau$ .

**Proposition 7.8.** The computation of the matrix  $\Phi_\tau$  from the matrix  $\Phi$  and  $\tau \in S(\mathbf{F}_q)$  requires

$$\begin{aligned} \text{time: } & \tilde{O}(a^2 a' p d^{5n} e^n d_t), \\ \text{space: } & \tilde{O}(a^2 a' p d^{5n} e^n d_t). \end{aligned}$$

*Proof.* We first recall that the Teichmüller lift  $\hat{\tau} \in \mathcal{S}(\mathbf{Z}_q)$  can be computed to  $p$ -adic precision  $N_\Phi + \delta \in \tilde{O}(ad^n)$  in time  $\tilde{O}(a^2 d^n \log^2(p))$ . Next, we observe that the scalar-matrix product  $s\Phi \bmod t^K$  over  $\mathbf{Q}_q[t]$  requires time

$$\tilde{O}(b^2 K a' (ad^n) \log(p)) \subset \tilde{O}(a^2 a' p d^{5n} e^n d_t).$$

Finally, we consider the substitution of  $\hat{\tau}$  into the  $b^2$  entries of the matrix  $s\Phi \bmod t^K$ . Each of these can be thought of as a modular composition of polynomials over  $\mathbf{Q}_q$ , where the modulus  $m(t)$  is an irreducible polynomial defining the extension  $\mathbf{Q}_q/\mathbf{Q}_q$  as a quotient of  $\mathbf{Q}_q[t]$ , which is of degree  $a/a'$ . However, care has to be taken to include the additional reduction modulo  $m(t)$  of the polynomials of degree less than  $K$ , so that polynomials involved in the modular composition have degree less than  $a/a'$ .

Thus, the substitutions require time

$$\tilde{O}\left(b^2 (K(a' \log(p))(ad^n) + (a/a')(a' \log(p))(ad^n))\right) \subset \tilde{O}(a^2 a' p d^{5n} e^n d_t).$$

Clearly, evaluating and inverting  $s(\hat{\tau})$  and performing the scalar multiplication can be ignored, and the result on the time complexity now follows.

The space requirement is dominated by the matrix  $s\Phi \bmod t^K$ , which has size

$$\tilde{O}(b^2 K(a' \log(p))(ad^n)) \subset \tilde{O}(a^2 a' p d^{5n} e^n d_t). \quad \square$$

Finally, we consider the computation of the polynomial  $\chi(T)$ .

**Proposition 7.9.** The computation of  $\chi(T)$  from  $\Phi_\tau$  requires

$$\begin{aligned} \text{time: } & \tilde{O}(a^2 \log^2(p) d^{n(\omega+1)}), \\ \text{space: } & \tilde{O}(a^2 \log(p) d^{3n}). \end{aligned}$$

*Proof.* In order to compute  $\Phi_\tau^{(a)}$  using fast exponentiation for semilinear maps as in [25, Lemma 32], we first need to apply powers of  $\sigma$  to  $O(b^2 \log(a))$  elements of  $\mathbf{Q}_q$  and then multiply  $O(\log(a))$  matrices of size  $b \in O(d^n)$ . This can be done in time

$$\tilde{O}\left(b^2 \log(a)(a \log^2(p) + (a \log(p))(ad^n)) + \log(a)b^\omega (a \log(p))(ad^n)\right) \subset \tilde{O}(a^2 \log^2(p) d^{n(\omega+1)}).$$

Next, we compute the reverse characteristic polynomial of matrix  $\Phi_\tau^{(a)} \in M_{b \times b}(\mathbf{Q}_q)$ , which can be accomplished in  $O(b^\omega \log(b))$  field operations. This amounts to a time complexity of

$$\tilde{O}(b^\omega (a \log(p))(ad^n)) \subset \tilde{O}(a^2 \log(p) d^{n(\omega+1)}).$$

Rounding this polynomial to  $\mathbf{Z}[T]$  can be ignored.

We need to store  $O(\log(a))$  matrices of size  $b$  with entries in  $\mathbf{Q}_q$ . This requires space  $\tilde{O}(b^2 (a \log(p))(ad^n)) \subset \tilde{O}(a^2 \log(p) d^{3n})$ .  $\square$

We can now state the total time and space requirements of Algorithm 6.1. Recall that  $P \in \mathbf{Z}_q[t][x_0, \dots, x_n]$  denotes a homogeneous polynomial of degree  $d$  satisfying Assumption 4.11 and that  $\tau \in S(\mathbf{F}_q)$ , where  $\mathbf{F}_q/\mathbf{F}_p$  denotes a finite field extension of characteristic  $p$ . Moreover, we write  $a = \log_p(q)$ ,  $a' = \log_p(q)$  and let  $d_t$  be the degree of  $P$  in the variable  $t$ . Finally, we let  $e$  denote the base of the natural logarithm and  $\omega$  an exponent for matrix multiplication.

**Theorem 7.10.** The computation of  $Z(X_\tau, T)$  using Algorithm 6.1 requires

$$\begin{aligned} \text{time: } & \tilde{O}\left(a^3 p d^{4n} + a^2 a' p d^{n(\omega+4)} e^{2n} d_t^2 + a a' (d^{n(\omega+2)} e^{n(\omega+1)} + d^{5n} e^{3n}) d_t\right), \\ \text{space: } & \tilde{O}(a^2 a' p d^{5n} e^n d_t + a a' d^{4n} e^{3n} d_t). \end{aligned}$$

Alternatively, computing the matrix  $\Phi_0$  as in the proof of Proposition 7.6, the computation of  $Z(X_\tau, T)$  requires

$$\begin{aligned} \text{time: } & \tilde{O}\left(a^2 p^2 d^{2n} + a^2 a' p d^{n(\omega+4)} e^{2n} d_t^2 + a a' (d^{n(\omega+2)} e^{n(\omega+1)} + d^{5n} e^{3n}) d_t\right), \\ \text{space: } & \tilde{O}(a^2 p^2 d^{2n} + a^2 a' p d^{5n} e^n d_t + a a' d^{4n} e^{3n} d_t). \end{aligned}$$

*Proof.* This follows by adding all complexities from the previous propositions and leaving out terms that are dominated by other terms or powers of logarithms of other terms.  $\square$

**Remark 7.11.** In [21], Lauder took  $d_t = 1$  and showed that his algorithm requires

$$\begin{aligned} \text{time: } & \tilde{O}(a^3 p^2 (d^{n(\omega+5)} e^{3n} + d^{6n} e^{5n})), \\ \text{space: } & \tilde{O}(a^3 p^2 d^{6n} e^{4n}). \end{aligned}$$

His main goal was to show that these complexities are  $(pad^n)^{O(1)}$ , which was not the case for previously known algorithms such as [1, 25]. Our Theorem 7.10 improves Lauder's complexity bounds by lowering the constants implicit in the exponent  $O(1)$ . To our knowledge, the complexity bounds presented in Theorem 7.10 are therefore the best ones known. Note that since a natural measure for the input size is  $\log(p)ad^n$ , these bounds are only polynomial in the input size provided  $p$  is fixed, which is something that all  $p$ -adic point counting algorithms tend to have in common.

## 8 Examples

In this section we apply Algorithm 6.1 to some examples using our implementation<sup>1</sup>. This implementation is restricted to the case  $q = p$ , i.e. to families of hypersurfaces defined over a prime field. In order to provide some context for the runtimes presented below, note that all computations were carried out on a machine with two Intel Core i7-3540M processors running at 3GHz and with 8GB of RAM, but only used a single processor. Moreover, timings were obtained using the C function `clock()` and are stated in minutes (m) or seconds (s).

### 8.1 Quintic curve

We consider the family of genus six curves over  $\mathbf{Z}$  given by the polynomial

$$P = x_0^5 + x_1^5 + x_2^5 + tx_0x_1x_2^3,$$

which Gerkmann [10, §7.4] considers as an element of  $\mathbf{Z}_p[t][x_0, x_1, x_2]$  for  $p = 2, 3, 7$ . Note that these are, in fact, three examples. The connection matrix  $M \in M_{12 \times 12}(\mathbf{Q}(t))$  only has to be computed once, and turns out to have denominator  $r = 27t^5 + 3125$ . The set of exponents at each of the zeros of  $r$  is  $\{-1, 0\}$ , and after changing basis by

$$W = \text{diag}(t^{-1}, t, t^{-2}, t^{-1}, 1, 1, 1, 1, 1, t^2, t^2, 1)$$

as in Remark 6.3, the set of exponents at  $\infty$  is  $\{-2/3, 2/3, 1, 4/3, 7/3, 8/3, 13/3, 14/3\}$ . Note that by Remark 6.15, we only need to determine the bottom half of the coefficients of the polynomial  $\chi(T)$  directly.

#### 8.1.1 Precisions

*Prime  $p = 2$ .* We take  $\log_p(\mathfrak{q}) = 50$  and let  $\tau \in \mathbf{F}_q$  be a zero of the Conway polynomial of  $\mathbf{F}_q/\mathbf{F}_p$ , i.e. the standard irreducible polynomial used to represent this extension. We first compute  $\delta = 0$  and  $N_{\Phi} = N'_{\Phi} = 153$ . As the roots of  $r$  are 2-adic integers and distinct modulo 2, we can apply Theorem 6.1 everywhere. We find  $\theta_z = 320$  at all zeros  $z$  of  $r$  and  $\theta_{\infty} = 12$ , so that we can take  $s = r^{320}$  and  $K = 1613$ . We now compute the remaining  $p$ -adic precisions  $N_{\Phi_0} = 174$ ,  $N_C = 163$ ,  $N_{C^{-1}} = 164$ ,  $N_M = 187$ ,  $N'_C = 184$ ,  $N'_{C^{-1}} = 183$ ,  $N'_{\Phi_0} = 176$ , and  $N'_M = 188$ .

*Prime  $p = 3$ .* We take  $\log_p(\mathfrak{q}) = 40$  and let  $\tau \in \mathbf{F}_q$  be a zero of the Conway polynomial of  $\mathbf{F}_q/\mathbf{F}_p$ . We first compute  $\delta = 0$  and  $N_{\Phi} = N'_{\Phi} = 122$ . As the roots of  $r$  are all contained in the residue disk at  $\infty$ , we cannot apply Theorem 6.1 and have to apply Theorem 6.4 instead. At each of the zeros  $z$  of  $r$  we find  $\mu_z = 0$ ,  $\nu_z = -1$ ,  $\theta_z = 397$  and at  $\infty$  we find  $\mu_{\infty} = -3$ ,  $\nu_{\infty} = -2$ ,  $\theta_{\infty} = 793$ , so that we can take  $s = r^{397}$  and  $K = 2779$ . We now compute the remaining  $p$ -adic precisions  $N_{\Phi_0} = 137$ ,  $N_C = 129$ ,  $N_{C^{-1}} = 130$ ,  $N_M = 147$ ,  $N'_C = 146$ ,  $N'_{C^{-1}} = 143$ ,  $N'_{\Phi_0} = 139$ , and  $N'_M = 147$ .

*Prime  $p = 7$ .* We take  $\log_p(\mathfrak{q}) = 10$ , and let  $\tau \in \mathbf{F}_q$  be a zero of the Conway polynomial of  $\mathbf{F}_q/\mathbf{F}_p$ . We first compute  $\delta = 0$  and  $N_{\Phi} = N'_{\Phi} = 31$ . As the zeros of  $r$  are 7-adic integers and distinct modulo 7, we can apply Theorem 6.1 everywhere. We find  $\theta_z = 224$  at all zeros  $z$  of  $r$  and  $\theta_{\infty} = 25$ , so that we can take  $s = r^{224}$  and  $K = 1146$ . We now compute the remaining  $p$ -adic precisions  $N_{\Phi_0} = 38$ ,  $N_C = 34$ ,  $N_{C^{-1}} = 37$ ,  $N_M = 44$ ,  $N'_C = 43$ ,  $N'_{C^{-1}} = 40$ ,  $N'_{\Phi_0} = 40$ , and  $N'_M = 44$ .

---

<sup>1</sup>This implementation is available at <https://github.com/SPancratz/deformation>.

### 8.1.2 Timings

We now compare the performance of our FLINT implementation with the timings reported by Gerkmann. To save space, we do not include the polynomials  $\chi(T)$  that we obtained from these computations.

Computation	$p = 2$		$p = 3$		$p = 7$	
	P-T	G	P-T	G	P-T	G
$M$	0.00s		0.00s		0.00s	
$\Phi_0$	0.03s	2.65m	0.03s	5.86m	0.01s	1.31m
$\Phi$	0.67s	1.33m	1.28s	1.38m	0.29s	0.89m
$Z(X_\tau, T)$	9.20s	3.96m	6.42s	101.40s	0.15s	1.09m
Total	9.90s	7.94m	7.73s	8.93m	0.45s	3.29m

Our timings in these examples are a factor of 50 – 500 lower than the ones provided by Gerkmann.

## 8.2 Quartic surface

We consider the family of quartic K3 surfaces over  $\mathbf{Z}_3$  given by

$$P = x_0^4 + x_1^4 + x_2^4 + x_3^4 + tx_0x_1x_2x_3,$$

which Gerkmann considers in [10, §7.5]. The connection matrix  $M \in M_{21 \times 21}(\mathbf{Q}(t))$  turns out to have denominator  $r = t^4 - 256$ . The set of exponents at each of the zeros of  $r$  is  $\{-3/2, -1/2, 0\}$ , and after changing basis by

$$W = \text{diag}(t^{-2}, 1, 1, 1, 1, 1, 1, 1, 1, 1, t^{-1}, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1)$$

as in Remark 6.3, the set of exponents at  $\infty$  is  $\{1, 2, 3\}$ .

### 8.2.1 Precisions

We take  $a = \log_3(\mathfrak{q}) = 20$ , let  $\alpha \in \mathbf{F}_q$  be a zero of the Conway polynomial of  $\mathbf{F}_q/\mathbf{F}_3$ , and take  $\tau = \alpha^{2345}$ . We first compute  $\delta = 0$  and  $N_\Phi = N'_\Phi = 43$ . Since the zeros of  $r$  are 3-adic integers and different modulo 3, we can apply Theorem 6.1 everywhere. We find  $\theta_z = 148$  at all zeros of  $r$  and  $\theta_\infty = 6$ , so that we can take  $s = r^{148}$  and  $K = 599$ . We now compute the remaining  $p$ -adic precisions  $N_{\Phi_0} = 65$ ,  $N_C = 53$ ,  $N_{C^{-1}} = 55$ ,  $N_M = 74$ ,  $N'_C = 73$ ,  $N'_{C^{-1}} = 68$ ,  $N'_{\Phi_0} = 68$  and  $N'_M = 75$ .

### 8.2.2 Timings

Computation	P-T	G
$M$	0.00s	7.00s
$\Phi_0$	0.01s	45.26m
$\Phi$	0.22s	19.90m
$Z(X_\tau, T)$	0.76s	18.66m
Total	0.99s	83.82m

As the final result of the computation we find that  $\mathfrak{q}\chi(T/\mathfrak{q})$  is equal to

$$\begin{aligned} & -3486784401T^{21} - 39675197243T^{20} - 191506614866T^{19} - 482588946510T^{18} \\ & - 552821487569T^{17} + 243001138765T^{16} + 1641410078472T^{15} + 1793016627512T^{14} \end{aligned}$$

$$\begin{aligned}
& -410199003010T^{13} - 2617001208822T^{12} - 1586643774924T^{11} + 1586643774924T^{10} \\
& + 2617001208822T^9 + 410199003010T^8 - 1793016627512T^7 - 1641410078472T^6 \\
& - 243001138765T^5 + 552821487569T^4 + 482588946510T^3 + 191506614866T^2 \\
& + 39675197243T + 3486784401.
\end{aligned}$$

Our timings in this example are about 5,000 times lower than the ones presented by Gerkmann.

Additionally, we should mention that Gerkmann does not include timings for part of his computations. For example, he omits the time that is required for the computation of the  $p$ -adic precision parameter that he calls  $\delta$ , which involves solving  $b^2$  differential equations similar to the one for the matrix  $C$ . Moreover, it appears that there are minor errors in the precision analysis, e.g. the final  $p$ -adic precision is not sufficient to recover the exact zeta function. Finally, the polynomial  $\chi(T)$  provided by Gerkmann for this example does not satisfy Theorem 2.1, so cannot be correct.

The remaining examples could not have been computed with previous implementations of the deformation method and, to our knowledge, neither with any other point counting method. For example, Lauder noted that he could not compute the connection matrix for a family of quintic curves or quartic surfaces given by a polynomial with more than a *few* nonzero terms. Indeed, this was the main motivation for the work in the PhD thesis of the first author and the present paper. We are now able to compute the zeta function of e.g. quintic curves and quartic surfaces over small finite fields given by a polynomial with *all* of its coefficients nonzero.

### 8.3 Generic quintic curve

We consider the family of generic quintic curves over  $\mathbf{Z}_{11}$  given by

$$\begin{aligned}
P = & x_0^5 + x_1^5 + x_2^5 + t(3x_0^4x_1 - x_0^4x_2 + 2x_0x_1^4 + x_1^4x_2 + 4x_0x_2^4 + 5x_1x_2^4 + x_0^3x_1^2 \\
& + x_0^3x_2^2 + x_0^2x_1^3 + x_1^3x_2^2 + x_0^2x_2^3 + x_1^2x_2^3 + x_0^3x_1x_2 + x_0x_1^3x_2 \\
& + x_0x_1x_2^3 + x_0^2x_1^2x_3 + x_0^2x_1x_2^2 + x_0x_1^2x_2^2).
\end{aligned}$$

The connection matrix  $M \in M_{12 \times 12}(\mathbf{Q}(t))$  has denominator  $r = r_1r_2$ , with polynomials  $r_1, r_2 \in \mathbf{Z}[t]$  that are irreducible of degree 30 and 48, respectively. The set of exponents is  $\{0, 1\}$  at the zeros of  $r_1$  and  $\{-1, 0\}$  at the zeros of  $r_2$ . Moreover, the matrix  $M$  has a simple pole at  $\infty$  and the set of exponents is  $\{1, 2\}$  there.

#### 8.3.1 Precisions

We take  $a = \log_{11}(\mathfrak{q}) = 10$  and let  $\tau$  be a zero of the Conway polynomial of  $\mathbf{F}_q/\mathbf{F}_{11}$ . We first compute  $\delta = 0$  and  $N_{\mathfrak{p}} = N'_{\mathfrak{p}} = 31$ . Since the zeros of  $r$  are 11-adic integers and different modulo 11, we can apply Theorem 6.1 everywhere. We find  $\theta_z = 352$  at the zeros of  $r_2$  and  $\theta_{\infty} = 9$  at  $\infty$ . At the residue disk of a zero  $z$  of  $r_1$ , noting that  $R$  has no other zeros there, we get a better bound by applying Theorem 6.4 with  $\mu_z = -1$ ,  $\nu_z = 0$  and find  $\theta_z = 1$ , so that we can take  $s = r_1r_2^{352}$  and  $K = 16936$ . We now compute the remaining  $p$ -adic precisions  $N_{\mathfrak{p}_0} = 40$ ,  $N_C = 35$ ,  $N_{C^{-1}} = 36$ ,  $N_M = 47$ ,  $N'_C = 46$ ,  $N'_{C^{-1}} = 43$ ,  $N'_{\mathfrak{p}_0} = 42$  and  $N'_M = 47$ .

### 8.3.2 Timings

Computation	P-T
$M$	4.43s
$\Phi_0$	0.04s
$\Phi$	3.76m
$Z(X_\tau, T)$	9.48s
Total	3.99m

As the final result of the computation we find that  $\chi(T)$  is equal to

$$\begin{aligned}
& 304481639541418099574449295360278774639038415066698088621947601T^{12} \\
& + 3777543732986291528931322507772938448980494046897871937792T^{11} \\
& + 23639674223084796290417361507756397439403378558130350T^{10} \\
& + 54141350391870148138663709375646947695242620108T^9 \\
& - 363231942297281636316475334779570949613459T^8 \\
& - 4138991673785569248268236480720472276T^7 \\
& - 28015243113507339254470240817992T^6 - 159576046483273177468242676T^5 \\
& - 539921137173243550659T^4 + 3102762464729708T^3 \\
& + 52231690350T^2 + 321792T + 1.
\end{aligned}$$

### 8.4 Generic quartic surface

We consider the family of generic quartic K3 surfaces over  $\mathbf{Z}_7$  given by

$$\begin{aligned}
P = x_0^4 + x_1^4 + x_2^4 + x_3^4 + t( & -3x_0^3x_1 + 2x_0^3x_2 - 2x_0x_1x_2x_3 + x_0^3x_3 - x_0x_1^3 - 3x_1^3x_2 \\
& + x_2^3x_3 + 2x_1^3x_3 + x_0x_2^3 - 2x_1x_2^3 - x_0x_3^3 + x_1x_3^3 \\
& + 3x_2x_3^3 + x_0^2x_1^2 + 3x_0^2x_2^2 + x_0^2x_3^2 + 2x_1^2x_2^2 - 2x_1^2x_3^2 \\
& + x_2^2x_3^2 + 2x_0^2x_1x_2 + x_0^2x_1x_3 + 3x_0^2x_2x_3 - x_0x_1^2x_2 \\
& + 2x_0x_1^2x_3 + 3x_1^2x_2x_3 - x_0x_1x_2^2 + 3x_0x_2^2x_3 + x_1x_2^2x_3 \\
& + 2x_0x_1x_3^2 + 2x_0x_2x_3^2 + 2x_1x_2x_3^2).
\end{aligned}$$

The connection matrix  $M \in M_{21 \times 21}(\mathbf{Q}(t))$  has denominator  $r = r_1r_2r_3$ , with polynomials  $r_1, r_2, r_3 \in \mathbf{Z}[t]$  that are irreducible of degree 16, 104 and 108, respectively. The matrix  $M$  has a simple pole at  $\infty$  and the set of exponents is  $\{1, 2, 3\}$  there.

#### 8.4.1 Precisions

We take  $\tau$  to be  $1 \in \mathbf{F}_7$ . We first compute  $\delta = 0$  and  $N_\Phi = N'_\Phi = 4$ . Since we do not know the exponents of  $M$  at its finite poles, we cannot use Theorem 6.1 at poles outside the residue disk at infinity. Applying Theorem 6.4 at all the zeros  $z$  of  $R$ , using the bound  $\text{ord}_z(\Delta_k^{-1}) \geq -\text{ord}_z(\det(\Delta_k))$ , we find that we can take  $s = \det(\Delta_2)\det(\Delta_3)\det(\Delta_4)^{67}$ , which has degree 25027. However, most of the zeros of  $R$  do not lie in the residue disk of a pole of  $M$  and hence the corresponding factors can be removed from  $s$ , which decreases the degree of  $s$  to 8833. We can apply Theorem 6.1 at  $\infty$  to find  $\theta_\infty = -4$ , so that we can take  $K = 8830$ . We now compute the remaining  $p$ -adic precisions  $N_{\Phi_0} = 22$ ,  $N_C = 12$ ,  $N_{C^{-1}} = 14$ ,  $N_M = 30$ ,  $N'_C = 29$ ,  $N'_{C^{-1}} = 24$ ,  $N'_{\Phi_0} = 25$ , and  $N'_M = 30$ .

### 8.4.2 Timings

Computation	P-T
$M$	3.55m
$\Phi_0$	0.02s
$\Phi$	17.53m
$Z(X_\tau, T)$	6.7s
Total	21.19m

As the final result of the computation we find that  $7\chi(T/7)$  is equal to

$$7T^{21} - 5T^{20} + 6T^{19} - 6T^{18} + 4T^{17} - 11T^{16} + 5T^{15} - 9T^{14} + 4T^{13} + 3T^{12} + 4T^{11} + 4T^{10} + 3T^9 + 4T^8 - 9T^7 + 5T^6 - 11T^5 + 4T^4 - 6T^3 + 6T^2 - 5T + 7.$$

### 8.5 Larger primes

We consider the family of quartic surfaces over  $\mathbf{Z}$  given by the polynomial

$$P = x_0^4 + 2x_1^4 + 3x_2^4 + 4x_3^4 + t(x_0x_1x_2x_3 + 2x_0^2x_2^2 + 3x_0x_3^3)$$

which we consider as an element of  $\mathbf{Z}_p[t][x_0, x_1, x_2, x_3]$  for various primes  $p$ , most of which are much larger than those in the previous examples. The connection matrix  $M \in M_{21 \times 21}(\mathbf{Q}(t))$  has denominator  $r = r_1r_2r_3r_4$ , with polynomials  $r_1, r_2, r_3, r_4 \in \mathbf{Z}[t]$  that are irreducible of degree 3, 5, 12 and 16, respectively. The set of exponents at each of the zeros of  $r$  is a subset of the set  $\{-3/2, -1/2, 0, 1\}$ , and after changing basis by

$$W = \text{diag}(t^{-1}, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, t^{-1}, 1, 1, t^{-1}, 1, t)$$

as in Remark 6.3, the set of exponents at  $\infty$  is  $\{1, 3/2, 2, 3\}$ . We take  $\tau$  to be  $1 \in \mathbf{F}_p$ .

#### 8.5.1 Precisions

For all primes  $p$  that we consider, the zeros of  $r$  are  $p$ -adic integers and different modulo  $p$ . Therefore, we can apply Theorem 6.1 everywhere. As an example, we determine the precisions in the case  $p = 2^9 + 9$ . We first compute  $\delta = 0$  and  $N_\Phi = N'_\Phi = 3$ . We find  $\theta_z = 1824$  at all zeros  $z$  of  $r$  and  $\theta_\infty = 4$ , so that we can take  $s = r^{1824}$  and  $K = 65668$ . We now compute the remaining  $p$ -adic precisions  $N_{\Phi_0} = 9$ ,  $N_C = 5$ ,  $N_{C^{-1}} = 7$ ,  $N_M = 14$ ,  $N'_C = 13$ ,  $N'_{C^{-1}} = 8$ ,  $N'_{\Phi_0} = 11$  and  $N'_M = 14$ .

#### 8.5.2 Timings

$p$	$2^2 + 1$	$2^3 + 3$	$2^4 + 1$	$2^5 + 5$	$2^6 + 3$
Computation					
$M$	0.10s	0.10s	0.10s	0.10s	0.10s
$\Phi_0$	0.01s	0.00s	0.01s	0.01s	0.00s
$\Phi$	5.89s	9.19s	9.38s	20.06s	42.18s
$Z(X_\tau, T)$	0.07s	0.14s	0.08s	0.37s	0.91s
Total	6.07s	9.43s	9.57s	20.54s	43.19s



$p$	$2^7 + 3$	$2^8 + 1$	$2^9 + 9$	$2^{10} + 7$	$2^{11} + 5$
Computation					
$M$	0.10s	0.10s	0.10s	0.10s	0.10s
$\Phi_0$	0.00s	0.00s	0.00s	0.00s	0.00s
$\Phi$	84.78s	166.68s	359.06s	748.57s	1569.01s
$Z(X_\tau, T)$	1.61s	3.62s	7.09s	14.50s	32.03s
Total	86.49s	170.40s	366.25s	763.18s	1601.15s

Our timings in this example confirm that the running time of the algorithm is (quasi)linear in  $p$  and the memory usage also turns out to be (quasi)linear in  $p$  as predicted. In the case  $p = 2^{11} + 5$ , the computation requires about 6 GB of memory. As an example, for the prime  $p = 2^{11} + 5$  we find that  $p\chi(T/p)$  is equal to

$$\begin{aligned}
& 2053T^{21} - 4885T^{20} + 6922T^{19} - 7050T^{18} + 1163T^{17} + 7077T^{16} - 12948T^{15} \\
& + 12948T^{14} - 9130T^{13} + 3722T^{12} + 128T^{11} + 128T^{10} + 3722T^9 - 9130T^8 \\
& + 12948T^7 - 12948T^6 + 7077T^5 + 1163T^4 - 7050T^3 + 6922T^2 - 4885T + 2053.
\end{aligned}$$

**Remark 8.1.** In all of our timings, we have not included the time required to compute the  $p$ -adic and  $t$ -adic precisions, since we used MAGMA for this. Note, however, that we can readily determine  $\det(\Delta_k)$  from the  $LUP$  decomposition of  $\Delta_k$  and that the factorisation of the polynomials  $r$ ,  $R$  over  $\mathbf{Q}$  and  $\mathbf{F}_p$  was instantaneous in all cases. The only step that required noticeably more time was the computation of the exponents in the generic examples. For the family of generic quintic curves, this required 10s, 47s and 1.5s at the zeros of  $r_1$ , the zeros of  $r_2$  and at  $\infty$ , respectively. For the family of generic quartic surfaces, this required 13s and 59s at the zeros of  $r_1$  and at  $\infty$ , respectively, but almost four hours for both the zeros of  $r_2$  and  $r_3$ . Note, however, that in this last case we only use the exponents at  $\infty$  in the precision analysis and that the other exponents are not needed for the result of the computation to be provably correct.

## References

- [1] T.G. Abbott, K.S. Kedlaya, and D. Roe. Bounding Picard numbers of surfaces using  $p$ -adic cohomology. In *Arithmetic, Geometry, and Coding Theory (AGCT-10)*, 2006.
- [2] P. Berthelot. Géométrie rigide et cohomologie des variétés algébriques de caractéristique  $p$ . *Mém. Soc. Math. Fr. (N.S.)*, 23, 1986.
- [3] E. Bombieri. On exponential sums in finite fields. *Invent. Math.*, 88:71–105, 1966.
- [4] R.P. Brent. The complexity of multiple-precision arithmetic. In R.S. Anderssen and R.P. Brent, editors, *The Complexity of Computational Problem Solving*, pages 126–165. University of Queensland Press, 1976.
- [5] P. Deligne. La conjecture de Weil. I. *Inst. Hautes Études Sci. Publ. Math.*, 43, 1974.
- [6] P. Deligne and N.M. Katz. *SGA 7 II, Groupes de Monodromie en Géométrie Algébrique*. Springer Verlag, 1973.
- [7] B. Dwork. On the zeta function of a hypersurface I. *Publication Mathématiques de l’IHÉS*, 12:5–68, 1962.

- [8] B. Dwork. On the zeta function of a hypersurface II. *The Annals of Mathematics, Second Series*, 80(2):227–299, 1964.
- [9] J.Y. Étéssé and B. Le Stum. Fonctions L associées aux F-isocristaux surconvergens. I. interprétation cohomologique. *Math. Ann.*, 296, 1993.
- [10] R. Gerkmann. Relative rigid cohomology and deformation of hypersurfaces. *Int. Math. Res. Pap. IMRP*, 1:67, 2007. ISSN 1687-3017.
- [11] P.A. Griffiths. On the periods of certain rational integrals. I, (resp. II). *Ann. of Math. (2)*, 90(3):460–495 (resp. 496–541), November 1969.
- [12] W. Hart, S. Pancratz, A. Novocin, F. Johansson, and D. Harvey. *FLINT: Fast Library for Number Theory – Version 2.2*, June 2011. <http://www.libflint.org>.
- [13] H. Hubrechts. Fast arithmetic in unramified  $p$ -adic fields. *Finite Fields Appl.*, 16, 2010.
- [14] N.M. Katz. On the differential equations satisfied by period matrices. *Inst. Hautes Études Sci. Publ. Math.*, 1968.
- [15] K.S. Kedlaya. Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology. *Journal of the Ramanujan Mathematical Society*, 16, 2001.
- [16] K.S. Kedlaya. *Search techniques for root-unitary polynomials*, volume 463 of *Contemp. Math.*, pages 71–81. Amer. Math. Soc., Providence, RI, 2008.
- [17] K.S. Kedlaya.  *$p$ -adic Differential Equations*. Cambridge Univ. Press, 2010.
- [18] K.S. Kedlaya. Effective  $p$ -adic cohomology for cyclic cubic threefolds, Computational Algebraic and Analytic Geometry. *Contemporary Mathematics 572*, American Mathematical Society, 2013.
- [19] K.S. Kedlaya and J. Tuitman. Effective bounds for Frobenius structures. *Rendiconti del Seminario Matematico della Università di Padova*, page 9, 2012.
- [20] W. Keller-Gehrig. Fast algorithms for the characteristic polynomial. *Theoretical computer science*, 36:309–317, 1985.
- [21] A.G.B. Lauder. Counting solutions to equations in many variables over finite fields. *Foundations of Computational Mathematics*, 4(3):221–267, 2004.
- [22] A.G.B. Lauder. Deformation theory and the computation of zeta functions. *Proc. London Math. Soc.*, 3:565–602, 2004.
- [23] A.G.B. Lauder. A recursive method for computing zeta functions of varieties. *LMS J. Comp. Math.*, 9:222–269, 2006.
- [24] A.G.B. Lauder. Degenerations and limit Frobenius structures in rigid cohomology. *LMS J. Comput. Math.*, 14:1–33, 2011.
- [25] A.G.B. Lauder and D. Wan. Counting points on varieties over finite fields of small characteristic. In *Algorithmic number theory: lattices, number fields, curves and cryptography*, volume 44 of *Math. Sci. Res. Inst. Publ.*, pages 579–612. Cambridge Univ. Press, Cambridge, 2008.
- [26] B. Mazur. Frobenius and the Hodge filtration. *Bull. Amer. Math. Soc.*, 78, 1972.

- [27] R. Schoof. Counting points on elliptic curves over finite fields, 18ièmes Journées Arithmétiques, Bordeaux 1993. *Journal de Théorie des Nombres de Bordeaux*, 7:219–254, 1995.
- [28] Virginia Vassilevska Williams. Multiplying matrices faster than Coppersmith-Winograd [extended abstract]. In *STOC'12—Proceedings of the 2012 ACM Symposium on Theory of Computing*, pages 887–898. ACM, New York, 2012.