

FROBENIUS LIFTS AND POINT COUNTING FOR SMOOTH CURVES

AMNON BESSER, FRANÇOIS-RENAUD ESCRIVA, AND ROB DE JEU

ABSTRACT. We describe an algorithm to compute the zeta-function of a proper, smooth curve over a finite field, when the curve is given together with some auxiliary data. Our method is based on computing the matrix of the action of a semi-linear Frobenius on the first cohomology group of the curve by means of Serre duality. The cup product involved can be computed locally, after first computing local expansions of a globally defined lift of Frobenius. The resulting algorithm's complexity is softly cubic in the field degree, which is also the case with Kedlaya's algorithm in the hyperelliptic case.

1. INTRODUCTION

Let p be a prime number and let k be a finite field of cardinality q and characteristic p . An important problem of algorithmic number theory is to count the number of points of a smooth (and usually proper) variety Y defined over k . By point counting we mean, more precisely, the computation of the matrix of the k -linear relative Frobenius map, acting on some étale or crystalline cohomology group of Y . It is well-known that obtaining this matrix to a sufficiently high precision allows an exact determination of its characteristic polynomial as its coefficients satisfy the Weil bounds (see Section 8).

The modern theory of point counting begins with the paper of Schoof [18] for counting points on an elliptic curve E by effectively computing the action of Frobenius on the first étale cohomology group of E . This direction of using étale cohomology is pursued by various other authors, still providing the best method when the field is prime ($p = q$) or close to being prime.

Other point counting methods, beginning with the work of Satoh [17], use crystalline cohomology. To describe these methods, let us fix some more notation.

Notation 1.1. Let K be a finite Galois extension of the field \mathbb{Q}_p of p -adic numbers, with ramification index e , valuation ring R , uniformizer π , and residue field $R/\pi R$ isomorphic to k . We normalize the valuation on K by $v(p) = 1$. We let σ be an automorphism of K , and denote by $\bar{\sigma}$ the induced map on k , which is given by $x \mapsto x^{p'}$ with p' a positive power of p .

For point counting one usually takes $e = 1$ and $p' = p$ but the theory works in this generality, and it will help us in future work concerning syntomic regulators. We note that when $e = 1$ the automorphism σ is uniquely determined by its reduction.

In counting methods based on crystalline cohomology, one computes an effective representation for the crystalline cohomology group $H_{\text{cr}}^i(Y/R) \otimes K$. This has

2010 *Mathematics Subject Classification.* Primary: 14F30, 14G10, 14G15, 14Q50; secondary 14G22.

Key words and phrases. curve over finite field, zeta function, rigid cohomology.

a σ -semi-linear endomorphism ϕ_{cr}^* . It is obtained via functoriality of crystalline cohomology from the relative Frobenius $\bar{\phi}$ on Y , i.e., the morphism of schemes

$$\bar{\phi}: Y \rightarrow Y^{(p')}, \text{ where } Y^{(p')} = Y \times_{k, \bar{\sigma}} k,$$

obtained by raising to the p' th power on the structure sheaf. The sought after linear Frobenius is then obtained as a (twisted) power of this.

When Y can be lifted to characteristic 0, and $e < p - 1$, in particular if p is odd and $e = 1$, crystalline cohomology is the de Rham cohomology of the lift, and if the Frobenius endomorphism can be lifted as well, then the endomorphism ϕ is simply the action of the lift on this de Rham cohomology. This is the case in, for example, Satoh's algorithm.

Finding lifts of Frobenius for a proper variety is rarely possible. An alternative is to only lift Frobenius on an affine open piece. As crystalline cohomology is infinite dimensional in this case, one has to use a more refined cohomology theory, the Monsky-Washnitzer cohomology [16], which is a special case of Berthelot's rigid cohomology [4]. This cohomology theory associates to the affine variety $\text{Spec}(\bar{A})$ the de Rham cohomology of $A_K^\dagger = A^\dagger \otimes_R K$, where A^\dagger is a "weakly complete" R -algebra whose reduction modulo π is \bar{A} . The action of ϕ is computed from the action of a σ -semi-linear endomorphism of A^\dagger reducing to the p -power map.

The use of Monsky-Washnitzer cohomology in point counting algorithms was pioneered in the seminal paper of Kedlaya [15] on counting points on hyperelliptic curves. Kedlaya's ideas can be extended to more general curves [11, 10, 5] (see also the overview [6]).

Kedlaya type algorithms generally consist of two main components.

- (1) An explicit lift of Frobenius to an endomorphism of A^\dagger , usually given in a straightforward manner.
- (2) A reduction algorithm that identifies a basis for $H_{\text{dr}}^i(A_K^\dagger)$ and shows how to explicitly write any i -form as a linear combination of basis elements plus an exact differential.

Extending each of these steps from hyperelliptic curves to more general curves in an efficient way proved to be a non-trivial task.

In this work we describe a point counting algorithm for curves under the following fairly general assumptions: we shall consider a proper, smooth curve $f: C \rightarrow \text{Spec}(R)$ over R with geometrically irreducible fibres. We shall denote by C_K and C_k its generic and special fibre respectively. Note that by Corollaire 7.4 of [1, Exposé III] we can lift any proper, smooth curve over k to a smooth, proper curve C over $W(k)$, necessarily with geometrically irreducible generic fibre if C_k is geometrically irreducible.

For the rest of this paper, we shall work with the following situation and notations.

- The genus of C_K and C_k is g .
- We are given a Zariski open affine $X = \text{Spec}(A)$ in C that contains the generic point of C_k , where $A = R[x_1, \dots, x_n]/(f_2, \dots, f_n)$ with given generators f_2, \dots, f_n of the defining ideal; moreover, the reduction $\bar{X} = \text{Spec}(\bar{A})$ with $\bar{A} = A \otimes_R k = k[x_1, \dots, x_n]/(\bar{f}_2, \dots, \bar{f}_n)$ is a smooth complete intersection. (See Assumption 3.5 for the terminology and Remark 3.20 for the existence of such an X .)

- We know $\omega_1, \dots, \omega_{2g}$ in $\Omega_{A/R}^1$ that give a basis for the cohomology group $H_{\text{dr}}^1(C_K/K)$.
- We let \tilde{K} be a finite field extension of K , with valuation ring \tilde{R} , such that $C_{\tilde{R}} \setminus X_{\tilde{R}}$ consists of the union of distinct sections $Q_i : \text{Spec}(\tilde{R}) \rightarrow C_{\tilde{R}}$, which we tacitly identify with their images. We denote the image of the closed point of $\text{Spec}(\tilde{R})$ under Q_i by q_i . We do not assume that the q_i are distinct.

To perform point counting on these curves, we introduce three new techniques. The first is a general explicit procedure for lifting Frobenius in smooth, complete intersections situations inspired by Section 2 of [2]. This method introduces a variable for each defining equation f_j , and uses those to find a correction to the naive approximate lift given by raising to the power p . Using this correction gives a map on $R\langle x_1, \dots, x_n \rangle^\dagger$ that maps the defining ideal to itself and reduces to the desired map on \overline{A} . We make this procedure explicit and provide estimates on the overconvergence of the resulting lift.

The second is a technique that avoids a (generally computationally expensive) reduction algorithm by replacing it with residue computations. One observes that in order to know the matrix of ϕ_{cr}^* above, it suffices to compute the cup products $\omega_i \cup \omega_j$ as well as the cup products $\phi_{\text{cr}}^* \omega_i \cup \omega_j$. Our techniques reduce the computation of cup products to a computation of residues of forms $(\int \omega_j) \phi \omega_i$ on certain annuli, called ends, which are “at the boundary” of the rigid space associated with A^\dagger .

Finally, essential for improving the performance of the algorithm, we use a local lifting technique, which will compute the expansion of the lifting of Frobenius locally near the boundary, instead of computing it globally and restricting to the boundary.

Overall, the resulting algorithm for point counting is asymptotically softly cubic in the field degree. This is the same complexity as Kedlaya’s algorithm [15], which is restricted to the case of hyperelliptic curves, and the algorithm of Castryck, Deneff and Vercauteren for non-degenerate curves [5]. The dependence on the genus is somewhat worse for general curves but reduces in specific situations. Finally, the dependence on p is essentially linear. We have not attempted an improvement in this direction in the style of [13].

A (far from optimized) implementation of the above point counting algorithm will be available within a few days.

The paper is organized as follows. In Section 2 we explain how to obtain the matrix of ϕ from cup products on rigid analytic spaces. In Section 3 we discuss how to obtain the desired lift ϕ on A^\dagger . Although we shall need it only in the case of curves, we present the result and the estimates on the coefficients involved for more general R -algebras A that reduce to smooth complete intersections over k . Section 4 makes the resulting maps and estimates more explicit where X is an affine plane curve or a localization of such a curve. It also briefly discusses how to recover Kedlaya’s approach to hyperelliptic curves from our work. Section 5 discusses how to obtain the expansions of the action of our lift at the ends, thus avoiding the computation of the global lift constructed in Section 3. Section 6 returns to some of the examples discussed in Section 4, considering them from the points of view of leaving out only one point, or obtaining a simpler lift ϕ by localizing more. Section 7 describes how to turn the estimates of the preceding theory into finite precision calculations that still enable us to recover the zeta-function of C_k , and

Section 8 describes an algorithm to do this, given suitable input, and discusses its complexity.

Finally, we would like to thank Bruno Chiarellotto, Kiran Kedlaya, Deepam Patel, and Jan Tuitman for interesting and useful discussions.

Throughout the paper, we use the following notation.

Notation 1.2. We let $R[[x_1, \dots, x_n]]$ denote the formal power series in x_1, \dots, x_n with coefficients in R , $R\langle x_1, \dots, x_n \rangle$ the subring where the coefficients tend to 0 in R , and $R\langle x_1, \dots, x_n \rangle^\dagger$ the subring of $R\langle x_1, \dots, x_n \rangle$ consisting of overconvergent power series. We shall often use multi-index notation, writing \mathbf{x} for x_1, \dots, x_n , and \mathbf{x}^I for $x_1^{i_1} \dots x_n^{i_n}$ if $I = (i_1, \dots, i_n)$. With $|I| = i_1 + \dots + i_n$ we can then define $R\langle \mathbf{x} \rangle^\dagger$ as those $\sum_I a_I \mathbf{x}^I$ in $R\langle \mathbf{x} \rangle$ for which γ and δ exist with $\gamma > 0$ and $v(a_I) \geq \gamma|I| + \delta$ for all I . Equivalently, there exists a D in $(\mathbb{Q}_{>0})^n$ and δ in \mathbb{Q} such that $v(a_I) \geq D \cdot I + \delta$ for all I , where $D \cdot I$ is the inner product.

2. COMPUTING THE MATRIX OF FROBENIUS USING CUP PRODUCTS AND RESIDUES

In this section we describe the strategy for computing the matrix of Frobenius. For ease of presentation we give a geometric description, based on Coleman's work [9, 7]. We then translate this into the more algebraic language that will be used in the rest of the paper.

To rely directly on Coleman's work, it is convenient to first change scalars to the field \mathbb{C}_p of “complex p -adic numbers”. Recall that this is the completion of the algebraic closure of \mathbb{Q}_p . Its residue field is the algebraic closure $\overline{\mathbb{F}_p}$ of the finite field with p elements.

Consider $C_{\mathbb{C}_p}$ as a rigid analytic space over \mathbb{C}_p . Let q_i be one of the $\overline{\mathbb{F}_p}$ rational points in $C_k \setminus \overline{X}$. Let $\mathcal{D}_i \subset C_{\mathbb{C}_p}$ be the rigid analytic subspace whose underlying set is the set of all points whose reduction is q_i . This is called the residue disc of q_i by Coleman.

As C is smooth, each of these \mathcal{D}_i is isomorphic to an open unit disc $\{z \in \mathbb{C}_p, |z| < 1\}$. We choose a parameter t_i on \mathcal{D}_i realizing this isomorphism. For each $0 < r < 1$ we let U_r be the rigid subspace of $C_{\mathbb{C}_p}$ obtained by removing the subsets $\{|t_i| \leq r\} \subset \mathcal{D}_i$ (cf. [9, 2.1]). These U_r are examples of “wide open spaces” in Coleman's terminology.

We wish to compute the action of Frobenius on the cohomology of $C_{\mathbb{C}_p}$. We assume we are given forms $\omega_1, \dots, \omega_{2g}$ of the second kind on $C_{\mathbb{C}_p}$, whose cohomology classes form a basis of $H_{\text{dR}}^1(C_{\mathbb{C}_p}/\mathbb{C}_p)$, such that all poles of the ω_j are contained in the union of the \mathcal{D}_i . By choosing a sufficiently large r_0 we may assume that the ω_j have no poles in $U = U_{r_0}$.

We extend σ to an automorphism of \mathbb{C}_p . We stress that this extension is not actually used and is needed only so that we can formulate things over \mathbb{C}_p . We will use a superscript σ on the objects defined above to denote the same object with structural morphism to \mathbb{C}_p twisted by σ (in the rigid analytic context this works better than twisted tensoring). The following result also contains the definition of the ends \mathcal{E}_i .

Proposition 2.1. *There exist $r < 1$, and with $U' = U_r$, a morphism $\phi : U' \rightarrow U^\sigma$ whose reduction is the p' -power map. Furthermore, the morphism ϕ has the property that $\phi(\mathcal{E}'_i) \subset \mathcal{E}_i^\sigma$ with $\mathcal{E}'_i = U' \cap \mathcal{D}_i$ and $\mathcal{E}_i^\sigma = U^\sigma \cap \mathcal{D}_i^\sigma$.*

Proof. This is essentially [9, Theorem 2.2] only in a semi-linear version. The proof is the same. \square

Recall that an annulus is a rigid analytic space isomorphic, via a parameter t , to a space of the form $\mathcal{E}_r = \{r < |z| < 1\}$. The space of rigid analytic functions on such an annulus is

$$(2.2) \quad \left\{ \begin{array}{l} \sum_{m \in \mathbb{Z}} a_m t^m \text{ with } a_m \text{ in } \mathbb{C}_p \text{ satisfying} \\ \lim_{m \rightarrow -\infty} |a_m| s^{-m} = 0 \text{ for all } s > r \text{ and} \\ \lim_{m \rightarrow \infty} |a_m| s^m = 0 \text{ for all } s < 1 \end{array} \right\}.$$

The parameter t_i restrict to isomorphisms $\mathcal{E}_i \rightarrow \mathcal{E}_{r_0}$ and $\mathcal{E}'_i \rightarrow \mathcal{E}_r$, so that both \mathcal{E}_i and \mathcal{E}'_i are annuli with parameter t_i .

Definition 2.3. Let ω be a rigid analytic form on some annulus \mathcal{E} with parameter t , and write

$$\omega = \sum_{m \in \mathbb{Z}} a_m t^m dt.$$

Then we let the *residue* of ω on \mathcal{E} with respect to the parameter t be $\text{Res}_{\mathcal{E}} \omega = a_{-1}$.

The set of all parameters on an annulus \mathcal{E} breaks into two classes, known as orientations [7, Lemma 2.1 and ensuing remarks] such that the residues with respect to any two parameters are identical if they are in the same orientation and differ by a sign otherwise. An annulus with a choice of parameter in the same orientation class is called an oriented annulus. The annuli \mathcal{E}_i are oriented by the parameters t_i and all parameters that are obtained on the \mathcal{E}_i as restrictions of parameters on \mathcal{D}_i give the same orientation [7, Cor 3.7a]. The choice of t_i is therefore irrelevant for the residue and we may denote it simply by $\text{Res}_{\mathcal{E}_i}$.

Remark 2.4. It is easy to see that for an annulus \mathcal{E} oriented by the parameter t , we have $\text{Res}_{\mathcal{E}} = \text{Res}_{\mathcal{E}'}$, where \mathcal{E}' is a subannulus defined by the condition $r' < |t| < 1$.

The analogue of the residue theorem holds [7, Proposition 4.3].

Theorem 2.5. *For a rigid analytic analytic form ω on U we have $\sum_i \text{Res}_{\mathcal{E}_i} \omega = 0$.*

We recall the following basic result [8, Corollary 5.1].

Theorem 2.6. *Let ω_1 and ω_2 be forms of the second kind on $C_{\mathbb{C}_p}$. Then the cup product of their cohomology classes can be computed as*

$$[\omega_1] \cup [\omega_2] = \sum_x \text{Res}_x \omega_2 \int \omega_1,$$

where the sum is over all points x and the integral is a local integral with arbitrary constant term.

The key points to notice are that the integral makes sense since, with respect to a local parameter z at each point, there is no term $az^{-1}dz$ to integrate, and that the constant of integration does not matter as in the residue computation it is going to multiply the residue of ω_2 , which is 0. If one of the forms is df for a rational function f , then the residue theorem easily shows that the right-hand side is indeed 0.

Definition 2.7. A rigid analytic form ω on U will be called of the second kind if we have $\text{Res}_{\mathcal{E}_i} \omega = 0$ for every annulus \mathcal{E}_i . If η is another such form, the cup product pairing of ω and η is defined by

$$\langle \omega, \eta \rangle = \langle \omega, \eta \rangle_U = \sum_i \text{Res}_{\mathcal{E}_i} \eta \int \omega.$$

Just like in the algebraic setting of Theorem 2.6, it is clear from the residue theorem, Theorem 2.5, that the pairing is well-defined and factors via $H_{\text{dr}}^1(U)$. It is further clear from Remark 2.4 that if U' is a smaller wide open space as above then

$$\langle \omega|_{U'}, \eta|_{U'} \rangle_{U'} = \langle \omega, \eta \rangle_U.$$

The usefulness of the pairing above for the computation of Frobenius rests on the following result.

Proposition 2.8 ([7, Proposition 4.5]). *Let $\alpha_1, \alpha_2 \in H_{\text{dr}}^1(C_{\mathbb{C}_p}/\mathbb{C}_p)$ and let ω_1 and ω_2 be forms of the second kind on U such that the class of ω_i in $H_{\text{dr}}^1(U/\mathbb{C}_p)$ is the restriction to U of α_i . Then $\alpha_1 \cup \alpha_2 = \langle \omega_1, \omega_2 \rangle_U$.*

The automorphism σ acts on differential forms and cohomology classes by sending them to the “same” forms and classes on the twisted objects. Note that as a vector space map, it is σ -semi-linear, so that as expected, for example, it acts on differential forms on an annulus \mathcal{E} with parameter t by

$$\left(\sum_m a_m t^m dt \right)^\sigma = \sum_m a_m^\sigma t^m dt.$$

The cohomology group $H_{\text{dr}}^1(C_{\mathbb{C}_p}/\mathbb{C}_p)$ has a σ -semi-linear endomorphism. Indeed, it is isomorphic to $H_{\text{cr}}^1(C/R) \otimes_R \mathbb{C}_p$ and the endomorphism is obtained by extending ϕ_{cr}^* on $H_{\text{cr}}^1(C/R)$ σ -semi-linearly. We continue to denote this by ϕ_{cr}^* . To explicitly compute ϕ_{cr}^* , we note that, under restriction to $H_{\text{dr}}^1(U)$, it is compatible with the map

$$H_{\text{dr}}^1(U) \xrightarrow{\sigma} H_{\text{dr}}^1(U^\sigma) \xrightarrow{\phi^*} H_{\text{dr}}^1(U') \rightarrow H_{\text{dr}}^1(U),$$

where the last map is the inverse of the restriction map, which is an isomorphism by [7, Theorem 4.2]. This, and the compatibility of the pairing with restrictions, immediately give the following.

Corollary 2.9. *Under the assumptions of Proposition 2.8 we have*

$$\alpha_1 \cup (\phi_{\text{cr}}^*(\alpha_2)) = \langle \omega_1, \phi^*(\omega_2^\sigma) \rangle_{U'}.$$

We can now describe our approach to computing the matrix of ϕ_{cr}^* .

Method 2.10. Assuming that one knows how to effectively compute the pairing $\langle \cdot, \cdot \rangle_U$, the above gives the following simple algorithm for computing the matrix M of ϕ^* with respect to the basis induced by the $\{\omega_1, \dots, \omega_{2g}\}$.

- (1) Compute the cup product matrix M_1 with entries $\omega_i \cup \omega_j$ by using Theorem 2.6.
- (2) Compute the cup product matrix $M_2 = M_1 M$ with entries $\langle \omega_i, \phi^* \omega_j^\sigma \rangle_{U'}$.
- (3) Deduce the matrix M of ϕ_{cr}^* as $M_1^{-1} M_2$.

From this we can deduce the desired the zeta function.

Method 2.11. Using Method 2.10, compute the zeta function of C_k as follows.

- (1) Compute the matrix M of ϕ_{cr}^* with a sufficiently high precision (see Section 8).
- (2) Compute the matrix of the linear Frobenius as

$$M' = \sigma^{l-1}(M) \times \sigma^{l-2}(M) \times \cdots \times \sigma(M) \times M$$

with $q = p^l$.

- (3) Let $P_1(T) = \det(1 - TM')$. Its coefficients are a priori in \mathbb{Z}_p , but in fact are integers satisfying certain bounds deduced from the Weil bounds on the roots of P_1 . Given a sufficiently high precision, $P_1(T)$ can therefore be determined precisely.
- (4) Deduce the zeta fuction as $Z(T) = \frac{P_1(T)}{(1-T)(1-qT)}$.

It remains to make concrete the computation of $\langle \omega, \phi^* \eta^\sigma \rangle_{U'}$ for any two forms of the second kind on U . By our assumptions the parameters t_i at the annuli can be chosen to be \tilde{K} -rational. The endomorphism ϕ is induced by an endomorphism of dagger algebras [9, 2.2]. The restriction of ϕ to \mathcal{E}'_i is determined by the Laurent series expansion of $\phi^* t_i$, say $f_i(t_i)$, with coefficients in \tilde{K} . We then have

$$(2.12) \quad \langle \omega, \phi^* \eta^\sigma \rangle_{U'} = \sum_i \text{Res}_{\mathcal{E}'_i} \phi^* \eta^\sigma \int \omega,$$

and given $f_i(t_i)$, each residue term is computed in terms of Laurent series expansions $\omega = \sum_m a_m t_i^m dt_i$ and $\eta = \sum_m b_m t_i^m dt_i$. It is the coefficient of t_i^{-1} in

$$\left(\sum_m b_m (f_i(t_i))^m \right) \left(\sum'_m \frac{a_m}{m+1} t_i^{m+1} \right),$$

where the prime denotes that we leave out the term with $m = -1$ in the sum (as $a_{-1} = 0$). We shall describe more efficient methods for carrying out this computation in later sections, but at this point it is clear that it can be done in \tilde{K} .

Remark 2.13. Let us sketch the dictionary between this section and the rest of this work, which is algebraic rather than geometric. Rather than having a map of rigid spaces $\phi : U' \rightarrow U^\sigma$ we simply have a σ -semi-linear endomorphism of the algebra A^\dagger . We denote this by the same letter ϕ . This has the effect that the action on functions and differential forms, which in this section is obtained by first applying σ to the coefficients and then applying ϕ^* , becomes in later sections simply the application of ϕ to the same objects.

3. THE GLOBAL FROBENIUS

Let R, π, k, σ be as in Notation 1.1. In this section we explain our strategy for computing a lift of Frobenius on our dagger algebras over R , inspired by the work of Arabia [2]. Even though we ultimately use this only for curves, given the current limitation of our cup product method for computing cohomology, the method applies, and we describe it here, in greater generality for any A as in Assumption 3.5. By and large, this method was already developed in the master thesis of F.-R. Escriva. Later we discovered that another approach, but with a less transparent presentation, is contained in the unpublished PhD thesis of R. Gerkmann [11].

Our goal in this section is to lift the p' -power endomorphism $\bar{\phi}$ of \bar{A} to a σ -linear endomorphism ϕ of $A^\dagger = R\langle x_1, \dots, x_n \rangle^\dagger / (f_{r+1}, \dots, f_n)$, and obtain estimates on the coefficients of the $\phi(x_i)$. (See Remark 2.13 for the relation with the notation in

Section 2.) We begin though, by explaining it in the simplest possible case of one equation in two variables over \mathbb{Z}_p and ignoring the issue of overconvergence.

Suppose then that we have $f(x, y)$ in $\mathbb{Z}_p[x, y]$ such that the reduction $\overline{f}(x, y)$ defines a non-singular curve in \mathbb{A}^2 . Our goal is to lift the Frobenius morphism $(x, y) \mapsto (x^p, y^p)$ to a morphism ϕ of the affine curve defined by f , viewed as a rigid analytic variety.

Let f_x and f_y denote the partial derivatives of f with respect to the two variables. The non-singularity of \overline{f} means that one can find polynomials \overline{P}_1 , \overline{P}_2 and $\overline{\Delta}$ in $\mathbb{F}_p[x, y]$ such that

$$\overline{P}_1 \overline{f}_x + \overline{P}_2 \overline{f}_y = 1 + \overline{\Delta} \overline{f}.$$

We arbitrarily lift \overline{P}_1 , \overline{P}_2 and $\overline{\Delta}$ to polynomials P_1 , P_2 and Δ in $\mathbb{Z}_p[x, y]$, so that the congruence

$$(3.1) \quad f_x P_1 + f_y P_2 \equiv 1 + \Delta f$$

holds modulo p . We now seek our lift of Frobenius of the form

$$\phi(x, y) = (x^p, y^p) + s \times (P_1(x^p, y^p), P_2(x^p, y^p))$$

where s in $p\mathbb{Z}_p\langle x, y \rangle$ is chosen to solve the equation in the variable S ,

$$(3.2) \quad f((x^p, y^p) + S \times (P_1(x^p, y^p), P_2(x^p, y^p))) - f(x, y)^p - f(x, y)^p \Delta(x^p, y^p) S = 0.$$

Clearly, if s satisfies the above equation then $f(\phi(x, y))$ is divisible by f (even f^p), so that it indeed maps the curve defined by f to itself. Furthermore, since by assumption the coefficients of s are divisible by p , we see that $\phi(x, y) \equiv (x^p, y^p)$ modulo p , so it is indeed a lift of Frobenius.

The equation (3.2) is an equation in one variable S over $\mathbb{Z}_p\langle x, y \rangle$, and 0 is a solution modulo p . Its derivative with respect to S at $S = 0$ is

$$f_x(x^p, y^p) P_1(x^p, y^p) + f_y(x^p, y^p) P_2(x^p, y^p) - f(x^p, y^p) \Delta(x^p, y^p),$$

which, in light of (3.1), reduces to 1 modulo p . The existence and uniqueness of the solution in $p\mathbb{Z}_p\langle x, y \rangle$ is thus guaranteed by Hensel's lemma, and it can be recovered efficiently using Newton iterations starting from the approximate solution 0.

We shall consider the following very simple (and for point counting obviously uninteresting) example at various points in this paper in order to illustrate our estimates.

Example 3.3. Consider $f(x, y) = x^2 - y^2 - 1$ in $\mathbb{Z}_p[x, y]$ with $p \neq 2$. Then $\overline{2}^{-1} x \overline{f}_x + \overline{2}^{-1} y \overline{f}_y = \overline{1} + \overline{1} \cdot \overline{f}$ in $\mathbb{F}_p[x, y]$. Now we write down

$$(3.4) \quad \begin{aligned} G(S) &= f(x^p + 2^{-1} x^p S, y^p + 2^{-1} y^p S) - f(x, y)^p - f(x, y)^p S \\ &= 4^{-1} (x^{2p} - y^{2p}) S^2 + (x^{2p} - y^{2p} - f(x, y)^p) S - f(x^p, y^p) - f(x, y)^p \end{aligned}$$

in $\mathbb{Z}_p[x, y][S]$. We solve this for the unique solution $S = s$ in $p\mathbb{Z}_p\langle x, y \rangle$. Then $\phi(x, y) = (x^p + 2^{-1} x^p s, y^p + 2^{-1} y^p s)$ induces an endomorphism of $\mathbb{Z}_p\langle x, y \rangle$ that descends to an endomorphism of $\mathbb{Z}_p\langle x, y \rangle / (f(x, y))$ because it maps the ideal $(f(x, y))$ to itself by construction, and it reduces to the Frobenius map $\overline{\phi}(x, y) = (x^p, y^p)$ modulo p .

We now describe the general case, still ignoring overconvergence.

Recall the shorthand $R[\mathbf{x}]$ of Notation 1.2. We shall also write $\mathbb{M}^{a,b}$ and \mathbb{M}^a for $a \times b$ and $a \times a$ matrices, and if f_{r+1}, \dots, f_n in $R[\mathbf{x}]$ are given, then we let

Jac_f in $\mathbb{M}^{n-r,n}(R[\mathbf{x}])$ be the resulting Jacobian matrix. We shall lift the p' -power endomorphism $\overline{\phi}$ of \overline{A} to a σ -linear endomorphism ϕ of $R\langle\mathbf{x}\rangle/(f_{r+1}, \dots, f_n)$ for the following A . In particular, by Remark 3.20 below, this will apply to a suitable Zariski open part X of C/R .

Assumption 3.5. In $R[\mathbf{x}]$, for $0 \leq r \leq n-1$, we are given f_{r+1}, \dots, f_n , such that

$$(3.6) \quad A = R[\mathbf{x}]/(f_{r+1}, \dots, f_n).$$

If $\overline{\text{Jac}_f}$ is the reduction modulo π of Jac_f , then the unit ideal in \overline{A} is generated by the determinants of the $(n-r) \times (n-r)$ minors of $\overline{\text{Jac}_f}$.

Under this assumption, Arabia shows in the proof of [2, Théorème 2.1.2] that there exist matrices

$$(3.7) \quad P \in \mathbb{M}^{n,n-r}(R[\mathbf{x}]), \quad \Delta^{r+1}, \dots, \Delta^n \in \mathbb{M}^{n-r}(R[\mathbf{x}])$$

such that

$$(3.8) \quad \text{Jac}_f \times P \equiv \text{Id}_{n-r} + \sum_{j=r+1}^n f_j \Delta^j \text{ modulo } \pi.$$

Let ψ be the σ -linear endomorphism of $R\langle\mathbf{x}\rangle$ that sends each x_i to $x_i^{p'}$, so that it maps an element $g(\mathbf{x})$ to $g^\sigma(\psi(\mathbf{x}))$, where the superscript σ means we apply σ to the coefficients. We shall look for a σ -linear ϕ , defined by its action on the column vector of variables \mathbf{x} as

$$(3.9) \quad \phi(\mathbf{x}) = \psi(\mathbf{x}) + \psi(P)\mathbf{s},$$

where \mathbf{s} is then a column vector in $\pi R\langle\mathbf{x}\rangle^{n-r}$. We want \mathbf{s} to satisfy $G(\mathbf{s}) = 0$, where the column vector $G(\mathbf{S}) = (G_{r+1}(\mathbf{S}), \dots, G_n(\mathbf{S}))$ with entries in $R\langle\mathbf{x}\rangle[\mathbf{S}]$, is given by

$$(3.10) \quad G(\mathbf{S}) = f^\sigma(\psi(x) + \psi(P)\mathbf{S}) - f^{p'} - \sum_{j=r+1}^n f_j^{p'} \psi(\Delta^j)\mathbf{S},$$

for f^σ the vector $(f_{r+1}^\sigma, \dots, f_n^\sigma)$, $f^{p'}$ the vector $(f_{r+1}^{p'}, \dots, f_n^{p'})$, and \mathbf{S} the vector (S_{r+1}, \dots, S_n) .

In a way similar to the case of one equation in two variables discussed before, one finds that

- $G(0) \equiv 0$ modulo π ;
- $\text{Jac}_G(0) = \text{Jac}_{f^\sigma}(\psi(x)) \times \psi(P) - \sum_{j=r+1}^n f_j^{p'} \psi(\Delta^j)$, hence $\text{Jac}_G(0) \equiv \text{Id}_{n-r}$ modulo π .

Therefore the equation may be solved uniquely for \mathbf{s} in $\pi R\langle\mathbf{x}\rangle^{n-r}$ by Hensel's Lemma, and this can be done effectively using Newton iteration. It is now clear that ϕ is σ -linear, reduces to the p' -power map $\overline{\phi} : k[\mathbf{x}] \rightarrow k[\mathbf{x}]$, and maps the ideal (f_{r+1}, \dots, f_n) into itself. Overall, we obtained the following result.

Theorem 3.11. *Let f_{r+1}, \dots, f_n in $R[x_1, \dots, x_n]$ with $0 \leq r \leq n-1$ be given, and suppose that $A = R[x_1, \dots, x_n]/(f_{r+1}, \dots, f_n)$ satisfies Assumption 3.5. Fix P and $\Delta^{r+1}, \dots, \Delta^n$ as in (3.7) and (3.8), and let $G(\mathbf{S})$ be given by (3.10). Then there exists a unique lift of the p' -power map on \overline{A} to a σ -semi-linear endomorphism of $R\langle\mathbf{x}\rangle/(f_{r+1}, \dots, f_n)$ of the form (3.9) with \mathbf{s} in $\pi R\langle\mathbf{x}\rangle^{n-r}$ satisfying $G(\mathbf{s}) = 0$.*

To be able to effectively use this lift of Frobenius, we need to know that it preserves overconvergence, and know explicit bounds on the rate of convergence. To this end, we first need explicit bounds on the rate of convergence obtained in Hensel's Lemma. These are provided by Lemma 3.14 below. In order to describe them, it will be convenient to introduce some notation.

Notation 3.12. For non-zero D in $\mathbb{Q}_{\geq 0}^n$, let $V_D = \{v \text{ in } (\mathbb{R}_{\geq 0})^n \text{ with } D \cdot v \leq 1\}$.

In the process of obtaining our estimates in Lemma 3.14 and similar results in Section 5, we shall introduce suitably ramified extensions. In order to avoid interrupting the flow of the argument, we impose the following.

Convention 3.13. If α is in $\mathbb{Q}_{>0}$, then π^α means that we extend the ring R to the valuation ring R' in a finite extension K' of K for which α is attained as a valuation. In other words, such that π^α can be interpreted as a integer power of a uniformizer of R' .

Lemma 3.14. *Let $G_{r+1}(\mathbf{S}), \dots, G_n(\mathbf{S})$ in $R[\mathbf{x}][\mathbf{S}]$ be of maximal total degree $N > 0$ in \mathbf{S} . For $l = 0, \dots, N$, let $G_{j,l}(\mathbf{S})$ consist of the terms of $G_j(\mathbf{S})$ that are homogeneous in \mathbf{S} of degree l . Assume that the $G_j(0)$ are in $\pi R[\mathbf{x}]$ and that the determinant of $\text{Jac}_G(0)$ is in $R^* + \pi R[\mathbf{x}]$. Then there is a unique solution \mathbf{s} in $(\pi R\langle \mathbf{x} \rangle)^{n-r}$ of $G_{r+1}(\mathbf{S}) = \dots = G_n(\mathbf{S}) = 0$; in fact, it lies in $(\pi R\langle \mathbf{x} \rangle^\dagger)^{n-r}$.*

Moreover, $\mathbf{s} = \sum_I a_I \mathbf{x}^I$ where for each coordinate $a_{I,j}$ we have the following estimate, independent of j . If D in $(\mathbb{Q}_{\geq 0})^n$, and a, b in $\mathbb{Q}_{>0}$ are such that the Newton polytope of $G_{j,l}(\mathbf{S})$ is contained in $(a + b)V_D$ for $l = 0, \dots, N$, then for each I we have

$$v(a_{I,j}) \geq \frac{D \cdot I + 2a + b}{2e(a + b)}.$$

Proof. View $G = (G_{r+1}, \dots, G_n)$ as column vector. Then the existence and uniqueness of \mathbf{s} in $(\pi R\langle \mathbf{x} \rangle)^{n-r}$ are obtained from Hensel's lemma, by starting with $z_0 = (0, \dots, 0)$ as approximate solution of the vector equation $G(\mathbf{S}) \equiv 0$ modulo π , and applying Newton iteration $z_{i+1} = z_i - \text{Jac}_G(z_i)^{-1} G(z_i)$ for $i \geq 1$.

For the estimate, let ε be in $\mathbb{Q}_{>0}$ and define $\mu = \frac{1}{2(a+b)+\varepsilon} D$ in $\mathbb{Q}_{\geq 0}^n$ and $\nu = \frac{2(a+b)-b}{2(a+b)+\varepsilon}$ in $\mathbb{Q}_{>0}$. Then

$$(3.15) \quad \begin{aligned} \mu \cdot I &< 1 - \nu \text{ for all } I \text{ in } bV_D; \\ \mu \cdot I &< \frac{1}{2} \text{ for all } I \text{ in } (a + b)V_D; \\ \mu \cdot I &\leq (l - 1)\nu \text{ for all } I \text{ in } (al + b)V_D \text{ with } l = 2, \dots, N. \end{aligned}$$

Using Convention 3.13 above, we apply to each $\pi^{-\nu} G_j(\mathbf{S})$ the substitutions $S_j \leftarrow \pi^\nu S'_j$ and $x_i \leftarrow \pi^{-\mu_i} x'_i$. We shall abbreviate the latter to $\mathbf{x} \leftarrow \pi^{-\mu} \mathbf{x}$. In order to describe the result we abuse notation and write $G_{j,l}(x, \mathbf{S})$ for $G_{j,l}(\mathbf{S})$. Then we obtain

$$G_j(\mathbf{S}') = \sum_{l=0}^N \pi^{\nu(l-1)} G_{j,l}(\pi^{-\mu} \mathbf{x}', \mathbf{S}')$$

in $K'[\mathbf{x}'][\mathbf{S}']$. Applying the first inequality in (3.15) to all $G_{j,0}$, the second to all $G_{j,1}$, and the third to all $G_{j,l}$ for $l \geq 2$, one sees that each $G_j(\mathbf{S}')$ is in $R'[\mathbf{x}'][\mathbf{S}']$. Moreover, each $G_{j,0}$ is in $\pi' R'[\mathbf{x}']$, and the determinant of $\text{Jac}_G(0)$ is in $R'^* + \pi' R'[\mathbf{x}']$. By Hensel's lemma there exists a unique solution $\sum_{I \geq 0} b_I \mathbf{x}'^I$ in $(\pi' R' \langle \mathbf{x}' \rangle)^{n-r}$ of

$G_{r+1}(\mathbf{S}') = \cdots = G_n(\mathbf{S}') = 0$. Thus $\sum_I \pi^{\mu \cdot I + \nu} b_I \mathbf{x}^I$ and \mathbf{s} are two solutions of $G_{r+1}(\mathbf{S}) = \cdots = G_n(\mathbf{S}) = 0$ in $(\pi' R' \langle x \rangle)^{n-r}$, but by Hensel's lemma in $R' \langle x \rangle$ there is only one such solution. So for each I we find

$$v(a_I) > \frac{1}{e} (\mu \cdot I + \nu) = \frac{D \cdot I + (2a + b)}{e(2(a + b) + \varepsilon)}.$$

Letting ε go to 0 we find $v(a_I) \geq \frac{D \cdot I + (2a + b)}{2e(a + b)}$. Using $(1, \dots, 1)$, a sufficiently large and $b = 0$ shows that \mathbf{s} is in $(\pi R(\mathbf{x})^\dagger)^{n-r}$. \square

We can now lift the endomorphism $\bar{\phi}$ of \bar{A} to an endomorphism of A^\dagger .

Theorem 3.16. *Let ϕ be the lift of Frobenius constructed in Theorem 3.11. Then ϕ preserves A^\dagger . Furthermore, the following estimate holds for the coefficients $b_I = b_{i,I}$ in each $\phi(x_i) = x_i^{p'} + \sum_I b_{i,I} x^I$, and is independent of i . Let Γ be the intersection of all V_D that contain the Newton polytopes of all f_j . Fix d in $\mathbb{Q}_{>0}$ such that the Newton polytopes of all coefficients in the matrices P and $\Delta^{r+1}, \dots, \Delta^n$ in (3.7) are included in $d\Gamma$. If c is in $\mathbb{Q}_{>0}$, then $v(b_I) > \frac{c}{2e(d+1)p'} + \frac{1}{2e}$ whenever I is not in $c\Gamma$.*

Proof. Let $G(\mathbf{S})$ be as in (3.10). We recall that the lift ϕ is given by the formula

$$\phi(g(\mathbf{x})) = g^\sigma(\psi(\mathbf{x}) + \psi(P)\mathbf{s})$$

using the unique \mathbf{s} in $(\pi R(\mathbf{x})^{n-r})$ with $G(\mathbf{s}) = 0$.

We now prove the estimate of the coefficients, which will also show that A^\dagger is preserved. Note that Γ automatically contains the Newton polytopes of all (higher) partial derivatives of all f_j . Then one checks easily that the Newton polytopes of the entries of the homogeneous part of degree l in \mathbf{S} of $G(\mathbf{S})$ are contained in $(dl + 1)p'\Gamma$.

Write $s_j = \sum_I a_{j,I} x^I$. If I is not in $c\Gamma$, then $D \cdot I > c$ for some D in $(\mathbb{Q}_{\geq 0})^n$ with $\Gamma \subseteq V_D$. Then by Lemma 3.14, with $a = dp'$ and $b = p'$, we have

$$(3.17) \quad v(a_{j,I}) \geq \frac{D \cdot I + p'(2d + 1)}{2e(d + 1)p'} > \frac{c + p'(2d + 1)}{2e(d + 1)p'}.$$

Fix i , and write $\psi(P_{i,j}) = \sum_{K \in p'd\Gamma} d_{j,K} x^K$. Then $\phi(x_i) = x_i^{p'} + \sum_{j=r+1}^n \psi(P_{i,j}) s_j = x_i^{p'} + \sum_I b_I x^I$ with

$$b_I = \sum_{j=r+1}^n \sum_{K+L=I} d_{j,K} a_{j,L}.$$

Take c in $\mathbb{Q}_{>0}$ and assume I is not in $c\Gamma$. If $c \leq p'd$, then $v(b_I) \geq \frac{1}{e} > \frac{c}{2e(d+1)p'} + \frac{1}{2e}$ because $a_{j,L}$ is in πR . If $c > p'd$, then in $I = K + L$ we have that L is not in $(c - dp')\Gamma$. By (3.17) we then have $v(a_{j,L}) > \frac{(c - p'd) + p'(2d + 1)}{2e(d + 1)p'} = \frac{c}{2e(d + 1)p'} + \frac{1}{2e}$. Because all $d_{j,K}$ are in R , our estimate has been proved. \square

Remark 3.18. In Theorem 3.16 one can sometimes prescribe that $\phi(x_i) = x_i^{p'}$ for some i . If A is given by a presentation

$$0 \rightarrow (f_{r+1}, \dots, f_n) \rightarrow R[\mathbf{x}] \rightarrow A \rightarrow 0$$

and a is a positive integer with $a \leq r$, let us denote by J_a the matrix consisting of the last $n - a$ columns of $\text{Jac}_{(f)}$. If the $(n - r)$ -minors of \bar{J}_a generate the unit ideal of \bar{A} , then one can compute a lift ϕ of $\bar{\phi}$ with $\phi(x_i) = x_i^{p'}$ for $i = 1, \dots, a$. Namely,

we can apply the result of Arabia (3.8) with our R replaced with $R[x_1, \dots, x_a]$, and $R[x_1, \dots, x_n]$ with $R[x_1, \dots, x_a][x_{a+1}, \dots, x_n]$. We then obtain matrices P_a in $\mathbb{M}^{n-a, n-r}((R[x_1, \dots, x_n]))$ and $\Delta^{r+1}, \dots, \Delta^n$ in $\mathbb{M}^{n-r}((R[x_1, \dots, x_n]))$ with $J_a \times P_a \equiv \text{Id}_{n-r} + \sum_{j=r+1}^n f_j \Delta^j$ modulo π . This means we have satisfied (3.8) with a matrix P for which the first a rows are identically 0, and (3.10) now becomes

$$G(\mathbf{S}) = f^\sigma(\psi(x_1), \dots, \psi(x_a), \psi(x_{a+1}) + \psi(P_{a+1,*})\mathbf{S}, \dots, \psi(x_n) + \psi(P_{n,*})\mathbf{S}) \\ - f_j^{p'} - \sum_{j=r+1}^n f_j^{p'} \psi(\Delta^j)\mathbf{S}.$$

We return to our running example, Example 3.3, as an illustration of the estimates in Theorem 3.16.

Example 3.19. We apply the estimates of Theorem 3.16 to the data in Example 3.3, so that we have $m = 2$, $r = 1$, $P = \begin{pmatrix} 2^{-1}x \\ 2^{-1}y \end{pmatrix}$, $f_2(x, y) = x^2 - y^2 - 1$, $\Delta^2 = (1)$, $\Gamma = V_D$ for $D = (\frac{1}{2}, \frac{1}{2})$, and $d = \frac{1}{2}$. Then (i, j) is not in $c\Gamma$ if and only if $i + j > 2c$. Therefore, if $\phi(x) = x^p + \sum_{i,j \geq 0} b_{i,j} x^i y^j$, then $i + j > 2c$ implies $v(b_{i,j}) > \frac{c}{3p} + \frac{1}{2}$. Equivalently, $v(b_{i,j}) \geq \frac{i+j}{6p} + \frac{1}{2}$ for all (i, j) . The same estimates holds for the coefficients $b'_{i,j}$ in $\phi(y) = y^p + \sum_{i,j} b'_{i,j} x^i y^j$.

We conclude this section by showing that our theorems apply to suitable open parts of smooth, Noetherian schemes over R .

Remark 3.20. Suppose that Y is a smooth, Noetherian scheme Y over R of relative dimension $r \geq 0$. Then there exists a Zariski open affine part that is of the form (3.6), and such that the unit ideal of A is generated by the determinants of the $(n-r) \times (n-r)$ minors of Jac_f . Moreover, there exist matrices P in $\mathbb{M}^{n, n-r}(R[\mathbf{x}])$ and $\Delta^{r+1}, \dots, \Delta^n$ in $\mathbb{M}^{n-r}(R[\mathbf{x}])$ such that

$$\text{Jac}_f \times P = \text{Id}_{n-r} + \sum_{j=r+1}^n f_j \Delta^j$$

in $\mathbb{M}^{n-r}(R[\mathbf{x}])$.

Namely, let y be the generic point of the special fibre Y_k . Since Y is smooth over R of relative dimension r , there exists an open neighbourhood U of y in Y and an immersion j of U into an affine space \mathbb{A}_R^m , such that, locally around $z = j(y)$, the ideal sheaf defining $j(U)$ in some open of \mathbb{A}_R^m is generated by $m - r$ sections g_{r+1}, \dots, g_m . Furthermore, the differentials $dg_{r+1}(z), \dots, dg_m(z)$ are linearly independent in $\Omega_{\mathbb{A}_R^m/R}^1 \otimes k(z)$. Note that every open $V \subset U$ containing y also has this property.

According to [12, Proposition (17.2.5)], after localizing more if necessary, there exists such an open affine neighbourhood of y on which the conormal exact sequence splits. We may assume it is given by an algebra $A = R[\mathbf{x}]/J$, for an ideal $J = (f_{r+1}, \dots, f_n)$ of $R[\mathbf{x}]$. Then the morphism δ in the exact sequence of A -modules

$$J/J^2 \xrightarrow{\delta} \Omega_{R[\mathbf{x}]/R}^1 \otimes_{R[\mathbf{x}]} A \longrightarrow \Omega_{A/R}^1 \longrightarrow 0$$

is injective and admits a retraction. Therefore, $A \cdot df_{r+1} \oplus \dots \oplus A \cdot df_n \cong A^{n-r}$ is a direct summand of $\Omega_{R[\mathbf{x}]/R}^1 \otimes_{R[\mathbf{x}]} A \cong A^n$, and there exists a right inverse P in $\mathbb{M}^{n, n-r}(A)$ of Jac_f .

4. EXAMPLES OF THE GLOBAL FROBENIUS

In this section we make the construction of ϕ in Theorem 3.16 more explicit in the case of plane curves and their localisations. Note that then $r = 1$ and $n = 2$ or 3 .

Example 4.1. Let us first treat the case of a smooth curve in $R[x, y]$, defined by $f(x, y)$, with the current notation. There exist P_1, P_2 and Δ in $R[x, y]$ such that $\frac{f_x}{P_1 f_x + P_2 f_y} = 1 + \overline{\Delta} \cdot \overline{f}$ in $k[x, y]$, and (3.10) becomes

$$\begin{aligned} G(S) &= f^\sigma(x^{p'} + \psi(P_1)S, y^{p'} + \psi(P_2)S) - f^{p'} - f^{p'}\psi(\Delta)S \\ &= \psi(f) - f^{p'} + \left(f_x^\sigma(x^{p'}, y^{p'})\psi(P_1) + f_y^\sigma(x^{p'}, y^{p'})\psi(P_2) - f^{p'}\psi(\Delta) \right) S \\ &\quad + (\dots)S^2 + \dots \end{aligned}$$

With s the unique solution in $\pi R\langle x, y \rangle^\dagger$ of $G(S) = 0$, the map from $A^\dagger = R\langle x \rangle^\dagger / (f)$ to itself is given by mapping the class of x to that of $x^{p'} + P_1^\sigma(x^{p'}, y^{p'})s$, and the class of y to that of $y^{p'} + P_2^\sigma(x^{p'}, y^{p'})s$.

Moreover, let Γ be the intersection of all V_D that contain the polytope of f , and let d be a positive rational number such that the Newton polytopes of P_1, P_2 and Δ are included in $d\Gamma$. Then $\phi(x) = x^{p'} + \sum_{i,j \geq 0} b_{i,j}x^i y^j$ where, for each positive rational number c , we have $v(b_{i,j}) > \frac{c}{2e(d+1)p'} + \frac{1}{2e}$ whenever (i, j) is not in $c\Gamma$. The same estimates apply to the coefficients in $\phi(y) - y^{p'}$.

Example 4.2. Let us treat an explicit case of Example 4.1. Consider the elliptic curve over \mathbb{Z}_p with $p \neq 2, 3$ defined by $f(x, y) = y^2 - x^3 - 1$. Then we even have $\frac{1}{3}xf_x + \frac{1}{2}yf_y = 1 + f$ in $\mathbb{Z}_p[x, y]$. Let us take $p' = p$. Noting that σ is the identity here, we have to find the unique solution s in $p\mathbb{Z}_p\langle x, y \rangle^\dagger$ of $G(S) = 0$, with $G(S)$ the polynomial

$$\begin{aligned} G(S) &= f(x^p + \frac{1}{3}x^p S, y^p + \frac{1}{2}y^p S) - f^p - f^p S \\ &= -\frac{1}{27}x^{3p}S^3 + \left(\frac{1}{4}y^{2p} - \frac{1}{3}x^{3p}\right)S^2 + (1 + f(x^p, y^p) - f^p)S + f(x^p, y^p) - f^p. \end{aligned}$$

The map of $\mathbb{Z}_p\langle x, y \rangle^\dagger / (y^2 - x^3 - 1)$ to itself is then given by mapping the class of x to that of $x^p + \frac{1}{3}x^p s$, and the class of y to that of $y^p + \frac{1}{2}y^p s$. The polytope Γ has vertices $(0, 0)$, $(3, 0)$ and $(0, 2)$, and equals V_D with $D = \frac{1}{6}(2, 3)$. We can take $d = \frac{1}{2}$, so that $\phi(x) = x^p + \sum_{i,j \geq 0} b_{i,j}x^i y^j$ with $v(b_{i,j}) > \frac{c}{3p} + \frac{1}{2}$ whenever $2i + 3j > 6c$. In fact, (i, j) is not in $c\Gamma$ if and only if $2i + 3j > 6c$, so choosing $c = \frac{2i+3j}{6} - \varepsilon$ with $\varepsilon > 0$ and letting ε go to 0 we find that $v(b_{i,j}) \geq \frac{2i+3j}{18p} + \frac{1}{2}$. The same estimates apply to the coefficients in $\phi(y) - y^p$.

Example 4.3. Let us consider an irreducible affine curve defined by $f(x, y)$ with f_y not identically 0 modulo π . Let $A = R[x, y, z] / (f, z f_y - 1)$. Notice that A satisfies the assumption of Remark 3.18 with $n = 3$ and $r = k = 1$. Let h denote

$$\frac{\partial^2 f}{\partial y^2}. \text{ Then we have } \text{Jac} = \begin{pmatrix} f_x & f_y & 0 \\ z f_{x,y} & z h & f_y \end{pmatrix}, \text{ so we can take } P = \begin{pmatrix} 0 & 0 \\ z & 0 \\ -z^3 h & z \end{pmatrix},$$

$\Delta_2 = 0$ and $\Delta_3 = \begin{pmatrix} 1 & 0 \\ -z^2 h & 1 \end{pmatrix}$. Thus, we have to find the unique solution (s_2, s_3)

in $(\pi R\langle x, y, z \rangle^\dagger)^2$ of the equations

$$\begin{aligned} G_2(S_2, S_3) &= f^\sigma(\psi(\mathbf{x}) + \psi(P)\mathbf{S}) - f^{p'} - (zf_y - 1)^{p'} S_2 \\ &= f^\sigma(\psi(x), \psi(y) + \psi(z)S_2) - f^{p'} - (zf_y - 1)^{p'} S_2 \end{aligned}$$

and

$$G_3(S_2, S_3) = f_3^\sigma(\psi(\mathbf{x}) + \psi(P)\mathbf{S}) - (zf_y - 1)^{p'} (1 - \psi(z^2 h)S_2 + S_3)$$

with $f_3(x, y, z) = zf_y - 1$. Note that the first term in $G_3(S_2, S_3)$ is then given explicitly as $(\psi(z) - \psi(z^3 h)S_2 + \psi(z)S_3)f_y^\sigma(\psi(x), \psi(y) + \psi(z)S_2) - 1$.

Observe that G_2 is a polynomial in S_2 only, and that by Lemma 3.14 there exists a unique solution s_2 in $\pi R\langle x, y, z \rangle^\dagger$ of $G_2(S_2) = 0$. Then the map ϕ from $R\langle x, y, z \rangle^\dagger$ to itself maps x to $x^{p'}$, and y to $y^{p'} + z^{p'} s_2$.

Let us notice that all the coefficients of P and Δ_3 lie in 3Γ , where Γ is the intersection of all V_D that contain the Newton polytopes of f and of $zf_y - 1$. Thus, if we write $\phi(y) = y^{p'} + \sum_I b_I x^I$, then for every I that is not in $c\Gamma$ with c in $\mathbb{Q}_{>0}$ fixed, we have the estimate $v(b_I) > \frac{c}{8ep'} + \frac{1}{2e}$.

In order to determine $\phi(z)$ in $R\langle x, y, z \rangle^\dagger$ one would have to solve the equations, but the class of $\phi(z)$ in A^\dagger is determined by $\phi(z)\phi(f_y) = 1$. Note that

$$\phi(f_y) = f_y^\sigma(x^{p'}, y^{p'} + z^{p'} s_2) = \psi(f_y) + F_1 = f_y^{p'} - F_2 = z^{-p'} - F_2,$$

where F_1 and F_2 are in $\pi R\langle x, y, z \rangle^\dagger$. Therefore the class of $\phi(z)$ equals that of $z^{p'}(1 + \sum_{m=1}^\infty (z^{p'} F_2)^m)$.

Example 4.4. Let us apply Example 4.3 to $y^2 - Q(x)$, where $p \neq 2$, $Q(x)$ in $R[x]$ is of degree $2g + 1$, and its reduction in $k[x]$ has degree $2g + 1$ and no multiple roots. (In other words, if we take $R = W(k)$, the Witt vectors of k , then we are in the situation studied in [15].) Inverting $2y$, we obtain an open part corresponding to $R[x, y, z]/(y^2 - Q(x), 2yz - 1)$. We have $\text{Jac} = \begin{pmatrix} -Q'(x) & 2y & 0 \\ 0 & 2z & 2y \end{pmatrix}$, so we can take

$$P = \begin{pmatrix} 0 & 0 \\ z & 0 \\ -2z^3 & z \end{pmatrix}, \Delta_2 \text{ the zero matrix, and } \Delta_3 = \begin{pmatrix} 1 & 0 \\ -2z^2 & 1 \end{pmatrix}.$$

In order to find a lift ϕ of the relative Frobenius on \overline{A}^\dagger , we have to find the solution $\mathbf{s} = (s_2, s_3)$ in $(\pi R\langle x, y, z \rangle^\dagger)^2$ of $G(\mathbf{S}) = 0$, where

$$G_2(\mathbf{S}) = (y^{p'} + z^{p'} S_2)^2 - Q^\sigma(x^{p'}) - (y^2 - Q(x))^{p'} - (2yz - 1)^{p'} S_2$$

and

$$G_3(\mathbf{S}) = 2(y^{p'} + z^{p'} S_2)(z^{p'} - 2z^{3p'} S_2 + z^{p'} S_3) - 1 - (2yz - 1)^{p'} (1 - 2z^{2p'} S_2 + S_3).$$

If $\mathbf{s} = (s_2, s_3)$ is the unique solution in $(\pi R\langle x, y, z \rangle^\dagger)^2$, then $y^{p'} + z^{p'} s_2$ is the unique solution for $\phi(y)$ in $A^\dagger = R\langle x, y, z \rangle^\dagger/(f, 2yz - 1)$ of $\phi(y)^2 - Q^\sigma(x^{p'}) = 0$ that is congruent to $y^{p'}$ modulo π , hence it must coincide with the explicit formula given in [15] when $p' = p$ and $R = W(k)$.

5. EXPANSIONS AT THE ENDS

We now return to our curve as described in Section 1. We extend the base field K to \tilde{K} , and R to \tilde{R} , so that $C_{\tilde{R}} \setminus X_{\tilde{R}}$ is the union of the ‘missing points’ Q_i . Let \mathcal{E} be one of the ends of the rigid analytic space corresponding to $C_{\tilde{R}} \setminus X_{\tilde{R}}$ described in Section 2, and fix Q , one of the missing points that lies in the corresponding residue disc \mathcal{D} .

Because for this \mathcal{E} we only need this section Q , we do not have to extend R to \tilde{R} ; it suffices to replace R with a suitable $R_Q \subseteq \tilde{R}$. As this makes no difference to the proofs we avoid this cumbersome notation and write R instead of R_Q or \tilde{R} .

In Theorem 3.16 we have constructed a lift ϕ of $\bar{\phi}$. In order to calculate the contribution of \mathcal{E} to the right hand side of (2.12), we could calculate the expansion of $\phi(\eta)$ as follows. We first apply σ to the coefficients of η in order, compute the $\phi(x_i)$ as well as their expansions, and substitute the latter into η^σ . Instead, we never compute the $\phi(x_i)$ but expand the x_i in the defining equations (3.10) and solve those. This way we can obtain expansions of the $\phi(x_i)$ directly, without the need of substituting expansions into expansions. Another advantage is that we work with expressions that contain only the local parameter, not all the variables x_i . Also, in practice the local expansions can converge on a larger annulus than one might expect from the behaviour of the global $\phi(x_i)$ (see Examples 5.7 and 5.17).

The drawback is of course that we have to do solve the equations for all ends \mathcal{E} , so if there are many of those, it may be better to compute the $\phi(x_i)$ globally first and then substitute expansions of the x_i . In order to maintain this flexibility, we also discuss how the estimates on the coefficients in the global $\phi(x_i)$ translate into estimates on the coefficients in their local expansions.

Let t be a local equation of Q on C (as scheme, not rigid analytic space), which we shall also view as a parameter on \mathcal{D} and \mathcal{E} , and use it to make the restriction map of rigid analytic functions U_r (for a suitable $r < 1$) to \mathcal{E} explicit on A^\dagger .

Let $\mathcal{O}_{C,q}$ be the local ring at the reduction q of Q of C . Note that $\mathcal{O}_{C,q}/(t) \simeq R$, and the completion of $\mathcal{O}_{C,q}$ with respect to (t) is isomorphic with $R[[t]]$. We shall refer to the resulting map $\mathcal{O}_{C,q} \rightarrow R[[t]]$, or any of the analogues described below, as the expansion map at Q . If a in A is such that in \mathcal{D} it only has a pole along Q , then $t^{-\text{ord}_Q(a)}a$ is in $\mathcal{O}_{C,q}$ and a has an expansion in $R((t))$.

More generally, let

$$\widehat{R((t))} = \left\{ \sum_{m \in \mathbb{Z}} a_m t^m \text{ with all } a_m \text{ in } R \text{ and } \lim_{m \rightarrow -\infty} a_m = 0 \right\}$$

be the π -adic completion of $R((t))$. Then any element in $R((t))$ that is not in $\pi R((t))$ is in $\widehat{R((t))}^*$: we can write it as $t^d f - \pi g$ with f in $R[[t]]^*$ and g in $R((t))$, which has inverse $t^{-d} f^{-1} (1 + \sum_{m \geq 1} (\pi t^{-d} f^{-1} g)^m)$. If a is any element in A , then using local equations in $\mathcal{O}_{C,q}$ of irreducible divisors on C containing q , one sees that there is some h in $\mathcal{O}_{C,q}$ such that ha is in $\mathcal{O}_{C,q}$. Because a does not restrict to 0 on C_k , we can assume the same about h . Because the composition $\mathcal{O}_{C,q} \rightarrow R[[t]] \rightarrow k[[t]]$ descends to the expansion map on $\mathcal{O}_{C_k,q}$, it follows that h maps to a unit u in $\widehat{R((t))}$. Then a has the expansion in $\widehat{R((t))}$ obtained by expanding ha and multiplying by u^{-1} .

As $\widehat{R((t))}$ is π -adically complete, the expansion map $A = R[\mathbf{x}]/(f_2, \dots, f_n) \rightarrow \widehat{R((t))}$ at Q extends to $R(\mathbf{x})/(f_2, \dots, f_n) \rightarrow \widehat{R((t))}$. We shall see later that this

extension restricted to A^\dagger takes values in a suitable subring $R_*((t))$ of $\widehat{R((t))}$. The extension also induces a map

$$(5.1) \quad \xi : R\langle \mathbf{x} \rangle \rightarrow \widehat{R((t))}.$$

We shall abuse notation and denote by ξ the map to $\widehat{R((t))}$ from any of $R\langle \mathbf{x} \rangle$, $R\langle \mathbf{x} \rangle^\dagger$, and A^\dagger .

In order to describe the image of $R\langle \mathbf{x} \rangle^\dagger$ under this map, together with estimates, below, we introduce a subring $R_*((t))$ of $\widehat{R((t))}$. We shall show in Proposition 5.5 that ξ maps $R\langle \mathbf{x} \rangle^\dagger$ into $R_*((t))$, together with a description for bounds on the coefficients involved.

In many applications the expansions of the x_j will be in $R((t))$. We therefore include statements that deal with this case specifically, namely Remarks 5.15 and 5.16.

In order to describe our estimates on coefficients we introduce the following subsets of $\widehat{R((t))}$. Note that each element in them is a rigid function as described in (2.2) on (a possibly narrower) \mathcal{E} .

Notation 5.2. For any rational numbers α and β with $\alpha > 0$ we let

$$R_{\alpha,\beta}((t)) = \left\{ \sum_{m \in \mathbb{Z}} a_m t^m \text{ with all } a_m \text{ in } R \text{ and } v(a_m) \geq -\alpha m + \beta \right\}.$$

We also let $R_*((t)) = \bigcup_{\alpha,\beta} R_{\alpha,\beta}((t))$.

It can be helpful to visualize the conditions on the a_m by drawing the region in the plane in which the pairs $(m, v(a_m))$ for non-zero a_m can lie, as in Figure 5.1.

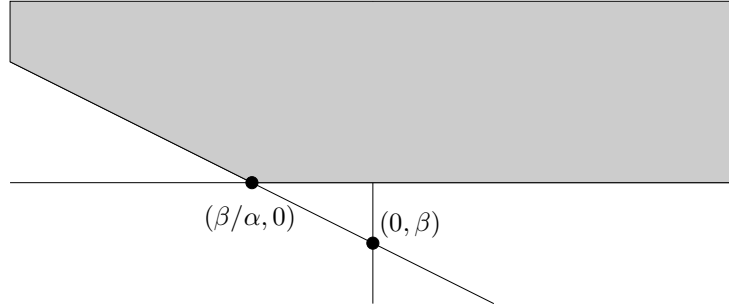


FIGURE 5.1.

The following is easily established.

Lemma 5.3. *The subsets above have the following properties.*

- (1) *The elements in $R_{\alpha,\beta}((t))$ converge for $p^{-\alpha} < |t| < 1$.*
- (2) *$R_{\alpha_1,\beta_1}((t)) \times R_{\alpha_2,\beta_2}((t)) \rightarrow R_{\min(\alpha_1,\alpha_2),\beta_1+\beta_2}((t))$ under multiplication in $\widehat{R((t))}$.*
- (3) *$R_*((t))$ is a subring of $\widehat{R((t))}$, as are the $R_{\alpha,0}((t))$.*
- (4) *$R_{\alpha,0}((t))$ is π -adically complete.*

- (5) The units of $R_{\alpha,0}((t))$ are those $\sum_m a_m t^m$ with a_0 in R^* . (Write such an element as $u + w$ with $u = \sum_{n \geq 0} a_n t^n$ and $w = \sum_{m < 0} a_m t^m$. Then its inverse is $u^{-1}(1 - u^{-1}w + u^{-2}w^2 - \dots)$.)
- (6) If c is an element of R with $v(c) = \gamma > 0$, then $cR_{\alpha,\beta}((t))$ is contained in $R_{\alpha,0}((t))$ if $\beta + \gamma \geq 0$, and in $R_{-\gamma\alpha/\beta,0}((t))$ if $\beta + \gamma < 0$ (see Figure 5.2). Note that $-\gamma\alpha/\beta < \alpha$ when $\beta + \gamma < 0$.

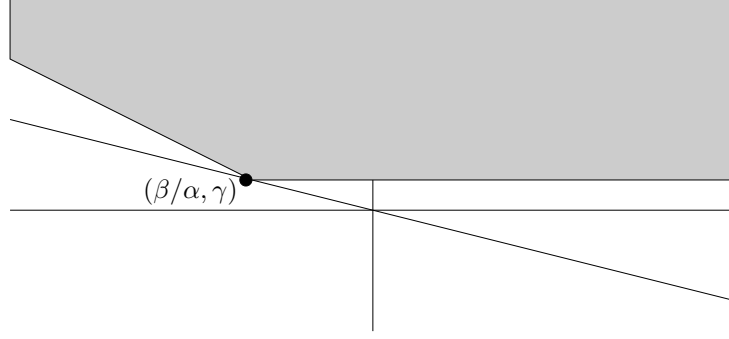


FIGURE 5.2.

Remark 5.4. For a finite subset T of $\mathbb{R} \cup \{\infty\}$, we define $\min^+(T)$ as $\min(T \cap \mathbb{R}_{>0})$; i.e., we ignore all negative numbers as well as ∞ . Then this last property states that $cR_{\alpha,\beta}((t))$ is contained in $R_{\alpha',0}((t))$ with $\alpha' = \min^+\{\alpha, -\gamma\alpha/\beta\}$.

We now fulfill an earlier promise, and show that the expansion map maps $R(\mathbf{x})^\dagger$ to $R_*(t)$. In particular, each element in A^\dagger is mapped to a rigid function on (a possibly narrower) \mathcal{E} .

Proposition 5.5. *The expansion map ξ in (5.1) maps $R(\mathbf{x})^\dagger$ to $R_*(t)$. More precisely, if $g(\mathbf{x}) = \sum_I a_I \mathbf{x}^I$ in $R(\mathbf{x})^\dagger$ with $v(a_I) \geq D \cdot I + \delta$ for some D in $(\mathbb{Q}_{>0})^m$ and δ in \mathbb{Q} , then $\xi(g(\mathbf{x}))$ is in $R_{\gamma,\delta}(t)$ where γ is obtained as follows:*

- (1) if all $\xi(x_i)$ are in $R((t))$, take γ in $\mathbb{Q}_{>0}$ with $d_i \geq -\gamma \text{ord}_t(x_i)$ for all i ;
- (2) if each $\xi(x_i)$ is in some $R_{\alpha,\beta_i}((t))$, let γ' in $\mathbb{Q}_{>0}$ be such that $-d_i \leq \beta_i \alpha^{-1} \gamma'$ for all i , and take $\gamma = \min\{\gamma', \alpha\}$.

Proof. (1) Write $D = (d_1, \dots, d_n)$, and let $D' = (d'_1, \dots, d'_n)$ with $d'_i = \text{ord}_t(x_i)$. Note that each $\xi(x^I)$ is in $t^{D' \cdot I} R[[t]]$. We have $v(a_I) \geq D \cdot I + \delta \geq -\gamma D' \cdot I + \delta$, so that $a_I t^{D' \cdot I}$ is in $R_{\gamma,\delta}((t))$. The same then holds for each $\xi(a_I x^I)$, hence for $\xi(g(x))$. (Of course, if all $d'_i \geq 0$ then we can take γ arbitrarily large and recover that $\xi(g(x))$ is in $R[[t]]$.)

(2) Let $B = (\beta_1, \dots, \beta_n)$ so that the expansion of $a_I x^I$ is in $a_I R_{\alpha,B \cdot I}((t))$ by Lemma 5.3(2). Then the vertex for the corresponding region as in Figure 5.2 occurs at $(\alpha^{-1} B \cdot I, v(a_I))$. But this point is above $(\alpha^{-1} B \cdot I, \max\{0, D \cdot I + \delta\})$, which is to the right of $(-\gamma'^{-1} D \cdot I, \max\{0, D \cdot I + \delta\})$. As I varies, those last points all lie in the region for $R_{\gamma',\delta}((t))$. If $\alpha \geq \gamma'$ then the same holds for the regions for all $a_I R_{\alpha,B \cdot I}((t))$. If $\alpha \leq \gamma'$ then it holds if we enlarge our region to that of $R_{\alpha,\delta}((t))$. \square

Remark 5.6. Note that if at least one $d'_i < 0$ in part (1) of Proposition 5.5, then $\gamma = \min^+ \{-d_i/d'_i\}$ is in $\mathbb{Q}_{>0}$, and is the best possible choice. If $\gamma = -d_j/d'_j$, then $D \cdot I = -\gamma D' \cdot I$ for all I having non-zero j -th entry and zeroes elsewhere. So for this γ the statement of part (1) appears to be optimal.

The same cannot be said for part (2) in general, because the estimate is based on the vertex at the bend in Figure 5.2, which may not correspond to an actual point $(m, v(a_m))$ for an element of $R_*(t)$. For example, suppose $n = 1$, $D = (d_1)$, and take $\alpha = 2$, $\beta = -1$. Then Proposition 5.5 gives us $\gamma' = 2d_1$ as largest possible γ' , and the result $\xi(g(x))$ is in $R_{\gamma, \delta}(t)$ with $\gamma = \min\{2d_1, 1\}$. On the other hand, if $e = 1$, then $R_{2, -1}(t) \subset R_{1, 0}(t)$. Taking $g(x)$ in this larger set, we can now take any γ' in $\mathbb{Q}_{>0}$. The result $\xi(g(x))$ lies in $R_{1, \delta}(t)$. (Note that d_1 drops out in this example because $R_{1, 0}(t)$ is a ring, so all $\xi(x)^i$ are in it.)

Example 5.7. Let us return to the estimates obtained in Example 3.19. There we had an element $\sum_{i,j} b_{i,j} x^i y^j$ with $v(b_I) \geq \frac{i+j}{6p} + \frac{1}{2}$, so that $D = (\frac{1}{6p}, \frac{1}{6p})$ and $\delta = \frac{1}{2}$. Both x and y have poles of order 1 at each of the two points at infinity, so the largest γ we can take is $\frac{1}{6p}$. Then Proposition 5.5(1) states that $\xi(\sum_{i,j} b_{i,j} x^i y^j)$ is in $R_{\frac{1}{6p}, \frac{1}{2}}(t)$.

Note that we could compute the expansions of the $\phi(x_i)$ constructed in Theorem 3.11, by first computing the $\xi(x_j)$ and substituting those into the $\phi(x_i)$. However, unless there are many ends, it should be much more efficient if we can compute the expansions of the $\phi(x_i)$ directly from their definition. That this can be done is the content of Theorem 5.8. In Theorem 5.14 we shall discuss estimates on the coefficients in the expansions obtained by this method. Note that the global estimates obtained in Theorem 3.16 give us estimates on the expansions as well by applying Proposition 5.5, but the two estimates can be quite different (see Examples 5.7 and 5.17).

Theorem 5.8. *Let P and $\Delta^2, \dots, \Delta^n$ and $G(\mathbf{S})$ be as in Theorem 3.16, and let ϕ be the resulting σ -linear endomorphism of A^\dagger . Then the expansions at Q of the $\phi(x_i)$ can be computed directly. More precisely, if $H(\mathbf{S})$ is obtained from (3.10) by applying ξ to the coefficients, then there is a unique solution $\tilde{\mathbf{s}}$ in $(\pi \widehat{R}(t))^{n-r}$ of $H(\mathbf{S}) = 0$, and $\xi(\phi(\mathbf{x})) = \xi(\psi(\mathbf{x})) + \xi(\psi(P))\tilde{\mathbf{s}}$.*

Proof. Recall that ϕ is induced by the σ -linear endomorphism of $R\langle \mathbf{x} \rangle^\dagger$ mapping $g(\mathbf{x})$ to $g^\sigma(\psi(\mathbf{x}) + \psi(P)\mathbf{s})$, with \mathbf{s} the unique solution in $(\pi R\langle \mathbf{x} \rangle^\dagger)^{n-r}$ of $G(\mathbf{S}) = 0$. So $\xi(\phi(\mathbf{x})) = \xi(\psi(\mathbf{x})) + \xi(\psi(P))\xi(\mathbf{s})$. Because $\xi(\mathbf{s})$ is in $(\pi R_*(t))^{n-r}$ by Proposition 5.5, it suffices to show that $H(\mathbf{S}) = 0$ has a unique solution $\tilde{\mathbf{s}}$ in $(\widehat{R}(t))^{n-r}$.

By that proposition the coefficients in $H(\mathbf{S})$ are in $R_*(t)$, and $H(\mathbf{S})$ has inherited the following properties from $G(\mathbf{S})$:

- $H(0) \equiv 0$ modulo $\pi R_*(t)$;
- $\text{Jac}_H(0) = \xi(\text{Jac}_G(0))$, hence $\text{Jac}_H(0) \equiv \text{Id}_{n-r}$ modulo $\pi R_*(t)$.

Applying Hensel's lemma for the π -adically complete ring $\widehat{R}(t)$ finishes the proof. \square

Remark 5.9. Note that applying ξ to the coefficients of (3.10) kills the terms involving the f_j . In particular, $H(\mathbf{S})$ is obtained by applying ξ to the coefficients in $f^\sigma(\psi(x) + \psi(P)\mathbf{S})$, hence is determined by f and P . The solution $\tilde{\mathbf{s}}$ we then obtain as the appropriate solution of $f^\sigma(\xi(\psi(x)) + \xi(\psi(P))\mathbf{S}) = 0$.

In order to give estimates on the coefficients involved in the solution $\tilde{\mathbf{s}}$ described in Theorem 5.8, we need some lemmas and remarks. The reader should think of those as the local analogue of Lemma 3.14.

Lemma 5.10. *Let $G_{r+1}(\mathbf{S}), \dots, G_n(\mathbf{S})$ in $R_{\alpha,0}((t))[\mathbf{S}]$ for some $\alpha > 0$ be of total maximal degree $N > 0$ in the variables $\mathbf{S} = (S_{r+1}, \dots, S_n)$. Assume that each $G_j(0)$ is in $\pi^b R_{\alpha,0}((t))$ for some integer $b \geq 1$, and that the determinant of $\text{Jac}_G(0)$ is in $R_{\alpha,0}((t))^*$. Then there is a unique solution \mathbf{s} in $(\pi^b R_{\alpha,0}((t)))^{n-r}$.*

Proof. Apply Hensel's lemma to the equation $G(\mathbf{S}) = 0$, starting with $z_0 = (0, \dots, 0)$ as approximate solution, and observe that under Newton iteration $z_{i+1} = z_i - \text{Jac}_G(z_i)^{-1}G(z_i)$ we stay in $\pi^b R_{\alpha,0}((t))$ all the time. \square

Remark 5.11. Note that this is sharp for polynomials of the form $(S+1)^{N-1}(S-z)$ with z in $\pi R_{\alpha,0}((t))$.

Lemma 5.12. *Let $H_{r+1}(\mathbf{S}), \dots, H_n(\mathbf{S})$ be in $R_*((t))[\mathbf{S}]$ of total maximal degree $N \geq 1$. Assume that there exist $\alpha_l > 0$ and β_l for $l = 0, \dots, N$, and an integer $a \geq 1$, such that*

- all $H_j(0)$ are in $\pi^a R_{\alpha_0, \beta_0}((t))$;
- the entries of $\text{Jac}_H(0)$ are in $R_{\alpha_1, 0}((t))$ and its determinant is in $R_{\alpha_1, 0}((t))^*$;
- the homogeneous parts of degree l of all $H_j(\mathbf{S})$ are in $R_{\alpha_l, \beta_l}((t))[\mathbf{S}]$ for $l = 2, \dots, N$.

Then $H(\mathbf{S}) = 0$ has a unique solution \mathbf{s} with coordinates in $\pi R_*((t))$.

In fact, if we write such a coordinate as $\sum_m a_m t^m$, then we have the following bound. For any ν in $\mathbb{Q}_{>0}$ satisfying $\nu < a$, let

$$(5.13) \quad \alpha'_\nu = \min^+ \left\{ \alpha_0, \dots, \alpha_N, -\frac{(a-\nu)\alpha_0}{e\beta_0}, -\frac{\nu\alpha_2}{e\beta_2}, -\frac{2\nu\alpha_3}{e\beta_3}, \dots, -\frac{(N-1)\nu\alpha_N}{e\beta_N} \right\}.$$

Then $v(a_m) \geq \max\{0, -\alpha'_\nu m\} + \frac{\nu}{e}$.

Proof. That there is a unique solution with coordinates in $\pi \widehat{R}((t))$ is again a consequence of Hensel's lemma, since all $R_{\alpha, \beta}((t))$ are in the π -adically complete ring $\widehat{R}((t))$.

Now fix a ν in $\mathbb{Q}_{>0}$ with $\nu < a$, and let ε in $\mathbb{Q}_{>0}$ satisfy $\varepsilon < a - \nu$. We shall be using Convention 3.13 again. Let $G_j(\mathbf{S}') = \pi^{-\nu} H_j(\pi^\nu \mathbf{S}')$ for $j = r+1, \dots, n$. Then $G_j(0)$ is in $\pi^{a-\nu} R'_{\alpha_0, \beta_0}((t))$, $\text{Jac}_G(0) = \text{Jac}_H(0)$ has entries in $R'_{\alpha_1, 0}((t))$ and determinant in $R'_{\alpha_1, 0}((t))^*$, and the homogeneous parts of degree l of all the $G_j(\mathbf{S}')$ are in $\pi^{(l-1)\nu} R'_{\alpha_l, \beta_l}((t))[\mathbf{S}']$ for $l = 2, \dots, N$. We can apply Lemma 5.10 (but with R replaced with R' , π^a with π^ε , and α with α'), provided that $\pi^{a-\nu-\varepsilon} R'_{\alpha_0, \beta_0}((t))$, $R'_{\alpha_1, 0}((t))$, and the $\pi^{(l-1)\nu} R'_{\alpha_l, \beta_l}((t))$ for $l = 2, \dots, N$ are all in $R'_{\alpha', 0}((t))$. By Remark 5.4, this is the case when the following hold simultaneously:

- $\alpha' \leq \min^+ \{\alpha_0, -(a-\nu-\varepsilon)\alpha_0/(e\beta_0)\}$;
- $\alpha' \leq \alpha_1$;
- $\alpha' \leq \min^+ \{\alpha_l, -(l-1)\nu\alpha_l/(e\beta_l)\}$ for $l = 2, \dots, N$.

Therefore we can certainly take

$$\alpha' = \alpha'_{\nu, \varepsilon} = \min^+ \left\{ \alpha_0, \dots, \alpha_N, -\frac{(a-\nu-\varepsilon)\alpha_0}{e\beta_0}, -\frac{\nu\alpha_2}{e\beta_2}, \dots, -\frac{(N-1)\nu\alpha_N}{e\beta_N} \right\}.$$

From Lemma 5.10 we obtain that the vector equation $G(\mathbf{S}') = 0$ has a unique solution \mathbf{s}' with coordinates in $\pi^\varepsilon R'_{\alpha',0}((t))$. Then $\pi^\nu \mathbf{s}'$ is a solution of $H(\mathbf{S}) = 0$ in $\pi^{\varepsilon+\nu} R'_*((t)) \subset \pi^\alpha R'_*((t))$. But from Hensel's lemma in $R'_*((t))$, we see that $H(\mathbf{S}) = 0$ has a unique solution with coordinates in $\pi^a \widehat{R}'((t))$, hence $\mathbf{s} = \pi^\nu \mathbf{s}'$ has coordinates in $\pi^{\nu+\varepsilon} R'_{\alpha',0}((t))$. As the coordinates are actually in R , letting ε go to zero finishes the proof. \square

We can now obtain our main estimates for the expansions of the $\phi(x_i)$.

Theorem 5.14. *Let $\tilde{\mathbf{s}}$ be the unique solution of $H(\mathbf{S}) = 0$ constructed in Theorem 5.8. Then we have the following estimates for the coefficients in $\tilde{\mathbf{s}}$.*

- (1) *If there are positive integers a and b such that the coefficients of the homogeneous parts of degree l are in $\pi^{at-d_0} R[[t]]$ for $l = 0$, in $R + \pi^b t^{-d_1} R[[t]]$ for $l = 1$, in $t^{-d_l} R[[t]]$ for $l = 2, \dots, N$, and the determinant of $\text{Jac}_H(0)$ is in $R^* + \pi^b t^{-d_1} R[[t]]$, then for every ν in $\mathbb{Q}_{>0}$ with $\nu < a$, we have that $\tilde{\mathbf{s}}$ is in $R_{\alpha_\nu, \frac{\nu}{e}}((t))$, where*

$$\alpha_\nu = \frac{1}{e} \min^+ \left\{ \frac{b}{d_1}, \frac{(a-\nu)}{d_0}, \frac{\nu}{d_2}, \frac{2\nu}{d_3}, \dots, \frac{(N-1)\nu}{d_N} \right\}.$$

- (2) *If in the statement of (1) we replace $t^{-d_l} R((t))$ with $R_{\alpha, -d_l \alpha}((t))$ for $l = 0, \dots, N$, then the coordinates of $\tilde{\mathbf{s}}$ are in $R_{\min\{\alpha, \alpha_\nu\}, \frac{\nu}{e}}((t))$, with α_ν as in (1), again for all ν in $\mathbb{Q}_{>0}$ with $\nu < a$.*

Proof. Clearly, $t^{-d_l} R[[t]] \subset R_{\alpha_l, \beta_l}((t))$ if $-d_l \geq \frac{\beta_l}{\alpha_l}$. We take $\beta_l = d_l \alpha_l$ with α_l very large for $l \neq 1$. For $l = 1$ we note that $\pi^b t^{-d_1} R[[t]] \subset R_{\min\{\frac{b}{e d_1}, 0\}}((t))$ (which we interpret as $R[[t]]$ if $d_1 \leq 0$). We now apply Lemma 5.12 to $H(\mathbf{S})$ as in Theorem 5.8. Then (5.13) simplifies to the given expression for α_ν (except if all $d_l \leq 0$, in which case $\alpha = +\infty$; but (5.13) can be made arbitrarily large in the same way). This proves part (1).

For part (2), we observe that $\pi^b R_{\alpha, -d_1 \alpha}((t)) \subset R_{\min\{\alpha, \frac{b}{e d_1}\}, 0}((t))$ and apply Lemma 5.12 to $H(\mathbf{S})$ as in Theorem 5.8. \square

Remark 5.15. In explicit examples one can try to maximize the bound given in Theorem 5.14, but as a crude estimate, let us assume $N \geq 2$, and take $\gamma > 0$ and $\delta \geq 0$ such that $d_l \leq (l-1)\gamma + \delta$ for $l = 2, \dots, N$. Then

$$\frac{1}{e} \min^+ \left\{ \frac{b}{d_1}, \frac{(a-\nu)}{d_0}, \frac{\nu}{\gamma + \delta} \right\} \leq \alpha_\nu$$

because $\frac{(l-1)\nu}{(l-1)\gamma + \delta}$ increases with l . If $d_0 \leq 0$ then we can let ν approach a and obtain $\tilde{\alpha} = \frac{1}{e} \min^+ \left\{ \frac{b}{d_1}, \frac{a}{\gamma + \delta} \right\}$, so that $\tilde{\mathbf{s}}$ has coordinates in $R_{\alpha_\nu, \frac{\nu}{e}}((t)) \subseteq R_{\tilde{\alpha}, \frac{a}{e}}((t))$. If $d_0 > 0$, then we equate the last two entries and solve for ν , which gives $\tilde{\nu} = \frac{a(\gamma + \delta)}{d_0 + \gamma + \delta}$. With $\tilde{\alpha} = \frac{1}{e} \min^+ \left\{ \frac{b}{d_1}, \frac{a}{d_0 + \gamma + \delta} \right\}$ we have $\alpha_{\tilde{\nu}} \geq \tilde{\alpha}$, and $\tilde{\mathbf{s}}$ has coordinates in $R_{\tilde{\alpha}, \frac{\tilde{\nu}}{e}}((t))$.

Remark 5.16. Although Theorem 5.14 and Remark 5.15 give estimates when all coordinates in Lemma 5.12 have entries in $R((t))$, they do not take into account the coefficients involved in R . One can sometimes obtain better estimates by following the method of the proof of Theorem 5.14 and applying Lemma 5.10 directly. Namely, in case (1) of the theorem, take ν in $\mathbb{Q}_{>0}$ with $\nu < a$ and consider $G(\mathbf{S}') = \pi^{-\nu} H(\pi^\nu \mathbf{S})$. We can then determine an α_ν as in the lemma by taking the

minimum of $-v(a_i)/i$ over all $a_i t^i$ with $i < 0$ in all coefficients of $G(\mathbf{S}')$. (Note that we replace π^a with π^ε for some ε in $\mathbb{Q}_{>0}$ again and let ε approach 0.) It follows that the solution $\tilde{\mathbf{s}}'$ has coordinates in $\pi^{-\nu} R_{\alpha_\nu, 0}((t))$. Varying ν we can select an α_ν that is optimal, or close to optimal. Similar considerations apply in case (2) of the theorem.

Example 5.17. Let us return to Example 3.3 and obtain local estimates. In Example 5.7 we derived local estimates from the global one in Example 3.19. Recall that $p \neq 2$. There are two points at infinity, $[1, 1, 0]$ and $[1, -1, 0]$. With local parameter $t = 1/x$ we find the expansions $x(t) = t^{-1}$ and $y(t) = \pm t^{-1} \sqrt{1 - t^2} = \pm t^{-1} (1 - \frac{1}{2}t^2 - \frac{1}{8}t^4 - \frac{1}{16}t^6 - \dots)$. Using those in (3.4) we obtain

$$H(S) = 4^{-1} A(t) S^2 + A(t) S - A(t) + 1$$

with $A(t) = x(t)^{2p} - y(t)^{2p} = x(t)^{2p} - (x(t)^2 - 1)^p = pt^{-2p+2} + \dots$ in $1 + pt^{-2p+2} R((t))$. Then α_ν in Theorem 5.14(1) becomes $\min \left\{ \frac{1}{2p-2}, \frac{1-\nu}{2p-2}, \frac{\nu}{2p-2} \right\}$. The best possible is when $\nu = \frac{1}{2}$, so that the solution \tilde{s} that we want lies in $R_{\frac{1}{4p-4}, \frac{1}{2}}((t))$. The final estimate of Remark 5.15 also gives this if we take $\delta = 2p - 2$ and let γ approach 0. But if we let $m > 0$, extend R to R' by working inside a totally ramified of degree m over \mathbb{Q}_p , then we can apply Lemma 5.10 directly with $\alpha = \frac{1-1/m}{2p-2}$ and $b = 1$. Letting m go to infinity we find that \tilde{s} is in $R_{\frac{1}{2p-2}, 0}((t))$. Multiplying with $2^{-1}x_i(t)^p$ or $2^{-1}y_i(t)^p$ we obtain the local expansions of $\xi(\sum_{i,j} b_{i,j} x^i y^j)$ of Example 5.7 again. Remembering that every coefficient in s contains a factor p , we find that the local expansion is in $R_{\frac{1}{2p-2}, \frac{-p}{2p-2}}((t))$. This compares quite favourably with the estimates obtained in Example 3.19, which were derived directly from estimates on the global Frobenius ϕ .

6. EXAMPLES OF THE LOCAL FROBENIUS

In this section we revisit some of the examples in Section 4. In particular, we investigate the case of an hyperelliptic curve as in Example 4.4, leaving out either the point at infinity, or all the Weierstrass points. We work out those cases mostly as an illustration of the differences between leaving out as few points as possible, or opting for localizing but imposing $\phi(x) = x^{p'}$.

The reader should bear in mind that for those curves, using the closed formula as in [15] for ϕ with $\phi(x) = x^{p'}$, one can certainly get more precise information about the expansions $\xi(\phi(y))$ than by our general methods. Also, due to the low degree in y of the defining equation, the problem of computing $\phi(y)$ or its expansion for this $\phi(x)$ is of a rather different nature than in the case of a more general curve.

Let the notation and assumptions be as in Example 4.4.

Example 6.1. Let X to be the open affine corresponding to $R[x, y]/(f)$, so that we leave out only the point at infinity. Since \overline{Q} has no multiple roots, there exist polynomials $\overline{a}(x)$ of degree at most $2g$ and $\overline{b}(x)$ of degree at most $2g - 1$ in $k[x]$ such that $-\overline{a}(x)\overline{Q}'(x) + \overline{b}(x)\overline{Q}(x) = 1$ in $k[x]$. Then

$$\overline{a} \overline{f}_x + 2^{-1} y \overline{b} \overline{f}_y = 1 + \overline{b} \overline{f}$$

in $k[x, y]$. We lift \overline{a} and \overline{b} to a and b of degree at most $2g$ and $2g - 1$ in $R[x]$, so that a and $2^{-1}yb$ have a pole at infinity of order at most $4g$ and $6g - 1$ respectively.

Using those, the $H(S)$ defined in Theorem 5.8 becomes

$$\begin{aligned} H(S) &= (y(t)^{p'} + \frac{1}{2}y(t)^{p'}b^\sigma(x(t)^{p'})S)^2 - Q^\sigma(x(t)^{p'} + a^\sigma(x(t)^{p'})S) \\ &= \sum_{l=0}^{2g+1} H_l S^l. \end{aligned}$$

Choosing a parameter t centred at the missing point, the expansions $x(t)$ and $y(t)$ are in $t^{-2}R[[t]]$ and $t^{-2g-1}R[[t]]$ respectively. So H_0 is in $\pi t^{-2p'(2g+1)}R[[t]]$, H_1 is in $R^* + \pi t^{-8p'g}R[[t]]$, and H_l is in $t^{-2p'(l(2g-1)+2g+1)}R[[t]] = t^{-2p'((l-1)(2g-1)+4g)}R[[t]]$ for $l = 2, \dots, 2g+1$.

Applying Theorem 5.8, there is a unique solution \tilde{s} in $\widehat{\pi R((t))}$ of $H(S) = 0$. Moreover, Remark 5.15 gives us the following estimate on \tilde{s} . For every ν in $\mathbb{Q}_{>0}$, with $\nu < 1$, \tilde{s} is in $R_{\alpha_\nu, \frac{\nu}{e}}((t))$, where

$$\frac{1}{e} \min^+ \left\{ \frac{1}{8p'g}, \frac{(1-\nu)}{2p'(2g+1)}, \frac{\nu}{2p'(6g-1)} \right\} \leq \alpha_\nu.$$

Equating the last two entries and solving for ν gives $\tilde{\nu} = \frac{6g-1}{8g}$. With $\tilde{\alpha} = \frac{1}{e} \frac{1}{16p'g}$ we have $\alpha_{\tilde{\nu}} \geq \tilde{\alpha}$, and \tilde{s} is in $R_{\tilde{\alpha}, \frac{\tilde{\nu}}{e}}((t))$.

Note that $x(t)^{p'}$ is in $R_{\tilde{\alpha}, -2p'\tilde{\alpha}}((t))$, hence $a^\sigma(x(t)^{p'})$ is in $R_{\tilde{\alpha}_\nu, -4p'g\tilde{\alpha}}((t))$, and $\xi(\phi(x)) = x(t)^{p'} + a^\sigma(x(t)^{p'})\tilde{s}$ is in $R_{\tilde{\alpha}_\nu, \beta}((t))$ with $\beta = \min\{-2p'\tilde{\alpha}, -4p'g\tilde{\alpha} + \frac{\tilde{\nu}}{e}\}$. Similarly, $\xi(\phi(y)) = y(t)^{p'} + \frac{1}{2}b^\sigma(x(t)^{p'})\tilde{s}$ is in $R_{\tilde{\alpha}, \beta'}((t))$ with $\beta' = \min\{-p'(2g+1)\tilde{\alpha}, -2p'(2g-1)\tilde{\alpha} + \frac{\tilde{\nu}}{e}\}$.

Example 6.2. Let us now invert $2y$ as in Example 4.4, so that we work with the open affine corresponding to $R[x, y, z]/(y^2 - Q(x), 2yz - 1)$ and the missing points are the $2g+2$ Weierstrass points. The vector $H(\mathbf{S})$ defined in Theorem 5.8 has entries

$$H_2(\mathbf{S}) = (y(t)^{p'} + z(t)^{p'}S_2)^2 - Q^\sigma(x(t)^{p'}) = H_{2,0} + H_{2,1}S_2 + H_{2,2}S_2^2$$

and

$$H_3(\mathbf{S}) = 2(y(t)^{p'} + z(t)^{p'}S_2)(z(t)^{p'} - 2z(t)^{3p'}S_2 + z(t)^{p'}S_3) - 1.$$

As in Example 4.3, the first condition involves only S_2 , and by Lemma 5.12, $H_2(S_2) = 0$ has a unique solution \tilde{s}_2 in $\pi R_*((t))$. To give estimates on \tilde{s}_2 , we need to study three distinct cases.

Case 1: the missing point is the point at infinity. Then the expansions $\xi(x)$, $\xi(y)$ and $\xi(z)$ are in $t^{-2}R[[t]]$, $t^{-2g-1}R[[t]]$ and $t^{2g+1}R[[t]]$ respectively. Hence $H_{2,0}$ is in $\pi t^{-2p'(2g+1)}R[[t]]$, $H_{2,1}$ is in R^* , and $H_{2,2}$ is in $t^{2p'(2g+1)}R[[t]]$. Letting ν approach 0 and taking b large in Theorem 5.14 applied to H_2 , we get that \tilde{s}_2 is in $R_{\alpha, 0}((t))$ for $\alpha = \frac{1}{2ep'(2g+1)}$ (and of course all of its coefficients are in πR). Then $\xi(\phi(y)) = y(t)^{p'} + z(t)^{p'}\tilde{s}_2$ is in $R_{\alpha, -\frac{1}{2e}}((t))$. We also have

$$(6.3) \quad \xi(\phi(z)) = \frac{1}{2}\xi(\phi(y))^{-1} = \frac{1}{2}y(t)^{-p'} \frac{1}{1 + 2p'z(t)^{2p'}\tilde{s}_2},$$

which is in $t^{p'(2g+1)}R_{\alpha, 0}((t))$ because $z(t)^{2p'}\tilde{s}_2$ is in $\pi R_{\alpha, 0}((t))$.

Case 2: the missing point is a Weierstrass point $(a, 0)$. Here we can choose y to be the local parameter, and the expansions $\xi(x)$ and $\xi(z)$ are in $R[[t]]$ and $t^{-1}R[[t]]$ respectively. Therefore $H_{2,0}$ is in $\pi R[[t]]$, $H_{2,1}$ is in R^* , and $H_{2,2}$ is in $t^{-2p'}R[[t]]$.

Now letting ν approach $a = 1$ and taking b large in Theorem 5.14 applied to H_2 , we get that \tilde{s}_2 is in $R_{\alpha, \frac{1}{e}}((t))$ with $\alpha = \frac{1}{2e p'}$. Then $\xi(\phi(y))$ is in $t^{-p'} R_{\alpha, \frac{1}{e}}((t))$ as this contains both $y(t)^{p'}$ and $z(t)^{p'} \tilde{s}_2$. Computing $\xi(\phi(z))$ as in (6.3) we see that it is in $t^{-p'} R_{\alpha, 0}((t))$.

7. FINITE PRECISION ESTIMATES

In this section we explain how to use the methods that were discussed in Section 5 to get the cup products required in Method 2.10 up to a given precision. Here knowing c in K or \tilde{K} up to precision N means that we have an explicit \tilde{c} in K or \tilde{K} with $v(c - \tilde{c}) \geq N$. In order to simplify notation, for a in \mathbb{Q} , we shall write I_a for $\{x \text{ in } K \text{ with } v(x) \geq a\}$, so that we want to find a representative \tilde{c} of a class in K/I_N .

We place ourselves in the situation of Section 5, so fix an end \mathcal{E} and a local parameter t for the corresponding residue disc \mathcal{D} . As in that section, we write R for what might be an extension of the original R .

We shall use the images of the $R_{\alpha, \beta}((t))$ with finite precision for the coefficients.

Notation 7.1. For α, N in $\mathbb{Q}_{>0}$ and β in \mathbb{Q} , we define the set

$$(7.2) \quad S_{\alpha, \beta}^N((t)) = \left\{ \sum_m \overline{d_m} t^m \text{ with } \sum_m d_m t^m \text{ in } R_{\alpha, \beta}((t)) \right\} \subseteq S^N((t)),$$

where we take the coefficients in the quotient ring $S^N = R/I_N$.

As d_m satisfies $v(d_m) \geq -m\alpha + \beta$, its image $\overline{d_m}$ in S^N is trivial if $m \leq (\beta - N)/\alpha$.

Our basic computational problem is as follows. Given forms η and ω of the second kind with expansions

$$\eta = \sum'_m a_m t^m dt, \quad \omega = \sum'_m b_m t^m dt$$

in the local parameter t , we need to determine

$$\text{Res}_{\mathcal{E}} \omega \int \eta = \sum'_m \frac{a_m b_{-m-2}}{m+1}.$$

We want to show that this residue can be obtained up to precision N via a finite object with which we can compute. For this we shall use the quotients

$$S_{\alpha, \beta}^N((t))/t^L = S_{\alpha, \beta}^N((t))/t^L S_{\alpha, \beta}^N((t))$$

for positive exponents L . Note that we have products

$$(7.3) \quad S_{\alpha, \beta_1}^N((t))/t^L \times S_{\alpha, \beta_2}^N((t))/t^L \rightarrow S_{\alpha, \beta_1 + \beta_2}^N((t))/t^L$$

that are compatible with the products on the $R_{\alpha, \beta_i}((t))$.

Let us first analyse more closely the structure of $S_{\alpha, \beta}^N((t))/t^L$.

Lemma 7.4. *If $\sum a_m t^m$ is in $S_{\alpha, \beta}^N((t))/t^L$, then we have a_m in $I_{f(m)}/I_{g(m)}$, with $f(m) = \max(0, -\alpha m + \beta)$ and $g(m) = \max(f(m), \min(N, f(m - L)))$.*

Proof. The statement means more precisely that we have a map onto the above set which is compatible with the obvious map from $R_{\alpha, \beta}((t))$ to R which extracts the coefficient a_m . The condition with f is obvious from the lower bounds on coefficients in $R_{\alpha, \beta}((t))$. The condition with g comes from the fact that we are multiplying by t^L and quotienting out by the result. In particular, the coefficient of t^m in the

resulting class must be taken modulo the possible coefficients of t^{m-L} . Finally, $g(m)$ has to be at least as large as $f(m)$. This is because even though the precision is capped at N , if we know it is 0 to a higher precision then it is definitely known to this higher precision (and noting that $f(m) \leq f(m-L)$ because $\alpha, L > 0$). \square

For our estimates we shall assume for simplicity that $\beta_i \leq 0$. This occurs in practice and can be assumed by at worse replacing a positive β_i with 0.

Proposition 7.5. *Given N in $\mathbb{Q}_{>0}$, the map $(\omega, \eta) \mapsto \text{Res}_{\mathcal{E}} \omega \int \eta + I_N$ factors via $S_{\alpha_1, \beta_1}^{N_1}((t))/t^{L_1} \cdot dt \times S_{\alpha_2, \beta_2}^{N_2}((t))/t^{L_2} \cdot dt$ for suitable N_1, N_2 in $\mathbb{Q}_{>0}$ and positive integers L_1, L_2 .*

Proof. We observe that we have a well-defined multiplication map

$$I_{a_1}/I_{b_1} \times I_{a_2}/I_{b_2} \rightarrow I_{a_1+a_2}/I_{\min(a_1+b_2, a_2+b_1)}.$$

From this, the above lemma and the definition of the residue, it is clear that we can factor the residue as required if we have for all $m \neq -1$ that

$$\min(g_1(m) + f_2(-m-2), f_1(m) + g_2(-m-2)) \geq N + v(m+1).$$

To achieve this, we start by observing that the left hand side is greater than or equal to $f_1(m) + f_2(-m-2)$, which is independent of any choice of N_i and L_i . This is at least $\max(-\alpha_1 m + \beta_1, -\alpha_2(-m-2) + \beta_2)$ and thus, for sufficiently large $|m|$, the above inequality certainly holds independently of the choice of the L_i and N_i . We therefore need to find them so that the condition is satisfied for the finitely many remaining m .

To this end, we may first guarantee the condition after taking $N_i = \infty$ and finding appropriate L_i . Then N_i can be taken sufficiently large to make sure that the inequalities still hold. As noted before, $f_i(m) \leq f_i(m-L_i)$. Thus, for the remaining m 's our goal is to choose L_i so that

$$\min(f_1(m-L_1) + f_2(-m-2), f_1(m) + f_2(-m-2-L_2)) \geq N + v(m+1).$$

Clearly, for each fixed m , this will be achieved for sufficiently large L_1 and L_2 . \square

For computational purposes we provide a way of finding the relevant constants.

Proposition 7.6. *The following algorithm provides constants L_i and N_i satisfying the conditions of Proposition 7.5.*

- (1) Find integers $M_+ \geq 0$ and $M_- \leq -2$ with $-\alpha_1 m + \beta_1 - \log_p(|m+1|) \geq N$ for $m < M_-$ and $-\alpha_2(-m-2) + \beta_2 - \log_p(m+1) \geq N$ for $m > M_+$. Define $M_{\log} = \log_p(\max(M_+ + 1, -M_- - 1))$.
- (2) Let L_1 and L_2 be positive integers satisfying the following conditions.
 - (a) Let m_0 be the smallest integer not equal to -1 with $-\alpha_1 m_0 + \beta_1 \leq 0$. Let L_2 satisfy $-\alpha_2(-m_0-2-L_2) + \beta_2 \geq N + M_{\log}$.
 - (b) Let m_1 be the largest integer not equal to -1 with $-\alpha_2(-m_1-2) + \beta_2 \leq 0$. Let L_1 satisfy $-\alpha_1(m_1-L_1) + \beta_1 \geq N + M_{\log}$.
 - (c) If $\alpha_2 > \alpha_1$, then $-\alpha_1 M_- + \beta_1 - \alpha_2(-M_- - 2 - L_2) + \beta_2 \geq N + M_{\log}$.
 - (d) If $\alpha_1 > \alpha_2$, then $-\alpha_1(M_+ - L_1) + \beta_1 - \alpha_2(-M_+ - 2) + \beta_2 \geq N + M_{\log}$.
- (3) Take $N_1 = N_2 \geq N + M_{\log}$.

Proof. Note that the first step implies that $f_1(m) + f_2(-m-2) \geq N + \log_p |m+1|$ for all $m \neq -1$ not in $[M_-, M_+]$, as was done in the proof of Proposition 7.5. For the remaining $m \neq -1$, we may replace the term $v(m+1)$ in the required inequality

by M_{\log} , which is the maximum of $\log_p(|m+1|)$ for all such m . Our goal is then to choose

$$(7.7) \quad L_1 \text{ such that } f_1(m-L_1) + f_2(-m-2) \geq N + M_{\log},$$

$$(7.8) \quad L_2 \text{ such that } f_1(m) + f_2(-m-2-L_2) \geq N + M_{\log}$$

for all $m \neq -1$ in $[M_-, M_+]$.

First consider the smallest integer $m_0 \neq -1$ for which $f_1(m_0) = 0$. The condition on L_2 coming from (7.8) at m_0 is $f_2(-m_0-2-L_2) \geq N + M_{\log}$, which follows from (2a). For $m > m_0$ we still have $f_1(m) = 0$ while $f_2(-m-2-L_2)$ is increasing in m , so the condition (7.8) continues to hold.

Now consider (7.8) for $m < m_0$. It is then implied by

$$-\alpha_1 m + \beta_1 - \alpha_2(-m-2-L_2) + \beta_2 \geq N + M_{\log},$$

which we already imposed for $m = m_0$. This is equivalent with

$$L_2 \geq \alpha_2^{-1}((\alpha_1 - \alpha_2)m - \beta_1 - 2\alpha_2 - \beta_2 + N + M_{\log}).$$

Suppose that $\alpha_2 \leq \alpha_1$. Then this induces a weaker bound on L_2 when m decreases, so the existing condition coming from m_0 suffices. On the other hand, for $\alpha_2 > \alpha_1$ we should add an extra condition on L_2 coming from the smallest $m \neq -1$ in $[M_-, M_+]$. For this (2c) suffices.

Similarly, we may consider the largest m_1 for which $f_2(-m_1-2) = 0$. Then (7.7) for $m = m_1$ is $f_1(m_1-L_1) \geq N + M_{\log}$, which follows from (2b), and it continues to hold for all $m < m_1$. For $m > m_1$, it is implied by $-\alpha_1(m-L_1) + \beta_1 - \alpha_2(-m-2) + \beta_2 \geq N + M_{\log}$. As before, we get the extra condition (2d).

The estimate on the N_i is obvious (and probably not quite optimal). \square

The computations in Section 5 will give us the α_i and β_i for η and ω from which we can compute the parameters L_i and N_i . Then, as the computation of the local expansion of $\phi(\omega)$ does not involve a loss in precision, the residue calculation can be done using the $S_{\alpha_i, \beta_i}^{N_i}((t))/t^{L_i} \cdot dt$.

8. ALGORITHM AND IMPLEMENTATION

In this section we describe the resulting algorithm for point counting and give a rough estimate for its complexity. It is hard to give a very precise bound because this could vary significantly among different types of curves. We have also made various simplifying assumptions. We shall be using the soft \mathcal{O} notation $\tilde{\mathcal{O}}$, meaning that logarithmic factors are neglected compared with polynomial ones, so that for example $\mathcal{O}(l \log^9(l)) = \tilde{\mathcal{O}}(l)$.

We first recall some basic facts about the zeta function of C_k from [19]. As mentioned in Method 2.11, the zeta-function of C_k is obtained as $Z(T) = \frac{P_1(T)}{(1-T)(1-qT)}$, where $P_1(T) = a_0 + \dots + a_{2g}T^{2g}$ in $\mathbb{Z}[T]$ is $\det(1 - TM')$. Then $a_0 = 1$ and $a_{2g-i} = q^{g-i}a_i$ for $i = 0, \dots, g$, so that only need to know a_1, \dots, a_g . Moreover, if we write $P_1(T) = \prod_{j=1}^{2g} (1 - \alpha_j T)$ in $\mathbb{C}[T]$, then all $|\alpha_j| = q^{\frac{1}{2}}$, therefore we have $|a_i| \leq \binom{2g}{i} q^{\frac{i}{2}}$ for $i = 1, \dots, g$. Hence, it suffices to know $\alpha_1, \dots, \alpha_g$ up to precision $N = \log_p(2 \binom{2g}{g} q^{g/2})$ in order to determine their correct value in \mathbb{Z} . Asymptotically we have $N = \tilde{\mathcal{O}}(g^2 l)$.

To simplify matters, we shall assume that K is unramified over \mathbb{Q}_p and that $C \setminus X$ consists of a finite number of disjoint R sections. Not assuming this probably does not change the complexity much because one is typically working over a larger extension but at the same time the results of the computation, being Galois conjugates of one another, can be computed once for a bunch of points.

We let $q = p^l$ be the size of the residue field k . We are interested in asymptotics in l , so we shall be assuming that l is very large compared with p and g . We shall assume that other required data: Number of missing residue discs, degrees of defining functions, degrees of functions showing up in the matrix P , are linear in g . Note that there may well be situations where this is over pessimistic. For example, for all hyperelliptic curves with odd degree models we can manage with just the residue disc at infinity. We shall also not keep track on the dependence on the number of defining equations, as this tends to be very small.

To compute the zeta function we need to compute the entries in M to precision N . Since we are assuming that K is unramified we have at our disposal the results of Berthelot [3, (2.1.4) of Chapter VII], to the effect that the cup product pairing on crystalline cohomology is perfect. One further knows that Frobenius acts on integral crystalline cohomology and that $H_{\text{cr}}^1(C_k/R) \cong H_{\text{dr}}^1(C/R)$ [14, 3.4.2]. This implies that the entries of both matrices M_1 and M_2 from Method 2.10 are integral and the determinant of M_1 is invertible, provided we start with a basis for the integral de Rham cohomology of C . Thus, both matrices are still required at precision N . We ignore here the issue of finding an integral basis, but this is in practice easily done using expansions of polar parts.

Using the contents of Sections 2, 3, 5, and 7, we can now give an algorithm that computes the numerator $P_1(T)$ of the zeta function of a curve.

Algorithm 8.1.

INPUT:

- A presentation of an R -algebra $A = R[\mathbf{x}]/(f)$ that satisfies Assumption 3.5, and such that A corresponds to an open affine $X \subset C$ with $C \setminus X$ consisting of the union of disjoint sections Q_i .
- Matrices P and $\Delta^{r+1}, \dots, \Delta^n$ in $\mathbb{M}^{n, n-r}(R[\mathbf{x}])$ and $\mathbb{M}^{n-r}(R[\mathbf{x}])$ respectively, such that $\text{Jac}_{(f)} \times P \equiv \text{Id}_{n-r} + \sum_{j=r+1}^n f_j \Delta^j$ modulo p .
- For every missing point Q , the local expansions $\xi(x_i)$ at Q .
- A set of representatives $\omega_1, \dots, \omega_{2g}$ in $\Omega_{A^\dagger/R}^{1,f}$, for a basis of the image of $H_{\text{cr}}^1(C_k/R)$ inside $H_{\text{rig}}^1(\overline{X}/K)$.

Step 1: preliminary precision estimates.

- (1) Determine the required precision $N = \log_p(2 \binom{2g}{g} q^{g/2})$.
- (2) For all missing points $Q = Q_1, \dots, Q_r$ do
 - (a) Compute, in $\widehat{R((t))}[Z]$, $H(\mathbf{S})$ as defined in Theorem 5.8.
 - (b) Using the estimates from Theorem 5.14 and Remark 5.15, determine γ in $\mathbb{Q}_{>0}$ and δ in \mathbb{Q} such that the components of $\tilde{\mathbf{s}}$ lie in $R_{\gamma, \delta}((t))$.
 - (c) Using the equality $\xi(\phi(x_i)) = x_i(t)^p + \sum_{j=r+1}^n \xi(\psi(P_{i,j})) \tilde{s}_i$, determine $\tilde{\alpha}$ in $\mathbb{Q}_{>0}$ and $\tilde{\beta}_i$ in \mathbb{Q} such that each $\phi(x_i)$ has its expansion in $R_{\tilde{\alpha}, \tilde{\beta}_i}((t))$.
 - (d) For every form ω , compute α in $\mathbb{Q}_{>0}$ and β in \mathbb{Q} , such that $\phi(\omega)$ has its expansion in $R_{\alpha, \beta}((t))$.

- (e) Using those, compute, as explained in Section 7, the precision L_i in t required for the various residue computations.
- (f) If the precision in t of the $x_i(t)$ is not big enough, then exit with an error, otherwise continue.
- (g) Also compute the biggest N_i needed in the computations of the expansions of the $\phi(\omega)$.

Step 2: computation of the matrix M_1 .

Step 3: computation of the local lifts of ϕ .

For all missing points $Q = Q_1, \dots, Q_r$ do

- (1) Use Newton iteration to compute, up to precision N_i , the solution $\tilde{\mathbf{s}}$ of $H(\mathbf{S}) = 0$ with $\tilde{\mathbf{s}} \equiv 0$ modulo p .
- (2) Deduce from that the Laurent series $\xi(\phi(x_i)) = x_i(t)^p + \sum_{j=r+1}^n \xi(\psi(P_{i,j})) \tilde{s}_j$ up to the same precision.

Step 4: computation of the matrix M_2 .

For all forms ω, η in the given basis and for all missing point Q do

- (1) With notation as in Section 7, find the class of η in $S_{\alpha_1, \beta_1}^{N_1}((t))/t^{L_1} \cdot dt$, represented in the form $\sum \bar{a}_m t^m \cdot dt$.
- (2) Use the multiplication in (7.3) to get the class of $\phi(\omega)$ in $S_{\alpha, \beta}^{N_2}((t))/t^{L_2} \cdot dt$, represented in the form $\sum \bar{c}_m t^m \cdot dt$.
- (3) Compute the value $\sum_m' \frac{\bar{a}_m \bar{c}_{-m-2}}{m+1}$ of $\text{Res}_{\mathcal{E}} \phi(\omega) \int \eta$ in K/I_N .
- (4) Sum these residues over all \mathcal{E} to obtain the entry in R/I_N of M_2 corresponding to $\langle \eta, F(\omega) \rangle_U$.

Step 5: computation of the zeta function $Z(T)$.

- (1) Compute the product $M_1^{-1} M_2$ corresponding to the matrix M of the action of the σ -linear Frobenius, up to precision N .
- (2) With $q = p^r$, compute $M' = \sigma^{r-1}(M) \times \sigma^{r-2}(M) \times \dots \times \sigma(M) \times M$, the matrix of the action of the linear Frobenius, up to precision N .
- (3) Lift the coefficients $\bar{a}_1, \dots, \bar{a}_g$ of the characteristic polynomial $\sum_{i=0}^{2g} \bar{a}_i T^i$ of M' to the unique integral numbers a_i satisfying $|a_i| \leq \binom{2g}{i} q^{\frac{i}{2}}$.
- (4) Let $a_0 = 1$ and compute a_{2g-i} as $q^{g-i} a_i$ for $i = 0, \dots, g$.

OUTPUT: If the starting precision is high enough, the numerator $P_1(T)$ of the zeta function of C_k .

This algorithm has the following complexity.

Proposition 8.2. *The asymptotic complexity of this algorithm is $\tilde{O}(pl^3)$, where the \tilde{O} term depends polynomially on the genus.*

Proof. In this proof we shall also make an attempt to estimate the dependency on the genus. The computation of the matrices M_1 and M_2 involve a cup product computation, which in turn decomposes into certain residue computations as described in Section 7. We consider the computations of M_2 as these are clearly more time consuming.

The computation is “essentially” done integrally. In other words, considering the residue computation in Section 7 the integration introduces denominators, but

these are fairly mild. For the asymptotics this introduces logarithmic factors that will be swallowed by the \tilde{O} -notation.

By Section 7 the complexity of the residue computation is controlled by the parameter α of overconvergence. Indeed, if our forms are in $R_{\alpha,0}((t))$ (it is clear that from the point of view of the asymptotic complexity the parameter β may be neglected), then all residue computation may be done in the quotient rings $S_{\alpha,0}^{N_i}((t))/t^{L_i}$ of the rings defined in (7.2), where L_i is approximately N/α . and N_i is approximately N . Element in $S_{\alpha,0}^{N_i}((t))/t^{L_i}$ are Laurent series, truncated from both above and below at L_i , with coefficients in R/I_{N_i} (with some divisibility conditions for the negative coefficients and modulo lower powers of p for the positive ones). The complexity of operations in this ring, including the final residue operation, and using fast arithmetic, is $\tilde{O}(L_i)$ operations in R/I_{N_i} which is $\tilde{O}(L_i N_i)$ operations in the residue field k . As this has size p^l , operations take $\tilde{O}(\log(p^l)) = \tilde{O}(l)$, taking into account that p will occur polynomially in the complexity. We can take $L_1 = L_2 = L$ and $N_i = N$ for evaluating the complexity.

Let us now count the number of ring operations required to compute the elements of M_2 . For each residue disc we first need to compute the expansion of the $\phi(x_i)$. Here, we first need to compute the coefficients for the required equations and then carry out Newton iterations to solve them. As the convergence of the solution is with respect to the p -adic topology, the number of iterations is proportional to the log of the p -adic precision, which is N , hence ultimately to $\log(l)$. After that, we have to substitute the expressions for $\phi(x_i)$ into the forms, an operation which has a complexity of operations in $S_{\alpha,0}^N((t))/t^L$ proportional to the total degree of the defining expressions for these forms. This will be roughly quadratic in g . By our asymptotic assumptions (here we are being rather rough as we are assuming that g is small compared with $\log(l)$ and not just l), the dominant term will be the Newton iteration. Each such iteration involves a computation, controlled by the size of f , which is polynomial in g (for a plane curve, the total degree is of order \sqrt{g} , so the total number of multiplications and additions required to carry out the Newton iteration is of order $O(g\sqrt{g})$). Overall, the computation is done in about $O(g^{\mu_1} \log(l))$ operations, here for a plane curve $\mu_1 = 3/2$. This has to be further multiplied by the number of residue discs, assumed to be $O(g)$. Absorbing $\log(l)$ into the soft O , we get an overall complexity of

$$\tilde{O}(g^{\mu_1+1} L N l) = \tilde{O}(g^{\mu_1+1} L N^2 / \alpha) = \tilde{O}(g^{\mu_1+1} l N^2 / \alpha) = \tilde{O}(g^{\mu_1+5} l^3 / \alpha).$$

Thus, the overall complexity depends on the size of α . This can be estimated using Part (1) of Theorem 5.14. We assume that the entries in the matrix P will have poles of order $O(g^{\mu_2})$ at the removed points Q_i (for plane curves one may take $\mu_2 = 1/2$). The defining equation further involves applying ψ to the entries in P (see Remark 5.9), multiplying the order of pole by p . Thus, overall we can expect $\alpha = 1/O(pg^{\mu_3})$, which gives an overall complexity $\tilde{O}(g^{\mu_1+\mu_3+5} l^3 p)$ for the residue computation. Other required operations fall within this bound [15]. \square

REFERENCES

- [1] *Revêtements étales et groupe fondamental (SGA 1)*. Documents Mathématiques (Paris) [Mathematical Documents (Paris)], 3. Société Mathématique de France, Paris, 2003. Séminaire de géométrie algébrique du Bois Marie 1960–61. [Algebraic Geometry Seminar of Bois Marie 1960–61], Directed by A. Grothendieck, With two papers by M. Raynaud,

- Updated and annotated reprint of the 1971 original [Lecture Notes in Math., 224, Springer, Berlin; MR0354651 (50 #7129)].
- [2] A. Arabia. Relèvements des algèbres lisses et de leurs morphismes. *Comment. Math. Helv.*, 76(4):607–639, 2001.
 - [3] P. Berthelot. *Cohomologie cristalline des schémas de caractéristique $p > 0$* . Lecture Notes in Mathematics, Vol. 407. Springer-Verlag, Berlin, 1974.
 - [4] P. Berthelot. Finitude et pureté cohomologique en cohomologie rigide. *Invent. Math.*, 128(2):329–377, 1997. With an appendix in English by A.J. de Jong.
 - [5] W. Castryck, J. Denef, and F. Vercauteren. Computing zeta functions of nondegenerate curves. *IMRP Int. Math. Res. Pap.*, pages Art. ID 72017, 57, 2006.
 - [6] A. Chambert-Loir. Compter (rapidement) le nombre de solutions d'équations dans les corps finis. *Astérisque*, (317):Exp. No. 968, vii, 39–90, 2008. Séminaire Bourbaki. Vol. 2006/2007.
 - [7] R. Coleman. Reciprocity laws on curves. *Compositio Math.*, 72(2):205–235, 1989.
 - [8] R. Coleman. Duality for the de Rham cohomology of an abelian scheme. *Ann. Inst. Fourier (Grenoble)*, 48(5):1379–1393, 1998.
 - [9] R. Coleman and E. de Shalit. p -adic regulators on curves and special values of p -adic L -functions. *Invent. Math.*, 93(2):239–266, 1988.
 - [10] J. Denef and F. Vercauteren. Counting points on C_{ab} curves using Monsky-Washnitzer cohomology. *Finite Fields Appl.*, 12(1):78–102, 2006.
 - [11] R. Gerkmann. *The p -adic Cohomology of Varieties over Finite Fields and Applications on the Computation of Zeta Functions*. PhD thesis, Universitat Duisburg-Essen, 2003.
 - [12] A. Grothendieck and J. Dieudonné. Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas IV. *Inst. Hautes Études Sci. Publ. Math. No.*, 20,24,28,32, 1967.
 - [13] D. Harvey. Kedlaya's algorithm in larger characteristic. *Int. Math. Res. Not. IMRN*, (22):Art. ID rnm095, 29, 2007.
 - [14] L. Illusie. Report on crystalline cohomology. In *Algebraic geometry (Proc. Sympos. Pure Math., Vol. 29, Humboldt State Univ., Arcata, Calif., 1974)*, pages 459–478. Amer. Math. Soc., Providence, R.I., 1975.
 - [15] K. Kedlaya. Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology. *J. Ramanujan Math. Soc.*, 16(4):323–338, 2001.
 - [16] P. Monsky and G. Washnitzer. Formal cohomology. I. *Ann. of Math. (2)*, 88:181–217, 1968.
 - [17] T. Satoh. The canonical lift of an ordinary elliptic curve over a finite field and its point counting. *J. Ramanujan Math. Soc.*, 15(4):247–270, 2000.
 - [18] R. Schoof. Elliptic curves over finite fields and the computation of square roots mod p . *Math. Comp.*, 44(170):483–494, 1985.
 - [19] A. Weil. Numbers of solutions of equations in finite fields. *Bull. Amer. Math. Soc.*, 55:497–508, 1949.

AMNON BESSER, MATHEMATICAL INSTITUTE, 24–29 ST GILES', OXFORD OX1 3LB, UNITED KINGDOM

FACULTEIT DER EXACTE WETENSCHAPPEN, AFDELING WISKUNDE, VU UNIVERSITY AMSTERDAM, DE BOELELAAN 1081A, 1081 HV AMSTERDAM, THE NETHERLANDS

FACULTEIT DER EXACTE WETENSCHAPPEN, AFDELING WISKUNDE, VU UNIVERSITY AMSTERDAM, DE BOELELAAN 1081A, 1081 HV AMSTERDAM, THE NETHERLANDS