

Counting Points on C_{ab} Curves using Monsky-Washnitzer Cohomology

Jan Denef^a, Frederik Vercauteren^b

^a*Department of Mathematics, University of Leuven, Celestijnenlaan 200B, B-3001
Leuven-Heverlee, Belgium*

^b*Computer Science Department, University of Bristol, Woodland Road, Bristol
BS8 1UB, United Kingdom*

Abstract

We describe an algorithm to compute the zeta function of any C_{ab} curve over any finite field \mathbb{F}_{p^n} . The algorithm computes a p -adic approximation of the characteristic polynomial of Frobenius by computing in the Monsky-Washnitzer cohomology of the curve and thus generalizes Kedlaya's algorithm for hyperelliptic curves. For fixed p the asymptotic running time for a C_{ab} curve of genus g over \mathbb{F}_{p^n} is $O(g^{5+\varepsilon}n^{3+\varepsilon})$ and the space complexity is $O(g^3n^3)$.

Key words: C_{ab} curves, zeta function, Monsky-Washnitzer cohomology, cryptography, Kedlaya's algorithm

1 Introduction

One of the most important problems in computational algebraic geometry is computing zeta functions of algebraic varieties over finite fields. Although Lauder and Wan [17] showed that for fixed characteristic this problem can be solved in polynomial time, their algorithm is too slow to be practical. So far, most work has focused on Jacobians of curves, especially elliptic and hyperelliptic curves, which have applications in cryptography [15,16,24]. Due to the nature of these algorithms, there is a fundamental dichotomy depending on the characteristic of the finite field.

Email addresses: `jan.denef@wis.kuleuven.ac.be` (Jan Denef),
`frederik@cs.bris.ac.uk` (Frederik Vercauteren).

For large characteristic, the l -adic approach currently is most efficient, but only leads to a practical algorithm for elliptic curves: the Schoof-Elkies-Atkin algorithm [32] counts the number of \mathbb{F}_q -rational points in time $O((\log q)^{4+\varepsilon})$. Pila [29] generalized Schoof's algorithm to abelian varieties, but requires explicit equations for the Jacobian and the group law, which is already very difficult for genus 2. Furthermore, the time complexity of this algorithm is at least doubly exponential in the genus of the curve. Adleman and Huang [1,2] and later, Huang and Ierardi [12], improved Pila's algorithm for arbitrary curves and obtained a running time which still is exponential in the genus of the curve.

For small characteristic, p -adic methods lead to much faster algorithms. These algorithms currently come in two different flavours. The first approach is to compute an approximation of the canonical lift and the Frobenius endomorphism, from which the number of points can be easily deduced. Satoh [31] was the first to describe such an algorithm to count the number of points on an elliptic curve over \mathbb{F}_{p^n} in time $O(n^{3+\varepsilon})$ for p fixed. An overview of the many variants and optimizations of this algorithm can be found in [35]. The second approach is to compute the action of the Frobenius endomorphism on suitable cohomology groups; such as Monsky-Washnitzer cohomology by Kedlaya [14] and Dwork cohomology by Lauder and Wan [18,19].

In this paper, we develop a practical algorithm to compute the zeta function of a C_{ab} curve over any finite field of small characteristic. Our approach is similar to Kedlaya's algorithm [14] for hyperelliptic curves since we also compute in the Monsky-Washnitzer cohomology of the curve. The resulting algorithm however is much more general, since it works for any C_{ab} curve over any finite field. Furthermore, the method we use to lift the Frobenius endomorphism is valid for any non-singular affine curve. The time and space complexity for a C_{ab} curve of genus g defined over a finite field \mathbb{F}_{p^n} , are $O(g^{5+\varepsilon}n^{3+\varepsilon})$ and $O(g^3n^3)$ respectively where p is assumed to be fixed.

For special types of C_{ab} curves, two practical algorithms are currently known. The first is an algorithm by Gaudry and Gürel [11] who showed that Kedlaya's algorithm can be easily extended to superelliptic curves. The second is an extension by Ritzenthaler [30] of Mestre's algorithm [23] for ordinary hyperelliptic curves defined over a finite field of characteristic two. However, this extension is limited to ordinary non-hyperelliptic curves of genus 3. Furthermore, since the time complexity of Mestre's algorithm is exponential in the genus, any extension to genus larger than 3 will necessarily become less efficient.

The remainder of this paper is organized as follows: Section 2 recalls the formalism of Monsky-Washnitzer cohomology and Section 3 analyzes the cohomology of C_{ab} curves. Section 4 provides a detailed description of the re-

sulting algorithm and a complexity analysis. Section 5 presents running times and memory usages of an implementation in the \mathbf{C} programming language and contains an example of a $C_{3,5}$ -curve suitable for use in cryptography.

2 Monsky-Washnitzer Cohomology

In this section we briefly recall the definition of Monsky-Washnitzer cohomology as introduced by Monsky and Washnitzer [25–27]; more details can be found in the lectures by Monsky [28] and the survey by van der Put [34].

Let \mathbb{Q}_q be a degree n unramified extension of \mathbb{Q}_p with valuation ring \mathbb{Z}_q and residue field $\mathbb{Z}_q/(p\mathbb{Z}_q) = \mathbb{F}_q$. For \overline{X} a smooth affine variety over a finite field \mathbb{F}_q with coordinate ring \overline{A} , Elkik [7] showed that there always exists a smooth finitely generated \mathbb{Z}_q -algebra A such that $A/(pA) \cong \overline{A}$.

In general, A does not admit a lift of the Frobenius endomorphism \overline{F} on \overline{A} , but its p -adic completion A^∞ will. However, the de Rham cohomology of A^∞ is larger than that of A as illustrated by the following example: consider the affine line over \mathbb{F}_p , so $A = \mathbb{Z}_q[x]$, then each term in $\sum_{n=0}^{\infty} p^n x^{p^n-1} dx$ is an exact differential form, but its sum is not, since $\sum_{n=0}^{\infty} x^{p^n}$ is not in A^∞ . The main problem is that the series $\sum_{n=0}^{\infty} p^n x^{p^n-1}$ does not converge fast enough for its integral to converge as well.

Monsky and Washnitzer solve this problem by working with a subalgebra A^\dagger of A^∞ , whose elements satisfy growth conditions. This *dagger ring* or *weak completion* A^\dagger is defined as follows: write $A := \mathbb{Z}_q[x_1, \dots, x_n]/(f_1, \dots, f_m)$, then

$$A^\dagger := \mathbb{Z}_q\langle x_1, \dots, x_n \rangle^\dagger / (f_1, \dots, f_m),$$

where $\mathbb{Z}_q\langle x_1, \dots, x_n \rangle^\dagger$ consists of overconvergent power series

$$\left\{ \sum a_\alpha x^\alpha \in \mathbb{Z}_q[[x_1, \dots, x_n]] \mid \exists \gamma, \rho \in \mathbb{R}, \gamma > 0, 0 < \rho < 1, \forall \alpha : |a_\alpha|_p \leq \gamma \rho^{|\alpha|} \right\},$$

with $\alpha := (\alpha_1, \dots, \alpha_n)$, $x^\alpha := x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ and $|\alpha| := \sum_{i=1}^n \alpha_i$.

The Monsky-Washnitzer cohomology is then defined as the de Rham cohomology of $A^\dagger \otimes \mathbb{Q}_q$. Let $D^1(A^\dagger)$ be the universal module of differentials

$$D^1(A^\dagger) := (A^\dagger dx_1 + \cdots + A^\dagger dx_n) / \left(\sum_{i=1}^m A^\dagger \left(\frac{\partial f_i}{\partial x_1} dx_1 + \cdots + \frac{\partial f_i}{\partial x_n} dx_n \right) \right).$$

Let $D^i(A^\dagger) := \wedge^i D^1(A^\dagger)$ be the i -th exterior product of $D^1(A^\dagger)$ and denote with $d_i : D^i(A^\dagger) \rightarrow D^{i+1}(A^\dagger)$ the exterior differentiation. Since $d_{i+1} \circ d_i = 0$

we get the de Rham complex $D(A^\dagger)$

$$0 \longrightarrow D^0(A^\dagger) \xrightarrow{d_0} D^1(A^\dagger) \xrightarrow{d_1} D^2(A^\dagger) \xrightarrow{d_2} D^3(A^\dagger) \cdots$$

The i -th cohomology group of $D(A^\dagger)$ is defined as $H^i(\bar{A}/\mathbb{Z}_q) := \text{Ker } d_i / \text{Im } d_{i-1}$ and $H^i(\bar{A}/\mathbb{Q}_q) := H^i(\bar{A}/\mathbb{Z}_q) \otimes_{\mathbb{Z}_q} \mathbb{Q}_q$ defines the i -th Monsky-Washnitzer cohomology group.

For smooth, finitely generated \mathbb{F}_q -algebra's \bar{A} , van der Put [34] proved that the map $\bar{A} \mapsto H^\bullet(\bar{A}/\mathbb{Q}_q)$ is well defined and functorial, which justifies the notation. Replacing A^\dagger with A in the above construction of the i -th Monsky-Washnitzer cohomology group $H^i(\bar{A}/\mathbb{Q}_q)$ gives rise to the i -th algebraic de Rham cohomology group $H_{DR}^i(A/\mathbb{Q}_q)$. Unlike the Monsky-Washnitzer cohomology, the algebraic de Rham cohomology essentially depends on the algebra A and in general $H^i(\bar{A}/\mathbb{Q}_q)$ will not be isomorphic to $H_{DR}^i(A/\mathbb{Q}_q)$.

Let \mathcal{F} be a lift of the q -th power Frobenius endomorphism of \bar{A} to A^\dagger , then \mathcal{F} induces an endomorphism \mathcal{F}_* on the cohomology groups $H^i(\bar{A}/\mathbb{Q}_q)$. The main theorem of Monsky-Washnitzer cohomology is that these groups satisfy a Lefschetz fixed point formula.

THEOREM 1 (LEFSCHETZ FIXED POINT FORMULA) *Let \bar{X}/\mathbb{F}_q be a smooth affine variety of dimension d , then the number of \mathbb{F}_q -rational points on \bar{X} equals*

$$\sum_{i=0}^d (-1)^i \text{Tr} \left(q^d \mathcal{F}_*^{-1} | H^i(\bar{A}/\mathbb{Q}_q) \right).$$

3 Cohomology of C_{ab} Curves

Let \mathbb{F}_q be a finite field with $q = p^n$ elements and fix an algebraic closure $\bar{\mathbb{F}}_q$. For coprime positive integers $a, b \in \mathbb{N}$, a C_{ab} curve \bar{C} is defined by an equation of the form

$$\bar{C} : y^a + \sum_{i=1}^{a-1} \bar{f}_i(x) y^i + \bar{f}_0(x) = 0, \quad (1)$$

with $\bar{f}_i(x) \in \mathbb{F}_q[x]$ for $i = 0, \dots, a-1$, $\deg \bar{f}_0 = b$ and $a \deg \bar{f}_i + bi < ab$ for $i = 1, \dots, a-1$. Furthermore, \bar{C} should be non-singular as an affine curve. Let $\bar{C}(x, y)$ denote the polynomial $y^a + \sum_{i=1}^{a-1} \bar{f}_i(x) y^i + \bar{f}_0(x)$, then the coordinate ring of \bar{C} is $\bar{A} = \mathbb{F}_q[x, y]/(\bar{C}(x, y))$. Matsumoto [21] showed that a C_{ab} curve is always absolutely irreducible and has a unique \mathbb{F}_q -rational place \bar{P}_∞ at infinity. Furthermore, the pole divisors of the functions x and y are $a\bar{P}_\infty$ and $b\bar{P}_\infty$ respectively. Since \bar{C} is non-singular as an affine curve, the genus follows

easily from the Hurwitz formula [9] and is given by

$$g = \frac{(a-1)(b-1)}{2}.$$

Let \mathbb{Q}_q be a degree n unramified extension of \mathbb{Q}_p , with valuation ring \mathbb{Z}_q and residue field $\mathbb{Z}_q/(p\mathbb{Z}_q) = \mathbb{F}_q$. Take arbitrary lifts $f_i(x) \in \mathbb{Z}_q[x]$ of $\bar{f}_i(x)$ such that $\deg f_i = \deg \bar{f}_i$ for $i = 0, \dots, a-1$ and consider the C_{ab} curve C defined by the equation

$$C : y^a + \sum_{i=1}^{a-1} f_i(x)y^i + f_0(x) = 0. \quad (2)$$

Let $C(x, y)$ be the polynomial $y^a + \sum_{i=1}^{a-1} f_i(x)y^i + f_0(x)$, then the coordinate ring of C is $A = \mathbb{Z}_q[x, y]/(C(x, y))$.

Denote with A^\dagger the weak completion of A . Using the equation of the curve, we can represent any element of A^\dagger as a power series $\sum_{j=0}^{a-1} \sum_{i=0}^{\infty} a_{i,j} x^i y^j$. The growth condition on the dagger ring implies that there exist real numbers δ and $\epsilon > 0$ such that $\text{ord}_p(a_{i,j}) \geq \epsilon(i+j) + \delta$. Lift the p -th power Frobenius σ on \mathbb{F}_q to the Frobenius substitution Σ on \mathbb{Z}_q . Any extension of Σ to an endomorphism of A^\dagger satisfies

$$\Sigma(x) \equiv x^p \pmod{p}, \quad \Sigma(y) \equiv y^p \pmod{p}, \quad \Sigma(C(x, y)) = 0. \quad (3)$$

Let $\Sigma(x) := x^p + \delta_x Z$ and $\Sigma(y) := y^p + \delta_y Z$ with $Z \in A^\dagger$ and δ_x, δ_y polynomials over \mathbb{Z}_q which will be determined later, then Z must satisfy

$$G(Z) := \Sigma(C(x, y)) = C^\Sigma(x^p + \delta_x Z, y^p + \delta_y Z) = 0, \quad (4)$$

where $C^\Sigma(x, y)$ is obtained by applying Σ to the coefficients of $C(x, y)$. Note that $Z = 0$ is a solution of the above equation modulo p . A zero of $G(Z)$ can be computed using the Newton iteration $Z_{k+1} \leftarrow Z_k - G(Z_k)/G'(Z_k)$ only if the derivative $G'(0)$ is invertible in A^\dagger , i.e. if $G'(0) \pmod{p}$ is a unit in \mathbb{F}_q . This leads to the following condition on the polynomials δ_x and δ_y

$$\begin{aligned} G'(0) &\equiv \delta_x \frac{\partial C^\Sigma}{\partial x}(x^p, y^p) + \delta_y \frac{\partial C^\Sigma}{\partial y}(x^p, y^p) \pmod{p} \\ &\equiv \delta_x \left(\frac{\partial C}{\partial x}(x, y) \right)^p + \delta_y \left(\frac{\partial C}{\partial y}(x, y) \right)^p \pmod{p}. \end{aligned} \quad (5)$$

Since the affine curve \bar{C} is non-singular, Hilbert's Nullstellensatz implies that we can find polynomials $\bar{\alpha}, \bar{\beta}, \bar{\gamma} \in \mathbb{F}_q[x, y]$ such that

$$\bar{\alpha}(x, y) \frac{\partial \bar{C}}{\partial x}(x, y) + \bar{\beta}(x, y) \frac{\partial \bar{C}}{\partial y}(x, y) + \bar{\gamma}(x, y) \bar{C}(x, y) = 1. \quad (6)$$

Thus $G'(0)$ will be invertible in A^\dagger if δ_x and δ_y are arbitrary lifts of $\bar{\alpha}^p$ and $\bar{\beta}^p$ respectively. Note that the Newton polytopes of the polynomials $\bar{\alpha}$ and $\bar{\beta}$ determine the degrees of the coefficients of $G(Z)$, which in turn influence the rate of convergence of the power series that satisfies $G(Z) = 0$. So before we can prove a lower bound on the convergence rate of the power series $\Sigma(x)$ and $\Sigma(y)$, we need to bound the Newton polytopes of the polynomials $\bar{\alpha}$, $\bar{\beta}$ and $\bar{\gamma}$. To this end we prove the following lemma.

LEMMA 1 *Let C be a C_{ab} curve defined by the polynomial $C(x, y) \in \mathbb{Z}_q[x, y]$ and assume that C is non-singular as an affine curve. Let $\mathcal{N}(C)$ denote the Newton polytope of $C(x, y)$, then there exists polynomials $\alpha, \beta, \gamma \in \mathbb{Z}_q[x, y]$ with Newton polytopes $\mathcal{N}(\alpha) \subset 2\mathcal{N}(C)$, $\mathcal{N}(\beta) \subset 2\mathcal{N}(C)$, $\mathcal{N}(\gamma) \subset 2\mathcal{N}(C)$ such that*

$$\alpha(x, y) \frac{\partial C}{\partial x}(x, y) + \beta(x, y) \frac{\partial C}{\partial y}(x, y) + \gamma(x, y) C(x, y) = 1. \quad (7)$$

PROOF: Define the polynomials $F_0, F_1, F_2 \in \mathbb{Z}_q[X, Y]$ by

$$F_0 := \frac{\partial C}{\partial x}(X^a, Y^b), \quad F_1 := \frac{\partial C}{\partial y}(X^a, Y^b), \quad F_2 := C(X^a, Y^b).$$

Note that the Newton polytope of F_2 is given by $ab \cdot S_2$ with S_2 the standard simplex in \mathbb{R}^2 . The transformation $x \leftarrow X^a, y \leftarrow Y^b$ can thus be interpreted as a reduction to the case where the polynomial F_2 is dense. Furthermore, since C is a C_{ab} curve, we have $\deg F_0 = (b-1)a$ and $\deg F_1 = (a-1)b$. Let F_i^h be the homogenization of F_i for $i = 0, 1, 2$, then the system of homogeneous equations

$$F_0^h(X, Y, Z) = F_1^h(X, Y, Z) = F_2^h(X, Y, Z) = 0$$

has no solutions in $\mathbb{P}^2(\overline{\mathbb{F}}_q)$. Indeed, if $Z \neq 0$ then this follows immediately from the fact that C is non-singular as an affine curve. If $Z = 0$ the system of equations reduces to

$$aY^{(a-1)b} = 0, \quad b\lambda X^{a(b-1)} = 0, \quad Y^{ab} = \lambda X^{ab},$$

with λ the leading coefficient of $C(x, 0)$. Since $\gcd(a, b) = 1$ and λ is a unit in \mathbb{Z}_q , the only solution is $(0, 0)$ which does not correspond to a point in $\mathbb{P}^2(\overline{\mathbb{F}}_q)$. Applying Theorem 2 to F_0, F_1, F_2 shows that there exist polynomials $G_0, G_1, G_2 \in \mathbb{Z}_q[X, Y]$ with $\deg G_0 \leq 2ab - b - 2$, $\deg G_1 \leq 2ab - a - 2$, $\deg G_2 \leq 2ab - a - b - 2$ and

$$G_0 F_0 + G_1 F_1 + G_2 F_2 = 1. \quad (8)$$

Without loss of generality we can assume that all monomials in G_0, G_1, G_2 are of the form $X^{ai} Y^{bj}$ for $i, j \in \mathbb{N}$. Indeed, we can simply leave out all terms in

G_0, G_1, G_2 that are not of this form and equation (8) will still hold. Finally, let $\alpha, \beta, \gamma \in \mathbb{Z}_q[x, y]$ be defined by

$$\alpha(X^a, Y^b) := G_0(X, Y), \quad \beta(X^a, Y^b) := G_1(X, Y), \quad \gamma(X^a, Y^b) := G_2(X, Y),$$

then it is clear that $\mathcal{N}(\alpha) \subset 2\mathcal{N}(C)$, $\mathcal{N}(\beta) \subset 2\mathcal{N}(C)$, and $\mathcal{N}(\gamma) \subset 2\mathcal{N}(C)$, which finishes the proof. \square

THEOREM 2 *Let \mathbb{K} be a field or a discrete valuation ring and let \mathfrak{m} be the maximal ideal of \mathbb{K} . Let $f_0, \dots, f_n \in \mathbb{K}[x_1, \dots, x_n]$ with $\deg f_i = d_i$ and define*

$$\rho = d_0 + \dots + d_n - n - 1.$$

Denote with f_i^h the homogenization of f_i for $i = 0, \dots, n$. Assume that there are no points in projective n -space over the algebraic closure of \mathbb{K}/\mathfrak{m} that satisfy the system of homogeneous equations

$$f_0^h = f_1^h = \dots = f_n^h = 0.$$

Then there exists polynomials $g_0, \dots, g_n \in \mathbb{K}[x_1, \dots, x_n]$ with $\deg g_i \leq \rho + 1 - d_i$ for $i = 0, \dots, n$ such that

$$\sum_{i=0}^n g_i f_i = 1.$$

PROOF: Applying Lemma 2 to f_0^h, \dots, f_n^h shows that there exists polynomials $G_0, \dots, G_n \in \mathbb{K}[x_0, \dots, x_n]$ such that

$$x_0^{\rho+1} = G_0 f_0^h + \dots + G_n f_n^h,$$

and since $x_0^{\rho+1}$ and f_0^h, \dots, f_n^h are homogeneous, we can assume that the G_i are homogeneous and

$$\deg G_i = \rho + 1 - \deg f_i = \rho + 1 - d_i \quad \text{or} \quad G_i = 0$$

for $i = 0, \dots, n$. Substituting $x_0 = 1$ then finishes the proof. \square

LEMMA 2 *Let \mathbb{K} be a field or a discrete valuation ring and let \mathfrak{m} be the maximal ideal of \mathbb{K} . Let $h_0, \dots, h_n \in \mathbb{K}[x_0, \dots, x_n]$ be homogeneous polynomials over \mathbb{K} with $\deg h_i = d_i$ for $i = 0, \dots, n$ and let*

$$\rho = d_0 + \dots + d_n - n - 1.$$

Suppose that there are no points in projective n -space over the algebraic closure of \mathbb{K}/\mathfrak{m} that satisfy the system of homogeneous equations

$$h_0 = h_1 = \dots = h_n = 0.$$

Then any monomial of degree $\rho + 1$ over \mathbb{K} belongs to the ideal (h_0, \dots, h_n) of $\mathbb{K}[x_0, \dots, x_n]$ generated by h_0, \dots, h_n .

PROOF: The proof consists of two parts. In the first part, we assume that \mathbb{K} is a field. For any graded ring R , let h_R be the Hilbert function of R , i.e. for any $r \in \mathbb{Z}$ we have by definition

$$h_R(r) := \dim_{\mathbb{K}}\{f \in R \mid f \text{ is homogenous and } \deg f = r\}. \quad (9)$$

Let $R_i := \mathbb{K}[x_0, \dots, x_n]/(h_0, \dots, h_i)$ for $i = 0, \dots, n$ and $R_{-1} := \mathbb{K}[x_0, \dots, x_n]$, then we have that

$$h_{R_{-1}}(r) = \binom{r+n}{n}, \quad (10)$$

whenever $r+n \geq 0$ and hence $h_{R_{-1}}(r)$ is a polynomial in r for $r \geq -n$. Since the system of equations $h_0 = \dots = h_n = 0$ only has the solution $(0, \dots, 0)$ over the algebraic closure of \mathbb{K} , the dimension of R_n as a vectorspace over \mathbb{K} is finite. Hence $h_{R_n}(r) = 0$ for r big enough. Moreover, since the Krull dimension of R_n is zero, h_0, \dots, h_n is a regular sequence. This means that the homomorphism

$$R_i \rightarrow R_i : f \mapsto fh_{i+1} \quad (11)$$

is injective for $i = -1, 0, \dots, n-1$. Since the cokernel of this map is R_{i+1} we obtain that

$$h_{R_{i+1}}(r) = h_{R_i}(r) - h_{R_i}(r - d_{i+1}), \quad (12)$$

for all $r \in \mathbb{Z}$. Furthermore, since $h_{R_{-1}}$ is a polynomial of degree $n+1$ for $r \geq -n$, we conclude that for $i = 0, \dots, n-1$, h_{R_i} is a polynomial of degree $n-i$ for $r \geq -n + \sum_{j=0}^i d_j$. However, we have shown that $h_{R_n}(r) = 0$ for r big enough and thus $h_{R_n}(r) = 0$ whenever $r \geq -n + d_0 + \dots + d_n$. This finishes the proof of the first part.

In the second part of the proof, we assume that \mathbb{K} is a discrete valuation ring with maximal ideal \mathfrak{m} . Note that the first part of the proof implies that Lemma 2 holds for \mathbb{K}/\mathfrak{m} .

Let $S_r(\mathbb{K})$ be the \mathbb{K} -module of homogeneous polynomials over \mathbb{K} of degree r in the variables x_0, \dots, x_n . Consider the \mathbb{K} -linear map $W_{\mathbb{K}}$

$$\begin{aligned} W_{\mathbb{K}} : S_{\rho+1-d_0}(\mathbb{K}) \oplus \dots \oplus S_{\rho+1-d_n}(\mathbb{K}) &\rightarrow S_{\rho+1}(\mathbb{K}) \\ (g_0, \dots, g_n) &\mapsto g_0h_0 + \dots + g_nh_n, \end{aligned}$$

then we have to prove that this map is surjective. The first part of the proof shows that the map

$$W_{\mathbb{K}/\mathfrak{m}} : S_{\rho+1-d_0}(\mathbb{K}/\mathfrak{m}) \oplus \dots \oplus S_{\rho+1-d_n}(\mathbb{K}/\mathfrak{m}) \rightarrow S_{\rho+1}(\mathbb{K}/\mathfrak{m})$$

is surjective. Hence the matrix of the linear map $W_{\mathbb{K}/\mathfrak{m}}$ over the field \mathbb{K}/\mathfrak{m} has a minor of maximal dimension whose determinant is non-zero. Therefore, the

matrix of the \mathbb{K} -linear map $W_{\mathbb{K}}$ has a minor whose determinant is a unit in \mathbb{K} , which proves that $W_{\mathbb{K}}$ is surjective. \square

REMARK 1 The first part of Theorem 2, i.e. for \mathbb{K} a field, is a classical result by Macaulay [20]. The proof of Macaulay's theorem was communicated to us by Martin Sombra. Furthermore, Theorem 2 and Lemma 2 remain valid for any local ring \mathbb{K} and the proofs are exactly the same.

Lemma 1 implies that $\mathcal{N}(\bar{\alpha}) \subset 2\mathcal{N}(\bar{C})$ and $\mathcal{N}(\bar{\beta}) \subset 2\mathcal{N}(\bar{C})$. Therefore we can choose δ_x and δ_y as arbitrary lifts of $\bar{\alpha}^p$ and $\bar{\beta}^p$ such that

$$\mathcal{N}(\delta_x) \subset 2p\mathcal{N}(C) \quad \text{and} \quad \mathcal{N}(\delta_y) \subset 2p\mathcal{N}(C).$$

REMARK 2 Note that to compute $\bar{\alpha}, \bar{\beta}$ and $\bar{\gamma}$, we can simply apply linear algebra over \mathbb{F}_q , instead of using a variant of Buchberger's algorithm [4].

Using Newton iteration we can compute a solution to equation (4) as an element of the p -adic completion of A . Furthermore, a theorem by Bosch [3] implies that there exists a solution in A^\dagger . However, this theorem does not provide an explicit lower bound on the rate of convergence, which is needed in the complexity analysis. Therefore, we prove the following lemma.

LEMMA 3 *Let C be a C_{ab} curve over \mathbb{Z}_q with coordinate ring A and let $G(Z) = \sum_{k=0}^d g_k(x, y)Z^k \in A[Z]$ with $g_k(x, y) = \sum_{j=0}^{a-1} \sum_{i=0}^{d_k} a_{i,j,k}x^i y^j$. If $G(0) \equiv 0 \pmod{p}$ and $G'(0) \equiv 1 \pmod{p}$, then $G(Z) = 0$ has a unique solution $Z_0 \in A^\dagger$ with $Z_0 \equiv 0 \pmod{p}$ and $Z_0 = \sum_{j=0}^{a-1} \sum_{i=0}^{\infty} b_{i,j}x^i y^j$*

$$\text{ord}_p(b_{i,j}) \geq \frac{i}{2(b+m)},$$

where $m = \max_k \{d_k\}$.

PROOF: Let $\bar{\mathbb{Q}}_q$ be an algebraic closure of \mathbb{Q}_q and $\bar{\mathbb{Z}}_q$ the ring of integral elements of $\bar{\mathbb{Q}}_q$. Take $\epsilon_1 = p^{1/k_1}, \epsilon_2 = p^{1/k_2}, \epsilon_3 = p^{1/k_3} \in \bar{\mathbb{Z}}_q$ with $k_1, k_2, k_3 \in \mathbb{Q}_{>0}$. Consider the transformation $x' = \epsilon_1 x, y' = \epsilon_2 y$ and $Z' = \epsilon_3^{-1} Z$. Since C is a C_{ab} curve, $(y')^a$ will be an integral linear combination of $(y')^i$ and $(x')^j$ for $i = 0, \dots, a-1$ and $j = 0, \dots, b$ if

$$k_1 \geq \frac{b}{a} k_2. \tag{13}$$

After the change of variables $x = \epsilon_1^{-1} x', y = \epsilon_2^{-1} y', Z = \epsilon_3 Z'$ and multiplication with ϵ_3^{-1} , the equation $G(Z) = 0$ becomes

$$\sum_{k=0}^d \epsilon_3^{k-1} g_k(\epsilon_1^{-1} x', \epsilon_2^{-1} y')(Z')^k = 0. \tag{14}$$

Let \bar{P} be the maximal ideal of $\bar{\mathbb{Z}}_q$ containing p . Since $G'(0) \equiv 1 \pmod{p}$, we can choose k_1, k_2 such that $g_1(\epsilon_1^{-1}x', \epsilon_2^{-1}y') \in 1 + \bar{P}$. Indeed, it suffices to take k_1, k_2 large enough such that

$$\frac{d_1}{k_1} + \frac{a-1}{k_2} < 1. \quad (15)$$

The equation $G(0) \equiv 0 \pmod{p}$ implies that $\epsilon_3^{-1}g_0(\epsilon_1^{-1}x', \epsilon_2^{-1}y') \in \bar{P}$ if k_1, k_2, k_3 are chosen such that

$$\frac{d_0}{k_1} + \frac{a-1}{k_2} + \frac{1}{k_3} < 1. \quad (16)$$

Finally we can choose k_1, k_2, k_3 such that $\epsilon_3^{k-1}g_k(\epsilon_1^{-1}x', \epsilon_2^{-1}y')$ for $k = 2, \dots, d$ have integral coefficients; it suffices to take

$$\frac{k-1}{k_3} \geq \frac{d_k}{k_1} + \frac{a-1}{k_2} \quad k = 2, \dots, d. \quad (17)$$

Let $m = \max_k \{d_k\}$, then one easily verifies that

$$k_1 \geq 2(b+m), \quad k_2 = \frac{a}{b}k_1, \quad k_3 = 2,$$

satisfy inequalities (13) and (15-17).

Hensel's lemma implies that there exists a unique element $Z'_0 \in \bar{\mathbb{Z}}_q[[x', y']]$ with $Z'_0 \equiv 0 \pmod{\bar{P}}$ which satisfies equation (14). Using the equation of the curve and inequality (13), we can write Z'_0 as $\sum_{j=0}^{a-1} \sum_{i=0}^{\infty} c_{i,j} (x')^i (y')^j$ with $c_{i,j} \in \bar{\mathbb{Z}}_q$. Substituting $x' = \epsilon_1 x$, $y' = \epsilon_2 y$ in Z'_0 and multiplying with ϵ_3 we obtain the unique solution $Z_0 = \sum_{j=0}^{a-1} \sum_{i=0}^{\infty} \epsilon_1^i \epsilon_2^j \epsilon_3 c_{i,j} x^i y^j$ of $G(Z) = 0$ with $Z_0 \equiv 0 \pmod{p}$. Since $\text{ord}_p(\epsilon_1^i \epsilon_2^j \epsilon_3 c_{i,j}) \geq \text{ord}_p(\epsilon_1^i)$, we conclude that

$$\text{ord}_p(b_{i,j}) \geq \frac{i}{k_1} = \frac{i}{2(b+m)}.$$

□

Since $G(Z) = C^\Sigma(x^p + \delta_x Z, y^p + \delta_y Z)$ with $C(x, y)$ the equation of a C_{ab} curve, we can obtain a much better bound than the one given in Lemma 3.

COROLLARY 1 *With the notation of Lemma 3, suppose $\delta_x, \delta_y \in \mathbb{Z}_q[x, y]$ satisfy $\mathcal{N}(\delta_x) \subset 2p\mathcal{N}(C)$, $\mathcal{N}(\delta_y) \subset 2p\mathcal{N}(C)$ and*

$$\delta_x \left(\frac{\partial C}{\partial x}(x, y) \right)^p + \delta_y \left(\frac{\partial C}{\partial y}(x, y) \right)^p \equiv 1 \pmod{p}$$

in $\mathbb{Z}_q[x, y]/(C(x, y))$. Let $G(Z) = C^\Sigma(x^p + \delta_x Z, y^p + \delta_y Z)$, then $G(Z) = 0$ has

a unique solution $Z_0 = \sum_{j=0}^{a-1} \sum_{i=0}^{\infty} b_{i,j} x^i y^j$ in A^\dagger with $Z_0 \equiv 0 \pmod{p}$ and

$$\text{ord}_p(b_{i,j}) \geq \frac{i}{7pb}.$$

PROOF: Since $G(Z) = C^\Sigma(x^p + \delta_x Z, y^p + \delta_y Z)$, the degree in Z is $d := \max\{a, b\}$. Let $G(Z) = \sum_{k=0}^d g_k(x, y) Z^k$, then an easy calculation shows that

$$\mathcal{N}(g_k) \subset (2k+1)p\mathcal{N}(C).$$

This implies that the $d_k := \deg_x(g_k)$ in the proof of Lemma 3 are bounded by $d_k \leq (2k+1)pb$ for $k = 0, \dots, d$. We can therefore use the values

$$k_1 = 7pb, \quad k_2 = 7pa, \quad k_3 = 14/11,$$

which ends the proof of Corollary 1. \square

Lemma 3 implies that we can lift the Frobenius \bar{F} to an endomorphism \mathcal{F} on the dagger ring A^\dagger by defining $\mathcal{F} := \Sigma^n$. Before we can actually compute the zeta function using the Lefschetz fixed point theorem, we need to determine a basis of the \mathbb{Q}_q -vector space $H^1(\bar{A}/\mathbb{Q}_q)$. To this end we first construct a basis for the algebraic de Rham cohomology $H_{DR}^1(A/\mathbb{Q}_q)$ of A .

Every element of $H_{DR}^1(A/\mathbb{Q}_q)$ can be written as a linear combination of differentials of the form $x^i y^j dx$ and $x^i y^j dy$ with $i, j \in \mathbb{N}$. Using the equation of the curve we can take $0 \leq j < a$. Since $d(x^i y^{j+1})$ is exact, we conclude that $H_{DR}^1(A/\mathbb{Q}_q)$ is generated by differentials of the form $x^i y^j dx$ with $i, j \in \mathbb{N}$ and $0 < j < a$. Differentiating the equation of the curve and multiplying with $x^l y^j$ leads to

$$x^l \left(\sum_{k=1}^{a-1} f'_k(x) y^k + f'_0(x) \right) y^j dx = -x^l (a y^{a-1} + \sum_{k=1}^{a-1} f_k(x) k y^{k-1}) y^j dy.$$

Since $d(x^l (\frac{a}{a+j} y^{a+j} + \sum_{k=1}^{a-1} \frac{k}{k+j} f_k(x) y^{k+j}))$ is exact, we conclude that

$$\begin{aligned} x^l \left(\sum_{k=1}^{a-1} \frac{j}{k+j} f'_k(x) y^k + f'_0(x) \right) y^j dx \\ - l x^{l-1} \left(\frac{a}{a+j} y^a + \sum_{k=1}^{a-1} \frac{k}{k+j} f_k(x) y^k \right) y^j dx \equiv 0. \end{aligned} \quad (18)$$

The differentials $\omega_1 = x^l f'_0(x) y^j dx$ and $\omega_2 = -l x^{l-1} \frac{a}{a+j} y^{a+j} dx$ determine the pole order of the above exact differential at P_∞ . Let λ be the leading coefficient of f_0 , then the pole order of ω_1 is determined by $\lambda b x^{l+b-1} y^j dx$. Replacing y^a

by $-f_0(x) - \sum_{i=1}^{a-1} f_i(x)y^i$ in ω_2 shows that the pole order of ω_2 is determined by $l\frac{a}{a+j}\lambda x^{l+b-1}y^j dx$. Thus the pole order of (18) is equal to the pole order of

$$(b + l\frac{a}{a+j})\lambda x^{l+b-1}y^j dx.$$

Note that the leading coefficient $(b + la/(a+j))\lambda$ is non-zero. Since C is a C_{ab} curve, we have $\text{ord}_{P_\infty}(x^i) = -ia$, $\text{ord}_{P_\infty}(y^j) = -jb$ and $\text{ord}_{P_\infty}(dx) = -(a+1)$. Therefore we conclude that the exact differential (18) has a pole at P_∞ of order $a(l+b) + jb + 1$. The differential $x^i y^j dx$ with $0 < j < a$ can thus be reduced by subtracting a suitable multiple of the exact differential given in equation (18) for $l = i - b + 1$. Note that the polynomial in equation (18) is understood to be reduced using the equation of the curve. This implies that the reduction of $x^i y^j dx$ is of the form $\sum_{l=1}^{a-1} \sum_{k=0}^N a_{k,l} x^k y^l dx$ with $a_{k,l} \in \mathbb{Q}_q$ and this latter differential has a strictly smaller pole order than the former. Furthermore, taking $l = 0$ in equation (18) shows that also differentials of the form $x^{b-1} y^j dx$ with $0 < j < a$ can be reduced. This ends the proof that the algebraic de Rham cohomology $H_{DR}^1(A/\mathbb{Q}_q)$ is generated by the differentials $x^i y^j dx$ for $i = 0, \dots, b-2$ and $j = 1, \dots, a-1$. Since $\dim H_{DR}^1(A/\mathbb{Q}_q) = 2g$, these differentials also form a basis of $H_{DR}^1(A/\mathbb{Q}_q)$.

To prove that the first Monsky-Washnitzer cohomology group $H^1(\bar{A}/\mathbb{Q}_q)$ is generated by the same differential forms as the algebraic de Rham cohomology, we need to bound the denominators introduced during the reduction process.

LEMMA 4 *Let C be a C_{ab} curve over \mathbb{Z}_q and let $A = \mathbb{Z}_q[x, y]/(C(x, y))$ denote the coordinate ring of C . Suppose that*

$$x^k y^l dx = \sum_{j=1}^{a-1} \sum_{i=0}^{b-2} a_{i,j} x^i y^j dx + dS, \quad (19)$$

with $k, l \in \mathbb{N}$, $0 \leq l < a$, $a_{i,j} \in \mathbb{Q}_q$ and $S \in A \otimes \mathbb{Q}_q$. Then $p^m a_i \in \mathbb{Z}_q$, $p^m S - \beta \in A$, with $m = \lceil \log_p((k+1)a + lb) \rceil + \Delta$ and β a suitable element in \mathbb{Q}_q . Furthermore, Δ is bounded by $4(a-1)b \lceil \log_p(2a-1) \rceil$.

PROOF: The proof has two distinct parts. The first part is similar to Kedlaya's argument in [14, Lemma 3], and is based on a local analysis around the point at infinity P_∞ of the curve C . Since $\gcd(a, b) = 1$ we can find $c, d \in \mathbb{N}$, with $0 < c < b$ and $0 < d < a$ such that

$$ac - bd = -1.$$

Let $t = x^c/y^d$, then t is a local parameter at P_∞ and one verifies that

$$x = t^{-a} \left(\frac{1}{(-\lambda)^d} + \sum_{j=1}^{\infty} \alpha_j t^j \right) \quad \text{and} \quad y = t^{-b} \left(\frac{1}{(-\lambda)^c} + \sum_{j=1}^{\infty} \beta_j t^j \right), \quad (20)$$

where λ equals the leading coefficient of $C(x, 0)$ and $\alpha_j, \beta_j \in \mathbb{Z}_q$. Note that λ is a unit in \mathbb{Z}_q , since $\deg C(x, 0) = \deg \bar{C}(x, 0) = b$. Expressing x, y as functions of t we get $x^i y^j = u_{i,j} t^{-ia-jb} + \dots$ and $dx = (-uat^{-a-1} + \dots)dt$ with $u_{i,j}$ and u units in \mathbb{Z}_q . Writing $S = \sum_{j=0}^{a-1} \sum_{i=0}^N b_{i,j} x^i y^j$ with $b_{i,j} \in \mathbb{Q}_q$, $N \in \mathbb{N}$ and substituting these expressions in equation (19) gives

$$\left(\sum_{j \geq -(k+1)a-lb-1} \gamma_j t^j \right) dt = \left(\sum_{j \geq -2g-ab} \eta_j t^j \right) dt + d \left(\sum_{j \geq -Na-(a-1)b} \nu_j t^j \right),$$

with $\gamma_j \in \mathbb{Z}_q$ and $\eta_j, \nu_j \in \mathbb{Q}_q$ for all j . Integrating with respect to t and multiplying with p^m leads to an equation of the form

$$\sum_{j \geq -(k+1)a-lb} \gamma'_j t^j = \sum_{j \geq -2g-ab+1} \eta'_j t^j + \sum_{j \geq -Na-(a-1)b} p^m \nu_j t^j, \quad (21)$$

with $\gamma'_j \in \mathbb{Z}_q$ and $\eta'_j \in \mathbb{Q}_q$ for all j . Indeed, the integration process introduces denominators which become integral upon multiplication with p^m .

Equation (21) implies that $b_{i,j} = 0$ for

$$ia + jb > \max\{(k+1)a + lb, 2g + ab - 1\},$$

so it suffices to take $N = \max\{k+1+b, 2b-1\}$. Indeed, since a and b are coprime, the pole orders of $x^i y^j$ for $i, j \in \mathbb{N}$ and $0 \leq j < a$ are all different. Furthermore, we claim that equation (21) also implies that $p^m b_{i,j}$ is integral for $ia + jb \geq 2g + ab$. To see this, choose $(r, s) \in \mathbb{N} \times \mathbb{N}$ such that $b_{r,s} \neq 0$ and $ra + sb$ maximal. If $ra + sb \geq 2g + ab$, then $p^m b_{r,s}$ will be integral, since $b_{r,s} = \nu_{-ra-sb}/u_{r,s}$ with $u_{r,s}$ a unit in \mathbb{Z}_q and from equation (21) it follows that $p^m \nu_j$ is integral for $j \leq -2g - ab$. Bringing the expression for $p^m b_{r,s} x^r y^s$ to the left hand side of equation (21) and repeating the same argument shows that $p^m b_{i,j}$ is integral for $ia + jb \geq 2g + ab$.

We now turn to the second part of the proof which determines Δ . Define the differential

$$\omega = p^m x^k y^l dx - p^m d \left(\sum_{0 \leq j < a} \sum_{\substack{0 \leq i \leq N \\ ia+jb \geq 2g+ab}} b_{i,j} x^i y^j \right), \quad (22)$$

then we have just shown that ω has integral coefficients. Let C_x and C_y denote the partial derivatives of $C(x, y)$ to x and y respectively. From equation (22) it is clear that in $D^1(A \otimes \mathbb{Q}_q)$ we have

$$\begin{aligned} C_x \omega &= P_1(x, y) dy, \\ C_y \omega &= P_2(x, y) dx, \end{aligned}$$

with $P_1, P_2 \in \mathbb{Z}_q[x, y]$. Note that a priori we cannot bound the degrees of P_1 and P_2 independently of k . However, equation (19) and the definition of S shows that we can also write

$$\omega = p^m \sum_{j=1}^{a-1} \sum_{i=0}^{b-2} a_{i,j} x^i y^j dx + p^m d \left(\sum_{0 \leq j < a} \sum_{\substack{0 \leq i \leq N \\ ia+jb < 2g+ab}} b_{i,j} x^i y^j \right). \quad (23)$$

Multiplying this equation with C_x and C_y respectively leads to

$$\begin{aligned} C_x \omega &= P'_1(x, y) dy, \\ C_y \omega &= P'_2(x, y) dx, \end{aligned}$$

with P'_1, P'_2 polynomials over \mathbb{Q}_q , but of bounded degree. To make this bound explicit, we compute the pole orders of $C_x \omega$ and $C_y \omega$. From equation (23) it is clear that $-\text{ord}_{P_\infty} \omega \leq 2g + ab$. Furthermore, an easy calculation shows that $-\text{ord}_{P_\infty} C_x = (b-1)a$, $-\text{ord}_{P_\infty} C_y = (a-1)b$, $-\text{ord}_{P_\infty} dx = a+1$ and $-\text{ord}_{P_\infty} dy = b+1$. Therefore, we conclude that

$$\begin{aligned} -\text{ord}_{P_\infty} P'_1(x, y) &\leq 3ab - 2a - 2b, \\ -\text{ord}_{P_\infty} P'_2(x, y) &\leq 3ab - 2a - 2b. \end{aligned} \quad (24)$$

Using the equation of the curve, we can assume that the degree in y of P_1, P_2, P'_1 and P'_2 is smaller than a . Since $C_x \omega = P_1(x, y) dy = P'_1(x, y) dy$, we have $P_1 = P'_1$ and similarly, $P_2 = P'_2$. Thus P_1 and P_2 have integral coefficients and their pole orders are bounded by (24).

Since the curve is non-singular, Lemma 1 implies that there exist polynomials $\alpha, \beta \in \mathbb{Z}_q[x, y]$ such that $\alpha C_x + \beta C_y = 1$ in the ring A . Furthermore, the Newton polytopes of α and β satisfy

$$\mathcal{N}(\alpha) \subset 2\mathcal{N}(C) \quad \text{and} \quad \mathcal{N}(\beta) \subset 2\mathcal{N}(C).$$

Therefore, we can recover ω as

$$\omega = \alpha P_1 dy + \beta P_2 dx,$$

with $-\text{ord}_{P_\infty} \alpha P_1 \leq 5ab - 2a - 2b$ and $-\text{ord}_{P_\infty} \beta P_2 \leq 5ab - 2a - 2b$. From equation (22) also follows that

$$\omega \equiv p^m \sum_{j=1}^{a-1} \sum_{i=0}^{b-2} a_{i,j} x^i y^j dx,$$

so the $p^m a_{i,j}$ are obtained by reducing $\omega = \alpha P_1 dy + \beta P_2 dx$. To bound the denominators introduced during this second reduction stage, we analyse the explicit reduction formula (18). In every reduction step, the valua-

tion of the denominators is trivially bounded by $\lfloor \log_p(2a-1) \rfloor$ since $j < a$. The bound on the pole order of βP_2 implies that $\deg_x(\beta P_2) \leq 5b-3$, so the total number of steps to reduce $\beta P_2 dx$ is strictly less than $4(a-1)b$. Let $T(x, y) = \int \alpha(x, y) P_1(x, y) dy$, then clearly $\alpha P_1 dy \equiv -\frac{\partial T}{\partial x}(x, y) dx$ and $-\text{ord}_{P_\infty} \frac{\partial T}{\partial x}(x, y) \leq 5ab-3a-b$. This implies that the total number of steps to reduce $\alpha P_1 dy$ is also strictly less than $4(a-1)b$. Taking into account that $T(x, y)$ becomes integral upon multiplication with $\lfloor \log_p a \rfloor$, we conclude that $\Delta \leq 4(a-1)b \lfloor \log_p(2a-1) \rfloor$. \square

Lemma 4 implies that the basis for $H_{DR}^1(A/\mathbb{Q}_q)$ also generates $H^1(\bar{A}/\mathbb{Q}_q)$, since the reduction process converges. Furthermore, comparing dimensions leads to $\dim H_{DR}^1(A/\mathbb{Q}_q) = 2g = \dim H^1(\bar{A}/\mathbb{Q}_q)$, so the basis for $H_{DR}^1(A/\mathbb{Q}_q)$ is also a basis for $H^1(\bar{A}/\mathbb{Q}_q)$.

Let \tilde{C} be the unique smooth projective curve birational to C . Applying the Lefschetz fixed point theorem to \bar{C} then leads to

$$\begin{aligned} \#\tilde{C}(\mathbb{F}_{q^k}) &= 1 + \#\bar{C}(\mathbb{F}_{q^k}) \\ &= 1 + \text{Tr}\left(q^k \mathcal{F}_*^{-k} | H^0(\bar{A}/\mathbb{Q}_q)\right) - \text{Tr}\left(q^k \mathcal{F}_*^{-k} | H^1(\bar{A}/\mathbb{Q}_q)\right) \\ &= 1 + q^k - \sum_{i=1}^{2g} \alpha_i^k, \end{aligned}$$

with α_i the eigenvalues of $q\mathcal{F}_*^{-1}$ on $H^1(\bar{A}/\mathbb{Q}_q)$. The Weil conjectures [36] imply that there exist algebraic integers $\beta_1, \dots, \beta_{2g}$ such that for all $k > 0$ we have

$$\#\tilde{C}(\mathbb{F}_{q^k}) = q^k + 1 - \sum_{i=1}^{2g} \beta_i^k.$$

Furthermore, the β_i satisfy $\beta_i \beta_{g+i} = q$ and $|\beta_i| = \sqrt{q}$ for $i = 1, \dots, 2g$ where the indices are taken modulo $2g$. Comparing the zeta function using both formulae for $\#\tilde{C}(\mathbb{F}_{q^k})$ shows that $\{\alpha_i\} = \{\beta_i\}$. Since $\alpha_i \alpha_{g+i} = q$, the α_i are also the eigenvalues of \mathcal{F}_* on $H^1(\bar{A}/\mathbb{Q}_q)$. Let $\chi(t)$ be the characteristic polynomial of \mathcal{F}_* on $H^1(\bar{A}/\mathbb{Q}_q)$, then we conclude that

$$Z(\tilde{C}/\mathbb{F}_q; t) = \frac{t^{2g} \chi(1/t)}{(1-t)(1-qt)}.$$

Since $\mathcal{F}_* = \Sigma_*^n$, we can recover $\chi(t)$ as the characteristic polynomial of the norm $M_{\mathcal{F}} = \Sigma_*^{n-1}(M) \cdots \Sigma_*(M)M$ of the matrix M through which Σ_* acts on $H^1(\bar{A}/\mathbb{Q}_q)$.

4 Detailed Algorithm

In this section, we give a detailed description of the algorithm to compute the characteristic polynomial of Frobenius $\chi(t)$ and the zeta function of a smooth projective C_{ab} curve \tilde{C} of genus g over a finite field \mathbb{F}_q with $q = p^n$.

The Weil conjectures imply that $\chi(t) = t^{2g} + a_1 t^{2g-1} + \dots + a_{2g}$ with $a_i \in \mathbb{Z}$ for $i = 1, \dots, 2g$ and $q^{g-i} a_i = a_{2g-i}$, so it suffices to compute a_1, \dots, a_g . Since the a_i are the sum of $\binom{2g}{i}$ i -fold products of eigenvalues of Frobenius, we have

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

Therefore it suffices to compute the action of \mathcal{F}_* on $H^1(\bar{A}/\mathbb{Q}_q)$ modulo p^B with

$$B \geq \left\lceil \log_p \left(2 \binom{2g}{g} q^{g/2} \right) \right\rceil.$$

However, the reduction of differential forms causes a loss of precision which needs to be taken into account if we are to recover the a_1, \dots, a_g modulo p^B . Suppose we have computed

$$\Sigma(x) = \sum_{j=0}^{a-1} \sum_{i=0}^L a_{i,j} x^i y^j \pmod{p^N} \quad \text{and} \quad \Sigma(y) = \sum_{j=0}^{a-1} \sum_{i=0}^L b_{i,j} x^i y^j \pmod{p^N},$$

with not all $a_{L,j}$ and $b_{L,j}$ zero, then Corollary 1 implies $\text{ord}_p(a_{i,j}) \geq \epsilon i + \delta$ and $\text{ord}_p(b_{i,j}) \geq \epsilon i + \delta$ with $\epsilon = (7pb)^{-1}$ and $\delta = -2/7$. The maximum loss of precision will be caused by the reduction of the differential $\Sigma(x)^{b-2} \Sigma(y)^{a-1} d\Sigma(x)$. Since $\Sigma(x)$ and $\Sigma(y)$ are overconvergent, also $\Sigma(x)^k$ and $\Sigma(y)^k$ for $k \in \mathbb{N}$ will be overconvergent with the same rate of convergence, i.e. ϵ does not change. However, an easy calculation shows that δ will change according to $\delta_k = -(2k)/7$ for $k \in \mathbb{N}$. Therefore, the maximum degree in x of $\Sigma(x)^{b-2} \Sigma(y)^{a-1} d\Sigma(x) \pmod{p^N}$ is bounded by

$$U := 7pbN + 2pb(a + b).$$

Applying Lemma 4 to the differential $x^U y^{a-1} dx$ shows that N should satisfy

$$N - \left\lceil \log_p(abp(7N + 2(a + b) + 1)) \right\rceil \geq B + \Delta. \quad (25)$$

Note that this implies that N is $O(ng)$, since $B + \Delta$ itself is $O(ng)$.

REMARK 3 Since the matrix M is not necessarily defined over \mathbb{Z}_q , we could lose an extra cn bits of precision during the computation of $M_{\mathcal{F}}$, where p^c is the largest denominator appearing in M . By Corollary 1 and Lemma 4, c is bounded by $O(g \log a)$ independently of n . In theory we would therefore have to replace the bound B by $B + cn$, which does not change the complexity of

the algorithm. In practice however it turns out that the largest denominator appearing in $M_{\mathcal{F}}$ is always the same as the largest denominator appearing in M and therefore it is not necessary to increase B . This phenomenon can be heuristically explained as follows: since the eigenvalues of $\mathcal{F}_* = \Sigma_*^n$ on $H^1(\bar{A}/\mathbb{Q}_q)^-$ have non-negative p -adic valuation there is a \mathbb{Z}_q -submodule of $H^1(\bar{A}/\mathbb{Q}_q)^-$ which is stable under the action of Σ_* . For this \mathbb{Z}_q -submodule we can take for instance the canonical image of the crystalline cohomology of C over \mathbb{Z}_q . Note that the \mathbb{Z}_q -submodule generated by $x^i y dx$ for $i = 0, \dots, 2g - 1$ is not canonical and in general not stable under Σ_* . Let A_0 be the matrix that expresses $x^i y dx$ for $i = 0, \dots, 2g - 1$ in terms of a basis of such a stable \mathbb{Z}_q -submodule and let A be A_0 times a power of p such that A is a matrix over \mathbb{Z}_q which is not zero modulo p . Then $M = A^{-1}U\Sigma(A)$ where U is the matrix of Σ_* with respect to the new basis. Note that U is a matrix over \mathbb{Z}_q and that the norm of M equals $A^{-1}U\Sigma(U) \cdots \sigma^{n-1}(U)A$. Thus the loss of precision is no more than $2d$ bits where d is the p -adic valuation of $\det(A)$. If U and A are generic enough then $|c - d|$ is small. Furthermore, the bound (25) turns out to be slightly larger than what is needed and compensates for the loss of $2d$ bits.

The function `CAB_CURVE_ZETA_FUNCTION` given in Algorithm 1 computes the zeta function of a smooth projective C_{ab} curve \tilde{C} over \mathbb{F}_q with $q = p^n$. In step 1 we determine the minimal precision N that satisfies (25). Given a curve $\bar{C} : y^a + \sum_{i=1}^{a-1} \bar{f}_i(x)y^i + \bar{f}_0(x) = 0$, the function `LIFT_CAB_CURVE` takes arbitrary lifts $f_i(x) \in \mathbb{Z}_q[x]$ of $\bar{f}_i(x)$ such that $\deg f_i = \deg \bar{f}_i$ and returns the curve $C : y^a + \sum_{i=1}^{a-1} f_i(x)y^i + f_0(x) = 0$. In step 3 we compute $\bar{\alpha}, \bar{\beta}, \bar{\gamma} \in \mathbb{F}_q[x]$ satisfying equation (6) using the function `NULLSTELLENSATZ`. This function can be implemented as a variant of Buchberger's Gröbner basis algorithm [4], but Remark 2 implies that we can simply use linear algebra over \mathbb{F}_q which is much faster. In step 4 we compute $\Sigma(x) \bmod p^N$ and $\Sigma(y) \bmod p^N$ using the function `LIFT_FROBENIUS_X_Y` given in Algorithm 2. In step 3, this function takes lifts $\delta_x, \delta_y \in A := \mathbb{Z}_q[x, y]/(C)$ with $\delta_x \equiv \bar{\alpha}^p \bmod p$ and $\delta_y \equiv \bar{\beta}^p \bmod p$. The remainder of Algorithm 2 is a basic Newton iteration to determine the zero Z_s of the polynomial $G(Z) = C^{\Sigma}(x^p + \delta_x Z, y^p + \delta_y Z) \in A[Z]$ with $Z_s \equiv 0 \bmod p$.

The function `INVERT_SERIES_CAB` in step 5.3 takes as input an element $J \in A^\dagger$ with $J \equiv 1 \bmod p$ and computes a series $I \in A^\dagger$ such that $IJ \equiv 1 \bmod p^N$. Since this is an easy Newton iteration on the equation $H(Z) = JZ - 1 = 0$, we have omitted the pseudo-code.

Given $\Sigma_x \equiv \Sigma(x) \bmod p^N$ and $\Sigma_y \equiv \Sigma(y) \bmod p^N$, we compute the action of Σ_* on a basis of $H^1(\bar{A}/\mathbb{Q}_q)$ in step 5. To reduce each of the $2g$ differentials $\Sigma_x^i \Sigma_y^j d\Sigma_x$ for $i = 0, \dots, b - 2$ and $j = 1, \dots, a - 1$, we call the function `RED_MW_COHOM_CAB` described in Algorithm 3. In steps 1 and 2 we compute a polynomial $F(x, y) \in A$ such that $\Sigma_x^i \Sigma_y^j d\Sigma_x \sim F(x, y) dx \bmod p^N$, where \sim means equivalence modulo exact differentials. Step 3 computes the

ALGORITHM 1 (Cab_Curve_Zeta_Function)

INPUT: A C_{ab} curve \bar{C} over \mathbb{F}_{p^n} given by Equation (1).

OUTPUT: The zeta function $Z(\tilde{C}/\mathbb{F}_{p^n}; t)$.

1. $B \geq \lceil \log_p \left(2 \binom{2g}{g} q^{g/2} \right) \rceil$;
 $N - \lceil \log_p(abp(7N + 2(a + b) + 1)) \rceil \geq B + \Delta$;
 2. $g = (a - 1)(b - 1)/2$; $C = \text{Lift_Cab_Curve}(\bar{C})$;
 3. $(\bar{\alpha}, \bar{\beta}, \bar{\gamma}) = \text{Nullstellensatz}(\frac{\partial \bar{C}}{\partial x}, \frac{\partial \bar{C}}{\partial y}, \bar{C})$;
 4. $(\Sigma_x, \Sigma_y) = \text{Lift_Frobenius_x_y}(\bar{\alpha}, \bar{\beta}, C, N)$;
 5. For $j = 1$ To $a - 1$ Do
 - 5.1. For $i = 0$ To $b - 2$ Do
 - 5.1.1. $V_{i,j} = \text{Red_MW_Cohom_Cab}(\Sigma_x^i \Sigma_y^j, \Sigma_x, C, B, N)$;
 - 5.1.2. $I = (b - 1)(j - 1) + i$;
 - 5.1.3. For $k = 0$ To $2g - 1$ Do $M[I][k] = V_{i,j}[k]$;
 6. $M_{\mathcal{F}} \equiv \Sigma^{n-1}(M) \cdots \Sigma(M)M \pmod{2^B}$;
 7. $\chi(t) = \text{Characteristic_Pol}(M_{\mathcal{F}}) \pmod{2^B}$;
 8. For $i = 0$ To g Do
 - 8.1. If $\text{Coeff}(\chi, 2g - i) > \binom{2g}{i} q^{i/2}$ Then
 $\text{Coeff}(\chi, 2g - i) - = 2^B$;
 - 8.2. $\text{Coeff}(\chi, i) = q^{g-i} \text{Coeff}(\chi, 2g - i)$;
 9. Return $Z(\tilde{C}/\mathbb{F}_{p^n}; t) = \frac{t^{2g} \chi(1/t)}{(1 - t)(1 - qt)}$.
-

reduction of $F(x, y) dx$ on the basis of $H^1(\bar{A}/\mathbb{Q}_q)$ by subtracting exact differentials until $\deg_x F(x, y) < b - 1$. In step 3.1 we call INDEX_MAX_POL_ORDER which returns the pair (i, j) such that $i > b - 2$ and $x^i y^j dx$ is the term in $F(x, y) dx$ with maximum pole order at P_∞ . Steps 3.2 to 3.8 compute a suitable multiple of the exact differential given in (18) and reduce $F(x, y) dx$. Finally, in step 5 we return the coefficient vector of $F(x, y) dx$ which is correct modulo p^B .

The result of step 5 of Algorithm 1 is an approximation modulo p^B of the matrix M through which Σ_* acts on $H^1(\bar{A}/\mathbb{Q}_q)$. In step 6 we compute its norm $M_{\mathcal{F}}$ as $M_{\mathcal{F}} \equiv \Sigma^{n-1}(M) \cdots \Sigma(M)M \pmod{p^B}$. In steps 7 and 8 we recover the characteristic polynomial of Frobenius from the first g coefficients of the characteristic polynomial of $M_{\mathcal{F}}$ and in step 9 we return $Z(\tilde{C}/\mathbb{F}_{p^n}; t)$.

ALGORITHM 2 (`Lift_Frobenius_x_y`)

INPUT: Polynomials $\bar{\alpha}, \bar{\beta} \in \mathbb{F}_{p^n}[x, y]$, C_{ab} curve C over \mathbb{Z}_q with $\bar{\alpha} \frac{\partial \bar{C}}{\partial x} + \bar{\beta} \frac{\partial \bar{C}}{\partial y} \equiv 1 \pmod{p}$, precision N .

OUTPUT: Polynomials $\Sigma_x, \Sigma_y \in \mathbb{Z}_q[x, y]/(C)$ with $\Sigma_x \equiv \Sigma(x) \pmod{p^N}$ and $\Sigma_y \equiv \Sigma(y) \pmod{p^N}$.

1. $S = \lceil \log_2 N \rceil + 1$; $T = N$;
 2. For $i = S$ Down To 1 Do $P[i] = T$; $T = \lceil T/2 \rceil$;
 3. $\delta_x \equiv \bar{\alpha}^p \pmod{p}$; $\delta_y \equiv \bar{\beta}^p \pmod{p}$; $Z_s = 0$;
 4. $G(Z) \equiv C^\Sigma(x^p + \delta_x Z, y^p + \delta_y Z)$; $H(Z) \equiv \frac{\partial G}{\partial Z}(Z)$;
 5. For $i = 2$ To B Do
 - 5.1. $D_i \equiv G(Z_s) \pmod{p^{P[i]}}$;
 - 5.2. $N_i \equiv H(Z_s) \pmod{p^{P[i-1]}}$;
 - 5.3. $I_i = \text{Invert_Series_Cab}(N_i, C, P[i-1])$;
 - 5.4. $\Delta_i \equiv (D_i/p^{P[i-1]}) \cdot I_i \pmod{p^{P[i-1]}}$;
 - 5.5. $Z_s \equiv Z_s - p^{P[i-1]} \Delta_i \pmod{p^{P[i]}}$;
 6. Return $\Sigma_x \equiv x^p + \delta_x Z_s \pmod{p^N}$, $\Sigma_y \equiv y^p + \delta_y Z_s \pmod{p^N}$.
-

5 Complexity Analysis

In this section we analyse the time and space requirements of Algorithm 1 for a smooth projective C_{ab} curve \tilde{C} over \mathbb{F}_q with $q = p^n$, assuming p is fixed.

Given a precision N , we represent elements of $\mathbb{Z}_q/(p^N \mathbb{Z}_q)$ as polynomials over $\mathbb{Z}_p/(p^N \mathbb{Z}_p)$ modulo a monic sparse irreducible polynomial $f(t) \in \mathbb{Z}_p[t]$. Each element of this ring requires $O(nN)$ space, so we can perform multiplication and inversion in time $O(n^\mu N^\mu)$, where μ is constant such that multiplying two m -bit integers takes $O(m^\mu)$ time. The coordinate ring $A_N = (\mathbb{Z}_q/(p^N \mathbb{Z}_q))[x, y]/(C)$ consists of bivariate polynomials $\sum_{j=0}^{a-1} \sum_{i=0}^L a_{i,j} x^i y^j$ with $a_{i,j} \in \mathbb{Z}_q/(p^N \mathbb{Z}_q)$. Corollary 1 implies that for $\Sigma(x) \pmod{p^N}$ and $\Sigma(y) \pmod{p^N}$ the maximum degree L is bounded by $pb(7N + 2)$, so each of these objects takes $O(abnN^2)$ space. Furthermore, the valuation of the coefficients $a_{i,j}$ grows linearly with i , which implies that the size of $\Sigma(x)^i \Sigma(y)^j \pmod{p^N}$ also is $O(abnN^2)$. Packing these objects in a large integer, we can therefore perform multiplication and inversion in time $O((abnN^2)^\mu)$.

In step 1 of Algorithm 1 we determine N satisfying inequality (25), which

ALGORITHM 3 (Red_MW_Cohom_Cab)

INPUT: Polynomials $D, \Sigma_x \in A := \mathbb{Z}_q[x, y]/(C)$, C_{ab} curve C given by equation $y^a + \sum_{i=1}^{a-1} f_i(x)y^i + f_0(x) = 0$, precision B and N .

OUTPUT: Coefficient vector V of polynomial $R \in \mathbb{Q}_q[x, y]/(C)$ with $\deg_x R(x, y) < b - 1$ and $R(x, y)dx \sim D(x, y)d\Sigma_x \pmod{2^B}$.

1. $E(x, y) \equiv \int D(x, y) \frac{\partial \Sigma_x}{\partial y} dy \pmod{p^N}$;
 2. $F(x, y) \equiv D(x, y) \frac{\partial \Sigma_x}{\partial x} - \frac{\partial E}{\partial x}(x, y) \pmod{p^N}$;
 3. **While** ($\deg_x F(x, y) > b - 2$) **Do**
 - 3.1. $(i, j) = \text{Index_Max_Pole_Order}(F(x, y))$;
 - 3.2. $l = i - b + 1$;
 - 3.3. $\Delta_x \equiv x \sum_{k=1}^{a-1} \frac{j}{k+j} f'_k(x) y^k + x f'_0(x) \pmod{p^N}$;
 - 3.4. $\Delta_y \equiv -l \frac{a}{a+j} y^a - l \sum_{k=1}^{a-1} \frac{k}{k+j} f_k(x) y^k \pmod{p^N}$;
 - 3.5. $\Delta \equiv y^j x^{l-1} (\Delta_x + \Delta_y) \pmod{(p^N, C)}$;
 - 3.6. $\gamma = \text{Coeff}(\Delta, i, j)$;
 - 3.7. $\nu = \text{Coeff}(F(x, y), i, j)$;
 - 3.8. $F(x, y) \equiv F(x, y) - \nu \gamma^{-1} \Delta \pmod{p^N}$;
 4. **For** $i = 0$ **To** $b - 2$ **Do**
 - 4.1. **For** $j = 1$ **To** $a - 1$ **Do**
 - 4.1.1. $V[(b - 1)(j - 1) + i] \equiv \text{Coeff}(F(x, y), i, j)$;
 5. **Return** $V \pmod{p^B}$;
-

implies that N is $O(gn)$. The function `NULLSTELLENSATZ` in step 3 consists of solving a system of linear equations over \mathbb{F}_q of dimension $O(ab)$ and can thus be solved in $O((ab)^3 n^\mu)$ time using Gaussian elimination. In step 4 we compute $\Sigma(x) \pmod{p^N}$ and $\Sigma(y) \pmod{p^N}$ using the function `LIFT_FROBENIUS_X_Y`. The complexity of Algorithm 2 is determined by step 5 which is a Newton iteration on the polynomial $G(Z) = C^\Sigma(x^p + \delta_x Z, y^p + \delta_y Z)$. Since the precision doubles in every iteration, we conclude that the complexity is determined by the last iteration. Using Horner's rule we need $O(\max\{a, b\})$ multiplications of objects of size $O(abnN^2)$, so the total time complexity of Algorithm 2 is $O(\max\{a, b\}(abnN^2)^\mu)$ and the space complexity is $O(abnN^2)$.

Step 5 of Algorithm 1 computes an approximation of the matrix M through which Σ_* acts on $H^1(\overline{A}/\mathbb{Q}_q)$ using `RED_MW_COHOM_CAB` to reduce the $2g$

differential forms $\Sigma_x^i \Sigma_y^j d\Sigma_x$ for $i = 0, \dots, b-2$ and $j = 1, \dots, a-1$. Computing these differentials takes $O(g)$ multiplications of objects of size $O(abnN^2)$ and thus requires $O(g(abnN^2)^\mu)$ time. The complexity of Algorithm 3 which is used to reduce each of these differentials, is determined by step 4. For each of the $O(abN)$ terms in $F(x, y)$ we need to perform $O(g)$ multiplications of elements in $\mathbb{Z}_q/(p^N\mathbb{Z}_q)$, so the overall time complexity of Algorithm 3 is $O(gabN(nN)^\mu)$. Since we need to reduce $O(g)$ differentials, the complexity of step 5 of Algorithm 1 is

$$O(g(abnN^2)^\mu + g^2abN(nN)^\mu).$$

In step 6 we need to determine the norm of a $2g \times 2g$ matrix M over \mathbb{Q}_q as $\Sigma^{n-1}(M) \cdots \Sigma(M)M$, using a simple square and multiply algorithm suggested by Kedlaya [14]. This algorithm needs $O(\log n)$ multiplications of $2g \times 2g$ matrices at a cost of $O(g^3(nN)^\mu \log n)$ time and $O(g^2 \log n)$ applications of powers of Σ which takes $O(g^2n(nN)^\mu \log n)$ time if we precompute $\Sigma^{2^i}(t)$ for $i = 0, \dots, \lfloor \log_2 n \rfloor$. The overall time complexity of step 6 thus becomes $O((n+g)g^2(nN)^\mu \log n)$.

Finally, we need to compute the characteristic polynomial of a $2g \times 2g$ matrix over \mathbb{Q}_q , which can be done using the classical algorithm based on the Hessenberg form [5, Section 2.2.4]. The complexity of this algorithm is $O(g^3)$ ring operations or $O(g^3(nN)^\mu)$ time.

Finally, note that $O(ab)$ is $O(g)$ since $2g = (a-1)(b-1)$ and that N is $O(gn)$ due to inequality (25). This finishes the proof of the following theorem if we take $\mu = 1 + \varepsilon$ with $\varepsilon \in \mathbb{R}_{>0}$.

THEOREM 3 *There exists a deterministic algorithm to compute the zeta function of a smooth C_{ab} curve of genus g defined over \mathbb{F}_{p^n} which requires $O(g^{5+\varepsilon}n^{3+\varepsilon})$ bit-operations and $O(g^3n^3)$ space for p fixed.*

6 Implementation and Numerical Results

In this section we present running times of an implementation of Algorithm 1 in the C programming language and give an example of a C_{ab} curve whose Jacobian has almost prime group order.

The basic operations on integers modulo 2^N for $N \leq 256$ are implemented in assembly language. Elements of $\mathbb{Z}_q/(2^N\mathbb{Z}_q)$ are represented as polynomials over $\mathbb{Z}/(2^N\mathbb{Z})$ modulo a degree n irreducible polynomial, which is either a trinomial or a pentanomial. For multiplication of elements in $\mathbb{Z}_q/(2^N\mathbb{Z}_q)$, polynomials

over $\mathbb{Z}_q/(2^N\mathbb{Z}_q)$ and Laurent series over $\mathbb{Z}_q/(2^N\mathbb{Z}_q)[x]$ we used a combination of Karatsuba [13] and Toom [33] multiplication.

Table 1 contains running times and memory usages of our algorithm for $C_{3,4}$ and $C_{3,5}$ curves over various finite fields of characteristic 2. These results were obtained on an AMD XP 1700+ processor running Linux Redhat 7.1. Note that the field degrees are chosen such that gn is constant across each row.

Table 1

Running time (s) and memory usage (MB) for genus 3 and 4 C_{ab} curves over \mathbb{F}_{2^n}

gn	$C_{3,4}$ curves				$C_{3,5}$ curves			
	Lift \mathcal{F}	Matrix	Total	Mem	Lift \mathcal{F}	Matrix	Total	Mem
120	364	995	1360	51.8	573	1866	2440	62.8
144	727	3345	4073	63.1	1111	3814	4926	111
168	982	3994	4978	129	1543	5549	7094	147
192	1562	5732	7297	163	2645	9445	12093	185
240	3966	11937	15909	307	6038	21035	27078	347
288	6935	23097	30044	526	11157	33618	44786	595

To illustrate the effectiveness of the algorithm, we give an example of a C_{ab} curve whose Jacobian has almost prime group order. The correctness of this result is easily proved by multiplying a random divisor with the given group order and verifying that the result is principal, i.e. is the zero element in the Jacobian $J_{\tilde{C}}(\mathbb{F}_q)$. The given curve is non-supersingular, since the coefficient a_g of $\chi(t)$ is odd [10]. Furthermore, the curve also withstands the MOV-FR attack [8,22].

Let $\mathbb{F}_{2^{47}}$ be defined as $\mathbb{F}_2[w]/\overline{P}(w)$ with $\overline{P}(w) = w^{47} + w^5 + 1$ and consider the random $C_{3,5}$ curve \overline{C}_4 of genus 4 defined by

$$y^3 + \left(\sum_{i=0}^1 f_{2,i}x^i\right)y^2 + \left(\sum_{i=0}^3 f_{1,i}x^i\right)y + \sum_{i=0}^5 f_{0,i}x^i = 0,$$

where

$$\begin{array}{lll} f_{0,0} = 341D2BD9C6D0 & f_{0,1} = 2EA67315735F & f_{0,2} = 26011B32E639 \\ f_{0,3} = 7042D4480690 & f_{0,4} = 3AFFCD251865 & f_{0,5} = 74F966B7C1A5 \\ f_{1,0} = 552915B9D5BD & f_{1,1} = 0DAD08369AD4 & f_{1,2} = 674BB4A87953 \\ f_{1,3} = 232A2568DAF0 & f_{2,0} = 489EC7EDF33C & f_{2,1} = 1C8AB33409FA \end{array}$$

The group order of the Jacobian $J_{\tilde{C}_4}$ of \overline{C}_4 over $\mathbb{F}_{2^{47}}$ is

$$\#J_{\tilde{C}_4} = 2 \cdot 196159431833516415148362696405532740472648081387048967549,$$

where the last factor is prime. The coefficients a_1 , a_2 , a_3 and a_4 of the characteristic polynomial of Frobenius $\chi(t) = t^8 + \sum_{i=1}^4 a_i t^{8-i} + \sum_{i=1}^4 q^i a_{4-i} t^{4-i}$ are given by

$$\begin{aligned} a_1 &= 1867333, \\ a_2 &= 30460424199008, \\ a_3 &= 1107508027267882794005, \\ a_4 &= 9346402437739386469819573567. \end{aligned}$$

7 Conclusion

In this paper we described a new algorithm to compute the zeta function of a C_{ab} curve over a finite field of small characteristic. For a C_{ab} curve of genus g over \mathbb{F}_{p^n} , the algorithm requires $O(g^{5+\varepsilon}n^{3+\varepsilon})$ bit-operations and $O(g^3n^3)$ space for p fixed. This algorithm currently is the only practical algorithm to compute the zeta function of an arbitrary C_{ab} curve.

The key idea is a novel method, different from the one we used in [6], to lift the Frobenius endomorphism to the dagger ring of a non-singular affine curve. Furthermore, the technique used to prove a tight bound on the convergence rate of the resulting power series remains valid for any non-singular affine curve. Only the explicit description of a basis for the first Monsky-Washnitzer cohomology group and the reduction formulae to express any differential on this basis are limited to C_{ab} curves.

A first implementation in the C programming language shows that cryptographic sizes are now feasible for any genus g . However, since the algorithm is very general, it runs about $20g$ times slower than the algorithm for hyperelliptic curves [6]. For example, the order of a 168-bit Jacobian of a $C_{3,4}$ curve can be computed in 1.4 hours.

References

- [1] L. M. Adleman and M.-D. Huang. Counting rational points on curves and abelian varieties over finite fields. In H. Cohen, editor, *Algorithmic Number Theory Symposium, Proceedings ANTS-II*, volume 1122 of *Lecture Notes in Comput. Sci.*, pages 1–16. Springer, Berlin, 1996.

- [2] L. M. Adleman and M.-D. Huang. Counting points on curves and abelian varieties over finite fields. *J. Symbolic Comput.*, 32(3):171–189, 2001.
- [3] S. Bosch. A rigid analytic version of M. Artin’s theorem on analytic equations. *Math. Ann.*, 255(3):395–404, 1981.
- [4] B. Buchberger. A theoretical basis for the reduction of polynomials to canonical forms. *ACM SIGSAM Bull.*, 10(3):19–29, 1976.
- [5] H. Cohen. *A course in computational algebraic number theory*. Springer-Verlag, Berlin, 1993.
- [6] J. Denef and F. Vercauteren. An extension of Kedlaya’s algorithm to hyperelliptic curves in characteristic 2. Accepted for publication in *J. Cryptology*, November 2002.
- [7] R. Elkik. Solutions d’équations à coefficients dans un anneau hensélien. *Ann. Sci. École Norm. Sup. (4)*, 6:553–603 (1974), 1973.
- [8] G. Frey and H.-G. Rück. A remark concerning m -divisibility and the discrete logarithm in the divisor class group of curves. *Math. Comp.*, 62(206):865–874, 1994.
- [9] W. Fulton. *Algebraic curves. An introduction to algebraic geometry*. W. A. Benjamin, Inc., New York-Amsterdam, 1969.
- [10] S. D. Galbraith. Supersingular curves in cryptography. In C. Boyd, editor, *Advances in Cryptology, Proceedings Asiacrypt 2001*, volume 2248 of *Lecture Notes in Comput. Sci.*, pages 495–513. Springer, Berlin, 2001.
- [11] P. Gaudry and N. Gürel. An extension of Kedlaya’s point-counting algorithm to superelliptic curves. In C. Boyd, editor, *Advances in Cryptology, Proceedings Asiacrypt 2001*, volume 2248 of *Lecture Notes in Comput. Sci.*, pages 480–494. Springer, Berlin, 2001.
- [12] M.-D. Huang and D. Ierardi. Counting points on curves over finite fields. *J. Symbolic Comput.*, 25(1):1–21, 1998.
- [13] A. A. Karatsuba and Y. Ofman. Multiplication of multidigit numbers on automata. *Soviet Physics Doklady*, 7:595–596, 1963.
- [14] K. S. Kedlaya. Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology. *J. Ramanujan Math. Soc.*, 16(4):323–338, 2001.
- [15] N. Koblitz. Elliptic curve cryptosystems. *Math. Comp.*, 48(177):203–209, 1987.
- [16] N. Koblitz. Hyperelliptic cryptosystems. *J. Cryptology*, 1(3):139–150, 1989.
- [17] A. Lauder and Wan. D. Counting points on varieties over finite fields of small characteristic. In J.P. Buhler and P. Stevenhagen, editors, *Algorithmic Number Theory: Lattices, Number Fields, Curves and Cryptography*, Mathematical Sciences Research Institute Publications, 2002. To appear.

- [18] A. G. B. Lauder and D. Wan. Computing zeta functions of Artin-Schreier curves over finite fields. *LMS J. Comput. Math.*, 5:34–55 (electronic), 2002.
- [19] A. G. B. Lauder and D. Wan. Computing zeta functions of Artin-Schreier curves over finite fields II. To appear in a special issue of the Journal of Complexity, 2002.
- [20] F. Macaulay. On some formulas in elimination. *Proc. London Math. Soc.*, 3:3–27, 1902.
- [21] R. Matsumoto. The C_{ab} curve. Available at <http://www.rmatsumoto.org/cab.ps>.
- [22] A. J. Menezes, T. Okamoto, and S. A. Vanstone. Reducing elliptic curve logarithms to logarithms in a finite field. *IEEE Trans. Inform. Theory*, 39(5):1639–1646, 1993.
- [23] J.-F. Mestre. Algorithmes pour compter des points en petite caractéristique en genre 1 and 2. Available at <http://www.math.univ-rennes1.fr/crypto/2001-02/mestre.ps>.
- [24] V. S. Miller. Use of elliptic curves in cryptography. In H. C. Williams, editor, *Advances in Cryptology, Proceedings Crypto 1985*, volume 218 of *Lecture Notes in Comput. Sci.*, pages 417–426. Springer, Berlin, 1986.
- [25] P. Monsky and G. Washnitzer. Formal cohomology. I. *Ann. of Math. (2)*, 88:181–217, 1968.
- [26] P. Monsky. Formal cohomology. II. The cohomology sequence of a pair. *Ann. of Math. (2)*, 88:218–238, 1968.
- [27] P. Monsky. Formal cohomology. III. Fixed point theorems. *Ann. of Math. (2)*, 93:315–343, 1971.
- [28] P. Monsky. *p-adic analysis and zeta functions*. Kinokuniya Book-Store Co. Ltd., Tokyo, 1970.
- [29] J. Pila. Frobenius maps of abelian varieties and finding roots of unity in finite fields. *Math. Comp.*, 55(192):745–763, 1990.
- [30] C. Ritzenthaler. Methode A.G.M. pour les courbes ordinaires de genre 3 non hyperelliptiques sur F_{2^N} . Available at <http://arxiv.org/abs/math.NT/0303072>, 2003.
- [31] 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.
- [32] R. Schoof. Counting points on elliptic curves over finite fields. *J. Théor. Nombres Bordeaux*, 7(1):219–254, 1995. Les Dix-huitièmes Journées Arithmétiques (Bordeaux, 1993).
- [33] A. L. Toom. The complexity of a scheme of functional elements simulating the multiplication of integers. *Dokl. Akad. Nauk SSSR*, 150:496–498, 1963.

- [34] M. van der Put. The cohomology of Monsky and Washnitzer. *Mém. Soc. Math. France (N.S.)*, 23:4, 33–59, 1986. Introductions aux cohomologies p -adiques (Luminy, 1984).
- [35] F. Vercauteren. *Computing Zeta Functions of Curves over Finite Fields*. PhD thesis, Katholieke Universiteit Leuven, November 2003. Available at <http://www.cs.bris.ac.uk/~frederik/>.
- [36] A. Weil. Numbers of solutions of equations in finite fields. *Bull. Amer. Math. Soc.*, 55:497–508, 1949.