An Extension of Kedlaya's Algorithm to Hyperelliptic Curves in Characteristic 2

Jan Denef[1] and Frederik Vercauteren[2,3] ⋆

[1] Department of Mathematics
University of Leuven
Celestijnenlaan 200B, B-3001 Leuven-Heverlee, Belgium
jan.denef@wis.kuleuven.ac.be

[2] Department of Electrical Engineering
University of Leuven
Kasteelpark Arenberg 10, B-3001 Leuven-Heverlee, Belgium
frederik.vercauteren@esat.kuleuven.ac.be

[3] Computer Science Department
University of Bristol
Woodland Road, Bristol BS8 1UB, United Kingdom
frederik@cs.bris.ac.uk

Abstract. We present an algorithm for computing the zeta function of an arbitrary hyperelliptic curve over a finite field $\mathbb{F}_q$ of characteristic 2, thereby extending the algorithm of Kedlaya for odd characteristic. For a genus g hyperelliptic curve defined over $\mathbb{F}_{2^n}$, the average-case time complexity is $O(g^{4+\varepsilon}n^{3+\varepsilon})$ and the average-case space complexity is $O(g^3n^3)$, whereas the worst-case time and space complexities are $O(g^{5+\varepsilon}n^{3+\varepsilon})$ and $O(g^4n^3)$ respectively.

Keywords: Hyperelliptic curves, cryptography, Kedlaya's algorithm, Monsky-Washnitzer cohomology

1 Introduction

Computing the zeta function of abelian varieties over finite fields is one of the most important problems in computational algebraic geometry and has many applications [29], e.g. the construction of cryptosystems based on Jacobians of curves. The most important systems use elliptic curves as introduced by Miller [22] and Koblitz [16] or hyperelliptic curves which were proposed by Koblitz [17]. More general, but less practical systems work in the Jacobian of superelliptic curves [12] and of $\mathcal{C}_{ab}$ curves [1].

The problem of counting the number of points on elliptic curves over finite fields of any characteristic can be solved in polynomial time using Schoof's algorithm [33] and its improvements due to Atkin [2] and Elkies [7]. An excellent

⋆ F.W.O. research assistant, sponsored by the Fund for Scientific Research - Flanders (Belgium).

account of the resulting SEA-algorithm can be found in [3] and [20]. For finite fields of small characteristic, Satoh [30] described an algorithm based on p-adic methods which is asymptotically faster than the SEA-algorithm. Skjernaa [34] and Fouquet, Gaudry and Harley [9] extended the algorithm to characteristic 2 and Vercauteren [36] presented a memory efficient version. Mestre proposed a variant of Satoh's algorithm based on the Arithmetic-Geometric Mean, which has the same asymptotic behaviour as [36], but is faster by some constant. Recently, Satoh, Skjernaa and Taguchi [31] described an algorithm which has a better complexity than all previous algorithms, but requires some precomputations. A nice overview of all these variants can be found in the survey by Satoh [32].

The equivalent problem for higher genus curves seems to be much more difficult. Pila [28] described a theoretical generalization of Schoof's approach, but the algorithm is not practical, not even for genus 2 curves as shown by Gaudry and Harley [13]. An extension of Satoh's method to higher genus curves needs the Serre-Tate canonical lift of the Jacobian of the curve, which need not be a Jacobian itself and thus is difficult to compute with. The AGM method does generalize to hyperelliptic curves, but currently only the genus 2 case is practical.

Recently Kedlaya [15] described a p-adic algorithm to compute the zeta function of hyperelliptic curves over finite fields of small *odd* characteristic, using the theory of Monsky-Washnitzer cohomology. The running time of the algorithm is $O(g^{4+\varepsilon}n^{3+\varepsilon})$ for a hyperelliptic curve of genus g over $\mathbb{F}_{p^n}$. The algorithm readily generalizes to superelliptic curves as shown by Gaudry and Gurel [14].

A related approach by Lauder and Wan [18] is based on Dwork's proof of the rationality of the zeta function and leads to a polynomial time algorithm for computing the zeta function of an arbitrary variety over a finite field. Note that Wan [37] suggested the use of p-adic methods, including the method of Dwork and Monsky, already several years ago. Despite the polynomial time complexity of the Lauder and Wan algorithm, it is not practical for cryptographical sizes. Using Dwork cohomology, Lauder and Wan [19] adapted their original algorithm for the special case of Artin-Schreier curves, resulting in an $O(g^{5+\varepsilon}n^{3+\varepsilon})$ time algorithm. In [6], we described an extension of Kedlaya's algorithm to Artin-Schreier curves in characteristic 2 which has the same time complexity $O(g^{5+\varepsilon}n^{3+\varepsilon})$.

In this paper we extend Kedlaya's algorithm to *arbitrary* hyperelliptic curves defined over a finite field of characteristic 2. For a genus g hyperelliptic curve defined over $\mathbb{F}_{2^n}$, the average-case time complexity is $O(g^{4+\varepsilon}n^{3+\varepsilon})$ and the average-case space complexity is $O(g^3n^3)$, whereas the worst-case time and space complexities are $O(g^{5+\varepsilon}n^{3+\varepsilon})$ and $O(g^4n^3)$ respectively.

Furthermore, a first implementation of this algorithm in the `C` programming language shows that cryptographical sizes are now feasible for any genus g. For instance, computing the order of a 160-bit Jacobian of a hyperelliptic curve of genus 2, 3 or 4 takes less than 100 seconds.

The remainder of the paper is organized as follows: after recalling the formalism of Monsky-Washnitzer cohomology in Section 2, we study cohomology of hyperelliptic curves over finite fields and show how to extend Kedlaya's algorithm to characteristic 2 in Section 3. Section 4 contains a ready to implement description of the resulting algorithm and a detailed complexity analysis. In Section 5, we present running times and memory usages of an implementation of this algorithm in the `C` programming language and we give a few examples of hyperelliptic curves suitable for use in cryptography.

2 Monsky-Washnitzer Cohomology

In this section we briefly recall the definition and main properties of Monsky-Washnitzer cohomology. More details can be found in the seminal papers by Monsky and Washnitzer [24–26], the lectures by Monsky [27] and the survey by van der Put [35].

Let $\overline{X}$ be a smooth affine variety over a finite field $k := \mathbb{F}_q$ with coordinate ring $\overline{A}$. Let R denote a complete discrete valuation ring with uniformizer π, residue field $R/\pi R = k$ and fraction field K of characteristic 0. Elkik [8] showed that there always exists a smooth finitely generated R-algebra A such that $A/\pi A \cong \overline{A}$. To compute the zeta function of $\overline{X}$ we need to lift the Frobenius endomorphism $\overline{F}$ on $\overline{A}$ to the R-algebra A, but in general this is not possible. Note that for elliptic curves, Satoh solves this problem by using the Serre-Tate canonical lift which does admit a lift of the Frobenius endomorphism. To remedy this difficulty one could work with the π-adic completion A^∞ of A. But again we run into difficulties since the de Rham cohomology of A^∞ is larger than that of A. As an example, consider the affine line over $\mathbb{F}_p$, so $A = R[x]$, 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 $A := R[x_1, \ldots, x_n]/(f_1, \ldots, f_m)$, then

$$A^\dagger := R\langle x_1, \ldots, x_n \rangle^\dagger / (f_1, \ldots, f_m), \tag{1}$$

where $R\langle x_1, \ldots, x_n \rangle^\dagger$ consists of power series

$$\left\{ \sum a_\alpha x^\alpha \in R[[x_1, \ldots, x_n]] \mid \exists C, \rho \in \mathbb{R}, C > 0, 0 < \rho < 1, \forall \alpha : |a_\alpha| \le C \rho^{|\alpha|} \right\}, \tag{2}$$

with $\alpha := (\alpha_1, \ldots, \alpha_n)$, $x^\alpha := x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ and $|\alpha| := \sum_{i=0}^{n} \alpha_i$. Equivalently, $R\langle x_1, \ldots, x_n \rangle^\dagger$ can be defined as the set of overconvergent power series, i.e. elements of $R[[x_1, \ldots, x_n]]$ that converge in a polydisc

$$\{(x_1, \ldots, x_n) \in K^n \mid |x_1| \le \rho_1, \ldots, |x_n| \le \rho_n\} \tag{3}$$

with all $\rho_i > 1$. A homomorphic image of $R\langle x_1, \ldots, x_n \rangle^\dagger$ is called a weakly complete finetely generated (w.c.f.g.) algebra over R. The ring $A^\dagger$ clearly is a w.c.f.g. algebra and furthermore satisfies $A^\dagger / \pi A^\dagger = \overline{A}$ and is flat over R. An algebra which satisfies these three properties is called a *lift* of $\overline{A}$. One can show that if $\overline{A}$ is smooth and finitely generated, there always exists a lift $A^\dagger$ of $\overline{A}$ and that every lift of $\overline{A}$ is R-isomorphic to $A^\dagger$. Furthermore, let $\overline{B}/k$ be smooth and finitely generated, with lift $B^\dagger$ and let $\overline{G} : \overline{A} \to \overline{B}$ be a morphism of k-algebra's, then there exists an R-homomorphism $G : A^\dagger \to B^\dagger$ lifting $\overline{G}$. This last property implies that we can lift the q-power Frobenius from $\overline{A}$ to $A^\dagger$.

For $A^\dagger$ we can define the universal module $D^1(A^\dagger)$ of differentials

$$D^1(A^\dagger) := (A^\dagger\ dx_1 + \cdots + A^\dagger\ dx_n)/(\sum_{i=1}^{m} A^\dagger(\frac{\partial f_i}{\partial x_1}\ dx_1 + \cdots + \frac{\partial f_i}{\partial x_n}\ dx_n)). \quad (4)$$

Let $D^i(A^\dagger) := \bigwedge^i D^1(A^\dagger)$ be the i-th exterior product of $D^1(A^\dagger)$ and denote with $d_i : D^i(A^\dagger) \to D^{i+1}(A^\dagger)$ the exterior differentiation. Since $d_{i+1} \circ d_i = 0$ we get the de Rham complex $D(A^\dagger)$

$$0 \longrightarrow D^0(A^\dagger) \xrightarrow{d_0} D^1(A^\dagger) \xrightarrow{d_1} D^2(A^\dagger) \xrightarrow{d_2} D^3(A^\dagger) \cdots \quad (5)$$

The i-th cohomology group of $D(A^\dagger)$ is defined as $H^i(\overline{A}/R) := \mathrm{Ker}\ d_i/\mathrm{Im}\ d_{i-1}$ and $H^i(\overline{A}/K) := H^i(\overline{A}/R) \otimes_R K$ finally defines the i-th Monsky-Washnitzer cohomology group. One can prove that for smooth, finitely generated k-algebra's $\overline{A}$ the map $\overline{A} \mapsto H^\bullet(\overline{A}/K)$ is well defined and functorial, which justifies the notation. Let F be a lift of the q-power Frobenius endomorphism of $\overline{A}$ to $A^\dagger$, then F induces an endomorphism F_* on the cohomology groups. The main theorem of Monsky-Washnitzer cohomology is that the $H^i(\overline{A}/K)$ satisfy a Lefschetz fixed point formula.

Theorem 1 (Lefschetz fixed point formula) *Let $\overline{X}/\mathbb{F}_q$ be a smooth affine variety of dimension d, then the number of $\mathbb{F}_q$-rational points on $\overline{X}$ equals*

$$\sum_{i=0}^{d} (-1)^i \mathrm{Tr}\left(q^d F_*^{-1} | H^i(\overline{A}/K)\right). \quad (6)$$

3 Cohomology of Hyperelliptic Curves

3.1 Overview of Kedlaya's Construction

Let $\mathbb{F}_q$ be a finite field with $q = p^n$ elements and fix an algebraic closure $\overline{\mathbb{F}}_q$. Throughout this section we will assume that p is a small odd prime. Let $\overline{Q}(x)$ be a monic polynomial of degree $2g+1$ over $\mathbb{F}_q$ without repeated roots and let $\overline{C}$ be the affine hyperelliptic curve defined by the equation $y^2 = \overline{Q}(x)$. Kedlaya does not work with the curve $\overline{C}$ itself, but with the affine curve $\overline{C}'$ which is obtained from $\overline{C}$ by removing the locus of $y = 0$, i.e. the points $(\overline{\xi}_i, 0) \in \overline{\mathbb{F}}_q \times \overline{\mathbb{F}}_q$ where $\overline{\xi}_i$ is a zero of $\overline{Q}(x)$. The coordinate ring $\overline{A}$ of $\overline{C}'$ is clearly given by $\mathbb{F}_q[x, y, y^{-1}]/(y^2 - \overline{Q}(x))$. It is not really necessary to work with the curve $\overline{C}'$ instead of $\overline{C}$, but in practice it is more efficient to do so.

Let K be a degree n unramified extension of $\mathbb{Q}_p$, with valuation ring R, such that $R/pR = \mathbb{F}_q$. Take any monic lift $Q(x) \in R[x]$ of $\overline{Q}(x)$ and let C be the smooth affine hyperelliptic curve defined by $y^2 = Q(x)$. Let C' be the curve obtained from C by removing the locus of $y = 0$. Then the coordinate ring of C' is $A = R[x, y, y^{-1}]/(y^2 - Q(x))$. Let $A^\dagger$ denote the weak completion of A. Since $\overline{F} = \overline{\sigma}^n$, with $\overline{\sigma}$ the p-power Frobenius, it is sufficient to lift $\overline{\sigma}$ to an endomorphism σ of $A^\dagger$. It is natural to define σ as the Frobenius substitution on R and to extend it to $A^\dagger$ by mapping x to $x^\sigma := x^p$ and y to y^σ with

$$y^\sigma := y^p \left(1 + \frac{Q(x)^\sigma - Q(x)^p}{Q(x)^p}\right)^{1/2} = y^p \sum_{i=0}^{\infty} \binom{1/2}{i} \frac{(Q(x)^\sigma - Q(x)^p)^i}{y^{2pi}}. \tag{7}$$

An easy calculation shows that $\mathrm{ord}_p \binom{1/2}{i} \geq 0$ which implies that y^σ is an element of $A^\dagger$, since p divides $Q(x)^\sigma - Q(x)^p$. Note that it is essential that y^{-1} is an element of $A^\dagger$, which explains why we compute with C' instead of C. By choosing a different lift of $\overline{F}$ one can avoid working with C' altogether, but this will be less efficient since the analogue of the Newton iteration (7) is more involved.

Since C' has dimension one, the only non-trivial Monsky-Washnitzer cohomology groups are $H^0(\overline{A}/K)$ and $H^1(A/K)$. Finding a basis for $H^0(\overline{A}/K)$ is easy since by definition $H^0(\overline{A}/K) := \mathrm{Ker}\, d_0$, with d_0 the derivation from $A^\dagger$ into $D^1 A^\dagger$, which implies that $H^0(\overline{A}/K)$ is a one dimensional K-vectorspace. The case $H^1(\overline{A}/K)$ is more difficult and proceeds in two steps. Kedlaya first constructs a basis for the algebraic de Rham cohomology of A and devises reduction formulae to express any differential form on this basis. Then he proves that these formulae lead to a convergent process when applied to the de Rham cohomology of $A^\dagger$, i.e. $H^1(\overline{A}/K)$ and concludes that the basis for the algebraic de Rham cohomology also is a basis for $H^1(\overline{A}/K)$.

The de Rham cohomology of A splits into eigenspaces under the hyperelliptic involution: a positive eigenspace generated by $x^i/y^2\, dx$ for $i = 0, \ldots, 2g$ and a negative eigenspace generated by $x^i/y\, dx$ for $i = 0, \ldots, 2g-1$. Using the equation of the curve, any differential form can be written as $\sum_{k=-B_U}^{B_L} \sum_{i=0}^{2g} a_{i,k} x^i/y^k\, dx$ with $a_{i,k} \in K$ and $B_U, B_L \in \mathbb{N}$. Since $Q(x)$ has no repeated roots, we can always write an arbitrary polynomial $P(x) \in K[x]$ as $P(x) = S(x)Q(x) + T(x)Q'(x)$. Using the fact that $d(T(x)/y^{s-2})$ is exact, one obtains

$$\frac{P(x)}{y^s}\, dx \equiv \left(S(x) + \frac{2T'(x)}{(s-2)}\right) \frac{dx}{y^{s-2}}, \tag{8}$$

where $\equiv$ means equality modulo exact differentials. This congruence can be used to reduce everything to the case $k = 1$ and $k = 2$. A differential $P(x)/y\, dx$ with $\deg P(x) = m \geq 2g$ can be reduced by repeatedly subtracting suitable multiples of the exact differential $d(x^{i-2g} y)$ for $i = m, \ldots 2g$. Finally, it is clear that the differential $P(x)/y^2\, dx$ is congruent to $(P(x) \bmod Q(x))/y^2\, dx$ modulo exact differentials.

Kedlaya then proves two lemmata which bound the denominators introduced during the above reduction process. The result is as follows: let $A(x) \in R[x]$ be a polynomial of degree at most $2g$, then for $k \in \mathbb{Z}$ the reduction of $A(x)y^{2k+1}\, dx$ becomes integral upon multiplication by $p^{\lfloor \log_p(2|k|+1) \rfloor}$. This implies that the reduction process converges for elements of $D^1(A^\dagger)$.

The final step in the algorithm consists of computing the action induced by σ on a basis of $H^1(\overline{A}/K)$. Using the Lefschetz fixed point theorem, Kedlaya shows that it is sufficient to compute the matrix M through which σ acts on the anti-invariant part $H^1(\overline{A}/K)^-$ of $H^1(\overline{A}/K)$. Therefore we only need to compute $(x^i/y\,dx)^\sigma = px^{p(i+1)-1}/y^\sigma\,dx$ for $i = 0, \ldots, 2g-1$. Using the aforementioned reduction process we express $(x^i/y\,dx)^\sigma$ on the basis of $H^1(\overline{A}/K)^-$ and compute the matrix M. The characteristic polynomial of Frobenius can then be recovered from the coefficients of the characteristic polynomial of the matrix $MM^\sigma \cdots M^{\sigma^{n-1}}$ through which the Frobenius $F = \sigma^n$ acts on $H^1(\overline{A}/K)^-$.

3.2 Cohomology of Hyperelliptic Curves over $\mathbb{F}_{2^n}$

Let $\mathbb{F}_q$ be a finite field with $q = 2^n$ elements and fix an algebraic closure $\overline{\mathbb{F}}_q$. Consider the smooth affine hyperelliptic curve $\overline{C}$ of genus g defined by the equation

$$\overline{C} : y^2 + \overline{h}(x)y = \overline{f}(x)\,, \tag{9}$$

with $\overline{h}(x), \overline{f}(x) \in \mathbb{F}_q[x]$, $\overline{f}(x)$ monic of degree $2g+1$ and $\deg \overline{h}(x) \le g$. Write $\overline{h}(x)$ as $\overline{c} \cdot \prod_{i=0}^{s}(x - \overline{\theta}_i)^{m_i}$ with $\overline{\theta}_i \in \overline{\mathbb{F}}_q$, $\overline{c} \in \mathbb{F}_q \setminus \{0\}$ the leading coefficient of $\overline{h}(x)$ and define $\overline{H}(x) = \prod_{i=0}^{s}(x - \overline{\theta}_i) \in \mathbb{F}_q[x]$. If $h(x)$ is a constant, we set $\overline{H}(x) = 1$. Without loss of generality we can assume that $\overline{H}(x) \,|\, \overline{f}(x)$. Indeed, the isomorphism defined by $x \mapsto x$ and $y \mapsto y + \sum_{i=0}^{s} \overline{b}_i x^i$ transforms the curve in

$$y^2 + \overline{h}(x)y = \overline{f}(x) - \sum_{i=0}^{s} \overline{b}_i^2 x^{2i} - \overline{h}(x) \sum_{i=0}^{s} \overline{b}_i x^i\,. \tag{10}$$

The polynomial $\overline{H}(x)$ will divide the right hand side of the above equation if and only if $\overline{f}(\overline{\theta}_j) = \sum_{i=0}^{s} \overline{b}_i^2 \cdot \overline{\theta}_j^{2i}$ for $j = 0, \ldots, s$. This is a system of linear equations in the indeterminates $\overline{b}_i^2$ and its determinant is a Vandermonde determinant. Since the $\overline{\theta}_j$ are the zeros of a polynomial defined over $\mathbb{F}_q$, the system of equations is invariant under the q-th power Frobenius automorphism $\overline{F}$ and it follows that the $\overline{b}_i^2$ and therefore the $\overline{b}_i$ are elements of $\mathbb{F}_q$. We conclude that we can always assume that $\overline{H}(x) \,|\, \overline{f}(x)$.

Let $\overline{\pi} : \overline{C}(\overline{\mathbb{F}}_q) \to \mathbb{A}^1(\overline{\mathbb{F}}_q)$ be the projection on the x-axis. It is clear that $\overline{\pi}$ ramifies at the points $(\overline{\theta}_i, 0) \in \overline{\mathbb{F}}_q \times \overline{\mathbb{F}}_q$ for $i = 0, \ldots, s$ where $\overline{H}(\overline{\theta}_i) = 0$. Note that the ordinate of these points is zero, since we assumed that $\overline{H}(x) \,|\, \overline{f}(x)$. Let $\overline{C}'$ be the curve obtained from $\overline{C}$ by removing the ramification points $(\overline{\theta}_i, 0)$ for $i = 0, \ldots, s$. Then the coordinate ring $\overline{A}$ of $\overline{C}'$ is

$$\mathbb{F}_q[x, y, \overline{H}(x)^{-1}]/(y^2 + \overline{h}(x)y - \overline{f}(x)) \tag{11}$$

Analogous to the odd characteristic case, it is not really necessary to work with the affine curve $\overline{C}'$ instead of $\overline{C}$, but again it turns out to be more efficient. The coordinate ring of $\overline{C}'$ contains the inverse of $\overline{H}(x)$ which will enable us to choose a particular lift of the Frobenius endomorphism $\overline{F}$ of $\overline{A}$.

Let K be a degree n unramified extension of $\mathbb{Q}_2$ with valuation ring R and residue field $R/2R = \mathbb{F}_q$. Write $\overline{h}(x) = \overline{c} \cdot \prod_{i=0}^{r} \overline{P}_i(x)^{t_i}$, where the $\overline{P}_i(x)$ are monic irreducible over $\mathbb{F}_q$. Let $D = \max_i t_i$, then $\overline{h}(x)$ divides $\overline{H}(x)^D$, since we have the identity $\overline{H}(x) = \prod_{i=0}^{r} \overline{P}_i(x)$. Lift $\overline{P}_i(x)$ for $i = 0, \ldots, r$ to any monic polynomial $P_i(x) \in R[x]$. Define $H(x) = \prod_{i=0}^{r} P_i(x)$ and $h(x) = c \cdot \prod_{i=0}^{r} P_i(x)^{t_i}$, with c any lift of $\overline{c}$ to R. Since $\overline{H}(x)$ divides $\overline{f}(x)$ we can define $Q_{\overline{f}}(x) = \overline{f}(x)/\overline{H}(x)$. Let $Q_f(x) \in R[x]$ be any monic lift of $Q_{\overline{f}}(x)$ and finally set $f(x) = H(x)Q_f(x)$. The result is that we have now constructed a lift C of the curve $\overline{C}$ to R defined by the equation

$$C : y^2 + h(x)y = f(x)\,. \tag{12}$$

Note that due to the careful construction of C we have the following properties: $H(x)\,|\,h(x)$, $H(x)\,|\,f(x)$ and $h(x)\,|\,H(x)^D$. Let K^{ur} be the maximal unramified extension of K with valuation ring R^{ur}. For $k = 0, \ldots, s$, let θ_k be the zeros of $H(x)$ and note that these are units in R^{ur}. Furthermore, let $\pi : C(\overline{K}) \to \mathbb{A}^1(\overline{K})$ be the projection on the x-axis, then the $(\theta_k, 0)$ are ramification points of π.

Consider the curve C' obtained from C by deleting the ramification points $(\theta_k, 0)$ for $k = 0, \ldots, s$, then the coordinate ring A of C' is

$$R[x, y, H(x)^{-1}]/(y^2 + h(x)y - f(x)) \tag{13}$$

and there exists an involution $\imath$ on A which sends x to x and y to $-y - h(x)$. Let $A^\dagger$ denote the weak completion of A. Using the equation of the curve, we can represent any element of $A^\dagger$ as a series $\sum_{i=-\infty}^{+\infty}(U_i(x) + V_i(x)y)S(x)^i$, with the degree of $U_i(x)$ and $V_i(x)$ smaller that the degree of $S(x)$, where $S(x) = H(x)$ if $\deg H(x) > 0$ and $S(x) = x$ if $H(x) = 1$. The growth condition on the dagger ring implies that there exist real numbers δ and $\epsilon > 0$ such that $\mathrm{ord}_2(U_i(x)) \geq \epsilon \cdot |i| + \delta$ and $\mathrm{ord}_2(V_i(x)) \geq \epsilon \cdot |i+1| + \delta$, where $\mathrm{ord}_2(P(x))$ is defined as $\min_j \mathrm{ord}_2(p_j)$ for $P(x) = \sum p_j x^j \in K[x]$.

Lift the 2-power Frobenius $\overline{\sigma}$ on $\mathbb{F}_q$ to the Frobenius substitution σ on R. We extend σ to an endomorphism of $A^\dagger$ by mapping x to x^2 and y to y^σ, with

$$(y^\sigma)^2 + h(x)^\sigma\, y^\sigma - f(x)^\sigma = 0 \quad \text{and} \quad y^\sigma \equiv y^2 \bmod 2. \tag{14}$$

Using Newton lifting we can compute the solution to the above equations as an element of the 2-adic completion of A as

$$W_{k+1} \equiv W_k - \frac{W_k^2 + h(x)^\sigma\, W_k - f(x)^\sigma}{2W_k + h(x)^\sigma} \bmod 2^{k+1}. \tag{15}$$

The only remaining difficulty in the above Newton iteration is that we have to invert $2W_k + h(x)^\sigma$ in the ring A^∞. Since $h(x)\,|\,H(x)^D$, it makes sense to define $Q_H(x) := H(x)^D/h(x)$ and we clearly have $1/h(x) = Q_H(x)/H(x)^D$. We can now compute the inverse of $2W_k + h(x)^\sigma$ as

$$\frac{Q_H(x)^2}{H(x)^{2D} \cdot \left(1 + \frac{Q_H(x)^2(2W_k + h(x)^\sigma - h(x)^2)}{H(x)^{2D}}\right)}. \tag{16}$$

Note that $h(x)^\sigma \equiv h(x)^2 \bmod 2$, which implies that the denominator in the above formula is invertible in A^∞. Contrary to the odd characteristic case it is not immediately clear that the solution $W := \lim_{k\to+\infty} W_k$ is an element of $A^\dagger$. The existence of such a solution follows immediately from a theorem by Bosch [4], but since we need an explicit estimate of the rate of convergence, we prove the following lemma.

Lemma 1 *For $k \geq 1$, let $W_k = \sum_{i=-L_k}^{A_k} U_i(x)S(x)^i + \sum_{i=-L_k}^{B_k} V_i(x)S(x)^i y \in A$, with $S(x) = H(x)$ if $\deg H(x) > 0$ and $S(x) = x$ if $H(x) = 1$, satisfy*

$$W_k^2 + h(x)^\sigma W_k - f(x)^\sigma \equiv 0 \bmod 2^k \quad \textit{and} \quad W_k \equiv y^2 \bmod 2 \tag{17}$$

with $\mathrm{ord}_2(U_i(x)) < k$ for $-L_k \leq i \leq A_k$ and $\mathrm{ord}_2(V_i(x)) < k$ for $-L_k \leq i \leq B_k$. Then A_k, B_k and L_k can be bounded for $k \geq 1$ as

$$\begin{aligned} A_k &\leq 2k(d_S^f - 2d_S^h) + 2d_S^h, \\ B_k &\leq 2(k-1)(d_S^f - 2d_S^h) + (d_S^f - d_S^h), \\ L_k &\leq 4kD - 2D, \end{aligned} \tag{18}$$

with $d_S^f := \deg f(x)/\deg S(x)$ and $d_S^h := \deg h(x)/\deg S(x)$.

`Proof:` The lemma is clearly valid for $k = 1$ since $W_1 = f(x) - h(x)y$ which implies that $A_1 \leq d_S^f$, $B_1 \leq d_S^h$ and $L_1 \leq 0$. The Newton iteration (15) can be rewritten as

$$h(x)^2 W_{k+1} \equiv -W_k^2 + (h(x)^2 - h(x)^\sigma) W_k + f(x)^\sigma \bmod 2^{k+1}. \tag{19}$$

Let $\alpha_k(x) := \sum_{i=-L_k}^{A_k} U_i(x)S(x)^i$ and $\beta_k(x) := \sum_{l=-L_k}^{B_k} V_i(x)S(x)^i$ such that $W_k = \alpha_k(x) + \beta_k(x)y$. Note that $W_k \equiv W_{k-1} \bmod 2^{k-1}$, so we can define

$$\Delta_{\alpha,k}(x) := \frac{\alpha_k(x) - \alpha_{k-1}(x)}{2^{k-1}} \qquad \text{and} \qquad \Delta_{\beta,k}(x) := \frac{\beta_k(x) - \beta_{k-1}(x)}{2^{k-1}}, \tag{20}$$

for $k \geq 1$ and $\Delta_{\alpha,0}(x) := \Delta_{\beta,0}(x) := 0$. It is clear that W_k can be written as

$$W_k = \Delta_{\alpha,1} + 2\Delta_{\alpha,2} + \cdots + 2^{k-1}\Delta_{\alpha,k} + y\left(\Delta_{\beta,1} + 2\Delta_{\beta,2} + \cdots + 2^{k-1}\Delta_{\beta,k}\right). \tag{21}$$

Plugging this into the Newton iteration gives the following equation

$$\begin{aligned} h(x)^2 W_{k+1} \equiv &- \sum_{\substack{1\leq i<j \\ i+j-1<k+1}} 2^{i+j-1}\left(\Delta_{\alpha,i}\Delta_{\alpha,j} + (f(x) - h(x)y)\,\Delta_{\beta,i}\Delta_{\beta,j}\right) \\ &- y \sum_{i+j-1<k+1} 2^{i+j-1}\Delta_{\alpha,i}\Delta_{\beta,j} - \sum_{2(i-1)<k+1} 2^{2(i-1)}\left(\Delta_{\alpha,i}^2 + (f(x) - h(x)y)\Delta_{\beta,i}^2\right) \\ &+ (h(x)^2 - h(x)^\sigma) \sum_{i<k+1} 2^{i-1}(\Delta_{\alpha,i} + \Delta_{\beta,i}y) + f(x)^\sigma \bmod 2^{k+1}. \end{aligned} \tag{22}$$

By definition $Q_H(x)h(x) = H(x)^D$, which implies $1/h(x)^2 = Q_H(x)^2/H(x)^{2D}$ and $\deg Q_H(x) = D \deg H(x) - \deg h(x)$. Since $\deg \Delta_{\alpha,i} \leq A_i$ and $\deg \Delta_{\beta,i} \leq B_i$, we conclude that A_{k+1} is less than or equal to

$$\max\left(\max_{i+j<k+2}(A_i + A_j, B_i + B_j + d_S^f), \max_{2i<k+3}(2A_i, 2B_i + d_S^f), \right. \\ \left. \max_{i<k+1} A_i + 2d_S^h, 2d_S^f\right) - 2d_S^h. \quad (23)$$

Using the bounds given in (18) for A_i and B_i we see that A_{k+1} also satisfies the bounds (18). A similar reasoning can be used to prove that B_{k+1} and L_{k+1} also satisfy the given bounds. □

The previous lemma indeed shows that we can lift the q-power Frobenius $\overline{F}$ to an endomorphism F on the dagger ring $A^\dagger$; it suffices to take $F := \sigma^n$. Before we can actually compute the zeta function using the Lefschetz fixed point theorem, we need to determine a basis of the K-vectorspace $H^1(\overline{A}/K)$.

Analogous to the odd characteristic case, the algebraic de Rham cohomology $H^1_{DR}(A/K)$ of A splits into eigenspaces under the hyperelliptic involution. The positive eigenspace $H^1_{DR}(A/K)^+$ is generated by $x^i/H(x)\,dx$ for $i = 0, \ldots, s$ and the negative eigenspace $H^1_{DR}(A/K)^-$ is generated by $x^i y\,dx$ for $i = 0, \ldots, 2g-1$. Note that the positive eigenspace corresponds to the deleted ramification points $(\theta_k, 0)$ for $k = 0, \ldots, s$. Every element of $H^1_{DR}(A/K)$ can be written as a linear combination of differentials of the form $x^k H(x)^m y^l\ dx$, $x^k H(x)^m y^l\ dy$ with $k, l \in \mathbb{N}$ and $m \in \mathbb{Z}$. Using the equation of the curve, we can reduce to the case $l = 0$ or 1. Since $d(x^k H(x)^m y)$ and $d(x^k H(x)^m y^2)$ are exact, we conclude that $H^1_{DR}(A/K)$ is generated by differentials of the form $x^k H(x)^m\ dx$ and $x^k H(x)^m y\ dx$ with $k \in \mathbb{N}$ and $m \in \mathbb{Z}$.

It is clear that $x^k H(x)^m\ dx$ is exact for $k \in \mathbb{N}$ and $m \geq 0$. If $\deg H(x) > 0$ and $m < 0$ we can assume that $0 \leq k < \deg H(x)$ and since $H(x)$ is squarefree we can write x^k as $A(x)H(x) + B(x)H'(x)$, which leads to

$$x^k H(x)^m\ dx = A(x)H(x)^{m+1}\ dx + B(x)H'(x)H(x)^m\ dx\,. \quad (24)$$

Since $d(B(x)H(x)^{m+1})$ is exact we can reduce the above differential further for $m < -1$ by using the relation

$$B(x)H'(x)H(x)^m\ dx \equiv -\frac{B'(x)H(x)^{m+1}}{m+1}\ dx\,, \quad (25)$$

where $\equiv$ means equality modulo exact differentials. As a result we can now reduce any form $x^k H(x)^m\ dx$ to a linear combination of the differentials $x^i/H(x)\,dx$ for $i = 0, \ldots, s$.

For $m > 0$ we can reduce the differential form $x^k H(x)^m y\ dx$ for $k \in \mathbb{N}$ if we know how to reduce the form $x^i y\,dx$ for $i \in \mathbb{N}$. Rewriting the equation of the curve as $(2y + h(x))^2 = 4f(x) + h(x)^2$ and differentiating both sides leads to

$(2y+h(x))\,d(2y+h(x)) = (2f'(x)+h(x)h'(x))\,dx$. Furthermore, for all $j \geq 1$, we have the following relations

$$\begin{aligned} x^j(2f'(x)+h(x)h'(x))(2y+h(x))\,dx &= x^j(2y+h(x))^2\,d(2y+h(x)) \\ &\equiv -\frac{1}{3}(2y+h(x))^3\,dx^j \\ &= -\frac{j}{3}x^{j-1}(4f(x)+h(x)^2)(2y+h(x))\,dx\,. \end{aligned}$$

Since $P(x)h(x)\,dx$ is exact for any polynomial $P(x) \in K[x]$, we finally obtain that

$$\left[x^j(2f'(x)+h(x)h'(x)) + \frac{j}{3}x^{j-1}(4f(x)+h(x)^2)\right] y\,dx \equiv 0\,.$$

The polynomial between brackets has degree $2g+j$ and its leading coefficient is $2(2g+1)+4j/3 \neq 0$. Note that the formula is also valid for $j=0$. This means that we can reduce $x^i y\,dx$ for any $i \geq 2g$ by subtracting a suitable multiple of the above differential for $j = i-2g$.

For $m < 0$ we need an extra trick to reduce the form $x^k H(x)^m y\,dx$ with $k \in \mathbb{N}$. Recall that $Q_f(x) = f(x)/H(x)$ and since the curve is non-singular, we conclude that $\gcd(Q_f(x), H(x)) = 1$. Furthermore, $H(x)$ has no repeated roots which implies $\gcd(H(x), Q_f(x)H'(x)) = 1$. Let $i = -m > 0$, then we can partially reduce $x^k y/H(x)^i\,dx$ by writing x^k as $A(x)H(x) + B(x)Q_f(x)H'(x)$, which leads to

$$\frac{x^k}{H(x)^i}\,y\,dx = \frac{A(x)}{H(x)^{i-1}}\,y\,dx + \frac{B(x)Q_f(x)H'(x)}{H(x)^i}\,y\,dx\,. \tag{26}$$

The latter differential form can be reduced using the following congruence

$$\begin{aligned} \frac{B(x)}{H(x)^i}(2f'(x)+h(x)h'(x))(2y+h(x))\,dx &= \frac{B(x)}{H(x)^i}(2y+h(x))^2\,d(2y+h(x)) \\ &\equiv -\frac{1}{3}(2y+h(x))^3 d\left(\frac{B(x)}{H(x)^i}\right)\,. \end{aligned} \tag{27}$$

Substituting the expressions $h(x) = Q_h(x)H(x)$, $f(x) = Q_f(x)H(x)$ and $(2y+h(x))^2 = 4f(x)+h(x)^2$, we get

$$\begin{aligned} &\frac{B(x)Q_f(x)H'(x)}{H(x)^i} y\,dx \equiv \\ &\qquad \frac{B(iH'Q_h^2 - 6Q_f' - 3Q_h h') - B'(4Q_f + Q_h h)}{(6-4i)H^{i-1}}\,y\,dx + \frac{I}{H}\,dx\,, \end{aligned} \tag{28}$$

where $I(x)/H(x)\,dx$ is a suitable invariant differential. As a result we can write any form $x^k H(x)^m y\;dx$ for $k \in \mathbb{N}$ and $m \in \mathbb{Z}$ as a linear combination of the differentials $x^i y\,dx$ for $i = 0, \ldots, 2g-1$ and $x^i/H(x)\,dx$ for $i = 0, \ldots, s$.

To show that the Monsky-Washnitzer cohomology $H^1(\overline{A}/K)$ is generated by the same differential forms as the algebraic de Rham cohomology, we need to bound the denominators introduced during the reduction process. Therefore we prove the following two lemmata.

Lemma 2 *Let $A := R[x,y]/(y^2 + h(x)y - f(x))$ and suppose that*

$$x^r y\ dx = \sum_{i=0}^{2g-1} a_i x^i y\ dx + dS, \tag{29}$$

with $r \in \mathbb{N}$, $a_i \in K$ and $S \in A \otimes K$. Then $2^m a_i \in R$, $2^{m'} S - \beta \in A$, where $m = 3 + \lfloor \log_2(r + g + 1) \rfloor$, $m' = 1 + m + \lfloor \log_2(2g + \deg h(x)) \rfloor$ and β some suitable element in K.

`Proof:` The proof has two distinct parts. The first part is similar to Kedlaya's argument in [15, Lemma 3], and is based on a local analysis around the point at infinity of the curve C. Put $t = x^g/y$, then one easily verifies that

$$x = t^{-2}\left(1 + \sum_{j=1}^{\infty} \alpha_j t^j\right) \quad \text{and} \quad y = t^{-2g-1}\left(1 + \sum_{j=1}^{\infty} \beta_j t^j\right), \tag{30}$$

with $\alpha_j, \beta_j \in R$. To see this, put $z = 1/x$, rewrite the equation of the curve C as $z + tz^{g+1}h(1/z) - t^2 z^{2g+1} f(1/z) = 0$ and write z as a power series in t using Newton iteration. The relation (29) can be rewritten as

$$2^{m-1} x^r (2y + h(x))\ dx = \sum_{i=0}^{2g-1} 2^{m-1} a_i x^i (2y + h(x))\ dx + \ dT, \tag{31}$$

with $T \in A \otimes K$. Considering the involution $\imath$ of A which sends x to x and $2y + h(x)$ to $-(2y + h(x))$, we see that we can write $T = \sum_{i=0}^{N} A_i x^i (2y + h(x))$, with N big enough and $A_i \in K$. This yields

$$2^{m-1} x^r (2y + h(x))\ dx - \sum_{i=0}^{2g-1} 2^{m-1} a_i x^i (2y + h(x))\ dx = d\left(\sum_{i=0}^{N} A_i x^i (2y + h(x))\right). \tag{32}$$

In the above equation we express x and y in terms of t using equalities (30). Since $x^i y = t^{-2i-2g-1} + \cdots$, we get $x^i(2y + h(x))\ dx = (-4t^{-2i-2g-4} + \cdots)\ dt$, which yields

$$2^{m-1} \sum_{j=-\max(2r+2g+4,6g+2)} \gamma_j t^j\ dt = d\left(\sum_{i=0}^{N} 2A_i(t^{-2i-2g-1} + \cdots) + A_i(c\, t^{-2i-2\deg h(x)} + \cdots)\right), \tag{33}$$

with $\gamma_j \in K$ for all j and $\gamma_j \in R$ when $j < -2(2g-1) - 2g - 4 = -6g - 2$ and c the leading coefficient of $h(x)$. Note that c is a unit in R. Integrating with respect to t and dividing by 2 gives

$$\sum_{j \geq -\max(2r+2g+3,6g+1)} \gamma'_j t^j = \sum_{i=0}^{N} A_i (t^{-2i-2g-1} + \cdots) + \sum_{i=0}^{N} \frac{A_i}{2} (c t^{-2i-2\deg h(x)} + \cdots), \tag{34}$$

with $\gamma'_j \in K$ for all j and $\gamma'_j \in R$ when $j < -6g-1$. Indeed the integration process introduces denominators which become integral after multiplication with $2^{\lfloor \log(2r+2g+2) \rfloor} = 2^{m-2}$ if $r \geq 2g-1$. A first consequence of (34) is that $A_i = 0$ for all $i > \max(r+1, 2g)$. We claim that (34) implies that $A_i \in R$ for all $i > 2g$. Suppose the claim is false. Then let i_0 be the largest integer with $i_0 > 2g$ and $A_{i_0} \notin R$. Note that $-2i_0 - 2g - 1 < -6g - 1$, since $i_0 > 2g$. Hence the monomials in the left hand side of (34) with degree $\leq -2i_0 - 2g - 1$ have coefficients in R. Moreover the monomials of degree $< -2i_0 - 2g - 1$, in the first sum in the right hand side of (34) also have coefficients in R, but this is false for the monomial of degree $-2i_0 - 2g - 1$. Hence the second sum in the right hand side of (34) contains a monomial of degree $-2i_0 - 2g - 1$ whose coefficient is not in R. That means that there is a maximal i_1 with $A_{i_1}/2 \notin R$ and $-2i_1 - 2\deg h(x) \leq -2i_0 - 2g - 1$. Because of parity we have that $-2i_1 - 2\deg h(x) < -2i_0 - 2g - 1$. Since c is a unit, the right hand side of (34) contains a monomial of degree $-2i_1 - 2\deg h(x) < -2i_0 - 2g - 1$ whose coefficient is not in R. But this contradicts what we said about the left hand side. This finishes the claim that $A_i \in R$ for all $i > 2g$.

We now turn to the second part of the proof. Note that $(2y + h(x))^2 = v(x)$ with $v(x) := 4f(x) + h(x)^2$. Moreover, $d(2y + h(x)) = \frac{w(x)}{2y+h(x)}\, dx$, where $w(x) := 2f'(x) + h(x)h'(x)$. We will use these formulae to deduce from (32) a relation which does not involve y. For this purpose we multiply (32) with $\frac{2y+h(x)}{dx} = \frac{w(x)}{d(2y+h(x))}$ obtaining

$$2^{m-1} x^r v(x) - \sum_{i=0}^{2g-1} 2^{m-1} a_i x^i v(x) = \sum_{i=0}^{N} A_i i x^{i-1} v(x) + \sum_{i=0}^{N} A_i x^i w(x). \tag{35}$$

We rewrite this in the form

$$\left(\sum_{i=0}^{2g-1} 2^{m-1} a_i x^i \right) v(x) + \left(\sum_{i=0}^{2g} A_i i x^{i-1} \right) v(x) + \left(\sum_{i=0}^{2g} A_i x^i \right) w(x) = F(x), \tag{36}$$

where

$$F(x) := 2^{m-1} x^r v(x) - \sum_{i=2g+1}^{N} A_i i x^{i-1} v(x) - \sum_{i=2g+1}^{N} A_i x^i w(x) \tag{37}$$

is a polynomial over R, since $A_i \in R$ for all $i > 2g$. From equations (36) and (37) it follows that $\sum_{i=0}^{2g} A_i \theta_k^i$ has valuation ≥ 0 for each root θ_k of $H(x)$, because

$v(\theta_k) = 0$ and $w(\theta_k) \neq 0$. To get rid of the disturbing factor 2 in the definition of $w(x)$, we consider $q(x) := h'(x)H(x)/h(x) \in R[x]$ and $u(x) := \frac{1}{2}(w(x) - q(x)v(x)/H(x)) = f'(x) - 2q(x)f(x)/H(x)$. Note that $u(x) \in R[x]$, $\deg q(x) = \max(0, \deg H(x) - 1)$, $\deg u(x) = 2g$ and that the leading coefficient of $u(x)$ is a unit in R. Rewrite equation (36) in such a way that $w(x)$ gets replaced by $u(x)$:

$$\left(\sum_{i=0}^{2g-1} 2^{m-1}a_i x^i + \sum_{i=0}^{2g} A_i i x^{i-1} + \frac{q(x)}{H(x)} \sum_{i=0}^{2g} A_i x^i\right) v(x) + \left(\sum_{i=0}^{2g} 2A_i x^i\right) u(x) = F(x). \quad (38)$$

Write $q(x)\sum_{i=0}^{2g} A_i x^i = H(x)\sum_{i=0}^{2g-1} B_i x^i + \mathrm{Rem}(x)$, with $\mathrm{Rem}(x) \in K[x]$ of degree $< \deg H(x)$. Since $\sum_{i=0}^{2g} A_i \theta_k^i$ has valuation ≥ 0 for each root θ_k of $H(x)$, the same holds for $\mathrm{Rem}(\theta_k)$. Thus $\mathrm{Rem}(x) \in R[x]$ since the discriminant of $H(x)$ is a unit in R. Hence

$$\left(\sum_{i=0}^{2g-1} \left(2^{m-1}a_i + (i+1)A_{i+1} + B_i\right) x^i\right) v(x) + \left(\sum_{i=0}^{2g} 2A_i x^i\right) u(x) = F(x) - \frac{\mathrm{Rem}(x)v(x)}{H(x)}. \quad (39)$$

We consider (39) as a system of $4g+1$ linear equations in the unknowns $2^{m-1}a_i + (i+1)A_{i+1} + B_i$ for $i = 0, \ldots, 2g-1$ and $2A_i$ for $i = 0, \ldots, 2g$. The determinant of this system is the resultant $\mathrm{Res}(v(x), u(x))$ of $v(x)$ and $u(x)$ because $\deg v(x) = 2g+1$ and $\deg u(x) = 2g$. This resultant is a unit in R because the valuation of $v(\xi)$ is zero for each root ξ of $u(x)$, since the resultant of $f'(x)$ and $h(x)$ is a unit. We conclude that the solutions of the linear system are elements of R, thus $2A_i \in R$ and $2^{m-1}a_i + (i+1)A_{i+1} + B_i \in R$. From the definition of the B_i it follows that $2B_i \in R$ since $2A_i \in R$ and $\mathrm{Rem}(x) \in R[x]$. Hence $2^m a_i \in R$, which concludes the proof of Lemma 2. $\square$

Remark Lemma 2 remains valid when we replace $\sum_{i=0}^{2g-1}$ by $\sum_{i=\kappa}^{2g-1+\kappa}$ whenever $r \geq \kappa \in \mathbb{N}$. The proof is the same, except that we also have to show that $A_i = 0$ for all $i < \kappa$. This follows from (32) using a local analysis at a point on the curve with $x = \theta_k$. Such a local analysis is given in the proof of Lemma 3 below.

Lemma 3 *Let* $A := R[x, y, H(x)^{-1}]/(y^2 + h(x)y - f(x))$ *with* $\deg h(x) > 0$ *and suppose that*

$$\frac{B(x)}{H(x)^r} y \ dx = \sum_{i=0}^{2g-1} a_i x^i y \ dx + \sum_{i=0}^{s} \frac{b_i x^i}{H(x)} \ dx + \ dS, \quad (40)$$

where $r \in \mathbb{N}$, $B(x) \in R[x]$ *of degree* $< \deg H(x)$, $a_i, b_i \in K$ *and* $S \in A \otimes K$. *Then* $2^m a_i \in R$, $2^{m'} b_i \in R$, $2^{m'} S - \beta \in A$, *with* $m = 3 + \lfloor \log_2(r+1) \rfloor$, $m' = 1 + m + \lfloor \log_2(2g + \deg h(x)) \rfloor$ *and* β *some suitable element in* K.

Proof: The proof again consists of two distinct parts. The first part is similar to Kedlaya's argument in [15, Lemma 2] and is based on a local analysis around the ramification points $(\theta_k, 0)$ for $k = 0, \ldots, s$. In the completion of the local ring of the curve at $(\theta_k, 0)$ we can write

$$x - \theta_k = \gamma_{k,2} y^2 + \sum_{j \geq 3} \gamma_{k,j} y^j, \tag{41}$$

with $\gamma_{k,j} \in R^{\mathrm{ur}}$ and $\gamma_{k,2}$ a unit in R^{ur}. Indeed, to see this write $h(x)$ and $f(x)$ as a Taylor expansion around θ_k and use the equation of the curve and the condition $f'(\theta_k) \neq 0 \bmod 2$, to express $x - \theta_k$ as a power series in y using Newton iteration.

Applying the involution $\imath$ to equation (40), we see that this relation implies

$$\begin{aligned} 2^{m-1} B(x) H(x)^{-r} (2y + h(x))\; dx - \sum_{i=0}^{2g-1} 2^{m-1} a_i x^i (2y + h(x))\; dx \\ = d\left(\sum_{i=-N}^{M} B_i(x) H(x)^i (2y + h(x)) \right), \end{aligned} \tag{42}$$

with N and M large enough integers. Expressing $x - \theta_k$ in terms of y, we get $B_i(x) H(x)^i = u_{k,i} B_i(\theta_k) y^{2i} + \cdots$ with $u_{k,i}$ a unit in R^{ur}. Substituting this in equation (42) and dividing by 2 we obtain

$$\begin{aligned} &2^{m-2} \sum_{j \geq -2r+2} \gamma'_{k,j} y^j \; dy \\ &= d\left(\sum_{i=-N}^{M} (u_{k,i} B_i(\theta_k) y^{2i+1} + \cdots) + (\frac{u_{k,i} B_i(\theta_k)}{2} \frac{\gamma_{k,2}^{m_k} h^{(m_k)}(\theta_k)}{m_k!} y^{2i+2m_k} + \cdots) \right) \end{aligned} \tag{43}$$

with $\gamma'_{k,j} \in K^{\mathrm{ur}}$ for all j and $\gamma'_{k,j} \in R^{\mathrm{ur}}$ when $j \leq 1$. Integrating the left hand side of this equation with respect to y yields a series whose terms of degree ≤ 2 have coefficients in R^{ur}. The leading term of the right hand side is $u_{k,-N} B_{-N}(\theta_k) y^{-2N+1}$, which implies that $B_{-N}(\theta_k)$ is integral for $k = 0, \ldots, s$. Since the discriminant of $H(x)$ is a unit in R we conclude that $B_{-N}(x)$ has integral coefficients. Bringing the integral terms to the left hand side and repeating the same argument, shows that $B_i(x) \in R[x]$ for $i = -N, \ldots, 0$. This terminates the first part of the proof.

The second part of the proof proceeds along the same lines as in Lemma 2. Rewrite the sum $\sum_{i=1}^{M} B_i(x) H(x)^i (2y + h(x))$ as $\sum_{i=0}^{M'} A_i x^i (2y + h(x))$ with $M' \in \mathbb{N}$ and $A_i \in K$. Using the same formulae as in Lemma 2 we deduce from (42) a relation which does not involve y by multiplying both sides with

$\frac{2y+h(x)}{dx} = \frac{w(x)}{d(2y+h(x))}$, which leads to

$$2^{m-1}\frac{B(x)}{H(x)^r}v(x) - \sum_{i=0}^{2g-1} 2^{m-1}a_i x^i v(x) = \sum_{i=-N}^{0} B_i(x)H(x)^i w(x) + \sum_{i=0}^{M'} A_i x^i w(x)$$
$$+ \sum_{i=-N}^{0} \left(B_i(x) i H(x)^{i-1} H'(x) + B_i'(x)H(x)^i\right) v(x) + \sum_{i=0}^{M'} A_i i x^{i-1} v(x)\,. \quad (44)$$

Comparing the valuation at infinity of both sides shows that $A_i = 0$ for $i > 2g$. We can therefore rewrite the above equation in the form

$$\left(\sum_{i=0}^{2g-1} 2^{m-1}a_i x^i\right) v(x) + \left(\sum_{i=0}^{2g} A_i i x^{i-1}\right) v(x) + \left(\sum_{i=0}^{2g} A_i x^i\right) w(x) = F(x), \quad (45)$$

where

$$F(x) := 2^{m-1}\frac{B(x)}{H(x)^r}v(x) - \sum_{i=-N}^{0} B_i(x)H(x)^i w(x)$$
$$- \sum_{i=-N}^{0} (B_i(x) i H(x)^{i-1} H'(x) + B_i'(x)H(x)^i)v(x) \quad (46)$$

is a polynomial over R since the $B_i(x) \in R[x]$ for $i = -N, \ldots, 0$ and the left-hand side of (45) is a polynomial. The local analysis around $(\theta_k, 0)$ shows that $\sum_{i=0}^{2g} A_i \theta_k^i$ has valuation ≥ 0 for $k = 0, \ldots, s$. It is now easy to see that the rest of the proof is exactly the same as in the proof of Lemma 2, hence $2^m a_i \in R$ and this concludes the proof of Lemma 3. $\square$

Remark Lemma 3 remains valid when we replace the term $\sum_{i=0}^{2g-1} a_i x^i y\ dx$ in equation (40) by $\sum_{i=-\kappa}^{\Delta-\kappa} C_i(x)H(x)^i y\ dx$, with $\Delta = \lfloor (2g-1)/\deg H(x) \rfloor$ and $C_i(x) \in K[x]$ of degree $< \deg H(x)$ whenever $r \geq \kappa \in \mathbb{N}$. The proof is exactly the same.

Remark If $r = 0$, then in the above proof the $B_i(x)$ are zero for all $i \leq 0$, and for $0 \leq i \leq 2g-1$ the a_i are completely determined by (45) as we saw by considering resultants. This shows that the $x^i y\ dx$ for $i = 0, \ldots, 2g-1$ and the $\frac{x^i}{H(x)}\ dx$ for $i = 0, \ldots, s$ are linearly independent in $H^1_{DR}(A/K)$.

Lemma 2 and 3 show that the basis for $H^1_{DR}(A/K)$ is a generating set for $H^1(\overline{A}/K)$, since the reduction process converges. Indeed, for $\sum_{k,l} a_{k,l} x^k S(x)^l y \in A^\dagger$ with $k, l \in \mathbb{Z}$ and $0 \leq k < \deg S(x)$ the valuation of $a_{k,l}$ grows as a linear function of $|l|$, while the valuation of the denominators introduced during the reduction process are only logarithmic in $|l|$.

The Monsky-Washnitzer cohomology $H^1(\overline{A}/K)$ is the direct sum of the $\imath$-invariant part $H^1(\overline{A}/K)^+$ on which $\imath$ acts trivially and the $\imath$-anti-invariant part $H^1(\overline{A}/K)^-$ on which $\imath$ acts as multiplication by -1. Let r_k be the number of ramification points $(\overline{\theta}, 0)$ defined over $\mathbb{F}_{q^k}$, then the Lefschetz fixed point formula applied to C' gives

$$\begin{aligned}\#C(\mathbb{F}_{q^k}) - r_k &= \#C'(\mathbb{F}_{q^k}) \\ &= \mathrm{Tr}\left(q^k F_*^{-k} | H^0(\overline{A}/K)\right) - \mathrm{Tr}\left(q^k F_*^{-k} | H^1(\overline{A}/K)\right) \\ &= q^k - \mathrm{Tr}\left(q^k F_*^{-k} | H^1(\overline{A}/K)^+\right) - \mathrm{Tr}\left(q^k F_*^{-k} | H^1(\overline{A}/K)^-\right) \\ &= q^k - r_k - \mathrm{Tr}\left(q^k F_*^{-k} | H^1(\overline{A}/K)^-\right).\end{aligned}$$

Let $\widetilde{C}$ be the unique smooth projective curve birational to $\overline{C}$, then

$$\#\widetilde{C}(\mathbb{F}_{q^k}) = q^k + 1 - \mathrm{Tr}\left(q^k F_*^{-k} | H^1(\overline{A}/K)^-\right) = q^k + 1 - \sum_{i=1}^{2g} \alpha_i^k,$$

where α_i are the eigenvalues of qF_*^{-1} on $H^1(\overline{A}/K)^-$. By the Weil conjectures there exists a polynomial $\chi(t) \in \mathbb{Z}[t]$ of the form $t^{2g} + a_1 t^{2g-1} + \cdots + a_{2g}$, whose roots $\beta_1, \ldots, \beta_{2g}$ satisfy $\beta_i \beta_{g+i} = q$ for $i = 1, \ldots, g$, $|\beta_i| = \sqrt{q}$ for $i = 1, \ldots, 2g$ and $\#\widetilde{C}(\mathbb{F}_{q^k}) = q^k + 1 - \sum_{i=1}^{2g} \beta_i^k$ for all $k > 0$. This implies that we can label the β's such that $\alpha_i = \beta_i$ for $i = 1, \ldots, 2g$. Since $\alpha_i \alpha_{g+i} = q$, the α_i are also the eigenvalues of F_* on $H^1(\overline{A}/K)^-$. It is well known that the zeta function $Z(\widetilde{C}/\mathbb{F}_q; t)$ can be written as

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

Therefore, it is sufficient to compute $\chi(t)$ as the characteristic polynomial of F_* on $H^1(\overline{A}/K)^-$.

4 Algorithm and Complexity

Using the formulae of the previous section, we describe an algorithm for computing the characteristic polynomial of Frobenius $\chi(t)$ and the zeta function of a smooth projective hyperelliptic curve $\widetilde{C}$ of genus g over $\mathbb{F}_q$ with $q = 2^n$.

4.1 Precision of Computation

We have shown that $\chi(t) = t^{2g} + a_1 t^{2g-1} + \cdots + a_{2g}$ can be computed as the characteristic polynomial of F_* on $H^1(\overline{A}/K)^-$. The Weil conjectures imply that $q^{g-i} a_i = a_{2g-i}$, so it suffices to compute $a_1, \ldots, a_g$. Furthermore, for $i = 1, \ldots, g$ the a_i can be bounded by

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

Therefore it suffices to compute the action of F_* on a basis of $H^1(\overline{A}/K)^-$ modulo 2^B with

$$B \geq \left\lceil \log_2 \left(2 \binom{2g}{g} q^{g/2} \right) \right\rceil . \tag{47}$$

However, it is not sufficient to compute y^σ modulo 2^B since we need to take into account the loss of precision introduced during the reduction process of the differential forms.

Let $y^\sigma \equiv \alpha_N + \beta_N y \mod 2^N$ and write $\beta_N = \sum_{i=-L_N}^{B_N} V_i(x) S(x)^i$, then Lemma 1 implies that $L_N \leq 4ND - 2D$ and $B_N \leq 2(N-1)(d_S^f - 2d_S^h) + (d_S^f - d_S^h)$, with $d_S^f := \deg f(x) / \deg S(x)$ and $d_S^h := \deg h(x) / \deg S(x)$.

Algorithm 1 (`Hyperelliptic_Zeta_Function`)

IN: *Hyperelliptic curve $\overline{C}$ over $\mathbb{F}_q$ given by equation $y^2 + \overline{h}(x)y = \overline{f}(x)$.*
OUT: *The zeta function $Z(\widetilde{C}/\mathbb{F}_q; t)$.*

---

1. $B = \left\lceil \log_2 \left(2\binom{2g}{g} q^{g/2} \right) \right\rceil$; $N - \max(c_{N,1}, c_{N,2}) > B$;

2. $(h(x), f(x), H(x), D) =$ `Lift_Curve`$(\overline{h}(x), \overline{f}(x))$;

3. $\alpha_N, \beta_N =$ `Lift_Frobenius_y`(h, f, H, D, N);

4. `For` $i = 0$ `To` $2g - 1$ `Do`

  4.1. $Red_i(x) =$ `Reduce_MW_Cohomology`$(2x^{2i+1}\beta_N, h, f, H, B)$;

  4.2. `For` $j = 0$ `To` $2g - 1$ `Do` $M[j][i] =$ `Coeff`(Red_i, j);

5. $M_F = M M^\sigma \cdots M^{\sigma^{n-1}} \mod 2^B$;

6. $\chi(T) =$ `Characteristic_Pol`$(M_F) \mod 2^B$;

7. `For` $i = 0$ `To` g `Do`

  7.1. `If` `Coeff`$(\chi, 2g - i) > \binom{2g}{i} q^{i/2}$ `Then` `Coeff`$(\chi, 2g - i)$ $- = 2^B$;

  7.2. `Coeff`$(\chi, i) = q^{g-i}$ `Coeff`$(\chi, 2g - i)$;

8. `Return` $Z(\widetilde{C}/\mathbb{F}_q; t) = \dfrac{t^{2g}\chi(1/t)}{(1-t)(1-qt)}$.

Since we have to reduce the forms $x^{2i+1} y^\sigma \, dx$ for $i = 0, \ldots, 2g - 1$, the loss of precision will be determined by the reduction of $x^{4g-1} V_{B_N}(x) S(x)^{B_N} y \, dx$ and $x V_{-L_N} S(x)^{-L_N} y \, dx$. The highest power of x appearing in the former differential form is less than $2N(\deg f(x) - 2 \deg h(x)) + 6g$ and by Lemma 2 the loss of precision is bounded by $c_{N,1} := 3 + \lfloor \log_2 (2N(\deg f(x) - 2 \deg h(x)) + 7g + 1) \rfloor$. Similarly, Lemma 3 implies that the loss of precision introduced during the reduction of the latter differential form is bounded by $c_{N,2} := 3 + \lfloor \log_2 (4ND - 2D + 1) \rfloor$.

As a result, we conclude that it is sufficient to compute modulo 2^N with

$$N - \max(c_{N,1}, c_{N,2}) > B \ . \tag{48}$$

4.2 Detailed Algorithm

The function `Hyperelliptic_Zeta_Function` given in Algorithm 1 computes the zeta function of a smooth projective hyperelliptic curve $\widetilde{C}$ defined over $\mathbb{F}_q$ with $q = 2^n$. Step 1 determines the minimal precision N satisfying inequality (48).

Algorithm 2 (`Lift_Frobenius_y`)

IN: *Curve $C : y^2 + h(x)y = f(x)$ over R, polynomial $H(x) \in R[x]$ with $H|h$ and $H|f$, $D \in \mathbb{N}$ such that $h|H^D$ and precision N.*
OUT: *Series $\alpha_N, \beta_N \in R[x, H, H^{-1}]$ with $y^\sigma \equiv \alpha_N + \beta_N y \bmod 2^N$.*

---

1. $B = \lceil \log_2 N \rceil + 1$; $T = N$; $Q_H := H^D \text{ div } h$;
2. `For` $i = B$ `Down To 1 Do` $P[i] = T$; $T = \lceil T/2 \rceil$;
3. $\alpha \equiv f \bmod 2$; $\beta \equiv -h \bmod 2$; $\gamma = 1$; $\delta = 0$;
4. `For` $i = 2$ `To` B `Do`
   - 4.1. $T_A \equiv \big((\alpha + h^\sigma) \cdot \alpha + \beta^2 \cdot f - f^\sigma\big) \cdot Q_H^2 \cdot H^{-2D} \bmod 2^{P[i]}$;
   - 4.2. $T_B \equiv (2\alpha - h \cdot \beta + h^\sigma) \cdot \beta \cdot Q_H^2 \cdot H^{-2D} \bmod 2^{P[i]}$;
   - 4.3. $D_A \equiv 1 + (h^\sigma - h^2 + 2\alpha) \cdot Q_H^2 \cdot H^{-2D} \bmod 2^{P[i-1]}$;
   - 4.4. $D_B \equiv 2\beta \cdot Q_H^2 \cdot H^{-2D} \bmod 2^{P[i-1]}$;
   - 4.5. $V_A \equiv D_A \cdot \gamma + D_B \cdot \delta \cdot f - 1 \bmod 2^{P[i-1]}$;
   - 4.6. $V_B \equiv D_A \cdot \delta + D_B \cdot (\gamma - \delta \cdot h) \bmod 2^{P[i-1]}$;
   - 4.7. $\gamma \equiv \gamma - (V_A \cdot \gamma + V_B \cdot \delta \cdot f) \bmod 2^{P[i-1]}$;
   - 4.8. $\delta \equiv \delta - (V_A \cdot \delta + V_B \cdot (\gamma - \delta \cdot h)) \bmod 2^{P[i-1]}$;
   - 4.9. $\alpha \equiv \alpha - (T_A \cdot \gamma + T_B \cdot \delta \cdot f) \bmod 2^{P[i]}$;
   - 4.10. $\beta \equiv \beta - (T_A \cdot \delta + T_B \cdot (\gamma - \delta \cdot h)) \bmod 2^{P[i]}$;
5. `Return` $\alpha_N = \alpha$, $\beta_N = \beta$.

In step 2 we call the subroutine `Lift_Curve`, which first constructs an isomorphic curve such that $\overline{H}(x) \,|\, \overline{h}(x)$ and $\overline{H}(x) \,|\, \overline{f}(x)$ and lifts the curve using the construction described in Section 3.2. The result of this function is a hyperelliptic curve $C : y^2 + h(x)y = f(x)$ over R, a polynomial $H(x)$ and an integer D such that $H(x) \,|\, h(x)$, $H(x) \,|\, f(x)$ and $h(x) \,|\, H(x)^D$. Since this function is rather straightforward, we have omitted the pseudo-code.

In step 3 we compute $y^\sigma \bmod 2^N$ using the function `Lift_Frobenius_y` given in Algorithm 2. The parameters α_N, β_N are Laurent series in $S(x)$ with coefficients polynomials over $R \bmod 2^N$ of degree $< \deg S(x)$. This function implements the Newton iteration (15), but has quadratic, instead of linear, convergence. Note that Algorithm 2 is in fact a double Newton iteration: $\alpha + \beta y$ converges to y^σ, whereas $\gamma + \delta y$ is an approximation of the inverse of the denominator (16) in the Newton iteration.

Once we have determined an approximation of y^σ, we compute the action of σ_* on the basis of $H^1(\overline{A}/K)^-$ as $2x^{2i+1}y^\sigma\, dx$ for $i = 0, \ldots, 2g-1$. In step 4 we reduce these forms using the function `Reduce_MW_Cohomology` given in Algorithm 3, which is based on the reduction formulae devised in Section 3.2. Given a differential $Gy\, dx$ with $G \in R[x, H, H^{-1}]$, this function computes a polynomial $\Lambda \in K[x]$, with $\deg \Lambda < 2g$ such that for a given precision B we have the following equivalence modulo exact forms and invariant forms $\Lambda y\, dx \sim Gy\, dx \bmod 2^B$, where $\bmod 2^B$ means modulo $2^B(Ry\, dx + \cdots + Rx^{2g-1}y\, dx)$. The result of step 4 of Algorithm 1 is an approximation modulo 2^B of the matrix M through which σ_* acts on $H^1(\overline{A}/K)^-$. In step 5 we compute its norm M_F as $MM^\sigma \cdots M^{\sigma^{n-1}}$. Note that since M is not necessarily defined over R, we have to compute this product with a high enough precision to obtain the correct result.

Algorithm 3 (`Reduce_MW_Cohomology`)

IN: *Series $G \in R[x, H, H^{-1}]$, polynomials $h, f, H \in R[x]$ and precision B.*
OUT: *$\Lambda \in K[x]$, with $\deg \Lambda < 2g$ such that $\Lambda y\, dx \sim Gy\, dx \bmod 2^B$.*

1. $N - \max(c_{N,1}, c_{N,2}) > B$;
2. $D_G = \deg G$; $V_G =$ `Valuation`(G); $D_T = (D_G + 1) \cdot \deg H$; $T = 0$;
3. `For` $i = D_G$ `Down To` 0 `Do` $T = T \cdot H +$ `Coeff`$(G, i) \bmod 2^N$;
4. `For` $i = D_T$ `Down To` $2g$
   - 4.1. $P \equiv x^{i-2g}(2f' + h \cdot h') + \frac{i-2g}{3} x^{i-2g-1}(4f + h^2) \bmod 2^N$;
   - 4.2. $T \equiv T - ($`Coeff`$(T,i) \cdot P)/$ `Coeff`$(P, i) \bmod 2^N$;
5. $Q_f = f \text{ div } H$; $Q_h = h \text{ div } H$; $P = 0$;
6. `For` $i = V_G$ `To` -1
   - 6.1. $V \equiv P +$ `Coeff`$(G,i) \bmod 2^N$;
   - 6.2. $P \equiv V \text{ div } H \bmod 2^N$; $V \equiv V - P \cdot H \bmod 2^N$;
   - 6.3. $C, L_A, L_B =$ `XGCD`$(V \cdot H,\ V \cdot Q_f \cdot H',\ N)$;
   - 6.4. $P \equiv P + L_A + \frac{L_B \cdot (-iQ_h^2 \cdot H' - 3(2Q_f' + Q_h \cdot h')) - L_B' \cdot (4Q_f + Q_h h)}{6+4i} \bmod 2^N$;
7. `Return` $\Lambda \equiv T + P \bmod 2^B$.

In steps 6 and 7 we recover the characteristic polynomial of Frobenius from the first g coefficients of the characteristic polynomial of M_F. Finally, we return the zeta function of the smooth projective hyperelliptic curve $\widetilde{C}$ birational to $\overline{C}$ in Step 8.

4.3 Complexity

In this section we analyze the space and time requirements of Algorithm 1 for a genus g hyperelliptic curve over $\mathbb{F}_{2^n}$ assuming fast arithmetic, i.e. multiplication of two objects of bit-size $O(m)$ can be computed in time $O(m^{1+\varepsilon})$. Before proceeding through the individual steps of the algorithm, we analyze the complexity of the basic operations in Algorithm 1 and the asymptotic behaviour of the bounds given in Lemma 1.

For a fixed precision N, let R_N denote the degree n unramified extension of $\mathbb{Z}_2/2^N\mathbb{Z}_2$. Elements of R_N are represented as polynomials over $\mathbb{Z}/2^N\mathbb{Z}$ modulo a sparse irreducible polynomial $P(t)$ of degree n. Since each element of this ring requires $O(nN)$ space, we can perform the basic operations, i.e. multiplication and division, in time $O(n^{1+\varepsilon}N^{1+\varepsilon})$.

Computing the Frobenius substitution σ on R_N can be accomplished in time $O(n^{2+\varepsilon}N^{1+\varepsilon})$ as follows. Since t is a root of $P(t)$, t^σ will also be a root of $P(t)$ and $t^\sigma \equiv t^2 \bmod 2$. Therefore, t^σ can be computed using the Newton iteration $T_{k+1} = T_k - P(T_k)/P'(T_k)$ initialized with t^2. Since the Newton iteration converges quadratically and we compute with the minimal precision in each step, the total complexity will be determined by the last step which takes $O(n)$ multiplications in R_N. Precomputing $t^\sigma \bmod 2^N$ can thus be accomplished in time $O(n^{2+\varepsilon}N^{1+\varepsilon})$. After this precomputation, we can compute the Frobenius substitution of any element $E(t)$ as $E(t^\sigma)$, which needs $O(n)$ multiplications in R_N and thus takes $O(n^{2+\varepsilon}N^{1+\varepsilon})$ time.

Lemma 1 bounds the maximum bit-size of the Laurent series we compute with and therefore determines the complexity of Algorithm 1. Since these bounds depend on the degree and splitting type of $h(x)$, we make a distinction between average-case and worst-case complexity. To this end we introduce three parameters which allow us to analyze both cases simultaneously.

- Let the asymptotic behaviour of $\deg f(x) - 2\deg h(x)$ be $O(g^\lambda)$. Since the degree of $f(x)$ is $2g+1$ and $h(x)$ is a random polynomial of degree $\leq g$, we conclude that $\lambda = 0$ on average and $\lambda = 1$ in the worst case.
- Let the asymptotic behaviour of $\deg H(x)$ be $O(g^\mu)$. With very high probability a random polynomial of degree $\leq g$ has $O(g)$ different roots, which implies that $\mu = 1$ on average and $\mu = 0$ in the extreme case.
- Let the asymptotic behaviour of D be $O(g^\nu)$, then $\nu = 0$ on average and $\nu = 1$ in the worst case, since a random polynomial only has roots with multiplicity $O(1)$.

The function `Lift_Frobenius_y` in Step 3 of Algorithm 1 is a Newton lifting. Since the precision doubles in every iteration, we see that its complexity is determined by the last iteration, which consists of $O(1)$ multiplications of Laurent series in $S(x)$ with coefficients polynomials over R_N of degree less than $\deg S(x)$. Lemma 1 implies that the bit-size of these objects is $O((g^{\lambda} + g^{\mu+\nu})nN^2)$. Since the cost of the other operations in `Lift_Frobenius_y`, e.g. computing the Frobenius substitution of $O(g)$ elements of R_N, is less than the $O(1)$ multiplications, the overall time complexity of Step 3 is $O((g^{\lambda} + g^{\mu+\nu})^{1+\varepsilon}n^{1+\varepsilon}N^{2+\varepsilon})$.

In step 4 of Algorithm 1 we reduce the $2g$ differential forms $2x^{2i+1}\beta_N y\ dx$ for $i = 0, \ldots, 2g-1$ using the function `Reduce_MW_Cohomology` given in Algorithm 3. Write β_N as $\sum_{i=-L_N}^{B_N} V_i(x)S(x)^i$, then Step 2 essentially is Horner's rule to compute $\sum_{i=0}^{B_N} V_i(x)S(x)^i$. Note that in practice we perform this step only once for all of the $2g$ reductions and use a binary tree algorithm which is asymptotically faster than Horner's method. The complexity of Step 2 then becomes $O(g^{\lambda+\varepsilon}n^{1+\varepsilon}N^{2+\varepsilon})$. Lemma 1 implies that Substeps 3.1 and 3.2 have to be executed $O(g^{\lambda}N)$ times and since each iteration consists of $O(g)$ multiplications in R_N, the time complexity of Step 3 is $O(g^{1+\lambda}n^{1+\varepsilon}N^{2+\varepsilon})$. In Step 5 the dominant operations are $O(1)$ multiplications of polynomials over R_N of degree $O(g)$ and the extended GCD computation of two such polynomials. The former operation clearly takes time $O(g^{1+\varepsilon}n^{1+\varepsilon}N^{1+\varepsilon})$ and using Moenck's algorithm [23] the latter operation can also be performed in time $O(g^{1+\varepsilon}n^{1+\varepsilon}N^{1+\varepsilon})$. Note that in practice we precompute polynomials $A(x)$ and $B(x)$ such that $A(x)H(x) + B(x)Q_f(x)H'(x) = 1$ and compute $L_A(x)$ as the reduction of $A(x)V(x)$ modulo $Q_f(x)H'(x)$ and $L_B(x)$ as the reduction of $V(x)B(x)$ modulo $H(x)$. Lemma 1 implies that these operations have to be repeated $O(g^{\nu}N)$ times, so the time complexity of Step 5 is $O(g^{1+\nu+\varepsilon}n^{1+\varepsilon}N^{2+\varepsilon})$. Since we have to reduce $O(g)$ differential forms, the overall time complexity of Step 4 of Algorithm 1 is $O((g^{2+\lambda} + g^{2+\nu+\varepsilon})n^{1+\varepsilon}N^{2+\varepsilon})$.

In Step 5 we need to determine the norm of a $2g \times 2g$ matrix M over R_N as $MM^{\sigma}\cdots M^{\sigma^{n-1}}$. This can be accomplished by computing $M_{i+1} = M_i M_i^{\sigma^{2^i}}$ for $i = 0, \ldots, \lfloor \log_2 n \rfloor$ and combining these to recover the norm of M. Multiplication of two matrices takes $O(g^3)$ ring operations at a cost of $O(g^3 n^{1+\varepsilon}N^{1+\varepsilon})$ time. To compute $M_i^{\sigma^{2^i}}$ for $i = 0, \ldots, \lfloor \log_2 n \rfloor$, we need $O(g^2 \log n)$ applications of powers of σ. If we precompute $t^{\sigma^{2^i}}$, this requires $O(g^2 n^{2+\varepsilon}N^{1+\varepsilon})$ time.

Finally, we need to compute the characteristic polynomial of a $2g \times 2g$ matrix over R_N, 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 $O(g^3 n^{1+\varepsilon}N^{1+\varepsilon})$ time.

Since equation (48) implies that N is $O(gn)$, the overall time complexity of Algorithm 1 is $O((g^{\lambda} + g^{\nu})g^{4+\varepsilon}n^{3+\varepsilon})$ and the overall space complexity becomes $O((g^{\lambda} + g^{\mu+\nu})g^2 n^3)$. Note that this means the following:

- Average case: the time complexity reduces to $O(g^{4+\varepsilon}n^{3+\varepsilon})$ and the space complexity is $O(g^3 n^3)$.
- Worst case: the time complexity grows to $O(g^{5+\varepsilon}n^{3+\varepsilon})$ and the space complexity becomes $O(g^4 n^3)$.

5 Implementation and Numerical Results

In this section we present running times of an implementation of Algorithm 1 in the `C` programming language and give some examples of Jacobians of hyperelliptic curves with almost prime group order.

The basic operations on integers modulo 2^N for $N \leq 256$ were written in assembly language. Elements of R_N are represented as polynomials over $\mathbb{Z}/2^N\mathbb{Z}$ modulo a degree n irreducible polynomial, which we chose to be either a trinomial or a pentanomial. For multiplication of elements in R_N, polynomials over R_N and Laurent series over $R_N[x]$ we used Karatsuba's algorithm. In the near future, we plan to implement Toom's algorithm which will lead to a further speed-up of about 50%.

5.1 Running Times and Memory Usage

Table 1 contains running times and memory usages of our algorithm for genus 2, 3 and 4 hyperelliptic 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 fields are chosen such that gn, and therefore the bit size of the group order of the Jacobian, is constant across each row.

Table 1. Running time (s) and memory usage (MB) for genus 2, 3 and 4 hyperelliptic curves over $\mathbb{F}_{2^n}$

Size of Jacobian	Genus 2 curves		Genus 3 curves		Genus 4 curves	
gn	Time (s)	Mem (MB)	Time (s)	Mem (MB)	Time (s)	Mem (MB)
120	30	4.5	38	5.4	35	5.2
144	44	5.7	61	7.3	59	7.2
168	71	8.6	101	11	100	11
192	116	13	143	14	139	13
216	170	16	196	17	185	16

5.2 Hyperelliptic Curve Examples

In this subsection we give three examples of Jacobians of hyperelliptic curves with almost prime group order. The correctness of these results 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 $J_{\widetilde{C}}(\mathbb{F}_q)$. It is clear that the given curves are non-supersingular, since the coefficient a_g is odd [11]. Furthermore, all curves withstand the MOV-FR attack [10, 21].

Genus 2 hyperelliptic curve over $\mathbb{F}_{2^{83}}$

Let $\mathbb{F}_{2^{83}}$ be defined as $\mathbb{F}_2[t]/\overline{P}(t)$ with $\overline{P}(t) = t^{83}+t^7+t^4+t^2+1$ and consider the random hyperelliptic curve C_2 of genus 2 defined by

$$y^2 + (\sum_{i=0}^{2} h_i x^i)y = x^5 + \sum_{i=0}^{4} f_i x^i\,,$$

where

$$\begin{array}{ll} h_0 = \texttt{7FF29B08993336B479CD2} & h_1 = \texttt{32C101713C722F8FB5BC9} \\ h_2 = \texttt{553E16B6A3BC6B2432CA8} & \\ f_0 = \texttt{7AD44882C02B9743CD58B} & f_1 = \texttt{327254FA330B44958262A} \\ f_2 = \texttt{204AB23E12828D061AF04} & f_3 = \texttt{1C827250FFDEFF93B43BE} \\ f_4 = \texttt{13D80106C0E5571DFD139} & \end{array}$$

The group order of the Jacobian $J_{\widetilde{C}_2}$ of C_2 over $\mathbb{F}_{2^{83}}$ is

$$\#J_{\widetilde{C}_2} = 2 \cdot 46768052394566313810931349196246034325781246483037\,,$$

where the last factor is prime. The coefficients a_1 and a_2 of the characteristic polynomial of Frobenius $\chi(T) = T^4 + a_1T^3 + a_2T^2 + a_3T + a_4$ are given by

$$a_1 = -4669345964042 \quad \text{and} \quad a_2 = 18983903513383986646766787\,.$$

Genus 3 hyperelliptic curve over $\mathbb{F}_{2^{59}}$

Let $\mathbb{F}_{2^{59}}$ be defined as $\mathbb{F}_2[t]/\overline{P}(t)$ with $\overline{P}(t) = t^{59}+t^7+t^4+t^2+1$ and consider the random hyperelliptic curve C_3 of genus 3 defined by

$$y^2 + (\sum_{i=0}^{3} h_i x^i)y = x^7 + \sum_{i=0}^{6} f_i x^i\,,$$

where

$$\begin{array}{ll} h_0 = \texttt{569121E97EB3821} & h_1 = \texttt{49F340F25EA38A2} \\ h_2 = \texttt{2DE854D48D56154} & h_3 = \texttt{0B6372FF7310443} \\ f_0 = \texttt{1104FDBEB454C58} & f_1 = \texttt{0C426890E5C7481} \\ f_2 = \texttt{34967E2EB7D50C3} & f_3 = \texttt{1F1728AA28C616C} \\ f_4 = \texttt{1AE177BFE49826A} & f_5 = \texttt{3895A0E400F7D18} \\ f_6 = \texttt{6DF634A1E2BFA8E} & \end{array}$$

The group order of the Jacobian $J_{\widetilde{C}_3}$ of C_3 over $\mathbb{F}_{2^{59}}$ is

$$\#J_{\widetilde{C}_3} = 2 \cdot 95780971407243394633762332360123160334059170481903949\,,$$

where the last factor is prime. The coefficients a_1, a_2 and a_3 of the characteristic polynomial of Frobenius $\chi(T) = T^6 + a_1T^5 + a_2T^4 + a_3T^3 + a_4T^2 + a_5T + a_6$ are given by

$$\begin{aligned} a_1 &= 620663068, \\ a_2 &= 848092512078818380, \\ a_3 &= 341008017371409573053936945\,. \end{aligned}$$

Genus 4 hyperelliptic curve over $\mathbb{F}_{2^{43}}$

Let $\mathbb{F}_{2^{43}}$ be defined as $\mathbb{F}_2[t]/\overline{P}(t)$ with $\overline{P}(t) = t^{43}+t^6+t^4+t^3+1$ and consider the random hyperelliptic curve C_4 of genus 4 defined by

$$y^2 + (\sum_{i=0}^{4} h_i x^i)y = x^9 + \sum_{i=0}^{8} f_i x^i \,,$$

where

$h_0 =$ `28E79976104`	$h_1 =$ `6D6B97FBB9B`	$h_2 =$ `2D6524209DB`
$h_3 =$ `7F68B16B438`	$h_4 =$ `1407613976D`	
$f_0 =$ `4D8C53D03FB`	$f_1 =$ `427CDCD7B63`	$f_2 =$ `282064866B4`
$f_3 =$ `54FE7CA7C26`	$f_4 =$ `7D3E9ACFE87`	$f_5 =$ `45A6C030DDF`
$f_6 =$ `0F470E4047B`	$f_7 =$ `7BC7F15221C`	$f_8 =$ `2F380FD7563`

The group order of the Jacobian $J_{\widetilde{C}_4}$ of C_4 over $\mathbb{F}_{2^{43}}$ is

$$\#J_{\widetilde{C}_4} = 2 \cdot 2993154057417792912224847413075158366114567502366357 \,,$$

where the last factor is prime. The coefficients a_1, a_2, a_3 and a_4 of the characteristic polynomial of Frobenius $\chi(T) = T^8 + a_1T^7 + a_2T^6 + a_3T^5 + a_4T^4 + a_5T^3 + a_6T^2 + a_7T + a_8$ are given by

$$\begin{aligned} a_1 &= -3808120, \\ a_2 &= 4933477855906, \\ a_3 &= 6263305780455915698, \\ a_4 &= -14840229309879529733065395. \end{aligned}$$

6 Conclusion

We have presented an extension of Kedlaya's algorithm for computing the zeta function of an arbitrary hyperelliptic curve C over a finite field $\mathbb{F}_q$ of characteristic 2. As a byproduct we obtain the group order of the Jacobian associated to C which forms the basis of the cryptographic schemes based on hyperelliptic curves. For a genus g hyperelliptic curve defined over $\mathbb{F}_{2^n}$, the average-case time complexity is $O(g^{4+\varepsilon}n^{3+\varepsilon})$ and the average-case space complexity is $O(g^3n^3)$, whereas the worst-case time and space complexities are $O(g^{5+\varepsilon}n^{3+\varepsilon})$ and $O(g^4n^3)$ respectively. A first implementation of this algorithm in the `C` programming language shows that cryptographical sizes are now feasible for any genus g. Computing the order of a 160-bit Jacobian of a hyperelliptic curve of genus 2, 3 or 4 takes less than 100 seconds. In the near future we plan to use the formalism of Monsky-Washnitzer cohomology as a basis for computing the zeta function of any non-singular C_{ab} curve over finite fields of small characteristic.

References

1. S. Arita. Algorithms for computations in Jacobians of C_{ab} curves and their application to discrete-log-based public key cryptosystems. In *Proceedings of Conference on The Mathematics of Public Key Cryptography*, Toronto, June 12-17, 1999.
2. A.O.L. Atkin. The number of points on an elliptic curve modulo a prime. *Series of e-mails to the* NMBRTHRY *mailing list*, 1992.
3. I.F. Blake, G. Seroussi, and N.P. Smart. *Elliptic curves in cryptography.* London Mathematical Society Lecture Note Series. 265. Cambridge University Press., 1999.
4. S. Bosch. A rigid analytic version of M. Artin's theorem on analytic equations. *Math. Ann.*, 255:395–404, 1981.
5. H. Cohen. *A course in computational algebraic number theory.* Graduate Texts in Mathematics. 138. Berlin: Springer-Verlag. xxi, 534 p., 1993.
6. J. Denef and F. Vercauteren. An extension of Kedlaya's algorithm to Artin-Schreier curves in characteristic 2. In C. Fieker and D.R. Kohel, editors, *Algorithmic number theory. 5th international symposium. ANTS-V*, volume 2369 of *Lecture Notes in Computer Science*, pages 308–323. Springer-Verlag Berlin, 2002.
7. N. Elkies. Elliptic and modular curves over finite fields and related computational issues. *Computational Perspectives on Number Theory*, pages 21–76, 1998.
8. R. Elkik. Solutions d'équations a coefficients dans un anneau henselien. *Ann. Scient. Ec. Norm. Syp.*, 6(4):553–604, 1973.
9. M. Fouquet, P. Gaudry, and R. Harley. On Satoh's algorithm and its implementation. *J. Ramanujan Math. Soc.*, 15:281–318, 2000.
10. 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, April 1994.
11. S. Galbraith. Supersingular curves in cryptography. In C. Boyd, editor, *Advances in Cryptology - ASIACRYPT 2001*, volume 2248 of *Lecture Notes in Computer Science*, pages 495–513, 2001.
12. S. Galbraith, S. Paulus, and N. Smart. Arithmetic on superelliptic curves. *Math. Comp.*, 71(237):393–405, 2002.
13. P. Gaudry and R. Harley. Counting points on hyperelliptic curves over finite fields. In Wieb Bosma, editor, *Algorithmic number theory. 4th international symposium. ANTS-IV*, volume 1838 of *Lecture Notes in Computer Science*, pages 313–332, 2000.
14. P. Gaudry and N. Gürel. An extension of Kedlaya's algorithm for counting points on superelliptic curves. In C. Boyd, editor, *Advances in Cryptology - ASIACRYPT 2001*, volume 2248 of *Lecture Notes in Computer Science*, pages 480–494, 2001.
15. K.S. Kedlaya. Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology. *Journal of the Ramanujan Mathematical Society*, 16:323–338, 2001.
16. N. Koblitz. Elliptic curve cryptosystems. *Math. Comput.*, 48:203–209, 1987.
17. N. Koblitz. Hyperelliptic cryptosystems. *J. Cryptology*, 1(3):139–150, 1989.
18. A.G.B. Lauder and D. Wan. Counting points on varieties over finite fields of small characteristic. Preprint 2001.
19. A.G.B. Lauder and D. Wan. Computing zeta functions of Artin-Schreier curves over finite fields. *London Mathematical Society JCM*, 5:34–55, 2002.
20. R. Lercier. *Algorithmique des courbes elliptiques dans les corps finis.* PhD thesis, Laboratoire d'Informatique de l'École polytechnique (LIX), 1997. Available at `http://ultralix.polytechnique.fr/~lercier`.

21. A. Menezes, T. Okamoto, and S. Vanstone. Reducing elliptic curve logarithms to logarithms in a finite field. In *Proceedings of the twenty third annual ACM Symposium on Theory of Computing, New Orleans, Louisiana, May 6–8, 1991*, pages 80–89, 1991.
22. V. Miller. Uses of elliptic curves in cryptography. In C. Boyd, editor, *Advances in Cryptology - ASIACRYPT 1991*, volume 218 of *Lecture Notes in Computer Science*, pages 460–469, 1993.
23. R.T. Moenck. Fast computation of GCDs. *Fifth Annual ACM Symposium on Theory of Computing (Austin Tex., 1973)*, pages 142–151, 1973.
24. P. Monsky and G. Washnitzer. Formal cohomology. I. *Ann. of Math.*, 88:181–217, 1968.
25. P. Monsky. Formal cohomology. II: The cohomology sequence of a pair. *Ann. of Math.*, 88:218–238, 1968.
26. P. Monsky. Formal cohomology. III: Fixed point theorems. *Ann. of Math.*, 93:315–343, 1971.
27. P. Monsky. *p-adic analysis and zeta functions.* Lectures in Mathematics, Department of Mathematics Kyoto University. 4. Tokyo, Japan, 1970.
28. J. Pila. Frobenius maps of abelian varieties and finding roots of unity in finite fields. *Math. Comput.*, 55(192):745–763, 1990.
29. B. Poonen. Computational aspects of curves of genus at least 2. In H. Cohen, editor, *Algorithmic number theory. 5th international symposium. ANTS-II*, volume 1122 of *Lecture Notes in Computer Science*, pages 283–306. Springer-Verlag Berlin, 1996.
30. T. Satoh. The canonical lift of an ordinary elliptic curve over a finite field and its point counting. *J. Ramanujan Math. Soc.*, 15:247–270, 2000.
31. T. Satoh, B. Skjernaa, and Y. Taguchi. Fast computation of canonical lifts of elliptic curves and its application to point counting. *Preprint*, 2001.
32. T. Satoh. On p-adic point counting algorithms for elliptic curves over finite fields. In C. Fieker and D.R. Kohel, editors, *Algorithmic number theory. 5th international symposium. ANTS-V*, volume 2369 of *Lecture Notes in Computer Science*, pages 43–66. Springer-Verlag Berlin, 2002.
33. R. Schoof. Elliptic curves over finite fields and the computation of square roots mod p. *Math. Comp.*, 44:483–494, 1985.
34. B. Skjernaa. Satoh's algorithm in characteristic 2. *To appear in Math. Comp.*, 2000.
35. M. van der Put. The cohomology of Monsky and Washnitzer. *Mém. Soc. Math. France*, 23:33–60, 1986.
36. F. Vercauteren, B. Preneel, and J. Vandewalle. A memory efficient version of Satoh's algorithm. In *Advances in Cryptology - EUROCRYPT 2001*, volume 2045 of *Lecture Notes in Computer Science*, pages 1–13, 2001.
37. D. Wan. Computing zeta functions over finite fields. *Contemporary Mathematics*, 225:131–141, 1999.