Computing Zeta Functions of Hyperelliptic Curves over Finite Fields of Characteristic 2

Frederik Vercauteren[1,2] ⋆

[1] Department of Electrical Engineering
University of Leuven
Kasteelpark Arenberg 10, B-3001 Leuven-Heverlee, Belgium
frederik.vercauteren@esat.kuleuven.ac.be
[2] 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 small odd characteristic. For a genus g hyperelliptic curve over $\mathbb{F}_{2^n}$, the asymptotic running time of the algorithm is $O(g^{5+\varepsilon}n^{3+\varepsilon})$ and the space complexity is $O(g^3n^3)$.

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

1 Introduction

Since elliptic curve cryptosystems were introduced by Koblitz [16] and Miller [23], various other systems based on the discrete logarithm problem in the Jacobian of curves have been proposed, e.g. hyperelliptic curves [17], superelliptic curves [10] and $\mathcal{C}_{ab}$ curves [1]. One of the main initialization steps of these cryptosystems is to generate a suitable curve defined over a given finite field. To ensure the security of the system, the curve must be chosen such that the group order of the Jacobian is divisible by a large prime.

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 [32] and its improvements due to Atkin [2] and Elkies [6]. An excellent account of the resulting SEA-algorithm can be found in [3] and [20]. For finite fields of small characteristic, Satoh [29] described an algorithm based on p-adic methods which is asymptotically faster than the SEA-algorithm. Skjernaa [33] and Fouquet, Gaudry and Harley [7] extended the algorithm to characteristic 2 and Vercauteren [35] presented a memory efficient version. Mestre proposed a

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

variant of Satoh's algorithm based on the Arithmetic-Geometric Mean, which has the same asymptotic behavior as [35], but is faster by some constant. Satoh, Skjernaa and Taguchi [30] described an algorithm which has a better complexity than all previous algorithms, but requires some precomputations.

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 as shown by Gaudry and Harley [12]. 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 [14] 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 $O(g^{4+\varepsilon} \log^{3+\varepsilon} q)$ for a hyperelliptic curve of genus g over $\mathbb{F}_q$. The algorithm readily generalizes to superelliptic curves as shown by Gaudry and Gurel [11].

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 [36] suggested the use of p-adic methods, including the method of Dwork and Monsky, already several years ago. Despite the polynomial 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 $O(g^{5+\varepsilon} \log^{3+\varepsilon} q)$ time algorithm. Denef and Vercauteren [4] described an extension of Kedlaya's algorithm for Artin-Schreier curves in characteristic 2 which has the same running time $O(g^{5+\varepsilon} \log^{3+\varepsilon} q)$.

In this paper we describe an extension of Kedlaya's algorithm to compute the zeta function of an *arbitrary* hyperelliptic curve C defined over a finite field $\mathbb{F}_q$ of characteristic 2. The resulting algorithm has running time $O(g^{5+\varepsilon} \log^{3+\varepsilon} q)$ and needs $O(g^3 \log^3 q)$ storage space for a genus g curve. 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 theoretical version of this paper, co-authored by Jan Denef [5], provides a detailed description of the underlying mathematics of the algorithm and contains several proofs which we have omitted from the current article.

The remainder of the paper is organized as follows: after recalling some basics about curves and zeta functions in Section 2, we give a brief overview of the formalism of Monsky-Washnitzer cohomology in Section 3. In Section 4 we study the cohomology of hyperelliptic curves over finite fields of characteristic 2 and in Section 5 we present a ready to implement description of the resulting algorithm. We conclude in Section 6 with some numerical examples obtained by an implementation of our algorithm in the `C` programming language.

2 Hyperelliptic Curves, Zeta Functions and *p*-adics

In this section we briefly recall the definition of a hyperelliptic curve, the main properties of its zeta function and some basic facts about p-adic numbers. More details can be found in the elementary books by Fulton [9], Lorenzini [21] and Koblitz [15] or in the standard reference by Hartshorne [13].

2.1 Hyperelliptic Curves

Let $\mathbb{F}_q$ be a finite field with $q = p^n$ elements and fix an algebraic closure $\overline{\mathbb{F}}_q$ of $\mathbb{F}_q$. For $k \in \mathbb{N}_0$, let $\mathbb{F}_{q^k}$ be the unique subfield of $\overline{\mathbb{F}}_q$ of order q^k. An affine hyperelliptic curve C of genus g is a plane curve defined by an equation of the form

$$C : y^2 + \overline{h}(x)y = \overline{f}(x)\,, \tag{1}$$

where $\overline{f}(x) \in \mathbb{F}_q[x]$ is a monic polynomial of degree $2g+1$ and $\overline{h}(x) \in \mathbb{F}_q[x]$ is a polynomial of degree at most g. Furthermore, the curve should be non-singular, i.e. there is no point in $C(\overline{\mathbb{F}}_q)$ such that both partial derivatives

$$2y + \overline{h}(x) \quad \text{and} \quad \overline{h}'(x)y - \overline{f}'(x)\,,$$

simultaneously vanish. Note that for $g = 1$ we recover the definition of an elliptic curve and that for $g > 1$ the hyperelliptic curve C is singular at the point at infinity. However, there always exists a unique smooth projective curve $\widetilde{C}$ birational to C. Since the degree of $\overline{f}(x)$ is odd, $\widetilde{C}$ has a unique place of degree 1 (i.e. a point) at infinity. Note that there exists an involution $\imath$ on $\widetilde{C}$ which sends the point (x, y) to the point $(x, -y - \overline{h}(x))$.

Let $\widetilde{C}(\mathbb{F}_{q^k})$ denote the set of points on $\widetilde{C}$ with coordinates in $\mathbb{F}_{q^k}$. If $\widetilde{C}$ is an elliptic curve, one can define an additive abelian group law on the set $\widetilde{C}(\mathbb{F}_{q^k})$ by the chord-tangent method. For a hyperelliptic curve with $g > 1$ this is no longer possible; instead one computes in the group of points on the Jacobian $J_{\widetilde{C}}(\mathbb{F}_{q^k})$ of the curve.

A divisor D on a curve $\widetilde{C}$ is a finite formal sum of points

$$D = \sum_{P \in \widetilde{C}(\overline{\mathbb{F}}_q)} n_P P\,,$$

where $n_P \in \mathbb{Z}$. The degree of D is defined as $\sum n_P$. A divisor is called $\mathbb{F}_{q^k}$-rational if it is stable under the action of the q^k-th power Frobenius endomorphism $F_k : \overline{\mathbb{F}}_q \to \overline{\mathbb{F}}_q : x \mapsto x^{q^k}$. Every function on the curve gives rise to a so called principal divisor, i.e. the degree zero divisor consisting of the formal sum of the poles and zeros of the function. The Jacobian $J_{\widetilde{C}}(\mathbb{F}_{q^k})$ is then defined as the group of $\mathbb{F}_{q^k}$-rational divisors of degree zero modulo principal divisors. This is a finite abelian group and forms the basis of the cryptographic schemes based on hyperelliptic curves. In this article we give an efficient algorithm for computing the group order of $J_{\widetilde{C}}(\mathbb{F}_{q^k})$ for $k \in \mathbb{N}_0$ and $\mathbb{F}_q$ a finite field of characteristic 2.

2.2 Zeta-Functions

Let N_k denote the number of $\mathbb{F}_{q^k}$-rational points on $\widetilde{C}$, i.e. $N_k = \#\widetilde{C}(\mathbb{F}_{q^k})$. The zeta function $Z(\widetilde{C}/\mathbb{F}_q;T)$ of $\widetilde{C}$ is then defined as

$$Z(\widetilde{C}/\mathbb{F}_q;T) := \exp\left(\sum_{k=1}^{\infty} \frac{N_k T^k}{k}\right) . \tag{2}$$

Weil [37] conjectured and proved that $Z(\widetilde{C}/\mathbb{F}_q;T)$ has many remarkable properties, which we summarize in the next theorem.

Theorem 1 (Weil) *Let $\widetilde{C}$ be a smooth projective curve of genus g defined over a finite field $\mathbb{F}_q$, then*

$$Z(\widetilde{C}/\mathbb{F}_q;T) = \frac{\Psi(T)}{(1-qT)(1-T)} , \tag{3}$$

where $\Psi(T) \in \mathbb{Z}[T]$ is a degree $2g$ polynomial with integer coefficients. Since $Z(\widetilde{C}/\mathbb{F}_q;0) = 1$, we have $\Psi(0) = 1$. Write $\Psi(T) = \prod_{i=1}^{2g}(1-\omega_i T)$, then $|\omega_i| = \sqrt{q}$ for $i = 1,\ldots,2g$, and we can label the ω_i such that $\omega_i \cdot \omega_{g+i} = q$ for $i = 1,\ldots,g$. Substituting the expression for $\Psi(T)$ in equation (3) and taking the logarithm of equations (2) and (3), it follows that

$$N_k = \#\widetilde{C}(\mathbb{F}_{q^k}) = q^k + 1 - \sum_{i=1}^{2g} \omega_i^k . \tag{4}$$

Furthermore, $\Psi(1) = \#J_{\widetilde{C}}(\mathbb{F}_q)$ is the group order of the Jacobian of $\widetilde{C}$ over $\mathbb{F}_q$.

The above theorem shows that it is sufficient to compute the zeta function of a hyperelliptic curve $\widetilde{C}/\mathbb{F}_q$ to recover the group order of its Jacobian $J_{\widetilde{C}}(\mathbb{F}_q)$ as $\Psi(1)$. Let $F : \overline{\mathbb{F}}_q \to \overline{\mathbb{F}}_q : x \mapsto x^q$ be the q-th power Frobenius automorphism, then F extends naturally to the Jacobian $J_{\widetilde{C}}(\mathbb{F}_q)$. Denote with $\chi(T)$ the characteristic polynomial of F on $J_{\widetilde{C}}(\mathbb{F}_q)$, then one can prove that $\Psi(T) = T^{2g}\chi(1/T)$.

2.3 *p*-adic Numbers

Let $\mathcal{K}$ be the degree n unramified extension of $\mathbb{Q}_p$ with valuation ring $\mathcal{R}$ and residue field $\mathcal{R}/p\mathcal{R} = \mathbb{F}_q$. The field $\mathcal{K}$ can be constructed as follows: let $\overline{P}(t)$ be a monic, irreducible polynomial of degree n over $\mathbb{F}_p$, such that $\mathbb{F}_q \simeq \mathbb{F}_p[t]/(\overline{P}(t))$. Take any lift $P(t) \in \mathbb{Z}_p[t]$ of $\overline{P}(t)$ of degree n, then $\mathcal{K}$ is isomorphic with $\mathbb{Q}_p[t]/(P(t))$. In practice, we represent an element α of $\mathcal{R}$ as a polynomial $\sum_{i=0}^{n-1} \alpha_i t^i$, with $\alpha_i \in \mathbb{Z}/(p^N\mathbb{Z})$, where N is called the precision of the representation. The Galois group of $\mathcal{K}$ over $\mathbb{Q}_p$ is cyclic of order n and there exists a unique generator Σ which reduces to the p-th power Frobenius $\sigma : \mathbb{F}_q \to \mathbb{F}_q : x \mapsto x^p$. This generator Σ is called the Frobenius substitution on $\mathcal{K}$. By definition Σ is a $\mathbb{Q}_p$-linear automorphism, so we can compute $\Sigma(\alpha)$ as $\sum_{i=0}^{n-1} \alpha_i \Sigma(t)^i$. Since $P(t)$ is defined over $\mathbb{Z}_p$, it follows that $P(\Sigma(t)) = 0$, which implies that $\Sigma(t)$ can be computed by the Newton iteration $Y \to Y - P(Y)/P'(Y)$ initialized with t^p. Note that Σ is not a simple powering like σ.

3 Monsky-Washnitzer Cohomology

We specialize the formalism of Monsky-Washnitzer cohomology to smooth affine plane curves. The more general case of a smooth affine variety can be found in the seminal papers by Monsky and Washnitzer [27, 24, 26], the lectures by Monsky [25] and the survey by van der Put [34].

Let C be a smooth affine plane curve over a finite field $\mathbb{F}_q$ with $q = p^n$ and let $\mathcal{K}$ be a degree n unramified extension of $\mathbb{Q}_p$ with valuation ring $\mathcal{R}$, such that $\mathcal{R}/p\mathcal{R} = \mathbb{F}_q$. The aim of Monsky-Washnitzer cohomology is to express the zeta function of the curve C in terms of a Frobenius operator $\mathcal{F}$ acting on p-adic cohomology groups $H^i(C/\mathcal{K})$ associated to C. Although "p-adic cohomology groups" sounds very complicated, these groups are simply finite dimensional $\mathcal{K}$-vectorspaces. Furthermore, the Frobenius operator $\mathcal{F}$ acts linearly on these vectorspaces which implies that $\mathcal{F}$ can be represented as a matrix over $\mathcal{K}$. For smooth affine plane curves the only non-trivial cohomology groups are $H^0(C/\mathcal{K})$ and $H^1(C/\mathcal{K})$. Let $M_\mathcal{F}$ be the matrix through which the Frobenius operator $\mathcal{F}$ acts on $H^1(C/\mathcal{K})$. The crux of the whole construction is that the characteristic polynomial of $M_\mathcal{F}$ is equal to $\chi(T)$, i.e. the characteristic polynomial of Frobenius on C.

In the remainder of this section we will give a middlebrow overview of the construction of the cohomology group $H^1(C/\mathcal{K})$. Suppose that the smooth affine plane curve C is given by an equation $\overline{g}(x, y) = 0$ and let $A := \mathbb{F}_q[x, y]/(\overline{g}(x, y))$ be its coordinate ring. Take any lift $g(x, y) \in \mathcal{R}[x, y]$ of $\overline{g}(x, y)$ and let $\mathcal{C}$ be the curve defined by $g(x, y) = 0$ with coordinate ring $\mathcal{A} := \mathcal{R}[x, y]/(g(x, y))$. To compute the zeta function of C in terms of a Frobenius operator, one needs to lift the Frobenius endomorphism F on A to the $\mathcal{R}$-algebra $\mathcal{A}$, but in general this is not possible. Note that in the special case of elliptic curves, Satoh [29] solves this problem by using the Serre-Tate canonical lift, which does admit a lift of the Frobenius endomorphism.

A first attempt to remedy this difficulty is to work with the p-adic completion $\mathcal{A}^\infty$ of $\mathcal{A}$, since we can lift F to $\mathcal{A}^\infty$. But then a new problem arises since the de Rham cohomology of $\mathcal{A}^\infty$, which provides the vectorspaces we are looking for, is too big. For example, consider the affine line over $\mathbb{F}_p$, then $\mathcal{A} = \mathcal{R}[x]$ and $\mathcal{A}^\infty$ is the ring of power series $\sum_{k=0}^\infty r_k x^k$ with $r_i \in \mathcal{R}$ and $\lim_{k\to\infty} r_k = 0$. We would like to define $H^1(A/\mathcal{K})$ as $(\mathcal{A}^\infty \otimes \mathcal{K})\, dx / \frac{d}{dx}(\mathcal{A}^\infty \otimes \mathcal{K})$, but this turns out to be infinite dimensional. For instance, it is clear that each term in the differential form $\sum_{n=0}^\infty p^n x^{p^n - 1} dx$ is exact, but its sum is not since $\sum_{n=0}^\infty x^{p^n}$ is not in $\mathcal{A}^\infty$. The fundamental problem is that $\sum_{n=0}^\infty p^n x^{p^n-1}$ does not converge fast enough for its integral to converge as well.

Monsky and Washnitzer therefore work with a subalgebra $\mathcal{A}^\dagger$ of $\mathcal{A}^\infty$, whose elements satisfy growth conditions. This *dagger ring* or *weak completion* $\mathcal{A}^\dagger$ is defined as follows: let $\mathcal{A} = \mathcal{R}[x, y]/(g(x, y))$, then $A^\dagger := \mathcal{R}\langle x, y\rangle^\dagger/(g(x, y))$, where $\mathcal{R}\langle x, y\rangle^\dagger$ is the ring of overconvergent power series

$$\left\{ \sum r_{i,j} x^i y^j \in \mathcal{R}[[x, y]] \mid \exists\, \delta, \varepsilon \in \mathbb{R}, \varepsilon > 0, \forall (i, j) : \operatorname{ord}_p r_{i,j} \geq \varepsilon(i + j) + \delta \right\} .$$

The ring $\mathcal{A}^\dagger$ satisfies $\mathcal{A}^\dagger/p\mathcal{A}^\dagger = A$ and depends up to $\mathcal{R}$-isomorphism only on A. Furthermore, Monsky and Washnitzer show that if E is an $\mathbb{F}_q$-endomorphism of A, then there exists an $\mathcal{R}$-endomorphism $\mathcal{E}$ of $\mathcal{A}$ lifting E. In particular, we can lift the Frobenius endomorphism F on A to an $\mathcal{R}$-endomorphism $\mathcal{F}$ on $\mathcal{A}$.

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

$$\mathcal{D}^1(\mathcal{A}^\dagger) := (\mathcal{A}^\dagger\ dx + \mathcal{A}^\dagger\ dy)/(\mathcal{A}^\dagger(\frac{\partial g}{\partial x}\ dx + \frac{\partial g}{\partial y}\ dy)) . \tag{5}$$

Taking the total differential of the equation $g(x, y) = 0$ gives $\frac{\partial g}{\partial x}\ dx + \frac{\partial g}{\partial y}\ dy = 0$, which accounts for the module $\mathcal{A}^\dagger(\frac{\partial g}{\partial x}\ dx + \frac{\partial g}{\partial y}\ dy)$ in the above definition.

The first cohomology group is then defined as $H^i(A/\mathcal{R}) := \mathcal{D}^1(\mathcal{A}^\dagger)/d(\mathcal{A}^\dagger)$ and $H^1(A/\mathcal{K}) := H^1(A/\mathcal{R}) \otimes_{\mathcal{R}} \mathcal{K}$ finally defines the first Monsky-Washnitzer cohomology group. Elements of $d(\mathcal{A}^\dagger)$, i.e. differentials of the form $d(l(x, y))$ for $l(x, y) \in \mathcal{A}^\dagger$, are called exact. One can prove that $H^1(A/\mathcal{K})$ is well defined and is in fact a *finite dimensional* vectorspace over $\mathcal{K}$. Furthermore, for a smooth affine curve of genus g, the dimension of $H^1(A/\mathcal{K})$ is $2g+m-1$, where m is the number of points needed to complete the affine curve to a projective curve.

4 Cohomology of Hyperelliptic Curves in Characteristic 2

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

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

with $\overline{h}(x), \overline{f}(x) \in \mathbb{F}_q[x]$, $\overline{f}(x)$ monic of degree $2g+1$ and $\deg \overline{h}(x) \leq g$. Write $\overline{h}(x)$ as $\overline{c} \cdot \prod_{i=0}^{s} (x - \overline{\theta}_i)^{m_i}$ with $\overline{\theta}_i \in \overline{\mathbb{F}}_q$, $\overline{c} \in \mathbb{F}_q$ 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 $\overline{H}(x) \mid \overline{f}(x)$. Indeed, the isomorphism defined by $x \mapsto x$ and $y \mapsto y + \sum_{i=0}^{s} b_i x^i$ transforms the curve in

$$y^2 + h(x)y = f(x) - \sum_{i=0}^{s} b_i^2 x^{2i} - h(x) \sum_{i=0}^{s} b_i x^i .$$

The polynomial $\overline{H}(x)$ will divide the right hand side of the above equation if and only if $f(\overline{\theta}_j) = \sum_{i=0}^{s} b_i^2 \cdot \overline{\theta}_j^{2i}$ for $j = 0, \ldots, s$. This is a system of linear equations in the indeterminates 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 F and it follows that the b_i^2 and therefore the b_i are elements of $\mathbb{F}_q$. We conclude that we can always assume that $\overline{H}(x) \mid \overline{f}(x)$.

Let $\overline{\pi} : C(\overline{\mathbb{F}}_q) \to \mathbb{A}^1(\overline{\mathbb{F}}_q)$ be the projection on the x-axis. It is clear that $\overline{\pi}$ ramifies at the points $(\theta_i, 0) \in \overline{\mathbb{F}}_q \times \overline{\mathbb{F}}_q$ 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 $\overline{H}(x) \mid \overline{f}(x)$. Let

C' be the curve obtained from C by removing the ramification points $(\theta_i, 0)$ for $i = 0, \ldots, s$. Then the coordinate ring A of C' is

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

Note that it is not really necessary to work with the open subset C' instead of with C itself, but it is more efficient to do so. The coordinate ring of C' contains the inverse of $\overline{H}(x)$ which will enable us to choose a particular lift of the Frobenius endomorphism F of A.

Let $\mathcal{K}$ be a degree n unramified extension of $\mathbb{Q}_2$ with valuation ring $\mathcal{R}$ and residue field $\mathcal{R}/2\mathcal{R} = \mathbb{F}_q$. Write $\overline{h}(x) = \overline{c} \cdot \prod_{i=1}^{r} \overline{P}_i(x)^{t_i}$, where the $\overline{P}_i(x)$ are 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 $P_i(x) \in \mathcal{R}[x]$ with $P_i(x) \equiv \overline{P}_i(x) \bmod 2$. 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 $\mathcal{R}$. Since $\overline{H}(x)$ divides $\overline{f}(x)$ we can define $\overline{Q_{\overline{f}}}(x) = \overline{f}(x)/\overline{H}(x)$. Let $Q_f(x) \in \mathcal{R}[x]$ be any monic lift of $\overline{Q_{\overline{f}}}(x)$ and finally set $f(x) = H(x) \cdot Q_f(x)$. The result is that we have now constructed a lift $\mathcal{C}$ of the curve C to $\mathcal{R}$ defined by the equation

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

Note that due to the careful construction of $\mathcal{C}$ we have the following properties: $H(x) \mid h(x)$, $H(x) \mid f(x)$ and $h(x) \mid H(x)^D$. Furthermore, let $\pi : \mathcal{C}(\overline{\mathcal{K}}) \to \mathbb{A}^1(\overline{\mathcal{K}})$ be the projection on the x-axis, then it is clear that π ramifies at $(\theta_i, 0)$ for $i = 0, \ldots, s$ where the θ_i are the zeros of $H(x)$.

Let $\mathcal{C}'$ be the curve obtained from $\mathcal{C}$ by deleting the points $(\theta_i, 0)$ for $i = 0, \ldots, s$, then the coordinate ring $\mathcal{A}$ of $\mathcal{C}'$ is

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

Let $\mathcal{A}^\dagger$ denote the weak completion of $\mathcal{A}$. Using the equation of the curve, we can represent any element of $\mathcal{A}^\dagger$ as a series $\sum_{i=-\infty}^{\infty}(U_i(x) + V_i(x)y)H(x)^i$, with the degree of $U_i(x)$ and $V_i(x)$ smaller that the degree of $H(x)$ if $\deg H(x) > 0$. If $H(x) = 1$, every element can be written as $\sum_{i=0}^{\infty}(U_i + V_i y)x^i$ with $U_i, V_i \in \mathcal{K}$. 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 $\mathrm{ord}_2(W(x))$ is defined as $\min_j \mathrm{ord}_2(w_j)$ for $W(x) = \sum w_j x^j \in \mathcal{K}[x]$.

Since $F = \sigma^n$ with σ the 2-nd power Frobenius, it clearly is sufficient to lift σ to an endomorphism Σ of $\mathcal{A}^\dagger$. It is natural to define Σ as the Frobenius substitution on $\mathcal{R}$ and to extend it to $\mathcal{R}[x]$ by mapping x to x^2. Using the equation of the curve we see that $\Sigma(y)$ must satisfy

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

In practice $\Sigma(y)$ is computed as a Laurent series $\sum_{i=-B_L}^{B_U}(S_i(x) + T_i(x)y)H(x)^i$ if $\deg H(x) > 0$ or $\sum_{i=0}^{B_U}(S_i + T_i y)x^i$ if $H = 1$, via the Newton iteration

$$W_{k+1} = W_k - \frac{W_k^2 + \Sigma(h(x)) \cdot W_k - \Sigma(f(x))}{2 \cdot W_k + \Sigma(h(x))} \bmod 2^{k+1}. \qquad (6)$$

Note that we have to invert $2 \cdot W_k + \Sigma(h(x))$ in the dagger ring $\mathcal{A}^\dagger$. Since $h(x) \mid H(x)^D$, we can define $Q_H(x) = H(x)^D/h(x)$, which immediately leads to $1/h(x) = Q_H(x)/H(x)^D$. We can now compute the inverse of $2 \cdot W_k + \Sigma(h(x))$ as

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

Note that $\Sigma(h(x)) \equiv h(x)^2 \bmod 2$, which implies that the denominator in the above formula is invertible in $\mathcal{A}^\dagger$. Here we are using the fact that $1/H(x)$ is an element of $\mathcal{A}^\dagger$, which explains why we work with $\mathcal{C}'$ instead of with $\mathcal{C}$.

A detailed analysis of the Newton iteration shows that if we write W_k as $\sum_{i=-L_k}^{U_k}(S_i(x)+T_i(x)y)H(x)^i$ for $\deg H(x) > 0$ or $\sum_{i=0}^{U_k}(S_i+T_iy)x^i$ if $H(x) = 1$, with $\mathrm{ord}_2(S_i(x)) < k$, $\mathrm{ord}_2(T_i(x)) < k$ and $L_k, U_k \in \mathbb{N}$, then we get the following bounds for L_k and U_k:

$$L_k \le 4kD \quad \text{and} \quad U_k \le 2k\left(\frac{\deg f(x) - 2\deg h(x)}{\deg H(x)}\right) + 2\frac{\deg h(x)}{\deg H(x)} . \tag{7}$$

In [5] we prove that the first Monsky-Washnitzer cohomology group $H^1(A/\mathcal{K})$ splits into eigenspaces under the hyperelliptic involution: a positive eigenspace $H^1(A/\mathcal{K})^+$ with basis $x^i/H(x)\,dx$ for $i = 0, \ldots, s$ and a negative eigenspace $H^1(A/\mathcal{K})^-$ with basis $x^iy\,dx$ for $i = 0, \ldots, 2g-1$. Note that the positive eigenspace corresponds to the deleted ramification points $(\theta_i, 0)$ for $i = 0, \ldots, s$ and that only the negative eigenspace $H^1(A/\mathcal{K})^-$ is related to the original curve C.

The final step in the algorithm is to compute the action of the Frobenius operator $\mathcal{F} = \Sigma^n$ on the basis of the first Monsky-Washnitzer cohomology group $H^1(A/\mathcal{K})$. However, since only $H^1(A/\mathcal{K})^-$ corresponds to the original curve C, it is sufficient to compute the action of $\mathcal{F}$ on $H^1(A/\mathcal{K})^-$ to recover the zeta function of $\widetilde{C}$. Let $M_{\mathcal{F}}$ be the matrix through which $\mathcal{F}$ acts on $H^1(A/\mathcal{K})^-$, then we can prove [5] that the characteristic polynomial of $M_{\mathcal{F}}$ is precisely the characteristic polynomial $\chi(T)$ of the Frobenius morphism on the hyperelliptic curve $\widetilde{C}$. Let M be the matrix of Σ on $H^1(A/\mathcal{K})^-$, i.e.

$$\Sigma(x^jy\;dx) \equiv \sum_{i=0}^{2g-1} M(i,j)x^iy\;dx \quad \text{for } j = 0, \ldots, 2g-1 ,$$

then one easily verifies that $M_{\mathcal{F}} = M\Sigma(M)\cdots\Sigma^{n-1}(M)$.

The only remaining difficulty in computing M is the reduction of $\Sigma(x^jy\;dx)$ on the basis of $H^1(A/\mathcal{K})^-$. Since $\Sigma(x^jy\;dx) = \Sigma(x)^j\Sigma(y)\;d(\Sigma(x))$, we get the following expansion $\Sigma(x^jy\;dx) = 2x^{2j+1}\sum_{i=-\infty}^{\infty}(S_i(x) + T_i(x)y)H(x)^i\;dx$ if $\deg H(x) > 0$ and $\Sigma(x^jy\;dx) = 2x^{2j+1}\sum_{i=0}^{\infty}(S_i + T_iy)x^i\;dx$ if $H(x) = 1$.

For $i \ge 0$ we can reduce the differential form $T_i(x)H(x)^iy\,dx$ (or $T_ix^iy\;dx$ if $H = 1$), if we know how to reduce the form $x^ky\,dx$ for $k \in \mathbb{N}$. 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 $l \geq 1$, we have the following relations

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

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

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

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

For $i < 0$ we need an extra trick to reduce the form $T_i(x)H(x)^i y\,dx$. 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 $\gcd(H(x), Q_f(x)H'(x)) = 1$. We can partially reduce $T_k(x)/H(x)^k y\,dx$ where $k = -i > 0$, by writing $T_k(x)$ as $A_k(x)H(x) + B_k(x)Q_f(x)H'(x)$, which leads to

$$\frac{T_k(x)}{H(x)^k}\,y\,dx = \frac{A_k(x)}{H(x)^{k-1}}\,y\,dx + \frac{B_k(x)Q_f(x)H'(x)}{H(x)^k}\,y\,dx\,.$$

The latter differential form can be reduced using the following congruence

$$\frac{B_k(x)}{H(x)^k}(2f'(x) + h(x)h'(x))(2y + h(x))\,dx \equiv -\frac{1}{3}(2y + h(x))^3 d\left(\frac{B_k(x)}{H(x)^k}\right)\,.$$

Substituting the expressions $h(x) = Q_h(x)H(x)$ and $f(x) = Q_f(x)H(x)$ we get

$$\frac{B_k Q_f H'}{H^k} y\,dx \equiv \frac{B_k(kH'Q_h^2 - 6Q_f' - 3Q_h h') - B_k'(4Q_f + Q_h h')}{(6 - 4k)H^{k-1}}\,y\,dx + \frac{I}{H}\,dx\,,$$

where $I(x)/H(x)\,dx$ is some invariant differential. However, we can ignore all invariant differentials since we know that $H^1(A/\mathcal{K})^-$ is stable under Σ.

5 Algorithm and Complexity

Using the formulae devised in the previous section, we describe an algorithm to compute the zeta function of a hyperelliptic curve $\widetilde{C}$ of genus g over $\mathbb{F}_q$ with $q = 2^n$. Theorem 1 implies that it is sufficient to compute the characteristic polynomial $\chi(T)$ of Frobenius and that $\chi(T)$ can be written as

$$\chi(T) = \prod_{i=1}^{2g}(T - \omega_i) = T^{2g} + a_1 T^{2g-1} + \cdots + a_{2g}\,,$$

Algorithm 1 (`Hyperelliptic_Zeta_Function`)

IN: *Hyperelliptic curve 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. $B = \left\lceil \log_2 \left(\binom{2g}{g} q^{g/2} \right) \right\rceil + 1$; $N - 3 - \lfloor \log_2(2N \deg f + g) \rfloor \geq B$;
2. $h(x), f(x), H(x), D =$ `Lift_Curve`$(\overline{h}, \overline{f})$;
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`$(2x^{2i+1}\beta_N, h, f, H, N)$;
   - 4.2. `For` $j = 0$ `To` $2g - 1$ `Do` $M[j][i] =$ `Coeff`(Red_i, j);
5. $M_{\mathcal{F}} = M \Sigma(M) \cdots \Sigma^{n-1}(M) \bmod 2^N$;
6. $\chi(T) =$ `Characteristic_Pol`$(M_{\mathcal{F}}) \bmod 2^B$;
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` $Z(\widetilde{C}/\mathbb{F}_q; T) = \dfrac{T^{2g}\chi(1/T)}{(1-T)(1-qT)}$.

with $\omega_i \cdot \omega_j = q$ for $i = 1, \ldots, g$, $|\omega_i| = \sqrt{q}$ and $a_i \in \mathbb{Z}$ for $i = 1, \ldots, 2g$. Since $q^{g-i}a_i = a_{2g-i}$ for $i = 0, \ldots, g$, it suffices to compute $a_1, \ldots, a_g$. Moreover, a_i is the sum of $\binom{2g}{i}$ products of i different zeros of the characteristic polynomial of Frobenius, so we can bound the a_i for $i = 1, \ldots, g$ by

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

Hence, to recover all the coefficients $a_1, \ldots, a_{2g}$, we need to compute an approximation of the characteristic polynomial $\chi(T)$ modulo 2^B, with

$$B \geq \left\lceil \log_2 \left(\binom{2g}{g} q^{g/2} \right) \right\rceil + 1.$$

However, it is not sufficient to compute $\Sigma(y) \bmod 2^B$, since the reduction process causes some loss of precision. In [5] we prove that for $i \in \mathbb{Z}$ the valuation of the denominators introduced during the reduction of $T_i(x)H(x)^i y\, dx$ is bounded by $c_1 = 3 + \lfloor \log_2(-i+1) \rfloor$ for $i < 0$ and $c_2 = 3 + \lfloor \log_2((i+1) \cdot \deg H + g + 1) \rfloor$ for $i \geq 0$. Combining this with the rate of convergence (7) of the Newton iteration for computing $\Sigma(y)$, we conclude that it is sufficient to compute $\Sigma(y) \bmod 2^N$

Algorithm 2 (`Lift_Frobenius_y`)

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

1. $B = \lceil \log_2 N \rceil + 1$; $T = N$; $Q_H := H^D \operatorname{div} h$;
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. $T_A \equiv \big((\alpha + \Sigma(h)) \cdot \alpha + \beta^2 \cdot f - \Sigma(f)\big) \cdot Q_H^2 \cdot H^{-2D} \bmod 2^{P[i]}$;
   - 4.2. $T_B \equiv (2\alpha - h \cdot \beta + \Sigma(h)) \cdot \beta \cdot Q_H^2 \cdot H^{-2D} \bmod 2^{P[i]}$;
   - 4.3. $D_A \equiv 1 + (\Sigma(h) - h^2 + 2\alpha) \cdot Q_H^2 \cdot H^{-2D} \bmod 2^{P[i-1]}$;
   - 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` $\alpha_N = \alpha$, $\beta_N = \beta$.

where $N \in \mathbb{N}$ satisfies

$$N - 3 - \lfloor \log_2(2N \deg f + g) \rfloor \geq B\,.$$

The function `Hyperelliptic_Zeta_Function` given in Algorithm 1 computes the zeta function of a hyperelliptic curve C defined over $\mathbb{F}_q$ where $q = 2^n$. In step 2 we call the subroutine `Lift_Curve`, which first constructs an isomorphic curve such that $\overline{H}(x) \mid \overline{h}(x)$ and $\overline{H}(x) \mid \overline{f}(x)$ and lifts the curve following the construction described in Section 4. The result of this function is a hyperelliptic curve $\mathcal{C}: y^2 + h(x)y = f(x)$ over $\mathcal{R}$ and a polynomial $H(x)$ such that $H(x) \mid h(x)$, $H(x) \mid f(x)$ and $h(x) \mid H(x)^D$. Since this function is rather straightforward, we have omitted the pseudo-code.

In step 3 we compute $\Sigma(y) \bmod 2^N$ using the function `Lift_Frobenius_y` given in Algorithm 2. This function implements the Newton iteration (6), but has quadratic, instead of linear, convergence. The parameters α_N, β_N are Laurent series in $H(x)$, with coefficients polynomials over $\mathcal{R} \bmod 2^N$ of degree smaller than $\deg H(x) > 0$. If $H(x) = 1$, then α_N, β_N are Laurent series in x.

Algorithm 3 (`Reduce_MW_Cohomology`)

IN: *Series* $G \in \mathcal{R}[x, H, H^{-1}]$*, polynomials* $h, f, H \in \mathcal{R}[x]$ *and precision* N.
OUT: $R \in \mathcal{K}[x]$*, with* $\deg R < 2g$ *such that* $Ry\,dx \equiv Gy\,dx$ *in* $H^1(\overline{A}/K)^-$.

---

1. $D_G = \deg G$; $V_G =$ `Valuation(`G`)`; $D_T = (D_G + 1) \cdot \deg H$; $T = 0$;
2. `For` $i = D_G$ `Down To` 0 `Do` $T = T \cdot H +$ `Coeff(`G, i`)` $\bmod 2^N$;
3. `For` $i = D_T$ `Down To` $2g$
  3.1. $P \equiv x^{i-2g}(2f' + h \cdot h') + \frac{i-2g}{3} x^{i-2g-1}(4f + h^2) \bmod 2^N$;
  3.2. $T \equiv T - ($`Coeff(`T, i`)`$\cdot P)/$ `Coeff(`P, i`)` $\bmod 2^N$;
4. $Q_f = f \text{ div } H$; $Q_h = h \text{ div } H$; $P = 0$;
5. `For` $i = V_G$ `To` -1
  5.1. $V \equiv P +$ `Coeff(`G,i`)` $\bmod 2^N$;
  5.2. $P \equiv V \text{ div } H \bmod 2^N$; $V \equiv V - P \cdot H \bmod 2^N$;
  5.3. $C, L_A, L_B =$ `XGCD(`$V \cdot H,\ V \cdot Q_f \cdot H',\ N$`)`;
  5.4. $P \equiv P + L_A + \frac{L_B \cdot (-iQ_h^2 \cdot H' - 3(2Q_f' + Q_h \cdot h')) - L_B' \cdot (4Q_f + Q_h h)}{6+4i} \bmod 2^N$;
6. `Return` $R \equiv T + P \bmod 2^N$.

Note that the function `Lift_Frobenius_y` is a double Newton iteration: $\alpha + \beta y$ converges to $\Sigma(y)$, whereas $\gamma + \delta y$ is an approximation of the inverse of the denominator in the Newton iteration.

Once we have determined an approximation of $\Sigma(y)$, we compute the action of Σ on the basis of $H^1(A/\mathcal{K})^-$ as $2x^{2i+1}\Sigma(y)\,dx$ for $i = 0, \ldots, 2g-1$. In step 4 we reduce these forms with the function `Reduce_MW_Cohomology` given in Algorithm 3. Note that this algorithm is based on the reduction formulae given in Section 4. The result of step 4 of Algorithm 1 is an approximation modulo 2^B of the matrix M through which Σ acts on $H^1(A/\mathcal{K})^-$. In step 5 we compute its norm $M_{\mathcal{F}}$ as $M\Sigma(M)\cdots\Sigma^{n-1}(M)$. Note that since M is not necessarily defined over $\mathcal{R}$, we have to compute this product with slightly increased precision to obtain the correct result. In steps 6 and 7 we recover the characteristic polynomial of Frobenius from the first g coefficients of the characteristic polynomial of $M_{\mathcal{F}}$. Finally, we return the zeta function of the smooth projective hyperelliptic curve $\widetilde{C}$ birational to C in Step 8.

The complexity analysis of the algorithm is similar to Kedlaya's algorithm in [14, Section 5], except that in our case the reduction takes $O(g^{5+\varepsilon}n^{3+\varepsilon})$ time instead of $O(g^{4+\varepsilon}n^{3+\varepsilon})$ time. A detailed complexity analysis can be found in [5], which proves that the zeta function of a genus g hyperelliptic curve C over a finite field $\mathbb{F}_q$ with $q = 2^n$ elements, can be computed deterministically in $O(g^{5+\varepsilon}n^{3+\varepsilon})$ bit operations with space complexity $O(g^3n^3)$.

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 some examples of Jacobians of hyperelliptic curves with almost prime group order.

The basic operations on integers modulo 2^N where $N \leq 256$ were written in assembly language. Elements of $\mathcal{R}$ mod 2^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 $\mathcal{R}_N := \mathcal{R} \bmod 2^N$, polynomials over $\mathcal{R}_N$ and Laurent series over $\mathcal{R}_N[x]$ 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%.

6.1 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 $g \cdot n$, and therefore the bit size of the group order of the Jacobian, is constant across each row.

Table 1. Running times (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	
$g \cdot n$	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

6.2 Hyperelliptic Curve Examples

In this subsection we give two 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 both curves are non-supersingular: for the genus 2 curve note that a_2 is odd and for the genus 3 curve this is trivial since there are no hyperelliptic supersingular curves of genus 3 in characteristic 2 [31]. Furthermore, both curves withstand the MOV-FR attack [8, 22].

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

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

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

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

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

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

7 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 $J_{\widetilde{C}}(\mathbb{F}_q)$ associated to C which forms the basis of the cryptographic schemes based on hyperelliptic curves. The resulting algorithm runs in $O(g^{5+\varepsilon}n^{3+\varepsilon})$ bit operations and needs $O(g^3n^3)$ storage space for a genus g hyperelliptic curve over $\mathbb{F}_{2^n}$. 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 affine curve over finite fields of small characteristic.

References

1. S. Arita. Algorithms for computations in Jacobians of C_{ab} curve 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. J. Denef and F. Vercauteren. An extension of Kedlaya's algorithm to Artin-Schreier curves in characteristic 2. *Algorithmic number theory. 5th international symposium. ANTS-V*, 2002.
5. J. Denef and F. Vercauteren. An extension of Kedlaya's algorithm to hyperelliptic curves in characteristic 2. *Preprint*, 2002.
6. N. Elkies. Elliptic and modular curves over finite fields and related computational issues. *Computational Perspectives on Number Theory*, pages 21–76, 1998.
7. M. Fouquet, P. Gaudry, and R. Harley. On Satoh's algorithm and its implementation. *J. Ramanujan Math. Soc.*, 15:281–318, 2000.
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, April 1994.
9. W. Fulton. *Algebraic curves.* Math. Lec. Note Series. W.A. Benjamin Inc., 1969.
10. S. Galbraith, S. Paulus, and N. Smart. Arithmetic on superelliptic curves. *Math. Comp.*, 71(237):393–405, 2002.
11. P. Gaudry and N. Gürel. An extension of Kedlaya's algorithm for counting points on superelliptic curves. In *Advances in Cryptology - ASIACRYPT 2001*, volume 2248 of *Lecture Notes in Computer Science*, pages 480–494, 2001.
12. 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.
13. R. Hartshorne. *Algebraic geometry.* Number 52 in Graduate Texts in Mathematics. Springer-Verlag, 1997.

14. K.S. Kedlaya. Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology. *Journal of the Ramanujan Mathematical Society*, 16:323–338, 2001.
15. N. Koblitz. *p-adic Numbers, p-adic Analysis and Zeta-Functions*, volume 58 of *GTM*. Springer-Verlag, 1977.
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. D. Lorenzini. *An Invitation to Arithmetic Geometry*. Number 9 in Graduate Studies in Mathematics. American Mathematical Society, 1996.
22. 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.
23. V. Miller. Uses of elliptic curves in cryptography. *Advances in Cryptology - ASIACRYPT '91, Lecture notes in Computer Science*, 218:460–469, 1993.
24. P. Monsky. Formal cohomology. II: The cohomology sequence of a pair. *Ann. of Math.*, 88:218–238, 1968.
25. P. Monsky. *p-adic analysis and zeta functions.* Lectures in Mathematics, Department of Mathematics Kyoto University. 4. Tokyo, Japan, 1970.
26. P. Monsky. Formal cohomology. III: Fixed point theorems. *Ann. of Math.*, 93:315–343, 1971.
27. P. Monsky and G. Washnitzer. Formal cohomology. I. *Ann. of Math.*, 88:181–217, 1968.
28. J. Pila. Frobenius maps of abelian varieties and finding roots of unity in finite fields. *Math. Comput.*, 55(192):745–763, 1990.
29. 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.
30. T. Satoh, B. Skjernaa, and Y. Taguchi. Fast computation of canonical lifts of elliptic curves and its application to point counting. *Preprint*, 2001.
31. J. Scholten and J. Zhu. Hyperelliptic curves in characteristic 2. *International Mathematics Research Notices*, 2002(17):905–917, 2002.
32. R. Schoof. Elliptic curves over finite fields and the computation of square roots mod p. *Math. Comp.*, 44:483–494, 1985.
33. B. Skjernaa. Satoh's algorithm in characteristic 2. *To appear in Math. Comp.*, 2000.
34. M. van der Put. The cohomology of Monsky and Washnitzer. *Mém. Soc. Math. France*, 23:33–60, 1986.
35. 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.
36. D. Wan. Computing zeta functions over finite fields. *Contemporary Mathematics*, 225:131–141, 1999.
37. A. Weil. *Sur les Courbes Algébriques et les Variétés qui s'en Déduisent*. Hermann, 1948.