A Quasi Quadratic Time Algorithm for Hyperelliptic Curve Point Counting. The Ramanujan Journal, 12(3):399-423, December 2006. Springer Berlin / Heidelberg.

A Quasi Quadratic Time Algorithm for Hyperelliptic Curve Point Counting*

Reynald Lercier[1,2] and David Lubicz[1,3]

[1] CELAR, Route de Laillé, F-35570 Bruz, France
[2] reynald.lercier@m4x.org
[3] lubicz@celar.fr

Abstract. We describe an algorithm to compute the cardinality of Jacobians of ordinary hyperelliptic curves of small genus over finite fields $\mathbb{F}_{2^n}$ with cost $O(n^{2+o(1)})$. This algorithm is derived from ideas due to Mestre. More precisely, we state the mathematical background behind Mestre's algorithm and develop from it a variant with quasi-quadratic time complexity. Among others, we present an algorithm to find roots of a system of generalized Artin-Schreier equations and give results that we obtain with an efficient implementation. Especially, we were able to obtain the cardinality of curves of genus one, two or three in finite fields of huge size.

1 Introduction

In [15], Koblitz draws attention to the fact that higher dimensional Jacobian varieties should be considered as interesting replacement for elliptic curves as groups in which the discrete logarithm problem is supposed to be hard. In order to avoid instances of such groups in which the discrete logarithm problem is easy to handle by the use of the Polhig-Hellman algorithm, a prerequisite to the use of such Jacobians in the same way as elliptic curves is to be able to compute their number of rational points. The attention was at first focused on the Jacobians of hyperelliptic curves because of the existence of memory saving representations of their rational points [27] and the existence of efficient algorithms to compute the group law [2].

The history of algorithms to count points on the Jacobians of hyperelliptic curves is quite parallel to the one of elliptic curve point counting. In [29], Pila describes an adaptation of Schoof's algorithm [33] to the case of hyperelliptic curves. Although the complexity of this algorithm is polynomial, it is not well suited for practical use since the improvements due to Elkies and Atkin appeared to be hard to generalize in this case. Nevertheless, Pila's algorithm has been improved in [8], leading to a computation of the number of points on a hyperelliptic curve defined over a prime field of cryptographic size [9].

In the case of finite fields of small characteristic, as in the case of elliptic curves, p-adic methods lead to dramatic improvements. These methods may be divided into two main categories:

- Cohomological methods which compute the action of the Frobenius morphism on cohomology groups defined over characteristic zero fields. These methods rely on either Monsky-Washnitzer cohomology as described in [13] and [6] or on Dwork cohomology as in [17]. Both techniques lead to polynomial time algorithms which work properly on hyperelliptic curves of any genus defined over a small characteristic finite field.
- Lifting methods which compute the action of the Frobenius morphism on the canonical lift of the Jacobian of the hyperelliptic curves. This leads to a very efficient method for elliptic curves and even curves of genus two defined over a field of characteristic two as described in [23].

The purpose of this article is to describe an efficient p-adic point counting algorithm which belongs to the latter category. This algorithm is a variant of some ideas due to Mestre [22]. It can be considered as a generalization of the classical AGM algorithm which leads to a more efficient point counting algorithm for elliptic curves defined over a field of characteristic two [19, 12]. More precisely, we prove the following result.

* January 10, 2015

Theorem 1. *Let $\kappa = \mathbb{F}_{2^n}$ be a finite field of characteristic two and X be a hyperelliptic curve defined over κ, the Jacobian of which is ordinary and κ-simple, then there exists an algorithm with asymptotic time complexity $O(n^{2+o(1)})$-bit operations and asymptotic space complexity $O(n^2)$-bits to compute the characteristic polynomial of the Frobenius morphism acting on the curve X.*

The conditions for the Jacobian of X in Theorem 1 are generic. This practically means that, if we pick "at random" a curve, the algorithm almost always returns the correct result.

After having fixed some notations and stated the problem that we study (Sect. 2), we introduce some facts about theta functions (Sect. 3) since it turns out that these mathematical objects are of importance in the remainder of the article. Then, we explore Mestre's algorithm from a mathematical viewpoint (Sect. 4) before explaining how we can derive from it an efficient variant (Sect. 5). Sections 4 and 5 are organized in a similar way. At first, we are interested in the lifting of the Jacobian of a curve. Then, we look carefully at the action of a specific isogeny on this lift and finally derive from it an action on the determinant of the invariant differentials on this Jacobian. The very last stage requires one to pick random points on the Jacobian in order to obtain the correct characteristic polynomial of the Frobenius morphism. This turns the algorithm into a probabilistic method.

Notations and complexity hypothesis. Throughout this article, p is a small prime (typically $p = 2$), $q = p^n$ and $\mathbb{F}_q$ is the finite field with q elements. We denote by K_q the unramified extension of degree n of $\mathbb{Q}_p$, by $\mathbb{Z}_q$ or R_q its valuation ring, by σ the Frobenius substitution of K_q considered as an extension of $\mathbb{Q}_p$ and by F the n^{th}-power Frobenius σ^n. For each $i \in \mathbb{N}^*$, we have a canonical projection $\pi_i : R_q \longrightarrow R_q/p^iR_q$ (π_1 is the projection onto the finite field $\mathbb{F}_q$). If an object can be represented by a finite set of elements S of R_q, we say that we have computed this object to precision m, if we can compute representatives of the image of S by the projection π_m.

We denote by v the canonical valuation of K_q, that is the one deduced from the unique extension to K_q of the p-adic valuation of $\mathbb{Q}_p$. Let $M_{k,l}(K_q)$ denote the K_q-vector space of matrices with coefficients in K_q. If $x = (x_{ij}) \in M_{k,l}(K_q)$, we denote by v the valuation given by $v(x) = \min\{v(x_{ij}), i = 1, \ldots, k, j = 1, \ldots, l\}$. Let us note that we have $v(xy) \geqslant v(x)+v(y)$ for all $x \in M_{k,l}(K_q)$ and $y \in M_{l,m}(K_q)$. Moreover, for any $\Sigma \in \mathrm{Gal}(K_q/\mathbb{Q}_p)$ and $x = (x_{ij}) \in M_{k,l}(K_q)$, we put $x^\Sigma = (t_{ij}) \in M_{k,l}$ the matrix defined by $t_{ij} = x_{ij}^\Sigma$. In the same manner, if $(x, y) \in M_{k,l}(K_q) \times M_{k,l}(K_q)$, we say that $x \equiv y \bmod p^m, m \in \mathbb{N}$ if for $1 \leqslant i \leqslant k$ and $1 \leqslant j \leqslant l$, $x_{ij} \equiv y_{ij} \bmod p^m$.

Finally, we assume that the multiplication of two n-bit length integers takes $O(n^\mu)$-bit operations. With the FFT multiplication algorithm, $\mu = 1 + \epsilon$ for any positive real ϵ as long as n is large enough, with Karatsuba, $\mu = \log_2(3)$ and with a naive multiplication algorithm, $\mu = 2$. Following the conventions of [32], we denote by $T_{w,n}$ the complexity in time of multiplying two elements of R_{p^n} with precision w. Furthermore, in the following $S_{w,n}$ is the complexity of the Frobenius (or the inverse Frobenius) substitution.

2 Point Counting

Let C be a projective smooth algebraic curve of genus g defined over a field $\kappa = \mathbb{F}_q$ with $q = p^n$. Let $\overline{\kappa}$ be the algebraic closure of κ. We recall that the Frobenius σ (resp. the n^{th}-power Frobenius F) is the affine morphism defined locally from C to a curve C' (resp. C) on the κ-algebra affine coordinate rings A and A' by the map $x \longrightarrow x^p$ (resp. $x \longrightarrow x^{p^n}$). We can define the set of κ-rational points of C as the $\overline{\kappa}$-points of C which are invariant under the action of F.

Then we can associate with C its Jacobian variety, J, which is a group variety of dimension g defined over κ with $\mathrm{Pic}_0(C)$ as underlying group structure. For an integer ℓ prime to p, we denote by $J[\ell]$ the subgroup of ℓ-torsion points of J. It is isomorphic as a group to $(\mathbb{Z}/\ell\mathbb{Z})^{2g}$. Moreover, if for $i \in \mathbb{N}$, $[i]$ denotes the multiplication by i in J, then, for $i > j$, we have a canonical projection $J[\ell^i] \longrightarrow J[\ell^j]$ given by the morphism $[\ell^{i-j}]$ which verifies the usual compatibility relations, so that we can define the Tate module as the projective limit $T_\ell = \varprojlim J[\ell^i]$. This is a free $\mathbb{Z}_\ell$ module of dimension $2g$. The elements of the Galois group of $\mathrm{Gal}(\overline{\kappa}/\kappa)$ act upon J and consequently upon $J[\ell]$ in a way which fits

with the projection morphism, so that we get a morphism $\rho_\ell : \mathrm{Gal}(\overline{\kappa}/\kappa) \longrightarrow \mathrm{Aut}_{\mathbb{Z}_\ell}(T_\ell)$, called the ℓ-adic representation. Tensoring T_ℓ by $\mathbb{Q}_\ell$ over $\mathbb{Z}_\ell$, we obtain a morphism $\rho_\ell : \mathrm{Gal}(\overline{\kappa}/\kappa) \longrightarrow \mathrm{Aut}_{\mathbb{Q}_\ell}(\mathbb{Q}_\ell^{2g})$.

As a consequence, we can define the characteristic polynomial χ_F of the n^{th}-power Frobenius morphism which is a generator of $\mathrm{Gal}(\overline{\kappa}/\kappa)$. Let us recall that χ_F is a monic integer polynomial and that the Riemann hypothesis for curves states that if we set $\chi_F(x) = \prod(x - \lambda_i)$ with $\lambda_i \in \mathbb{C}$, then $|\lambda_i| = q^{1/2}$. Furthermore, it is well known that $\chi_F(1)$ is simply the number of κ-rational points of $J(C)$. Our aim is to give an efficient algorithm to compute χ_F for projective smooth algebraic hyperelliptic curves of genus g defined over an extension κ of degree n of $\mathbb{F}_2$.

Now, given a hyperelliptic curve C defined over κ and its Jacobian variety J, one can consider the set S of algebraic group schemes defined over the Witt vectors $W(\kappa)$ which reduce modulo 2 to J. There is a distinguished element of S, called the canonical lift, with the property that there exists an automorphism acting on it which reduces modulo 2 to the Frobenius morphism. If J is ordinary, by classical considerations on the equivalence between the rational representation of the endomorphisms ring of an abelian variety and the direct sum of the analytic representation and its conjugate [35], one can see that the action of the dual of the Frobenius morphism on the differential forms of the dual of the canonical lift gives half of the eigenvalues of the Frobenius morphism. From these remarks, we deduce the general strategy of the algorithm described in this paper. First, we compute to a given precision the values of certain invariants called Theta constants attached to the canonical lift of J by iterating "duplication" formulas. Then we compute the action of the lift of the dual of the Frobenius morphism on these invariants and finally, we recover the determinant of the action of the Frobenius morphism by computing a quotient of some Theta constants.

3 Theta Functions and Hyperelliptic Curves

3.1 Theta Functions with Rational Characteristic

Let V be a $\mathbb{C}$-vector space of dimension g, and assume we are given an embedding of $\mathbb{R}$ into $\mathbb{C}$, so that we can view V as a $\mathbb{R}$-vector space of dimension $2g$. Let Λ be a lattice of V, that is a discrete subgroup of V of rank $2g$ over $\mathbb{Z}$. We consider the quotient space $W = V/\Lambda$ and the canonical projection $\pi : V \longrightarrow W$. It is well known that W inherits the structure of an analytic variety from V and that V is the universal covering of the analytic torus W. In this article, we are interested only in analytic tori which have a significance in algebraic geometry, that is the ones which are endowed with a projective embedding.

In order to characterize these tori, we take a basis e of V and we identify by means of e, as $\mathbb{C}$-vector space, V with $\mathbb{C}^g$. In such a basis, Λ can be represented by a $g \times 2g$ matrix with coefficients in $\mathbb{C}$, the column vectors of which are generators of Λ represented in the basis e. It can then be shown that a torus is analytically isomorphic to a projective analytic variety if and only if we can choose e such that, Λ is represented by a matrix of the form $(\Delta_g|\Omega)$ with Δ_g a diagonal matrix of dimension g with integer coefficients and Ω a symmetric matrix with complex coefficients such that $\mathrm{Im}\,\Omega > 0$. If Δ_g is the identity matrix I_g, then we say that W admits a principal polarization. In the sequel, we only consider principally polarized analytic tori. We denote by $\mathscr{H}_g$ the Siegel upper half plane, that is the set of such matrices Ω. Every point $x \in \mathbb{C}^g$ can then be written as $x = \eta I_g + \varepsilon\Omega$, where $\left[\begin{smallmatrix}\eta\\ \varepsilon\end{smallmatrix}\right] \in (\mathbb{R}^g)^2$ is called the characteristic of x. In the sequel we always assume that these conditions are fulfilled so that W is an Abelian variety.

We can associate with such an Abelian variety its Riemann theta function, which is a global holomorphic function of V verifying the following functional equations,

$$\theta(-z,\Omega) = \theta(z,\Omega), \qquad \theta(z+\alpha,\Omega) = \theta(z,\Omega),$$
$$\theta(z+\Omega\alpha,\Omega) = \exp(-\pi i\,{}^t\alpha\Omega\alpha - 2\pi i\,{}^t\alpha z)\theta(z,\Omega),$$

for $z \in \mathbb{C}^g$ and $\alpha \in \mathbb{Z}^g$. Such a function can be given by convergent series of holomorphic functions,

$$\theta(z,\Omega) = \sum_{N\in\mathbb{Z}^g} \exp(\pi i\,{}^tN\Omega N + 2\pi i\,{}^tNz).$$

More generally, we can consider functions on V which satisfy the following functional equations for $z \in \mathbb{C}^g$, $\eta, \varepsilon \in \mathbb{Q}^g$, $\alpha \in \mathbb{Z}^g$,

$$\theta_\ell \left[\begin{smallmatrix}\eta\\ \varepsilon\end{smallmatrix}\right](z+\alpha,\Omega) = \exp(2\pi i \ell\, {}^t\eta\alpha)\theta_\ell \left[\begin{smallmatrix}\eta\\ \varepsilon\end{smallmatrix}\right](z,\Omega),$$
$$\theta_\ell \left[\begin{smallmatrix}\eta\\ \varepsilon\end{smallmatrix}\right](z+\Omega\alpha,\Omega) = \exp(-2\pi i \ell\, {}^t\varepsilon\alpha)\exp(-\pi i \ell\, {}^t\alpha\Omega\alpha - 2\pi i\, {}^t\alpha z)\theta_\ell \left[\begin{smallmatrix}\eta\\ \varepsilon\end{smallmatrix}\right](z,\Omega).$$

Such a function is called an ℓ-th order theta functions with characteristic $[\eta, \varepsilon]$. The relation with Riemann theta functions is the following. First, we have

$$\theta \left[\begin{smallmatrix}\eta\\ \varepsilon\end{smallmatrix}\right](z,\Omega) = \exp(\pi i\, {}^t\eta\Omega\eta + 2\pi i\, {}^t\eta(z+\varepsilon))\theta(z+\Omega\eta+\varepsilon,\Omega),$$

and then, it can be shown that a basis of the $\mathbb{C}$-vector space of ℓ-th order theta functions is provided by the functions

$$\theta \left[\begin{smallmatrix}\eta+\rho/\ell\\ \epsilon\end{smallmatrix}\right](\ell z, \ell\Omega) \tag{1}$$

with $\rho \in (\mathbb{Z}/\ell\mathbb{Z})^g$ [7].

3.2 Some Relations between Theta Functions

Let Θ be the theta divisor on W, that is the unique divisor such that $\pi^{-1}(\Theta)$ is the zero set of the Riemann theta function and $\mathscr{B}$ be the line bundle associated to Θ. The divisor Θ is defined modulo a translation by the data of a rational $(1,1)$ cohomology class on W which is called the polarization of W. This polarization simply is the cohomology class of the curvature form of $\mathscr{B}$ or the Poincaré dual of Θ. The Kodaira embedding theorem asserts that for ℓ sufficiently large, global holomorphic sections of $\mathscr{B}^{\otimes\ell}$ provide a projective immersion of W (in fact, by a theorem due to Lefschetz, $\ell = 2$ suits and for $\ell \geqslant 3$ this immersion is an embedding). Moreover, the ℓ-th order theta functions with rational characteristic $\left[\begin{smallmatrix}\eta\\ \epsilon\end{smallmatrix}\right]$ can be seen as global sections of the line bundle $\mathscr{B}^{\otimes\ell}$ translated by the point of characteristic $\frac{1}{\ell}\left[\begin{smallmatrix}\eta\\ \epsilon\end{smallmatrix}\right]$. By taking the quotient of these sections or sum of first and second order logarithmic derivatives of these sections, we obtain all the global meromorphic sections of the line bundle associated with the divisor $\pi^{-1}(\ell\Theta)$. For instance, in the case of elliptic curves, we recover the classical functions $\mathscr{P}$ and $\mathscr{P}'$ of Weierstrass. As a matter of fact, there exists numerous relations between all these theta functions. Among them, we state those which are used in Mestre's algorithm.

Riemann duplication formulas. First, we have the following duplication formulas due to Riemann [7, p. 3], for $z_1, z_2, \in \mathbb{C}^g$ and $\eta, \eta', \varepsilon \in \frac{1}{2}\mathbb{Z}^g$,

$$\theta \left[\begin{smallmatrix}\eta\\ \varepsilon\end{smallmatrix}\right](2z_1, 2\Omega)\theta \left[\begin{smallmatrix}\eta'\\ \varepsilon\end{smallmatrix}\right](2z_2, 2\Omega) = \frac{1}{2^g}\sum_{e\in(\mathbb{Z}/2\mathbb{Z})^g} (-1)^{4\, {}^t\eta e}\theta \left[\begin{smallmatrix}\eta+\eta'\\ \varepsilon+e\end{smallmatrix}\right](z_1+z_2,\Omega)\theta \left[\begin{smallmatrix}\eta+\eta'\\ e\end{smallmatrix}\right](z_1-z_2,\Omega), \tag{2}$$

which enable us to compute the values of theta functions with respect to a duplicated period matrix. Let us note that these formulas apply to any Abelian variety.

Jacobian of hyperelliptic curves. Thomae-Fay formulas only deal with Abelian varieties which come from Jacobian varieties of hyperelliptic curves defined over $\mathbb{C}$. All Abelian varieties of dimension two are Jacobian varieties of hyperelliptic curves whereas this is not the case for a higher dimension. It should be mentioned that in the case of varieties of genus three, Ritzenthaler gives an analog of the Thomae-Fay formulas [30].

Let X be a hyperelliptic curve defined over $\mathbb{C}$ of genus g, that is a projective algebraic smooth curve which we view as a two sheeted covering of the projective line $\mathbb{P}^1_{\mathbb{C}}$. Such a curve can be provided with an embedding in $\mathbb{P}^2_{\mathbb{C}}$ by an equation of the form

$$y^2 + h(x)y = u(x), \tag{3}$$

with $\deg u(x) = 2g+2$ and $\deg h(x) \leqslant g+1$. It is a consequence of a theorem due to Riemann that such a curve together with a twofold map $X \to \mathbb{P}^1_{\mathbb{C}}$ is defined modulo an isomorphism by its ramification points in $\mathbb{P}^1(\mathbb{C})$, $B = \{a_1, \ldots, a_{2g+2}\}$. For simplicity, in the sequel we assume that $B \subset \mathbb{C} \subset \mathbb{P}^1_{\mathbb{C}}$. We know that $H_1(X, \mathbb{Z})$ is a free $\mathbb{Z}$-module of rank $2g$, a basis of which may be represented by A-cycles and B-cycles. Their images by the projection $(x, y) \longrightarrow x$ can be drawn, for instance, as in Fig. 1. In this article, all the statements use this basis to represent $H_1(X, \mathbb{Z})$.

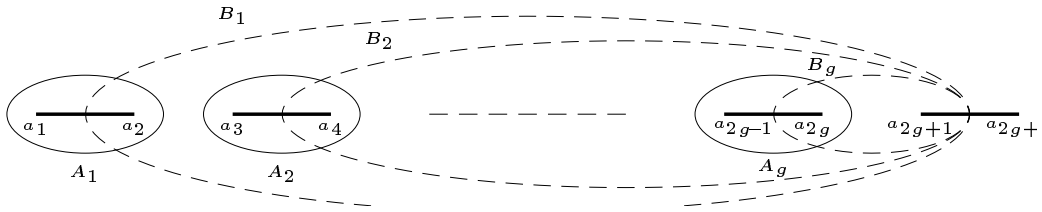

Fig. 1. A basis of $H_1(X, \mathbb{Z})$ with X, a hyperelliptic curve.

Moreover, $H^0(X, \Omega^1)$ is a $\mathbb{C}$-vector space of dimension g. Let $\omega_1, \ldots, \omega_g$ be a basis of $H^0(X, \Omega^1)$. Then, we consider the lattice $\Lambda' \subset \mathbb{C}^g$ generated by the $\mathbb{R}$-free $2g$ vectors defined by the period integrals

$$\chi_i = \left(\int_{A_i} \omega_j \right)_{j=1,\ldots,g}, \qquad \chi_{i+g} = \left(\int_{B_i} \omega_j \right)_{j=1,\ldots,g},$$

and we normalize $(\omega_j)_{j=1,\ldots,g}$ so that $(\chi_i)_{i=1,\ldots,g}$ is the canonical basis of $\mathbb{C}^g$. Then, putting $\Omega_{ij} = \int_{B_i} \omega_j$, it is an immediate consequence of Riemann bilinear relations that the matrix Ω_{ij} is symmetric and that $\mathrm{Im}\,(\Omega_{ij})$ is definite positive, so that $\mathbb{C}^g/\Lambda$ with Λ, the lattice generated by the column vectors of $(I_g|\Omega)$, is an algebrizable torus called the analytic Jacobian of X.

There is now a very convenient description of the 2-torsion part of $\mathrm{Pic}_0(X)$ in terms of its ramification points B. Let L be the divisor class in $\mathrm{Pic}(X)$ of $2a_{2g+2}$ and, for T a subset of B of even cardinality, e_T be defined in $\mathrm{Pic}_0(X)$ by $e_T = \sum_{P \in T} P - (\sharp T/2)L$.

Lemma 1. *Let the symmetric difference $\circ$ of two sets T and T' be defined by $T \circ T' = T \cup T' - T \cap T'$, then*

- $2e_T = 0$;
- $e_{T \circ T'} = e_T + e_{T'}$;
- $e_T = e'_T$ *if and only if* $T = T'$ *or* $T = B - T'$.

From this, we deduce immediately that the set $\{e_T \mid T \subset B \text{ with } \sharp T \bmod 2 = 0\}$ generates the sub-$\mathbb{Z}/2\mathbb{Z}$-module of $\mathrm{Pic}_0(X)$ of 2-torsion points. We remark that this description of $\mathrm{Pic}_0(X)$ is available independently of the base field of the variety X as long as the ramification points of X are rational over that field. It is moreover easy to relate the set $\{e_T\}$ with its image in the analytic Jacobian by the Jacobi correspondence with respect to the A-cycles and B-cycles chosen basis.

Lemma 2 ([27, p. 3.86])**.** *Let Λ_Ω be the lattice generated by the matrix $(I_g|\Omega)$. If $D - (\deg D)\, a_{2g+2}$ is a degree zero divisor of X, we put*

$$I(D) = {}^t\left(\sum_{P_j \in D} \int_{a_{2g+2}}^{P_j} \omega_j \right)_{j=1,\ldots,g} \in \mathbb{C}^g/\Lambda_\Omega.$$

Then $I(e_{\{a_{2i-1}, a_{2i}\}}) = {}^t(0, \ldots, 1/2, \ldots, 0) \bmod \Lambda_\Omega$, where $1/2$ is at the i-th position and, similarly, $I(e_{\{a_{2i}, \ldots, a_{2g+1}\}}) = {}^t(\Omega_{1i}/2, \ldots, \Omega_{gi}/2) \bmod \Lambda_\Omega$.

Thomae-Fay Formulas. We are now going to state the Thomae-Fay formulas. Let $S = \{a_1, a_3, \ldots, a_{2g+1}\}$ be the subset of points of B with odd index and U_i, be the set of pairs $\{a_{2i-1}, a_{2i}\}$ for $i = 1, \ldots, g$. Let $V_{1/2}^g$ be the set of vectors of dimension g the components of which are in the set $\{0, 1/2\}$ and for $\varepsilon \in V_{1/2}^g$, we put $U_\varepsilon = \cup_j U_j$ with j spanning the set of indices of non zero components in ε. With these settings, the Thomae-Fay formulas are [27, p. 120],

$$\theta \left[\begin{smallmatrix} 0 \\ \varepsilon \end{smallmatrix} \right]^4 (0, \Omega) = \pm\zeta \prod_{a_i, a_j \in S \circ U_\varepsilon, i<j} (x_{a_i} - x_{a_j}) \prod_{a_i, a_j \notin S \circ U_\varepsilon, i<j} (x_{a_i} - x_{a_j}) \tag{4}$$

for all $\varepsilon \in V_{1/2}^g$, ζ a constant independent of ε which can be computed explicitly (see for instance [7, p. 47]), x_{a_i}, the x-coordinates of the points a_i and $\circ$, the symmetric difference.

Action of $\mathrm{Sp}_{2g}(\mathbb{Z})$. There exists a group action of $\mathrm{Sp}_{2g}(\mathbb{Z})$ on $\mathbb{C}^g \times \mathscr{H}_g$. If $\left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix} \right) \in \mathrm{Sp}_{2g}(\mathbb{Z})$ with $(\alpha, \beta, \gamma, \delta) \in M_g(\mathbb{Z})^4$, then this action is defined by

$$\left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix} \right) (z, \Omega) = ({}^t(\gamma\Omega + \delta)^{-1} z, (\alpha\Omega + \beta)(\gamma\Omega + \delta)^{-1}).$$

Let Γ_n be the subgroup of elements $M \in \mathrm{Sp}_{2g}(\mathbb{Z})$ such that $M \equiv I_{2g} \bmod n$. With these notations, we can state a functional equation satisfied by the theta functions [26, p. 189]. For all $z \in \mathbb{C}^g$, $(\eta, \varepsilon) \in V_{1/2}^g \times V_{1/2}^g$ and $\left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix} \right) \in \Gamma_2$,

$$\theta \left[\begin{smallmatrix} \eta \\ \varepsilon \end{smallmatrix} \right]^2 ({}^t(\gamma\Omega + \delta)^{-1} z, (\alpha\Omega + \beta)(\gamma\Omega + \delta)^{-1}) = \pm \det(\gamma\Omega + \delta) \theta \left[\begin{smallmatrix} \eta \\ \varepsilon \end{smallmatrix} \right]^2 (z, \Omega). \tag{5}$$

4 Mestre's Algorithm

Let $q = 2^n$, $\kappa = \mathbb{F}_q$, K_q be the unramified extension of degree n of $\mathbb{Q}_2$ and R_q be its integer ring with maximal ideal $\mathfrak{M}$, we give in this section an overview of Mestre's algorithm. We begin with a brief account on Satoh's algorithm for elliptic curves.

Satoh's algorithm overview. Let E be an ordinary elliptic curve defined over $\mathbb{F}_q$. Then, we can consider a lift $\tilde{E}$ of E to K_q. This is an elliptic curve defined over K_q which reduces modulo two to E. All these curves may be obtained by taking, for instance, a minimal Weierstrass equation [36, p. 172] defined over K_q which reduces modulo two to the Weierstrass equation of E. Then we can consider a sequence of isogenous elliptic curves $\tilde{E}_i$ with $\tilde{E} = \tilde{E}_0$ and morphisms $\sigma_i : \tilde{E}_i \longrightarrow \tilde{E}_{i+1}$. By a theorem due to Lubin-Serre-Tate [20], if σ_i reduces modulo two to the Frobenius morphism, then the sequence $\tilde{E}_i$ converges p-adically towards the canonical lift E^{can} of E. This lift is defined by the property that we have an isomorphism induced by the reduction morphism $\mathrm{End}(E^{\mathrm{can}}) \simeq \mathrm{End}(E)$. In fact, in his algorithm, Satoh [31] uses the dual of the Frobenius morphism which is easier to handle in the case of non-supersingular curves because it is separable. Then it is easy to compute the n^{th}-power Frobenius morphism or its dual as the composition of n Frobenius morphisms. The unit eigenvalue of the Frobenius morphism can be obtained either, as the first coefficient of the action of the lift of the Frobenius on the formal group of the elliptic curve or, alternatively, by the way of the injection $\mathrm{End}(E^{\mathrm{can}}) \longrightarrow K_q$ given by the action of an endomorphism on the invariant differentials [36, p. 163].

A convergence theorem. Let R be an integral ring with quotient field K, κ a field and $\pi : R \to \kappa$ a surjective ring morphism. An element $x \in R$ is a lift of $x_0 \in \kappa$ if $\pi(x) = x_0$. More generally, a scheme X over $\mathrm{Spec}(R)$ is a lift of a scheme X_0 over $\mathrm{Spec}(\kappa)$ if, we have that $X \times_{\mathrm{Spec}(R)} \mathrm{Spec}(\kappa)$ is $\mathrm{Spec}(\kappa)-$isomorphic to X_0. A variety X_K over K is a lift of a variety over κ if there exists a lift X of X_0 over $\mathrm{Spec}(R)$ such that X_K is isomorphic to $X \times_{\mathrm{Spec}(R)} \mathrm{Spec}(K)$. In practice, if X_0 is a hyperelliptic curve over κ, the equation of such a lift, if it exists, may be obtained by lifting the coefficients of (3).

If J_0 is the Jacobian variety of X_0, which is a projective algebraic variety over $\kappa = \mathbb{F}_q$, we can consider a lift J^1 over K_q of J_0. Let us denote by $\mathfrak{J}^1$ the Néron model of J^1, which is a group scheme over R_q, and

following [3], let $\mathfrak{J}^1[2]^{\mathrm{loc}}$ be the subgroup of the R_q-points of 2-torsion of $\mathfrak{J}^1$ which reduces to zero modulo two. Let $\mathfrak{J}^2$ be the quotient of $\mathfrak{J}^1$ by $\mathfrak{J}^1[2]^{\mathrm{loc}}$, we get an isogeny, $\mathfrak{J}^1 \longrightarrow \mathfrak{J}^2$, which modulo two reduces to the Frobenius morphism. Repeatedly, we obtain a sequence of isogenies between Néron models,

$$\mathfrak{J}^1 \xrightarrow{\sigma^1_{\mathrm{ner}}} \cdots \xrightarrow{\sigma^{m-1}_{\mathrm{ner}}} \mathfrak{J}^m \xrightarrow{\sigma^m_{\mathrm{ner}}} \cdots \xrightarrow{\sigma^{m+n-1}_{\mathrm{ner}}} \mathfrak{J}^{m+n} \quad . \tag{6}$$

By a generalization of a theorem due to Lubin-Serre-Tate [20] [3, Theorem 4 p. 3], there exists an isomorphism

$$\Phi : \mathfrak{J}^m \times_{\mathrm{Spec}(R_q)} \mathrm{Spec}(R_q/\mathfrak{M}^m) \longrightarrow \mathfrak{J}^{m+n} \times_{\mathrm{Spec}(R_q)} \mathrm{Spec}(R_q/\mathfrak{M}^m) \tag{7}$$

which lifts the n^{th}-power Frobenius morphism of $J^m = \mathfrak{J}^m \times_{\mathrm{Spec}(R_q)} \mathrm{Spec}(\kappa)$ to the precision m. In other words, $\mathfrak{J}^m \times_{\mathrm{Spec}(R_q)} \mathrm{Spec}(K_q)$ is an approximation of the canonical lift of J_0 to precision m.

Lifting isogenies. For computational reasons, we only consider finite lifts. An element $x \in R_q$ is a finite lift of $x_0 \in \mathbb{F}_q$ if x is a lift of x_0 and x can be written as a finite sum $\sum_{i=0}^m f_{j_i} \varpi^i$ where $m \in \mathbb{N}$, ϖ is the uniformizer of R_q, $f_1, \ldots, f_{2^n}$ a system of representatives of $\mathbb{F}_q$ in R_q and $j_i \in \{1, \ldots, 2^n\}$. This can be formulated in another way. Let K be a number field obtained by an extension of $\mathbb{Q}$ of degree n which is inert above the prime two. Such a field may be defined, for instance, by quotienting $\mathbb{Q}[T]$ by the principal ideal defined by any lift in $\mathbb{Z}[T]$ of a defining polynomial of the extension $\mathbb{F}_q/\mathbb{F}_2$ [28, p. 47]. Then, an element $x \in R_q$ is a finite lift of $x_0 \in \mathbb{F}_q$, if it is a lift of x_0 and if it is in the dense image of the canonical morphism $K \longrightarrow K \otimes_{\mathbb{Q}} \mathbb{Q}_p = K_q$.

Now, let X_0 be a hyperelliptic curve of genus g over κ given with an embedding in $\mathbb{P}^2_\kappa$ by (3). In the sequel, we assume that the Jacobian variety J_0 of X_0 is ordinary, which means that its 2-rank is equal to g. By the description of the 2-torsion of J_0 in terms of the divisors with support in the ramification points given by Lemma 1, as the x-coordinates of the ramification points of X_0, with respect to the projection $(x, y) \longrightarrow x$, are the zeros of the discriminant $\Delta = h(x)$, this means that $\deg h(x) = g + 1$. Moreover, we may take $\deg u(x) = 2g + 2$ [8].

Now in order to make the link between (6) and the theta functions, we consider X, a lift of X_0 over K given by any finite lift of (3). We suppose that the ramification points $B = \{a_1, \ldots, a_{2g+2}\}$ are rational over K. Their x-coordinates are given as the zeros of the discriminant $\Delta = h(x)^2 - 4u(x)$ and we may index the ramification points so that $a_i \simeq a_{i+1} \bmod 2$. Let J^1_{alg} be the Jacobian variety of X which is a projective group variety over K. To define an analytic model for J^1_{alg}, we fix an embedding $\iota : K \longrightarrow \mathbb{C}$ such that we may consider X and J^1_{alg} as projective algebraic varieties over $\mathbb{C}$. Taking again the same conventions for the A-cycles and B-cycles as in Sect. 3.2, we can define a period matrix $(I_g|\Omega)$ with respect to a basis of $\mathbb{C}^g$, an analytic torus $J^1_{\mathrm{an}} = \mathbb{C}^g/\Lambda_\Omega$ with an analytic isomorphism $\phi : J^1_{\mathrm{an}} \longrightarrow J^1_{\mathrm{alg}}$. An immediate consequence of the Lemma 2 is that the g-rank of the sub-$\mathbb{Z}/2\mathbb{Z}$-module of the 2-torsion of J^1_{an} generated by the elements with coordinates $(0, \ldots, 1/2, \ldots, 0)$ is sent by ϕ to the elements of $\mathrm{Pic}_0(X)$ generated by the elements e_{T_i} with $T_i = \{a_{2i-1}, a_{2i}\}$, $i = 1, \ldots, g$. But with the chosen numbering of the ramifications points, this is exactly the sub-module of J^1_K which is sent to zero in J_0 by the reduction modulo two. Moreover, from Lemma 1 and from the fact that the ramification points of X are defined over K, we know that the 2-torsion of J^1_{alg} is defined over K.

Now, if J^2_{an} is defined by the lattice $\Lambda_{2\Omega}$, we can consider the isogeny $J^1_{\mathrm{an}} \longrightarrow J^2_{\mathrm{an}}$ defined by the inclusion of lattices $2\Lambda_\Omega \subset \Lambda_{2\Omega}$. By the Gaga principle [34], this gives an isogeny $\sigma^1 : J^1_{\mathrm{alg}} \longrightarrow J^2_{\mathrm{alg}}$ which, by definition, is obtained by quotienting J^1_{alg} by the 2-torsion part of J^1_{alg} which reduces to zero modulo two. As this subgroup is defined over K, σ^1 is a K-morphism of K-varieties. Repeatedly, we get the following commutative diagram,

$$\begin{array}{ccccccccc}
J^1_{\mathrm{an}} & \xrightarrow{\sigma^1_{\mathrm{an}}} & \cdots & \xrightarrow{\sigma^{m-1}_{\mathrm{an}}} & J^m_{\mathrm{an}} & \xrightarrow{\sigma^m_{\mathrm{an}}} & \cdots & \xrightarrow{\sigma^{m+n-1}_{\mathrm{an}}} & J^{m+n}_{\mathrm{an}} \\
\downarrow & & & & \downarrow & & & & \downarrow \\
J^1_{\mathrm{alg}} & \xrightarrow{\sigma^1_{\mathrm{alg}}} & \cdots & \xrightarrow{\sigma^{m-1}_{\mathrm{alg}}} & J^m_{\mathrm{alg}} & \xrightarrow{\sigma^m_{\mathrm{alg}}} & \cdots & \xrightarrow{\sigma^{m+n-1}_{\mathrm{alg}}} & J^{m+n}_{\mathrm{alg}}
\end{array} \quad .$$

Take a minimal extension K' of K such that the second row is a sequence of K'-morphisms of K' varieties. Then tensoring over $\mathbb{Q}$ by $\mathbb{Q}_p$, this row gives a sequence of K_q-morphism of K_q-varieties,

$$J^1_{K_q} \xrightarrow{\sigma^1_{\mathrm{loc}}} \cdots \xrightarrow{\sigma^{m-1}_{\mathrm{loc}}} J^m_{K_q} \xrightarrow{\sigma^m_{\mathrm{loc}}} \cdots \xrightarrow{\sigma^{m+n-1}_{\mathrm{loc}}} J^{m+n}_{K_q} \quad . \tag{8}$$

because the 2-torsion points of $J^r_{K_q}$, $r = 1, \ldots, m+n$ are rational over K_q.

Let us denote by $\mathfrak{J}^r$, $r = 1, \ldots, m+n$, the Néron models associated to the $J^r_{K_q}$. The preceding diagram defines isogenies on the general fiber of the $\mathfrak{J}^r$ which, as the Néron models are projective schemes, extend to morphisms between the $\mathfrak{J}^r$ which are isogenies too. Moreover, by definition, the sequence obtained is exactly of the same form as (6). Moreover, as the schemes $\mathfrak{J}^r$ have good reductions modulo p and reduce to J^r_0, the schemes $\mathfrak{J}^r$ reduce modulo p to J^r_0. All this is summarized in the following diagram,

$$\begin{array}{ccccccccc}
\mathfrak{J}^1 & \xrightarrow{\sigma^1_{\mathrm{ner}}} & \cdots & \xrightarrow{\sigma^{m-1}_{\mathrm{ner}}} & \mathfrak{J}^m & \xrightarrow{\sigma^m_{\mathrm{ner}}} & \cdots & \xrightarrow{\sigma^{m+n-1}_{\mathrm{ner}}} & \mathfrak{J}^{m+n} \\
\downarrow & & & & \downarrow & & & & \downarrow \\
J^1_0 & \xrightarrow{\overline{\sigma}^1_\kappa} & \cdots & \xrightarrow{\overline{\sigma}^{m-1}_\kappa} & J^m_0 & \xrightarrow{\overline{\sigma}^m_\kappa} & \cdots & \xrightarrow{\overline{\sigma}^{m+n-1}_\kappa} & J^{m+n}_0
\end{array} \quad .$$

From now on, we fix $m \in \mathbb{N}^*$ which measures the precision of the p-adic approximation of the canonical lift of X_0 in our computations.

Theta functions revisited. In this section, if $\iota : A \to B$ is an isogeny between abelian varieties defined over a field (κ, K_q, or $\mathbb{C}$), then we use $\widehat{\iota} : \hat{B} \to \hat{A}$ to denote its dual isogeny. Let $F_{\mathrm{an}} = \sigma^{m+n-1}_{\mathrm{an}} \circ \ldots \circ \sigma^m_{\mathrm{an}}$.

Let J^m_{can} be the canonical lift of J^m_0. By [3], J^m_{can} is defined over K_q. We choose an embedding of K_q in $\mathbb{C}$ and put $J^m_{\mathrm{can}_{\mathbb{C}}} = J^m_{\mathrm{can}} \times_{\mathrm{Spec}(K_q)} \mathrm{Spec}(\mathbb{C})$. We can reproduce a sequence of isogenies, dual of that of (8), which lifts the sequence of the dual isogenies of the little Frobenius morphisms,

$$\hat{J}^{m+n}_{\mathrm{can}} \xrightarrow{\widehat{\sigma}^{m+n-1}_{\mathrm{can}}} \cdots \xrightarrow{\widehat{\sigma}^m_{\mathrm{can}}} \hat{J}^m_{\mathrm{can}} \xrightarrow{\widehat{\sigma}^{m-1}_{\mathrm{can}}} \cdots \xrightarrow{\widehat{\sigma}^1_{\mathrm{can}}} \hat{J}^1_{\mathrm{can}} \quad .$$

Then, by definition of the canonical lift, there exists an isomorphism $\mu : \hat{J}^m_{\mathrm{can}} \to \hat{J}^{m+n}_{\mathrm{can}}$ which gives by a base change to $\mathbb{C}$ over K_q an isomorphism $\mu_{\mathbb{C}} : \hat{J}^m_{\mathrm{can}_{\mathbb{C}}} \to \hat{J}^{m+n}_{\mathrm{can}_{\mathbb{C}}}$. Analytically, this isomorphism is defined by an element $M_{2g} = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \in \mathrm{Sp}_{2g}$ which, in fact, is in Γ_2 following [30] . Let Φ_{an} be the automorphism acting on J^m_{an} defined by Γ_2. Then the induced morphism Φ_{ner} on the Néron models $\mathfrak{J}^m$ reduces modulo $\mathfrak{M}^m$ to the isomorphism Φ of (7). So, if we put $D_{\mathrm{an}} = \Phi_{\mathrm{an}} \circ \widehat{F}_{\mathrm{an}}$, the morphism induced by D_{an} on the Néron model reduces modulo $\mathfrak{M}^m$ to the lift of the dual of the Frobenius morphism acting on $\hat{J}^{m+n}_0$. We have the following commutative diagram on the invariant differential forms of the analytic Jacobians,

$$\begin{array}{ccc}
H^0(J^{m+n}_{\mathrm{an}}, \Omega^1) & \xleftarrow[D^*_{\mathrm{an}}]{} & H^0(J^m_{\mathrm{an}}, \Omega^1) \\
& \nwarrow^{\widehat{F}^*_{\mathrm{an}}} & \downarrow{\scriptstyle \Phi^*_{\mathrm{an}}} \\
& & H^0(J^m_{\mathrm{an}}, \Omega^1)
\end{array} \quad .$$

Now let (e_α) be the basis of the invariant differential forms given by the coordinate forms in the identification $J^m_{\mathrm{an}} = \mathbb{C}^g / \Lambda_\Omega$. Put $\Omega' = (\alpha\Omega + \beta)(\gamma\Omega + \delta)^{-1}$. We have

$$\mathbb{C}^g / \Lambda_{2^n\Omega} \xrightarrow{\widehat{F}_{\mathrm{an}}} \mathbb{C}^g / \Lambda_\Omega \xrightarrow{\Phi_{\mathrm{an}}} \mathbb{C}^g / \Lambda_{\Omega'}$$

and $D^*_{\mathrm{an}} = \widehat{F}^*_{\mathrm{an}} \circ \Phi^*_{\mathrm{an}}$. As the action of $\widehat{F}^*_{\mathrm{an}}$ expressed in the base (e_α) is the identity, we see immediately that the action of Φ_{an} on the coordinate forms of $\mathbb{C}^g$ that is $(\gamma\Omega + \delta)^{-1}$ gives the action of the dual of the Frobenius morphism on the invariant differential forms computed with precision m.

As a consequence of (5), we have

$$\theta^2\left[\begin{smallmatrix}0\\ \varepsilon\end{smallmatrix}\right](0,\Omega') = \pm\det(\gamma\Omega+\delta)\theta^2\left[\begin{smallmatrix}0\\ \varepsilon\end{smallmatrix}\right](0,\Omega).$$

The Néron models associated to $\mathbb{C}^g/\Lambda_{\Omega'}$ and $\mathbb{C}^g/\Lambda_{2^n\Omega}$ are isomorphic modulo $\mathfrak{M}^m$ and because the Theta constants by [25] provide a global parametrization of the moduli space of principally polarized abelian varieties, we have $\theta^2\left[\begin{smallmatrix}0\\ \varepsilon\end{smallmatrix}\right](0,2^n\Omega)/\theta^2\left[\begin{smallmatrix}0\\ \varepsilon\end{smallmatrix}\right](0,\Omega') \equiv 1 \bmod 2^m$. If we denote by $\lambda_1,\ldots,\lambda_g$ the unit root part of the Frobenius morphism acting on X, as the Jacobian J^m is ordinary by hypothesis, the determinant $\pm\det(\gamma\Omega+\delta)^{-1}$ is simply the product $\lambda = \pm\lambda_1\ldots\lambda_g$ with precision m and is equal to the quotient

$$\theta^2\left[\begin{smallmatrix}0\\ \epsilon\end{smallmatrix}\right](0,\Omega)/\theta^2\left[\begin{smallmatrix}0\\ \epsilon\end{smallmatrix}\right](0,2^n\Omega). \tag{9}$$

From this discussion, we easily deduce Mestre's original algorithm to compute λ at precision m. We choose an embedding of K in $\mathbb{C}_2$ and a lift of X_0 over K such that the square root of the products $\prod_{a_i,a_j\in S\circ U_\varepsilon,i<j}(x_{a_i}-x_{a_j})\prod_{a_i,a_j\notin S\circ U_\varepsilon,i<j}(x_{a_i}-x_{a_j})$ needed in the Thomae-Fay formulas are in K. We compute the values of $c\theta^2\left[\begin{smallmatrix}0\\ \varepsilon_i\end{smallmatrix}\right](0,\Omega)$ with Ω defined by the preceding lift over K and $c\in\mathbb{C}$ such that $c\theta^2\left[\begin{smallmatrix}0\\ \varepsilon_i\end{smallmatrix}\right](0,\Omega)\in K$. Riemann duplication formulas are homogeneous, so that

$$c\theta^2\left[\begin{smallmatrix}0\\ \varepsilon_i\end{smallmatrix}\right](0,2^{r+1}\Omega) = \vartheta_i(c\theta^2\left[\begin{smallmatrix}0\\ \varepsilon_1\end{smallmatrix}\right](0,2^r\Omega),\ldots,c\theta^2\left[\begin{smallmatrix}0\\ \varepsilon_{2^g}\end{smallmatrix}\right](0,2^r\Omega))$$

where ϑ_i is a rational function. After each use of these formulas, the theta constants $c\theta^2\left[\begin{smallmatrix}0\\ \varepsilon_i\end{smallmatrix}\right](0,2^{r+1}\Omega)\in\mathbb{C}_2$ are attached to a model over K_q of a Jacobian variety which is the canonical lift of a Jacobian over $\mathbb{F}_q$ to a 2-adic precision increased by one. Once the wanted precision m is reached, n more iterations finally yield λ. This algorithm can be improved (cf. Sect. 5), using the following result.

Lemma 3. *With the above notations, let*

$$\alpha_i = \theta^2\left[\begin{smallmatrix}0\\ \varepsilon_i\end{smallmatrix}\right](0,2^r\Omega)/\theta^2\left[\begin{smallmatrix}0\\ \varepsilon_{2^g}\end{smallmatrix}\right](0,2^r\Omega), i=1,\ldots,2^g-1,$$

and we suppose that $\alpha_i\in K'$. Let us denote by ϕ the map $K'\longrightarrow K_q = K'\otimes_{\mathbb{Q}}\mathbb{Q}_p$, then

$$\vartheta_i(\phi(\alpha_1),\ldots,\phi(\alpha_{2g-1}),1) = (\phi(\alpha_i))^\sigma, \tag{10}$$

where σ is the lift of the Frobenius morphism to K_q.

Proof. Let Θ and Θ' be respectively the theta divisors of $J_{\mathrm{an}} = \mathbb{C}^g/\Lambda_{2^r\Omega}$ and $J'_{\mathrm{an}} = \mathbb{C}^g/\Lambda_{2^{r+1}\Omega}$. Then by [11, p. 317], $\mathscr{B}_\Theta^{\otimes 2}$ and $\mathscr{B}_{\Theta'}^{\otimes 2}$ are very ample line bundles on J_{an} and J'_{an} and the $s_i = \theta^2\left[\begin{smallmatrix}0\\ \varepsilon_i\end{smallmatrix}\right](z,2^r\Omega)$ (resp. $s'_i = \theta^2\left[\begin{smallmatrix}0\\ \varepsilon_i\end{smallmatrix}\right](z,2^{r+1}\Omega)$), $i=1,\ldots,2^g$, are global sections of these bundles. So possibly completing the s_i and s'_i with the same number of global sections of $L_\Theta^{\otimes 2}$ and $L_{\Theta'}^{\otimes 2}$ such that s_j and s'_j are given by theta functions with the same characteristics following (1), then for a $N>2^g$ we obtain an embedding of J_{an} (resp. J'_{an}) in $\mathbb{P}^N_{\mathbb{C}}$ provided in homogeneous coordinates by $z\longrightarrow(s_i(z/2))_{i=1,\ldots,N}$ (resp. $z\longrightarrow(s'_i(z))_{i=1,\ldots,N}$). So, there exists an automorphism ξ of $\mathbb{P}^N_{\mathbb{C}}$ such that we have the following commutative diagram,

$$\begin{array}{ccc} J_{\mathrm{an}}\subset\mathbb{P}^N_{\mathbb{C}} & \longrightarrow & J'_{\mathrm{an}}\subset\mathbb{P}^N_{\mathbb{C}} \\ \downarrow\xi & & \downarrow\xi \\ J_{\mathrm{alg}} & \xrightarrow{\sigma'} & J'_{\mathrm{alg}} \end{array},$$

where J_{alg} and J'_{alg} are algebraic varieties over K' and σ' is a morphism of K'-varieties. The last row induces by base change a morphism $J_{K_q}\longrightarrow J'_{K_q}$ which is up to an automorphism τ of J'_{alg} the Frobenius morphism. In fact, as the embedding provided by the theta functions is canonical following [24], τ is independent of J_{an} and it is easily checked on an example that it is the identity morphism.

Now, let $t_i(z) = s_i(z)/s_{2^g}(z)$ for $i=1,\ldots,\widehat{2^g},\ldots,N$ and $t'_i(z) = s'_i(z)/s'_{2^g}(z)$ for $i=1,\ldots,\widehat{2^g}$, $\ldots,N$ where the hat means that we skip that index. Then the t_i (resp. the t'_i) form an affine system of coordinates in a open neighborhood U (resp. U') of the point O which we can suppose to be K_q-rational. Then the map $U\longrightarrow U'$ given by $(t_1(z/2),\ldots,\widehat{t_{2^g}(z/2)},\ldots,t_N(z/2))\longrightarrow(t'_1(z),\ldots,\widehat{t'_{2^g}(z)},\ldots,t'_N(z))$ is simply the Frobenius morphism and the result comes immediately with $z=0$. □

5 An $O(n^{2+\epsilon})$ Algorithm

In order to compute the characteristic polynomial χ_F of the Frobenius F defined on an ordinary hyperelliptic curve over $\mathbb{F}_{2^n}$, the algorithm that we consider in this part belongs to the so-called "lift" and "norm" algorithms as introduced by Satoh in [31]. It consists of four main phases which, once fixed as in Sect. 2 an embedding of K in $\mathbb{C}$ and $\mathbb{C}_2$ (so that we can consider any element of K as a finite element of $K_q \subset \mathbb{C}_2$ and consider its precision with respect to its 2-adic valuation), are summarized as follows.

Initialization phase. Given a hyperelliptic curve X defined explicitly over a finite field $\mathbb{F}_{2^n}$, one computes at small precision the values taken by 2^g theta constants $\theta_i = c\theta^2 \left[\begin{smallmatrix} 0 \\ \varepsilon_i \end{smallmatrix}\right](0, \Omega)$, $i = 1, \ldots, 2^g$, c and Ω chosen such that $\theta_i \in K$. These theta constants are the values taken at $z = 0$ by the theta functions with 2^g characteristics attached to one lattice linked to X (cf. Sect. 3).

Lift phase. Using the Riemann duplication formulas given in Sect. 4, one has to solve a multivariate system $G(x) = x^\sigma$ in $\mathbb{Z}_q$ at a precision m large enough. The solution is a vector with $2^g - 1$ components. Each component of such a solution is the quotient of a theta constant divided by a fixed characteristic theta constant. This can be done, from the theta constants computed at small precision in the initialization phase, thanks to a lift algorithm.

Norm phase. Computing the norm $\mathrm{N}_{\mathbb{Z}_q/\mathbb{Z}_2}$ of an element of $\mathbb{Z}_q$ derived from these $2^g - 1$ quotients of theta constants yields at precision m the product $\lambda_1 \cdots \lambda_g$ of the g eigenvalues (invertible modulo 2) of F.

LLL phase. Getting the characteristic polynomial χ_F of the Frobenius of X can be done as described by Mestre. At first, we build a symmetric polynomial $P_{sym}(x)$ of degree 2^{g-1} whose roots are of the form $x + q/x$ where x is the product of g terms which belong to $\{\lambda_1, q/\lambda_1\}, \ldots, \{\lambda_g, q/\lambda_g\}$. Let us note that $\eta = \lambda + 2^{gn}/\lambda$ is one of these roots. Finally, we compute the roots of $P_{sym}(x)$ over $\mathbb{C}$ and recombine them in order to find $\chi_F(\pm x)$.

In the following, we describe completely these phases for finite fields of characteristic two with Gaussian Normal Bases and for ordinary hyperelliptic curves of arbitrary small genus.

Remark 1. Harley's ideas for elliptic curves [12], which are completely described in a nice synthesis due to Vercauteren [38], can be easily generalized to the hyperelliptic case. More precisely, the unramified extension $\mathbb{Z}_q$ may be defined in the same way as Harley and the norm phase is identical. The `NewtonLift` algorithm and the LLL phase are the same as below. The only difference is the `ArtinSchreierRoot` algorithm. Harley gave a method to compute a root of an equation of the form $x^\sigma = ax + b = 0$ where x, a and b are p-adic integers such that $v(a) > v(b)$. In our case, the only difference is that a and b are matrices, the generalization is straightforward.

5.1 Initialization Phase

Gaussian normal basis. When K is a Galois extension of κ which is generated by an element α, then we know that α^{σ^i}, $0 \leqslant i < n$ is a basis of K over κ called a normal basis. This basis is well suited to compute the action of the Galois group of K. Lifting to $\mathbb{Z}_{2^n}$ Gaussian Normal Basis defined on finite fields [21], we get, restricted to the characteristic two case, the following result [14].

Proposition 1. *Let n, t be positive integers such that $nt + 1$ is an odd prime. Let γ be a primitive $(nt + 1)$-th root of unity in some extension field of $\mathbb{Q}_2$. If $\gcd(nt/e, n) = 1$ where e denotes the order of 2^n modulo $nt + 1$, then for any primitive t-th root of unity τ in $\mathbb{F}_{nt+1}$, $\alpha = \sum_{i=0}^{t-1} \gamma^{\tau^i}$, generates a normal basis over $\mathbb{Q}_2$ called a Gaussian Normal Basis (GNB) of type t. Furthermore, $[\mathbb{Q}_2(\alpha) : \mathbb{Q}_2] = n$.*

H. Y. Kim et al. handled elements of $\mathbb{Z}_{2^n}$ with such a representation by working in the basis defined by γ. If we denote by $T_{m,n}$ the complexity of the product of two elements of $\mathbb{Z}_{2^n}$ with precision m, this yields $T_{m,n} = O((tnm)^\mu)$. Computing σ^k can be done by a simple permutation of the nt components of an element. This can be easily done at precision m in $S_{m,n} = O(nmt)$-bit operations. A more elaborated implementation strategy (with indexes) yields a $O(nt)$ time complexity [14].

Hyperelliptic curves. We assume in the following that an ordinary hyperelliptic curve X of genus g defined over $\mathbb{F}_{2^n}$ is given by an affine model of the form $y^2 + h(x)y = q(x)h(x)$ where $h(x)$ and $q(x)$ are polynomials over $\mathbb{F}_{2^n}$ of degree $g+1$ such that $h(x)$ has $g+1$ roots with multiplicity exactly one over $\mathbb{F}_{2^n}$. At the cost of an increase of the coefficient field and thanks to a change of variables, such a parameterization can be always found (cf. [23]).

Theta constants with Thomae-Fay formulas. In order to get the theta constants at small precision, we first lift in $\mathbb{Z}_{2^n}$ the affine model of X as $(2y + h(x))^2 = h(x)(h(x) + 2^2 q(x))$. From Hensel's lemma, it is not hard to see that $h(x)$ and $h(x) + 4q(x)$ completely split over $\mathbb{Z}_{2^n}$, this yields an equation of the form

$$y^2 = \prod_{i=0}^{2g+1} (x - a_i) \text{ such that } a_i \in \mathbb{Z}_{2^n} \text{ and } a_{2i} \equiv a_{2i+1} \bmod 2^2.$$

Then, the Thomae-Fay formulas (cf. (4)) enable to compute 2^g theta constants $\theta_0^{(1)}, \ldots, \theta_{2^g-1}^{(1)}$ at small precision through

$$\theta_e^{(1)} = \sqrt{\prod_{0 \leqslant i < j \leqslant g} (a_{2i+e_i} - a_{2j+e_j})(a_{2i+1-e_i} - a_{2j+1-e_j})},$$

where $e_0 = 0$ and where e is written in basis 2 as $e_g 2^{g-1} + \cdots + e_1$. Moreover, the square root is chosen such that $\theta_e^{(1)} \equiv 1 \bmod 2^2$.

5.2 Lift Phase

The purpose of this phase is to compute quotients of theta constants at precision m. This precision depends on g and n (cf. Sect. 5.4). Typically we have $m \simeq n/2$ for $g = 1$.

Mestre's method. The method as proposed by Mestre increases the precision by one at each step thanks to the use of the Riemann duplication formulas. This can be geometrically interpreted as jumping from one lattice to another lattice. The initial lattice is the Jacobian of the lift of X over K_q. The other lattices correspond to 2-isogenous analytic abelian varieties $J^i_{K_q}$ (cf. Sect. 4). We denote by $\theta_e^{(i)}$ the theta constants attached to $J^i_{K_q}$.

Let $G : \mathbb{Z}_q^{2^g-1} \longrightarrow \mathbb{Z}_q$ be defined by $G(t_1) = 2\frac{\sqrt{t_1}}{1+t_1}$ if $g = 1$ and more generally for $g > 1$ by

$$G(t_1, \cdots, t_{2^g-1}) = 2\frac{\sqrt{t_1} + \sqrt{t_2}\sqrt{t_3} + \cdots + \sqrt{t_{2^g-2}}\sqrt{t_{2^g-1}}}{1 + t_1 + \cdots + t_{2^g-1}}, \tag{11}$$

that is the dehomogenization of (2) with respect to θ_0. Let $\tau_e^{(i)} = \theta_e^{(i)}/\theta_0^{(i)}$, then Mestre's method consists in iterating m times (11), i.e.

$$\forall e \in \{1, \ldots, 2^g - 1\},\ \tau_e^{(i+1)} = G(\tau_e, \tau_{i_2}^{(i)}, \tau_{i_3}^{(i)}, \ldots, \tau_{i_{2^g-2}}^{(i)}, \tau_{i_{2^g-1}}^{(i)}),$$

where, for each e, the indexes $i_2, \ldots, i_{2^g-1}$ are such that

$$\{\{0, e\}, \{i_2, i_3\}, \ldots, \{i_{2^g-2}, i_{2^g-1}\}\} = \{\{j, j \oplus e\} \mid j \in \{1, \ldots, 2^g - 1\}\} \tag{12}$$

($\oplus$ denotes the exclusive or of two integers, i.e. the integer the bits of which are the sum modulo two of the bits of the operands). It is not difficult to see that the resulting algorithm has a quasi-cubic complexity in n if $m = O(n)$.

We can obtain a complexity which is quasi-quadratic using (10), i.e.

$$\forall e \in \{1, \ldots, 2^g - 1\},\ \tau_e^{(i+1)} = (\tau_e^{(i)})^\sigma.$$

So, instead of jumping from lattices to lattices, we can stay on the initial lattice (the one associated to a lift of X over K) and, with the notations given above, we can compute roots $\tau_1, \ldots, \tau_{2^g-1}$ (such that $\tau_e = \theta_e/\theta_0 \bmod 2^4$) of the system of equations given by,

$$\forall e \in \{1, \ldots, 2^g - 1\},\ \tau_e^\sigma = G(\tau_e, \tau_{i_2}, \tau_{i_3}, \ldots, \tau_{i_{2^g-2}}, \tau_{i_{2^g-1}}). \tag{13}$$

Such an equation can be efficiently solved thanks to a vectorial version of the `Newtonlift` algorithm of [19] as described in detail in the next section. This algorithm may be viewed as an adaptation to our case of the multivariate version of the well known algorithm of Newton to find a root of a polynomial function [16, pages 493-494]. It is based on a vectorial version of the algorithm `ArtinSchreierRoot` [19] which gives a root of a generalized Artin-Schreier equation.

Newton lift. Let $x = (x_1, \ldots, x_k)$ and $y = (y_1, \ldots, y_k)$ be two tuples of variables and for $i = 1, \ldots, k$, $\phi_i(x, y) \in \mathbb{Z}_q[x_1, \ldots, x_k, y_1, \ldots, y_k]$ be a system of k polynomials in these variables which define a function $\phi : \mathbb{Z}_q^k \times \mathbb{Z}_q^k \mapsto \mathbb{Z}_q^k$. In the sequel, if $\Sigma \in \mathrm{Gal}(K_q/\mathbb{Q}_p)$, we put $y^\Sigma = (y_1^\Sigma, \ldots, y_k^\Sigma)$. In this paragraph, we present an algorithm to solve an equation which appears very naturally with such algorithms, that is $\phi(x, x^\Sigma) = 0$. We wish to find a solution $x \in \mathbb{Z}_q^k$ of a system of equations of this kind, given a solution known at small precision. For the sake of generality, p can be below any prime.

Theorem 2. *For $(x_0, y_0) \in \mathbb{Z}_q^k \times \mathbb{Z}_q^k$, we denote in the following by $\partial\phi/\partial x(x_0, y_0) \in M_k(\mathbb{Z}_q)$ (resp. $\partial\phi/\partial y(x_0, y_0) \in M_k(\mathbb{Z}_q)$) the matrix x_{ij} (resp. y_{ij}) of partial derivatives*

$$x_{ij} = (\partial\phi_i/\partial x_j)(x_0, y_0),\ \textit{(resp. } y_{ij} = (\partial\phi_i/\partial y_j)(x_0, y_0)),\ 1 \leqslant i, j \leqslant k.$$

Let $x_0 \in \mathbb{Z}_q^k$ be a zero of $\phi(x, x^\Sigma) = 0 \bmod p^w$, $w \in \mathbb{N}$. We suppose moreover that we have

$$\det(\left(\frac{\partial\phi}{\partial y}\right)(x_0, x_0^\Sigma)) \neq 0, \tag{14}$$

$$v(\left(\frac{\partial\phi}{\partial y}\right)^{-1}(x_0, x_0^\Sigma)\frac{\partial\phi}{\partial x}(x_0, x_0^\Sigma)) > 0 \tag{15}$$

and

$$v(\left(\frac{\partial\phi}{\partial y}\right)^{-1}(x_0, x_0^\Sigma)\phi(x_0, x_0^\Sigma)) > v(\left(\frac{\partial\phi}{\partial y}\right)(x_0, x_0^\Sigma)), \tag{16}$$

then a solution of the equation $\phi(x, x^\Sigma) = 0 \bmod p^m$ can be computed in $O(\log(n)n^\mu m^\mu)$ time complexity.

Algorithm 5.1 `NewtonLift`

Algorithm to compute a root of $\phi(x, x^\Sigma) \bmod p^m$, knowing a solution x_0 modulo p^{2r+1} where $r = v(\phi(x_0, x_0^\Sigma)) - v((\partial\phi/\partial y)^{-1}(x_0, x_0^\Sigma)v(\phi(x_0, x_0^\Sigma)))$.

INPUT: $x_0 \in (\mathbb{Z}_q/p^{2r+1}\mathbb{Z}_q)^k$, $m \in \mathbb{N}$.
OUTPUT: x a solution of $\phi(x, x^\Sigma) \bmod p^m$.

Step 1. **if** $m \leqslant 2r + 1$ **then return** x_0;
Step 2. $w := \lceil \frac{m}{2} \rceil + r$;
Step 3. $x :=$ `NewtonLift`(x_0, w);
Step 4. Lift x to $\mathbb{Z}_q/p^m\mathbb{Z}_q$; $y := x^\Sigma \bmod p^m$;
Step 5. $\Delta_x := \partial_x\phi(x, y) \bmod p^{w-r}$; $\Delta_y := \partial_y\phi(x, y) \bmod p^{w-r}$;
Step 6. $V := \phi(x, y) \bmod p^m$;
Step 7. $a, b :=$ `ArtinSchreierRoot`$(-\Delta_y^{-1}V/(p^{w-r}), -\Delta_y^{-1}\Delta_x, w - r, n)$;
Step 8. **return** $x + p^{w-r}(1 - a)^{-1}b$;

Proof. We prove the correctness of Algorithm 5.1 and establish its complexity.

Correctness. Let $f(x) = \phi(x, x^\Sigma)$. We put $0 < r = v(f(x_0)) - v((\partial\phi/\partial y)^{-1}(x_0, x_0^\Sigma) f(x_0))$, we assume inductively that we know a root x_0 of $\phi(x, x^\Sigma)$ at precision $w = \lceil m/2 \rceil + r$ and we explain why the algorithm returns a root of the same equation at precision m which satisfies (14), (15) and (16). First, let $x_0^\uparrow$ be any lift of x_0 at precision $2w - 2r$,

$$\forall \delta \in \mathbb{Z}_q^k,\ f(x_0^\uparrow + p^{w-r}\delta) - f(x_0^\uparrow) \equiv p^{w-r}(\Delta_x \delta + \Delta_y \delta^\Sigma) \bmod p^{2w-2r},$$

with $\Delta_x \equiv (\partial\phi/\partial x)(x_0^\uparrow, x_0^{\uparrow\Sigma}) \bmod p^{w-r}$ and $\Delta_y \equiv (\partial\phi/\partial y)(x_0^\uparrow, x_0^{\uparrow\Sigma}) \bmod p^{w-r}$. We want to find δ at precision $w - r$ such that $f(x_0^\uparrow + p^{w-r}\delta) \equiv 0 \bmod p^{2w-2r}$, which we can restate in the following form,

$$-\frac{f(x_0^\uparrow)}{p^{w-r}} \equiv \Delta_x \delta + \Delta_y \delta^\Sigma \bmod p^{w-r}. \tag{17}$$

Rewriting (17) as $\delta^\Sigma \equiv a\delta + b \bmod p^{w-r}$, with $a = -\Delta_y^{-1}\Delta_x \in M_k(\mathbb{Z}_q)$ because of (15) and $b = -\Delta_y^{-1} f(x_0^\uparrow)/p^{w-r} \in \mathbb{Z}_q^k$, we recognize an Artin-Schreier equation since $a \in M_k(\mathbb{Z}_q)$ and $b \in \mathbb{Z}_q^k$. By induction hypothesis, we have $v(a) > 0$ and $(1 - a)$ is an invertible matrix (cf. Rem. 2). Then calling algorithm 5.2 for Σ with a and b, yields a solution δ at precision $w - r$ and $x_0^\uparrow + p^{w-r}\delta$ is a root of f with precision at least equal to m.

We now put $x_1 = x_0^\uparrow + p^{w-r}\delta$ and we verify (14), (15) and (16). Condition (14) is trivially fulfilled by induction hypothesis. Now, we can consider $\partial\phi_i/\partial y$ as a function from $\mathbb{Z}_q^k$ to $\mathbb{Z}_q^k$. A Taylor expansion then gives

$$\frac{\partial\phi_i}{\partial y}(x_1, x_1^\Sigma) = \frac{\partial\phi_i}{\partial y}(x_0^{\uparrow\Sigma}, x_0^\uparrow) + p^{w-r}C, \tag{18}$$

with $C \in \mathbb{Z}_q^k$ and $v((\partial\phi/\partial y)(x_1, x_1^\Sigma)) = v((\partial\phi/\partial y)(x_0^\uparrow, x_0^{\uparrow\Sigma}))$. The same argument applied to $v((\partial\phi/\partial x)(x_1, x_1^\Sigma))$, yields $v((\partial\phi/\partial x)(x_1, x_1^\Sigma)) = v((\partial\phi/\partial x)(x_0^{\uparrow\Sigma}, x_0^\uparrow))$. Moreover, if we set $r' = v(\partial\phi/\partial y)$, then (18) implies

$$\left(\frac{\partial\phi}{\partial y}\right)^{-1}(x_1, x_1^\Sigma) = \left(\frac{\partial\phi}{\partial y}\right)^{-1}(x_0^\uparrow, x_0^{\uparrow\Sigma}) + p^{w-r-r'}C,$$

with $C' \in \mathbb{Z}_q^k$. Finally, hypothesis (16) gives that $v((\partial\phi/\partial y)^{-1}(x_1, x_1^\Sigma)) = v((\partial\phi/\partial y)^{-1}(x_0^\uparrow, x_0^{\uparrow\Sigma}))$, so that (15) and (16) are fulfilled.

Complexity. The algorithm calls itself recursively $O(\log n)$ times with arguments which are two times larger at each call. The step with the largest cost is the call to `ArtinSchreierRoot` algorithm. From Lemma 4, its asymptotic complexity is $O(\log n)\max(S_{w,n}, T_{w,n})$ where w is nearly multiplied by two at each recursive call. Therefore, the asymptotic complexity of this algorithm is $O(\log n)\max(S_{m,n}, T_{m,n})$. For finite fields with Gaussian Normal Basis, this results in a $O(\log(n) n^\mu m^\mu)$ time complexity. □

We say that an equation is a (vectorial) generalized Artin-Schreier equation if it can be written in the form

$$x^\Sigma = ax + b, \text{ with } a \in M_k(\mathbb{Z}_q), b \in \mathbb{Z}_q^k. \tag{19}$$

The following lemma allows us to find a solution $x \in \mathbb{Z}_q^k$ of such an equation.

Lemma 4. *Let $a \in M_k(\mathbb{Z}_q), b \in \mathbb{Z}_q^k$. Then a solution of an equation of the form $x^\Sigma = ax + b$ can be computed to precision m in $O(\log n)\max(S_{m,n}, T_{m,n})$ time complexity.*

Algorithm 5.2 `ArtinSchreierRoot`

Algorithm to compute at precision m a square matrix A and a vector B, of dimension k, such that a solution of an equation $x^\Sigma = ax + b \bmod p^m$ satisfies $x^{\Sigma^\nu} = Ax + B \bmod p^m$.

INPUT: $a \in M_k(\mathbb{Z}_q/p^m\mathbb{Z}_q)$ and $b \in (\mathbb{Z}_q/p^m\mathbb{Z}_q)^k$, $m, \nu \in \mathbb{N}$.
OUTPUT: $A \in M_k(\mathbb{Z}_q/p^m\mathbb{Z}_q)$ and $B \in (\mathbb{Z}_q/p^m\mathbb{Z}_q)^k$.

Step 1. **if** $\nu = 1$ **then return** $a \bmod p^m$, $b \bmod p^m$;
Step 2. A, $B := \texttt{ArtinSchreierRoot}(a, b, m, \lfloor \frac{\nu}{2} \rfloor)$;
Step 3. $A := AA^{\Sigma^{\lfloor \frac{\nu}{2} \rfloor}} \bmod p^m$; $B := AB^{\Sigma^{\lfloor \frac{\nu}{2} \rfloor}} + B \bmod p^m$;
Step 4. **if** $\nu \bmod 2 = 1$ **then** $A := Aa^{\Sigma} \bmod p^m$; $B := Ab^{\Sigma} + B \bmod p^m$;
Step 5. **return** A, B;

Proof. We prove the correctness of Algorithm 5.2 and establish its complexity.

Correctness. By an easy recurrence with starting point $x^{\Sigma} = ax + b$, we can write that for all $i \in \mathbb{N}$, $x^{\Sigma^i} \equiv a_i x + b_i \bmod p^w$. To compute a_i and b_i, algorithm 5.2 is an adaptation of the classical "square and multiply" algorithm (used for exponentiations) based on the following composition formula,

$$\forall (i, i') \in \mathbb{Z}^2,\ x^{\Sigma^{i+i'}} = a_i^{\Sigma^{i'}} a_{i'} x + a_i^{\Sigma^{i'}} b_{i'} + b_i^{\Sigma^{i'}}.$$

Especially, we know that $x^{\Sigma^n} = x$, which means that $(1 - a_n)x = b_n$.

Complexity. The algorithm goes through step 3 or step 4 $O(\log n)$ times and these steps are performed in $\max(S_{m,n}, T_{m,n})$. Therefore, the asymptotic complexity in time of this algorithm is $O(\log n) \max(S_{m,n}, T_{m,n})$. □

Remark 2. It should be noted that if $v(a) > 0$ then by a trivial induction $v(a_n) > 0$ and as a consequence $(1 - a_n)$ is an invertible matrix.

Remark 3. In order to solve (13), we may apply these algorithms to $\Sigma = \sigma$ and to the polynomials

$$\phi_i(x, y) = y_i^2 (1 + x_1^2 + \cdots + x_{2^g-1}^2) - \sum_{0 \leqslant j \leqslant 2^g - 1} x_j x_{i \oplus j} \quad .$$

In this case, we have, evaluated at quotients of theta constants, that $v(\partial\phi/\partial x) = 3$, $v(\partial\phi/\partial y) = g + 1$, and that the valuation of the matrix $a = (\partial\phi/\partial y)^{-1}(\partial\phi/\partial x)$ is equal to $2 - g$. This valuation is thus negative for curves of genus greater than two. However, we observe that the matrix $a^{\sigma^k} a^{\sigma^{k-1}} \cdots a^{\sigma} a$ is of valuation $2 - g + k$. Therefore, if one applies the algorithms `NewtonLift` and `ArtinSchreierRoot` without any change, except that the precision at each recursive call is decreased by a gap smaller than g, one obtains a correct result.

5.3 Norm Phase

Equation (9) yields in our case,

$$\lambda \equiv \mathrm{N}_{\mathbb{Z}_{2^n}/\mathbb{Z}_2} \left(\frac{2^g}{1 + \tau_1 + \cdots + \tau_{2^g-1}} \right) \bmod 2^m.$$

In a Gaussian Normal Basis of type t, H. Y. Kim et al. described an algorithm of the type "divide and conquer" in order to compute such a norm. This algorithm has got a $O(\log(n) n^{\mu} m^{\mu})$ time complexity.

5.4 LLL Phase

The end of our variant is the same as Mestre's original method [23]. At first, using the LLL algorithm, one obtains a symmetric polynomial $P_{sym}(x)$ whose roots are of the form $x + q/x$ where x is the product of g terms which belong to $\{\lambda_1, q/\lambda_1\}, \ldots, \{\lambda_g, q/\lambda_g\}$. Then we compute its roots over $\mathbb{C}$ and obtain from them $\chi_F(\pm x)$ at least when this last polynomial is irreducible. By [37] this is always the case when the Jacobian of X is κ-simple. A last check on the curve allows us to obtain χ_F. We explicitly determine the complexity of the method and give bounds on the precision m needed when the genus increases.

Lattice reduction. The computation of P_{sym} can be easily done by reducing over $\mathbb{Z}$ the lattice $\mathscr{L}$ precisely given by

$$\begin{bmatrix} \Upsilon \times M_1 & \Upsilon \times M_2 & \cdots & \Upsilon \times M_{2^{g-1}+1} & \Upsilon \times 2^m \\ 0 & 0 & \cdots & 2^{\lfloor n \times S_{2^{g-1}+1} \rfloor} & 0 \\ 0 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 2^{\lfloor n \times S_2 \rfloor} & \cdots & 0 & 0 \\ 2^{\lfloor n \times S_1 \rfloor} & 0 & \cdots & 0 & 0 \end{bmatrix},$$

where

$$[M_i]_{i=1,\ldots,2^{g-1}+1} = \left[2^{(2^{g-1}-1-i)n} \eta^i \bmod 2^m \mid i \in \{0,\ldots,2^{g-1}-1\} \right] \cup [\eta^{2^{g-1}} \bmod 2^m, 2^m].$$

and

$$[S_i]_{i=1,\ldots,2^{g-1}+1} = \left[\frac{(i-1)(g-2)}{2} \mid i \in \{1,\ldots,2^{g-1}\} \right] \cup \left[\frac{2^{g-1}(g-2)}{2} + 1 \right]$$

(the basis vectors are in columns, $\eta = \lambda + 2^{gn}/\lambda$ and Υ is some arbitrarily large constant). The coefficients of P_{sym} are components of a vector Π of small norm in $\mathscr{L}$. Asymptotic estimates state that a lattice reduction using the LLL algorithm [18, 5] can compute it if its euclidian norm $||\ ||_2$ (or sup-norm $||\ ||_1$) satisfy $||\Pi||_1 \leqslant ||\Pi||_2 \leqslant \det(\mathscr{L})^{1/\dim \mathscr{L}}$. Since we can precisely evaluate, on the first hand, the norm $||\ ||_1$ of Π as a function of n and g and, on the other hand, the determinant of $\mathscr{L}$ as a function of m, g and the size of Υ (product of the elements on diagonal), this yields

$$m > \frac{2^{2g}(g-2) + 2^{g+1}(g+2)}{16}\, n.$$

We give numeric values in Table 1. In practice, n must be sufficiently large for these estimates on m to be accurate enough to yield P_{sym}. For $g = 3$, for instance, we observe more precisely that a precision of $m = 9n + 100$ is in fact needed.

Table 1. Asymptotic values of the precision m as a function of g and n.

g	1	2	3	4	5	6	7	8	9	10
m	$n/2$	$2n$	$9n$	$44n$	$220n$	$1088n$	$5264n$	$24896n$	$115392n$	$525824n$

Remark 4. For the specific case $g = 2$, $\chi_F(\pm x)$ can be recovered from λ directly without computing P_{sym}. In this case, the precision m can be decreased as low as $3n/2$. We refer to [23] for this.

Computing χ_F. Getting a fixed number of candidates over $\mathbb{C}$ for approximations of the eigenvalues of the Frobenius can be easily done from roots of P_{sym} computed in $\mathbb{C}$ with the classical Newton method. We enumerate the polynomials whose roots are theses candidates. A polynomial obtained in this way and such that its coefficients are close enough to integers is marked as a candidate for $\chi_F(\pm x)$. To confirm that such a candidate is equal to $\chi_F(\pm x)$, it remains to check that the order of the Jacobian is $\chi_F(1)$ or $\chi_F(-1)$.

Complexity. At fixed genus, the LLL step consists in applying LLL to a lattice of fixed dimension. Therefore, its complexity is the size of the coefficients of the matrix times the cost for one integer multiplication. This yields, with asymptotically fast algorithms for multiplying integers, a $O(m^{1+\mu})$ complexity in time. The cost of the second step is determined by the computation of roots of polynomials over $\mathbb{C}$ and requires $O(m^\mu)$. Finally, checking that the order of the Jacobian is $\chi_F(\pm 1)$ needs $O(m)$ applications of the group law, that is to say a complexity in time equal to $O(mn^\mu)$ with Cantor formulas [2].

5.5 Complexity of the Whole Algorithm

Once compared the complexities of the four phases stated above, it turns out, that for fixed g, the complexity in time of this variant of Mestre's algorithm is $O(n^{2\mu}\log n)$. The complexity in space is equal to $O(n^2)$.

Remark 5. There are 2^g theta constants. Each of them involves the computation at precision $m \simeq 2^{2g+o(1)}n$ of 2^g terms. As a function of the genus, the algorithm's running time is thus equal to $O(2^{4g+o(1)}n^{2+o(1)})$ and the complexity in space, $O(2^{3g+o(1)}n^2)$.

5.6 Implementation Insights

We implemented over finite fields $\mathbb{F}_{2^n}$ with Gaussian normal basis of type 1 this variant of Mestre's method. This was done with the the Magma computer algebra system, version 2.10 [1], for any genus. Of course, we have no hope with such a method to compute the characteristic polynomial of the Frobenius of a hyperelliptic curve with genus larger than 10 (even over $\mathbb{F}_2$, cf. table 1) but the genus 4 example that we give below was computed with this implementation. Besides, we wrote a carefully optimized C software for the specific cases $g = 1$, $g = 2$ and $g = 3$. Results are given below too.

A genus 4 example. In order to illustrate the algorithm, we are going to compute the characteristic polynomial of the Frobenius of the hyperelliptic curve of genus 4 defined over $\mathbb{F}_{2^4} \simeq \mathbb{F}_2[t]/(t^4+t^3+t^2+t+1)$ the affine model of which is $y^2 + h(x)y + q(x)h(x) = 0$ where

$$\begin{aligned} h(x) &= (x + t^3 + t^2 + t + 1)(x + t^2)(x + t^3 + 1)(x + t + 1)(x + t^3 + t^2 + 1), \\ q(x) &= x^5 + \left(t^3 + t^2 + t + 1\right) x^4 + x^3 + t^3x^2 + \left(t^3 + t + 1\right) x. \end{aligned}$$

The x-coordinates of the ten 2-torsion points of a lift of the curve in the unramified 2-adic extension defined by $t^4 + t^3 + t^2 + t + 1$ are, at precision 6,

$$\begin{aligned} a = [&-t - 1,\ 4\,t^3 - 24\,t^2 - 13\,t + 15,\ -t^2,\ -28\,t^3 + 11\,t^2 - 20\,t - 28,\ -13\,t^3 + 24\,t^2 + 4\,t - 1, \\ &- t^3 - 1,\ 3\,t^3 - 17\,t^2 - 8\,t - 9,\ -t^3 - t^2 - 1,\ -9\,t^3 + 27\,t^2 + 15\,t + 23,\ -t^3 - t^2 - t - 1]. \end{aligned}$$

The Thomae-Fay formulas yield 15 constants $\tau_e = \theta_e/\theta_0$ which, at precision 7, are equal to

$$\begin{aligned} \tau = [&-32\,t^3 + 16\,t^2 + 8\,t - 55, -56\,t^3 - 40\,t^2 - 32\,t + 49, -8\,t^3 + 24\,t^2 - 40\,t + 9, \\ &- 48\,t^3 + 48\,t^2 - 48\,t + 9, 48\,t^3 + 64\,t^2 - 40\,t + 1, 24\,t^3 + 24\,t^2 + 64\,t - 55, -56\,t^3 - 40\,t^2 + 56\,t - 47, \\ &- 32\,t^3 - 24\,t^2 + 56\,t - 47, 64\,t^3 + 24\,t^2 - 48\,t + 57, -40\,t^3 - 32\,t^2 - 8\,t - 15, 8\,t^3 + 64\,t^2 - 23, \\ &48\,t^3 - 24\,t^2 + 8\,t + 41, 16\,t^3 + 24\,t^2 + 32\,t - 63, 40\,t^3 - 16\,t^2 - 40\,t - 39, -40\,t^3 - 48\,t^2 - 32\,t + 1]. \end{aligned}$$

A call to `NewtonLift` successively lifts τ at precision 345. This yields, in hexadecimal notation,

$$\begin{aligned} \tau = [&-\texttt{2AF4761F43EBADC244C1BC1D33E90C24141C48F828C8E05A9E7ADB00EC35D6F88BD03D0C05C445A4BFF230}\,t^3 \\ &+ \texttt{1F66D441F994F38896AF5CB90E34007AD48632BBBC09695F6E2E5A4ED676ED6752EBE9B9239EACB570F370}\,t^2 \\ &+ \texttt{1F173EE17446547549FBE4BE2CA778C1AA31398B6AB73966621BF4D4A63B45131165F0E1847B040F40E648}\,t \\ &+ \texttt{487AD2E1552D785AC648ED52E76D6195E111BCB022D02B334512B58E067205652901ADD8E97630C49196A9}, \\ &\vdots \\ &], \end{aligned}$$

and

$$\lambda = \texttt{18184F8253A78523EE4F72D801B910F4A83B8B844AAA42D2CC911C89846B4B24D5B0DB3F56FA9354B37C56D} \bmod 2^{345}.$$

After the Lattice reduction step, one obtains,

$$P_{sym}(x) = x^8 + 467\,x^7 - 2^4 \cdot 25988\,x^6 - 2^8 \cdot 837798\,x^5 + 2^{12} \cdot 9084572\,x^4 + 2^{16} \cdot 417375179\,x^3 + 2^{20} \cdot 1472562912\,x^2 - 2^{24} \cdot 37930023936\,x - 2^{28} \cdot 253989847040,$$

and finally,

$$\chi_F(x) = x^8 - 2\,x^7 + 12\,x^6 - 62\,x^5 + 339\,x^4 - 2^4 \cdot 62\,x^3 + 2^8 \cdot 12\,x^2 - 2^{12} \cdot 2\,x + 2^{16}.$$

Some Timings. The C software that we developed uses a finite field `C` library called `ZEN` [4] built over GMP [10]. We measured the time needed to compute the order of the Jacobians of hyperelliptic curves of genus one, two and three defined over finite fields $\mathbb{F}_{2^n}$ of various sizes on a 731 MHz DEC alpha computer. We give these timings on one 731 MHz Compaq Alpha processor in Table 2. Let us note that at the time of writing the largest such computations ever done are, for $g = 1$ a 130020-bit computation by Harley [12], for $g = 2$ and $g = 3$ the 32070-bit and 4098-bit computations given in Table 2.

Table 2. Timings to count points on Jacobians of hypertelliptic curves of small genus over $\mathbb{F}_{2^n}$.

n	$g = 1$			$g = 2$			$g = 3$		
	Lift	Norm	Total	Lift	Norm	Total	Lift	Norm	Total
1018	2.5s	1.5s	4s	2mn	5s	2mn 5	8h 30	1mn	8h 31
2052	10s	7s	17s	8mn 30	25s	8mn 55	1d 3	5 mn	1d 3
4098	1mn	45s	1mn 45	50mn 5	2mn 15	52mn 20	6d 8	25mn	6d 8
8218	6mn 30	4mn 30	11mn	4h 52	13mn	5h 5	-	-	-
16420	34mn	23mn	57mn	1d 5	1h	1d 6	-	-	-
32770	3h 17	2h 18	5h 35	7d 22	6h	8d 4	-	-	-
65538	15h 45	13h 20	1d 5	-	-	-	-	-	-
100002	1d 18	1d 16	3d 10	-	-	-	-	-	-

We designed our implementation for finite fields with a Gaussian Normal Basis of type 1 in order to experimentally check the quadratic behavior of the algorithm. Therefore, the exponents n used for our experiments are even. Finite fields with prime exponents are usually preferred for cryptographic purposes. They can be handled through Gaussian Normal Basis of larger types. For instance, since multiplying two elements over a GNB of type 2 can be done in two times the time needed to multiply two elements over a GNB of type 1 for finite fields of similar size [14], it is not difficult to derive timings of such an implementation for counting points over GNB of type 2. Similar arguments hold for larger types.

6 Conclusion

We describe an algorithm the complexity of which is quasi-quadratic to implement Mestre's ideas for hyperelliptic curves of small genus over finite field of small characteristic and we prove its validity. These ideas seem to be rather competitive for a genus smaller or equal to five and seem to be general enough to be extended to more general cases. Especially, we refer to [30] for non hyperelliptic curves of genus three.

Acknowledgments. We express our gratitude to Jean-Marc Couveignes for his very helpful remarks and Michael Harrison for some implementation insights. We also thank Frederik Vercauteren and Christophe Ritzenthaler for their comments on earlier drafts of this paper.

References

[1] W. Bosma, J. Cannon, and C. Playoust. The Magma Algebra System I: The User Language. *J. Symbolic Comp.*, 24(3):235–265, 1997.

[2] D. G. Cantor. Computing in the Jacobian of a hyperelliptic curve. *Math. Comp.*, 48(177):95–101, 1987.

[3] R. Carls. Generalized AGM sequences and approximation of canonical lifts. Available at `http://www.math.leidenuniv.nl/~carls`, April 2003.

[4] F. Chabaud and R. Lercier. *ZEN, User Manual*, 1996.

[5] D. Coppersmith. Small solutions to polynomial equations, and low exponent RSA vulnerabilities. *J. Cryptology*, 10(4):233–260, 1997.

[6] J. Denef and F. Vercauteren. An extension of Kedlaya's algorithm to Artin-Schreier curves in characteristic 2. In Claus Fieker and David R. Kohel, editors, *Algorithmic Number Theory, 5th International Symposium, ANTS-V*, pages 369–384. Springer, July 2002.

[7] J. D. Fay. *Theta functions on Riemann surfaces.* Springer-Verlag, Berlin, 1973. Lecture Notes in Mathematics, Vol. 352.

[8] P. Gaudry. *Algorithmique des courbes hyperelliptiques et applications à la cryptologie.* PhD thesis, École Polytechnique, 2000.

[9] P. Gaudry. Cardinality of a genus 2 hyperelliptic curve over GF($5 \cdot 10^{24} + 41$). Email at the Number Theory List, September 2002.

[10] Free Software Foundation GNU. GMP library. Available at `http://www.swox.com/gmp/`, 2002.

[11] P. Griffiths and J. Harris. *Principles of algebraic geometry.* Wiley Classics Library. John Wiley & Sons Inc., New York, 1994. Reprint of the 1978 original.

[12] R. Harley. Asymptotically optimal p-adic point-counting. E-mail to the NMBRTHRY mailing list, December 2002.

[13] K.S. Kedlaya. Counting points on hyperelliptic curves using Monsky Washnitzer cohomology. *Journal of the Ramanujan Mathematical Society*, 16:323–328, 2001.

[14] H. Y. Kim, J. Y. Park, J. H. Cheon, J. H. Park, J. H. Kim, and S. G. Hahn. Fast Elliptic Curve Point Counting Using Gaussian Normal Basis. In Claus Fieker and David R. Kohel, editors, *Algorithmic Number Theory, 5th International Symposium, ANTS-V*, pages 292–307, Berlin, July 2002. Springer Verlag.

[15] N. Koblitz. Hyperelliptic cryptosystems. *J. Cryptology*, 1(3):139–150, 1989.

[16] S. Lang. *Algebra. 3rd revised ed.* Graduate Texts in Mathematics. 211. New York, NY: Springer., 2002.

[17] A. G. B. Lauder and D. Wan. Computing Zeta functions of Artin-Schreier curves over finite fields. *LMS J. Comput. Math.*, 5:34–55 (electronic), 2002.

[18] A. K. Lenstra, H. W. Lenstra, Jr., and L. Lovász. Factoring polynomials with rational coefficients. *Mathematische Ann.*, 261:513–534, 1982.

[19] R. Lercier and D. Lubicz. Counting Points on Elliptic Curves over Finite Fields of Small Characteristic in Quasi Quadratic Time. In Eli Biham, editor, *Advances in Cryptology—EUROCRYPT '2003*, Lecture Notes in Computer Science. Springer-Verlag, May 2003.

[20] J. Lubin, J.-P. Serre, and J. Tate. Elliptic curves and formal groups. Available at `http://ma.utexas.edu/users/voloch/lst.html`, 1964.

[21] A. J. Menezes, I. F. Blake, X. Gao, R. C. Mullin, S. A. Vanstone, and T. Yaghoobian. *Applications of finite fields.* The Kluwer International Series in Engineering and Computer Science. Boston: Kluwer Academic Publishers. xi, 218 p., 1993.

[22] J.-F. Mestre. Lettre à Gaudry et Harley, 2001. Available at `http://www.math.jussieu.fr/~mestre`.

[23] J.-F. Mestre. Notes of a talk given at the seminar of cryptography of Rennes, 2002. Available at `http://www.math.univ-rennes1.fr/crypto/2001-02/mestre.ps`.

[24] D. Mumford. On the equations defining abelian varieties. I. *Invent. Math.*, 1:287–354, 1966.

[25] D. Mumford. On the equations defining abelian varieties. II. *Invent. Math.*, 3:75–135, 1967.

[26] D. Mumford. *Tata lectures on theta I*, volume 28 of *Progress in Mathematics.* Birkhäuser Boston Inc., Boston, MA, 1983. With the assistance of C. Musili, M. Nori, E. Previato and M. Stillman.

[27] D. Mumford. *Tata lectures on theta II*, volume 43 of *Progress in Mathematics.* Birkhäuser Boston Inc., Boston, MA, 1984. Jacobian theta functions and differential equations, With the collaboration of C. Musili, M. Nori, E. Previato, M. Stillman and H. Umemura.

[28] J. Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences].* Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[29] J. Pila. Frobenius maps of abelian varieties and finding roots of unity in finite fields. *Math. Comp.*, 55(192):745–763, 1990.

[30] C. Ritzenthaler. *Problèmes arithmétiques relatifs à certaines familles de courbes sur les corps finis.* PhD thesis, Université Paris 7 - Denis Diderot, June 2003.

[31] T. Satoh. The canonical lift of an ordinary elliptic curve over a finite field and its point counting. *J. Ramanujan Math. Soc.*, 15(4):247–270, 2000.

[32] T. Satoh, B. Skjernaa, and Y. Taguchi. Fast computation of canonical lifts of elliptic curves and its application to point counting. *Finite Fields and Their Applications*, 9(1):89–101, 2003.
[33] R. Schoof. Counting points on elliptic curves over finite fields. *J. Théorie des nombres de Bordeaux*, 7:483–494, 1998.
[34] J.-P. Serre. Géométrie algébrique et géométrie analytique. *Ann. Inst. Fourier, Grenoble*, 6:1–42, 1955–1956.
[35] G. Shimura. *Abelian varieties with complex multiplication and modular functions*. Princ. Univ. Press, NJ, 1998.
[36] J. H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1986. Corrected reprint of the 1986 original.
[37] J. Tate. Endomorphisms of abelian varieties over finite fields. *Invent. Math.*, 2:134–144, 1966.
[38] F. Vercauteren. *Computing zeta functions of curves over finite fields*. PhD thesis, Katholieke Universiteit Leuven, 2003. Preprint.