

A POINT COUNTING ALGORITHM USING COHOMOLOGY  
WITH COMPACT SUPPORT

GWELTAZ CHATEL AND DAVID LUBICZ

*Abstract*

We describe an algorithm to count the number of rational points of an hyperelliptic curve defined over a finite field of odd characteristic which is based upon the computation of the action of the Frobenius morphism on a basis of the Monsky-Washnitzer cohomology with compact support. This algorithm follows the vein of a systematic exploration of potential applications of cohomology theories to point counting.

Our algorithm decomposes in two steps. A first step which consists of the computation of a basis of the cohomology and then a second step to obtain a representation of the Frobenius morphism. We achieve a  $\tilde{O}(g^4n^3)$  time complexity and  $O(g^3n^3)$  memory complexity where  $g$  is the genus of the curve and  $n$  is the absolute degree of its base field. We give a detailed complexity analysis of the algorithm as well as a proof of correctness.

1. *Introduction*

The problem of counting the number of rational points on a smooth projective algebraic curve defined over a finite field has attracted a lot of attention in recent years driven by well known cryptographic applications.

The known point counting algorithms for a curve  $C$  over a finite field  $k$  with Jacobian  $J(C)$  can roughly be divided in two large classes, the  $\ell$ -adic algorithms and the  $p$ -adic algorithms.

The  $\ell$ -adic point counting algorithms can be interpreted as the computation of the action of the Frobenius morphism on the  $\ell$ -adic Tate module of the Jacobian,  $\ell$  being prime to the characteristic of the base field. The  $\ell$ -adic point counting algorithms all follow an original idea of Schoof [33] which consists in computing the action of the Frobenius morphism on the group of  $\ell$ -torsion points of  $J(C)$  for primes  $\ell$  big enough to recover the zeta function of the curve by the Chinese remainder theorem. In the case that  $C$  is an elliptic curve, this first algorithm has subsequently been improved by Elkies, Atkin and other authors [10, 33] and resulted in a very efficient algorithm. Some of these techniques have been adapted in the case of higher genus curves [29] but some improvement have yet to be done in order to be able to reach cryptographic size fields. Nevertheless some progress has been made [13, 14] in that direction.

On the other side, the  $p$ -adic point counting algorithms can be interpreted as the computation of the action of the Frobenius morphism on some  $p$ -adic cohomology

group. The first such algorithm has been described by Satoh [32]. The algorithm of Satoh relies on the computation of the action of the Frobenius morphism on the invariant differential forms of the canonical lift of an ordinary Jacobian. It has been generalized and made more efficient in a series of papers [31, 25, 26, 15, 23, 24]. Other authors have explored other possible representations of the Frobenius morphism. In [17], Kedlaya explains how to obtain a basis of the Monsky-Washnitzer cohomology of an hyperelliptic curve and compute the Frobenius morphism acting on it. Lauder used Dwork cohomology to obtain general point counting algorithms [20, 21]. Later on, Lauder introduced deformation techniques in which one consider a one parameter family of curves and use the Gauss-Manin connection in order to carry over this family the action of the Frobenius morphism [18].

Pursuing the exploration of possible  $p$ -adic cohomology theories, we propose in this paper to use Monsky-Washnitzer cohomology with compact support. This cohomology theory comes with a Lefschetz trace formula and as a consequence can be used to compute the number of rational points of a curve defined over a finite field. Starting with an hyperelliptic curve defined over a finite field of odd characteristic, we explain how to represent elements of the Monsky-Washnitzer cohomology with compact support and obtain a basis of this vector space. Then we compute the representation of the Frobenius morphism.

Our algorithm breaks into two steps. The first step is the computation of a basis of the Monsky-Washnitzer cohomology with compact support. Unlike the case of the algorithm of Kedlaya this step is non trivial from an algorithmic point of view. The two main features of this part of our algorithm are:

- The use of the stability of the cohomology of Monsky-Washnitzer with compact support by finite étale descent to reduce the computation of a basis of the cohomology to the computation of a basis of the global horizontal sections of an isocrystal over the affine line. These global sections verify a differential equation provided by the Gauss-Manin connection that we interpret as the solutions of a linear system. This is the so called global method.
- Unfortunately, the global method is inefficient since it involves the inversion of a matrix the size of which is in the order of the analytic precision required for the computations. We explain how to speed up the computation of the basis by taking advantage of local inhomogeneous differential equations deduced from the Gauss-Manin connection. Once we have computed global solutions for the Gauss-Manin connection up to a small analytic precision it is possible to prolong them locally using an asymptotically fast algorithm such as [2].

The second step of the algorithm is the computation of a lift of the Frobenius morphism as well as its action on a basis of the cohomology. The computation of a lift of the Frobenius morphism that we describe in this paper is standard, being just an adaptation of [17] to our case. Nonetheless, for the action of the Frobenius morphism, we explain how it is possible to turn into an efficient algorithm the knowledge of local differential equations deduced from the twist of the Gauss-Manin connection by the Frobenius morphism.

We give a proof of correctness for our algorithm. As usual for the  $p$ -adic algorithms, the main problem lies in the assessment of the analytic and  $p$ -adic precisions necessary to recover the characteristic polynomial of the Frobenius morphism. For this we used a variant of a result of Lauder [19]. We provide the algorithm with

a detailed complexity analysis. In this complexity estimate, we suppose that the characteristic  $p$  of the base field of the hyperelliptic curve is fixed and consider complexity bounds when the genus  $g$  and the absolute degree  $n$  of the base field increase. Using the soft-O notation to neglect the logarithmic terms, we obtain a  $\tilde{O}(g^4 n^3)$  time complexity with a  $O(g^3 n^3)$  memory consumption. In order to achieve this time complexity, we use in an essential manner asymptotically fast algorithms to compute with power series [1, 3, 28, 2]. We remark that the time complexity of our algorithm has the same complexity bounds as the algorithm of Kedlaya.

1.0.0.1. *Organisation of the paper.* In Section 2, we recall the basic construction of the cohomology of an overconvergent isocrystal over the affine line. In Section 3, we deduce from it an algorithm to compute a basis of the cohomology. We give a proof of correctness and a detailed complexity analysis of this algorithm in Section 4. In Section 5, we explain how to compute the action of the Frobenius morphism on this basis and recover the zeta function of the curve. In Section 6, we obtain complexity estimates for the whole algorithm and discuss practical results and implementations.

1.0.0.2. *Notations.* In all this paper,  $k$  is a finite field of odd characteristic  $p$ . We denote by  $W(k)$  the ring of Witt vectors with coefficients in  $k$  and by  $K$  the field of fractions of  $W(k)$ . For all  $x \in K$ ,  $v_p(x)$  and  $|x|$  denote the usual  $p$ -adic valuation and norm of  $x$ .

We use the notation  $\underline{\ell}$  for a multi-index  $(\ell_0, \dots, \ell_k)$  where  $k > 0$  is an integer. For instance,  $\underline{0}$  is the  $k$ -fold multi-index  $(0, \dots, 0)$ . For  $\underline{\ell}$  and  $\underline{m}$  two multi-indexes  $\underline{\ell} > \underline{m}$  means that for all  $i \in \{0, \dots, k\}$ ,  $\ell_i > m_i$ . Moreover if  $\underline{\ell}$  is a multi-index, we set  $|\underline{\ell}| = \max\{|\ell_i|, i = 0, \dots, k\}$ .

We recall that an element  $f = \sum_{\underline{\ell}} a_{\underline{\ell}} t^{\underline{\ell}}$  of  $K[[t_0, \dots, t_k]]$  is called overconvergent if there exists  $\eta_0 > 1$  such that  $\lim |a_{\underline{\ell}}| \eta_0^{|\underline{\ell}|} = 0$ . The sub-ring of  $K[[t_0, \dots, t_k]]$  consisting of overconvergent elements is denoted by  $K[t_0, \dots, t_k]^\dagger$  and is called the weak completion of  $K[t_0, \dots, t_k]$ . Let  $(a_\ell)_{\ell \in \mathbb{N}}$  be a sequence in  $W(k)$  and  $\eta > 0$ , in the following we use the more compact notation,  $|a_\ell| \eta^\ell \rightarrow_{\pm\infty} 0$  to say that  $\lim_{\ell \rightarrow \pm\infty} |a_\ell| \eta^\ell = 0$ .

If  $x \in W(k)$ , we say that we have computed  $x$  to  $p$ -adic precision  $P_2 \in \mathbb{N}^*$  if we have computed a representative of  $x$  in  $W(k)/p^{P_2}W(k)$ . Let  $x \in K$  and write  $x = p^{v_p(x)}.z$  where  $z$  is an invertible element of  $W(k)$ . We say that we have computed  $x$  to relative precision  $P_2$  if we have computed  $z$  to precision  $P_2$ . We say that we have computed  $x$  to absolute precision  $P_2$  if we have computed  $z$  to precision  $\max(P_2 - v_p(x), 0)$ . Of course for an invertible element  $x$  of  $W(k)$  absolute and relative precisions are the same and we say simply that this is the precision of  $x$ .

The relative precision is the right notion to assess the time and memory consumption of the algorithms. On the other side, the absolute precision is used to prove the correctness of the result but is not sufficient to obtain complexity bounds for our algorithms. One of the main results of the paper, Theorem 1 states that the discrepancy between relative and absolute precision of all approximations of elements of  $K$  computed in the course of our algorithm is in the order of  $\log(P_1)$  where  $P_1$  is the analytic precision of the computations and as a consequence can

be neglected in the complexity estimates.

In the same way, if  $f \in K[[t_0, \dots, t_k]]$ , we say that we have computed  $f$  to analytic precision  $P_1 \in \mathbb{N}^*$  if we have computed a representative of  $f$  in the ring  $K[[t_0, \dots, t_k]]/\mathfrak{M}_1^P K[[t_0, \dots, t_k]]$  where  $\mathfrak{M}$  is the ideal generated by  $(t_0, \dots, t_k)$ .

## 2. Basic definitions

In order to fix the notations, we first recall some basic facts about Monsky-Washnitzer cohomology with compact support. In the same way as the theory without support, the Monsky-Washnitzer cohomology with compact support associates to a smooth affine curve  $C_k$  of genus  $g$  over the finite field  $k$  a graded  $K$ -vector space of finite dimension denoted by  $(H_{MW,c}^i(C_k/K))_{i \in \{0,1,2\}}$ . There exists a trace formula in this theory which can be used to recover the zeta function of  $C_k$  by computing the action of the Frobenius morphism over the cohomology groups. We remark that as we are dealing with curves, only  $H_{MW,c}^1(C_k/K)$  is non trivial. Moreover, we will use the property of stability of this cohomology theory by finite étale descent to do all our computations over the affine line. This entails working with non-trivial coefficients which are overconvergent modules with connection.

### 2.1. The geometric setting

In the following, we focus on the case of hyperelliptic curves which constitute the simplest family of curves with arbitrary genus. Let  $k$  be a finite field of odd characteristic. Let  $C_k$  be the affine model of a smooth genus  $g$  hyperelliptic curve over  $k$  given by an equation  $Y^2 = \prod_{i=1}^{2g+1} (X - \lambda_i)$  where  $\lambda_i \in k$ . Let  $\pi_k : C_k \rightarrow \mathbb{A}_k^1$  be the projection along the  $Y$ -axis. If we denote by  $U_k$  the étale locus of  $\pi_k$  and by  $V_k$  its image, we have a diagram

$$\begin{array}{ccc} C_k & \longleftarrow & U_k \\ \downarrow \pi_k & & \downarrow \pi_k \\ \mathbb{A}_k^1 & \longleftarrow & V_k \end{array} \quad , \quad (1)$$

where the horizontal maps are open immersions and where  $\pi_k$  is finite étale over  $V_k$ . We let  $A_k$  and  $B_k$  be the coordinate rings of  $U_k$  and  $V_k$ . By [11], Theorem 6, we can lift diagram (1) to a diagram

$$\begin{array}{ccc} C & \longleftarrow & U \\ \downarrow \pi & & \downarrow \pi \\ \mathbb{A}_{W(k)}^1 & \longleftarrow & V \end{array} \quad , \quad (2)$$

of smooth  $W(k)$ -schemes where the horizontal maps are open immersions and  $\pi$  is finite étale over  $V$ . Let  $A$  and  $B$  be the coordinate rings of  $U$  and  $V$  respectively. Let  $\Lambda_k = \{\bar{\lambda}_1, \dots, \bar{\lambda}_{2g+1}, \infty\}$  be the complement of  $V_k(\bar{k})$  in  $\mathbb{P}_k^1(\bar{k})$ . We can suppose that  $B = W(k)[t, (t - \lambda_1)^{-1}, \dots, (t - \lambda_{2g+1})^{-1}]$  where  $t$  is an indeterminate and where  $\lambda_i \in W(k)$  lifts  $\bar{\lambda}_i$  for  $i = 1, \dots, 2g + 1$ . Let  $\Lambda = \{\lambda_1, \dots, \lambda_{2g+1}, \infty\}$ ,  $A_K = A \otimes_{W(k)} K$  and  $B_K = B \otimes_{W(k)} K$ . By finite étale descent (cf Corollary 2.6.6 of [34]) we have  $H_{MW,c}^1(U_k/K) = H_{MW,c}^1(V, \pi_* A_K^\dagger)$ . In the following, we always consider  $A_K^\dagger$  with its  $B_K^\dagger$ -module structure provided by  $\pi$ .

There is a Gauss-Manin connection on  $A_K^\dagger$  and the computation of a basis of the cohomology of a curve comes to the computation of horizontal sections for this connection. In the remaining, if  $t$  is an affine parameter, we will use the notation  $(t - \infty) = t^{-1}$  to indicate a local parameter at the infinity.

## 2.2. The space $B_c$

In this section, we give a definition of the Monsky-Washnitzer cohomology with compact support over a Zariski open subset of the affine line. Note that in this situation this theory coincides with the so-called dual theory of Dwork [8]. Let  $B$ ,  $\Lambda$  as before.

DEFINITION 1. For  $\lambda \in \mathbb{P}_K^1$  rational, let

$$R_\lambda = \left\{ \sum_{n \in \mathbb{Z}} a_\ell (t - \lambda)^\ell \mid a_\ell \in K, \forall \eta < 1, |a_\ell| \eta^\ell \rightarrow_{+\infty} 0, \text{ and} \right. \\ \left. \exists \eta_0 > 1, |a_\ell| \eta_0^{|\ell|} \rightarrow_{-\infty} 0 \right\},$$

be the ring of power series converging on a subset  $\eta_0^{-1} < |t - \lambda| < 1$  with  $\eta_0 > 1$ . The Robba ring associated to  $B$  is the ring

$$\mathcal{R}_B = \bigoplus_\Lambda R_\lambda.$$

We recall that the weak completion of  $B_K = K[t, (t - \lambda_1)^{-1}, \dots, (t - \lambda_{2g+1})^{-1}]$  is

$$B_K^\dagger = \left\{ \sum_{\ell \geq 0} a_\ell t^{\ell_0} (t - \lambda_1)^{-\ell_1} \dots (t - \lambda_{2g+1})^{-\ell_{2g+1}} \mid a_\ell \in K, \exists \eta_0 > 1, \right. \\ \left. |a_\ell| \eta_0^{|\ell|} \rightarrow_{|\ell| \rightarrow \infty} 0 \right\}.$$

The space  $B_c$  of analytic functions with compact support is by definition the quotient of  $\mathcal{R}_B$  by the image of a certain map from  $B_K^\dagger$  into  $\mathcal{R}_B$  that we describe in the following. For  $\lambda \in \Lambda$ , let

$$\phi_\lambda : B_K^\dagger \rightarrow R_\lambda \tag{3}$$

be the injective map which sends  $b_K \in B_K^\dagger$  to the element  $b_\lambda \in R_\lambda$  which is the local development of  $b_K$  at  $\lambda$ .

Let  $i_D : B_K^\dagger \rightarrow \mathcal{R}_B$ , be defined as  $b_K \mapsto \bigoplus_{\lambda \in \Lambda} \phi_\lambda(b_K)$ . Obviously,  $i_D$  is an injection and by definition the space  $B_c$  is the quotient of  $\mathcal{R}_B$  by the image of  $i_D$ . As a consequence, we obtain the short exact sequence of  $K$ -vector spaces

$$0 \longrightarrow B_K^\dagger \xrightarrow{i_D} \mathcal{R}_B \xrightarrow{p_c} B_c \longrightarrow 0, \tag{4}$$

where  $p_c$  is the canonical projection.

Actually, the space  $B_c$  comes with a natural structure of  $B_K^\dagger$ -module that we describe now. To define it, we let

$$R_\lambda^\dagger = \left\{ \sum_{\ell < 0} a_n (t - \lambda)^\ell \mid a_\ell \in K, \exists \eta_0 > 1, |a_{-\ell}| \eta_0^\ell \rightarrow_{+\infty} 0 \right\},$$

and

$$\tilde{R}_\lambda^\dagger = \left\{ \sum_{\ell \leq 0} a_\ell (t - \lambda)^\ell \mid a_\ell \in K, \exists \eta_0 > 1, |a_{-\ell}| \eta_0^\ell \rightarrow_{+\infty} 0 \right\}.$$

DEFINITION 2. Let  $\Lambda_0 = \Lambda \setminus \{\infty\}$ . The principal part at  $\lambda \in \Lambda_0$  is the function defined by

$$\begin{aligned} \text{Pr}_\lambda : R_\lambda &\rightarrow R_\lambda^\dagger, \\ \text{Pr}_\lambda\left(\sum_{\ell \in \mathbb{Z}} a_\ell(t - \lambda)^\ell\right) &= \sum_{\ell < 0} a_\ell(t - \lambda)^\ell. \end{aligned}$$

The principal part at  $\infty$  is the function defined by

$$\begin{aligned} \text{Pr}_\infty : R_\infty &\rightarrow \tilde{R}_\infty^\dagger, \\ \text{Pr}_\infty\left(\sum_{\ell \in \mathbb{Z}} a_\ell t^{-\ell}\right) &= \sum_{\ell \leq 0} a_\ell t^{-\ell}. \end{aligned}$$

We also define the analytic part at any  $\lambda \in \Lambda$  as the identity minus the principal part at  $\lambda$ .

For all  $b_c \in B_c$ , by the Mittag-Leffler theorem (see [30, VI.3.4]), there exists a unique element  $\sigma(b_c)$  of  $\mathcal{R}_B$ , such that  $p_c(\sigma(b_c)) = b_c$  and for all  $\lambda \in \Lambda$ ,  $\text{Pr}_\lambda(\sigma(b_c)) = 0$ . In this way, we have defined a map  $\sigma$  from  $B_c$  to  $\mathcal{R}_B$  and it is immediately verified that  $\sigma$  is a section of  $p_c$  in the exact sequence (4). We now identify  $B_c$  with its image by  $\sigma$  so that we can write

$$B_c = \bigoplus_{\lambda \neq \infty} \tilde{R}_{\lambda,c} \oplus R_{\infty,c}$$

where we denote for  $\lambda \in \mathbb{P}_K^1$  rational

$$R_{\lambda,c} = \left\{ \sum_{\ell > 0} a_\ell(t - \lambda)^\ell \mid a_\ell \in K, \forall \eta < 1, |a_\ell| \eta^\ell \rightarrow_{+\infty} 0 \right\},$$

and

$$\tilde{R}_{\lambda,c} = \left\{ \sum_{\ell \geq 0} a_\ell(t - \lambda)^\ell \mid a_\ell \in K, \forall \eta < 1, |a_\ell| \eta^\ell \rightarrow_{+\infty} 0 \right\}.$$

It is important for the following to remark that  $\sigma \circ p_c$  is given locally as the identity minus the local expansion of the sum of all the principal parts.

The action of  $B_K^\dagger$  over  $B_c$  is given by

$$f.g = p_c(i_D(f). \sigma(g))$$

where  $f \in B_K^\dagger$ ,  $g \in B_c$  and  $\cdot$  is the product in  $\mathcal{R}_B$ .

### 2.3. The space $M_c$

The computation of the space  $H_{MW,c}^1(U_k/K)$  comes to the computation of the de Rham module of analytic forms with compact support. Applying the finite étale descent theorem [34, Cor.2.6.6], this space of analytic functions is

$$M_c = A_K^\dagger \otimes_{B_K^\dagger} B_c.$$

For  $\lambda \in \Lambda_0$ , let  $M_{c,\lambda} = A_K^\dagger \otimes_{B_K^\dagger} \tilde{R}_{\lambda,c}$  and let  $M_{c,\infty} = A_K^\dagger \otimes_{B_K^\dagger} R_{\infty,c}$ . We have,

$$M_c = \bigoplus_{\lambda \in \Lambda} M_{c,\lambda}.$$

An element of  $M_{c,\lambda}$  can be written as

$$m_\lambda = \sum_{j=0,1} Y^j \sum_{\ell=0}^{\infty} b_{j,\ell}^\lambda (t-\lambda)^\ell.$$

with  $b_{j,\ell}^\lambda \in K$  and with  $b_{j,0}^\infty = 0$ . We keep the convention of notation  $(t-\infty) = t^{-1}$ .

The finite  $B_K^\dagger$ -module  $M_c$  comes with a connection given by

$$\begin{aligned} \nabla_c : M_c &\rightarrow M_c \otimes_{B_K^\dagger} \Omega_{B_K^\dagger}^1, \\ m \otimes g_c &\mapsto \nabla_{GM}(m) \otimes g_c + m \otimes \frac{\partial}{\partial t} g_c dt, \end{aligned}$$

where  $\nabla_{GM}$  is the natural Gauss-Manin connection on  $A_K^\dagger$ . In our case this natural connection is given by the partial derivative with respect to  $Y$  acting on the  $B_K^\dagger$ -module  $A_K^\dagger$ . By definition, the space  $H_{MW,c}^1(V, \pi_* A_K^\dagger)$  is the kernel of  $\nabla_c$ . As a consequence to compute a basis of  $H_{MW,c}^1(V, \pi_* A_K^\dagger)$  we have to compute a basis of the space of solutions of the differential equation

$$\nabla_c(m_c) = 0 \tag{5}$$

defined over  $M_c$ . An example of computation of  $\nabla_c$  is provided by (13). Note that by classical results (see for example [22]) the dimension of this space is equal to  $2g$  plus the number of points we took off the affine line, which in our case gives  $4g+1$ .

### 3. An algorithm to compute a basis of an overconvergent isocrystal

We show in this section that the solutions of Equation (5) can be computed by solving a linear system over  $K$ . First, we explain how the action of a linear endomorphism of  $M_c$  with rational coefficients can be computed up to a certain analytic precision by solving a system of linear equations. From this, we deduce two methods, the global method given in Section 3.2 and the local method presented in Section 3.3, for the computation of a basis of solutions of Equation (5). The global method is slow but useful to compute the first analytic development of the solutions required for the quicker local method.

#### 3.1. Action of a rational endomorphism of $M_c$

Let  $Mat$  be a square matrix of dimension 2 with coefficients in the field of rational functions in the indeterminate  $t$  over  $K$ . We make the assumption that the poles of the coefficients of  $Mat$  are contained in  $\Lambda$ . This is always true in the case that  $Mat$  is the connection matrix of  $\nabla_{GM}$  since the connection can only have poles in the locus of the ramification points. For  $m \in M$  and  $g_c \in B_c$ , define  $m_c = m \otimes g_c \in M_c = M \otimes B_c$ . Using the basis  $\{1, Y\}$  of  $M_c$  over  $B_c$  to write  $m_c$  as a column vector of dimension 2 with coefficients in  $B_c$ , our aim is to compute

$$Mat.m_c = (Mat.m) \otimes g_c.$$

We rewrite  $Mat$  as the quotient of a matrix with polynomial coefficients by a polynomial with the lowest possible degree denoted by  $\Delta$ . Let  $o_\lambda$  be the order of the roots of  $\Delta$  at the point  $\lambda \in \Lambda_0$ . Let  $m_o = \max_{\lambda \in \Lambda_0} (o_\lambda)$ . For the rest of the section, we denote by  $M^\vee$  the transpose of a matrix  $M$ .

We explain how we associate vectors with coefficients in  $K$  to elements of  $M_c$ .

DEFINITION 3. Let  $n > 0$  be a positive integer. Let  $m_c \in M_c$  that we can write as  $(m_{\lambda_1}, \dots, m_{\lambda_{2g+1}}, m_\infty)$  with

$$m_{\lambda_i} = \sum_{j=0,1} Y^j \otimes \sum_{\ell=0}^{\infty} b_{j,\ell}^{\lambda_i} (t - \lambda_i)^\ell,$$

where  $b_{j,\ell}^{\lambda_i} \in W(k)$  and  $b_{j,0}^\infty = 0$ , following our conventions. For all  $\lambda \in \Lambda$ , we let

$$v_{m_c, n}^\lambda = (b_{0,0}^\lambda, b_{0,1}^\lambda, \dots, b_{0,n}^\lambda, b_{1,0}^\lambda, \dots, b_{1,n}^\lambda)^\vee, \quad (6)$$

and denote by  $v_{m_c, n}$  the vector

$$v_{m_c, n} = (b_{0,0}^{\lambda_1}, b_{0,1}^{\lambda_1}, \dots, b_{0, m_o+n}^{\lambda_1}, \dots, b_{1, m_o+n}^{\lambda_1}, \dots, b_{1, m_o+n}^\infty)^\vee, \quad (7)$$

which can be written by blocks as

$$v_{m_c, n} = (v_{m_c, m_o+n}^{\lambda_1, \vee}, \dots, v_{m_c, m_o+n}^{\infty, \vee})^\vee. \quad (8)$$

DEFINITION 4. Let  $n \geq 0$  be an integer. Let  $h$  be a rational function in the indeterminate  $t$  with coefficients in  $K$ . Let  $S_{h, \lambda}$  be the Laurent series obtained by expanding  $h$  around  $\lambda \in \Lambda$ . We write

$$S_{h, \lambda} = a_o(t - \lambda)^{-m_o} + a_1(t - \lambda)^{-m_o+1} + \dots + a_{m_o+n}(t - \lambda)^n + \dots$$

and define  $M_{h, \lambda, n}^+$  a matrix of size  $(n+1, m_o+n+1)$ , by

$$M_{h, \lambda, n}^+ = \begin{cases} \begin{pmatrix} a_{m_o} & \dots & a_0 & 0 & 0 & \dots & 0 \\ a_{m_o+1} & \dots & a_1 & a_0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ a_{m_o+n} & \dots & \dots & \dots & \dots & \dots & a_0 \end{pmatrix} & \text{if } \lambda \neq \infty, \\ \begin{pmatrix} 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 \\ 0 & a_{m_o} & \dots & a_1 & a_0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & a_{m_o+n-1} & \dots & \dots & \dots & \dots & \dots & a_0 \end{pmatrix} & \text{if } \lambda = \infty. \end{cases}$$

We let  $M_{\lambda, n}^+$  be the block matrix obtained by replacing in  $Mat$  each of its coefficient equal to a rational function  $h$  by  $M_{h, \lambda, n}^+$ .

DEFINITION 5. We keep the same notations as in the preceding definition. Let  $\lambda' \neq \lambda \in K$ . Let  $h$  be a rational function in the indeterminate  $t$ . Write

$$S_{h, \lambda} = a_o(t - \lambda)^{-m_o} + a_1(t - \lambda)^{-m_o+1} + \dots + a_{m_o+n}(t - \lambda)^n + \dots$$

For  $r \geq 0$  an integer, let  $\eta_0^r, \eta_1^r, \dots, \eta_n^r$  be the  $n+1$  first coefficients of the expansion of  $\sum_{\ell=0}^r a_\ell (t - \lambda)^{-m_o+\ell}$  around  $\lambda'$  (it is a power series). Let  $M_{h, \lambda, n}^{-, \lambda'}$  be the matrix

of dimension  $(n + 1, m_o + n + 1)$  given by

$$M_{h,\lambda,n}^{-,\lambda'} = - \begin{pmatrix} \eta_0^{m_o-1} & \dots & \eta_0^0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ \eta_n^{m_o-1} & \dots & \eta_n^0 & 0 & \dots & 0 \end{pmatrix} \quad \text{if } \lambda \neq \infty,$$

$$M_{h,\lambda,n}^{-,\lambda'} = - \begin{pmatrix} \eta_0^{m_o} & \dots & \eta_0^0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ \eta_n^{m_o} & \dots & \eta_n^0 & 0 & \dots & 0 \end{pmatrix} \quad \text{if } \lambda = \infty.$$

Let  $M_{\lambda,n}^{-,\lambda'}$  be the block matrix obtained by replacing in  $Mat$  each of its coefficient equal to a rational function  $h$  by  $M_{h,\lambda,n}^{-,\lambda'}$ .

We remark that in this definition, if  $\lambda' = \infty$ , then the first line of  $M_{h,\lambda,n}^{-,\lambda'}$  is null, which corresponds to our convention to set the constant term at the infinity to zero. This convention implies that the  $m_o^{th}$  column of  $M_{h,\lambda,n}^{-,\lambda'}$  is zero if  $\lambda = \infty$ .

DEFINITION 6. Still keeping the same notations, for  $n > 0$  an integer, let  $M_n$  be the matrix of dimension  $(2(1 + n)(2g + 2), 2(m_o + n + 1)(2g + 2))$  given by

$$M_n = \begin{pmatrix} M_{\lambda_1,n}^+ & M_{\lambda_2,n}^{-,\lambda_1} & \dots & M_{\infty,n}^{-,\lambda_1} \\ M_{\lambda_1,n}^{-,\lambda_2} & M_{\lambda_2,n}^+ & \dots & M_{\infty,n}^{-,\lambda_2} \\ \dots & \dots & \dots & \dots \\ M_{\lambda_1,n}^{-,\infty} & M_{\lambda_2,n}^{-,\infty} & \dots & M_{\infty,n}^+ \end{pmatrix}.$$

LEMMA 1. Let  $Mat$  be a square matrix of dimension 2 with coefficients in the field of rational functions in the indeterminate  $t$  over  $K$ . Let  $m_c = m \otimes g_c \in M_c$ , then

$$v_{Mat.m \otimes g_c, n - m_o} = M_n.v_{m \otimes g_c, n},$$

where  $v$  is defined by (8).

Proof. We saw in the last section that the action of an overconvergent function  $h \in B_K^\dagger$  on  $g_c \in B_c$  is given by multiplying  $i_D(h)$  by  $\sigma(g_c)$  in the Robba ring  $\mathcal{R}_B$  and then apply  $\sigma \circ p_c$ . This last operation can be done by subtracting the sum of all the principal parts in all the components of  $\sigma(B_c)$ .

Now, the matrix  $M_{\lambda,n}^+$  is such that for any  $m_c \in M_c$  its product with the local component vector  $v_{m_c,n}^{\lambda,\vee}$  gives the first  $n + 1$  terms of the analytic parts of the local product  $Mat.m_\lambda$ . In the same manner, the matrix  $M_{\lambda,n,m_o+1}^{-,\lambda'}$  is such that its product with the local component vector  $v_{m_c,n}^{\lambda,\vee}$  gives the first  $n + 1$  terms of the expansion locally around  $\lambda'$  of the opposite of the principal part in  $\lambda$  of the local product  $Mat.m_\lambda$ .  $\square$

### 3.2. Global method

We can use the notations introduced in Section 3.1 to rewrite the differential equation (5). Here, we let  $Mat$  be the matrix  $Mat_{\nabla_{GM}}$  of the Gauss-Manin connection for the basis  $\{1, Y\}$  of  $M_c$  as a  $B_K^\dagger$ -module. From the computation 13, it is clear that we have  $m_o = 1$ .

DEFINITION 7. Let  $n$  be a positive integer. Let  $D_n$  be the matrix with dimension  $(2(1+n)(2g+2), 2(n+2)(2g+2))$  given by

$$D = \begin{pmatrix} D_{\lambda_1, n} & 0 & \dots & \dots & 0 \\ 0 & D_{\lambda_2, n} & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & \dots & \dots & D_{\infty, n} \end{pmatrix},$$

where  $D_{\lambda_i, n}$  is the diagonal block matrix with dimension  $(2(n+1), 2(n+2))$  such that the diagonal blocks are given by the  $(n+1, n+2)$ -matrices

$$\tilde{D}_{\lambda_i, n} = \begin{pmatrix} 0 & 1 & 0 & \dots & \dots & \dots & 0 \\ 0 & 0 & 2 & 0 & \dots & \dots & \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & \dots & 0 & n+1 & 0 & \dots \end{pmatrix},$$

and where  $D_{\infty, n}$  is the block diagonal  $(2(n+1), 2(n+2))$  matrix the blocks of which are all equal to the  $(n+1, n+2)$  matrix

$$\tilde{D}_{\infty, n} = \begin{pmatrix} 0 & \dots & \dots & \dots & \dots & \dots & 0 \\ 0 & 0 & \dots & \dots & \dots & \dots & 0 \\ 0 & -1 & 0 & \dots & \dots & \dots & 0 \\ 0 & 0 & -2 & 0 & \dots & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & \dots & 0 & -(n-1) & 0 & \dots \end{pmatrix}.$$

PROPOSITION 1. Let  $n > 1$  be an integer. Let  $m_c \in M_c$  be a solution of Equation (5). Then the vector  $v_{m_c, n}$  is a solution of the linear system  $(M_n + D_n) \cdot v = 0$ .

*Proof.* By definition of  $\nabla_c$ , this is a consequence of Lemma 1 and of the fact that the matrix  $D_n$  is such that  $v_{m \otimes \frac{\partial}{\partial t} g_c, n-1} = D_n v_{m \otimes g_c, n}$ .  $\square$

### 3.3. Local method

Let  $\lambda \in \Lambda$ . To simplify the exposition, we suppose in the following that  $\lambda \neq \infty$ . The case  $\lambda = \infty$  can be treated exactly in the same way. In the following,  $K((t-\lambda))$  denotes the field of Laurent series in the indeterminate  $(t-\lambda)$ .

The local method rests on the remark that Equation (5) locally at  $\lambda$  can be regarded as a classical inhomogeneous differential equation if we know enough terms of the global solution.

PROPOSITION 2. Let  $m_c = (m_{\lambda_1}, \dots, m_{\lambda_{2g+1}}, m_{\infty}) \in H_{MW, c}^1(V, \pi_* A_K^\dagger)$ . For  $\lambda \in \Lambda$ , let  $\nabla_{GM, \lambda}$  be the action of the Gauss-Manin connection on the local component in  $\lambda$  of an element of  $M_c$ . For all  $\lambda \in \Lambda$ , there exists a unique  $u = u_0 + Y u_1$ , with  $(u_0, u_1) \in (K((t-\lambda)))^2$  such that  $m_\lambda$  is a solution of a non-homogeneous differential equation:

$$\frac{\partial}{\partial t} m_\lambda + \nabla_{GM, \lambda} m_\lambda = u. \tag{9}$$

*Proof.* Let  $m_c = (m_{\lambda_1}, \dots, m_{\lambda_{2g+1}}, m_{\infty}) \in H_{MW, c}^1(V, \pi_* A_K^\dagger)$ . By definition, it satisfies the equation

$$\nabla_c(m_c) = 0.$$

By rewriting each  $m_\lambda$ ,  $\lambda \in \Lambda$ , as

$$m_\lambda = \sum_{i=0,1} Y^i \otimes g_i^\lambda,$$

where  $g_i^\lambda \in \tilde{R}_{\lambda,c}$  we have

$$\begin{aligned} \nabla_c(m_c) = & \left( \sum_{i=0,1} \nabla_{GM}(Y^i) \otimes g_i^{\lambda_1} + \sum_{i=0,1} Y^i \otimes \frac{\partial}{\partial t} g_i^{\lambda_1}, \dots, \right. \\ & \left. \sum_{i=0,1} \nabla_{GM}(Y^i) \otimes g_i^\infty + \sum_{i=0,1} Y^i \otimes \frac{\partial}{\partial t} g_i^\infty \right) dt. \end{aligned}$$

Let  $f_i \in B_K^\dagger$  be such that

$$\begin{aligned} \nabla_c(m_c) = & \left( \sum_{i=0,1} f_i \cdot Y^i \otimes g_i^{\lambda_1} + \sum_{i=0,1} Y^i \otimes \frac{\partial}{\partial t} g_i^{\lambda_1}, \dots, \right. \\ & \left. \sum_{i=0,1} f_i \cdot Y^i \otimes g_i^\infty + \sum_{i=0,1} Y^i \otimes \frac{\partial}{\partial t} g_i^\infty \right) dt. \end{aligned}$$

Set

$$u = \sum_{i=0,1} Y^i \otimes \phi_\lambda \left( \sum_{\lambda' \in \Lambda} Pr_{\lambda'}(\phi_{\lambda'}(f_i) \cdot g_i^{\lambda'}) \right),$$

where  $\phi_\lambda$  is defined by (3) and  $Pr_\lambda$  is given by Definition 2. We have

$$\frac{\partial}{\partial t} m_\lambda - \nabla_{GM,\lambda} m_\lambda = u,$$

by definition of  $p_c$ . This concludes the proof of the proposition.  $\square$

Let  $m_c = (m_{\lambda_1}, \dots, m_{\lambda_{2g+1}}, m_\infty) \in H_{MW,c}^1(V, \pi_* A_K^\dagger)$ . For  $\lambda \in \Lambda$ , write

$$m_\lambda = \sum_{i=0,1} Y^i \otimes g_i^\lambda,$$

where  $g_i^\lambda \in \tilde{R}_{\lambda,c}$ . Let  $\Phi$  be the morphism of  $K$ -vector spaces defined by  $\Phi : H_{MW,c}^1(V, \pi_* A_K^\dagger) \rightarrow (K[Y])^{2g+2}$ ,

$$m_\lambda = \sum_{i=0,1} Y^i \otimes g_i^\lambda \mapsto \left( \sum_{i=0,1} Y^i \otimes g_i^{\lambda_1}(0), \dots, \sum_{i=0,1} Y^i \otimes g_i^{\lambda_{2g+1}}(0), 0 \right).$$

**COROLLARY 1.** *The map  $\Phi : H_{MW,c}^1(V, \pi_* A_K^\dagger) \mapsto (K[Y])^{2g+2}$  is injective.*

*Proof.* Let  $m_c = (m_{\lambda_1}, \dots, m_{\lambda_{2g+1}}, m_\infty) \in H_{MW,c}^1(V, \pi_* A_K^\dagger)$ . By Proposition 2, for all  $\lambda \in \Lambda$ ,  $m_\lambda$  satisfies a degree 1 local inhomogeneous differential equation and there is a unique solution of this equation with constant term given by  $\Phi(m_c)$ .  $\square$

We have to check that the solution that we obtain satisfies the condition that the constant term at the infinity point is zero.

DEFINITION 8. Let  $n > 0$  be an integer. Let  $Rel_n$  be the sub- $K$ -vector space of  $K^{2(2g+2)(n+2)}$  generated by the vectors

$$(e_1, \dots, e_{2(2g+2)(n+2)})^\vee$$

such that the  $e_i$  are zero for

$$i \in \{2((2g+1)(n+2) + 1 + j(n+2)) | j \in \{0, 1\}\}.$$

The linear system we associated to the equation

$$\nabla_c(m_c) = 0$$

admits trivial solutions that we have to put aside. These solutions come from the fact that the derivation with respect to  $t$  increases the degree locally at the point at infinity. For instance, when truncating above the degree  $n > 0$ , then  $(0, \dots, 0, 1 \otimes t^{-n})$  corresponds always to a solution of the linear system even though in general it is not a solution of the equation  $\nabla_c(m_c) = 0$ .

DEFINITION 9. Let  $n > 0$  be an integer. Let  $Triv_n$  be the sub- $K$ -vector-space of  $K^{2(2g+2)(n+2)}$  spanned by the vectors

$$(e_1, \dots, e_{2(2g+2)(n+2)})^\vee$$

such that the  $e_i$  are zero, except for

$$i \in \{2(2g+1)(n+2) + j(n+3-s) | j \in \{1, 2\}, s \in \{1, 2\}\}.$$

In order to get rid of the terms of  $Triv_n$ , we simply truncate the solutions and keep only the resulting independent vectors with coefficients in  $K$ . It would be enough to truncate only the local part at infinity, but we truncate globally for the sake of clarity. Note also that by Corollary 1, a solution with all local constant terms equal to zero is globally equal to zero, so that we don't drop any valid solution by truncating.

DEFINITION 10. If  $n > 2$  and if  $v = (v_1, \dots, v_{2(2g+2)(n+2)})$  is an element of  $K^{2(2g+2)(n+2)}$  we let

$$Tronc(v, n) = (v_1, \dots, v_{n-2}, v_{n+1}, \dots, v_{2n-2}, v_{2n+1}, \dots, v_{2(2g+2)(n+2)-2})^\vee.$$

In particular, we have

$$Tronc(v_{m_c, n}, n) = v_{m_c, n-2}.$$

PROPOSITION 3. Let  $n > 0$  be an integer. Let  $v$  be a solution of the linear system

$$(M_{n+2} + D_{n+2})v = 0$$

in  $Rel_n$ . Then there exists a unique element  $m \in \oplus_\Lambda M_{c, \lambda} \otimes K[[t - \lambda]]$  solution of the Equation (5) such that

$$v_{m, n} = Tronc(v, n)$$

where we have generalized in an evident manner the definition  $v_{m, n}$  to  $\oplus_\Lambda M_{c, \lambda} \otimes K[[t - \lambda]]$ . More precisely, there exists  $v_{Triv} \in Triv_{n+2}$  such that  $v_{m, n+2} = v + v_{Triv}$ .

*Proof.* From Corollary 1, a solution is uniquely determined by its first terms.  $\square$

An approximation of a formal solution of a differential equation can be computed by one or the other of the above explained methods, but nothing has been said, up to now, about the convergence of the solutions that we approximate. We have yet to prove that a formal solution of the differential equation is in  $M_c$ . This can be done by finding some conditions for the convergence on the coefficients of a formal solution.

### 3.4. Explicit upper bound of the coefficients of a basis of the cohomology

We present an upper bound on the valuation of the coefficients of a basis of the space  $H_{MW,c}^1(V) = H_{MW,c}^1(U, \pi_* A_K^\dagger)$ .

**PROPOSITION 4.** *Let  $m_c = (m_{\lambda_1}, \dots, m_{\lambda_{2g+1}}, m_\infty)$  be an element of the vector space  $H_{MW,c}^1(U, \pi_* A_K^\dagger)$ . Let  $u = u^0 + u^1 Y$ , with for  $j = 0, 1$ ,  $u^j = \sum_{\ell=0}^\infty u_\ell^j (t - \lambda)^\ell$ . Suppose that  $m_\lambda$  is a solution of the equation*

$$\frac{\partial}{\partial t} m_\lambda + \nabla_{GM,\lambda} m_\lambda = u,$$

then there exists a real number  $B > 0$  such that for  $j = 0, 1$  and all  $\ell$

$$v_p(u_\ell^j) > B.$$

*Proof.* Let  $m_c = (m_{\lambda_1}, \dots, m_{\lambda_{2g+1}}, m_\infty) \in H_{MW,c}^1(V, \pi_* A_K^\dagger)$  with

$$m_{\lambda_i} = \sum_{j=0,1} Y^j \sum_{\ell=0}^\infty b_{j,\ell}^{\lambda_i} (t - \lambda_i)^\ell,$$

with  $b_{j,\ell}^{\lambda_i} \in K$  and with  $b_{j,0}^\infty = 0$  (still keeping the convention  $t - \infty = t^{-1}$ ). Let  $\lambda \in \Lambda$ . Writing the Gauss-Manin connection as a quotient:

$$\nabla_{GM} = \frac{G(t)}{\Delta(t)},$$

where  $G(t)$  is a linear transformation which can be written in the basis  $\{1, Y\}$  as a  $(2, 2)$ -matrix with coefficients in  $W(k)[t]$  and  $\Delta(t) \in W(k)[t]$  has simple roots. By Proposition 2, and because each  $\lambda' \in \Lambda_0$  is at most a simple root of  $\Delta$ , the vector  $m^\lambda$  satisfies the equation

$$\frac{\partial}{\partial t} m^\lambda + \nabla_{GM,\lambda} m^\lambda = u,$$

with

$$u = \sum_{\lambda' \in \Lambda} \frac{G(\lambda')}{\Delta'(\lambda')} c^{\lambda'} (t - \lambda')^{-1},$$

where  $c^{\lambda'} = b_{0,0}^{\lambda'} + Y b_{1,0}^{\lambda'}$ .

We have for all  $\lambda, \lambda' \in \Lambda_0$ ,

$$v_p(\lambda - \lambda') = 0$$

by hypothesis. As a consequence, if one writes  $u = u^0 + Y u^1$ , with for  $j = 0, 1$ ,  $u^j = \sum u_\ell^j (t - \lambda)^\ell$ , then

$$v_p(u_\ell^j) \geq \min_{\lambda' \in \Lambda} \left( v_p \left( \frac{G(\lambda')}{\Delta'(\lambda')} c^{\lambda'} \right) \right), \quad (10)$$

where we extend  $v_p$  on vectors with coefficients in  $W(k)$  by taking the minimum of the valuation of the components.

Equation (10) follows the remark that expanding in a neighbourhood of  $\lambda$ , we find

$$(t - \lambda')^{-1} = - \sum_{\ell=0}^{\infty} \frac{1}{(\lambda' - \lambda)^{\ell+1}} (t - \lambda)^{\ell}.$$

As a consequence, we can take

$$B = \min_{\lambda' \in \Lambda} \left( v_p \left( \frac{G(\lambda')}{\Delta'(\lambda')} c^{\lambda'} \right) \right),$$

in the statement of the theorem. □

**THEOREM 1.** *Let  $m_c = (m_{\lambda_1}, \dots, m_{\lambda_{2g+1}}, m_{\infty})$  be an element of  $H_{MW,c}^1(V, \pi_* A_K^{\dagger})$  with*

$$m_{\lambda_i} = \sum_{j=0,1} Y^j \sum_{\ell=0}^{\infty} b_{j,\ell}^{\lambda_i} (t - \lambda_i)^{\ell},$$

with  $b_{j,\ell}^{\lambda_i} \in W(k)$  and with  $b_{j,0}^{\infty} = 0$ . Let  $\lambda \in \Lambda$ . Then there exist  $\alpha \in \mathbb{R}$  and  $\beta \in \mathbb{R}$  such that

$$v_p(b_{j,\ell}^{\lambda}) \geq -(\alpha \log_p(\ell) + \beta), \tag{11}$$

for all  $j$  and all  $\ell$ . Moreover,  $\alpha$  and  $\beta$  can be made explicit (see the Remark 1).

*Proof.* We prove that the hypothesis of the Theorem 2.3.3 of [4] are verified. By a direct computation, we find that the local exponents of  $Mat_{\nabla_{GM}}$  are in  $\{0, -\frac{1}{2}\}$ , so that they are prepared and the hypothesis 1 is satisfied. The hypothesis 4 is already contained in our statement. The hypothesis 2 can be checked by applying the classical Dwork's trick (see for example [16], Proposition 3.1). In order to be able to apply this result, it is necessary to provide the  $B_K^{\dagger}$ -module  $(\pi_* A_K^{\dagger}, \nabla_{GM})$  with a Frobenius morphism. Fix a Frobenius morphism  $F$  on  $A_K^{\dagger}$  lifting the  $p^{\text{th}}$  power on  $A_k$  such that  $F$  sends  $X$  over  $X^p$  and acting on  $K$  as the Frobenius automorphism. Then  $F$  induces a Frobenius morphism  $F_{GM}$  over  $(\pi_* A_K^{\dagger}, \nabla_{GM})$  and the Dwork's trick applies. In the same manner, we provide the dual module with connection  $(\pi_* A_K^{\dagger}, \nabla^{\vee})$  with the Frobenius morphism  $F_{GM}^{-1}$ . The hypothesis 3 is true from Proposition 4, and the hypothesis 5 is easily verified in our case. The expression of  $B$  given in the proof of the Proposition 4 gives the theorem. □

The following proposition proves that the formal solutions of the differential system 5 are in  $M_c$ . This indeed shows the correctness of the algorithm described in Section 4.1.

Taking back the notation of the Section 3,

**PROPOSITION 5.** *Let  $v$  be a solution of the linear system  $(M_n + D_n)v = 0$  belonging to  $Rel_n$  and let  $m \in \oplus_{\Lambda} M_{c,\lambda} \otimes K[[t - \lambda]]$  be the unique solution of the Equation (5) such that  $v_{m,n} = Tronc(v, n)$ . Then  $m$  is an element of  $M_c$ .*

*Proof.* From the Theorem 1, the coefficients of the local part  $m_{\lambda}$  of  $m$  satisfy the logarithmic bounds of Equation (11) for all  $\lambda \in \Lambda$ . In particular, this implies that the  $m_{\lambda}$  are all in  $R_{\lambda,c}$ . □

REMARK 1. One can obtain explicit formulas for the constants  $\alpha$  and  $\beta$  of the theorem. The proof of Theorem 2.3.3 (inspired from methods of Alan Lauder) in [4] gives the expressions

$$\alpha = 2\alpha' + 2$$

and

$$\beta = 2\beta' + 2\log_p(3) - B$$

the constants  $\alpha'$  and  $\beta'$  are computed in [19, Note 4.11], with the following expressions:

$$\alpha' = 2(1 + \log_p(2)) + 3$$

and

$$\beta' = \alpha' \log_p(5) + \beta_2 + \beta_3$$

where

$$\beta_2 = 2(1 + \log_p(2)) + 3$$

and

$$\beta_3 = 4\left(\frac{2}{p-1} + 4\log_p(3) + 2\log_p(2)\right).$$

REMARK 2. Let us consider the term  $B$ . Recall that we saw in the proof of Proposition 4 that we have (we keep the notations of the proof)

$$B \geq \min_{\lambda \in \Lambda} \left( v_p \left( \frac{G(\lambda)}{\Delta'(\lambda)} c^\lambda \right) \right). \quad (12)$$

where  $c^\lambda$  is formed by the constant terms of the element of the cohomology group we consider so that we can suppose that its  $p$ -adic valuation is zero. Now since the matrix of the connection is

$$\text{Mat}_{\nabla_{GM}} = Q(t)^{-1} \begin{pmatrix} 0 & 0 \\ 0 & \frac{Q'(t)}{2} \end{pmatrix}$$

the only non-zero term of  $\frac{G(\lambda')}{\Delta'(\lambda')}$  is  $1/2$  and we can suppose  $B = 0$ .

#### 4. Description of the algorithm and complexity analysis

In this section, we present an algorithm, based on the results of Section 3, to compute a basis of the Monsky-Washnitzer cohomology with compact support of an hyperelliptic curve. The algorithm takes as input:

- a finite field of odd characteristic  $k$ ,
- a genus  $g$  hyperelliptic curve  $\overline{C}_k$  over  $k$ , given by an equation  $Y^2 = \prod_{i=1}^{2g+1} (X - \overline{\lambda}_i)$ , with  $\overline{\lambda}_i \in k$  distinct,
- two positive integers  $P_1$  and  $P_2$ ,

and returns a basis of the space  $H_{MW,c}^1(V, \pi_* A_K^\dagger)$  computed with analytic precision  $P_1$  and absolute  $p$ -adic precision  $P_2$ .

4.1. An algorithm for the computation of a basis of the cohomology of Monsky-Washnitzer of a curve

Denote by  $C_k$  an affine plane model of  $\overline{C}_k$ . We denote by  $t$  the coordinate on  $\mathbb{A}_k^1$ .

4.1.1. The set up

For  $i = 1, \dots, 2g + 1$ , let  $\lambda_i \in W(k)$  lifting  $\bar{\lambda}_i$ . Let  $\overline{C}_K$  be the hyperelliptic curve over  $K$  given by the equation

$$Y^2 = Q(X) \quad \text{with} \quad Q(X) = \prod_{i=1}^{2g+1} (X - \lambda_i).$$

Denote by  $\infty$  the point an infinity of  $\overline{C}_K$ . Keeping the notations of Section 3, we let  $\Lambda = \{\lambda_1, \dots, \lambda_{2g+1}, \infty\}$  and  $\Lambda_0 = \Lambda \setminus \{\infty\}$ . Let  $V$  be the subvariety of  $\mathbb{P}_K^1$  whose geometric point set is the complementary of  $\Lambda$ , let  $U = \pi^{-1}(V)$  where  $\pi$  is the projection along the  $Y$ -axis. Let  $U_k$  and  $V_k$  be respectively  $U$  and  $V$  modulo  $p$ .

The algorithm goes through the following 3 steps.

4.1.2. Step 1: computation of the connection matrix

The Gauss-Manin connection matrix on  $A_K^\dagger$  is easily described. We fix from now on the basis  $\{1, Y\}$  of the  $B_K^\dagger$ -module  $A_K^\dagger$ . The matrix is given by the derivation with respect to  $Y$  in  $A_K^\dagger$  seen as a  $B_K^\dagger$ -module. Since in  $\Omega_A^1$  we have  $dY = \frac{Q'(X)}{2Q(X)} Y.dX$ , the Gauss-Manin connection matrix over  $A_K^\dagger$  associated to the projection  $\pi : U \rightarrow V$  is:

$$Mat_{\nabla_{GM}} = Q(t)^{-1} \begin{pmatrix} 0 & 0 \\ 0 & \frac{Q'(t)}{2} \end{pmatrix}. \tag{13}$$

4.1.3. Step 2: Computation of the matrix  $M_n$

(see Section 3.1) Here  $n$  is the analytic precision of the computation which will be fixed later, depending on whether we use the local or the global method.

In order to obtain the matrix  $M_n$ , we have to compute for  $\lambda \in \Lambda$  the local development in  $\lambda$  of  $Q'(t)/Q(t)$  that we denote by  $S_{\nabla, \lambda}(t)$  and for each  $\lambda, \lambda' \in \Lambda$  the local development in  $\lambda'$  of the principal part of  $S_{\nabla, \lambda}(t)$ .

The development of  $Q'(t)$  in  $\lambda$  is nothing but the evaluation  $Q'(t + \lambda)$  which can be done using Horner's method or the Paterson-Stockmeyer algorithm [28]. The computation of a development of  $1/Q(t)$  in  $\lambda$  can be done by

- computing a local development  $S_{Q, \lambda}(t)$  of  $Q(t)$  in  $\lambda$  using Horner's method;
- inverting  $S_{Q, \lambda}(t)$  using a Newton iteration.

The case of  $\lambda = \infty$  can be treated in a similar manner.

Then we have to compute the product of the local developments in  $\lambda$  of  $Q'(t)$  and  $1/Q(t)$  to obtain  $S_{\Delta, \lambda}(t)$ .

As  $S_{\nabla, \lambda}(t)$  can only have simple poles, the computation of a local development of the principal part of  $S_{\nabla, \lambda}(t)$  in  $\lambda'$  comes to the computation of an inverse locally at zero of a term of the form  $t + \lambda - \lambda'$  which can be done by a Newton iteration.

4.1.4. Step 3: solving the equation  $\nabla_c(m_c) = 0$

The next step is to solve the equation  $\nabla_c(m_c) = 0$  on  $M_c$ . We have to compute modulo  $(t - \lambda)^{P_1}$  locally at  $\lambda \in \Lambda$  and modulo  $p^{P_2}$  for the  $p$ -adic precision. In section 3, we have given two ways to obtain a basis of solutions of the differential equation  $\nabla_c(m_c) = 0$ . We use the local method after determining the first terms of a basis thanks to the global method. It should be remarked that due to the special form of the connection associated to a hyperelliptic curve, it is possible in the case we consider to compute directly these terms. Still we present the global method for its general interest.

4.1.4.1. *Global method.* We first use the global method to compute a basis of solutions at small fixed analytic precision. For this, we have to compute the matrices  $M_1$  and  $D_1$  and solve the linear system

$$(M_1 + D_1)v = 0,$$

over  $K$ . Then it is necessary to put aside the trivial solutions belonging to  $Triv_1$  and project the remaining ones onto  $Rel_1$ . To conclude, we truncate the remaining vectors as explained in Proposition 9.

4.1.4.2. *Local method.* Denote by  $m_c^1, \dots, m_c^{4g+1} \in M_c$  the elements of a basis of the space  $H_{MW,c}^1(V, \pi_* A_K^\dagger)$  computed up to analytic precision 1 with the global method. For  $j = 1, \dots, 4g + 1$ , we write,  $m_c^j = (m_{\lambda_1}^j, \dots, m_{\lambda_{2g+1}}^j, m_\infty^j)$ .

For a fixed  $\lambda \in \Lambda$ , we explain how to lift  $m_c^j$ , for  $j = 1, \dots, 4g + 1$ , using the local differential equation provided by Proposition 2. For this, we have to compute the constant term of Equation (9). The general expression of this coefficient is

$$u_j = \sum_{i=0,1} Y^i \otimes \phi_\lambda \left( \sum_{\lambda' \in \Lambda} Pr_{\lambda'}(\phi_{\lambda'}(f_i) \cdot g_{j,i}^{\lambda'}) \right),$$

where  $f_i$  depends only on the Gauss-Manin connection and for  $\lambda \in \Lambda$ ,  $g_{j,i}^\lambda \in \tilde{R}_{\lambda,c}$  is such that

$$m_\lambda^j = \sum_{i=0,1} Y^i \otimes g_{j,i}^\lambda.$$

As  $f_i$  has only simple poles, we can write

$$\phi_\lambda \left( \sum_{\lambda' \in \Lambda} Pr_{\lambda'}(\phi_{\lambda'}(f_i) \cdot g_{j,i}^{\lambda'}) \right) = \sum_{\lambda' \in \Lambda} \phi_\lambda(Pr_{\lambda'}(\phi_{\lambda'}(f_i))) \cdot g_{j,i}^{\lambda'}(0).$$

We remark that  $g_{j,i}^{\lambda'}(0)$  can be computed with the global method. As a consequence, once we have computed for a fixed  $\lambda \in \Lambda$ ,  $r_{\lambda,\lambda'} = \phi_\lambda(Pr_{\lambda'}(\phi_{\lambda'}(f_i)))$ , it is possible to recover  $u_j$  by computing a linear combination of the  $r_{\lambda,\lambda'}$  with coefficient in  $K$ .

Equation (9) can be rewritten as an equation of the form

$$Z' = AZ + B,$$

where  $A$  (resp.  $B$ ) is a  $(2, 2)$ -matrix (resp.  $(2, 1)$ -matrix) with coefficients in  $K[[t]]$ . It is possible to compute an approximation of the unique solution  $Z$  of this equation satisfying  $Z(0) = v$  with precision  $P_1$  using an asymptotically fast algorithm such as given by Proposition 1 of [2]. The initial value  $v$  comes from the global method.

REMARK 3. It should be remarked that the algorithm described in Proposition 1 of [2] to compute a solution of a differential system to analytic precision  $P_1$  may involve divisions by multiples of a uniformizing element of  $K$ . We explain that it is easy in our case to control the loss of absolute  $p$ -adic precision induced by this algorithm.

For this, we first recall the idea of the algorithm given in Proposition 1 of [2]. Denote by  $\mathcal{E}(B, \lambda, P_1)$  the vector equation

$$tZ' + (\lambda I - tA) = B \pmod{t^{P_1}},$$

where  $\lambda \in K$ . We remark that we want to solve  $\mathcal{E}(tB, 0, P_1)$ .

Let  $d$  be a positive integer and let  $B_0$  and  $B_1$  be polynomials in  $t$  of respective degrees  $d - 1$  and  $P_1 - d - 1$  such that

$$B \pmod{t^{P_1}} = B_0 + t^d B_1 \pmod{t^{P_1}}.$$

If  $z_0$  is a solution of  $\mathcal{E}(B_0, \lambda, d)$ , we let

$$R(z_0, B_0, \lambda, d, P_1) = (tz'_0 + (\lambda I - tA)z_0 - B_0)/t^d \pmod{t^{P_1-d}}, \quad (14)$$

and denote by  $z_1$  a solution of  $\mathcal{E}(B_1 - R, \lambda + d, P_1 - d)$  where  $R = R(z_0, B_0, \lambda, d, P_1)$ . The algorithm described in Proposition 1 of [2] rests upon a divide and conquer strategy based on the remark that  $z = z_0 + t^d z_1$  is a solution of  $\mathcal{E}(B, \lambda, P_1)$ . When the required analytic precision is 1, a solution of  $\mathcal{E}(B', \lambda', 1)$  is given by  $B'(0)/\lambda'$ . It is easily seen that in the course of the algorithm  $\lambda'$  is running over all the values in  $\{1, \dots, P_1\}$ .

Now, write  $B = \sum_{i=0}^{P_1-1} B_i t^i$ ,  $B_i \in K$  and let  $z = \sum_{i=0}^{P_1-1} z_i t^i$ ,  $z_i \in K$  be the solution of  $\mathcal{E}(B, 0, P_1)$  satisfying a given initial condition. We explain that if  $v_p(z_i) \geq -v_0$  and  $v_p(B_i) \geq -v_0$  for  $v_0$  a positive integer, when doing all the computations of the algorithm of [2] with relative  $p$ -adic precision  $v_0 + P_2$  we obtain an approximation of  $z$  with absolute  $p$ -adic precision  $P_2$ . All the arithmetic operation in the algorithm are sums except in the computation of  $R(z_0, B_0, \lambda, d, P_1)$  and the computation of terms of the form  $B'(0)/\lambda$ . First, the terms of the form  $B'(0)/\lambda$  are coefficients of  $z$  and by hypothesis their valuation is bigger than  $-v_0$ .

Next, if we write  $z_0 = \sum_{i=0}^{d-1} z_{0,i} t^i$ ,  $z_{0,i} \in K$  and  $B_0 = \sum_{i=0}^{d-1} B_{0,i} t^i$ ,  $B_{0,i} \in K$ , we have:

$$R(z_0, B_0, \lambda, d, P_1) = -Az_{0,d-1}.$$

As a consequence,  $B_1(0) - R = B_1(0) + Az_{0,d-1}$  and we know that pursuing the divide and conquer algorithm we end up by solving an equation of the form  $\mathcal{E}(B_1(0) - R, \lambda, 1)$  for a certain  $\lambda \in \{1, \dots, P_1\}$ . Thus  $(B_1(0) - R)/\lambda$  is a coefficient of  $z$  and  $v_p(B_1(0) + Az_{0,d-1}) \geq -v_0$ . But as  $v_p(B_1(0)) \geq -v_0$  by hypothesis (and an easy recurrence), we have  $v_p(R(z_0, B_0, \lambda, d, P_1)) \geq -v_0$ .

#### 4.2. Complexity analysis

In order to assess the complexity of our algorithm we use the computational model of a Random Access Machine [27]. In this paper, we use the soft-O notation and choose to ignore logarithmic terms in the complexity functions. For instance, using the algorithm of Schönhage-Strassen, the multiplication of two  $n$ -bit length integers takes  $\tilde{O}(n)$  time. We suppose that  $k$  is a finite field of cardinality  $q$  and characteristic  $p$ . In the following we assume the sparse modulus representation

which is explained in [6, pp.239]. Let  $x, y \in W(k)/p^{P_2}W(k)$ , under this assumption one can compute the product  $xy$  with precision  $P_2$  by performing  $M = \tilde{O}(\log(q)P_2)$  bit operations. The storage requirement for an element of  $W(k)$  with precision  $P_2$  is  $O(\log(q)P_2)$ .

Let  $h = \sum_{\ell \geq 0} a_\ell t^\ell \in W(k)[[t]]$  with  $a_\ell \in W(k)$ . We say that we have computed  $h$  up to precision  $P_1$  if we have computed a representative of  $h \pmod{t^{P_1}}$ . Using the algorithm given in [35], the multiplication of two polynomials of degree  $P_1$  with coefficients in  $W(k)$  takes  $\tilde{O}(P_1)$  operations in  $W(k)$ . As a consequence, the multiplication of two elements of  $W(k)[[t]]$  with precision  $P_1$  takes  $N = \tilde{O}(\log(q)P_2P_1)$  time. The storage requirement for an element of  $W(k)[[t]]$  with analytic precision  $P_1$  and  $p$ -adic precision  $P_2$  is  $O(\log(q)P_1P_2)$ .

Now, we give time and memory complexity bounds for the computation of a basis of the cohomology with analytic precision  $P_1$  and absolute  $p$ -adic precision  $P_2$  under the hypothesis that  $P_1 = O(P_2)$ . In this case, Theorem 1 shows that the  $p$ -adic valuation of the coefficients of the elements of the computed basis of  $H_{MW,c}^1(V, \pi_* A_K^\dagger)$  is greater than  $-\log_p(P_2)$ . As a consequence, in order to perform the computations with absolute  $p$ -adic precision  $P_2$  we have to compute with relative  $p$ -adic precision at most  $P_2 + \log_p(P_2)$ . In our complexity analysis, we neglect this  $\log_p(P_2)$  term and suppose that the absolute and relative precision are the same.

We refer to Section 4.1 for the description of each step.

#### 4.2.1. Step 1:

The asymptotic running time of this step is clearly negligible with respect to the other steps.

#### 4.2.2. Step 2:

Using the local method, we only have to compute  $M_1$  which makes the running time of this step also negligible with respect to the other steps.

#### 4.2.3. Step 3:

In this step, we use the global method to compute the first terms of the solutions required for the local method.

4.2.3.1. *The global method.* We have to inverse a matrix with coefficients in  $K$  the dimension of which is in the order of  $g$ . The total cost is  $\tilde{O}(g^3 \log(q)P_2)$  time and  $O(g^2 \log(q)P_2)$  memory.

4.2.3.2. *The local method.* We keep the notations of Section 4.1 Step 3. First, for a fixed  $\lambda \in \Lambda$ , we give the running time and memory usage for the computation of a lift of  $m_j^\lambda$  for  $j$  running in  $\{1, \dots, 4g + 1\}$ .

We compute  $r_{\lambda, \lambda'} = \phi_\lambda(\text{Pr}_{\lambda'}(\phi_{\lambda'}(f_i)))$  for  $\lambda' \in \Lambda$ . In order to do this, we have to develop  $f_i$  in  $\lambda'$ . With our hypothesis the only non trivial  $f_i$  has the form  $Q'(t)/Q(t)$ .

Suppose that  $\lambda, \lambda' \in \Lambda_0$ . The computation of a local development of  $Q'$  in  $\lambda'$  can be done with the evaluation  $Q'(t + \lambda')$ . Using Horner's method or the Paterson-Stockmeyer algorithm [28], it takes  $O(gM)$  time. The computation of a local development of  $1/Q(t)$  in  $\lambda'$  with a Newton iteration takes  $O(\log(P_1)N)$  time. Then we have to compute the product of the local developments of  $Q'$  and  $1/Q$ . This product takes  $O(N)$  time. Taking the principal part is trivial. Then we use again

a Newton iteration to compute a development in  $\lambda$  of a principal part of the form  $1/(t - \lambda')$ . If  $\lambda = \infty$  or  $\lambda' = \infty$ , we have to adapt slightly the preceding algorithms with no change on the complexity estimate. We are done for the computation of  $r_{\lambda, \lambda'}$ .

We have to repeat this operation  $O(g)$  times to obtain all the coefficients  $r_{\lambda, \lambda'}$  at the expense of  $\tilde{O}(g \log(q) P_1 P_2)$  time and  $\tilde{O}(g \log(q) P_1 P_2)$  memory.

Then in order to lift  $m_\lambda^j$ , for  $j = 1, \dots, 4g + 1$ , we have to solve an equation of the form  $Z' = AZ + B$ . This is a first order linear differential equation and applying Theorem 2 of [2] in conjunction with Remark 3, a solution of this equation with analytic precision  $P_1$  and relative  $p$ -adic precision  $P_2$  can be computed in  $O(N)$  time.

Now, we have to repeat all the preceding operations for  $\lambda$  running in  $\Lambda$ . In all the computational time is  $\tilde{O}(g^2 \log(q) P_1 P_2)$  and the memory consumption is  $O(g \log(q) P_1 P_2)$ .

**PROPOSITION 6.** *Let  $P_1$  and  $P_2$  be positive integers. The global time for the computation of a basis of  $H_{MW,c}^1(V, \pi_* A_K^\dagger)$  with analytic precision  $P_1$  and absolute  $p$ -adic precision  $P_2$  under the hypothesis that  $P_1 = O(P_2)$  is bounded by  $\tilde{O}(g^2 \log(q) P_1 P_2)$ . The memory consumption is  $O(g \log(q) P_1 P_2)$ .*

### 4.3. An example

In this section, we give a detailed example of computation. In order to simplify the presentation, we represent the elements of  $\mathbb{Q}_5$  as rational numbers so all our computations with the  $p$ -adic numbers are exact. We consider the case of the elliptic curve with equation  $Y^2 = X^3 - X$  over  $\mathbb{F}_5$ . We lift the equation to  $Y^2 - X^3 + X \in \mathbb{Z}_5[X, Y]$  so that we are interested in the finite module  $M$  with basis  $\{1, Y\}$  over  $\mathbb{Q}_5[t, t^{-1}, (t-1)^{-1}, (t+1)^{-1}]^\dagger$ . We denote as before  $\Lambda = \{\infty, 0, 1, -1\}$  and consider the connection on  $M$  given by the matrix

$$Mat_{\nabla_{GM}} = (\Delta(t))^{-1} \begin{pmatrix} 0 & 0 \\ 0 & \frac{3t^2-1}{2} \end{pmatrix},$$

where  $\Delta(t) = t^3 - t$ . Let  $h(t) = 1/(2\Delta)(3t^2 - 1)$  be the only non-zero term of this matrix. Its local development in Laurent series at the elements of  $\Lambda$  are:

- at  $\infty$ :  $\frac{3}{2}t + t^3 + O(t^4)$ ,
- at  $0$ :  $\frac{1}{2}t^{-1} - t - t^3 + O(t^4)$ ,
- at  $1$ :  $\frac{1}{2}t^{-1} + \frac{11}{8} - \frac{5}{8}t + \frac{9}{16}t^2 - \frac{17}{32}t^3 + O(t^4)$ ,
- at  $-1$ :  $\frac{1}{2}t^{-1} - \frac{11}{8} - \frac{5}{8}t - \frac{9}{16}t^2 - \frac{17}{32}t^3 + O(t^4)$ .

So that we have:

$$M_{h, \infty, 1}^+ = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix},$$

$$M_{h, 0, 1}^+ = \begin{pmatrix} 0 & \frac{1}{2} & 0 \\ -1 & 0 & \frac{1}{2} \end{pmatrix},$$

$$M_{h, 1, 1}^+ = \begin{pmatrix} \frac{11}{8} & \frac{1}{2} & 0 \\ -\frac{5}{8} & \frac{11}{8} & \frac{1}{2} \end{pmatrix},$$



Its kernel is spanned by the vectors:

- $v_1 = (1, 0)^\vee$ ,
- $v_2 = (0, 1, 0)^\vee$ ,
- $v_3 = (0, 0, 1, 0)^\vee$ ,
- $v_4 = (0, 0, 0, 1, 0)^\vee$ ,
- $v_5 = (0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)^\vee$ ,
- $v_6 = (0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)^\vee$ ,
- $v_7 = (0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)^\vee$ ,
- $v_8 = (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)^\vee$ ,
- $v_9 = (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0)^\vee$ ,
- $v_{10} = (0, 0, 0, 0, 0, 0, 0, 0, 0, 1, -\frac{1}{3}, \frac{3}{5}, 0, 0, 0, 0, \frac{1}{6}, -\frac{29}{24}, 0, 0, 0, -1, -\frac{5}{4}, -\frac{91}{80})^\vee$ ,
- $v_{11} = (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, -\frac{2}{3}, 0, 0, 0, 0, 1, -\frac{13}{12}, \frac{43}{48}, 0, 0, 0, -1, -\frac{13}{12}, -\frac{43}{48})^\vee$ .

The first six vectors are trivial or non-relevant solutions since either their truncature is zero either setting their constant term at the infinity to zero makes them null, so that we find that  $H_{MW,c}^1(V, \pi_* A_K^\dagger)$  has dimension 5. Since our curve is of genus 1 and since we took off three points out of it, this agrees with the theoretical dimension.

### 5. The action of Frobenius on the basis

We keep in this section the notations already introduced, and suppose furthermore that the roots  $\lambda$  of  $Q$  are Teichmüller elements [6]. We explain how to compute a lifting of the Frobenius morphism to  $M_c$  and obtain its action on a basis of  $H_{MV,c}^1(U, \pi_* A_K^\dagger)$ . Of course all the computations are made with finite analytic and  $p$ -adic precisions and the key point here is the determination of sufficient precisions in order to guarantee the correctness of the final result.

#### 5.1. Lifting the Frobenius morphism

Following Kedlaya [17], we define a lift  $F$  of the  $p$ -th Frobenius on  $A_K^\dagger$  by setting  $F(X) = X^p$  and

$$F(Y) = Y^p \left( 1 + \frac{Q^\sigma(X^p) - Q(X)^p}{Q(X)^p} \right)^{1/2}$$

where  $\sigma$  is the canonical Witt vectors Frobenius. The expansion of the square root can be computed using a Newton iteration (see [17]). We then have the

**PROPOSITION 7.** *For all positive integer  $n$  the element  $F(Y) \pmod{p^n}$  can be written as  $Y$  times a rational fraction in  $X$  such that its numerator and denominator are relatively primes, its denominator is  $Q(X)^d$  with  $d \leq pn - \frac{p-1}{2}$  and its poles order at the infinity  $(2g + 1)[p/2]$ .*

*Proof.* The only non obvious fact from the expression of the Newton iteration is the bound for  $d$ . Since we have

$$F(Y) = Y^p \left( 1 + \frac{Q^\sigma(X^p) - Q(X)^p}{Q(X)^p} \right)^{1/2},$$

we can write

$$F(Y) = Y \cdot Q(X)^{\frac{p-1}{2}} \sum_{k \geq 0} \binom{1/2}{k} \frac{p^k E(X)^k}{Q(X)^{pk}},$$

where  $E(X) = 1/p \cdot (Q^\sigma(X^p) - Q(X)^p)$  and  $E$  having integral coefficients. In particular, since the binomial coefficients are  $p$ -adic integers we have

$$F(Y) = \sum a_{i,j} \frac{X^i}{Q(X)^j}$$

with

$$v_p(a_{i,j}) \geq j/p + \frac{p-1}{2p}$$

and we are done. □

DEFINITION 11. We denote by  $F_n$  of the  $\sigma$ -linear endomorphism of  $A_K^\dagger$  lifting the Frobenius endomorphism on  $A_k$  up to absolute  $p$ -adic precision  $n$  by setting  $F_n(X) = X^p$  and  $F_n(Y)$  equal to the truncated development of the rational fraction obtained with Proposition 7.

### 5.2. Twisted local equation

In the relative situation that we consider, the Frobenius lifting decomposes as a Frobenius lift on  $B_K^\dagger$ , which sends  $t$  to  $t^p$  that we denote  $F_B$  (the 'local' Frobenius), and a Frobenius on the  $B_K^\dagger$ -module  $A_K^\dagger$  (making it an  $F$ -isocrystal). By abuse of notation, we also denote by  $F_B$  the extension by linearity of  $F_B$  to  $M_{c,\lambda}$  and  $A_K^\dagger$ . We first consider the computation of the action of  $F_B$ .

A direct way to compute the action of  $F_B$  on a element  $m_c \in M_c$  is to make the evaluation  $t \mapsto t^p$  in all the local developments at  $\lambda \in \Lambda$ , apply  $\sigma$  on the coefficients and develop the result to recover a series in  $(t - \lambda)$ .

The following remark leads to a more efficient method. Let  $m_c \in M_c$  representing an element of a basis of  $H_{MW,c}^1(U, \pi_* A_K^\dagger)$ . We recall that, by Proposition 2, a local component  $m_\lambda$  of  $m_c$  in  $\lambda \in \Lambda$  satisfies a non-homogeneous differential equation

$$\frac{\partial}{\partial t} m_\lambda - M_{\nabla,\lambda} m_\lambda = u. \tag{15}$$

From this equation, we deduce the

PROPOSITION 8. For  $\lambda \in \Lambda$ , the image of  $m_\lambda \in M_{c,\lambda}$  by the local Frobenius  $F_B(m_\lambda)$  satisfies a local differential equation

$$\begin{aligned} (t^p - \sigma(\lambda)) \frac{\partial}{\partial t} F_B(m_\lambda) - pt^{p-1} F_B((t - \lambda) M_{\nabla,\lambda}) F_B(m_\lambda) \\ = pt^{p-1} (t^p - \sigma(\lambda)) F_B(u). \end{aligned} \tag{16}$$

Proposition 8 yields a very efficient algorithm to compute the action of  $F_B(m_\lambda)$  given its first terms. Note that here the assumption that  $\lambda$  is a Teichmüller lifting is crucial.

### 5.3. Formulas for the theoretical precision

In this paragraph, we explain how to apply the isocrystal Frobenius. Here arises a technical difficulty. Since this computation consists in replacing  $Y$  by  $F(Y)$ , where

$F(Y)$  is  $Y$  times an element of  $B_K^\dagger$ , this operation comes to the computation of the action of an overconvergent function in  $B_K^\dagger$  (with infinite negative powers) on an element of  $M_c$  (with infinite positive powers). In order to perform this to a certain precision, we take advantage of the sharp control we have on the size of the coefficients of both terms. The following theorem gives expressions for sufficient absolute  $p$ -adic precision and analytic precision.

**THEOREM 2.** *Let  $m_c \in M_c$  be an element of the vector space  $H_{MW,c}^1(V, \pi A_K^\dagger)$ . Write  $m_c = (m_{\lambda_1}, \dots, m_{\lambda_{2g+1}}, \infty)$  with*

$$m_{\lambda_i} = \sum_{j=0,1} Y^j \sum_{\ell=0}^{\infty} b_{j,\ell}^{\lambda_i} (t - \lambda_i)^\ell,$$

where  $b_{j,\ell}^{\lambda_i} \in K$  and  $b_{j,0}^\infty = 0$ . Let  $\alpha$  and  $\beta$  be integers such that

$$v_p(b_{j,\ell}^\lambda) > -(\alpha \log_p \ell + \beta)$$

for all  $j, \ell$  and  $\lambda \in \Lambda$ . Then if we set

$$n = \max(2\alpha \log_p \left( \frac{\alpha}{2 \ln(p)} \right), 2(\alpha + \beta + P_2))$$

and

$$P_1 = pn - \frac{p-1}{2},$$

the image by  $F_n$  of  $m_c$  truncated at the degree  $P_1$  and modulo  $p^{P_2}$  is equal to the image of  $m_c$  by  $F$  modulo  $p^{P_2}$ .

*Proof.* If we write

$$F(Y) = \sum_{j=0,1} f_j(X) Y^j,$$

the image by  $F$  of  $m_c$  is given by the products

$$f_j(t) \cdot \sigma(b_{j,\ell}^\lambda) (F_B(t - \lambda))^i,$$

that is to say

$$f_j(t) \cdot \sigma(b_{j,\ell}^\lambda) (t^p - \sigma(\lambda))^i$$

for all  $\ell$  and  $j$ . Now for  $n$  positive, we have  $F_n(Y) = \sum_{j=0,1} \tilde{f}_{n,j}(X) Y^j$  with  $p^n$  dividing  $f_j(t) - \tilde{f}_{n,j}(t)$ , and  $\tilde{f}_{n,j}(t)$  has its degree bounded by  $pn - \frac{p-1}{2}$ .

Here we have to use the following easy lemma

**LEMMA 2.** *Let  $\lambda \in W(t)$  be a Teichmüller element. Let*

$$S = \sum_{\ell=0}^{\infty} b_\ell (t - \lambda)^\ell$$

with  $b_\ell \in K$  be such that there exist integers  $\alpha$  and  $\beta$  with

$$v_p(b_\ell) \geq -(\alpha \log_p \ell + \beta)$$

for all  $\ell \in \mathbb{N}$ . If we write

$$F(S) = \sum_{\ell=0}^{\infty} \sigma(b_\ell)(t^p - \sigma(\lambda))^\ell = \sum_{\ell=0}^{\infty} a_\ell(t - \lambda)^\ell$$

then we have for all  $\ell \in \mathbb{N}$

$$v_p(a_\ell) \geq -(\alpha \log_p \ell + \beta).$$

In order to prove Theorem 2 using the preceding lemma, we have to find  $n$  and  $P_1$  such that for all  $\ell > P_1$  we have  $v_p\left((f_j(t) - \tilde{f}_{n,\ell}(t)) \cdot \sigma(b_{j,\ell}^\lambda)\right) \geq P_2$ .

We have to solve the inequality

$$\alpha \log_p(pn - \frac{p-1}{2}) + \beta - n \leq -P_2. \quad (17)$$

If we set  $\beta' = \alpha + \beta + P_2$ , it is sufficient to solve

$$n - \alpha \log_p n - \beta' \geq 0. \quad (18)$$

Now if we have  $n/2 \geq \beta'$  and

$$n/2 - \alpha \log_p n \geq 0 \quad (19)$$

we are done. Equation (19) is true for  $n > -\frac{2\alpha}{\ln(p)} W(-1, -\frac{2}{\alpha})$  where  $W(-1, \cdot)$  is the real branch defined on the interval  $[-1/e, 0]$  of the classical Lambert function. In particular, given that

$$-W(-1, -1/t) < \ln(t)$$

for all  $t$  of the interval, the proposition is true. We refer to [7] for a detailed survey on the Lambert function.  $\square$

#### 5.4. Recovering the zeta function

From the action of the Frobenius morphism on a basis of  $H_{MW,c}^1(V, \pi_* A_K^\dagger)$ , it is easy to recover the zeta function of the curve  $\overline{C}_k$  thanks to the Lefschetz trace formula (see [12, Cor.6.4]). In our case this formula reads

$$Z(\overline{C}_k, t) = \frac{\det(1 - t\phi_c^1)}{(1-t)(1-qt)}$$

where  $\phi_c^1$  is the representation of the Frobenius morphism acting on  $H_{MW,c}^1(\overline{C}/K)$ .

By the preceding results of this section, we can compute the matrix  $M_F$  of the action of the  $p$ -power Frobenius on a basis of the space  $H_{MW,c}^1(V, \pi_* A_K^\dagger)$ .

We explain how to recover the Zeta function of our initial curve from it. We can embed the space  $H_{MW,c}^1(C_k/K)$  in  $H_{MW,c}^1(U_k/K)$  and thanks to the localization exact sequence in Monsky-Washnitzer cohomology with compact support (deriving from the one in rigid cohomology, see [34])

$$0 \rightarrow H_{MW,c}^0((C_k \setminus U_k)/K) \rightarrow H_{MW,c}^1(U_k/K) \rightarrow H_{MW,c}^1(C_k/K) \rightarrow 0$$

give a description of a supplement. Namely

$$\{(1 \otimes 1, 0, \dots, 0), \dots, (0, \dots, 1 \otimes 1, 0)\}$$

in  $\bigoplus_{\lambda \in \Lambda_0} (A_K^\dagger \otimes_{B_K^\dagger} \tilde{R}_{\lambda,c}) \oplus (A_K^\dagger \otimes_{B_K^\dagger} R_{\infty,c})$  is a basis of such a supplement (we identify here  $H_{MW,c}^1(U_k/K)$  and  $H_{MW,c}^1(V_k/K, \pi_* A_K^\dagger)$ ) that we call  $W$ . Let  $\tilde{M}_F$  denote the matrix of the action of the  $p$ -th Frobenius on a basis of a supplement of  $W$ . Let  $n$  be the absolute degree of  $k$  the base field of  $C_k$ . By computing the product

$$\tilde{M}_\Sigma = \tilde{M}_F \tilde{M}_F^\sigma \dots \tilde{M}_F^{\sigma^n},$$

we recover the matrix of the total Frobenius.

### 5.5. Description of the algorithm and complexity analysis

The computation of the Frobenius representation on  $H_{MW,c}^1(V, \pi_* A_K^\dagger)$  can be done in three steps. Here again, we suppose that  $P_1 = O(P_2)$  so that by Theorem 1, the relative and absolute  $p$ -adic precisions are the same modulo a  $\log(P_2)$  term that we neglect.

#### 5.5.1. Step 1: Lift of the Frobenius morphism

Write

$$F(Y) = YQ(X)^{(p-1)/2} \left( 1 + \frac{Q^\sigma(X^p) - Q(X)^p}{Q(X)^p} \right)^{1/2},$$

and for each  $\lambda \in \Lambda$ , compute a local analytic development up to precision  $P_1$  of the square root using a Newton iteration as in [17].

The dominant step of this operation is the Newton iteration with running time  $\tilde{O}(\log(q)P_1P_2)$ . This Newton iteration has to be repeated  $O(g)$  times for the total cost of  $\tilde{O}(g \log(q)P_1P_2)$ .

#### 5.5.2. Step 2: Computation of the representation of the Frobenius morphism

We denote by  $m_c^1, \dots, m_c^{4g+1} \in M_c$  the elements of a basis of the vector space  $H_{MW,c}^1(V, \pi_* A_K^\dagger)$  computed with analytic precision 1. For  $j = 1, \dots, 4g+1$ , we can write  $m_c^j = (m_{\lambda_1}^j, \dots, m_{\lambda_{2g+1}}^j, m_\infty^j)$ .

Next, for a fixed  $\lambda \in \Lambda$ , we do the following operations:

1. For  $j = 1, \dots, 4g+1$ , compute the action of the local Frobenius  $F_B(m_\lambda^j)$  up to the analytic precision  $P_1$  using the local differential equation given by Proposition 8.
2. In the expression of  $F_B(m_\lambda^j)$ , replace  $Y$  by  $\nabla_{GM,\lambda}(Y) = Y \sum_{\ell=-d_0}^{P_1} a_\ell t^\ell$  where  $Y \sum_{\ell=-d_0}^{P_1} a_\ell t^\ell$  is the local expression in  $\lambda$  of the lift of the relative Frobenius morphism obtained in Step 1 and develop to obtain  $m'^j_\lambda$ .

For the first operation, we have to compute the constant term  $F_B(u_j)$  of Equation (16) associated to  $m_\lambda^j$ . Keeping the notations of Section 4.1 Step 3, we have

$$F_B\left(\sum_{\lambda' \in \Lambda} \phi_\lambda(P_{r_{\lambda'}}(\phi_{\lambda'}(f_i))) \cdot g_{j,i}^{\lambda'}(0)\right) = \sum_{\lambda' \in \Lambda} \phi_\lambda(F_B(P_{r_{\lambda'}}(\phi_{\lambda'}(f_i)))) \cdot g_{j,i}^{\lambda'}(0)^\sigma.$$

For  $\lambda' \in \Lambda$ , we have to compute the action of  $F_B$  on principal parts of the form  $1/(t - \lambda')$  and develop in  $\lambda$ . This can be done by computing a local development in  $\lambda$  of  $t^p - \lambda'$  and then use a Newton iteration to inverse the result. These operations

take  $\tilde{O}(\log(q)P_1P_2)$  time and has to be repeated  $O(g)$  times with  $O(g \log(q)P_1P_2)$  memory consumption.

Using the asymptotically fast algorithm provided by Theorem 2 of [2] and Remark 3 the total amount of time for solving  $O(g)$  equations is  $\tilde{O}(g \log(q)P_1P_2)$ .

The second step just consists in  $O(g)$  products of series with analytic precision  $P_1$  which takes  $\tilde{O}(g \log(q)P_1P_2)$  time.

For  $\lambda$  running in  $\Lambda$ , all the preceding operations allows us to recover  $m_\lambda^j$  with analytic precision  $P_1$  for  $j = 1, \dots, 4g + 1$  and  $\lambda \in \Lambda$  in  $\tilde{O}(g^2 \log(q)P_1P_2)$  time and  $O(g \log(q)P_1P_2)$  memory consumption.

The next thing to do is for  $j = 1, \dots, 4g + 1$  and for  $\lambda \in \Lambda_0$ , subtract the principal part of  $m_\lambda^j$  to  $m_\infty^j$  to recover  $F_\infty(m_\infty^j)$ . In order to compute the contribution of the principal part of  $m_\lambda^j$  in  $\infty$ , we have to obtain a local development in  $\infty$  of an element of  $R_\lambda$ . By considering a Laurent series in  $\lambda$  as an analytic series in  $\lambda$  times a term of the form  $1/(t - \lambda)^{m_o}$ , we have to compute a local development in  $\infty$  of an analytic series  $S_\lambda(t)$  and on the other side of a term of form  $1/(t - \lambda)^{m_o}$  and then take the product. The local development in  $\infty$  of  $S_\lambda(t)$  with analytic precision  $P_1$  can be done by computing the evaluation  $S_\lambda(1 + \lambda t)$  which can be decomposed into the evaluation of  $S_\lambda(1 + t')$  using the shift operator for polynomials described in [1] and the substitution  $t' = \lambda t$ . This can be done in  $\tilde{O}(\log(q)P_1P_2)$  time. To compute a development  $1/(t - \lambda)^{m_o}$  in  $\infty$  we have to compute a development of  $1/(1 + \lambda t)$  and raise the result to the power  $m_o$ . As  $m_o$  is in the order of  $P_1$  this can be done in  $\tilde{O}(\log(P_1) \log(q)P_1P_2)$ .

All these operations have to be repeated  $O(g^2)$  times for a total cost of

$$\tilde{O}(g^2 \log(q)P_1P_2).$$

The following lemma shows that in order to express  $F(m_c)$  as a linear combination of the basis vectors of  $H_{MW,c}^1(V, \pi_* A_K^\dagger)$  it is enough to do it for the local component at the infinity point.

LEMMA 3. Let  $m_c = (m_{\lambda_1}, \dots, m_{\lambda_{2g+1}}, m_\infty)$  be an element of  $H_{MW,c}^1(V, \pi_* A_K^\dagger)$  such that for each  $\lambda \in \Lambda$  we have  $m_\lambda = Y.f_\lambda$  with  $f_\lambda$  a power series in  $t - \lambda$ . Write  $f_\infty = \sum_{\ell=0}^\infty b_\ell t^\ell$ . If for  $\ell = 1, \dots, 2g + 1$ ,  $b_\ell = 0$  then  $m_c = 0$ .

Proof. Let  $a_i$  be the constant term of  $f_{\lambda_i}$ . Let  $t' = t^{-1}$ . By Proposition 2, the power series  $f_\infty(t')$  satisfies an equation

$$\frac{\partial}{\partial t'} f_\infty + t' H(t') f_\infty = u(t'),$$

where  $H$  is a power series and

$$u(t') = \frac{1}{2} \sum_{\ell \geq 0} \sum_{i=1, \dots, 2g+1} a_i \lambda_i^\ell t^{\ell+1}.$$

If  $f_\infty = \sum_{\ell=0}^\infty b_\ell t^\ell$  with  $b_\ell = 0$  for  $\ell = 1, \dots, 2g + 1$ , taking care of the fact that with our convention  $b_0 = 0$ , we have

$$\sum_{i=1, \dots, 2g+1} a_i \lambda_i^\ell = 0$$

for  $\ell = 0, \dots, 2g$ . Now, since the  $\lambda_i$  are distinct the matrix

$$M = \begin{pmatrix} 1 & \lambda_1 & \dots & \lambda_1^{2g} \\ 1 & \lambda_2 & \dots & \lambda_2^{2g} \\ \dots & \dots & \dots & \dots \\ 1 & \lambda_{2g} & \dots & \lambda_{2g}^{2g} \end{pmatrix}^\vee$$

is a Vandermonde matrix and for  $i = 1, \dots, 2g+1$ ,  $a_i = 0$ . We conclude by applying Corollary 1.  $\square$

Using the preceding lemma, the decomposition of  $F(m_c)$  in terms of the basis vectors costs  $\tilde{O}(g^3 \log(q)P_2)$  using the algorithm of Gauss.

In all, the running time of Step 2 is  $\tilde{O}(g^2 \log(q)P_1P_2)$  and the memory consumption is  $O(g \log(q)P_1P_2 + g^2 \log(q)P_2)$ .

### 5.5.3. Step 3: Norm computation

Compute

$$\tilde{M}_\Sigma = \tilde{M}_F \tilde{M}_F^\sigma \dots \tilde{M}_F^{\sigma^n},$$

using the divide and conquer approach presented in [17]. This requires

- $O(\log(n))$  multiplications of  $2g \times 2g$  matrices each one of can be done in  $\tilde{O}(g^3 \log(q)P_2)$  time;
- $\tilde{O}(g^2)$  application of the Frobenius morphism at the expense of  $\tilde{O}(\log(q)P_2)$  time ([6]).

The overall time and memory consumption are given respectively by  $\tilde{O}(g^3 \log(q)P_2)$  and  $O(g^2 \log(q)P_2)$ .

**PROPOSITION 9.** *Let  $C_k$  be an hyperelliptic curve of genus  $g$  over the finite field  $k$  with cardinality  $q$ . We suppose that the ramification points of  $C_k$  are rational. Let  $\mathcal{B}$  be a basis of  $H_{MW,c}^1(C_k/K)$  with analytic precision  $P_1$  and absolute  $p$ -adic precision  $P_2$  as given by Proposition 6. Under the hypothesis that  $P_1 = O(P_2)$ , there exists an algorithm to compute the action of the Frobenius morphism on  $\mathcal{B}$  with the same precisions as above with time complexity  $\tilde{O}(g^2 \log(q)P_1P_2) + \tilde{O}(g^3 \log(q)P_2)$  and memory complexity  $O(g \log(q)P_1P_2 + g^2 \log(q)P_2)$ .*

## 6. Overall complexity analysis

In this paragraph, we gather the results of Section 4.2 and Section 5.5 in order to give time and memory complexity bounds for the computation of the number of rational points of an hyperelliptic curve defined over a finite field of characteristic  $p$  and cardinality  $q = p^n$  using our algorithm.

First, we have to assess the analytic precision  $P_1$  and absolute  $p$ -adic precision  $P_2$  of the computations. By the Riemann hypothesis for curves, we know that it is enough to compute the coefficients of the matrix  $\tilde{M}_F$  with precision  $g/2.n + (2g + 1) \log_p(2)$ .

Next, by Theorem 2, we can take  $P_1 = O(P_2)$  and we get the

**THEOREM 3.** *Let  $C_k$  be an hyperelliptic curve of genus  $g$  over the finite field  $k$ . Let  $n$  be the absolute degree of  $k$ . We suppose that the ramification points of  $C_k$  are*

rational. There exists an algorithm to compute the characteristic polynomial of the Frobenius morphism acting on  $H_{MW,c}^1(C_k/K)$  with  $\tilde{O}(g^4n^3)$  time complexity and  $O(g^3n^3)$  memory complexity.

The algorithm described in the preceding sections have been implemented in magma [5]. Our implementation is very experimental and is only aimed at showing the correctness of our algorithm.

## 7. Conclusion

In this paper we have described an algorithm to count the number of rational points of a hyperelliptic curve over a finite field of odd characteristic using Monsky-Washnitzer cohomology with compact support. The worst case complexity of our algorithm is quasi-cubic in the absolute degree of the base field. We remark that the base computation can be easily adapted for more general curves. The reason why we focus on the case of hyperelliptic curves in this paper is that for more general curves the assessment of the analytic precision necessary for the computations is more difficult. Actually, in order to treat more general curves it is necessary to obtain an explicit logarithmic bound for the elements of a basis of the cohomology. The result we used in this paper guarantees such a bound provided that the connection matrix has only simple poles and that the exponents of the local differential equations are prepared. Following [9, pp. 106] this last condition on the exponents means that they are non integral or null rational numbers which differences are zero if they are integral. In our case, the exponents are 0 and  $-1/2$ .

### 7.0.4. Acknowledgement

The authors would like to express their deep gratitude to Bernard Le Stum for the important suggestions and advices he gave during the elaboration of this paper.

## References

1. A. V. AHO, K. STEIGLITZ and J. D. ULLMAN, ‘Evaluating polynomials at fixed sets of points.’ *SIAM J. Comput.* 4 (1975) 533–539. 297, 321
2. A. BOSTAN, F. CHYZAK, F. OLLIVIER, B. SALVY, É. SCHOST and A. SEDOGLAVIC, ‘Fast computation of power series solutions of systems of differential equations.’ ‘SODA,’ (2007) pp. 1012–1021, pp. 1012–1021. 296, 297, 311, 312, 314, 321
3. ALIN BOSTAN, BRUNO SALVY and ÉRIC SCHOST, ‘Power series composition and change of basis.’ ‘ISSAC’08,’ (ed. DAVID J. JEFFREY) (ACM Press, To appear) Proceedings of ISSAC’08, Hagenberg, Austria. 297
4. G. CHATEL, ‘Comptage de points : Application des méthodes cristallines.’ Thesis of the Université de Rennes1. 308, 309
5. G. CHATEL and D. LUBICZ, ‘Magma implementation of point counting algorithm using cohomology with compact support.’, (2008). Available at <http://perso.univ-rennes1.fr/david.lubicz/programs/>. 323

6. HENRI COHEN, GERHARD FREY, ROBERTO AVANZI, CHRISTOPHE DOCHE, TANJA LANGE, KIM NGUYEN and FREDERIK VERCAUTEREN (eds), *Handbook of elliptic and hyperelliptic curve cryptography*. Discrete Mathematics and its Applications (Boca Raton) (Chapman & Hall/CRC, Boca Raton, FL, 2006). ISBN 978-1-58488-518-4; 1-58488-518-1. [313](#), [316](#), [322](#)
7. R. M. CORLESS, G. H. GONNET, D. E. G. HARE, D. J. JEFFREY and D. E. KNUTH, ‘On the Lambert  $W$  function.’ *Adv. Comput. Math.* 5 (1996) 329–359. [319](#)
8. BERNARD DWORK, *Generalized hypergeometric functions*. Oxford Mathematical Monographs (The Clarendon Press Oxford University Press, New York, 1990). ISBN 0-19-853567-8. Oxford Science Publications. [299](#)
9. BERNARD DWORK, GIOVANNI GEROTTO and FRANCIS J. SULLIVAN, *An introduction to  $G$ -functions*, vol. 133 of *Annals of Mathematics Studies* (Princeton University Press, Princeton, NJ, 1994). ISBN 0-691-03681-0. [323](#)
10. NOAM D. ELKIES, ‘Elliptic and modular curves over finite fields and related computational issues.’ ‘Computational perspectives on number theory (Chicago, IL, 1995),’ (Amer. Math. Soc., Providence, RI, 1998), vol. 7 of *AMS/IP Stud. Adv. Math.* pp. 21–76, pp. 21–76. [295](#)
11. RENÉE ELKIK, ‘Solutions d’équations à coefficients dans un anneau hensélien.’ *Ann. Sci. École Norm. Sup. (4)* 6 (1973) 553–603 (1974). [298](#)
12. JEAN-YVES ÉTESSE and BERNARD LE STUM, ‘Fonctions  $L$  associées aux  $F$ -isocristaux surconvergens. I. Interprétation cohomologique.’ *Math. Ann.* 296 (1993) 557–576. [319](#)
13. PIERRICK GAUDRY, ‘Algorithmique des courbes hyperelliptiques et applications à la cryptologie.’ Ph.D. thesis, École Polytechnique, (2000). [295](#)
14. PIERRICK GAUDRY, ‘Cardinality of a genus 2 hyperelliptic curve over  $\text{GF}(5 \cdot 10^{24} + 41)$ .’ Email at the Number Theory List, (Sep. 2002). [295](#)
15. PIERRICK GAUDRY, ‘A comparison and a combination of SST and AGM algorithms for counting points of elliptic curves in characteristic 2.’ ‘Advances in cryptology—ASIACRYPT 2002,’ (Springer, Berlin, 2002), Lecture Notes in Comput. Sci. . [296](#)
16. NICHOLAS KATZ, ‘Travaux de Dwork.’ ‘Séminaire Bourbaki, 24ème année (1971/1972), Exp. No. 409,’ (Springer, Berlin, 1973) pp. 167–200. Lecture Notes in Math., Vol. 317, pp. 167–200. Lecture Notes in Math., Vol. 317. [308](#)
17. K.S. KEDLAYA, ‘Counting points on hyperelliptic curves using Monsky Washnitzer cohomology.’ *Journal of the Ramanujan Mathematical Society* 16 (2001) 323–328. [296](#), [316](#), [320](#), [322](#)
18. ALAN G. B. LAUDER, ‘Deformation theory and the computation of zeta functions.’ *Proc. London Math. Soc. (3)* 88 (2004) 565–602. [296](#)
19. ALAN G. B. LAUDER, ‘A recursive method for computing zeta functions of varieties.’ *LMS J. Comput. Math.* 9 (2006) 222–269 (electronic). [296](#), [309](#)
20. ALAN G. B. LAUDER and DAQING WAN, ‘Computing zeta functions of Artin-Schreier curves over finite fields.’ *LMS J. Comput. Math.* 5 (2002) 34–55 (electronic). [296](#)

21. ALAN G. B. LAUDER and DAQING WAN, ‘Computing zeta functions of Artin-Schreier curves over finite fields. II.’ *J. Complexity* 20 (2004) 331–349. [296](#)
22. BERNARD LE STUM, ‘Filtration par le poids sur la cohomologie de de Rham d’une courbe projective non singulière sur un corps ultramétrique complet.’ *Rend. Sem. Mat. Univ. Padova* 93 (1995) 43–85. [301](#)
23. R. LERCIER and D. LUBICZ, ‘Counting Points on Elliptic Curves over Finite Fields of Small Characteristic in Quasi Quadratic Time.’ ‘Advances in Cryptology—EUROCRYPT ’2003,’ (ed. ELI BIHAM) (Springer-Verlag, 2003), Lecture Notes in Computer Science . [296](#)
24. REYNALD LERCIER and DAVID LUBICZ, ‘A quasi quadratic time algorithm for hyperelliptic curve point counting.’ *Ramanujan J.* 12 (2006) 399–423. [296](#)
25. JEAN-FRANÇOIS MESTRE, ‘Lettre à Gaudry et Harley.’, (2001). Available at <http://www.math.jussieu.fr/mestre>. [296](#)
26. JEAN-FRANÇOIS 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>. [296](#)
27. CHRISTOS H. PAPADIMITRIOU, *Computational complexity* (Addison-Wesley Publishing Company, Reading, MA, 1994). ISBN 0-201-53082-1. [312](#)
28. MICHAEL S. PATERSON and LARRY J. STOCKMEYER, ‘On the number of non-scalar multiplications necessary to evaluate polynomials.’ *SIAM J. Comput.* 2 (1973) 60–66. [297](#), [310](#), [313](#)
29. J. PILA, ‘Frobenius maps of abelian varieties and finding roots of unity in finite fields.’ *Math. Comp.* 55 (1990) 745–763. [295](#)
30. ALAIN M. ROBERT, *A course in p-adic analysis*, vol. 198 of *Graduate Texts in Mathematics* (Springer-Verlag, New York, 2000). ISBN 0-387-98669-3. [300](#)
31. 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 (2003) 89–101. [296](#)
32. TAKAKAZU SATOH, ‘The canonical lift of an ordinary elliptic curve over a finite field and its point counting.’ *J. Ramanujan Math. Soc.* 15 (2000) 247–270. [296](#)
33. R. SCHOOF, ‘Counting points on elliptic curves over finite fields.’ *J. Théorie des nombres de Bordeaux* 7 (1998) 483–494. [295](#)
34. NOBUO TSUZUKI, ‘On the Gysin isomorphism of rigid cohomology.’ *Hiroshima Math. J.* 29 (1999) 479–527. [298](#), [300](#), [319](#)
35. JOACHIM VON ZUR GATHEN and JÜRGEN GERHARD, *Modern computer algebra* (Cambridge University Press, Cambridge, 2003), 2nd edn. ISBN 0-521-82646-2. [313](#)

Gweltaz Chatel [gweltaz.chatel@laposte.net](mailto:gweltaz.chatel@laposte.net)

IRMAR, Université de Rennes 1, France

David Lubicz [david.lubicz@univ-rennes1.fr](mailto:david.lubicz@univ-rennes1.fr)

IRMAR, Université de Rennes 1, France