p-ADIC COHOMOLOGY AND COUNTING POINTS ON VARIETIES OVER FINITE FIELDS

MASHA VLASENKO

These notes were written to prepare a course for the Advanced School on L-functions and Modular Forms held at ICTP Trieste on September 1-5, 2014. The goal is to describe Kedlaya's algorithm for computing zeta functions of hyperelliptic curves over finite fields (see [Ked01] and [Ed03]). It involves explicit construction of a matrix of the Frobenius operator on the p-adic cohomology modulo a given power p^N. The algorithm is implemented in Sage and Magma, e.g.

```
C := HyperellipticCurve(x^5-x^2+1);
p:=11;
FrobeniusMatrix(C,p);
```

Contents

1. Point counting via cohomology

Let p be a prime number and q be a power of p. For an algebraic variety X over the finite field $\mathbb{F}_q$ we denote $N_s = \#X(\mathbb{F}_{q^s})$ for $s \geq 1$, and the zeta function of X is defined as the formal power series

$$Z(X/\mathbb{F}_q, T) \;=\; \exp\Big(\sum_{s=1}^{\infty} N_s \frac{T^s}{s}\Big) \in \mathbb{Q}[[T]]\,.$$

André Weil conjectured in late 1940's that $Z(X/\mathbb{F}_q, T)$ is always a rational function of T, and more things in the case when X is a smooth projective variety of dimension n:

$$Z(X/\mathbb{F}_q, T) \;=\; \prod_{i=0}^{2n} P_i(T)^{(-1)^{i-1}} \;=\; \frac{P_1(T)\dots P_{2n-1}(T)}{P_0(T)\dots P_{2n}(T)}\,.$$

where $P_i(T)$ are polynomials with integer coefficients and constant term 1 satisfying

- $P_i(T) = \prod_{j=1}^{\beta_i}(1-\alpha_{ij}T)$, $\alpha_{ij} \in \overline{\mathbb{Q}}$, $|\alpha_{ij}| = q^{i/2}$
- if X is a reduction modulo p of a smooth variety $\mathfrak{X}$ over a number field then $\beta_i = \dim H^i(\mathfrak{X}(\mathbb{C}); \mathbb{C})$
- $Z\big(X/\mathbb{F}_q, \frac{1}{q^n T}\big) \;=\; (-q^{n/2}T)^{\chi(X)}\, Z(X/\mathbb{F}_q, T)$ where $\chi(X) = \beta_0 - \beta_1 + \beta_2 - \dots$ is the Euler characteristic of X; in particular, for every α_{ij} we have that $q^n/\alpha_{ij} = \alpha_{2n-ij'}$ is a reciprocal root of P_{2n-i}

Weil proposed a plan for proving his conjectures based upon an as yet unknown cohomology theory. If $F : X \to X$ is the q-power Frobenius map, then $X(\mathbb{F}_{q^s})$ is precisely the set of fixed points of $F^s : X(\overline{\mathbb{F}_q}) \to X(\overline{\mathbb{F}_q})$. Since late 1930's the following "trace formula" was known due to Solomon Lefschetz: for a continuous mapping of a compact topological space to itself the number of fixed points (if finite, and counted with proper multiplicities) is equal to the alternate sum of the traces of the induced map on

Date: September 18, 2014.

the rational cohomology groups of the space. The cohomology theory conceived by Weil would associate to a variety $X/\mathbb{F}_q$ vector spaces $H^i(X;K)$ of finite dimension over some K, a field of characteristic 0, with an induced action of Frobenius F_* on them, such that

$$N_s \;=\; \sum_{i=0}^{2n} (-1)^i \operatorname{tr}\Big(\big(q^n F_*^{-1}\big)^s \;\Big|\; H^i(X;K)\Big)\,, \tag{1.1}$$

where $n = \dim X$. This would immediately imply the rationality, along with the formula

$$Z(X/\mathbb{F}_q, T) \;=\; \prod_i \det\Big(1 \,-\, q^n F_*^{-1} T \;\Big|\; H^i(X;K)\Big)^{(-1)^i}\,. \tag{1.2}$$

The rationality part of Weil's conjectures was first proved by Bernard Dwork around 1960. Surprisingly, his proof didn't rely on any cohomology theory. Dwork proved instead that the zeta function is meromorphic as a p-adic function, and then deduced that it must be rational by means of p-adic analysis. We will come back to Dwork's proof in a moment.

First cohomology theory of the kind described by Weil was the étale cohomology, constructed in early 1960's by Alexander Grothendieck and Michael Artin. Given any prime $l \neq p$, one has the l-adic étale cohomology groups $H^i(X;\mathbb{Q}_l)$. Every l works equally well, they are finite dimensional $\mathbb{Q}_l$-vector spaces whose dimension is independent of l. In late 1970's Pierre Deligne proved the remaining part of the Weil conjectures (local Riemann hypothesis) with the help of l-adic cohomology.

In his proof of rationality, Dwork also interpreted the number of points as a trace of a linear operator on a vector space over $\mathbb{Q}_p$, but his space was of infinite dimension. Inspired by Dwork's ideas, Monsky and Washnitzer constructed in late 1960s a functor which associates with each smooth affine variety X over $\mathbb{F}_q$ vector spaces $H^i(X;K)$ where $K = \mathbb{Q}_q$ is the unramified extension of degree $\log_p(q)$ of the field of p-adic numbers (see [vdP84] for a simplified and refined account of their work). However, no one could prove those spaces were finite dimensional. Monsky was able to make sense of both (1.1) and (1.2) using the concept of *nuclear operators*. Eventually, the construction of p-adic cohomology was accomplished in both directions: it was defined for more general varieties and schemes (rigid cohomology) and the groups were proved to be of finite dimension. The finiteness theorems were proved in various versions and generalizations by Berthelot ("Finitude et pureté cohomologique rigide en cohomologie rigide", 1997), Grosse-Klönne ("Finiteness of de Rham cohomology in in rigid analysis", 2002), Kedlaya ("Finiteness of rigid cohomology with coefficients",2003), Mebkhout ("Analogue p-adique du Théorème de Turrittin et le Théorème de la monodromie p-adique",2002) and Tsuzuki ("Cohomological descent of rigid cohomology for proper coverings", 2003).

In contrast to étale cohomology, the p-adic construction appears to be very useful if one wants to actually compute zeta functions. It was Kedlaya's paper [Ked01] that introduced p-adic cohomology in the computational world by giving a general algorithm for hyperelliptic curves.

2. Algebraic de Rham cohomology

2.1. **Smooth affine varieties.** Let K be a field of characteristic zero, and let R be a finitely generated, reduced (i.e., it has no non-zero nilpotent elements) K-algebra and $X = \mathrm{Spec}R$ be the corresponding affine variety over K.

The *module of Kähler differentials* $\Omega_{R/K}$ is the R-module generated by symbols dr for $r \in R$, modulo the relations dr for $r \in K$ and $d(ab) - a\,db - b\,da$ for $a, b \in R$. The module $\Omega_{R/K}$ is finitely generated over R, and the map $d : R \to \Omega_{R/K}$ is a derivation. It has the universal property that for any K-linear derivation $D : R \to M$ to an R-module M, there is a unique R-linear map $\psi : \Omega_{R/K} \to M$ such that $D = \psi \circ d$.

Assume that X is smooth and $\dim(X) = n$. In this case $\Omega_{R/K}$ is a projective R-module of rank n. Let

$$\Omega^i_{R/K} \;=\; \Lambda^i_R\, \Omega_{R/K}$$

be the i-th alternating power of $\Omega_{R/K}$ over R. The map d induces maps $d : \Omega^i_{R/K} \to \Omega^{i+1}_{R/K}$, and the composition $d \circ d$ is zero. We thus have a complex

$$R \xrightarrow{d} \Omega_{R/K} \xrightarrow{d} \Omega^2_{R/K} \xrightarrow{d} \ldots \xrightarrow{d} \Omega^n_{R/K}\,,$$

called the *de Rham complex of* X.

The elements of $\Omega^i_{R/K}$ are referred to as *i-forms*. An i-form is *closed* if it is in the kernel of $d : \Omega^i_{R/K} \to \Omega^{i+1}_{R/K}$, and exact if it is in the image of $d : \Omega^{i-1}_{R/K} \to \Omega^i_{R/K}$. The quotient of the space of closed i-forms

by the space of exact i-forms is called the *(algebraic) de Rham cohomology* of X, denoted $H^i_{dR}(X)$. Note that for $i > n$, $\Omega^i_{R/K} = 0$ and so $H^i_{dR}(X) = 0$.

Example 2.1.1. *(affine spaces)* $X = \mathbb{A}^n$, $R = K[x_1, \ldots, x_n]$, $H^0_{dR}(\mathbb{A}^n) = K$, $H^i_{dR}(\mathbb{A}^n) = 0$ *for* $i > 0$.

Example 2.1.2. *(punctured affine line) Let* $Q(x) \in K[x]$ *be a monic polynomial with distinct roots,* $\deg Q = d$. *Consider*

$$X = \mathbb{A}^1 \setminus \text{ roots of } Q\,.$$

Here $R = K[x, y]/(yQ(x) - 1)$. Since

$$\begin{aligned} Q(x)dy + yQ'(x)dx &= 0\,, \\ dy &= -y^2Q'(x)dx\,, \end{aligned}$$

we see that $\Omega_{R/K} = Rdx$, the free R-module of rank 1 generated by dx. Every element of R can be uniquely written as $y^nP(x)$ with $n \geq 0$ and $Q \nmid P$, and we have

$$\begin{aligned} d(y^nP) &= (y^nP' - ny^{n+1}PQ')dx \\ &= y^{n+1}(QP' - nPQ')dx \end{aligned}$$

It is clear that $H^0_{dR}(X) = K$. In $H^1_{dR}(X)$ we interpret the above formula for $n > 1$ as

$$y^nPQ'dx \sim \frac{1}{n-1}P'y^{n-1}dx$$

($\sim$ means being homologous, that is differing by an exact differential). Since Q has no double roots, $Q(x)$ and $Q'(x)$ are coprime and there exist polynomials $A(x), B(x) \in K[x]$ such that $AQ + BQ' = 1$. The following reduction process

$$\begin{aligned} y^nSdx &= y^n(AQ + BQ')Sdx = y^{n-1}ASdx + y^nBSQ'dx \\ &\sim y^{n-1}ASdx + y^nBSQ'dx \sim y^{n-1}\big(AS + \frac{1}{n-1}(BS)'\big)dx \end{aligned}$$

will then bring any 1-form to the shape $(S(x) + T(x)y)dx$. Moreover, one can clearly assume that $\deg T < d$ and $S = 0$, since $S(x)dx$ is always exact. We are left with the forms $T(x)y\,dx$, $\deg T < d$. One can easily see that such a from is exact if and only if $T = 0$, hence

$$y\,dx, xy\,dx, \ldots, x^{d-1}y\,dx$$

form a basis of $H^1_{dR}(X) = K^d$.

Example 2.1.3. *(affine hyperelliptic curve)*

$$\begin{aligned} Q(x) &= x^d + \ldots \quad \in K[x] \\ &\quad \textit{monic, of degree } d\textit{, without double roots} \\ R &= K[x, y] \,/\, (y^2 - Q(x)) \\ C &= \operatorname{Spec} R \end{aligned}$$

Let us first show that the module of Kähler differentials $\Omega_{R/K}$ is a free R-module of rank 1. As R is generated over K by x and y, we have that $\Omega_{R/K}$ is generated over R by dx and dy subject to the relation $0 = d\Big(y^2 - Q(x)\Big) = 2\,y\,dy - Q'(x)\,dx$, that is

$$\Omega_{R/K} = R\,dx + R\,dy \,/\, (2ydy - Q'(x)dx)\,.$$

Since Q has no double roots, $Q(x)$ and $Q'(x)$ are coprime and there exist polynomials $A(x), B(x) \in K[x]$ such that $AQ + BQ' = 1$. Consider

$$\omega = A\,y\,dx + 2B\,dy$$

so that

$$\begin{aligned} dx &= (AQ + BQ')dx = Ay^2dx + 2Bydy = y\,\omega\,, \\ dy &= (AQ + BQ')dy = Ay^2dy + BQ'dy \\ &= \frac{1}{2}AyQ'dx + BQ'dy = \frac{1}{2}Q'\omega\,. \end{aligned}$$

We see that $\Omega_{R/K} = R\,\omega$. Hence de Rham complex is given by

$$d : R \to \Omega_{R/K}$$

and $H^i_{dR}(C) = 0$ when $i > 1$. To compute $H^0_{dR}(C) = \mathrm{Ker}(d)$ and $H^1_{dR}(C) = \mathrm{Coker}(d)$, we observe that

$$R = K[x] \oplus K[x]y\,,$$

and the differential is given by

$$\begin{aligned} d\Big(P(x)+S(x)y\Big) &= P'(x)dx + S'(x)ydx + S(x)dy \\ &= \Big(P'(x)y + S'(x)y^2 + \frac{1}{2}Q'(x)S(x)\Big)\omega \\ &= \Big(\big(S'Q + \frac{1}{2}Q'S\big) + P'y\Big)\omega\,. \end{aligned}$$

Therefore $P(x)+S(x)y \in \mathrm{Ker}(d)$ if and only if

$$\begin{aligned} P' = 0 \quad &\Leftrightarrow \quad P = const\,, \\ S'Q + \frac{1}{2}Q'S = 0 \quad &\Leftrightarrow \quad S = 0\,. \end{aligned}$$

(The latter is true because if $S = ax^k + \ldots$ then the leading term of $S'Q + \frac{1}{2}Q'S$ is given by $a(k+\frac{d}{2})x^{k+d-1}$.) It follows that

$$H^0_{dR}(C) = K\,.$$

Since P' can be any polynomial in $K[x]$ and we have just seen that $S'Q + \frac{1}{2}Q'S$ can have leading term of any degree $\geq d-1$, it follows that

$$\omega, x\omega, \ldots, x^{d-2}\omega\,.$$

form a basis of $H^1_{dR}(C) = K^{d-1}$.

Example 2.1.4. *(affine hyperelliptic curve without points where $y = 0$)*

$$\begin{aligned} Q(x) &= x^d + \ldots \quad \in K[x] \\ &\qquad \textit{monic, of } \textbf{odd} \textit{ degree } d\textit{, without double roots} \\ R &= K[x,y,z] \,/\, (y^2 - Q(x), yz - 1) \\ C' &= \mathrm{Spec}\, R \end{aligned}$$

(The answer is different when d is even. Please find out the difference as an **exercise**.) We write $R = K[x,y,y^{-1}] \,/\, (y^2 - Q(x))$. Clearly, $\Omega_{R/K}$ is again a free R-module of rank 1. This time we can use as a generator simply dx, and $dy = \frac{1}{2}Q'(x)y^{-1}dx$. Every element of R can be represented in the form $(P(x)+S(x)y)y^{-2k}$ for some non-negative k, and the differential is then given by

$$\begin{aligned} d\Big(\frac{P(x)+S(x)y}{y^{2k}}\Big) &= \frac{P'(x)}{y^{2k}}dx + (-2k)\frac{P(x)}{y^{2k+1}}\frac{Q'(x)}{2y}dx \\ &+ \frac{S'(x)}{y^{2k-1}}dx + (1-2k)\frac{S(x)}{y^{2k}}\frac{Q'(x)}{2y}dx \\ &= \Big(\frac{P'Q - kPQ'}{y^{2k+2}} + \frac{S'Q + \big(\frac{1}{2}-k\big)SQ'}{y^{2k+1}}\Big)\,dx \end{aligned}$$

It will be useful to observe that there is an involution acting on R which sends $x \mapsto x$, $y \mapsto -y$. R can be thus decomposed into '+' and '-' eigenspaces of this involution $R = R^+ \oplus R^-$, elements of R^+ being of the form $P(x)y^{-2k}$ and elements of R^- being $S(x)y^{1-2k}$. This involution commutes with the differential and leads to the decomposition of the de Rham complex and the de Rham cohomology groups $H^i_{dR}(C') = H^i_{dR}(C')^+ \oplus H^i_{dR}(C')^-$ for $i = 0, 1$. The $+$-groups we compute from

$$\begin{aligned} d :& R^+ \to R^+\,dx \\ & P(x)y^{-2k} \mapsto (P'Q - kPQ')y^{-2k-2}\,dx \end{aligned}$$

$P(x)y^{-2k}$ belongs to $H^0_{dR}(C')^+$ precisely when $P'Q = kPQ'$. If $k = 0$ then $P' = 0$, so $P = const$. If $k > 0$, since Q and Q' are coprime, it follows that P is divisible by Q, so we can represent our element with a smaller k. Therefore $H^0_{dR}(C')^+ = K$. To compute $H^1_{dR}(C')^+$ we interpret the above formula for the differential as the forms

$$\frac{P'}{y^{2k}}dx \sim k\frac{PQ'}{y^{2k+2}}dx$$

being cohomologous (i.e., they differ by an exact form). If $k > 1$ we have

$$\frac{P(x)}{y^{2k}}dx = \frac{P(AQ+BQ')}{y^{2k}}dx \sim \frac{PA}{y^{2k-2}}dx + \frac{1}{k-1}\frac{(PB)'}{y^{2k-2}}dx\,,$$

so every form can be reduced to something of the form $E(x)y^{-2}dx$. Further, subtracting multiples of $Q(x)y^{-2}dx$ (those are exact forms), we can assume that $\deg E < \deg Q = d$. Let us check that the form $E(x)y^{-2}dx$ with $\deg E < d$ is exact if and only if $E = 0$. Suppose for some P and non-negative k we have

$$\frac{P'Q - kPQ'}{y^{2k+2}} \;=\; \frac{E}{y^2}\,.$$

If $k = 0$, this is possible only when $P' = 0$, and so $P = const$ and $E = 0$ in this case. If $k > 0$, it follows that

$$P'Q - kPQ' \;=\; EQ^{2k}$$

and therefore P is divisible by Q, which means one can make k smaller. This proves that the forms

$$\frac{dx}{y^2}\,, x\frac{dx}{y^2}\,, \ldots\,, x^{d-1}\frac{dx}{y^2}$$

form a basis of $H^1_{dR}(C')^+ = K^d$.

To compute the $-$-cohomology groups, we work with

$$d : R^- \to R^-\,dx$$

$$S(x)y^{1-2k} \mapsto \big(S'Q + (\frac{1}{2} - k)SQ'\big)y^{-1-2k}\,dx$$

The expression $S'Q + (\frac{1}{2} - k)SQ'$ can vanish only when $S = 0$ (because $d = \deg Q$ is odd, we used this argument earlier), hence $H^0_{dR}(C')^- = 0$. In $H^1_{dR}(C')^-$ we have

$$\frac{S'}{y^{2k-1}}dx \;\sim\; (k - \frac{1}{2})\frac{SQ'}{y^{2k+1}}dx\,,$$

so the same way as above we can reduce any form to $E(x)y^{-1}dx$. Further, using the above formula with $k = 0$, the expression $S'Q + \frac{1}{2}SQ'$ can have its leading term of any power $\geq d - 1$, hence we can reduce to the case $\deg E < d - 1$. Let us show that $E(x)y^{-1}dx$ with $\deg E < d - 1$ is exact if and only if $E = 0$. Suppose for some S and non-negative k we have

$$\frac{S'Q + (\frac{1}{2} - k)SQ'}{y^{1+2k}} \;=\; \frac{E}{y}\,.$$

If $k > 0$, it follows that Q divides S and we can decrease k. If $k = 0$ comparing degrees we see that we can only have $S = 0$ and $E = 0$. Therefore we proved that

$$\frac{dx}{y}\,, x\frac{dx}{y}\,, \ldots\,, x^{d-2}\frac{dx}{y}$$

form a basis of $H^1_{dR}(C')^- = K^{d-1}$.

2.2. **Cohomology of projective varieties, excision and comparison with topological cohomology.** Here is Grothendieck's definition of the algebraic de Rham cohomology of a smooth (not necessarily affine) variety X. For a variety X over K one constructs a sheaf $\Omega_{X/K}$ of Kähler differentials, which is coherent. If X is smooth of dimension n then $\Omega_{X/K}$ is locally free of rank n. The exterior derivative is now a map of sheaves $d : \mathcal{O}_X \to \Omega_{X/K}$ and we construct the de Rham complex of X

$$0 \to \mathcal{O}_X \stackrel{d}{\to} \Omega_{X/K} \stackrel{d}{\to} \Omega^2_{X/K} \stackrel{d}{\to} \ldots \stackrel{d}{\to} \Omega^n_{X/K} \to 0.$$

The algebraic de Rham cohomology $H^i_{dR}(X)$ is defined as hypercohomology $\mathbb{H}^i(\Omega^{\cdot}_{X/K})$.

We will not use the above definition in actual computations, so the reader unfamiliar with sheaf cohomology might simply skip it. We will list several properties which will be important for us.

- Unlike in the affine case, we no longer automatically have $H^i_{dR}(X) = 0$ whenever $i > \dim(X)$. (This happens because we use hypercohomology to define algebraic de Rham cohomology.) We will see some examples soon.
- Let X be smooth and $K = \mathbb{C}$. The set of complex points of X is a complex analytic variety denoted by X^{an}, the *analytification* of X, and there is a functorial isomorphism

$$H^i_{dR}(X) \widetilde{\to} H^i_{Betti}(X^{an}, \mathbb{C})\,.$$

- There is an excision exact sequence in de Rham cohomology. If X is a smooth K-variety, Z is a smooth subvariety of pure codimension m, and $U = X \setminus Z$, then

$$\ldots \to H^{i-2m}_{dR}(Z) \to H^i_{dR}(X) \to H^i_{dR}(U) \to H^{i-2m+1}_{dR}(Z) \to \ldots$$

Topological comparison allows one compute dimensions of cohomology groups in certain situations, while excision allows to reduce computation of de Rham cohomology to affine pieces.

Example 2.2.1. *We know that $H^0_{dR}(\mathbb{A}^n) = K$ and $H^i_{dR}(\mathbb{A}^n) = 0$ when $i > 0$. Using excision and induction on n one can show that*

$$H^i_{dR}(\mathbb{P}^n) \;=\; \begin{cases} K & 0 \le i \le 2n, i \text{ even} \\ 0, & \text{otherwise} \end{cases}$$

(Check that this agrees with topological picture when $K = \mathbb{C}$.)

Example 2.2.2. *Compute $H^i_{dR}(\mathbb{A}^1 \setminus \{Q(x) = 0\})$ (see Example 2.1.2) using excision. Do the same using topological comparison.*

Example 2.2.3. *Let's see how the above properties work in the relation to hyperelliptic curves. Assume $K = \mathbb{C}$. An affine hyperelliptic curve*

$$C \;=\; \{y^2 = Q(x)\}\,, \quad \deg Q = d\,, \quad \operatorname{res}(Q, Q') \neq 0$$

can be completed to a smooth projective curve $\overline{C}$ (here we don't explain why this is always the case). Since we have a degree 2 map from $\overline{C}$ to $\mathbb{P}^1$ (given by x on C)

$$\begin{array}{ccc} C & \hookrightarrow & \overline{C} \\ x\downarrow & & \downarrow \\ \mathbb{A}^1 & \hookrightarrow & \mathbb{P}^1 \end{array}$$

$\overline{C} \setminus C$ will consists of one or two points. Let's find out how many.

Let us denote $Z \;=\; \overline{C} \setminus C$ and $\varepsilon = \#Z$, which is 1 or 2. As $\overline{C}$ is a Riemann surface, we denote its genus by g. We triangulate $\mathbb{P}^1(\mathbb{C})$ using the roots of $Q(x) = 0$ and ∞ as vertices ($d + 1$ points, which are lifted to $d + \varepsilon$ points on $\overline{C}$), some d 1-cells joining them (they lift to $2d$ 1-cells) and one 2-cell (lifts to two). For the Euler characteristic of $\overline{C}$ we then have

$$\chi(\overline{C}) \;=\; d + \varepsilon \;-\; 2d \;+\; 2 \;=\; 2 - 2g$$

Therefore we have $2g = d - \varepsilon$ and $\varepsilon \;=\; 1$ or 2 when d is odd or even respectively.

Next, let's show that $H^1_{dR}(C) \cong H^1_{dR}(\overline{C})$ when d is odd. (Our computation in Example 2.1.3 suggests this, but we want to obtain this result using properties of cohomology rather than direct computation.) Excision gives

$$0 \to H^0(\overline{C}) \to H^0(C) \to 0 \to H^1(\overline{C}) \to H^1(C) \to H^0(Z) \to H^2(\overline{C}) \to 0$$

We know dimensions of $H^i(\overline{C})$ from topological comparison (Betti numbers of a Riemann surface of genus g are $1, 2g, 1$), and Z has only H^0 of dimension $\#Z = \varepsilon$. We know that $H^i(C) = 0$ for $i > 1$, because C is affine. It follows immediately that $H^0(C) \cong H^0(\overline{C})$, and $H^1(C) \cong H^1(\overline{C})$ when d is odd.

Example 2.2.4. *Show that $H^1_{dR}(C')^- \cong H^1_{dR}(\overline{C})$ when d is odd, where C' is the hyperelliptic curve without the divisor of y (see Example 2.1.4)*

Let $Z' = \overline{C} \setminus C'$. The excision sequence looks like in the previous example, we consider the part

$$0 \to H^1(\overline{C}) \to H^1(C') \to H^0(Z') \to H^2(\overline{C}) \to 0\,,$$

and split it under the hyperelliptic involution

$$\begin{aligned} 0 \to H^1(\overline{C})^+ \to H^1(C')^+ \to H^0(Z')^+ \to H^2(\overline{C})^+ \to 0 \\ 0 \to H^1(\overline{C})^- \to H^1(C')^- \to \quad 0 \quad \to H^2(\overline{C})^- \to 0 \end{aligned}$$

observing that $H^0(Z')^- = 0$ because Z' is invariant under the involution. Here we will cheat a bit by using our previous computations: we observe that $H^1_{dR}(C)$ has only differentials odd with respect to hyperelliptic involution in its basis, meaning that $H^1_{dR}(C)^+ = 0$ and $H^1_{dR}(C) = H^1_{dR}(C)^-$. The same is true for $H^1_{dR}(\overline{C})$ by the isomorphism from the previous example. Therefore $H^1_{dR}(\overline{C})^+ = 0$ and $H^1_{dR}(\overline{C}) = H^1_{dR}(\overline{C})^- \cong H^1_{dR}(C')^-$.

In this section we established that $H^1_{dR}(\overline{C}) \cong H^1_{dR}(C) \cong H^1_{dR}(C')^-$, and according to our computations in the previous section, a basis in those cohomology spaces is given by the forms

$$\frac{dx}{y}\,, x\frac{dx}{y}\,, \ldots\,, x^{d-2}\frac{dx}{y}\,.$$

3. Monsky-Washnitzer cohomology

3.1. **Definition.** Let X be a smooth affine variety over $k = \mathbb{F}_q$ with coordinate ring $\overline{R}$. The Monsky-Washnitzer cohomology of X is the de Rham cohomology of a certain lift of $\overline{R}$ to characteristic 0 on which the Frobenius action is also defined. Below we sketch a construction of such a lift following [vdP84, Section 2].

Let V be a complete discrete valuation ring with $V/\pi V = k$, where π is a uniformizer in V (a generator of the the maximal ideal). We denote by K the field of fractions of V. Note that $\mathrm{char} K = 0$. For example, one could take $V = \mathbb{Z}_q = W(\mathbb{F}_q)$. In this case $K = \mathbb{Q}_q$ is the unique unramified extension of $\mathbb{Q}_p$ of degree $\log_p q$. The lift of Frobenius to K is denoted by σ. We have $\sigma(x) \equiv x^p \mod \pi$.

According to a result of R. Elkik ("Solutions d'équations á coefficients dans un anneau henselienne", 1973) there exist an V-algebra R^0, finitely generated and smooth over V such that $R^0/\pi R^0 \equiv \overline{R}$. Write

$$R^0 \;=\; V[t_1, \ldots, t_r]/(f_1, \ldots, f_m)\,.$$

Consider the rings

$$V\langle t_1, \ldots, t_r\rangle \;=\; \Big\{\sum_\alpha a_\alpha t^\alpha \mid a_\alpha \in V,\, \lim_{|\alpha|\to\infty} a_\alpha = 0\Big\}$$

and

$$V\langle t_1, \ldots, t_r\rangle^\dagger \;=\; \Big\{\sum_\alpha a_\alpha t^\alpha \mid a_\alpha \in V\,,\quad \liminf_{|\alpha|\to\infty} \frac{\mathrm{ord}_p a_\alpha}{|\alpha|} > 0\Big\}\,.$$

Exercise 3.1.1. *Prove that the following definitions of the "dagger ring" are equivalent to the one above:*

(i) $\Big\{\sum_\alpha a_\alpha t^\alpha \mid a_\alpha \in V\,, |a_\alpha| < c\rho^{|\alpha|}$ *for some* $c > 0$ *and* $0 < \rho < 1\Big\}$;

(ii) $\Big\{\sum_{m=0}^\infty p^m A_m(t_1, \ldots, t_r) \mid A_m \in V[t_1, \ldots, t_r]\,,\ \deg A_m < C(m+1)$ *for some* $C > 0\Big\}$.

The elements of $V\langle t_1, \ldots, t_r\rangle^\dagger$ are called *overconvergent power series*. Every element converges in a polydisc $\{(t_1, \ldots, t_r) \in K^n |\ |t_1| \le \rho_1, \ldots, |t_r| \le \rho_r\}$ with all $\rho_i > 1$.

For any ring A over V we write $\widehat{A} = \varprojlim A/\pi^n A$ for its π-adic completion. Clearly, $V\langle t_1, \ldots, t_r\rangle$ is the π-adic completion of both $V[t_1, \ldots, t_r]$ and $V\langle t_1, \ldots, t_r\rangle^\dagger$. We define $||\sum_\alpha a_\alpha t^\alpha|| = \sup_\alpha |a_\alpha|$, which makes sense in all three rings.

Proposition 3.1.2. (i) *The ring* $V\langle t_1, \ldots, t_r\rangle^\dagger$ *is Noetherian.*

(ii) $V[t_1, \ldots, t_r] \to V\langle t_1, \ldots, t_r\rangle^\dagger$ *is flat.*

A weakly complete finitely generated (w.c.f.g.) algebra over V is a homomorphic image of some $V\langle t_1, \ldots, t_r\rangle^\dagger$. For a w.c.f.g. algebra

$$R \;=\; V\langle t_1, \ldots, t_r\rangle^\dagger/(f_1, \ldots, f_m)$$

one defines a module of differentials

$$D^1(R) \;=\; R\,dt_1 + \ldots + R\,dt_r/ \text{ the submodule generated by } \frac{\partial f_i}{\partial t_1}dt_1 + \ldots + \frac{\partial f_i}{\partial t_r}dt_r\,, i = 1, \ldots, m$$

This is the universal finite module of continuous differentials of R/V. It doesn't depend on the chosen representation of R.

Proposition 3.1.3. (i) $R/\pi R \equiv \overline{R}$

(ii) $D^1(R) \otimes \overline{R} \equiv \Omega^1_{\overline{R}/k}$

(iii) $D^1(R)$ *is a projective module of rank* $n = \dim \overline{R}$

The de Rham complex of R is defined as

$$D^0(R) \xrightarrow{d} D^1(R) \xrightarrow{d} D^2(R) \xrightarrow{d} \ldots \xrightarrow{d} D^n(R)\,,$$

where $D^i(R) = \Lambda^i D^1(R)$ and d is the exterior differentiation. The ith cohomology group of the complex $D(R)$ is denoted by $H^i(X; V)$ or $H^i(\overline{R}/V)$. Further $H^i_{MW}(X; K) := H^i(X; V) \otimes_V K$ is the definition of the *Monsky-Washnitzer cohomology.*

Exercise 3.1.4. *(Monsky-Washnitzer cohomology of the affine line) Consider cohomology of the following complexes:*

$$\mathbb{Z}_p[x] \overset{d}{\mapsto} \mathbb{Z}_p[x]\,dx$$
$$\mathbb{Z}_p[[x]] \overset{d}{\mapsto} \mathbb{Z}_p[[x]]\,dx$$
$$\mathbb{Z}_p\langle x\rangle \overset{d}{\mapsto} \mathbb{Z}_p\langle x\rangle\,dx$$
$$\mathbb{Z}_p\langle x\rangle^\dagger \overset{d}{\mapsto} \mathbb{Z}_p\langle x\rangle^\dagger\,dx$$

Notice that $H^0 \cong \mathbb{Z}_p$ in all cases. Show that H^1 is torsion in the first and last cases and non-torsion in the middle two. In particular, we see that $H^1_{MW}(\mathbb{A}^1;\mathbb{Q}_p) = 0$.

For a smooth and finitely generated k-algebra, a w.c.f.g. algebra A is called *a lift* of $\overline{A}$ if A is flat over V and $A/\pi A \equiv \overline{A}$. The following theorem (from [vdP84]) shows that Frobenius can be lifted to the de Rham complex and that its action on Monsky-Washnitzer cohomology is independent of the choices that one makes in this construction.

Proposition 3.1.5. *There exists a lift A of $\overline{A}$. Moreover:*

(i) *Every lift of $\overline{A}$ is isomorphic to A.*
(ii) *Let $\overline{C}/k$ be smooth and finitely generated, let C be a lift of $\overline{C}$ and let $f : \overline{A} \to \overline{C}$ be a morphism of k-algebras. There exists a V-homomorphism $F : A \to C$ lifting f.*
(iii) *Let B be a w.c.f.g. algebra and $F_0, F_1 : A \to B$ two homomorphisms with $F_0 = F_1 \mod \pi$. The induced mappings*
$$(F_0)_*, (F_1)_* \ : \ D(A) \otimes_V K \to D(B) \otimes_V K$$
are homotopic.

Exercise 3.1.6. *Let $Q \in \mathbb{Z}_p[x]$ be a monic polynomial of degree d without double roots modulo p. We would like to compute Monsky-Washnitzer cohomology of the punctured affine line, as in Example 2.1.2. Consider $R = \mathbb{Z}_p\langle x, y\rangle^\dagger/(yQ(x) - 1)$. Show that R is isomorphic to the ring of Laurent series*

$$\sum_{n\in\mathbb{Z}} P_n(x)y^n$$

where $P_n \in \mathbb{Z}_p[x]$ are polynomials of degree at most $d-1$ such that

$$\liminf_{n\to+\infty} \frac{\nu_p(P_n)}{n} > 0 \qquad \text{and} \qquad \liminf_{n\to+\infty} \frac{\nu_p(P_{-n})}{n} > 0\,.$$

3.2. **Kedlaya's estimates for p-powers in the reduction process on hyperelliptic curves.** Let $\overline{Q}(x) \in \mathbb{F}_q[x]$ be a polynomial of odd degree $d = 2g+1$ over $\mathbb{F}_q$ without repeated roots, so that the normalization of the projective closure of the affine curve $y^2 = \overline{Q}(x)$ is a smooth hyperelliptic curve of genus g. Let C' be the affine curve obtained by deleting the support of the divisor of y (that is, the point at infinity and the Weierstrass points). Let $Q(x) \in \mathbb{Z}_q[x]$ be an arbitrary monic lift of $\overline{Q}(x)$. Consider

$$R^0 \ = \ \mathbb{Z}_q[x, y, y^{-1}]/(y^2 - Q(x))$$

and its *weak completion*

$$R \ = \ \mathbb{Z}_q\langle x, y, y^{-1}\rangle^\dagger/(y^2 - Q(x))\,.$$

The elements of R can be viewed as series

$$\sum_{n\in\mathbb{Z}} (P_n(x) + S_n(x)y)y^{2n}$$

where $P_n, S_n \in \mathbb{Z}_q[x]$ are polynomials of degree at most $d-1$ such that

$$\liminf_{n\to+\infty} \frac{\nu_p(P_n)}{n}\,,\ \liminf_{n\to+\infty} \frac{\nu_p(P_{-n})}{n}\,,\ \liminf_{n\to+\infty} \frac{\nu_p(S_n)}{n}\,,\ \liminf_{n\to+\infty} \frac{\nu_p(S_{-n})}{n}$$

are all positive. (**Exercise:** check that.)

Now we lift the p-power Frobenius map to $\Psi : R \to R$. Let $\sigma : \mathbb{Z}_q \to \mathbb{Z}_q$ be the canonical Frobenius, and $\Psi(x) = x^p$. Consider the polynomial

$$E(x) \ = \ \frac{Q^\sigma(x^p) - Q(x)^p}{p} \in \mathbb{Z}_q[x]$$

and define

$$\Psi(y) \;=\; y^p\Big(1+\frac{pE(x)}{y^{2p}}\Big)^{1/2} \;=\; y^p\sum_{k\ge 0}\binom{1/2}{k}p^kE(x)^ky^{-2pk}\,,$$

$$\Psi(y^{-1}) \;=\; y^{-p}\Big(1+\frac{pE(x)}{y^{2p}}\Big)^{-1/2} \;=\; y^{-p}\sum_{k\ge 0}\binom{-1/2}{k}p^kE(x)^ky^{-2pk}\,.$$

One can prove that $\binom{\pm 1/2}{k}\in\mathbb{Z}_p$ (we assume $p\neq 2$). **Exercise:** Check that the above series are overconvergent.

Further, we compute the matrix of Frobenius on $H^1(C';\mathbb{Q}_p)^-$ in the basis

$$\frac{dx}{y}\,,x\frac{dx}{y}\,,\dots\,,x^{d-2}\frac{dx}{y}$$

from Example 2.1.4.

$$\begin{aligned}\Psi\big(x^i\frac{dx}{y}\big) \;&=\; \Big(px^{p(i+1)-1}y^{1-p}\sum_{k\ge 0}\binom{-1/2}{k}p^kE(x)^ky^{-2pk}\Big)\frac{dx}{y}\\ &=\; \Big(y^{1-p}\sum_{k\ge 0}\binom{-1/2}{k}p^{k+1}E(x)^kx^{p(i+1)-1}y^{1-p(1+2k)}\Big)\frac{dx}{y}\end{aligned}$$

The degree of E is at most $pd-1$, $i\le d-2$, hence the degree of $E(x)^kx^{p(i+1)-1}$ is at most

$$k(pd-1)\;+\;p(d-1)-1<(k+1)pd\,.$$

So, for $k\ge 0$ we can write

$$\binom{-1/2}{k}E(x)^kx^{p(i+1)-1}y^{1-p(1+2k)} \;=\; \sum_{\substack{-(2k+1)p\,<\,j\,<\,p\\ j\text{ even}}} c_{i,k,j}(x)\,y^j$$

$$\Big(\;c_{i,k,j}\in\mathbb{Z}_q[x]\,,\;\deg c_{i,k,j}<d\;\Big)$$

$$\Psi\big(x^i\frac{dx}{y}\big) \;=\; \Big(\sum_{\substack{k\,\ge\,0,\,j\text{ even}\\ -(2k+1)p\,<\,j\,<\,p}} p^{k+1}\,c_{i,k,j}(x)\;y^j\Big)\frac{dx}{y}$$

Proposition 3.2.1 (see [Ked01, Ed03])**.** *Let $c(x)\in\mathbb{Z}_q[x]\,,\ \deg c(x)<d$. Then*

(i) *for $m>0$, the reduction of $c(x)dx/y^{2m+1}$ becomes integral upon multiplication by $p^{\lfloor\log_p(2m-1)\rfloor}$;*
(ii) *for $m\ge 0$, the reduction of $c(x)y^{2m}\,dx/y$ becomes integral upon multiplication by $p^{\lfloor\log_p(d(2m+1))\rfloor}$.*

Proof. (i) Let $c(x)dx/y^{2m+1}\sim b(x)dx/y$, $b\in\mathbb{Q}_q[x]$, $\deg b<d-1$. By our reduction algorithm there exists $f=\sum_{j\text{ odd}}f_j(x)y^j$, $f_j\in\mathbb{Q}_q[x]$, $\deg f_j(x)<d$ such that

$$df \;=\; c(x)dx/y^{2m+1}\;-\;b(x)dx/y\,.$$

The expansion of f is unique and each term contributes as

$$\begin{aligned}d\Big(f_j(x)y^j\Big) \;&=\; \Big(f_j'(x)y^{j+1}\;+\;\frac{j}{2}f_j(x)Q'(x)y^{j-1}\Big)\frac{dx}{y}\\ &=\; \Big(g_j(x)y^{j+1}\;+\;e_j(x)y^{j-1}\Big)\frac{dx}{y}\end{aligned}$$

where

$$\frac{j}{2}f_j(x)Q'(x) \;=\; e_j+h_jQ\,,\quad e_j\neq 0,\,\deg e_j<d,\,\deg h_j<d-1$$

$$g_j \;=\; f_j'+h_j\Rightarrow\deg g_j<d-1$$

Since $e_j\neq 0$ we see that summation in $f=\sum f_jy^j$ must start with $j=1-2m$. To see what's the upper bound let's analyse whether $g_j=0$ is possible:

$$g_j \;=\; 0\Rightarrow h_j \;=\; -f_j'$$

$$e_j \;=\; \frac{j}{2}f_jQ'+f_j'Q\Rightarrow f_j \;=\; const$$

In this case $e_j = \frac{j}{2} f_j Q'$ has degree $d-1$ which can't be changed by adding g_{j-2} because $\deg g_{j-2} < d-1$. Since the leading term in df is $b(x)dx/y$ and $\deg b < d-1$ it follows that the summation should go up to $j=-1$:

$$f \;=\; \sum_{\substack{j\,=\,1\,-\,2m \\ \text{odd}}}^{-1} f_j(x) y^j \,.$$

Let r be a root of $Q(x)$ in $\overline{\mathbb{Z}_q}$ (actually, in some finite extension $\mathbb{Z}_{q^f}$). Then $(x,y)=(r,0)$ is a point on our curve, y is a uniformizer at this point and (**Exercise**) x can be written as a power series in y with integral coefficients (that is, in $\mathbb{Z}_{q^f}$). Locally near $(r,0)$ we write

$$df \;=\; c(x)dx/y^{2m+1} \,-\, b(x)dx/y \;=\; \sum_{j=-2m}^{\infty} c_j\, y^j\, dy$$

with $c_j \in \mathbb{Q}_{q^f}$, and $c_j \in \mathbb{Z}_{q^f}$ when $j<0$ because $c(x) \in \mathbb{Z}_q[x]$. Then

$$f \;=\; \sum_{j=-2m}^{\infty} \frac{c_j}{j+1} y^{j+1} \,.$$

Let $e = \lfloor \log_p(2m-1) \rfloor$. It follows that

$$p^e\, f_{1-2m}(r) \;=\; p^e \lim_{(x,y)\to(r,0)} y^{2m-1} f \;=\; p^e \frac{c_{-2m}}{1-2m} \in \mathbb{Z}_{q^f} \,.$$

This is true for any root of $Q(x)$ in the place of r, and therefore $f_{2m-1}(x) \in \mathbb{Z}_q[x]$. Indeed, let e' be the smallest power of p such that $p^{e'} f_{1-2m}(x) \in \mathbb{Z}_q[x]$. If $e' > e$ then the reduction of $p^{e'} f_{1-2m}(x)$ modulo p (this is a non-zero polynomial over $\mathbb{F}_q$) has d distinct roots in $\mathbb{F}_{q^f}$ (if we assume that all roots of $Q(x)$ are in $\mathbb{Z}_{q^f}$), namely the reductions of the roots of $Q(x)$ modulo p. This is impossible since $\deg f_{1-2m} < d$. We proved that $e' \le e$, and in particular $p^e f_{1-2m} \in \mathbb{Z}_q[x]$.

Now, $p^e f - p^e f_{1-2m}(x)/y^{2m-1}$ has integral coefficients near negative powers when expanded as a power series in y near $(r,0)$ for every root r of $Q(x)$. By the same argument as above $p^e f_{3-2m}(x) \in \mathbb{Z}_q[x]$, and so on. We have that $p^e f_j(x) \in \mathbb{Z}_q[x]$ for every j, and hence $p^e b(x) \in \mathbb{Z}_q[x]$.

(ii) Let first $m>0$. Consider again the function f such that $df \;=\; c(x)y^{2m}dx/y \,-\, b(x)dx/y$. By the same arguments as in part (i), the bounds of summation in the unique representation $f = \sum_{j \text{ odd}} f_j(x) y^j$, $\deg f_j < d$ are

$$f \;=\; \sum_{\substack{j\,=\,1 \\ \text{odd}}}^{2m+1} f_j(x) y^j \,,$$

and $f_{2m+1} \neq 0$ only when $\deg c(x) = d-1$, in which case $f_{2m+1} = const$.

Uniformizer at ∞ is $z = \frac{x^{\frac{d-1}{2}}}{y}$ and we have $v_\infty(x) = -2$, $v_\infty(y) = -d$ (**Exercise**). Therefore

$$\begin{aligned}
v_\infty\big(\frac{dx}{y}\big) \;&=\; d-3 \\
v_\infty\big(b(x)\frac{dx}{y}\big) \;&\ge\; -2(d-2)+d-3 \;=\; 1-d \\
v_\infty\big(c(x)y^{2m}\frac{dx}{y}\big) \;&\ge\; -2(d-1)-2md+d-3 \;=\; -(2m+1)d-1
\end{aligned}$$

and in the local coordinate at infinity

$$df \;=\; \Big(\sum_{k=-(m+1)d-1}^{\infty} c_k\, z^k \Big)\, dz \,, \qquad \begin{array}{l} c_k \in \mathbb{Q}_q \\ \\ c_k \in \mathbb{Z}_q \text{ when } k < 1-d \end{array}$$

If we define $e = \lfloor \log_p((2m+1)d) \rfloor$, then

$$f \;=\; \sum_{k=-(2m+1)d-1}^{\infty} \frac{c_k}{k+1}\, z^{k+1} \;=\; \sum_{k=-(2m+1)d}^{\infty} a_k\, z^k \qquad p^e\, a_k \in \mathbb{Z}_q \text{ when } k < 2-d$$

Since the valuations $v_\infty(x^iy^j) = -2i - dj$ for $0 \le i < d$, $j \ge 1$ are all different and all less then $2-d$, we conclude that $p^e f_j(x) \in \mathbb{Z}_q[x]$ for $1 \le j \le 2m+1$, and hence $p^e b(x) \in \mathbb{Z}_q[x]$.

If $m = 0$ we only have to reduce the term $x^{d-1}dx/y$:

$$dy \;=\; \frac{1}{2}Q'(x)\frac{dx}{y} \;=\; \big(\frac{d}{2}x^{d-1} + \text{ terms of smaller degree }\big)\frac{dx}{y}\,,$$

hence the reduction of $x^{d-1}dx/y$ becomes integral after multiplication by $p^{\lfloor \log_p(d)\rfloor}$. □

It follows that

$$\begin{aligned} c_{i,k,j}(x)y^j\,\frac{dx}{y} \sim b_{i,k,j}(x)\,\frac{dx}{y} \\ b_{i,k,j}(x) \in \mathbb{Q}_q[x]\,,\ \deg b_{i,k,j}(x) \le d-2 \\ p^{\lfloor \log_p(-j-1)\rfloor} b_{i,k,j}(x) \in \mathbb{Z}_q[x]\ (j<0)\,, \\ p^{\lfloor \log_p\left(d(j+1)\right)\rfloor} b_{i,k,j}(x) \in \mathbb{Z}_q[x]\ (j\ge 0)\,. \end{aligned}$$

Let

$$\begin{aligned} m_k = \max\Big(\max_{\substack{-(2k+1)p < j < 0 \\ j \text{ even}}} \lfloor \log_p(-j-1)\rfloor \ ,\ \max_{\substack{0 \le j < p \\ j \text{ even}}} \lfloor \log_p\Big(d(j+1)\Big)\rfloor \ \Big) \\ = \ \lfloor \log_p \max\Big((2k+1)p-2\,,\, dp\Big)\rfloor\,. \end{aligned}$$

We then have

$$\Psi\big(x^i\frac{dx}{y}\big) \sim \Big(\sum_{k\ge 0} p^{k+1}\ b_{i,k}(x)\Big)\,\frac{dx}{y}$$

with

$$\begin{aligned} b_{i,k}\Big(=\sum_j b_{i,j,k}\Big) \in \mathbb{Q}_q[x]\,,\ \deg b_{i,k}(x) \le d-2 \\ p^{m_k} b_{i,k}(x) \in \mathbb{Z}_q[x]\,. \end{aligned}$$

Therefore if we need the matrix of $\Psi \mod p^N$ we should make k in the above summation to run while

$$k + 1 - m_k < N\,.$$

The q-power Frobenius is then given by $F = \sigma^{f-1}(\Psi)\cdot \ldots \sigma(\Psi)\cdot\Psi$ where $f = \log_p(q)$.

3.3. **The algorithm.** We have

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

where

$$P(T) = \det(1 - qF^{-1}T | H^1_{MW}(C)) \in \mathbb{Z}[T]$$

is a polynomial of degree $2g = d-1$. According to the Weil conjectures, the reciprocal roots $\alpha_1, \ldots, \alpha_{2g}$ (= eigenvalues of qF^{-1}) can be numbered so that $\alpha_i\alpha_{g+i} = q$ for $i = 1, \ldots, g$. It follows that qF^{-1} and F have the same eigenvalues: $P(T) = \det(1 - qF^{-1}T) = \det(1 - FT)$. Since $H^1_{MW}(C)$ is the same as $H^1_{MW}(C')^-$, we will use the formula

$$P(T) = \det(1 - FT | H^1_{MW}(C')^-)\,.$$

It remains to analyse what is the smallest power p^N modulo which it is sufficient to know the matrix F.

Consider the coefficients

$$P(T) \;=\; \prod_{i=1}^{2g}(1-\alpha_i T) \;=\; 1 + a_1T + a_2T^2 + \cdots + a_{2g-1}T^{2g-1} + q^gT^{2g}\,.$$

We have the following estimate

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

Since $P(T) = q^gT^{2g}P(1/(qT))$ ($a_{2g-i} = q^{g-i}a_i$) it is enough to determine only $a_1, \ldots, a_g$. Therefore we want to know $P(T)$ modulo p^{N_1} where $N_1 = \lceil \log_p(2\binom{2g}{g}q^{g/2})\rceil$.

Let $N_2 = \min_{k\ge 0}(k+1-m_k)$. If $N_2 \ge 0$ then Ψ is integral and we need to know Ψ modulo $N = N_1$. (**Exercise:** Show that if $p > d$ then $N_2 \ge 0$.) If $N_2 < 0$ there might be entries with negative valuation in Ψ, but the valuation is at most N_2. Therefore it is enough to know F modulo

$$N \;=\; N_1 + f(d-1)\max(0, -N_2)$$

in order to know the determinant of $F = \Psi \cdot \sigma(\Psi) \cdot \ldots \cdot \sigma^{f-1}(\Psi)$ modulo N_1.

We will describe the algorithm in the simple case when $q = p$ and the curve $y^2 = Q(x)$ is given to us with $Q \in \mathbb{Q}[x]$ and p is such that reduction modulo p is good: p divides neither denominators of the coefficients of $Q(x)$ nor the resultant of $Q(x)$ and $Q'(x)$. Then:

- Determine N such that we need to know the matrix of F modulo p^N.
- Find $M = M(N)$ such that $k + 1 - m_k > N$ for $k > M$.
- Consider $S(x) = Q(x^p) - Q(x)^p$. ($S(x) = pE(x)$ is the notation of the previous section.) For each $i = 0, \ldots, d-2$ reduce the form

$$\left(px^{p(i+1)-1}y^{1-p}\sum_{k=0}^{M}\binom{-1/2}{k}S(x)^k y^{-2pk}\right)\frac{dx}{y} \quad \sim \quad b_i(x)\frac{dx}{y} \;=\; \sum_{j=0}^{d-2} b_{ji}x^j\;\frac{dx}{y}.$$

It follows from the estimates in the previous section that $F \equiv (b_{ji})_{j,i=0}^{d-2} \mod p^N$.

Exercise: Program the above algorithm. Compare your results with functions FrobeniusMatrix() in Magma and frobenius_polynomial() in Sage.

In the general case we have $q = p^f$ and the curve is given by $\overline{Q} \in \mathbb{F}_q[x]$. One then lifts $\overline{Q}$ to a polynomial Q with coefficients in $\mathbb{Q}_q$. Actually, it is enough to work modulo some high power of p. The reader can find details in the literature.

References

[Ked01] Kiran S. Kedlaya, *Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology*, Journal of the Ramanujan Mathematical Society 16 (2001), 323–338; errata, ibid. 18 (2003), 417–418

[Ed03] Bas Edixhoven, *Point counting after Kedlaya*, EIDMA-Stieltjes graduate course, Leiden, September 22–26, 2003

[Ked07] Kiran S. Kedlaya, *p-adic cohomology: from theory to practice*, Lecture notes from the 2007 Arizona Winter School

[vdP84] Marius van der Put, *The cohomology of Monsky and Washnitzer*, Mémoires de la Société Mathématique de France, Nouvelle Série (23): 33–59

A sample program in PARI/GP

```
\\ Q: monic polynomial of odd degree with integer coefficients
\\ p: prime
\\ N: integer (default value = 5)
\\ returns Frobenius matrix on the 1st p-adic cohomology of the hyperelliptic curve (y^2=Q(x) mod p)
frobenius(Q,p,{N=5})={
local(d,M,r,q,a,b,A,B,E,F,s,dw,w,da);
d=poldegree(Q);
if(p<=d,print("choose prime p > ",d);return(0));
if(!isprime(p),print(p," is not a prime number");return(0););
if(polresultant(Q,deriv(Q))%p==0,print("the polynomial has double roots mod ",p);return(0));

\\STEP 1: find M such that M terms in the expression for Frobenius on y^{-1} are enough
M=0;
while(M+1-floor(max(log((2*M+1)*p-2),log(d*p))/log(p))<N,M++);
print("M=",M);

\\STEP 2: construct A,B such that AQ+BQ'=1 using the Euclidean algorithm
r=vector(d+2);
r[1]=Q;
r[2]=deriv(Q);
q=vector(d+2);\\ r[i]=q[i]*r[i+1]+r[i+2]
i=1;
while(poldegree(r[i+1])>0,r[i+2]=r[i]%r[i+1];q[i]=(r[i]-r[i+2])/r[i+1];if(q[i]==0,print("AQ+BQ'=1 do
a=vector(i-1,j,0);b=vector(i-1,j,0);\\1=a[j]*r[j]+b[j]*r[j+1]
a[i-1]=1/r[i+1];b[i-1]=-q[i-1]/r[i+1];
forstep(j=i-1,2,-1,a[j-1]=b[j];b[j-1]=a[j]-b[j]*q[j-1]);
A=a[1];B=b[1];


\\STEP 3 : compute Frobenius on y^(-1)
E=subst(Q,x,x^p)-Q^p; \\ E is divisible by p
a=vector(p*M+1+(p-1)/2,i,0);
a[1+(p-1)/2]=1;
for(k=1,M,a[1+(p-1)/2+k*p]=E*(-1/2-k+1)/k*a[1+(p-1)/2+(k-1)*p]);
\\ F(y^-1) = sum(i>=0,  a[1+i]*y^(-2i) 1/y )

\\STEP 4 : compute Frobenius matrix on differentials
\\ F(x^i dx/y) = sum(j>=0, s[1+j]*y^(-2j) ) dx/y
F=matrix(d-1,d-1);
for(i=0,d-2,\
s=vector(p*M+1+(p-1)/2,j,p*x^(p*i+p-1)*a[j]);\
forstep(j=p*M+(p-1)/2,1,-1, s[j]=s[j]+s[j+1]*A+deriv(s[j+1]*B/(j-1/2)));\
while(poldegree(s[1])>=d-1,dw=poldegree(s[1]);w=polcoeff(s[1],dw);da=dw-d+1;s[1]=s[1]-w/(da+d/2)*(da
for(k=0,d-2,F[1+k,1+i]=polcoeff(s[1],k)+O(p^N));\
);
return(F);
}
```