数理解析研究所講究録 1361 巻 2004 年 56-69

三浦理論に基づくKedlayaの位数計算の一般化
Generalizing Kedlaya's order counting based on Miura theory

鈴木譲
Joe Suzuki

February 7, 2004

Abstract

Kedlaya の Monsky-Washinitzer Cohomology における Leschetz 不動点定理を用いて、hyper-楕円曲線の $\mathbb{F}_q$ 有理点の個数を求める方法は、その後 super-楕円曲線や C_ab 曲線にまで拡張されたが、それ以上の一般化は困難とみなされてきた。本稿では、1990 年代初頭に三浦によって提案されたアフィン多様体の表現方法を用いて、3 変数以上で表現される曲線の場合への Kedlaya の方法の拡張を試みる。特に、telescopic 曲線のある特別な場合 (強 telescopic 曲線) に対して、その一般化された方法が適用されることが示されている。

1 Monsky-Washinitzer Cohomology

Let $k = \mathbb{F}_q$ with $q = p^m$ and prime p odd, $R = W(\mathbb{F}_q)$ the Witt ring of $\mathbb{F}_q$, and $K = \mathbb{Q}_q$ the quotient field of R. Let X be a smooth affine variety over k, $\bar{A}$ the coordinate ring of X, $\mathcal{A}$ a smooth R-algebra with $\mathcal{A} \otimes_R k \cong \bar{A}$, and $\mathcal{A}^\infty$ the p-adic completion of $\mathcal{A}$. Let v_p denote the p-adic valuation on R. Fix $x_1, \cdots, x_n \in \mathcal{A}^\infty$ whose reductions $\bar{x}_1, \cdots, \bar{x}_n$ generate $\bar{A}$ over k.

Definition 1 (Monsky-Washinitzer [4]) The week completion $\mathcal{A}^\dagger$ of $\mathcal{A}$ is the substring of $\mathcal{A}^\infty$ consisting of elements $z = \sum_{i_1 \cdots i_n} a_{i_1 \cdots i_n} x_1^{i_1} \cdots x_n^{i_n}$ such that

$$i_1 + \cdots + i_n \geq d \Longrightarrow \frac{\min_{i_1 \cdots i_n} v_p(a_{i_1 \cdots i_n})}{i_1 + \cdots + i_n} > c$$

for some d and $c > 0$.

Let Ω be the $\mathcal{A}^\dagger$ module of different forms over K generated by symbols dx, $x \in \mathcal{A}^\dagger \otimes_R K$ and subject to the relations

1. $d(x+y) = dx + dy$ for $x, y \in \mathcal{A}^\dagger \otimes_R K$;
2. $d(xy) = xdy + ydx$ for $x, y \in \mathcal{A}^\dagger \otimes_R K$; and
3. $dx = 0$ for $x \in K$.

We define the exterior derivative $d : \wedge^r\Omega \to \wedge^{r+1}\Omega$ by,

$$\omega = \sum \alpha_{i_1,\cdots,i_r} dx_{i_1} \wedge \cdots \wedge dx_{i_r} \longmapsto d(\omega) = \sum d(\alpha_{i_1,\cdots,i_r}) \wedge dx_{i_1} \wedge \cdots \wedge dx_{i_r} ,$$

where $\alpha_{i_1,\cdots,i_r} \in \mathcal{A}^\dagger$, the sum runs over $1 \leq i_1 < \cdots < i_r \leq n$, and $\wedge^r\Omega$ denotes the r-th exterior power of Ω.

Definition 2 (Monsky-Washinitzer [4]) In the sequence of homomorphisms

$$0 \longrightarrow \wedge^0\Omega \xrightarrow{d} \wedge^1\Omega \xrightarrow{d} \cdots \xrightarrow{d} \wedge^n\Omega \longrightarrow 0 ,$$

the cohomology groups of the de Rham complex over $\mathcal{A}^\dagger \otimes_R K$

$$H^r(\bar{\mathcal{A}}; K) := \frac{ker(d : \wedge^r\Omega \to \wedge^{r+1}\Omega)}{im(d : \wedge^{r-1}\Omega \to \wedge^r\Omega)} ,$$

$r = 0, \cdots, n$, are called the Monsky-Washnitzer cohomology groups, where $\wedge^{-1}\Omega = \wedge^{n+1}\Omega = 0$.

In general, it is known that

1. $H^r(\bar{\mathcal{A}}; K) = 0$ is a finite dimensional K-vector space; and
2. $H^0(\bar{\mathcal{A}}; K) = K$, $H^1(\bar{\mathcal{A}}; K) \equiv \Omega$ modulo dx, $x \in \mathcal{A}^\dagger \otimes_R K$.

Hereafter, we assume the variety is a curve, so that $H^r(\bar{\mathcal{A}}; K) = 0$, $r = 2, \cdots, n$.

If we lift the p-power Frobenius of $\bar{\mathcal{A}}$ to an endomorphism σ of $\mathcal{A}^\dagger$, then the q-power Frobenius on $\bar{\mathcal{A}}$ will be lifted to an endmorphism $F := \sigma^m$. In general, an endomorphism ϕ of $\mathcal{A}^\dagger$ induces an endmorphism ϕ_* on the cohomology groups.

Theorem 1 (Leschetz fixed point formula [5]) Suppose $\mathcal{A}^\dagger$ admits an endmorphism F lifting the q-power Frobenius on $\bar{\mathcal{A}}$. Then, the number of homomorphisms $\bar{\mathcal{A}} \to \mathbb{F}_q$ equals

$$\sum_{r=0}^{n} (-1)^r Tr(qF_*^{-1} | H^r(\bar{\mathcal{A}}; K)) . \tag{1}$$

If we assume curves, then (1) reduces to $Tr(qF_*^{-1}|K) - Tr(qF_*^{-1}|\Omega$ modulo dx, $x \in \mathcal{A}^\dagger \otimes_R K)$.

2 Kedlaya's Method

Kedraya [2] proposed an order counting method for hyperelliptic curves $C : y^2 = \bar{Q}(x)$ ($\bar{Q}(x)$: a polynomial of degree over $\mathbb{F}_q$ without repeated roots) using the Lefschetz fixed point formula. Kedlaya considered the curve C' excluding the points on $y = 0$ from C. Then, the coordinate ring $\bar{\mathcal{A}}$ of C' is $k[x, y, y^{-1}]/(y^2 - \bar{Q}(x))$. Let $\mathcal{A} = R[x, y, y^{-1}]/(y^2 - Q(x))$, and $\mathcal{A}^\dagger$ the weak completion of $\mathcal{A}$. Then, the elements of $\mathcal{A}^\dagger$ can be viewed as series $\sum_{j=-\infty}^{\infty} \sum_{i=0}^{2g} a_{ij} x^i y^j$ with $a_{ij} \in R$ such that

$$\liminf_{j \to \infty} \frac{\min_i\{v_p(a_{ij})\}}{j} > 0 \text{ and } \liminf_{j \to -\infty} \frac{\min_i\{v_p(a_{ij})\}}{j} > 0 .$$

The essential point is that Kedlaya found for the curve C' an admissible endomorphism σ over $\mathcal{A}^\dagger$ that is obtained by lifting the p-power Frobenius of $\bar{\mathcal{A}}$, which is needed to apply the Leschetz fixed point formula. We can lift the p-power Frobenius to an endomorphism σ by defining it as the cannonical Witt vector Frobenius on R, then extending to $R[x]$ by mapping $x \in \mathcal{A}^\dagger$ to $x^p \in \mathcal{A}^\dagger$ and $y \in \mathcal{A}^\dagger$ to

$$y^\sigma = y^p (1 + \frac{Q(x)^\sigma - Q(x)^p}{Q(x)^p})^{1/2} = y^p \sum_{i=0}^{\infty} \frac{(1/2)(1/2-1)\cdots(1/2-i+1)}{i!} \frac{(Q(x)^\sigma - Q(x)^p)^i}{y^{2pi}} \in \mathcal{A}^\dagger .$$

Then, the de Rham cohomology of $\mathcal{A}$ splits $H^1(\bar{\mathcal{A}}; K)$ into eigenspaces under the hyperelliptic involution: a positive eigenspace $H^1(\bar{\mathcal{A}}; K)_+$ generated by $x^i dx/y^2$ for $i = 0, \cdots, 2g-1$, and a negative eigenspace $H^1(\bar{\mathcal{A}}; K)_-$ generated by $x^i dx/y$ for $i = 0, \cdots, 2g-1$. In fact, using the formula

$$dx \equiv 0, x \in \mathcal{A}^\dagger \otimes_R K ,$$

any form $\sum_{j=-\infty}^{\infty} \sum_{i=0}^{2g-1} a_{i,j} x^i dx/y^j$ can be reduced either to $\sum_{i=0}^{2g-1} b_{i,j} x^i dx/y$ or to $\sum_{i=0}^{2g-1} b_i x^i dx/y^2$, with $b_{i,j}, b_i \in K$, depending on whether j is odd or even. Since $(dx)^{\sigma_*} = p x^{p-1} dx$ and

$$(\frac{1}{y})^\sigma = y^{-p} (1 + \frac{Q(x)^\sigma - Q(x)^p}{Q(x)^p})^{1/2} = \sum_{i=0}^{\infty} \frac{(-1/2)(-1/2-1)\cdots(-1/2-i+1)}{i!} \frac{(Q(x)^\sigma - Q(x)^p)^i}{y^{(2i+1)p}} ,$$

we have a matrix $M = (m_{i,j}), m_{i,j} \in K$ such that

$$(\frac{x^i dx}{y})^{\sigma_*} \equiv \sum_{j=0}^{2g-1} m_{i,j} \frac{x^j dx}{y} .$$

Based on the Leschetz fixed point formula, Kedraya showed $q^i + 1 - \#C(\mathbb{F}_{q^i})$ equals the trace of $q^i F_*^{-i}$ on the negative eigenspace $H^1(\bar{\mathcal{A}}; K)_-$ of $H^1(\bar{\mathcal{A}}; K)$ for all $i > 0$:

$$\begin{aligned}
\#C(\mathbb{F}_{q^i}) - d &= \#C'(\mathbb{F}_{q^i}) \\
&= Tr(q^i F_*^{-i}, H^0(\bar{\mathcal{A}}; K)) - Tr(q^i F_*^{-i}, H^1(\bar{\mathcal{A}}; K)) \\
&= Tr(q^i F_*^{-i}, H^0(\bar{\mathcal{A}}; K)) - Tr(q^i F_*^{-i}, H^1(\bar{\mathcal{A}}; K)_+) - Tr(q^i F_*^{-i}, H^1(\bar{\mathcal{A}}; K)_-) \\
&= Tr(q^i F_*^{-i}, H^0(\bar{\mathcal{A}}'; K)) - Tr(q^i F_*^{-i}, H^1(\bar{\mathcal{A}}'; K)) - Tr(q^i F_*^{-i}, H^1(\bar{\mathcal{A}}; K)_-) \\
&= q^i + 1 - d - Tr(q^i F_*^{-i}, H^1(\bar{\mathcal{A}}; K)_-)
\end{aligned}$$

where $d = \#\{(x,y) \in E(\mathbb{F}_{q^i}) | x \in \mathbb{F}_{q^i}, y = 0\}$, and $\bar{A}' = k[x, y^{-2}]$. (Note that the Leschetz fixed point formula has been applied in the second and last equlities for $\bar{A}$ and $\bar{A}'$, respectively.)

By the Weil conjectures, there exists a polynomial

$$x^{2g} + a_1 x^{2g-1} + \cdots + a_{2g} \tag{2}$$

whose roots $\alpha_1, \cdots, \alpha_{2g}$ satisfy $\alpha_j \alpha_{g+j} = q$ for $j = 1, \cdots, g$, $|\alpha_j| = \sqrt{q}$ for $j = 1, \cdots, 2g$, and

$$q^i + 1 - \#C(\mathbb{F}_{q^i}) = \sum_{j=1}^{2g} \alpha_j^i$$

for all $i > 0$. Thus, the eigenvalues of qF_*^{-1} on $H^1(\bar{A}; K)_-$ are precisely the α_j, as are the eigenvalues of F_* itself. Since $a_j = a_{2g-j}$, it suffices to determine $a_1, \cdots, a_g$. Since $\alpha_1, \cdots, \alpha_{2g}$ are the roots of (2), the coefficients $a_0, \cdots, a_g$ are bounded by

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

Thus to determine the zeta function, it suffices to compute the action of F_* on a suitable basis of $H^1(\bar{A}; K)_-$ modulo p^N for $N \geq (g/2)m + (2g+1)\log_p 2$.

If $z^{\sigma_*} \equiv zM$ for $z \equiv [\frac{dx}{y}, \frac{xdx}{y}, \cdots, \frac{x^{2g-1}dx}{y}]$ and some $M \in K^{2g \times 2g}$, then

$$z^{F_*} \equiv zMM^{\sigma_*}M^{\sigma_*^2} \cdots M^{\sigma_*^{m-1}} .$$

Hence, if we compute the product $\mathcal{M} = MM^{\sigma_*}M^{\sigma_*^2} \cdots M^{\sigma_*^{m-1}}$ and its characteristic polynomial modulo p^N, we can recover the characteristic polynomial of Frobenious from the first g coefficients.

3 Miura Theory

By $< A >=< a_1, \cdots, a_n >$ we denote the monoid generated by n positive integers in $A = \{a_1, \cdots, a_n\}$ such that $a_i \notin < a_1, \cdots, a_{i-1}, a_{i+1}, \cdots, a_n >$ for $1 \leq i \leq n$ and $gcd(a_1, \cdots, a_n) = 1$. We define $\Psi_A : \mathbb{N}^n \to < A >$ by $\Psi_A(s_1, \cdots, s_n) = \sum_{i=1}^n a_i s_i$.

Definition 3 (C_A order) $\alpha >_A \beta$ for $\alpha = (\alpha_1, \cdots, \alpha_n)$ and $\beta = (\beta_1, \cdots, \beta_n) \in \mathbb{N}^n$ if

1. $\Psi_A(\alpha_1, \cdots, \alpha_n) > \Psi_A(\beta_1, \cdots, \beta_n)$, or
2. $\Psi_A(\alpha_1, \cdots, \alpha_n) = \Psi_A(\beta_1, \cdots, \beta_n)$ and $\alpha_1 = \beta_1, \cdots, \alpha_{i-1} = \beta_{i-1}, \alpha_i < \beta_i$ for some $1 \leq i \leq n$.

For monomial $x_1^{s_1} \cdots x_n^{s_n}$ with $s_1, \cdots, s_n \in \mathbf{N}$, we define

$$\bar{\Psi}_A(x_1^{s_1} \cdots x_n^{s_n}) := \Psi_A(s_1, \cdots, s_n) ,$$

which is extended for polynomial $\sum_t r_t x_1^{s_{t1}} \cdots x_n^{s_{tn}} \in \kappa[x_1, \cdots, x_n]$ with $r_t \in \kappa$ and $s_{t1}, \cdots, s_{tn} \in \mathbf{N}$, as

$$\bar{\Psi}_A(\sum_t r_t x_1^{s_{t1}} \cdots x_n^{s_{tn}}) := \max_t \bar{\Psi}_A(x_1^{s_{t1}} \cdots x_n^{s_{tn}}) .$$

Also, we define $M_A(l) \in \mathbf{N}^n$ to be the minimal $M \in \mathbf{N}^n$ with respect to $>_A$ satisfying $\Psi_A(M) = l$,

$$B(A) := \{M_A(l) | l \in < A >\} ,$$

and

$$V(A) := \{L_1 + L_2 \in \mathbf{N}^n \backslash B(A) \mid L_1 \in \mathbf{N}^n \backslash B(A) \Longrightarrow L_2 = (0, \cdots, 0)\} .$$

Let κ be a field. Suppose we are given a smooth curve C defined over κ with a κ-rational point P such that

$$\mathcal{M}_P := \{-v_P(f) | f \in \mathcal{L}(\infty P)\} = A .$$

Theorem 2 (Miura [3]) The curve C is an affine variety in n variables with $I := \{F_M = 0 | M \in V(A)\}$ such that

$$F_M = X^M + \alpha_L X^L + \sum_{N \in B(A), \Psi_A(N) < \Psi_A(L)} \alpha_N X^N , \tag{3}$$

where we denote $X^M := \Pi_i X_i^{M_i}$ for $M = (M_1, \cdots, M_n) \in \mathbf{N}^n$, and $X_i \in \mathcal{L}(\infty P)$ is a function such that $(X_i)_\infty = a_i P$. Moreover, L is the unique element in $B(A)$ satisfying $\Psi_A(M) = \Psi_A(L)$, and $\alpha_L \neq 0$, $\alpha_N \in \kappa$, and that P is the only point at infinity ($P = P_\infty$), thus

$$\mathcal{L}(\infty P) = \kappa[x_1, \cdots, x_n]$$

(the coordinate ring of C), where $x_i \equiv X_i \bmod F_M = 0$ for all $M \in V(A)$.

Example 1 $A = \{a, b\}$ with $gcd(a, b) = 1$. Then,

$$B(A) = \{(m, l) | 0 \leq l \leq a - 1, m = 0, 1, \cdots\}$$

and

$$V(A) = \{(0, a)\} .$$

Hence, the curve C is defined by the equation:

$$Y^a = \alpha_{ab} X^b + \sum_{ma+lb<ab} \alpha_{ma+lb} X^m Y^l , \tag{4}$$

where $\alpha_{ab}, \alpha_{ma+lb} \in k$. By transforming the variables X and Y to $\alpha_{ab}^s X$ and $\alpha_{ab}^t Y$ with $s, t \in \mathbf{Z}$, respectively, we can set $\alpha_{ab} = 1$. (Note $gcd(a, b) = 1$).

Example 2 $A = \{4, 6, 5\}$. Then,

$$\begin{aligned} B(A) &= \{(0,0,0),(1,0,0),(0,0,1),(0,1,0),(1,0,1),(1,1,0),(0,1,1), \\ &\quad (3,0,0),(2,0,1),(2,1,0),(1,1,1),(4,0,0),\cdots\} \end{aligned}$$

and

$$V(A) = \{(0,2,0),(0,0,2)\} .$$

Hence, the curve C is defined by the equations:

$$Y^2 = \beta_{12}X^3 + \beta_{11}YZ + \beta_{10}XY + \beta_9 XZ + \beta_6 Y + \beta_5 Z + \beta_4 X + \beta_0$$

$$Z^2 = \gamma_{10}XY + \gamma_9 XZ + \gamma_6 Y + \gamma_3 Z + \gamma_4 X + \gamma_0 ,$$

where $\beta_i, \gamma_j \in \kappa$.

Hereafter, we fix an element in A, say a_1, and denote by $b_l, l = 0, 1, \cdots$, the minimal $b \in < a_2, \cdots, a_n >$ such that $b \equiv l \bmod a_1$. Clearly, $b_l = b_{l+ma_1}$ for $m = 0, 1, \cdots$.

Theorem 3 (Miura [3]) We define $T(A) := \{(s_1, s_2, \cdots, s_n) \in B(A) | s_1 = 0\}$. Then,

$$T(A) = \{M_A(b_l) | 0 \leq l \leq a_1 - 1\} , \tag{5}$$

$\#T(A) = a_1$, and $\{x^{M_A(b_l)}, l = 0, 1, \cdots, a_1 - 1\}$ is a $\kappa[x_1]$-basis of $\kappa[x_1, \cdots, x_n]$.

Example 3 If $A = \{a, b\}$, then $T(A) = \{(0,0),(0,1),\cdots,(0,a-1)\}$, so that the coordinate ring is

$$\kappa[x, y] = \kappa[x] + \kappa[x]y + \cdots + \kappa[x]y^{a-1} .$$

Example 4 If $A = \{4, 6, 5\}$, then $T(A) = \{(0,0,0),(0,0,1),(0,1,0),(0,1,1)\}$ and $b_0 = 0, b_1 = 5, b_2 = 6, b_3 = 9$, so that the coordinate ring is

$$\kappa[x, y, z] = \kappa[x] + \kappa[x]z + \kappa[x]y + \kappa[x]yz .$$

Proposition 1

$$g = \#(\mathbf{N} \setminus < A >) = \sum_{l=0}^{a_1 - 1} \lfloor b_l / a_1 \rfloor , \tag{6}$$

where $\lfloor x \rfloor$ is the largest integer no more than x.

We fix the order of $a_1, \cdots, a_n \in A$ as $\bar{A} = (a_1, \cdots, a_n)$.

Definition 4 (Nijenhuis-Wilf [6]) $\bar{A} = (a_1, \cdots, a_n)$ satisfying

$$a_i / d_i \in < a_1 / d_{i-1}, \cdots, a_{i-1} / d_{i-1} > , \tag{7}$$

where $d_i = gcd(a_1, \cdots, a_i)$, is said to be *telescopic*. Furthermore, any curve with a k-rational point P such that

1. $\mathcal{M}_P = A$

2. an ordered $\bar{A}$ of $\mathcal{A}$ is telescopic

is said to be *telescopic*. In particular, if $n = 2$, the curve is telescopic.

Example 5 $\bar{A} = (4, 6, 5)$ satisfies (7) although $\bar{A} = (4, 5, 6)$ does not. However, the curve with $\mathcal{M}_P = A$ is telescopic for A.

Theorem 4 (Nijenhuis-Wilf [6]) In general,

$$g \leq [1 + \sum_{i=1}^{n} (\frac{d_{i-1}}{d_i} - 1)a_i]/2 \,, \tag{8}$$

where $d_0 = 0$. The equation follows if and only if $A = (a_1, \cdots, a_n)$ is telescopic.

Theorem 5 (Miura [3]) If a curve with A is telescopic, then

1. $T(A) = \{(0, t_2, \cdots, t_n) | 0 \leq t_i \leq d_{i-1}/d_i - 1, i = 2, \cdots, n\}$

2. $V(A) = \{(0, \cdots, 0, d_{i-1}/d_i, 0, \cdots, 0) | i = 2, \cdots, n\}$.

Example 6 If $A = \{4, 6, 5\}$, then $T(A) = \{(0,0,0), (0,1,0), (0,0,1), (0,1,1)\}$ and $V(A) = \{(0,2,0), (0,0,2)\}$. Furthermore, $(b_0, b_1, b_2, b_3) = (0, 5, 6, 11)$ with $a_1 = 4$, so that $g = 4$ from Proposition 1, which is also obtained from Theorem 4.

If, in Theorem 2, the ideal a nonsingular curve is given by

$$I = \{X_i^{d_{i-1}/d_i} - h_i(X_1, \cdots, X_{i-1}) = 0 | i = 2, \cdots, n\}$$

for some $h_i \in k[X_1, \cdots, X_{i-1}]$, $i = 2, \cdots, n$, then the curve is said to be *strongly telescopic*.

4 Cohomology of Smooth Curves

The notation follows Stichtenoth [9].

Let C be a smooth curve defined over $k = \mathbb{F}_q$ expressed by some $A = \{a_1, \cdots, a_n\}$ and $F_M = 0, M \in V(A)$. Then, the coordinate ring of C is

$$\bar{A} = k[\bar{x}_1, \cdots, \bar{x}_n] \,,$$

where $\bar{x}_i \equiv X_i \bmod F_M(X_1, \cdots, X_n) = 0$ for all $M \in V(A)$. In this section, we assume that each $\bar{x}_i$ has a pole only at P_∞. Hereafter, we denote by $\bar{I} \subset k[\bar{x}_1, \cdots, \bar{x}_n]$ the ideal generated by $F_M = 0, M \in V(A)$.

Let $I = \{F_2, \cdots, F_n\} \subset K[x_1, \cdots, x_n]$ be the ideal associated with $\mathcal{A}^\infty$, which defines an affine variety over K in n variables. We consider the function field F/K, where

$F/K(x_i)$ is an algebraic extension with degree $[F : K(x_i)] = a_i$. From the equations $dF_i = 0$, $i = 2, \cdots, n$, we obtain the unique relation

$$\omega_* := \frac{dx_1}{f_1(x_1, \cdots, x_n)} = \cdots = \frac{dx_n}{f_n(x_1, \cdots, x_n)} , \tag{9}$$

where $f_i(x_1, \cdots, x_n) = 0$, $i = 1, \cdots, n$, have no common zero. This is possible because, if $f_i = tf_i^*$ at $P \in \mathbb{P}_F$ with $v_P(f_i^*) = 0$ for $i = 1, \cdots, n$, where t is a uniformaizer at P, then we can replace f_i by f_i^*.

Since, if $P \neq P_\infty$, $v_P(dx_i) \geq 0$ and $v_P(f_i) \geq 0$, and since $deg(w_*) = 2g - 2$, we have

$$(\omega_*) = (2g - 2)P_\infty . \tag{10}$$

On the other hand, since P_∞ lies over $(x_i)_\infty = a_i P_\infty$ and $degP_\infty = 1$, so we have $e(P_\infty|(x_i)_\infty) = a_i$. Since $charK = 0$, from Dedekind's different theorem, $d(P_\infty|(x_i)_\infty) = e(P_\infty|(x_i)_\infty) - 1 = a_i - 1$. Furthermore, in general,

$$(dx_i) = -2(x_i)_\infty + Diff(F/K(x_i)) \tag{11}$$

$i = 1, \cdots, n$, where $Diff(F/K(x_i)) := \sum_{P \in \mathbb{P}_F} \sum_{P'|P} d(P'|P)P'$ is the different of $F/K(x_i)$. Combining (10)(11) with $(w_*) = (dx_i) - (f_i)$, we obtain $(f_i)_\infty = (a_i + 2g - 1)P_\infty$. Since (f_i) is a principle divisor, $\bar{\Psi}_A(f_i) = a_i + 2g - 1$.

In this section, we obtain $2g$ independent elements in $H^1(\bar{A}; K)$ over K for $\bar{A} = k[\bar{x}_1, \cdots \bar{x}_k]$ with $(x_i)_\infty = a_i P_\infty$, $a_i \geq 0$, $i = 1, \cdots, n$. Hereafter, we denote $\omega \equiv 0$ if differntial $\omega \in \Omega$ is exact, say $H^1(\bar{A}; K) \equiv \Omega$. We can eliminate the highest degree monomial in $f_i(x_1, \cdots, x_n)\omega_*$ with respect to $>_A$ by the relation $dx_i = f_i(x_1, \cdots, x_n)\omega_* \equiv 0$ for $i = 1, \cdots, n$.

Theorem 6 Ω is generated by

$$\sum_{h \in H(A)} \mathcal{A}^\dagger \otimes_{W(\mathbb{F}_q)} Kx^{M_A(h)}\omega_* \tag{12}$$

modulo exact differentials, where

$$H(A) := [\{b_l + 2g - 1 - a_1 v | 0 \leq l \leq a_1 - 1, v = 1, \cdots\} \cup \{2g - 1\}] \cap < A >$$

and $\bar{A} = k[\bar{x}_1, \cdots, \bar{x}_n]$ with $(x_i)_\infty = a_i P_\infty$, $a_i \geq 0$, $i = 1, \cdots, n$. In particular, $\#H(A) = 2g$.

Proof. From Theorem 3, $\mathcal{A}$ can be expressed by

$$\mathcal{A} = \sum_{l=0}^{a_1 - 1} R[x_1]y_l ,$$

where $y_l := x^{M_A(b_l)}$. Then, from (9), we find $g_{j,l}(x_1, y_1, \cdots, y_{a-1}) \in \mathcal{A}$ such that

$$\omega_* = \frac{dx_1^j y_l}{g_{j,l}(x_1, y_1 \cdots, y_{a_1-1})} \tag{13}$$

for $(j,l) \in G(a_1) := \{(j,l) | j = 0, 1, \cdots, 0 \le l \le a_1 - 1\} \backslash \{(0,0)\}$, and obtain

$$\bar{\Psi}_A(g_{j,l}) = ja_1 + b_l + 2g - 1 \ . \tag{14}$$

From $dx_1^j y_l \equiv 0$ with $(j,l) \in G(a_1)$, $cx^{M_A(ja_1+b_l+2g-1)}\omega_*$ with $c \in K$ can be reduced to lowere degree terms. However, for each l, terms $cx^{M_A(2g-1)}\omega_*$ and $cx^{M_A(b_l+2g-1-a_1v)}\omega_*$ with $c \in K$ and $v = 1, 2, \cdots$ cannot be reduced using those relations. Hence, Ω modulo exact differentials is spanned by $\{x^{M_A(h)}\omega_* | h \in H(A)\}$.

Furthermore, since $dx \in \Omega$ only if $x \in \mathcal{A}^\dagger \otimes_R K$, and that all the linear relation we can use for reduction is of the form $dx_1^j y_l \equiv 0$ with $(j,l) \in G(a_1)$ up to K, $\{x^{M_A(h)}\omega_* | h \in H(A)\}$ is actually linearly independent.

If we define by e_l the minimal e_l $(0 \le l \le a_1 - 1)$ such that $e_l \equiv b_l + 2g - 1 \bmod a_1$, then e_l ranges over $0 \le l \le a_1 - 1$, which means $\sum_l (b_l + 2g - 1 - e_l) = \sum_l (b_l + 2g - 1 - l)$. Hence,

$$\sum_l \lfloor \frac{b_l + 2g - 1}{a_1} \rfloor = \sum_l \frac{b_l + 2g - 1 - l}{a_1} = \sum_l \frac{b_l + 2g - 1 - e_l}{a_1} = \sum_{l=0}^{a-1} \frac{b_l - l}{a_1} + 2g - 1 = 3g - 1 \ ,$$

where Proposition 1 has been applied in the last equality. So, we have

$$\sum_{l=0}^{a-1} \lfloor \frac{b_l + 2g - 1}{a_1} \rfloor - g + 1 = 2g$$

if $2g - 1 \in < A >$, and

$$\sum_{l=0}^{a-1} \lfloor \frac{b_l + 2g - 1}{a_1} \rfloor - (g - 1) = 2g$$

if $2g - 1 \notin < A >$. In any case, $\#H(A) = 2g$. □

Example 7 If $A = \{a, b\}$, from Proposition 1 $g = (a-1)(b-1)/2$, thus $2g - 1 = b(a-1) - a$. We know there exists an injective $\phi : \{0, \cdots, a-1\} \to \{0, \cdots, a-1\}$ such that $b_l = \phi(l)b$ and $\phi(0) = 0$. Since

$$b_l + 2g - 1 - ja = b\phi(l) + ab - a - b - ja = b(h(l) - 1) + a(b - 1 - j) \in H(A)$$

for $1 \le l \le a-1$ and $1 \le j \le b-1$. However, for $l = 0$, $b_0 + 2g - 1 - ja = ab - (j+1)a - b \notin < a, b >$. Thus, we have

$$H(A) = \{ja + lb | 0 \le j \le b-2, 0 \le l \le a-2\} \ .$$

Hence, Ω is generated by $\{x^j y^l \omega_* | 0 \leq j \leq b-2, 0 \leq l \leq a-2\}$ over K modulo exact differentials. If the curve is superelliptic, the equation (4) with $\alpha_{a,b} = 1$ reduces to

$$Y^a = X^b + \sum_{j=0}^{b-1} \alpha_{ja} X^j .$$

Then, $\omega_* = \dfrac{dx}{ay^{a-1}}$, and Ω is generated by $\{x^j \dfrac{dx}{y^l} | 0 \leq j \leq b-2, 1 \leq l \leq a-1\}$ over K modulo exact differentials.

Example 8 If $A = \{4, 6, 5\}$, then $H(A) = \{0, 4, 5, 6, 8, 9, 10, 14\}$. Hence, Ω is generated by

$$\{w_*, xw_*, x^2 w_*, zw_*, xzw_*, yw_*, xyw_*, x^2 y^2 w_*\}$$

over K modulo exact differentials. Furthermore, if the curve is defined by

$$y^2 = x^3 + x + 1, \; z^2 = xy + x + 1 ,$$

then

$$w_* = \frac{dx}{yz} = \frac{dy}{z(3x^2+1)/2} = \frac{dz}{x(3x^2+1)/2 + y(y+1)} ,$$

and Ω is generated by

$$\{\frac{1}{yz}, \frac{x}{yz}, \frac{x^2}{yz}, \frac{1}{y}, \frac{x}{y}, \frac{1}{z}, \frac{x}{z}, \frac{x^2 y}{z}\}$$

over K modulo exact differentials.

5 Kedlaya's Method for Strongly Telescopic Curves

We apply Kedlaya's method to strongly telescopic curves in n variables $\bar{x}_1, \bar{x}_2, \cdots, \bar{x}_n$ with

$$\bar{I} = \{\bar{x}_2^{m_2} = \bar{h}_2(\bar{x}_1), \bar{x}_3^{m_3} = \bar{h}_3(\bar{x}_1, \bar{x}_2), \cdots, \bar{x}_n^{m_n} = \bar{h}_n(\bar{x}_1, \cdots, \bar{x}_{n-1})\} , \tag{15}$$

where $\bar{h}_i \in k[\bar{x}_1, \cdots, \bar{x}_{i-1}]$, $i = 2, \cdots, n$.

Let C be such a curve, and C' the affine curve obtained from C by deleting the support of the divisors of $\bar{x}_2, \cdots, \bar{x}_n$; then the coordinate ring $\bar{\mathcal{A}}$ of C' is $k[\bar{x}_1, \bar{x}_2, \cdots, \bar{x}_n, \bar{x}_2^{-1}, \cdots, \bar{x}_n^{-1}]/(\bar{I})$.

We fix $\mathcal{A} = R[x_1, x_2, \cdots, x_n, x_2^{-1}, \cdots, x_n^{-1}]/(I)$ such that $\mathcal{A} \otimes_R k \cong \bar{\mathcal{A}}$, where

$$I = \{x_2^{m_2} = h_2(x_1), x_3^{m_3} = h_3(x_1, x_2), \cdots, x_n^{m_n} = h_n(x_1, \cdots, x_{n-1})\} ,$$

and $h_i \in R[x_1, \cdots, x_{i-1}]$, $i = 2, \cdots, n$, and let $\mathcal{A}^\dagger$ be the weak completion of $\mathcal{A}$.

Let v_p denote the p-adic valuation on R. Then, $\sum_{t_1 \geq 0, t_2 \cdots, t_n \in \mathbb{Z}} s_{t_1, \cdots, t_n} x_1^{t_1} \cdots x_n^{t_n} \in \mathcal{A}^\dagger, s_{t_1, \cdots, t_n} \in R$, if and only if

$$\liminf_{r \to \infty} \min_{t_1 \geq 0, r = |t_1 + \cdots + t_n|} \frac{v_p(s_{t_1, \cdots, t_n})}{r} > 0 . \tag{16}$$

We can lift the p-power Frobenious to an endomorphism σ of $\mathcal{A}^\dagger$ by defining it as the canonical Witt vector Frobenius on R, then extending to $R[x_1]$ by mapping x_1 to x_1^p. Apparently, p divides $x_1^\sigma - x_1^p = 0$. If p divides $x_2^\sigma - x_2^p, \cdots, x_{i-1}^\sigma - x_{i-1}^p$, then p divides

$$x_i^\sigma - x_i^p = h_i(x_1, \cdots, x_{i-1})^\sigma - h_i(x_1, \cdots, x_{i-1})^p \ .$$

Thus, p divides $h_j(x_1, \cdots, x_{j-1})^\sigma - h_j(x_1, \cdots, x_{j-1})^p$ for all $j = 1, \cdots, n$, and

$$\begin{aligned}(x_i^{-1})^\sigma &= x_i^{-p}\left(1 + \frac{h_i(x_1, \cdots, x_{i-1})^\sigma - h_i(x_1, \cdots, x_{i-1})^p}{h_i(x_1, \cdots, x_{i-1})^p}\right)^{-1/m_i} \\ &= x_i^{-p}\sum_{j=0}^{\infty}\binom{-1/m_i}{j}\frac{(h_i(x_1, \cdots, x_{i-1})^\sigma - h_i(x_1, \cdots, x_{i-1})^p)^j}{x_i^{pm_i j}} \in \mathcal{A}^\dagger \otimes_R K \quad (17)\end{aligned}$$

Let $F = \sigma^{\log_p q}$; then F is a lift of the q-power Frobenius, so we may apply the Lefschetz fixed point formula to it and use the result to compute the zeta function of C

Any form can be written as $\sum_{t_1 \geq 0}\sum_{t_2, \cdots, t_n} s_{t_1, \cdots, t_n} x_1^{t_1} \cdots x_n^{t_n} dx_1$. Then, there are $h_i^*(x_1, \cdots, x_{i-1}) \in K[x_1, \cdots, x_{i-1}]$, $i = 2, \cdots, n$, such that

$$\omega_* := \frac{dx_1}{x_2^{m_2 - 1} \cdots x_n^{m_n - 1}} = \frac{dx_2}{h_2^*(x_1) x_3^{m_3 - 1} \cdots x_n^{m_n - 1}} = \cdots = \frac{dx_n}{h_n^*(x_1, \cdots, x_{n-1})} \quad (18)$$

Notice that no common zero in the denominators: otherwise the curve is singular. Then, the denominator $x_2^{m_2 - 1} \cdots x_n^{m_n - 1}$ has degree $\sum_{i=2}^n a_i(m_i - 1)$ equal to $a_1 + 2g - 1$, which means the curve is telescopic (see Theorem 4). Thus, if $t_i > 0$ for $i = 2, \cdots, n$, from the theory in the previous section and (18), they are reduced to the case $-m_i + 1 \leq t_i \leq 0$ for $i = 2, \cdots, n$.

From nonsingularity of C, for any $B \in K[x_1]$ and $t_i, i = 2, \cdots, n$, there exist $U, V \in K[x_1, \cdots, x_{n-1}]$ such that

$$\begin{aligned} & B(x_1) \\ = \ & U(x_1, \cdots, x_{n-1}) h_2(x_1) \cdots h_n(x_1, \cdots, x_{n-1}) \\ & + V(x_1, \cdots, x_{n-1})[c_2 h_2^*(x_1) h_3(x_1, x_2) \cdots h_n(x_1, \cdots, x_{n-1}) \\ & + c_3 x_2 h_3^*(x_1, x_2) h_4(x_1, x_2, x_3) \cdots h(x_1, \cdots, x_{n-1}) + \\ & \cdots + c_n x_2 \cdots x_{n-1} h_n^*(x_1, \cdots, x_{n-1})] \end{aligned} \quad (19)$$

if $c_i \neq 0$ for all $i = 2, \cdots, n$. In fact, each pair of x_i and $h_i^*(x_1, \cdots, x_{i-1})$, $i = 2, \cdots, n$, cannot be zero at the same time, so that we obtain $\bar{U}, \bar{V} \in K[x_1, \cdots, x_{n-1}]$ such that

$$\begin{aligned} 1 = \ & \bar{U}(x_1, \cdots, x_{n-1}) h_2(x_1) \cdots h_n(x_2, \cdots, x_{n-1}) \\ & + \bar{V}(x_1, \cdots, x_{n-1})[c_2 h_2^*(x_1) h_3(x_1, x_2) \cdots h_n(x_1, \cdots, x_{n-1}) \\ & + c_3 x_2 h_3^*(x_1, x_2) h_4(x_1, x_2, x_3) + \cdots + c_n x_2 \cdots x_{n-1} h_n^*(x_1, \cdots, x_{n-1})] \end{aligned}$$

and $U = \bar{U}B, V = \bar{V}B \in K[x_1, \cdots, x_{n-1}]$. On the other hand,

$$\begin{aligned}
0 &\equiv d[\frac{S(x_1, \cdots, x_{n-1})}{x_2^{t_2-m_2} \cdots x_n^{t_n-m_n}}] \\
&= dS(x_1, \cdots, x_{n-1}) x_2^{m_2-t_2} \cdots x_n^{m_n-t_n} \\
&\quad -(t_2 - m_2) S(x_1, \cdots, x_{n-1}) x_2^{m_2-1-t_2} x_3^{m_3-t_3} \cdots x_n^{m_n-t_n} dx_2 \\
&\quad - \cdots - (t_n - m_n) S(x_1, \cdots, x_{n-1}) x_2^{m_2-t_2} \cdots x_{n-1}^{m_{n-1}-t_{n-1}} x_n^{m_n-1-t_n} dx_n \\
&= dS(x_1, \cdots, x_{n-1}) h_2(x_1) \cdots h_n(x_1, \cdots, x_{n-1}) / x_2^{t_2} \cdots x_n^{t_n} \\
&\quad -S(x_1, \cdots, x_{n-1})[\frac{t_2 - m_2}{m_2 - 1} h_2^*(x_1) h_3(x_1, x_2) \cdots h_n(x_1, \cdots, x_{n-1}) \\
&\quad + \frac{t_3 - m_3}{m_3 - 1} x_2 h_3^*(x_1, x_2) h_4(x_1, x_2, x_3) \cdots h_n(x_1, \cdots, x_{n-1}) \\
&\quad + \cdots + \frac{t_n - m_n}{m_n - 1} x_2 \cdots x_{n-1} h_n^*(x_1, \cdots, x_{n-1})] \frac{dx_1}{x_2^{t_2} \cdots x_n^{t_n}} \qquad (20)
\end{aligned}$$

for any $S \in K[x_1, \cdots, x_{n-1}]$ if $t_i \neq m_i$ for all $i = 2, \cdots, n$.

Combining (19) and (20), there exist $U, V \in K[x_1, \cdots, x_{n-1}]$ such that

$$B(x_1) \frac{dx_1}{x_2^{t_2} \cdots x_n^{t_n}} \equiv \frac{U(x_1, \cdots, x_{n-1}) dx_1 + dV(x_1, \cdots, x_{n-1})}{x_2^{t_2-m_2} \cdots x_n^{t_n-m_n}} . \qquad (21)$$

Furthermore, from (18) and (21),

$$\begin{aligned}
dV &= \frac{\partial V}{\partial x_1} dx_1 + \cdots + \frac{\partial V}{\partial x_n} dx_n \\
&= [\frac{\partial V}{\partial x_1} + \frac{\partial V}{\partial x_2} \frac{dx_2}{dx_1} + \cdots + \frac{\partial V}{\partial x_n} \frac{dx_n}{dx_1}] dx_1 \\
&= [\frac{\partial V}{\partial x_1} + \frac{\partial V}{\partial x_2} \frac{h_2^*(x_1)}{x_2^{m_2-1}} + \cdots + \frac{\partial V}{\partial x_n} \frac{h_n^*(x_1, \cdots, x_{n-1})}{x_2^{m_2-1} \cdots x_n^{m_n-1}}] dx_1
\end{aligned}$$

Hence, there exist $B_{s_2, \cdots, s_n} \in K[x_1]$ such that

$$B(x_1) \frac{dx_1}{x_2^{t_2} \cdots x_n^{t_n}} \equiv \sum_{s_2 < t_2, \cdots, s_{n-1} < t_{n-1}} B_{s_2, \cdots, s_n}(x_1) \frac{dx_1}{x_2^{s_2} \cdots x_n^{s_n}} \qquad (22)$$

with $s_n = t_n - m_n$.

Therefore, if $t_i \geq m_i$ for all $i = 2, \cdots, n$, (22) can be applied to reduce the degrees of the denominator. However, even if $0 \leq t_i \leq m_i - 1$ for some i, by multiplying denominator and numerator by $x_i^{m_i}$ and $h_i(x_1)$, respectively, we can keep the degree of x_i between $-m_i + 1$ and 0. In any case, the differential forms are generated by the basis, which consists of $2g$ elements given by Theorem 1 with $w_* = x_2^{m_2-1} \cdots x_n^{m_n-1}$. Also, we notice that for each $k = 2, \cdots, n$, if $m_k \nmid t_k$, then $(s_2, \cdots, s_k) \neq (0, \cdots, 0)$ during the reduction process. Hence, there exist $B'_{s_2, \cdots, s_k} \in K[x_1]$ such that

$$B(x_1) \frac{dx_1}{x_2^{t_2} \cdots x_k^{t_k}} \equiv \sum_{0 \leq s_2 \leq m_2 - 1, \cdots, 0 \leq s_{k-1} \leq m_{k-1} - 1} B'_{s_2, \cdots, s_k}(x_1) \frac{dx_1}{x_2^{s_2} \cdots x_k^{s_k}} \qquad (23)$$

for each $1 \leq s_k \leq m_k$ with $s_k \equiv t_k \bmod m_k$. Therefore, All the forms with $m_k \not| t_k$ are reduced to $x^{M_A(h)}\omega_*$ for some $h \in H(A)$. So, we obtain the following theorem from (17):

Theorem 7 If $p \not| m_2, \cdots, m_n$, then

$$\{\sum_{h\in H(A)} Kx^{M_A(h)}\omega_*\}^\sigma \equiv \sum_{h\in H(A)} Kx^{M_A(h)}\omega_* \,. \tag{24}$$

Let M be the matrix of the action σ, and denote the product by $\mathcal{M} = MM^\sigma M^{\sigma^2}\cdots M^{\sigma^{m-1}}$

Finally, we derive that the number of $\mathbb{F}_q$-rational points in the curve is $q+1-Tr(\mathcal{M})$. In fact, if we define

$$C_i := \{(\bar{x}_1, \cdots, \bar{x}_i) \in \mathbb{F}_q^i | \bar{f}_j(\bar{x}_1, \cdots, \bar{x}_i) = 0, j = 2, \cdots, i\} \cup \{P_\infty\}$$

$C_i^0 := \{(\bar{x}_1, \cdots, \bar{x}_i) \in C_i | \bar{x}_{i+1} = 0\}$, and $C_i^1 := C_i - C_i^0$, we have

$$\begin{aligned}
\#C_i - \#C_{i-1}^0 &= Tr(qF_*^{-1}|K) - Tr(qF_*^{-1}|H^1(k[x_1, x_2, \cdots, x_i, x_2^{-1}, \cdots, x_i^{-1}], K)) \\
&= Tr(qF_*^{-1}|K) - Tr(qF_*^{-1}| \sum_{0\leq s_2\leq m_2-1,\cdots,0\leq s_{i-1}\leq m_{i-1}-1} \frac{K[x]dx}{x_2^{s_2}\cdots x_{n-1}^{s_{i-1}}x_n^{m_i}}) \\
&\quad -Tr(qF_*^{-1}| \sum_{0\leq s_2\leq m_2-1,\cdots,0\leq s_{i-1}\leq m_{i-1}-1,1\leq s_i\leq m_i-1} \frac{K[x]dx}{x_2^{s_2}\cdots x_i^{s_i}}) \\
&= \#C_{i-1}^1 - Tr^{(i)}
\end{aligned}$$

for all $i = 2, \cdots, n$, and $\#C_1 = q+1$ where

$$Tr^{(i)} = Tr(qF_*^{-1}| \sum_{0\leq s_2\leq m_2-1,\cdots,0\leq s_i\leq m_i-1} \frac{K[x]dx}{x_2^{s_2}\cdots x_i^{s_i}}) \,.$$

Hence,

$$\begin{aligned}
\#C_n &= q+1-\sum_{i=2}^{n} Tr^{(i)} \\
&= q+1-Tr(qF_*^{-1}| \sum_{0\leq s_2\leq m_2-1,\cdots,0\leq s_n\leq m_n-1} \frac{K[x]dx}{x_2^{s_2}\cdots x_n^{s_n}}) \\
&= q+1-Tr(qF_*^{-1}| \sum_{h\in H(A)} Kx^{M_A(h)}\omega_*) \,.
\end{aligned}$$

From a similar discussion in Section 2, we obtain $\#C_n = q+1-Tr(\mathcal{M})$.

Example 9 For Example 7, the same basis, shown in Example 5, is obtained as the one Gaudry and Gürel [1] showed for superelliptic curves with two variables.

謝辞: なお、本研究は、文部省科学研究費 基盤研究 (B)(2) 課題番号 13440032 「代数曲線における離散対数問題と情報セキュリティ」(研究代表者: 鈴木譲) の援助を受けている。また、文部省在外研究員で Brown 大学滞在中に Joseph H. Silverman 氏には、この研究のために多くの時間を割いていただいた。

References

[1] F. Gaudry and N. Gürel. "An Extension of Keedlaya's Point-Counting Algorithm to Superelliptic Curves", Asiacrypt 2002.

[2] K. Kedlaya. "Counting Points on Hyperelliptic Curves using Monsky-Washnitzer Cohomology", *J. Ramanujan Math. Soc.* 2001.

[3] S. Miura. *Error Correcting Codes based on Algebraic Curves* (in Japanese). Doctorial Thesis, University of Tokyo, 1998.

[4] P. Monsky and G. Washnitzer, "Formal cohomology. I", *Ann. of Math. (2)* **88** (1968), 181-217.

[5] P. Monsky and G. Washnitzer, "Formal cohomology. III". Fixed point theorems, *Ann. of Math. (2)* **93** (1971), 315-343.

[6] A. Nijenhuis and H. S. Wilf, "Representations of integeres by linear forms in non-negative integers", *J. Number Theory* 4 (1972), 98-106.

[7] R. Schoof, "Elliptic Curves over finite fields and the computation of square roots mod p", *Math Comp* 44 (1985), 483-494.

[8] J. Silverman. *Arithmetic of Elliptic Curves Graduate Texts in Mathematics* **106**. Springer-Verlag, 1986.

[9] H. Stichtenoth. *Algebraic Function Fields and Codes*. Springer-Verlag, 1986.