Generalizing Kedlaya's order counting based on Miura theory

Joe Suzuki

Abstract

K. Kedlaya proposed an method to count the number of $\mathbb{F}_q$-rational points in a hyper-elliptic curve, using the Leschetz fixed points formula in Monsky-Washinitzer Cohomology. The method has been extended to super-elliptic curves (Gaudry and Gürel) immediately, to characteristic two hyper-elliptic curves, and to C_{ab} curves (J. Denef, F. Vercauteren). Based on Miura theory, which is associated with how a curve is expressed as an affine variety, this paper applies Kedlaya's method to so-called strongly telescopic curves which are no longer plane curves and contain super-elliptic curves as special cases.

1 Monsky-Washinitzer Cohomology

Let $k = \mathbb{F}_{q^i}$ for some $i \geq 1$ with $q = p^m$ and p prime, $R = W(k)$ the Witt ring of k, and K the quotient field of R. Let $\bar{\mathcal{A}}$ the coordinate ring of a smooth affine variety over k, $\mathcal{A}$ a smooth R-algebra with $\mathcal{A} \otimes_R k \cong \bar{\mathcal{A}}$, 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 $\bar{\mathcal{A}}$ 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 $z = \sum_{l_1 \cdots l_n} a_{l_1 \cdots l_n} x_1^{l_1} \cdots x_n^{l_n}$ such that

$$l \geq d(z) \Longrightarrow \frac{\min_{l_1 + \cdots + l_n = l} v_p(a_{l_1 \cdots l_n})}{l} > c(z)$$

for some $d(z) \in \mathbb{Z}$ and $c(z) > 0$.

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,

$$\omega = \sum \alpha_{l_1, \cdots, l_r} dx_{l_1} \wedge \cdots \wedge dx_{l_r} \longmapsto d(\omega) = \sum d(\alpha_{l_1, \cdots, l_r}) \wedge dx_{l_1} \wedge \cdots \wedge dx_{l_r} \ ,$$

where $\alpha_{l_1, \cdots, l_r} \in \mathcal{A}^\dagger$, the sum runs over $1 \leq l_1 < \cdots < l_r \leq n$, 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. $H^r(\bar{\mathcal{A}}; K)$, $r = 0, 1, \cdots, n$, are finite dimensional K-vector spaces; and
2. $H^0(\bar{\mathcal{A}}; K) = K$

If we lift the p-power Frobenius $\bar{\sigma}$ 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^i-power Frobenius on $\bar{\mathcal{A}}$. Then, the number of homomorphisms $\bar{\mathcal{A}} \to k$ equals

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

2 Kedlaya's Method

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

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

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

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

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 $x^l dx/y^2$ for $l = 0, \cdots, 2g-1$, and a negative eigenspace $H^1(\bar{\mathcal{A}};K)_-$ generated by $x^l dx/y$ for $l = 0, \cdots, 2g-1$. In fact, using the formula

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

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

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

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

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

For the Monsky-Washnitzer cohomology groups, since $dx \wedge dy = dy \wedge d(1/y) = d(1/y) \wedge dx = 0$ for $\bar{\mathcal{A}}$, we have

1. $H^1(\bar{\mathcal{A}};K) \equiv \Omega$; modulo dx, $x \in \mathcal{A}^\dagger \otimes_R K$; and
2. $H^0(\bar{\mathcal{A}};K) = 0$, $r = 2, 3, \cdots, n$;

Based on the Leschetz fixed point formula, Kedraya showed $q^i + 1 - \#C(k)$ 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 $i > 0$: for another coordinate ring $\bar{\mathcal{A}}' = k[\bar{x}, \bar{y}^{-2}]$ for $\bar{y}^2 = \bar{Q}(\bar{x})$, we have $H^0(\bar{\mathcal{A}}';K) = 0$, $r = 2, 3, \cdots, n$, so that

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

where $d = \#\{(\bar{x}, \bar{y}) \in k^2 | \bar{y}^2 = \bar{Q}(\bar{x}), \bar{y} = 0\}$. (Note that the Leschetz fixed point formula has been applied in the second and last equlities for $\bar{\mathcal{A}}$ and $\bar{\mathcal{A}}'$, 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

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

with $k = \mathbb{F}_{q^i}$ for all $i > 0$. Thus, the eigenvalues of qF_*^{-1} on $H^1(\bar{\mathcal{A}};K)_-$ 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

$$|a_i| \leq \left(\begin{array}{c} 2g \\ i \end{array} \right) q^{i/2} \leq 2^{2g} q^{g/2} \ .$$

Thus to determine the zeta function, it suffices to compute the action of F_* on a suitable basis of $H^1(\bar{\mathcal{A}};K)_-$ 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

Let F/K be an algebraic function field of one variable over K with a place P_∞ of degree one. Without loss of generality, we suppose the set of pole numbers of P_∞, M_{P_∞}, is some monoid $< A >$ generated by n positive integers in $A = \{a_1, \cdots, a_n\}$ such that $a_j \notin < a_1, \cdots, a_{j-1}, a_{j+1}, \cdots, a_n >$ for $1 \leq j \leq n$ and $gcd(a_1, \cdots, a_n) = 1$.

Let $x_j \in F$, $1 \leq j \leq n$, be functions such that $(x_j)_\infty = a_j P_\infty$. Then,

$$\mathcal{L}(\infty P_\infty) := \cup_{m=0}^{\infty}\mathcal{L}(mP_\infty) = K[x_1, \cdots, x_n] .$$

Hence, the mapping

$$\Theta : \begin{cases} K[X_1, \cdots, X_n] & \to & K[x_1, \cdots, x_n] = \mathcal{L}(\infty P_\infty) \\ f(X_1, \cdots, X_n) & \mapsto & f(x_1, \cdots, x_n) \end{cases}$$

gives a surjective homorphism, i.e., $K[X_1, \cdots, X_n]/\mathrm{Ker}\ \Theta \simeq \mathcal{L}(\infty P_\infty)$.

Let $\mathbb{N}$ be the nonnegative integers. We wish to obtain Ker Θ. To this end, we define $\Psi_A : \mathbb{N}^n \to < A >$ by $\Psi_A(s_1, \cdots, s_n) = \sum_{j=1}^n a_j s_j$.

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 $\alpha_1 = \beta_1, \cdots, \alpha_{j-1} = \beta_{j-1}, \alpha_j < \beta_j$ for some $1 \leq j \leq n$.

If we define

$$B(A) := \{\text{the least } M \in \mathbb{N}^n \text{ w.r.t. } C_A \text{ order} | \Psi_A(M) \in < A >\}$$

and

$$V(A) := \{L \in \mathbb{N}^n \backslash B(A) | L = L_1 + L_2, L_1 \in \mathbb{N}^n \backslash B(A)\ L_2 \in \mathbb{N}^n \Longrightarrow L_2 = (0, \cdots, 0)\} ,$$

then one easily checks

$$\mathbb{N}^n \backslash B(A) = V(A) + \mathbb{N}^n .$$

Let $x^M := \Pi_j x_j^{M_j}$ for $M = (M_1, \cdots, M_n) \in \mathbb{N}^n$. Since $\Psi_A : B(A) \to < A >$ is bijective and $\dim_k(\mathcal{L}((l+1)P_\infty)/\mathcal{L}(lP_\infty)) \leq \deg P_\infty = 1$ for each $l \geq 0$, $\{x^m | m \in B(A)\}$ is a k-basis of $\mathcal{L}(\infty P_\infty)$. Furthermore, for each $M \in \mathbb{N}^n \backslash B(A)$, there exists a relation such that

$$x^M + \alpha_L x^L + \sum_{N \in B(A), \Psi_A(N) < \Psi_A(L)} \alpha_N x^N = 0 \ , \tag{3}$$

where L is the unique element in $B(A)$ satisfying $\Psi_A(M) = \Psi_A(L)$, and $\alpha_L \neq 0$, $\alpha_N \in K$.

Let

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

where we donote $\Pi_j X_j^{m_j}$ by X^M for $M = (m_1, \cdots, m_n) \in \mathbb{N}^n$. Then, we have

Theorem 2 (Miura [3])

$$\text{Ker } \Theta = \{F^{(M)} | M \in V(A)\} \ .$$

The affine algebraic set Ker Θ associated with $(F/K, P_\infty)$ is a smooth affine variety with coordinate ring $K[x_1, \cdots, x_n]$.

Example 1 (C_{ab} curves) $A = \{a, b\}$ 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 $s, t \in \mathbb{Z}$, respectively, we can set $\alpha_{ab} = 1$. (Note $gcd(a, b) = 1$). If $\alpha_{ma+lb} = 0$ for $l \neq 0$ ($gcd(a_1, p) = 1$ is required), the curve is called *super-elliptic*.

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 $\beta_i, \gamma_j \in K$.

Without loss of generality, we fix an element $a_1 \in A$ such that $(a_1, p) = 1$. Such an a_1 exists because the number of gaps, g, is finite, and $(a_j, p) = 1$ for some j. Let b_l denote the minimal $b \in < a_2, \cdots, a_n >$ such that $b \equiv l \bmod a_1$, $l = 0, 1, \cdots$. Clearly, $b_l = b_{l+ma_1}$ for $m = 0, 1, \cdots$.

Let $T(A) := \{(s_1, s_2, \cdots, s_n) \in B(A) | s_1 = 0\}$. Then,

Theorem 3 (Miura [3])

$$T(A) = \{M \in B(A) | \Psi_A(M) = b_l, l = 0, 1, \cdots, a_1 - 1\} , \tag{5}$$

$\#T(A) = a_1$, and $\{x^M | M \in T(A)\}$ is a $K[x_1]$-basis of $K[x_1, \cdots, x_n]$.

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

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

for $y^a = x^b + \sum_{ma+lb<ab} \alpha_{ma+lb} x^m y^l$, where $\alpha_{ma+lb} \in K$.

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

$$K[x, y, z] = K[x] + K[x]z + K[x]y + K[x]yz$$

for

$$\begin{aligned} y^2 &= \beta_{12}x^3 + \beta_{11}yz + \beta_{10}xy + \beta_9 xz + \beta_6 y + \beta_5 z + \beta_4 x + \beta_0 \\ z^2 &= \gamma_{10}xy + \gamma_9 xz + \gamma_6 y + \gamma_3 z + \gamma_4 x + \gamma_0 \ , \end{aligned}$$

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

Proposition 1

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

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

$$a_j / d_j \in < a_1 / d_{j-1}, \cdots, a_{j-1} / d_{j-1} > , \tag{7}$$

where $d_j = gcd(a_1, \cdots, a_j)$, is said to be *telescopic.* Furthermore, any curve with a K-rational point P_∞ such that

1. $\mathcal{M}_{P_\infty} = A$
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 $\mathcal{M}_{P_\infty} = A$ is telescopic for A.

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

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

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. $T(A) = \{(0, t_2, \cdots, t_n) | 0 \leq t_j \leq d_{j-1}/d_j - 1, j = 2, \cdots, n\}$
2. $V(A) = \{(0, \cdots, 0, d_{j-1}/d_j, 0, \cdots, 0) | j = 2, \cdots, n\}$.

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 Ker $\Theta = \{F^{(M)} | M \in V(A)\}$ is given by

$$\{\bar{F}_j(X_1, \cdots, X_j) | j = 2, 3, \cdots, n\}$$

for some $\bar{F}_j := X_j^{d_{j-1}/d_j} - h_j(X_1, \cdots, X_{j-1})$, $h_j \in k[X_1, \cdots, X_{j-1}]$, $j = 2, \cdots, n$, then the curve is said to be *strongly telescopic.*

4 Cohomology of Smooth Curves

We consider the coordinate ring $\bar{\mathcal{A}} = k[\bar{x}_1, \bar{x}_2, \cdots, \bar{x}_n, \bar{x}_2^{-1}, \cdots, \bar{x}_n^{-1}]$ for some

$$\bar{F}_j(\bar{x}_1, \cdots, \bar{x}_n) = 0 \ ,$$

$j = 2, \cdots, n$, and assume that the curve is smooth. Let $\mathcal{A} = R[x_1, x_2, \cdots, x_n, x_2^{-1}, \cdots, x_n^{-1}]$ such that $\mathcal{A} \otimes_R k \cong \bar{\mathcal{A}}$, and $\mathcal{A}^\dagger$ the weak completion of $\mathcal{A}$.

For monomial $\bar{x}_1^{l_1} \cdots \bar{x}_n^{l_n}$ with $(\bar{x}_1)_\infty = a_1, \cdots, (\bar{x}_n)_\infty = a_n$ and $l_1, \cdots, l_n \in \mathbb{N}$, we define for $A = \{a_1, \cdots, a_n\}$

$$\Psi(\bar{x}_1^{l_1} \cdots \bar{x}_n^{l_n}) := \Psi_A(l_1, \cdots, l_n) \ ,$$

which is extended for polynomial $\sum_j r_j \bar{x}_1^{l_{j1}} \cdots \bar{x}_n^{l_{jn}} \in k[\bar{x}_1, \cdots, \bar{x}_n]$ with $r_j \in k$ and $l_{j1}, \cdots, l_{jn} \in \mathbb{N}$, as

$$\Psi(\sum_j r_j \bar{x}_1^{l_{j1}} \cdots \bar{x}_n^{l_{jn}}) := \max_j \Psi(\bar{x}_1^{l_{j1}} \cdots \bar{x}_n^{l_{jn}}) \ .$$

Let F_j be the lifted polinomial associated with $\bar{F}_j$, $j = 2, \cdots, n$. From the equations $dF_j = 0$, $j = 2, \cdots, n$, 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 $f_j(x_1, \cdots, x_n) = 0$, $j = 1, \cdots, n$, have no common zero. This is possible because, if $f_j = t f_j^*$ at $P \in \mathbb{P}_F$ with $v_P(f_j^*) = 0$ for $j = 1, \cdots, n$, where t is a uniformaizer at P, then we can replace f_j by f_j^*. Since, if $P \neq P_\infty$, $v_P(dx_j) \geq 0$ and $v_P(f_j) \geq 0$, and since $deg(w_*) = 2g-2$, we have

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

Since (f_j) is a principle divisor, $\Psi(f_j) = a_i + 2g - 1$.

In this section, we find $2g$ independent elements in $H^1(\bar{\mathcal{A}}; K)$ over K. Hereafter, we denote $\omega \equiv 0$ if differntial $\omega \in \Omega$ is exact, say $H^1(\bar{\mathcal{A}}; K) \equiv \Omega$. 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 $i = 1, \cdots, n$.

For $b \in < A >$, let $M_A(b)$ denote the $M \in B(A)$ such that $\Psi_A(M) = b$.

Theorem 6

$$K[x_1, \cdots, x_n]\omega_* \equiv \sum_{h \in H(A)} K x^{M_A(h)} \omega_*$$

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

Proof. From Theorem 3,

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

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

$$\omega_* = \frac{dx_1^j y_l}{g_{j,l}(x_1, y_1 \cdots, y_{a_1 - 1})} \tag{11}$$

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

$$\Psi(g_{j,l}) = j a_1 + b_l + 2g - 1 \ . \tag{12}$$

From $dx_1^j y_l \equiv 0$ with $(j, l) \in G(a_1)$, $c x^{M_A(j a_1 + b_l + 2g - 1)} \omega_*$ with $c \in K$ can be reduced to lower degree terms. Hence, Ω modulo exact differentials is spanned by $\{x^{M_A(h)} \omega_* | h \in H(A)\}$.

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

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

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

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

if $2g - 1 \in < A >$ ($2g-1$ is a nongap), and

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

if $2g - 1 \notin < A >$ ($2g-1$ is a gap). $\Box$

Example 7 If $A=\{a,b\}$ with $gcd(a,b)=1$, Proposition 1 implies $g=(a-1)(b-1)/2$, 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

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

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

$$Y^a=X^b+\sum_{j=0}^{b-1}\alpha_{ja}X^j\ . \tag{13}$$

Then, $\omega_*=\dfrac{dx}{ay^{a-1}}$, and $K[x,y]\omega_*$ for (13) is generated by $\{x^j\dfrac{dx}{y^l}|0\le j\le b-2, 1\le l\le a-1\}$ 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

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

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

$$y^2=x^3+x+1,\ z^2=xy+x+1\ , \tag{14}$$

then

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

and $K[x,y,z]\omega_*$ for (14) is generated by

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

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

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 $k[\bar{x}_1,\bar{x}_2,\cdots,\bar{x}_n,\bar{x}_2^{-1},\cdots,\bar{x}_n^{-1}]$ for $\bar{I}$.

We fix $\mathcal{A} = R[x_1, x_2, \cdots, x_n, x_2^{-1}, \cdots, x_n^{-1}]$ for 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 $h_j \in R[x_1, \cdots, x_{j-1}]$, $j = 2, \cdots, n$, 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 $x_2^\sigma - x_2^p, \cdots, x_{j-1}^\sigma - x_{j-1}^p$, then p divides

$$x_j^\sigma - x_j^p = h_j(x_1, \cdots, x_{j-1})^\sigma - h_j(x_1, \cdots, x_{j-1})^p \ .$$

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

$$\begin{aligned} x_j^\sigma &= x_j^p (1 + \frac{h_j(x_1, \cdots, x_{j-1})^\sigma - h_j(x_1, \cdots, x_{j-1})^p}{h_j(x_1, \cdots, x_{j-1})^p})^{1/m_j} \\ &= x_j^p \sum_{l=0}^{\infty} \binom{1/m_i}{j} \frac{(h_j(x_1, \cdots, x_{j-1})^\sigma - h_j(x_1, \cdots, x_{j-1})^p)^l}{x_j^{pm_j l}} \in \mathcal{A}^\dagger \otimes_R K \ . \end{aligned} \tag{17}$$

$$\begin{aligned} (x_j^{-1})^\sigma &= x_j^{-p} (1 + \frac{h_j(x_1, \cdots, x_{j-1})^\sigma - h_j(x_1, \cdots, x_{j-1})^p}{h_j(x_1, \cdots, x_{j-1})^p})^{-1/m_j} \\ &= x_j^{-p} \sum_{l=0}^{\infty} \binom{-1/m_i}{j} \frac{(h_j(x_1, \cdots, x_{j-1})^\sigma - h_j(x_1, \cdots, x_{j-1})^p)^l}{x_j^{pm_j l}} \in \mathcal{A}^\dagger \otimes_R K \ . \end{aligned} \tag{18}$$

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 $h_j^*(x_1, \cdots, x_{j-1}) \in K[x_1, \cdots, x_{j-1}]$, $j = 2, \cdots, n$, such that

$$\omega_* := \frac{dx_1}{x_2^{m_2-1} \cdots x_n^{m_n-1}} = \frac{dx_2}{h_2^*(x_1) x_3^{m_3-1} \cdots x_n^{m_n-1}} = \cdots = \frac{dx_n}{h_n^*(x_1, \cdots, x_{n-1})} \tag{19}$$

and no common zero in the denominators. Then, the denominator $x_2^{m_2-1} \cdots x_n^{m_n-1}$ has degree $\sum_{j=2}^n a_j(m_j - 1)$ equal to $a_1 + 2g - 1$, which means the curve is telescopic (see Theorem 4). Thus, if $t_j \geq 0$ for $j = 2, \cdots, n$, from the theory in the previous section and (19), they are reduced to some in $\sum_{h \in H(A)} K x^{M_A(h)} \omega_*$.

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

$$B(x_1)$$

$$
\begin{aligned}
&= U(x_1,\cdots,x_{n-1})h_2(x_1)\cdots h_n(x_1,\cdots,x_{n-1}) \\
&\quad +V(x_1,\cdots,x_{n-1})[c_2h_2^*(x_1)h_3(x_1,x_2)\cdots h_n(x_1,\cdots,x_{n-1}) \\
&\quad +c_3x_2h_3^*(x_1,x_2)h_4(x_1,x_2,x_3)\cdots h(x_1,\cdots,x_{n-1})+ \\
&\quad \cdots+c_nx_2\cdots x_{n-1}h_n^*(x_1,\cdots,x_{n-1})]
\end{aligned} \tag{20}
$$

if $c_j \neq 0$ for some $j=2,\cdots,n$. In fact, each pair of x_j and $h_j^*(x_1,\cdots,x_{j-1})$, $j=2,\cdots,n$, 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

$$
\begin{aligned}
1 &= \bar{U}(x_1,\cdots,x_{n-1})h_2(x_1)\cdots h_n(x_2,\cdots,x_{n-1}) \\
&\quad +\bar{V}(x_1,\cdots,x_{n-1})[c_2h_2^*(x_1)h_3(x_1,x_2)\cdots h_n(x_1,\cdots,x_{n-1}) \\
&\quad +c_3x_2h_3^*(x_1,x_2)h_4(x_1,x_2,x_3)+\cdots+c_nx_2\cdots x_{n-1}h_n^*(x_1,\cdots,x_{n-1})]
\end{aligned}
$$

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

$$
\begin{aligned}
0 &\equiv d[\frac{S(x_1,\cdots,x_{n-1})}{x_2^{t_2-m_2}\cdots x_n^{t_n-m_n}}] \\
&= dS(x_1,\cdots,x_{n-1})x_2^{m_2-t_2}\cdots x_n^{m_n-t_n} \\
&\quad -(t_2-m_2)S(x_1,\cdots,x_{n-1})x_2^{m_2-1-t_2}x_3^{m_3-t_3}\cdots x_n^{m_n-t_n}dx_2 \\
&\quad -\cdots-(t_n-m_n)S(x_1,\cdots,x_{n-1})x_2^{m_2-t_2}\cdots x_{n-1}^{m_{n-1}-t_{n-1}}x_n^{m_n-1-t_n}dx_n \\
&= dS(x_1,\cdots,x_{n-1})h_2(x_1)\cdots h_n(x_1,\cdots,x_{n-1})/x_2^{t_2}\cdots x_n^{t_n} \\
&\quad -S(x_1,\cdots,x_{n-1})[\frac{t_2-m_2}{m_2-1}h_2^*(x_1)h_3(x_1,x_2)\cdots h_n(x_1,\cdots,x_{n-1}) \\
&\quad +\frac{t_3-m_3}{m_3-1}x_2h_3^*(x_1,x_2)h_4(x_1,x_2,x_3)\cdots h_n(x_1,\cdots,x_{n-1}) \\
&\quad +\cdots+\frac{t_n-m_n}{m_n-1}x_2\cdots x_{n-1}h_n^*(x_1,\cdots,x_{n-1})]\frac{dx_1}{x_2^{t_2}\cdots x_n^{t_n}}
\end{aligned} \tag{21}
$$

for any $S \in K[x_1,\cdots,x_{n-1}]$ if $t_j \neq m_j$ for some $j=2,\cdots,n$.

Combining (20) and (21), there exist $U,V \in K[x_1,\cdots,x_{n-1}]$ such that

$$
B(x_1)\frac{dx_1}{x_2^{t_2}\cdots x_n^{t_n}} \equiv \frac{U(x_1,\cdots,x_{n-1})dx_1+dV(x_1,\cdots,x_{n-1})}{x_2^{t_2-m_2}\cdots x_n^{t_n-m_n}}\ . \tag{22}
$$

Furthermore, from (19) and (22),

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

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

$$
B(x_1)\frac{dx_1}{x_2^{t_2}\cdots x_n^{t_n}} \equiv \sum_{s_2<t_2,\cdots,s_{n-1}<t_{n-1}} B_{s_2,\cdots,s_n}(x_1)\frac{dx_1}{x_2^{s_2}\cdots x_n^{s_n}} \tag{23}
$$

with $s_n = t_n - m_n$.

Therefore, if $t_j \geq m_j$ for all $i = 2, \cdots, n$, (23) can be applied to reduce the degrees of the denominator. If $0 \leq t_j \leq m_j - 1$ for some j, by multiplying denominator and numerator by $x_j^{m_j}$ and $h_j(x_1)$, respectively, we can keep the degree of x_j between $-m_j + 1$ and 0. If $m_l \leq t_l$ for some $2 \leq l \leq j - 1$ and $0 \leq t_j \leq m_j - 1$, then multiply denominator and numerator by $x_j^{m_j}$ and $h(x_1, \cdots, x_{j-1})$, respectively. In any case, the differential forms are generated by the basis, which consists of $2g$ elements given by Theorem 1 with $w_* = x_2^{m_2-1} \cdots x_n^{m_n-1}$. Even if $t_{j+1} = \cdots = t_n = 0$, if $m_j \not| t_j$, there exist $B'_{s_2,\cdots,s_j} \in K[x_1]$ such that

$$B(x_1)\frac{dx_1}{x_2^{t_2} \cdots x_j^{t_j}} \equiv \sum_{0 \leq s_2 \leq m_2-1, \cdots, 0 \leq s_j \leq m_j-1} B'_{s_2,\cdots,s_j}(x_1)\frac{dx_1}{x_2^{s_2} \cdots x_j^{s_j}} \ . \tag{24}$$

Notice that the degrees of x_j and x_j^{-1} in x_j^σ and $(x_j^{-1})^\sigma$ are $-pm_jl + 1$ and $-pm_jl - 1$, $l = 0, 1, \cdots$, and that they cannot be divided by m_j. Also, $(dx_1)^\sigma = x_1^{p-1} dx_1$. This implies:

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

$$\{\sum_{h \in H(A)} Kx^{M_A(h)}\omega_*\}^\sigma \equiv \sum_{h \in H(A)} Kx^{M_A(h)}\omega_* \ . \tag{25}$$

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 k-rational points in the curve is $q^i + 1 - Tr(\mathcal{M})$. In fact, if we define for $j = 2, \cdots, n$,

$$C_j := \{(\bar{x}_1, \cdots, \bar{x}_j) \in k | \bar{F}_l(\bar{x}_1, \cdots, \bar{x}_l) = 0, l = 2, \cdots, j\} \cup \{P_\infty\}$$

$C_j^0 := \{(\bar{x}_1, \cdots, \bar{x}_j) \in C_j | \bar{x}_j = 0\}$, and $C_j^1 := C_{j-1} - C_j^0$, we have

$$\begin{aligned}
\#C_j - \#C_j^0 &= Tr(q^i F_*^{-i}|K) - Tr(q^i F_*^{-i}|H^1(k[x_1, x_2, \cdots, x_j, x_2^{-1}, \cdots, x_j^{-1}]/(\bar{I}), K)) \\
&= Tr(q^i F_*^{-i}|K) - Tr(q^i F_*^{-i}| \sum_{0 \leq s_2 \leq m_2-1, \cdots, 0 \leq s_{j-1} \leq m_{j-1}-1} \frac{K[x]dx}{x_2^{s_2} \cdots x_{j-1}^{s_{j-1}} x_j^{m_j}}) \\
&\quad -Tr(q^i F_*^{-i}| \sum_{0 \leq s_2 \leq m_2-1, \cdots, 0 \leq s_{j-1} \leq m_{j-1}-1, 1 \leq s_j \leq m_j-1} \frac{K[x]dx}{x_2^{s_2} \cdots x_j^{s_j}}) \\
&= \#C_j^1 - Tr^{(j)}
\end{aligned}$$

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

$$Tr^{(j)} = Tr(q^i F_*^{-i}| \sum_{0 \leq s_2 \leq m_2-1, \cdots, 1 \leq s_i \leq m_j-1} \frac{K[x]dx}{x_2^{s_2} \cdots x_j^{s_j}}) \ ,$$

and Leschetz fixed point formula has been applied in the first and last equations as $\bar{\mathcal{A}} = k[x_1, x_2, \cdots, x_j, x_2^{-1}, \cdots, x_j^{-1}]$ for $\bar{I}$ and $\bar{\mathcal{A}} = k[x_1, x_2, \cdots, x_j, x_2^{-1}, \cdots, x_{j-1}^{-1}, x_j^{-m_j}]$ for $\bar{I}$.

Hence,

$$
\begin{aligned}
\#C_n &= q^i + 1 - \sum_{j=2}^{n} Tr^{(j)} \\
&= q^i + 1 - Tr(q^i F_*^{-i}| \sum_{0\le s_2\le m_2-1,\cdots,0\le s_n\le m_n-1} \frac{K[x_1]dx_1}{x_2^{s_2}\cdots x_n^{s_n}}) \\
&= q^i + 1 - Tr(q^i F_*^{-i}| \sum_{h\in H(A)} Kx^{M_A(h)}\omega_*) \ .
\end{aligned}
$$

From a similar discussion in Section 2, we obtain the number of $\mathbb{F}_q$-rational points $\#C_n$ to be $q+1-Tr(\mathcal{M})$.

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.

Acknowledgements: This work was partially done while the author was staying in Brown University (2001-2002). Discussion with Professor Joseph H. Silverman was helpful.

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 nonnegative 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.

[10] J. Denef, F. Vercauteren. "Computing zeta functions of C_{ab} curves using Monsky-Washnitzer cohomology". Preprint October 2003