Ark. Mat., **59** (2021), 229–246
DOI: 10.4310/ARKIV.2021.v59.n1.a9

On the existence of curves with prescribed a-number

Zijian Zhou

Abstract. We study the existence of Artin-Schreier curves with large a-number. We show that Artin-Schreier curves with large a-number can be written in certain forms and discuss their supersingularity. We also give a basis of the de Rham cohomology of Artin-Schreier curves. By computing the rank of the Hasse-Witt matrix of the curve, we also give bounds on the a-number of trigonal curves of genus 5 in small characteristic.

1. Introduction

Let k be an algebraically closed field of characteristic $p>0$. By a curve we mean a smooth irreducible projective curve defined over k. Let X be a curve defined over k and $\mathrm{Jac}(X)$ be its Jacobian. Such a curve has several invariants, e.g. the a-number and the p-rank. The a-number of the curve X is defined as $a_X = \dim_k(\mathrm{Hom}(\alpha_p, \mathrm{Jac}(X)))$ with α_p the group scheme which is the kernel of Frobenius on the additive group scheme $\mathbb{G}_a$. The a-number of X is equal to $g-r$ where g is the genus of X and r is the rank of the Cartier-Manin matrix, that is, the matrix for the Cartier operator defined on $H^0(X, \Omega^1_X)$. We refer to [3] and [14] for the properties of the Cartier operator. The p-rank of a curve X is the number f_X such that $\#\mathrm{Jac}(X)[p](k)=p^{f_X}$. One sees that $1\leq a_X+f_X\leq g$. Moreover, a curve is called supersingular if its Jacobian is isogenous to a product of supersingular elliptic curves.

A curve X of genus g is called superspecial if $a_X=g$. Ekedahl [5] showed that for a superspecial curve X one has $g\leq p(p-1)/2$. It is known that the locus of principally polarized abelian varieties with given a-number a has codimension

Key words and phrases: Cartier operator, Cartier-Manin matrix, Hasse-Witt matrix, Artin-Schreier curve, trigonal curve, a-number.
2010 Mathematics Subject Classification: 11G20, 15B33, 14H05, 14F40.

$a(a+1)/2$ in the moduli space $\mathcal{A}_g \otimes \mathbb{F}_p$ of principally polarized abelian varieties of dimension g, see [12, Corollary 5.4]. It is interesting to see how these loci intersect the Torelli locus of Jacobian varieties. The cases with $a=g$ or close to g are here of special interest. For hyperelliptic curves with $p=2$, Elkin and Pries [7] gave a complete description of their a-numbers. For an Artin-Schreier curve X, that is, a $\mathbb{Z}/p\mathbb{Z}$-Galois cover of $\mathbb{P}^1$, Farnell and Pries [8] first gave non-trivial examples of families of Artin-Schreier curves with constant a-number. Booher and Cais [2] gave upper and lower bounds for a-numbers of Artin-Schreier curves.

For an Artin-Schreier curve of genus g with $p=2$ and $a_X=g-1$, it was known that the curve has genus $g\leq 3$ [15, Corollary 3.2] and can be written as certain form [7, Theorem 1.2]; for $p\geq 3$, we show that an Artin-Schreier curve with a-number $g-1$ has genus $g\leq p(p-1)/2$ and can be written as $y^p-y=f(x)$ with $f(x)$ a polynomial whose degree divides $p+1$, see Proposition 2.2. Moreover, we have the following.

Theorem 1.1. *Let k be an algebraically closed field with* $\mathrm{char}(k)=p\geq 3$. *Let X be an Artin-Schreier curve of genus $g>0$ with equation $y^p-y=f(x)$. If $a_X=g-1$, then $f(x)\in k[x]$ and if $d=\deg f(x)$ then either $p=5, d=3$ and X is isomorphic to a supersingular curve of genus 4 with equation*

$$y^5-y=x^3+a_1x, \quad a_1\neq 0\,, \tag{1}$$

or $p=3, d=4$ and X is isomorphic to a supersingular curve of genus 3 with equation

$$y^3-y=x^4+a_2x^2, \quad a_2\neq 0\,. \tag{2}$$

Note that for a curve X with $a_X=g-1$, we have $f_X=0$ or 1 since $a_X+f_X\leq g$. Moreover by the Deuring-Shafarevich formula [16], an Artin-Schreier curve X has p-rank $(m-1)(p-1)$, where m is the number of branch points. Hence it is not possible for Artin-Schreier curves to have $a_X=g-1$ and $f_X=1$ when p is odd. We prove these results mainly by explicitly calculating the action of the Cartier operator on a basis of holomorphic differential forms. To show the supersingularity we use the de Rham cohomology.

Let X be an Artin-Schreier curve with $a_X=g-2$. Then for $p\geq 5$, by the Deuring-Shafarevich formula the curve X can be written as $y^p-y=f(x)$ with $f(x)$ a polynomial. For $p=3$, we give an explicit form of X, see Proposition 2.5. Moreover, we have the following.

Proposition 1.2. *Let X be an Artin-Schreier curve of genus $g>0$ given by an equation $y^p-y=f(x)$, where $f(x)\in k[x]$ and* $\deg f(x)=d$. *If $d\,|\,p+1$ and $a_X=g-2$, then $p=7, d=4$ and X is isomorphic to the supersingular curve of genus 9 with equation*

$$y^7-y=x^4+a_1x, \quad a_1\in k^*\,.$$

Recall that a result of Re [13] states that if X is a non-hyperelliptic curve of genus g, then

$$a_X \leq \frac{p-1}{p+1}\left(\frac{2g}{p}+g+1\right).$$

The following results improve Re's bound for trigonal curves of genus 5 in low characteristics. Note that a trigonal curve of genus 5 is not hyperelliptic; see, for example, [10, Section 2.1].

Theorem 1.3. *Let k be an algebraically closed field of characteristic 2. If X is a trigonal curve of genus 5 defined over k, then $a_X \leq 2$.*

Theorem 1.4. *Let k be an algebraically closed field of characteristic 3. If X is a trigonal curve of genus 5 defined over k, then $a_X \leq 3$.*

For $g=5$ and $p=2$, Re's bound says that $a_X \leq 3$, while our result implies that $a_X \leq 2$. Also for $g=5$ and $p=3$, Re's bound says that $a_X \leq 4$, while our result implies $a_X \leq 3$.

2. On the existence of Artin-Schreier curves with prescribed *a*-number

Let $\operatorname{char}(k)=p\geq 3$. Before giving the proof of Theorem 1.1, we recall and prove several results needed for Theorem 1.1 and give a basis of the de Rham cohomology for Artin-Schreier curves.

Since $a_X+f_X\leq g$, a superspecial curve has p-rank 0. Moreover for superspecial Artin-Schreier curves we have the following result of Irokawa and Sasaki [9].

Theorem 2.1. *Let k be an algebraically closed field of $\operatorname{char}(k)=p\geq 3$. Let X be a superspecial Artin-Schreier curve with equation $y^p-y=f(x)$, where $f(x)\in k[x]$ and $\deg f(x)=d\geq 2$ with $\gcd(p,d)=1$. Then X is isomorphic to a curve given by $y^p-y=x^d$ with $d|p+1$.*

For the next step, $a_X=g-1$, we have the following.

Proposition 2.2. *Let k be an algebraically closed field with $\operatorname{char}(k)=p>0$. Let X be an Artin-Schreier curve of genus $g\geq 1$. If $a_X=g-1$, then*

(1) *if $p=2$, then $g\leq 3$ and the curve X can be either written as $y^2+y=f(x)$, where $f(x)\in k[x]$ and $\deg f(x)=5$ or 7, or as $y^2+y=f_0(x)+1/x$ with $\deg f_0(x)=1$ or 3 and $f_0(x)\in xk[x]$;*

(2) *if $p\geq 3$, then $g\leq (p-1)p/2$ and X is isomorphic to a curve with equation*

$$y^p-y=x^d+a_{d-2}x^{d-2}+\ldots+a_1x,$$

where $d\,|\,p+1$. Moreover if $d=p+1$, then at least one of the a_i with $2\leq i\leq d-2$ is non-zero. If $d<p+1, d\mid p+1$, then at least one of the a_i with $1\leq i\leq d-2$ is non-zero.

Proof. Part (1) of Proposition 2.2 was known, see for example [7, Theorem 1.2]. Here we only give a proof of part (2).

Suppose that $f(x)$ has poles at $\infty, Q_1, \ldots, Q_m$ for some $m \in \mathbb{Z}_{\geq 0}$. Let $x - \xi_i$ be a local parameter at Q_i. Write $x_i = 1/(x - \xi_i)$ for $i = 1, \ldots, m$ and $x_0 = x$. Then $f(x)$ can be written as

$$f(x) = f_0(x) + \sum_{i=1}^{m} f_i(1/(x - \xi_i)) = \sum_{i=0}^{m} f_i(x_i)\,, \tag{3}$$

where $\deg f_i(x) = d_i$. By [17, Lemma 1], a basis of $H^0(X, \Omega_X^1)$ is given by $B = \cup_{s=0}^{m} B_s$ where

$$\begin{aligned} B_0 &= \{x^i y^j \,\mathrm{d}x | i, j \in \mathbb{Z}_{\geq 0},\ ip + jd \leq (p-1)(d_0 - 1) - 2\}, \\ B_s &= \{x_s^i y^j \,\mathrm{d}x |\ i \in \mathbb{Z}_{\geq 1}, j \in \mathbb{Z}_{\geq 0},\ ip + jd \leq (p-1)(d_s + 1)\}, \quad s = 1, \ldots, m\,. \end{aligned}$$

The condition $a_X = g - 1$ is equivalent to the rank of the Cartier operator $\mathrm{rank}(\mathcal{C})$ being equal to 1. Note that if $f(x) = \sum_{i=0}^{m} f_i(x_i)$ as in (3), we always have $x_s \,\mathrm{d}x \in B$ for $1 \leq s \leq m$. Note that $\mathcal{C}(x_s \,\mathrm{d}x) \neq 0$ and we get $\mathrm{rank}(\mathcal{C}) \geq m$.

If $p \geq 3$, then by the Deuring-Shafarevich formula, the p-rank of X is 0 since the a-number of X is $g - 1$. We show the following:

(a) For all $p \geq 3$, we have $d \leq p + 1$;

(b) If $p = 5$ and $d = 4$, then $\mathrm{rank}(\mathcal{C}) \geq 2$;

(c) If $p \geq 7$ and $d \geq 3$ with $d \nmid p + 1$, then $\mathrm{rank}(\mathcal{C}) \geq 2$.

Then by a change of coordinates and by Theorem 2.1, one can easily prove the existence of non-zero coefficients in f. After excluding the cases where $\mathrm{rank}(\mathcal{C}) \geq 2$ or $\mathrm{rank}(\mathcal{C}) = 0$, what is left are curves with a-number $g - 1$. Note that if $d = 2$ and $f(x) \in k[x]$, the curve with equation $y^p - y = f(x)$ is superspecial.

By a change of coordinates, we may assume

$$f(x) = x^d + a_{d-2} x^{d-2} + \ldots + a_1 x + a_0, \quad d \geq 3\,.$$

Then a basis of $H^0(X, \Omega_X^1)$ is

$$B = B_0 = \{x^i y^j \,\mathrm{d}x |\ i, j \in \mathbb{Z}_{\geq 0}, pi + jd \leq (p-1)(d-1) - 2\}.$$

(a) If $d \geq p + 2$, then by definition we have $x^{p-1} \,\mathrm{d}x \in B$. There exist $l, b \in \mathbb{Z}_{\geq 0}$ such that $d = lp + b$ with $l = 1$ and $2 \leq b \leq p - 1$ or $l \geq 2$ and $1 \leq b \leq p - 1$. One can show $x^{p-1-b} y \,\mathrm{d}x \in B$ by checking $(p - 1 - b)p + d \leq (p - 1)(d - 1) - 2$. Then

$$\begin{aligned} \mathcal{C}(x^{p-1-b} y \,\mathrm{d}x) &= \mathcal{C}(x^{p-1-b}(y^p - f(x)) \,\mathrm{d}x) \\ &= y\mathcal{C}(x^{p-1-b} \,\mathrm{d}x) - \mathcal{C}(x^{p-1-b} f(x) \,\mathrm{d}x) \neq 0 \end{aligned}$$

as the leading term of $x^{p-1-b} f(x)$ is x^{lp+p-1}. This contradiction shows that $d \leq p + 1$.

(b) For $p=5$, by (a) we have $d\leq p+1$. If $d\nmid p+1$, then $d=4$ and $y^1\,\mathrm{d}x, y^2\,\mathrm{d}x\in B$. Additionally, we have $\mathcal{C}(y^i\,\mathrm{d}x)=y^{i-1}\,\mathrm{d}x$ for $i=1,2$ and hence $\operatorname{rank}(\mathcal{C})\geq 2$, a contradiction. We therefore have $d|p+1$.

(c) For $p\geq 7$ and $d\leq p+1$, assume we have $d\nmid p+1$. Then there exists $l\in\mathbb{Z}_{>0}$ such that $ld\leq p\leq (l+1)d$. Furthermore, we have $ld\leq p-1$ and $(l+1)d\geq p+2$ as $\gcd(d,p)=1$ and $d\nmid p+1$. Then there exists b' satisfying $ld+b'=p-1$ for $0\leq b'\leq d-3$.

If $d=p-1$, then $l=1$, $b'=0$, we get $y\,\mathrm{d}x$, $y^2\,\mathrm{d}x\in B$ and $\mathcal{C}(y^i\,\mathrm{d}x)=y^{i-1}\,\mathrm{d}x$ for $i=1,2$. This implies $\operatorname{rank}(\mathcal{C})\geq 2$, a contradiction. If $d=p-2$, $l=1$ and $b'=1$, then we have $i(p-1)\leq(p-1)(p-2)-2$, which implies $xy\,\mathrm{d}x$, $xy^2\,\mathrm{d}x\in B$. Then $\mathcal{C}(xy\,\mathrm{d}x)$ and $\mathcal{C}(xy^2\,\mathrm{d}x)$ are linearly independent and hence $\operatorname{rank}(\mathcal{C})\geq 2$. Now if $d\leq p-3$, we show that $x^{b'}y^l\,\mathrm{d}x\in B$. This is equivalent to showing $ld+b'p\leq(p-1)(d-1)-2$. By substituting b' with $b'=p-1-ld$ in the inequality, we only need to show $d(l+1)(p-1)\geq p^2+1$, which is clear since $(l+1)d\geq p+2$.

Now we show that $x^{b'}y^l\,\mathrm{d}x, x^{b'}y^{l+1}\,\mathrm{d}x\in B$. It suffices to show $ld+d+b'p\leq(p-1)(d-1)-2$. We have $ld+d+b'p\leq(p-1)-b'+d+b'p$ as $b'=p-1-ld$. Hence we only need to show

$$d\leq(d-b'-2)(p-1)-2\,. \tag{4}$$

Note that $b'\leq d-3$, we have $(d-b'-2)(p-1)-2\geq p-3\geq d$. Then $x^{b'}y^l\,\mathrm{d}x$, $x^{b'}y^{l+1}\,\mathrm{d}x\in B$ and

$$\mathcal{C}(x^{b'}y^j\,\mathrm{d}x)=\sum_{t=0}^{j}(-1)^t\binom{j}{t}(y^{l-t})\mathcal{C}(x^{b'}f^t(x)\,\mathrm{d}x)=0,\quad j=l,l+1\,.$$

Put $t=l$, then $\mathcal{C}(x^{b'}f^l(x))=\mathcal{C}(x^{b'+ld}+\dots)\,\mathrm{d}x)\neq 0$, which implies $\operatorname{rank}(\mathcal{C})\geq 2$. Therefore we have $d|p+1$. $\square$

Now we will use the de Rham cohomology $H^1_{dR}(X)$ for a curve X of genus g. Recall that this is a vector space of dimension $2g$ provided with a non-degenerate pairing, cf. [12, Section 12]. Let X be an Artin-Schreier curve over k of genus g with equation

$$y^p-y=h(x)\,, \tag{5}$$

where $h(x)\in k[x]\backslash k$ is non-zero of degree d. Let $\pi\colon X\to\mathbb{P}^1$ be the $\mathbb{Z}/p$-cover. Put $U_1=\pi^{-1}(\mathbb{P}^1-\{0\})$ and $U_2=\pi^{-1}(\mathbb{P}^1-\{\infty\})$. For the open affine cover $\mathcal{U}=\{U_1,U_2\}$, we consider the de Rham cohomology $H^1_{dR}(X)$ as in [11, Section 5], i.e.

$$H^1_{dR}(X)=Z^1_{dR}(\mathcal{U})/B^1_{dR}(\mathcal{U})$$

with $Z^1_{dR}(\mathcal{U})=\{(t,\omega_1,\omega_2)|t\in\mathcal{O}_X(U_1\cap U_2),\omega_i\in\Omega^1_X(U_i),\mathrm{d}t=\omega_1-\omega_2\}$ and $B^1_{dR}(\mathcal{U})=\{(t_1-t_2,\mathrm{d}t_1,\mathrm{d}t_2)|t_i\in\mathcal{O}_X(U_i)\}$.

Under the action of the Verschiebung operator V on $H^1_{dR}(X)$, one has $V(H^1_{dR}(X))=H^0(X,\Omega^1_X)$ and V coincides with the Cartier operator on $H^0(X,\Omega^1_X)$.

For $1\leq i\leq g$, put $s(x)=xh'(x)$ with $h'(x)$ the formal derivative of $h(x)$ and write $s(x)=s^{\leq i}(x)+s^{>i}(x)$ with $s^{\leq i}(x)$ the sum of monomials of degree $\leq i$. Then we have the following proposition.

Proposition 2.3. *Let X be an Artin-Schreier curve over k with equation $y^p-y=h(x)$, where $h(x)\in k[x]$ and $\deg h(x)=d$. Then $H^1_{dR}(X)$ has a basis with respect to $\mathcal{U}=\{U_1,U_2\}$ consisting of the following residue classes with representatives in $Z^1_{dR}(\mathcal{U})$:*

$$\alpha_{i,j}=[(0,x^iy^j\,\mathrm{d}x,x^iy^j\,\mathrm{d}x)], \tag{6}$$

$$\beta_{i,j}=\left[\left(\frac{y^{p-1-j}}{x^{i+1}},-\frac{\phi_{i,j}(x,y)}{x^{i+2}}\mathrm{d}x,\frac{(p-1-j)s^{>i+2}(x)y^{p-2-j}}{x^{i+2}}\mathrm{d}x\right)\right], \tag{7}$$

where $i,j\in\mathbb{Z}_{\geq 0}, pi+jd\leq(p-1)(d-1)-2$ and $\phi_{i,j}(x,y)=(p-1-j)s^{\leq i+2}(x)y^{p-2-j}+(i+1)y^{p-1-j}$.

Proof. We use the exact sequence

$$0\longrightarrow H^0(X,\Omega^1_X)\longrightarrow H^1_{dR}(X)\longrightarrow H^1(X,\mathcal{O}_X)\longrightarrow 0\,.$$

The elements $\alpha_{i,j}$ are images of $x^iy^j\,\mathrm{d}x$ under the embedding of $H^0(X,\Omega^1_X)\rightarrow H^1_{dR}(X)$.

Clearly, $\omega_{i,j}=x^iy^j\,\mathrm{d}x$ form a basis of $H^0(X,\Omega^1_X)$ for $i,j\in\mathbb{Z}_{\geq 0}$ with $pi+dj\leq(p-1)(d-1)-2$. On the other hand, we may identify $\mathcal{O}_X(U_2)$ with the k-algebra $k[x,y]$ defined by (5). Moreover, x^iy^j with $i\geq 0, 0\leq j\leq p-1$ form a basis of the image of $\mathcal{O}_X(U_2)$ in $\mathcal{O}_X(U_1\cap U_2)$. Additionally, we have $x^iy^j\in\mathcal{O}_X(U_1)$ for $0\leq j\leq p-1$ and $-pi\geq dj$. Then the residue classes $[x^iy^j]$ form a basis of $H^1(X,\mathcal{O}_X)$ for $i<0, 0\leq j\leq p-1$ and $-pi-dj<0$. By substituting $i=-(i'+1), j=p-1-j'$, the residue classes $[x^{i+1}y^{p-1-j}]$ form a basis with $i\geq 0, 0\leq j\leq p-1$ and $pi+jd\leq(d-1)(p-1)-2$.

Now we check the equality that $\mathrm{d}f_{i,j}=\omega_{i,j,1}-\omega_{i,j,2}$ for residue classes $\beta_{i,j}=[(f_{i,j},\omega_{i,j,1},\omega_{i,j,2})]$. Note that

$$\begin{aligned}\mathrm{d}f_{i,j}&=\mathrm{d}\frac{y^{p-1-j}}{x^{i+1}}=\frac{(p-1-j)x^{i+1}y^{p-2-j}\,\mathrm{d}y}{x^{2i+2}}-\frac{(i+1)x^iy^{p-1-j}\,\mathrm{d}x}{x^{2i+2}}\\&=\frac{-(p-1-j)x^{i+1}y^{p-2-j}h'(x)\,\mathrm{d}x}{x^{2i+2}}-\frac{(i+1)x^iy^{p-1-j}\,\mathrm{d}x}{x^{2i+2}}\\&=-\frac{\phi_{i,j}(x,y)\,\mathrm{d}x}{x^{i+2}}-\frac{(p-1-j)y^{p-2-j}s^{>i+2}(x)\,\mathrm{d}x}{x^{i+2}}=\omega_{i,j,1}-\omega_{i,j,2}\,,\end{aligned}$$

which ends the proof. $\square$

Remark 2.4. The pairing $\langle\ ,\ \rangle$ for this basis is as follows: $\langle\alpha_{i_1,j_1},\beta_{i_2,j_2}\rangle\neq 0$ if $(i_1,j_1)=(i_2,j_2)$ and $\langle\alpha_{i_1,j_1},\beta_{i_2,j_2}\rangle=0$ otherwise. Indeed, for $(i_1,j_1)=(i_2,j_2)$ we have $\mathrm{ord}_\infty(y^{p-1}/x\,\mathrm{d}x)=-1$ and hence $\langle\alpha_{i_1,j_1},\beta_{i_2,j_2}\rangle\neq 0$. For other cases, the proof is similar to the proof of [18, Theorem 4.2.1].

2.1. Proof of Theorem 1.1

Note that by Proposition 2.2 (2), curve X can be written as certain form with $\mathrm{rank}(\mathcal{C})=1$. For $d\leq 2$, the situation is trivial and $\mathrm{rank}(\mathcal{C})=0$ for all $p>0$. Then we may assume that the polynomial $f(x)$ has the form:

$$f(x)=x^d+a_{d-2}x^{d-2}+\ldots+a_1x\,,\quad d>2\,.$$

Also a basis of $H^0(X,\Omega^1_X)$ is given by forms below:

$$B=\{x^iy^j\,\mathrm{d}x|ip+jd\leq(p-1)(d-1)-2\}\,.$$

(1) For $p\geq 7$, we show that $\mathrm{rank}(C)\neq 1$. Indeed, if $a_i=0$ for $i\in\{1,2,\ldots,d-2,d\}$, then by Theorem 2.1 we have $\mathrm{rank}(\mathcal{C})=0$. Otherwise, let i_0 be the largest integer in $\{1,2,\ldots,d-2\}$ such that $a_{i_0}\neq 0$. There are non-negative integers l, m, b satisfying $ld=p+1$ and $d-2=mi_0+b$ with $b\leq i_0-1$.

Suppose $2\leq i_0\leq d-2$, we show that $x^by^{l-1+m}\,\mathrm{d}x\in B$. This is equivalent to showing

$$bp+(l+m-1)d\leq(d-1)(p-1)-2,$$

for $m\geq 1$, $i_0\geq 2$. By substituting $b=d-2-mi_0$, one can show this is equivalent to $m(pi_0-d)\geq 2$, which is trivial as $d|p+1$ and $m(pi_0-d)\geq 2p-d\geq 2$.

Now if $d=p+1$, then we have $l=1$ and $x^by^m\,\mathrm{d}x\in B$ as showed above. If $b=0$, we have $d-2=p-1=mi_0$. By $i_0\geq 2$, we have $m\leq(p-1)/2$. We show that $y^{m+1}\,\mathrm{d}x\in B$ if $p\geq 5$. It is sufficient to show that $(m+1)\leq(p-1)(d-1)-2=p(p-1)-2$. This is true for $p\geq 5$. Then $\mathcal{C}(y^{m+1}\,\mathrm{d}x)\neq 0$ and $\mathcal{C}(y^m\,\mathrm{d}x)\neq 0$ are linearly independent. This implies $\mathrm{rank}(\mathcal{C})\geq 2$ for $b=0$. Suppose $b\geq 1$. We show that $x^{b-1}y^{m+1}\in B$. Note that $d-2=p-1=mi_0+b$. By a similar fashion, we only need to show $m(i_0-1)(p-1)\geq 4$, which is true if $p\geq 5$. Then

$$\begin{aligned}\omega_{b,m}:=\mathcal{C}(x^by^m\,\mathrm{d}x)=\mathcal{C}(x^b(y^p-f(x))^m\,\mathrm{d}x)&=\mathcal{C}((-1)^mx^ba^m_{i_0}(x^{i_0})^m\,\mathrm{d}x)+\ldots\\&=\mathcal{C}((-1)^ma^m_{i_0}x^{p-1}\,\mathrm{d}x)+\ldots\neq 0\,.\end{aligned}$$

Similarly, we have

$$\begin{aligned}\omega_{b-1,m+1}:&=\mathcal{C}(x^{b-1}y^{m+1}\,\mathrm{d}x)=\mathcal{C}(x^{b-1}(y^p-f(x))^{m+1}\,\mathrm{d}x)\\&=\mathcal{C}((m+1)(-1)^{m+1}a_{p+1}a^m_{i_0}x^{2p-1}\,\mathrm{d}x)+\ldots\neq 0\,.\end{aligned}$$

Since $\omega_{b,m}$ and $\omega_{b-1,m+1}$ are k-linearly independent, we have $\mathrm{rank}(\mathcal{C})\geq 2$.

If $d|p{+}1$ and $d{\le}(p{+}1)/2$, we show that $x^b y^{l+m}\,\mathrm{d}x{\in}B$, which is equivalent to $bp{+}(l{+}m)d{\le}(d{-}1)(p{-}1){-}2$. Since $m(pi_0{-}d){\ge}2p{-}d$, we only need to show $m(pi_0{-}d){-}d{\le}2$, which is true for $p{\ge}7$. Hence $\mathcal{C}(x^b y^{l+m}\,\mathrm{d}x){\neq}0$ and $\mathcal{C}(x^b y^{l+m-1}\,\mathrm{d}x){\neq}0$ by the same method above.

Assume $i_0{=}1$ and $a_i{=}0$ for any $i{\in}2,3,...,d{-}2$, if $d{=}p{+}1$, by a simple change of coordinates and by Theorem 2.1 the curve is superspecial and $\mathrm{rank}(\mathcal{C}){=}0$. Otherwise we have $d{<}p{+}1$, in this case we have $d{-}2{=}m{+}b$. We show that $y^{l+m+b-1}\,\mathrm{d}x$, $y^{l+m+b}\,\mathrm{d}x{\in}B$, which is equivalent to showing

$$(l{+}m{+}b{-}1)d \le (d{-}1)(p{-}1){-}2 \quad \text{and} \quad (l{+}m{+}b)d \le (d{-}1)(p{-}1){-}2\,,$$

respectively. These can be simplified to

$$d^2{-}(p{+}2)d{+}2p{+}2 \le 0, \quad d^2{-}(p{+}1)d{+}2p{+}2 \le 0\,.$$

These two inequalities hold for $p{\ge}11$. For $p{=}7$, we have $d|p{+}1{=}8$ and hence $d{\ge}4$. Then those two inequalities also hold.

Moreover, we have

$$\begin{aligned}\mathcal{C}(y^{l+m+b-1}\,\mathrm{d}x) &= \mathcal{C}((y^p - f(x))^{l+m+b-1}\,\mathrm{d}x)\\ &= \mathcal{C}((-1)^{l+m+b-1}(x^d)^{l-1}(a_1x)^{m+b}\,\mathrm{d}x) + \dots\\ &= \mathcal{C}((-1)^{l+m+b-1}a_1^{m+b}x^{p-1}\,\mathrm{d}x) + \dots \neq 0\end{aligned}$$

and $\mathcal{C}(y^{l+m+b}\,\mathrm{d}x){=}\mathcal{C}((-1)^{l+m+b-1}a_1^{m+b}x^{p-1}y^p\,\mathrm{d}x){+}...{\neq}0$. Then $\mathrm{rank}(\mathcal{C}){\ge}2$.

(2) For $p{=}5$ and $d{=}p{+}1{=}6$, to get $\mathrm{rank}(\mathcal{C}){=}1$ we must have $i_0{\ge}2$, otherwise X is superspecial by Theorem 2.1. Then $x^{b-1}y^{m+1}\,\mathrm{d}x, x^b y^m\,\mathrm{d}x{\in}B$ for $b{\ge}1$ and $y^{m+1}\,\mathrm{d}x, y^m\,\mathrm{d}x{\in}B$ for $b{=}0$ (similar to the case $p{=}7$). This implies $\mathrm{rank}(\mathcal{C}){\ge}2$. As for $d{=}3$, if $a_{d-2}{=}a_1{=}0$, then it is superspecial by Theorem 2.1. If $a_1{\neq}0$, then $y^2\,\mathrm{d}x{\in}B$ and $\mathrm{rank}(\mathcal{C}){=}1$.

For the supersingularity, let X be a curve given by equation $y^5{-}y{=}x^3{+}a_1x$ with $a_1{\neq}0$. Then we have $H^0(X,\Omega_X^1){=}\langle \mathrm{d}x, x\,\mathrm{d}x, y\,\mathrm{d}x, y^2\,\mathrm{d}x\rangle$ and $\mathcal{C}(H^0(X,\Omega_X^1)){=}\langle\,\mathrm{d}x\,\rangle$. Moreover by using Proposition 2.3, one can compute that X has Ekedahl-Oort type $[4,3,2]$ and the curve X is supersingular by [4, Step 2, p. 1379]. For the definition of Ekedahl-Oort type we refer [6].

(3) For $p{=}3$, if $d{=}2$ the curve is superspecial. If $d{=}4$, then we may assume that $a_2{\neq}0$ in $f(x)$, otherwise by a simple change of coordinates we may assume the curve is given by equation $y^3{-}y{=}a_4x^4$, which is superspecial by the Theorem 2.1.

If $a_2{\neq}0$, then by a change of coordinate we get $f(x){=}x^4{+}a_2x^2$. A basis of $H^0(X,\Omega_X^1)$ is $\{\mathrm{d}x, x\,\mathrm{d}x, y\,\mathrm{d}x\}$ with $\mathcal{C}(\mathrm{d}x){=}\mathcal{C}(x\,\mathrm{d}x){=}0$ and $\mathcal{C}(y\,\mathrm{d}x){=}\mathcal{C}({-}a_2x^2\,\mathrm{d}x){=}{-}a_2^{1/3}\,\mathrm{d}x{\neq}0$. This implies $\mathrm{rank}(\mathcal{C}){=}1$. Similarly using Proposition 2.3, a curve given by equation $y^3{-}y{=}x^4{+}a_2x^2$ with $a_2{\neq}0$ has Ekedahl-Oort type $[3,2]$ and hence is supersingular by [4, Step 2, p. 1379].

2.2. Proof of Proposition 1.2

Let X be an Artin-Schreier curve given by equation $y^p-y=f(x)$ with $\deg f(x)=d|p+1$ and $\mathrm{rank}(\mathcal{C})=2$. We may assume that the polynomial $f(x)$ has the form:

$$f(x)=x^d+a_{d-2}x^{d-2}+\ldots+a_1x\,.$$

By the proof of Theorem 1.1, there is an integer $n\in\{1,2,\ldots,d-2\}$ such that $a_n\neq 0$. Again denote by i_0 the largest integer in $\{1,2,\ldots,d-2\}$ such that $a_{i_0}\neq 0$ and let l,m,b be the same as in the proof of Theorem 1.1.

For $p\geq 7$, if $d=p+1$, we show that in this case $\mathrm{rank}(\mathcal{C})\geq 3$. Indeed by Theorem 2.1, we have $i_0\geq 2$ and $d-2=p-1=mi_0+b$. If $b=0$, then $d-2=p-1=mi_0$ and $m\leq(p-1)/2$. Moreover from the proof of Theorem 1.1, part (1), we have $y^m\,\mathrm{d}x, y^{m+1}\,\mathrm{d}x\in B$. We show that $y^{m+2}\,\mathrm{d}x\in B$. It suffices to show that $(m+2)d\leq (p-1)(d-1)-2$, which is equivalent to showing $(m+2)(p+1)\leq p^2-p-2$ for any $1\leq m\leq(p-1)/2$. This is true for $p\geq 7$. On the other hand, note that $\mathcal{C}(y^m\,\mathrm{d}x)$, $\mathcal{C}(y^{m+1}\,\mathrm{d}x)$ and $\mathcal{C}(y^{m+2}\,\mathrm{d}x)$ are linearly independent. Then $\mathrm{rank}(\mathcal{C})\geq 3$ in this case. Now if $b\geq 1$, we showed that $x^by^m\,\mathrm{d}x, x^{b-1}y^{m+1}\,\mathrm{d}x\in B$. By a similar argument as in the case $b=0$ above, one can show that $x^by^{m+1}\,\mathrm{d}x\in B$. Additionally, $\mathcal{C}(x^by^m\,\mathrm{d}x), \mathcal{C}(x^{b-1}y^{m+1}\,\mathrm{d}x)$ and $\mathcal{C}(x^by^{m+1}\,\mathrm{d}x)$ are linearly independent. Then we have $\mathrm{rank}(\mathcal{C})\geq 3$ for $p\geq 7$ and $d=p+1$.

Now if $d|p+1$ and $d<p+1$, then $l=(p+1)/d\geq 2$. If $i_0\geq 2$, we show that $\mathrm{rank}(\mathcal{C})\geq 3$ for $p\geq 7$. Note that we have $x^by^{l+m-1}\,\mathrm{d}x, x^by^{l+m}\,\mathrm{d}x\in B$ by the part (1) of the proof of Theorem 1.1. We now claim that $x^by^{l+m+1}\,\mathrm{d}x\in B$. By definition of B, it suffices to show

$$(l+m+1)d+bp\leq(p-1)(d-1)-2\,.$$

By substituting $b=d-2-mi_0$ and $p=ld-1$, the inequality can be simplified to $(i_0l-1)m\geq 3$. This is true as $i_0\geq 2, l\geq 2$ and $m\geq 1$. For $i_0=1$, we show that $\mathrm{rank}(\mathcal{C})\geq 3$ for $p\geq 11$. Note that in this case we have $d-2=m$. One can easily show that $y^{l+m}\,\mathrm{d}x, y^{l+m-1}\,\mathrm{d}x\in B$ by the definition of B. Additionally, we show that $y^{l+m+1}\,\mathrm{d}x\in B$ for $p\geq 11$. Indeed, it suffices to show $(l+m+1)d\leq(p-1)(d-1)-2$, which can be simplified to $2l+d\leq p$. Note that $ld=p+1$, we only need to show $2(p+1)/d+d\leq p$ which can be rewritten as $d^2-dp+2(p+1)\leq 0$. This is true for $3\leq d\leq(p+1)/2$.

For $p=7$ and $i_0=1$, we have $d=4$ and the curve is given by equation $y^7-y=x^4+a_1x$ with $a_1\in k^*$. Then

$$B=\{x^iy^j\,\mathrm{d}x, | i,j\in\mathbb{Z}_{\geq 0}, 7i+4j\leq 16\}$$

and $\mathcal{C}(x^iy^j\,\mathrm{d}x)=0$ for all i,j except $(i,j)=(0,4),(0,3),(1,2)$. Moreover, $\mathcal{C}(y^4\,\mathrm{d}x)$ and $\mathcal{C}(y^3\,\mathrm{d}x)$ are linearly independent and $\mathcal{C}(y^3\,\mathrm{d}x)=\xi\mathcal{C}(xy^2\,\mathrm{d}x)$ for some $\xi\in k^*$.

Then $\operatorname{rank}(\mathcal{C})=2$. Using Proposition 2.3 and by [4, Step 2, p. 1379] as above, the curve is supersingular.

Now let $p=5$. If $d=3$, then by Theorem 2.1 and Theorem 1.1, we have $a_X=g$ or $g-1$. For $d=6$, we get $d-2=4=mi_0+b$. Additionally for $i_0=2,3,4$, one can easily show that $y^2\,\mathrm{d}x, y^3\,\mathrm{d}x, xy^3\,\mathrm{d}x\in B$ and $\mathcal{C}(y^2\,\mathrm{d}x), \mathcal{C}(y^3\,\mathrm{d}x)$ and $\mathcal{C}(xy^2\,\mathrm{d}x)$ are linearly independent. Hence $\operatorname{rank}(\mathcal{C})\geq 3$ and $a_X\leq g-3$ with $g=10$.

For $p=3$ and $d\,|\,p+1=4$, by Theorem 2.1 and Theorem 1.1, we have $a_X\geq g-1$.

Similar to Proposition 2.2, we have the following.

Proposition 2.5. *Let k be an algebraically closed field with $\operatorname{char}(k)=p\geq 3$. Let X be an Artin-Schreier curve of genus $g\geq 1$ with equation $y^p-y=f(x)$, where $f(x)\in k(x)$. If $a_X=g-2$, then*

(1) if $p=3$, then $g\leq 7$ and the curve X can be either written as $y^3-y=f(x)$, where $f(x)\in k[x]$ and $\deg f(x)\leq 8$, or as $y^3-y=f_0(x)+f_1(1/x)$ with $f_0(x), f_1(x)\in k[x]$ and $\deg f_0(x)\leq 4, \deg f_1(x)\leq 2$;

(2) if $p\geq 5$, then $g\leq (2p+1)(p-1)/2$ and X is isomorphic to a curve with equation

$$y^p-y=f(x), \quad f(x)\in k[x]\,.$$

The proof of part (1) is similar to the part (1) of the proof of Proposition 2.2 and hence we omit it. For part (2), one can first show f is a polynomial using the Deuring-Shafarevich formula and then prove the proposition by analysing the degree of f.

3. On the existence of trigonal curves with prescribed a-number

Now we study the existence of trigonal curves with prescribed a-number and give proofs of Theorems 1.3 and 1.4. We deal here with genus 5. It is well known that a trigonal curve X of genus 5 is a normalization of a quintic curve C in $\mathbb{P}^2$ with a unique singular point [1, Exercise I-6, p. 279], see also [10, Lemma 2.2.1].

3.1. Set up

For a trigonal curve X of genus 5 defined over k, let $\phi: X\to\mathbb{P}^1$ be a morphism of degree 3. Then using the base point free pencil trick and Clifford Theorem one can easily show that ϕ is unique (up to isomorphism of $\mathbb{P}^1$) and X is not hyperelliptic.

Lemma 3.1. *Let p be either 2 or 3. If X is a trigonal curve of genus 5 over k, then*

(1) *X is a normalization of a quintic curve C in $\mathbb{P}^2$ with a unique singular point of multiplicity* 2. *Moreover,*

(*i*) *If C has a node, then C is given by a homogeneous polynomial $F \in k[x,y,z]$ of degree* 5 *with*

$$F = xyz^3 + f\,,$$

where f is a sum of monomials not divisible by z^3.

(*ii*) *If C has a cusp, then C is given by a homogeneous polynomial $F \in k[x,y,z]$ of degree* 5 *with*

$$F = x^2z^3 + f\,,$$

where f is a sum of monomials not divisible by z^3 and the coefficient of y^3z^2 in f is non-zero.

(2) *The normalization of any C with one singular point in* (*i*) *and* (*ii*) *is a trigonal curve of genus* 5.

Proof. Kudo and Harashita proved the lemma for $p \neq 2$ in [10, Lemma 2.2.1] (note that we can assume $\varepsilon = 0$ in the statement of Lemma 2.2.1 in [10] since k is algebraically closed). For $p = 2$, we show that part (1) is true and since the proof of the other part is similar to the case $p \geq 3$ we omit it.

Assuming the singular point is (0:0:1), the curve C is given by $F = Qz^3 + f$, where Q is a quadratic form in $k[x,y]$ and f is a sum of monomials in x, y of degree >2.

If Q is non-degenerate, then C has a node. We may change coordinates so that Q equals xy, we arrive at $F = xyz^3 + f$ with f a sum of monomials in x, y of degree >2.

If Q is degenerate, then C has a cusp. We may change coordinates so that Q equals x^2, we arrive at $F = x^2z^3 + f$ with f a sum of monomials in x, y of degree >2. □

We recall the following proposition.

Proposition 3.2. ([10, Proposition 2.3.1]) *Let X be a trigonal curve of genus* 5 *defined over k. Let C be an associated quintic curve in $\mathbb{P}^2$ given by Lemma 3.1. Let $h_{l,m}$ $(1 \leq l, m \leq 5)$ be the coefficient of the monomial $x^{pi_l - i_m} y^{pj_l - j_m} z^{pk_l - k_m}$ in F^{p-1}, where*

l	1	2	3	4	5
i_l	3	1	2	2	1
j_l	1	3	2	1	2
k_l	1	1	1	2	2

Then the Hasse-Witt matrix H of X is given by $H = (h_{l,m})$.

3.2. The proof of Theorem 1.3

Let $p=2$ and X be a trigonal curve of genus 5 defined over k. we start by simplifying the defining equation of the singular model $C\subset\mathbb{P}^2$ of X.

Lemma 3.3. *Let k be an algebraically closed field with $\mathrm{char}(k)=2$. In the notation of Lemma 3.1 case (i), we can choose f as*

$$f=(x^3+b_1y^3)z^2+\sum_{i=1}^{5}(a_ix^{5-i}y^{i-1})z+\sum_{i=6}^{11}a_ix^{11-i}y^{i-6} \tag{8}$$

or

$$f=\sum_{i=1}^{5}(a_ix^{5-i}y^{i-1})z+\sum_{i=6}^{11}a_ix^{11-i}y^{i-6}\,. \tag{9}$$

For case (ii), we can choose f as

$$f=y^3z^2+\sum_{i=1}^{5}(a_ix^{5-i}y^{i-1})z+\sum_{i=6}^{11}a_ix^{11-i}y^{i-6}\,. \tag{10}$$

Proof. For the case (i) of Lemma 3.1, the curve C is given by $F=xyz^3+f$, where f is the sum of monomials, which have degree >2 in x,y. By a linear transformation $z\mapsto z+\alpha x+\beta y$, we may assume the coefficients of x^2yz^2 and xy^2z^2 are zero. Then

$$f=(b_0x^3+b_1y^3)z^2+\sum_{i=1}^{5}a_ix^{5-i}y^{i-1}z+\sum_{i=6}^{11}a_ix^{11-i}y^{i-6}\,,$$

where $b_0,b_1,a_1,\ldots,a_{11}\in k$. Note that if $(b_0,b_1)\neq(0,0)$, by symmetry we may assume $b_0\neq 0$. By scaling $x\mapsto\alpha x, y\mapsto\beta y$ with $\alpha\beta=1$ and $\alpha^3=1$, we may assume $b_0=1$. On the other hand, if $b_0=b_1=0$ in f, then we have

$$f=\sum_{i=1}^{5}a_ix^{5-i}y^{i-1}z+\sum_{i=6}^{11}a_ix^{11-i}y^{i-6}\,.$$

For the case (ii) of Lemma 3.1, the curve C is given by $F=x^2z^3+f$, where f is the sum of monomials, which have degree >2 in x,y and the coefficient of y^3z^2 is non-zero. Consider $y\mapsto y+\gamma x$ and then consider $z\mapsto z+\alpha x+\beta y$, we may assume the coefficients of x^3z^2, x^2yz^2 and xy^2z^2 are zero. Moreover, by scaling $y\mapsto\delta y$ with $\delta^3=1$, we may assume the coefficient of y^3z^2 is equal to 1. Then we have

$$f=y^3z^2+\sum_{i=1}^{5}a_ix^{5-i}y^{i-1}z+\sum_{i=6}^{11}a_ix^{11-i}y^{i-6}\,,\quad a_1,\ldots,a_{11}\in k\,. \qquad\square$$

Now we can give a proof of Theorem 1.3.

Proof of Theorem 1.3. Let C be a singular model of X given by Lemma 3.1. If C has a node, then by Lemma 3.3, f is either given by (8) or (9). If f is given by (8), then by Proposition 3.2, the Hasse-Witt matrix H of X is equal to

$$\begin{pmatrix} a_2 & 0 & a_1 & a_7 & a_6 \\ 0 & a_4 & a_5 & a_{11} & a_{10} \\ a_4 & a_2 & a_3 & a_9 & a_8 \\ 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & b_1 & 0 \end{pmatrix}. \tag{11}$$

Let e_i be the i-th row of H. Then e_4 and e_5 are linearly independent and rank$(H)\geq$ 2.

Now we show rank$(H)\geq 3$ in this case. Indeed, if rank$(H)=2$, then e_i for $i=1,2,3$ is a linear combination of e_4 and e_5. By the shape of H, we have

$$a_1=a_3=a_5=a_7=a_{10}=0, \quad a_4=a_8, \quad a_2=a_6, \quad b_1a_4=a_{11}, \quad b_1a_2=a_9\,.$$

Hence C is given by

$$\begin{aligned} F &= xyz^3+(x^3+b_1y^3)z^2+(a_2x^3y+a_4xy^3)z+a_2x^5+a_4x^3y^2+b_1a_2x^2y^3+b_1a_4y^5 \\ &= (z+a_2^{1/2}x+a_4^{1/2}y)^2(b_1y^3+x^3+xyz) \end{aligned}$$

and C is reducible. This contradiction shows that rank$(H)\geq 3$.

Now if f is given by (9), then again by Proposition 3.2 the Hasse-Witt matrix H of X is equal to

$$\begin{pmatrix} a_2 & 0 & a_1 & a_7 & a_6 \\ 0 & a_4 & a_5 & a_{11} & a_{10} \\ a_4 & a_2 & a_3 & a_9 & a_8 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \end{pmatrix}. \tag{12}$$

Then we have rank$(H)\geq 2$. Moreover, if rank$(H)=2$, then we have $a_i=0$ for all $i\in\{1,\ldots,11\}$ with $i\neq 2,4$. This implies

$$F=xyz^3+a_2x^3yz+a_4xy^3z=xy(z^3+a_2x^2z+a_4y^2)\,,$$

a contradiction. Hence we have rank$(H)\geq 3$ if C has a node.

If the curve C has a cusp, then by Lemma 3.3, f is given by (10). Hence by Proposition 3.2, the Hasse-Witt matrix of X is equal to

$$\begin{pmatrix} a_2 & 0 & a_1 & a_7 & a_6 \\ 0 & a_4 & a_5 & a_{11} & a_{10} \\ a_4 & a_2 & a_3 & a_9 & a_8 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}. \tag{13}$$

Then we still have $\mathrm{rank}(H)\geq 2$. We show $\mathrm{rank}(H)\geq 3$ by showing that C has at least two singular points if $\mathrm{rank}(H)=2$. Indeed, suppose $\mathrm{rank}(H)=2$. By (13), we obtain $a_2=a_4=a_6=a_8=a_{10}=0$. This implies

$$F=x^2z^3+y^3z^2+(a_1x^4+a_3x^2y^2+a_5y^4)z+a_7x^4y+a_9x^2y^3+a_{11}y^5\,.$$

Denote by F_x (resp. F_y, F_z) the formal partial derivative with respect to the variable x (resp. y, z). Note that we have

$$F_x=0,\ F_y=y^2z^2+a_7x^4+a_9x^2y^2+a_{11}y^4,\quad F_z=x^2z^2+a_1x^4+a_3x^2y^2+a_5y^4\,.$$

By setting $x=1$ in F_x, F_y and F_z, one can easily show that $(1{:}a{:}b)$ is a singular point. Then there are at least two singular points on C. By the genus formula for plane curves, the genus of X is less than 5, a contradiction.

Now we have $\mathrm{rank}(H)\geq 3$ for any trigonal curve X of genus 5 over k. Then $a_X\leq 2$. □

3.3. The proof of Theorem 1.4

Let $p=3$ and X be a trigonal curve of genus 5 defined over k. We now give the reductions of the defining equations of the singular model $C\subset\mathbb{P}^2$ of X given by Lemma 3.1.

Lemma 3.4. *Let k be an algebraically closed field with* $\mathrm{char}(k)=3$. *In the notation of Lemma 3.1 case (i), we can choose f as*

$$(14)\quad (b_0x^3+b_1y^3+b_2x^2y+b_3xy^2)z^2+\sum_{i=1}^{5}a_ix^{5-i}y^{i-1}z+a_6x^5+\sum_{i=8,\,i\neq 10}^{11}a_ix^{11-i}y^{i-6}.$$

For the case (ii), we can choose f as

$$(15)\quad \left(y^3+\sum_{i=2}^{3}b_ix^{4-i}y^{i-1}\right)z^2+\sum_{i=1}^{5}a_ix^{5-i}y^{i-1}z+a_7x^4y+a_8x^3y^2+a_{10}xy^4+a_{11}y^5.$$

Proof. If C has a node, then by Lemma 3.1, $F=xyz^3+f$ with f the sum of monomials, which have degree >2 in x, y. By a linear transform $z\mapsto z+\alpha x+\beta y$ we may assume the coefficients of x^4y and xy^4 is zero. Then f is equal to

$$(b_0x^3+b_1y^3+b_2x^2y+b_3xy^2)z^2+\sum_{i=1}^{5}a_ix^{5-i}y^{i-1}z+a_6x^5+a_8x^3y^2+a_9x^2y^3+a_{11}y^5\,.$$

By Lemma 3.1, if C has a cusp, then $F=xyz^3+f$ with f the sum of monomials, which have degree >2 in x,y and the coefficient of y^3z^2 is non-zero. By a linear transform $z\mapsto z+\alpha x+\beta y$, we may assume the coefficients of x^5 and x^2y^3 is zero. Moreover, by scaling $y\mapsto \delta y$, we may assume the coefficient of y^3z^2 is 1. Then we have

$$f=(y^3+b_2x^2y+b_3xy^2)z^2+\sum_{i=1}^{5}a_ix^{5-i}y^{i-1}z+a_7x^4y+a_8x^3y^2+a_{10}xy^4+a_{11}y^5\,. \quad \square$$

Proof of Theorem 1.4. Let C be the singular model given by Lemma 3.1. Denote by H the Hasse-Witt matrix of X given by Proposition 3.2 and by $e_i=(e_{i,1},\dots,e_{i,5})$ the i-th row of H. Then we have $\mathrm{rank}(H)\geq 1$ because of the Ekedahl's genus bound for superspecial curve [5]. Suppose $\mathrm{rank}(H)=1$. We consider different cases for the singular point of C.

If the curve C has a node, by Lemma 3.4, f is given by (14). If at least one of the b_0,b_1 is non-zero, by symmetry we may assume $b_0\neq 0$. By scaling we may assume $b_0=1$. Moreover, by Proposition 3.2, we have $e_4=(2b_2,0,2,b_2^2+2b_3+2a_2,b_2+2a_1)$ which is non-zero. Then $e_i=\lambda_ie_4$ with $\lambda_i\in k$ for $i=1,2,3,5$. In particular, we have

$$e_5=(0,2b_3,2b_1,2b_1b_3+2a_5,2b_1b_2+b_3^2+2a_4)=\lambda_5e_4\,.$$

This implies that $b_3=0$ and $b_1b_2=0$.

If $b_1=0$, then $e_5=(0,0,0,2a_5,2a_4)$ is the zero vector. Hence $a_4=a_5=0$. Note that in this case we have $e_{3,1}=2a_{11}$ and $e_{3,1}=\lambda_3e_{4,1}=0$. Then $a_{11}=0$ and

$$F=xyz^3+(x^3+b_2x^2y)z^2+(a_1x^4+a_2x^3y+a_3x^2y^2)z+a_6x^5+a_8x^3y^2+a_9x^2y^3\,.$$

One can easily check that $(0{:}0{:}1)$ and $(0{:}1{:}0)$ are common zeros of $F=F_x=F_y=F_z=0$. Then C has at least two singular points, a contradiction.

Now if $b_1\neq 0$, then the equation $b_1b_2=0$ implies $b_2=0$. Consider a change of coordinate $x\mapsto\alpha x, y\mapsto\beta y$ and multiply F by $1/(\alpha\beta)$. The coefficients of x^3 and y^3 in F become α^2/β and β^2b_1/α. By taking $\beta=\alpha^2$ and $\alpha=b_1^{-1/3}$, we may assume $b_0=b_1=1$. Then $e_5=\lambda_5e_4$ implies $a_2=a_5$ and $a_1=a_4$. Additionally, we have

$$e_1=(2a_1a_3+a_2^2+2a_8,a_1^2+2a_6,2a_1a_2,2a_1a_8+2a_3a_6,2a_2a_6),$$
$$e_2=(a_2^2+2a_{11},a_1^2+2a_2a_3+2a_9,2a_1a_2,2a_1a_{11},2a_2a_9+2a_3a_{11})\,.$$

Then by $e_1=\lambda_1e_4$ and $e_2=\lambda_2e_4$, we have

$$a_6=a_1^2,\quad a_8=a_2^2-a_1a_3,\quad a_9=a_1^2-a_2a_3,\quad a_{11}=a_2^2\,.$$

If $a_3=0$, then one can easily show that $(-1{:}1{:}0)$ and $(0{:}0{:}1)$ are common zeros of $F=F_x=F_y=F_z=0$ and hence are singular points of C, a contradiction. If $a_3\neq 0$, then $F_z=2(x^3+y^3)z+a_1x^4+a_2x^3y+a_3x^2y^2+a_1xy^3+a_2y^4$ and by substituting

$$z=(a_1x^4+a_2x^3y+a_3x^2y^2+a_1xy^3+a_2y^4)/(x+y)^3$$

in F_x and F_y and by letting $y=1$, we have $(x(x+y)^9F_x)|_{y=1}=((x+y)^9F_y)|_{y=1}$ and

$$((x+y)^9F_x)|_{y=1}=(a_1^3+a_1a_2)x^{12}+(a_1a_2+a_2^3+2a_3^2)x^9+(a_3^3+a_3^2)x^6 \\ +(a_1^3+a_1a_2+2a_3^2)x^3+a_1a_2+a_2^3\,.$$

Since $a_3\neq 0$, one can check that it has solutions with $x\neq -1,0$. Then there exists another singular point on C which is distinct from $(0{:}0{:}1)$, a contradiction.

Now if $b_0=b_1=0$, we have $e_4=(2b_2,0,0,b_2^2+2a_2,2a_1)$ and $e_5=(0,2b_3,0,2a_5,b_3^2+2a_4)$. Since $\operatorname{rank}(H)=1$, we have at least one of the b_2,b_3 is zero. By symmetry we may assume $b_3=0$. If $b_2\neq 0$, by scaling we may assume $b_2=1$. Note that we have $e_i=\lambda_ie_4$ with $\lambda_i\in k$ for $i=1,2,3,5$. In particular for $i=5$, it is straightforward to see that $\lambda_5=0$ and $a_4=a_5=0$. Moreover, $e_{2,2}=2a_{11}=\lambda_2e_{4,2}=0$. Then by a similar fashion, one can show that $(0{:}0{:}1)$ and $(0{:}1{:}0)$ are singular points of C, a contradiction. If $b_3=b_2=0$, then

$$e_1=(2a_1a_3+a_2^2,a_1^2,2a_1a_2,2a_1a_8+2a_3a_6,2a_2a_6),\quad e_4=(0,0,0,2a_2,2a_1)\,.$$

This implies $a_1=a_2=0$ otherwise e_1 and e_4 are linearly independent. Similarly one has $a_4=a_5=0$ by checking the linearly independence of e_2 and e_5. Now we have $e_4=e_5=0$ and

$$e_1=(0,0,0,2a_3a_6,0),\quad e_2=(0,0,0,0,2a_3a_{11}),\quad e_3=(0,0,a_3,2a_3a_9,2a_3a_8)\,.$$

Since $\operatorname{rank}(H)=1$, we obtain that $a_6=a_{11}=0$ and $F=y(xz^3+a_3x^2yz+a_8x^3y+a_9x^2y^2)$, a contradiction.

Now if C has a cusp, then by Lemma 3.4, f is given by (15). Moreover, by Proposition 3.2, we have

$$e_4=(2b_3,0,2b_2,b_2^2+2a_3,2a_2),\quad e_5=(0,2,0,2b_3,2b_2+b_3^2+2a_5)\,.$$

If $\operatorname{rank}(H)=1$, then $e_i=\lambda_ie_5$ with $\lambda_i\in k$ for $i=1,2,3,4$. In particular, $e_4=\lambda_4e_5$ implies $\lambda_4=b_2=b_3=a_2=a_3=0$. Then we obtain

$$\begin{aligned} e_1&=(0,a_1^2,0,2a_1a_8,2a_1a_7),\\ e_2&=(a_5^2+2a_{11},a_4^2,2a_4a_5+2a_{10},2a_4a_{11}+2a_5a_{10},2a_4a_{10}),\\ e_3&=(2a_8,2a_1a_4,2a_1a_5+2a_7,2a_1a_{11}+2a_4a_8+2a_5a_7,2a_1a_{10}+2a_4a_7)\,. \end{aligned}$$

Hence by $e_i = \lambda_i e_5$ for $i = 1, 2, 3$, we get $a_7 = 2a_1 a_5, a_8 = 0, a_{10} = 2a_4 a_5, a_{11} = a_5^2$. Additionally, one can easily check that $F = F_x = F_y = F_z = 0$ have common zeros $(0{:}0{:}1), (0{:}1{:}0)$ if $a_5 = 0$ and $(0{:}0{:}1), (0{:}1/(2a_5){:}1)$ if $a_5 \neq 0$, a contradiction. Then $\mathrm{rank}(H) \geq 2$ if C has a cusp.

In any case, we have $\mathrm{rank}(H) \geq 2$ and hence $a_X \leq 3$. $\square$

Acknowledgments. I would like to thank my supervisor, Professor Gerard van der Geer, for his patient and continuous guidance and kind advice throughout my research studies. I also would like to thank Katsura and Pries for helpful comments.

References

1. Arbarello, E., Cornalba, M., Griffiths, P. A. and Harris, J., *Geometry of algebraic curves. Vol. I*, Grundlehren der Mathematischen Wissenschaften. **267**, Springer, New York, 1985.
2. Booher, J. and Bryden, binitsCais, a-numbers in Artin-Schreier covers, *Preprint*, 2018.
3. Cartier, P., Une nouvelle opération sur les formes différentielles, *C. R. Acad. Sci. Paris* **244** (1957), 426–428.
4. Chai, C. and Oort, F., Monodromy and irreducibility of leaves, *Ann. Math.* **173** (2011), 1359–1396.
5. Ekedahl, T., On supersingular curves and abelian varieties, *Math. Scand.* **60** (1987), 151–178.
6. Ekedahl, T. and van der Geer, G., Cycle Classes of the E-O Stratification on the Moduli of Abelian Varieties, in *Algebra, Arithmetic, and Geometry: Volume I: In Honor of Yu. I. Manin*, pp. 567–636, Birkhäuser, Boston, 2009.
7. Elkin, A. and Pries, R., Ekedahl-Oort strata of hyperelliptic curves in characteristic 2, *Algebra Number Theory* **7** (2013), 507–532.
8. Farnell, S. and Pries, R., Families of Artin-Schreier curves with Cartier-Manin matrix of constant rank, *Linear Algebra Appl.* **439** (2013), 2158–2166.
9. Irokawa, S. and Sasaki, R., A remark on Artin-Schreier curves whose Hasse-Witt maps are the zero maps, *Tsukuba J. Math.* **15** (1991), 185–192.
10. Kudo, M. and Harashita, S., Superspecial trigonal curves of genus 5. *Preprint*, 2018, arXiv:1804.11277
11. Oda, T., The first de Rham cohomology group and Dieudonné modules, *Ann. Sci. Éc. Norm. Supér.* **4** (1969), 63–135.
12. Oort, F., A Stratification of a Moduli Space of Polarized Abelian Varieties in Positive Characteristic, in *Moduli of Curves and Abelian Varieties: The Dutch Intercity Seminar on Moduli*, pp. 47–64, Vieweg+Teubner Verlag, Wiesbaden, 1999.
13. Re, R., The rank of the Cartier operator and linear systems on curves, *J. Algebra* **236** (2001), 80–92.
14. Seshadri, C. S. L'opération de Cartier. Applications, *Sémin. Claude Chevalley* **4** (1958–1959), 1–26.

15. Stöhr, K. and Voloch, J., A formula for the Cartier operator on plane algebraic curves, *J. Reine Angew. Math.* **377** (1987), 49–64.
16. Subrao, D., The p-rank of Artin-Schreier curves, *Manuscr. Math.* **16** (1975), 169–193.
17. Sullivan, F. J., p-torsion in the class group of curves with too many automorphisms, *Arch. Math. (Basel)* **26** (1975), 253–261.
18. Tait, J., *Group actions on differentials of curves and cohomology bases of hyperelliptic curves*, Ph.D. Thesis, University of Southampton, 2014.

Zijian Zhou
College of Liberal Arts and Sciences
National University of Defense Technology
410073 Changsha
China
zhouzijian.edu@gmail.com

Received November 25, 2019
in revised form September 27, 2020