The $a$-Number of Certain Hyperelliptic Curves

Vahid Nourozi\(^1\) • Farhad Rahmati\(^1\) • Saeed Tafazolian\(^2\)

Received: 27 August 2021 / Accepted: 17 June 2022 / Published online: 25 July 2022
© The Author(s), under exclusive licence to Shiraz University 2022

Abstract
The $a$-number of an algebraic curve $X$ is the dimension of the space of exact holomorphic differentials on $X$. In this paper, we give a formula for the $a$-number of family of hyperelliptic curves defined by the equations $y^2 = x^m + 1$ and $y^2 = x^m + x$ for infinitely many values of $m$.

Keywords $a$-Number • Cartier operator • Super-singular curves • Maximal curves

1 Introduction
Let $k$ be an algebraically closed field of characteristic $p > 0$. Let $A$ be an abelian variety defined over $k$. Let $a_p$ be the group scheme $\text{Spec}(k[X]/(X^p))$ with co-multiplication given by $X \to 1 \otimes X + X \otimes 1$.

The group $\text{Hom}(a_p,A)$ can be considered as $k$-vector space since $\text{End}(a_p) = k$. The $a$-number $a(A)$ defined to be the dimension of the vector space $\text{Hom}(a_p,A)$.

Let $X$ be a (non-singular, projective, geometrically irreducible, algebraic) curve defined over $k$. One can define the $a$-number $a(X)$ of $X$ as the $a$-number of its Jacobian variety $J_X$. As a matter of fact, the $a$-number of a curve is a birational invariant which can be defined as the dimension of the space of exact holomorphic differentials.

In this work, we consider the hyperelliptic curve $X$ given by the equation $y^2 = x^m + 1$ or $y^2 = x^m + x$ over $k$.

These families of hyperelliptic curves have been investigated for several reasons by many authors [see Kodama and Washio (1990), Tafazolian (2012b), Tafazolian (2012a), Valentini (1995)]. The main goal of this paper is to determine the $a$-number of $X$ for infinitely many values of $m$ which is stated in Theorems 3.1, 3.2 and 4.1.

2 The Cartier Operator
Let $k$ be an algebraically closed field of characteristic $p > 0$. Let $X$ be a projective nonsingular hyperelliptic curve defined over $k$ of genus $g$. The Cartier operator is a $p$-linear operator acting on the sheaf $\Omega^1_X$ of differential forms on $X$.

Let $K(X)$ be the function field of a curve $X$ of genus $g$ defined over an algebraically closed field $K$ of characteristic $p > 0$. A separating variable for $K(X)$ is an element...
1. \( C(\gamma x + \delta) = f(C(\gamma) + C(\delta)) \)
2. \( C(\omega) = 0 \iff \exists h \in \mathcal{H}, \omega = dh \)
3. \( C(\omega) = \omega \iff \exists h \in \mathcal{H}, \omega = dh/h \)

**Remark 2.2** Moreover, one can easily show that

\[
C(x^i dx) = \begin{cases} 0 & \text{if } p \mid j + 1 \\
x^{i-1} dx & \text{if } j + 1 = ps.
\end{cases}
\]

If \( \text{div} \ (\omega) \) is effective, then differential \( \omega \) is holomorphic. The set \( H^0(\mathcal{X}, \Omega^1) \) of holomorphic differentials is a \( g \)-dimensional \( k \)-vector subspace of \( \Omega^1 \) such that \( C(H^0(\mathcal{X}, \Omega^1)) \subseteq H^0(\mathcal{X}, \Omega^1) \). If \( \mathcal{X} \) is a curve, then the \( \text{a-number of } \mathcal{X} \) equals the dimension of the kernel of the Cartier operator \( H^0(\mathcal{X}, \Omega^1) \) (or equivalently, the dimension of the space of exact holomorphic differentials on \( \mathcal{X} \)) (see Li and Oort 1998 [5.2.8]).

The Cartier operator and Hasse-Witt-matrix are dual to each other under the duality given by the Riemann-Roch theorem. Let \( B = \{ \omega_1, \ldots, \omega_g \} \) be a basis of the \( k \)-module of holomorphic differentials in \( H^0(\mathcal{X}, \Omega^1) \). Then the representation matrix \( M \) over \( k \) of \( C \) with respect to this basis is called the Hasse-Witt matrix.

Let \( k \) be a field of characteristic \( p > 2 \). Then \( \mathcal{X} \) can be defined by an affine equation of the form

\[
y^2 = f(x)
\]

where \( f(x) \) is a polynomial over \( k \) of degree \( d = 2g + 1 \) or \( d = 2g + 2 \) without multiple roots.

The differential \( 1 \)-forms of the first kind on \( \mathcal{X} \) form a \( k \)-vector space \( H^0(\mathcal{X}, \Omega^1) \) of dimension \( g \) with basis \( \mathcal{B} = \{ \omega_i = x^{i-1} dx/y, i = 1, \ldots, g \} \).

The images under the operator \( C \) are determined in the following way (see Yui 1978). Rewrite

\[
\omega_i = \frac{x^{i-1} dx}{y} = x^{i-1} y^{-p} y^{i-1} dx = y^{-p} x^{i-1} \sum_{j=0}^{N} c_j x^j dx,
\]

where the coefficients \( c_j \in k \) are obtained from the expansion

\[
y^{p-1} = f(x)^{(q-1)/2} = \sum_{j=0}^{N} c_j x^j \quad \text{with } N = \frac{p - 1}{2} (d).
\]

Then we get for \( i = 1, \ldots, g \),

\[
\omega_i = y^{-p} \left( \sum_{l+j=0 \mod p} c_l x^{l+j-1} dx \right) + \sum_{l} c_{(l+1)p-i} \frac{x^{(l+1)p} dx}{y^p}.
\]

Note here that \( 0 \leq l \leq \frac{N+k}{p} - 1 < g - \frac{1}{2} \cdot \frac{p}{d} \).

On the other hand, we know from Remark 2.2 that if \( C(x^{i-1} dx) \neq 0 \) then \( r \equiv 0 \pmod{p} \). Thus we have

\[
C(\omega_i) = \sum_{l=0}^{g-1} (c_{(l+1)p-1})^{1/p} \cdot \frac{x^l}{y^{ix}} dx.
\]

If we write \( \omega = (\omega_1, \ldots, \omega_g) \) as a row vector, we have

\[
C(\omega) = M(\mathcal{X})^{(1/p)} \omega,
\]

where \( M(\mathcal{X}) \) is the \((g \times g)\) matrix with elements in \( k \) given as

\[
M(\mathcal{X}) = \begin{pmatrix} c_p & c_{p-1} & \ldots & c_2 & c_1 \\ c_2 & c_{p-1} & \ldots & c_3 & c_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ c_g & c_{g-1} & \ldots & c_{2g-p} & c_{2g-p} \end{pmatrix}.
\]

### 3 The \( a \)-number of \( y^2 = x^m + 1 \)

In this section, we consider the hyperelliptic curve \( \mathcal{X} \) given by the equation \( y^2 = x^m + 1 \) over \( k \). This curve of genus \( g = (m-1)/2 \) (resp. \( g = (m-2)/2 \)) if \( m \) is odd (resp. \( m \) is even).

Let \( B = \{ \omega_i = x^{i-1} dx/y, i = 1, \ldots, g \} \) be a basis for the differential \( 1 \)-forms of the first kind on \( \mathcal{X} \). Then the rank of the Cartier operator \( C \) on the curve \( \mathcal{X} \) equals the number of \( i \) with \( i \leq g \) such that
\[ \mathcal{G}(w_i) = \frac{1}{y} \mathcal{G}(x^{i-1}y^{p-1}dx) \\
= \frac{1}{y} \mathcal{G}\left((x^m + 1)^{\frac{i-1}{2}}x^{-1}dx\right) \\
= \frac{1}{y} \mathcal{G}\left(\sum_{j=0}^{\frac{i-1}{2}} a_jx^{j+i-1}dx\right) \neq 0, \]

where \((x^m + 1)^{\frac{i-1}{2}} = \sum_{j=0}^{\frac{i-1}{2}} a_jx^{jm}\). From this, we must have an equation of congruences mod \(p\),

\[ i + mj - 1 \equiv p - 1, \quad (3.1) \]

for some \(0 \leq j \leq \frac{(p-1)}{2}\). Equivalently, the following equation of

\[ m(p - 1 - h) + i - 1 \equiv p - 1, \quad (3.2) \]

has a solution \(h\) for \(0 \leq h \leq \frac{p - 1}{2}\).

For the rest of this section, \(M_m := M(\mathcal{X})\) is the matrix representing the \(p\)-th power of the Cartier operator \(\mathcal{G}\) on the curve \(\mathcal{X}\) with respect to the basis \(B\).

**Theorem 3.1** Let \(\mathcal{X}\) be a hyperelliptic curve given by the equation \(y^2 = x^m + 1\). Suppose that \(m = sp + 1\), then

1. If \(s = 2k + 1\) and \(k \geq 0\), then the \(a\)-number of the curve \(\mathcal{X}\) equals

\[ \frac{(k + 1)(p - 1)}{2}. \]

2. If \(s = 2k\) and \(k \geq 1\), then the \(a\)-number of the curve \(\mathcal{X}\) equals

\[ \frac{k(p - 1)}{2}. \]

**Proof**

(1) First, if \(m = sp + 1 = (2k + 1)p + 1\) with \(k \geq 0\), then we prove that \(\text{rank } (M_m) = \frac{k(p - 1)}{2}\).

In this case, \(i \leq g\) and Eq. (3.2) mod \(p\) reads

\[ i - h - 1 \equiv 0. \quad (3.3) \]

If \(k = 0\), then \(m = p + 1\).

Take \(i \in \mathbb{Z}_0^+\) such that \(i = lp + h + 1\), then

\[ 1 \leq lp + h + 1 \leq \frac{p - 1}{2}. \]

This implies that \(h \geq 0\) and \(h \leq -\frac{3}{2}\), thus a contradiction. Thus, \(\text{rank } (M_{p+1}) = 0\).

If \(k = 1\), then \(m = 3p + 1\); in this case, we have

\[ \frac{p}{2} \leq i \leq \frac{3p - 1}{2}. \]

We need to find the solutions \(h\) mod \(p\) of the Eq. (3.3). Then

\[ \frac{p}{2} \leq l \leq \frac{3p - 1}{2}. \]

As \(h + 1 \geq 0\) we obtain

\[ \begin{cases} l \geq 0 \\ l < 3/2 \end{cases} \]

Thus, we have two choices for \(l\), i.e., \(l = 0\) or \(l = 1\). From this we have \(\frac{1}{2}(p + 1)\) choices for \(h\), and so we conclude \(\text{rank } (M_{3p+1}) = \frac{1}{2}(p + 1)\).

For \(k \geq 2\), and \(m = sp + 1\) we can say \(\text{rank } (M_{(2k+1)p+1}) = \text{rank } (M_{(2k-1)p+1}) + \frac{1}{2}(p + 1)\) plus the number of \(i\) such that there is the solutions \(h\) mod \(p\) of the equation

\[ i \equiv h + 1 \]

with \(\frac{(2k - 1)p}{2} \leq i \leq \frac{(2k + 1)p - 1}{2}\). Then

\[ \frac{(2k - 1)p}{2} \leq lp + h + 1 \leq \frac{(2k + 1)p - 1}{2}. \]

This implies that

\[ \begin{cases} l \geq \frac{2k - 1}{2} \\ l < \frac{2k + 1}{2} \end{cases} \]

or equivalently we obtain \(k = l\). In this case, we have \(\frac{1}{2}(p + 1)\) choices for \(h\). Therefore we get

\[ \text{rank } (M_{(2k+1)p+1}) = \text{rank } (M_{(2k-1)p+1}) + \frac{1}{2}(p + 1). \]

Now the our claim on the rank of \(M_{(2k+1)p+1}\) follows by induction on \(k\).

Then \(a(\mathcal{X}_{(2k+1)p+1}) = \frac{(k + 1)(p - 1)}{2}\) can be computed from

\[ a(\mathcal{X}_{(2k+1)p+1}) = g(\mathcal{X}_{(2k+1)p+1}) - \text{rank } (M_{(2k+1)p+1}). \]

(2) First, we claim that \(\text{rank } (M_{sp+1}) = \frac{k(p + 1)}{2}\), with \(m = 2kp + 1\) and \(k \geq 1\).

In this case, \(i \leq g\) and Eq. (3.2) mod \(p\) reads

\[ i - h - 1 \equiv 0. \quad (3.4) \]

If \(k = 1\), then \(m = 2p + 1\).

Take \(i \in \mathbb{Z}_0^+\) so that \(i = lp + h + 1\), then \(1 \leq lp + h + 1 \leq p\). Thus, we have one choice for \(l\). From this, we have \(\frac{1}{2}(p + 1)\) choice for \(h\), and yielding \(\text{rank } (M_{2p+1}) = \frac{1}{2}(p + 1)\).

If \(k = 2\), then \(m = 4p + 1\), in this case we have
$1 \leq i \leq 2p$. We need to find the solutions $h \mod p$ of the above Eq. (3.4). Then

$1 \leq lp + h + 1 \leq 2p$.

As $h + 1 \geq 0$

\[
\begin{cases}
   l \geq 0 \\
   l < 2.
\end{cases}
\]

Thus, we have two choices for $l$, i.e., $l = 0$ or $l = 1$. From this we have $(p + 1)$ choices for $h$, and yielding rank $(M_{4p+1}) = (p + 1)$.

For $k \geq 3$, and $m = sp + 1$ we can say rank $(M_{2kp+1})$ equals rank $(M_{2(k-1)p+1})$ plus the number of $i$ such that there is $h$ solution of the equation mod $p$

$i \equiv h + 1$

with $1 \leq i \leq 2kp$. Then

$(2k - 2)p \leq lp + h + 1 \leq 2kp$.

Hence

$l = 2k$.

In this case, we have $\frac{1}{2}(p + 1)$ choice for $h$. This implies that

\[
\text{rank} \ (M_{2kp+1}) = \text{rank} \ (M_{2(k-1)p+1}) + \frac{1}{2}(p + 1).
\]

Now our claim on the rank of $M_{2kp+1}$ follows by induction on $k$. Then $a(\mathcal{X}_{2kp+1}) = \frac{(k)(p - 1)}{2}$ can be computed from

$a(\mathcal{X}_{2kp+1}) = g(\mathcal{X}_{2kp+1}) - \text{rank} \ (M_{2kp+1})$.

\[
4 \text{ The $a$-number of $y^2 = x^m + x$}
\]

In this section, we consider the hyperelliptic curve $\mathcal{X}$ given by the equation $y^2 = x^m + x$ over $k$. This curve is of genus $g = (m - 1)/2$ (resp. $g = (m - 2)/2$) if $m$ is odd (resp. $m$ is even).

Let $\mathcal{B} = \{\omega_i = \frac{f^{-i}}{x^i}, i = 1, \ldots, g\}$ be a basis for the differential $1$-forms of the first kind on $\mathcal{X}$. Then the rank of the Cartier operator $\mathcal{C}$ on the curve $\mathcal{X}$ equals the number of $i$ with $i \leq g$ such that

\[
cc\mathcal{C}(\omega_i) = \frac{1}{y}\mathcal{C}(x^{-i}y^{p-1} dx)
\]

\[
= \frac{1}{y}\mathcal{C}\left(x^{-i}(x^{m-1} + 1)^{i-1} dx\right)
\]

\[
= \frac{1}{y}\mathcal{C}\left(\sum_{j=0}^{i-1} a_j x^{j+i-1} dx\right) \neq 0
\]

where $(x^{m-1} + 1)^{\frac{i-1}{2}} = \sum_{j=0}^{i-1} a_j x^{j(m-1)}$. From this, we must have the equation of congruences mod $p$,

\[
i + (m - 1)j - 1 \equiv p - 1,
\]

for some $0 \leq j \leq \frac{(p - 1)}{2}$. Equivalently, the following equation

\[
m(p - 1 - h) + t + i - 1 \equiv p - 1,
\]

has a solution $h$ for $0 \leq t \leq h \leq \frac{p - 1}{2}$.

\[\text{Theorem 4.1} \ Let \mathcal{X} \ be \ a \ hyperelliptic \ curve \ given \ by \ the \ equation \ y^2 = x^m + x. \ If \ m = sp \ for \ s = 2k + 1 \ and \ k \geq 0, \ then \ the \ a\text{-number} \ of \ the \ curve \ \mathcal{X} \ equals \ \frac{(k + 1)(p - 1)}{2}.
\]

\[\text{Proof} \ First, \ we \ claim \ that \ rank \ (M_{sp}) = \frac{k(p + 1)}{2}, \ with \ m = (2k + 1)p \ and \ k \geq 0. \ In \ this \ case, \ i \leq g \ and \ Eq. \ (4.2) \ mod \ p \ reads \ i + t \equiv 0.
\]

\[\text{If} \ k = 0, \ then \ m = p \ where \ i \leq g \ and \ Eq. \ (4.3) \ becomes \ i \equiv -t.
\]

Take $l \in \mathbb{Z}^\times$ such that $i = lp - t$, then $1 \leq lp - t \leq \frac{p}{2}$. From this $t \geq -1$ and $t \geq 0$, a contradiction. Thus, rank $(M_p) = 0$.

If $k = 1$, then $m = 3p$; in this case, we have $\frac{p}{2} \leq i \leq \frac{3p}{2}$.

We need to find the solutions $h \mod p$ of the above Eq. (4.4). Then
\[ \frac{p}{2} \leq lp - t \leq \frac{3p}{2}. \]

As \( t \geq 0 \)
\[
\begin{cases} 
    l \geq 0 \\
    l < 3/2.
\end{cases}
\]

Thus we have two choices for \( l \), i.e., \( l = 0 \) or \( l = 1 \). From this we have \( \frac{1}{2} (p + 1) \) choices for \( t \), and yielding \( \text{rank} \left( M_{2p} \right) = \frac{1}{2} (p + 1) \).

For \( k \geq 2 \), and \( m = sp \) we can say \( \text{rank} \left( M_{(2k+1)p} \right) \) equals \( \text{rank} \left( M_{(2k-1)p} \right) \) plus the number of \( i \) such that there is a solution \( t \) of the equation \( \eta = t \)
\[
\begin{align*}
    i \equiv & -t \\
    \text{with } \left( \frac{2k - 1}{2} \right) & \leq i \leq \left( \frac{2k + 1}{2} \right).
\end{align*}
\]

Then \( \left( \frac{2k - 1}{2} \right) \leq lp - t \leq \left( \frac{2k + 1}{2} \right) \).

Hence
\[ \l = k. \]

In this case we have \( \frac{1}{2} (p + 1) \) choices for \( t \). This implies that
\[
\text{rank} \left( M_{(2k+1)p} \right) = \text{rank} \left( M_{(2k-1)p} \right) + \frac{1}{2} (p + 1).
\]

Now our claim on the rank of \( M_{(2k+1)p} \) follows by induction on \( k \).

Then \( a(X_{(2k+1)p}) = \frac{(k + 1)(p - 1)}{2} \) can be computed from
\[
a(X_{(2k+1)p}) = g(X_{(2k+1)p}) - \text{rank} \left( M_{(2k+1)p} \right).
\]

\[ \square \]

**Author Contributions** All authors contributed to the study’s conception and design. Material preparation, data collection, and analysis were performed by VN, FR, and ST. The first draft of the manuscript was written by VN and all authors commented on previous versions of the manuscript. All authors read and approved the final manuscript. Also, Conceptualization: VN; Methodology: ST; Formal analysis and investigation: FR; Writing - original draft preparation: VN; Writing—review and editing: ST and FR; Supervision: FR; and Software: VN.

**Funding** We express our deep gratitude to the referees for their valuable comments and suggestions which led to improve the exposition. This paper was written while Vahid Nourozi was visiting Unicamp (Universidade Estadual de Campinas) supported by TWAS/CNPq (Brazil) with fellowship number 314966/2018-8 and the third author was supported by CNPq-Brazil (Grant 310194/2019-9).

**Data Availability** The data and code that support the findings of this study are openly available in Magma software at http://magma.maths.usyd.edu.au/

**Declarations**

**Conflict of interest** The authors have not disclosed any conflict of interest.

**Ethical Statement** Hereby, I Farhad Rahmati consciously assure that for the manuscript The a-number of Certain Hyperelliptic Curve the following is fulfilled: (1) This material is the authors’ own original work, which has not been previously published elsewhere. (2) The paper is not currently being considered for publication elsewhere. (3) The paper reflects the authors’ own research and analysis in a truthful and complete manner. (4) The paper properly credits the meaningful contributions of co-authors and co-researchers. (5) The results are appropriately placed in the context of prior and existing research. (6) All sources used are properly disclosed (correct citation). Literally copying of text must be indicated as such by using quotation marks and giving proper reference. (7) All authors have been personally and actively involved in substantial work leading to the paper, and will take public responsibility for its content. I agree with the above statements and declare that this submission follows the policies of Solid State Ionics as outlined in the Guide for Authors and in the Ethical Statement.

**References**

Cartier P (1957) Une nouvelle opération sur les formes différentielles. C R Acad Sci Paris 244:426–428

Cartier P (1958) Questions de rationalité des diviseurs en géométrie algébrique. Bull Soc Math France 86:177–251

González J (1997) Hasse-Witt matrices for the Fermat curves of prime degree. Tohoku Math J 49:149–163

Gross BH (1990) Group representations and lattices. J Am Math Soc 3:929–960

Kodama T, Washio T (1988) Hasse-Witt matrices of Fermat curves. Manuscr Math 60:185–195

Kodama T, Washio T (1990) A family of hyperelliptic function fields with Hasse-Witt invariant zero, J Number Theory 36:187–200

Li K-Z, Oort F (1998) Moduli of supersingular abelian varieties, vol 1680. Lecture Notes in Mathematics, Springer-Verlag, Berlin

Montanucci M, Speziali P (2018) The a-numbers of Fermat and Hurwitz curves. J Pure Appl Algebra 222:477–488

Pries R, Weir C (2015) The Ekedahl-Oort type of Jacobians of Hermitian curves. Asian J Math 19:845–869

Seshadri CS (1958) L’opération de Cartier. Applications. In: Variétés de Picard, vol 4 of Séminaire Claude Chevalley. Secrétariat Mathématiques, Paris, pp 1–26

Stohr K, Voloch JF (1987) A formula for the Cartier operator on plane algebraic curves. J Reine Angew Math 377:49–64

Tafazolian S (2012) A note on certain maximal hyperelliptic curves. Finite Fields Appl 18:1013–1016

Tafazolian S (2012) A family of maximal hyperelliptic curves. J Pure Appl Algebra 216:1528–1532

Tsfasman M, Vladut S, Nogin D (2007) Algebraic geometric codes: basic notions, vol 139 of mathematical surveys and monographs. American Mathematical Society, Providence, RI

Valentini R (1995) Hyperelliptic curves with zero Hasse-Witt matrix. Manuscrpta Math 86:185–194

Yui N (1978) On the Jacobian varieties of hyperelliptic curves over fields of characteristic \( p \geq 2 \). J Algebra 52:378–410