

Transactions on Combinatorics ISSN (print): 2251-8657, ISSN (on-line): 2251-8665 Vol. 10 No. 2 (2021), pp. 121-128. © 2021 University of Isfahan



THE a-NUMBER OF JACOBIANS OF CERTAIN MAXIMAL CURVES

VAHID NOUROZI, SAEED TAFAZOLIAN* AND FARHAD RAHMATI

ABSTRACT. In this paper, we compute a formula for the *a*-number of certain maximal curves given by the equation $y^q + y = x^{\frac{q+1}{2}}$ over the finite field \mathbb{F}_{q^2} . The same problem is studied for the maximal curve corresponding to $\sum_{t=1}^{s} y^{q/2^t} = x^{q+1}$ with $q = 2^s$, over the finite field \mathbb{F}_{q^2} .

1. Introduction

Let \mathcal{C} be a geometrically irreducible, projective, and non-singular algebraic curve defined over the finite field \mathbb{F}_{ℓ} of order ℓ . Let $\mathcal{C}(\mathbb{F}_{\ell})$ denotes the set of \mathbb{F}_{ℓ} -rational points of \mathcal{C} . In the study of curves over finite fields, a fundamental problem is on the size of $\mathcal{C}(\mathbb{F}_{\ell})$. The very basic result here is the Hasse-Weil bound which asserts that

$$| #\mathcal{C}(\mathbb{F}_{\ell}) - (\ell+1) | \le 2g\sqrt{\ell},$$

where $g = g(\mathcal{C})$ is the genus of \mathcal{C} .

The curve \mathcal{C} is called maximal over \mathbb{F}_{ℓ} if the number of elements of $\mathcal{C}(\mathbb{F}_{\ell})$ satisfies

$$#\mathcal{C}(\mathbb{F}_{\ell}) = \ell + 1 + 2g\sqrt{\ell}.$$

We only consider maximal curves of positive genus and hence ℓ will always be a square, say $\ell = q^2$.

•

Communicated by Dariush Kiani

Manuscript Type: Research Paper

 $[\]operatorname{MSC}(2010)$: Primary: 11G20; Secondary: 11M38, 13

Keywords: a-number; Cartier operator; Super-singular Curves; Maximal Curves

Received: 31 August 2020, Accepted: 31 January 2021

^{*}Corresponding author.

http://dx.doi.org/10.22108/toc.2021.124678.1758

In [10], Ihara showed that if a curve C is maximal over \mathbb{F}_{q^2} , then

$$g \le g_1 := \frac{q(q-1)}{2}.$$

In [6] authors showed that

either
$$g \le g_2 := \lfloor \frac{(q-1)^2}{4} \rfloor$$
 or $g_1 = \frac{q(q-1)}{2}$

Rück and Stichtenoth [16] showed that, up to \mathbb{F}_{q^2} -isomorphism, there is just one maximal curve over \mathbb{F}_{q^2} of genus $\frac{q(q-1)}{2}$, namely the so-called Hermitian curve over \mathbb{F}_{q^2} which can be defined by the affine equation

$$y^q + y = x^{q+1}.$$

If q is odd, from [5] there is a unique maximal curve \mathcal{X} over \mathbb{F}_{q^2} of genus $g = \frac{(q-1)^2}{4}$ which can be defined by the affine equation

(1.1)
$$y^q + y = x^{\frac{q+1}{2}}.$$

For q even, from [1] there is a unique maximal curve \mathcal{Y} over \mathbb{F}_{q^2} of genus $g = \lfloor \frac{(q-1)^2}{4} \rfloor = \frac{q(q-2)}{4}$ which can be defined by the affine equation

(1.2)
$$\sum_{t=1}^{s} y^{q/2^{t}} = x^{q+1} \text{ with } q = 2^{s},$$

provided that q/2 is a Weierstrass non-gap at some point of the curve. It is easy to see that a maximal curve C is supersingular, since all slopes of its Newton polygon are equal 1/2. This fact implies that the Jacobin X := Jac(C) has no *p*-torsion points over $\overline{\mathbb{F}}_p$. A relevant invariant of the *p*-torsion group scheme of the Jacobian of the curve is the *a*-number.

Consider the multiplication by p-morphism $[p]: X \to X$ which is a finite flat morphism of degree p^{2g} . It factors as $[p] = V \circ F$. Here, $F: X \to X^{(p)}$ is the relative Frobenius morphism coming from the p-power map on the structure sheaf; and the Verschiebung morphism $V: X^{(p)} \to X$ is the dual of F. The kernel of multiplication-by-p on X, is defined by the group of X[p]. The important invariant is the *a*-number $a(\mathcal{C})$ of curve \mathcal{C} defined by

$$a(\mathcal{C}) = \dim_{\bar{\mathbb{F}}_n} \operatorname{Hom}(\alpha_p, X[p]),$$

where α_p is the kernel of the Frobenius endomorphism on the group scheme $\operatorname{Spec}(k[X]/(X^p))$. Another definition for the *a*-number is

$$a(\mathcal{C}) = \dim_{\mathbb{F}_p}(\operatorname{Ker}(F) \cap \operatorname{Ker}(V)).$$

A few results on the rank of the Carteir operator (especially *a*-number) of curves is introduced by Kodama and Washio [11], Gonzlez [8], Pries and Weir [15], Yui [19] and Montanucci and Speziali [13].

In this paper, we determine the *a*-number of certain maximal curves. In the case $g = g_1$, the *a*-number of the Hermitian curves is computed by Gross in [9]. Here we compute the *a*-number of maximal curves over \mathbb{F}_{q^2} with genus $g = g_2$ for infinitely many values of q.

In Section 3, we prove that the *a*-number of the curve \mathcal{X} with Equation (1.1) is $a(\mathcal{X}) = \frac{p-1}{8}(p^{s-1} + 1)(q-1)$, see Theorem 3.2. In Section 4, we prove that the *a*-number of the curve \mathcal{Y} with Equation (1.2) is $\frac{q^2}{16}$, see Theorem 4.1. The proofs use directly the action of the Cartier operator on $H^0(\mathcal{C}, \Omega^1)$.

2. The Cartier operator

Let k be an algebraically closed field of characteristic p > 0. Let \mathcal{C} be a curve defined over k. The Cartier operator is a 1/p-linear operator acting on the sheaf $\Omega^1 := \Omega^1_{\mathcal{C}}$ of differential forms on \mathcal{C} in positive characteristic p > 0.

Let $K = k(\mathcal{C})$ be the function field of the curve \mathcal{C} of genus g defined over k. A separating variable for K is an element $x \in K \setminus K^p$.

Definition 2.1. (The Cartier operator). Let $\omega \in \Omega_{K/K_q}$. There exist f_0, \ldots, f_{p-1} such that $\omega = (f_0^p + f_1^p x + \cdots + f_{p-1}^p x^{p-1}) dx$. The Cartier operator \mathfrak{C} is defined by

$$\mathfrak{C}(\omega) := f_{p-1} dx$$

The definition does not depend on the choice of x (see [17, Proposition 1]).

We refer the reader to [17, 2, 3, 18] for the proofs of the following statements.

Proposition 2.2. (Global Properties of \mathfrak{C}). For all $\omega \in \Omega_{K/K_q}$ and all $f \in K$,

- $\mathfrak{C}(f^p\omega) = f\mathfrak{C}(\omega);$
- $\mathfrak{C}(\omega) = 0 \Leftrightarrow \exists h \in K, \omega = dh;$
- $\mathfrak{C}(\omega) = \omega \Leftrightarrow \exists h \in K, \omega = dh/h.$

If div(ω) is effective then differential ω is holomorphic. The set $H^0(\mathcal{C}, \Omega^1)$ of holomorphic differentials is a *g*-dimensional *k*-vector subspace of Ω^1 such that $\mathfrak{C}(H^0(\mathcal{C}, \Omega^1)) \subseteq H^0(\mathcal{C}, \Omega^1)$. If \mathcal{C} is a curve, then the *a*-number of \mathcal{C} equals the dimension of the kernel of the Cartier operator $H^0(\mathcal{C}, \Omega^1)$ (or equivalently, the dimension of the space of exact holomorphic differentials on \mathcal{C}) (see [12, 5.2.8]).

The following theorem is due to Gorenstein; see [4, Theorem 12].

Theorem 2.3. A differential $\omega \in \Omega^1$ is holomorphic if and only if it is of the form $(h(x, y)/F_y)dx$, where H : h(X, Y) = 0 is a canonical adjoint.

Theorem 2.4. [13] With the above assumptions,

$$\mathfrak{C}(h\frac{dx}{F_y}) = \left(\frac{\partial^{2p-2}}{\partial x^{p-1}\partial y^{p-1}}(F^{p-1}h)\right)^{\frac{1}{p}}\frac{dx}{F_y}$$

for any $h \in K(\mathcal{X})$.

The differential operator ∇ is defined by

$$\nabla = \frac{\partial^{2p-2}}{\partial x^{p-1} \partial y^{p-1}},$$

has the property

(2.1)
$$\nabla(\sum_{i,j} c_{i,j} X^i Y^j) = \sum_{i,j} c_{ip+p-1,jp+p-1} X^{ip} Y^{jp}.$$

3. The *a*-number of Curve \mathcal{X}

In this section, we consider the curve \mathcal{X} is given by the equation $y^q + y = x^{\frac{q+1}{2}}$ of genus $g(\mathcal{X}) = \frac{(q-1)^2}{4}$, with $q = p^s$ and p > 2 over \mathbb{F}_{q^2} . From Theorem 2.3, one can find a basis for the space $H^0(\mathcal{X}, \Omega^1)$ of holomorphic differentials on \mathcal{X} , namely

$$\mathcal{B} = \{x^i y^j dx \mid 1 \le \frac{q+1}{2}i + qj \le g\}.$$

Proposition 3.1. The rank of the Cartier operator \mathfrak{C} on the curve \mathcal{X} equals the number of pairs (i, j) with $\frac{q+1}{2}i + qj \leq g$ such that the system of congruences mod p

(3.1)
$$\begin{cases} kq + h - k + j \equiv 0, \\ (p - 1 - h)(\frac{(q+1)}{2}) + i \equiv p - 1, \end{cases}$$

has a solution (h,k) for $0 \le h \le \frac{p-1}{2}, 0 \le k \le h$.

Proof. By Theorem 2.4, $\mathfrak{C}((x^iy^j/F_y)dx) = (\nabla(F^{p-1}x^iy^j))^{1/p}dx/F_y$. So, we apply the differential operator ∇ to

(3.2)
$$(y^{q} + y - x^{\frac{q+1}{2}})^{p-1} x^{i} y^{j} = \sum_{h=0}^{p-1} \sum_{k=0}^{h} {\binom{p-1}{h}} {\binom{p-1}{k}} {\binom{p-1}{k}} {\binom{p-1}{k}} {\binom{p-1-h}{2}} {\binom{q+1-h}{2}} {\binom{q+1-h}{2}} {\binom{p-1}{2}} {\binom{p-1}{k}} {$$

for each i, j such that $\frac{q+1}{2}i + qj \leq g$.

From the Formula (2.1), $\nabla (y^q + y + x^{\frac{q+1}{2}})^{p-1} x^i y^j \neq 0$ if and only if for some (h, k), with $0 \leq h \leq \frac{p-1}{2}$ and $0 \leq k \leq h$, satisfies both the following congruences mod p:

(3.3)
$$\begin{cases} kq + h - k + j \equiv 0, \\ (p - 1 - h)(\frac{(q+1)}{2}) + i \equiv p - 1. \end{cases}$$

Take $(i, j) \neq (i_0, j_0)$ in this situation both $\nabla (y^q + y + x^{\frac{q+1}{2}})^{p-1} x^i y^j$ and $\nabla (y^q + y + x^{\frac{q+1}{2}})^{p-1} x^{i_0} y^{j_0}$ are nonzero. We claim that they are linearly independent over k. To show independence, we prove that, for each (h, k) with $0 \leq h \leq p-1$ and $0 \leq k \leq h$ there is no (h_0, k_0) with $0 \leq h_0 \leq p-1$ and $0 \leq k_0 \leq h_0$ such that

(3.4)
$$\begin{cases} kq + h - k + j = k_0q + h_0 - k_0 + j_0, \\ (p - 1 - h)(\frac{(q+1)}{2}) + i = (p - 1 - h_0)(\frac{(q+1)}{2}) + i_0 \end{cases}$$

If $h = h_0$, then $j \neq j_0$ by $i = i_0$ from the second equation, therefore $k \neq k_0$. We may assume $k > k_0$. Then $j - j_0 = (q - 1)(k - k_0) > q - 1$, a contradiction as $j - j_0 \leq \frac{(q-1)^2}{4q}$. Similarly, if $k = k_0$, then Trans. Comb. 10 no. 2 (2021) 121-128

 $h \neq h_0$ by $(i, j) \neq (i_0, j_0)$. We assume that $h > h_0$. Then $i - i_0 = \frac{q+1}{2}(h - h_0) > \frac{q+1}{2}$, a contradiction as $i - i_0 \leq \frac{(q-1)^2}{2(q+1)}$.

For the rest in this Section, $A_s := A(\mathcal{X})$ denotes the matrix representing the *p*-th power of the Cartier operator \mathfrak{C} on the curve \mathcal{X} with respect to the basis \mathcal{B} , where $q = p^s$. Now we are able to compute the *a*-number of curve \mathcal{X} .

Theorem 3.2. If $q = p^s$ for $s \ge 1$ and p > 2, then the a-number of the curve \mathcal{X} equals

$$\frac{p-1}{8}(p^{s-1}+1)(q-1).$$

Proof. First we prove that, if $q = p^s, s \ge 1$, then $\operatorname{rank}(A_s) = \frac{p+1}{8}(p^s-1)(p^{s-1}-1)$. In this case, $\frac{q+1}{2}i + qj \le g$ and System (3.1) mod p reads

(3.5)
$$\begin{cases} h - k + j \equiv 0, \\ -\frac{h}{2} - \frac{1}{2} + i \equiv p - 1 \end{cases}$$

First assume that s = 1, for q = p, we have $\frac{p+1}{2}i + pj \leq g$ and System (3.5) becomes

$$\left\{ \begin{array}{l} j=k-h,\\ i=p+\frac{h}{2}-\frac{1}{2}, \end{array} \right.$$

in this case $\frac{p+1}{2}i + pj \leq g$ that is, $\frac{h(1-3p)}{4} + kp \leq \frac{-p^2-3p+2}{4}$ then $h \geq \frac{-p^2-3p+2}{1-3p}$, thus $h \geq \frac{3p+10}{9}$ a contradiction by Proposition 3.1. As a consequence, there is no pair (i, j) for which the above system admits a solution (h, k). Thus, rank $(A_1) = 0$.

Let s = 2, so $q = p^2$. For $\frac{p^2+1}{2}i + p^2j \leq g$, the above argument still works. Therefore, $\frac{(p-1)^2}{4} + 1 \leq \frac{p^2+1}{2}i + p^2j \leq \frac{(p^2-1)^2}{4}$ and our goal is to determine for which (i, j) there is a solution (h, k) of the system mod p

$$\begin{cases} h - k + j \equiv 0, \\ -\frac{h}{2} - \frac{1}{2} + i \equiv p - 1 \end{cases}$$

Take $l, m \in Z_0^+$ so that

$$\begin{cases} j = lp + k - h, \\ i = mp + p + \frac{h}{2} - \frac{1}{2} \end{cases}$$

In this situation, $i < \frac{2g}{p^2+1} = \frac{(p^2-1)^2}{2(p^2+1)}$, so $mp + p + \frac{h}{2} - \frac{1}{2} \leq \frac{(p^2-1)^2}{2(p^2+1)}$. Then $m \leq \frac{(p^2-1)^2}{2(p^2+1)}$. And $j < \frac{(p^2-1)^2}{4p^2}$, so $lp + k - h < \frac{(p^2-1)^2}{4p^2}$, Then $l < \frac{(p^2-1)^2}{4p^2}$. From this we can say that $\frac{p^2-1}{4} - 1 \leq l \leq \frac{p^2-1}{4}$, and $\frac{p^2-1}{2} \leq m \leq \frac{p^2-1}{2}$. In this way, $\frac{(p^2-1)^2}{8}$ suitable values for (i, j) are obtained, whence $\operatorname{rank}(A_2) = \frac{(p^2-1)^2}{8}$.

For $s \ge 3$, rank (A_s) equals rank (A_{s-1}) plus the number of pairs (i, j) with $\frac{(p^{s-1}-1)^2}{4} + 1 \le \frac{q+1}{2}i + qj \le \frac{(p^s-1)^2}{4}$ such that the system mod p

$$\begin{cases} h - k + j \equiv 0, \\ -\frac{h}{2} - \frac{1}{2} + i \equiv p - 1 \end{cases}$$

has a solution. With our usual conventions on l, m, a computation shows that such pairs (i, j) are obtained for $0 \le l \le \frac{(p^s-1)^2}{4p^{s+1}}$ from this we have $\frac{p^{s-2}(p^2-1)}{4} - 1 \le l \le \frac{p^{s-2}(p^2-1)}{4}$, and $0 \le m \le \frac{(p^s-1)^2}{2(p^s+1)}$ from this we have $\frac{(p^{s-1}-1)(p+1)}{2} - 1 \le m \le \frac{(p^{s-1}-1)(p+1)}{2}$. In this case we have

$$\frac{(p^{s-1}-1)(p+1)p^{s-2}(p^2-1)}{8}$$

choices for (h, k). Therefore we get

$$\operatorname{rank}(A_s) = \operatorname{rank}(A_{s-1}) + \frac{(p^{s-1} - 1)(p+1)p^{s-2}(p^2 - 1)}{8}.$$

Now our claim on the rank of A_s follows by induction on s. Hence

$$\begin{aligned} a(\mathcal{X}) &= \frac{(p^s - 1)^2}{4} - \frac{(p + 1)(p^s - 1)(p^{s-1} - 1)}{8} \\ &= \frac{(p^s - 1)}{8}(p^s + p - p^{s-1} - 1) \\ &= \frac{(p^s - 1)}{8}(p(p^{s-1} + 1) - (p^{s-1} + 1)) \\ &= \frac{(p^s - 1)}{8}((p^{s-1} + 1)(p - 1)) \\ &= \frac{(p - 1)}{8}((p^{s-1} + 1)(q - 1)). \end{aligned}$$

For the finite feild \mathbb{F}_{q^2} let m be an integer number, such that m divides (q+1). In this case the curve $y^q + y = x^m$ is maximal over \mathbb{F}_{q^2} . From this fact we are led to the following problem.

Problem 3.3. What is the dimension of the space of exact holomorphic differentials of $y^q + y = x^m$ where $m \mid (q+1)$

4. The *a*-number of Curve \mathcal{Y}

In this section, we consider the curve \mathcal{Y} given by the equation $\sum_{t=1}^{s} y^{q/2^{t}} = x^{q+1}$ of genus $g(\mathcal{Y}) = \frac{q(q-2)}{4}$, with $q = 2^{s}$ and p = 2 over $\mathbb{F}_{q^{2}}$. With the simple computation, we have $\operatorname{div}_{\infty}(x) = q/2P_{1}$ and $\operatorname{div}_{\infty}(y) = (q+1)P_{1}$, so one can find a basis for the space $H^{0}(\mathcal{Y}, \Omega^{1})$ of holomorphic differentials on \mathcal{Y} , namely

(4.1)
$$\mathcal{B}' = \{ x^i y^j dx \mid (q+1)i + \frac{q}{2}j \le 2g - 2 \}.$$

Theorem 4.1. If $q = 2^s$ for $s \ge 1$, then the a-number of the curve \mathcal{Y} equals

http://dx.doi.org/10.22108/toc.2021.124678.1758

 $\frac{q^2}{16}.$

Proof. In characteristic two, every 1-form $\omega \in H^0(\mathcal{Y}, \Omega^1)$ can be written as $\omega = (f^2 + g^2 x)dx$. So we have

(4.2)
$$\mathfrak{C}((f^2 + g^2 x)dx) = gdx$$

in characteristic two. By Equation (4.2), *a*-number of \mathcal{Y} is the dimensional vector space of regular 1-forms of the form $f^2 dx$. For each even integers i, j, we have $\mathfrak{C}(x^i y^j dx) = 0$. So we want to find (i, j), where i is an odd number and j is an even number. We know that $0 \leq i \leq \frac{2g-2}{2(q+1)}$ and $0 \leq j \leq \frac{2g-2}{2q}$. Therefore this follows from the fact that

$$\frac{q}{4} - 1 < \frac{2g - 2}{2(q + 1)} < \frac{q}{4}$$

there are $\frac{q}{4}$ choices of *i* and from the fact that

$$\frac{q}{4}-1<\frac{2g-2}{2q}<\frac{q}{4}$$

there are $\frac{q}{4}$ choices of j. Hence

$$a(\mathcal{Y}) = \frac{q^2}{16}$$

Acknowledgments

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 second author was supported by FAPESP/SP-Brazil grant 2018/24604 - 6.

References

- [1] M. Abdon and F. Torres, On maximal curves in characteristic two, Manuscripta Math., 99 (1999) 39–53.
- [2] P. Cartier, Une nouvelle opration sur les formes diffrentielles. C. R. Acad. Sci. Paris, 244 (1957) 426-428.
- [3] P. Cartier, Questions de rationalit des diviseurs en gomtrie algbrique, Bull. Soc. Math. France, 86 (1958) 177–251.
- [4] D. Gorenstein, An arithmetic theory of adjoint plane curves, Trans. Am. Math. Soc., 72 (1952) 414-436.
- [5] R. Fuhrmann, A. Garcia and F. Torres, On maximal curves, J. Number Theory, 67 (1997) 29-51.
- [6] R. Fuhrmann and F. Torres, The genus of curves over finite fields with many rational points, *Manuscripta Math*, 89 (1996) 103–106.
- [7] H. Friedlander, D. Garton, B. Malmskog, R. Pries and C. Weir, The a-number of Jacobians of Suzuki curves, Proc. Amer. Math. Soc., 141 (2013) 3019–3028.
- [8] J. Gonzlez, Hasse-Witt matrices for the Fermat curves of prime degree, Tohoku Math. J., 49 (1997) 149–163.
- [9] B. H. Gross, Group representations and lattices, J. Am. Math. Soc., 3 (1990) 929–960.
- [10] Y. Ihara, Some remarks on the number of rational points of algebraic curves over finite fields, J. Fac. Sci. Tokyo, 28 (1981) 721–724.
- [11] T. Kodama and T. Washio, Hasse-Witt matrices of Fermat curves, Manuscr. Math., 60 (1988) 185–195.

- [12] K.-Z. Li and F. Oort, Moduli of Supersingular Abelian Varieties, Lecture Notes in Mathematics, 1680, Springer-Verlag, Berlin, 1998, iv+116pp.
- [13] M. Montanucci and P. Speziali, The a-numbers of Fermat and Hurwitz curves, J. Pure Appl. Algebra, 222 (2018) 477–488.
- [14] V. Nourozi, F. Rahmati and S. Tafazolian, The a-number of certain hyperelliptic curves, ArXiv: 1902.03672v2, 2019.
- [15] R. Pries and C. Weir, The Ekedahl-Oort type of Jacobians of Hermitian curves, Asian J. Math., 19 (2015) 845–869.
- [16] H. G. Rück and H. Stichtenoth, A characterization of Hermitian function fields over finite fields, J. Reine Angew. Math., 457 (1994) 185–188.
- [17] C. S. Seshadri, Loperation de Cartier, Applications, In Varietes de Picard, 4, of Sminaire Claude Chevalley. Secrtariat Mathmatiques, Paris, 1958–1959.
- [18] M. Tsfasman, S. Vladut and D. Nogin, Algebraic geometric codes: basic notions, 139, of Mathematical Surveys and Monographs, American Mathematical Society, Providence, RI, 2007.
- [19] N. Yui, On the Jacobian Varieties of Hyperelliptic Curves over Fields of Characteristic p, J. Algebra, 52 (1978) 378–410.

Vahid Nourozi

Faculty of Mathematics and Computer Science, Amirkabir University of Technology (Tehran Polytechnic), 424 Hafez Ave., Tehran 15914, Iran

Email: nourozi@aut.ac.ir

Saeed Tafazolian

IMECC/UNICAMP, R. Sergio Buarque de Holanda, 651, Cidade Universitaria, Zeferino Vaz, 13083-859, Campinas, SP, Brazil

Email: tafazolian@ime.unicamp.br

Farhad Rahmati

Faculty of Mathematics and Computer Science, Amirkabir University of Technology, (Tehran Polytechnic), 424 Hafez Ave., Tehran 15914, Iran

Email: frahmati@aut.ac.ir