



The a -number of maximal curves of third largest genus

Vahid Nourozi^a, Saeed Tafazolian^{*b}

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

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

ABSTRACT: The a -number is an invariant of the isomorphism class of the p -torsion group scheme. In this paper, we compute a closed formula for the a -number of $y^q + y = x^{\frac{q+1}{3}}$ and $\sum_{t=1}^s y^{q/3^t} = x^{q+1}$ with $q = 3^s$ over the finite field \mathbb{F}_{q^2} using the action of the Cartier operator on $H^0(\mathcal{C}, \Omega^1)$.

Review History:

Received:07 September 2021

Accepted:10 October 2021

Available Online:01 February 2022

Keywords:

a -Number

Cartier operator

Super-singular Curves

Maximal Curves

AMS Subject Classification (2010):

11G20; 14G15; 14H25

1. Introduction

Let \mathcal{C} be an irreducible, non-singular, projective algebraic curve defined over the finite field \mathbb{F}_{q^2} with q^2 elements. The famous Hasse-Weil bound states that \mathcal{C} can have at most $q + 1 + 2g(\mathcal{C})\sqrt{q}$ points defined over \mathbb{F}_{q^2} , where $g(\mathcal{C})$ denotes the genus of the curve \mathcal{C} . The curve \mathcal{C} is called \mathbb{F}_{q^2} -maximal if it attains the Hasse-Weil bound.

An important and well-studied example of an \mathbb{F}_{q^2} -maximal curve is given by Hirschfeld, J.W.P., et al., see [9]. It is a plane curve, which the affine equation can define

$$y^q + y = x^{\frac{q+1}{3}}, \quad (1)$$

where $g(\mathcal{C}) = \frac{(q-1)(q-2)}{6}$ and $p \equiv 2 \pmod{3}$. And there is a unique maximal curve \mathcal{C} over \mathbb{F}_{q^2} of genus $g = \frac{q(q-3)}{6}$, which can be defined by the affine equation

$$\sum_{t=1}^s y^{q/3^t} = x^{q+1} \quad \text{with } q = 3^s, \quad (2)$$

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

*Corresponding author.

E-mail addresses: nourozi@aut.ac.ir, nourozi.v@gmail.com, saeed@unicamp.br

A few results on the rank of the Cartier operator (especially a -number) of curves are introduced by Kodama and Washio [11], González [5], Pries and Weir [16], Yui [22], and Montanucci and Speziali [13] and, Nourozi, Tafazolian and Rahmati [14, 15].

In this paper, we determine the a -number of maximal curves of third largest genus.

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 $\Omega^1 := \Omega_{\mathcal{C}}^1$ 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 $\omega \in \Omega_{K/K^p}$. There exist f_0, \dots, f_{p-1} such that $\omega = (f_0^p + f_1^p x + \dots + f_{p-1}^p x^{p-1})dx$. 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 [18, Proposition 1]).

We refer the reader to [18, 2, 3, 20] for the proofs of the following statements.

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

- $\mathfrak{C}(f^p \omega) = f \mathfrak{C}(\omega)$;
- $\mathfrak{C}(\omega) = 0 \Leftrightarrow \exists h \in K, \omega = dh$;
- $\mathfrak{C}(\omega) = \omega \Leftrightarrow \exists h \in K, \omega = dh/h$;
- $\mathfrak{C}(\omega_1 + \omega_2) = \mathfrak{C}(\omega_1) + \mathfrak{C}(\omega_2)$.

Remark 2.3. Moreover, one can easily show that

$$\mathfrak{C}(x^j dx) = \begin{cases} 0 & \text{if } p \nmid j + 1 \\ x^{s-1} dx & \text{if } j + 1 = ps. \end{cases}$$

This operator \mathfrak{C} induces a map $\mathfrak{C} : H^0(\mathcal{C}, \Omega^1) \rightarrow H^0(\mathcal{C}, \Omega^1)$ which is σ^{-1} -linear, that is, it satisfies Proposition 2.2, with σ^{-1} denoting the Frobenius automorphism of k . We are interested in the relation between the rank of the Cartier operator, defined as $\dim_k H^0(\mathcal{C}, \Omega^1)$, and the genus $g(\mathcal{C})$.

The important invariant is the a -number $a(\mathcal{C})$ of curve \mathcal{C} defined by

$$a(\mathcal{C}) := \dim_k \text{Hom}(\alpha_p, X[p]),$$

where α_p is the kernel of the Frobenius endomorphism on the group scheme \mathbb{G}_a ($\alpha_p \simeq \text{Spec}(k[x]/x^p)$ as a scheme), and the group scheme $X[p]$ is the kernel of multiplication-by- p on X . When $X = J(\mathcal{C})$, the Jacobian variety of a curve \mathcal{C} , we write $a(\mathcal{C})$ instead of a $J(\mathcal{C})$ and refer to it as the a -number of \mathcal{C} . Another definition for the a -number is

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

The following theorem is due to Gorenstein; see [6, Theorem 12].

Theorem 2.4. 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 2.5. [13] With the above assumptions,

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

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 following property

$$\nabla\left(\sum_{i,j} c_{i,j} X^i Y^j\right) = \sum_{i,j} c_{ip+p-1, jp+p-1} X^{ip} Y^{jp}. \tag{3}$$

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

In this section, we assume that the curve \mathcal{X} is given by the equation $y^q + y = x^{\frac{q+1}{3}}$ of genus $g(\mathcal{X}) = \frac{(q-1)(q-2)}{6}$, with $q = p^s$ and $q \equiv 2 \pmod 3$ over \mathbb{F}_{q^2} . From Theorem 2.4, one can find a basis for the space $H^0(\mathcal{X}, \Omega^1)$ of holomorphic differentials on \mathcal{X} , namely

$$\mathcal{B} = \{x^i y^j dx \mid 1 \leq \frac{q+1}{3}i + qj \leq g\}.$$

Proposition 3.1. *The rank of the Cartier operator \mathfrak{C} on the curve \mathcal{X} equals the number of pairs (i, j) with $\frac{q+1}{3}i + qj \leq g$ such that the system of congruences mod p*

$$\begin{cases} kq + h - k + j \equiv 0, \\ (p - 1 - h)\left(\frac{q+1}{3}\right) + i \equiv p - 1, \end{cases} \quad (4)$$

has a solution (h, k) for $0 \leq h \leq \lfloor \frac{p-1}{3} \rfloor, 0 \leq k \leq h$.

Proof. By Theorem 2.5, $\mathfrak{C}((x^i y^j / F_y) dx) = (\nabla(F^{p-1} x^i y^j))^{1/p} dx / F_y$. So, by applying the differential operator ∇ to

$$(y^q + y - x^{\frac{q+1}{3}})^{p-1} x^i y^j = \sum_{h=0}^{p-1} \sum_{k=0}^h \binom{p-1}{h} \binom{h}{k} (-1)^{h-k} x^{(p-1-h)\left(\frac{q+1}{3}\right)+i} y^{kq+h-k+j} \quad (5)$$

for each i, j such that $\frac{q+1}{3}i + qj \leq g$.

From the Formula (3), $\nabla(y^q + y - x^{\frac{q+1}{3}})^{p-1} x^i y^j \neq 0$ if and only if for some (h, k) , with $0 \leq h \leq \lfloor \frac{p-1}{3} \rfloor$ and $0 \leq k \leq h$, satisfies both the following congruences mod p :

$$\begin{cases} kq + h - k + j \equiv 0, \\ (p - 1 - h)\left(\frac{q+1}{3}\right) + i \equiv p - 1. \end{cases} \quad (6)$$

Take $(i, j) \neq (i_0, j_0)$, in this situation both $\nabla(y^q + y - x^{\frac{q+1}{3}})^{p-1} x^i y^j$ and $\nabla(y^q + y - x^{\frac{q+1}{3}})^{p-1} x^{i_0} y^{j_0}$ are nonzero. We claim that they are linearly independent over k . To show independence, we prove that, for each (h, k) with $0 \leq h \leq \lfloor \frac{p-1}{3} \rfloor$ and $0 \leq k \leq h$ there is no (h_0, k_0) with $0 \leq h_0 \leq \lfloor \frac{p-1}{3} \rfloor$ and $0 \leq k_0 \leq h_0$ such that

$$\begin{cases} kq + h - k + j = k_0q + h_0 - k_0 + j_0, \\ (p - 1 - h)\left(\frac{q+1}{3}\right) + i = (p - 1 - h_0)\left(\frac{q+1}{3}\right) + i_0. \end{cases} \quad (7)$$

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 $j - j_0 \leq \frac{(q-1)(q-2)}{6q}$. Similarly, if $k = k_0$, then $h \neq h_0$ by $(i, j) \neq (i_0, j_0)$. We assume that $h > h_0$. Then $i - i_0 = \frac{q+1}{3}(h - h_0) > \frac{q+1}{3}$, a contradiction as $i - i_0 \leq \frac{(q-1)(q-2)}{3(q+1)}$. \square

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 odd $s \geq 1$, $p > 2$ and $p \equiv 2 \pmod 3$, then the a -number of the curve \mathcal{X} equals*

$$\frac{(q-1)(q-2) - (3q-8)(p^{s-1} - 1)}{6}.$$

Proof. First we prove that, if $q = p^s, s \geq 1$ and be odd where $p \equiv 2 \pmod 3$, then $\text{rank}(A_s) = \frac{(3q-8)(p^{s-1} - 1)}{6}$.

In this case, $\frac{q+1}{3}i + qj \leq g$ and System (4) mod p reads

$$\begin{cases} h - k + j \equiv 0, \\ -\frac{h}{3} - \frac{1}{3} + i \equiv p - 1. \end{cases} \quad (8)$$

First assume that $s = 1$, for $q = p$, we have $\frac{p+1}{3}i + pj \leq g$ and System (8) becomes

$$\begin{cases} j = k - h, \\ i = p + \frac{h}{3} - \frac{2}{3}, \end{cases}$$

in this case $\frac{p+1}{3}i + pj \leq g$ that is, $\frac{h(1-16p)}{3} + 6kp \leq \frac{-3p^2-13p+8}{3}$ then $h \geq \frac{-3p^2-13p+8}{1-16p}$ 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, $\text{rank}(A_1) = 0$.

Let $s = 3$, so $q = p^3$. For $\frac{p^3+1}{3}i + p^3j \leq g$, the above argument still works. Therefore, $\frac{(p-1)(p-2)}{6} + 1 \leq \frac{p^3+1}{3}i + p^3j \leq \frac{(p^3-1)(p^3-2)}{6}$ and our goal is to determine for which (i, j) there is a solution (h, k) of the system mod p

$$\begin{cases} h - k + j \equiv 0, \\ -\frac{h}{3} - \frac{1}{3} + i \equiv p - 1. \end{cases}$$

Take $l, m \in \mathbb{Z}_0^+$ so that

$$\begin{cases} j = lp + k - h, \\ i = mp + p + \frac{h}{3} - \frac{2}{3}. \end{cases}$$

In this situation, $i < \frac{3g}{p^3+1} = \frac{(p^3-1)(p^3-2)}{2(p^3+1)}$, so $mp + p + \frac{h}{3} - \frac{2}{3} \leq \frac{(p^3-1)(p^3-2)}{2(p^3+1)} \leq \frac{3p^3-8}{6}$. Then $m \leq \frac{3p^3-8}{6}$. And $j < \frac{(p^3-1)(p^3-2)}{6p^3}$, so $lp + k - h < \frac{(p^3-1)(p^3-2)}{6p^3} \leq p^2 - 1$, Then $l < p^2 - 1$. In this way, $\frac{(p^2-1)(3p^3-8)}{6}$ suitable values for (i, j) are obtained, whence $\text{rank}(A_2) = \frac{(p^2-1)(3p^3-8)}{6}$.

For $s \geq 5$, $\text{rank}(A_s)$ equals $\text{rank}(A_{s-1})$ plus the number of pairs (i, j) with $\frac{(p^{s-1}-1)(p^{s-1}-2)}{6} + 1 \leq \frac{q+1}{3}i + qj \leq \frac{(p^s-1)(p^s-2)}{6}$ such that the system mod p

$$\begin{cases} h - k + j \equiv 0, \\ -\frac{h}{3} - \frac{1}{3} + i \equiv p - 1, \end{cases}$$

has a solution. With our usual conventions on l, m , a computation shows that such pairs (i, j) are obtained for $0 \leq m \leq \frac{(p^s-1)(p^s-2)}{2(p^s+1)}$ from this we have $p^{s-2}(p-1) - 1 \leq m \leq p^{s-2}(p-1)$, and $0 \leq l \leq \frac{(p^s-1)(p^s-2)}{6p^s}$ from this we have $\frac{3(p^{s-1}-1)(p+1)-5}{6} - 1 \leq t \leq \frac{3(p^{s-1}-1)(p+1)-5}{6}$. In this case we have

$$\frac{(3(p^{s-1} - 1)(p + 1) - 5)p^{s-2}(p - 1)}{6}$$

choices for (h, k) . Therefore we get

$$\text{rank}(A_s) = \text{rank}(A_{s-1}) + \frac{(3(p^{s-1} - 1)(p + 1) - 5)p^{s-2}(p - 1)}{6}.$$

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

$$\begin{aligned} a(\mathcal{X}) &= \frac{(p^s - 1)(p^s - 2)}{6} - \frac{(3p^s - 8)(p^{s-1} - 1)}{6} \\ &= \frac{(p^s - 1)(p^s - 2) - (3p^s - 8)(p^{s-1} - 1)}{6}. \end{aligned}$$

□

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

In this section, we consider the curve \mathcal{Y} is given by the equation $\sum_{t=1}^s y^{q/3^t} = x^{q+1}$ of genus $g(\mathcal{Y}) = \frac{q(q-3)}{6}$, with $q = 3^s$ and $p = 3$ over \mathbb{F}_{q^2} . With the simple computation, we have $\text{div}(x) = q/3P_1$ and $\text{div}(y) = (q+1)P_1$ so one can find a basis for the space $H^0(\mathcal{Y}, \Omega^1)$ of holomorphic differentials on \mathcal{Y} , namely

$$\mathcal{B} = \{x^i y^j dx \mid (q+1)i + \frac{q}{3}j \leq 2g - 2\}.$$

Theorem 4.1. *If $q = 3^s$ and $s \geq 1$, then the a -number of the curve \mathcal{Y} equals*

$$\frac{q(q+1)}{18}.$$

Proof. We want to find (i, j) that $\mathfrak{C}(x^i y^j dx) = 0$. We know that $0 \leq i \leq \frac{2g-2}{q+1}$ and $0 \leq j \leq \frac{3(2g-2)}{q}$. Therefore this follows from the fact that

$$\frac{q}{9} - 1 < \frac{2g-2}{q+1} < \frac{q}{9},$$

there are $\frac{q}{9}$ choices of i and from the fact that

$$\frac{q+1}{2} - 1 < \frac{3(2g-2)}{q} < \frac{q+1}{2},$$

there are $\frac{q+1}{2}$ choices of j . Hence

$$a(\mathcal{Y}) = \frac{q(q+1)}{18}.$$

□

Example 4.1. consider the curve \mathcal{Y} with function field $K(x, y)$ given by

$$y + y^3 = x^{10}.$$

It is easily seen that a basis for $H^0(\mathcal{X}, \Omega^1)$ is given by

$$\mathcal{B} = \{dx, xdx, x^2dx, x^3dx, x^4dx, x^5dx, ydx, xydx, x^2ydx\}.$$

Let us compute the image of $\mathfrak{C}(\omega)$ for any $\omega \in \mathcal{B}$. It is straightforward to see that

$$\mathfrak{C}(dx) = \mathfrak{C}(xdx) = \mathfrak{C}(x^3dx) = \mathfrak{C}(x^4dx) = 0.$$

Also,

$$\mathfrak{C}(ydx) = \mathfrak{C}((x(x^3)^3 - y^3)dx) = 0.$$

It is also straightforward to see that

$$\mathfrak{C}(x^2dx) = dx, \quad \mathfrak{C}(x^5dx) = xdx.$$

Finally,

$$\mathfrak{C}(xydx) = x^3dx, \quad \mathfrak{C}(x^2ydx) = -ydx.$$

Hence, $a(\mathcal{Y}) = 5$.

Acknowledgements. 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 CNPq-Brazil (Grant 310194/2019-9).

References

- [1] W. Bosma, J. Cannon, C. Playoust, The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235-265, (1997). Computational algebra and number theory (London, 1993).
- [2] P. Cartier. Une nouvelle opération sur les formes différentielles, *C. R. Acad. Sci. Paris*, 244 (1957), 426-428.
- [3] P. Cartier. Questions de rationalité des diviseurs en géométrie algébrique, *Bull. Soc. Math. France*, 86 (1958), 177-251.
- [4] R. Fuhrmann, F. Torres, The genus of curves over finite fields with many rational points, *Manuscripta Math.* 89 (1996), 103-106.
- [5] J. González, Hasse-Witt matrices for the Fermat curves of prime degree, *Tohoku Math. J.* 49 (1997), 149-163.
- [6] D. Gorenstein, An arithmetic theory of adjoint plane curves, *Trans. Am. Math. Soc.* 72 (1952), 414-436.
- [7] B. H. Gross, Group representations and lattices, *J. Am. Math. Soc.* 3, (1990), 929-960.
- [8] J. Hirschfeld, G. Korchmáros, et al., On the number of rational points on an algebraic curve over a finite field, *Bulletin of the Belgian Mathematical Society-Simon Stevin*, 5 (1998), 313-340.
- [9] J. Hirschfeld, G. Korchmáros, F. Torre., Algebraic Curves over a Finite Field, PRINCETON; OXFORD: Princeton University Press, 2008. Accessed February 13, (2021). doi:10.2307/j.ctt1287kdw.
- [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, T. Washio, Hasse-Witt matrices of Fermat curves, *Manuscr. Math.* 60, (1988), 185-195.
- [12] K.-Z. Li, F. Oort, *Moduli of Supersingular Abelian Varieties*, Lecture Notes in Mathematics, vol.1680, Springer-Verlag, Berlin, (1998), iv+116pp.
- [13] M. Montanucci, P. Speziali, The a -numbers of Fermat and Hurwitz curves, *J. Pure Appl. Algebra*, 222, (2018), 477-488.
- [14] V. Nourozi, F. Rahmati, S. Tafazolian, The a -number of certain hyperelliptic curves, *ArXiv: 1902.03672v2*, (2019).
- [15] V. Nourozi, S. Tafazolian, F. Rahmati, The a -number of jacobians of certain maximal curves, *Transactions on Combinatorics*, 10 (2), (2021), 121-128.
- [16] R. Pries, C. Weir, The Ekedahl-Oort type of Jacobians of Hermitian curves, *Asian J. Math.* 19, (2015), 845-869.
- [17] H. G. Ruck, H. Stichtenoth, A characterization of Hermitian function fields over finite fields, *J. Reine Angew. Math.* 457 (1994), 185-188.
- [18] C. S. Seshadri, L'opération de Cartier. Applications, In *Variétés de Picard*, volume 4 of Séminaire Claude Chevalley. Secrétariat Mathématiques, Paris, 1958-1959.
- [19] S. Tafazolian, F. Torres, On the curve $y^n = x^m + x$ over finite fields, *Journal of Number Theory*, 145 (2014), 51-66.
- [20] M. Tsfasman, S. Vladut, D. Nogin, *Algebraic geometric codes: basic notions*, volume 139 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 2007.
- [21] K. Yang, P. V. Kumar, H. Stichtenoth, On the weight hierarchy of geometric Goppa codes, *IEEE Trans. Inform. Theory*, 40 (1994), 913-920.
- [22] N. Yui, On the Jacobian Varieties of Hyperelliptic Curves over Fields of Characteristic p , *J. Algebra*, 52 (1978), 378-410.

Please cite this article using:

Vahid Nourozi, Saeed Tafazolian, The a -number of maximal curves of third largest genus,
AUT J. Math. Com., 3(1) (2022) 11-16
DOI: 10.22060/AJMC.2021.20511.1069

