Bulletin of the Iranian Mathematical Society Vol. 39 *No. 3 (2013), pp 405-413.*

A NOTE ON SUPERSPECIAL AND MAXIMAL CURVES

A. KAZEMIFARD, A. R. NAGHIPOUR AND S. TAFAZOLIAN*

Communicated by Teo Mora

ABSTRACT. In this note we review a simple criterion, due to Ekedahl, for superspecial curves defined over finite fields. Using this we generalize and give some simple proofs of some well-known results on superspecial curves.

1. Introduction

Let k be an algebraically closed field of characteristic $p > 0$. A curve of genus 1 is said to be supersingular if, as an elliptic curve defined over k, its group of p-torsion k-points is trivial. A curve $\mathcal{C}$ of genus $g > 1$ is said to be supersingular if its Jacobian variety $\mathcal{J}_{\mathcal{C}}$ is isogenous, as an abstract abelian variety, to the product of g supersingular elliptic curves. One property of supersingular curves which can be stated in elementary terms is the following. We know after A. Weil that the number of $\mathbb{F}_q$-points of a curve of genus g defined over $\mathbb{F}_q$ satisfies the following limitations:

$$q + 1 - 2g\sqrt{q} \leq \#\mathcal{C}(\mathbb{F}_q) \leq 1 + q + 2g\sqrt{q},$$

where $\mathcal{C}(\mathbb{F}_q)$ denotes the set of $\mathbb{F}_q$-rational points of the curve $\mathcal{C}$.

MSC(2010): Primary: 11G20; Secondary: 11M38, 14G15.
Keywords: Cartier operator, supersingular curves, finite fields, maximal curves.
Received: 8 October 2011, Accepted: 30 March 2012.
*Corresponding author

Here we are interested in maximal (resp. minimal) curves over $\mathbb{F}_{q^2}$, that is, we will consider curves $\mathcal{C}$ attaining Hasse-Weil's upper (lower, respectively) bound:

$$\#\mathcal{C}(\mathbb{F}_{q^2}) = q^2 + 1 + 2gq \ (\ q^2 + 1 - 2gq).$$

It is easy to see that a maximal (or minimal) curve $\mathcal{C}$ is supersingular, since all slopes of its Newton polygon are equal to $1/2$. On the other hand, if a curve $\mathcal{C}$ defined over a finite field $\mathbb{F}_q$ is supersingular, then $\mathcal{C}$ is maximal or minimal over some finite extensions of $\mathbb{F}_q$.

Among supersingular curves there is an interesting class called superspecial, which are curves such that their Jacobian (over an algebraically closed field) is isomorphic to product of supersingular elliptic curves. On the other hand, according to Nygaard [7] we know that if $\mathcal{C}$ is a curve defined over k, then the curve $\mathcal{C}$ is superspecial if and only if the Cartier operator $\mathbb{C} : H^0(\mathcal{C}, \Omega^1_{\mathcal{C}}) \to H^0(\mathcal{C}, \Omega^1_{\mathcal{C}})$ vanishes identically.

In this paper we review a simple criterion due to Ekedahl for superspecial curves defined over finite fields. In fact, it has been shown that a curve $\mathcal{C}$ over a field k is superspecial if and only if $\mathcal{C}$ descends to a maximal or minimal curve over $\mathbb{F}_{p^2}$, where $p = \mathrm{char}(k)$ (see Theorem 2.6).

Then using this result, we give generalization and some simple proofs of some of the results in [11] and [13] (see Section 3).

2. **Main Results**

In this section first we review some well-known properties of maximal and minimal curves.

Let $\mathcal{C}$ be a curve of genus $g > 0$ over the finite field $\mathbb{F}_q$ with q elements. The *zeta function* of $\mathcal{C}$ is a rational function of the form

$$Z(\mathcal{C}/\mathbb{F}_q) = \frac{L_{\mathcal{C}}(t)}{(1-t)(1-qt)},$$

where $L_{\mathcal{C}}(t) \in \mathbb{Z}[t]$ is a polynomial of degree $2g$ with integral coefficients. From [10, p. 229] we know that a curve $\mathcal{C}$ is maximal (minimal, respectively) over $\mathbb{F}_{q^2}$ if and only if $L_{\mathcal{C}}(t) = (1+qt)^{2g}$ ($L_{\mathcal{C}}(t) = (1-qt)^{2g}$, respectively).

We recall the following basic result concerning Jacobians. Let $\mathcal{C}$ be a curve, $\mathscr{F}$ the Frobenius endomorphism (relative to the base field) of the Jacobian $\mathcal{J}$ of $\mathcal{C}$, and let $h(t) = t^{2g}L(t^{-1})$ be the characteristic polynomial of $\mathscr{F}$. Let $h(t) = \prod_{i=1}^{T} h_i(t)^{r_i}$ be the irreducible factorization

of $h(t)$ over $\mathbb{Z}[t]$. Then

$$\prod_{i=1}^{T} h_i(\mathbb{F}) = 0 \quad \text{on} \quad \mathcal{J}. \tag{2.1}$$

This follows from the semisimplicity of $\mathbb{F}$ and the fact that the representation of endomorphisms of $\mathcal{J}$ on the Tate module is faithful (see [12, Theorem 2] and [5, VI, Section 3]). In the case of a maximal curve over $\mathbb{F}_{q^2}$, we have $h(t) = (t+q)^{2g}$. Therefore from (2.1) we obtain the following result, which is contained in the proof of [9, Lemma 1].

Lemma 2.1. *The curve $\mathcal{C}$ is a maximal (minimal, respectively) curve over $\mathbb{F}_{q^2}$ if and only if the Frobenius map $\mathbb{F}_{q^2}$ (relative to $\mathbb{F}_{q^2}$) of the Jacobian $\mathcal{J}$ of the curve $\mathcal{C}$ acts as multiplication by $-q$ (by $+q$, respectively).*

Corollary 2.2. *Let $\mathcal{C}$ be a curve defined over $\mathbb{F}_{q^2}$.*

- *If the curve $\mathcal{C}$ is a maximal curve over $\mathbb{F}_{q^2}$, then $\mathcal{C}$ is minimal (maximal, respectively) over $\mathbb{F}_{q^{2r}}$ for r even (odd, respectively).*
- *If the curve $\mathcal{C}$ is a minimal curve over $\mathbb{F}_{q^2}$, then $\mathcal{C}$ is minimal over any finite extension of $\mathbb{F}_{q^2}$.*

Proof. These claims follow from the fact that the Frobenius $\mathbb{F}_{q^{2r}}$ is related to $\mathbb{F}_{q^2}$ by the formula $\mathbb{F}_{q^{2r}} = (\mathbb{F}_{q^2})^r$. □

The following observation (with a different proof) is attributed to J. P. Serre in the literature (see [4]):

Proposition 2.3. *A subcover of a maximal (minimal, respectively) curve is also maximal (minimal, respectively).*

Proof. If there is a non-constant morphism defined over the field k between two curves $f : \mathcal{C} \longrightarrow \mathcal{D}$, then we have an induced homomorphism $f^* : \mathcal{J}_{\mathcal{D}} \longrightarrow \mathcal{J}_{\mathcal{C}}$ on the Jacobians. Furthermore, $\mathcal{J}_{\mathcal{D}}$ is isogenous to an abelian subvariety of $\mathcal{J}_{\mathcal{C}}$ (because $\mathrm{Ker}(f^*)$ is finite). Thus, if the Frobenuis of $\mathcal{J}_{\mathcal{C}}/\mathbb{F}_{q^2}$ is equal to $\pm q$, then the same is true for the Frobenius of $\mathcal{J}_{\mathcal{D}}$. Therefore it follows from Lemma 2.1 that a subcover $\mathcal{D}$ of a maximal (minimal, respectively) curve $\mathcal{C}$ is also maximal (minimal, respectively). □

We have the following fact due to Ekedahl which is established in the course of proving Theorem 1.1 in [1, p. 166].

Theorem 2.4. *Let $\mathcal{C}$ be a curve defined over a field k of characteristic $p > 0$. If the Jacobian $\mathcal{J}_{\mathcal{C}}$ is a product of supersingular curves, then the curve $\mathcal{C}$ descends to $\mathbb{F}_{p^2}$ with Frobenius p or $-p$.*

The following proposition is also crucial for us (see [1, Proposition 1.2]):

Proposition 2.5. *Let $\mathcal{A}$ be an abelian variety defined over $\mathbb{F}_{q^2}$, where $q = p^n$. If the Frobenius $\mathbb{F}$ relative to $\mathbb{F}_{q^2}$ acts on the abelian variety $\mathcal{A}$ as multiplication by $\pm q$, then we have that $\mathbb{F}^n = 0$ on $H^1(\mathcal{A}, \mathbb{O}_{\mathcal{A}})$. In particular, if q is a prime then $\mathcal{A}$ is a product of supersingular elliptic curves over $\mathbb{F}_{p^2}$.*

Thus using the above facts we conclude:

Theorem 2.6. *Let $\mathcal{C}$ be a curve defined over $\mathbb{F}_{q^2}$, $q = p^r$. Then $\mathcal{C}$ is superspecial if and only if it is ($\mathbb{F}_{q^2}$- isomorphic) to a twist of a curve over $\mathbb{F}_{q^2}$ which descends to a maximal or a minimal curve over $\mathbb{F}_{p^2}$.*

Proof. Suppose $\mathcal{C}$ is a maximal or a minimal curve over $\mathbb{F}_{p^2}$. Then from Lemma 2.1 we know that on the Jacobian, the Frobenius is equal to multiplication by $\pm p$. So the result follows from Proposition 2.5. The converse follows from Theorem 2.4. □

Corollary 2.7. *Let $\mathcal{C}$ be a curve of genus g defined over a field k with $char(k) = p > 0$. If the curve $\mathcal{C}$ is superspecial, then either $g = p(p-1)/2$ or $g \leq (p-1)^2/4$.*

Proof. Suppose the curve $\mathcal{C}$ is superspecial. By Theorem 2.4, $\mathcal{C}$ descends to a minimal or a maximal curve over $\mathbb{F}_{p^2}$. It is easy to see that the genus of a minimal curve over $\mathbb{F}_{p^2}$ is not larger than $p/2$ (see [8, Proposition 2.1]). Thus the result follows from [2]. □

Corollary 2.8. *Let $\mathcal{C}$ and $\mathcal{D}$ be two curves defined over a field k. Suppose there is a non-constant morphism defined over the field k between two curves $f : \mathcal{C} \longrightarrow \mathcal{D}$. If $\mathcal{C}$ is superspecial, then $\mathcal{D}$ is also superspecial.*

3. Examples

In this section we use the above facts to give some simple proofs for being superspecial of some families of curves. Moreover, we generalize some well-known results on superspecial curves.

From [10, Proposition 5.3.3] we know that if a curve $\mathcal{C}$ is maximal over $\mathbb{F}_{q^2}$, then its genus satisfies

$$g \leq \frac{q^2-q}{2}. \tag{3.1}$$

There is a unique maximal curve over $\mathbb{F}_{q^2}$ which attains the above genus bound, and it can be given by the affine equation (see [9])

$$y^q + y = x^{q+1}, \tag{3.2}$$

or birationally equivalently, it is given by

$$x^{q+1} + y^{q+1} = 1. \tag{3.3}$$

This is the so-called *Hermitian curve* over $\mathbb{F}_{q^2}$, denoted by $\mathcal{H}(q+1)/\mathbb{F}_{q^2}$. From [10, Example 6.3.6] we know that $\mathcal{H}(q+1)/\mathbb{F}_{q^2}$ is a maximal curve over $\mathbb{F}_{q^2}$. Using Proposition 2.3 one way to construct explicit maximal curves over $\mathbb{F}_{q^2}$, is to find equations for subcovers of the Hermitian curve. In the following we use this idea to give some superspecial curves as subcovers of the Hermitian curve.

Proposition 3.1. *Let p be a prime and let $m, n \geq 1$. Set $r := lcm(m,n)$ and $s := m(n-1)$. Then the following curves are maximal over $\mathbb{F}_{p^2}$ and hence are superspecial.*

(a) $\mathcal{C}_{m,n} : x^m \pm y^n = 1$ if r is a divisor of $p+1$.

(b) $\mathcal{C}'_{m,n} : y^m = x^n - x$ if s is a divisor of $p+1$.

(c) $\mathcal{C}_m : y^p + y = x^m$ if m is a divisor of $p+1$.

Proof. The Hermitian curve $\mathcal{H}(p+1)$ is maximal over $\mathbb{F}_{p^2}$. By Theorem 2.6 it is superspecial. Now according to Proposition 2.3, it is sufficient to show that these curves are covered by the Hermitian curve $\mathcal{H}(p+1)$. For the part (a), put $p+1 = r\ell$, $r = m\alpha$ and $r = n\beta$. The result follows from the following morphism

$$\begin{cases} \mathcal{H}(p+1) & \to & \mathcal{C}_{m,n} \\ (x,y) & \mapsto & (x^{\alpha\ell}, y^{\beta\ell}). \end{cases}$$

Now suppose $s = m(n-1)$ is a divisor of $p+1$. From part (a) we know that the curve $\mathcal{C}_{s,s}$ is superspecial. Again to prove part (b), according to Proposition 2.3, it is sufficient to show that these curves are covered by the curve $\mathcal{C}_{s,s}$. But this follows from the following morphism

$$\begin{cases} \mathcal{C}_{s,s} & \to & \mathcal{C}'_{m,n} \\ (x,y) & \mapsto & (x^m, xy^{n-1}). \end{cases}$$

The last part can be concluded by similar arguments. □

We should mention that all of the above facts are true also over a finite field $\mathbb{F}_{q^2}$, not just for $q = p$. Now using the above proposition we give simple proofs of some results on certain classes of superspecial curves. All of the following results are well-known, but they have been proved using the Cartier operators. Here we will see that they are special cases of the above proposition.

3.1. **Fermat curves.** Let $\mathcal{C}(m)$ be the Fermat curve defined over $\mathbb{F}_{p^2}$ by the equation

$$x^m + y^m = 1,$$

where m is an integer such that $m \geq 3$ and $\gcd(m, p) = 1$.

In this case we have that $\mathcal{C}(m) = \mathcal{C}_{m,m}$ and so according to Proposition 3.1 (a) we conclude the following result (see [6, Theorem 3]):

Theorem 3.2. *Let m be a divisor of $p + 1$. The Fermat curve $\mathcal{C}(m)$ defined by the equation $y^m + x^m = 1$ is superspecial over $\mathbb{F}_{p^2}$.*

3.2. **Picard curves.** Let $p > 3$ be a prime number, and let $\mathcal{C}$ be a smooth projective curve over $\mathbb{F}_{p^2}$ with an affine model

$$y^3 = x^4 + a_3x^3 + a_2x^2 + a_1x + a_0,\ a_i \in \mathbb{F}_{p^2}.$$

Here we assume that $f(x) = x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$ is a polynomial with no multiple roots. The curve $\mathcal{C}$ is called a Picard curve.

In [11], using Cartier operators, Takizawa found a classification of the p-adic Newton polygons associated to two families of Picard curves. Here we conclude the following results as a corollary of Proposition 3.1(a), (b).

Theorem 3.3. *Let $p > 3$ be a prime number.*

1) Let $\mathcal{C}_1$ be the Picard curve

$$y^3 = x^4 - 1.$$

If $p \equiv 11 \pmod{12}$, then $\mathcal{C}_1$ is superspecial.

2) Let $\mathcal{C}_2$ be the Picard curve

$$y^3 = x^4 - x.$$

If $p \equiv 8 \pmod{9}$, then $\mathcal{C}_2$ is superspecial.

Remark 3.4. In [11] it was mentioned without proof that if $p \equiv 2 \pmod 9$ or $p \equiv 5 \pmod 9$, then the curve $\mathcal{C}_2 : y^3 = x^4 - x$ is supersingular. This can be deduced from Proposition 2.3 by observing that in this case 9 is a divisor of $p^3 + 1$. Hence the curve $\mathcal{C}(9)$ is maximal over $\mathbb{F}_{p^6}$ and so the curve $\mathcal{C}_2$ is maximal over $\mathbb{F}_{p^6}$ and thus it is supersingular.

3.3. **Hyperelliptic curves.** Let $\mathbb{F}_p$ be a finite field of characteristic $p > 2$. Let $\mathcal{C}$ be a projective nonsingular hyperelliptic curve over $\mathbb{F}_p$ of genus g. Then $\mathcal{C}$ can be defined by an affine equation of the form

$$y^2 = f(x),$$

where $f(x)$ is a polynomial over $\mathbb{F}_p$ of degree $2g + 1$, without multiple roots. If $\mathcal{C}$ is superspecial, then we have an upper bound on the genus (see [1]), namely

$$g(\mathcal{C}) \leq \frac{p-1}{2}.$$

In [13] a characterization of hyperelliptic curves with zero Hasse-Witt matrix is given. Thus by Nygaard [7] we have a classification of such curves which are superspecial. Here we can obtain the following theorem as a corollary of Proposition 3.1(c).

Theorem 3.5. *The hyperelliptic curve $\mathcal{C}$ given by the equation $y^2 = x^p + x$ is superspecial over $\mathbb{F}_p$.*

We also deduce the following result (see [13, Theorem 2]):

Theorem 3.6. *Let g be a positive integer with $2 \leq g \leq (p-1)/2$. The following hyperelliptic curves are superspecial*

1) $y^2 = x^{2g+1} + x$ *if* $p \equiv -1$ *or* $2g + 1 \pmod{4g}$,

2) $y^2 = x^{2g+1} - 1$ *if* $p \equiv -1 \pmod{2g+1}$.

Proof. Consider the curve $\mathcal{C}$ defined by $y^2 = x^{2g+1} + x$. If $p \equiv 1 + 2g \pmod{4g}$, then we set $p - 1 - 2g = 4ga$ and $p + 1 = 2b$. Now if we consider the following morphism

$$\begin{cases} \mathcal{H}(p+1) : y^{p+1} = x^p + x & \to & \mathcal{C} \\ (x, y) & \mapsto & (x^{2a+1}, x^a y^b), \end{cases}$$

then $\mathcal{C}$ is covered by the Hermitian curve $\mathcal{H}(p+1)$ and so is maximal over $\mathbb{F}_{p^2}$. This implies that the curve $\mathcal{C}$ is superspecial. The rest follows from Proposition 3.1(a), (b). □

Remark 3.7. All of the above examples are covered by the Hermitian curve. But the authors of [3] construct maximal curves over $\mathbb{F}_{p^6}$ which are not covered by the Hermitian curve. However, it is not clear (in fact unlikely) that these curves are superspecial.

Acknowledgments

This research was in part supported by a grant from IPM (No. 88140029). The second author was supported by Shahrekord university. Also we would like to thank referees for their valuable comments that improved the exposition.

References

[1] T. Ekedahl, On supersingular curves and abelian varieties, *Math. Scand.* **60** (1987), no. 2, 151–178.
[2] R. Fuhrmann and F. Torres, The genus of curves over finite fields with many rational points, *Manuscripta Math.* **89** (1996), no. 1, 103–106.
[3] M. Giulietti and G. Korchmáros, A new family of maximal curves over a finite field, *Math. Ann.* **343** (2009), no. 1, 229–245.
[4] G. Lachaud, Sommes d'Eisenstein et nombre de points de certaines courbes algébriques sur les corps finis, *C. R. Acad. Sci. Paris Sér. I Math.* **305** (1987), no. 16, 729–732.
[5] S. Lang, Abelian Varieties, Interscience Publishers Ltd., New York, 1959.
[6] T. Kodama and T. Washio, Hasse-Witt matrices of Fermat curves, *Manuscripta Math.* **60** (1988), no. 2, 185–195.
[7] N. O. Nygaard, Slopes of powers of Frobenius on crystalline cohomology, *Ann. Sci. École Norm. Sup.* **14** (1981), no. 4, 369–401.
[8] J. E. A. Rodriguez and P. Viana, Eventually minimal curves, *Bull. Braz. Math. Soc. (N.S.)* **36** (2005), no. 1, 39–58.
[9] H. G. Rück and H. Stichtenoth, A characterization of Hermitian function fields over finite fields, *J. Reine Angew. Math.* **457** (1994) 185–188.
[10] H. Stichtenoth, Algebraic Function Fields and Codes, Second edition, Graduate Texts in Mathematics, 254, Springer-Verlag, Berlin, 2009.
[11] Y. Takizawa, Some remarks on the Picard curves over a finite field, *Math. Nachr.* **280** (2007), no. 7, 802–811.
[12] J. Tate, Endomorphisms of abelian varieties over finite fields, *Invent. Math.* **2** (1966) 134–144.
[13] R. C. Valentini, Hyperelliptic curves with zero Hasse-Witt matrix, *Manuscripta Math.* **86** (1995), no. 2, 185–194.

Ahmad Kazemifard
Department of Mathematics, Shahrekord University, Shahrekord, Iran
Email: kazemifard.ahmad@stu.sku.ac.ir

Ali Reza Naghipour
Department of Mathematics, Shahrekord University, Shahrekord, Iran
Email: naghipour@sci.sku.ac.ir

Saeed Tafazolian
School of Mathematics, Institute for Research in Fundamental Sciences (IPM), P.O. Box 19395-5746, Tehran, Iran
and

Department of Mathematics, Institute for Advanced Studies in Basic Sciences (IASBS), P.O. Box 45195-1159, Zanjan, Iran
Email: tafazolian@iasbs.ac.ir