Finite Fields and Their Applications 42 (2016) 81–92

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Explicit maximal and minimal curves over finite fields of odd characteristics ☆

Ferruh Özbudak [a], Zülfükar Saygı [b,*]

[a] Department of Mathematics and Institute of Applied Mathematics, Middle East Technical University, Dumlupınar Bul., No:1, 06800, Ankara, Turkey
[b] Department of Mathematics, TOBB University of Economics and Technology, Söğütözü, 06530, Ankara, Turkey

ARTICLE INFO

Article history:
Received 5 July 2015
Received in revised form 5 July 2016
Accepted 10 July 2016
Available online 26 July 2016
Communicated by Chaoping Xing

MSC:
11G20

Keywords:
Algebraic curves
Rational points
Maximal curves
Minimal curves

ABSTRACT

In this work we present explicit classes of maximal and minimal Artin–Schreier type curves over finite fields having odd characteristics. Our results include the proof of Conjecture 5.9 given in [1] as a very special subcase. We use some techniques developed in [2], which were not used in [1].

1. Introduction

Algebraic curves over finite fields have various applications in coding theory, cryptography, quasi-random numbers and related areas (see, for example, [6,7,11,12]). For these

☆ A part of this paper is presented at Workshop on Coding Theory and Cryptography 2015, Paris, France, 2015.

* Corresponding author.
E-mail addresses: ozbudak@metu.edu.tr (F. Özbudak), zsaygi@etu.edu.tr (Z. Saygı).

http://dx.doi.org/10.1016/j.ffa.2016.07.006
1071-5797/

applications it is important to know the number of rational points of the curve. Throughout this paper by a curve we mean a smooth, geometrically irreducible and projective curve over a finite field of odd characteristic.

Let p be an odd prime, e be a positive integer, $q = p^e$ and n be a positive integer. Let $\mathbb{F}_{q^n}$ denote the finite field with q^n elements. Let $h \geq 0$ and

$$S(x) = s_0 x + s_1 x^q + \cdots + s_h x^{q^h} \in \mathbb{F}_{q^n}[x]$$

be an $\mathbb{F}_q$-linearized polynomial of degree q^h in $\mathbb{F}_{q^n}[x]$. We consider the Artin–Schreier type curves χ given by

$$\chi: \quad y^q - y = xS(x) = \sum_{i=0}^{h} s_i x^{q^i+1}. \tag{1.1}$$

These curves are related to the quadratic forms

$$Q(x) = \mathrm{Tr}(xS(x)) \tag{1.2}$$

where Tr denote the trace map from $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$. Let $N(Q)$ denote the cardinality

$$N(Q) = |\{x \in \mathbb{F}_{q^n} \mid \mathrm{Tr}\,(xS(x)) = 0\}|$$

and let $N(\chi)$ be the number of $\mathbb{F}_{q^n}$ rational points of the curve χ. Then using Hilbert's Theorem 90 we have

$$N(\chi) = 1 + qN(Q),$$

and hence determining $N(\chi)$ is the same as determining $N(Q)$. Note that in general, it is difficult to determine $N(\chi)$. For the number $N(\chi)$, the Hasse–Weil inequality states that

$$q^n + 1 - 2g(\chi)\sqrt{q^n} \leq N(\chi) \leq q^n + 1 + 2g(\chi)\sqrt{q^n} \tag{1.3}$$

where $g(\chi)$ is the genus of χ. We know that there exist curves attaining the Hasse–Weil bounds. If the upper bound is attained then the curve is called a maximal curve and if the lower bound is attained then the curve is called a minimal curve. Here we note that using [11, Proposition 3.7.10] the genus of the curve χ in (1.1) is $g(\chi) = \dfrac{(q-1)q^h}{2}$.

Using the relations between the curve χ in (1.1) and the quadratic form Q in (1.2) some characterizations and classification results on maximal and minimal curves are obtained in [3,4,8–10] for the curves over finite fields with even characteristics. Also using similar relations some results are obtained for the curves over finite fields with odd characteristics in [1]. Furthermore for all integers $n \equiv 0 \mod 12$ and for all primes p, $5 \leq p \leq 29$ with $\gcd(p, n) = 1$ the following conjecture is given in [1, Conjecture 5.9].