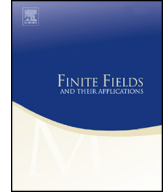




ELSEVIER

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa


Optimal curves of low genus over finite fields



Alexey Zaytsev

Immanuel Kant Baltic Federal University, Nevsky 14a, Kaliningrad, Russia

ARTICLE INFO

Article history:

Received 31 March 2015

Received in revised form 12

September 2015

Accepted 24 September 2015

Available online 11 November 2015

Communicated by Chaoping Xing

MSC:

14H25

11R58

Keywords:

Curves over finite field

Function fields over finite fields

Maximal curves

ABSTRACT

We investigate maximal and minimal curves of genus 4 and 5 over finite fields with discriminant -11 and -19 . As a result the Hasse–Weil–Serre bound is improved.

© 2015 Elsevier Inc. All rights reserved.

1. Introduction

In this paper we study maximal and minimal curves of low genus over finite fields of certain discriminants. As a result we are able to improve the Hasse–Weil–Serre upper and lower bounds [12] for the number of rational points on these curves.

By a curve over a finite field \mathbb{F}_q we mean an absolutely irreducible nonsingular projective algebraic variety of dimension 1 over \mathbb{F}_q and by the discriminant $d(\mathbb{F}_q)$ of a finite field \mathbb{F}_q we mean the integer $m^2 - 4q$, where $m = [2\sqrt{q}]$.

E-mail address: alzaytsev@kantiana.ru.

It is well known that the set of the Hasse–Weil bounds for a curve C

$$|\#C(\mathbb{F}_{q^i}) - q - 1| \leq 2gq^{i/2},$$

is equivalent to the Riemann hypothesis of the zeta function of the curve C . It shows the importance of such bounds in its own. An improvement of the Hasse–Weil bound was proposed by J-P. Serre:

$$|\#C(\mathbb{F}_q) - q - 1| \leq g[2\sqrt{q}].$$

This is called the Hasse–Weil–Serre bound (see [12]).

A curve C of genus g over a finite field \mathbb{F}_q is called a maximal (resp. minimal) optimal curve if its number of rational points attains the upper (resp. lower) Hasse–Weil–Serre bound $q + 1 \pm g[2\sqrt{q}]$.

In case of discriminant $d(\mathbb{F}_q) \in \{-11, -19\}$ an optimal curve is ordinary (see [Proposition 3.1](#) and [Proposition 4.1](#)). Therefore we can use the canonical lifts of the Jacobian and the equivalence of categories between the category of ordinary principally polarized abelian varieties over \mathbb{F}_q and the category of certain unimodular irreducible hermitian modules over the ring of integers \mathcal{O}_K of the imaginary quadratic field K of discriminant equal to $d(\mathbb{F}_q)$ (see [1,3] or [6]). This method of studying curves over finite fields via hermitian modules was proposed by J-P. Serre [13,14] and pursued by K. Lauter and E. Howe [5,7,8]. It turns out that if the discriminant is either -11 or -19 then the class number of \mathcal{O}_K is 1 and there is a classification of hermitian modules. In this paper we prove non-existence of optimal curves under certain conditions [Theorem 1.1](#). The combination of these results and the fact of non-existence curves of defect 1 (see [6, p. 5, [Proposition 2](#)]) of genus greater than 2 implies the following improvement.

Theorem 1.1. *Let C be a curve of genus g over a finite field \mathbb{F}_q of characteristic p . Then we have that*

$$|\#C(\mathbb{F}_q) - q - 1| \leq g[2\sqrt{q}] - 2,$$

if the following conditions on q and g hold:

$d(\mathbb{F}_q)$	q	g
-11	$p \neq 3, q < 10^4$	$g = 4$
-11	$p > 5$	$g = 5$
-19	$q < 10^3$ and $q \equiv 1 \pmod{5}$	$g = 4$

Unfortunately, we do not know whether the obtained bound is exact or not.

Our method uses the explicit classification of hermitian lattices by A. Schiemann [10]. We also use some information on generators for the automorphism groups of such lattices of dimensions 4 and 5 over the imaginary quadratic extension K of \mathbb{Q} with discriminant $d(K) = -19$ provided to us by R. Schulze-Pillot [11].

Download English Version:

<https://daneshyari.com/en/article/4582744>

Download Persian Version:

<https://daneshyari.com/article/4582744>

[Daneshyari.com](https://daneshyari.com)