

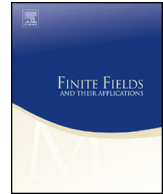


ELSEVIER

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa



Exact evaluation of second moments associated with some families of curves over a finite field

Ravi Donepudi^a, Junxian Li^{a,*}, Alexandru Zaharescu^{b,a}^a Department of Mathematics, University of Illinois, 1409 West Green Street, Urbana, IL 61801, USA^b Simion Stoilow Institute of Mathematics of the Romanian Academy, P.O. Box 1-764, RO-014700 Bucharest, Romania

ARTICLE INFO

Article history:

Received 29 February 2016

Received in revised form 1 August 2017

Accepted 17 August 2017

Available online 5 September 2017

Communicated by James W.P. Hirschfeld

MSC:

primary 11T23

secondary 11T99

Keywords:

Families of polynomials

Curves over finite fields

Exponential sums

Exact formulae

ABSTRACT

Let \mathbb{F}_q be the finite field with q elements. Given an N -tuple $Q \in \mathbb{F}_q^N$, we associate with it an affine plane curve C_Q over \mathbb{F}_q . We consider the distribution of the quantity $q - \#C_{q,Q}$ where $\#C_{q,Q}$ denotes the number of \mathbb{F}_q -points of the affine curve C_Q , for families of curves parameterized by Q . Exact formulae for first and second moments are obtained in several cases when Q varies over a subset of \mathbb{F}_q^N . Families of Fermat type curves, Hasse–Davenport curves and Artin–Schreier curves are also considered and results are obtained when Q varies along a straight line.

© 2017 Elsevier Inc. All rights reserved.

* Corresponding author.

E-mail addresses: donepud2@illinois.edu (R. Donepudi), jli135@illinois.edu (J. Li), zaharescu@illinois.edu (A. Zaharescu).

1. Introduction

Given an elliptic curve E over the finite field \mathbb{F}_q with q elements, the number of points of E over \mathbb{F}_q can be expressed as $q + 1 - T_E$, where T_E is the trace of the Frobenius of E . A classical result of Hasse [7] states that

$$|T_E| \leq 2\sqrt{q}.$$

Questions on the distribution of the number of points have been studied by a number of authors. In particular, for a fixed \mathbb{F}_q , one can consider the trace distribution of a family of elliptic curves. Let $E_{q,a,b}$ denote the elliptic curve with Weierstrass form $y^2 = x^3 + ax + b$, and let $T_{E_{q,a,b}}$ denote the trace of Frobenius of $E_{q,a,b}$. In [2], Birch gave asymptotic formulae for the average of even moments $\sum_{a,b \in \mathbb{F}_q} T_{E_{q,a,b}}^{2R}$ by using the Selberg trace formula. More recently, in [8], He and Mc Laughlin obtained exact formulae for $\sum_{a \in \mathbb{F}_p} T_{E_{p,a,b}}^2$ when the field is taken to be the prime field \mathbb{F}_p . For a smooth algebraic curve \mathcal{C} over \mathbb{F}_q of genus g , a well known theorem of Weil [11] states that

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

where $\#\mathcal{C}_q$ denotes the number of \mathbb{F}_q -points of the projective curve. As with the case of elliptic curves where $g = 1$, the distribution of the quantity $T_{\mathcal{C}_q} := q + 1 - \#\mathcal{C}_q$ has also attracted attention. In the present paper, we establish exact formulae for the first and second moments of analogous quantities to $T_{\mathcal{C}_q}$ over some general families of affine plane curves over a finite field \mathbb{F}_q .

For fixed non-negative integers $a_i, b_i, i \in \{1, 2, \dots, N\}$ and an N -tuple

$$Q = (c_1, c_2, \dots, c_N) \in \mathbb{F}_q^N,$$

we associate with it a plane curve \mathcal{C}_Q whose affine model is given by

$$\mathcal{C}_Q : \sum_{i=1}^N c_i x^{a_i} y^{b_i} = 0. \quad (2)$$

We set $T_Q = q - \#\mathcal{C}_Q$, where $\#\mathcal{C}_Q$ denotes the number of \mathbb{F}_q -points, which are the \mathbb{F}_q -solutions (x, y) to the defining equation (2) of \mathcal{C}_Q . We will use points or solutions instead of \mathbb{F}_q -points or \mathbb{F}_q -solutions for short later on. Note that if we homogenize equation (2), then the points at infinity are determined by the highest degree homogeneous equation in x and y . For elliptic curves in Weierstrass form, there is only one point at infinity, and our definition of T_Q matches the usual definition of T_Q as $q + 1 - \#PC$, where $\#PC$ is the number of point on the projective curve associated to \mathcal{C} . In either case, T_Q measures the difference between the number of points on the curve and the expected value. Given a subset $S \subseteq \mathbb{F}_q^N$, we are interested in the distribution of T_Q as Q ranges over S . In particular, we consider the variance of T_Q for $Q \in S$,

Download English Version:

<https://daneshyari.com/en/article/5771568>

Download Persian Version:

<https://daneshyari.com/article/5771568>

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