Finite Fields and Their Applications 49 (2018) 80–93

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

The second largest number of points on plane curves over finite fields

Masaaki Homma [a], Seon Jeong Kim [b,*]

[a] *Department of Mathematics and Physics, Kanagawa University, Hiratsuka 259-1293, Japan*
[b] *Department of Mathematics and RINS, Gyeongsang National University, Jinju 660-701, Republic of Korea*

A R T I C L E I N F O

Article history:
Received 15 September 2015
Received in revised form 30 August 2017
Accepted 15 September 2017
Available online xxxx
Communicated by James W.P. Hirschfeld

MSC:
11G20
13F20
14G15
14N05

Keywords:
Finite field
Basis of the ideal
Plane curve

A B S T R A C T

A basis of the ideal of the complement of a linear subspace in a projective space over a finite field is given. As an application, the second largest number of points of plane curves of degree d over the finite field of q elements is also given for $d \geq q+1$.

* Corresponding author.
E-mail addresses: homma@kanagawa-u.ac.jp (M. Homma), skim@gnu.kr (S.J. Kim).

http://dx.doi.org/10.1016/j.ffa.2017.09.007

1. Introduction

Let C be a curve of degree d in the projective plane $\mathbb{P}^2$ with the homogeneous coordinate X, Y, Z defined over the finite field $\mathbb{F}_q$ of q elements, which has no $\mathbb{F}_q$-line components, and $F(X, Y, Z)$ a homogeneous polynomial in $\mathbb{F}_q[X, Y, Z]$ which defines the curve C. We are interested in the set

$$C(\mathbb{F}_q) := \{(a, b, c) \in \mathbb{P}^2(\mathbb{F}_q) \mid F(a, b, c) = 0\},$$

where $\mathbb{P}^2(\mathbb{F}_q)$ denotes the set of $\mathbb{F}_q$-points of $\mathbb{P}^2$. The number of $C(\mathbb{F}_q)$ is denoted by $N_q(C)$.

The study of $N_q(C)$ has long history, and several upper bonds for $N_q(C)$ under a fixed degree d are known, e.g., the Hasse–Weil bound, the Stöhr–Voloch bound for Frobenius classical/non-classical curves. One can consult [1] for those known results.

We proved the Sziklai bound recently in the series of papers [2–4], which says that

> $N_q(C) \leq (d-1)q + 1$ unless C is a curve over $\mathbb{F}_4$ which is projectively equivalent to the curve defined by
>
> $$(X + Y + Z)^4 + (XY + YZ + ZX)^2 + XYZ(X + Y + Z) = 0$$
>
> over $\mathbb{F}_4$.

In order to give a brief explanation of what we will do, we should explain some notation.

Notation 1.1. The number of points of $\mathbb{P}^n(\mathbb{F}_q)$ is denoted by $\theta_q(n)$, that is,

$$\theta_q(n) = q^n + \cdots + q + 1 = \frac{q^{n+1} - 1}{q - 1}.$$

Let $x_0, \ldots, x_n$ be coordinates of $\mathbb{P}^n$, and $f_1, \ldots, f_n$ homogeneous polynomials over $\mathbb{F}_q$. The algebraic set in $\mathbb{P}^n$ over the algebraic closure of $\mathbb{F}_q$ defined by equations $f_1 = \cdots = f_n = 0$ is frequently denoted by $\{f_1 = \cdots = f_n = 0\}$.

Here we summarize symbols related to plane curves, which are used in this paper, and also agree with those in [5].

- $\mathcal{C}_d(\mathbb{F}_q)$: the set of plane curves of degree d over $\mathbb{F}_q$ without $\mathbb{F}_q$-linear components
- $\mathcal{C}_d^i(\mathbb{F}_q) := \{C \in \mathcal{C}_d(\mathbb{F}_q) \mid \text{C is absolutely irreducible}\}$
- $\mathcal{C}_d^s(\mathbb{F}_q) := \{C \in \mathcal{C}_d(\mathbb{F}_q) \mid \text{C is nonsingular}\}$
- $M_q(d) = \max\{N_q(C) \mid C \in \mathcal{C}_d(\mathbb{F}_q)\}$
- $M_q^i(d) = \max\{N_q(C) \mid C \in \mathcal{C}_d^i(\mathbb{F}_q)\}$
- $M_q^s(d) = \max\{N_q(C) \mid C \in \mathcal{C}_d^s(\mathbb{F}_q)\}$