Finite Fields and Their Applications 48 (2017) 87–102

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Number of rational branches of a singular plane curve over a finite field

Nazar Arakelian

Centro de Matemática, Computação e Cognição, Universidade Federal do ABC, Avenida dos Estados, 5001, CEP 09210-580, Santo André, SP, Brazil

A R T I C L E   I N F O

Article history:
Received 20 January 2017
Received in revised form 17 July 2017
Accepted 19 July 2017
Available online 8 August 2017
Communicated by Neal Koblitz

MSC:
primary 11G20, 14H05, 14H50
secondary 14HXX

Keywords:
Algebraic curves
Rational points
Finite fields

A B S T R A C T

Let $\mathcal{F}$ be a plane singular curve defined over a finite field $\mathbb{F}_q$. Via results of [11] and [1], the linear system of plane curves of a given degree passing through the singularities of $\mathcal{F}$ provides potentially good bounds for the number of points on a non-singular model of $\mathcal{F}$. In this note, the case of a curve with two singularities such that the sum of their multiplicities is precisely the degree of the curve is investigated in more depth. In particular, such plane models are completely characterized, and for $p > 3$, a curve of this type attaining one of the obtained bounds is presented.

1. Introduction

For a prime number p, let $\mathbb{F}_q$ be the finite field with q elements, where q is a power of p. Let $\mathcal{F}$ be a (projective, geometrically irreducible, algebraic) plane curve of degree d, genus $\mathfrak{g}$, defined over $\mathbb{F}_q$. Denote by $N_m(\mathcal{F})$ the number of $\mathbb{F}_{q^m}$-rational points on a non-singular model of $\mathcal{F}$ (or equivalently, the number of $\mathbb{F}_{q^m}$-rational branches of $\mathcal{F}$),

E-mail address: n.arakelian@ufabc.edu.br.

http://dx.doi.org/10.1016/j.ffa.2017.07.004
1071-5797/

where $m \geq 1$ is an integer. One of the most challenging problems regarding $\mathcal{F}$ is the determination of the number $N_m(\mathcal{F})$ in terms of $q, d, \mathfrak{g}$ and other covariants. In fact, there are only few families of curves for which such an explicit formula for $N_m(\mathcal{F})$ is known, see [3,4,6,9] for instance. This fact has been motivating the search for estimates for $N_m(\mathcal{F})$ over the last years. The most remarkable of them is the Hasse–Weil bound, presented by A. Weil in the 1940s, which states

$$|N_m(\mathcal{F}) - (q^m + 1)| \leq 2\mathfrak{g}\sqrt{q^m}. \tag{1}$$

Introduced in 1986, the Stöhr–Voloch technique is also one of the most significant approaches to estimate $N_m(\mathcal{F})$ [11]. This technique depends on the linear series of the curve. More precisely, let g_n^r be a base-point-free linear series on $\mathcal{F}$ of degree n and dimension r, defined over $\mathbb{F}_{q^m}$. The Stöhr–Voloch main theorem [11, Theorem 2.13] states that, associated to g_n^r and q^m, there exists a sequence of non-negative integers $(\nu_0, \ldots, \nu_{r-1})$, with $0 = \nu_0 < \cdots < \nu_{r-1}$, such that

$$N_m(\mathcal{F}) \leq \frac{(\nu_1 + \cdots + \nu_{r-1})(2\mathfrak{g} - 2) + (q^m + r)n}{r}. \tag{2}$$

The bound (2) improves the Hasse–Weil bound in many instances (see [11]). In [1] a bound obtained via a variation of Stöhr–Voloch method is presented: if g_n^r is defined over $\mathbb{F}_q$, given positive integers u, m with $u < m$ and $\gcd(u, m) = 1$, there are positive integers c_i (depending on i and g_n^r) with $i = 1, u, m, m - u$, such that

$$\begin{aligned} &(c_1 - c_u - c_m - c_{m-u})N_1(\mathcal{F}) + c_u N_u(\mathcal{F}) + c_m N_m(\mathcal{F}) + c_{m-u} N_{m-u}(\mathcal{F}) \\ &\leq (\kappa_0 + \cdots + \kappa_{r-2})(2\mathfrak{g} - 2) + (q^u + q^m + r - 1)n, \end{aligned} \tag{3}$$

where $(\kappa_0, \ldots, \kappa_{r-2})$ is a sequence of non-negative integers, which depends also on g_n^r, such that $0 \leq \kappa_0 < \cdots < \kappa_{r-2}$, see [1, Theorem 4.4]. Here, we have $c_1 \geq q^u + 2(r-1)$ and $c_{m-u} \geq q^u$, and these numbers can be bigger, depending on some properties of $\mathcal{F}$ and g_n^r. As shown in [1], the bound (3) improves Hasse–Weil and Stöhr–Voloch bounds in many situations.

It can be seen directly from (2) that the application of the Stöhr–Voloch method to a linear series g_n^r such that r is large compared to n, has good chances to yield efficient upper bounds for the number of rational points on a non-singular model of the curve. The same holds for bound (3). In this sense, given a plane singular curve $\mathcal{F}$, we show that the bounds for the number of its rational branches arising from linear systems of plane curves of the same degree passing through the singularities of $\mathcal{F}$ are potentially good (Section 3). The case where $\mathcal{F}$ satisfies the following property is investigated more in depth (Section 4):

(H) $\mathcal{F}$ has at least two singularities P_1 and P_2 defined over $\mathbb{F}_q$ with multiplicities r_1 and r_2, respectively, such that $r_1 + r_2 = d$.