Journal of Number Theory 177 (2017) 91–99

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Degree matrices and enumeration of rational points of some hypersurfaces over finite fields

Ruyun Wang, Binbin Wen, Wei Cao *

Department of Mathematics, Ningbo University, Ningbo, Zhejiang 315211, PR China

A R T I C L E   I N F O

Article history:
Received 15 November 2016
Received in revised form 13 January 2017
Accepted 13 January 2017
Available online 6 March 2017
Communicated by D. Wan

MSC:
11T06
11T55
11D79

Keywords:
Degree matrix
Rational point
Gauss sum

A B S T R A C T

Let f be a polynomial over the finite field $\mathbb{F}_q$ with degree matrix $D_f \in \mathbb{Z}_{\geq 0}^{n\times m}$ and $N(f)$ be the number of $\mathbb{F}_q$-rational points on the hypersurface defined by $f = 0$. For an $M \in \mathbb{Z}^{n\times m}$, let $D_f \overset{r_q}{\sim} M$ denote that D_f is row equivalent to M in the ring $\mathbb{Z}/(q-1)\mathbb{Z}$. Sun has originally found the formula for $N(f)$ when $n = m$ and $0 < D_f \overset{r_q}{\sim} \mathrm{diag}(1, \dots, 1)$, which was extended to $m \leq n$ by Cao and Sun. In this paper we obtain the formula for $N(f)$ when $m \leq n$ and $0 < D_f \overset{r_q}{\sim} \mathrm{diag}(\lambda_1, \dots, \lambda_m)$ with $\lambda_i \in \{1, 2\}$, which further generalizes the results of Sun and Cao.

1. Introduction

Let $\mathbb{F}_q$ be the finite field of order q where $q = p^h$ and p is an odd prime. Let $f(x_1, \dots, x_n)$ be a nonzero polynomial in n variables of the form

$$f = a_1 x_1^{d_{11}} \cdots x_n^{d_{n1}} + \cdots + a_m x_1^{d_{1m}} \cdots x_n^{d_{nm}}, \quad a_i \in \mathbb{F}_q^*,\ d_{ij} \in \mathbb{Z}_{\geq 0}. \tag{1}$$

* Corresponding author.
E-mail address: caowei@nbu.edu.cn (W. Cao).

http://dx.doi.org/10.1016/j.jnt.2017.01.028

The degree matrix of f, denoted D_f, is defined to be the $n \times m$ matrix $D_f = (D_1, \ldots, D_m)$ with $D_j = (d_{1j}, \ldots, d_{nj})^{\mathrm{T}}$ for $j = 1, \ldots, m$. Let $N(f)$ be the number of $\mathbb{F}_q$-rational points on the affine hypersurface $f = 0$ in $\mathbb{A}^n(\mathbb{F}_q)$, namely,

$$N(f) = \#\{(x_1, \ldots, x_n) \in \mathbb{A}^n(\mathbb{F}_q) \mid f(x_1, \ldots, x_n) = 0\}.$$

Though it is difficult to obtain an explicit formula for $N(f)$ in general, it has been studied extensively because of its theoretical importance as well as applications in cryptology and coding theory; refer to [6] for detail. We simple write $D_f > 0$ when all the entries in D_f are positive. Sun [7] discovered the following result.

Theorem 1.1. *Let f be of the form as in (1) with $D_f > 0$. If $m = n$ and* $\gcd(\det(D_f), q-1) = 1$, *then for $b \in \mathbb{F}_q$ we have*

$$N(f-b) = \begin{cases} q^n - (q-1)^n + \frac{(q-1)^n + (-1)^n(q-1)}{q} & \text{if } b = 0, \\ \frac{(q-1)^n - (-1)^n}{q} & \text{if } b \neq 0. \end{cases}$$

Sun's theorem was extended to $m \leq n$ by Cao and Sun [2], which can be stated in a stronger version as below.

Theorem 1.2. *Let f be of the form as in (1) with $D_f > 0$. If $m \leq n$ and D_f is left invertible in the ring $\mathbb{Z}/(q-1)\mathbb{Z}$, then for $b \in \mathbb{F}_q$ we have*

$$N(f-b) = \begin{cases} q^n - q^{-1}(q-1)^{n-m+1}((q-1)^m - (-1)^m) & \text{if } b = 0, \\ q^{-1}(q-1)^{n-m}((q-1)^m - (-1)^m) & \text{if } b \neq 0. \end{cases}$$

Provided that the augmented degree matrix (see Section 2) is taken into consideration, Theorem 1.2 can be further strengthened (see [4,3]). However we will study another generalization of Theorem 1.2 in this paper. Note that condition that D_f is left invertible in $\mathbb{Z}/(q-1)\mathbb{Z}$ is equivalent to say that D_f is row equivalent to a diagonal matrix with all the diagonal elements being 1 in $\mathbb{Z}/(q-1)\mathbb{Z}$, which we write in notation as $D_f \overset{r_q}{\sim} \Lambda = \mathrm{diag}(1, \ldots, 1)$. In this paper we will consider the case that $D_f \overset{r_q}{\sim} \mathrm{diag}(\lambda_1, \ldots, \lambda_m)$ with $\lambda_i \in \{1, 2\}$. Some preliminary knowledge will be introduced in Section 2 and main results will be given in Section 3. It will be seen that the formula for $N(f)$ becomes more complicated than those in Theorems 1.1 and 1.2 and several concise formulae for $N(f)$ will be obtained in special cases.

2. Preliminaries

We first briefly introduce a formula for $N(f)$ in terms of Gauss sums; for detail, see [1,5,8,9]. Let $\mathbb{Q}_p$ be the field of p-adic numbers and let $\mathbb{C}_p$ be the completion of an algebraic closure of $\mathbb{Q}_p$. Let χ be the Teichmüller character of the multiplicative group $\mathbb{F}_q^*$.