Finite Fields and Their Applications 28 (2014) 188–198

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Invariant factors of degree matrices and L-functions of certain exponential sums

Meiling Zhu, Wei Cao *

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

ARTICLE INFO

Article history:
Received 10 December 2013
Received in revised form 15 February 2014
Accepted 18 February 2014
Available online 15 March 2014
Communicated by Igor Shparlinski

MSC:
11T06
11T23
11M38

Keywords:
Invariant factor
L-function
Exponential sum
Gauss sum

ABSTRACT

Let f be a multivariate Laurent polynomial over a finite field and $L^*(f,T)$ the corresponding L-function of the toric exponential sum of f. In this paper, we obtain an explicit formula for the L-function $L^*(f,T)$ in terms of Gauss sums provided that the invariant factors of the degree matrix of f satisfy certain conditions. As an application, we also compute the zeta functions for some hypersurfaces.

1. Introduction

Let $\mathbb{F}_q$ be the finite field of q elements with characteristic p and $\mathbb{F}_q^*$ its multiplicative group. For each positive integer k, let $\mathbb{F}_{q^k}$ be the extension of $\mathbb{F}_q$ of degree k. Let $f(x_1,\ldots,x_n) \in \mathbb{F}_q[x_1,\ldots,x_n]$ be a polynomial in n variables. Let $N_k(f)$ denote the

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

http://dx.doi.org/10.1016/j.ffa.2014.02.008
1071-5797/

number of $\mathbb{F}_{q^k}$-rational points on the affine hypersurface $f = 0$ in $\mathbb{A}^n(\mathbb{F}_{q^k})$. Suppose that f has the sparse representation as a sum of m nonzero monomials:

$$f(x_1, \ldots, x_n) = \sum_{j=1}^{m} a_j x_1^{d_{1j}} \cdots x_n^{d_{nj}}, \quad a_j \in \mathbb{F}_q^*. \tag{1}$$

Let $V_j = (d_{1j}, \ldots, d_{nj})^T \in \mathbb{Z}_{\geqslant 0}^n$. The *degree matrix* of f is defined to be the matrix

$$D = (V_1, \ldots, V_m) \in \mathbb{Z}_{\geqslant 0}^{n \times m}.$$

Clearly, f is completely determined by the coefficient vector $\mathbf{a} = (a_1, \ldots, a_m)$ and the degree matrix D; we simply write $f = (\mathbf{a}, D)$ for short. Let $\widetilde{V}_j = (1, V_j^T)^T$. The *augmented degree matrix of* f is defined to be the matrix

$$\widetilde{D} = (\widetilde{V}_1, \ldots, \widetilde{V}_m) \in \mathbb{Z}_{\geqslant 0}^{(n+1) \times m}.$$

The (augmented) degree matrices are useful to study the polynomials over finite fields. Cao and Sun [4] found an explicit formula for the number of solutions of a given polynomial provided that its degree matrix is nonsingular in a certain sense. This result was generalized in [5] to the augmented degree matrix via the Smith normal form.

Let Ω be a subset of the set $\{0, 1, \ldots, q-1\}$ and $\Omega^m = \prod_{j=1}^m \Omega$ be the direct product of Ω. For any $\mathbf{l} = (l_1, \ldots, l_m) \in \Omega^m$, define $\sigma(\mathbf{l})$ and $s(\mathbf{l})$ to be the number of nonzero entries in $(l_1, \ldots, l_m)$ and $l_1\widetilde{V}_1 + \cdots + l_m\widetilde{V}_m$, respectively.

Theorem 1. *(See [5].) Assume $\widetilde{D} \in \mathbb{Z}_{\geqslant 0}^{(n+1) \times m}$ with $m \leqslant n+1$. Suppose that $\widetilde{D}$ has the Smith normal form with the diagonal entries $\lambda_1, \ldots, \lambda_m$ where $\lambda_i | \lambda_{i+1}$ for $i = 1, \ldots, m-1$ and $\lambda_m > 0$. If $\gcd(\lambda_m, q^r - 1) = 1$ for some positive integer r, then*

$$N_r(f) = \sum_{\mathbf{l} \in \Omega^m} (-1)^{\sigma(\mathbf{l})} \left(q^r - 1\right)^{s(\mathbf{l}) - \sigma(\mathbf{l})} q^{r(n - s(\mathbf{l}) + \sigma(\mathbf{l}))},$$

where $\Omega = \{0, q^r - 1\}$.

In other words, Theorem 1 deals with the case that the augmented degree matrix has full column rank and the greatest invariant factor λ_m is coprime to $q^r - 1$. How about the other case in which $\gcd(\lambda_m, q^r - 1) \neq 1$? This paper will address this problem. In fact, we will do more, namely, to compute the L-functions of certain exponential sums. Let us give the definition of L-function in this setting.

In the following, unless otherwise stated, we always assume that $f(x_1, \ldots, x_n) \in \mathbb{F}_q[x_1, x_1^{-1}, \ldots, x_n, x_n^{-1}]$ is a Laurent polynomial having m nonzero monomials as in (1) with $V_j = (d_{1j}, \ldots, d_{nj})^T \in \mathbb{Z}^n$, and its degree matrix is defined similarly to be $D = (V_1, \ldots, V_m) \in \mathbb{Z}^{n \times m}$. Let ζ_p be a fixed complex primitive p-th root of unity. For the Laurent polynomial $f(x_1, \ldots, x_n)$, we form the toric exponential sum

$$S_k^*(f) = \sum_{x_1,\ldots,x_n \in \mathbb{F}_{q^k}^*} \zeta_p^{\mathrm{Tr}_k(f(x_1,\ldots,x_n))},$$

where Tr_k denotes the absolute trace map from $\mathbb{F}_{q^k}$ to the prime field $\mathbb{F}_p$. The corresponding L-function is defined as follows:

$$L^*(f,T) = \exp\left(\sum_{k=1}^{\infty} S_k^*(f)\frac{T^k}{k}\right).$$

Such L-function encodes important arithmetic and geometric information about the associated polynomial. For example, the first slope of the Newton polygon of $L^*(f,T)$ is related to the p-adic estimate for $S_k^*(f)$. And the Dwork–Bombieri–Grothendieck theorem tells that $L^*(f,T)$ is a rational function, i.e.,

$$L^*(f,T) = \frac{\prod_{i=1}^{d_1}(1-\alpha_i T)}{\prod_{j=1}^{d_2}(1-\beta_j T)}, \tag{2}$$

where the finitely many numbers α_i $(1 \leqslant i \leqslant d_1)$ and β_j $(1 \leqslant j \leqslant d_2)$ are non-zero algebraic integers. Equivalently, one has

$$S_k^*(f) = \sum_{i=1}^{d_2} \beta_i^k - \sum_{j=1}^{d_1} \alpha_j^k.$$

But it is difficult to calculate the L-functions in general. We do not even know exactly the number d_1 of zeros and the number d_2 of poles in most cases, although good upper bounds are available, see [1–3]. In this paper, we will show that if the invariant factors of the degree matrix satisfy certain conditions then an explicit formula for the corresponding L-function can be obtained in terms of Gauss sums, which also reveals some information about d_i $(i = 1, 2)$ in these cases.

Some necessary preliminaries on Gauss sums and q-action are reviewed in Sections 2 and 3 respectively, which can also be found in [9,11–13]. The main results are given in Section 4. As an application, we compute the zeta functions for some hypersurfaces in Section 5, which generalizes Theorem 1.

2. Gauss sums

Let ξ_{q-1} be a complex primitive $(q-1)$-th root of unity. Fix any prime ideal $\mathfrak{p}$ in $\mathbb{Z}[\xi_{q-1}]$ lying over p. Then $\mathbb{Z}[\xi_{q-1}]/\mathfrak{p}$ is a finite field of order q, which we identify with $\mathbb{F}_q$. Let ω be the Teichmüller character on $\mathbb{F}_q$, i.e., an isomorphism

$$\omega : \mathbb{F}_q^* \to \left\{1, \xi_{q-1}, \xi_{q-1}^2, \ldots, \xi_{q-1}^{q-2}\right\}$$

satisfying $\omega(a) \pmod{\mathfrak{p}} = a$ for all $a \in \mathbb{F}_q^*$. The Teichmüller character ω has order $q-1$, so all the characters of $\mathbb{F}_q^*$ are generated by ω, namely $\widehat{\mathbb{F}_q^*} = \{\omega^l\colon\ l = 0, 1, \ldots, q-2\}$ with $\omega^l(a) := \omega(a)^l$. Extend ω^l to $\mathbb{F}_q$ by setting $\omega^l(0) = 0$ for $l > 0$ and $\omega^0(0) = 1$. Recall that Tr_k denotes the absolute trace map from $\mathbb{F}_{q^k}$ to the prime field $\mathbb{F}_p$. For brevity, we write Tr for the case $k = 1$. Define the $(q-1)$ Gauss sums over $\mathbb{F}_q$ by

$$G_q(l) = -\sum_{a\in\mathbb{F}_q^*} \omega(a)^{-l}\zeta_p^{\mathrm{Tr}(a)}, \quad 0 \leqslant l \leqslant q-2.$$

From the above definition, one easily calculated that $G_q(0) = 1$. For each $a \in \mathbb{F}_q^*$, the Gauss sums satisfy the following interpolation relation

$$\zeta_p^{\mathrm{Tr}(a)} = \sum_{l=0}^{q-2} \frac{G_q(l)}{1-q}\omega(a)^l.$$

Let $f(x_1, \ldots, x_n)$ be a Laurent polynomial of the form as in (1) with the degree matrix D of order $n \times m$. Using the formula

$$\sum_{t\in\mathbb{F}_q^*} \omega(t)^l = \begin{cases} 0, & \text{if } (q-1) \nmid l, \\ q-1, & \text{if } (q-1) \mid l, \end{cases}$$

one then calculates that

$$\begin{aligned} S_1^*(f) &= \sum_{x_1,\ldots,x_n\in\mathbb{F}_q^*} \zeta_p^{\mathrm{Tr}(f(x_1,\ldots,x_n))} = \sum_{x_1,\ldots,x_n\in\mathbb{F}_q^*} \prod_{j=1}^{m} \zeta_p^{\mathrm{Tr}(a_j x^{V_j})} \\ &= \sum_{x_1,\ldots,x_n\in\mathbb{F}_q^*} \prod_{j=1}^{m} \sum_{l_j=0}^{q-2} \frac{G_q(l_j)}{1-q}\omega(a_j)^{l_j}\omega\big(x^{V_j}\big)^{l_j} \\ &= \sum_{l_1=0}^{q-2} \cdots \sum_{l_m=0}^{q-2} \left(\prod_{j=1}^{m} \frac{G_q(l_j)}{1-q}\omega(a_j)^{l_j}\right) \sum_{x_1,\ldots,x_n\in\mathbb{F}_q^*} \omega\big(x^{l_1V_1+\cdots+l_mV_m}\big) \\ &= (-1)^m \sum_{\sum_{j=1}^m l_jV_j\equiv 0 \pmod{q-1}} (q-1)^{n-m} \prod_{j=1}^{m} \omega(a_j)^{l_j} G_q(l_j). \end{aligned}$$

This gives a formula for the exponential sums $S_1^*(f)$ over the field $\mathbb{F}_q$. One can similarly deduce a formula for the exponential sums $S_k^*(f)$ over the k-th extension field $\mathbb{F}_{q^k}$ by simply replacing q by q^k and noting the fact that $\omega(a_j)$ remains unchanged:

$$S_k^*(f) = (-1)^m \sum_{\sum_{j=1}^m l_jV_j\equiv 0 \pmod{q^k-1}} \big(q^k-1\big)^{n-m} \prod_{j=1}^{m} \omega(a_j)^{l_j} G_{q^k}(l_j). \tag{3}$$

3. q-Action (Frobenius action)

Let $D \in \mathbb{Z}^{n\times m}$ be the degree matrix of a Laurent polynomial f as in (1). Denote by $S(D)$ the set of rational solutions to the linear system

$$Du \equiv 0 \pmod 1, \quad u = (u_1, \ldots, u_m)^T \in \mathbb{Q}^m,\ 0 \leqslant u_i < 1.$$

The set $S(D)$ has a natural abelian group structure under addition modulo 1. When the matrix D has full column rank, the order of $S(D)$ can be given in terms of the invariant factors of D.

Lemma 2. *If the matrix D has exactly m nonzero invariant factors $\lambda_1, \ldots, \lambda_m$, then $|S(D)| = \prod_{j=1}^m \lambda_j$.*

Proof. By the Smith normal form theorem, there exist two unimodular matrices $U \in GL_n(\mathbb{Z})$ and $V \in GL_m(\mathbb{Z})$ such that D is equivalent to $\Lambda := UDV = (\lambda_{ij})$ with $\lambda_{ij} = 0$ for $i \neq j$ and $\lambda_{jj} = \lambda_j$ $(j = 1, \ldots, m)$. Clearly, $|S(\Lambda)| = \prod_{j=1}^m \lambda_j$. Since both U and V are invertible, one has $|S(D)| = |S(\Lambda)|$. The result follows. □

Now assume that $|S(D)|$ is finite. Let $S_p(D)$ denote the prime to p part of $S(D)$. It is a subgroup of order equal to the prime to p factor of $|S(D)|$. That is,

Lemma 3. *If the matrix D has exactly m nonzero invariant factors $\lambda_1, \ldots, \lambda_m$. Let $\lambda_i = p^{r_i}\lambda_i'$ with $\lambda_i' \in \mathbb{Z}$ and $p \nmid \lambda_i'$ for $i = 1, \ldots, m$, then $|S_p(D)| = \prod_{j=1}^m \lambda_j'$.*

Recall $\operatorname{char} \mathbb{F}_q = p$. Then multiplication by q induces an automorphism of the group $S_p(D)$. This map is also called the q-action (Frobenius action) of $S_p(D)$. For each $u \in S_p(D)$, let $O(u)$ denote the orbit of u under the q-action and $\circ(u)$ the length of $O(u)$. Since the order of $S_p(D)$ is finite, $\circ(u)$ is also finite. Note that $\circ(u)$ is just the least positive integer d such that $(q^d - 1)u \in \mathbb{Z}^n$. For each positive integer d, denote by $S_p(D, d)$ the set of $u \in S_p(D)$ with $\circ(u) = d$. Then we have the disjoint decomposition $S_p(D) = \bigcup_{d\geqslant 1} S_p(D, d)$.

Let $u = (u_1, \ldots, u_m)$ and $u' = (u_1', \ldots, u_m')$ be two elements in $S_p(D, d)$ which are in the same orbit under q-action, i.e. $O(u) = O(u')$. Then one checks from the above definition of Gauss sums that

$$G_{q^d}\big(u_i\big(q^d - 1\big)\big) = G_{q^d}\big(u_i'\big(q^d - 1\big)\big) \tag{4}$$

for all $1 \leqslant i \leqslant m$, where $G_{q^d}(k)$ is the Gauss sum defined over the finite extension field $\mathbb{F}_{q^d}$. Thus, the q-action does not change the Gauss sum. For $u \in S_p(D, d)$ and any integer k, the well known Hasse–Davenport relation [6] says that

$$G_{q^{dk}}\big(u\big(q^{dk} - 1\big)\big) = G_{q^d}\big(u\big(q^d - 1\big)\big)^k. \tag{5}$$

4. L-functions

In this section, we will give an explicit formula for the L-function of the toric exponential sums of the Laurent polynomial if its degree matrix has full column rank. To make our theorem have wider application, we introduce the concept of p-equivalence between matrices.

Let A, B be two integer matrices of the same order. If $S_p(A) = S_p(B)$, then the matrices A and B are said to be *p-equivalent*. One easily shows that $S_p(A) = S_p(B)$ if A is transformed into B by a sequence of elementary row operations consisting of: (1) row swap, (2) row multiplication by p or p^{-1}, and (3) row addition.

Theorem 4. *Let $f = (\mathbf{a}, D)$ be a Laurent polynomial in n variables with coefficient vector $\mathbf{a} = (a_1, \ldots, a_m) \in (\mathbb{F}_q^*)^m$ and degree matrix $D \in \mathbb{Z}^{n\times m}$ having full column rank. Suppose that D is p-equivalent to the block matrix $D' = \left(\begin{smallmatrix} D_1 & 0 \\ 0 & D_2 \end{smallmatrix}\right)$ with $D_i \in \mathbb{Z}^{n_i\times m_i}$ for $i = 1, 2$, and all the invariant factors of D_1 being the powers of p. Then we have*

$$L^*(f,T) = \prod_{d\geqslant 1}\prod_{u\in S_p(D,d)} \times \prod_{i=0}^{n-m}\left(1 - T^d q^{di} \prod_{j=m_1+1}^{m} \omega(a_j)^{u_j(q^d-1)} G_{q^d}\big(u_j\big(q^d-1\big)\big)\right)^{\frac{\binom{n-m}{i}(-1)^{n-i-1}}{d}}. \tag{6}$$

Proof. Define a new polynomial g by $g = (\mathbf{a}, D')$ where $\mathbf{a} = (a_1, \ldots, a_m)$ is also the coefficient vector of f. Let k be an arbitrary positive integer. Since D is p-equivalent to D', both the linear systems $DX \equiv 0 \pmod{q^k - 1}$ and $D'Y \equiv 0 \pmod{q^k - 1}$ have the same solution sets. It follows from (3) that $S_k^*(f) = S_k^*(g)$. Due to the arbitrariness of k, one has $L^*(f,T) = L^*(g,T)$. So it suffices to calculate the L-function $L^*(g,T)$. Since $D' = \left(\begin{smallmatrix} D_1 & 0 \\ 0 & D_2 \end{smallmatrix}\right)$ and D_1 has m_1 invariant factors that are all powers of p, the solutions $\mathbf{l} = (l_1, \ldots, l_m)$ to the linear system $D'\mathbf{l} \equiv 0 \pmod{q^k - 1}$ must have the form of $l_1 = \cdots = l_{m_1} = 0$. This implies that

$$\prod_{j=1}^{m_1} \omega(a_j)^{l_j} G_{q^k}(l_j) = 1. \tag{7}$$

Applying the trick of interchanging the sums, by (3) and (7) one has

$$\sum_{k=1}^{\infty} S_k^*(f)\frac{T^k}{k} = (-1)^m \sum_{d\geqslant 1}\sum_{u\in S_p(D,d)}\sum_{k\geqslant 1}\big(q^{dk}-1\big)^{n-m} \times \prod_{j=m_1+1}^{m} \omega(a_j)^{u_j(q^{dk}-1)} G_{q^{dk}}\big(u_j\big(q^{dk}-1\big)\big)\frac{T^{dk}}{dk}. \tag{8}$$

Also note that for $u \in S_p(D,d)$

$$\omega(a_j)^{u_j(q^{dk}-1)} = \omega(a_j)^{u_j(q^d-1)k}. \tag{9}$$

Using formulae (4), (5), (8) and (9), one can calculate that

$$\begin{aligned}
&L^*(g,T)\\
&\quad= \exp\Bigg((-1)^m \sum_{d\geqslant 1}\sum_{u\in S_p(D,d)}\sum_{k\geqslant 1}\big(q^{dk}-1\big)^{n-m}\\
&\qquad\times \prod_{j=m_1+1}^{m}\omega(a_j)^{u_j(q^{dk}-1)}G_{q^{dk}}\big(u_j\big(q^{dk}-1\big)\big)\frac{T^{dk}}{dk}\Bigg)\\
&\quad= \exp\Bigg(\sum_{d\geqslant 1}\frac{(-1)^{m-1}}{d}\sum_{u\in S_p(D,d)}\sum_{i=0}^{n-m}\binom{n-m}{i}(-1)^{n-m-i}\\
&\qquad\times\sum_{k\geqslant 1}\Bigg(-\frac{q^{dik}\prod_{j=m_1+1}^{m}\omega(a_j)^{u_j(q^d-1)k}G_{q^d}(u_j(q^d-1))^k T^{dk}}{k}\Bigg)\Bigg)\\
&\quad= \exp\Bigg(\sum_{d\geqslant 1}\sum_{u\in S_p(D,d)}\sum_{i=0}^{n-m}\frac{\binom{n-m}{i}(-1)^{n-i-1}}{d}\\
&\qquad\times\log\Bigg(1-T^d q^{di}\prod_{j=m_1+1}^{m}\omega(a_j)^{u_j(q^d-1)}G_{q^d}\big(u_j\big(q^d-1\big)\big)\Bigg)\Bigg)\\
&\quad= \prod_{d\geqslant 1}\prod_{u\in S_p(D,d)}\prod_{i=0}^{n-m}\exp\Bigg(\frac{\binom{n-m}{i}(-1)^{n-i-1}}{d}\\
&\qquad\times\log\Bigg(1-T^d q^{di}\prod_{j=m_1+1}^{m}\omega(a_j)^{u_j(q^d-1)}G_{q^d}\big(u_j\big(q^d-1\big)\big)\Bigg)\Bigg)\\
&\quad= \prod_{d\geqslant 1}\prod_{u\in S_p(D,d)}\prod_{i=0}^{n-m}\Bigg(1-T^d q^{di}\prod_{j=m_1+1}^{m}\omega(a_j)^{u_j(q^d-1)}G_{q^d}\big(u_j\big(q^d-1\big)\big)\Bigg)^{\frac{\binom{n-m}{i}(-1)^{n-i-1}}{d}}.
\end{aligned}$$

Since $L^*(f,T) = L^*(g,T)$, the theorem is proved. □

Remark 1. For each of the d elements in the orbit of $u \in S_p(D,d)$ under the q-action, the corresponding factor in (6) is the same. Thus we can remove the power $1/d$ if we restrict u to run over the q-orbits of $S_p(D,d)$.

Now assume $\gcd(|S(D_2)|,p) = 1$. In this case, the greatest invariant factor of D_2 is equal to the maximum order of the elements of $S_p(D)$. Thus, if the greatest invariant

factor of D_2 is a divisor of $q-1$, then the q-action on $S_p(D)$ becomes trivial, i.e. $(q-1)u \in \mathbb{Z}^m$ for any $u \in S_p(D)$. So we have

Corollary 5. *Under the same assumption as in Theorem 4, if $q-1$ is divisible by the greatest invariant factor of D_2, then*

$$L^*(f,T) = \prod_{u\in S_p(D)} \prod_{i=0}^{n-m} \left(1 - Tq^i \prod_{j=m_1+1}^{m} \omega(a_j)^{u_j(q-1)} G_q\big(u_j(q-1)\big)\right)^{\binom{n-m}{i}(-1)^{n-i-1}}.$$

For the case that D is a square matrix, the formula for L-functions becomes relatively simpler, which was obtained by Wan [9–11] in his work on the Newton polygon of L-functions.

Corollary 6. *Under the same assumption as in Theorem 4, if $n = m$, then*

$$L^*(f,T)^{(-1)^{n-1}} = \prod_{d\geqslant 1} \prod_{u\in S_p(D,d)} \left(1 - T^d \prod_{j=m_1+1}^{m} \omega(a_j)^{u_j(q^d-1)} G_{q^d}\big(u_j(q^d-1)\big)\right)^{\frac{1}{d}}. \quad (10)$$

Note that the right side of (10) is indeed a polynomial of degree equal to the order of $S_p(D)$ by Remark 1. In particular, if D is a square matrix and all the invariant factors of D are coprime to p, the polynomial f is said to be non-degenerate and the degree of $L^*(f,T)^{(-1)^{n-1}}$ is equal to the order of $S(D)$, which coincides with Adolphson–Sperber's theorem [2], and the formula for the corresponding L-function in this case was generalized to the twisted diagonal exponential sums by Hong [7].

Recall that in general one does not know the numbers of zeros and poles of an arbitrarily given L-function, which are denoted by d_1 and d_2 respectively as in (2). However, we can show that the numbers of zeros and poles of the L-function in Theorem 4 are equal if $n > m$ and give a tight upper bound for them.

Corollary 7. *Let f be a Laurent polynomial with the degree matrix $D \in \mathbb{Z}^{n\times m}$ having full column rank. If $n > m$, then the numbers of zeros and poles of $L^*(f,T)$ are equal; namely, $d_1 = d_2 \leqslant 2^{n-m-1}|S_p(D)|$.*

Proof. Let $N = |S_p(D)|$. First assume that there is no common factor between the numerator and denominator of the L-function. From (6), one sees that

$$d_1 + d_2 = \sum_{i=0}^{n-m} \binom{n-m}{i} N = 2^{n-m} N. \quad (11)$$

From (6), when n is an odd integer, we have

$$d_1 = \sum_{\substack{i=0 \\ 2|i}}^{n-m} \binom{n-m}{i} N = \sum_{i=0}^{n-m} \binom{n-m}{i} \left(\frac{1+(-1)^i}{2}\right) N = 2^{n-m-1} N.$$

Otherwise, i.e. n is an even integer, we have

$$d_1 = \sum_{\substack{i=0 \\ 2\nmid i}}^{n-m} \binom{n-m}{i} N = \sum_{i=0}^{n-m} \binom{n-m}{i} \left(\frac{1-(-1)^i}{2}\right) N = 2^{n-m-1} N.$$

In either case, one deduces from (11) that $d_1 = d_2 = 2^{n-m-1}N$. Now consider the case that there are common factors between the numerator and denominator of the L-function. Due to the one-to-one correspondence between the canceled common factors in the numerator and denominator, one easily concludes that $d_1 = d_2 \leqslant 2^{n-m-1}N$. □

5. Application to computation of zeta functions

For a given polynomial $f \in \mathbb{F}_q[x_1, \ldots, x_n]$ and a positive integer k, recall that $N_k(f)$ denotes the number of $\mathbb{F}_{q^k}$-rational points on the affine hypersurface $f = 0$ in $\mathbb{A}^n(\mathbb{F}_{q^k})$, and the zeta function of f is defined to be the generating function

$$Z(f, T) = \exp\left(\sum_{r=1}^{\infty} N_r(f) \frac{T^r}{r}\right).$$

In this section, we use Theorem 4 to compute the zeta functions for a class of hypersurfaces over the field $\mathbb{F}_q$. For simplicity, we only consider the polynomial with positive degree matrix. That is, we assume the polynomial $f = (\mathbf{a}, D)$ has the coefficient vector $\mathbf{a} = (a_1, \ldots, a_m) \in (\mathbb{F}_q^*)^m$ and the degree matrix $D \in \mathbb{Z}_{>0}^{n\times m}$. So the augmented degree matrix of f, denoted $\widetilde{D}$, is also a positive matrix of order $(n+1) \times m$. Let $N_1^*(f)$ denote the number of solutions $(x_1, \ldots, x_n) \in (\mathbb{F}_q^*)^n$ to the equation $f = 0$. It is easy to see that

$$N_1(f) = q^n - (q-1)^n + N_1^*(f). \tag{12}$$

Using the similar notation and deduction as in Section 2, one gets

$$qN_1^*(f) = (q-1)^n + (-1)^m (q-1)^{n+1-m} \sum_{\widetilde{D}\mathbf{l} \equiv 0 \pmod{q-1}} \prod_{j=1}^{m} \omega(a_j)^{l_j} G_q(l_j) \tag{13}$$

where $\mathbf{l} = (l_1, \ldots, l_m)$ with $0 \leqslant l_j \leqslant q-2$. By (12) and (13) we have

$$N_1(f) = q^n - \frac{(q-1)^{n+1}}{q} + \frac{1}{q}(-1)^m (q-1)^{n+1-m} \sum_{\widetilde{D}\mathbf{l} \equiv 0 \pmod{q-1}} \prod_{j=1}^{m} \omega(a_j)^{l_j} G_q(l_j),$$

where the sum is defined as in (13). Replacing q by q^k one gets a formula for $N_k(f)$ over the k-th extension field $\mathbb{F}_{q^k}$. By the similar technique as in the proof of Theorem 4, it is not hard to get

Theorem 8. *Let $f = (\mathbf{a}, D)$ be a polynomial in n variables with coefficient vector $\mathbf{a} = (a_1, \ldots, a_m) \in (\mathbb{F}_q^*)^m$ and degree matrix $D \in \mathbb{Z}_{>0}^{n\times m}$. Suppose that the augmented degree matrix $\widetilde{D}$ has full column rank and is p-equivalent to the block matrix $D' = \left(\begin{smallmatrix} D_1 & 0 \\ 0 & D_2 \end{smallmatrix}\right)$ with $D_i \in \mathbb{Z}^{n_i\times m_i}$ for $i = 1, 2$, and all invariant factors of D_1 being the powers of p. Then we have*

$$Z(f,T) = \prod_{d\geqslant 1}\prod_{u\in S_p(\widetilde{D},d)} \times \prod_{i=0}^{n+1-m}\left(1 - T^d q^{d(i-1)} \prod_{j=m_1+1}^{m} \omega(a_j)^{u_j(q^d-1)} G_{q^d}\big(u_j\big(q^d-1\big)\big)\right)^{\frac{\binom{n+1-m}{i}(-1)^{n-i}}{d}} \times \prod_{r=1}^{n+1}\big(1-q^{n-r}T\big)^{\binom{n+1}{r}(-1)^r}.$$

To finish this paper, we take an example to show that some known results can be deduced from Theorem 8. Let f be a polynomial with positive degree matrix $D \in \mathbb{Z}_{>0}^{n\times m}$. Further assume that D has full column rank and all its invariant factors are the powers of p. By Theorem 8, the zeta function of f is

$$Z(f,T) = \prod_{i=0}^{n+1-m}\big(1-q^{i-1}T\big)^{\binom{n+1-m}{i}(-1)^{n-i}} \prod_{r=1}^{n+1}\big(1-q^{n-r}T\big)^{\binom{n+1}{r}(-1)^r}.$$

Thus for any positive integer k, we have

$$\begin{aligned} N_k(f) &= \sum_{i=0}^{n+1-m}\binom{n+1-m}{i} q^{k(i-1)}(-1)^{n-i+1} + \sum_{r=1}^{n+1}\binom{n+1}{r} q^{k(n-r)}(-1)^{r+1} \\ &= q^{kn} - \frac{(q^k-1)^{n+1-m}((q^k-1)^m - (-1)^m)}{q^k}. \end{aligned}$$

This result was first proven for the case $m = n$ by Sun [8], and later was generalized to the case $m \leqslant n+1$ by Cao and Sun [4,5].

Acknowledgments

The authors sincerely thank the editor and referees for their helpful comments which led to a substantial improvement of this paper. This work was jointly supported by the National Natural Science Foundation of China (Grant Nos. 11371208 and 61373007),

and Ningbo Natural Science Foundation (Grant Nos. 2012A610034 and 2013A610102), and sponsored by the K.C. Wong Magna Fund of Ningbo University.

References

[1] A. Adolphson, S. Sperber, Newton polyhedra and the degree of the L-function associated to an exponential sum, Invent. Math. 88 (1987) 555–569.
[2] A. Adolphson, S. Sperber, Exponential sums and Newton polyhedra: Cohomology and estimates, Ann. Math. 130 (1989) 367–406.
[3] E. Bombieri, On exponential sums in finite fields, II, Invent. Math. 47 (1978) 29–39.
[4] W. Cao, Q. Sun, On a class of equations with special degrees over finite fields, Acta Arith. 130 (2007) 195–202.
[5] W. Cao, Smith normal form of augmented degree matrix and its applications, Linear Algebra Appl. 431 (2009) 1778–1784.
[6] H. Davenport, H. Hasse, Die Nullstellen der Kongruenzzetafunktionen in gewissen zyklischen Fällen, J. Reine Angew. Math. 172 (1935) 151–182.
[7] S. Hong, L-functions of twisted diagonal exponential sums over finite fields, Proc. Am. Math. Soc. 135 (2007) 3099–3108.
[8] Q. Sun, Formula for the number of solutions of a class of equations over finite fields, Chin. Ann. Math., Ser. A 18 (1997) 403–408.
[9] D. Wan, Newton polygons and congruence decompositions of L-functions over finite fields, Contemp. Math. 133 (1992) 221–241.
[10] D. Wan, Newton polygons of zeta functions and L-functions, Ann. Math. 137 (1993) 249–293.
[11] D. Wan, Variation of p-adic Newton polygons for L-functions of exponential sums, Asian J. Math. 8 (2004) 427–474.
[12] D. Wan, Mirror Symmetry for Zeta Functions, AMS/IP Stud. Adv. Math., vol. 38, Amer. Math. Soc., Providence, RI, 2006, pp. 159–184.
[13] D. Wan, Modular counting of rational points over finite fields, Found. Comput. Math. 8 (2008) 597–605.