Exponential sums nondegenerate
relative to a lattice

Alan Adolphson and Steven Sperber

Exponential sums nondegenerate relative to a lattice

Alan Adolphson and Steven Sperber

Our previous theorems on exponential sums often did not apply or did not give sharp results when certain powers of a variable appearing in the polynomial were divisible by p. We remedy that defect in this paper by systematically applying *p-power reduction*, making it possible to strengthen and extend our earlier results.

1. Introduction

In the papers [AS 1987a; 1987b; 1989; 1990a; 1990b] we established properties of the L-functions of exponential sums on affine space $\mathbb{A}^n$ and the torus $\mathbb{T}^n$. The purpose of this article is to prove a general result that leads to a sharpening of the theorems of those papers.

Let p be a prime, let $q = p^r$, and let $\mathbb{F}_q$ be the field of q elements. Let $f \in \mathbb{F}_q[x_1^{\pm 1}, \ldots, x_n^{\pm 1}]$ be a Laurent polynomial, say,

$$f = \sum_{j \in J} a_j x^j, \tag{1.1}$$

where $a_j \in \mathbb{F}_q^{\times}$ and J is a finite subset of $\mathbb{Z}^n$. Let $\mathbb{Z}\langle J \rangle$ be the subgroup of $\mathbb{Z}^n$ generated by the elements of J. By the basic theory of abelian groups, there exists a basis $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n$ for $\mathbb{Z}^n$ and integers $d_1, \ldots, d_k$ such that $d_1\boldsymbol{u}_1, \ldots, d_k\boldsymbol{u}_k$ is a basis for $\mathbb{Z}\langle J \rangle$. After a coordinate change on $\mathbb{T}^n$, we may assume that $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n$ is the standard basis. The Laurent polynomial f may then be written in the form

$$f = g(x_1^{d_1}, \ldots, x_k^{d_k}),$$

for some $g \in \mathbb{F}_q[x_1^{\pm 1}, \ldots, x_k^{\pm 1}]$. Write $d_i = p^{b_i} e_i$ for each i, where $b_i \geq 0$ and $(e_i, p) = 1$. Since raising to the p-th power is an automorphism of $\mathbb{F}_q$, the exponential sums associated to the polynomials f and $g(x_1^{e_1}, \ldots, x_k^{e_k})$ are identical. Furthermore, the theorems in the aforementioned papers generally produce sharper results when applied to $g(x_1^{e_1}, \ldots, x_k^{e_k})$ than when applied to f. (Thus there is no

improvement over our earlier work if $p \nmid [\mathbb{Z}^k : \mathbb{Z}\langle J \rangle]$.) We refer to $g(x_1^{e_1}, \ldots, x_k^{e_k})$ as the *p-power reduction* of f.

Over $\mathbb{A}^n$, the technique of p-power reduction is less versatile because one cannot make the same sorts of coordinate changes. One has a standard toric decomposition $\mathbb{A}^n = \bigcup_{A \subseteq \{1, \ldots, n\}} \mathbb{T}_A$, where $\mathbb{T}_A$ denotes the $|A|$-dimensional torus with coordinates $\{x_i\}_{i \in A}$. Given $f \in \mathbb{F}_q[x_1, \ldots, x_n]$, one can try to analyze the corresponding exponential sum on $\mathbb{A}^n$ by analyzing its restriction to each of these tori, but the picture is complicated by the fact that p-power reduction may require different coordinate changes on different tori. It thus seems worthwhile to generalize our previous results to apply directly to the polynomial as given, to avoid the task of performing p-power reduction on a case-by-case basis.

Let M_J be the *prime-to-p saturation* of $\mathbb{Z}\langle J \rangle$,

$$M_J = \{u \in \mathbb{Z}^n \mid ku \in \mathbb{Z}\langle J \rangle \text{ for some } k \in \mathbb{Z} \text{ satisfying } (k, p) = 1\},$$

and let $\mathbb{R}\langle J \rangle$ denote the subspace of $\mathbb{R}^n$ spanned by the elements of J. We will get a strengthening of our earlier results when M_J is a proper subset of $\mathbb{Z}^n \cap \mathbb{R}\langle J \rangle$. Let

$$[\mathbb{Z}^n \cap \mathbb{R}\langle J \rangle : \mathbb{Z}\langle J \rangle] = p^a e,$$

where $a \geq 0$ and $(e, p) = 1$. Then

$$[\mathbb{Z}^n \cap \mathbb{R}\langle J \rangle : M_J] = p^a, \tag{1.2}$$

so $M_J \neq \mathbb{Z}^n \cap \mathbb{R}\langle J \rangle$ if and only if $a > 0$.

Part of the motivation for this work was a desire to understand Theorems 3.6.5 and 3.6.7 from [Katz 2005] from our point of view. Suppose that $f \in \mathbb{F}_q[x_1, \ldots, x_n]$ is a homogeneous polynomial of degree $d = p^k e$, $(e, p) = 1$, $k \geq 1$. Katz showed that if $f = 0$ defines a smooth hypersurface in $\mathbb{P}^{n-1}$, then the L-function associated to the exponential sum defined by f (see Section 2 for the definition) is a polynomial (n odd) or the reciprocal of a polynomial (n even) of degree

$$\frac{1}{p^k}((d-1)^n + (-1)^n(p^k - 1)),$$

all of whose reciprocal roots have absolute value $q^{n/2}$. Note that in this situation $[\mathbb{Z}^n : M_J] = p^k$. Our results in [AS 1989] do not apply to polynomials of degree divisible by p. However, we show here that when M_J is a proper subset of $\mathbb{Z}^n$ one can weaken the definition of nondegeneracy used in that article and still deduce analogous conclusions. In particular, we show that the above theorem of Katz is true as well for nonhomogeneous polynomials, provided that the homogeneous part of highest degree defines a smooth hypersurface in $\mathbb{P}^{n-1}$ and $[\mathbb{Z}^n : M_J] = p^k$. In other words, the conclusion remains true when one perturbs the smooth homogeneous polynomial by adding arbitrary terms of degrees $p^k e'$, $e' < e$. (In earlier

work, analogous results for exponential sums involving polynomials of degree divisible by p were proved under the additional assumption that the homogeneous form of second highest degree "behaved nicely" relative to the leading form: see [AS 2000; 2009; Rojas-León 2006].)

This generalization of Katz's theorem (Proposition 5.1 below) will be derived as a consequence of Theorem 4.17. Another consequence of that theorem is the following result. Consider the Dwork family of hypersurfaces

$$x_1^n + \cdots + x_n^n + \lambda x_1 \ldots x_n = 0$$

in $\mathbb{P}^{n-1}$. If $n = p^k e$, where $k \geq 1$ and $(p, e) = 1$, and $\lambda \neq 0$, this hypersurface is singular (except for $n = 2, 3$). We show (Corollary 5.9 below) that the zeta function of this hypersurface has the form

$$Z(t) = \frac{R(t)^{(-1)^{n-1}}}{(1-t)(1-qt)\ldots(1-q^{n-2}t)},$$

where $R(t)$ is a polynomial of degree

$$(p^k - 1)e^{n-1} + e^{-1}((e-1)^n + (-1)^n(e-1)),$$

all of whose reciprocal roots have absolute value $q^{(n-2)/2}$. (Zeta functions of the Dwork family have also been studied recently in [Rojas-León and Wan 2007] and [Katz 2007].)

As another example, we strengthen the classical theorem of Chevalley–Warning. Let $f = \sum_{j \in J} a_j x^j \in \mathbb{F}_q[x_1, \ldots, x_n]$ and let $N(f)$ denote the number of solutions of $f = 0$ with coordinates in $\mathbb{F}_q$. Let $\mathbb{N}$ denote the nonnegative integers, let $\mathbb{N}_+$ denote the positive integers, and let $J' = \{(j, 1) \in \mathbb{N}^{n+1} \mid j \in J\}$. Let $\Delta(J')$ denote the convex hull of $J' \cup \{(0, \ldots, 0)\}$ in $\mathbb{R}^{n+1}$.

Theorem 1.3. *Let μ be the smallest positive integer such that $\mu \Delta(J')$, the dilation of $\Delta(J')$ by the factor μ, contains a point of $M_{J'} \cap (\mathbb{N}_+)^{n+1}$. Then $\mathrm{ord}_q N(f) \geq \mu - 1$, where ord_q denotes the p-adic valuation normalized by $\mathrm{ord}_q q = 1$.*

For example, the equation $\sum_{i=1}^n x_i^{p^{k_i}} = 0$ has q^{n-1} solutions: since raising to the p-th power is an automorphism of $\mathbb{F}_q$, one can assign arbitrary values to $x_1, \ldots, x_{n-1}$ and there will be a unique value of x_n satisfying the equation. Since $M_{J'} = \mathbb{Z}\langle J' \rangle$ is the lattice generated by the $\{(0, \ldots, 0, p^{k_i}, 0, \ldots, 0, 1)\}_{i=1}^n$, $\mu = n$ and Theorem 1.3 gives the precise divisibility by q.

For a more subtle example, let $p = 3$, $n = 3$, and consider the polynomial

$$f = x_1 x_2^2 + x_2 x_3^2 + x_1^2 x_3.$$

The lattice $M_{J'} = \mathbb{Z}\langle J' \rangle$ is the rank-three sublattice of $\mathbb{Z}^4$ with basis the vectors

$$\boldsymbol{u}_1 = (1, 2, 0, 1), \, \boldsymbol{u}_2 = (0, 1, 2, 1), \, \boldsymbol{u}_3 = (2, 0, 1, 1).$$

The only point of $\Delta(J') \cap (\mathbb{N}_+)^4$ is $(1, 1, 1, 1)$ and one has

$$(1, 1, 1, 1) = \tfrac{1}{3}(\boldsymbol{u}_1 + \boldsymbol{u}_2 + \boldsymbol{u}_3), \tag{1.4}$$

thus $(1, 1, 1, 1) \notin M_{J'}$. It follows that $\mu > 1$, so Theorem 1.3 implies that $N(f)$ is divisible by 3^r. (In fact, $\boldsymbol{u}_1 + \boldsymbol{u}_2 \in M_{J'} \cap (\mathbb{N}_+)^4$, so $\mu = 2$.) On the other hand, since the degree of f equals the number of variables, the classical Chevalley–Warning Theorem does not predict the divisibility of $N(f)$ by 3. If we take the same polynomial f but assume $p \neq 3$, then (1.4) shows that

$$(1, 1, 1, 1) \in M_{J'},$$

so $\mu = 1$ and Theorem 1.3 does not predict any divisibility by p.

   Theorem 1.3 is a special case of Theorem 3.3, which we prove by the method of [Ax 1964], as applied in [AS 1990a]. Ax expresses an exponential sum as a sum of certain products of Gauss sums; Stickelberger's Theorem computes the valuation of each Gauss sum, so one must determine which of these products of Gauss sums has minimal valuation. This minimum is in general difficult to calculate directly, so one replaces the set of valuations by a larger set whose minimum is easier to calculate. We used a convexity argument in [AS 1990a, Lemma 1], which is the approach we take here. Another method for estimating this minimum is via the "p-weight" of the polynomial: see [Moreno et al. 2004, Section 4] for a description of this approach and references to related work. The results obtained from these two approaches do not seem comparable, that is, neither implies the other as far as we know.

   The first main idea of this paper is that when computing the action of Dwork's Frobenius operator, which gives the L-function of the exponential sum on the torus, one can ignore the action of Frobenius on power series whose exponents lie outside of M_J since such power series contribute nothing to the spectral theory of Frobenius. This idea is explained in Section 2. The second main idea is the notion of nondegeneracy relative to a lattice, which is introduced in Section 4. It guarantees that the p-power reduction of f will be nicely behaved. This leads to precise formulas for the degree of the L-function and the number of roots of a given archimedian weight.

2. Trace formula

Let $\Psi : \mathbb{F}_q \to \mathbb{Q}(\zeta_p)$ be a nontrivial additive character and define

$$S_m(\mathbb{T}^n, f) = \sum_{x \in \mathbb{T}^n(\mathbb{F}_{q^m})} \Psi(\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(f(x))),$$

where $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}$ denotes the trace map. In the special case where $f \in \mathbb{F}_q[x_1, \ldots, x_n]$, we can also define

$$S_m(\mathbb{A}^n, f) = \sum_{x \in \mathbb{A}^n(\mathbb{F}_{q^m})} \Psi(\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(f(x))).$$

There are corresponding L-functions

$$L(\mathbb{T}^n, f; t) = \exp\Big(\sum_{m=1}^{\infty} S_m(\mathbb{T}^n, f)\frac{t^m}{m}\Big)$$

and

$$L(\mathbb{A}^n, f; t) = \exp\Big(\sum_{m=1}^{\infty} S_m(\mathbb{A}^n, f)\frac{t^m}{m}\Big).$$

Let $\mathbb{Q}_p$ denote the field of p-adic numbers and $\mathbb{Z}_p$ the ring of p-adic integers. Set $\Omega_1 = \mathbb{Q}_p(\zeta_p)$. Then Ω_1 is a totally ramified extension of $\mathbb{Q}_p$ of degree $p - 1$. Let K denote the unramified extension of $\mathbb{Q}_p$ of degree r and set $\Omega_0 = K(\zeta_p)$. The Frobenius automorphism $x \mapsto x^p$ of $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ lifts to a generator τ of $\mathrm{Gal}(\Omega_0/\Omega_1)$ by setting $\tau(\zeta_p) = \zeta_p$. Let Ω be the completion of an algebraic closure of Ω_0. Let "ord" denote the additive valuation on Ω normalized by $\mathrm{ord}\, p = 1$ and let "ord_q" denote the additive valuation normalized by $\mathrm{ord}_q\, q = 1$.

Let $E(t) = \exp(\sum_{i=0}^{\infty} t^{p^i}/p^i)$ be the Artin–Hasse exponential series. Let $\gamma \in \Omega_1$ be a solution of $\sum_{i=0}^{\infty} t^{p^i}/p^i = 0$ satisfying $\mathrm{ord}\, \gamma = 1/(p-1)$ and set

$$\theta(t) = E(\gamma t) = \sum_{i=0}^{\infty} \lambda_i t^i \in \Omega_1[\![t]\!].$$

The series $\theta(t)$ is a splitting function in Dwork's terminology and its coefficients satisfy

$$\mathrm{ord}\, \lambda_i \geq \frac{i}{p-1}. \tag{2.1}$$

Define the *Newton polyhedron* of f, written $\Delta(f)$, to be the convex hull in $\mathbb{R}^n$ of the set $J \cup \{(0, \ldots, 0)\}$. Let $C(f)$ be the cone in $\mathbb{R}^n$ over $\Delta(f)$, that is, $C(f)$ is the union of all rays in $\mathbb{R}^n$ emanating from the origin and passing through $\Delta(f)$. For any lattice point $u \in C(f) \cap \mathbb{Z}^n$, let $w(u)$, the *weight* of u, be defined as the smallest positive real number (necessarily rational) such that $u \in w(u)\Delta(f)$, where $w(u)\Delta(f)$ denotes the dilation of $\Delta(f)$ by the factor $w(u)$. Then

$$w : C(f) \cap \mathbb{Z}^n \to \frac{1}{N}\mathbb{Z}$$

for some positive integer N. We fix a choice $\tilde{\gamma}$ of N-th root of γ and set $\tilde{\Omega}_0 = \Omega_0(\tilde{\gamma})$, $\tilde{\Omega}_1 = \Omega_1(\tilde{\gamma})$. We extend $\tau \in \mathrm{Gal}(\Omega_0/\Omega_1)$ to a generator of $\mathrm{Gal}(\tilde{\Omega}_0/\tilde{\Omega}_1)$ by setting $\tau(\tilde{\gamma}) = \tilde{\gamma}$. Let $\tilde{\mathbb{O}}_0$ be the ring of integers of $\tilde{\Omega}_0$.

Let M be a lattice such that $M_J \subseteq M \subseteq \mathbb{Z}^n \cap \mathbb{R}\langle J \rangle$, let $L = \mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{Z})$, and let $\ell \in L$. We extend ℓ to a function on $\mathbb{Z}^n \cap \mathbb{R}\langle J \rangle$ as follows. For $u \in \mathbb{Z}^n \cap \mathbb{R}\langle J \rangle$ we have $p^a u \in M$ by (1.2), so we may define

$$\ell(u) = p^{-a}\ell(p^a u).$$

This definition identifies L with a subgroup of $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}^n \cap \mathbb{R}\langle J \rangle, p^{-a}\mathbb{Z})$. Define

$$M_0(f) = \{u \in \mathbb{Z}^n \cap C(f) \mid \mathrm{ord}\,\ell(u) \geq 0 \text{ for all } \ell \in L\}.$$

Note that $M_0(f) = M \cap C(f)$. For $i > 0$ let

$$M_i(f) = \{u \in \mathbb{Z}^n \cap C(f) \mid \inf_{\ell \in L}\{\mathrm{ord}\,\ell(u)\} = -i\}.$$

Note that since L has finite rank, the infimum over L always exists. Furthermore, we have $M_i(f) = \varnothing$ for $i > a$ and

$$\mathbb{Z}^n \cap C(f) = \bigcup_{i=0}^{a} M_i(f).$$

We consider the following spaces of power series (where $b \in \mathbb{R}$, $b \geq 0$, $c \in \mathbb{R}$, and $0 \leq i \leq a$):

$$L_i(b, c) = \left\{ \sum_{u \in M_i(f)} A_u x^u \mid A_u \in \Omega_0,\ \mathrm{ord}\,A_u \geq b w(u) + c \right\},$$

$$L_i(b) = \bigcup_{c \in \mathbb{R}} L_i(b, c),$$

$$B_i = \left\{ \sum_{u \in M_i(f)} A_u \tilde{\gamma}^{Nw(u)} x^u \mid A_u \in \tilde{\mathbb{O}}_0,\ A_u \to 0 \text{ as } u \to \infty \right\},$$

$$B_i' = \left\{ \sum_{u \in M_i(f)} A_u \tilde{\gamma}^{Nw(u)} x^u \mid A_u \in \tilde{\Omega}_0,\ A_u \to 0 \text{ as } u \to \infty \right\}.$$

We also define $L(b, c)$, $L(b)$, B, B' as the unions of these spaces for $i = 0, \ldots, a$. Note that if $b > 1/(p-1)$, then $L_i(b) \subseteq B_i'$ and for $c \geq 0$, $L_i(b, c) \subseteq B_i$. Similarly $L(b) \subseteq B'$ and for $c \geq 0$, $L(b, c) \subseteq B$. Define a norm on B_i, $i = 0, \ldots, a$, as follows. If

$$\xi = \sum_{u \in M_i(f)} A_u \tilde{\gamma}^{Nw(u)} x^u,$$

then set

$$\|\xi\| = \sup_{u \in M_i(f)} |A_u|.$$

One defines a norm on B in an analogous fashion.

Let $\hat{f} = \sum_{j \in J} \hat{a}_j x^j$ be the Teichmüller lifting of f, that is, $\hat{a}_j^q = \hat{a}_j$ and the reduction of $\hat{f}$ modulo p is f. Set

$$F(x) = \prod_{j \in J} \theta(\hat{a}_j x^j), \qquad F_0(x) = \prod_{i=0}^{r-1} F^{\tau^i}(x^{p^i}).$$

The estimate (2.1) implies that $F(x)$ and $F_0(x)$ are well-defined and satisfy

$$F(x) \in L_0\left(\frac{1}{p-1}, 0\right), \quad F_0(x) \in L_0\left(\frac{p}{q(p-1)}, 0\right).$$

We define the operator ψ on series by

$$\psi\left(\sum_{u \in \mathbb{Z}^n} A_u x^u\right) = \sum_{u \in \mathbb{Z}^n} A_{pu} x^u.$$

Clearly, $\psi(L(b, c)) \subseteq L(pb, c)$.

Lemma 2.2. *For $1 \leq i < a$ we have*

$$\psi(L_i(b, c)) \subseteq L_{i+1}(b, c),$$

and for $i = a$ we have

$$\psi(L_a(b, c)) = 0.$$

Furthermore, the same assertions hold with $L_i(b, c)$ replaced by B_i'.

Proof. Let $\ell \in L$ and $pu \in M_i(f)$. Since $\text{ord}\, \ell(pu) \geq -i$, it follows that $\text{ord}\, \ell(u) \geq -i - 1$. By definition of $M_i(f)$ the first inequality is an equality for some $\ell \in L$. The second inequality is then an equality also for that ℓ, hence $u \in M_{i+1}(f)$. $\square$

The operator $\alpha = \psi^r \circ F_0$ is

- an $\widetilde{\Omega}_0$-linear endomorphism of the space B', and
- an Ω_0-linear endomorphism of $L(b)$ for $0 < b \leq p/(p-1)$.

The operator $\alpha_0 = \tau^{-1} \circ \psi \circ F_0$ is

- an $\widetilde{\Omega}_1$-linear endomorphism of B',
- an Ω_1-linear endomorphism of $L(b)$ for $0 < b \leq p/(p-1)$,
- an $\widetilde{\Omega}_0$-semilinear endomorphism of B', and
- an Ω_0-semilinear endomorphism of $L(b)$ for $0 < b \leq p/(p-1)$.

It follows from [Serre 1962] that the operators α^m and α_0^m acting on B' and $L(b)$ for $0 < b \le p/(p-1)$ have well defined traces. In addition, the Fredholm determinants $\det(I - t\alpha)$ and $\det(I - t\alpha_0)$ are well defined and p-adically entire. The Dwork trace formula asserts

$$S_m(\mathbb{T}^n, f) = (q^m - 1)^n \mathrm{Tr}(\alpha^m), \tag{2.3}$$

where α acts either on B' or on some $L(b)$, $0 < b \le p/(p-1)$, and the nontrivial additive character implicit on the left-hand side is given by

$$\Psi(x) = \theta(1)^{\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(x)}.$$

Let δ be the operator on formal power series with constant term 1 defined by $g(t)^{\delta} = g(t)/g(qt)$. Using the relationship $\det(I - t\alpha) = \exp(-\sum_{m=1}^{\infty} \mathrm{Tr}(\alpha^m) t^m/m)$, Equation (2.3) is equivalent to

$$L(\mathbb{T}^n, f; t)^{(-1)^{n-1}} = \det(I - t\alpha)^{\delta^n}. \tag{2.4}$$

Let Γ be the map on power series defined by

$$\Gamma\left(\sum_{u \in \mathbb{Z}^n} A_u x^u\right) = \sum_{u \in M_0(f)} A_u x^u.$$

Define $\tilde{\alpha} = \Gamma \circ \alpha$, an endomorphism of B_0' and $L_0(b)$ for $0 < b \le p/(p-1)$. The main technical result of this paper is the following.

Theorem 2.5. *If $M_J \subseteq M$, then as operator on B_0' and $L_0(b)$ for $0 < b \le p/(p-1)$ the map $\tilde{\alpha}$ satisfies*

$$S_m(\mathbb{T}^n, f) = (q^m - 1)^n \mathrm{Tr}(\tilde{\alpha}^m).$$

Equivalently,

$$L(\mathbb{T}^n, f; t)^{(-1)^{n-1}} = \det(I - t\tilde{\alpha})^{\delta^n}.$$

Proof. To fix ideas, we work with the space B'. Note that if $u \in M_0(f)$ and $v \in M_i(f)$, $1 \le i \le a$, then $u + v \in M_i(f)$. This shows that multiplication by F and F_0 are stable on B_i' for $i = 1, \ldots, a$. Lemma 2.2 then implies that $\alpha(B_i') \subseteq B_{i+1}'$ for $i = 1, \ldots, a-1$ and $\alpha(B_a') = 0$. It follows that any power of α acting on $\bigcup_{i=1}^{a} B_i'$ has trace 0, so on $\bigcup_{i=1}^{a} B_i'$ we have $\det(I - t\alpha) = 1$. From [Serre 1962, Proposition 9] we then get

$$\det(I - t\alpha \mid B') = \det\left(I - t\alpha \mid B' / \bigcup_{i=1}^{a} B_i'\right).$$

Under the Banach space isomorphism $B_0' \cong B' / \bigcup_{i=1}^{a} B_i'$, the operator $\tilde{\alpha}$ is identified with the operator induced by α on $B' / \bigcup_{i=1}^{a} B_i'$. This proves the theorem. $\square$

3. First applications

To improve the results of [AS 1987a], one can replace the space $L(p/(p-1))$ and its associated counting function $W(k)$ used there by the space $L_0(p/(p-1))$ for the lattice M_J and its associated counting function

$$W_0(k) = \text{card}\{u \in M_J \cap C(f) \mid w(u) = k/N\}. \tag{3.1}$$

But since the main results of [AS 1987a] are concerned with the n-torus $\mathbb{T}^n$, it is simpler to just replace f by its p-power reduction as described in the introduction. For example, the first inequality of Theorem 1.8 of that paper becomes the one in Theorem 3.2 below.

Theorem 3.2. *We have* $0 \le \deg L(\mathbb{T}^n, f; t)^{(-1)^{n-1}} \le n! \, V(f)/[\mathbb{Z}^n : M_J]$, *where* $V(f)$ *denotes the volume of* $\Delta(f)$ *relative to Lebesgue measure on* $\mathbb{R}^n$.

The second inequality of [AS 1987a, Theorem 1.8] can be similarly improved.

Suppose that $f \in \mathbb{F}_q[x_1, \ldots, x_n]$ and let $\omega(f)$ be the smallest positive real (hence rational) number such that $\omega(f)\Delta(f)$, the dilation of $\Delta(f)$ by the factor $\omega(f)$, contains a point of $M_J \cap (\mathbb{N}_+)^n$. We prove the following strengthening of [AS 1987b, Theorem 1.2].

Theorem 3.3. *If f is not a polynomial in some proper subset of $\{x_1, \ldots, x_n\}$, then*

$$\text{ord}_q \, S_1(\mathbb{A}^n, f) \ge \omega(f).$$

As an example of Theorem 3.3, consider the polynomial

$$f(x_1, x_2) = x_1 x_2^4 + x_1^7 x_2^3 + x_1^{13} x_2^2.$$

If $p \ne 5$, then $M_J = \mathbb{Z}^2$; so $\omega(f) = 7/25$, which gives the estimate of [AS 1987b, Theorem 1.2]. Theorem 3.3 gives an improvement when $p = 5$. In this case,

$$M_J = \{(u_1, u_2) \in \mathbb{Z}^2 \mid u_1 + 6u_2 \text{ is divisible by } 25\}$$

so $\omega(f) = 1$.

Proof of Theorem 3.3. Let Φ_0 be the set of all functions $\phi : J \to \{0, 1, \ldots, q-1\}$ such that

$$\frac{1}{q-1} \sum_{j \in J} \phi(j) j \in (\mathbb{N}_+)^n.$$

For $\phi \in \Phi_0$ define $\phi' \in \Phi_0$ by

$$\phi'(j) = \begin{cases} 0 & \text{if } \phi(j) = 0, \\ \text{least positive residue of } p\phi(j) \text{ modulo } q-1 & \text{if } \phi(j) \ne 0. \end{cases}$$

We denote the i-fold iteration of this operation by $\phi^{(i)}$. Note that since $q = p^r$, one has $\phi^{(r)} = \phi$. By [AS 1990a, Equation 13] we have

$$\operatorname{ord}_q S_1(\mathbb{A}^n, f) \geq \min_{\phi \in \Phi_0} \left\{ \frac{1}{r} \sum_{i=0}^{r-1} \sum_{j \in J} \frac{\phi^{(i)}(j)}{q-1} \right\}. \tag{3.4}$$

Clearly $\sum_{j \in J} \phi^{(i)}(j) j \in \mathbb{Z}\langle J \rangle$ for all i, so

$$\frac{1}{q-1} \sum_{j \in J} \phi^{(i)}(j) j \in M_J \cap (\mathbb{N}_+)^n.$$

If we define Φ_1 to be the set of all functions $\phi : J \to \mathbb{R}_{\geq 0}$ such that

$$\frac{1}{q-1} \sum_{j \in J} \phi(j) j \in M_J \cap (\mathbb{N}_+)^n,$$

then $\frac{1}{q-1} \Phi_0 \subseteq \Phi_1$, so Equation (3.4) implies

$$\operatorname{ord}_q S_1(\mathbb{A}^n, f) \geq \min_{\phi \in \Phi_1} \left\{ \sum_{j \in J} \phi(j) \right\}.$$

The assertion of Theorem 3.3 then follows from [AS 1990a, Lemma 1] by taking the set L of that lemma equal to $M_J \cap (\mathbb{N}_+)^n$. (Theorem 3.3 can also be proved by repeating *mutatis mutandis* the argument of [AS 1987b, Section 4] with $L(p/(p-1))$ replaced by $L_0(p/(p-1))$.) $\qquad\square$

We derive a generalization of Theorem 1.3 from Theorem 3.3. Let $f_1, \ldots, f_r \in \mathbb{F}_q[x_1, \ldots, x_n]$ and let $N(f_1, \ldots, f_r)$ denote the number of solutions in $\mathbb{F}_q$ to the system $f_1 = \cdots = f_r = 0$. Let $y_1, \ldots, y_r$ be additional variables and set

$$F = \sum_{i=1}^{r} y_i f_i \in \mathbb{F}_q[x_1, \ldots, x_n, y_1, \ldots, y_r].$$

It is easily seen that

$$S_1(\mathbb{A}^{n+r}, F) = q^r N(f_1, \ldots, f_r).$$

Applying Theorem 3.3 to F gives the following result, of which Theorem 1.3 is the special case $r = 1$.

Corollary 3.5. $\operatorname{ord}_q N(f_1, \ldots, f_r) \geq \omega(F) - r$.

4. Nondegeneracy relative to a lattice

The results of [AS 1989; 1990b] are cohomological in nature and require a more detailed development. Suppose that $\mathbb{Z}\langle J \rangle$ has rank k. Let M be a lattice, $\mathbb{Z}\langle J \rangle \subseteq M \subseteq \mathbb{Z}^n \cap \mathbb{R}\langle J \rangle$, and set $L = \text{Hom}_{\mathbb{Z}}(M, \mathbb{Z})$. For $\ell \in L$ we define a "differential operator" E_ℓ on the ring $\mathbb{F}_q[x^u \mid u \in M]$ by linearity and the formula

$$E_\ell(x^u) = \ell(u)x^u.$$

This definition is motivated by the fact that if we write

$$\ell(u_1, \ldots, u_n) = \sum_{j=1}^{n} a_j u_j,$$

where $u = (u_1, \ldots, u_n) \in M \subseteq \mathbb{Z}^n$ and the a_j are rational numbers, and put $E_\ell = \sum_{j=1}^{n} a_j x_j \partial/\partial x_j$, then in characteristic 0,

$$E_\ell(x^u) = \sum_{j=1}^{n} a_j x_j \frac{\partial}{\partial x_j}(x^u) = \ell(u)x^u.$$

Let f be given by (1.1) and let σ be a subset of $\Delta(f)$. Define

$$f_\sigma = \sum_{j \in J \cap \sigma} a_j x^j.$$

We say that f is *nondegenerate relative to* $(\Delta(f), M)$ if for every face σ of $\Delta(f)$ that does not contain the origin, the Laurent polynomials $\{E_\ell(f_\sigma)\}_{\ell \in L}$ have no common zero in $(\bar{\mathbb{F}}_q^\times)^n$, where $\bar{\mathbb{F}}_q$ denotes an algebraic closure of $\mathbb{F}_q$. Note that the condition $\mathbb{Z}\langle J \rangle \subseteq M$ guarantees that all f_σ lie in $\mathbb{F}_q[x^u \mid u \in M]$, so the $E_\ell(f_\sigma)$ are defined. Note also that to check this condition, it suffices to check it on a set of the form $\{E_{\ell_i}\}_{i=1}^{k}$, where $\{\ell_i\}_{i=1}^{k}$ is any basis of L. (We remark that this idea, to replace the differential operators $x_i \partial/\partial x_i$ by certain linear combinations with coefficients that are not p-integral, appears in nascent form in [Dwork 1962], where it was needed to calculate the p-adic cohomology of smooth hypersurfaces of degree divisible by p.)

The condition used in [AS 1989], that f be nondegenerate relative to $\Delta(f)$, is equivalent to the condition that f be nondegenerate relative to $(\Delta(f), \mathbb{Z}^n \cap \mathbb{R}\langle J \rangle)$ in the sense of the present definition. We make the relationship between this definition and our earlier one more explicit. There is a basis $e_1, \ldots, e_n$ for $\mathbb{Z}^n$ and positive integers $d_1, \ldots, d_k$, $k \leq n$, such that $d_1 e_1, \ldots, d_k e_k$ is a basis for M. After a coordinate change on $\mathbb{T}^n$, we may take $e_1, \ldots, e_n$ to be the standard basis for $\mathbb{Z}^n$.

This implies that there exists a Laurent polynomial

$$g = \sum_{c \in C} b_c x^c \in \mathbb{F}_q[x_1^{\pm 1}, \ldots, x_k^{\pm 1}],$$

where C is a finite subset of $\mathbb{Z}^k$, such that

$$f(x_1, \ldots, x_n) = g(x_1^{d_1}, \ldots, x_k^{d_k}). \tag{4.1}$$

Note that (4.1) implies

$$[\mathbb{Z}\langle C \rangle : \mathbb{Z}\langle J \rangle] = d_1 \cdots d_k \ (= [\mathbb{Z}^n \cap \mathbb{R}\langle J \rangle : M]). \tag{4.2}$$

Remark. When we choose $M = M_J$, it follows from Equation (1.2) that each d_i is a power of p. In this case, the exponential sums associated to f and g are identical.

Proposition 4.3. *The Laurent polynomial f is nondegenerate relative to the pair $(\Delta(f), M)$ if and only if g is nondegenerate relative to $(\Delta(g), \mathbb{Z}^k)$.*

Proof. Equation (4.1) implies that there is a one-to-one correspondence between the faces of $\Delta(f)$ and the faces of $\Delta(g)$. Specifically, the face σ of $\Delta(f)$ corresponds to the face σ' of $\Delta(g)$ defined by

$$\sigma' = \{(d_1^{-1} u_1, \ldots, d_k^{-1} u_k) \in \mathbb{R}^k \mid (u_1, \ldots, u_k) \in \sigma\}.$$

Furthermore, we have

$$f_\sigma(x_1, \ldots, x_k) = g_{\sigma'}(x_1^{d_1}, \ldots, x_k^{d_k}).$$

Using $u_1, \ldots, u_k$ as coordinates on $\mathbb{Z}^k$, we may take as basis for $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}^k, \mathbb{Z})$ the linear forms $\{\ell_i'\}_{i=1}^k$ defined by

$$\ell_i'(u_1, \ldots, u_k) = u_i,$$

and we may take as basis for $L = \mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{Z})$ the linear forms $\{\ell_i\}_{i=1}^k$ defined by

$$\ell_i(u_1, \ldots, u_k) = d_i^{-1} u_i.$$

It is straightforward to check that for $i = 1, \ldots, k$,

$$E_{\ell_i}(f_\sigma)(x_1, \ldots, x_k) = E_{\ell_i'}(g_{\sigma'})(x_1^{d_1}, \ldots, x_k^{d_k}).$$

This implies the proposition. $\square$

Lemma 4.4. *Put $[\mathbb{Z}^n \cap \mathbb{R}\langle J \rangle : M_J] = p^a$ and let $M \subseteq \mathbb{Z}^n \cap \mathbb{R}\langle J \rangle$ be a lattice containing $\mathbb{Z}\langle J \rangle$. Then $M \subseteq M_J$ if and only if $p^a \mid [\mathbb{Z}^n \cap \mathbb{R}\langle J \rangle : M]$.*

Proof. Suppose that $p^a \mid [\mathbb{Z}^n \cap \mathbb{R}\langle J \rangle : M]$. Then $[M : \mathbb{Z}\langle J \rangle] = e'$ with $(e', p) = 1$. In particular, $e'm \in \mathbb{Z}\langle J \rangle$ for all $m \in M$, so $M \subseteq M_J$. The other direction of the assertion is clear. $\square$

There are restrictions on the lattices with respect to which f can be nondegenerate.

Proposition 4.5. *Let M be a lattice, $\mathbb{Z}\langle J \rangle \subseteq M \subseteq \mathbb{Z}^n \cap \mathbb{R}\langle J \rangle$.*

(a) *If f is nondegenerate relative to $(\Delta(f), M)$, then $M \subseteq M_J$.*

(b) *Suppose $M \subseteq M_J$. Then f is nondegenerate relative to $(\Delta(f), M)$ if and only if f is nondegenerate relative to $(\Delta(f), M_J)$.*

Proof. We may assume without loss of generality that $\mathbb{Z}\langle J \rangle$ is a subgroup of $\mathbb{Z}^n$ of rank n. For if $\mathrm{rank}(\mathbb{Z}\langle J \rangle) = k < n$, then by (4.1) we may take f to be a Laurent polynomial in $x_1, \ldots, x_k$, in which case $\mathbb{Z}\langle J \rangle$ is a subgroup of $\mathbb{Z}^n \cap \mathbb{R}\langle J \rangle (= \mathbb{Z}^k)$ of rank k.

We suppose M is not contained in M_J and prove that f must be degenerate relative to $(\Delta(f), M)$. By (4.2) and Lemma 4.4, we have $p^a \nmid [\mathbb{Z}\langle C \rangle : \mathbb{Z}\langle J \rangle]$. But $p^a \mid [\mathbb{Z}^n : \mathbb{Z}\langle J \rangle]$, so $p \mid [\mathbb{Z}^n : \mathbb{Z}\langle C \rangle]$. Arguing as in the proof of Equation (4.1) then shows that there exists a Laurent polynomial

$$h = \sum_{e \in E} c_e x^e \in \mathbb{F}_q[x_1^{\pm 1}, \ldots, x_n^{\pm 1}]$$

such that

$$g(x_1, \ldots, x_n) = h(x_1, \ldots, x_{n-1}, x_n^p). \tag{4.6}$$

To show f is degenerate relative to $(\Delta(f), M)$, it suffices by Proposition 4.3 to show that any Laurent polynomial g of the form (4.6) is degenerate relative to $(\Delta(g), \mathbb{Z}^n)$. The weight function w of Section 2 defines an increasing filtration on the ring $\mathbb{F}_q[x^u \mid u \in C(g) \cap \mathbb{Z}^n]$: level i/N of the filtration is spanned by the monomials of weight $\leq i/N$. If g were nondegenerate, then $\{x_i \partial g / \partial x_i\}_{i=1}^n$ would be a regular sequence in the associated graded ring and would generate a proper ideal of codimension $n! V(g)$ (by [Kouchnirenko 1976], see also [AS 1989, Section 2]). But, by Equation (4.6), $x_n \partial g / \partial x_n = 0$, and hence cannot be part of such a regular sequence. This contradiction establishes part (a) of Proposition 4.5.

Now suppose that $M \subseteq M_J$. Choose a basis $\{e^{(i)}\}_{i=1}^n$ for M_J and integers $d_1, \ldots, d_n$ such that $\{d_i e^{(i)}\}_{i=1}^n$ is a basis for M. By Lemma 4.4, $p \nmid d_1 \cdots d_n$. Let $\{\ell_i\}_{i=1}^n$ be the basis for $\mathrm{Hom}_{\mathbb{Z}}(M_J, \mathbb{Z})$ defined by

$$\ell_i(e^{(j)}) = \delta_{ij} \quad \text{(Kronecker's delta)}.$$

Then $\{d_i^{-1} \ell_i\}_{i=1}^n$ is a basis for $\mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{Z})$. And since $(d_i, p) = 1$ for all i, the $\{E_{\ell_i}(f_\sigma)\}_{i=1}^n$ have no common zero in $(\bar{\mathbb{F}}_q^\times)^n$ if and only if the same is true of the $\{E_{d_i^{-1}\ell_i}(f_\sigma)\}_{i=1}^n$. This establishes part (b) of Proposition 4.5. $\square$

By Proposition 4.5(a), we must have $M \subseteq M_J$ if we hope to have f nondegenerate relative to $(\Delta(f), M)$. On the other hand, we must have $M_J \subseteq M$ in order

for the trace formula (Theorem 2.5) to hold for M. Thus the only practical choice for M is to take $M = M_J$. Recall from Section 2 that if $g(t)$ is a power series with constant term 1, then $g(t)^\delta = g(t)/g(qt)$.

Theorem 4.7. *Suppose that $\mathbb{Z}\langle J \rangle$ has rank k and that f is nondegenerate relative to $(\Delta(f), M_J)$. Then $L(\mathbb{T}^n, f; t)^{(-1)^{n-1}} = P(t)^{\delta^{n-k}}$, where $P(t)$ is a polynomial of degree $k! \, V_{M_J}(f)$ and $V_{M_J}(f)$ denotes the volume of $\Delta(f)$ relative to Lebesgue measure on $\mathbb{R}\langle J \rangle$ normalized so that a fundamental domain for M_J has volume 1.*

Proof. One repeats the arguments of [AS 1989] with the modifications introduced for Theorem 2.5: replace $L(b)$ and B' by $L_0(b)$ and B'_0 and use $\tilde{\alpha}$ in place of α. We recall some of these details as they are needed in the proof of Theorem 4.17.

Let
$$\Omega^\bullet : 0 \to \Omega^0 \to \cdots \to \Omega^n \to 0$$

be the cohomological Koszul complex on B'_0 defined by the differential operators $\{\hat{D}_i\}_{i=1}^n$ constructed in [AS 1989, Section 2]. The endomorphism $\tilde{\alpha}$ of B'_0 constructed in Section 2 can be extended to an endomorphism $\tilde{\alpha}_\bullet$ of the complex $\Omega^\bullet$ by noting that $\Omega^i = (B'_0)^{\binom{n}{i}}$ and then defining $\tilde{\alpha}_i : \Omega^i \to \Omega^i$ to be

$$(q^{n-i}\tilde{\alpha})^{\binom{n}{i}} : (B'_0)^{\binom{n}{i}} \to (B'_0)^{\binom{n}{i}}. \tag{4.8}$$

Theorem 2.5 is equivalent to the assertion that

$$L(\mathbb{T}^n, f; t) = \prod_{i=0}^n \det(I - t\tilde{\alpha}_i \mid \Omega^i)^{(-1)^{i+1}},$$

which implies that

$$L(\mathbb{T}^n, f; t) = \prod_{i=0}^n \det(I - t\tilde{\alpha}_i \mid H^i(\Omega^\bullet))^{(-1)^{i+1}}. \tag{4.9}$$

Put $R = \mathbb{F}_q[x^u \mid u \in M_0(f)]$. The ring R has an increasing filtration defined by the weight function w of Section 2: $F_{i/N}R$ is the subspace spanned by $\{x^u \mid w(u) \leq i/N\}$. Let $\bar{R} = \bigoplus_{i=0}^\infty \bar{R}_{i/N}$ be the associated graded ring, that is, $\bar{R}_{i/N} = F_{i/N}R/F_{(i-1)/N}R$. Now suppose that f is nondegenerate relative to $(\Delta(f), M_J)$, let $\{\ell_i\}_{i=1}^k$ be a basis for $L = \mathrm{Hom}_\mathbb{Z}(M_J, \mathbb{Z})$, and let $\overline{E_{\ell_i}(f)} \in \bar{R}_1$ be the image in the associated graded ring of $E_{\ell_i}(f) \in F_1R$. The nondegeneracy hypothesis implies by the arguments in [Kouchnirenko 1976] that $\{\overline{E_{\ell_i}(f)}\}_{i=1}^k$ is a regular sequence in $\bar{R}$, that is, the (cohomological) Koszul complex on $\bar{R}$ defined by $\{\overline{E_{\ell_i}(f)}\}_{i=1}^k$ has vanishing cohomology except in top dimension. Furthermore, also by the methods in [Kouchnirenko 1976], one can show that the single nonvanishing cohomology group has dimension $k! \, V_{M_J}(f)$.

Since $M_J \subseteq \mathbb{Z}^n$, we may express the elements of L as linear forms in n variables. Write

$$\ell_i(u_1, \ldots, u_n) = \sum_{j=1}^{n} a_{ij} u_j, \quad a_{ij} \in p^{-a}\mathbb{Z}.$$

Put $\hat{D}_{\ell_i} = \sum_{j=1}^{n} a_{ij}\hat{D}_j$ and let $\Omega_\ell^\bullet$ be the cohomological Koszul complex on B_0' defined by $\{\hat{D}_{\ell_i}\}_{i=1}^{k}$. The Frobenius action $\tilde{\alpha}_i : \Omega_\ell^i \to \Omega_\ell^i$ is defined to be

$$(q^{k-i}\tilde{\alpha})^{\binom{k}{i}} : (B_0')^{\binom{k}{i}} \to (B_0')^{\binom{k}{i}}.$$

The "reduction mod p" [AS 1989, Lemma 2.10] of $\Omega_\ell^\bullet$ is the Koszul complex on $\bar{R}$ defined by $\{\overline{E_{\ell_i}(f)}\}_{i=1}^{k}$. Monsky's cohomological lifting theorem [Monsky 1970, Theorem 8.5; AS 1989, Theorem A.1] then implies that the cohomology of $\Omega_\ell^\bullet$ vanishes except in top dimension and that $H^k(\Omega_\ell^\bullet)$ has dimension $k! \, V_{M_J}(f)$. But since $\{\hat{D}_{\ell_i}\}_{i=1}^{k}$ are linear combinations of $\{\hat{D}_i\}_{i=1}^{n}$ and vice versa, it follows that (as Frobenius modules)

$$H^i(\Omega^\bullet) \cong (H^k(\Omega_\ell^\bullet))^{\binom{n-k}{n-i}},$$

where it is understood that the right-hand side vanishes if $i < k$. In particular we have $H^n(\Omega^\bullet) \cong H^k(\Omega_\ell^\bullet)$, hence

$$\det(I - t\tilde{\alpha}_i \mid H^i(\Omega^\bullet)) = \det(I - q^{n-i}t\tilde{\alpha}_n \mid H^n(\Omega^\bullet))^{\binom{n-k}{n-i}}.$$

From Equation (4.9) we then get

$$L(\mathbb{T}^n, f; t) = \prod_{i=k}^{n} \det(I - q^{n-i}t\tilde{\alpha}_n \mid H^n(\Omega^\bullet))^{(-1)^{i+1}\binom{n-k}{n-i}}. \qquad (4.10)$$

If we put

$$P(t) = \det(I - t\tilde{\alpha}_n \mid H^n(\Omega^\bullet)) \ (= \det(I - t\tilde{\alpha}_k \mid H^k(\Omega_\ell^\bullet))),$$

then $P(t)$ is a polynomial of degree $k! \, V_{M_J}(f)$ and (4.10) implies that

$$L(\mathbb{T}^n, f; t)^{(-1)^{n-1}} = P(t)^{\delta^{n-k}}.$$

This completes the proof of Theorem 4.7. □

Assume the hypotheses of Theorem 4.7. The quotient ring

$$\bar{R}/(\overline{E_{\ell_1}(f)}, \ldots, \overline{E_{\ell_k}(f)})$$

is a graded ring of dimension $k! \, V_{M_J}(f)$ over $\mathbb{F}_q$. Put

$$a_i = \dim_{\mathbb{F}_q}(\bar{R}/(\overline{E_{\ell_1}(f)}, \ldots, \overline{E_{\ell_k}(f)}))_{i/N}.$$

One can show that $a_i = 0$ for $i > kN$. By either repeating the argument of [AS 1989] or replacing the polynomial f by the polynomial $g(x_1^{e_1}, \ldots, x_n^{e_n})$ constructed in the introduction and applying [AS 1989, Theorem 3.10], one obtains the following generalization of part of [AS 1989, Theorem 3.10].

Theorem 4.11. *Under the hypotheses of Theorem 4.7, the Newton polygon of the polynomial $P(t)$ relative to the valuation* ord_q *lies on or above the Newton polygon relative to* ord_q *of the polynomial* $\prod_{i=0}^{kN}(1 - q^{i/N}t)^{a_i}$.

Remark. We recall the combinatorial description of the a_i. Let $W_0(i)$ be the counting function of Equation (3.1) and form the generating series

$$H(t) = \sum_{i=0}^{\infty} W_0(i)t^{i/N}.$$

Then

$$H(t) = \frac{\sum_{i=0}^{kN} a_i t^{i/N}}{(1-t)^k}.$$

Remark. The lower bound of Theorem 4.11 is generically sharp if, for some integer D depending on $\Delta(f)$, $p \equiv 1 \pmod{D}$ [Wan 1993].

We generalize Theorem 4.7 to the affine case. (The corresponding generalization of Theorem 4.11 is somewhat more involved so we postpone that to a future article.) Let

$$f = \sum_{j \in J} a_j x^j \in \mathbb{F}_q[x_1^{\pm 1}, \ldots, x_k^{\pm 1}, x_{k+1}, \ldots, x_n].$$

For each subset $A \subseteq \{k+1, \ldots, n\}$, let f_A be the polynomial obtained from f by setting $x_i = 0$ for all $i \in A$. Then

$$f_A = \sum_{j \in J_A} a_j x^j \in \mathbb{F}[x_1^{\pm 1}, \ldots, x_k^{\pm 1}, \{x_i\}_{i \notin A}], \tag{4.12}$$

where $J_A = \{j = (j_1, \ldots, j_n) \in J \mid j_i = 0 \text{ for } i \in A\}$. We call f *convenient* if for each such A one has

$$\dim \Delta(f_A) = \dim \Delta(f) - |A|.$$

Suppose f is convenient and nondegenerate relative to $(\Delta(f), M_J)$. The hypothesis that f be convenient guarantees that f_A is also convenient, and the hypothesis that f be nondegenerate relative to $(\Delta(f), M_J)$ implies that f_A is nondegenerate relative to $(\Delta(f_A), M_J \cap \mathbb{R}\langle J_A \rangle)$. By Proposition 4.5(a), we must then have $M_J \cap \mathbb{R}\langle J_A \rangle \subseteq M_{J_A}$. The reverse inclusion is clear, so

$$M_{J_A} = M_J \cap \mathbb{R}\langle J_A \rangle, \tag{4.13}$$

and we conclude that f_A is nondegenerate relative to $(\Delta(f_A), M_{J_A})$. Applying Theorem 4.7, we get that

$$L(\mathbb{T}^{n-|A|}, f_A; t)^{(-1)^{n-|A|-1}} = P_A(t)^{\delta^{n-\dim \Delta(f)}}, \tag{4.14}$$

where $P_A(t)$ is a polynomial of degree

$$\deg P_A(t) = (\dim \Delta(f_A))! \, V_{M_{J_A}}(f_A). \tag{4.15}$$

The standard toric decomposition of affine space gives

$$S_m(\mathbb{T}^k \times \mathbb{A}^{n-k}, f) = \sum_{A \subseteq \{k+1,\dots,n\}} S_m(\mathbb{T}^{n-|A|}, f_A),$$

hence

$$L(\mathbb{T}^k \times \mathbb{A}^{n-k}, f; t)^{(-1)^{n-1}} = \prod_{A \subseteq \{k+1,\dots,n\}} (L(\mathbb{T}^{n-|A|}, f_A; t)^{(-1)^{n-|A|-1}})^{(-1)^{|A|}}. \tag{4.16}$$

Put

$$\nu(f) = \sum_{A \subseteq \{k+1,\dots,n\}} (-1)^{|A|} (\dim \Delta(f_A))! \, V_{M_{J_A}}(f_A).$$

Theorem 4.17. *If $f \in \mathbb{F}_q[x_1^{\pm 1}, \dots, x_k^{\pm 1}, x_{k+1}, \dots, x_n]$ is nondegenerate relative to $(\Delta(f), M_J)$ and convenient, then*

$$L(\mathbb{T}^k \times \mathbb{A}^{n-k}, f; t)^{(-1)^{n-1}} = Q(t)^{\delta^{n-\dim \Delta(f)}}, \tag{4.18}$$

where $Q(t)$ is a polynomial of degree $\nu(f)$.

Proof. It follows from Equations (4.14) and (4.16) that Equation (4.18) holds with

$$Q(t) = \prod_{A \subseteq \{k+1,\dots,n\}} P_A(t)^{(-1)^{|A|}}, \tag{4.19}$$

a rational function of degree $\nu(f)$ by Equation (4.15). It remains only to show that $Q(t)$ is a polynomial.

In the proof of Theorem 4.7, we constructed a complex $\Omega^\bullet$ satisfying

$$H^i(\Omega^\bullet) \cong (H^n(\Omega^\bullet))^{\binom{n-\dim \Delta(f)}{n-i}} \tag{4.20}$$

and $L(\mathbb{T}^n, f; t)^{(-1)^{n-1}} = P(t)^{\delta^{n-\dim \Delta(f)}}$, where

$$P(t) = \det(I - t\tilde{\alpha}_n \mid H^n(\Omega^\bullet)). \tag{4.21}$$

Since f is nondegenerate and convenient, each of the polynomials f_A satisfies the hypotheses of that theorem, so analogous assertions are true. Let

$$\Omega_A^\bullet : 0 \to \Omega_A^0 \to \cdots \to \Omega_A^{n-|A|} \to 0$$

be the corresponding cohomological Koszul complex with differential operators $\{\hat{D}_i^A\}_{i \notin A}$ and Frobenius operators $\{\tilde{\alpha}_i^A\}_{i=0}^{n-|A|}$. We have

$$H^i(\Omega_A^\bullet) = (H^{n-|A|}(\Omega_A^\bullet))^{\binom{n-\dim \Delta(f)}{n-|A|-i}} \tag{4.22}$$

and $L(\mathbb{T}^{n-|A|}, f_A; t)^{(-1)^{n-|A|-1}} = P_A(t)^{n-\dim \Delta(f)}$, where

$$P_A(t) = \det(I - t\tilde{\alpha}_{n-|A|}^A \mid H^{n-|A|}(\Omega_A^\bullet)). \tag{4.23}$$

There is an exact sequence of complexes [Libgober and Sperber 1995, Equation (4.1)]:

$$\Omega^\bullet \to \bigoplus_{|A|=1} \Omega_A^\bullet[-1] \to \bigoplus_{|A|=2} \Omega_A^\bullet[-2] \to \cdots \to \Omega_{\{k+1,\dots,n\}}^\bullet[-n+k] \to 0.$$

Let $\bar{\Omega}^\bullet = \ker(\Omega^\bullet \to \bigoplus_{|A|=1} \Omega_A^\bullet[-1])$, so that there is an exact sequence

$$0 \to \bar{\Omega}^\bullet \to \Omega^\bullet \to \bigoplus_{|A|=1} \Omega_A^\bullet[-1] \to \cdots \to \Omega_{\{k+1,\dots,n\}}^\bullet[-n+k] \to 0. \tag{4.24}$$

Equations (4.20), (4.22), (4.24), and induction on $n - k$ show that

$$H^i(\bar{\Omega}^\bullet) \cong (H^n(\bar{\Omega}^\bullet))^{\binom{n-\dim \Delta(f)}{n-i}}. \tag{4.25}$$

Equation (4.24) implies that

$$\prod_{i=0}^n \det(I - t\tilde{\alpha}_i \mid H^i(\bar{\Omega}^\bullet))^{(-1)^{i+1}}$$

$$= \prod_{A \subseteq \{k+1,\dots,n\}} \left(\prod_{i=0}^{n-|A|} \det(I - t\tilde{\alpha}_i^A \mid H^i(\Omega_A^\bullet))^{(-1)^{i+|A|+1}} \right)^{(-1)^{|A|}}. \tag{4.26}$$

The inner product on the right-hand side of (4.26) equals $L(\mathbb{T}^{n-|A|}, f_A, t)^{(-1)^{|A|}}$, hence by (4.16) the right-hand side equals $L(\mathbb{T}^k \times \mathbb{A}^{n-k}, f; t)$. By (4.25) the left-hand side equals

$$\prod_{i=0}^{n-\dim \Delta(f)} \det(I - tq^i \tilde{\alpha}_n \mid H^n(\bar{\Omega}^\bullet))^{(-1)^{n-1}\binom{n-\dim \Delta(f)}{i}}.$$

We thus have

$$L(\mathbb{T}^k \times \mathbb{A}^{n-k}, f; t)^{(-1)^{n-1}} = \det(I - t\tilde{\alpha}_n \mid H^n(\bar{\Omega}^\bullet))^{\delta^{n-\dim \Delta(f)}}.$$

Comparison with Equation (4.18) then shows that

$$Q(t) = \det(I - t\tilde{\alpha}_n \mid H^n(\bar{\Omega}^\bullet)),$$

hence $Q(t)$ is a polynomial. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad$ □

We explain how to compute the archimedian absolute values of the roots of the polynomial $Q(t)$ under the hypothesis of Theorem 4.17. Take $M = M_J$ and let g be the Laurent polynomial associated to f by Equation (4.1). As noted in the proof of Proposition 4.3, the linear transformation $u_i \mapsto d_i^{-1} u_i$, $i = 1, \ldots, k$, identifies the faces σ of $\Delta(f)$ with the faces σ' of $\Delta(g)$. In particular, the face $\Delta(f_A)$ of $\Delta(f)$ will correspond to some face σ_A' of $\Delta(g)$. Let g_A denote the sum of those terms of g whose exponents lie on the face σ_A' (so that $\Delta(g_A) = \sigma_A'$). By the Remark preceding Proposition 4.3, we have

$$L(\mathbb{T}^{n-|A|}, g_A; t)^{(-1)^{n-|A|-1}} = L(\mathbb{T}^{n-|A|}, f_A; t)^{(-1)^{n-|A|-1}} = P_A(t)^{\delta^{n-\dim \Delta(f)}}. \quad (4.27)$$

The nondegeneracy of f_A relative to $(\Delta(f_A), M_{J_A})$ implies the nondegeneracy of g_A relative to $(\Delta(g_A), \mathbb{Z}^{\dim \Delta(g_A)})$. We can thus apply the results of [AS 1990b] and [Denef and Loeser 1991] to g_A to compute the number of roots of $P_A(t)$ of a given archimedian weight. By Equation (4.19) and the fact that $Q(t)$ is a polynomial, we then get the number of roots of $Q(t)$ of a given archimedian weight.

For applications in the next section, we calculate the number of reciprocal roots of largest possible archimedian absolute value $q^{(\dim \Delta(f))/2}$ of $Q(t)$. For $A \neq \varnothing$, all reciprocal roots of $P_A(t)$ have absolute value $< q^{(\dim \Delta(f))/2}$, so this is just the number of reciprocal roots of $P_\varnothing(t)$ of absolute value $q^{(\dim \Delta(f))/2}$. By Equation (4.27), this can be obtained by applying [AS 1990b, Theorem 1.10] to g: the number $w_{\dim \Delta(f)}$ of reciprocal roots of highest weight is

$$w_{\dim \Delta(f)} = \sum_{(0,\ldots,0) \subseteq \sigma' \subseteq \Delta(g)} (-1)^{\dim \Delta(g) - \dim \sigma'} (\dim \sigma')! \, V_{\mathbb{Z}^{\dim \sigma'}}(\sigma'). \quad (4.28)$$

Since $\Delta(g)$ is obtained from $\Delta(f)$ by an explicit linear transformation, we can express this in terms of invariants of $\Delta(f)$:

$$w_{\dim \Delta(f)} = \sum_{(0,\ldots,0) \subseteq \sigma \subseteq \Delta(f)} (-1)^{\dim \Delta(f) - \dim \sigma} (\dim \sigma)! \, V_{M_{J_\sigma}}(\sigma), \quad (4.29)$$

where $J_\sigma = J \cap \sigma$.

We note an important special case of this formula. If every face of $\Delta(f)$ that contains the origin is of the form $\Delta(f_A)$ for some $A \subseteq \{k+1, \ldots, n\}$, the right-hand side of Equation (4.29) is just $v(f)$. This gives the following result.

Corollary 4.30. *Under the hypothesis of Theorem 4.17, if every face of $\Delta(f)$ that contains the origin is of the form $\Delta(f_A)$ for some $A \subseteq \{k + 1, \ldots, n\}$, then all reciprocal roots of $Q(t)$ have archimedian absolute value $q^{(\dim \Delta(f))/2}$.*

As a special case of Corollary 4.30, we note the following result.

Corollary 4.31. *If $f \in \mathbb{F}_q[x_1, \ldots, x_n]$ is nondegenerate relative to $(\Delta(f), M_J)$ and convenient, then $L(\mathbb{A}^n, f; t)^{(-1)^{n-1}}$ is a polynomial of degree $\nu(f)$ all of whose reciprocal roots have absolute value $q^{n/2}$.*

5. Examples

We explain how Theorem 4.17 implies a generalization of the result of Katz quoted in the introduction.

Proposition 5.1. *Let $f \in \mathbb{F}_q[x_1, \ldots, x_n]$ have degree $d = p^k e$, $(e, p) = 1$, and suppose that every monomial appearing in f has degree divisible by p^k. If $f^{(d)}$, the homogeneous part of f of degree d, defines a smooth hypersurface in $\mathbb{P}^{n-1}$, then $L(\mathbb{A}^n, f; t)^{(-1)^{n-1}}$ is a polynomial of degree*

$$\nu(f) = \frac{1}{p^k}((d-1)^n + (-1)^n(p^k - 1)), \tag{5.2}$$

all of whose reciprocal roots have absolute value $q^{n/2}$.

Proof. Let $\boldsymbol{e}^{(1)}, \ldots, \boldsymbol{e}^{(n)}$ denote the standard basis for $\mathbb{R}^n$. Over any sufficiently large extension field of $\mathbb{F}_q$, we can make a coordinate change on $\mathbb{A}^n$ so that f is convenient and for any $A \subseteq \{1, \ldots, n\}$, the intersection of $f^{(d)} = 0$ with the coordinate hyperplanes $\{x_i = 0\}_{i \in A}$ is smooth. In particular, the equations $f_A^{(d)} = 0$ define smooth hypersurfaces in $\mathbb{P}^{n-|A|-1}$. The Newton polyhedron $\Delta(f)$ is then the simplex in $\mathbb{R}^n$ with vertices at the origin and the points $\{d\boldsymbol{e}^{(i)}\}_{i=1}^n$. The faces of $\Delta(f)$ not containing the origin are the convex hulls of the sets $\{d\boldsymbol{e}^{(i)}\}_{i \in A}$. It will be simpler to index these faces by their complements: let σ_A denote the face which is the convex hull of $\{d\boldsymbol{e}^{(i)}\}_{i \notin A}$.

Write $f = \sum_{j \in J} a_j x^j$, J a finite subset of $\mathbb{N}^n$. Let $M \subseteq \mathbb{Z}^n$ be the subgroup

$$M = \{(u_1, \ldots, u_n) \in \mathbb{Z}^n \mid u_1 + \cdots + u_n \text{ is divisible by } p^k\}.$$

Since all monomials in f have degree divisible by p^k, it follows that $\mathbb{Z}\langle J \rangle \subseteq M$. In fact, $M_J \subseteq M$. To see this, let $(u_1, \ldots, u_n) \in M_J$. By definition, there exists an integer c prime to p such that $c(u_1, \ldots, u_n) \in \mathbb{Z}\langle J \rangle$. This implies that $c \sum_{i=1}^n u_i$ is divisible by p^k. But since $(c, p) = 1$, one has $\sum_{i=1}^n u_i$ divisible by p^k, therefore $(u_1, \ldots, u_n) \in M$.

We claim that f is nondegenerate relative to $(\Delta(f), M)$. As basis for M we take the elements

$$(p^k, 0, \ldots, 0) \cup \{(-1, 0, \ldots, 0, 1, 0, \ldots, 0)\}_{i=2}^n,$$

where the 1 occurs in the i-th position, and as basis for $L = \text{Hom}_{\mathbb{Z}}(M, \mathbb{Z})$ we take the "dual basis", namely, the linear forms

$$\ell_1(u_1, \ldots, u_n) = p^{-k}(u_1 + \cdots + u_n)$$

and

$$\ell_i(u_1, \ldots, u_n) = u_i,$$

for $i = 2, \ldots, n$. Let $A \subseteq \{1, \ldots, n\}$ and let σ_A be the face of $\Delta(f)$ defined above. Note that

$$f_{\sigma_A} := \sum_{j \in J \cap \sigma_A} a_j x^j = f_A^{(d)}.$$

We must thus check that $\{E_{\ell_i}(f_A^{(d)})\}_{i=1}^n$ have no common zero in $(\bar{\mathbb{F}}_q^\times)^n$. But

$$E_{\ell_1}(f_A^{(d)}) = e^{-1} f_A^{(d)}$$

and

$$E_{\ell_i}(f_A^{(d)}) = x_i \frac{\partial f_A^{(d)}}{\partial x_i}$$

for $i = 2, \ldots, n$, so we must show that the system

$$f_A^{(d)} = x_2 \frac{\partial f_A^{(d)}}{\partial x_2} = \cdots = x_n \frac{\partial f_A^{(d)}}{\partial x_n} = 0 \tag{5.3}$$

has no solution in $(\bar{\mathbb{F}}_q^\times)^n$. Since $p \mid d$, the Euler relation implies that any common zero of $\{x_i \partial f_A^{(d)} / \partial x_i\}_{i=2}^n$ is also a zero of $x_1 \partial f_A^{(d)} / \partial x_1$, thus the system (5.3) is equivalent to the system

$$f_A^{(d)} = x_1 \frac{\partial f_A^{(d)}}{\partial x_1} = \cdots = x_n \frac{\partial f_A^{(d)}}{\partial x_n} = 0. \tag{5.4}$$

Furthermore, x_i does not appear in f_A if $i \in A$, hence the solutions of (5.4) in $(\bar{\mathbb{F}}_q^\times)^n$ are exactly the solutions of the set

$$\{f_A^{(d)}\} \cup \{\partial f_A^{(d)} / \partial x_i\}_{i \notin A} \tag{5.5}$$

in $(\bar{\mathbb{F}}_q^\times)^n$. However, the equation $f_A^{(d)} = 0$ defines a smooth hypersurface in $\mathbb{P}^{n-|A|-1}$, so any common zero of the set (5.5) must have $x_i = 0$ for all $i \notin A$. In particular, (5.5) has no common zero in $(\bar{\mathbb{F}}_q^\times)^n$. This implies that (5.4) has no solution in $(\bar{\mathbb{F}}_q^\times)^n$, proving the nondegeneracy of f relative to $(\Delta(f), M)$.

We can now compute $\nu(f)$. By Proposition 4.5(a) we have $M = M_J$, so

$$[\mathbb{Z}^{n-|A|} : M_{J_A}] = p^k \quad \text{for all } A \neq \{1, \ldots, n\}$$

and

$$(n - |A|)! \, V(f_A)/[\mathbb{Z}^{n-|A|} : M_{J_A}] = \begin{cases} d^{n-|A|}/p^k & \text{if } A \neq \{1, \ldots, n\}, \\ 1 & \text{if } A = \{1, \ldots, n\}. \end{cases}$$

Then clearly

$$\nu(f) = \frac{1}{p^k}((d-1)^n + (-1)^n(p^k - 1))$$

and the assertions of Proposition 5.1 follow from Theorem 4.17. Finally, note that if $L(\mathbb{A}^n, f; t)^{(-1)^{n-1}}$ is a polynomial of degree (5.2) over all sufficiently large extension fields of $\mathbb{F}_q$, then the same is true over $\mathbb{F}_q$ itself. The assertion about the absolute value of the roots follows immediately from Corollary 4.31. $\qquad\square$

Remark. There are many results in the literature that, like Proposition 5.1, assert that $L(\mathbb{A}^n, f; t)^{(-1)^{n-1}}$ is a polynomial if $f^{(d)}$ defines a smooth hypersurface and some additional condition is satisfied (see [Deligne 1974, Théorème 8.4; AS 2000, Theorem 1.11 and the following remark; Katz 2005, Theorem 3.6.5; AS 2009, Theorem 3.1]). One might ask if any additional condition is really necessary. Consider the three-variable polynomial

$$f = (z^p - z) + x^{p-1}y + y^{p-1}z.$$

The homogeneous part of degree p is smooth but f has the same L-function as

$$g = x^{p-1}y + y^{p-1}z.$$

Since $\sum_{z \in \mathbb{F}_q} \Psi(y^{p-1}z) = 0$ if $y \neq 0$, one calculates that $\sum_{x,y,z \in \mathbb{F}_q} \Psi(g(x, y, z)) = q^2$. This gives $L(\mathbb{A}^3, f; t) = (1 - q^2 t)^{-1}$, showing that smoothness of $f^{(d)}$ alone is not sufficient to guarantee that $L(\mathbb{A}^n, f; t)^{(-1)^{n-1}}$ will be a polynomial.

We apply Theorem 4.17 to compute the zeta functions of some possibly singular hypersurfaces. Let $f \in \mathbb{F}_q[x_1, \ldots, x_n]$ be a homogeneous polynomial and let $X \subseteq \mathbb{P}^{n-1}$ be the hypersurface $f = 0$. Write the zeta function $Z(X/\mathbb{F}_q, t)$ of X in the form

$$Z(X/\mathbb{F}_q, t) = \frac{R(t)^{(-1)^{n-1}}}{(1-t)(1-qt)\ldots(1-q^{n-2}t)}, \qquad (5.6)$$

where $R(t)$ is a rational function. The exponential sum associated to the polynomial $yf \in \mathbb{F}_q[x_1, \ldots, x_n, y^{\pm 1}]$ can be used to count points on the projective hypersurface X. The precise relation is given in [AS 1989, Equation (6.14)]:

$$L(\mathbb{A}^n \times \mathbb{T}, yf; t)^{(-1)^n} = R(qt)^\delta. \qquad (5.7)$$

Proposition 5.8. *Suppose that $yf \in \mathbb{F}_q[x_1, \ldots, x_n, y^{\pm 1}]$ is nondegenerate relative to $(\Delta(yf), M_J)$ and convenient. Then $R(t)$ is a polynomial of degree $\nu(yf)$, all of whose reciprocal roots have absolute value $q^{(n-2)/2}$.*

Proof. The assertion about the degree of $R(t)$ follows immediately by applying Theorem 4.17 to Equation (5.7). The assertion about the absolute values of the roots of $R(t)$ follows immediately from Corollary 4.30.   □

As an illustration of Proposition 5.8, consider the projective hypersurface $X \subseteq \mathbb{P}^{n-1}$ over $\mathbb{F}_q$ defined by the homogeneous equation

$$f(x_1, \ldots, x_n) = x_1^n + \cdots + x_n^n + \lambda x_1 \ldots x_n = 0,$$

where $\lambda \in \mathbb{F}_q$. If $p \nmid n$, this hypersurface is smooth for all but finitely many values of λ. If $p \mid n$, it is a singular hypersurface for all nonzero λ (except in the cases $p = n = 2$ and $p = n = 3$). We describe the zeta function when $p \mid n$.

Corollary 5.9. *Suppose that $n = p^k e$, where $k \geq 1$ and $(p, e) = 1$, and $\lambda \neq 0$. Then $R(t)$ is a polynomial of degree*

$$\deg R(t) = (p^k - 1)e^{n-1} + e^{-1}((e-1)^n + (-1)^n(e-1)), \tag{5.10}$$

all of whose reciprocal roots have absolute value $q^{(n-2)/2}$.

Remark. Note that the second summand on the right-hand side of Equation (5.10) is the dimension of the primitive part of middle-dimensional cohomology of a smooth hypersurface of degree e. When $\lambda = 0$, the hypersurface X_0 is smooth of degree e. (It is defined by the equation $x_1^e + \cdots + x_n^e = 0$.)

Proof of Corollary 5.9. The proof is a direct application of Proposition 5.8. We sketch the details. It is straightforward to check that yf is convenient: $\Delta(yf)$ is the n-simplex in $\mathbb{R}^{n+1}$ with vertices at the origin and the points

$$(n, 0, \ldots, 0, 1), (0, n, 0, \ldots, 0, 1), \ldots, (0, \ldots, 0, n, 1),$$

and for each subset $A \subseteq \{1, \ldots, n\}$, one has $\dim \Delta(yf_A) = n - |A|$. We have

$$J = \{(n, 0, \ldots, 0, 1), (0, n, 0, \ldots, 0, 1), \ldots, (0, \ldots, 0, n, 1), (1, \ldots, 1, 1)\} \subseteq \mathbb{Z}^{n+1},$$

thus $\mathbb{R}\langle J \rangle$ is the hyperplane in $\mathbb{R}^{n+1}$ with equation $u_1 + \cdots + u_n = nv$ and the lattice $\mathbb{Z}^{n+1} \cap \mathbb{R}\langle J \rangle$ has basis

$$B = \{(1, -1, 0, \ldots, 0), (0, 1, -1, 0, \ldots, 0), \ldots, (0, \ldots, 0, 1, -1, 0), (0, \ldots, 0, n, 1)\}.$$

It follows that $n! \, V_n(yf) = n^{n-1}$. Similarly, we have

$$(n - |A|)! \, V_{n-|A|}(yf_A) = \begin{cases} n^{n-1-|A|} & \text{if } |A| \leq n - 1, \\ 1 & \text{if } |A| = n. \end{cases}$$

Let the first $n - 1$ vectors in B be denoted $\boldsymbol{a}_i$, $i = 1, \ldots, n - 1$. The lattice $\mathbb{Z}\langle J \rangle$ has basis

$$n\boldsymbol{a}_1, \ldots, n\boldsymbol{a}_{n-2}, (n-1, -1, \ldots, -1, 0), (1, \ldots, 1, 1),$$

from which it follows that M_J has basis

$$p^k a_1, \ldots, p^k a_{n-2}, (n-1, -1, \ldots, -1, 0), (1, \ldots, 1, 1). \qquad (5.11)$$

One then checks that

$$[\mathbb{Z}^{n+1} \cap \mathbb{R}\langle J \rangle : M_J] = (p^k)^{n-2}.$$

If $|A| \geq 1$, then J_A consists of vectors $(0, \ldots, 0, n, 0, \ldots, 0, 1)$ for which the n occurs in the i-th entry for $i \notin A$ (the vector $(1, \ldots, 1, 1)$ does not appear), and the calculation is easier. One gets

$$[\mathbb{Z}^{n+1} \cap \mathbb{R}\langle J_A \rangle : M_{J_A}] = \begin{cases} (p^k)^{n-2} & \text{if } A = \varnothing, \\ (p^k)^{n-1-|A|} & \text{if } 1 \leq |A| \leq n-1, \\ 1 & \text{if } A = \{1, \ldots, n\}. \end{cases}$$

We then have

$$\frac{(n-|A|)! \, V_{n-|A|}(y f_A)}{[\mathbb{Z}^{n+1} \cap \mathbb{R}\langle J_A \rangle : M_{J_A}]} = \begin{cases} p^k e^{n-1} & \text{if } A = \varnothing, \\ e^{n-1-|A|} & \text{if } 1 \leq |A| \leq n-1, \\ 1 & \text{if } A = \{1, \ldots, n\}. \end{cases}$$

It is now straightforward to check that $\nu(yf)$ equals the expression on the right-hand side of (5.10).

It remains to check that yf is nondegenerate relative to $(\Delta(yf), M_J)$. The dual basis of the basis (5.11) for M_J is the set of linear forms

$$\ell_i(u_1, \ldots, u_n, v) = \sum_{j=1}^{i} \frac{1}{p^k} u_j + \frac{n-i}{p^k} u_n - ev, \quad i = 1, \ldots, n-2,$$

$$\ell_{n-1}(u_1, \ldots, u_n, v) = -u_n + v,$$

$$\ell_n(u_1, \ldots, u_n, v) = v.$$

The polynomials $(yf)_\sigma$ for faces σ of $\Delta(yf)$ that do not contain the origin are exactly the polynomials yf_A for $A \subset \{1, \ldots, n\}$, $|A| < n$. If $A = \varnothing$, we have

$$E_{\ell_n}(yf) - E_{\ell_{n-1}}(yf) = \lambda y x_1 \ldots x_n,$$

which has no zero in $(\bar{\mathbb{F}}_q^\times)^{n+1}$. So suppose that $1 \leq |A| \leq n-1$. Then

$$y f_A = \sum_{i \notin A} y x_i^n.$$

Suppose first that $n \notin A$. If $1 \in A$, then

$$E_{\ell_1}(y f_A) + e E_{\ell_n}(y f_A) = -e y x_n^n,$$

and if $i \in A$ for some i, $2 \le i \le n - 2$, then

$$E_{\ell_i}(yf_A) - E_{\ell_{i-1}}(yf_A) = -eyx_n^n.$$

Neither of these monomials vanishes on $(\bar{\mathbb{F}}_q^\times)^{n+1}$. If $i \notin A$ for all $i = 1, \ldots, n-2$, then $A = \{n - 1\}$. In this case we have

$$E_{\ell_1}(yf_A) + eE_{\ell_n}(yf_A) = ey(x_1^n - x_n^n),$$
$$E_{\ell_i}(yf_A) - E_{\ell_{i-1}}(yf_A) = ey(x_i^n - x_n^n) \quad \text{for } i = 2, \ldots, n-2,$$
$$E_{\ell_n}(yf_A) = y(x_1^n + \ldots + x_{n-2}^n + x_n^n).$$

If the first $n - 2$ expressions vanish, then $yx_1^n = \cdots = yx_{n-2}^n = yx_n^n$. The vanishing of the last expression is then equivalent to $(n - 1)yx_n^n = 0$, which is impossible in $(\bar{\mathbb{F}}_q^\times)^{n+1}$.

Now suppose that $n \in A$. If $1 \notin A$, then

$$E_{\ell_1}(yf_A) + eE_{\ell_n}(yf_A) = eyx_1^n,$$

and if $i \notin A$ for some i, $2 \le i \le n - 2$, then

$$E_{\ell_i}(yf_A) - E_{\ell_{i-1}}(yf_A) = eyx_i^n.$$

Neither of these monomials vanishes on $(\bar{\mathbb{F}}_q^\times)^{n+1}$. If $i \in A$ for $i = 1, \ldots, n-2$, then A contains all indices except $i = n - 1$ and $E_{\ell_n}(yf_A) = yx_{n-1}^n$, which does not vanish on $(\bar{\mathbb{F}}_q^\times)^{n+1}$.

Thus yf satisfies the hypotheses of Proposition 5.8. $\square$

Acknowledgements

References

[AS 1987a] A. Adolphson and S. Sperber, "Newton polyhedra and the degree of the L-function associated to an exponential sum", *Invent. Math.* **88**:3 (1987), 555–569. MR 89d:11064 Zbl 0623.12012

[AS 1987b] A. Adolphson and S. Sperber, "p-adic estimates for exponential sums and the theorem of Chevalley–Warning", *Ann. Sci. École Norm. Sup.* (4) **20**:4 (1987), 545–556. MR 89d:11112 Zbl 0654.12011

[AS 1989] A. Adolphson and S. Sperber, "Exponential sums and Newton polyhedra: cohomology and estimates", *Ann. of Math.* (2) **130**:2 (1989), 367–406. MR 91e:11094 Zbl 0723.14017

[AS 1990a] A. Adolphson and S. Sperber, "p-adic estimates for exponential sums", pp. 11–22 in *p-adic analysis* (Trento, 1989), edited by F. Baldassarri et al., Lecture Notes in Math. **1454**, Springer, Berlin, 1990. MR 92d:11086 Zbl 0727.11056

[AS 1990b] A. Adolphson and S. Sperber, "Exponential sums on $(\mathbf{G}_m)^n$", *Invent. Math.* **101**:1 (1990), 63–79. MR 92c:11083 Zbl 0764.11037

[AS 2000] A. Adolphson and S. Sperber, "Exponential sums on $\mathbf{A}^n$. III", *Manuscripta Math.* **102**:4 (2000), 429–446. MR 2002g:11124 Zbl 0987.11076

[AS 2009] A. Adolphson and S. Sperber, "Exponential sums on $\mathbf{A}^n$, IV", *Int. J. Number Theory* **5**:5 (2009), 747–764. Zbl 05603968

[Ax 1964] J. Ax, "Zeroes of polynomials over finite fields", *Amer. J. Math.* **86** (1964), 255–261. MR 28 #3986 Zbl 0121.02003

[Deligne 1974] P. Deligne, "La conjecture de Weil, I", *Inst. Hautes Études Sci. Publ. Math.* **43** (1974), 273–307. MR 49 #5013 Zbl 0287.14001

[Denef and Loeser 1991] J. Denef and F. Loeser, "Weights of exponential sums, intersection cohomology, and Newton polyhedra", *Invent. Math.* **106**:2 (1991), 275–294. MR 93a:14019 Zbl 0763.14025

[Dwork 1962] B. Dwork, "On the zeta function of a hypersurface", *Inst. Hautes Études Sci. Publ. Math.* **12** (1962), 5–68. MR 28 #3039 Zbl 0173.48601

[Katz 2005] N. M. Katz, *Moments, monodromy, and perversity: a Diophantine perspective*, Annals of Mathematics Studies **159**, Princeton University Press, Princeton, NJ, 2005. MR 2006j:14020 Zbl 1079.14025

[Katz 2007] N. Katz, "Another look at the Dwork family", preprint, 2007, Available at http://www.math.princeton.edu/~nmk/dworkfam64.pdf.

[Kouchnirenko 1976] A. G. Kouchnirenko, "Polyèdres de Newton et nombres de Milnor", *Invent. Math.* **32**:1 (1976), 1–31. MR 54 #7454 Zbl 0328.32007

[Libgober and Sperber 1995] A. Libgober and S. Sperber, "On the zeta function of monodromy of a polynomial map", *Compositio Math.* **95**:3 (1995), 287–307. MR 96b:14022 Zbl 0968.14006

[Monsky 1970] P. Monsky, *p-adic analysis and zeta functions*, Lectures in Mathematics, Department of Mathematics, Kyoto University **4**, Kinokuniya Book-Store Co. Ltd., Tokyo, 1970. MR 44 #215 Zbl 0256.14009

[Moreno et al. 2004] O. Moreno, K. W. Shum, F. N. Castro, and P. V. Kumar, "Tight bounds for Chevalley–Warning–Ax–Katz type estimates, with improved applications", *Proc. London Math. Soc.* (3) **88**:3 (2004), 545–564. MR 2005g:11114 Zbl 1102.11032

[Rojas-León 2006] A. Rojas-León, "Purity of exponential sums on $\mathbb{A}^n$", *Compos. Math.* **142**:2 (2006), 295–306. MR 2007e:11091 Zbl 05033723

[Rojas-León and Wan 2007] A. Rojas-León and D. Wan, "Moment zeta functions for toric Calabi–Yau hypersurfaces", *Commun. Number Theory Phys.* **1**:3 (2007), 539–578. MR 2008m:11126 Zbl 05608723

[Serre 1962] Jean-Pierre. Serre, "Endomorphismes complètement continus des espaces de Banach p-adiques", *Inst. Hautes Études Sci. Publ. Math.* **12** (1962), 69–85. MR 26 #1733 Zbl 0104.33601

[Wan 1993] D. Q. Wan, "Newton polygons of zeta functions and L functions", *Ann. of Math.* (2) **137**:2 (1993), 249–293. MR 94f:11074 Zbl 0799.11058

adolphs@math.okstate.edu　　*Department of Mathematics, Oklahoma State University, Stillwater, OK 74078, United States*

sperber@math.umn.edu　　*School of Mathematics, University of Minnesota, Minneapolis, MN 55455, United States*

Algebra & Number Theory

www.jant.org

Algebra & Number Theory

Volume 3   No. 8   2009